The Synchronization Experts.

HANDBUCH

LTOS 7.10

LANTIME Operating System Firmware
Konfiguration und
Management Handbuch

Meinberg Funkuhren GmbH & Co. KG

Inhaltsverzeichnis

1 Impressum

Herausgeber

Meinberg Funkuhren GmbH & Co. KG

Firmenanschrift:
Lange Wand 9
31812 Bad Pyrmont
Deutschland

Telefon:
+49 (0) 52 81 / 93 09 - 0

Telefax:
+49 (0) 52 81 / 93 09 - 230

Das Unternehmen wird im Handelsregister A des Amtgerichts Hannover unter der Nummer

17HRA 100322

geführt.

Geschäftsleitung:	Heiko Gerstung Andre Hartmann Natalie Meinberg Daniel Boldt
Internet:	https://www.meinberg.de
E-Mail:	info@meinberg.de

Veröffentlichungsinformationen

Handbuch-Version:	1.0
Revisionsdatum:	2025-09-25
PDF-Exportdatum:	2025-09-25

2 Urheberrecht und Haftungsausschluss

Die Inhalte dieses Dokumentes, soweit nicht anders angegeben, einschließlich Text und Bilder jeglicher Art sowie Übersetzungen von diesen, sind das geistige Eigentum von Meinberg Funkuhren GmbH & Co. KG (im Folgenden: „Meinberg“) und unterliegen dem deutschen Urheberrecht. Jegliche Vervielfältigung, Verbreitung, Anpassung und Verwertung ist ohne die ausdrückliche Zustimmung von Meinberg nicht gestattet. Die Regelungen und Vorschriften des Urheberrechts gelten entsprechend.

Inhalte Dritter sind in Übereinstimmung mit den Rechten und mit der Erlaubnis des jeweiligen Urhebers bzw. Copyright-Inhabers in dieses Dokument eingebunden.

Eine nicht ausschließliche Lizenz wird für die Weiterveröffentlichung dieses Dokumentes gewährt (z. B. auf einer Webseite für die kostenlose Bereitstellung von diversen Produkthandbüchern), vorausgesetzt, dass das Dokument nur im Ganzen weiter veröffentlicht wird, dass es in keiner Weise verändert wird, dass keine Gebühr für den Zugang erhoben wird und dass dieser Hinweis unverändert und ungekürzt erhalten bleibt.

Zur Zeit der Erstellung dieses Dokuments wurden zumutbare Anstrengungen unternommen, Links zu Webseiten Dritter zu prüfen, um sicherzustellen, dass diese mit den Gesetzen der Bundesrepublik Deutschland konform sind und relevant zum Dokumentinhalt sind. Meinberg übernimmt keine Haftung für die Inhalte von Webseiten, die nicht von Meinberg erstellt und unterhalten wurden bzw. werden. Insbesondere kann Meinberg nicht gewährleisten, dass solche externen Inhalte geeignet oder passend für einen bestimmten Zweck sind.

Meinberg ist bemüht, ein vollständiges, fehlerfreies und zweckdienliches Dokument bereitzustellen, und in diesem Sinne überprüft das Unternehmen seinen Handbuchbestand regelmäßig, um Weiterentwicklungen und Normänderungen Rechnung zu tragen. Dennoch kann Meinberg nicht gewährleisten, dass dieses Dokument aktuell, vollständig oder fehlerfrei ist. Aktualisierte Handbücher werden unter **https://www.meinberg.de** sowie **https://www.meinberg.support** bereitgestellt.

Sie können jederzeit eine aktuelle Version des Dokuments anfordern, indem Sie **techsupport@meinberg.de** anschreiben. Verbesserungsvorschläge und Hinweise auf Fehler erhalten wir ebenfalls gerne über diese Adresse.

Meinberg behält sich jederzeit das Recht vor, beliebige Änderungen an diesem Dokument vorzunehmen, sowohl zur Verbesserung unserer Produkte und Serviceleistungen als auch zur Sicherstellung der Konformität mit einschlägigen Normen, Gesetzen und Regelungen.

3 Revisionshistorie

Dieser Revisionsverlauf beschreibt initial die Änderungen im Vergleich zum LTOS 7.08 Handbuch.

Version	Datum	Änderungsnotiz
1.0	20.09.20245	Basisversion **Hinweise zur Datensicherheit- und Zugriffsskontrolle** → Kapitel 4.3, „Darstellung von sonstigen Informationen“ → Kapitel 10, „LANTIME Inbetriebnahme“ Benutzerhandbuch Sicherheit überarbeitet → Kapitel 11, „Benutzerhandbuch Sicherheit“ **Seite „System“ - Neustrukturierung des Menüs Konfiguration & Firmware Management** → Kapitel 13.1.9.15, „Konfigurationsmanagement“ → Kapitel 13.1.9.14, „Firmwareverwaltung“ **Erzwungene Passwortänderung beim erstmaligem Login** → Kapitel 10, „LANTIME Inbetriebnahme“ **Bearer Token Management im Menü „Benutzerverwaltung“** → Kapitel 13.1.9.11, „Bearer Token Management“ **Signalausgänge der PSX210 jetzt konfigurierbar** → Kapitel 13.1.7.13, „Option: Konfiguration Ausgänge“ **Technische Daten für PCTEL L1-Band-Antenne entfernt** → Kapitel 16.2, „Technische Daten - Antennen für LANTIME-Systeme“

4 Darstellungsmethoden in diesem Handbuch

4.1 Darstellung von kritischen Sicherheitswarnhinweisen

Sicherheitsrisiken werden mit Warnhinweisen mit den folgenden Signalwörtern, Farben und Symbolen angezeigt:

Vorsicht!

Das Signalwort bezeichnet eine Gefährdung mit einem **niedrigen Risikograd**. Dieser Hinweis macht auf einen Bedienungsablauf, eine Vorgehensweise oder Ähnliches aufmerksam, deren Nichtbefolgung bzw. Nichtausführung zu **leichten Verletzungen** führen kann.

Warnung!

Das Signalwort bezeichnet eine Gefährdung mit einem **mittleren Risikograd**. Dieser Hinweis macht auf einen Bedienungsablauf, eine Vorgehensweise oder Ähnliches aufmerksam, deren Nichtbefolgung bzw. Nichtausführung zu **schweren Verletzungen, unter Umständen mit Todesfolge**, führen kann.

Gefahr!

Das Signalwort bezeichnet eine Gefährdung mit einem **hohen Risikograd**. Dieser Hinweis macht auf einen Bedienungsablauf, eine Vorgehensweise oder Ähnliches aufmerksam, deren Nichtbefolgung bzw. Nichtausführung zu **schweren Verletzungen, unter Umständen mit Todesfolge**, führt.

4.2 Ergänzende Symbole bei Warnhinweisen

An manchen Stellen werden Warnhinweise mit einem zweiten Symbol versehen, welches die Besonderheiten einer Gefahrenquelle verdeutlicht.

Das Symbol „elektrische Gefahr“ weist auf eine Stromschlag- oder Blitzeinschlaggefahr hin.

Das Symbol „Absturzgefahr“ weist auf eine Sturzgefahr hin, die bei Höhenarbeit besteht.

Das Symbol „Laserstrahlung“ weist auf eine Gefahr in Verbindung mit Laserstrahlung hin.

4.3 Darstellung von sonstigen Informationen

Über die vorgenannten personensicherheitsbezogenen Warnhinweise hinaus enthält das Handbuch ebenfalls Warn- und Informationshinweise, die Risiken von Produktschäden, Datenverlust, Risiken für die Informationssicherheit beschreiben, sowie allgemeine Informationen bereitstellen, die der Aufklärung und einem einfacheren und optimalen Betrieb dienlich sind. Diese werden wie folgt dargestellt:

Achtung!

Mit solchen Warnhinweisen werden Risiken von Produktschäden, Datenverlust sowie Risiken für die Informationssicherheit beschrieben.

Hinweis:

In dieser Form werden zusätzliche Informationen bereitgestellt, die für eine komfortablere Bedienung sorgen oder mögliche Missverständnisse ausschließen sollen.

Cyber-Sicherheitshinweis

Mit solchen Warnhinweisen werden Cybersicherheitsrisiken aufgezeigt, die unter Umständen unautorisierten Personen Zugang über Kommunikationsschnittstellen auf Ihr Gerät gewähren können und die entsprechend anhand geeigneten administrativen oder sonstigen physischen Maßnahmen minimiert werden müssen. Solche Risiken können inhärent im System liegen oder aus einer unfachgerechten Systemkonfiguration entstehen.

4.4 Allgemein verwendete Symbole

In diesem Handbuch und auf dem Produkt werden auch in einem breiteren Zusammenhang folgende Symbole und Piktogramme verwendet.

Das Symbol „ESD“ weist auf ein Risiko von Produktschäden durch elektrostatische Entladungen hin.

Gleichstrom *(Symboldefinition IEC 60417-5031)*

Wechselstrom *(Symboldefinition IEC 60417-5032)*

Erdungsanschluss *(Symboldefinition IEC 60417-5017)*

Schutzleiteranschluss *(Symboldefinition IEC 60417-5019)*

Alle Stromversorgungsstecker ziehen *(Symboldefinition IEC 60417-6172)*

5 Wichtige Sicherheitshinweise

Die in diesem Kapitel enthaltenen Sicherheitshinweise sowie die besonders ausgezeichneten Warnhinweise, die in diesem Handbuch an relevanten Stellen aufgeführt werden, müssen in allen Installations-, Inbetriebnahme-, Betriebs- und Außerbetriebnahmephasen des Gerätes beachtet werden.

Beachten Sie außerdem die am Gerät selbst angebrachten Sicherheitshinweise.

Die Nichtbeachtung von diesen Sicherheitshinweisen und Warnhinweisen sowie sonstigen sicherheitskritischen Betriebsanweisungen in den Handbüchern zum Produkt oder eine unsachgemäße Verwendung des Produktes kann zu einem unvorhersehbaren Produktverhalten führen mit eventueller Verletzungsgefahr oder Todesfolge.

In Abhängigkeit von Ihrer Gerätekonfiguration oder den installierten Optionen sind einige Sicherheitshinweise eventuell für Ihr Gerät nicht anwendbar.

Meinberg übernimmt keine Verantwortung für Personenschäden, die durch Nichtbeachtung der Sicherheitshinweise, Warnhinweise und sicherheitskritischen Betriebsanweisungen in den Produkthandbüchern entstehen.

Die Sicherheit und der fachgerechte Betrieb des Produktes liegen in der Verantwortung des Betreibers!

Falls Sie weitere Hilfe oder Beratung zur Sicherheit Ihres Produktes benötigen, steht Ihnen der Technische Support von Meinberg jederzeit unter techsupport@meinberg.de zur Verfügung.

5.1 Bestimmungsgemäße Verwendung

Das Gerät darf nur bestimmungsgemäß verwendet werden! Die maßgebliche bestimmungsgemäße Verwendung wird ausschließlich in diesem Handbuch, sowie in der sonstigen, einschlägigen und direkt von Meinberg bereitgestellten Dokumentation beschrieben.

Zur bestimmungsgemäßen Verwendung gehört insbesondere die Beachtung von spezifizierten Grenzwerten! Diese Grenzwerte dürfen nicht über- bzw. unterschritten werden!

5.2 Produktdokumentation

Die Informationen in diesem Handbuch sind für eine sicherheitstechnisch kompetente Leserschaft bestimmt.

Als kompetente Leserschaft gelten:

- **Fachkräfte**, die mit den einschlägigen nationalen Sicherheitsnormen und Sicherheitsregeln vertraut sind, sowie
- **unterwiesene Personen**, die durch eine Fachkraft eine Unterweisung über die einschlägigen nationalen Sicherheitsnormen und Sicherheitsregeln erhalten haben.

Lesen Sie das Handbuch vor der Inbetriebnahme des Produktes achtsam und vollständig.

Wenn bestimmte Sicherheitsinformationen in der Produktdokumentation für Sie nicht verständlich sind, fahren Sie **nicht** mit der Inbetriebnahme bzw. mit dem Betrieb des Gerätes fort!

Sicherheitsvorschriften werden regelmäßig angepasst und Meinberg aktualisiert die entsprechenden Sicherheitshinweise und Warnhinweisen, um diesen Änderungen Rechnung zu tragen. Es wird somit empfohlen, die Meinberg-Webseite https://www.meinberg.de bzw. das Meinberg Customer Portal https://www.meinberg.support zu besuchen, um aktuelle Handbücher herunterzuladen.

Bitte bewahren Sie die gesamte Dokumentation für das Produkt (auch dieses Handbuch) in einem digitalen oder gedruckten Format sorgfältig auf, damit sie immer leicht zugänglich ist.

Meinbergs Technischer Support steht ebenfalls unter techsupport@meinberg.de jederzeit zur Verfügung, falls Sie weitere Hilfe oder Beratung zur Sicherheit Ihres Meinberg-Produkts benötigen.

5.3 Sicherheit bei der Installation

Dieses Einbaugerät wurde entsprechend den Anforderungen des Standards IEC 62368-1 (*Geräte der Audio-/Video-, Informations- und Kommunikationstechnik—Teil 1: Sicherheitsanforderungen*) entwickelt und geprüft. Bei Verwendung des Einbaugerätes in einem Endgerät (z. B. Gehäuseschrank) sind zusätzliche Anforderungen gemaß Standard IEC 62368-1 zu beachten und einzuhalten. Insbesondere sind die allgemeinen Anforderungen und die Sicherheit von elektrischen Einrichtungen (z. B. IEC, VDE, DIN, ANSI) sowie die jeweils gültigen nationalen Normen einzuhalten.

Das Gerät wurde für den Einsatz in einer industriellen oder kommerziellen Umgebung entwickelt und darf auch nur in diesen betrieben werden. Für Umgebungen mit höherem Verschmutzungsgrad gemäß Standard IEC 60664-1 sind zusätzliche Maßnahmen erforderlich, wie z. B. Einbau in einem klimatisierten Schaltschrank.

Wenn das Gerät aus einer kalten Umgebung in den Betriebsraum gebracht wird, kann Feuchtigkeit durch Kondensierung entstehen. Warten Sie, bis das Gerät an die Raumtemperatur angeglichen und absolut trocken ist, bevor Sie es in Betrieb nehmen.

Beachten Sie bei dem Auspacken, Aufstellen und vor Betrieb des Geräts unbedingt die Anleitung zur Hardware-Installation und die technischen Daten des Geräts, insbesondere Abmessungen, elektrische Kennwerte und notwendige Umgebungs- und Klimabedingungen.

Der Brandschutz muss im eingebauten Zustand sichergestellt sein. Verschließen oder verbauen Sie daher niemals Lüftungslöcher und/oder Ein- oder auslässe aktiver Lüfter.

Das Gerät mit der höchsten Masse muss in der niedrigsten Position eines Racks eingebaut werden, um den Gewichtsschwerpunkt des Gesamtracks möglichst tief zu verlagern und die Umkippgefahr zu minimieren. Weitere Geräte sind von unten nach oben zu platzieren.

Das Gerät muss vor mechanischen Beanspruchungen wie Vibrationen oder Schlag geschützt angebracht werden.

Bohren Sie **niemals** Löcher in das Gehäuse zur Montage! Haben Sie Schwierigkeiten mit der Rackmontage, kontaktieren Sie den Technischen Support von Meinberg für weitere Hilfe!

Prüfen Sie das Gehäuse vor der Installation. Bei der Montage darf das Gehäuse keine Beschädigungen aufweisen.

5.4 Elektrische Sicherheit

Dieses Meinberg-Produkt wird an einer gefährlichen Spannung betrieben.

Die Inbetriebnahme und der Anschluss des Meinberg-Produktes darf nur von einer Fachkraft mit entsprechender Eignung durchgeführt werden, oder von einer Person, die von einer Fachkraft entsprechend unterwiesen wurde.

Die Konfektionierung von speziellen Kabeln darf nur von einer Elektrofachkraft durchgeführt werden.

Arbeiten Sie **niemals** an stromführenden Kabeln!

Verwenden Sie **niemals** Kabel, Stecker und Buchsen, die sichtbar bzw. bekanntlich defekt sind! Der Einsatz von defekten, beschädigten oder unfachgerecht angeschlossenen Schirmungen, Kabeln, Steckern oder Buchsen kann zu einem Stromschlag führen mit eventueller Verletzungs- oder gar Todesfolge und stellt möglicherweise auch eine Brandgefahr dar!

Stellen Sie vor dem Betrieb sicher, dass alle Kabel und Leitungen einwandfrei sind. Achten Sie insbesondere darauf, dass die Kabel keine Beschädigungen (z. B. Knickstellen) aufweisen, dass sie durch die Installationslage nicht beschädigt werden, dass sie nicht zu kurz um Ecken herum gelegt werden und dass keine Gegenstände auf den Kabeln stehen.

Verlegen Sie die Leitungen so, dass sie keine Stolpergefahr darstellen.

Die Stromversorgung sollte mit einer kurzen, induktivitätsarmen Leitung angeschlossen werden. Vermeiden Sie nach Möglichkeit den Einsatz von Steckdosenleisten oder Verlängerungskabel. Ist der Einsatz einer solchen Vorrichtung unumgänglich, stellen Sie sicher, dass sie für die Bemessungsströme aller angeschlossenen Geräte ausdrücklich ausgelegt ist.

Niemals während eines Gewitters Strom-, Signal- oder Datenübertragungsleitungen anschließen oder lösen, sonst droht Verletzungs- oder Lebensgefahr, weil sehr hohe Spannungen bei einem Blitzschlag auf der Leitung auftreten können!

Bei dem Verkabeln der Geräte müssen die Kabel in der Reihenfolge der Anordnung angeschlossen bzw. gelöst werden, die in der zum Gerät gehörenden Benutzerdokumentation beschrieben ist. Stellen Sie alle Kabelverbindungen zum Gerät im stromlosen Zustand her, ehe Sie die Stromversorgung zuschalten.

Ziehen Sie **immer** Stecker an **beiden** Enden ab, bevor Sie an Steckern arbeiten! Der unsachgemäße Anschluss oder Trennung des Meinberg-Systems kann zu Stromschlag führen mit eventueller Verletzungs- oder gar Todesfolge!

Bei dem Abziehen eines Steckers ziehen Sie **niemals** am Kabel selbst! Durch das Ziehen am Kabel kann sich das Kabel vom Stecker lösen oder der Stecker selbst beschädigt werden. Es besteht hierdurch die Gefahr von direktem Kontakt mit stromführenden Teilen.

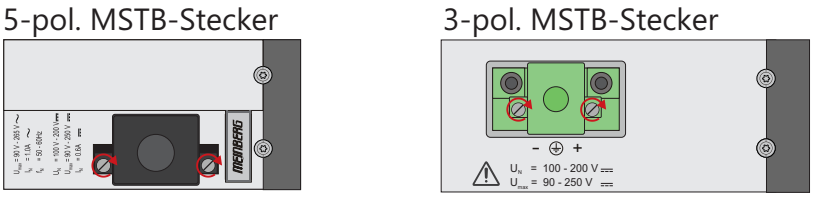


Abb.: Schraubverriegelung von MSTB-Steckern am Beispiel eines LANTIME M320

Achten Sie darauf, dass alle Steckverbindungen fest sitzen. Insbesondere bei dem Einsatz von Steckverbindern mit Schraubverriegelung, stellen Sie sicher, dass die Sicherungsschrauben fest angezogen sind. Das gilt insbesondere für die Stromversorgung, bei der 3-pol. MSTB und 5-pol. MSTB-Verbindungen (siehe Abbildung) mit Schraubverriegelung zum Einsatz kommen.

Vor dem Anschluss an die Spannungsversorgung muss zur Erdung des Gehäuses ein Erdungskabel an den Erdungsanschluss des Gerätes angeschlossen werden.

Es muss sichergestellt werden, dass bei der Montage im Schaltschrank keine Luft- und Kriechstrecken zu benachbarten spannungsführenden Teilen unterschritten werden oder Kurzschlüsse verursacht werden.

Achten Sie darauf, dass keine Gegenstände oder Flüssigkeiten in das Innere des Geräts gelangen!

Im Störfall oder bei Servicebedarf (z. B. bei beschädigten Gehäuse oder Netzkabel oder bei dem Eindringen von Flüssigkeiten oder Fremdkörpern), kann der Stromfluss unterbrochen werden. In solchen Fällen muss das Gerät sofort physisch von allen Stromversorgungen getrennt werden. Die Spannungsfreiheit muss wie folgt sichergestellt werden:

- Ziehen Sie den Stromversorgungsstecker von der Stromquelle.
- Lösen Sie die Sicherungsschrauben des geräteseitigen MSTB-Stromversorgungsstecker und ziehen Sie ihn vom Gerät.
- Verständigen Sie den Verantwortlichen für Ihre elektrische Installation.
- Wenn Ihr Gerät über eine oder mehrere Unterbrechungsfreie Stromversorgungen (USV) angeschlossen ist, muss die direkte Stromversorgungsverbindung zwischen dem Gerät und der USV zuerst getrennt werden.

5.4.1 Spezielle Informationen zu Geräten mit AC-Stromversorgung

Das Gerät ist ein Gerät der Schutzklasse 1 und darf nur an eine geerdete Steckdose angeschlossen werden (TN-System).

Zum sicheren Betrieb muss das Gerät durch eine Installationssicherung von max. 20 A abgesichert und mit einem Fehlerstromschutzschalter, gemäß den jeweils gültigen nationalen Normen, ausgestattet sein.

Die Trennung des Gerätes von der Netzspannung muss immer an der Steckdose und nicht am Gerät erfolgen.

Stellen Sie sicher, dass der Anschluss am Gerät oder die Netzsteckdose der Hausinstallation dem Benutzer frei zugänglich ist, damit in Notfall das Netzkabel aus der Steckdose gezogen werden kann.

Nichtkonforme Netzleitungen und nicht fachgerecht geerdete Netzsteckdosen stellen eine elektrische Gefährdung dar!

Geräte mit Netzstecker dürfen nur mit einer sicherheitsgeprüften Netzleitung des Einsatzlandes an eine vorschriftsmäßig geerdete Schutzkontakt-Steckdose angeschlossen werden.

5.4.2 Spezielle Informationen zu Geräten mit DC-Stromversorgung

Das Gerät muss nach den Bestimmungen der IEC 62368-1 außerhalb der Baugruppe spannungslos schaltbar sein (z. B. durch den primärseitigen Leitungsschutz).

Montage und Demontage des Steckers zur Spannungsversorgung ist nur bei spannungslos geschalteter Baugruppe erlaubt (z. B. durch den primärseitigen Leitungsschutz).

Die Zuleitungen sind ausreichend abzusichern und zu dimensionieren mit einem Anschlussquerschnitt von 1 mm^2 – 2,5 mm^2 / 17 AWG – 13 AWG).

Die Versorgung des Gerätes muss über eine geeignete Trennvorrichtung (Schalter) erfolgen. Die Trennvorrichtung muss gut zugänglich in der Nähe des Gerätes angebracht werden und als Trennvorrichtung für das Gerät gekennzeichnet sein.

5.5 Schutzleiter-/ Erdungsanschluss

Um einen sicheren Betrieb zu gewährleisten und um die Anforderungen der IEC 62368-1 zu erfüllen, muss das Gerät über die Schutzleiteranschlussklemme korrekt mit dem Schutzerdungsleiter verbunden werden.

Ist ein externer Erdungsanschluss am Gehäuse vorgesehen, muss dieser aus Sicherheitsgründen vor dem Anschluss der Spannungsversorgung mit der Potentialausgleichsschiene (Erdungsschiene) verbunden werden. Eventuell auftretender Fehlerstrom auf dem Gehäuse wird so sicher in die Erde abgeleitet.

Die für die Montage des Erdungskabels notwendige Schraube, Unterlegscheibe und Zahnscheibe befinden sich am Erdungspunkt des Gehäuses. Ein Erdungskabel ist nicht im Lieferumfang enthalten.

Bitte verwenden Sie ein Erdungskabel mit Querschnitt $\geq$ 1.5 mm^2, sowie eine passende Erdungsklemme/-öse. Achten Sie stets auf eine korrekte Crimpverbindung!

5.6 Sicherheitshinweise SFP-Module

Die von Meinberg empfohlenen optischen SFP-Module sind mit einem Klasse-1-Laser ausgestattet.

- Nur optische SFP-Module verwenden, die der Laser Klasse 1 des IEC Standard 60825-1 entsprechen. Optische Produkte, die diesem Standard nicht entsprechen, können Strahlungen erzeugen, die zu Augenverletzungen führen können.
- Niemals in das offene Ende eines Glasfaserkabels oder einer offenen Anschlussbuchse schauen.
- Unbenutzte Steckverbinder optischer Schnittstellen sollten stets mit einer passenden Schutzkappe versehen werden.
- Die Sicherheitshinweise und Herstellerangaben der verwendeten SFP-Module sind zu beachten.
- Das eingesetzte SFP-Modul muss den Schutz gegen transiente Spannungen gemäß IEC 62368-1 gewährleisten.
- Das eingesetzte SFP-Modul muss nach den geltenden Normen geprüft und zertifiziert sein.

5.7 Sicherheitshinweise für faseroptische Anschlüsse

Das Gerät ist mit faseroptischen Anschlüssen ausgestattet.

Niemals in das offene Ende eines Glasfaserkabels oder einer offenen Anschlussbuchse schauen.

Unbenutzte Steckverbinder optischer Schnittstellen sollten stets mit einer passenden Schutzkappe versehen werden.

5.8 Sicherheit bei der Pflege und Wartung

Reinigen Sie das Gerät ausschließlich mit einem weichen, trockenen Tuch.

Niemals das Gerät nass (z. B. mit Löse- oder Reinigungsmittel) reinigen! In das Gehäuse eindringende Flüssigkeiten können einen Kurzschluss verursachen, der wiederum zu einem Brand oder Stromschlag führen kann!

Weder das Gerät noch dessen Unterbaugruppen dürfen geöffnet werden. Reparaturen am Gerät oder Unterbaugruppen dürfen nur durch den Hersteller oder durch autorisiertes Personal durchgeführt werden. Durch unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen!

Öffnen Sie insbesondere **niemals** ein Netzteil, da auch nach Trennung von der Spannungsversorgung gefährliche Spannungen im Netzteil auftreten können. Ist ein Netzteil z. B. durch einen Defekt nicht mehr funktionsfähig, so schicken Sie es für etwaige Reparaturen an Meinberg zurück.

Einige Geräteteile können während des Betriebs sehr warm werden. Berühren Sie nicht diese Oberflächen!

Sind Wartungsarbeiten am Gerät auszuführen, obwohl das Gerätegehäuse noch warm ist, schalten Sie das Gerät vorher aus und lassen Sie es abkühlen.

5.9 Sicherheit mit Batterien

Die integrierte CR2032-Lithiumbatterie hat eine Lebensdauer von mindestens 10 Jahren.

Sollte ein Austausch erforderlich werden, sind folgende Hinweise zu beachten:

- Die Batterie darf nur mit demselben oder einem vom Hersteller empfohlenen gleichwertigen Typ ersetzt werden.
- Ein Austausch der Lithiumbatterie darf nur vom Hersteller oder autorisiertem Fachpersonal vorgenommen werden.
- Die Batterie darf nur dem vom Batteriehersteller angegebenen Luftdruck ausgesetzt werden.

Eine unsachgemäße Handhabung der Batterie kann zu einer Explosion oder zu einem Austritt von entflammbaren oder ätzenden Flüssigkeiten oder Gasen führen.

- **Niemals** die Batterie kurzschließen!
- **Niemals** versuchen, die Batterie wiederaufzuladen!
- **Niemals** die Batterie ins Feuer werfen oder im Ofen entsorgen!
- **Niemals** die Batterie mechanisch zerkleinern!

6 Wichtige Produkthinweise

6.1 Optimaler Betrieb des Geräts

- Achten Sie darauf, dass die Lüftungsschlitze nicht zugestellt werden bzw. verstauben, da sich sonst ein Wärmestau im Gerät während des Betriebes entwickeln kann. Auch wenn das System dafür ausgelegt ist, sich automatisch bei einer zu hohen Temperatur abzuschalten, kann das Risiko von Störungen im Betrieb und Produktschäden bei einer Überhitzung nicht ganz ausgeschlossen werden.
- Der bestimmungsgemäße Betrieb und die Einhaltung der EMV-Grenzwerte (Elektromagnetische Verträglichkeit) sind nur bei ordnungsgemäß montiertem Gehäusedeckel gewährleistet. Nur so werden Anforderungen bezüglich Kühlung, Brandschutz und die Abschirmung gegenüber elektrischen und (elektro)magnetischen Feldern entsprochen.

6.2 Wartungsarbeiten und Änderungen am Produkt

Achtung!

Es wird empfohlen, eine Kopie von gespeicherten Konfigurationsdaten zu erstellen (z. B. auf einem USB-Stick über das Webinterface), bevor Sie Wartungsarbeiten oder zugelassene Änderungen am Meinberg-System durchführen.

6.2.1 Batteriewechsel

Die Referenzuhr Ihres Meinberg-Systems ist mit einer Lithiumbatterie (Typ CR2032) ausgestattet, die für die lokale Speicherung der Almanach-Daten und den weiteren Betrieb der Real-Time-Clock (RTC) in der Referenzuhr sorgt.

Diese Batterie hat eine Lebensdauer von mindestens 10 Jahren. Falls das folgende unerwartete Verhalten am Gerät auftritt, ist es möglich, dass die Spannung der Batterie 3 V unterschreitet und ein Austausch der Batterie erforderlich wird:

- Die Referenzuhr hat nach dem Einschalten ein falsches Datum bzw. eine falsche Zeit.
- Die Referenzuhr startet immer wieder im Cold-Boot-Modus (d. h. bei Start verfügt das System über keinerlei Ephemeriden-Daten, wodurch die Synchronisation sehr viel Zeit benötigt, weil alle Satelliten neu gefunden werden müssen).
- Einige Konfigurationsoptionen mit Bezug zur Referenzuhr gehen bei jedem Neustart des Systems verloren.

In diesem Fall sollten Sie den Austausch bitte nicht eigenmächtig durchführen. Nehmen Sie Kontakt mit dem Meinberg Technischen Support auf, der Ihnen eine genaue Anleitung über den Austauschprozess bereitstellt.

6.2.2 Sicherungswechsel

Gefahr!

Dieses Gerät wird an einer gefährlichen Spannung betrieben.

Lebensgefahr durch elektrischen Schlag!

- Trennen Sie das Gerät vom Netz! Betätigen Sie hierzu die Trennvorrichtung (Schalter).
- Anschließend lösen Sie bitte die Sicherungsschrauben des Stromversorgungssteckers (falls vorhanden) und ziehen Sie diesen ab.

Meinberg empfiehlt, immer eine Ersatzsicherung bereitzuhalten, damit der Betrieb bei Auslösung der integrierten Sicherung Ihres Systems nicht länger als nötig unterbrochen wird. Achten Sie auf korrekte Nennspannung, Nennstrom, Charakteristik und Typ. Die erforderliche Nennspannung sowie der Nennstrom sind am Sicherungsfach des Gerätes gekennzeichnet.

Sicherungen tragen gemäß IEC 60127 genormte Kennzeichnungen, die Auskunft über ihre Spezifikationen geben. Eine Kennzeichnung *T 2.5 A H 250 V* bei einer Sicherung hat zum Beispiel die folgende Bedeutung:

- *T*: Die Auslösecharakteristik, hier *träge*
- *2.5 A*: Der Nennstrom, hier *2,5 Ampere*
- *H*: Das Schaltvermögen, hier *hoch*
- *250 V*: Die Nennspannung, hier *250 Volt*

Stellen Sie sicher, dass die neue Sicherung die folgenden Anforderungen sowie die auf dem Gerät gedruckten Angaben erfüllt:

Stromart	Kennzeichnungsvorgabe	Löschmittel	Auslösecharakteristik	Abmessungen
AC	IEC 60127-konform	Mit oder ohne	T (Träge)	5 x 20 mm
DC	IEC 60127-konform	Mit	T (Träge)	5 x 20 mm

Wechselprozedur

1. Unterbrechen Sie die Stromversorgung des Geräts und trennen Sie anschließend alle Signal- und Antennenleitungen sowie Störmelde-Relaiskontakte und serielle Schnittstellen vom Gerät. Prüfen Sie das Gerät auf Spannungsfreiheit und sichern Sie es gegen Wiedereinschalten!
2. Ziehen Sie die Sicherungshalterung aus dem Sicherungsfach heraus, indem Sie diese mit einem Schlitzschraubendreher gegen den Uhrzeigersinn drehen. Ersetzen Sie die Sicherung und setzen Sie die neu bestückte Sicherungshalterung in das Sicherungsfach ein. Drücken Sie es mit dem Schraubendreher ein und drehen Sie im Uhrzeigersinn, damit die Sicherungshalterung sicher sitzt.
3. Schließen Sie alle Leitungen in umgekehrter Reihenfolge wieder an. Schalten Sie das Gerät anschließend bei Bedarf wieder ein.

6.3 Vorbeugung von ESD-Schäden

Die Bezeichnung **EGB** (elektrostatisch gefährdetes Bauteil) entspricht der englischsprachigen Bezeichnung „**ESDS Device**“ (Electrostatic Discharge-Sensitive Device) und bezieht sich auf Maßnahmen, die dazu dienen, elektrostatisch gefährdete Bauelemente vor elektrostatischer Entladung zu schützen und somit vor einer Schädigung oder gar Zerstörung zu bewahren. Systeme und Baugruppen mit elektrostatisch gefährdeten Bauelementen tragen in der Regel das links dargestellte Kennzeichen.

Zum Schutz von EGB vor Schäden und Funktionsstörungen sind Vorsichtsmaßnahmen zu ergreifen.

- Vor dem Aus- bzw. Einbau eines Moduls sollen Sie sich zunächst erden (z. B. indem Sie einen geerdeten Gegenstand berühren), bevor Sie mit EGB in Kontakt kommen.
- Für sicheren Schutz sorgen Sie, wenn Sie bei der Arbeit mit EGB ein Erdungsband am Handgelenk tragen, welches Sie an einem unlackierten, nicht stromführenden Metallteil des Systems befestigen.
- Verwenden Sie nur Werkzeug und Geräte, die frei von statischer Aufladung sind.
- Stellen Sie sicher, dass Ihre Kleidung für die Handhabung von EGB geeignet ist. Tragen Sie insbesondere keine Kleidung, die für elektrostatische Entladungen anfällig ist (Wolle, Polyester). Stellen Sie sicher, dass Ihre Schuhe eine niederohmige Ableitung von elektrostatischen Ladungen zum Boden ermöglichen.
- Fassen Sie EGB nur am Rand an. Berühren Sie keine Anschlussstifte oder Leiterbahnen auf Baugruppen.
- Berühren Sie während des Aus- und Einbauens von EGB keine Personen, die nicht ebenfalls geerdet sind. Hierdurch ginge Ihre eigene, vor elektrostatischer Entladung schützende Erdung verloren und damit auch der Schutz des Gerätes vor solchen Entladungen.
- Bewahren Sie EGB stets in EGB-Schutzhüllen auf. Diese EGB-Schutzhüllen müssen unbeschädigt sein. EGB-Schutzhüllen, die extrem faltig sind oder sogar Löcher aufweisen, schützen nicht mehr vor elektrostatischer Entladung. EGB-Schutzhüllen dürfen nicht niederohmig und metallisch leitend sein, wenn auf der Baugruppe eine Lithium-Batterie verbaut ist.

6.4 Entsorgung

Entsorgung der Verpackungsmaterialien

Die von uns verwendeten Verpackungsmaterialien sind vollständig recyclefähig:

Material	Verwendung	Entsorgung (Deutschland)
Polystyrol	Sicherungsrahmen/Füllmaterial	Gelber Sack, Gelbe Tonne, Wertstoffhof
PE-LD (Polyethylen niedriger Dichte)	Zubehörverpackung	Gelber Sack, Gelbe Tonne, Wertstoffhof
Pappe und Kartonagen	Versandverpackung, Zubehörverpackung	Altpapier

Für Informationen zu der fachgerechten Entsorgung von Verpackungsmaterialien in anderen Ländern als Deutschland, fragen Sie bei Ihrem zuständigen Entsorgungsunternehmen bzw. Ihrer Entsorgungsbehörde.

Entsorgung des Geräts

Dieses Produkt unterliegt den Kennzeichnungsanforderungen der Richtlinie 2012/19/EU über Elektro- und Elektronik-Altgeräte („*WEEE-Richtlinie*“) und trägt somit dieses WEEE-Symbol. Das Symbol weist darauf hin, dass dieses Elektronikprodukt nur gemäß den folgenden Regelungen entsorgt werden darf.

Achtung!

Weder das Produkt **noch** die Batterie darf über den Hausmüll entsorgt werden. Fragen Sie bei Bedarf bei Ihrem zuständigen Entsorgungsunternehmen bzw. Ihrer Entsorgungsbehörde nach, wie Sie das Produkt oder die Batterie entsorgen sollen.

Dieses Produkt wird gemäß WEEE-Richtlinie als „**B2B**“-Produkt eingestuft. Darüber hinaus gehört es gemäß Anhang I der Richtlinie der Gerätekategorie „**IT- und Kommunikationsgeräte**“.

Zur Entsorgung kann es an Meinberg übergeben werden. Die Versandkosten für den Rücktransport sind vom Kunden zu tragen, die Entsorgung selbst wird von Meinberg übernommen. Setzen Sie sich mit Meinberg in Verbindung, wenn Sie wünschen, dass Meinberg die Entsorgung übernimmt. Ansonsten nutzen Sie bitte die Ihnen zur Verfügung stehenden länderspezifischen Rückgabe- und Sammelsysteme für eine umweltfreundliche, ressourcenschonende und konforme Entsorgung Ihres Altgerätes.

Entsorgung von Batterien

Für die Entsorgung gebrauchter Batterien sind die örtlichen Bestimmungen über die Beseitigung als Sondermüll zu beachten.

7 Vor dem Start

7.1 Text- und Syntaxkonventionen

In diesem Kapitel werden kurz die Text und Syntaxkonventionen beschrieben, die in diesem Handbuch Anwendung finden.

Web Interface: Beispiel Menü „Netzwerk“
Untermenü „Network → Network Interfaces“
Register im Submenü „Network → Network Interfaces → IPv4“

Die Menüführung wird logisch getrennt durch den Pfeil nach Rechts (→).

Verzeichnisnamen / Pfade Beispiel Lantime Konfigurationsdatei
Die Verzeichnisnamen und Pfade werden kursiv dargestellt.

Code und Kommandozeilenbefehle

```
- cmd/www-upload.htm

#Programmcode und Kommandozeilenbefehle werden in einer grauen Box mit
Monospace-Schrift angezeigt.
```

Benutzer-Passwörter:
Für Benutzerpasswörter und das Shared Secret sind derzeit folgende Zeichen erlaubt:

Erlaubter Zeichensatz für beide:

```
validchars[] = abcdefghijklmnopqrstuvwxyz
               ABCDEFGHIJKLMNOPQRSTUVWXYZ
               0123456789
               =-_.:#*?@/+![]
```

7.2 Empfohlene Werkzeuge

	LANTIME IMS SERIES						
	LANTIME M1000	LANTIME M1000S	LANTIME M2000S	LANTIME M3000	LANTIME M3000S	LANTIME M4000	LANTIME M500
Mounting Rackears	TORX T20	TORX T20	TORX T20	TORX T20	TORX T20	TORX T20	x
Mounting DIN rail	x	x	x	x	x	x	Phillips PH1 x 80
Replacing IMS modules	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8
FAN Installation	TORX T8	TORX T8	TORX T8	TORX T8	x	TORX T8 Flat head Screwdriver	x

	LANTIME SERIES						
	LANTIME M100 / M150	LANTIME M200 / M250	LANTIME M300 / M320	LANTIME M400 / M450	LANTIME M600	LANTIME M900	SyncFire
Mounting Rackears	x	TORX T20	TORX T20	x	TORX T20	TORX T20	x
Mounting DIN rail	Phillips PH1 x 80	x	x	Phillips PH1 x 80	x	x	x
Replacing Modules	x	x	x	x	x	TORX T8	TORX T10

Abbildung: benötigte Werkzeuge (von links nach rechts):

- Innensechskant 2,5 mm
- Kreuzschraubendreher PH1 x 80
- Schlitzschraubendreher
- TORX T20
- TORX T8

7.3 Liste der verwendeten Abkürzungen

AFNOR	Association Francaise de Normalisation time codes
AC	Wechselstrom
ASCII	American Standard Code for Information Interchange
BMC	Best Master Clock
BMCA	Best Master Clock Algorithmus
BNC	Bayonet Neil Councilman Connector
Bps	Bytes per second
bps	Bits per second
CAT5	Standard Netzwek-Kabel
CET	Central European Time
CLI	Command Line Interface
DB9	Steckverbinder vom Typ D-Subminiatur
DARS	Digital Audio Reference Signal
DC	Gleichstrom
DCF77	Ist ein langwelliges Zeitsignal. DCF77 steht für D=Deutschland (Deutschland), C=Langwellensignal, F=Frankfurt, 77=Frequenz: 77,5 kHz.
DCFMARK	Einzelimpuls mit programmierbarem Datum und Uhrzeit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSCP	Differentiated Services Code Points
DST	Daylight Saving Time
E1	Europäisches digitales Übertragungssignal bei 2,048 MHz, das in Telekommunikationsnetzen verwendet wird.
E2E	End-to-end
ETH	Ethernet
FTP	File Transfer Protocol
FW	Firmware
GE / GbE	Gigabit Ethernet
GLONASS	GLObal NAvigation Satellite System von den russischen Luftfahrt-Verteidigungskräften
GM	Grandmaster
GND	Ground (Connector)
GNSS	Global Navigation Satellite System (GPS, GLONASS, Galileo, Beidou)
GOAL	GPS Optical Antenna Link
GPS	Global Positioning System (USA)
GPIO	General Purpose Input Output
GSM	Global System for Mobile Communications
HMI	Human-Machine Interface
HP	Horizontale Pitch - ist eine Einheit, die die horizontale Breite von elektronischen Geräten im Rack misst.
HPS	High Performance Synchronization PTP/NTP/SyncE GBit Modul
HSR	High-availability Seamless Redundancy
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electric and Electronic Engineers
IEEE 1588	Protokoll zur hochpräzisen Synchronisation im Nanosekundenbereich (PTP)
IP	Internet Protocol
IP 20	Schutzklasse 20
IRIG	Inter-range instrumentation group time codes
LCD	Liquid Crystal Display
LDAP(S)	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
LINUX	Unix-ähnliches Mehrbenutzer-Computer-Betriebssystem
LIU	Line Interface Unit- ein Modul zur Erzeugung von E1/T1-Signalen MBit/s (framed) und Clock (unframed)
LNE	Local Network Extention, zusätzliche Ethernet-Ports
MAC	Media Access Control
MD5	Message-Digest kryptographische Hash-Funktion
MESZ	Mitteleuropäische Sommerzeit
MEZ	Mitteleuropäische Zeit
MIB	Management Information Base
MRS	Multi Reference Source
MSF	Zeitzeichensender in Anthorn, UK
NIST	National Institute of Standards and Technology
NMEA	Communication standard from National Marine Electronics Association
NTP	Network Time Protocol
NTPD	NTP Daemon
OSV	Original Shipped Version (Firmware)
OUT	Output
P2P	Peer-to-Peer
PLC	Programmable Logic Controller
PLL	Phase Locked Loop
PPM	Pulse per Minute
PRP	Parallel Redundancy Protocol
PPS	Pulse per Second
PPH	Pulse per Hour
PTB	Physical - Technical Institute Braunschweig / Germany
PTP	Precision Time Protocol
RAM	Random Access Memory
RF	Frequency of radio waves, from 3 kHz to 300 GHz
RG58	Standard coaxial cable used to connect an antenna and a receiver
RJ45	Ethernet Connector with 8 conductors
RMC	Remote Monitoring Control
RoHS	Restriction of Hazardous Substances
RPS	Redundant Power Supply
RS-232	Serial port level
RS-485	Serial port level

RSC	Redundant Switch Control unit
RX	Receiving Data
SBC	Single Board Computer
SDU	Signal Distribution Unit
SHA-1	Secure Hash Algorithm 1
SMB	Subminiature coaxial connector
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SMTP	Simple Mail Transfer Protocol
SPS	Standard Positioning System
SSH	Secure SHell network protocol
SSU	Synchronization Supply Unit, specific clock used in telecommunication networks
SSM	Sync Status Messages, clock quality parameters in telecommunication networks.
ST	Bayonet-lock connector
Stratum	Value defines the NTP hierarchy
SYSLOG	Standard for computer data logging
T1	North American telecommunication signal at 1.544 MHz frequency
TACACS	Terminal Access Controller Access Control System
TAI	Temps Atomique International
TC	Time Code
TCA	Time Code Amplified
TCG	Time Code Generator
TCR	Time Code Receiver for IRIG A/B, AFNOR or IEEE1344 codes
TCP	Transmission Control Protocol
TTL	Transistor-to-Transistor Logic
TX	Data Transmission
U	Unit - is a unit measure the vertical height of rack mounted electronic equipment.
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UNIX	Multitasking, multi-user computer operating system
UTC	Universal Time Coordinate
VLAN	Virtual Local Area Network
WWVB	Time signal radio station Fort Collins, Colorado (USA)

8 Einleitung

Ein LANTIME ist eine vielseitige Zeit- und Frequenzsynchronisationslösung mit einem flexiblen Ansatz zur Unterstützung einer Vielzahl von Synchronisationsanforderungen in verschiedenen Anwendungen und Netzwerkumgebungen. Das System kombiniert eine leistungsstarke CPU mit dedizierter Hardware wie Referenzuhren oder I/O-Modulen und schafft so eine leistungsstarke Netzwerk-Appliance, die fast alle gängigen Zeit- und Frequenzsynchronisationsprotokolle und -signale unterstützt.

Die Basisinstallation eines LANTIME-Zeitservers ist ein sehr einfacher und unkomplizierter Prozess. Nach der Installation der Hardware müssen die Netzwerkadresse, die Netzmaske und das Standard-Gateway konfiguriert werden, um auf das Webinterface zugreifen zu können. Wenn alles korrekt eingerichtet ist, kann das Gerät, sobald es über das Netzwerk erreichbar ist, den NTP- oder PTP-Betrieb beginnen.

Zusätzlich zu den Zeitsynchronisationsprotokollen NTP und PTP unterstützt das LANTIME-System eine Reihe weiterer Netzwerkprotokolle, die hauptsächlich für die Fernverwaltung des Systems verwendet werden: HTTP(S), FTP, SSH und Telnet. Fernkonfiguration, Statusprüfungen und andere Wartungsverfahren wie Firmware-Updates oder Konfigurations-Backups können von jedem Webbrowser aus gesteuert werden. Aus Sicherheitsgründen kann jedes Protokoll für jede konfigurierte IP-Adresse aktiviert oder deaktiviert werden, wodurch potenzielle Angriffsvektoren reduziert und der Zugriff auf das Gerät effektiv kontrolliert werden kann.

Statusänderungen, Alarme oder andere wichtige Ereignisse werden in lokalen Protokolldateien gesichert und können zusätzlich an externe SYSLOG-Server weitergeleitet werden. Es werden eine Reihe von Benachrichtigungsprotokollen unterstützt, um das LANTIME-System in bereits bestehende IT-Monitoring-Lösungen zu integrieren. So sind beispielsweise SNMP-Traps oder automatisch generierte E-Mails zwei mögliche Optionen, um IT-Administratoren über wichtige Ereignisse zu informieren.

Die Installation mehrerer LANTIME-Geräte in einem Netzwerk ist eine Möglichkeit, Redundanz für wichtige Zeitsynchronisationsdienste im Netzwerk zu schaffen.

8.1 Netzwerk-Konfigurationskonzept

Das LANTIME System erlaubt durch sein flexibles Netzwerk-Konfigurationskonzept den Einsatz in den unterschiedlichsten Netzwerk-Umgebungen. Eine Trennung von physischen und logischen („virtuellen“) Interface-Konfigurationen deckt die meisten Anforderungen ab, die in Rechenzentren, Telekommikationsnetzwerken und industriellen Netzwerkumgebungen gestellt werden.

Jeder LANTIME Server verfügt über mindestens eine Ethernet-Schnittstelle, die vom CPU-Modul zur Verfügung gestellt wird (lan0). Dazu können je nach Modell und Modulausstattung noch mehrere weitere Netzwerk-Schnittstellen kommen, die entweder für die Verbindung in separate physische Netzsegmente verwendet werden, oder um redundante Anbindungen zu erlauben („Bonding“). Die LANTIME Firmware der siebten Generation kann bis zu 99 physische Netzwerk-Schnittstellen verwalten.

Die Konfiguration von IPv4 und IPv6 Adressen, unter denen der LANTIME Server aus den angeschlossenen Netzwerken erreicht werden kann, wird mittels logischer („virtueller“) Interface-Konfigurationen vorgenommen. Jedes logische Interface wird dabei einer physischen Netzwerkschnittstelle zugewiesen und kann außerdem auch einem IEEE 802.1q VLAN angehören. Die aktuelle Firmware unterstützt bis zu 99 logische Interface-Konfigurationen pro Server.

Die Netzwerkschnittstellen auf PTP-fähigen Modulen (für PTP und Hardware-NTP) sind davon ausgenommen, sie werden separat konfiguriert und unterstützen in der aktuellen Firmware-Version eine IPv4 und IPv6 Adresse sowie eine VLAN ID. Redundanz und Konnektivität zu mehreren Netzwerken und Netzwerk-Segmenten kann durch den Einsatz mehrerer PTP-fähiger Module erreicht werden.

Pro logischem Interface können die Netzwerkdienste für Zeitsynchronisation (NTP, TIME) und Management (HTTP, HTTPS, SSH, SNMP, TELNET, ...) einzeln aktiviert und deaktiviert werden. Das erlaubt zum Beispiel die Verwendung des Systems als NTP Server mit einer IP Adresse A (nur NTP aktiviert) und gleichzeitig das Management über eine zweite IP Adresse B, für die die gewünschten Management-Protokolle aktivert werden.

8.2 Optionen und Zusatzfunktionen

- Externe NTP-Zeitserver
- Freie Konfiguration von NTP hinsichtlich Authentifizierung und Zugriffskontrolle über Adress- und Netzmaskenbeschränkung
- Erweiterte Menüführung für Konfiguration und Überwachung über Telnet, SSH oder serielle Terminalschnittstelle
- Optional zusätzliche 10/100/1000 MBit-Ethernet-Schnittstellen
- Erweiterte Statistikunterstützung mit Langzeitgrafik und Zugriffsstatistik für NTP
- Alarmmeldungen können auf externem Großdisplay VP100/20/NET angezeigt werden
- USB-Schnittstelle für erweiterte Funktionalität: Software-Update, Übertragung von sicheren Zertifikaten, Log-Dateien und Konfigurationen, Tastensperre

8.3 Benutzerinterface

- Terminal Anschluss über serielle Schnittstelle, LED Status Anzeige
- Web-Interface für Konfiguration, Statusinformationen und grafische Statistiken
- Telnet oder Secure Shell Login zur vollen Passwort-geschützten Bedienung des Linux Betriebssystems
- FTP Zugang für Update der Betriebssoftware und zum Downloaden von Logg-Dateien
- Unterstützung für SNMP (Simple Network Management Protocol) und automatische SNMP-Traps im Alarmfall
- SYSLOG Meldungen können auf einen anderen Rechner umgeleitet werden
- E-Mail-Benachrichtigung bei konfigurierbaren Ereignissen
- Simulation einer synchronen Funkuhr einstellbar, damit auch ohne Antenne einsetzbar

8.4 Ein- und Ausgangsoptionen

- Weitere Ethernet RJ45 Anschlüsse (bis zu acht weitere im 3HE, 4 im 1HE und 8 im HS - XL Gehäuse)
- Frequenz-/Pulsausgänge über BNC Buchsen (z.B. 10 MHz, 2.048 MHz, PPS)
- Höhere Freilaufgenauigkeit durch bessere Oszillatoren (OCXO-SQ, OCXO-HQ, OCXO-DHQ)
- IRIG B Ausgänge
- ANZ141NET oder VP100/20NET als Nebenuhr über Netzwerk anzuschließen

Zusätzliche Ethernet RJ45-Anschlüsse verfügbar:

System-Typ	CPU-C05F1	CPU-C15G2 (Q7)
LANTIME M4000	bis zu 25 (+24) Netzwerk-Ports	bis zu 26 (+24) Netzwerk-Ports
LANTIME M3000(S)	bis zu 25 (+24) Netzwerk-Ports	bis zu 26 (+24) Netzwerk-Ports
LANTIME M2000S	bis zu 25 (+24) Netzwerk-Ports	bis zu 26 (+24) Netzwerk-Ports
LANTIME M1000(S)	bis zu 17 (+16) Netzwerk-Ports	bis zu 18 (+16) Netzwerk-Ports
LANTIME M500	bis zu 9 (+8) Netzwerk-Ports	bis zu 10 (+8) Netzwerk-Ports
LANTIME M900	bis zu 9 (+8) Netzwerk-Ports	
LANTIME M600	bis zu 5 (+1) Netzwerk-Ports	
LANTIME M400	bis zu 5 (+4) Netzwerk-Ports	
LANTIME M450		bis zu 6 (+4) Netzwerk-Ports
LANTIME M300	bis zu 6 (+4) Netzwerk-Ports	
LANTIME M320		bis zu 6 (+4) Netzwerk-Ports

8.5 Network Time Protocol (NTP)

Das NTP-Protokoll wurde in den 1980er Jahren von Dave L. Mills an der Universität von Delaware erfunden. Das Ziel war es, die höchstmögliche Zeitsynchronisationsgenauigkeit für Computer im gesamten Netzwerk zu erreichen. Das Protokoll und die zugehörigen Algorithmen wurden in mehreren RFCs spezifiziert.

Das Public-Domain-Softwarepaket „NTP“ ist die Referenzimplementierung dieses Protokolls. Seit der ursprünglichen Implementierung wurde NTP verbessert und ist heute weltweit verbreitet. Das Protokoll unterstützt eine Zeitgenauigkeit bis in den Nanosekundenbereich hinein. Die tatsächlich erreichbare Genauigkeit hängt jedoch in großem Maß von den verwendeten Betriebssystemen und der Qualität der Netzwerkverbindungen ab.

Die aktuelle Version des Protokolls (NTP v4) wurde von der IETF standardisiert, und das grundlegende Format der Netzwerkpakete ist mit früheren NTP-Versionen kompatibel, so dass aktuelle NTP-Implementierungen zusammen mit älteren Versionen verwendet werden können, sofern nicht spezifische NTP v4-Funktionen verwendet werden. Zusätzlich zu NTP gibt es auch eine vereinfachte Version namens „SNTP“ (Simple Network Time Protocol), die die gleiche TCP/IP-UDP-Paketstruktur wie NTP verwendet, aber aufgrund der einfacheren Algorithmen in der Regel nur eine reduzierte Genauigkeit bietet und daher meist für einfache Clients verwendet wird. Das NTP-Paket enthält ein Hintergrundprogramm (Daemon oder Dienst), das die Systemzeit des Computers mit einer oder mehreren externen Referenzzeitquellen synchronisiert, bei denen es sich entweder um andere Geräte im Netzwerk oder um eine an den Computer angeschlossene Hardware-Referenzzeitquelle handeln kann.

Erfahren Sie mehr über das Network Time Protocol in unserem Whitepaper „Computer Time Synchronization Concepts“ Kapitel 6:
https://www.meinberg.de/german/info/#whitepaper

8.5.1 Von NTP unterstützte Computer-Plattformen

Das native Betriebssystem von NTP ist UNIX. Heute läuft NTP jedoch unter vielen UNIX-ähnlichen Systemen, und NTP v4 wurde auch auf Windows portiert. Es kann unter Windows NT, Windows 2000 und neueren Versionen bis Windows 11 verwendet werden.

Die Standard-NTP-Distribution kann **nicht** unter Windows 3.x und Windows 9x/ME ausgeführt werden, da einige Kernel-Features fehlen, die für eine präzise Zeitmessung erforderlich sind. Für Windows 9x/ME und andere Plattformen, die nicht direkt vom NTP-Paket unterstützt werden, gibt es einige NTP- oder SNTP-Programme im Internet. Eine Übersicht über die verfügbaren Anwendungen finden Sie auf der NTP-Support-Homepage: https://support.ntp.org/Main/ExternalTimeRelatedLinks

8.6 Option: Precision Time Protocol (PTP) / IEEE 1588

PTP/IEEE1588 ist ein Zeitsynchronisationsprotokoll, das Sub-Mikrosekunden-Genauigkeit über ein Standard-Ethernet-Kabel ermöglicht. Dieser Genauigkeitsgrad wird dadurch erreicht, dass die für PTP/IEEE1588 verwendeten Netzwerk-Ports mit einer sogenannten Hardware-Timestamping-Unit erweitert werden. Diese Komponente ermittelt sehr genau den Zeitpunkt, zu dem ein PTP Netzwerkpaket versendet bzw. empfangen wurde. Das auf Multicast- oder Unicast Paketen basierende Netzwerkprotokoll berücksichtigt diese Zeitstempel bei der Kompensation der Laufzeiten von Synchronisationspaketen und erreicht so die oben angegebene Genauigkeit.

Anders als z.B. NTP gibt es bei PTP lediglich eine Zeitquelle. Die sogenannte Grandmaster Clock ist der einzige Zeitgeber und wird von allen PTP Clients (Slave Clocks) als Zeitquelle verwendet. Sind zwei oder mehr Grandmaster Clocks in einem Netzwerk vorhanden, wird mittels eines im Standard festgelegten Algorithmus ermittelt, wer als Grandmaster Clock verwendet wird. Dieser „Best Master Clock“ (BMC) Algorithmus ist bei allen PTP Systemen identisch, daher werden alle PTP/IEEE1588 konformen Systeme die gleiche Grandmaster Clock auswählen. Die verbleibenden nicht ausgewählten Grandmaster Clocks gehen in den sogenannten Passiv-Modus und senden keine Synchronisationspakete, solange die aktive Grandmaster Clock diese „Sync-Messages“ versendet.

Die verwendete Netzwerk-Infrastruktur ist von entscheidender Bedeutung und nimmt großen Einfluss auf die erreichbare Genauigkeit eines PTP/IEEE1588 Netzwerks. Bei asymmetrischen Laufzeiten verschlechtert sich die Genauigkeit, daher sind Standard-Switche nicht so sehr für den Einsatz in PTP-Netzwerken geeignet. Die Store-And-Forward Technologie dieser Geräte läßt die Durchlaufzeiten der Netzwerkpakete lastabhängig teilweise dramatisch schwanken und erschwert dadurch die Laufzeit-Kompensation erheblich. Einfache Hubs mit zumindest fixen Durchleitzeiten dagegen stellen kein Problem dar. In größeren Netzwerken helfen spezielle Switches mit PTP/IEEE1588 Funktionalität dabei, die möglichen Genauigkeitsklassen zu erreichen. Diese Komponenten fungieren als sogenannte „Boundary Clocks“ (BC) oder „Transparent Clocks“ (TC) und gleichen die internen Laufzeiten durch eigene Timestamping-Units aus, in dem sie im „Boundary Clock“-Modus gegenüber der Grandmaster Clock als Slave (Client) agieren und den angeschlossenen Slaves selbst als Grandmaster erscheinen. Im „Transparent Clock“-Modus wird dem Sync-Paket beim Durchlaufen des Switches die Verweildauer („Residence Time“) innerhalb des Switctes als Korrekturwert mitgegeben. Intern wird die Zeitskala TAI (siehe Zeitskala in Global Parameters) verwendet.

8.6.1 PTPv2 IEEE 1588-2008 Konfigurationsanleitung

Eine der wichtigsten Aufgaben innerhalb eines Netzwerk Zeitsynchronisationsprojekts ist die Konfiguration der Geräte innerhalb einer PTP Infrastruktur. Die Einstellungen der beteiligten PTP Grandmaster Uhren als Zeitquellen und den Endgeräten („Slaves“) müssen zueinander passen, um spätere Probleme bei der Synchronisation im produktiven Einsatz zu vermeiden. Zusätzlich dazu müssen bei der Verwendung von weiteren PTP kompatiblen Netzwerkkomponenten, wie Switche, die PTP Einstellungen ebenfalls kompatibel sein.

Es ist daher sehr wichtig im Vorfeld Entscheidungen zu treffen, wie die Kommunikation zwischen den Geräten stattfinden soll. Die wesentlichen Punkte sind hierbei Entscheidung zugunsten eines bestimmten Netzwerkkommunikationstyps wie Unicast oder Multicast oder die Entscheidung, wie oft ein Master Synchronisationsnachrichten zu den Slaves senden soll.

Dieses Kapitel vermittelt einen einleitenden Überblick über die verschiendenen Konfigurationsparameter und deren Effekte auf die Synchronisation im allgemeinen. Eine detaillierte Beschreibung der einzelnen Konfigurationsparameter, die im LANTIME Menü vorgenommen werden können, befindet sich im nächsten Kapitel innerhalb dieser Dokumentation.

8.6.1.1 Allgemeine Optionen

Bevor mit dem Aufbau der Infrastruktur des PTP Netzes begonnen wird, sollten die folgenden Optionen bedacht werden:

1) Layer 2 (Ethernet) oder Layer 3 (UDP/IPv4) Verbindungen
2) Multicast oder Unicast
3) Two-Step oder One-Step Betrieb
4) End-to-End (E2E) oder Peer-to-Peer (P2P) Delay Mechanismus

Diese Optionen müssen für alle beteiligten PTP-Geräte definiert werden. Sollten teilnehmende Geräte abweichende Einstellungen haben oder diese nicht unterstützen, dann sind sie nicht in der Lage, eine funktionierende Synchronisation aufzubauen.

8.6.1.2 Netzwerk - Layer 2 oder Layer 3

PTP/IEEE 1588-2008 bietet die Möglichkeit, die PTP Nachrichten auf verscheidene Netzwerkkommunikationsebenen abzubilden. Bei allen Meinberg-PTP-Produkten kann man zwischen PTP über IEEE 802.3 Ethernet (Netzwerk Layer 2) oder UDP/IPv4 (Netzwerk Layer 3) wählen.

Layer 3 ist der empfohlene Modus, da er in den meisten Umgebungen funktioniert. Im Layer-2-Betrieb muss das Netzwerk in der Lage sein, reine Ethernet-Verbindungen zwischen Master- und Slave-Geräten herzustellen. Dies ist oft nicht der Fall, wenn das Netzwerk in verschiedene Netzwerksegmente aufgeteilt und innerhalb der Netzwerkinfrastruktur kein Layer 2 Routing vorgesehen ist.

Der einzige Vorteil bei der Verwendung im Layer 2 -Betrieb besteht in einer leichten Reduktion des Netzwerkverkehrs, da die übertragenen Netzwerkpakete nicht den UDP- und IP-Header beinhalten und somit 28 Bytes pro PTP Paket eingespart werden. Da PTP jedoch ein Protokoll mit wenig Datenverkehr ist, spielt dieses Argument nur eine Rolle, wenn entweder Netzwerkverbindung mit sehr geringer Bandbreite oder nach Bandbreite bezahlte Netzwerkverbindungen, z. B. über gemietete Leitungen verwendet werden müssen.

8.6.1.3 Multicast oder Unicast

Die erste Version von PTP (IEEE 1588-2002, auch bekannt als PTPv1) unterstützte nur die Übermittlung über Multicast-Nachrichten. Multicast hat den großen Vorteil, dass der Master nur ein Sync Paket an eine Multicast Adresse schicken muss, welches dann von allen Geräten empfangen wird, die auf dieser Multicast Adresse lauschen.

In der Version 2 des PTP Standards (IEEE 1588-2008) wurde zusätzlich der Betrieb über Unicast eingeführt. Die Unicast Kommunikation basiert auf einer Punkt-zu-Punkt Verbindung, bei welcher der Master ein Sync Paket zu jedem Slave Gerät schicken muss, was wesentlich mehr CPU Performance auf dem Master und eine erhöhte Netzwerklast zur Folge hat.

Unicast Kommunikation wird in bestimmten Netzwerkumgebungen verwendet, in denen Multicast Pakete durch Switche und Router geblockt werden (müssen).

8.6.1.4 Two-Step oder One-Step

PTP erfordert, das der Master periodisch SYNC Pakete zu den Slave Geräten schickt. Der Hardware-Zeitstempel-Ansatz von PTP erfordert ebenso, das der Master den Moment exakt bestimmt, bei welchem das SYNC Paket auf das Netzwerkkabel geht und diesen Zeitpunkt an die Slaves weiter gibt. Dies kann entweder durch das Aussenden einer separaten Nachricht geschehen (das so genannte „FOLLOWUP Paket“, auch Two-Step Verfahren genannt) oder durch direkte Manipulation des SYNC Pakets (im One-Step Verfahren) kurz bevor das Paket den Netzwerkport verlässt. Bei dieser Manipulation wird der Zeitstempel von der Hardware Zeitstempeleinheit direkt in das SYNC Paket geschrieben, kurz bevor es auf das Netzwerkkabel geht.

8.6.1.5 End-To-End (E2E) oder Peer-To-Peer (P2P) Delay Messungen

Zusätzlich zum Empfang der SYNC/FOLLOWUP Pakete, muss ein Slave auch in der Lage sein, die Paketlaufzeit vom Master zum Slave zu bestimmen, um den Offset zur Masteruhr korrekt berechnen zu können. Dieses „Delay Measurement“ wird vom Slave in einem bestimmten Interval durchgeführt. Eine Laufzeitmessung wird durchgeführt, indem der Slave ein sogenanntes DELAY_REQUEST Paket zum Master sendet und sich die Zeit der Aussendung dieses Pakets merkt. Der Master nimmt dann einen Zeitstempel beim Empfang dieses Pakets und sendet diesen Zeitstempel in einem DELAY_RESPONSE Paket an den Slave zurück.

IEEE 1588-2008 bietet zwei verschiedene Mechanismen zur Durchführung der Laufzeitmessung an. Ein Slave kann entweder die Gesamtlaufzeit zum Master bestimmten, dies wird dann **End-to-End** Mechanismus (oder kurz E2E) genannt. Alternativ kann ein PTP Gerät nur die Laufzeit zu seinem direkten Nachbarknoten im Netzwerk messen, wobei der Nachbarknoten sowohl ein PTP Endgerät wie auch ein Switch darstellen kann. Dieses Verfahren wird **Peer-to-Peer** Mechanismus (oder kurz P2P) genannt. Beim P2P-Verfahren werden die einzelnen Laufzeiten zwischen den Netzwerkknoten akkumuliert und dem durchlaufenden Sync Paket vom Master als Korrekturwert mitgegeben, so dass am Ende der Slave die Gesamtlaufzeit ermitteln kann.

Der Vorteil des P2P Verfahrens ist die deutliche Reduktion von möglichen Synchronisationsungenauigkeiten aufgrund von plötzlichen Topologieänderungen innerhalb des Netzwerks. **Beispiel:** In einer Ringtopologie wird die Paketlaufzeit verändert, wenn der Ring an einer Stelle aufbricht, da der Netzwerkverkehr unter Umständen in eine andere Richtung umgeleitet wird. Ein PTP Slave, der die Paketlaufzeit mit Hilfe des E2E Verfahrens ermittelt, würde in diesem Fall von einer falschen Paketlaufzeit ausgehen bis er die nächste Laufzeitmessung durchführt. Dieses Problem würde in einer P2P Infrastruktur nicht passieren, da zum Zeitpunkt der Topologieänderung bereits alle Laufzeiten zwischen den Links bekannt sind und ein Sync Paket vom Master bereits beim ersten Durchlauf über den neuen Netzwerkpfad mit den entsprechenden Korrekturwerten versehen wird.

Der Nachteil des P2P Verfahrens besteht darin, das alle beteiligten Netzwerkknoten, inklusive aller Switche zwischen Master und Slave, das P2P Verfahren beherrschen müssen. Ein Switch/Hub ohne P2P Unterstützung würde entweder alle empfangenen PDELAY_REQUEST Pakete an alle Ports weiterleiten und die Genauigkeit dadurch erheblich verschlechtern bzw. unbrauchbar machen oder im schlechtesten Fall alle PDELAY Pakete blocken und überhaupt keine Laufzeitmessung ermöglichen.

Daher bleibt das E2E Verfahren die einzige Wahl für die Verwendung von PTP über nicht PTPv2-kompatible Switche. Es bleibt eine akzeptable Möglichkeit, wenn redundante Netzwerktopologien nicht vorhanden sind oder man hinnehmen kann, dass Delay-Messungen kurzfristig verfälscht werden.

8.6.1.6 Nachrichtenintervalle

Die Entscheidung zwischen den verschiedenen oben beschriebenen Modi ist hauptsächlich durch die verwendete Netzwerkumgebung vorgegeben in welcher die PTP Geräte installiert werden. Zusätzlich zu den einzustellenden Modi müssen eine Reihe von Intervallen für bestimmte PTP Nachrichtentypen definiert werden, falls nicht die Standardeinstellungen verwendet werden sollen, die in den meisten Fällen jedoch nicht verändert werden müssen.

Es gibt jedoch Anwendungen, bei denen die Intervalle angepasst werden müssen. Dies ist beispielsweise der Fall, wenn durch hohe Netzwerklast Schwankungen bei den Paketlaufzeiten auftreten können (PDV - „Packet Delay Variation"). Probleme bei der Client Synchronisation können dann durch die Erhöhung der Frequenz der ausgesendeten SYNC Pakete vermieden werden, da in diesem Fall Messfehler schneller korrigiert werden.

Die Intervalle für die folgenden PTP Nachrichten können editiert werden:
1) ANNOUNCE Messages
2) SYNC/FOLLOWUP Messages
3) (P)DELAY_REQUEST Messages

8.6.1.7 ANNOUNCE Messages

Diese PTP Nachricht transportiert den Zustand und die Qualitätsinfomationen über den aktuell aktiven Master im PTP Netzwerk. Der Vorgang der zur Entscheidung führt, welcher Grandmaster im Netzwerk aktiv werden soll, wird „Best Master Clock Algorithm" (BMCA) genannt. Die notwendigen Parameter zur Ausführung des BMCA werden alle in der ANNOUNCE Message übertragen, die von einem Master periodisch ausgesendet wird.

Das Intervall mit welchem diese Nachricht gesendet wird, beeinflusst direkt die Umschaltzeit, die benötigt wird, um einen Wechsel des Masters durchzuführen, falls der aktuell aktive Master ausfällt oder ein „besserer" im Netz aktiv wird.

In der Zeit in der noch kein Master bestimmt wurde, ist es möglich, das mehrere potentielle (Grand-)Master Announce Messages aussenden. Dies geschieht u.a., wenn die Geräte innerhalb des PTP Netzwerks gleichzeitig gestartet werden. Ein PTP Gerät, welches grundsätzlich Master werden kann, empfängt gleichzeitig zur Aussendung der „eigenen" Announce Message die Announce Messages der anderen PTP Master Geräte. Sobald festgestellt wird, das ein anderer Master im Netzwerk existiert, welcher bessere Werte aufweist als die eigenen, wird der Master die weitere Aussendung von ANNOUNCE Messages einstellen. Auf diese Weise bleibt nach kurzer Zeit nur noch der „beste" Master übrig.

Ein Grandmaster, der nicht die Aufgabe des aktiven Masters übernimmt, wechselt in den „PASSIVE" Modus und wartet darauf, im Fall eines Fehlers des aktiven Masters die Master-Rolle wieder zu übernehmen.

Um einen Master auszuwählen, ist es erforderlich, dass mindestens zwei aufeinander folgende ANNOUNCE Messages empfangen werden. Der Empfang einer ersten ANNOUNCE Message muss innerhalb einer Wartezeit von mindestens 3 ANNOUNCE Message Intervallen erfolgen. Legt man beispielsweise ein ANNOUNCE Intervall von 2 Sekunden zugrunde (dies ist der Standardwert), so würde beim Ausfall eines Masters nach 6 Sekunden festgestellt werden, dass der Master einen Fehler hat und nach weiteren 4 Sekunden der neue Master feststeht.

Ein ANNOUNCE Intervall von 2 Sekunden hat demzufolge eine Umschaltzeit von mindestens 10 Sekunden zur Folge. Ein kürzeres ANNOUNCE Intervall ermöglicht daher im Fehlerfall prinzipiell eine schnellere Umschaltzeit. Ein zu kurzes Intervall kann jedoch in bestimmten Umgebungen kurzfristig zu Fehlentscheidungen führen. Es wird daher empfohlen die Standardeinstellung beizubehalten.

8.6.1.8 SYNC/FOLLOWUP Messages

Der aktive MASTER sendet SYNC Nachrichten (und im Two-Step Verfahren zugehörige FOLLOWUP Nachrichten) in einem konfigurierten Intervall aus. Dieses Intervall (Standard ist 1 SYNC/FOLLOWUP Paket einmal pro Sekunde) bestimmt, wie oft die SLAVES Synchronisationsinformationen erhalten um die eigene Uhr gegenüber der Masteruhr abzugleichen und nachzuführen.

Zwischen dem Empfang zweier Sync Nachrichten läuft die Slave Uhr frei auf der eigenen Zeitbasis, zum Beispiel dem Quarzoszillator. Ein wichtiger Faktor bei der Entscheidung welches SYNC Intervall zu wählen ist, ist die Stabilität des Oszillators. Ein sehr guter Oszillator benötigt eine geringere SYNC Rate, um die Stabilität zu halten als ein weniger guter Oszillator. Auf der anderen Seite wird die erforderliche Netzwerkbandbreite direkt beeinflusst, wenn das SYNC Intervall geändert wird.

Für Meinberg Slave Geräte ist die Standardeinstellung (einmal pro Sekunde) ausreichend um die bestmögliche Synchronisiationsgenauigkeit zu erreichen.

8.6.1.9 (P)DELAY_REQUEST Messages

Wie bereits bei der Erläuterung der Mechanismen für die Laufzeitmessungen („End-To-End“ oder „Peer-to-Peer“) erwähnt wurde, sind die Delay Messungen ein wichtiger Faktor bei der Realisierung der erforderlichen Genauigkeit. Im End-to-End Modus werden vom Slave standardmäßig alle 8 Sekunden Delay Messungen durchgeführt, in dem ein DELAY_REQUEST Paket an den Master gesendet wird, welcher dann in einem DELAY_RESPONSE Paket den Zeitstempel zum Zeitpunkt des Eintreffens des DELAY_REQUEST Pakets an den Slave zurückschickt. In Umgebungen, wo das Netzwerkdelay stark variiert, kann die Messrate erhöht werden, um schneller auf Fehlmessungen zu reagieren, die durch Verzögerungen innerhalb des Netzwerks entstanden sein können.

Meinberg Slave Geräte sind in der Lage den Effekt einer veralteten Delay Messung durch den Einsatz eines Filters und einer optimierten Oszillator-Regelung zu begrenzen. Dies verhindert, das eine Slave-Uhr große Sprünge durchführt selbst wenn durch hohe Netzwerklast „Ausreißer“ bei den Messungen vorkommen. Die Masteruhr wird über einen gewissen Zeitraum beobachtet, bevor eine Regelung des eigenen Oszillators durchgeführt wird. Mit einem „low cost“ Oszillator wäre dies nicht möglich, da vor allem die temperaturabhängige Drift und Alterungseffekte des Oszillators eine größere Abweichung zur Folge haben.

Im „Peer-to-Peer“ Modus ist eine Änderung des Intervalls nicht so kritisch, da nur die Laufzeit zum nächsten „Hop“ gemessen wird (Port-zu-Port) und eine Änderung der Laufzeit auf dieser kurzen Strecke sehr unwahrscheinlich ist.

Aktuelle Firmware-Versionen von Meinberg Grandmastern (V5.32a und älter) bieten keine Möglichkeit, die Rate der DELAY-Messages im Multicast-Modus zu ändern, sie ist auf eine Verzögerungsanfrage alle 8 Sekunden festgelegt. Slave Geräte dürfen einen Master nicht öfter anfragen als der Master in seinen DELAY_RESPONSE Messages vorgibt. Meinberg Grandmaster geben standardmäßig eine Delay Request Rate von 8 Sekunden vor.

8.6.1.10 Lucky Packet Filter

Falls im angeschlossenen PTP Netzwerk keine PTP Switches verwendet werden, sind die zu erwartenden Genauigkeiten abhängig von der Charakteristik der Switches. Netzwerk-Switches ohne PTP-Unterstützung haben die Eigenschaft, die PTP Pakete nicht deterministisch zu verzögern und damit die Zeitgenauigkeit der PTP-Messung zu verschlechtern (zeitlicher Jitter durch Variation der Paketlaufzeiten). Unter Jitter wird im folgenden die Varianz der gemessenen Offsets um einen bestimmten Mittelwert verstanden, der im betrachten Zeitrahmen ermittelt wird.

Dieser zeitliche Jitter kann zwischen 100 ns und 10000 ns (bisher getestete Switches) liegen. Bei Routern liegt dieser Jitter noch wesentlich höher.

Um diesen zeitlichen Netzwerk-Jitter zu reduzieren, wird ein **Lucky-Packet-Filter** angewendet. Mit Layer2 Switchen können dann Genauigkeiten im Submicrosekundenbereich erreicht werden. Ebenso werden Schwankungen durch Netzwerklast und Fehlmessungen eliminiert.

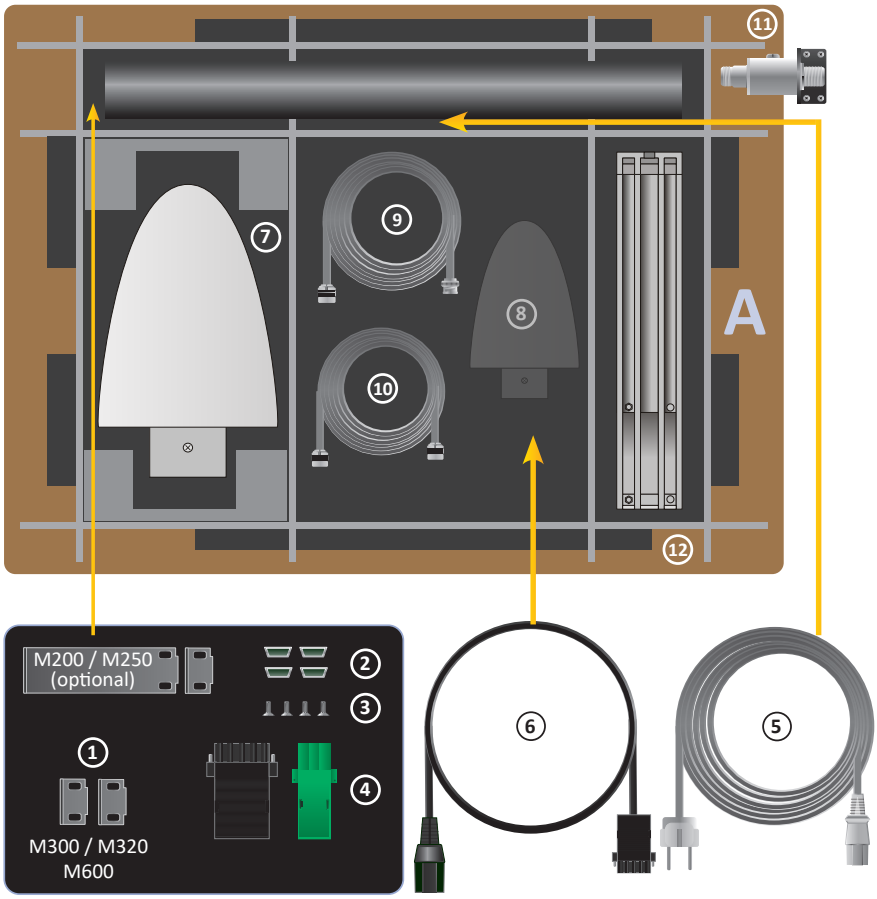
Funktionsweise
„Lucky-Packets“ sind Netzwerkpakete, die während der Übertragung im Netzwerk die geringste Verzögerung (Latenz) erfahren, beispielsweise weil die Warteschlangen auf den Switches leer sind. Im Kontext von PTP (Precision Time Protocol) werden diese besonders schnellen Pakete genutzt, um eine präzise Zeitmessung und Synchronisation zu ermöglichen. Es handelt sich um eine Methode, bei der ein Filter innerhalb eines bestimmten „Fensters“ nach dem Paket mit der geringsten Verzögerung sucht, welches dann für die weitere Verarbeitung verwendet wird, während andere, langsamere Pakete ignoriert werden.

Hinweis:

Der „Lucky-Packet-Filter“ wird bei allen Meinberg PTP-Modulen automatisch verwendet, wenn das Modul als **Slave** konfiguriert ist und mindestens 16 Sync und Delay Request Nachrichten ausgetauscht werden.

9 Auspacken des Systems

Nach dem Auspacken des LANTIME Zeitservers überprüfen Sie bitte den Inhalt auf Vollständigkeit. Vergleichen Sie den Inhalt der Lieferung mit der beigelegten Packliste.

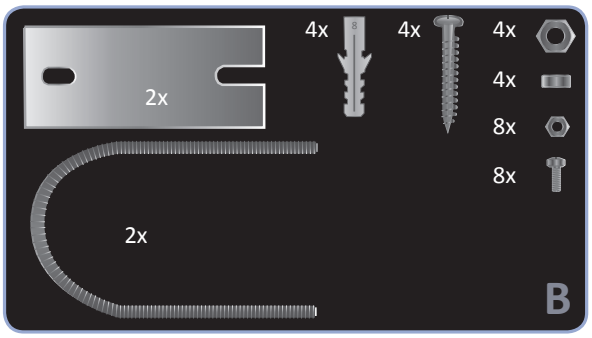


A LANTIME Paketinhalt

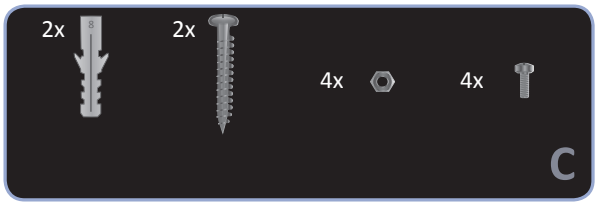
1. Montagewinkel für 19-Zoll-Rackmontage (optional für LANTIME M200 / M250)
2. Schutzabstandhalter (M200 / M250 / M300 / M320 / M600 / IMS-Rack-Systeme)
3. Schrauben für Halterungen (M200 / M250 / M300 / M320 / M600 / IMS-Rack-Systeme)
4. 3-poliger DFK-Stecker oder 5-poliger DFK-Stecker
   (zusätzlicher Anschluss bei AC/DC- oder DC-Netzteil)
5. Netzkabel (nur bei AC-Netzteil)
6. Option: Netzkabel mit 5-poligem Stecker

Nur mit mitgelieferter Antenne

7. Antenne
8. Option: Zweite Antenne
9. Antennenkabel
10. Option: Kabel für Überspannungsschutz
11. Option: Überspannungsschutz mit Halterung
12. Halterungen für Mast- oder Wandmontage (GPS-Antenne)
13. Mast für Antennenmontage (GPS-Antenne)



B **Montagesatz für GPS-Antenne**
(Wand- oder Mastmontage)



C **Montagesatz für Langwellenantenne**
(Wandmontage)

Hinweis: Bitte lesen Sie die Sicherheitshinweise und das Handbuch sorgfältig durch, um sich mit dem sicheren und korrekten Umgang mit elektronischen Geräten vertraut zu machen.

Die Produktdokumentation befindet sich auf dem USB-Flash-Speicher.

10 LANTIME Inbetriebnahme

- Anschluss des LANTIME
- Eingabe der IP-Adresse
- Anschluss der Antenne
- Konfiguration über das Webinterface

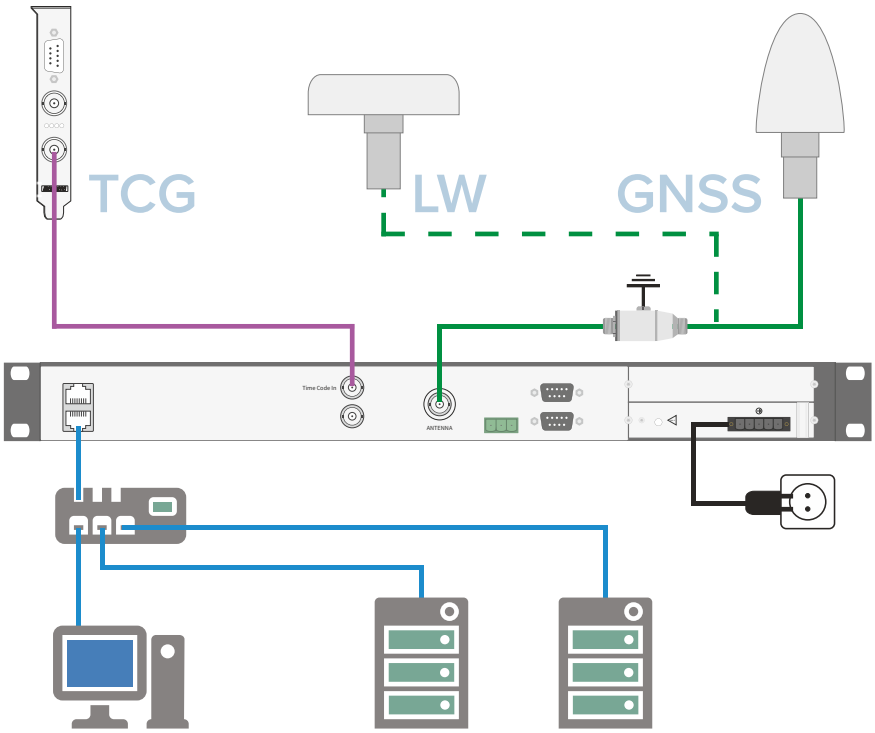


Abbildung: LANTIME Anschlussplan TCG = Timecode-Generator; LW = Langwellenempfänger; GNSS = Global Navigation Satellite System

Vergewissern Sie sich, dass sich der Netzschalter (falls vorhanden) in der Position „0“ (aus) befindet, und verbinden Sie das Stromnetzkabel mit dem Netzteil Ihres LANTIME. Verbinden Sie das Gerät dann mit einem geeigneten Netzwerkkabel mit Ihrem Computernetzwerk. Nach dem Einschalten der Stromversorgung wird die folgende Meldung angezeigt:

```
MEINBERG LANTIME
is booting  ...
please wait ...
......
```

Nach dem Ausführen einer Reihe von Selbsttests zum Einschalten befindet sich der Zeitserver im Betriebsmodus und der Hauptbildschirm erscheint.

Cyber-Sicherheitshinweis

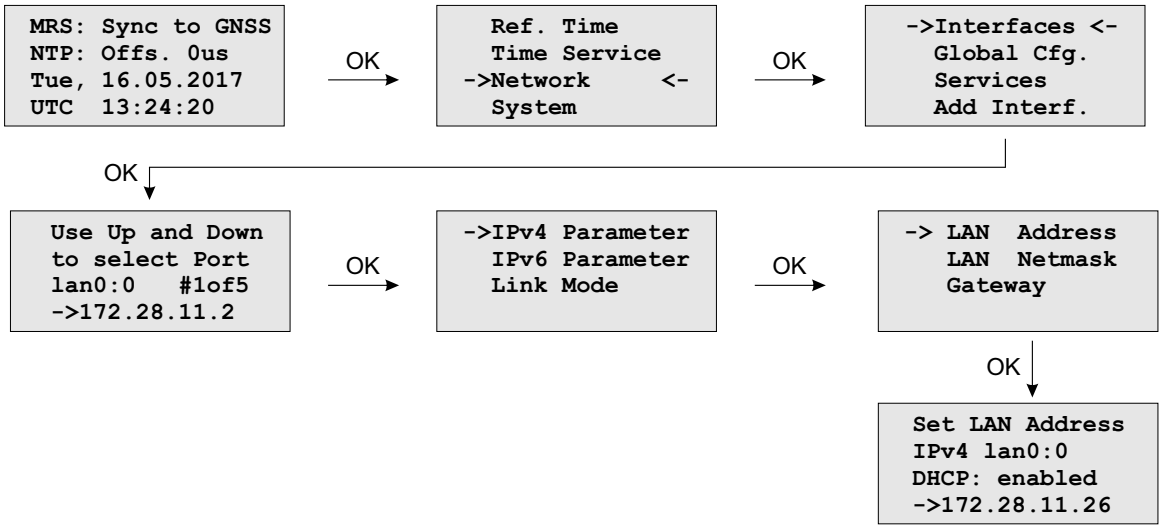
- Stellen Sie nach der initialen Inbetriebnahme sicher, dass physische Zugangskontrollmaßnahmen etabliert werden, sodass der physische Zugang zum Gerät auf autorisiertes Personal beschränkt wird.
- Stellen Sie sicher, dass Kabel so verlegt sind, dass sie nicht manipuliert werden können.
- Bieten Sie regelmäßige Schulungen für Mitarbeiter an, die mit der Handhabung des Geräts (und der Nutzung des Netzwerks im Allgemeinen) betreut sind.
- Stellen Sie sicher, dass alle kritischen Daten regelmäßig gesichert werden und dass die Sicherungen im Falle eines Angriffs für die Wiederherstellung leicht zugänglich sind.

Lesen Sie dazu auch das

→ Kapitel 13.1.5.1, „Anmeldung“ und → Kapitel 13.1.5.2, „Frontplatte“.

Eingabe der IP-Adresse

Die Erstinstallation erfordert die Einrichtung einer IP-Adresse, einer Netzmaske und (in den meisten Netzwerkumgebungen) eines Standard-Gateways. Um einen Überblick über die aktuelle Konfiguration zu erhalten, drücken Sie F2. Drücken Sie erneut F2 um zum Display-Menü „Netzwerk-Setup“ zu gelangen:



Navigieren Sie mit den Pfeiltasten zu „Interfaces“ und drücken Sie OK, um zum Konfigurationsmenü der angeschlossenen Netzwerkschnittstelle zu gelangen. Sie können den Netzwerkanschluss mit den Pfeiltasten „Nach unten“ und „Nach oben“ auswählen (↓ | ↑).

Manuelle Eingabe der IP-Adresse (nicht über DHCP)

Deaktivieren Sie DHCP und richten Sie eine gültige IP-Adresse, Netzmaske und (falls erforderlich) ein Standard-Gateway ein. Dies kann durch Auswählen eines Feldes mit den Pfeiltasten erreicht werden. Drücken Sie dann OK, um in den Bearbeitungsmodus zu wechseln.

Der Cursor kann mit den Tasten ← | → bewegt werden. Der Wert unter dem Cursor kann mit ↓ | ↑ geändert werden. Bestätigen Sie Ihre geänderten Werte mit OK und F2.

Anschluss der Antenne

Verbinden Sie das Antennenkabel mit der Antennenbuchse Ihres LANTIME. Im Falle eines Kurzschlusses erscheint folgende Meldung im Display:

```
ANTENNA
SHORT-CIRCUIT
DISCONNECT POWER
! ! !
```

Schalten Sie in diesem Fall das Gerät sofort aus und überprüfen Sie das Antennenkabel. Eine Anleitung zur Installation der Antenne finden Sie im Kapitel „Montage der Antenne“ in diesem Handbuch.

Konfiguration über das Web-Interface

Die Systemkonfiguration kann nun über das Netzwerk mit einem Standard-WEB-Browser geändert werden.

Verbinden Sie sich mit dem Webinterface, indem Sie die IP-Adresse des LANTIME in das Adressfeld Ihres Web-Browsers eingeben:

1. Aufrufen des Web-Interface
   Geben Sie die IP-Adresse Ihres LANTIME in das Adressfeld ein: https://xxx.xxx.xxx.xxx

2. LOGIN
   User: root
   Password: timeserver

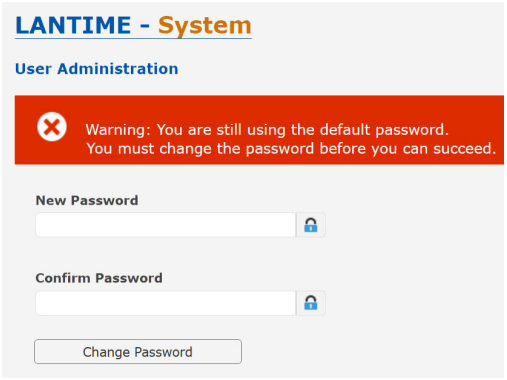


Abb. rechts: Weiterleitung beim erstmaligen Anmelden in das Menü „Benutzerverwaltung → Passwort ändern“

Cyber-Sicherheitshinweis

Bei der erstmaligen Anmeldung mit den oben genannten Zugangsdaten, werden Sie aufgefordert ein neues Passwort zu wählen. Damit wird sichergestellt, dass die Default-Zugangsdaten geändert werden und Ihr System vor unauthorisiertem Zugriff geschützt ist.

11 Benutzerhandbuch Sicherheit

Dieses Kapitel beschreibt die Konfiguration eines Betriebssystems der LANTIME-Serie (LTOS) in Bezug auf die Sicherheitsfunktionen. Es gliedert sich in die folgenden Abschnitte: allgemeiner Überblick, Sicherung des Managements, Sicherung des Zeitservice und zusätzliche Informationen zur Ausgabe von Ereignisprotokollen. Abschließend werden einige Hinweise für den Aktualisierungsprozess eines LANTIME gegeben.

Es werden allgemeinen Kenntnisse über Public-Key-Infrastrukturen, RSA, symmetrische Schlüssel und die Protokolle SSL, SSH, NTS, NTP und SNMP vorausgesetzt.

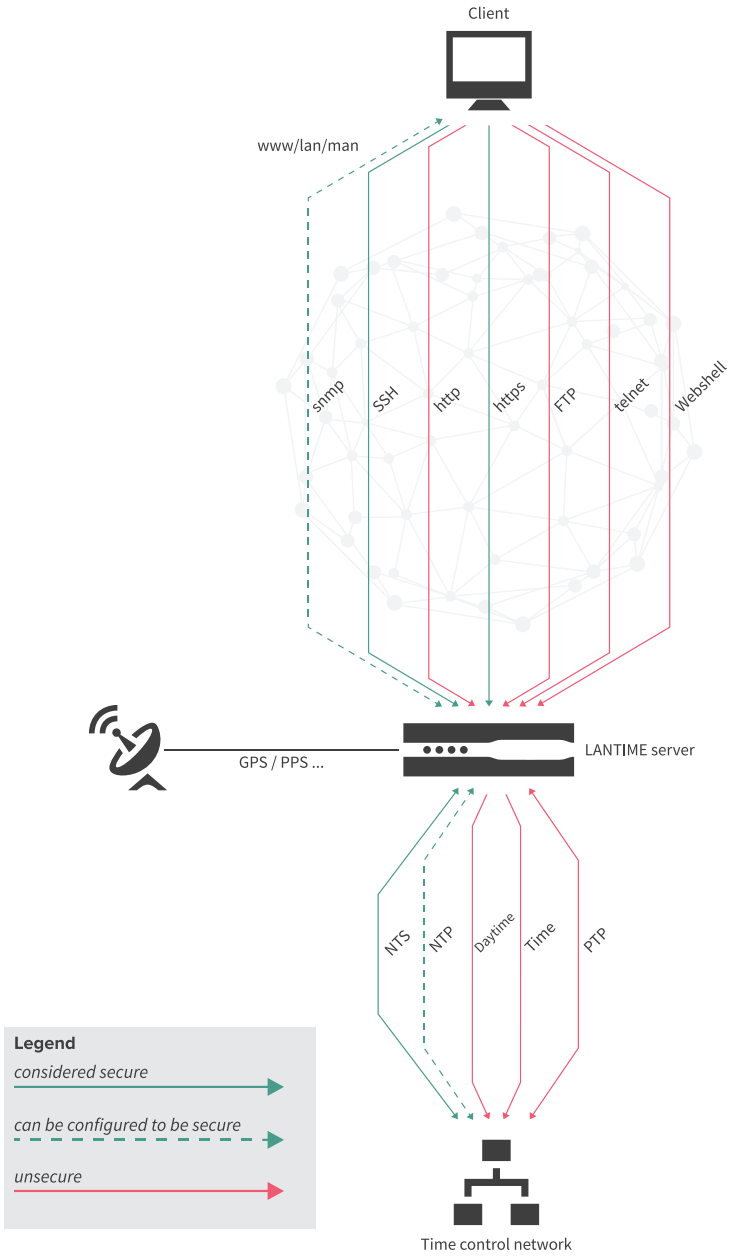


Abbildung 11.1: LANTIME Services

11.1 Allgemeine Informationen

Bevor Sie mit der Konfiguration beginnen, werfen Sie einen Blick auf Abb. 11.1, um die Dienste zu identifizieren, die eine Absicherung zulassen.

Generell ist eine sichere Verwaltung des LANTIME mit SSH, HTTPS und SNMP möglich. Wenn die Konfiguration über SNMP gewünscht wird, ist die Verwendung der Version 3 die einzige Möglichkeit, eine sichere Verbindung zur Verwaltung des Systems herzustellen. Es ist eine gute Vorgehensweise, alle nicht genutzten Dienste zu deaktivieren, um die Angriffsfläche zu minimieren. Wenn möglich, aktivieren Sie also nur einen der Dienste (SNMP hat nicht die volle Konfigurationsunterstützung, aber Sie können die anderen Dienste über SNMP aktivieren)!

Die Bereitstellung von gesicherten Zeitinformationen ist für NTS und NTP verfügbar. Bitte beachten Sie, dass das NTP-Protokoll nur Integrität und Authentizität, aber keine Vertraulichkeit bietet. Das NTS Protokoll erweitert diesen Schutz um die Anonymität von Clients über Netzwerkgrenzen hinweg (es werden auch Daten verschlüsselt, aber nicht die Zeitdaten, da diese nicht als schützenswert angesehen werden). Das NTS-Protokoll sollte dem NTP-Protokoll mit symmetrischen Schlüsseln vorgezogen werden.

Die PTP-Umsetzung im LTOS unterstützt derzeit keine IT-Sicherheitsfunktionen. Aus diesem Grund können Sie nur auf NTS und NTP zurückgreifen, um eine sichere Zeitsynchronisation zu gewährleisten.

Ein weiterer wichtiger Hinweis ist die Verwendung der neuesten Browser und Service-Clients, um die Auswahl der besten Sicherheitsalgorithmen für die Server- und Client-Kommunikation zu unterstützen. Durch die zeitnahe Installation von Updates können zudem bekannte Schwachstellen geschlossen und das Risiko eines erfolgreichen Angriffs minimiert werden.

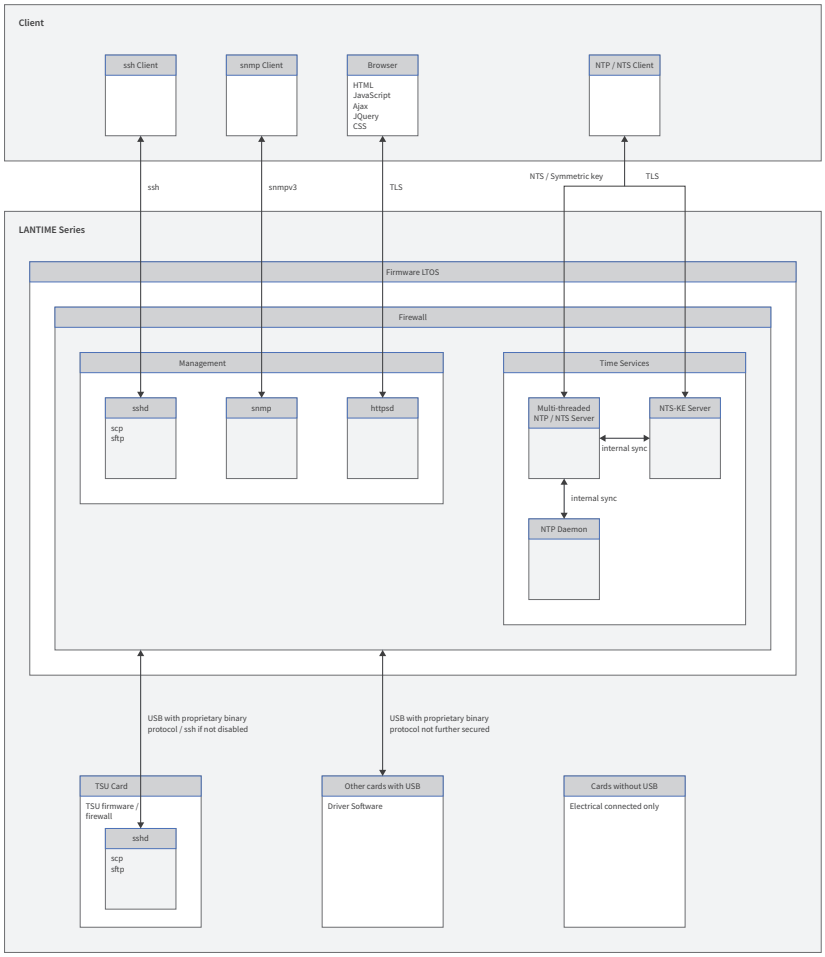


Abbildung 11.2: Die sicheren Protokolle im Detail

Die TSU-Karten von Meinberg bieten in der aktuellen Firmware-Version LTOS V7 nicht mehr die Möglichkeit, netzwerkseitig eine SSH-Verbindung aufzubauen. Der Zugriff ist nur über das CPU-Modul des LANTIME erlaubt. Es besteht weiterhin die Möglichkeit den SSH-Dienst einer TSU-Karte, wie in Abb. 11.3 dargestellt, komplett zu deaktivieren.

Services	Confidentiality	Integ.	Avail.	Auth.	Account.
https	x	x	0	x	(x)
ssh	x	x	0	x	(x)
nts	0	x	0	x	(x)
ntp	-	x	0	x	(x)

Tabelle: Übersicht der Sicherheitsziele

Diese Tabelle zeigt die Sicherheitsziele der Protokolle in der Übersicht. Die Verantwortlichkeit wird durch ein detailliertes Syslog der von jedem Benutzer oder Prozess ausgeführten Aktionen gewährleistet. Die Log-Dateien können jedoch durch root- bzw. super-User nachträglich verändert werden. Aus diesem Grund kann die Nichtabstreitbarkeit durch das System nicht gewährleistet werden. Die größtmögliche Verfügbarkeit der Dienste wird durch aktuelle Updates und IP-Blocking erreicht. Für mehr Schutz implementieren Sie Web Application Firewalls und herkömmliche Firewalls im Netzwerk, die in der Lage sind, DOS/DDOS-Angriffe zu erkennen und zu verhindern.

Bei allen Änderungen an der Konfiguration ist zu beachten, dass sie nach einem Neustart verloren gehen

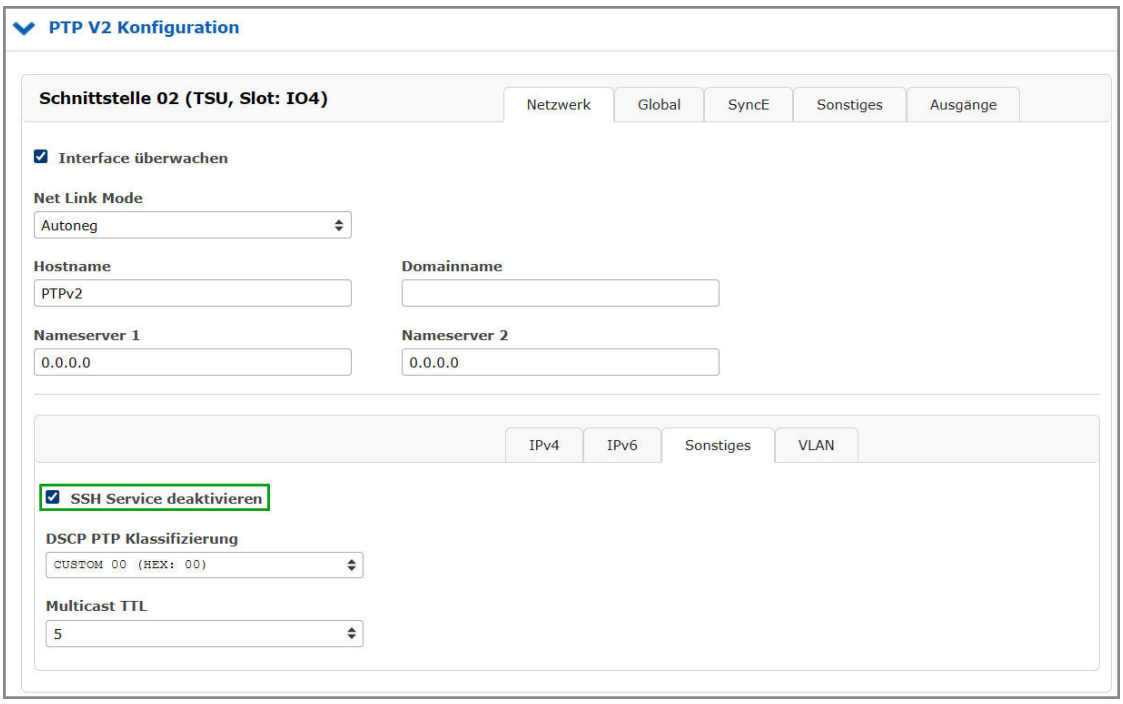


Abbildung 11.3: SSH auf TSU deaktivieren

oder von anderen Admins oder Superusern verworfen werden können, wenn sie nicht in der Startkonfiguration gespeichert sind.

11.2 Sicherstellung des Managements

Der sicherste Weg, einen LANTIME zu konfigurieren, besteht darin, den Client direkt mit dem LANTIME zu verbinden, bis nur noch sichere Kanäle eingerichtet sind. Dieses Handbuch verwendet als Beispiel das Web-Interface über ssl.

Nach dem Anschluss einer Referenzuhr und der folgenden Startprozedur eines LANTIME kann über das Frontpanel eine IP-Adresse konfiguriert werden (siehe Kapitel „LTOS Management und Überwachung → Konfiguration über das Webinterface → Netzwerk“). Jetzt ist es möglich, sich mit der konfigurierten IP-Adresse mit dem Webinterface zu verbinden. Verwenden Sie die Default-Anmeldeinformationen für die initiale Anmeldung:

Benutzer: *root*
Passwort: *timeserver*

Bei der erstmaligen Anmeldung mit den oben genannten Zugangsdaten, werden Sie aufgefordert ein neues Passwort zu wählen. Damit wird sichergestellt, dass die Default-Zugangsdaten geändert werden und Ihr System vor unauthorisiertem Zugriff geschützt ist. Die Abb. 11.4 zeigt den Dialog.

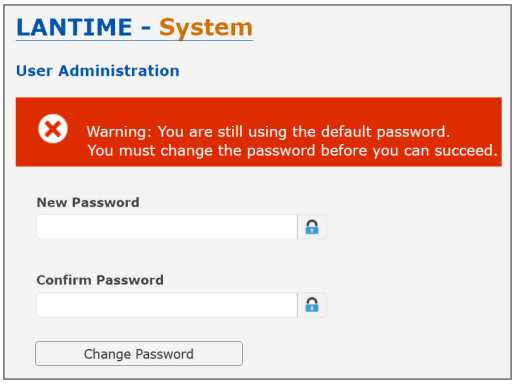


Abbildung 11.4: Neues Passwort für Benutzer „root“ erzwingen

Nach erfolgreicher Verbindung ist zunächst zu prüfen, ob eine neue Firmware-Version vorhanden ist (Update-Anweisungen siehe → Kapitel 13.1.9.14, „Firmwareverwaltung“. Nachdem das Update durchgeführt wurde, erzeugen oder injizieren Sie ein SSL-Zertifikat. In diesem Beispiel wird ein neues Zertifikat verwendet. Abb. 11.5 zeigt die Schaltfläche zum Starten der Zertifikats-Generierung.

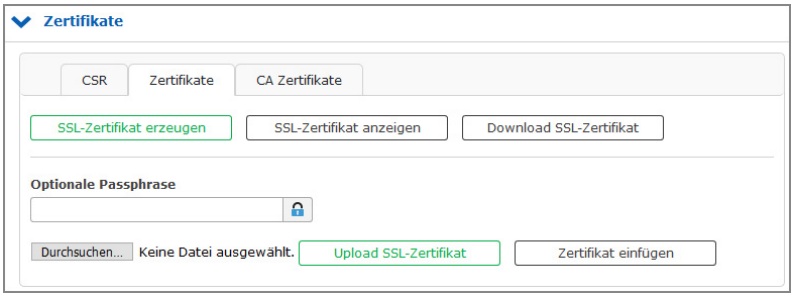


Abbildung 11.5: SSL-Zertifikat generieren - Schritt 1

Im nächsten Schritt müssen Sie die für das Zertifikat erforderlichen Informationen eingeben (siehe auch Kapitel „LTOS Management und Monitoring → Über das Webinterface → Sicherheit → Zertifikate“). Abb. 11.6 zeigt das Formular. Verwenden Sie als Schlüssellänge 2048 oder höher. Kürzere Laufzeiten der Gültigkeitsdauer sind besser als längere. In diesem Beispiel wählen wir drei Jahre als einen guten Wert von kurzer Dauer und akzeptablen Managementkosten.

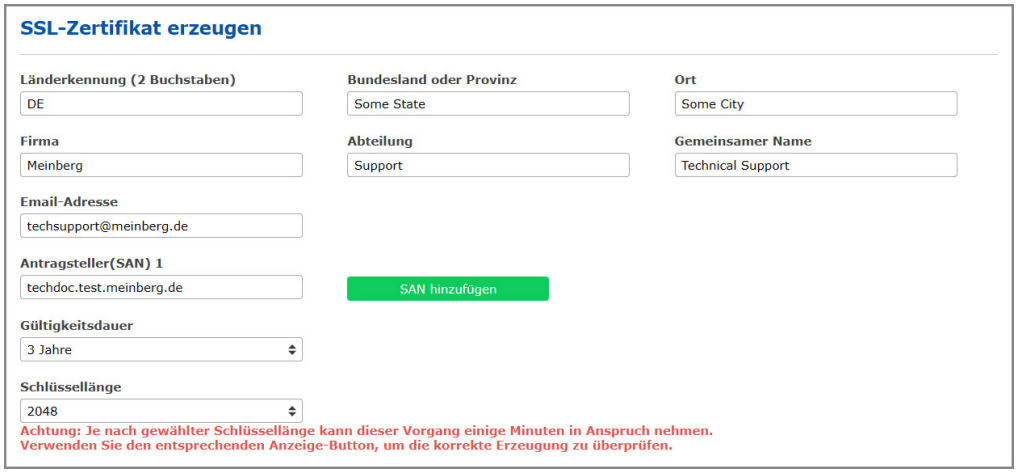


Abbildung 11.6: SSL-Zertifikat generieren Schritt 2

Abbildung 11.7: |Generiertes SSL-Zertifikat anzeigen

Sie können das generierte Zertifikat mit der Schaltfläche „SSL-Zertifikat anzeigen“ ausgeben. Benutzen Sie die Schaltfläche, um es mit dem Zertifikat zu vergleichen, das der Browser bei Ihrer nächsten HTTPS-Verbindung zum LANTIME bereitstellt. Beide sollten identisch sein! Der Importprozess ist in Abb. 11.8 dargestellt. Die Zahlen in der Abbildung beschreiben die Reihenfolge der auszuführenden Aktionen. Die vierte Zahl stellt den Vergleich mit dem zuvor heruntergeladenen Zertifikat des LANTIME dar. Wenn beide Zertifikate identisch sind, können Sie mit Schritt 5 fortfahren, um die Vertrauennswürdigkeit des LANTIME-Zertifikats zu bestätigen. Moderne Browserkonfigurationen zeigen Ihnen, dass die Verbindung nicht sicher ist, wenn Sie ein selbstsigniertes Zertifikat verwenden. Aufgrund dieses Verhaltens empfehlen wir die Implementierung einer Public-Key-Infrastruktur, um die Warnung zu vermeiden. Achten Sie zudem auf die Nutzung eines Subject Alternative Name (SAN), da moderne Browser auch hierauf prüfen. Zu diesem Zweck können Sie eine Zertifikatsanforderung erzeugen, herunterladen, signieren und das signierte Zertifikat über das Web-Frontend in Bild 11.5 wieder hochladen.

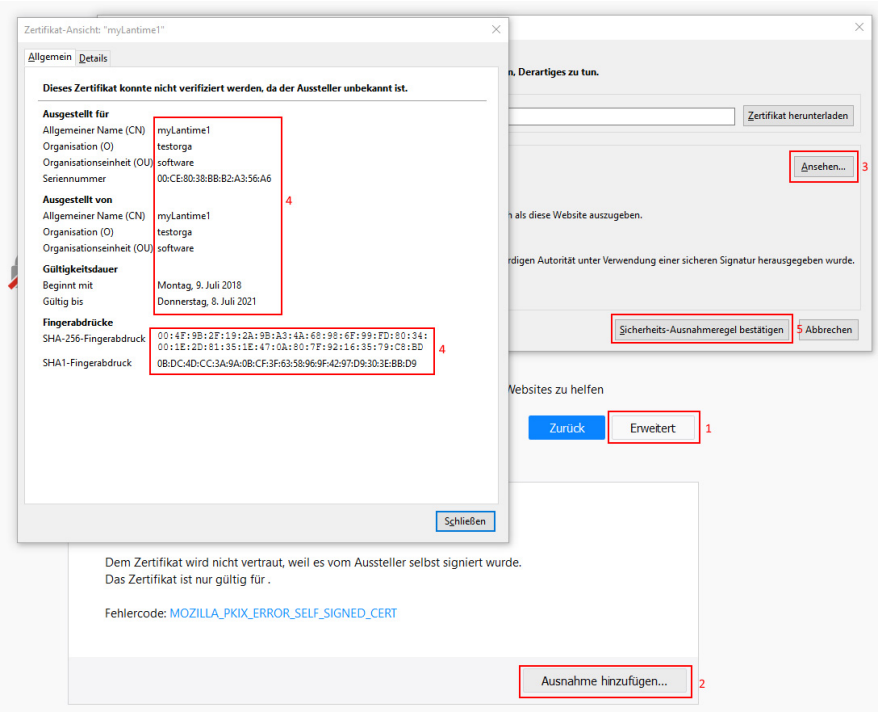


Abbildung 11.8: Importvorgang des neuen SSL-Zertifikats im Browser

Wenn die Verbindung über HTTPS möglich ist, können Sie alle anderen ungenutzten Dienste, wie in Abb. 11.9 angezeigt wird, deaktivieren. Zusätzlich stellt in diesem Beispiel nur eine Netzwerkschnittstelle die HTTPS-Webschnittstelle zur Verfügung. Somit sind auch Szenarien wie ein dediziertes Konfigurationsnetzwerk möglich.

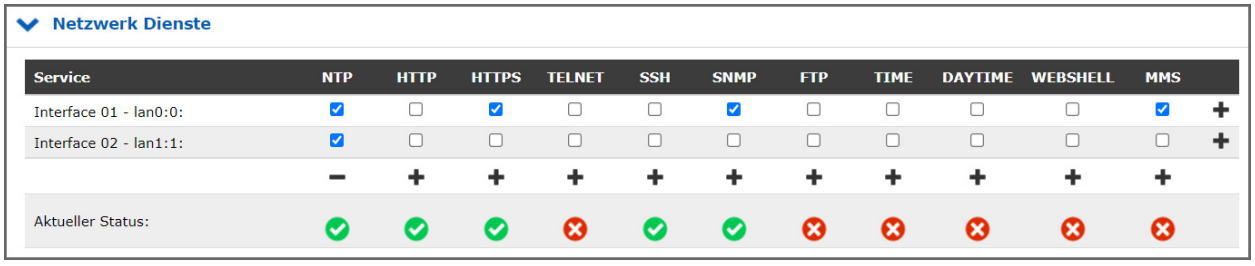


Abbildung 11.9: Dienste deaktivieren

Für den nächsten Schritt wird ein anderer Super-User als root benötigt. Gehen Sie zu Kapitel 13.1.9.4, um einen neuen Super-User zu erstellen. Nachdem Sie den neuen Super-User angelegt haben, melden Sie sich mit seinen Zugangsdaten an und deaktivieren Sie den Root-Login unter „Sicherheit → Anmeldung → Root-Zugang sperren“. Deaktivieren Sie bei Bedarf das Frontpanel unter „Sicherheit → Frontplatte → Frontplatte sperren“, sowie den USB-Anschluss und die lokale Konsole wie in Abb. 11.10 gezeigt wird. Darüber hinaus können Sie die Fernzugriffssteuerung auf autorisierte IP-Adressen einschränken die in einer „Whitelist“ eingetragen sind. (Hinweis: Die Fernzugriffssteuerung wird für SSH-Verbindungen nicht wirksam).

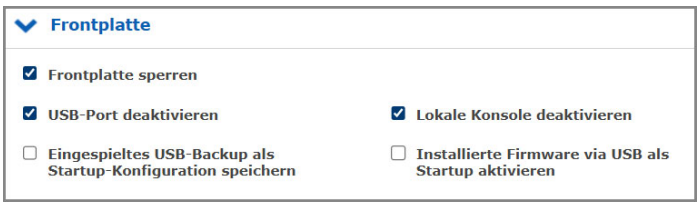


Abbildung 11.10: Sperren des Frontpanels und des USB-Ports

Der Timeout für Web-Sitzungen wird im Webinterface-Menü „Sicherheit“ unter „Anmeldung“ konfiguriert, wie in Abb. 11.11 dargestellt ist. Kürzere Laufzeiten minimieren das Sicherheitsrisiko.

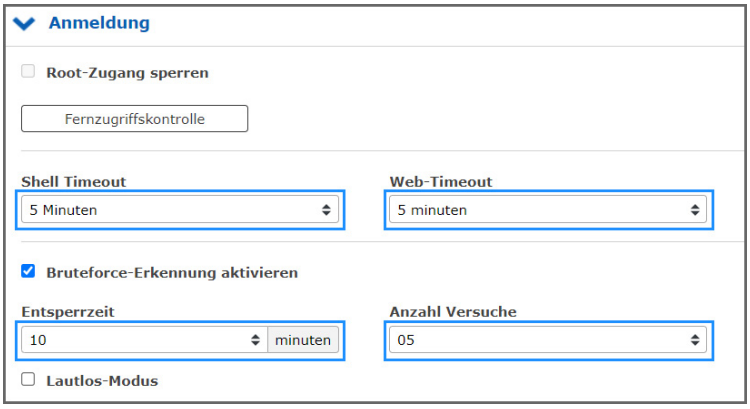


Abbildung 11.11: Timeout der Webschnittstelle einstellen

Bruteforce Angriffe auf Passwortphrasen können mit der Aktivierung von „Sicherheit → Anmeldung → Bruteforce-Erkennung aktivieren“ erschwert werden. Durch das Setzen der Sperrzeit und der Anzahl der Versuche wird die Zeit, wie lange ein Account nach x fehlgeschlagenen Anmeldeversuchen gesperrt wird, vorgegeben. Der Lautlos-Modus kann zusätzlich aktiviert werden, damit keine Ausgabe über den Sperrzustand eines Benutzers über die SSH-Schnittstelle getätigt wird. Dies verhindert das Preisgeben von gültigen Benutzernamen an Angreifer, reduziert jedoch die Nachvollziehbarkeit von Benutzern die versehentlich ihre Login-Daten zu oft falsch eingegeben haben und sich während der Sperrzeit auch mit gültigen Daten nicht anmelden können.

Außerdem kann eine Benachrichtigung „Benachrichtigung → Benachrichtigungen → Faillock: user banned“ aktiviert werden, damit ein gesperrter Benutzer über die konfigurierbaren Kanäle signalisiert wird. Im syslog-auth.log werden die Meldungen über gesperrte Benutzer immer aufgeführt.

Werden alle Schritte befolgt, ist der LANTIME gut konfiguriert, um ihn sicher zu verwaltet und zu überwachen. Denken Sie daran, zu überprüfen, ob die IP-Konfiguration und die Fernzugriffskontrolle in der produktiven Netzwerkumgebung funktionieren.

Optional können Sie SNMP zur Verwaltung des LANTIME konfigurieren. Die Sicherheitsoptionen finden Sie unter „Sicherheit → SNMP“. Abb. 11.12 zeigt das Menü.

Um eine sichere Verbindung über SNMP herzustellen, müssen Sie die Version 3 und den *authPriv-Modus* verwenden. Die zusätzlichen Parameter der Version 3 sind der Benutzername (Sicherheitsname), die Zugriffsrechte, das Authentifizierungs- und Datenschutzprotokoll/Algorithmen. Verwenden Sie SHA512 und AES256 als Algorithmen. Wie üblich werden längere Passwörter bevorzugt. Starten Sie anschließend den SNMP-Dienst auf der Registerkarte „Netzwerk → Netzwerkdienste“.

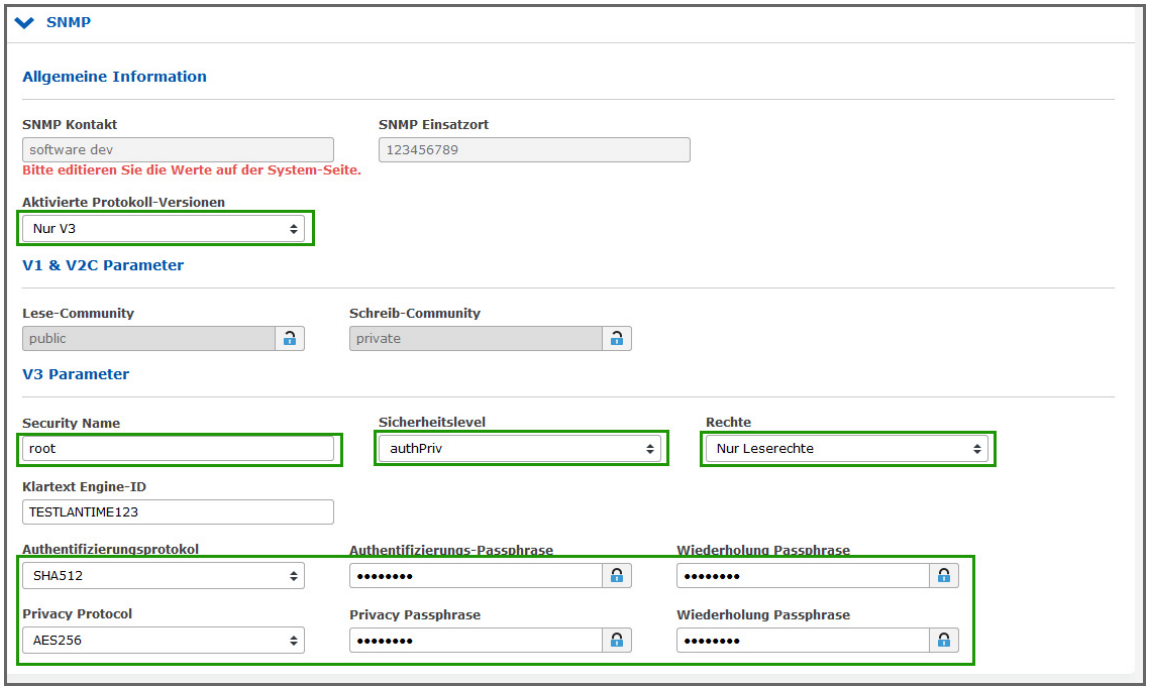


Abbildung 11.12: SNMP Konfiguration

11.3 Benutzer-Management und -Administration

Dieser Abschnitt beschreibt Benutzer- und Authentifizierungsverwaltung. Dieses Kapitel beschreibt die „normale“ Benutzerauthentifizierung und die externen Authentifizierungsserver Radius und TACACS+. Sie können auch im Kapitel „LTOS Management und Überwachung → Über das Webinterface → System → Externe Authentifizierung“ lesen, um weitere Informationen zu erhalten.

11.3.1 LANTIME Benutzerverwaltung

Der LANTIME liefert eine eingebaute Benutzerkonfiguration. Die Optionen finden Sie unter „System → Benutzerverwaltung“.

Es gibt drei verschiedene Benutzergruppen: Super-User, Admin-User und Info-User. Super-User dürfen alles tun, inklusive Bash-Zugang. Admin-User dürfen alles tun, was über die Weboberfläche einzustellen bzw. zu überwachen ist. Sie dürfen aber keine Operationen durchführen, die Superuserrechte vergeben würden. Info-User dürfen nur alle nicht sicherheitsrelevanten Informationen in der Weboberfläche sehen.

Die folgende Tabelle zeigt die Benutzerrechte der einzelnen Zugriffsebenen im Detail.

	Super User	Admin User	Info User
Vollständiger Zugriff auf die Befehlszeile	✓		
Ändern der Gerätekonfiguration durch das Webinterface	✓	✓	
Bearbeitung der zusätzlichen Konfigurationsdateien, die über das Webinterface* verfügbar sind.	✓		
Ausführen eines Firmware-Updates	✓		
Erstellen einer Diagnosedatei	✓		
Erstellen eines neuen Superuser-Accounts	✓		
Überprüfung aller Konfigurationswerte des Webinterfaces	✓	✓	✓

* Zusätzliche Netzwerkkonfiguration, zusätzliche NTP-Konfiguration, benutzerdefinierte Benachrichtigungen

Um einen Benutzer zu erstellen, verwenden Sie das Formular, das in Abb. 11.13 dargestellt ist. Super-User können alle Benutzertypen anlegen. Der Admin-User kann weitere Admin-User und Info-User anlegen. Geben Sie einen Namen, ein Passwort und die Gruppe des Benutzers ein und drücken Sie dann die Schaltfläche „Benutzer anlegen“. Wenn erfolgreich, wird der neue Benutzer in der Benutzerliste direkt unter dem Formular create user angezeigt. Wählen Sie die Benutzernamen und Passwörter so, dass sie nicht vorhersehbar sind.

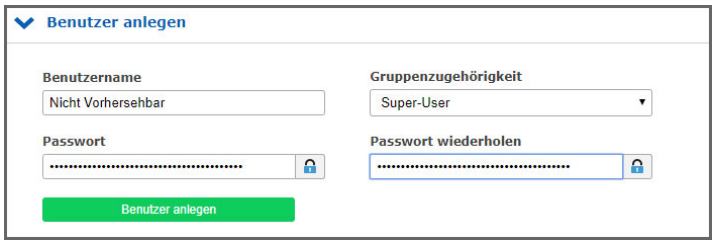


Abbildung 11.13: Einen neuen Super-User erstellen

Abbildung 11.14: Benutzer-Liste

Für Passwörter gibt es einige zusätzliche Optionen, die in Abb. 11.15 zu sehen sind. Wählen Sie eine lange Passwortlänge und ein periodisches Änderungsintervall. Zusätzlich können Sie mit der Einstellung „nur sichere Passwörter zulassen“ ein Passwort erzwingen, das viele verschiedene Zeichensätze enthält.

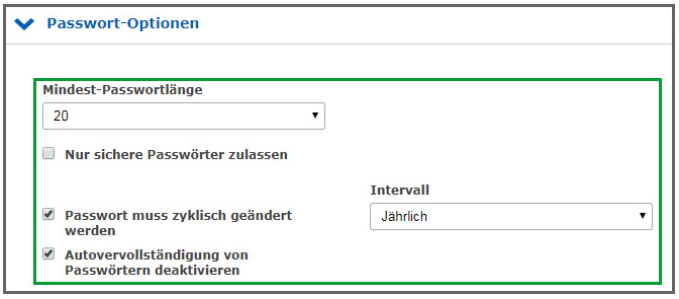


Abbildung 11.15: Passwort-Optionen

11.3.2 Externe Benutzerauthentifizierung: LDAP(S), Radius und TACACS+

Das Kapitel beschreibt die möglichen externen Authentifizierungsmethoden, die von der LANTIME Firmware zur Verfügung gestellt werden.

LDAP (Lightweight Directory Access Protocol)
LDAP basiert auf dem Client-Server-Modell und wird für sogenannte Verzeichnisdienste verwendet. LDAP beschreibt die Kommunikation zwischen dem LDAP-Client und dem Verzeichnisserver. Aus einem solchen Verzeichnis können objektbezogene Daten, wie z.B. Personendaten oder Rechnerkonfigurationen, ausgelesen werden.

RADIUS (Remote Authentication Dial-In User Service)
Ein RADIUS-Server ist ein zentraler Authentifizierungsserver, der von Diensten zur Authentifizierung von Clients in einem physischen oder virtuellen Netzwerk (VPN) verwendet wird. Der RADIUS-Server übernimmt die Authentifizierung für den Dienst, d.h. die Überprüfung von Benutzername und Passwort.

TACACS (Terminal Access Controller Access-Control-System)
TACACS ist ein Kommunikationsprotokoll zur Authentifizierung, das von der IETF standardisiert und weit verbreitet ist. TACACS-Server bieten eine zentrale Authentifizierungsinstanz für Benutzer. In typischen Cisco-Netzwerkumgebungen (z.B. Router und Switches) wird TACACS+ für die zentrale Benutzerverwaltung verwendet.

11.3.2.1 Reihenfolge der Authentifizierungsverfahren

Die Reihenfolge der Authentifizierung stellt sich wie folgt dar, wenn alle Authentifizierungsverfahren (LDAP, RADIUS, TACACS+ und LOKAL) aktiviert und konfiguriert wurden:

1. LDAP
2. RADIUS
3. TACACS+
4. Lokale Anmeldung

Bei gleichen Benutzernamen/Passwortphrasen in unterschiedlichen Systemen ist es also möglich, dass sich die Zugriffsrechte nicht wie gewünscht ergeben. Außerdem kann es so schnell zu intransparenten Log-Nachrichten kommen. Es ist also immer auf die Reihenfolge und konsistente Benutzerdaten/Rechte in den Diensten zu achten.

11.3.2.2 LDAP und LDAPS

Der LANTIME unterstützt die Verbindung zu einem LDAP-Server über LDAP und LDAPS. Meinberg empfiehlt die sichere Kommunikation über LDAPS einzurichten. Dazu muss eine zentrale Vertrauensstelle (RootCA) dem LANTIME bekannt gemacht werden.

Ein Zertifikat einer Zertifizierungsstelle kann über das Webinterface „Sicherheit → Zertifikate → CA Zertifikate“ hochgeladen werden. Der Abschnitt CA Zertifikate beschreibt die Optionen für den Upload von Root-CA-Zertifikaten. Wenn der LDAP-Server ein Zertifikat nutzt, welches von einer globalen Zertifizierungsstelle signiert/ausgestellt wurde, entfällt dieser Schritt. Die Liste von vertrauenswürdigen globalen Zertifizierungsstellen wird mit jedem LANTIME-Update aktualisiert.

Die Konfiguration einer LDAP(S) Anbindung wird im Kapitel „Webinterface → Benutzerverwaltung → Externe Authentifizierung → 13.1.9.7 (LDAP Setup)“ beschrieben.

11.3.2.3 Externe Authentifizierung über LDAP

Die externe Authentifizierung über LDAP kann in dem Webinterface unter „System → Benutzerverwaltung → Benutzer-Administration → Externe Authentifizierung → LDAP / LDAPS“ konfiguriert werden. Die LANTIME-Firmware unterstützt eine anonyme sowie benutzerbezogene Anmeldung. Für eine Microsoft-Active-Directory-Anmeldung muss ein Benutzername (LDAP Benutzer bzw. binddn) und eine Passwortphrase (LDAP Passwort bzw. bindpw) angegeben werden. Die Suchstrategie (Search Scope) für AD-Einträge kann über base (baseObject), one (singleLevel) und sub (wholeSubtree) verändert werden. Der dazugehörige Suchpfad im AD kann über das Feld „Search Base“ angegeben werden.

Ein Beispiel für einen Pfad wäre *„CN=Users,DC=test,DC=mbg,DC=de“*.

Damit die AD-Informationen auf die lokalen Einstellungen abgebildet werden können, müssen „Filter“ und „Mappings“ angelegt werden. Im AD können die Attribute frei gewählt werden, die die Information beinhalten sollen. Ein Filter wird angegeben, um die Ergebnismenge der LDAP-Antwort auf die erforderlichen Attribute zu beschränken. Das Mapping wird benötigt, um von RFC2307 abweichende Attribute des LDAP-Verzeichnisdienstes auf die korrekten im RFC angegeben Attribute, die von dem LDAP-Dienst auf dem LANTIME genutzt werden, abzubilden. Die User-ID für die passwd-Abbildung wird zum Beispiel durch folgendes Mapping von dem frei gewählten Attribut „sAMAccountName“ auf das im RFC2307 dafür vorgesehene Attribut „uid“ abgebildet: *„passwd uid sAMAccountName“*.

Die mindestens anzugebenden Informationen sind:

- Die User-ID (der Anmeldename)
- Die User-ID-Nummer (eine Nummer, die nicht durch einen lokalen Benutzer vergeben ist oder vergeben werden könnte)
- Die User-Gruppen-Nummer (Gruppenzugehörigkeit siehe unten)
- Das User-Home-Verzeichnis (neuer Ordner unter /home/)

Der einzige Wert, der im Verzeichnisserver nicht frei vergeben werden kann, ist die Gruppenzugehörigkeit im LTOS. Folgende Werte können z.B. im „gidNumber“ Attribut hinterlegt werden:

- Die Gruppe Super-User hat die Gruppen-ID = 0
- Die Gruppe Admin-User hat die Gruppen-ID = 4
- Die Gruppe Info-User hat die Gruppen-ID = 100

Die Verbindung zum LDAP-Server kann unter dem Menüpunkt „Global“ angegeben werden, so bald ein neuer LDAP-Server über den Button „LDAP Server hinzufügen“ hinzugefügt wurde. Es kann zwischen „ldap“ und „ldaps“ gewählt werden und es muss die URI des LDAP-Servers angegeben werden.

Hinweis:
Die URI muss bei einer ldaps-Verbindung mit der URI (im Common-Name oder den Subject-Alternative-Names) des LDAP-Server-Zertifikats übereinstimmen, da sonst die Verifizierung fehlschlägt.

Der Modus steuert, ob ein konfigurierter LDAP-Server angefragt wird. Sollte der Port vom Standard (389, 636) abweichen, kann über das Feld „Alternativer Port“ ein anderer ausgewählt werden. Über den Reiter „Misc“ können LDAP-Server wieder entfernt werden. Wenn alles eingestellt ist müssen die Einstellungen über den Button **„Speichern“** in die laufende Konfiguration übernommen werden. Nach dem Funktionstest kann die laufende Konfiguration als Startkonfiguration gespeichert werden.

Fehlermeldungen des ldap-Dienstes können über die System-Messages (CLI oder WEB) eingesehen werden. Authentifizierungsgfehler werden in die Datei */var/log/auth.log* geschrieben.

11.3.2.4 Radius- und TACACS+-Verbindung

Zusätzlich zu den von LANTIME selbst verwalteten Benutzern kann eine Radius- oder TACACS+-Verbindung zur Authentifizierung von Benutzern verwendet werden. Diese Verbindung muss in der Benutzerverwaltung unter „Externen Authentifizierungsserver erlauben“ freigegeben werden. Siehe Abb. 11.16 für die Eingabemöglichkeiten. Sie müssen zuerst die externe Authentifizierung aktivieren. Wählen Sie anschließend Radius oder TACACS+ aus dem Dropdown-Menü und geben Sie den Hostnamen, den vorab ausgetauschten Schlüssel und den korrekten Port ein. Von nun an ist es möglich, sich mit dem externen Authentifizierungsmechanismus anzumelden. Zunächst prüft das System den externen Server auf den Benutzer. Wenn kein Benutzer mit diesen Zugangsdaten existiert, prüft das System die lokalen Benutzer. Wie man einen externen Authentifizierungsserver konfiguriert wird im Kapitel „LTOS Management und Monitoring → Webinterface → Externe Authentifizierung“ beschrieben.

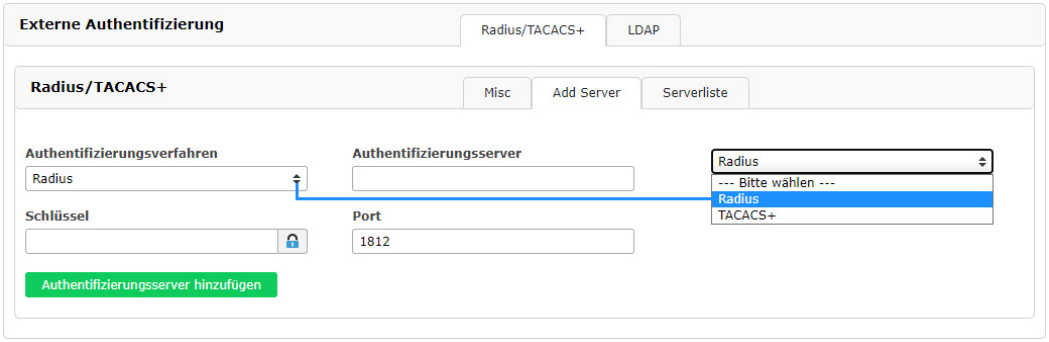


Abbildung 11.16: Webinterface Menü „System → Benutzerverwaltung → Externe Authentifizierung“

11.4 Absicherung von NTP und NTS

11.4.1 Sicherung des NTP-Zeitdienstes

Der NTP-Zeitdienst bietet mehrere Verfahren für eine authentifizierte und integritätsgesicherte Paketübertragung an. Derzeit gilt das NTP-Autokey-Verfahren als unsicher, weshalb dieser Leitfaden ausschließlich die Konfiguration des symmetrischen Schlüsselverfahrens und Network Time Security beschreibt.

Das Kapitel „LTOS Management und Überwachung → Über das Webinterface → NTP“ beschreibt alle Konfigurationsmöglichkeiten im Detail.

11.4.1.1 Konfiguration des symmetrischen Schlüsselverfahrens

Um eine Verbindung zu konfigurieren, benötigt das System einen Schlüssel. Verwenden Sie entweder neu generierte oder fügen Sie vorhandene Schlüssel in der Schlüsseldatei über die Schaltfläche **NTP-Schlüssel bearbeiten** im Menü „NTP → NTP Symmetrische Schlüssel“ hinzu. Wenn Sie die Schlüssel vom System automatisch generieren lassen, sind MD5 und SHA1 Schlüssel in der Schlüsseldatei vorhanden. Für die derzeit höchste Sicherheit sind jedoch AES128-CMAC Schlüssel zu verwenden. Diese können noch nicht automatisch generiert werden.

Wie Sie AES128-CMAC-Schlüssel erzeugen können, wird im Kapitel „Konfiguration → Webinterface → NTP → NTP Symmetrische Schlüssel“ beschrieben.

Die Abb. 11.17 zeigt Beispiele für generierte und modifizierte (AES128CMAC) NTP-Schlüssel. Die Schlüssel-IDs müssen den vertrauenswürdigen Schlüsseln im Menüpunkt „Allgemeine Einstellungen“ in der Registerkarte NTP hinzugefügt werden (siehe Abb. 11.18. Im Menü „NTP Zugriffsbeschränkung“ können Sie auch die Paketunterstützung für Modus 6 und 7 deaktivieren. Optional können Sie hier die Zugriffsbeschränkung aktivieren, um den Zugriff nur auf bekannte IP-Adressen zu ermöglichen. Die symmetrischen Schlüssel werden für jeden Verbindungstyp verwendet, d.h. Server zu Client, externer NTP-Server, Broadcast, Multicasting und Manycasting.

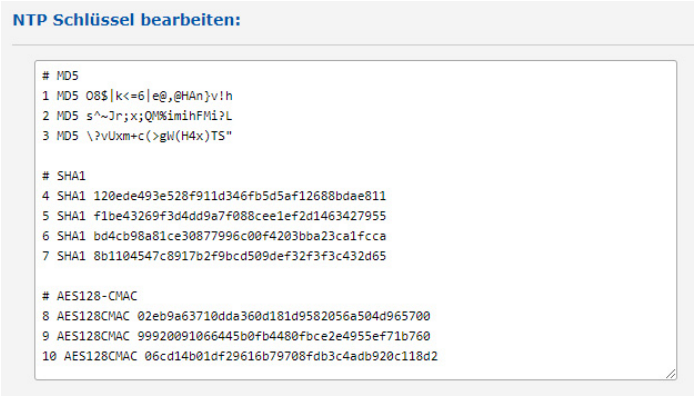


Abbildung 11.17: Symmetrische NTP-Schlüssel

Abbildung 11.18: Vertrauenswürdige Schlüssel-IDs

Die Einfügepunkte für die richtigen Schlüssel-IDs sind in Abb. 11.19, Abb. 11.20 und Abb. 11.21 markiert. Die Konfigurationsdatei eines Clients ist in Abb. 11.22 dargestellt. Sie enthält den Pfad zur Schlüsseldatei, die vertrauenswürdigen Schlüssel-IDs und die Server-IP, die in diesem Beispiel den Schlüssel mit der ID 1 verwendet.

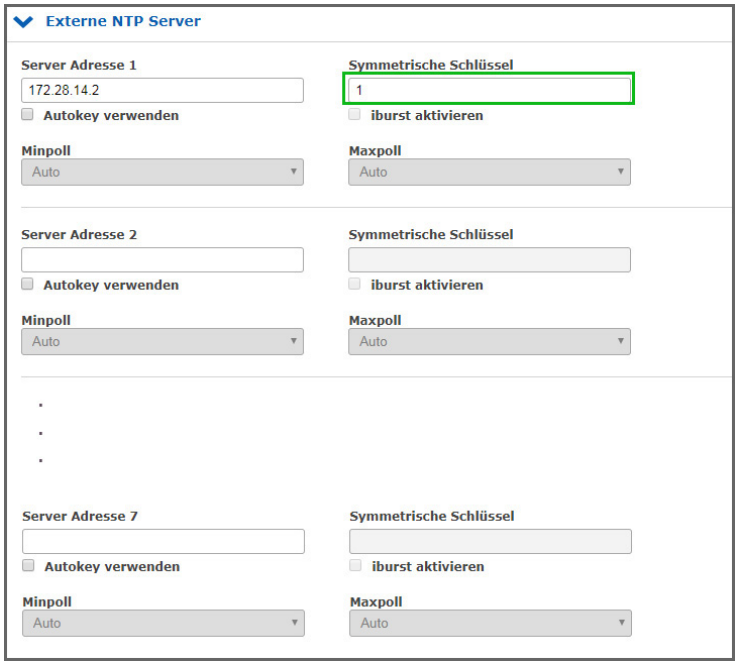


Abbildung 11.19: Externe Severkonfiguration

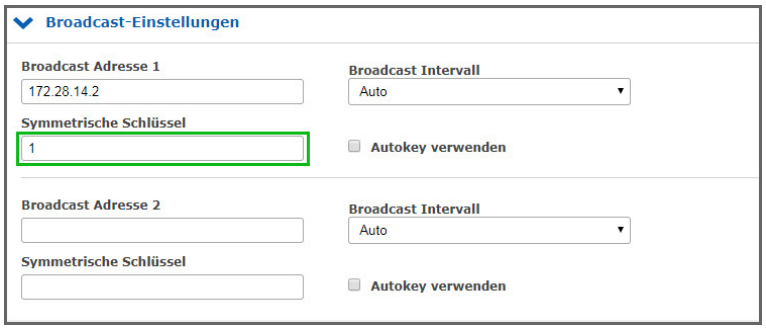


Abbildung 11.20: Broadcast-Konfiguration

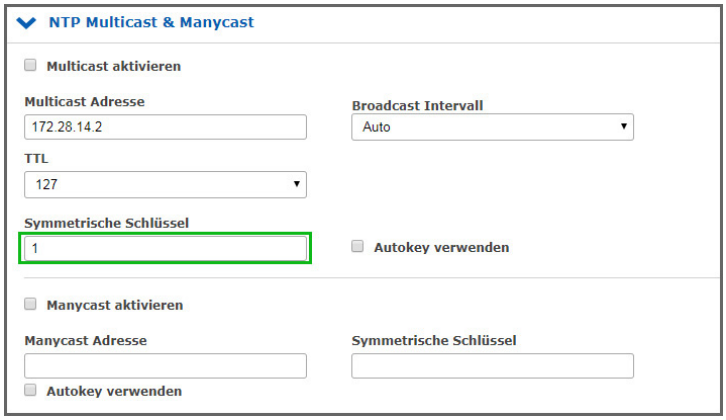


Abbildung 11.21: Multi- und Manycast-Konfiguration

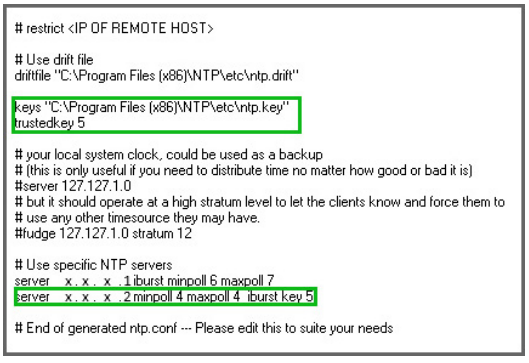


Abbildung 11.22: NTP Client-Konfiguration

11.4.2 Konfiguration von Network Time Security (NTS)

Mit Version 7.08 unterstützt die LTOS-Firmware Network Time Security (NTS) sowohl im Server- als auch im Client-Betrieb.

Hinweis:

Hinweis: NTS ist in der Light-Version der LTOS-Firmware nicht verfügbar.

11.4.2.1 Konfiguration des LANTIME-Gerätes als NTS-Server

Hinweis:

Diese Option ist auf LANTIME-Geräten mit CPU Modul-Typ C05F1 nicht verfügbar.

Der NTS-Server-Modus setzt sich aus einem NTS-KE-Server und einem NTS-fähigen NTP-Server zusammen. Der NTS-KE-Server nutzt für den TLS-basierten Austausch von Schlüsselmaterial dasselbe SSL-Zertifikat, welches auch vom Web-Server für HTTPS zum Einsatz kommt.

Grundvoraussetzung für den Betrieb des LANTIME-Gerätes als NTS-Server ist daher das Vorhandensein eines SSL-Zertifikats. Wie ein SSL-Zertifikat erzeugt oder injiziert werden kann, beschreiben die
→ Kapitel 11.2, „Sicherstellung des Managements“ und → Kapitel 13.1.5.4, „Zertifikate“.

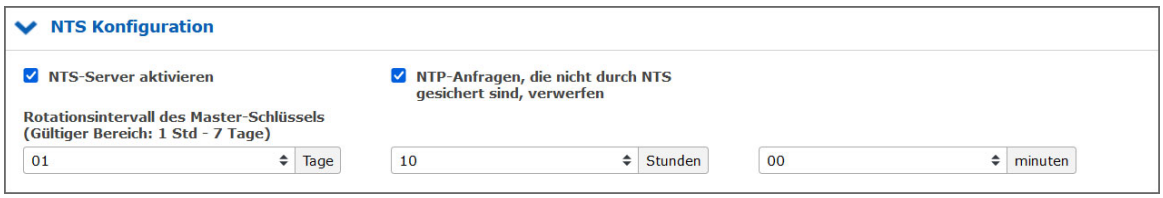


Abbildung 11.23: Webinterface Menü „NTP → NTS-Konfiguration“

Um den NTS-Server-Modus zu aktivieren, muss nun unter „NTP → NTS Konfiguration“ der Haken „NTS-Server aktivieren“ gesetzt sein (siehe Abb. 11.23).

11.4.2.2 Konfiguration von Network Time Security für externe NTP-Server

Hinweis: Diese Option ist derzeit nur auf LANTIME/MRS-Geräten verfügbar.

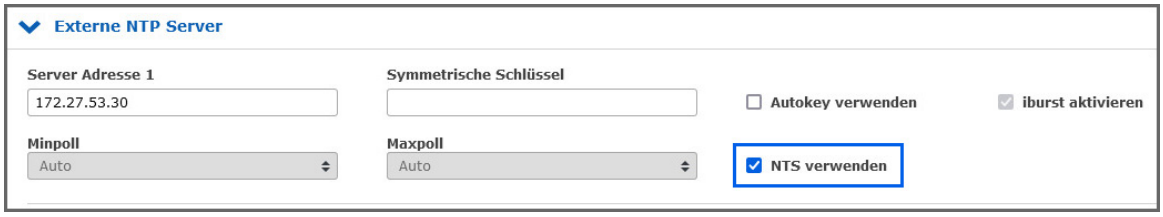


Abbildung 11.24: Externe NTP-Server

Um die NTS-gesicherte Zeitsynchronisation mit externen NTP-Servern zu aktivieren, muss im Menü „NTP → Externe NTP-Server“ der Haken „NTS Verwenden“ gesetzt sein (siehe Abb. 11.24). In diesem Fall muss in das Feld „Server Adresse“ die IP-Adresse oder der Hostname des dazugehörigen NTS-KE-Servers eingetragen werden.

Handelt es sich dabei um einen NTS-KE-Server, dessen TLS-Zertifikat von einer öffentlichen Zertifizierungsstelle signiert wurde, sind in der Regel keine weiteren Schritte notwendig. Es ist darauf zu achten, dass im Menü „Sicherheit → Zertifikate → CA Zertifikate“ die systemeigenen Wurzelzertifikate mit berücksichtigt werden.

Handelt es sich hingegen um einen nicht-öffentlichen NTS-KE-Server, muss das dazugehörige Wurzelzertifikat auf dem LANTIME-Gerät vorhanden sein. Verfolgen Sie dazu die in dem → Kapitel 13.1.5.5, „CA Zertifikate“ beschriebenen Schritte zum Hochladen eigener CA-Zertifikate.

11.5 Ausgabe von Ereignisprotokollen

Der LANTIME bietet viele Transportkanäle für Ereignisprotokollinformationen und eine fein abgestufte Benachrichtigungsauswahl für jeden dieser Kanäle. Derzeit kann von den Ereignistransportkanälen **syslog** und **SNMPv3** abgesichert werden. Es ist eine gute Praxis, Ereignisprotokollinformationen auf einem zentralen Server zu sammeln, um sie zu korrelieren und auf Anomalien zu überprüfen. Beachten Sie dabei mögliche sicherheitsrelevante Informationslecks aufgrund der fehlenden Verschlüsselung bei anderen Diensten als **syslog** und **SNMPv3**.

Externe syslog-Server können unter „Benachrichtigungen → Externe Syslogserver“ konfiguriert werden. Um diese sicher anzusprechen, muss das Transport-Protokoll „TLS“ gewählt werden. Die vollständigen Konfigurationsmöglichkeiten werden im ➜ Kapitel 13.1.4.1, „Externe Syslog-Server“ beschrieben.

Das Kapitel „LTOS Management und Monitoring → Über das Webinterface → Benachrichtigung“ beschreibt die Konfigurationsmöglichkeiten für die Transportkanäle. Wenn Sie **SNMPv3** mit der gewählten **authPriv**-Sicherheitsstufe verwenden, werden auch SNMP-Traps sicher versendet. Konfigurieren Sie die SNMP authPriv-Einstellung wie unter „Sicherheit → SNMP“ wie im ➜ Kapitel 11.2, „Sicherstellung des Managements“ beschrieben.

11.6 Aktualisieren und Sichern der LANTIME-Firmware

Laden Sie die neueste LTOS-Version unter https://www.meinberg.de/german/sw/firmware.htm herunter. Die heruntergeladene LTOS-Datei muss über die LANTIME-Weboberfläche unter „System → Firmware/Software Update“, wie in Abb. 11.25 dargestellt, hochgeladen werden. Die LTOS V7 Firmware ist mit einer digitalen Signatur ausgestattet, die beim Test „Preflight Checks“ direkt nach dem Upload überprüft wird. Sollte dieser Test eine fehlerhafte Signatur feststellen, wird eine Warnung ausgegeben und der Update-Prozess wird abgebrochen, wie in Abb. 11.26 gezeigt. Wenn dies geschieht, laden Sie die neue Firmware erneut von der Meinberg Web-Seite und wiederholen Sie den Vorgang. Bei wiederholten Warnungen kontaktieren Sie bitte den Meinberg-Support.

Im nächsten Schritt müssen Sie das Update bestätigen und die neue Firmware, wie in Abb. 11.26 gezeigt, aktivieren. Das Update war erfolgreich, wenn Abb. 11.27 angezeigt wird.

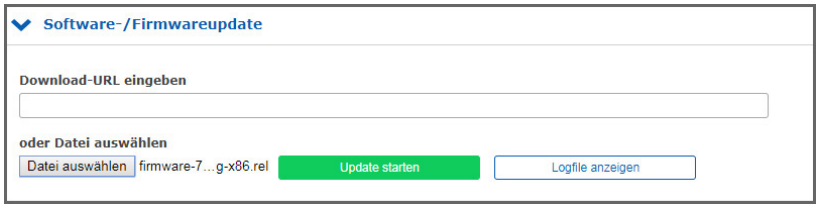


Abbildung 11.25: Firmware auswählen und hochladen

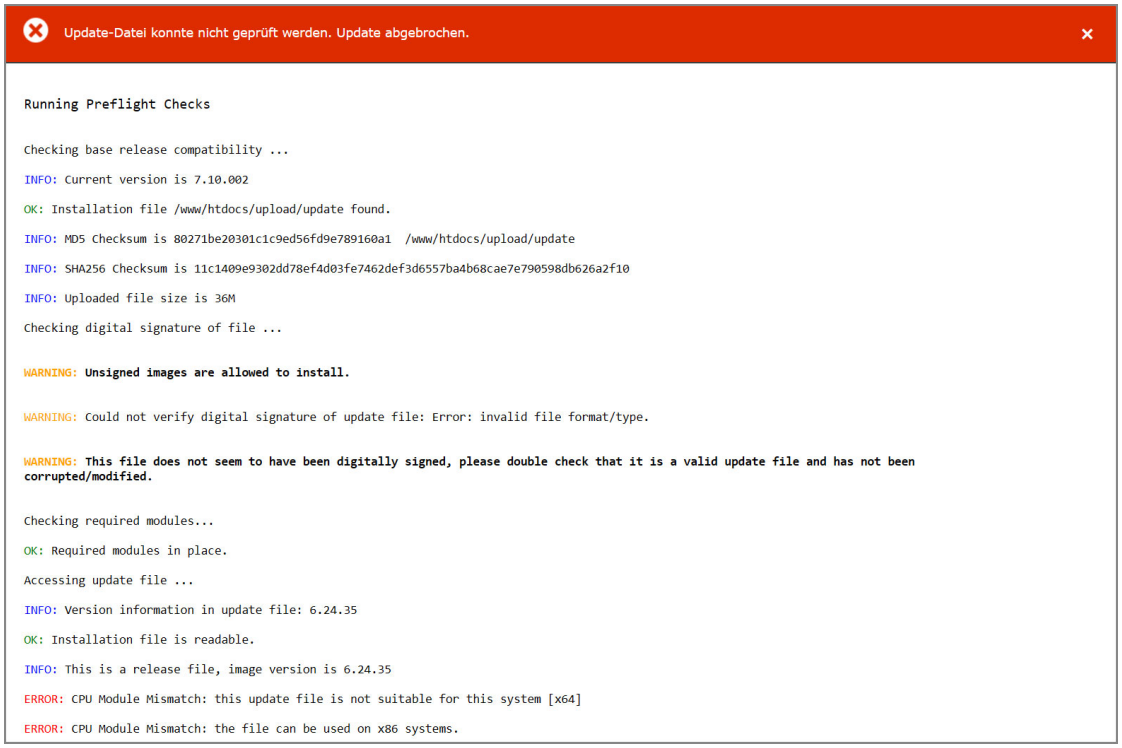


Abbildung 11.26: Firmware-Update-Prozedur - Preflight Check

Die Konfigurationseinstellungen des LANTIME bleiben bei einem Firmware Update erhalten, mit Ausnahme der

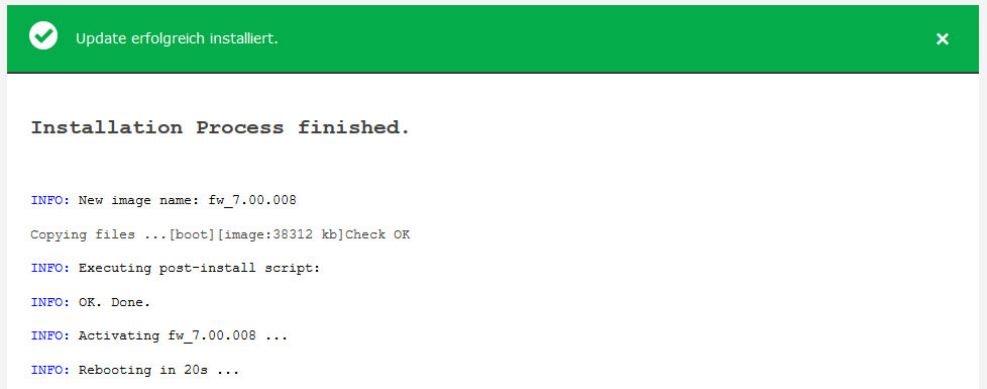


Abbildung 11.27: Firmware wurde aktualisiert

Konfigurationsdateien des Webservers und des SSH-Dienstes. Diese werden bei einem Update überschrieben, um aktuelle kryptografische Verfahren mit einem Update ausliefern zu können. Sollte die automatische Aktualisierung entgegen unserer Empfehlung nicht gewünscht sein, kann eine eigene kundenspezifische Konfigurationsdatei für diese Dienste hinterlegt werden.

SSH Konfiguration:
In der Konfigurationsdatei */etc/ssh/ssh.cfg* wird definiert, welche Konfigurationsdatei der SSH-Dienst verwenden soll. In der Werkskonfiguration enthält die Datei folgenden Eintrag:

```
[SSHD]
CONFIGFILE=/etc/standard/sshd_config
```

Sofern die Datei */etc/standard/sshd_config* als SSH-Konfigurationsdatei definiert ist, wird diese Datei bei einem Firmware-Update aktualisiert. Ist die Datei */etc/ssh/sshd_config* eingetragen, kann in dieser eine eigene Konfiguration angelegt werden, die bei einem Update nicht ersetzt wird.

Webserver Konfiguration:
In der Konfigurationsdatei */etc/webUI/webUI_custom.cfg* wird definiert, welche Konfigurationsdatei der Webserver verwenden soll. In der Werkskonfiguration enthält die Datei folgenden Eintrag:

```
[CUSTOM CONFIGURATION]
CUSTOM_CONFIG_PATH=
```

Sofern keine Datei als Webserver-Konfigurationsdatei definiert ist wird die Werkskonfigurationsdatei, die bei einem Firmware-Update aktualisiert wird, verwendet. Ist eine beliebige Datei unter */mnt/flash/data/* eingetragen, kann in dieser eine eigene Konfiguration angelegt werden, die bei einem Update nicht ersetzt wird. Dateien, die unter */mnt/flash/data* abgelegt werden sind nicht Teil einer Konfiguration, sie sind jedoch rebootsicher (persistent) gespeichert.

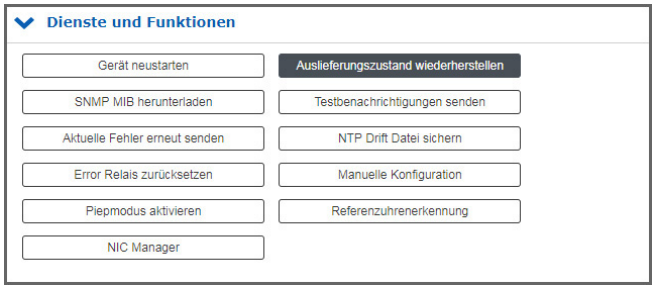


Abbildung 11.28: LANTIME auf Werkseinstellungen zurücksetzen

Damit der SSH-Dienst und der Webserver wieder automatische Konfigurationsupdates erhalten, können Sie die werksseitigen Pfade in diesen beiden Dateien wiederherstellen.

Das Wiederherstellen der werksseitigen Standardeinstellungen über das Webinterface, wie in Abb. 11.28 gezeigt, bewirkt, dass alle benutzerdefinierten Konfigurationseinstellungen bis auf die Netzwerkeinstellungen in der aktuellen Startup-Konfiguration zurückgesetzt werden. Im Detail bedeutet dies, dass u.a. Ihre Zertifikate, Zugangsdaten, SNMP, NTP und SSH-Schlüssel verloren gehen. Zuvor unter einem anderen Namen gespeicherte Konfigurationen bleiben auch bei einem Factory-Reset erhalten. Diese müssen, wenn gewünscht, zusätzlich über das Webinterface gelöscht werden.

Nach einem „Reset“ der Firmware über die Webschnittstelle werden alle Zertifikate auf die werkseitigen Voreinstellungen umgestellt. Der SSH-Schlüssel wird beim Hochfahren nach dem Reset zufällig neu generiert.

Ein Backup der LANTIME-Firmware, ob heruntergeladen oder auf der Flash-Speicherkarte des LANTIME gespeichert, erfolgt in Klartextform. Achten Sie daher darauf, dass kein Unbefugter Zugriff darauf hat. Das Gleiche gilt für eine Diagnosedatei.

12 Funkempfang (Antennen)

Es gibt 2 Arten von Funksignalen, die häufig für Timing-Anwendungen verwendet werden: **Satellitensignale von Global Navigation Satellite Systems (GNSS)**, und **Langwellensignale** von bestimmten lokalen Zeitzeichen-Sendern, die in einigen Ländern betrieben werden.

Die meisten GNSS-Signale können weltweit empfangen werden, während langwellige Signale nur bis zu einer bestimmten Entfernung um die Sendestation herum empfangen werden können. Außerdem können GNSS-Empfänger in der Regel die Signale mehrerer Satelliten gleichzeitig verfolgen, so dass die Signallaufzeit automatisch bestimmt und kompensiert werden kann, während Langwellenempfänger in der Regel nur das Signal einer einzelnen Station empfangen. Nicht zuletzt sind die verfügbaren Bandbreiten und Signalausbreitungseigenschaften ein weiterer Grund, warum der GNSS-Empfang in der Regel ein höheres Maß an Zeitgenauigkeit bietet als der Langwellenempfang.

12.1 Referenz-Zeitquellen

12.1.1 Meinberg GPS Empfänger

Unsere Satelliten-Funkuhr wurde mit dem Ziel entwickelt, dem Anwender eine hochgenaue Zeit- und Frequenzreferenz zu liefern. Hohe Genauigkeit und die Möglichkeit des weltweiten Einsatzes, 24 Stunden am Tag, sind die Hauptmerkmale dieses Systems, das seine Zeitinformationen von den Satelliten des Global Positioning System erhält. Das Global Positioning System (GPS) ist ein satellitengestütztes System zur Funkortung, Navigation und Zeitübertragung.

Dieses System wurde vom United States Department of Defense (Verteidigungsministeriom) installiert und bietet zwei Genauigkeitsstufen: den Standard Positioning Service (SPS) und den Precise Positioning Service (PPS).

Die Struktur der Sendedaten des SPS wurde freigegeben und der Empfang für den allgemeinen Gebrauch zur Verfügung gestellt, während die Zeit- und Navigationsdaten des noch genaueren PPS verschlüsselt übertragen werden und somit nur für bestimmte Benutzer (meist für militärisch Zwecke) zugänglich sind. Das Prinzip der Orts- und Zeitbestimmung mit Hilfe eines GPS-Empfängers basiert auf einer möglichst genauen Messung der Signallaufzeit von den einzelnen Satelliten zum Empfänger.

Die GPS-Satelliten umkreisen die Erde auf sechs Orbitalbahnen, in 20.000 km Höhe, einmal in etwa 12 Stunden. Damit ist sichergestellt, dass zu jeder Zeit mindestens vier Satelliten an jedem Punkt der Erde in Sichtweite sind. Vier Satelliten müssen gleichzeitig empfangen werden, damit der Empfänger seine räumliche Position (x, y, z) und die Abweichung seiner Uhr von der GPS-Systemzeit bestimmen kann.

Kontrollstationen auf der Erde messen die Umlaufbahnen der Satelliten und erfassen die Abweichungen der an Bord mitgeführten „Atomuhren“ von der GPS-Systemzeit. Die ermittelten Daten werden an die Satelliten gesendet und von den Satelliten als Navigationsdaten zur Erde zurückgesendet. Die hochpräzisen Bahndaten der Satelliten, die sogenannten Ephemeriden, werden benötigt, damit der Empfänger jederzeit die genaue Position der Satelliten im Weltraum berechnen kann.

Ein Satz von Bahndaten mit reduzierter Genauigkeit wird als Almanach bezeichnet. Mit Hilfe der Almanache berechnet der Empfänger zu ungefähr bekannter Position und Zeit, welche der Satelliten von seinem Standort aus sichtbar sind. Jeder der Satelliten sendet seine eigenen Ephemeriden sowie die Almanache aller vorhandenen Satelliten. Die GPS-Uhr arbeitet mit dem „Standard Positioning Service“. Der Datenstrom der Satelliten wird vom Mikroprozessor des Systems dekodiert und ausgewertet, so dass die GPS-Systemzeit mit einer Abweichung von weniger als 100 nsec wiedergegeben wird.

Unterschiedliche Laufzeiten der Signale von den Satelliten zum Empfänger werden durch die Bestimmung der Empfängerposition automatisch kompensiert. Durch die Nachführung des Hauptoszillators wird je nach Oszillatortyp eine Frequenzgenauigkeit von 1e-12 erreicht. Gleichzeitig wird die altersbedingte Drift kompensiert.

Der aktuelle Korrekturwert des Oszillators wird in einem nichtflüchtigen Speicher des Systems gespeichert.

12.1.2 Meinberg GNSS-Empfänger (GPS, GLONASS, Galileo, BeiDou)

Hohe Genauigkeit und die Möglichkeit des weltweiten Einsatzes rund um die Uhr sind die Hauptmerkmale des Systems, das seine Zeitinformationen von den Satelliten des amerikanischen GPS (Global Positioning System), des europäischen Galileo, des russischen GLONASS (Global Navigation Satellite System) und des chinesischen BeiDou erhält.

GPS wurde vom Verteidigungsministerium der USA (US Department Of Defense) installiert und arbeitet mit zwei Genauigkeitsklassen: den Standard Positioning Services (SPS) und den Precise Positioning Services (PPS). Die Struktur der gesendeten Daten des SPS ist veröffentlicht und der Empfang zur allgemeinen Nutzung freigegeben worden, während die Zeit- und Navigationsdaten des noch genaueren PPS verschlüsselt gesendet werden und daher nur bestimmten (meist militärischen) Anwendern zugänglich sind.

GLONASS wurde ursprünglich vom russischen Militär zur Echtzeit-Navigation und Zielführung von ballistischen Raketen entwickelt. Auch GLONASS-Satelliten senden zwei Arten von Signalen: ein Standard Precision Signal (SP) und ein verschleiertes High Precision Signal (HP).

BeiDou ist ein chinesisches Satellitennavigationssystem. Die zweite Generation des Systems, die offiziell als BeiDou-Navigationssatellitensystem (BDS) bezeichnet wird und auch unter dem Namen „COMPASS“ bekannt ist, besteht aus 35 Satelliten. BeiDou wurde im Dezember 2011 mit 10 Satelliten in Betrieb genommen, die für Dienstleistungen für Kunden im asiatisch-pazifischen Raum zur Verfügung gestellt wurden. Das System wurde Juni 2020 mit dem Start des letzten Satelliten fertiggestellt.

Galileo ist ein im Aufbau befindliches europäisches globales Satellitennavigations- und Zeitgebungssystem unter ziviler Kontrolle (European Union Agency for the Space Programme, EUSPA). Es soll weltweit Daten zur genauen Positionsbestimmung liefern und ähnelt im Aufbau dem US-amerikanischen GPS, dem russischen GLONASS und dem chinesischen Beidou-System. Die Systeme unterscheiden sich grundsätzlich teilweise nur durch Frequenznutzungs-/Modulationskonzepte und die Satellitenkonstellation.

Merkmale
Das GNS-Modul ist ein kombinierter GPS / Galileo / GLONASS / BeiDou-Empfänger und arbeitet mit dem „Standard Positioning Service“ (GPS) oder „Standard Precision“ (Galileo, GLONASS, BeiDou). Der Datenstrom von den Satelliten wird vom Mikroprozessor des Systems dekodiert. Durch die Analyse der Daten kann die GNSS-Systemzeit sehr genau reproduziert werden. Unterschiedliche Laufzeiten der Signale von den Satelliten zum Empfänger werden durch die Bestimmung der Empfängerposition automatisch kompensiert. Durch die Nachführung des Hauptoszillators (z.B. Oven Controlled Xtal Oscillator, OCXO) wird eine hohe Frequenzgenauigkeit erreicht. Gleichzeitig wird die altersbedingte Drift des Quarzes kompensiert. Der aktuelle Korrekturwert für den Oszillator wird in einem nichtflüchtigen Speicher des Systems gespeichert. Dieser Empfänger ist nicht nur für den stationären Betrieb, sondern auch für den mobilen Einsatz geeignet.

Der Meinberg GLN-Empfänger ist der Vorgänger der GNS-Uhr und empfängt GPS, Glonass und BeiDou.

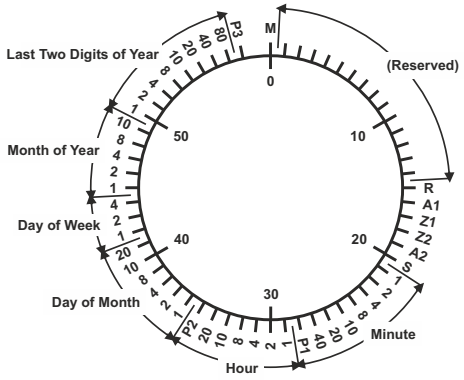
12.1.3 PZF Langwellen-Empfänger

Der deutsche Langwellensender DCF77 nahm 1970 den Dauerbetrieb auf. Die Einführung von Zeitcodes im Jahr 1973 bildet die Grundlage für die Entwicklung moderner Funkuhren. Die DCF77-Frequenz und das DCF77-Signal stammen aus den Atomuhren der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig, der Landesanstalt für Wissenschaft und Technik und der höchsten technischen Behörde der Bundesrepublik Deutschland für den Bereich der Messtechnik und physikalischen Sicherheitstechnik.

Die Trägerfrequenz von 77,5 kHz ist amplitudenmoduliert mit Zeitmarken pro Sekunde. Die BCD-Codierung des Zeittelegramms erfolgt durch Verschieben der Amplitude auf 25% für einen Zeitraum von 0,1s für eine logische '0' und für 0,2s für eine logische '1'. Der Empfänger rekonstruiert den Zeitrahmen durch Demodulation dieses DCF-Signals. Da das AM-Signal normalerweise durch Störsignale überlagert wird, ist eine Filterung des empfangenen Signals erforderlich. Die daraus resultierende Bandbreitenbegrenzung bewirkt eine Verzerrung der demodulierten Zeitmarken, die im Bereich von 10ms liegt. Schwankungen des Triggerpegels des Demodulators verschlechtern die Genauigkeit der Zeitmarken um zusätzliche +/-3ms. Da diese Präzision für viele Anwendungen nicht ausreicht, begann die PTB (Physikalisch-Technische Bundesanstalt), Zeitinformationen mit Hilfe der Korrelationstechnik zu verteilen.

Der DCF-Sender wird zusätzlich zum AM-Signal mit einem pseudozufälligen Phasenrauschen moduliert. Die Pseudozufallsfolge (PZF) enthält 512 Bit, die durch Phasenmodulation zwischen den AM-Zeitmarken übertragen werden. Die Bitfolge besteht aus der gleichen Anzahl von logischen '0' und logischen '1', um ein symmetrisches PZF zu erhalten, das die durchschnittliche Phase des Trägers konstant hält. Die Länge eines Bits beträgt 120 DCF-Takte, was 1,55ms entspricht. Der Träger von 77,5 kHz wird mit einer Phasenabweichung von +/-10 pro Bit moduliert. Die Bitfolge wird jede Sekunde übertragen, sie beginnt 200ms nach Beginn einer AM-Sekundenmarke und endet kurz vor der nächsten. Im Vergleich zu einem AM DCF77-Empfänger kann der Eingangsfilter eines Korrelationsempfängers breitbandig dimensioniert werden. Das eingehende Signal wird mit einem rekonstruierten Empfänger-PZF korreliert. Diese Korrelationsanalyse ermöglicht die Erzeugung von Zeitmarken, die einen Versatz von nur wenigen Mikrosekunden aufweisen. Darüber hinaus wird bei diesem Verfahren die Störfestigkeit erhöht, da Störsignale durch Mittelung des Eingangssignals unterdrückt werden. Durch das Senden der ursprünglichen oder der ergänzten Bitfolge wird die BCD-codierte Zeitinformation übertragen.

Die absolute Genauigkeit des erzeugten Zeitrahmens hängt von der Qualität des Empfängers und der Entfernung zum Sender, aber auch von den Übertragungsbedingungen ab. Daher ist die absolute Genauigkeit des Zeitrahmens im Sommer und am Tag besser als im Winter und in der Nacht. Der Grund für dieses Phänomen ist ein Unterschied im Anteil der Himmelswelle, die die Bodenwelle überlagert. Um die Genauigkeit des Zeitrahmens zu überprüfen, ist der Vergleich zweier Systeme mit kompensierter Laufzeit sinnvoll.



M	Start of Minute (0.1 s)	
R	RF Transmission via Secondary Antenna	
A1	Announcement of a Change in Daylight Saving Time	
Z1, Z2	Time Zone Identification	
	Z1, Z2 = 0, 1:	Daylight Saving Time Disabled
	Z1, Z2 = 1, 0:	Daylight Saving Time Enabled
A2	Announcement of a Leap Second	
S	Start of Time Code Information	
P1, P2, P3	Even Parity Bits	

Die PZF-Funkuhr ist ein Präzisions-Empfängersystem für den Zeitzeichensender DCF77. Es ist als Modul für den Einsatz in Systemen wie Meinberg IMS, LANTIME M-Modellen und als Computer-Steckkarte (PCI-Express) erhältlich. Der Mikroprozessor des Systems führt die Korrelation einer reproduzierten pseudozufälligen Bitfolge mit dem PZF der Senderseite durch und dekodiert gleichzeitig die AM-Zeit- und Datumsinformationen des DCF-Telegramms. Durch die Auswertung des pseudozufälligen Phasenrauschens kann ein Zeitraster erzeugt werden, das bis zu einem Faktor von tausend genauer ist als bei herkömmlichen AM-Funkuhren. Auf diese Weise ist auch eine genaue Einstellung des Hauptoszillators der Funkuhr möglich, so dass er neben der Verwendung als reiner Zeitempfänger auch als normaler Frequenzgenerator verwendet werden kann. Ist das PZF-Signal aus irgendeinem Grund vorübergehend nicht verfügbar, d.h. weil sich eine Störquelle in der Nähe befindet, schaltet

die Funkuhr automatisch auf das AM-Signal um - sofern dieses noch empfangen wird. Der Korrelationsempfänger verfügt über eine batteriegepufferte Hardwareuhr, die bei Ausfall der Versorgungsspannung die Zeit und das Datum übernimmt.

12.1.4 MSF Empfänger

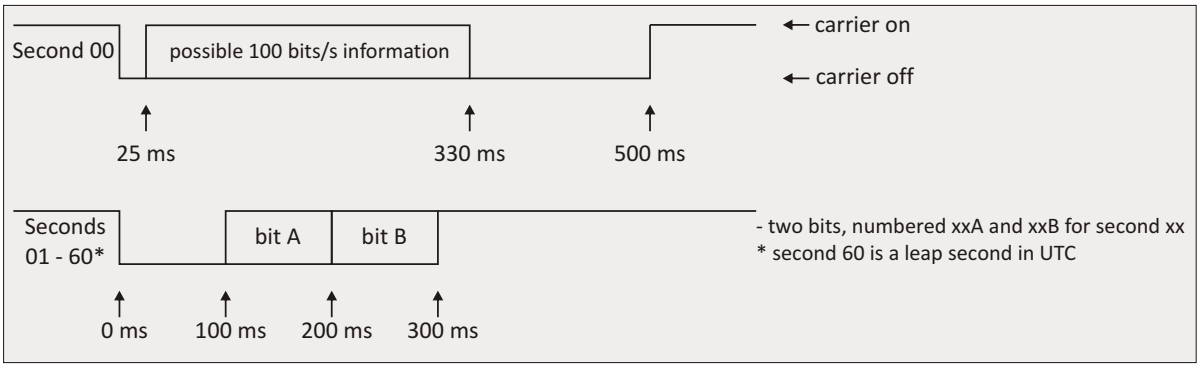
Die Übertragung des MSF-Signals von Anthorn dient der Verteilung des britischen Standards der Zeit- und Frequenzsignale. Diese Standards werden vom National Physical Laboratory (NPL) festgelegt. Das MSF-Signal bietet eine ausreichende Feldstärke für den Einsatz in Großbritannien und kann auch in weiten Teilen Nord- und Westeuropas empfangen werden.

Eine einfache On-Off-Modulation der Trägerfrequenz (60kHz) wird verwendet, um BCD-codierte Zeit- und Datumsinformationen zu übertragen. Jede UTC-Sekunde ist mit „Off" gekennzeichnet, dem mindestens 500 ms Trägerfrequenz vorausgehen. Dieser zweite Marker wird mit einer Genauigkeit von +-1 ms übertragen. Das Timecode-Format wird über einen Minuten-Frame angezeigt, mit dem die Daten in die nächste Minute übertragen werden. Die Bits „A" und „B" werden zum Senden der Informationen verwendet (siehe Grafikcodeformat unten).

Die erste Sekunde der Minute beginnt mit einer Periode von 500 ms mit dem Carrier „Off", um als Minutenmarker zu dienen. Die anderen 59 (oder in Ausnahmefällen 60 oder 58) Sekunden der Minute beginnen immer mit mindestens 100 ms „Off" und enden mit mindestens 700 ms Carrier „On". Die Sekunden 01-16 enthalten Informationen über die Differenz (DUT1) zwischen astronomischer Zeit und Atomzeit für die aktuelle Minute. Die verbleibenden Sekunden übermitteln den Zeit- und Datumscode. Die Zeit- und Datumscodeinformationen werden immer in Form von britischer Uhrzeit und Datum angegeben, d.h. UTC im Winter und UTC+1h bei gültiger Sommerzeit. Die ToD-Informationen haben Bezug zu der Minute, der der übertragenden Minute folgt.

Die MSF-Funkuhr ist ein Funkuhren-Empfängersystem für den Zeitzeichensender MSF. Es ist als Modul für den Einsatz in Systemen wie Meinberg IMS- und LANTIME-Modellen verfügbar. Der Mikroprozessor des Systems dekodiert die Zeit- und Datumsinformationen des eingehenden AM-Signals. Auf diese Weise ist auch eine genaue Einstellung des Hauptoszillators der Funkuhr möglich. Der MSF-Empfänger ist mit einer batteriegepufferten Hardware-Uhr ausgestattet, die bei Ausfall der Versorgungsspannung die Zeit und das Datum übernimmt.

Kodier-Format



DUT-Code
Der DUT1 wird auf die nächsten 100ms im Bereich von +/-800ms signalisiert. Eine positive Zahl bedeutet, dass die GMT einen höheren Wert als UTC hat. Die Bits 01B bis 16B werden verwendet, um den DUT-Code wie folgt zu signalisieren.

Zeit- und Datumscode

Zeit- und Datumsinformationen werden wie folgt kodiert und übertragen:

	Binary-Coded-Decimal Year (00-99)							
order	80	40	20	10	8	4	2	1
bit	17A	18A	19A	20A	21A	22A	23A	24A

	BCD month (01-12)					BCD day-of-month (01-31)						BCD day-of-week (0-6)		
order	10	8	4	2	1	20	10	8	4	2	1	4	2	1
bit	25A	26A	27A	28A	29A	30A	31A	32A	33A	34A	35A	36A	37A	38A

	BCD hour (00-23)					BCD minute (00-59)							
order	20	10	8	4	2	1	40	20	10	8	4	2	1
Bit	39A	40A	41A	42A	43A	44A	45A	46A	47A	48A	49A	50A	51A

Andere Kodierungen

Minuten-Identifier

Die Bits 53A bis 58A sind alle fest auf '1' gesetzt und werden immer von Bit 52A bei'0' eingeleitet und gefolgt von Bit 59A bei'0'. Diese Sequenz „01111110" erscheint nie an anderer Stelle im Bit xxA, so dass sie den folgenden zweiten 00-Minuten-Marker eindeutig identifiziert. In Minuten, die um eine positive oder negative Schaltsekunde verlängert oder verkürzt werden, werden alle diese Zahlen entsprechend um eins erhöht oder verringert (d.h. während dieser 61- oder 59-Sekunden-Minuten wird die Position des Zeit- und Datumscodes um eine Sekunde gegenüber dem Beginn der Minute verschoben).

Paritätsbits

Das Paritätsbit dient als Ergänzungsbit, um die Anzahl der mit 1 belegten Bits der Folge als gerade oder ungerade zu ergänzen.

Bit 54B aufgenommen mit den Bits 17A bis 24A
Bit 55B aufgenommen mit den Bits 25A bis 35A
Bit 56B aufgenommen mit den Bits 36A bis 38A
Bit 57B aufgenommen mit den Bits 39A bis 51A

Sommerzeit

Wenn die britische Normalzeit während eines Teils des Jahres einer einstündigen positiven Verrechnung unterliegt, wird dieser Zeitraum durch Setzen von Bit 58B auf „1" angezeigt. Bit 53B wird während der 61 aufeinanderfolgenden Minuten unmittelbar vor einer Änderung auf '1' gesetzt, wobei die letzte Minute 59 ist, wenn sich Bit 58B ändert.

Unbenutzte Bits

Die unbenutzten Bits sind derzeit auf '0' gesetzt, können aber in Zukunft verwendet werden.

12.1.5 WWVB Empfänger

Der NIST-Radiosender WWVB befindet sich in der Nähe von Fort Collins, Colorado, auf dem gleichen Gelände wie der Sender WWV. Die WWVB-Übertragung wird von Millionen von Menschen in ganz Nordamerika genutzt, um elektronische Zeitmessgeräte wie Wanduhren, Radiowecker und Armbanduhren zu synchronisieren. Darüber hinaus wird WWVB für anspruchsvolle Anwendungen wie Netzwerkzeitsynchronisation und Frequenzkalibrierung eingesetzt. Die WWVB-Übertragung wird vom National Institute of Standards and Technology (NIST) betrieben.

WWVB sendet kontinuierlich ein Zeit- und Frequenzsignal bei 60 kHz. Die Trägerfrequenz bietet eine stabile Frequenzreferenz, die auf die nationale Norm zurückführbar ist. Es gibt keine Sprachansagen auf dem Sender, aber ein Timecode wird mit dem 60 kHz Träger synchronisiert und kontinuierlich mit einer Rate von 1 Bit pro Sekunde mittels Pulsweitenmodulation übertragen. Der Übertragungs-Leistungspegel wird moduliert, um die Zeitdaten zu kodieren. Die Trägerleistung wird zu Beginn jeder Sekunde um 17 dB reduziert, so dass die Anstiegsflanke jedes negativen Going-Pulses pünktlich ist.

Die volle Leistung wird 0,2 s später für eine binäre #0#, 0,5 s später für eine binäre #1# oder 0,8 s später wiederhergestellt, um einen Positionsmarker zu übertragen. Es wird das Binärcodierte Dezimalformat (BCD) verwendet, das Binärziffern zu repräsentativen Dezimalzahlen kombiniert. Der Timecode enthält Jahr, Tag des Jahres, Stunde, Minute, Sekunde und Flags, die den Status der Sommerzeit, des Schaltjahres und der Schaltsekunden anzeigen. Der WWVB identifiziert sich damit, dass er seine Trägerphase um 45 Grad nach 10 Minuten nach der Stunde vorantreibt und nach 15 Minuten nach der Stunde in die Normalphase zurückkehrt. Wenn Sie die WWVB-Phase zeichnen, ergibt sich ein Phasenschritt von ca. 2,08 Mikrosekunden.

12.1.6 TCR Empfänger

Das Meinberg TCR-Board (Time Code Receiver) wurde für die Dekodierung von unmodulierten und modulierten IRIG- und AFNOR-Timecodes entwickelt. Modulierte Codes transportieren die Zeitinformation durch Modulation einer sinusförmigen Trägersignalamplitude, während unmodulierte Signale ein pulsweitenmoduliertes Gleichstromsignal verwenden.

Die automatische Verstärkungsregelung des Empfängers ermöglicht den Empfang von Signalen in einem Bereich von ca. 600 mV_{ss} bis 8 V_{ss}. Der potentialfreie Eingang kann über eine Steckbrücke wahlweise mit 50 Ohm, 600 Ohm oder 5 kOhm eingestellt werden. Modulierte Codes werden über einen integrierten SMB-Stecker auf das Modul gebracht.

Allgemeines über Zeitcodes
Die Übertragung von codierten Zeitsignalen gewann Anfang der 1950er Jahre zunehmend an Bedeutung. Insbesondere die US-Raketen- und Raumfahrtprogramme waren die treibenden Kräfte hinter der Entwicklung dieser Timecodes, die für die Korrelation von Daten verwendet wurden. Die Definition von Timecode-Formaten war völlig willkürlich und wurde den individuellen Vorstellungen jedes Konstrukteurs überlassen. Hunderte von verschiedenen Timecodes wurden gebildet, von denen einige von der „Inter Range Instrumentation Group“ (IRIG) in den frühen 60er Jahren standardisiert wurden.

Außer diesen „IRIG-Timecodes“ werden noch andere Formate wie NASA36, XR3 oder 2137 verwendet. Der TCR-Empfänger erzeugt den IRIG-B-, AFNOR NFS 87-500-Code sowie den IEEE1344-Code, der ein IRIG-Code ist, erweitert um Informationen für Zeitzone, Schaltsekunde und Datum.

12.2 GNSS-Signalempfang

Die Satelliten der meisten **Globalen Navigationssatellitensysteme (GNSS)** wie GPS, GLONASS und Galileo sind nicht stationär, sondern kreisen in mehreren Stunden um den Globus. Nur wenige GNSS-Systeme wie das chinesische Beidou-System arbeiten mit stationären Satelliten. Solche Systeme können nur in bestimmten Regionen der Erde empfangen werden.

GNSS-Empfänger müssen mindestens vier Satelliten verfolgen, um ihre eigene Position im Raum (x, y, z) sowie ihren Zeitversatz von der GNSS-Systemzeit (t) zu bestimmen. Nur wenn der Empfänger seine eigene Position genau bestimmen kann, kann auch die Laufzeitverzögerung der Satellitensignale genau kompensiert werden, was erforderlich ist, um eine genaue Zeit zu liefern. Wenn die Empfängerposition nur ungenau bestimmt werden kann, wird auch die Genauigkeit der abgeleiteten Zeit vermindert.

GNSS-Satellitensignale können nur direkt empfangen werden, wenn sich kein Gebäude in der Sichtflanke von der Antenne zum Satelliten befindet. Die Signale können an Gebäuden usw. reflektiert werden, und die reflektierten Signale könnten danach empfangen werden. In diesem Fall ist jedoch der Signalausbreitungsweg länger als erwartet, was einen kleinen Fehler in der berechneten Position verursacht. Das wiederum ergibt eine weniger genaue Zeit.

Da die meisten Satelliten nicht stationär sind, muss die Antenne an einem Ort installiert werden, der so viel freie Sicht auf den Himmel wie möglich hat (z.B. auf einem Dach), um einen kontinuierlichen und zuverlässigen Empfang und Betrieb zu ermöglichen. Der beste Empfang wird erreicht, wenn die Antenne einen freien Blickwinkel von 8° über dem Horizont hat. Wenn das nicht möglich ist, sollte die Antenne mit der besten freien Sicht zum Himmel in Richtung des Äquators installiert werden. Da die Satellitenbahnen zwischen den Breitengraden 55° Nord und 55° Süd liegen, ermöglicht diese Positionierung den bestmöglichen Empfang.

Meinberg bietet eigene GPS-Empfänger an, die mit einer Antennen- / Konvertereinheit arbeiten und somit sehr lange Antennenkabel ermöglichen. Einige Geräte enthalten jedoch auch GNSS-Empfänger, die neben GPS auch andere Satellitensysteme wie GLONASS, Galileo und BeiDou unterstützen. Diese Empfänger erfordern normalerweise einen anderen Antennentyp. Diese Unterschiede werden im nächsten Kapitel beschrieben.

12.2.1 Installation einer GPS-Antenne

Die folgenden Kapitel befassen sich mit der Auswahl eines geeigneten Antennenstandorts, der Montage der Antenne sowie der Errichtung eines wirksamen Überspannungsschutzes für die Antenneninstallation.

12.2.1.1 Auswahl des Antennenstandortes

Grundsätzlich gibt es zwei Möglichkeiten eine kompatible Meinberg GPS-Antenne (z. B. GPSANTv2) mit den im Lieferumfang enthaltenen Zubehör zu installieren:

1. Mastmontage

2. Wandmontage

Um ausreichend Satelliten zu empfangen, wählen Sie einen Standort, der eine unverbaute Sicht in alle Himmelsrichtungen ermöglicht (Abb. 1), da es ansonsten zu Problemen bei der Synchronisation Ihres angeschlossenen Meinberg-Zeitservers kommen kann.

Für eine optimale 360°-Sicht der Antenne empfiehlt Meinberg die Dachmontage an einem geeigneten Metallmast (siehe rechte Antennendarstellung, Abb. 1). Ist diese nicht möglich, sollte eine wandmontierte Antenne an einem Gebäude, ausreichend hoch über der Gebäudetraufe, montiert werden (siehe linke Antennendarstellung, Abb. 1).

So können Einschränkungen des Sichtbereichs der Antenne zu den Satelliten (Abschattungen o. Teilabschattung) und Reflektionen des Antennensignals von Oberflächen, wie z. B. Hausfassaden, vermieden werden.

1. Mastmontage
2. Antennenkabel
3. Wandmontage
4. Hauseinführung

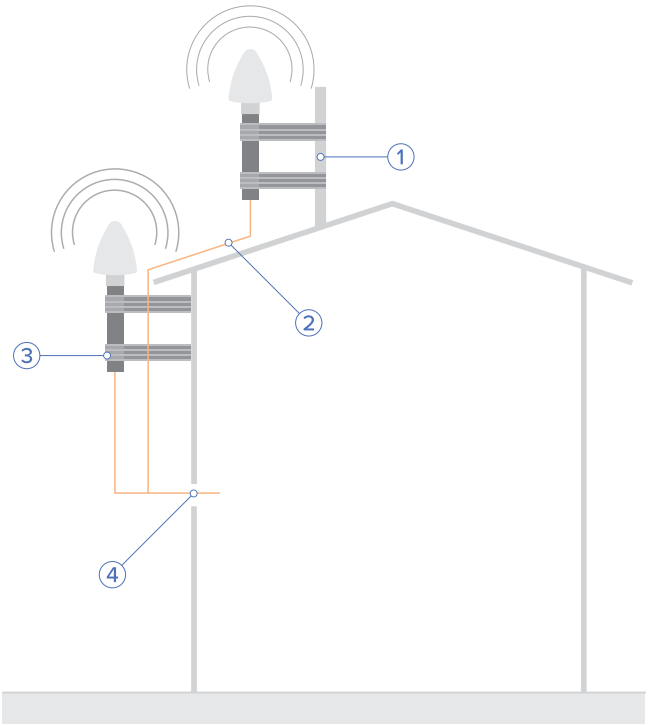


Abb. 1: Optimale Positionierungen

Befindet sich ein massives Hindernis (Gebäude oder Gebäudeteile) in der Sichtlinie zwischen Antenne und jeweiligen Satelliten (siehe Abb. 2), ist eine Abschattung, Teilabschattung und/oder Reflektion des Satellitensignals und damit ein gestörter Signalempfang zu erwarten.

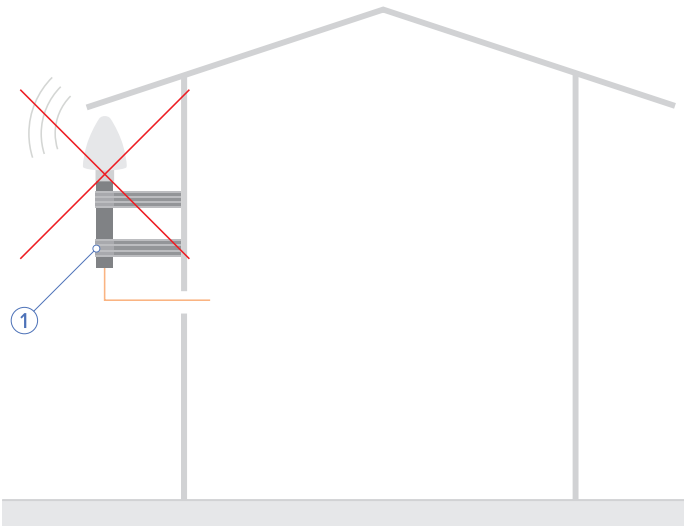


Abb. 2: Nicht empfohlene Positionierung einer wandmontierten (1) Antenne

Darüber hinaus dürfen sich im Öffnungswinkel der Antenne (ca. 98 Grad) keine leitfähigen Gegenstände, Freileitungen oder andere elektrische Licht- oder Stromkreise befinden, da diese bei den ohnehin schwachen Signalen im Frequenzband der Satellitenübertragung Störungen hervorrufen.

Weitere Installationskriterien für einen optimalen Betrieb:

- Vertikale Montage der Antenne (siehe Abb. 1)
- Mindestens in 50 cm Abstand zu anderen Antennen
- Freie Sicht Richtung Äquator
- Freie Sicht zwischen dem 55. südlichen und 55. nördlichen Breitenkreis (Satellitenlaufbahnen).

Hinweis:

Wenn diese Kriterien nicht eingehalten werden und freie Sichtfelder eingeschränkt sind, kann es zu Komplikationen bei der Synchronisation Ihres Meinberg-Produkts kommen, da vier Satelliten gefunden werden müssen, um eine exakte Position zu berechnen.

12.2.1.2 Montage der Antenne

Bitte lesen Sie vor der Montage sorgfältig die folgenden Sicherheitshinweise und beachten diese unbedingt.

Gefahr!

Antennenmontage ohne wirksame Absturzsicherung

Lebensgefahr durch Absturz!

- Achten Sie bei der Antennenmontage auf wirksamen Arbeitsschutz!
- Arbeiten Sie niemals ohne wirksame Absturzsicherung!

Gefahr!

Arbeiten an der Antennenanlage bei Gewitter

Lebensgefahr durch elektrischen Schlag!

- Führen Sie **keine** Arbeiten an der Antennenanlage oder der Antennenleitung durch, wenn die Gefahr eines Blitzeinschlages besteht.
- Führen Sie **keine** Arbeiten an der Antennenanlage durch, wenn der Sicherheitsabstand zu Freileitungen und Schaltwerken unterschritten wird.

Montieren Sie die Meinberg GPSANTv2- oder die GNSS Multi-Band-Antenne (wie auf Abb. 3 gezeigt) in min. 50 cm Distanz zu anderen Antennen, an einem stehenden Mastrohr mit bis zu 60 mm Außendurchmesser oder direkt an einer Wand mit dem im Lieferumfang enthaltenen Montagekit.

Item	Description	QTY
1	Antenna	1
2	M8 grounding stud	1
3	safety washer	1
4	M8 hex nut	1
5	Antenna pole	1
6	M4 hex nut	8
7	M4 x 12 phillips-head screw	8
8	threaded U-bolt (pole diameter max. 60 mm)	2
9	M6 spacer	4
10	M6 hex nut	4
11	pole clamp halves	4
12	pole bracket	2

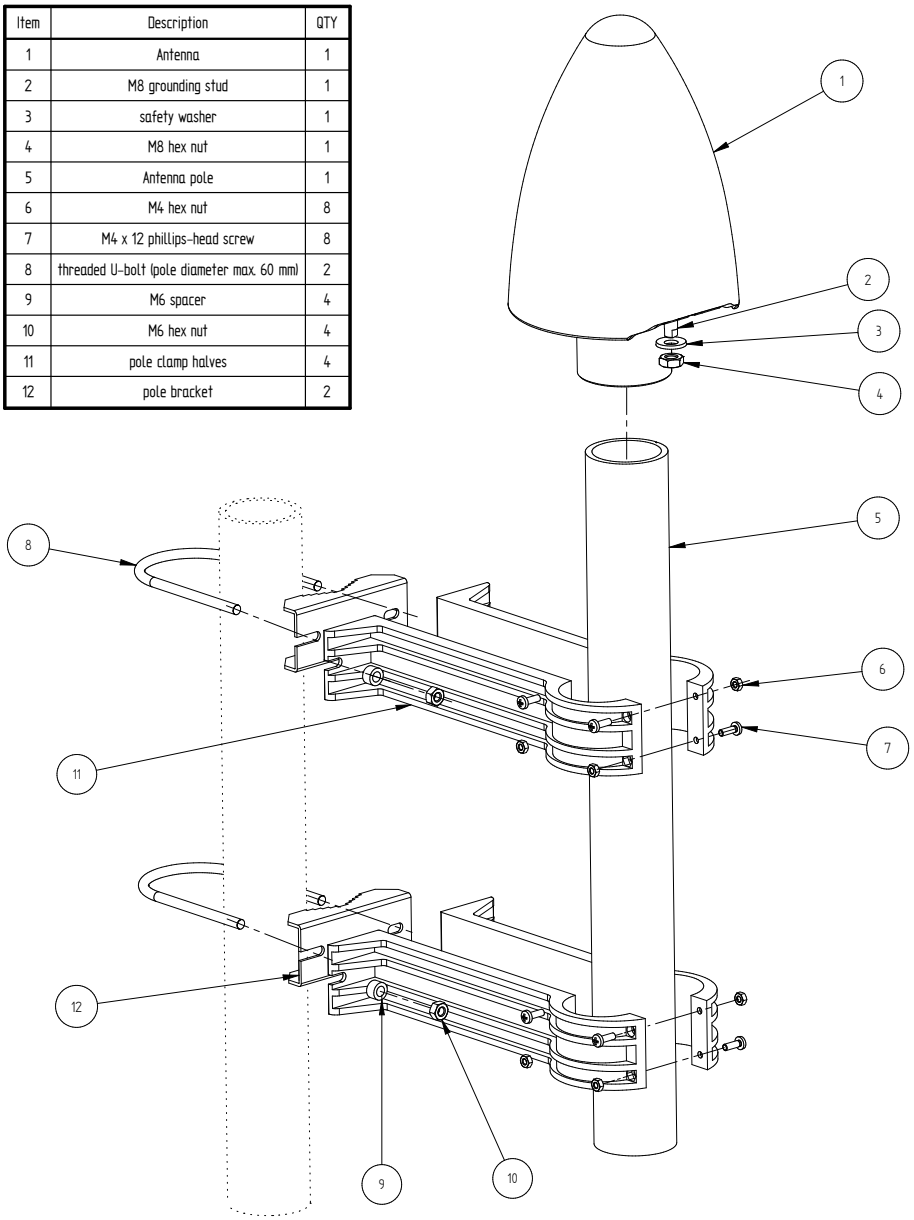


Abb. 3: Mastmontage einer Meinberg GPS- oder GNSS Multi-Band-Antenne

Die Abbildung 3 zeigt exemplarisch die Mastmontage einer Meinberg Antenne. Bei einer Montage direkt an einer Wand sind die vier mitgelieferten Wanddübel und M6x45-Schrauben zu verwenden und durch die vorgesehenen Langlöcher an den Mastschellenhälften (Abb. 3, Pos. 12) zu führen.

Im folgenden Kapitel wird die Verlegung des Antennenkabels erläutert.

12.2.1.3 Antennenkabel

Auswahl des richtigen Kabels

Meinberg bietet zusammen mit den Antennen passende Kabeltypen an, welche je nach Distanz von Antenne zur Meinberg-Referenzuhr bestellt werden können. Ermitteln Sie diese für Ihre Antenneninstallation zu überwindende Strecke vor Bestellung und wählen entsprechend den Kabeltyp aus.

Achtung!

Bitte vermeiden Sie bei Ihrer Antenneninstallation einen Mischbetrieb mit unterschiedlichen Kabeltypen. Beachten Sie dies ebenfalls beim Kauf von Kabeln für z.B. die Erweiterung einer bestehenden Kabelinstallation.

GPS/GNS-UC Referenzuhren

Die folgende Tabelle zeigt die typischen Spezifikationen der unterstützten Antennenkabeltypen bei der Übertragung der 35-MHz-Zwischenfrequenz:

Kabeltyp	RG58C/U	RG213	H2010 (Ultraflex)
Signallaufzeit bei 35 MHz*	503 ns/100 m	509 ns/100 m	387 ns/100 m
Dämpfung bei 35 MHz	8,48 dB/100 m	3,46 dB/100 m	2,29 dB/100 m
Gleichstromwiderstand	5,3 Ω/100 m	1,0 Ω/100 m	1,24 Ω/100 m
Kabeldurchmesser	5 mm	10,3 mm	10,2 mm
Max. Kabellänge	300 m	700 m	1100 m

Tabelle – Spezifikationen der von Meinberg empfohlenen Kabeltypen

** Die Signallaufzeit bei 100 m Kabel ermöglicht eine Umrechnung der Signallaufzeit bei einer anderen beliebigen Kabellänge.*

Verlegung des Antennenkabels

Beachten Sie bei Verlegung des Antennenkabels, dass die angegebene max. Leitungslänge nicht überschritten wird: Diese Länge ist vom verwendeten Kabeltyp und dessen Dämpfungsfaktor abhängig. Bei Überschreitung kann eine einwandfreie Übertragung der zu übermittelnden Daten und damit eine korrekte Synchronisierung der Referenzuhr nicht gewährleistet werden.

Verlegen Sie das Koaxialkabel von Antenne hin zum Gebäudeeintritt, wie auf Abbildung 5 und 6 im Kapitel **„Überspannungsschutz und Erdung“** gezeigt. Die Schirme des Antennenkabels sind, wie alle anderen metallischen Gegenstände der Antennenanlage (Antenne und Mast), in den Potentialausgleich mit einzubeziehen und miteinander zu verbinden.

Vorsicht!

Achten Sie bei der Verlegung des Antennenkabels darauf, dieses mit ausreichend Abstand zu stromführenden Leitungen (z.B. Starkstrom) zu verlegen, da diese durch „Übersprechen“ die Qualität des Antennensignals z. T. stark beeinträchtigen können. Weiterhin können z. B. bei Blitzeinschlägen, die auf einem Stromkabel auftretenden Überspannungen in das Antennenkabel „einkoppeln“ und so ihr System beschädigen.

Weitere zu beachtende Punkte bei der Verlegung des Antennenkabels:

- Der minimale Biegeradius des Kabels ist zu beachten.[1]
- Quetschungen oder Verletzung der Außenisolierung sind zu vermeiden.
- Beschädigungen oder Verschmutzungen am Koaxialstecker sind zu vermeiden.

[1] *Der Biegeradius ist der Radius, mit dem ein Kabel gebogen werden kann, ohne es zu beschädigen (einschließlich Knicken)*

Kompensation der Signallaufzeit des Antennenkabels

GPS/GNS-UC Referenzuhren

Bei der Ausbreitung des Signals von der Antenne zum Empfänger (Referenztakt) kann es zu einer gewissen Verzögerung kommen. Diese Verzögerung kann im LANTIME Web-Interface kompensiert werden.

Loggen Sie sich dazu im Webinterface Ihres LANTIME-Systems ein und gehen Sie dann wie folgt vor:

1. Öffnen Sie das Menü **„Uhr“** → **„Status & Konfiguration“**
2. Wählen Sie das entsprechende Uhrenmodul aus.
3. Klicken Sie auf den Reiter „**Verschiedenes**“.
4. Wählen Sie die Kompensationsmethode aus und tragen den entsprechenden Wert ein.

Indem Sie die Kompensationsmethode „**Nach Laufzeit**“ wählen, kann für die Signallaufzeit eine feste Ausgleichszeit (Offset) in Nanosekunden eingegeben werden. Dieser Wert wird auf der Grundlage der Daten im Datenblatt Ihres Kabels oder auf Basis Ihrer eigenen Verzögerungsmessungen berechnet.

Die beste Genauigkeit entsteht durch einen manuell berechneten Signallaufzeitwert. Es ist allerdings auch möglich, mit Auswahl der Option „**Nach Länge**“ die Länge des Kabels in Metern einzugeben: Damit wird eine automatische Schätzung der Laufzeit angewendet auf der Grundlage der bekannten Eigenschaften von RG58-Standardkabel.

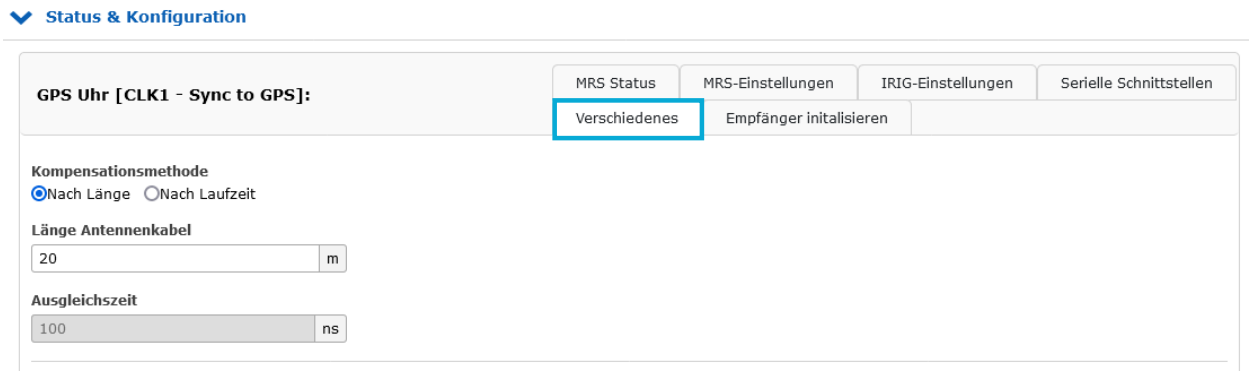


Abb. 4.1: „Uhr“ Menü im LANTIME OS Web Interface

Im nächsten Kapitel **„**Überspannungsschutz und Erdung**“** wird die Installation eines wirksamen Überspannungsschutzes für die Antenneninstallation erläutert.

12.2.2 Installation GNSS Antennen

Für unseren kombinierten GPS/GLONASS/Galileo/BeiDou Satellitenempfänger stehen zwei Antennen zur Verfügung, die für unterschiedliche Aufgaben bzw. Einsatzbereiche konzipiert sind.

Zum Standardzubehör gehört die aktive Multi GNSS L1-Antenne, welche die Signale der GPS-, GLONASS-, Galileo- und Beidou-Satellitensysteme empfangen kann. Diese eignet sich hervorragend für stationäre Anlagen, arbeitet mit einer vom Empfänger gelieferten 5V-DC-Versorgungsspannung und verfügt über einen integrierten Überspannungsschutz.

Für mobile Anwendungen, z.B. Kraftfahrzeuge, Schiffe, Bahn und Flugzeuge empfehlen wir den Einsatz der RV-76G, einer aktiven GNSS Antenne, die geeignet ist für die direkte Montage in ein Gehäuse (Karrosserie, Bordwände usw.).

12.2.2.1 Auswahl des Antennenstandortes

Grundsätzlich gibt es zwei Möglichkeiten die Multi-GNSS Antenne mit den im Lieferumfang enthaltenen Zubehör zu installieren:

1. Mastmontage

2. Wandmontage

Um ausreichend Satelliten zu empfangen, wählen Sie einen Standort, der eine unverbaute Sicht in alle Himmelsrichtungen ermöglicht (Abb. 1), da es ansonsten zu Problemen bei der Synchronisation Ihres Meinberg-Zeitservers kommen kann.

Für eine optimale 360°-Sicht der Antenne empfiehlt Meinberg die Dachmontage an einem geeigneten Metallmast (siehe rechte Antennendarstellung, Abb. 1). Ist diese nicht möglich, sollte eine wandmontierte Antenne an einem Gebäude, ausreichend hoch über der Gebäudetraufe, montiert werden (siehe linke Antennendarstellung, Abb. 1).

So können Einschränkungen des Sichtbereichs der Antenne zu den Satelliten (Abschattungen o. Teilabschattung) und Reflektionen des Antennensignals von Oberflächen, wie z. B. Hausfassaden, vermieden werden.

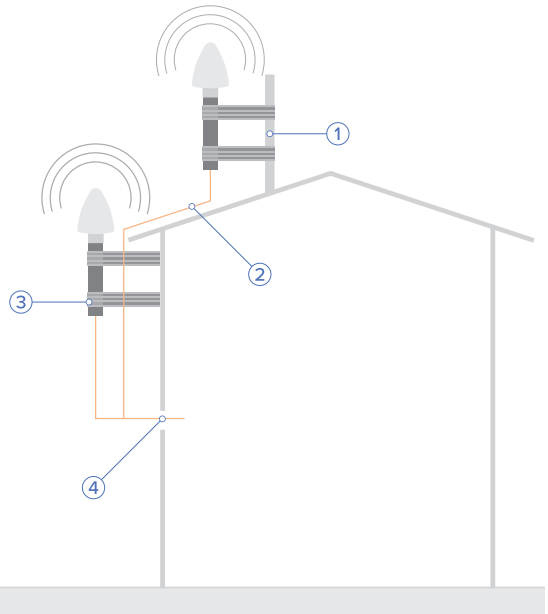


Abb. 1: Optimale Positionierungen

Befindet sich ein massives Hindernis (Gebäude oder Gebäudeteile) in der Sichtlinie zwischen Antenne und jeweiligen Satelliten (siehe Abb. 2), ist eine Abschattung, Teilabschattung und/oder Reflektion des Satellitensignals und damit ein gestörter Signalempfang zu erwarten.

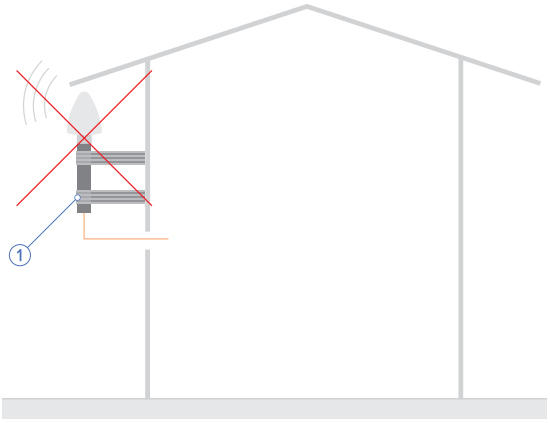


Abb. 2: Nicht empfohlene Positionierung einer wandmontierten Antenne

Darüber hinaus dürfen sich im Öffnungswinkel der Antenne (ca. 120 Grad) keine leitfähigen Gegenstände, Freileitungen oder andere elektrische Licht- oder Stromkreise befinden, da diese bei den ohnehin schwachen Signalen im Frequenzband der Satellitenübertragung Störungen hervorrufen.

Weitere Installationskriterien für einen optimalen Betrieb:

- Vertikale Montage der Antenne (siehe Abb. 1)
- Mindestens in 50 cm Abstand zu anderen Antennen
- Freie Sicht Richtung Äquator
- Freie Sicht zwischen dem 55. südlichen und 55. nördlichen Breitenkreis (Satellitenlaufbahnen).

Hinweis:

Wenn diese Kriterien nicht eingehalten werden und freie Sichtfelder eingeschränkt sind, kann es zu Komplikationen bei der Synchronisation Ihres Meinberg-Zeitservers kommen, da vier Satelliten gefunden werden müssen, um eine exakte Position zu berechnen.

12.2.2.2 Montage der Antenne

Bitte lesen Sie vor der Montage sorgfältig die folgenden Sicherheitshinweise und beachten diese unbedingt.

Gefahr!

Antennenmontage ohne wirksame Absturzsicherung

Lebensgefahr durch Absturz!

- Achten Sie bei der Antennenmontage auf wirksamen Arbeitsschutz!
- Arbeiten Sie niemals ohne wirksame Absturzsicherung!

Gefahr!

Arbeiten an der Antennenanlage bei Gewitter

Lebensgefahr durch elektrischen Schlag!

- Führen Sie keine Arbeiten an der Antennenanlage oder der Antennenleitung durch, wenn die Gefahr eines Blitzeinschlages besteht.
- Führen Sie keine Arbeiten an der Antennenanlage durch, wenn der Sicherheitsabstand zu Freileitungen und Schaltwerken unterschritten wird.

Meinberg GNS-Empfänger

Montieren Sie die L1-Antenne nach den genannten Kriterien und in min. 50 cm Distanz zu anderen Antennen an einem vertikalen Mastrohr von 60 mm – 215 mm ($2\,\frac{1}{2}$ – $8\,\frac{1}{2}$ inch) mit dem im Lieferumfang enthaltenen Montagekit.

Eine detaillierte Montageanleitung finden Sie unter dem Punkt „Downloads“ auf der Produktseite des Herstellers: https://www.pctel.com/antenna-product/gps-timing-reference-antenna-2/

Im folgenden Kapitel wird die Verlegung des Antennenkabels erläutert.

12.2.2.3 Antennenkabel

Auswahl des richtigen Kabels

Meinberg bietet zusammen mit den Antennen passende Kabeltypen an, welche je nach Distanz von Antenne zur Meinberg-Referenzuhr bestellt werden können. Ermitteln Sie diese für Ihre Antenneninstallation zu überwindende Strecke vor Bestellung und wählen entsprechend den Kabeltyp aus.

Achtung!

Bitte vermeiden Sie bei Ihrer Antenneninstallation einen Mischbetrieb mit unterschiedlichen Kabeltypen. Beachten Sie dies ebenfalls beim Kauf von Kabeln für z.B. die Erweiterung einer bestehenden Kabelinstallation.

Standardmäßig sind beide Kabelenden bei Auslieferung mit einem entsprechenden Stecker vorkonfektioniert, können aber auch nach Kundenwunsch unkonfektioniert ausgeliefert werden.

GNS-Referenzuhren

Die folgende Tabelle zeigt die typischen Spezifikationen der unterstützten Antennenkabeltypen bei der Übertragung der GNSS-Frequenzbänder:

Kabeltyp	H155	H2010 (Ultraflex)	HFJ240
Signallaufzeit bei 1575 MHz*	423 ns/100 m	386 ns/100 m	401 ns/100 m
Dämpfung 1575 MHz	-40,20 dB/100 m	-17,57 dB/100 m	-33,00 dB/100 m
Gleichstromwiderstand Leiter	3,24 Ω/100 m	1,24 Ω/100 m	1,05 Ω/100 m
Kabeldurchmesser	5,4 mm	10,2 mm	6,1 mm
Max. Kabellänge*	70 m	150 m	70 m
Min. Biegeradius (Festinstallation)	60 mm	40 mm	61 mm

Tabelle: Spezifikationen der von Meinberg empfohlenen Kabeltypen

** Die Signallaufzeit bei 100 m Kabel ermöglicht eine Umrechnung der Signallaufzeit bei einer anderen beliebigen Kabellänge.*

Verlegung des Antennenkabels

Beachten Sie bei Verlegung des Antennenkabels, dass die angegebene max. Leitungslänge nicht überschritten wird: Diese Länge ist vom verwendeten Kabeltyp und dessen Dämpfungsfaktor abhängig. Bei Überschreitung kann eine einwandfreie Übertragung der zu übermittelnden Daten und damit eine korrekte Synchronisierung der Referenzuhr nicht gewährleistet werden.

Vorsicht!

Achten Sie bei der Verlegung des Antennenkabels darauf, dieses mit ausreichend Abstand zu stromführenden Leitungen (z.B. Starkstrom) zu verlegen, da diese durch „Übersprechen“ die Qualität des Antennensignals z. T. stark beeinträchtigen können. Weiterhin können z. B. bei Blitzeinschlägen, die auf einem Stromkabel auftretenden Überspannungen in das Antennenkabel „einkoppeln“ und so ihr System beschädigen.

Weitere zu beachtende Punkte bei der Verlegung des Antennenkabels:

- Der minimale Biegeradius des Kabels ist zu beachten.[1]
- Quetschungen oder Verletzung der Außenisolierung sind zu vermeiden.
- Beschädigungen oder Verschmutzungen am Koaxialstecker sind zu vermeiden.

[1] *Der Biegeradius ist der Radius, mit dem ein Kabel gebogen werden kann, ohne es zu beschädigen (einschließlich Knicken)*

Im nächsten Kapitel **„Überspannungsschutz und Erdung“** wird die Installation eines wirksamen Überspannungsschutzes für die Antenneninstallation erläutert.

Kompensation der Signallaufzeit des Antennenkabels

GNS-Referenzuhren

Bei der Ausbreitung des Signals von der Antenne zum Empfänger (Referenztakt) kann es zu einer gewissen Verzögerung kommen. Diese Verzögerung kann im LANTIME Web-Interface kompensiert werden.

Loggen Sie sich dazu im Webinterface Ihres LANTIME-Systems ein und gehen Sie dann wie folgt vor:

1. Öffnen Sie das Menü **„Uhr“** → **„Status & Konfiguration“**
2. Wählen Sie das entsprechende Uhrenmodul aus
3. Klicken Sie auf den Reiter „Verschiedenes“
4. Wählen Sie die Kompensationsmethode aus und tragen den entsprechenden Wert ein.

Ein fester Signallaufzeit-Offset kann in Nanosekunden eingegeben werden, indem Sie „**Nach Verzögerung**“ wählen. Dieser Wert wird auf der Grundlage der Daten im Datenblatt Ihres Kabels berechnet oder auf Basis Ihrer eigenen Verzögerungsmessungen berechnet.

Die beste Genauigkeit entsteht durch einen manuell berechneten Signallaufzeitwert. Es ist allerdings auch möglich, mit Auswahl der Option „**Nach Länge**“ die Länge des Kabels in Metern einzugeben: Damit wird eine automatische Schätzung der Laufzeit angewendet auf der Grundlage der bekannten Eigenschaften von Belden H155-Standardkabel.

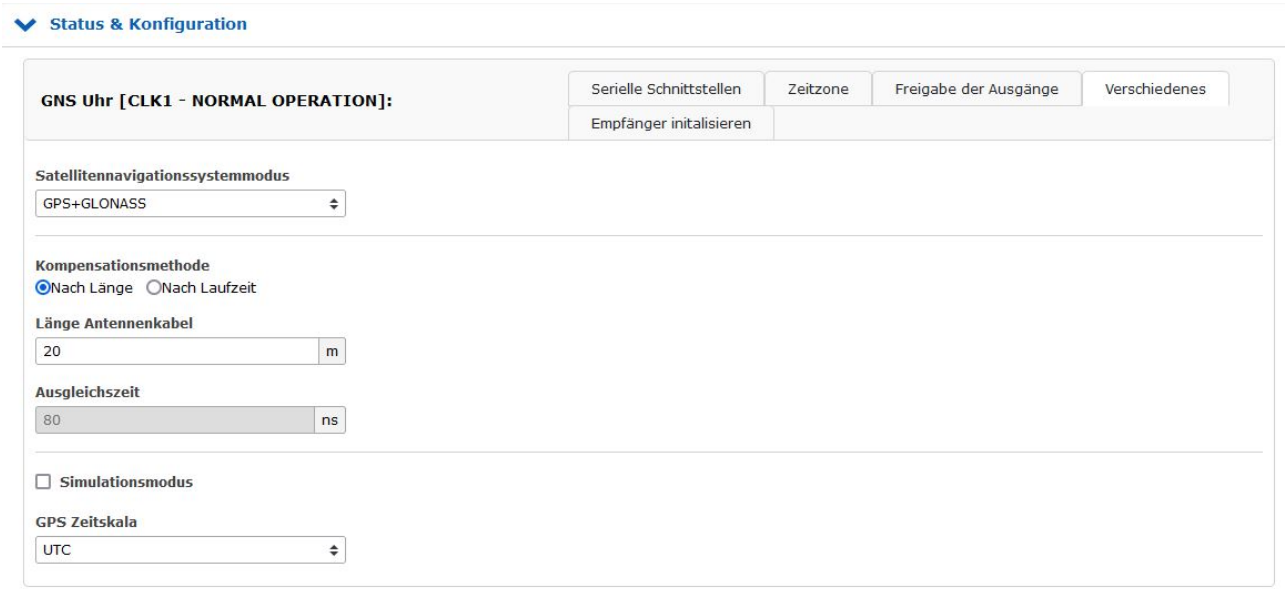


Abb. 4.1: „Uhr“ Menü im LANTIME OS Web Interface

12.2.3 Einschalten eines GNSS-Empfängers

Wenn sowohl die Antenne als auch die Stromversorgung angeschlossen sind, ist das System betriebsbereit. Je nach Art des im Empfänger installierten Oszillators dauert es ca. 3 Sekunden (OCXO-LQ) bis 3 Minuten (OCXO-MQ / HQ), bis der Oszillator aufgewärmt ist und die erforderliche Frequenzgenauigkeit erreicht hat.

Wenn der Empfänger einige gültige Almanach-Daten in seinem batteriegepufferten Speicher hat und sich die Position des Empfängers seit seinem letzten Betrieb nicht wesentlich verändert hat, kann der Empfänger ermitteln, welche Satelliten in Sicht sind. Zur Synchronisation und Erzeugung von Ausgangsimpulsen muss nur ein einziger Satellit empfangen werden, so dass die Synchronisation nach dem Einschalten mindestens eine Minute (OCXO-LQ) bis 10 Minuten (OCXO-MQ / HQ) erreicht werden kann. Nach 20 Minuten Betrieb ist der OCXO vollständig eingestellt und die erzeugten Frequenzen liegen innerhalb der vorgegebenen Toleranzen.

Wenn sich die Empfängerposition seit dem letzten Betrieb um einige hundert Kilometer verändert hat, können die erwarteten Satelliten nach dem Einschalten nicht in Sicht sein. In diesem Fall wechselt der Empfänger in den **Warm Boot** Modus, wo er nacheinander alle möglichen Satelliten scannt. Sobald der Empfänger mindestens 4 Satelliten gleichzeitig verfolgen kann, aktualisiert er seine eigene Position und wechselt in den **Normal Operation** Modus.

Wenn keine gültigen Daten in dem batteriegepufferten Speicher gefunden werden können, z.B. weil die Batterie abgeklemmt oder ersetzt wurde, muss der Empfänger nach Satelliten suchen und die aktuellen Almanach- und Ephemeridendaten sammeln. Dieser Modus heißt **Cold Boot** und dauert mindestens 12 Minuten bis alle benötigten Daten gesammelt wurden. Der Grund dafür ist, dass die Satelliten alle Daten einmal alle 12 Minuten wiederholt senden. Nachdem die Datenerfassung abgeschlossen ist, wechselt der Empfänger zum **Warm Boot** Modus um nach weiteren Satelliten zu scannen und schließlich in den **Normal Operation** Modus.

In der Default-Konfiguration werden weder Puls- und Synthesizerausgänge noch die seriellen Schnittstellen nach dem Einschalten freigegeben, solange bis die Synchronisation erreicht ist. Es ist jedoch möglich, einige oder alle dieser Ausgänge nach dem Einschalten sofort freizugeben.

Wenn das System in einer neuen Umgebung startet (z. B. bei veränderter Empfängerposition oder die Stromversorgung wurde neu angeschlossen), kann es einige Minuten dauern, bis die Ausgangsfrequenz des Oszillators richtig eingestellt ist. In diesem Fall ist auch die Genauigkeit der Ausgangsfrequenz und der Impulse vermindert, bis sich die Regelkreise des Empfängers wieder eingestellt haben.

Auf dem Display („Reference Time → Info GPS → GPS Satellites“) sowie über die grafische Web-Oberfläche („Clock → Receiver Information“) können Sie die Anzahl der Satelliten überprüfen - ob sie in Sicht sind (d.h. über dem Horizont) und ob sie als qualitativ gut eingestuft werden können.

12.3 Langwellen-Signalempfang

12.3.1 Allgemeines

Die Langwellenantenne **AW02** ist eine wetterfeste und temperaturbeständige Aktivantenne für den Außenbereich. Das System besteht aus einer Ferritantenne zum Empfang des Langwellensignals und einen Verstärker, die beide in einem Kunststoffgehäuse montiert sind. Die Basisversion wurde entwickelt, um das Signal vom deutschen Langwellensender **DCF77** zu empfangen, dessen Trägerfrequenz 77,5 kHz beträgt.

Der DCF77-Sender wird von der Physikalisch-Technischen Bundesanstalt (PTB) betrieben und befindet sich in Mainflingen bei Frankfurt am Main. Sein Signal kann in Deutschland und angrenzenden Ländern empfangen werden.

Die Antennen-Variante **AW02-MSF** ist für den britischen Langwellensender **MSF** verfügbar, der sich in Anthorn / UK befindet und die Uhrzeit und Frequenz des englischen National Physical Laboratory (NPL) übermittelt. Das Signal kann überall in Großbritannien und in weiten Teilen Nord- und Westeuropas empfangen werden.

Eine andere Variante ist der **AW02-WWVB**, der für die WWVB-Radiostation angepasst wurde, die sich in den Vereinigten Staaten in der Nähe von Fort Collins, Colorado, befindet und vom US National Institute of Standards und Technologie (NIST) unterhalten wird.

Obwohl sich diese Antennenvarianten je nach den Eigenschaften des zugehörigen Senders leicht unterscheiden, sind die grundlegenden Anforderungen für die Installation identisch.

Die Langwellenantennen können mit einer Kabellänge von bis zu 300 Metern (1000 ft) betrieben werden, wenn das Standard-Koaxialkabel RG58 verwendet wird. Sie werden vom Empfänger über das Antennenkabel mit Spannung versorgt, so dass keine externe Stromversorgung der Antenne erforderlich ist, wenn ein Koaxialkabel vom Empfänger direkt angeschlossen wird.

Überspannungsschutzgeräte sind optional erhältlich und sollten in der Antennenleitung verwendet werden, um den Empfänger vor hohen Spannungsspitzen zu schützen, z.B. durch Blitzeinschlag in der Nähe der Antenne.

Für längere Entfernungen von der Antenne zum Empfänger kann ein optionaler Verstärker verwendet werden, der eine zusätzliche Stromversorgung benötigt. Das **BLV** System ist ein Verstärker mit integriertem Überspannungsschutz.

Alternativ ist ein **DCF Optical Antenna Link (DOAL)** verfügbar, der eine Glasfaserverbindung zwischen der Antenne und dem Empfänger verwendet, die eine Länge von bis zu 2000m (6500ft) ermöglicht und so ein hohes Maß an Isolation und Überspannungsschutz durch die optische Übertragung liefert. Auch hier wurde das Basisgerät für DCF77 entwickelt, es sind aber auch Varianten für MSF und WWVB verfügbar. Da die Glasfaserverbindung die Antenne nicht mit Gleichstrom versorgen kann, ist in diesem Fall eine zusätzliche externe Stromversorgung der Antenne erforderlich.

Unsere Langwellen-Empfänger wurden speziell für Meinberg-Systeme entwickelt und sind nicht zwingend mit Empfängern von Drittherstellern kompatibel.

12.3.2 Installation einer Langwellenantenne

12.3.2.1 Geografische Überlegungen

Die Lage der Antenne spielt eine entscheidende Rolle bei der Empfangsqualität und damit für die Signalstärke des Langwellensignals. Daher sollte der Installationsort sorgfältig ausgewählt werden, um Schwierigkeiten bei der Synchronisation zu vermeiden. Wenn die Antenne nicht genau ausgerichtet ist, werden der Signalempfang und die Zeitgenauigkeit beeinträchtigt.

AWO2 - DCF77

Die Antenne muss gemäß den unten angegebenen Installationskriterien in Richtung Mainflingen, in der Nähe von Frankfurt am Main, ausgerichtet sein.

Das DCF77-Signal hat, vom Sendemast aus gemessen, eine theoretische Reichweite von 2000 km und ermöglicht die Synchronisation von DCF77-Empfängern in Deutschland und Ländern wie z. B. Frankreich, Dänemark, Schweden sowie Österreich und Italien. Empfindliche Empfänger können in den äußeren Empfangsregionen tageszeitabhängig noch ein ausreichend starkes Signal empfangen.

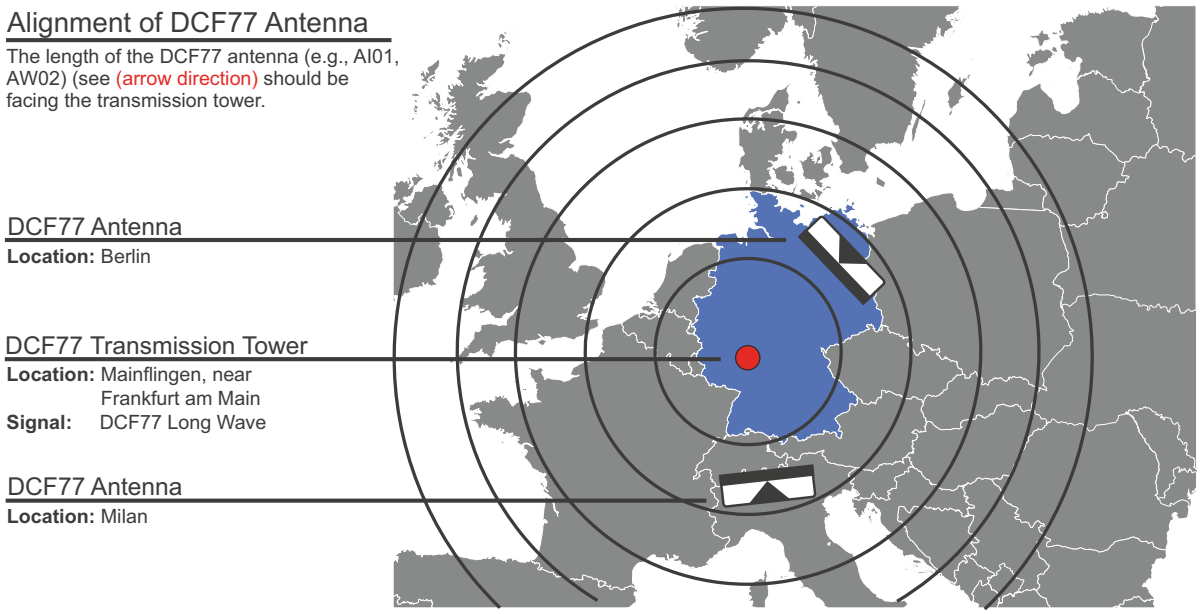


Abbildung: Ausrichtung einer Meinberg-Langwellenantenne von verschiedenen Standorten aus in Deutschland auf den DCF77-Sendemast in Mainflingen, Deutschland.

AWO2-60 - MSF und WWVB

Je nach Einsatzland muss die AW02-60-Antenne gemäß den unten angegebenen Installationskriterien in Richtung Anthorn (Großbritannien) oder Fort Collins, Colorado (USA) oder Frankfurt am Main (Deutschland) zeigen.

Das MSF-Signal hat eine theoretische Reichweite von 1000 km und bietet somit einen garantierten und flächendeckenden Empfang in Großbritannien und Irland. Es kann auch (allerdings ohne Gewähr) in Teilen Nord- und Westeuropas empfangen werden.

Das WWVB-Signal in den USA hat eine theoretische Reichweite von 1500 km, gemessen vom Sendemast in Colorado. Somit gehören Städte wie San Diego, Chicago und Sacramento zur äußersten Grenze des Empfangsbereichs dar, in denen der Empfang schwach und störungsbehaftet sein kann, vor allem in bebauten Umgebungen.

Die Karten auf der folgenden Seite geben einen Überblick der Empfangsabdeckung der jeweiligen Langwellensignale.

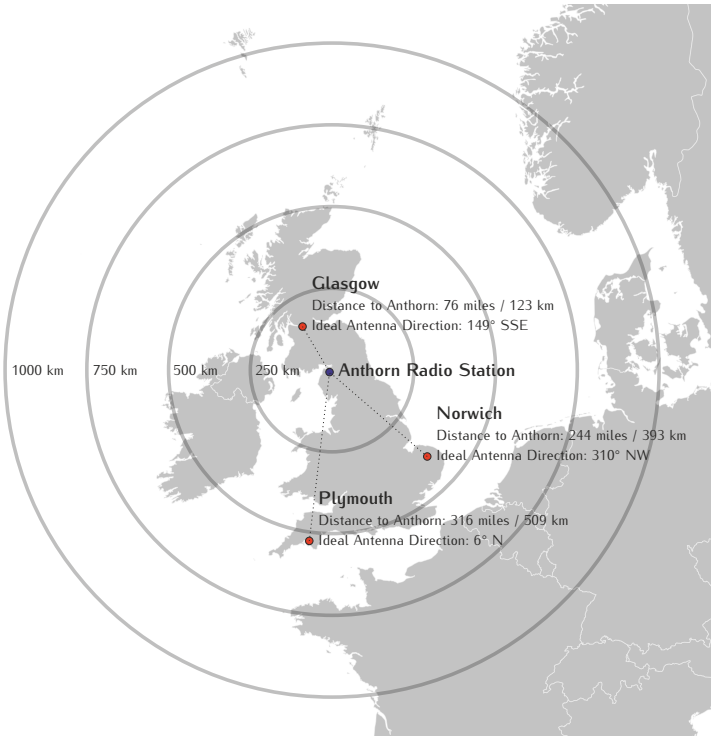


Abbildung: Ausrichtung einer AW02-60-Antenne von verschiedenen Standorten aus in Großbritannien auf den MSF-Sendeturm in Anthorn.

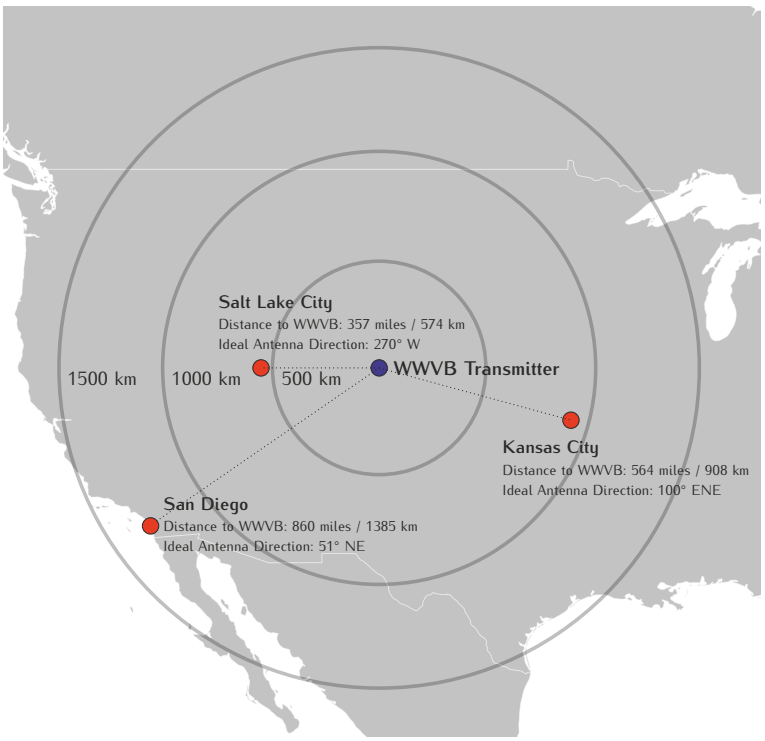


Abbildung: Ausrichtung einer AW02-60-Antenne von verschiedenen Standorten aus in den USA auf den WWVB-Sendeturm in der Nähe von Fort Collins, Colorado.

12.3.2.2 Auswahl des Antennenstandortes

Grundsätzlich gibt es zwei Möglichkeiten eine kompatible Meinberg Langwellen-Antenne (z.B. AW02) mit den im Lieferumfang enthaltenen Zubehör zu installieren:

1. Mastmontage

2. Wandmontage

Um sicherzustellen, dass das Langwellensignal zuverlässig empfangen werden kann und um Probleme bei der Synchronisation Ihres Meinberg-Produkts zu vermeiden, wählen Sie einen Standort, der eine unverbaute Sicht in Richtung Mainflingen (bei Frankfurt am Main) ermöglicht.

Die Sichtlinie zwischen Antenne und Signalquelle darf daher in keiner Weise beeinträchtigt werden. Die Antenne darf auch nicht unter Stromleitungen oder anderen elektrischen Stromkreisen installiert werden.

Weitere Installationskriterien für einen optimalen Betrieb:

- Die Antenne muss waagerecht montiert werden (siehe Abbildung).
- Sie sollte mindestens 30 cm (1 ft) von anderen Antennen entfernt sein.
- Die Längsseite der Antenne muss dem Sendemast zugewandt sein (siehe Abbildung).

Hinweis:

Wenn diese Kriterien nicht eingehalten werden, kann es zu Komplikationen bei der Synchronisation Ihres Meinberg-Systems kommen.

12.3.2.3 Montage der Meinberg-AW02-Antenne

Bitte lesen Sie vor der Installation sorgfältig die folgenden Sicherheitshinweise und beachten diese unbedingt.

Gefahr!

Antennenmontage ohne wirksame Absturzsicherung

Lebensgefahr durch Absturz!

- Achten Sie bei der Antennenmontage auf wirksamen Arbeitsschutz!
- Arbeiten Sie niemals ohne wirksame Absturzsicherung!

Gefahr!

Niemals an der Antennenanlage bei Gewitter arbeiten!

Lebensgefahr durch elektrischen Schlag!

- Führen Sie **keine** Arbeiten an der Antennenanlage oder der Antennenleitung durch, wenn die Gefahr eines Blitzeinschlages besteht.
- Führen Sie **keine** Arbeiten an der Antennenanlage durch, wenn der Sicherheitsabstand zu Freileitungen und Schaltwerken unterschritten wird.

12.3.2.4 Antennenkabel

Auswahl des richtigen Kabels

Meinberg bietet zusammen mit den Antennen passende Kabeltypen an, welche je nach Distanz von Antenne zur Meinberg-Referenzuhr bestellt werden können. Ermitteln Sie diese für Ihre Antenneninstallation zu überwindende Strecke vor Bestellung und wählen entsprechend den Kabeltyp aus.

Standardmäßig sind beide Kabelenden bei Auslieferung mit einem entsprechenden Stecker vorkonfektioniert, können aber auch nach Kundenwunsch unkonfektioniert ausgeliefert werden.

Achtung!

Bitte vermeiden Sie bei Ihrer Antenneninstallation einen Mischbetrieb mit unterschiedlichen Kabeltypen (z. B. RG58 und RG174). Beachten Sie dies ebenfalls beim Kauf von Kabeln für z. B. die Erweiterung einer bestehenden Kabelinstallation.

Die folgende Tabelle zeigt die typischen Spezifikationen der unterstützten Antennenkabeltypen bei der Übertragung der DCF77-Langwellenfrequenz:

Kabeltyp	RG58C/U	RG174U
Signallaufzeit bei 77,5 kHz	528 ns/100 m	558 ns/100 m
Dämpfung bei 77,5 kHz	0,57 dB/100 m	3,35 dB/100 m
Gleichstromwiderstand	5,3 Ω/100 m	33,8 Ω/100 m
Kabeldurchmesser	5 mm	2,8 mm
Max. Kabellänge	300 m	300 m

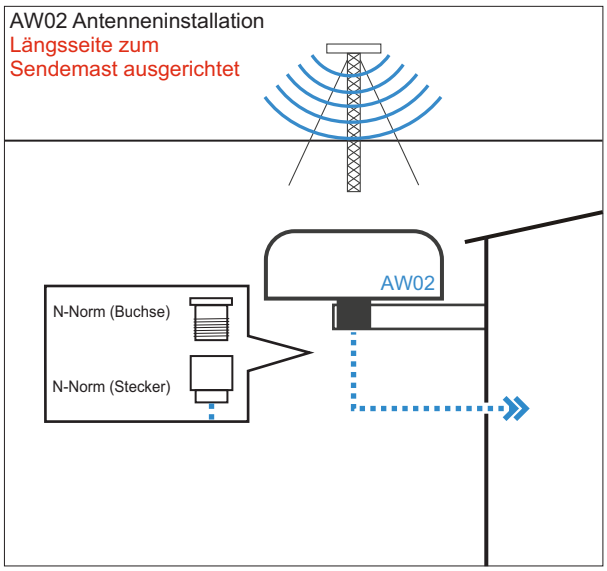
Tabelle 1: Spezifikationen der von Meinberg empfohlenen Kabeltypen

** Die Signallaufzeit bei 100 m Kabel ermöglicht eine Umrechnung der Signallaufzeit bei einer anderen beliebigen Kabellänge.*

Verlegung des Antennenkabels

Beachten Sie bei Verlegung des Antennenkabels, dass die angegebene max. Leitungslänge nicht überschritten wird: Diese Länge ist vom verwendeten Kabeltyp und dessen Dämpfungsfaktor abhängig. Bei Überschreitung kann eine einwandfreie Übertragung der zu übermittelnden Daten und damit eine korrekte Synchronisierung der Referenzuhr nicht gewährleistet werden.

Schließen Sie jetzt das Antennenkabel an die N-Norm Buchse der Antenne an. Führen Sie das andere Ende durch die Wand in das Gebäude.



Vorsicht!

Achten Sie bei der Verlegung des Antennenkabels darauf, dieses mit ausreichend Abstand zu stromführenden Leitungen (z. B. Starkstrom) zu verlegen, da diese durch „Übersprechen“ die Qualität des Antennensignals z. T. stark beeinträchtigen können. Weiterhin kann z. B. bei Blitzeinschlag, die auf einem Stromkabel auftretenden Überspannungen in das Antennenkabel „einkoppeln“ und so Ihr System beschädigen.

Weitere zu beachtende Punkte bei der Verlegung des Antennenkabels:

- Der minimale Biegeradius des Kabels ist zu beachten.[1]
- Quetschungen oder Verletzung der Außenisolierung sind zu vermeiden.
- Beschädigungen oder Verschmutzungen am Koaxialstecker sind zu vermeiden.

[1] *Der Biegeradius ist der Radius, mit dem ein Kabel gebogen werden kann, ohne es zu beschädigen (einschließlich Knicken)*

Im nächsten Kapitel **„Überspannungsschutz und Erdung“** wird die Installation eines wirksamen Überspannungsschutzes für die Antenneninstallation erläutert.

Kompensation der Signallaufzeit des Antennenkabels

Die Ausbreitung des Langwellensignals vom Sendemast zum Empfänger (Referenzuhr) kann eine gewisse Verzögerung mit sich bringen. Diese Verzögerung kann kompensiert werden, indem die Entfernung in Kilometern (Punkt zu Punkt, gerade Linie) zwischen dem Standort der Antenne und dem DCF77-Sendemast in Mainflingen, Deutschland, eingetragen wird.

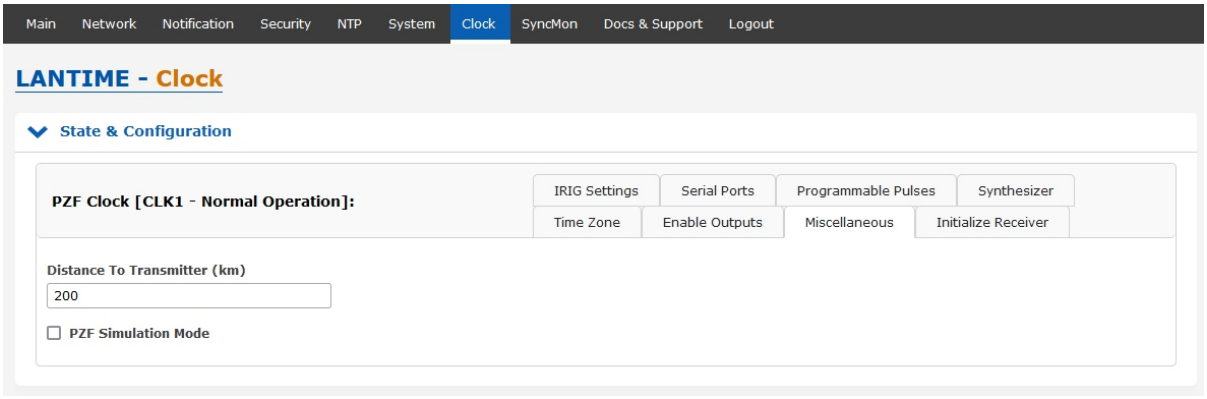


Abb. 4.1: „Uhr“ Menü im LANTIME OS Web Interface

12.3.2.5 Vorgehensweise bei der Antennenausrichtung

Bei der Ausrichtung Ihrer Antenne zeigt diese selbst keinen visuellen Status der Empfangsqualität des DCF77-Signals.

Schritt 1: Mit Hilfe eines Feldstärkemessgeräts kann die optimale Ausrichtung der montierten DCF77-Antenne überprüft werden. Dafür wird die Längsseite der Antenne (aufgedruckter Pfeil) zunächst grob in Richtung Frankfurt am Main ausgerichtet. Anschließend wird die Ausrichtung der Antenne feiner justiert, bis die Feldstärke im optimalen Bereich von –60 dB bis –70 dB liegt.

Steht kein Feldstärkemessgerät zur Verfügung, empfiehlt Meinberg die Ausrichtung und die damit verbundene Prüfung der Empfangsqualität zu zweit durchzuführen. Person 1 (an der Antenne) steht mit Person 2 (am Empfänger) in Verbindung.

Schritt 2: Person 1 dreht die Antenne langsam **gegen den Uhrzeigersinn**, bis Person 2 ein sekündliches Blinken der Modulations-LED ohne zwischenzeitliches Flackern beobachtet.

Ist dieses Verhalten noch nicht zu beobachten, wird die Antenne von der Ausgangsposition langsam im **Uhrzeigersinn** gedreht, bis Person 2 ein sekündliches Blinken der „Modulations"-LED ohne zwischenzeitliches Flackern beobachtet.

Bitte beachten Sie, dass ein hoher Signalpegel allein keine Garantie für einen guten Empfang ist, da ein solcher Pegel auch durch elektrisches Rauschen im entsprechenden Frequenzbereich verursacht werden kann.

Bei gutem Empfang sollte die angeschlossene DCF-Referenzuhr nach dem Einschalten innerhalb von drei Minuten synchronisieren.

Eine erfolgreiche Synchronisation ist erkennbar, wenn die „Sync After Reset"-LED von „aus" nach „grün" wechselt. Bei Empfangsstörungen wechselt die Farbe der „Free Run"-LED zum folgenden Minutenwechsel wieder auf rot. Befindet sich die Uhr für mehr als 12 Stunden im Freilauf, wird dies durch Blinken der „Sync"-LED angezeigt.

12.3.3 Einschalten eines DCF77 / PZF Empfänger

Wenn sowohl die Antenne als auch die Stromversorgung angeschlossen sind, ist das System betriebsbereit. Wenn der Empfang gut genug ist, dauert es bis zu drei Minuten nach dem Einschalten, bis der Empfänger synchronisiert ist. Ein hoher Wert für „Korrelation & Feld“ ist ein Indikator für eine gute Signalqualität.

Um die Feldstärke und den Signalkorrelationswert zu überprüfen, wählen Sie im Front-Display (wenn vorhanden) „Referenzzeit → Info PZF → Korrelation & Feld“.

Der Korrelationsstatus beginnt in einem „Rough-Modus“, wenn der Empfänger versucht, die erste Korrelation zu finden. Wenn eine gute Korrelation gefunden wurde, überprüft der Empfänger diese 20 Mal. Dieser Zustand wird als „Check“ bezeichnet und der Korrelationswert wird von 1 auf 20 erhöht. Wenn die Korrelationsqualität gut bleibt, wechselt der Zustand in den Modus „Fein“. Die Signalstärke sollte 100 oder höher sein.

Wenn keine Korrelation mit dem eingehenden Signal möglich ist, wechselt die Uhr automatisch in den DCF77 AM-Empfangsmodus und versucht, die Sekunden-Marken zu dekodieren.

12.4 Überspannungsschutz und Erdung

Die größte Gefahr für eine Antenneninstallation und nachgeschalteter Elektronik geht von Blitzeinschlägen aus. So erzeugt ein indirekter Blitzeinschlag in der Nähe der Antenne oder des Koaxialkabels hohe Spannungsspitzen, welche in das Kabel induzieren können.

Ohne einen Leitungsschutz können solche induzierten Spannungen zu einer erheblichen Beschädigung oder sogar Zerstörung von nicht nur der Antenne, sondern auch anderen Geräten im Innenraum führen, die an der Koaxialleitung anliegen, insbesondere von Ihrem Meinberg-System sowie angeschlossenen Empfängern und Signalverteilern. Solche Überspannungen stellen zudem ein Brand- und Verletzungsrisiko dar.

Aus diesem Grund müssen Antennen und Antennenkabel immer in die Gebäude-Potentialausgleichsanlage einbezogen werden, um die bei einem Einschlag in oder in unmittelbarer Nähe der Antenne auftretenden Blitzströme sicher in die Erde abzuleiten: Hier spricht man auch vom Blitzschutzpotentialaus-gleich.

Warnung!

Die Installation von Blitzschutzanlagen sowie Überspannungsschutzeinrichtungen (ÜSE) darf ausschließlich von Personal mit fachlichen Kenntnissen in der Elektroinstallation durchgeführt werden.

Meinberg GPSANTv2

In Meinbergs neuer Antennengeneration „GPSANTv2“ befindet sich ein integrierter Überspannungsschutz nach Norm IEC 61000-4-5 Level 4, welcher die Antenne wirksam vor Überspannung schützt. Weiterhin verfügt die Antenne über einen Erdungsanschluss um diese mittels Erdungskabel auf möglichst kurzem Weg an eine Potentialausgleichsleitung anzuschließen. Hier sind die Normen zur Antennenerrichtung VDE 0855 maßgeblich.

Für die Gebäudesicherheit und zum Schutz Ihres Meinberg-Systems bietet Meinberg optional den Überspannungsschutz MBG S-PRO an, auf den im weiteren Verlauf dieses Kapitels näher eingegangen wird.

Schutzmaßnahmen gegen auftretende Überspannungen

Maßgeblich für eine auf einem Gebäude installierten Antenne sind sowohl die Blitzschutznormen VDE 0185-305 (IEC 62305), die sich mit Gebäuden mit Blitzschutzanlage befasst, als auch die VDE 0855-1 (IEC 60728-11), welche auf den Potentialausgleich und die Erdung der Antennenanlage bei Gebäuden ohne äußeren Blitzschutz eingeht. Grundsätzlich gilt, dass Antennen immer in den Blitzschutzpotentialausgleich oder in die Gebäude-Potentialausgleichsanlage mit einbezogen werden müssen.

Bildet die Antenne den höchsten Punkt auf einem Gebäude oder einem Mast, sollte als Maßnahme des Überspannungsschutzes ein geschützter Bereich z. B. durch eine Fangstange hergestellt werden, welche die Antenne überragt. Auftretende Blitzenergie kann so von der Fangstange aufgenommen und die Blitzströme sicher über eine „Erdungsleitung“, die mit der Fangstange verbunden ist, gegen Erde abgeleitet werden.

Potentialausgleich

Als Potentialausgleich wird das Verbinden von metallischen, elektrisch leitfähigen Teilen der Antennenanlage bezeichnet, um so für Personen und angeschlossene Geräte gefährliche Spannungsunterschiede zu verhindern.

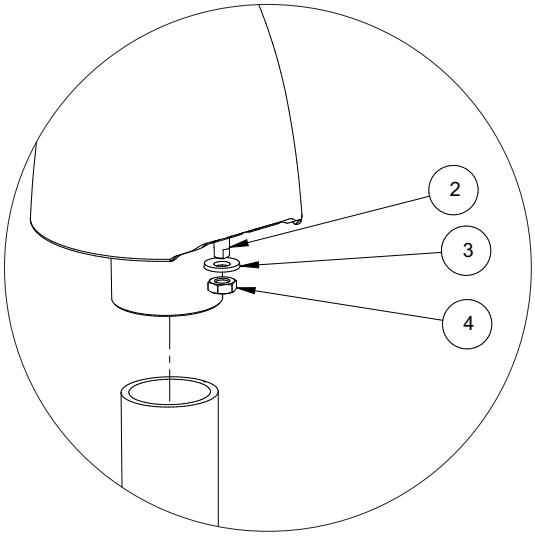
Hierfür sollten folgende Teile in den Potentialausgleich einbezogen und verbunden werden:

- die Schirme der Antennenkabel mit Hilfe von Schirmanschlussklemmen*
- die Innenleiter der Antennenkabel über Überspannungs-Schutzeinrichtungen
- Antennen, Antennenmasten
- Erder (z. B. Fundamenterder)

* Mindest-IP-Schutzart X4 bei Verwendung von Klemmen im Außenbereich.

Erdungsanschluss der Antenne

Wie erwähnt, muss die Antenne mittels Erdungskabel (nicht im Lieferumfang enthalten) mit einer Potentialausgleichsschiene verbunden werden. Konfektionieren Sie hierfür ein Erdungskabel mit einer empfohlenen Leitungsstärke von 4 mm^2 – 6 mm^2 und verwenden Sie einen für den M8 (0,315 Zoll) Erdungsbolzen passenden Ringkabelschuh.



Schritte bei der Montage des Erdungskabels:

1. Demontieren Sie die Mutter (Pos. 4) und die Spannscheibe (Pos. 3).
2. Führen Sie den Ringkabelschuh auf den Erdungsbolzen (Pos. 2).
3. Führen Sie zunächst die Spannscheibe (Pos. 3) auf den Erdungsbolzen (Pos. 2) und schrauben die M8-Mutter (Pos. 4) auf das Gewinde des Erdungsbolzens.
4. Schrauben Sie die Mutter (Pos. 4) mit einem Drehmoment von max. 6 Nm fest.

Schließen Sie nach der erfolgreichen Montage der Antenne das Erdungskabel an die Potentialausgleichsschiene an (siehe Abb. 5 u. 6).

Die folgenden Illustrationen zeigen eine nach den oben genannten Kriterien installierte Meinberg GPS-Antenne an einem Mast (z. B. Funkmast) sowie auf einem Hausdach.

Antenneninstallation ohne isolierte Fangeinrichtung

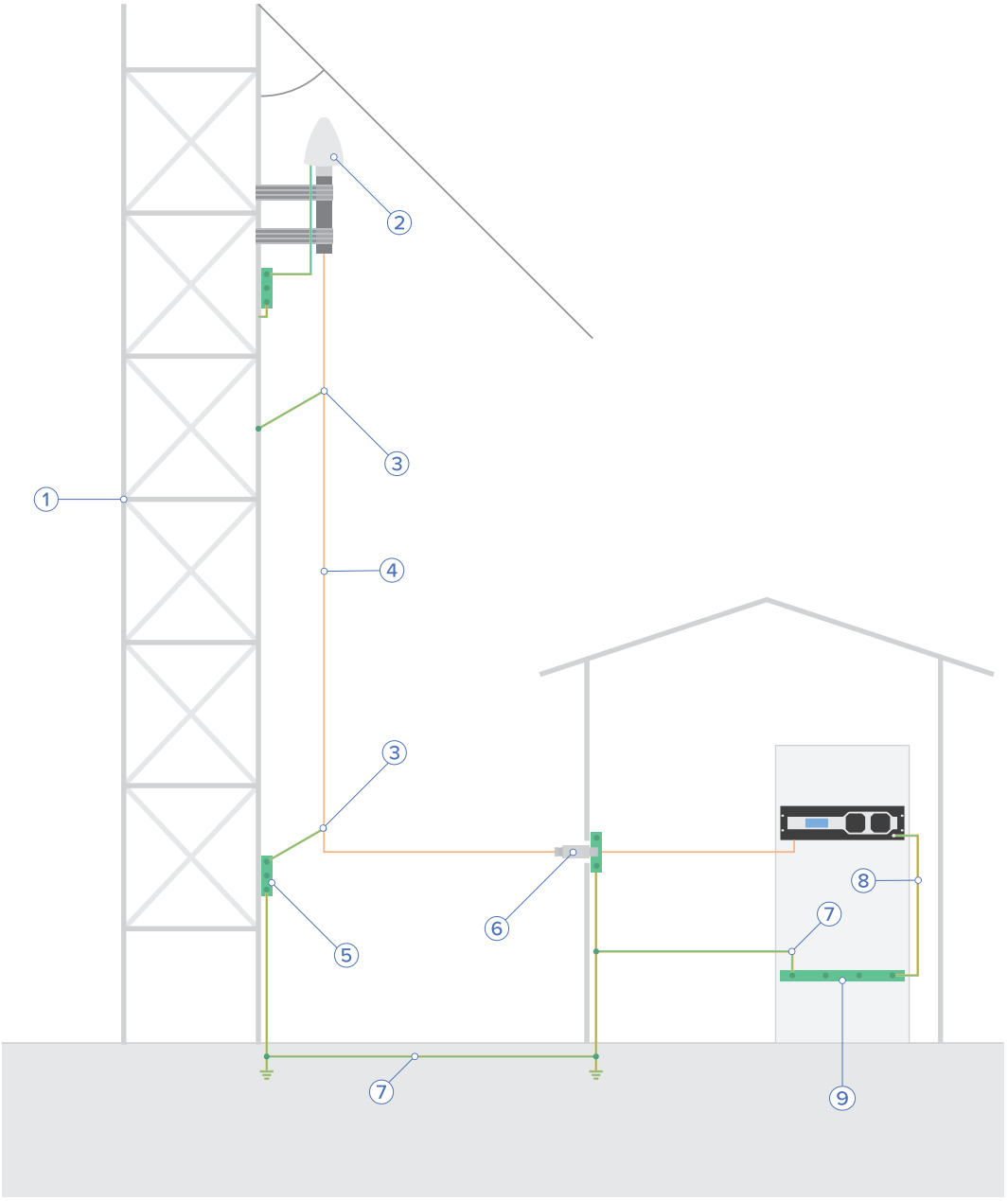


Abb.: Mastmontage

1	Antennenmast	6	Überspannungsschutz MBG S-PRO
2	Antenne	7	Potentialausgleichsleiter
3	Schirmerdungsklemme	8	Erdungsanschluss Gerät
4	Antennenkabel	9	Haupterdungsschiene
5	Potentialausgleichsschiene	α	Schutzwinkel

Antenneninstallation mit isolierter Fangeinrichtung

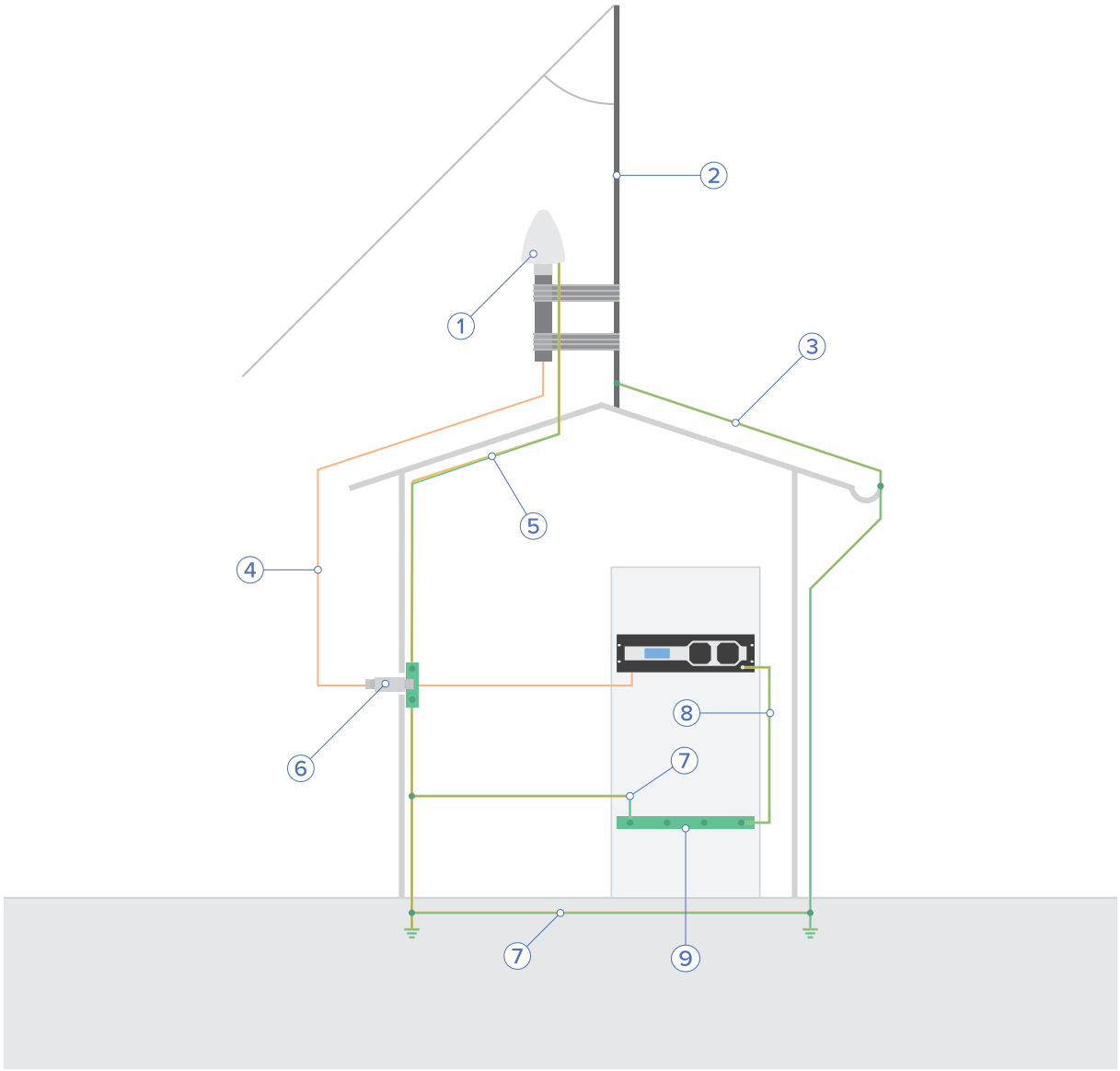


Abb. 6: Dachmontage

1	Antenne	6	Überspannungsschutz MBG S-PRO
2	Fangstange	7	Potentialausgleichsleiter
3	Fangleitung	8	Erdungsanschluss Gerät
4	Antennenkabel	9	Haupterdungsschiene
5	Erdungsanschluss Antenne	α	Schutzwinkel

Optionaler Überspannungsschutz MBG S-PRO

Hinweis:

Der Überspannungsschutz sowie das passende Koaxialkabel ist nicht im Standard-Lieferumfang einer Meinberg GPS-Antenne enthalten, ist jedoch optional bestellbar.

Aufbau

Der MBG S-PRO ist ein Überspannungsschutz (Phoenix CN-UB-280DC-BB) für koaxiale Leitungen. Er wird in die Antennenzuleitung eingebaut und besteht aus einem auswechselbaren Gasableiter, welcher nach dem Zünden die Energie vom Außenleiter des Kabels zum Erdungspotential ableitet.

Installationskriterien

Um im Überspannungsfall das Gebäude zu schützen, wird der MBG S-PRO am Gebäudeeintritt des Antennenkabels installiert. Der MBG S-PRO ist vor Spritzwasser zu schützen, entweder durch eine entsprechende Einhausung (IP65) oder eine geschützte Lage.

Optimale Installationsbedingungen:

- Installation am Gebäudeeintritt des Antennenkabels
- Erdungsleitung zur Potentialausgleichsschiene so kurz wie möglich

Montage und Anschluss

Der Überspannungsschutz hat keinen dedizierten Eingang/Ausgang und somit keine bevorzugte Einbaulage. Er verfügt an beiden Seiten über N-Norm Buchsen.

Montage

1.
Montieren Sie den Überspannungsschutz, wie auf der Darstellung gezeigt, an dem mitgelieferten Montagewinkel.

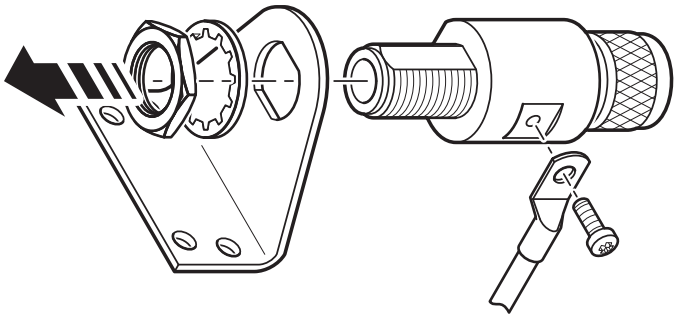


Abb. 7: Montage des Überspannungsschutzes

2.
Verbinden Sie den MBG S-PRO über eine möglichst kurze Erdungsleitung an einer Potentialausgleichsschiene. Wichtig ist weiterhin, dass die Erdungsleitung des Überspannungsschutzes mit der gleichen Potentialausgleichsschiene wie das angeschlossene Meinberg-System verbunden ist, damit keine zerstörenden Potentialunterschiede entstehen können.

3.
Schließen Sie das von der Antenne kommende Kabel an die eine Buchse des Überspannungsschutzes an und an die andere Buchse das Koaxialkabel, welches vom Überspannungsschutz zur nachgeschalteten Meinberg Referenzuhr führt.

Vorsicht!

Wenn keine weiteren Geräte (z. B. Power Splitter) zwischen Überspannungsschutz und nachgeschalteter Elektronik mit Feinschutz installiert sind, darf das Antennenkabel aus Sicherheitsgründen eine bestimmte Länge nicht überschreiten.

Detaillierte Montagehinweise und Spezifikationen des Überspannungsschutzes, entnehmen Sie bitte dem Anhang „Technische Daten - MBG S-PRO Überspannungsschutz“, sowie dem Datenblatt des Herstellers.

Datenblatt zum Download:

https://www.meinberg.de/download/docs/shortinfo/german/cn-ub-280dc-bb_pc.pdf

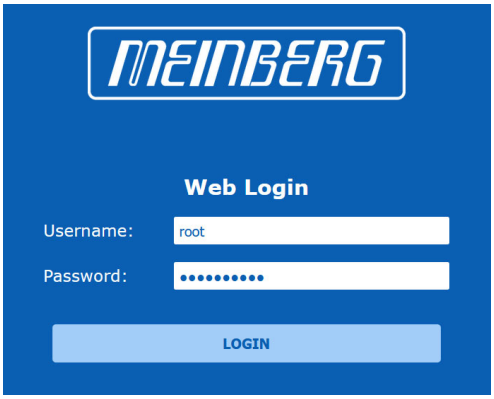
13 LTOS Management und Überwachung

13.1 Das Webinterface

13.1.1 Session Handling

Session-Handling der Web-Benutzerschnittstelle ab LTOS 7.08
Das Session-Handling der web-basierten Benutzerschnittstelle unterstützt mit der Version 7.08.002 die Authentifizierung über ein Formular („form-based auth“). Das bisherige Authentifizierungsverfahren „basic-auth“ des WebUI wird damit ersetzt. Der Sitzungsschlüssel wird nun in einem Cookie gespeichert und übertragen, um nach einer erfolgreichen Anmeldung den autorisierten Zugriff auf das Webinterface nachzuweisen. Die meisten Browser unterstützen dieses Authentifizierungsverfahren, sofern Cookies aktiviert sind, automatisch und Nutzer sollten keine grundlegenden Veränderungen im Umgang mit dem Webinterface feststellen können.

Die Abbildung rechts zeigt den Login-Bildschirm des LANTIME. Nachdem Sie mit der IP des LANTIMEs in der Adresszeile des Browsers das Webinterface geöffnet haben, können Sie sich jetzt hier anmelden. Im Auslieferungszustand melden Sie sich mit den Default-Zugangsdaten an:



User: **root**
Passwort: **timeserver**

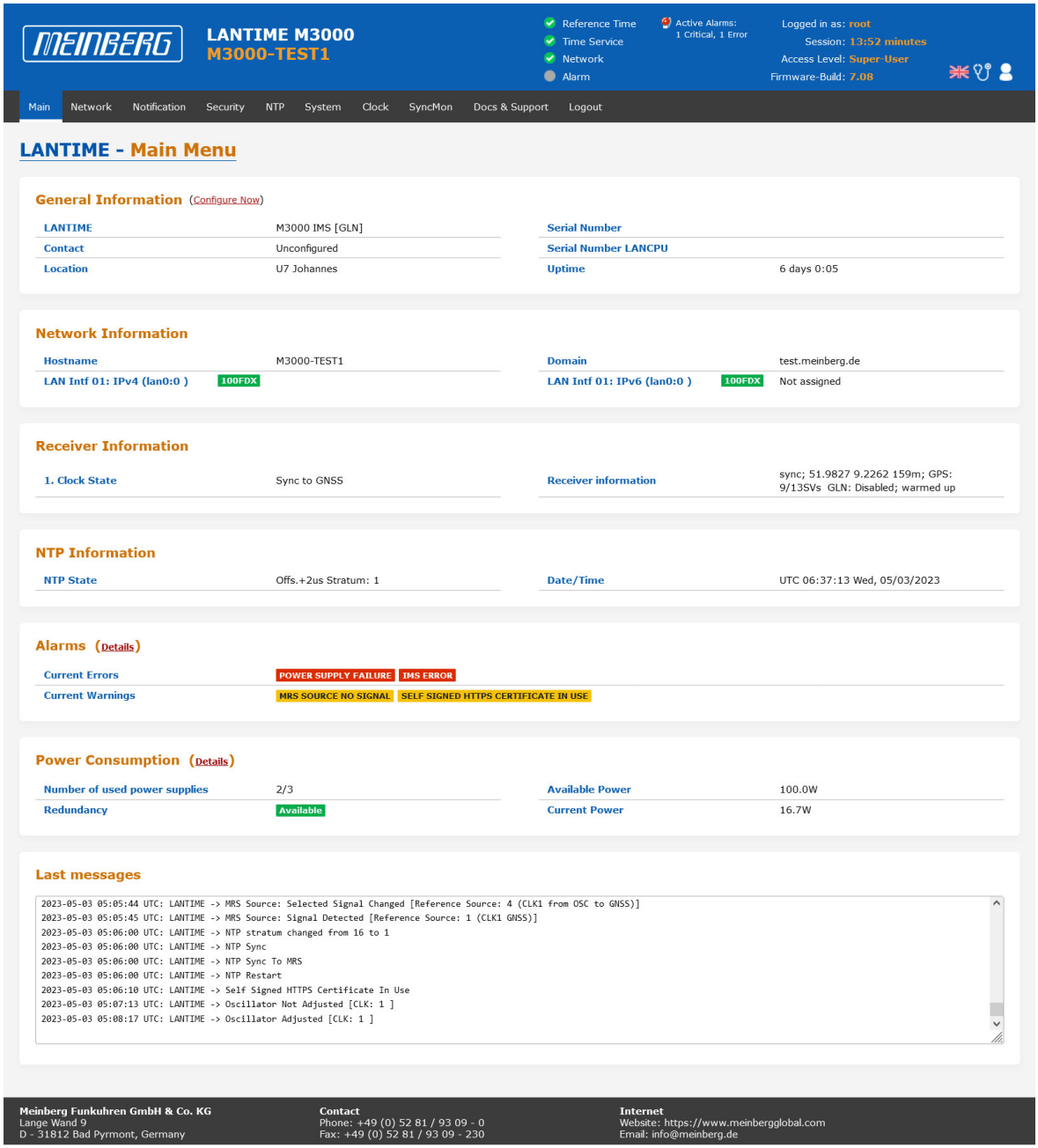
Cyber-Sicherheitshinweis

Das Standardpasswort muss sofort geändert werden, bevor Sie mit der Systemkonfiguration fortfahren. Wenn Sie sich zum ersten Mal anmelden, werden Sie direkt zum Menü „System → Benutzerverwaltung“ weitergeleitet. Sie können danach beliebig viele Benutzer mit unterschiedlichen Rechten anlegen (siehe ➜ Kapitel 13.1.9.4, „Benutzerverwaltung“).

Achtung!

Im Auslieferungszustand ist die Einstellung für „Bruteforce-Erkennung“ auf drei Versuche eingestellt. Sollten Sie beim Anmelden unter Umständen dreimal die falschen Logindaten eingegeben haben, dann müssen Sie drei Minuten warten, bevor Sie den nächsten Login-Versuch durchführen können. Die Einstellungen für Bruteforce-Erkennung und Sperrzeit werden im ➜ Kapitel 13.1.5, „Sicherheit“ beschrieben.

13.1.2 Startmenü

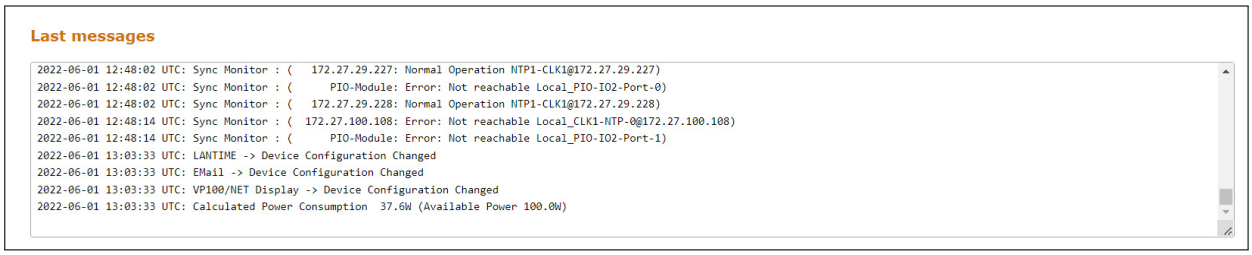


In diesem Kapitel finden Sie Konfigurations- und Statusinformationen Ihres LANTIME-Systems, auf die Sie über die Web-GUI zugreifen können.

Die Startseite gibt einen Überblick über die wichtigsten Konfigurations- und Statusparameter des Systems.

- Informationen über das LANTIME-Modell und die verwendete Firmware
- Netzwerkinformationen
- Status des Empfängers
- NTP-Status
- PTP-Status (Option)
- Letzte Nachrichten
- Statistiken (NTP/MRS Leistung, NTP Zugriff....)
- Erweiterte Statistiken mit Sync-Monitor
- Dokumentation (Handbücher), Supportinformationen

Das Feld im unteren Bereich zeigt die letzten Nachrichten des Systems mit einem Zeitstempel an. Die neuesten Nachrichten stehen ganz unten in der Liste. Dieses ist der Inhalt der Datei /var/log/lantime_messages, die nach jedem Systemstart erstellt wird (und nach einem Ausschalten oder Neustart verloren geht).



Über die Navigation oben auf der Seite erreichen Sie eine Reihe von Konfigurationsmenüs, die in den folgenden Kapiteln beschrieben werden.

13.1.2.1 Einleitung

Um eine http- oder eine gesicherte https-Sitzung mit dem Web Interface auf der CPU Ihres LANTIME-Systems zu starten, müssen Sie Ihren Internetbrowser öffnen und die IP-Adresse der Netzwerk-Schnittstelle eingeben, die Sie für diese Verbindung verwenden. Per Standardkonfiguration ist das https-Protokoll an jeder Netzwerkschnittstelle aktiviert. Http-Anfragen werden automatisch an https umgeleitet.

Wenn Sie nur eine dedizierte Netzwerkschnittstelle für Management und Monitoring und den Rest für andere Dienste nutzen möchten, finden Sie die entsprechenden Konfigurationsoptionen im Kapitel „LTOS Management und Überwachung → Webinterface → Netzwerk“ im Abschnitt Netzwerkdienste.

Wenn die Verbindung mit dem LANTIME korrekt hergestellt wurde, werden Sie aufgefordert, Login-Daten einzugeben, um die Web-Sitzung zu starten. Standardmäßig lautet die Eingabe von Benutzername/Passwort: root/timeserver.

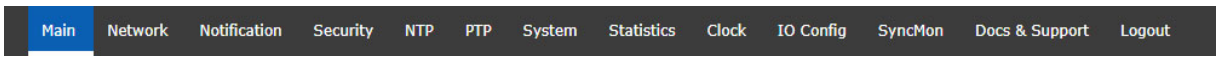
Aus Sicherheitsgründen müssen Sie alss *root*-Benutzer das Standard-Passwort nach der ersten Anmeldung ändern. Die entsprechenden Einstellungen zur Benutzerverwaltung finden Sie im Kapitel „LTOS Management und Überwachung → Das Webinterface → System“ im Abschnitt Benutzerverwaltung.

Die Hauptseite enthält einen Überblick über die wichtigsten Konfigurations- und Statusparameter des Systems, einschließlich:

- allgemeine Informationen (Modellname, Seriennummer, Betriebszeit seit dem letzten Neustart)
- zugeordnete Netzwerk- und PTP-Schnittstellen (beide in IPv4- oder IPv6-Konfiguration)
- Empfänger-Statusinformationen (synchronisieren oder nicht, bei GNSS-Empfängern einige zusätzliche Satellitendaten)
- SHS (Secure Hybrid System) Status in redundanter Empfängerkonfiguration, der einen Plausibilitätsmodus bietet, bei dem die Eingangszeiten beider Zeitsignale kontinuierlich miteinander verglichen werden. Weitere Informationen zum SHS-Modus und den entsprechenden Einstellungen finden Sie im Kapitel „LTOS Management und Überwachung → Das Webinterface → Sicherheit → SHS-Konfiguration“.

13.1.2.2 Das Hauptmenü - Navigation im Webinterface

Über die Navigation oben auf der Seite erreichen Sie eine Reihe von Konfigurationsmenüs, die in den folgenden Kapiteln beschrieben werden.



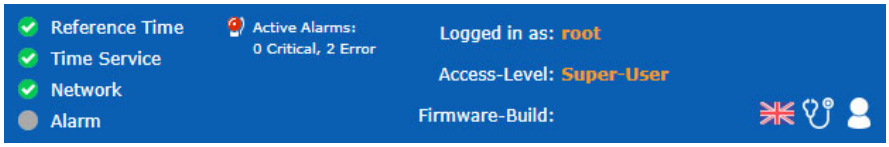
Wenn Sie auf der Hauptseite nach unten scrollen, finden Sie einen Abschnitt mit den letzten Protokollmeldungen, die während des LANTIME-Betriebes erzeugt wurden. Die Nachrichten in diesem Feld sind auf die letzten 50 begrenzt und chronologisch geordnet. Die Meldungen werden in der Datei */var/log/lantime_messages* gespeichert, die nach jedem Systemstart erstellt wird (und nach einem Ausschalten oder Neustart verloren geht). Um alle Protokollmeldungen in der Protokolldatei anzuzeigen, müssen Sie das CLI (Command Line Interface) verwenden. Zu Ihrer Information finden Sie eine Liste der verfügbaren CLI-Befehle für die LANTIME-Verwaltung und -Überwachung in der Kommandozeilen-Referenz.

13.1.2.3 Webinterface - Benachrichtigungen und Alarme

Oben auf der Hauptseite in der rechten Ecke finden Sie ein Bild der Status-LED-Lampen, die sich auch physisch an der Vorderseite eines LANTIME-Systems befinden (Modelle mit integrierter Frontplatteneinheit). Wenn das System in Betrieb ist und alles wie erwartet läuft, leuchten die oberen drei Status-LEDs grün und die Alarmanzeige erlischt. Wenn Sie nach dem Einschalten des Systems und nach Abschluss des Startvorgangs feststellen, dass eine oder mehrere LEDs rot leuchten, lesen Sie bitte das Kapitel über Troubleshooting und Alarmierungen.

Bitte beachten Sie: Der Start des Systems kann je nach Hardwarekonfiguration Ihres Systems einige Minuten dauern.

Neben den Status-LEDs werden alle aktiven Alarme angezeigt, die derzeit in einem LANTIME als kritisch und schwerwiegend eingestuft sind. Mit einem Mausklick auf die Alarme gelangen Sie zu einer Tabelle der Benachrichtigungsereignisse die die Alarme ausgelöst haben. Diese sind mit roten Indikatoren gekennzeichnet.



Weitere Informationen zur Beseitigung einer Ursache für jeden einzelnen Alarm finden Sie im Kapitel Troubleshooting und Alarmierungen.

Neben dem Alarmbereich auf der Hauptseite befindet sich ein Feld mit Informationen über Ihren Login-Status und Informationen darüber, zu welcher Access-Level-Gruppe Sie als aktueller Benutzer gehören. Es gibt drei Arten von Benutzern: Super-User, Admin-User und Info-User. Die genauen Definitionen der drei verschiedenen Benutzertypen und deren Zugriffsrechte finden Sie im Kapitel „LTOS Management und Überwachung → Das Webinterface → System → Benutzerverwaltung“.

In der oberen rechten Ecke der Hauptseite sehen Sie weitere Symbole. Die angezeigte Flagge zeigt das Sprachpaket an, das gerade für die Anzeige der Weboberfläche aktiviert ist. Im Moment können Sie zwischen englischen und deutschen Sprachpaketen wählen.

Neben dem Sprachkennung befindet sich ein „Arzt-Stethoskop-Symbol“. Dieses Icon ist mit einer Diagnose-Datei des Systems verknüpft. Alle notwendigen Daten für die Diagnose und Fehlersuche des Gerätes sind in dieser Datei enthalten. Durch Anklicken dieses Symbols wird sofort eine aktuelle Diagnosedatei zum Herunterladen erzeugt, die Sie auf Ihrem lokalen Computer speichern und weiterverwenden können. Der Download kann je nach Dateigröße, die mehrere MB betragen kann, bis zu 60 Sekunden dauern. In der Diagnose-Datei werden alle Daten über die Systemkonfiguration und Protokollmeldungen gesammelt. Die Diagnose-Datei kann auch ein wichtiges Werkzeug für das Meinberg-Support-Team sein, wenn Sie Hilfe bei der Konfiguration benötigen oder Probleme haben, die Sie nicht alleine lösen können. Mehr Informationen zur Diagnosedatei finden Sie im Kapitel „LTOS Management und Überwachung Konfiguration → Das Webinterface → System → Download Diagnosedatei“.

Die Weboberfläche ist in mehrere Dialogmenüs unterteilt, wobei einige der Menüpunkte (z.B. PTP, IO-Konfiguration, SyncMon) von den im LANTIME-System integrierten Hardwarekomponenten abhängen und nur in Systemen mit entsprechender Konfiguration erscheinen. Die restlichen Dialoge sind für alle LANTIME- und IMS-Systeme gleich.

Sie können zwischen den Dialogen wechseln, indem Sie auf einen Menüpunkt oben in der Menüzeile klicken. Haben Sie in einem Dialog etwas an den Einstellungen geändert, müssen Sie den „Speichern-Button“ betätigen, bevor Sie in einen anderen Topmenü-Eintrag wechseln. Wenn Sie auf „Logout“ klicken, wird Ihre laufende Web-Session mit dem LANTIME-Gerät sofort beendet.

Die beiden Dialoge „Main“ und „SyncMon“ liefern Ihnen nach dem letzten Neustart die Statusinformationen über das LANTIME-System. Der Rest der Dialoge bietet Konfigurationen von Funktionen für den LANTIME-Betrieb und die verwendeten Dienste. Die Dialoge mit Eigenschaft-Konfigurationen werden in einer Baumstruktur dargestellt, in der jedes Untermenü durch Anklicken des Zeichens „→“ am Anfang der Untermenüzeile zu einem Submenü erweitert werden kann. Wenn Sie den Dialog öffnen, wird der „→“ zu „↓“ und wenn Sie auf das „↓“-Symbol klicken, wird der aktuell geöffnete Dialog geschlossen. Sie können im aktuell ausgewählten Menü einige Dialoge gleichzeitig öffnen (siehe Abbildung auf der nächsten Seite).

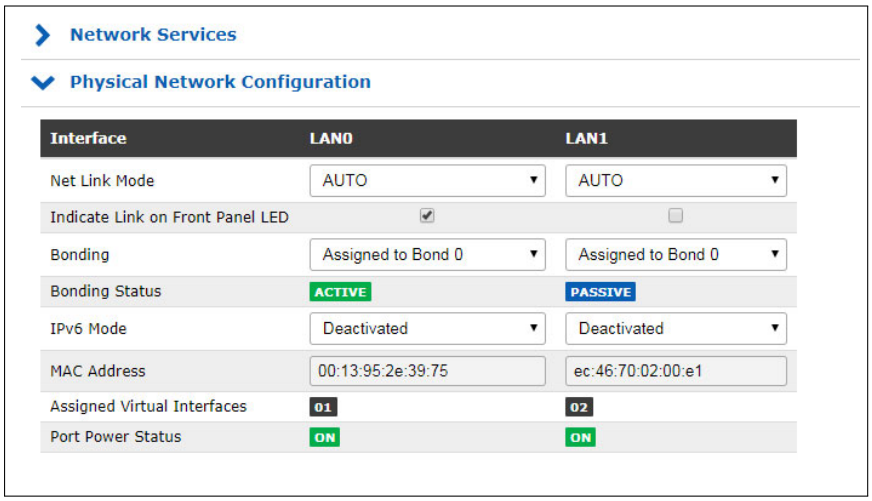


Abbildung: Eine Baumstruktur der einzelnen Menüs. Öffnen einer Verzweigung durch Anklicken eines „→-Symbols“ und Schließen durch „↓“ vor dem Menünamen.

Im Allgemeinen müssen Sie in jedem Konfigurationsmenü, in dem Sie sich befinden, beim Ausfüllen oder Bearbeiten eines oder mehrerer Funktionsfelder am Ende der Seite die Einstellung durch Anklicken der Schaltfläche „Einstellungen speichern“ am unteren Rand der Seite bestätigen. Wenn Sie diesen Schritt ausführen und die Einstellung erfolgreich übernommen wurde, erhalten Sie im Hauptmenü einen Dialog mit einer Bestätigungsnachricht auf einem grünen Feld. Gleichzeitig mit der Anwendung einer neuen Konfiguration erscheint eine Logmeldung in der Liste der letzten Meldungen im Hauptmenü: „Gerätekonfiguration geändert“.

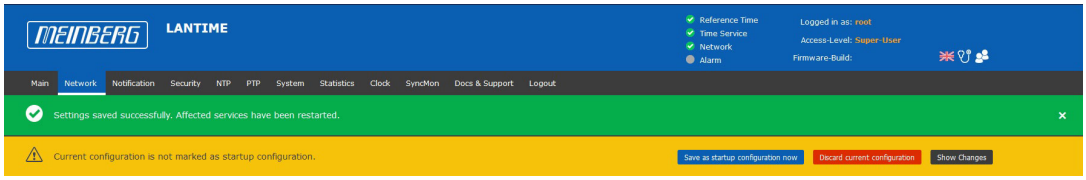


Abbildung: Einstellungen wurden erfolgreich gespeichert. Betroffene Dienste wurden neu gestartet.

Ein Dialog zum Speichern der Startkonfiguration. Optionen zum Speichern, Verwerfen der aktuellen Konfiguration und Anzeigen von Änderungen zwischen der Startkonfiguration und der aktuellen Konfiguration.

Neben der Konfigurationsmeldung erhalten Sie auch einen Aufmerksamkeitshinweis, der auf einer gelben Leiste angezeigt wird: „Die aktuelle Konfiguration ist noch nicht als Startkonfiguration gekennzeichnet“. Das bedeutet, dass Sie die neue Konfiguration zunächst durch Anklicken einer Schaltfläche „Jetzt sichern als Startkonfiguration“ bestätigen müssen, wenn Sie diese beim nächsten Systemstart als Startkonfiguration ausführen möchten. Wenn Sie auf diese Schaltfläche klicken, erhalten Sie eine weitere Bestätigungsnachricht: „Aktuelle Konfiguration wirklich als Startkonfiguration aktivieren?“, die Sie durch Anklicken der Schaltfläche „OK“ bestätigen. Die neue Konfiguration ist nun die aktive Startkonfiguration auf Ihrem LANTIME-System.

Wenn Sie hingegen zur zuletzt gespeicherten Startkonfiguration zurückkehren möchten, wählen Sie die Schaltfläche „Aktuelle Konfiguration verwerfen“, wenn die Meldung auf einer gelben Leiste erscheint.

Jeder Eintrag, den Sie in den angebotenen Dialogen eingeben, wird auf Plausibilität für dieses Feld geprüft. Wenn Sie z.B. falsche Zeichen verwendet haben (z.B. Buchstaben in der IP-Adresse oder Sonderzeichen, die nicht erlaubt sind) oder Sie eine ungültige Netzwerkkonfiguration angegeben haben, erhalten Sie eine Meldung auf einem roten Balken, die eine Fehlermeldung und den Zeitpunkt des Eigenschaften-Eintrags angibt. Der falsche Eintrag wird vom System nicht akzeptiert, auch nicht der Rest der neuen Einstellungen, die Sie zu diesem Zeitpunkt vorgenommen haben, daher müssen Sie die Konfigurationsschritte erneut durchführen. Siehe nachfolgend ein Beispiel für eine Warnmeldung, wenn ein Fehler bei der Eingabe eines Parameterwertes auftritt.

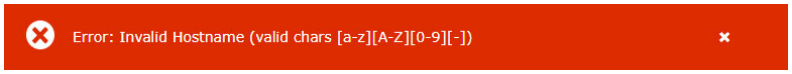
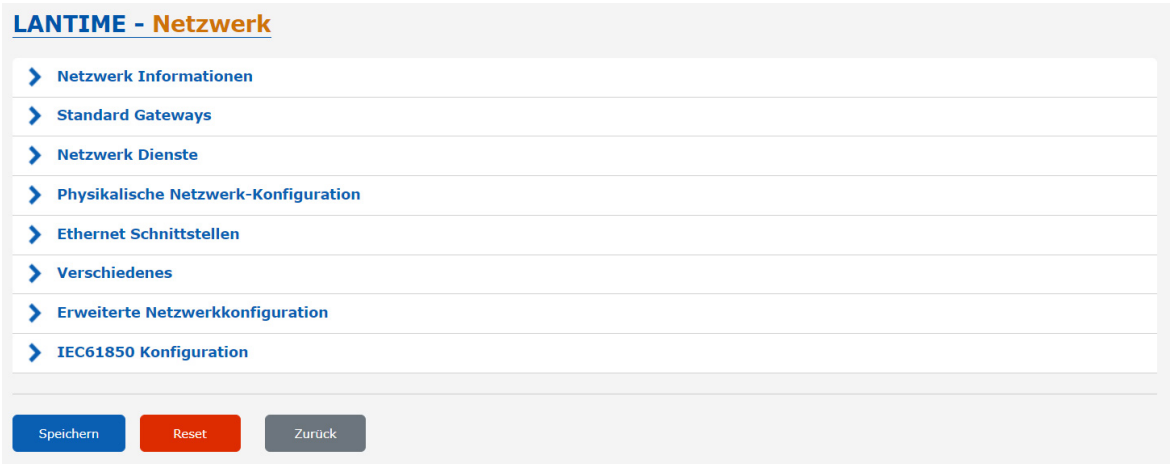


Abbildung: Anzeige einer Warnmeldung mit einer Fehlermeldung und Angabe, zu welchem Parameter die Meldung gehört.

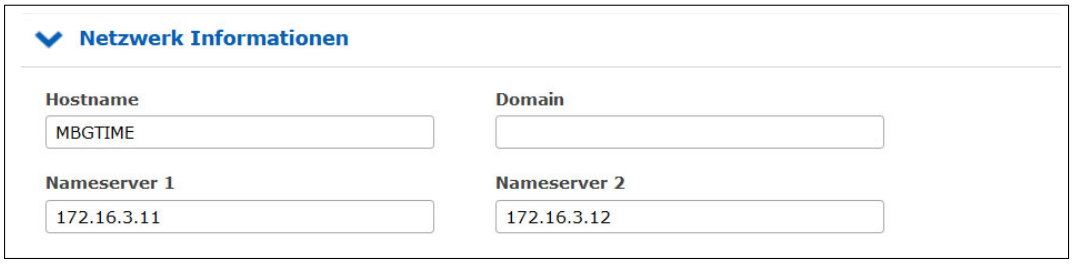
Erlaubte Zeichen und Sonderzeichen, mit denen Sie Dialogfelder ausfüllen können, finden Sie im Kapitel „Vor dem Start → Text- und Syntaxkonventionen“.

Zur Konfiguration der Systemfunktionen gehen Sie nun in das entsprechende Menü, das in einem der folgenden Kapiteln beschrieben wird.

13.1.3 Netzwerk



13.1.3.1 Netzwerk Informationen



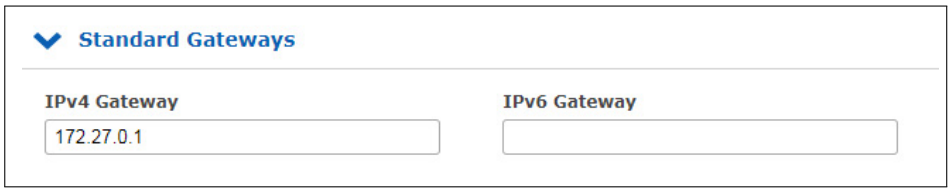
Hostname
Der Hostname des LANTIME ist ein eindeutiger Name eines Computers in einem Netzwerk. Jede im LANTIME konfigurierte IP-Adresse ist diesem Hostnamen zugeordnet.

Domain
Dieses Feld wird verwendet, um den Netzwerkdomain-Namen zu konfigurieren. Ein Netzwerkdomänenname ist ein textbasiertes Label, das leichter zu merken ist als die im Internetprotokoll verwendeten numerischen Adressen (z.B. meinberg.de).

Nameserver1
IP-Adresse des primären DNS-Servers im Netzwerk.
Der DNS-Server wird verwendet, um sowohl IP-Adressen als auch Hostnamen in einem Netzwerk aufzulösen.

Nameserver2
Hier kann ein alternativer Nameserver eingetragen werden.

13.1.3.2 Standard Gateways

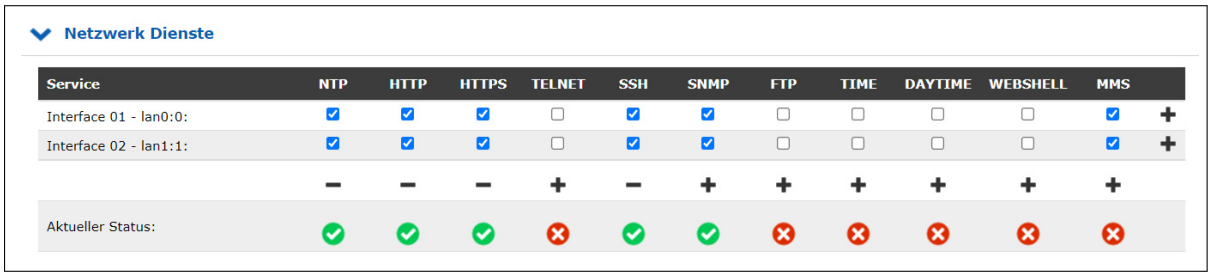


In diesem Menü können Sie Standardgateways konfigurieren, die für IPv4 und IPv6 verwendet werden. Für ein Standard-Gateway wird in der Hauptroutinentabelle eines LANTIME ein „default"-Eintrag angelegt. Wenn der LANTIME keine direkte Route oder Routingregel zu einer Ziel-IP hat, wird er immer versuchen, das Ziel über das Standard-Gateway zu erreichen.

IPv4 Gateway Konfiguration des standardmäßigen IPv4-Gateways.

IPv6 Gateway Konfiguration des standardmäßigen IPv6-Gateways.

13.1.3.3 Netzwerkdienste



In diesem Untermenü können Sie verschiedene Dienste für die vorhandenen virtuellen Netzwerkschnittstellen aktivieren oder deaktivieren. Mit den +/- Tasten können Sie ganze Zeilen oder Spalten in der Matrix markieren oder abwählen.

Die folgenden Service-Status sind möglich:

- Für mindestens eine virtuelle Schnittstelle wurde ein Dienst aktiviert und ist aktiv.
- Der Dienst wurde für keine virtuelle Schnittstelle aktiviert und wird daher gestoppt.

Die folgenden Dienste werden vom LANTIME unterstützt:

NTP: Network Time Protocol, UDP Port 123

HTTP: Hyper Transfer Protocol, TCP Port 80

HTTPS: Hyper Transfer Protocol Secure, TCP Port 443

TELNET: Teletype Network, TCP Port 23

SSH: Secure Shell, TCP Port 22

SNMP: Simple Network Management Protocol, UDP Port 161 / 162 (Traps)

FTP: File Transfer Protocol, TCP Port 20

TIME: Time Protocol, TCP/UDP Port 37

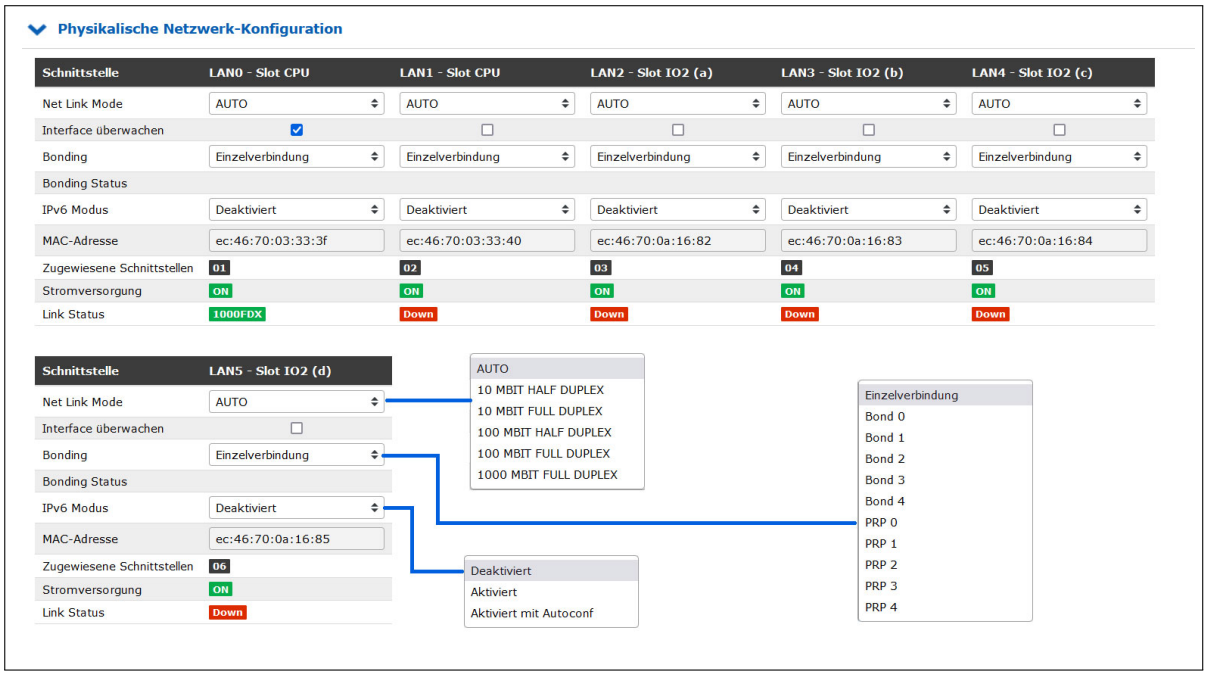
DAYTIME: UDP Port 13

WEBSHELL: Melden Sie sich über einen Webbrowser an einer Befehlszeilenschnittstelle eines LANTIME an. WEBSHELL arbeitet auf Port 4200. Eingabe im Webbrowser: [IP/HOSTNAME]: 4200

MMS: Die Manufacturing Message Specification (MMS) standardisiert den Austausch von Nachrichten im Produktionsbereich.

Hinweis: Zur Durchführung einer IEC61850-Konfiguration muss dieser Dienst aktiviert werden (siehe → Kapitel 13.1.3.10, „IEC 61850-Konfiguration“).
IEC61850 (MMS) arbeitet auf dem TCP-Port 102.

13.1.3.4 Physikalische Netzwerkkonfiguration



Net Link Mode
Ermöglicht die Konfiguration des Netzwerkverbindungsmodus der Schnittstelle. Sie können zwischen den unterstützten Verbindungsmodi der jeweiligen physikalischen Schnittstelle wählen.

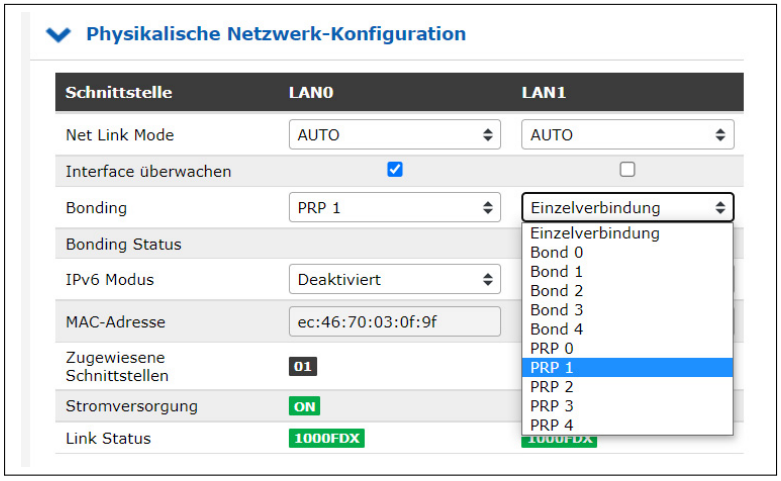
Der Standardwert AUTO (Autonegotiation) kann unter normalen Umständen unverändert bleiben. Autonegotiation bezieht sich auf ein Verfahren, das es zwei miteinander verbundenen Ethernet-Geräten ermöglicht, unabhängig voneinander die maximal mögliche Übertragungsgeschwindigkeit und das Duplexverfahren auszuhandeln und entsprechend zu konfigurieren.

Interface überwachen
Sobald einer der ausgewählten Netzwerkports keine Verbindung hat, wird dieser Status durch eine rote LED „Network“ auf der Frontplatte angezeigt und das Ereignis „Network Link Down“ gemeldet. Wenn an allen ausgewählten Ports eine Netzwerkverbindung verfügbar ist, leuchtet die LED „Network“ auf der Vorderseite grün.

Bonding
Hier können 2 oder mehr physikalische Netzwerkports zu einer Bonding-Gruppe zusammengefasst werden. Der LANTIME unterstützt die Bonding-Modi „Active - Backup“ und „LACP“. Der zu verwendende Modus kann im Submenü „Netzwerk → Sonstiges → Bonding-Modus“ ausgewählt werden. Weitere Informationen zur Funktionsweise der beiden Modi finden Sie im Submenü „Verschiedenes“.

PRP

PRP steht für Parallel Redundancy Protocol und ist seit 2010 in der Norm IEC 62439-3 definiert. PRP ist Layer-2-basiert und wurde für Computernetzwerke entwickelt, die eine zuverlässige Lösung in Bezug auf Hochverfügbarkeit und Betriebsfunktionalität benötigen. Ein LANTIME mit zwei oder mehr Schnittstellen und der Firmware 6.22.001 oder höher hat die Möglichkeit, als DAN zu fungieren („Dual Attached Node" - ein Gerät, das an beide redundanten Netzwerke angeschlossen ist).



Ab der LANTIME-Firmware-Version 7.0 ist PRP auch bequem über das Webinterface-Menü „Netzwerk → Physikalische Netzwerk-Konfiguration" einzustellen. Wählen Sie im Drop-Down-Menü „Bonding" für mindestens zwei Schnittstellen die gleiche PRP-Gruppe aus.

IPv6 Modus

Aktivierung oder Deaktivierung des IPv6-Protokolls.

MAC Adresse

Media Access Control, zeigt die MAC-Adresse der angegebenen physikalischen Schnittstelle an.

Zugewiesene Schnittstellen

Gibt an, welche virtuellen Schnittstellen der angegebenen physikalischen Schnittstelle zugeordnet sind.

Stromversorgung

Diese Funktion ist in IMS-Systemen verfügbar, in denen mehrere physikalische Schnittstellen verfügbar sein können. Der Port Power Status zeigt an, ob eine bestimmte physikalische Schnittstelle ein- oder ausgeschaltet ist.

Hinweis:

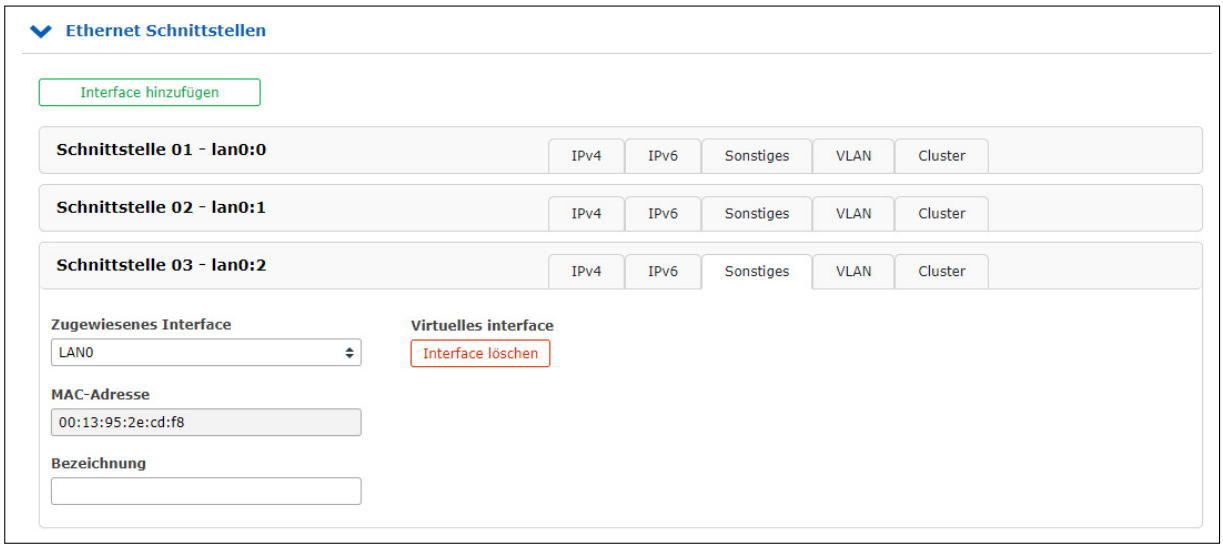
Der Status der Stromversorgung (Port Power Status) kann nur bei Netzwerkschnittstellen , die sich auf einer LNE-SFP-Netzwerkkarte befinden, in den Status „off" wechseln. Sollte zum Beispiel beim Nachrüsten eines IMS-Moduls die maximal zur Verfügung stehende Leistung nicht mehr ausreichen, dann wird ein vorhandenes LNE-SFP-Modul ausgeschaltet.

Prüfen Sie bitte vor dem Einsatz eines zusätzlichen IMS-Moduls immer die maximal zur Verfügung stehende Leistung der vorhandenen Netzteile im Webinterface-Menü „System → Leistungsaufnahme".

Link Status

Der Link Status gibt die von der jeweiligen Netzwerkschnittstelle erkannte Geschwindigkeit an.

13.1.3.5 Netzwerk-Schnittstellen



In diesem Menü werden die virtuellen Schnittstellen des LANTIME verwaltet. Jedem verfügbaren physikalischen Port können bis zu 99 virtuelle Schnittstellen zugeordnet werden. Der Name der virtuellen Schnittstelle besteht aus einer fortlaufenden Nummer der zugeordneten physikalischen Schnittstelle und der Nummer einer virtuellen Schnittstelle (beginnend mit Null).

Das obige Beispiel zeigt eine Konfiguration, in der der physikalischen Schnittstelle **LAN0** insgesamt drei virtuelle Schnittstellen zugeordnet sind, nämlich **lan0:0**, **lan0:1** und **lan0:2**.

Im Falle eines aktiven „Bonding“ wird die physikalische Schnittstelle durch den Namen der Bonding-Gruppe ersetzt, z.B. **bond0:0**.

Schnittstelle hinzufügen
Mit dieser Schaltfläche kann eine neue virtuelle Schnittstelle erstellt werden. Die neue virtuelle Schnittstelle ist standardmäßig dem physikalischen Port lan0 zugeordnet und wird am Ende der Eingabe dem gewünschten physikalischen Port zugewiesen. Die Zuordnung kann mit der Registerkarte „Sonstiges“ geändert werden.

Submenü IPv4:
In diesem Untermenü können die IPv4-Parameter konfiguriert oder die aktuelle Konfiguration des DHCP-Servers angezeigt werden.

TCP/IP Adresse: IPv4-Adresse der angegebenen Schnittstelle.

Netzmaske: Konfiguration der Subnetzmaske für die angegebene Schnittstelle.

Gateway: Konfiguration eines schnittstellenspezifischen Gateways. Diese Einstellung darf nur vorgenommen werden, wenn die IP der Schnittstelle NICHT im gleichen Subnetz wie das Standard-Gateway liegt und der netzwerkübergreifende Verkehr im Subnetz über das Gateway aktiviert werden soll.

DHCP-Client aktivieren: Mit dieser Einstellung kann ein DHCP-Client für die automatische Zuordnung der Netzwerkkonfiguration durch einen DHCP-Server aktiviert werden.

Submenü IPv6:
In diesem Menü können die IPv6-Parameter konfiguriert oder die von einem DHCP-Server vorgegebene Konfiguration angezeigt werden.

TCP/IP-Adresse: Ipv6-Adresse der angegebenen Schnittstelle

DHCP-Client aktivieren: Mit dieser Einstellung kann ein DHCPv6-Client für die automatische Zuordnung der Netzwerkkonfiguration durch einen DHCPv6-Server aktiviert werden.

Submenü Sonstiges:

Zugeordnete Schnittstelle: Legt fest, welches physikalische Netzwerk der aktuell ausgewählten virtuellen Schnittstelle zugeordnet ist.

„Virtuelles Interface“ Löschen-Button: Löscht die aktuell ausgewählte virtuelle Schnittstelle.

MAC-Adresse: Zeigt die MAC-Adresse des zugewiesenen physikalischen Netzwerkports an.

Label: Individuelle Textbeschreibung der Schnittstelle (Alias).

Submenü VLAN:
VLAN Option aktivieren: Aktivierung der getaggten VLAN-Funktion für die ausgewählte virtuelle Schnittstelle.

VLAN-Tag (0-4094): Hier können VLAN-Tags von 0-4094 eingegeben werden. Das ausgewählte Tag wird in den Datenbereich eines Ethernet-Pakets eingefügt.

Priorität: PCP (Priority Code Point). Legt die Priorität eines Ethernet-Frames fest.
Die Prioritäten können zwischen einer niedrigen Priorität, Wert 1 und einer hohen Priorität, Wert 7, eingestellt werden.

Der Prioritätswert 0 entspricht dem Best Effort.

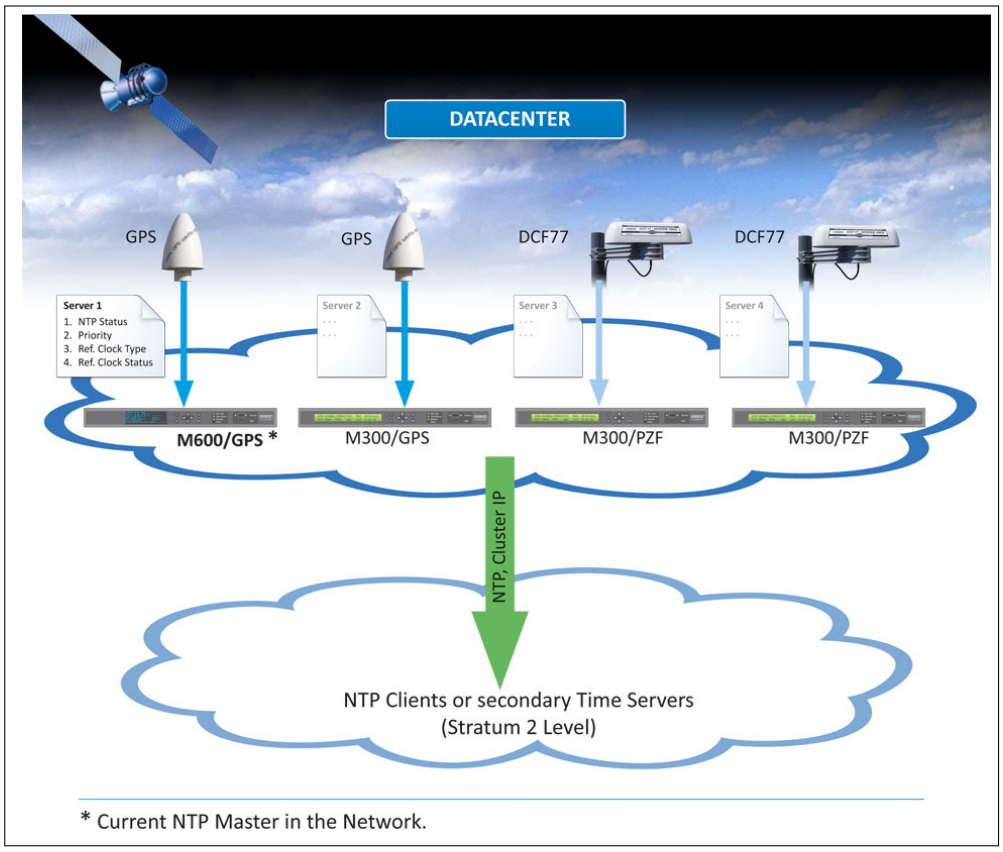
Submenü Cluster:

Der Cluster-Modus ist ein Verfahren zur redundanten Zeitsynchronisation durch Gruppieren (Clustering) mehrerer LANTIME NTP-Server. Innerhalb dieser Gruppe tauschen die teilnehmenden NTP-Server kontinuierlich Status- und Qualitätsinformationen untereinander aus. Die Statusinformationen werden miteinander verglichen und durch einen speziellen Algorithmus wird entschieden, welcher der NTP-Server als aktueller MASTER im Netzwerk fungieren soll. Der Rest der Gruppe fungiert als SLAVE und bleibt als Backup passiv. Verliert der aktuelle Master seine Synchronisationsquelle oder tritt ein anderer Fehler auf, übernimmt ein anderer NTP-Server aus dem Cluster die Masterrolle. Der aktuelle Master antwortet auf Anfragen von NTP-Clients über eine gemeinsame Cluster-IP. Auch wenn der Master durch einen anderen NTP-Server ersetzt wird, ändert sich diese IP nicht.

Die Konfiguration eines NTP-Clusters ist sinnvoll, wenn seitens der NTP-Clients nur eine IP-Adresse für einen externen NTP-Server konfiguriert werden kann und auch noch Redundanz erforderlich ist.

Der aktuelle Master wird nach den folgenden Parametern in dieser Reihenfolge ausgewählt:

1. NTP-Status (sync, not sync);
2. Priorität (vom Benutzer konfigurierbar, der niedrigste Wert hat die höchste Priorität, Standard = 0);
3. Ref-Clock-Typ - GNSS-Empfänger wie GPS haben die höchste Bewertung;
4. Ref-Clock-Status (sync, not sync).



13.1.3.6 IPv4 Cluster Konfiguration

Cluster-Option aktivieren: Über dieses Auswahlfeld kann die Clusterfunktion aktiviert werden.

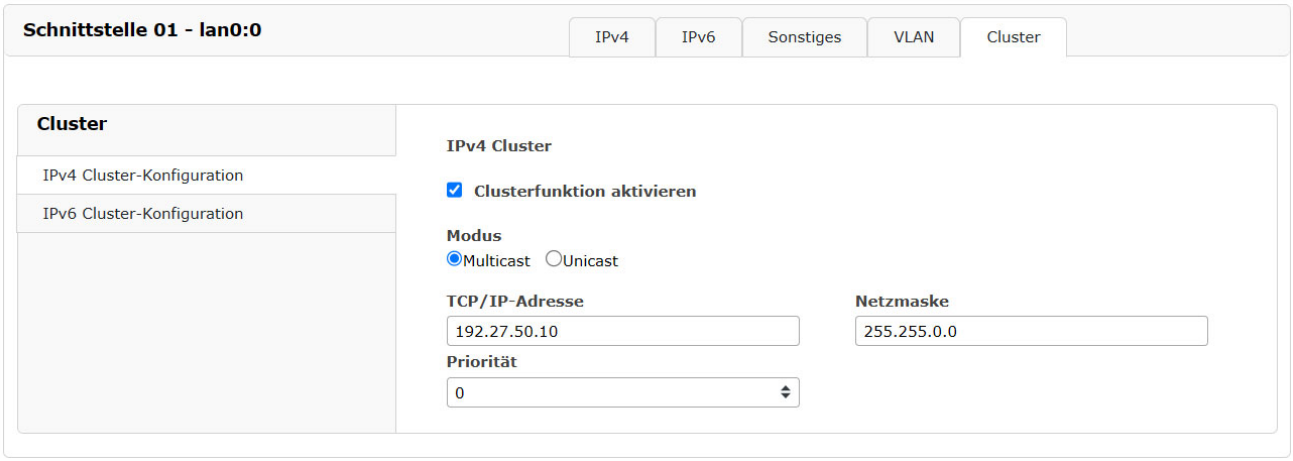
Modus: Die Clustermitglieder können ihre Statusinformationen entweder über Multicast- oder Unicast-Meldungen austauschen. Für Multicast wird standardmäßig eine Cluster-Multicast-Adresse 239.192.0.1 verwendet. Diese Einstellung kann im Menü „Netzwerk → Sonstiges“ geändert werden. Zusätzlich kann dort der Netzwerkport, der für die Clusterkommunikation verwendet wird, geändert werden. Standardmäßig wird der Port 7000 für die Clusternachrichten verwendet.

TCP/IP Adresse: IP-Adresse der NTP-Cluster-Schnittstelle. Für alle Clustermitglieder muss die gleiche Cluster-IP konfiguriert werden. Es wird empfohlen, eine Cluster-IP im gleichen Subnetz wie die entsprechende virtuelle Schnittstelle zu konfigurieren.

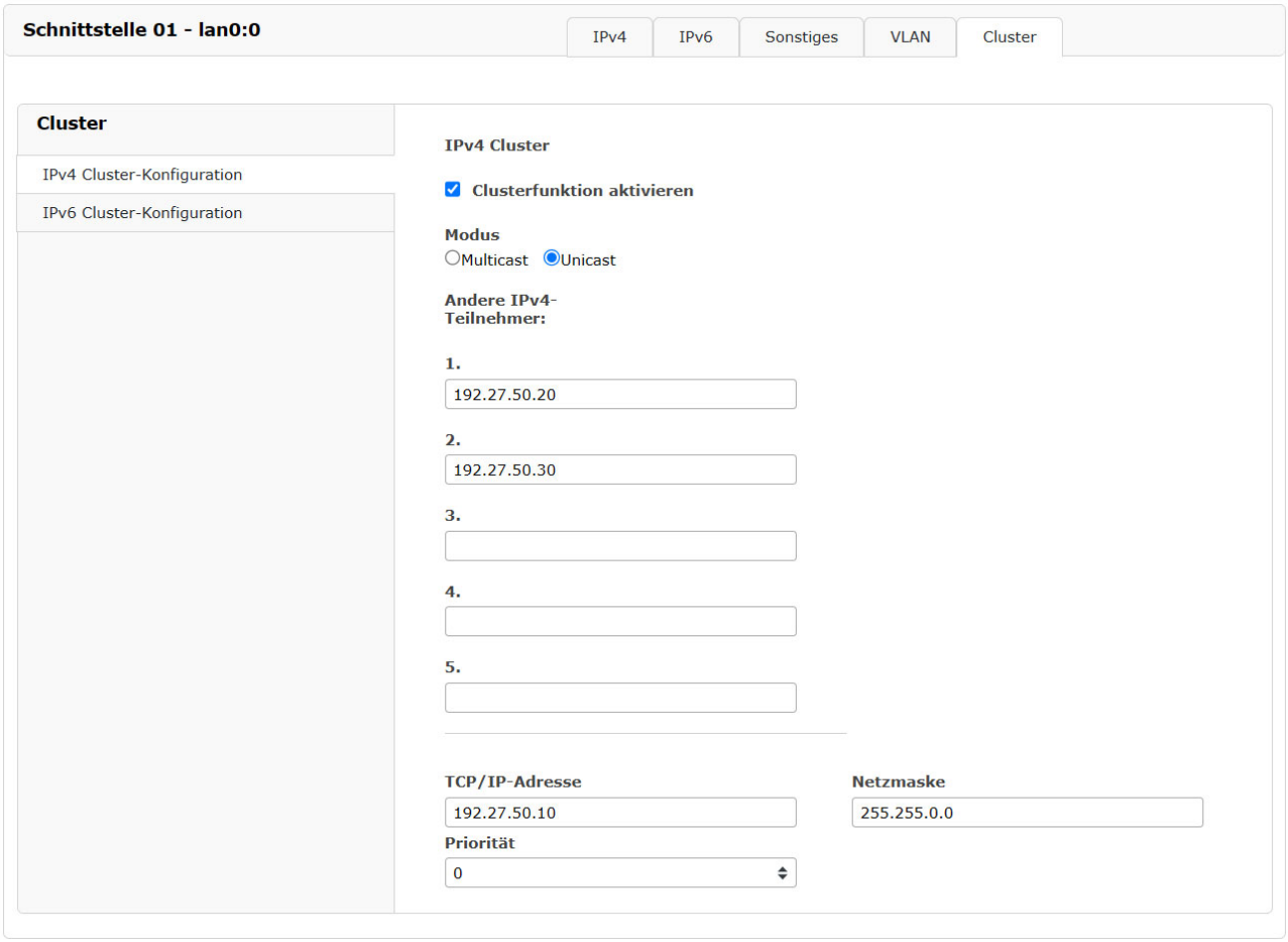
Netzmaske: Netzmaskenkonfiguration für die IPv4 Cluster-Schnittstelle.

Priorität: Die hier eingestellte Priorität wird bei der Bestimmung des MASTERs durch den Clusteralgorithmus berücksichtigt. Der niedrigste Wert hat die höchste Priorität.

Beispielkonfiguration für einen IPv4 Multicast Cluster:



Beispielkonfiguration für einen IPv4 Unicast-Cluster:



Im Unicast-Cluster müssen die IP-Adressen der Clustermitglieder in den Feldern für „Andere IPv4-Teilehmer“ eingetragen werden.

13.1.3.7 IPv6 Cluster Konfiguration

Hinweis:

Die IPv6 Cluster-Konfiguration ist erst ab der LTOS-Firmware 7.08.007 verfügbar.

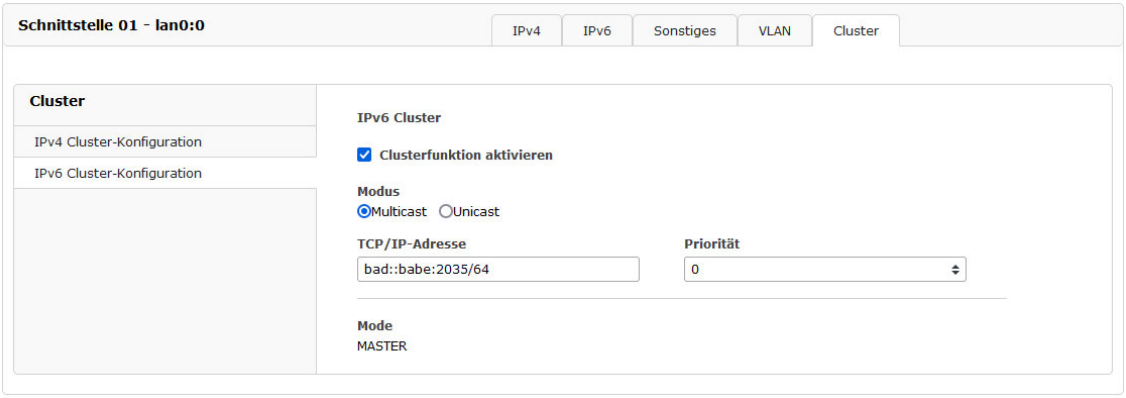
Cluster-Option aktivieren: Über dieses Auswahlfeld kann die Clusterfunktion aktiviert werden.

Modus: Die Clustermitglieder können ihre Statusinformationen entweder über Multicast- oder Unicast-Meldungen austauschen. Für Multicast wird standardmäßig eine Cluster-Multicast-Adresse FF08::c123:feed:0:1 verwendet. Diese Einstellung kann im Menü „Netzwerk → Sonstiges“ geändert werden. Zusätzlich kann dort der Netzwerkport, der für die Clusterkommunikation verwendet wird, geändert werden. Standardmäßig wird der Port 7001 für die Clusternachrichten verwendet.

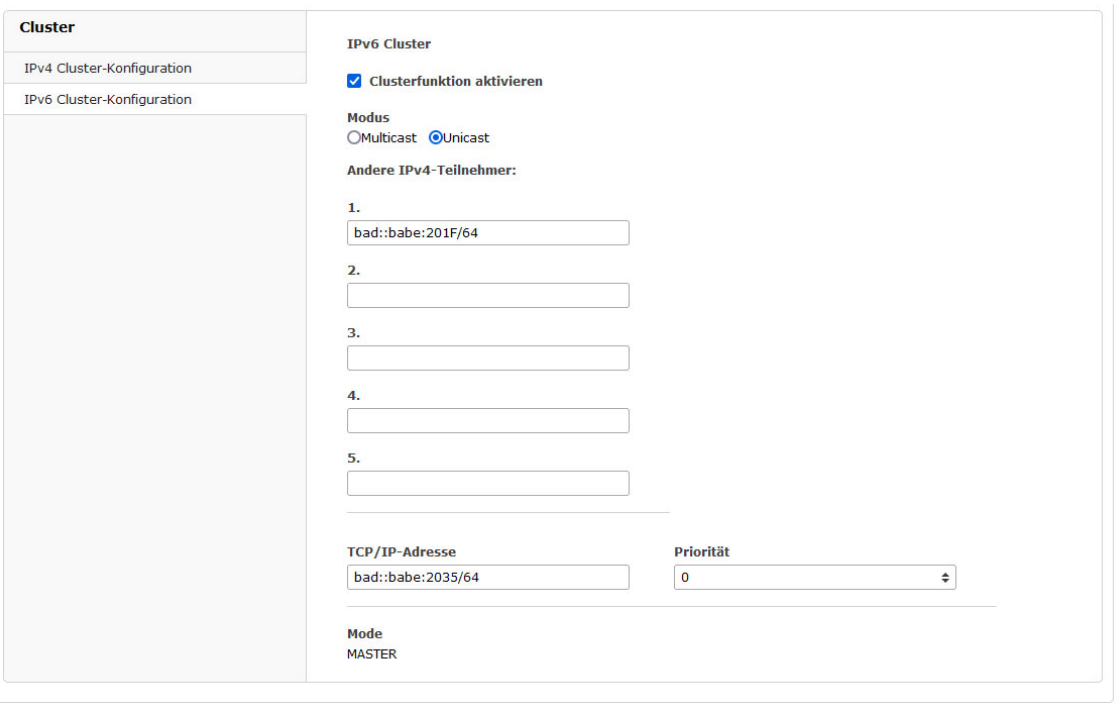
TCP/IP Adresse: IPv6-Adresse der NTP-Cluster-Schnittstelle. Für alle Clustermitglieder muss die gleiche Cluster-IP konfiguriert werden. Es wird empfohlen, eine Cluster-IP im gleichen Subnetz wie die entsprechende virtuelle Schnittstelle zu konfigurieren.

Priorität: Die hier eingestellte Priorität wird bei der Bestimmung des MASTERs durch den Clusteralgorithmus berücksichtigt. Der niedrigste Wert hat die höchste Priorität.

Beispielkonfiguration für einen IPv6 Multicast Cluster:

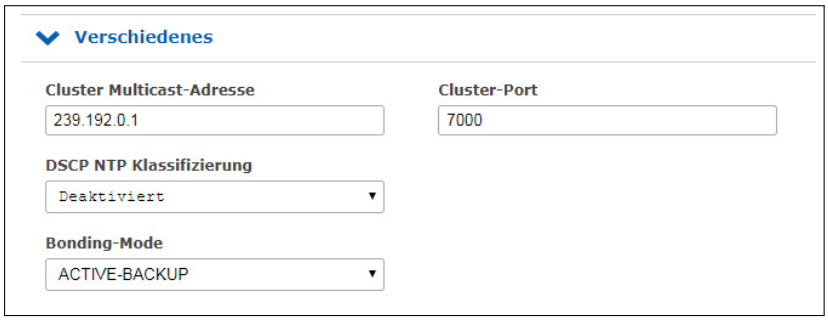


Beispielkonfiguration für einen IPv6 Unicast-Cluster:



Im Unicast-Cluster müssen die IP-Adressen der Clustermitglieder im Feld „Andere IPv6-Teilehmer“ eingetragen werden.

13.1.3.8 Verschiedenes



Cluster Multicast Adresse:
Konfiguration der Cluster-Multicast-Adresse. Über diese Adresse tauschen die LANTIME-Clustermitglieder ihre Statusmeldungen aus, wenn der Multicast-Modus aktiviert ist.

Cluster Port:
Konfiguration eines freien Netzwerkports für die Cluster-Kommunikation. Standardmäßig ist dieser Port auf 7000 eingestellt.

DSCP-NTP-Klassifikation:
DSCP = Differential Service Code Point. DSCP ist im Allgemeinen ein Verfahren zur Priorisierung des Datenverkehrs über IP. Im LANTIME ermöglicht diese Einstellung die Zuordnung der NTP-Pakete zu einer bestimmten Traffic-Klasse. Der DSCP besteht aus 6 Bits, wodurch 2*6 = 64 unterschiedliche Werte möglich sind (0 bis 63). Dies sind die Standardwerte von DSCP. Die Informationen über die Traffic-Klasse werden in einen Header eines IPv4-Pakets eingefügt. Router können diese Informationen auswerten und die NTP-Pakete wie priorisiert behandeln.

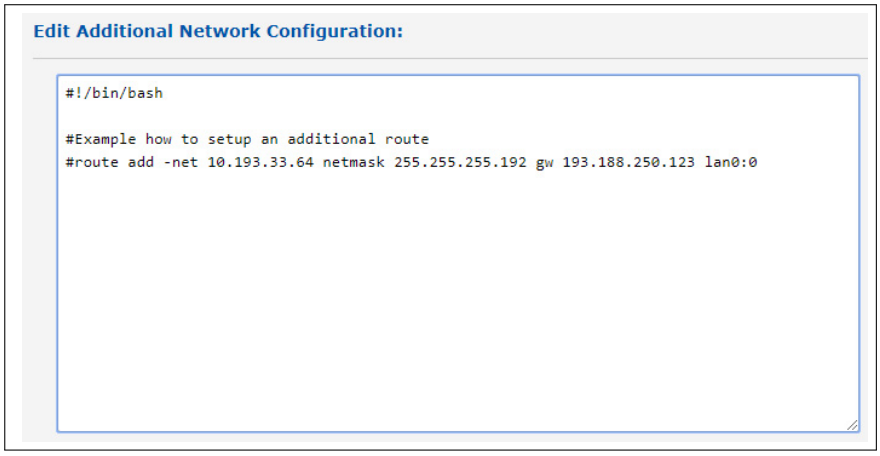
Bonding-Modus:
Im Menü „Netzwerk → Physikalische Netzwerkkonfiguration“ können zwei oder mehr physikalische Netzwerkports zu einer Bonding-Gruppe zusammengefasst werden. Der Bonding-Modus wird verwendet, um entweder den „ACTIVE BACKUP“ oder den „LACP“ Modus (Link Aggregation Control Protocol) zu konfigurieren, die vom LANTIME unterstützt werden.

ACTIVE-BACKUP:
Eine physikalische Schnittstelle in der Bonding-Gruppe wirkt wie ein „aktiver Slave“. Der gesamte Netzwerkverkehr eines LANTIME-Bond läuft über diese Schnittstelle. Die anderen physikalischen Schnittstellen in der Bonding-Gruppe sind passiv. Verliert die aktuell aktive Schnittstelle die Netzwerkverbindung, übernimmt die passive Schnittstelle nahtlos deren Funktion. Auch die MAC-Adresse des Netzwerkports bleibt unverändert.

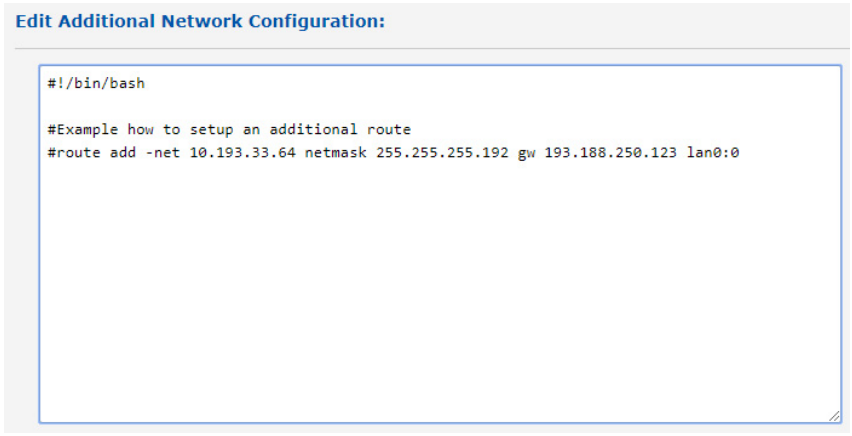
LACP:
LACP (802.3ad) ermöglicht eine Kombination mehrerer physikalischer Verbindungen zu einer logischen. Dies führt zu einer Lastverteilung und erhöht zusätzlich die Sicherheit im Fehlerfall im Vergleich zu „Active Backup“. Es ist wichtig, dass auch andere angeschlossene Netzwerkgeräte LACP unterstützen und die Netzwerkanschlüsse entsprechend konfiguriert sind.

13.1.3.9 Erweiterte Netzwerkeinstellungen

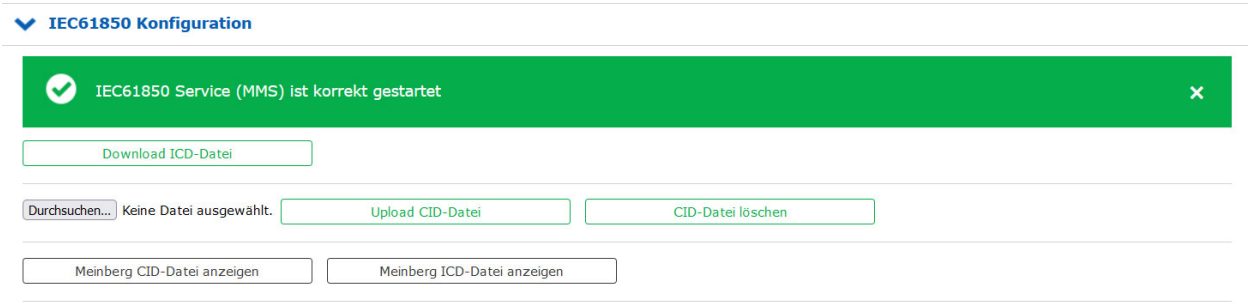
Die erweiterten Netzwerkeinstellungen sind aus Sicherheitsgründen nicht eingeschaltet. Die Funktion kann über eine SSH-Verbindung in der */etc/mbg/msc.cfg* mit dem Parameter „DISABLE SCRIPT“ nachträglich aktiviert / gesteuert werden.



In der erweiterten Netzwerkkonfiguration kann ein Bash-Skript bearbeitet werden, das bei jedem Neustart des LANTIME oder bei Änderungen der netzwerkbezogenen Konfiguration automatisch ausgeführt wird.



13.1.3.10 IEC 61850-Konfiguration

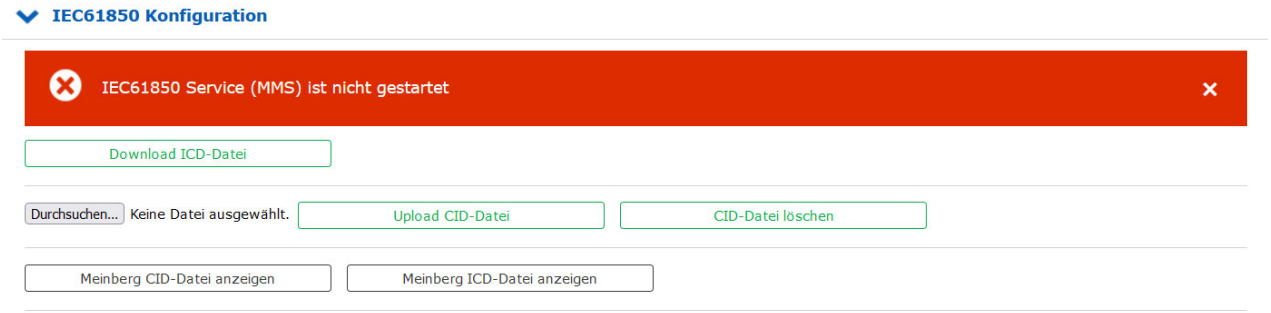


Die Norm IEC 61850 beschreibt Kommunikationsprotokolle, die von vernetzten Geräten im Bereich von Umspannwerken zum Datenaustausch verwendet werden. Diese Protokolle können sowohl in einem TCP/IP-Netzwerk (OSI-Schicht 3) als auch direkt in einem Ethernet-Netzwerk (OSI-Schicht 2, z.B. einem Substation-LAN) verwendet werden. Die Norm beschreibt ebenfalls Protokollmappings für diverse etablierte Echtzeitdatenmechanismen, insbesondere die **Manufacturing Message Specification (MMS)**, **Generic Object Oriented System Events (GOOSE)**, **Sampled Values (SV)** sowie **Sampled Measure Values (SMV)**.

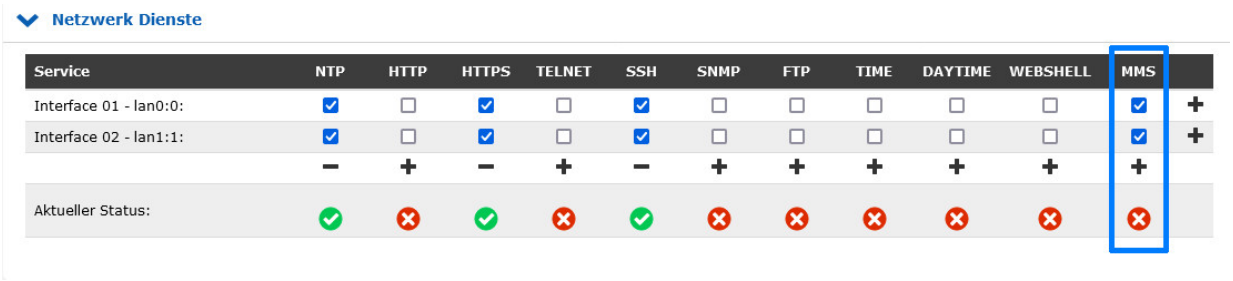
Diese Norm über die Datenkommunikation und -abstraktion legt eine gemeinsame Kommunikationssprache zwischen diversen Netzwerkgeräten untereinander fest, Komponenten wie IEDs (Intelligent Electronic Devices) und SCADA-Steuerungs- und Kontrollsysteme (Supervisory Control and Data Acquisition).

Die Fähigkeiten eines jeden IED wird anhand der XML-basierten Sprache **System Configuration Language (SCL)** in **IED Capability Description-Dateien (ICD)** beschrieben. Diese Dateien werden in ein **System Configuration Tool (SCT)** importiert, um dann Teil einer **System Configuration Description-Datei (SCD)** zu werden, mit der alle Geräte in einem vernetzten Umspannwerk beschrieben werden.

LANTIME-Server unterstützen das oben genannte MMS-Protokoll zur Kommunikation mit IEDs in elektrischen Versorgungsnetzen. Hierzu muss der MMS-Dienst des LANTIME aktiviert werden: Ist er abgeschaltet, wird folgende Warnung an prominenter Stelle gezeigt:



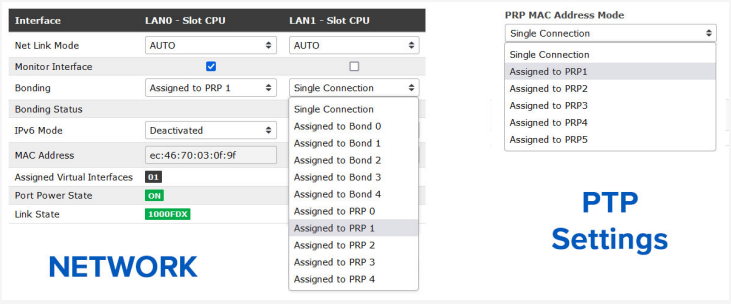
Der MMS-Dienst wird aktiviert, indem man im Menü **Netzwerk Dienste** auf der Seite **Netzwerk** das entsprechende Kontrollkästchen für die ausgewählten virtuellen Netzwerk-Schnittstellen aktiviert:



Hersteller von Geräten, die für elektrische Schaltanlagen konstruiert sind, stellen in der Regel selbst die entsprechenden ICD-Dateien bereit. Meinberg-LANTIME-Server stellen in dieser Hinsicht keine Ausnahme dar. Ein Klick auf **Download ICD-Datei** in diesem Bereich des Webinterface löst den Download der entsprechenden Datei aus. Die Inhalte der ICD-Datei lassen sich ebenfalls im Browser mit einem Klick auf **Meinberg ICD-Datei anzeigen** darstellen.

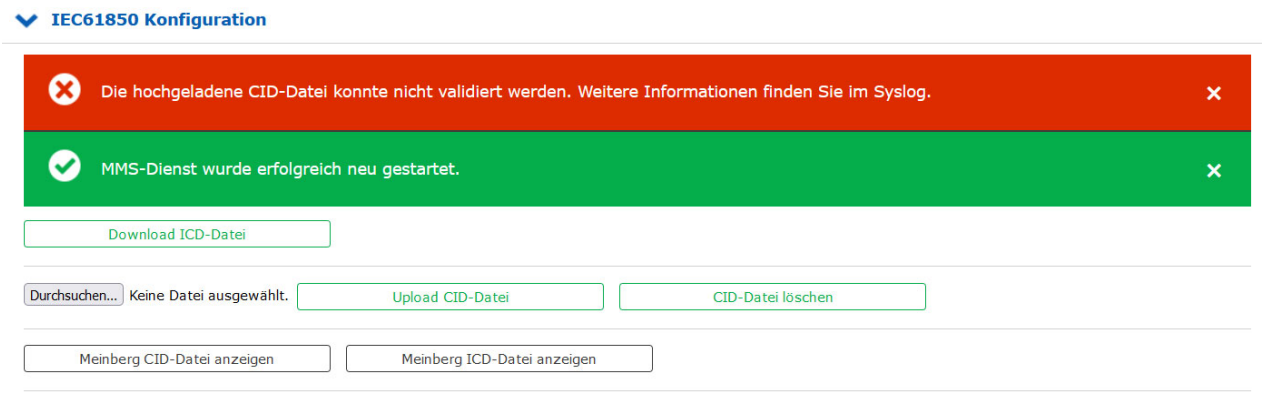
Achtung!

Vor dem Download der ICD-Datei müssen noch PRP-relevante Netzwerkeinstellungen im Menü „Netzwerk → Physikalische Netzwerkeinstellungen“ und Im Menü „PTP → PTP Konfiguration → Netzwerk“ über die Drop-Down-Box „MAC-Adresse im PRP-Mode“ vorgenommen werden.



Ist die ICD-Datei einmal in Ihr SCT eingespielt worden, sollte es in der Lage sein, eine **Configured IED Description-Datei (CID)** zu exportieren, mit der dann das „IED“ (also der LANTIME in diesem Fall) in die Lage versetzt wird, sich selbst für das Umspannwerk zu konfigurieren. Diese CID-Datei kann auf Ihren LANTIME hochgeladen werden, indem Sie die Schaltfläche ***Durchsuchen...*** betätigen, die passende CID-Datei aus dem entsprechenden Ordner im Datei-Explorer auswählen und dann die Schaltfläche **Upload CID-Datei** betätigen. Bei Erfolg erscheint eine Aufforderung, die neue Start-Konfiguration zu speichern.

Bleibt der Upload erfolglos (z.B. wegen Formatierungsfehlern in der CID-Datei) wird folgender Fehler angezeigt:

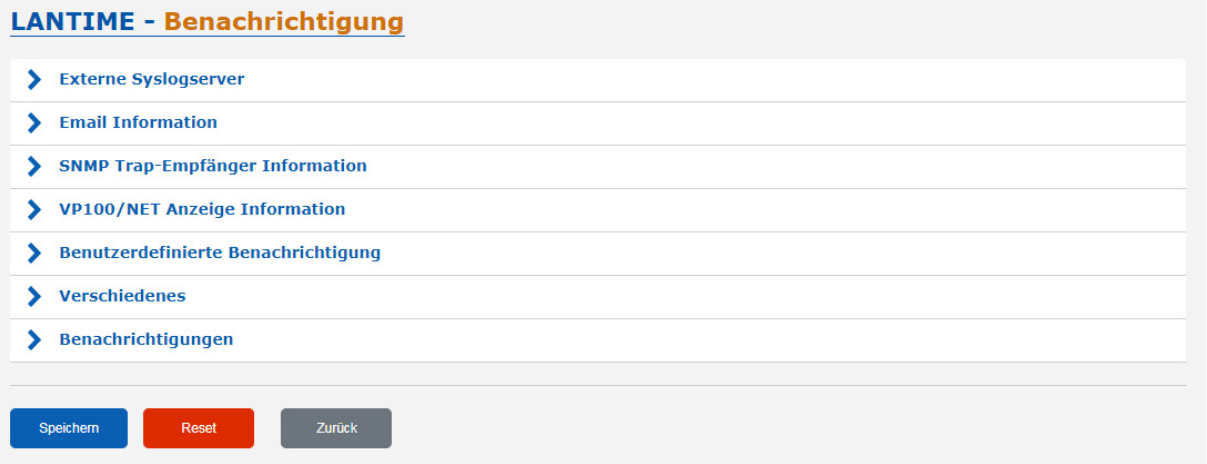


Hinweis:

Dieser Fehler wird auch dann angezeigt, wenn Sie **Upload CID-Datei** anklicken, ohne dass eine Datei ausgewählt wurde. Durch das Anklicken der Schaltfläche **Upload CID-Datei** wird kein Datei-Explorer geöffnet. Dieser wird nur mit einem Klick auf die Schaltfläche ***Durchsuchen...*** geöffnet.

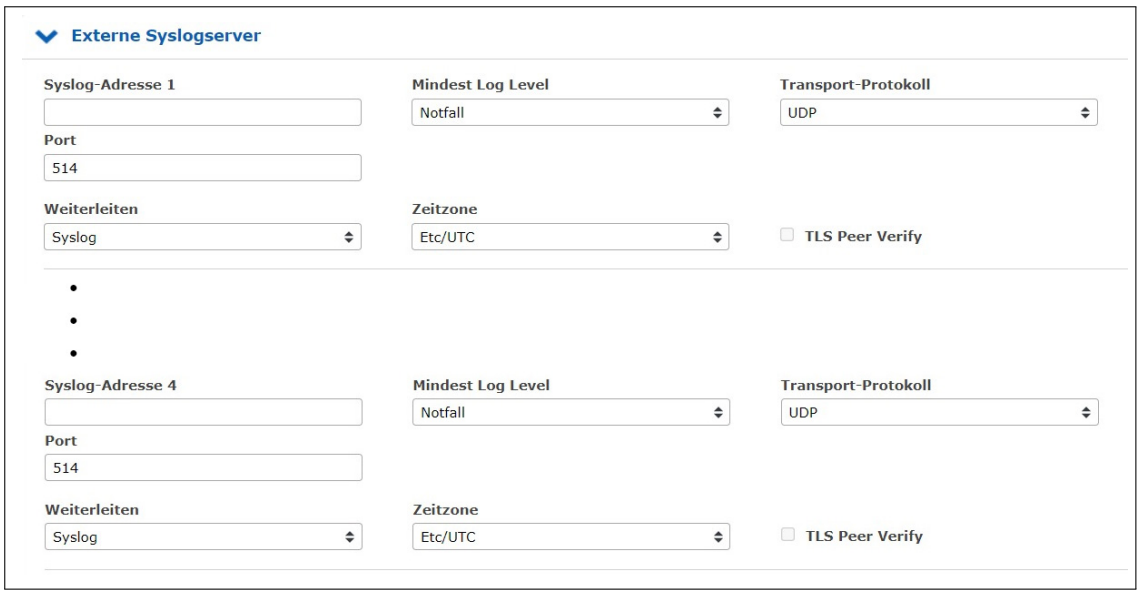
Detaillierte Informationen zum IEC 61850 Standard finden Sie im Anhang im Kapitel IEC 61850 Grundlagen

13.1.4 Benachrichtigung

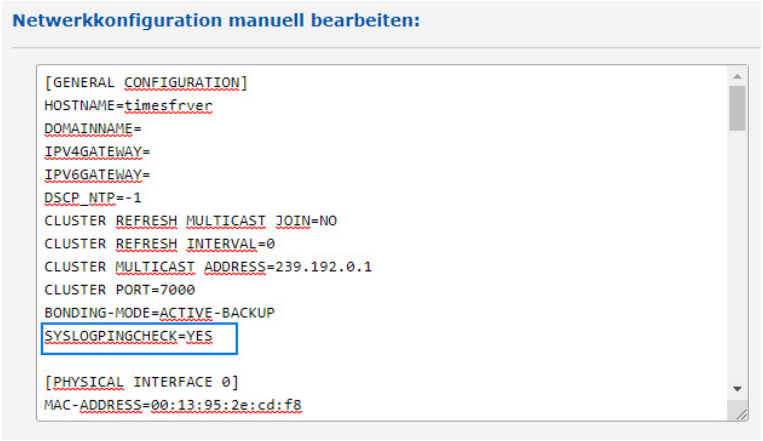


13.1.4.1 Externe Syslog-Server

Alle Informationen, die im LANTIME in SYSLOG (/var/log/auth.log usw.) geschrieben werden, können auch an einen Remote-Server weitergeleitet werden.



Syslog-Adresse(n):
Sie können bis zu 4 externe Syslog-Server über das Webinterface eingeben. Standardmäßig wird die Erreichbarkeit des Syslog Servers über Ping/ICMP überprüft. Wenn der registrierte Syslog-Server nicht erreichbar ist, wird er nicht in die Syslog-Konfigurationsdatei */etc/syslog-ng/syslog-ng/syslog-ng.conf* eingetragen. Falls ICMP aufgrund von Firewall-Einschränkungen im Netzwerk nicht erlaubt ist, können Sie den Pingcheck über die manuelle Netzwerkkonfiguration ausschalten. Um fortzufahren, navigieren Sie wie unten beschrieben:



„System → Dienste und Funktionen → Manuelle Konfiguration → Netzwerk-Konfiguration“: Geben Sie für den Parameter „SYSLOGPINGCHECK“ den Wert „NO“ ein und speichern Sie die neuen Einstellungen.

Minimaler Log-Level: Log-Level-Konfiguration
Notfall, Alarm, Kritisch, Fehler, Warnung, Ankündigung, Info, Debug

Transportprotokoll: Transportprotokoll-Konfiguration:

UDP	verbindungslose Übertragung
TCP	verbindungsorientiert
TLS	kann zum sicheren Transport der Logging-Informationen an einen externen Syslog-Server gewählt werden.

Port: Konfiguration des zu verwendenden Netzwerkanschlusses. Standardmäßig hat IANA den Port 514 für Syslog-Meldungen registriert.

Weiterleiten: Syslog
Alles, was intern in der Datei */var/log/messages* protokolliert wird, wird auch an den konfigurierten Syslog-Server gesendet (natürlich unter Berücksichtigung des konfigurierten Log-Levels).

Format:
```
Mar 22 15:35:56 su-rims1-1 PAM-tacplus[3431]:
user not authenticated by TACACS+
```

Notification/Test
Nur die Ereignisse, die in der Ereignisliste unter "Benachrichtigungen → Benachrichtigungenäufgeführt sind, werden an den Syslog-Server gesendet.

Format:
```
DAEMON.INFO: Mar 22 14:39:55 su-rims1-1 ext_syslog_cfg_text:
Device Configuration Changed
```

Notification/Splunk
Wie bei „Notification/Text“, nur in einem anderen Format:

Format:
```
Mar 22 14:41:46 su-rims1-1 ext_syslog_cfg_splunk:
msg_nr=20, msg_name=Device Configuration Changed,
msg_txt=, add_txt=
```

Notification/JSON
Wie bei „Notification/Text“, nur in einem anderen Format:

Format:

```
Mar 22 14:43:57 su-rims1-1 ext_syslog_cfg_json:
{
 “msg_nr“: “20“,
 “msg_name“: “Device Configuration Changed“,
 “msg_txt“: “...“,
 “add_txt“: “...“
}
```

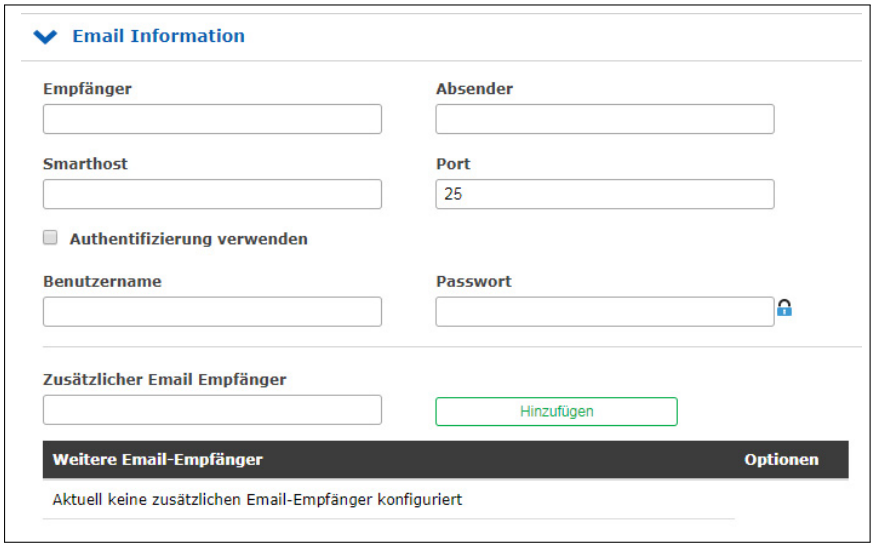
Zeitzone: Gibt die Zeitzone der weitergeleiteten Log-Ereignisse vor.

TLS Peer Verify: Die Option TLS Peer Verify gibt an, ob das Zertifikat des Logging-Servers überprüft werden soll. Eine authentische Verbindung ist nur mit dieser Einstellung möglich. Wenn diese Option aktiv ist, ist darauf zu achten, dass ein Root CA Zertifikat für den Syslog-Server unter icherheit → Zertifikate → CA Zertifikate"hochgeladen wurde.

Informationen zum Hochladen von CA Zertifikaten sind in Kapitel CA Zertifikate enthalten.

13.1.4.2 E-Mail-Information

Der LANTIME ist in der Lage, über bestimmte Systemereignisse per E-Mail zu informieren. Im Menü „E-Mail-Informationen“ können Sie die notwendigen Einstellungen vornehmen. Im Untermenü „Benachrichtigungen“ können Sie die Systemereignisse auswählen, für die der LANTIME eine Benachrichtigungs-E-Mail versenden soll.



Empfänger: E-Mail des gewünschten Empfängers.

Absender: Adresse des Absenders.

Smarthost: Für den Versand der E-Mails benötigen Sie einen Smarthost (Relay-Server). Bitte geben Sie hier die Serveradresse ein.

Port: Konfiguration des Netzwerkports. Die Standardeinstellung ist 25, da das SMTP (Simple Mail Transfer Protocol) standardmäßig den TCP-Port 25 verwendet.

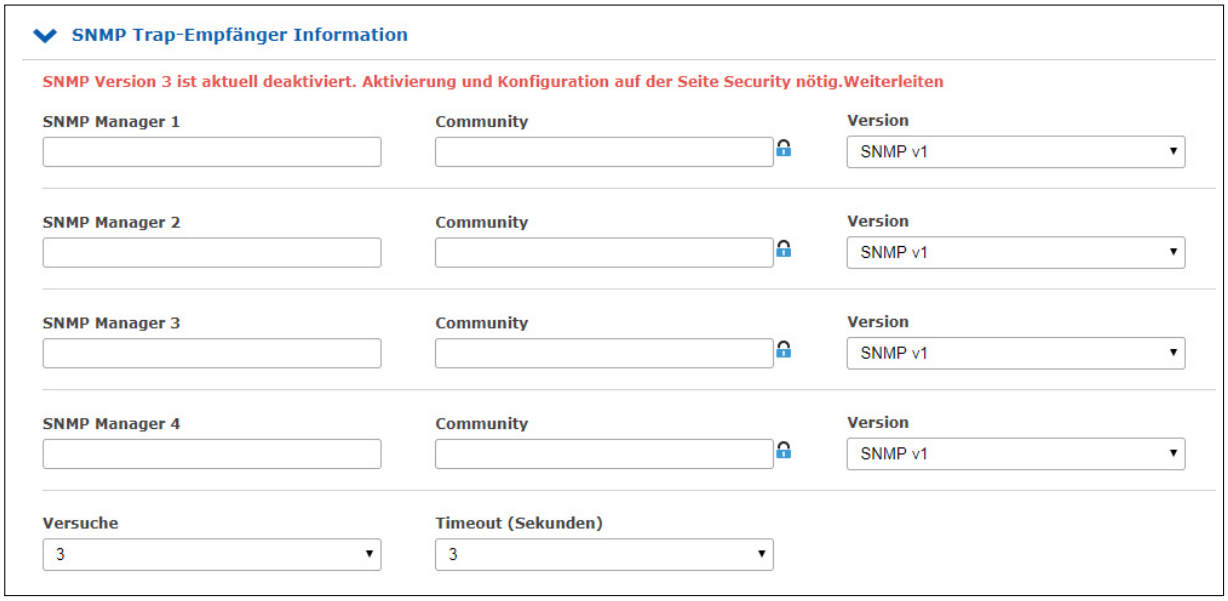
Authentifizierung verwenden (Checkbox): Viele Mailserver benötigen eine gültige Authentifizierung. Bitte markieren Sie das Kontrollkästchen, um sie zu aktivieren.

Benutzername/ Passwort: Bitte geben Sie einen gültigen Zugang für den E-Mail-Server ein.

Zusätzlicher Email Empfänger: Konfiguration zusätzlicher E-Mail-Empfänger.

13.1.4.3 SNMP-Trap-Empfänger

Der LANTIME ist in der Lage, mit Hilfe von SNMP-Traps über bestimmte Systemereignisse zu informieren. Im Menü „SNMP Trap Receiver“ können Sie bis zu 4 Trap-Empfänger konfigurieren. Im Untermenü „Benachrichtigungen“ können Sie die Systemereignisse auswählen, für die der LANTIME einen SNMP-Trap senden soll.



SNMP-Trap-Empfänger: IP-Adresse oder Hostname des SNMP-Trap-Empfängers.

Community: SNMP-Read-Community des Trap-Empfängers.

Version: SNMP-Version, die verwendet werden soll.

Anzahl der Wiederholungen: Gibt die Anzahl der Wiederholungen an, die ein LANTIME versucht einen Trap zu senden.

Timeout: Timeout-Wert für die Verbindungsdauer.

13.1.4.4 VP100/NET Display-Informationen

Das Meinberg VP100/20NET Netzwerkdisplay dient zur Anzeige von Uhrzeit und Datum. Dieses Display verfügt über eine integrierte Netzwerkkarte und einen SNTP-Client. Die Zeit wird von jedem NTP-Zeitserver über das NTP-Protokoll empfangen und damit die interne Uhr eingestellt. Diese Anzeige kann auch beliebige Zeichen als Lauftext anzeigen. Alle LANTIME-Alarmmeldungen können als Textnachrichten auf dem Display angezeigt werden. Im Untermenü „Benachrichtigungen“ können Sie die Systemereignisse auswählen, die vom LANTIME an die Anzeige gesendet werden sollen. Eine Meldung erscheint dreimal hintereinander als Lauftext auf dem Display.

Display: IP-Adresse der Netzwerkanzeige.

Serial number: Hier müssen Sie die korrekte Seriennummer des Displays eingeben.
Die Seriennummer wird angezeigt, wenn Sie die rote SET-Taste viermal drücken.

13.1.4.5 Benutzerdefinierte Benachrichtigungen

Achtung!

Die Bearbeitung der benutzerdefinierten Benachrichtigungen erfordert fortgeschrittene Kenntnisse der Systemadministration und ist daher standardmäßig deaktiviert.

Um diese Option freizuschalten, muss im Konfigurations-Editor unter dem Menü „System → Dienste und Funktionen → Manuelle Konfiguration → Standard Konfiguration → Sonstige Konfiguration“ der Eintrag **DISABLE SCRIPT** auf *NO* gesetzt werden.

Diese Option kann auch über eine SSH-Verbindung bzw. über eine serielle Terminal-Verbindung auf gleiche Weise mit der Bearbeitung von */etc/mbg/msc.cfg* aktiviert oder deaktiviert werden.

Der Aufruf des Editors für die benutzerdefinierten Benachrichtigungen erfordert immer Super-User-Berechtigungen, unabhängig von der Einstellung des **DISABLE SCRIPT**-Eintrags.

Über den Menüpunkt „Benutzerdefinierte Benachrichtigungen“ kann ein frei definierbares Skript erstellt werden, das bei bestimmten Systemereignissen ausgeführt werden soll. Dieses Skript kann über den Button „Benachrichtigung bearbeiten“ eingesehen und bearbeitet werden. Bei der Auslieferung enthält dieses Skript einige Kommentare.

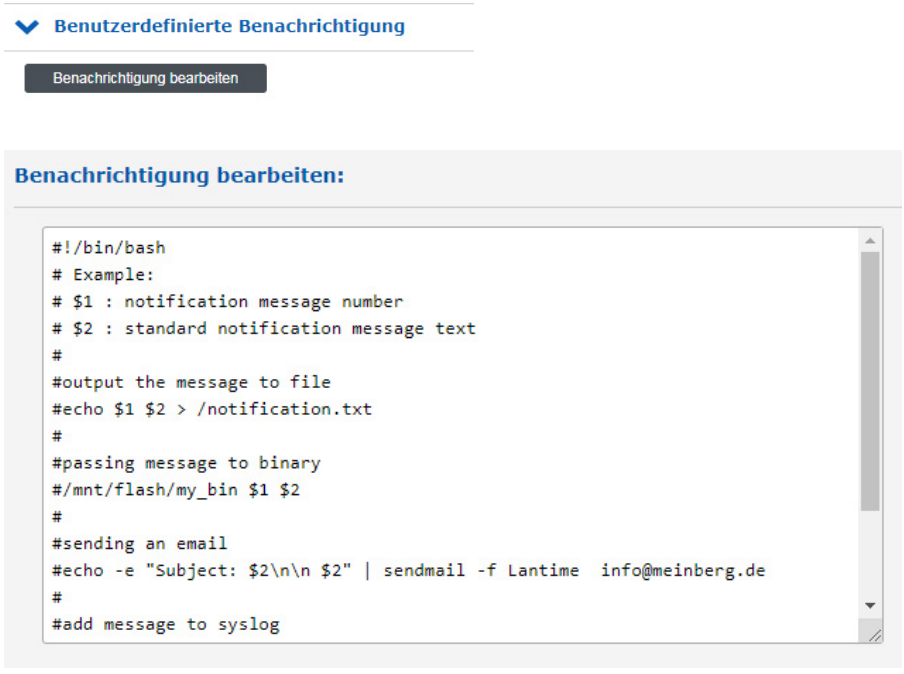
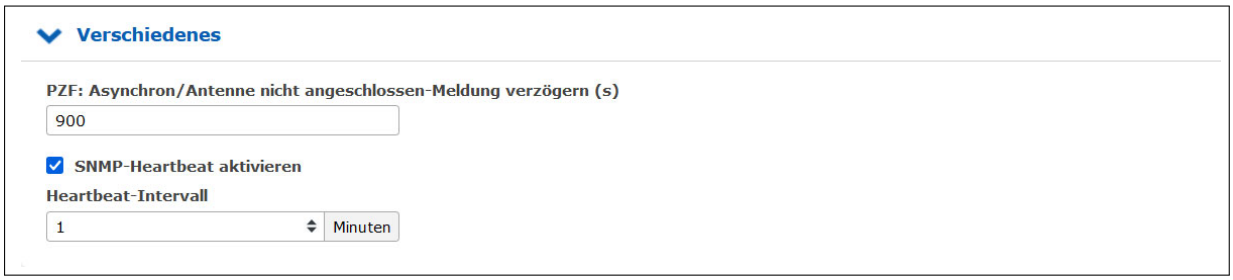


Abbildung: Im Submenü „Benachrichtigungen bearbeiten“ können Sie die Systemereignisse auswählen, bei denen das Skript ausgeführt werden soll.

13.1.4.6 Benachrichtigung - Verschiedenes



SNMP-Heartbeat aktivieren
Der Netzwerk-Heartbeat beschreibt eine Funktion, mit der der LANTIME zyklisch einen SNMP-Trap an die konfigurierten SNMP-Trap-Empfänger sendet, um sich als „alive" und „active" zu melden.

Objekt-ID
Die SNMP-OID des Traps lautet: 1.3.6.6.1.4.1.5597.30.3.0.88 (mbgLtNgTrapHeartbeat).

Heartbeat aktiv: Über dieses Kontrollkästchen kann der Heartbeat aktiviert werden.

Heartbeat-Intervall (m): Heartbeat-Intervall in Minuten.

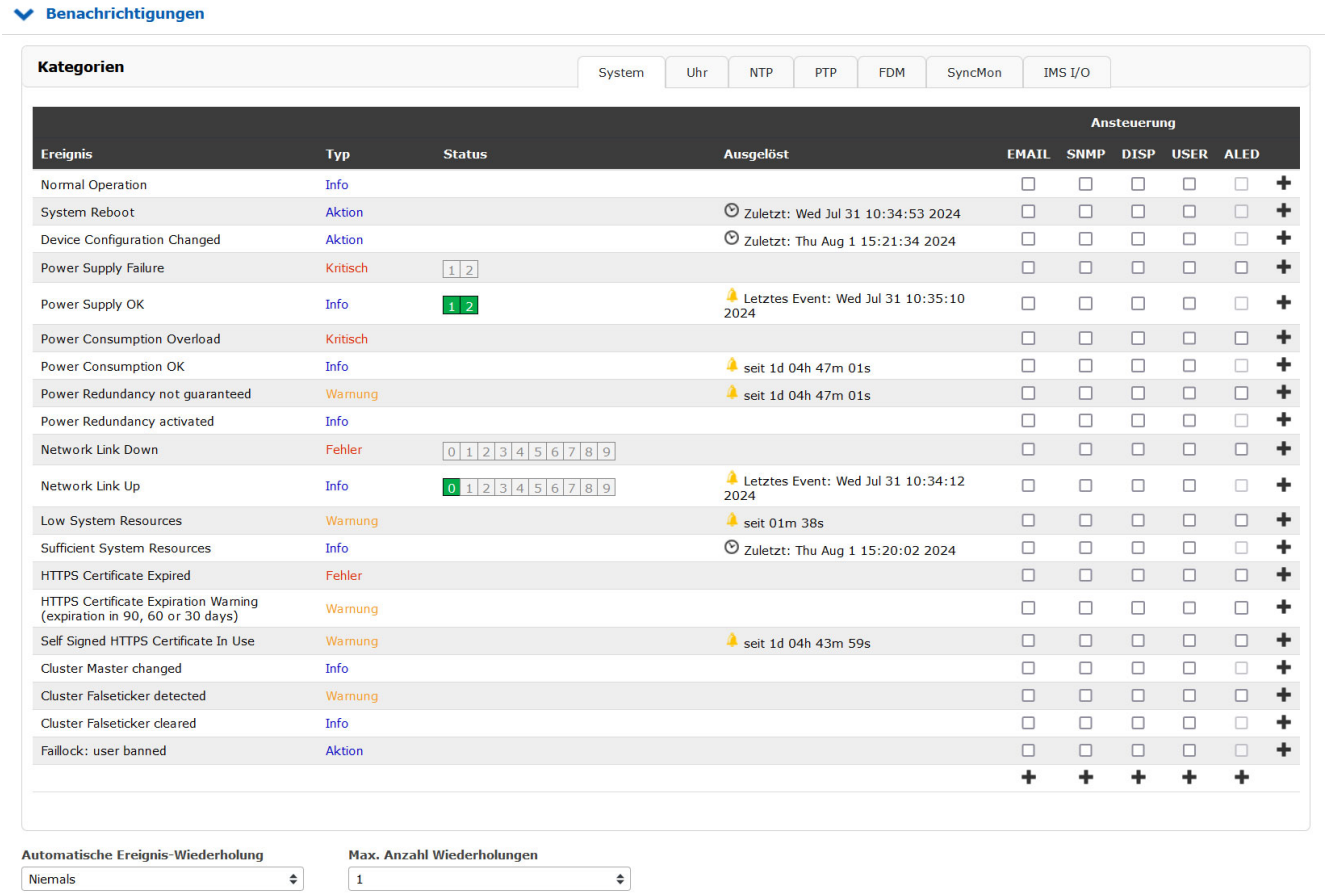
Nur beim Einsatz einer PZF-Uhr

PZF: Asynchron/Antenne nicht angeschlossen-Meldung verzögern (s)
Damit unnötige Benachrichtigungen vermieden werden, kann in diesem Feld ein Zeitintervall in Sekunden eingetragen werden. Wenn hier, wie in der Abbildung gezeigt, 900 (Sekunden) eingetragen wird, dann wartet das System nach Auftreten einer Empfangsstörung 900 Sekunden bzw. 15 Minuten, bevor eine Benachrichtigung versendet wird.

Der DCF77-Transmitter sendet pro Minute 59 Bits mit Zeit- und Datumsinformationen. Die PZF-Uhr macht einmal pro Minute eine Plausibilitätsprüfung. Sollte die Übertragung von nur einem Bit fehlschlagen, dann geht die Uhr in den „Async-Zustand". Sollte innerhalb des eingestellten Zeitintervalls (im Beispiel 900 Sekunden) der Sync-Zustand wiederhergestellt werden, dann wird keine Benachrichtigung versendet.

13.1.4.7 Benachrichtigungen-Ereignisse

Das Submenü „Benachrichtigungen“ gibt einen Überblick über alle Systemereignisse, die während des LANTIME-Betriebs auftreten können. Die Kontrollkästchen können verwendet werden, um externe Alarme für jedes Ereignis zu konfigurieren. Die folgenden Informationskanäle stehen zur Verfügung:



EMAIL: Sendet eine E-Mail basierend auf der E-Mail-Konfiguration (siehe Kapitel „E-Mail-Informationen“).

SNMP: Sendet einen SNMP Trap an den konfigurierten SNMP Trap (siehe Kapitel „SNMP Trap Receiver“).

DISP: Zeigt die Benachrichtigungen auf den konfigurierten Netzwerkdisplays an (siehe Kapitel „VP100/NET Display-Informationen“).

USER: Aktiviert das benutzerdefinierte Skript (siehe Kapitel „Benachrichtigungen“).

ALED: Wenn das Ereignis eintritt, leuchtet die Alarm-LED des LANTIME auf.

RELAY: Wenn das Ereignis eintritt, wird das Fehlerrelais am LANTIME auf ERROR gesetzt (siehe Kapitel „Error-Relais“).

1) Information; 2) Alarm; 3) Letzte Änderung

Kategorien

Zur besseren Übersicht werden die Ereignisse, die Benachrichtigungen auslösen können, in Kategorien einsortiert. Zur Auswahl der Kategorie stehen in diesem Menü folgende Reiter zur Verfügung:

System Systembenachrichtigungen wie z.B. „System Reboot“ bei Systemneustart.

Uhr Benachrichtigungen über den Status der eingesetzten Uhr, z.B. „Clock not Sync“ wenn die Referenzuhr nicht synchronisiert.

NTP NTP-Status-Benachrichtigungen, z.B. „NTP Stopped“, wenn der NTP-Dienst gestoppt wird.

PTP Statusbenachrichtigungen über das PTP-Modul, z.B. „PTP Link Down“ falss keine Netzwerkverbindung besteht.

FDM Benachrichtigungen über das eingesetzte FDM-Modul, z.B. „FDM Error“ wenn eingestellte Toleranzwerte von Zeit oder Frequenz nicht eingehalten werden.

SyncMon Benachrichtigungen vom Sync Monitor, z.B. „Sync Monitor Alert“ wenn ein Netzwerkknoten nicht erreichbar ist.

IMS/IO Statusmeldungen über die eingesetzten IMS I/O-Module, z.B. „IMS Error“ wenn ein Fehler in einem IMS-Modul festgestellt wird.

Eine vollständige Auflistung aller Benachrichtigungen und der jeweiligen Schweregrade ist im Kapitel Alle Events in der Übersicht zu finden.

IMS-Fehler zurücksetzen

Das Entfernen eines IMS Moduls löst einen permanenten Fehler im System aus. Sollten Module bewusst oder geplant entfernt werden, steht im Sub-Menü „Benachrichtigungen“ der Button **„IMS-Fehler zurücksetzen“** am unteren Ende der Event-Tabelle zur Verfügung. Mit dieser Schaltfläche können alle registrierten und angezeigten IMS-Fehler zurückgesetzt werden.

Automatische Ereigniswiederholung: Es kann ein Intervall konfiguriert werden, mit dem Benachrichtigungen erneut gesendet werden.

Max. Anzahl der Wiederholungen: Die Anzahl der Wiederholungen kann durch diesen Parameter begrenzt werden.

Beispiel:
Wird die „Automatische Ereigniswiederholung“ auf „Jede Stunde“ und die „Max. Anzahl der Wiederholungen“ auf den Wert 3 eingestellt, dann sendet das System insgesamt vier Benachrichtigungen. Die erste, wenn das Ereignis eintritt. Danach die nächsten drei Stunden eine Benachrichtigung pro Stunde.

13.1.4.8 Alle Events in der Übersicht

Ereignis	Schweregrade (nach X.733)	Beschreibung
System-Events		
Normal Operation	Info	Zeigt den normalen Betrieb des LANTIME an
System Reboot	Aktion	Das System ist neu gestartet
Device Configuration Changed	Aktion	Die Softwarekonfiguration des LANTIME wurde geändert
Power Supply Failure	Kritisch	Fehler an einem Netzteil erkannt -> Elektrische Sicherheit
Power Supply OK	Info	Betriebsbereites Netzteil
Power Consumption Overload	Kritisch	Überlastung des Netzteils/der Netzteile. Es sind nicht genügend Netzteile im Einsatz -> Redundante Stromversorgung
Power Consumption OK	Info	Die eingesetzten Netzteile liefern ausreichend Leistung für das System
Power Redundancy not guaranteed	Warnung	Bei Ausfall eines Netzteiles ist der weitere Betrieb nicht gewährleistet -> Redundante Stromversorgung
Power Redundancy activated	Info	Der Normalbetrieb ist auch nach dem Ausfall eines Netzteils gesichert
Network Link Down	Fehler	Keine Netzwerkverbindung an einem der LAN-Ports -> Netzwerk-Meldungen
Network Link Up	Info	Netzwerkverbindung am LAN-Anschluss erkannt
Low System Resources	Warnung	Geringe Systemressourcen erkannt
Sufficient System Resources	Info	Wiederhergestellte Systemressourcen
Fan Failure	Kritisch	Ein Fehler wurde bei einem Lüfter festgestellt -> Sonstige Meldungen
Fan OK	Info	Keine Fehler bei installierten Lüftern
Certificate Expired	Fehler	HTTPS-Zertifikat ist abgelaufen -> Zertifikate

Tabelle: Alle Benachrichtigungs-Events

Ereignis	Schweregrade (nach X.733)	Beschreibung
HTTPS Certificate Expiration Warning (expiration in 90, 60 or 30 days)	Warnung	HTTPS-Zertifikat endet in 90, 60 oder 30 Tagen ab -> Zertifikate
Self-Signed Certificate In Use	Warnung	Das eingesetzte Zertifikat ist selbst signiert und kommt nicht von einer offiziellen Zertifizierungsstelle -> Zertifikate
Cluster Master Changed	Info	Der Master eines LANTIME NTP-Clusters hat sich geändert -> Netzwerk
Cluster Falseticker detected	Warnung	Ein NTP-Falseticker wurde in der Clusterverbindung erkannt
Cluster Falseticker cleared	Info	Zuvor erkannter Cluster-Falseticker ist wieder in Ordnung
Faillock: user banned	Aktion	Fehlgeschlagener Login - User wird temporär gesperrt
NTP-Events		
NTP Not Sync	Fehler	NTP-Dienst ist nicht synchron -> NTP-Nachrichten
NTP Sync	Info	Der NTP-Dienst wurde erfolgreich synchronisiert
NTP Stopped	Kritisch	NTP-Dienst gestoppt -> NTP-Nachrichten
NTP Offset Limit exceeded	Fehler	Maximaler NTP-Offsetwert wurde überschritten -> SyncMon
NTP Offset Limit OK	Info	Maximaler NTP-Offset nicht überschritten -> SyncMon
Empfänger-Events		
CLK[NR] Not Responding	Kritisch	Empfängermodul reagiert nicht -> Referenzuhr-Nachrichten
CLK[NR] Not Sync	Fehler	Empfängermodul ist nicht synchron -> Referenzuhr-Nachrichten
CLK[NR] Sync	Info	Das Empfängermodul ist synchron zu seiner Zeitquelle
Antenna Faulty	Fehler	Keine Antenne oder kein ausreichendes Signal erkannt -> Referenzuhr-Nachrichten
Antenna Reconnect	Info	Antenne / Signal wurde vom LANTIME erkannt

Tabelle: Alle Benachrichtigungs-Events

Ereignis	Schweregrade (nach X.733)	Beschreibung
Antenna Short Circuit	Fehler	Kurzschluss am Antennenanschluss -> Referenzuhr-Nachrichten
Leap Second Announced	Info	Eine Schaltsekunde wurde angekündigt
SHS Time Limit OK	Info	Der eingestellte SHS-Zeitgrenzwert wurde nicht überschritten
SHS Time Limit Warnung	Warnung	Der eingestellte Schwellenwert für eine SHS Warnung wurde überschritten
SHS Time Limit Error	Kritisch	Der eingestellte Schwellenwert für einen SHS-Fehler wurde überschritten -> SHS-Konfiguration
MRS Source: Limit Exceed	Fehler	Eingestellte MRS-Grenzwerte wurden überschritten -> Referenzuhr-Nachrichten
MRS Source: No Signal	Warnung	Eine konfigurierte MRS-Zeitquelle ist nicht mehr verfügbar -> Referenzuhr-Nachrichten
MRS Source: Signal Detected	Info	Eine konfigurierte MRS-Zeitquelle ist verfügbar
MRS Source: Selected Signal Changed	Aktion	Die aktive MRS-Quelle hat sich geändert
MRS Source: Invalid Signal	Warnung	Eine konfigurierte MRS-Quelle liefert ein ungültiges Signal
MRS Source: Signal OK	Info	Die konfigurierte MRS-Quelle liefert ein korrektes Signal
Oscillator Adjusted	Info	Der interne Oszillator arbeitet stabil und ist justiert
Oscillator Not Adjusted	Warnung	Interner Oszillator ist nicht justiert -> Referenzuhr-Nachrichten
Trusted Source OK	Info	Die als vertrauenswürdig ausgewählte Quelle befindet sich im eingestellten Offset-Bereich -> Erweiterte Optionen
Trusted Source Error	Fehler	Offset-Grenzwertverletzung der verwendeten vertrauenswürdigen Quelle -> Erweiterte Optionen
Sync-Monitor-Events		

Tabelle: Alle Benachrichtigungs-Events

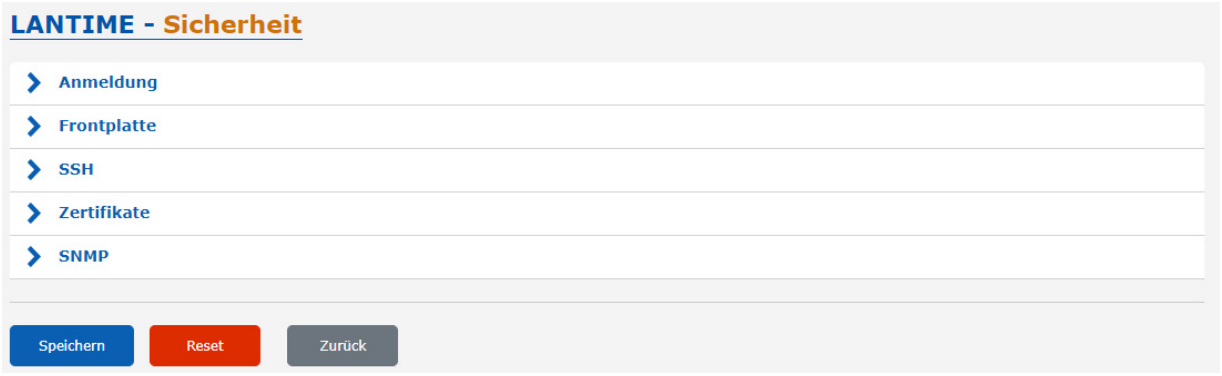
Ereignis	Schweregrade (nach X.733)	Beschreibung
Sync Monitor	Aktion	Die Limits des Sync-Monitors wurden überschritten
Sync Monitor Alert	Fehler	Fehlfunktion des SyncMon - überwachter Netzwerkknoten ist nicht erreichbar -> Error Logs
Sync Monitor OK	Info	Keine Störungen erkannt im Sync Monitor
FDM-Events (nur bei eingesetztem FDM-Modul)		
FDM Error	Fehler	Die Abweichung der Zeit oder Frequenz der überwachten Netzleitung ist auÃŸerhalb der eingestellten Toleranz
FDM OK	Info	Die überwachte Netzfrequenz- und Zeitabweichung befindet sich im eingestellten Toleranzbereich
PTP-Events (nur bei eingesetztem PTP-Modul)		
PTP Link Down	Fehler	Keine Netzwerkverbindung am PTP-Netzwerkanschluss
PTP Link Up	Info	Netzwerkverbindung am PTP-Netzwerkanschluss erkannt
PTP State Changed	Info	Der aktuelle PTP-Status hat sich geändert
PTP Error	Fehler	Ein PTP-Fehler wurde erkannt -> PTP Globaler Status
IMS I/O-Events (nur bei IMS-Systemen)		
IMS Error	Fehler	Es wurde ein Fehler in einem IMS-Modul festgestellt -> Sonstige Meldungen
IMS OK	Info	IMS-Modul ist fehlerfrei
Sync-E Input Quality Level Changed	Info	Der Qualitätsfaktor der SyncE-Referenz hat sich geändert -> Option SyncE-Konfiguration
ESI: ITU limits violated	Fehler	Überschreitung bzw. Unterschreitung der durch ITU-T festgelegten Empfehlungen -> IMS - LIU (Line Interface Unit)
ESI: ITU limits adhered	Info	ITU-Grenzwerte werden eingehalten
Port Error	Error	z.B. Kurzschluss auf dem Eingang einer IMS-VSI-Referenzkarte

Tabelle: Alle Benachrichtigungs-Events

Ereignis	Schweregrade (nach X.733)	Beschreibung
Port OK	Info	Signal am Port ist in Ordnung (die Karte muss das Port-Ereignis unterstützen - z.B. IMS-VSI)

Tabelle: Alle Benachrichtigungs-Events

13.1.5 Sicherheit



Diese Seite ermöglicht die Konfiguration von Zugriffsbeschränkungen und **snmp**. Das Menü bietet auch die Möglichkeit, SSH-Schlüssel und ein HTTPS-Zertifikat zu erstellen oder hochzuladen.

Wenn Sie sich nicht sicher sind, welche Werte erforderlich sind, wenden Sie sich bitte an Ihren Netzwerk-Administrator.

13.1.5.1 Anmeldung

Im Menü „Anmeldung“ können Sie allgemeine Sicherheitseinstellungen für das Anmeldeverhalten des LANTIME vornehmen.

Root-Zugang sperren:
Diese Funktion kann nur von einem Admin-Benutzer oder einem Superuser aktiviert werden. Wenn diese Funktion aktiv ist, kann sich der „root“-Benutzer nicht mehr am LANTIME anmelden.

Fernzugriffskontrolle:
In dieser Konfigurationsdatei können Sie eine Zugriffskontrolle für die LANTIME-Webschnittstelle konfigurieren, die auf dem IP-Protokoll basiert. In dieser Datei können Sie die IP-Adressen eingeben, die für den Zugriff auf die Weboberfläche zugelassen werden sollen. Nach dem ersten Eintrag ist der Zugriff auf alle anderen Clients automatisch gesperrt. Es können einzelne Client-IPs oder ganze Subnetze konfiguriert werden.

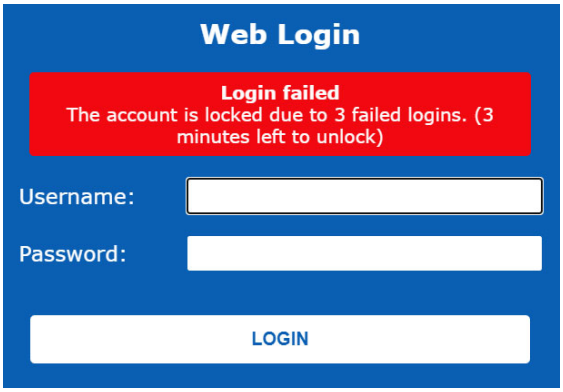
Shell Timeout:
Definiert ein Timeout in Sekunden. Nach Ablauf dieser Frist ohne Benutzerinteraktion wird die aktuelle Sitzung auf der Kommandozeile für den angemeldeten Benutzer beendet.

Web-Timeout:
Der Parameter Web-Timeout definiert, wie viele Minuten Inaktivität vergehen können, bis ein Benutzer automatisch von der Weboberfläche abgemeldet wird.

Bruteforce-Erkennung aktivieren:
Wenn die Bruteforce-Erkennung aktiviert ist, werden nach zu vielen fehlerhaften Anmeldeversuchen die Benutzer-Accounts vorübergehend gesperrt.

Entsperrzeit:
Die Entsperrzeit, ist die Zeit, bis ein gesperrter Benutzer wieder entsperrt wird.

Anzahl Versuche:
Mit der Anzahl der Versuche wird die Anzahl der Anmeldeversuche angegeben, die fehlschlagen müssen bis ein Benutzer-Account gesperrt wird.

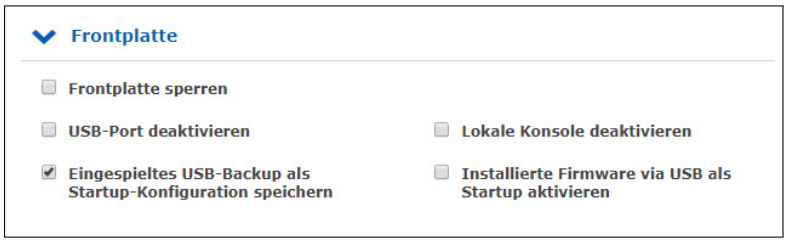


Lautlos-Modus:
Der Lautlos-Modus verhindert, dass über die SSH- und Web-Schnittstelle der Sperrzustand eines Benutzers ausgegeben wird. Dies verhindert somit auch das Preisgeben von gültigen Benutzernamen an Angreifer, reduziert jedoch die Nachvollziehbarkeit von Benutzern die aus Versehen ihre Login-Daten zu oft falsch eingegeben haben und sich während der Sperrzeit auch mit gültigen Daten nicht anmelden können.

Automatisches Neuladen der Hauptseite deaktivieren:
Verhindert das automatische Neuladen des Webinterfaces innerhalb 60 Sekunden, solange sich ein Benutzer im Hauptmenü vom LANTIME befindet.

13.1.5.2 Frontplatte

Dieses Menü ermöglicht allgemeine Sicherheitseinstellungen für das Frontpanel des LANTIME.



Frontplatte sperren:
Wenn die Funktion aktiviert ist, ist die Frontplatte eines LANTIME deaktiviert.

USB-Port deaktivieren:
Nach der Aktivierung dieser Funktion wird der USB-Anschluss eines LANTIME auf der Frontplatte deaktiviert und angeschlossene USB-Speichermedien können nicht erkannt werden.

Checkbox „Eingespieltes USB-Backup als Startup-Konfiguration speichern“
Sie können eine vorher gesicherte Konfiguration über das USB-Stick-Menü auf Ihrem LANTIME aufspielen, wenn Sie dieses Kontrollkästchen aktiviert haben, wird die hochgeladenen Konfiguration direkt als Startkonfiguration übernommen.

Checkbox „Installierte Firmware via USB als Startup aktivieren“
Durch die Aktivierung dieser Checkbox wird eine Firmware-Version, die über das USB-Menü auf dem LANTIME geladen wurde, direkt als aktive Firmware übernommen.

Siehe auch USB Stick.

13.1.5.3 SSH - Secure Shell

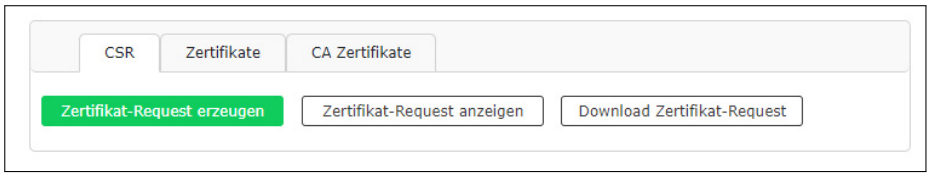
Über „Secure Shell Login“ (SSH) ist es möglich, eine gesicherte Verbindung zum LANTIME herzustellen. Alle Daten werden bei der Übertragung über Ethernet verschlüsselt. Um diesen Dienst nutzen zu können, muss SSH auf jeder Schnittstelle in den Netzwerkeinstellungen aktiviert sein (siehe auch das Konfigurationskapitel Netzwerkdienste). „Web GUI [rightarrow]] Netzwerk → Netzwerkdienste“).

Länge des Keys (Bits):
Legt die Schlüssellänge für einen neuen zu generierenden Schlüssel fest.

Generierung eines SSH-Keys:
Erzeugt ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, in konfigurierbarer Länge.

Zeige SSH-Key:
Mit dieser Schaltfläche können Sie die öffentlichen SSH-Schlüssel eines LANTIME anzeigen.

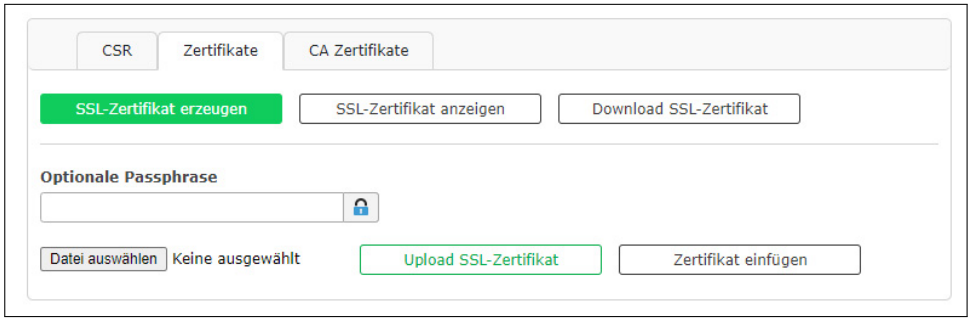
13.1.5.4 Zertifikate



HTTPS ist ein Standard für die verschlüsselte Übertragung von Daten zwischen Webbrowser und Webserver. Sie basiert auf X.509-Zertifikaten und asymmetrischen Krypto-Verfahren. Der Zeitserver verwendet diese Zertifikate um sich bei einem Client (Webbrowser) zu authentifizieren. Wenn sich ein Webbrowser zum ersten Mal mit dem HTTPS-Webserver Ihres LANTIME verbindet, werden Sie aufgefordert, das Zertifikat des Webservers zu akzeptieren.

Um sicherzustellen, dass Sie mit Ihrem bekannten Zeitserver kommunizieren, überprüfen Sie das Zertifikat und akzeptieren Sie es, wenn es mit dem im LANTIME gespeicherten übereinstimmt. Alle weiteren Verbindungen vergleichen das Zertifikat mit dem, welches in Ihrer Webbrowser-Konfiguration gespeichert ist. Anschließend werden Sie aufgefordert, das Zertifikat nur dann zu überprüfen, wenn es geändert wird.

Hinweis: Standardmäßig ist im LANTIME ein selbstsigniertes Zertifikat installiert, das nicht von einer Certificate-Authority (CA) signiert ist. Daher geben einige Webbrowser an, dass die Verbindung nicht sicher ist. Wenn Sie ein Zertifikat installieren möchten, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde, können Sie die Schaltfläche „SSL-Zertifikat hochladen“ verwenden. Weitere Details dazu finden Sie in den folgenden Anweisungen.



SSL-Zertifikat generieren:
Ermöglicht die Erstellung eines neuen selbstsignierten SSL-Zertifikats.

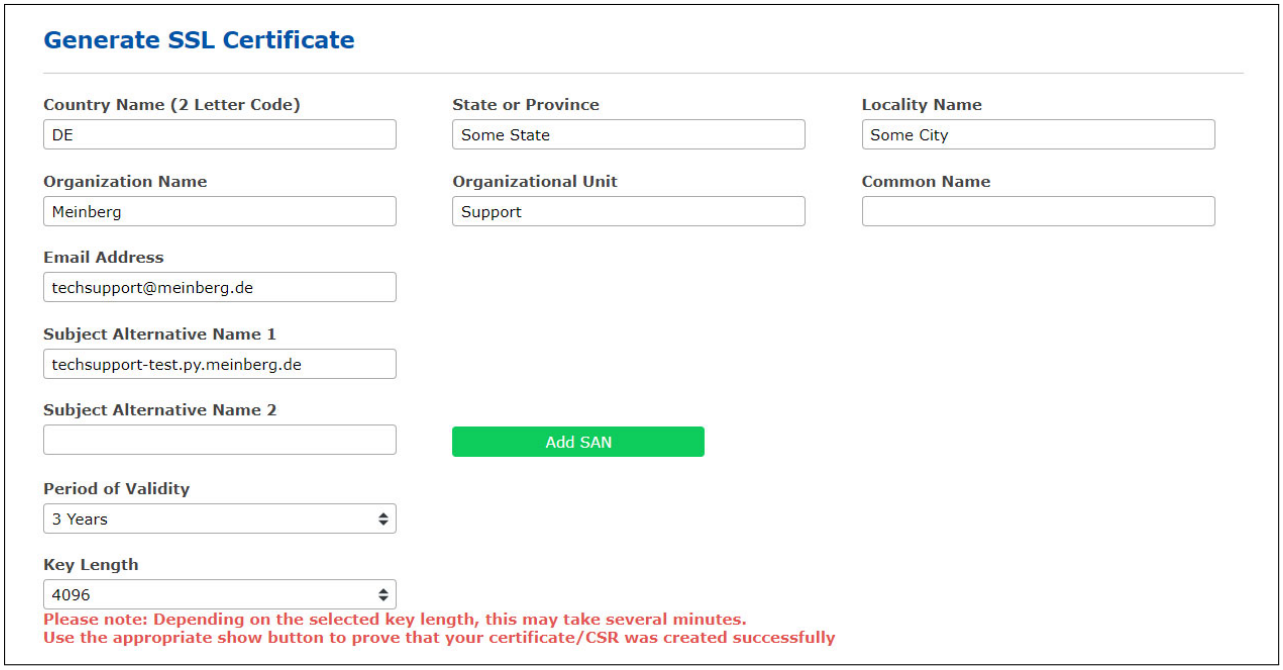
SSL-Zertifikat anzeigen:
Überprüfen Sie das aktuell installierte SSL-Zertifikat.

Download SSL-Zertifikat:
Ermöglicht das Herunterladen des aktuell installierten SSL-Zertifikats.

Optionale Passphrase
Ist der privater Schlüssel des SSL-Zertifikats mit einem Passwort geschützt, dann müssen Sie hier die „Passphrase“ eingeben. Der Webserver kann ansonsten nicht automatisch starten, da er den hochgeladenen Schlüssel nicht entschlüsseln kann.

SSL-Zertifikat hochladen:
Ermöglicht das Hochladen eines Zertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde. Dieses Zertifikat muss im PEM-Dateiformat vorliegen.

Zertifikatsanforderung generieren:
Die Funktion „Zertifikat-Request erzeugen“ ermöglicht das Erstellen einer Certificate-Signing-Request (CSR), die an eine Zertifizierungsstelle gesendet werden kann, um ein signiertes Zertifikat zu beantragen. Auf dem LANTIME wird dadurch ein Zertifikat und ein privater Schlüssel angelegt. Der Speicherort für die CSR ist *„/mnt/flash/data/https.req“*, der passende Schlüssel wird unter *„/mnt/flash/data/https.req.pk“* abgelegt.



Antragsteller (SAN - Subject Alternative Name)
Im Feld „Antragsteller (SAN)“ können Sie zusätzliche Hostnamen (Sites, IP-Adressen, Common Names usw.) angeben, die durch ein einzelnes SSL-Zertifikat, z. B. ein Multi-Domain-Zertifikat, geschützt werden sollen. Mehrere SANs können über die Schaltfläche „SAN hinzufügen“ angegeben werden. Der Typ des SAN wie z.B. IP oder DNS wird automatisch ermittelt. Der gemeinsame Name („Common Name“) kann getrennt vom SAN spezifiziert werden.

Hinweis:
Wenn Sie das bei der Zertifizierungsstelle eingereichte Zertifikat über den LANTIME und die Funktion „Zertifikat-Request erzeugen“ generiert haben, dann ist der passende Schlüssel für dieses Zertifikat bereits unter *„/mnt/flash/data/https.req.pk“* abgelegt. Nach dem Hochladen des signierten Zertifikates wird dieser zuvor erzeugte private Schlüssel verwendet.

Wenn das eingereichte und signierte Zertifikat nicht auf dem LANTIME erzeugt wurde, dann muss die PEM-Datei den privaten Schlüssel und das Zertifikat selbst enthalten.

Der Inhalt des privaten Schlüssels beginnt mit:
„—BEGIN RSA PRIVATE KEY—“
und endet mit
„—END RSA PRIVATE KEY—“

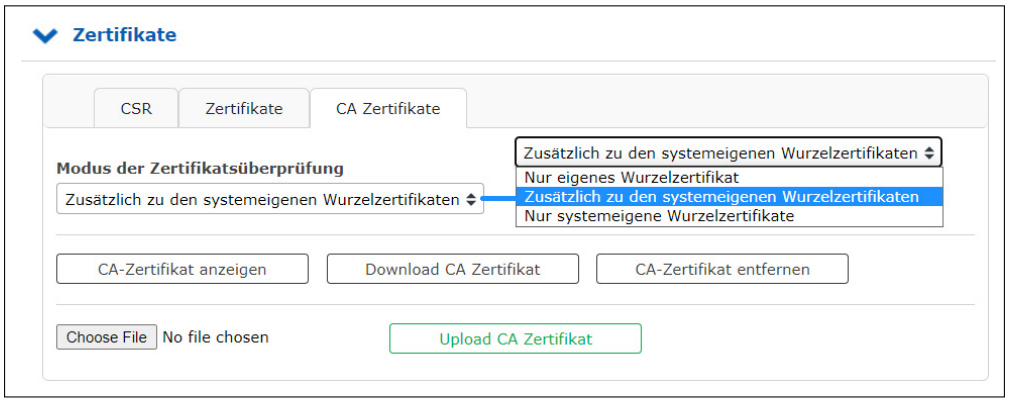
das Zertifikat selbst beginnt mit
„—BEGIN CERTIFICATE—“
und endet mit
„—END CERTIFICATE—“.

Dieses Beispiel ist ein Auszug aus einer PEM-Datei:

```
---BEGIN RSA PRIVATE KEY---
MIICXQIBAAKBgQC6FkGxyJ6+Bqxzfp3bNtEYyiRIAbQAIsHblYPG7aQk+8XbIXWB
...
aiLbmu7N3TEdWVDgro8kMuQC/Ugkttx7TdJJbqJoVsF5
---END RSA PRIVATE KEY---
---BEGIN CERTIFICATE---
MIIEJTCCA46gAwIBAgIJANF4dlCI2saDMA0GCSqGSIb3DQEBBQUAMIG+MQswCQYD
...
ekZ970dAaPca
---END CERTIFICATE---
```

13.1.5.5 CA Zertifikate

Die Funktionen in dem Menü „Sicherheit → Zertifikate → CA Zertifikate“ können genutzt werden, um eine eigene, nicht öffentliche Wurzelzertifizierungsstelle dem LANTIME hinzuzufügen. Dadurch können Programme und Dienste die eine TLS-Verbindung aufbauen, wie z.B. der LDAP-Dienst, den angefragten Server eindeutig identifizieren, obwohl kein (meist kostenpflichtiges) Zertifikat einer öffentlichen Zertifizierungsstelle genutzt wird.



Der Modus der Zertifikatsüberprüfung kann wie folgt gewählt werden:

Nur eigenes Wurzelzertifikat: Der LANTIME nutzt ausschließlich das hochgeladene eigene Wurzelzertifikat um Verbindungen zu verifizieren.

Zusätzlich zu den systemeigenen Wurzelzertifikaten: Der LANTIME nutzt das hochgeladene eigene Wurzelzertifikat sowie die systembekannten öffentlichen Zertifizierungsstellenzertifikate.

Nur systemeigene Wurzelzertifikate: Der LANTIME nutzt die systembekannten öffentlichen Zertifizierungsstellenzertifikate.

13.1.5.6 Hochladen von signierten mehrstufigen/verketteten Zertifikaten

Neben SSL-Zertifikaten werden auch mehrstufige/verkettete Zertifikate unterstützt. Die Zertifikatskette kann zusammen mit dem Serverzertifikat und dem privaten Schlüssel im pem-Format hochgeladen werden.

Die Zertifikatskette sollte in der richtigen Reihenfolge eingetragen werden, um eventuellen Problemen vorzubeugen. Das erste Zertifikat muss das Serverzertifikat sein, gefolgt von den Zwischenzertifikaten (Intermediate Certificates), bis schließlich das (optionale) Wurzelzertifikat das Ende der Datei markiert. Der Schlüssel für das Serverzertifikat sollte direkt vor oder direkt nach dem Serverzertifikat hinterlegt werden.

13.1.5.7 SNMP

Das Simple Network Management Protocol (SNMP) wird in Netzwerkmanagementsystemen zur Statusüberwachung von Geräten eingesetzt. SNMP arbeitet mit der Abfrage von „Objekten“. Über ein solches Objekt können wir Informationen über ein Netzwerkgerät sammeln. Die sogenannte Management Information Base (MIB) ist eine Datei, die alle Objekte enthält, die über SNMP verwaltet werden können.

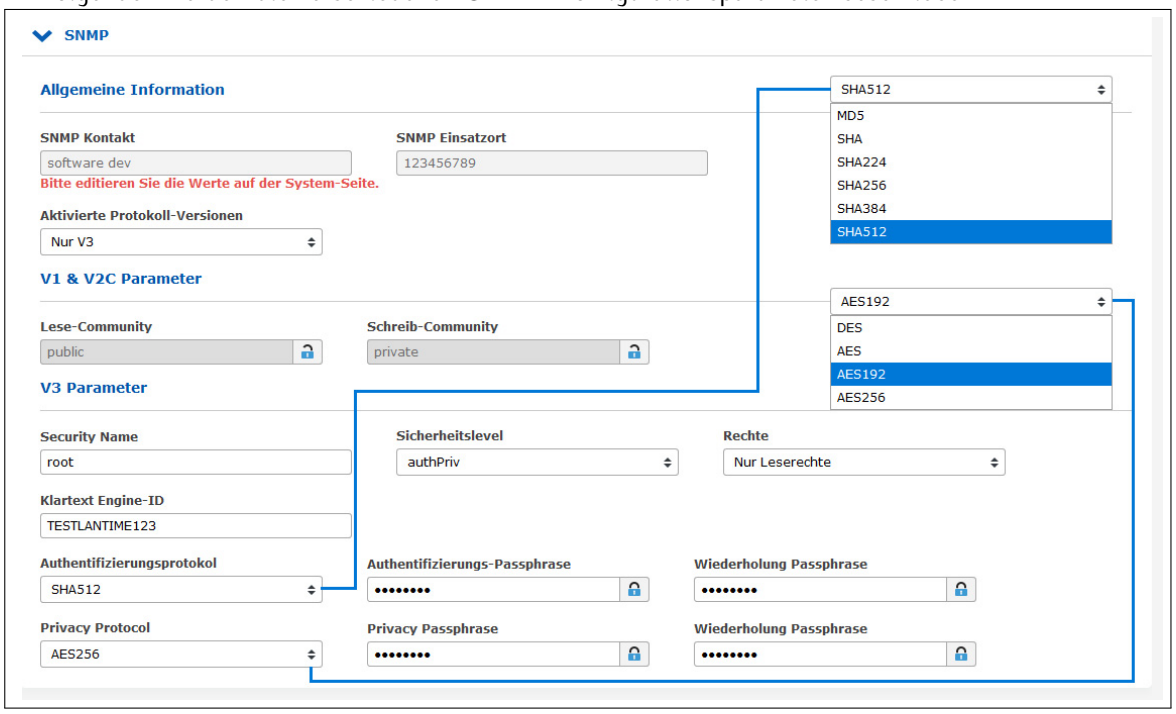
Die Meinberg SNMP-MIB-Dateien können auf der Seite „System → Dienste und Funktionen → SNMP MIB“ heruntergeladen werden. Die Dateien „MBG-SNMP-ROOT-MIB.mib“ und „MBG-LANTIME-NG-MIB.mib“ müssen zur Überwachung eines LANTIME-Systems verwendet werden.

(siehe auch Kapitel „Das Webinterface → System → Dienste und Funktionen“).

Standardmäßig ist der SNMP-Dienst auf einem LANTIME-System nicht aktiviert. Der Dienst kann auf jeder Schnittstelle auf der Seite „Netzwerk → Netzwerkdienste“ aktiviert werden.

(siehe auch Kapitel „Das Webinterface → Netzwerk → Netzwerkdienste“)

Im Folgenden werden die verschiedenen SNMP-Konfigurationsparameter beschrieben:



Aktivierte Protokoll-Versionen:
Konfiguration der SNMP-Protokollversion. Die folgenden Optionen können ausgewählt werden: „Nur V1/V2“, „Nur V3“, „V1/V2/V3“.

V1/V2 Parameter

Lese-Community:
Die Read-Community wird nur für die SNMP-Versionen V1 und V2 verwendet. Es ist wie eine Benutzerkennung oder ein Passwort, das den Zugriff auf die LANTIME SNMP-Objekte ermöglicht. Das SNMP-Überwachungssystem sendet den gelesenen Community-String zusammen mit allen SNMP-Anfragen. Wenn der Community-String korrekt ist, antwortet der LANTIME mit den angeforderten Informationen. Wenn der Community-String falsch ist, verwirft der LANTIME einfach die Anfrage und antwortet nicht.

Schreib-Community:
Die Write-Community wird nur für die SNMP-Versionen V1 und V2 verwendet. Es ist wie eine Benutzerkennung oder ein Passwort, das den Zugriff auf die LANTIME SNMP-Objekte ermöglicht. Das SNMP-Monitoring-System sendet die Write-Community-Zeichenkette zusammen mit allen SNMP-SET-Befehlen. Wenn der Community-String korrekt ist, wird der Befehl SNMP-SET ausgeführt. Wenn der Community-String falsch ist, wird der Befehl SNMP-SET nicht ausgeführt.

V3 Parameter

Security Name:
SNMP V3 Benutzername

Sicherheitslevel:
Nachrichten können unauthentifiziert, authentifiziert oder authentifiziert und verschlüsselt gesendet werden, indem die zu verwendende Sicherheitsstufe festgelegt wird:

noAuthnoPriv - unauthentifiziert und unverschlüsselt
authNoPriv - authentifiziert und unverschlüsselt
authPriv - authentifiziert und verschlüsselt

Klartext Engine-ID:
Innerhalb einer administrativen Domäne ist eine SNMP V3 Engine ID eine eindeutige Kennung einer SNMP-Engine. Hier kann eine Zeichenkette mit maximal 27 Zeichen eingegeben werden. Die Zeichenkette wird verwendet, um die hex engineID unter Verwendung des in RFC3411 beschriebenen Textformatschemas zu erzeugen. Wenn z.B. der String „hello“ als engineID konfiguriert ist, wäre die generierte hex engineID 800015dd0468656c6c6c6f.

- 15dd ist die hexadezimale Darstellung der Meinberg Unternehmens-ID 5597.
- 04 ist ein Indikator dafür, dass das Textformatschema verwendet wird, um die Engine-ID zu generieren.
- 68656c6c6c6f ist die hexadezimale Darstellung der Zeichenkette „hello“.

Rechte:
Konfiguration der Zugriffsebene (Lesezugriff oder Lese-/Schreibzugriff).

Authentifizierungsprotokoll:
Die für die Authentifizierung verwendeten Protokolle sind MD5 und SHA (Secure Hash Algorithm):

- MD5
- SHA
- SHA224
- SHA256
- SHA384
- SHA512

Authentifizierungs-Passphrase:
Benutzerpassphrase, die mindestens 8 Zeichen lang sein muss.

Datenschutzprotokoll:
Die für die Verschlüsselung verwendeten Protokolle sind DES (Data Encryption Standard) und AES (Advanced Encryption Standard):

- DES
- AES
- AES192
- AES256

Datenschutz-Passphrase:
Eine Passphrase, die beim Verschlüsseln von Paketen verwendet wird. Sie muss mindestens 8 Zeichen lang sein.

13.1.5.8 SHS-Konfiguration

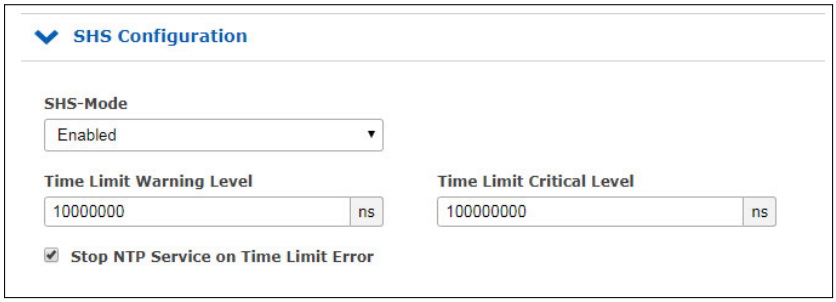
SHS ist die Abkürzung für Secure Hybrid System und ist auf LANTIME-Systemen mit zwei Referenzuhren verfügbar. Wenn der SHS-Modus aktiviert ist, wird nur die aktuell aktive Uhr zum Weiterleiten des Zeitsignals an den NTP-Dienst verwendet, die andere Uhr wird als „nicht ausgewählt“ angezeigt und nur zum Messen und Vergleichen einer Zeitdifferenz zwischen beiden Empfängern verwendet.

In dieser Hinsicht unterscheidet sich SHS von einem redundanten Modus. Im redundanten Modus schaltet eine Schalteinheit je nach Verfügbarkeit und Synchronisationsstatus zwischen der einen und der anderen Uhr um und der aktive Empfänger übergibt das Zeitsignal an den NTP-Dienst.

Der SHS-Modus sorgt für einen sicheren Betrieb und tritt in Aktion, wenn eine Zeitdifferenz zwischen beiden Empfängern ein konfigurierbares Zeitlimit überschreitet.

In diesem Fall werden Alarme ausgelöst und über konfigurierte Benachrichtigungskanäle (z.B. SNMP-Trap, E-Mail, Syslog-Nachricht) gesendet. Außerdem sollte der NTP auch in diesem Fall gestoppt werden, um den sicheren Betrieb des Zeitmessdienstes zu unterstützen. Deshalb müssen Sie in diesem Schritt „NTP-Dienst bei Zeitlimitfehler stoppen“ wählen.

Andererseits wird bei IMS-Systemen mit zwei Referenzuhren das von den Empfängern kommende Zeitsignal mit einer RSC-Karte (Redundant Switch Control Unit) kontinuierlich gemessen und miteinander verglichen. Die Messungen werden an den SHS-Modus weitergeleitet, wenn dieser aktiviert ist. Ähnlich wie bei LANTIME-Systemen mit SHS können die Alarme ausgelöst werden, wenn eine Differenz der beiden Signale die konfigurierten Zeitbegrenzungseinstellungen überschreitet und der NTP-Dienst zum Stoppen konfiguriert sein sollte.



SHS-Modus
Der SHS-Modus kann über dieses Auswahlfeld selektiv aktiviert oder deaktiviert werden. Wenn der SHS-Modus deaktiviert ist, findet kein Zeitvergleich statt und die Zeiten beider Empfänger werden direkt an den NTP-Dienst übertragen. Der NTP-Dienst entscheidet dann selbstständig, welche Zeit für die Synchronisation verwendet wird (redundanter Modus).

Time Limit Warning Level
Überschreitet die berechnete Zeitdifferenz zwischen den beiden Referenzuhren den konfigurierten Wert, erzeugt der LANTIME einen Alarm „SHS Time Limit Warning“. Dieser Alarm kann per E-Mail oder SNMP-Trap gesendet werden, wenn er in den Benachrichtigungseinstellungen entsprechend konfiguriert ist.
(Siehe auch Konfigurationskapitel „Das Webinterface → Benachrichtigung → E-Mail-Information“)

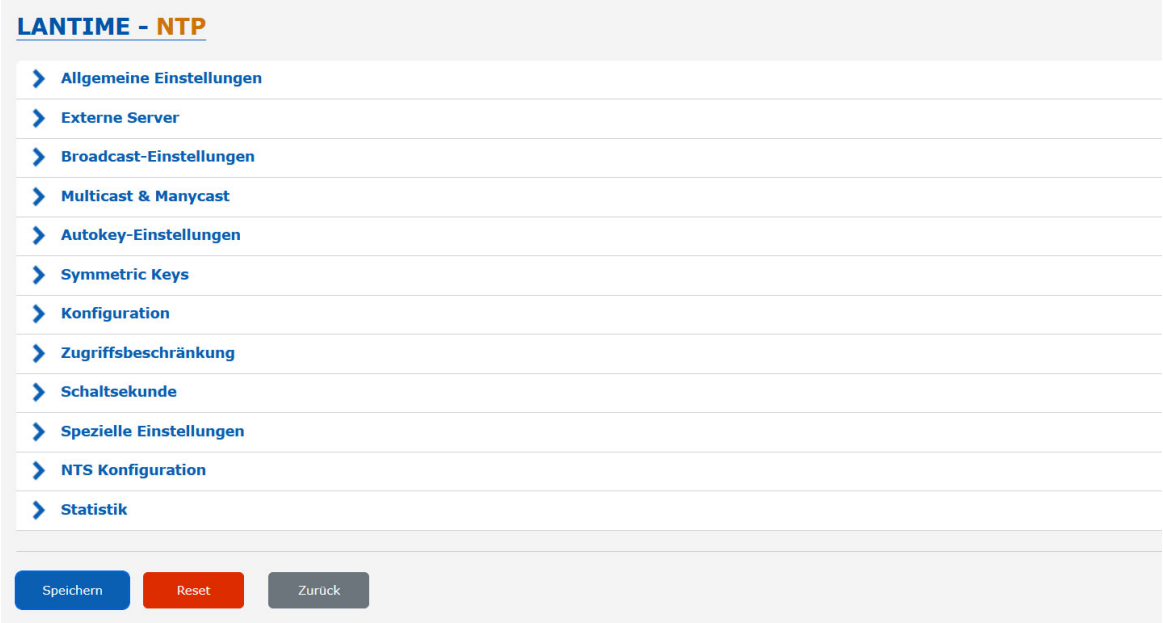
Bei LANTIME IMS-Systemen mit eingebauter RSC wird der Parameter in Nanosekunden konfiguriert. Für Systeme ohne RSC in Millisekunden.

Time Limit Error-Level (ms)
Überschreitet die berechnete Zeitdifferenz zwischen den beiden Referenzuhren den konfigurierten Wert, erzeugt der LANTIME einen Alarm „SHS Time Limit Warnung“. Dieser Alarm kann per E-Mail oder SNMP-Trap gesendet werden, wenn er in den Benachrichtigungseinstellungen entsprechend konfiguriert ist.

Bei LANTIME IMS-Systemen mit eingebauter RSC wird der Parameter in Nanosekunden konfiguriert. Für Systeme ohne RSC in Millisekunden.

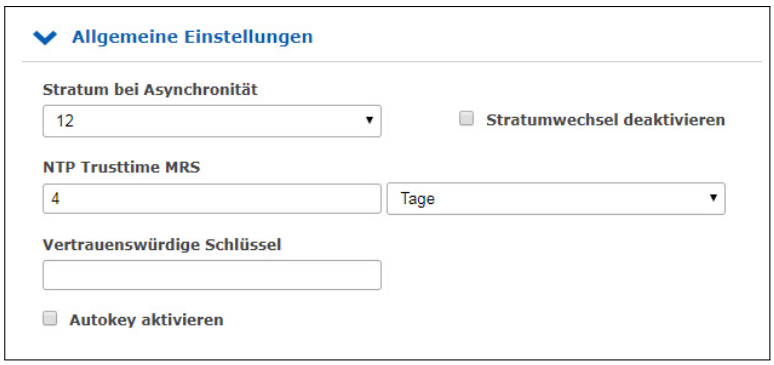
NTP-Dienst bei Zeitlimitfehler stoppen
Hier können Sie entscheiden, ob der NTP-Dienst mit dem kritischen „TimeLimitError“ beendet werden soll. In diesem Fall würde ein anfragender NTP-Client keine Antwort mehr vom Zeitserver erhalten.

13.1.6 NTP



Auf der Seite NTP-Konfiguration werden die zusätzlichen NTP-Parameter eingerichtet, die für einen spezifizierten Betrieb des NTP-Subsystems erforderlich sind.

13.1.6.1 Allgemeine Einstellungen



Stratum-Level wenn nicht synchron
Der Stratum-Level für NTP bezieht sich auf einen „Abstand" zu einer Referenzquelle und nicht auf die Genauigkeit. So hat beispielsweise ein Zeitserver mit einer internen Referenz wie GPS oder DCF77 intern einen „Level 0" und wird von einem externen Netzwerk als „Level 1" betrachtet. Mit der Einstellung „Stratum Level wenn nicht synchron" wird der Stratum-Wert konfiguriert, mit dem sich der Server im Netzwerk präsentiert, wenn keine Referenzzeitquelle verfügbar ist. Dieser Wert wird erst wirksam, wenn die konfigurierte NTP-Trustime für den internen Referenztakt abgelaufen ist und keine weiteren Zeitquellen wie z.B. externe NTP-Server zur Verfügung stehen.

Stratumwechsel deaktivieren
Durch die Aktivierung dieser Betriebsart präsentiert sich der Server immer (auch asynchron) als Stratum 1-Server im Netzwerk. Die Einstellung bei „Stratum-Level wenn nicht synchron" ist nicht mehr wirksam.

Beispiele:

a) Ein LANTIME, der mit seiner internen Referenzuhr wie GPS oder DCF77 synchronisiert wird, fungiert als Stratum 1 NTP-Server. Wenn die Funktion „Stratumwechsel deaktivieren" aktiv ist, fungiert der NTP-Server als Stratum 1-Server, wenn die Referenzuhr asynchron läuft und keine anderen Zeitquellen zur Verfügung stehen.

b) Ein LANTIME, der nur von einem externen NTP-Server mit Stratum 3 synchronisiert wird, fungiert in einem Netzwerk als Stratum 4 NTP-Server. Wenn die Funktion „Stratumwechsel deaktivieren" aktiviert ist, arbeitet der NTP-Server weiterhin als Stratum 4 NTP-Server, auch wenn die Verbindung zum externen NTP-Server unterbrochen wird.

c) Wechselt NTP des LANTIME mit aktiver Funktion „Stratumwechsel deaktivieren" von seinem internen Referenztaktgeber zu einem externen NTP-Server mit Stratum 2, ändert sich der Stratum des LANTIME von 1 auf 3.

NTP Trustime

Diese Einstellung legt fest, wie lange NTP der internen Referenzuhr eines Servers „vertrauen" soll, nachdem diese asynchron geworden ist. Der Status einer asynchronen Referenzuhr wird auch als „freilaufend" bezeichnet. Die Genauigkeit einer „freilaufenden" Referenzuhr hängt vom Typ des integrierten Oszillators ab. Die Vertrauenszeit sollte daher in Abhängigkeit von der Genauigkeit der „freilaufenden" Referenzuhr eingestellt werden.

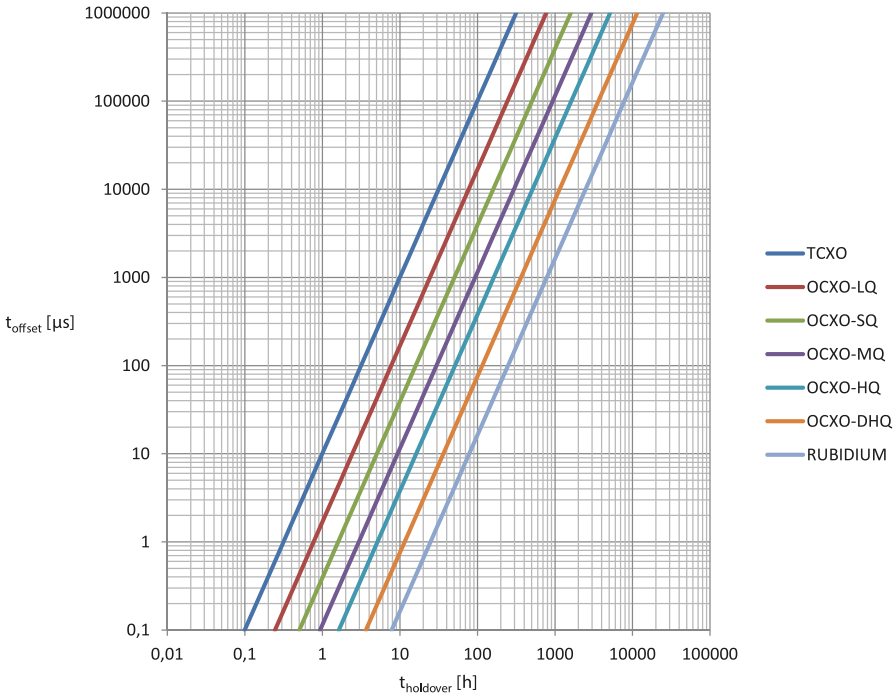


Abbildung: Verhältnis zwischen Holdover-Zeit (x) und Offset (y) unter Verwendung der eingesetzten Meinberg-Oszillatoren

Wie konfiguriere ich die richtige Trusttime in meiner Anwendungsumgebung?
Als Beispiel nehmen wir jetzt an, dass unser Empfänger einen eingebauten TCXO-Oszillator verfügt. Die Trusttime soll ab einem Offset von 1ms ablaufen. Anhand der Grafik kann abgelesen werden, dass nach 10 Stunden Holdover-Zeit dieser Offset erreicht wird. Demzufolge sollte eine Trusttime von 10 Stunden konfiguriert werden.

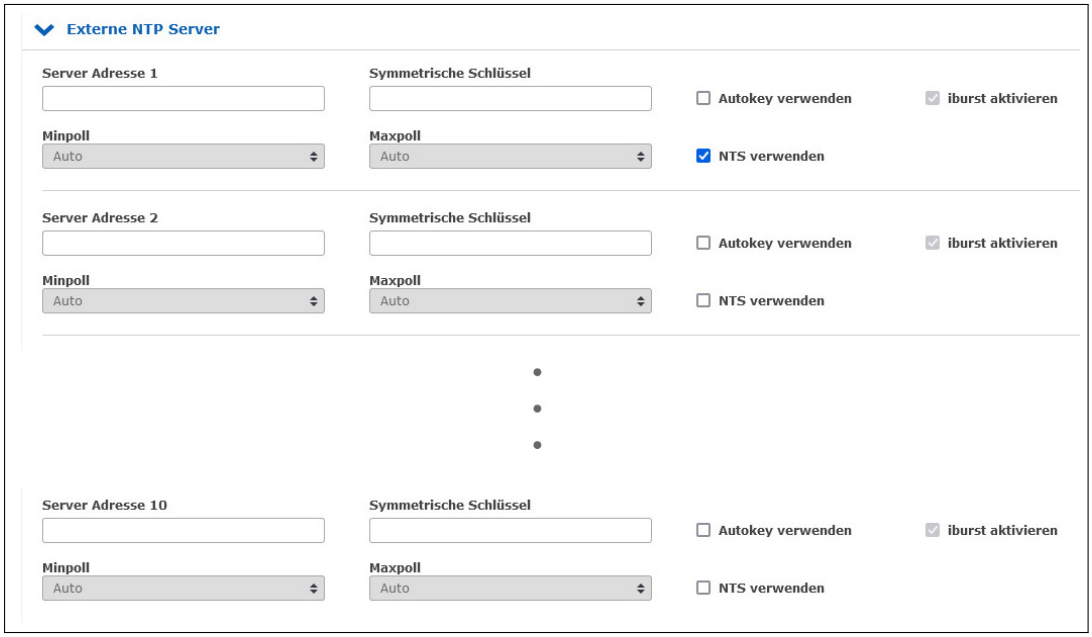
Vorgehensweise: Zunächst sollte in Erfahrung gebracht werden, welcher Oszillator eingesetzt wird. Gehen Sie dazu in das Webinterface-Menü „Monitoring und Management → Uhr → Empfänger-Informationen → Oszillator Typ". Danach können Sie sich für sich einen Offset festlegen, ab dem der NTP seinen Stratum bzw. die Trusttime verlieren soll.

Eine Liste der Oszillatoren, die für Meinberg Referenzuhren verfügbar sind:
https://www.meinberg.de/german/specs/gpsopt.htm

Vertrauenswürdige Schlüssel
In diesem Feld können Sie die IDs der symmetrischen Schlüssel eingeben, die für die Authentifizierung verwendet werden sollen. Wenn Sie mehr als einen Schlüssel haben, müssen die IDs mit einem Leerzeichen eingegeben werden, um sie voneinander zu trennen. Die symmetrischen Schlüssel können Sie im Untermenü „NTP Symmetric Keys" auf der NTP-Seite konfigurieren. Weitere Informationen finden Sie im Unterkapitel „NTP Symmetric Keys".

13.1.6.2 Externe NTP-Server

Über das Konfigurationsformular können Sie bis zu 10 externe NTP-Server als Backup für die interne Referenzuhr eingeben.



Server-Adresse:
IP oder Hostname eines externen Servers.

Symmetrische Schlüssel:
In diesem optionalen Feld können Sie die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit dem externen Server verwendet werden soll.

Damit die Authentifizierung funktioniert, müssen folgende Punkte berücksichtigt werden:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Untermenü „NTP → NTP Symmetric Keys“ auf der NTP-Seite bearbeiten.

b) Zusätzlich müssen Sie die ID in das Feld „Lokale Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ eingeben.

c) Auf dem externen Server muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Minpoll und Maxpoll (nicht verfügbar auf Geräten, die die MRS-Funktion unterstützen):
Mit diesen Einstellungen können Sie das minimale und maximale Abfrageintervall (Abfragezyklus) für einen bestimmten externen Server festlegen. NTP beginnt mit dem minimalen Abfrageintervall und ändert sich Schritt für Schritt zum Maximum des Abfrageintervalls.

iburst aktivieren (nicht verfügbar auf Geräten, die die MRS-Funktion unterstützen):
Die iburst-Aktivierung beschleunigt die anfängliche Synchronisation mit einem externen Server.

NTS verwenden (nur verfügbar auf Geräten, die die MRS-Funktion unterstützen)
Diese Option aktiviert Network Time Security für den jeweiligen externen NTP-Server. Ist NTS aktiviert, kann für diesen Server kein weiteres Authentifizierungsverfahren genutzt werden. Die Konfiguration von symmetrischen Schlüsseln oder Autokey wird somit für diesen Server ignoriert.

Damit die NTS-Authentifizierung funktioniert, müssen folgende Punkte berücksichtigt werden:

- Die eingetragene Server-Adresse muss der des NTS-KE-Servers entsprechen.
- Um den NTS-KE-Server verifizieren zu können, muss auf dem LANTIME ein entsprechendes Wurzelzertifikat vorhanden sein (siehe CA Zertifikate).

Besonderheit LANTIME/MRS:
Alle externen NTP-Server werden ausschließlich für statistische Zwecke angefordert und vom Zeitdienst niemals direkt als Synchronisierungs-Peer ausgewählt. Normale NTPv4-Server werden dazu in der NTPD-Konfigurationsdatei */etc/ntp.conf* als „noselect“ hinzugefügt.

Da NTPD derzeit keine Unterstützung für Network Time Security bietet, werden externe NTS-Server über einen separaten Chrony-Zeitdienst angefragt.

Die LANTIME MRS-Logik wählt dann den besten Server unter allen externen Servern aus. Der Auswahlalgorithmus für den besten externen NTP-Server wird in den folgenden Schritten beschrieben:

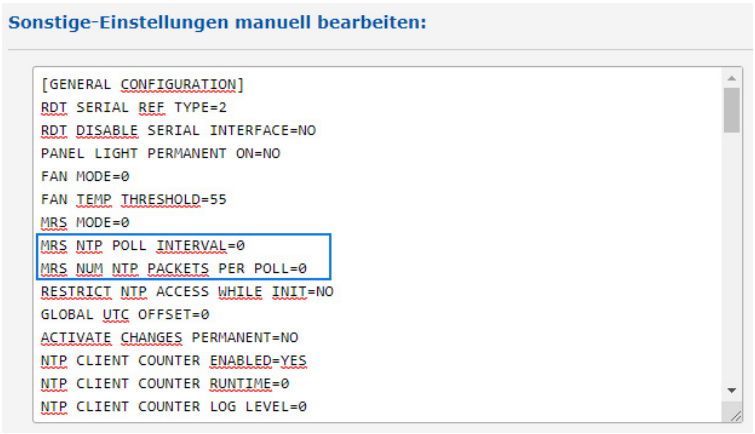
- Auswahl, welcher Server akzeptiert wird
- Gruppen von verschiedenen Offsets werden erstellt
- Auswahl der größten Gruppe
- Ausreißer werden gesucht und aus dieser Gruppe entfernt
- der Median wird als bester Server verwendet
- Prüfung, ob „last_best_external_NTP_server“ verwendet werden kann - um häufige Wechsel zwischen den NTP Servern zu reduzieren

Der beste Server kann im Web-Interface im Menü „Statistik → NTP-Status“ und in dem Menü „Uhr → Status & Konfiguration → MRS-Status“ überprüft werden. Der ermittelte Offset wird dann zur Steuerung des internen Oszillators verwendet, falls keine andere Referenzquelle mit einer höheren Priorität zur Verfügung steht.

Aufgrund dieser Besonderheit unterscheiden sich die Konfigurationsmöglichkeiten für externe NTP-Server. Die Parameter Minpoll, Maxpoll und Iburst können auf einem LANTIME/MRS nicht konfiguriert werden.

Für einen LANTIME/MRS können Sie das Standardabfrageintervall von 32 Sekunden über die manuelle Konfiguration des Servers einstellen. Um fortzufahren, folgen Sie dieser Menüführung:

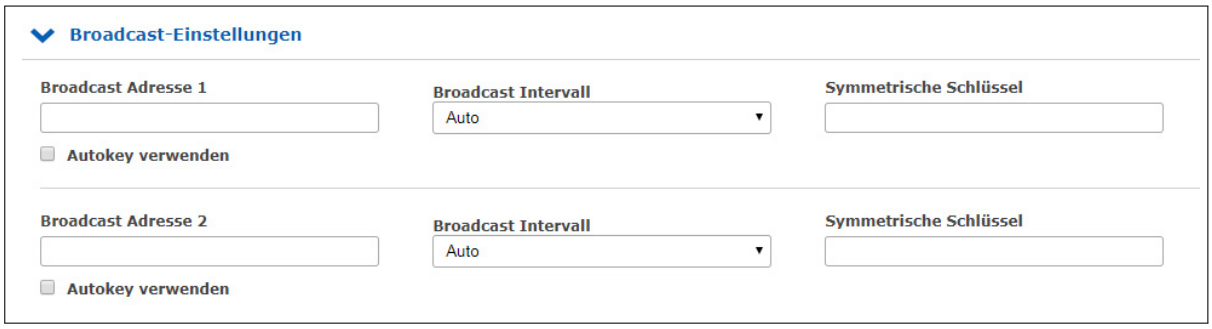
Webinterface - „System → Dienste und Funktionen → Manuelle Konfiguration → Standardkonfiguration → Sonstige Konfiguration“.



Mit dem Parameter „MRS NTP POLL INTERVAL“ können Sie das Polling-Intervall des externen Servers anpassen. Standardmäßig ist dieser Wert auf 0 gesetzt, d.h. externe Server werden alle 32 Sekunden abgefragt. Die Werte können zwischen 1 und 10 eingestellt werden und werden als Potenz von 2 verwendet, z.B. wenn dieser Wert auf 6 gesetzt wird, entspricht das $2_6 = 64$ Sekunden für ein Abfrageintervall.

Mit dem Parameter „MRS NUM NTP PACKETS PER POLL“ können Sie die Anzahl der gesendeten NTP-Abfragen pro Polling-Intervall einstellen. Standardmäßig ist dieser Wert auf 0 gesetzt, was bedeutet, dass 4 Pakete in einem bestimmten Polling-Intervall gesendet werden. Setzen Sie einen Wert zwischen 1 und 8, der der tatsächlichen Anzahl der Pakete entspricht.

13.1.6.3 Broadcast-Einstellungen



Wenn die NTP-Zeit im Broadcast-Modus in einem lokalen Netzwerk verteilt werden soll, können Sie in diesem Menü eine gültige Broadcast-Adresse eingeben. Bitte beachten Sie: Ab der NTP4-Version muss der Broadcast-Modus immer mit Authentifizierung verwendet werden.

Broadcast Addresse:
Hier muss eine gültige Broadcast-Adresse eines lokalen Netzwerks eingegeben werden, mit dem der LANTIME verbunden ist.

Broadcast Intervall:
Das Intervall, in dem der Server die NTP-Pakete an die konfigurierte Broadcast-Adresse sendet.

Symmetrische Schlüssel:
In diesem Feld können Sie die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit den NTP-Clients verwendet werden soll.

Folgendes muss beachtet werden, damit die Authentifizierung funktioniert:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Untermenü „NTP → NTP Symmetric Keys“ auf der NTP-Seite bearbeiten.

b) Zusätzlich müssen Sie die ID in das Feld „Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ eingeben.

c) Auf dem NTP-Client muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Im Folgenden finden Sie einen Auszug aus der NTP-Konfiguration eines Clients, der als Broadcast-Client mit Authentifizierung konfiguriert ist:

```
keys /etc/ntp.key
# Pfad zur NTP-Schlüsseldatei

trustedkey 1
# Die Schlüssel-ID, die für die Authentifizierung verwendet wird.

broadcastclient
# Dieser Client arbeitet als Broadcast-Client.
```

13.1.6.4 NTP Multicast und Manycast

13.1.6.5 NTP-Multicast

NTP Multicast bietet die Möglichkeit, die Zeit durch Multicast im Netzwerk zu verteilen. Die Internet Assigned Numbers Authority (IANA) hat exklusiv die Multicast-IP-Adresse 224.0.1.1.1 für NTP vergeben. Daher wird empfohlen, diese Adresse als Multicast-Adresse zu verwenden. Es können aber auch andere Adressen des Multicast-Adressraums eingestellt werden.

Der Multicast-Adressraum sieht wie folgt aus:

```
Ipv4: 224.0.0.0 -> 239.255.255.255
Ipv6: Jede FF00::/8 Adresse
```

Multicast Adresse: Hier muss eine korrekte Multicast-Adresse eingegeben werden.

Broadcast Intervall: Das Intervall, in dem der Server die NTP-Pakete an die konfigurierte Broadcast-Adresse sendet.

TTL: Der konfigurierte TimeToLive (TTL)-Wert bestimmt, wie viele Hops NTP-Pakete im Netzwerk passieren können. Jeder Netzwerk-Hop reduziert diesen Wert um 1, und wenn der Wert Null erreicht, wird das Netzwerkpaket gelöscht.

Symmetrische Schlüssel: Für NTP Multicast wird eine Authentifizierung empfohlen, ist aber nicht zwingend erforderlich. Wenn die Authentifizierung jedoch auf der Serverseite konfiguriert ist, ist es auch auf der Client-Seite notwendig, dies zu tun.

Im Feld „Symmetrische Schlüssel“ können Sie daher die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit den NTP-Clients verwendet werden soll.

Folgendes muss beachtet werden, damit die Authentifizierung funktioniert:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Untermenü „NTP → NTP Symmetric Keys“ auf der NTP-Seite bearbeiten.

b) Zusätzlich müssen Sie die ID in das Feld „Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ eingeben.

c) Auf dem NTP-Client muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Im Folgenden finden Sie einen Auszug aus der NTP-Konfiguration eines Clients, der als Multicast-Client mit Authentifizierung konfiguriert ist:

```
keys /etc/ntp.key                  # Pfad zur NPT-Schlüsseldatei
trustedkey 1                       # Die Schlüssel-ID, die für die Authentifizierung verwendet wird.
multicastclient 224.0.1.1 key 1    # Der Client hört auf die Multicast-Adresse 224.0.1.1.1 und
                                   # verwendet den Schlüssel mit der ID 1 zur Authentifizierung.
```

13.1.6.6 NTP-Manycast

NTP Manycast beschreibt die Möglichkeit, dass ein oder mehrere NTP-Server hinter einer Multicast-Adresse stehen. Im Gegensatz zur Multicast-Methode senden die Server jedoch keine NTP-Pakete periodisch an diese Mutlicast-IP. Die Manycast-Funktion ist viel mehr eine Methode, um den NTP-Dienst eines anfragenden Clients automatisch neu zu konfigurieren. Der NTP-Dienst des Clients wählt automatisch bis zu 3 Server aus, die für ihn „am besten" zu sein scheinen. Der NTP-Dienst konfiguriert sich dann selbstständig neu und stellt eine Unicast-Kommunikation mit diesen Servern her. Wie beim Multicasting wird empfohlen, Authentifizierungsmethoden zu verwenden.

Manycast aktivieren: Aktiviert das Manycast-Feature.

Manycast Adresse: Adressfeld zur Eingabe der Manycast-Adresse (Mutlicast-Adressraum)

Der Multicast-Adressbereich ist wie folgt:

```
Ipv4: 224.0.0.0 -> 239.255.255.255
Ipv6: Jede FF00::/8 Adresse
```

Symmetrische Schlüssel: Für NTP Manycast wird eine Schlüsselmethode zur Authentifizierung empfohlen, ist aber nicht zwingend erforderlich. Wenn die Authentifizierungsmethode jedoch auf der Serverseite konfiguriert ist, ist es notwendig, dies auch auf der Client-Seite zu tun.

Im Feld „Symmetrische Schlüssel" können Sie daher die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit den NTP-Clients verwendet werden soll.

Folgendes muss beachtet werden, damit die Authentifizierung funktioniert:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Submenü „NTP → NTP Symmetric Keys" im NTP-Menü bearbeiten.

b) Zusätzlich müssen Sie die ID in das Feld „Vertrauenswürdige Schlüssel" unter „NTP → Allgemeine Einstellungen" eingeben. .

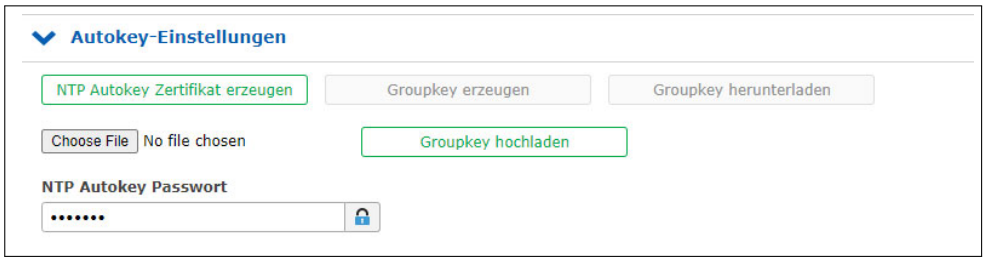
c) Auf dem NTP-Client muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Im Folgenden finden Sie einen Auszug aus der NTP-Konfiguration eines Clients,
der als Multicast-Client mit Authentifizierung konfiguriert ist:

```
keys /etc/ntp.key                 # Pfad zur NPT-Schlüsseldatei
trustedkey 1                      # Die Schlüssel-ID, welche für die Authentifizierung verwendet wird.
manycastclient 224.0.1.2 key 1    # Der Client hört auf die Multicast-Adresse 224.0.1.2 und verwendet
                                  # den Schlüssel mit der ID 1 zur Authentifizierung.
```

13.1.6.7 NTP Autokey Einstellungen

NTP-Version 4 unterstützt neben den symmetrischen Schlüsseln zusätzlich noch das sogenannte Autokey-Verfahren. Die Echtheit der empfangenen Zeit auf den NTP-Clients wird durch symmetrische Schlüssel sehr gut sichergestellt. Allerdings ist für eine höhere Sicherheit der periodische Austausch der verwendeten Schlüssel nötig, um einen Schutz, z.B. vor Replay-Attacken (d.h. Angriffen, bei denen aufgezeichneter Netzwerkverkehr einfach noch einmal abgespielt wird), zu erreichen.



Bei Netzwerken mit sehr vielen Clients kann dieses Austauschen der symmetrischen Schlüssel allerdings mit sehr viel Aufwand verbunden sein, weil auf jedem Client die Schlüssel für den/die NTP Server ausgetauscht werden müssen. Aus diesem Grund wurde von den NTP Entwicklern das Autokey-Verfahren eingeführt, das mit einer Kombination aus Gruppenschlüsseln (group keys) und öffentlichen Schlüsseln (public keys) arbeitet. Alle NTP Clients können somit die Zeitangaben, die sie von Servern ihrer eigenen Autokey-Gruppe erhalten, auf Echtheit überprüfen.

Beim Autokey-Verfahren werden sogenannte sichere Gruppen (secure groups) gebildet, in denen NTP Server und Clients zusammengefasst sind. Es gibt drei verschiedene Typen von Mitgliedern in einer solchen Gruppe:

a) Trusted Host
Ein oder mehrere vertrauenswürdige NTP Server. Um diesen Status zu erhalten, muss der Server ein als „Trusted“ gekennzeichnetes selbst-signiertes Zertifikat besitzen. Er sollte auf dem niedrigsten Stratum Level der Gruppe operieren.

b) Host
Ein oder mehrere NTP Server, die kein „Trusted“-Zertifikat besitzen, sondern nur ein selbstsigniertes Zertifikat (ohne die „Trusted“-Kennzeichnung).

c) Client
Ein oder mehrere NTP-Client-Systeme, die im Gegensatz zu den beiden erstgenannten Typen die Zeit lediglich empfangen und nicht in der Gruppe weiterverteilen. Alle Mitglieder der Gruppe (Trusted Hosts, Hosts und Clients) müssen im Besitz des gleichen Gruppenschlüssels sein. Der Gruppenschlüssel wird von einer Trusted Authority (TA) generiert und muss dann manuell auf alle Gruppenmitglieder verteilt werden (auf einem sicheren Weg, z.B. mittels scp). Die Rolle der TA kann ein Trusted Host in der Gruppe übernehmen (zum Beispiel ein LANTIME), es ist aber auch ohne Probleme möglich, den Gruppenschlüssel von einem nicht der Gruppe zugehörigen TA-Host erzeugen zu lassen.

Die verwendeten Public Keys können auf den Trusted Hosts der Gruppe periodisch manuell neu erzeugt werden (das ist sowohl im Webinterface als auch über das CLI-Setupprogramm möglich, über den Punkt „Generate new NTP public key“ im Bereich „NTP Autokey“ auf der Seite „Security Management“) und damit dann automatisch an alle anderen Mitglieder der Gruppe verteilt werden. Der Gruppenschlüssel bleibt gleich und somit entfällt das manuelle Update von Schlüsseln für alle Gruppenmitglieder.

Ein LANTIME kann in einer solchen Autokey-Gruppe sowohl TA und Trusted Host als auch einfacher Host sein. Um den LANTIME als TA und Trusted Host zu konfigurieren, schalten Sie das Autokey-Verfahren ein und initialisieren Sie per HTTPS-Webinterface den Gruppenschlüssel („Generate groupkey“). Dafür ist ein Crypto-Passwort nötig, das Sie ebenfalls im Webinterface ändern können. Den so erzeugten Gruppenschlüssel müssen Sie dann vom LANTIME herunterladen (z.B. über das HTTPS-Webinterface) und dann auf alle Clients und weiteren NTP Server der Gruppe kopieren (und diese Systeme ebenfalls für die Verwendung von Autokey konfigurieren).

Die ntp.conf aller Gruppenmitglieder muss folgende Zeilen enthalten:

```
crypto pw cryptosecret
keysdir /etc/ntp/
```

Dabei ist „cryptosecret“ in diesem Fall das Crypto-Passwort, das zum Erstellen des Group Keys und aller Public Keys verwendet wurde. Bitte beachten Sie, dass das Crypto-Passwort im Klartext in der ntp.conf steht und somit auf Nicht-LANTIME-Systemen sichergestellt sein sollte, dass nur „root“ diese Datei einsehen kann. Die Clients müssen zusätzlich noch den Eintrag der verwendeten NTP-Server ergänzen, um eine Nutzung von Autokey in Verbindung mit diesen Servern einzuschalten. Das sieht z.B. so aus:

```
server time.meinberg.de autokey version 4
server time2.meinberg.de
```

In diesem Beispiel wird der NTP Server time.meinberg.de mit Autokey verwendet, während time2.meinberg.de ohne jegliche Überprüfung der Echtheit der Zeit akzeptiert wird.

Möchten Sie den LANTIME zwar als Trusted Host verwenden, aber eine andere TA nutzen, dann erzeugen Sie mithilfe dieser Trusted Authority einen Gruppenschlüssel und binden ihn z.B. mithilfe des Webinterfaces auf Ihrem LANTIME ein (im Menüpunkt „NTP“ im Bereich „NTP Autokey“ den Menüpunkt „Upload Groupkey“).

Wenn Sie den LANTIME als einfachen NTP Server (nicht „trusted“) verwenden möchten, dann müssen Sie den Gruppenschlüssel Ihrer Gruppe hochladen („NTP“ -> “NTP Autokey“ -> “Upload Groupkey“) und ein eigenes, selbstsigniertes Zertifkat erzeugen (ohne es als „Trusted“ zu markieren). Da beim Generieren eines Zertifikats über das Webinterface oder das CLI-Setupprogramm grundsätzlich immer als „Trusted“ markierte Zertifikate erstellt werden, müssen Sie zum Erstellen von Zertifikaten ohne „Trusted“-Merkmal das Programm ntp-keygen manuell auf dem LANTIME aufrufen (in einer SSH-Sitzung):

```
LantimeGpsV4:/etc/ntp # ntp-keygen -q cryptosecret
```

Anschließend müssen die neu generierten ntpkeys manuell auf die Flash Disk kopiert werden:

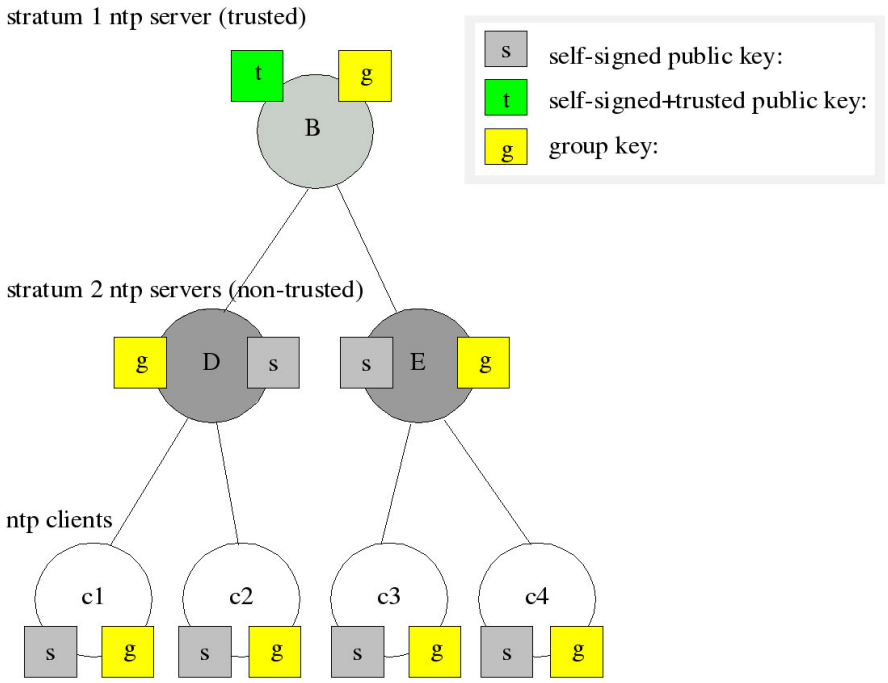
```
cp /etc/ntp/ntpkey_*   /mnt/flash/config/ntp/uploaded_groupkeys
```

Auch hier ist „cryptosecret“ wieder das verwendete Crypto-Passwort, das mit dem Crypto-Passwort in der ntp.conf übereinstimmen muss.

Eine detaillierte Anleitung zu ntp-keygen finden Sie auf der NTP-Homepage:
http://www.ntp.org

Beispiel:

Diese Autokey-Gruppe besteht aus einem Stratum-1-Server (B) sowie zwei Stratum-2-Servern (D, E) und mehreren Clients (im Schaubild sind 4 Clients abgebildet, c1 - c4). B ist der Trusted Host der Gruppe. Er besitzt den Gruppenschlüssel sowie ein als „Trusted" gekennzeichnetes, selbstsigniertes Zertifikat.

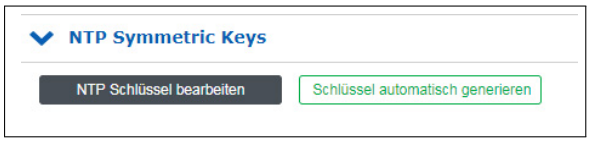


D und E sind NTP Server, die als Hosts der Gruppe nicht Trusted sind. Sie besitzen den Gruppenschlüssel und ein selbstsigniertes Zertifikat (das nicht als „Trusted" markiert wurde). Die Clients besitzen jeweils den Gruppenschlüssel und ebenfalls ein selbstsigniertes Zertifikat.

Um die gesamte Gruppe mit neuen Schlüsseln zu versorgen, muss lediglich auf B ein neuer „t"-Schlüssel generiert werden. Er wird dann automatisch an D und E verteilt, die dann gegenüber den Clients eine ununterbrochene Kette von Zertifikaten bis zu einem Trusted Host nachweisen können und somit als glaubwürdig eingestuft werden.

Mehr über die technischen Hintergründe und genauen Abläufe des Autokey-Verfahrens können Sie auf der NTP-Homepage http://www.ntp.org nachlesen.

13.1.6.8 NTP Symmetrische Schlüssel



Seit der NTP-Version 3 bietet NTP eine Authentifizierungsmethode mit symmetrischen Schlüsseln an. Mit der Schaltfläche „NTP Schlüssel bearbeiten“ kann die NTP-Schlüsseldatei des Servers bearbeitet werden. Bei der Auslieferung des Servers enthält die Datei einen Beispielschlüssel. Mit der Schaltfläche „Schlüssel automatisch generieren“ können Schlüssel automatisch generiert werden.

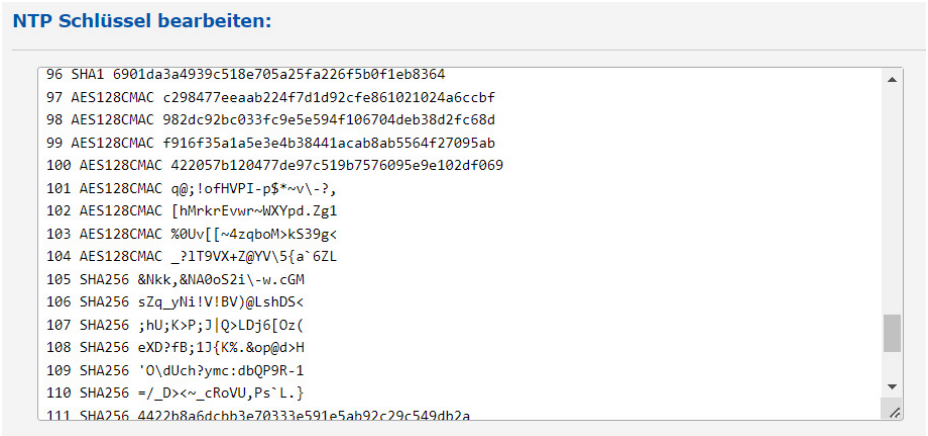


Abb.: Menü „NTP → NTP Symmetric Keys → NTP Schlüssel bearbeiten“

Achtung:
Wenn bereits symmetrische Schlüssel im Einsatz sind und beibehalten werden sollen, muss der Inhalt dieser Datei zwingend zwischengespeichert werden, bevor ein neuer Satz automatisch generiert wird. Der Inhalt der „alten“ Datei muss danach zusammen mit den neuen Schlüsseln wieder in das Feld NTP Schlüssel bearbeiten eingesetzt werden.

Im Folgenden finden Sie einen repräsentativen Auszug aus einer NTP-Schlüsseldatei:

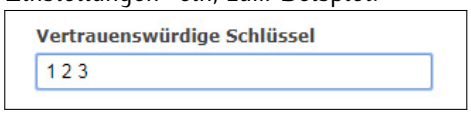
1	MD5	BtdW/<gj2*2M;!'~qAIN	# MD5 Key
2	SHA1	094c533b614d9e4bcb6e18a97a7b0e4d459025bd	# SHA1 Key
3	SHA256	bb48079a17b370fb0ae48bc1a09d5e0ab1ce59fc	# SHA256 Key
4	SHA512	56b98e4d4f57d415bebbb1a0ff72c625a57d865c	# SHA512 Key
5	AES128CMAC	02eb9a63710dda360d181d9582056a504d965700	# AES128-CMAC Key

Die erste Spalte enthält eine eindeutige Schlüssel-ID (Wertebereich 1 - 65535). Die zweite Spalte enthält den Schlüsseltyp („MD5“ für einen MD5-Schlüssel, „SHA1“ für einen SHA1-Schlüssel, AES128CMAC für einen AES128-CMAC-Schlüssel usw.). Die dritte Spalte enthält die Schlüsselkette, die zwischen 1 und 40 Zeichen lang sein kann.

Wie richte ich die Authentifizierung zwischen einem LANTIME und meinen NTP-Clients ein?

1. Fügen Sie die zu verwendenden Schlüssel in die Schlüsseldatei des Servers ein (wie im Auszug aus einer NTP-Schlüsseldatei dargestellt).

2. Geben Sie die IDs dieser Schlüssel in das Feld „Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ ein, zum Beispiel:



3. Nachfolgend ein exemplarischer Auszug aus der NTP-Konfiguration eines Linux-Clients, der den Schlüssel mit der ID 2 zur Authentifizierung mit dem Server 192.168.100.1 und den Schlüssel mit der ID 3 zur Authentifizierung mit dem Server 192.168.100.2 verwendet:

```
keys /etc/ntp.keys # Pfad zur Schlüsseldatei
trustedkey 2 3 # IDs der zu vertrauenswürdigen Schlüssel

server 192.168.100.1 iburst minpoll 6 maxpoll 6 key 2
server 192.168.100.2 iburst minpoll 6 maxpoll 6 key 3
```

In diesem Fall muss die Schlüsseldatei des Clients die Schlüssel mit den IDs 2 und 3 enthalten, die mit den Schlüsseln des Servers identisch sein müssen.

13.1.6.9 NTP-Konfiguration

Achtung!

Die Bearbeitung der zusätzlichen NTP-Parameter erfordert fortgeschrittene Kenntnisse der Systemadministration und ist daher standardmäßig deaktiviert.

Um diese Option freizuschalten, muss im Konfigurations-Editor unter dem Menü „System → Dienste und Funktionen → Manuelle Konfiguration → Standard Konfiguration → Sonstige Konfiguration“ der Eintrag **DISABLE SCRIPT** auf *NO* gesetzt werden.

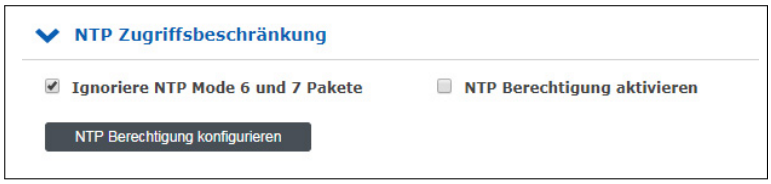
Diese Option kann auch über eine SSH-Verbindung bzw. über eine serielle Terminal-Verbindung auf gleiche Weise mit der Bearbeitung von */etc/mbg/msc.cfg* aktiviert oder deaktiviert werden.

Der Aufruf des Editors für die zusätzlichen NTP-Parameter erfordert immer Super-User-Berechtigungen, unabhängig von der Einstellung des **DISABLE SCRIPT**-Eintrags.

Die aktuelle NTP-Konfigurationsdatei wird über die Schaltfläche „NTP Konfigurationsdatei anzeigen“ angezeigt. Diese Datei wird bei jedem Neustart oder jeder Änderung der NTP-Konfiguration automatisch vom System erzeugt und kann nicht direkt bearbeitet werden.

Wenn zusätzliche Einstellungen für NTP (Authentication, Restriction ...) erforderlich sind, die nicht durch die vorhandenen Einstellungsmöglichkeiten auf der NTP-Seite abgedeckt sind, muss eine zusätzliche Konfigurationsdatei verwendet werden. Diese Datei kann über die Schaltfläche „Zusätzliche NTP Parameter bearbeiten“ bearbeitet und verwaltet werden. Bei jeder Erstellung der ‘ntp.conf‘ wird diese zusätzliche Datei automatisch an die ntp.conf angehängt.

13.1.6.10 NTP Zugriffsbeschränkungen



Das Menü „NTP Zugriffsbeschränkung“ kann verwendet werden, um den NTP-Zugang auf bestimmte IP-Adressen zu beschränken.

Um beispielsweise den Zugriff auf alle Adressen aus dem Subnetz 192.168.100.x zu ermöglichen, geben Sie unter IP-Adresse 192.168.100.0 und unter Netzmaske 255.255.255.255.0 ein. Der Zugriff kann auch für einzelne IP-Adressen erfolgen.

Um den eingeschränkten Zugang zu ermöglichen, muss die Option „NTP Berechtigung aktivieren“ aktiviert werden. Client-IP-Adressen, die nicht in den zulässigen IP-Adressbereichen enthalten sind, erhalten keine NTP-Antworten vom LANTIME.

Ignoriere NTP Mode 6 und 7 Pakete
Diese Einstellung bewirkt, dass interne Informationen, wie z.B. Zugriffsstatistiken, nicht von anderen NTP-fähigen Geräten im Netzwerk über den NTP-Dienst des Servers abgefragt werden können. Die Einstellung hat keinen Einfluss auf die Zeitsynchronisation zwischen NTP-Clients und dem Server.

NTP Berechtigung aktivieren
Durch Aktivieren dieser Einstellung werden die folgenden Zeilen in die NTP-Konfiguration des Servers geschrieben:

```
restrict default noquery
restrict -6 default noquery
restrict 127.0.0.1
restrict -6 ::1
```

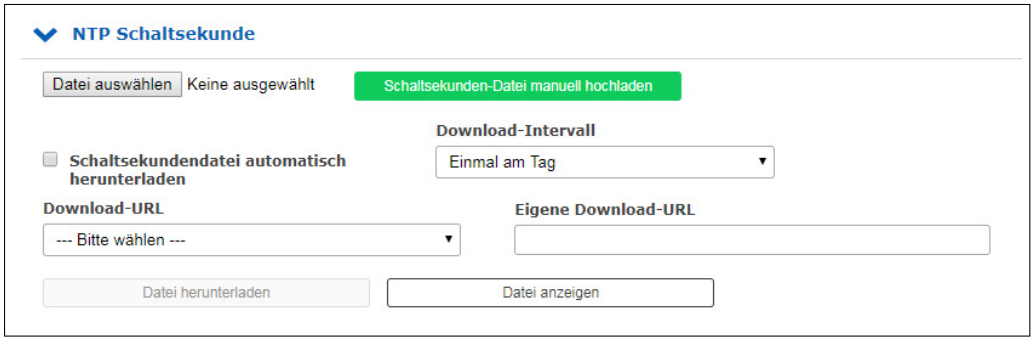
Diese Einstellungen bewirken, dass der Server nicht mehr auf NTP-Anfragen reagiert. Im Untermenü „NTP Berechtigungen konfigurieren“ können Sie eine „Whitelist“ von Client-IP-Adressen oder auch ganzen Subnetzen konfigurieren, deren Anfragen vom Server beantwortet werden dürfen.

13.1.6.11 NTP-Schaltsekunde

Die Zeitbasis für die meisten lokalen Zeitzonen der Welt heißt Coordinated Universal Time (UTC). Diese ist von mehreren Atomuhren abgeleitet, die in verschiedenen Ländern auf der ganzen Welt verteilt sind. Die Erdrotation ist nicht konstant und variiert im Laufe der Zeit, während die mittlere Erdrotationsgeschwindigkeit langsam abnimmt. Aus diesem Grund werden sogenannte „Schaltsekunden" in die UTC-Zeitskala eingefügt, die die UTC-Zeit mit der realen Erdrotation kompensieren. Eine Schaltsekunde wird immer um 23:59:59 (UTC) eingefügt, entweder am 31.12. oder 30.06. Andere Daten sind theoretisch möglich, wurden aber praktisch noch nicht verwendet.

Einige Protokolle oder Verfahren zur Übertragung der Zeitinformation, z. B. GNSS, NTP, PTP, DCF77 und IRIG, können Schaltsekunden voranstellen, um einem Empfänger die Möglichkeit zu geben, sich im Voraus auf eine Schaltsekunde vorzubereiten. Das GPS-Satellitensystem verteilt die Schaltsekundenansage sechs Monate vor dem Schaltsekunden-Ereignis. Meinberg LANTIME-Zeitserver mit GPS-Empfängern erhalten diese Mitteilung automatisch über das GPS-Signal. In der Protokolldatei des LANTIME wird der Eintrag „Leap Second Announced" (Schaltsekunde angekündigt) erzeugt, wenn das Datum der Schaltsekunde empfangen wird.

Andere Synchronisationsmethoden bieten diese Ankündigungsmöglichkeit nicht an, was zu einem zweiten Zeitsprung führen kann. Daher ist es notwendig, die NTP-Schaltsekundendatei auf diesen Systemen aktuell zu halten, damit um Mitternacht (UTC) eine Schaltsekunde korrekt eingefügt wird.



Im Menü „**NTP Schaltsekunde**" können Sie die aktuell gespeicherte Schaltsekundendatei ansehen, die Datei manuell hochladen oder einen automatischen Download von den folgenden Quellseiten konfigurieren:

Verfügbare Download-Quellen für Schaltsekundendateien:

1. NIST-Schaltsekundendatei:
   - ftp://ftp.boulder.nist.gov/pub/time/ (Verzeichnisauflistung)
   - ftp://ftp.boulder.nist.gov/pub/time/leap-seconds.list (aktuelle Schaltsekundendatei)

2. IERS (Earth Rotation and Reference Systems Service) Schaltsekundendatei:
   - https://hpiers.obspm.fr/iers/bul/bulc/ntp/ (Verzeichnisauflistung)
   - https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list (aktuelle Schaltsekundendatei)

3. Meinberg Schaltsekundendatei (Kopie der IERS-Schaltsekundendatei):
   - https://www.meinberg.de/download/ntp/leap-seconds.list
   - https://www.meinberg.de/download/ntp/leap_second

Hinweis:

Zusätzliche Informationen über das Einfügen einer Schaltsekunde finden Sie hier:

https://kb.meinbergglobal.com/kb/time_sync/ntp/leap_second_smearing/start

13.1.6.12 Spezielle Einstellungen

Zeitskala
Diese Einstellung konfiguriert die Zeitzone des NTP. Die Standardeinstellung ist „UTC“, da NTP standardmäßig auf UTC basiert und Standard NTP Clients UTC Zeit erwarten.

Die Einstellung „LOKALE ZEIT“ sollte nur gewählt werden, wenn der Zeitserver zur Synchronisation bestimmter Clients verwendet wird, die lokale Zeit benötigen. Wenn Sie hier „LOKALE ZEIT“ wählen, muss die genaue Zeitzone im Menü „System → Display“ konfiguriert werden.

Achtung: Die Verwendung von „LOKALE ZEIT“ ist ein Verstoß gegen den NTP-Standard und bewirkt, dass Standard-NTP-Clients fehlerhafte Zeiten akzeptieren und einen entsprechenden Zeitsprung durchführen.

Fester Offset (s)
Dieser Wert wird verwendet, um die Ausgabezeit des NTP-Dienstes zu manipulieren. Der konfigurierte Wert in Sekunden wird zur aktuellen Zeit addiert und bietet die Möglichkeit, die NTP-Zeit bei Bedarf zu manipulieren.

Achtung: Die Verwendung eines „Festen Offset“ ist eine Verletzung des NTP-Standards und bewirkt, dass Standard-NTP-Clients fehlerhafte Zeiten akzeptieren und einen entsprechenden Zeitsprung machen.

Max. Interner Offset (s)
Dieser Wert in Millisekunden gibt eine minimale Genauigkeit an, die der NTP-Dienst erreichen muss, bevor der Server beginnt, an die Clients Zeit zu verteilen. Die Eingabe eines Wertes von z.B. „1ms“ bedeutet, dass der Dienst wartet, bis die interne Uhr eine Genauigkeit von 1ms oder besser erreicht hat.

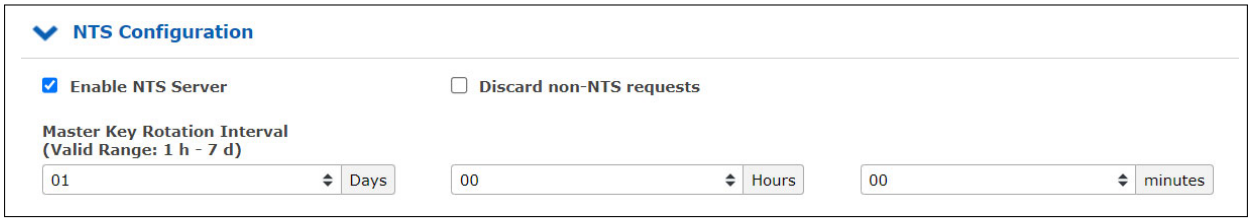
MRS Stratum durchreichen
Dieses Feature kommt nur zum Tragen, wenn man einen LANTIME mit MRS-Feature primär über NTP synchronisiert. Wenn „MRS Stratum durchreichen“ nicht aktiviert ist, präsentiert sich der LANTIME als Stratum 1 Server im Netzwerk. Wenn „MRS Stratum durchreichen“ aktiv ist, wird der Stratum des externen NTP Servers berücksichtigt. Ist der externe Server zum Beispiel ein Stratum 1 Server, würde sich der MRS LANTIME als Stratum 2 Server im Netzwerk darstellen.

13.1.6.13 NTS Konfiguration

Hinweis:

Diese Option ist auf LANTIME-Geräten mit CPU Modul-Typ C05F1 nicht verfügbar.

Voraussetzung für den NTS-Server-Modus ist die Konfiguration eines SSL-Zertifikats (siehe Kapitel Sicherstellung des Managements und Zertifikate).



NTS-Server aktivieren
Diese Einstellung aktiviert den NTS-Server-Modus. Damit wird auf dem LANTIME-Gerät zusätzlich zum NTP-Dienst ein NTS-KE-Server betrieben, welcher über eine TLS-gesicherte Verbindung Schlüsselmaterial an NTS-Clients bereitstellen kann.

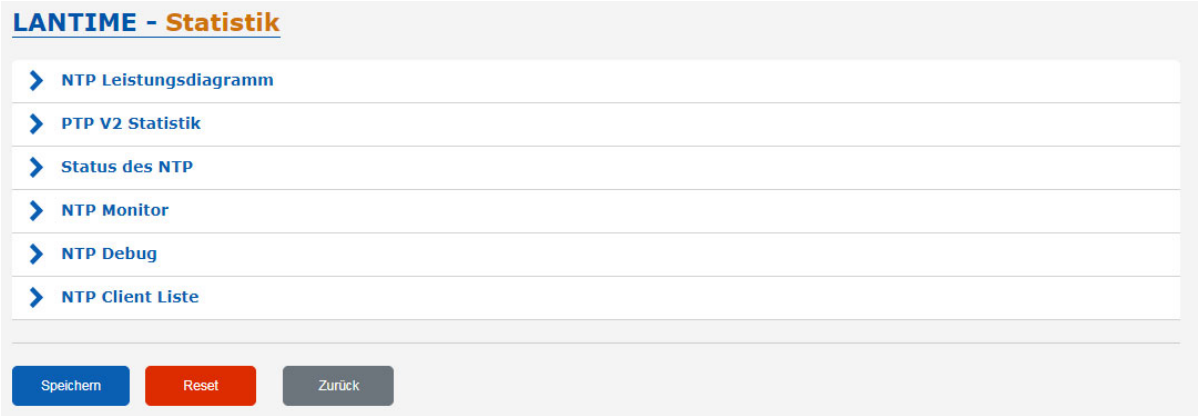
Da *NTPd* derzeit keine Unterstützung für NTS bietet, werden sämtliche NTP-Anfragen in diesem Fall von einer eigenen, NTS-fähigen NTP-Server-Implementierung beantwortet. Das Autokey-Verfahren wird von dieser Implementierung nicht unterstützt.

NTP-Anfragen, die nicht durch NTS gesichert sind, verwerfen
Diese Einstellung bewirkt, dass der NTS-Server alle NTP-Anfragen, die nicht durch NTS gesichert sind, verwirft und nicht beantwortet. Diese Einstellung hat keinen Effekt, wenn der NTS-Server nicht aktiviert ist.

Rotationsintervall des Master-Schlüssels
Diese Einstellung konfiguriert die Gültigkeitsdauer des internen, geheimen Master-Schlüssels, der für die Verschlüsselung von NTS Cookies verwendet wird. Nach Ablauf dieses Intervalls erzeugt der NTS-Server einen neuen Schlüssel, der fortan zum Einsatz kommt, und löscht den ältesten Schlüssel.

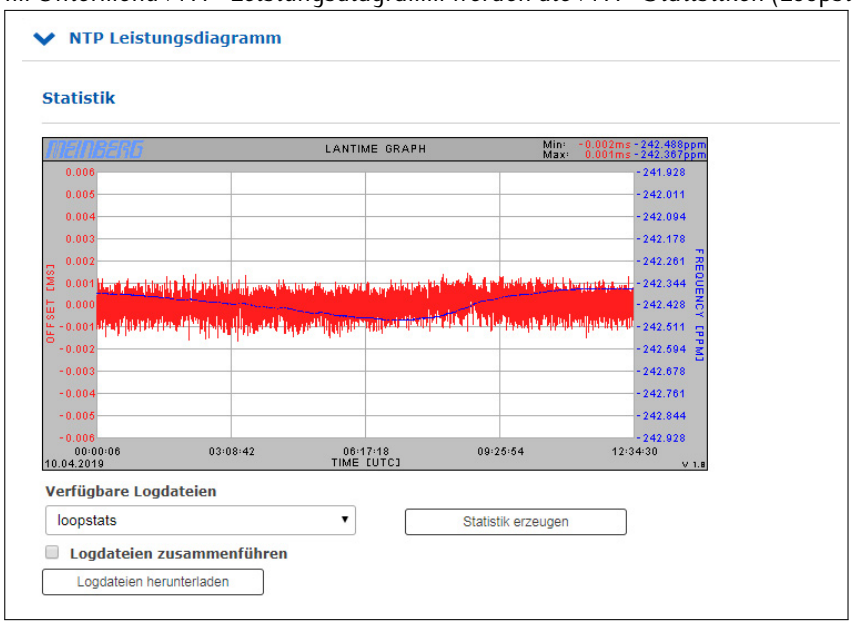
Der NTS-Server behält bis zu drei ältere Schlüssel, um Anfragen von NTS-Clients mit Cookies aus einem vorherigen Rotationsintervall weiterhin beantworten zu können.

13.1.6.14 NTP-Statistik



13.1.6.15 NTP Leistungsdiagramm

Im Untermenü NTP-Leistungsdiagramm werden die NTP-Statistiken (Loopstats) in Form eines Graphen dargestellt.



Die roten Linien und die primäre Y-Achse stellen den Versatz zwischen der Systemzeit und der NTP-Referenzzeitquelle (in ms) dar. Die blaue Linie und die sekundäre Y-Achse hingegen veranschaulichen die Frequenzanpassung des Oszillators, der vom ntpd (in PPM) auf der CPU aufgebaut ist, um die Systemzeit an die Referenzzeitquelle anzupassen.

Der minimale und maximale Messwert der Frequenzabweichung und der Offsets kann in der rechten oberen Ecke der Abbildung abgelesen werden.

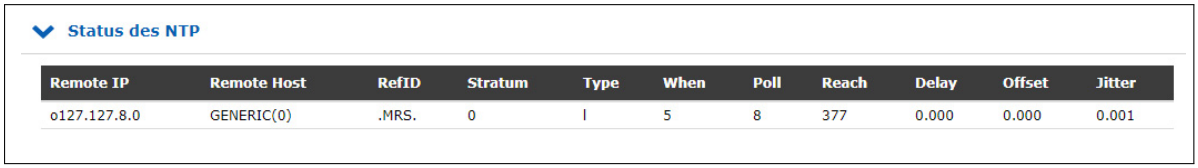
Verfügbare Logdateien:
Sie können die verfügbaren Protokolldaten über das Dropdown-Menü auswählen. Die ntpd erstellt für jeden Tag eine neue Loopstats-Datei.

Logdateien zusammenführen:
Nach dem Aktivieren des Kontrollkästchens und dem Klicken auf „Statistik erzeugen“ werden alle verfügbaren Protokolldateien zusammengeführt und als eine Grafik angezeigt.

13.1.6.16 NTP Status

Dieses Menü listet die aktuellen Zustände aller Referenzzeitquellen (Peers) auf, die dem NTP-Dienst zur Verfügung stehen. Für eingebaute Referenzuhren sowie normale externe NTPv4-Server entspricht dies der Ausgabe des Befehls *„ntpq -p“*. Für externe NTS-Server wird diese Anzeige um Statusinformationen von einem Chrony-Zeitdienst ergänzt. Daher kann es zu kleineren Unterschieden in der Darstellung kommen.

Das folgende Beispiel zeit die NTP-Status-Ausgabe eines LANTIME mit eingebauter GNSS-Referenzuhr und zwei konfigurierten externen NTP-Zeitservern:


Status des NTP

Remote IP	Remote Host	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
o127.127.8.0	GENERIC(0)	.MRS.	0	l	5	8	377	0.000	0.000	0.001

Remote IP:
IP-Adresse des NTP-Peers oder 127.127.x.x.x, wenn es sich um eine Hardware-Zeitreferenz handelt, z.B. eine Funkuhr oder einen GPS-Empfänger.

Eine Legende von Codes, die neben jeder IP-Adresse von NTP-Peers stehen, ist wie folgend:

‘*‘	Dieser Server ist für die Synchronisation ausgewählt.
‘o‘	Die Systemsynchronisation wird aus einem Puls pro Sekunde (PPS) Signal abgeleitet, entweder indirekt über den PPS-Referenztakttreiber oder direkt über eine Kernel-Schnittstelle.
‘+‘	Der Peer ist ein Kandidat für die Synchronisation.
‘-‘	Der Server ist nicht für die Synchronisation geeignet.
‘x‘	Der Server wird als Falseticker erkannt und ist nicht für die Synchronisation geeignet.
‘#‘	Der Server ist ein „Überlebender“, aber nicht unter den ersten sechs Servern.
‘	Der Peer wird als nicht erreichbar verworfen oder wird selbst mit diesem Server synchronisiert (Sync-Loop).

Remote Host:
Aufgelöster DNS-Name des NTP-Peers oder, für NTS-Server, Adresse des zugehörigen NTS-KE-Servers.

RefID:
Die Zeitreferenz des NTP-Peers.

Stratum:
Stratumwert des NTP-Peers.

Type:
(Typ des NTP-Peers)

l:	Lokaler Referenztaktgeber
b:	Broadcast oder Multicast
u:	Unicast
s:	symmetrischer Peer
a:	Manycast
c:	NTS-Server

When:
Wert in Sekunden. Zeigt an, wann der NTP-Peer zuletzt abgefragt wurde.

Poll:
Zeitraum in Sekunden. Gibt das Intervall an, in dem der NTP-Peer abgefragt wird.

Reach:
Oktalwert. Zeigt den Status der letzten 8 Abfragen an. Der Wert *„377“* (Binärwert *11111111*) bedeutet, dass die letzten 8 Abfragen erfolgreich waren.

Delay:
Wert in ms. Zeigt die Laufzeit des NTP-Pakets an.

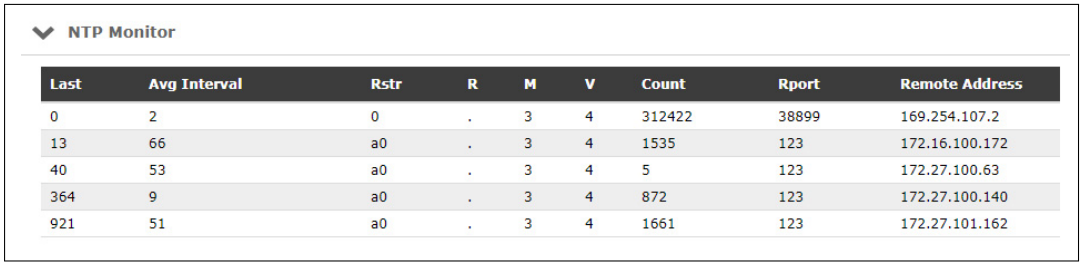
Offset:
Die NTP-Software vergleicht in regelmäßigen Abständen ihre eigene Systemzeit mit ihren Referenzzeitquellen. Dieser Prozess wird als „Polling“ bezeichnet. Nach jedem Polling-Vorgang wird die Paketauslösezeit ermittelt, berechnet und die aktuelle Zeitdifferenz („Offset“) berechnet und in Millisekunden angezeigt.

Jitter:
Die Paketübertragungszeit ändert sich mehr oder weniger je nach den Eigenschaften des Netzwerks während des „Pollings“ externer NTP-Quellen bei jedem Zeitvergleich, und auch der berechnete Zeitversatz variiert. Aus diesem Grund werden die Ergebnisse aufeinanderfolgender Zeitvergleiche gefiltert, indem gewichtete Mittelwerte für Paketlaufzeit und Zeitabstand berechnet werden. Die Abweichungen der einzelnen Werte von diesen Mittelwerten werden als „Jitter“ bezeichnet, und je höher der Jitterwert, desto ungenauer ist der berechnete Zeitabstand. Andererseits zeigt ein stetig zunehmender mittlerer Zeitversatz an, dass die Systemzeit von der Referenzzeit abweicht. Der Wert wird in Millisekunden angezeigt.

13.1.6.17 NTP Monitor

Das Untermenü „NTP Monlist“ listet alle NTP-Clients auf, die die LANTIME-Zeit über NTP abgefragt haben. Die Liste wird mit dem NTP Query-Tool erstellt und angezeigt. Der folgende ntpq-Befehl wird ausgegeben: *ntpq -c mrulist*

Weitere Informationen über das NTP Query-Tool finden Sie in der NTP-Dokumentation unter:
https://www.ntp.org/documentation/4.2.8-series/ntpq/


NTP Monitor

Last	Avg Interval	Rstr	R	M	V	Count	Rport	Remote Address
0	2	0	.	3	4	312422	38899	169.254.107.2
13	66	a0	.	3	4	1535	123	172.16.100.172
40	53	a0	.	3	4	5	123	172.27.100.63
364	9	a0	.	3	4	872	123	172.27.100.140
921	51	a0	.	3	4	1661	123	172.27.101.162

Last:
Zeit in Sekunden. Gibt an, wann der Client die Zeit vom LANTIME angefordert hat.

Avg Interval:
Intervall: Durchschnittliche Zeit in Sekunden zwischen zwei NTP-Anfragen.

Rstr:
Zeigt an, ob für diese Remote-IP Restrict Flags aktiv sind.

R:
Zeigt an, ob die „Rate Control“ aktiv ist oder nicht.

M:
NTP-Paket-Identifikation
0 → reserved
1 → symmetric active
2 → symmetric passive
3 → client
4 → server
5 → broadcast
6 → NTP control message
7 → reserved

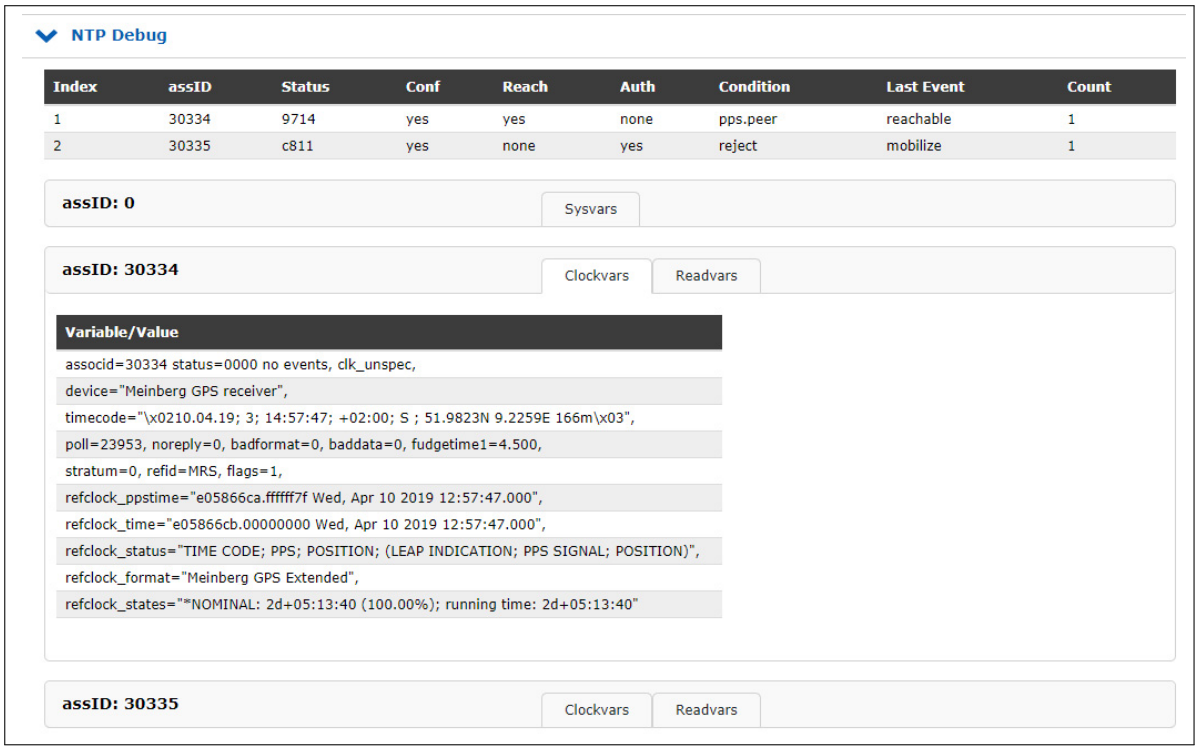
V:
NTP Version

Count:
Anzahl der von der entfernten Adresse empfangenen Pakete

Rport:
„Quell-Port“ des letzten empfangenen Pakets

Remote Address:
IP-Adresse des anfragenden Gerätes

13.1.6.18 NTP Debug



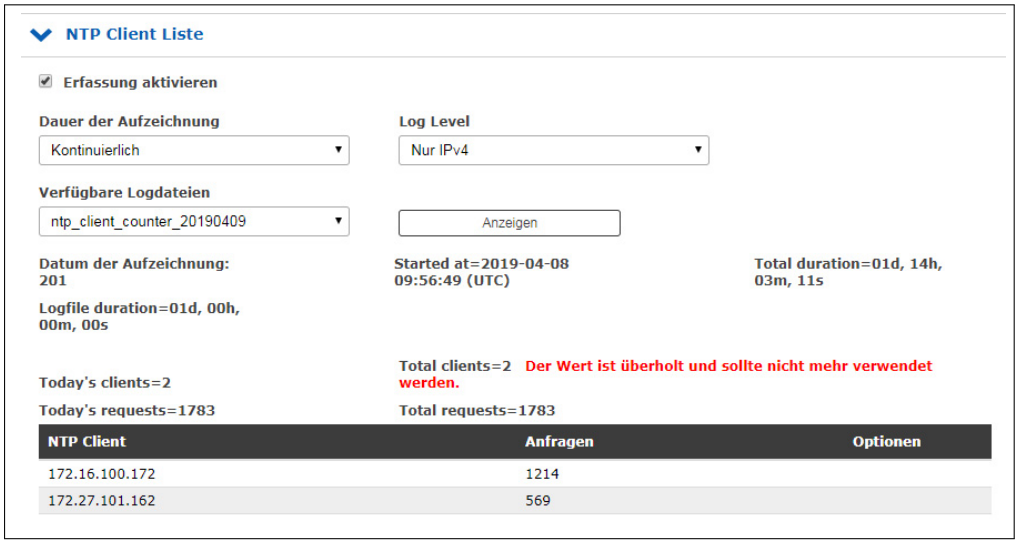
Das NTP Debug-Menü zeigt NTP-Debug-Informationen an, die vom LANTIME mit dem NTP Query-Tool (ntpq) abgefragt wurden. Das „ntpq“ wird mit den folgenden Parametern ausgeführt:

- „clockvar“
- „associations“
- „readvar“

Weitere Informationen über das Abfragetool finden Sie in der NTP-Dokumentation unter:
http://doc.ntp.org/current-stable/ntpq.html

13.1.6.19 NTP Client Liste

Zusätzlich zu den nativen NTP-Logging-Funktionen bietet der LANTIME die Möglichkeit, eine Liste aller NTP-Clients zu führen. Die Funktion ist standardmäßig ausgeschaltet und kann bei Bedarf aktiviert werden.



Erfassung aktivieren:
Aktiviert diese Funktion im LANTIME.

Dauer der Aufzeichnung:
Die Dauer, für die der LANTIME die Client-Liste führt. Bei der Konfiguration der kontinuierlichen Aufzeichnung werden alte Tagesstatistiken nach wenigen Tagen automatisch gelöscht um Platz zu sparen.

Log Level:
Legt fest, welche Version des IP-Protokolls berücksichtigt wird. Erhältlich sind IPv4, IPv6 oder beide Versionen in Kombination.

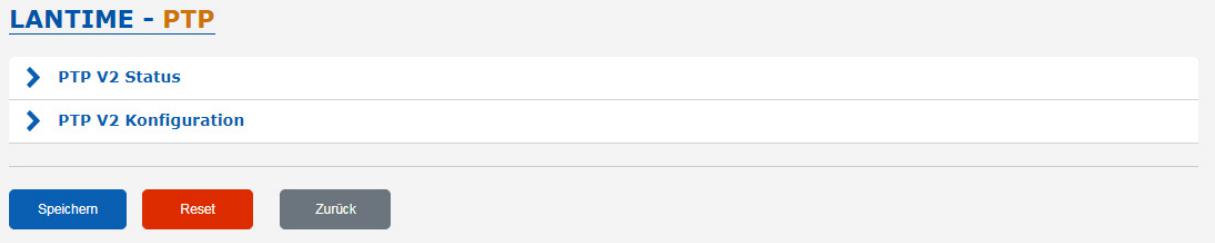
Verfügbare Protokolldateien:
Wenn die Client-Protokollierung aktiviert ist, werden an dieser Stelle Protokolldateien zur Anzeige bereitgestellt. Wählen Sie im Auswahlfeld die gewünschte Tagesstatistik aus und verwenden Sie die Schaltfläche „Anzeigen“, um die Statistik anzuzeigen. Sie erhalten dann eine entsprechende Client-Liste sowie weitere Statistiken.

NTP Client	Anfragen	Optionen
172.16.100.172	1214	Details
172.27.101.162	569	Details

Ein Klick auf Details zeigt Ihnen nun auch detaillierte Informationen über die empfangenen NTP-Pakete eines bestimmten Clients.

- Die Spalten 0-23 zeigen die Stunde des Tages an.
- Die 3 zusätzlichen Zeilen liefern Informationen darüber, ob das empfangene NTP-Paket den Modus 3, 4 oder einen anderen hat.
- Modus 3 → Client
- Modus 4 → Server

13.1.7 PTP



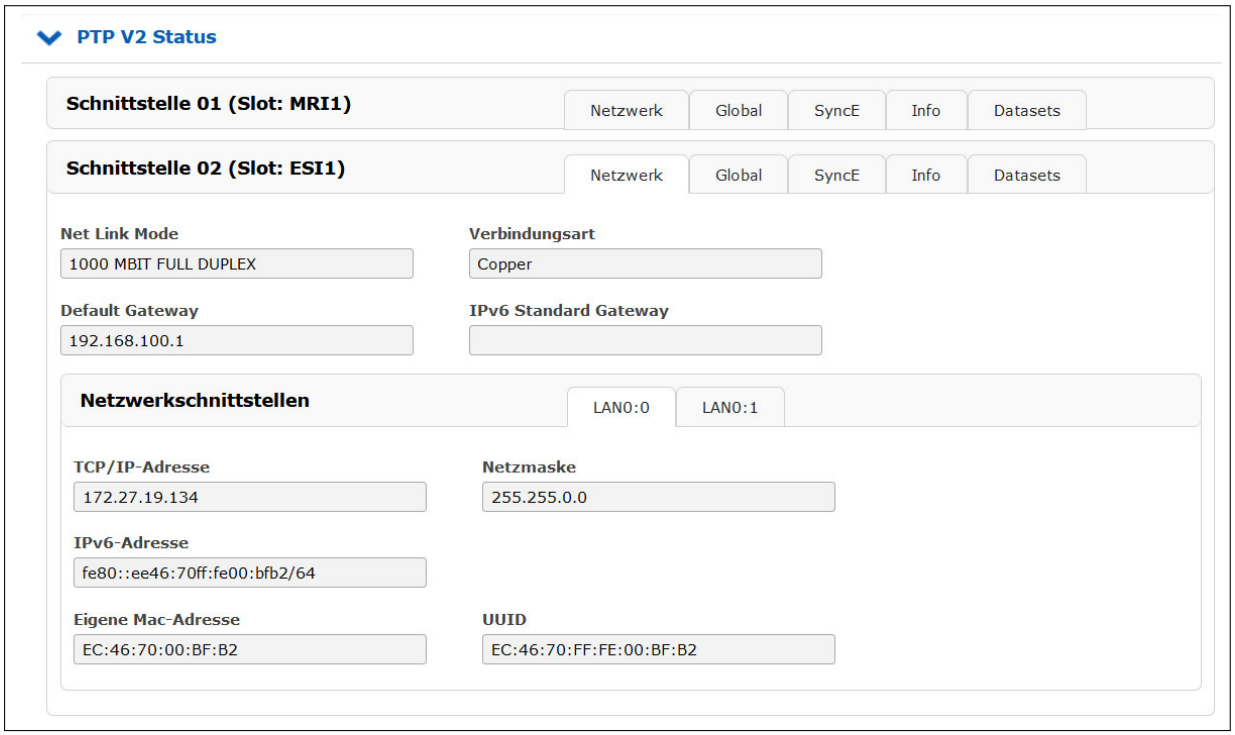
Alle Parameter für die korrekte PTP-Funktionalität können in einem übersichtlichen und benutzerfreundlichen Webinterface konfiguriert werden. Der konfigurierbare Parametersatz entspricht der aktuell im System installierten PTP-Kartenversion. Alle beschriebenen Funktionen sind mit HPS- und PSX-Modulen verfügbar. Für ältere TSU-Einheiten werden einige Untermenüs nicht angezeigt.

Wenn Sie sich am Web-GUI anmelden, folgen Sie bitte dem PTP-Dialog. Im Hauptmenü sind die folgenden Submenüs aufgelistet:

- PTP-Status
- PTP-Konfiguration

Wenn mehr als ein PTP-Modul (PTP-Ports) in das System integriert sind, können Status und Konfiguration für jeden Port separat bearbeitet werden. Alle physikalisch vorhandenen PTP-Schnittstellen werden im PTP-Menü aufglistet.

13.1.7.1 PTP Status Informationen



Der PTP-Statusdialog zeigt alle aktuellen Statusinformationen der ausgewählten PTP-Karte, entsprechend den im Submenü „PTP-Konfiguration“ vorgenommenen Einstellungen, an.

13.1.7.2 PTP Netzwerk-Status

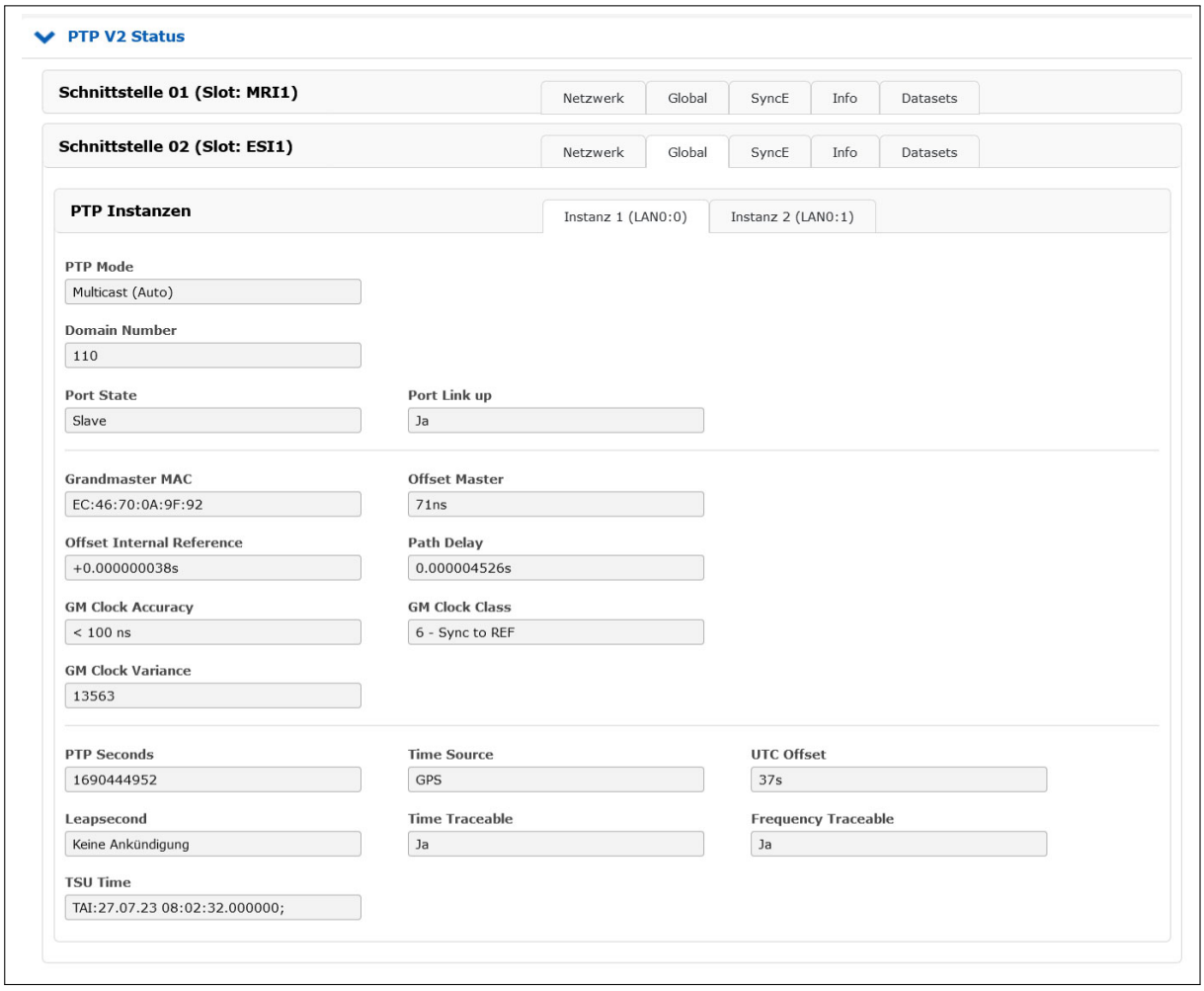
Mit der Registerkarte Netzwerk können Sie überprüfen, ob die Netzwerkeinstellungen der PTP-Karte gültig sind.

Lokale MAC-Adresse der PTP-Einheit
Wenn die PTP-Karte derzeit als Grandmaster (GM) betrieben wird, wird ihre lokale MAC-Adresse im Status der PTP-Slaves angezeigt, die sich derzeit mit diesem GM synchronisieren.

UUID
Die UUID ist die eindeutige Kennung des PTP-Ports, die auf der MAC-Adresse des PTP-Ports basiert.

13.1.7.3 PTP Globaler Status

Im Submenü „Global“ wird die aktuelle Betriebsart des ausgewählten PTP-Ports (Schnittstelle) angezeigt. Das Aussehen dieser Seite hängt vom Betriebsmodus der PTP-Karte ab. Verschiedene Zustände eines PTP-Ports sind möglich. Wenn das Gerät beispielsweise als PTP-Masterclock konfiguriert ist, zeigt diese Seite den Zustand „Master“ an. Bei MRS (Multi Reference Source) Geräten kann hier der PTP-Modus „Slave“ angezeigt werden.



Port-Status

Uninitialized Das PTP-Modul bootet, der Software-Daemon ist noch nicht gestartet, die IP-Adresse ist noch nicht vergeben.

Initializing In diesem Zustand initialisiert der Port seine Datensätze, Hardware und Kommunikationseinrichtungen.

Faulty Nicht in LANTIME-Systemen definiert.

Stopped Der PTP-Dienst wurde aufgrund einer fehlenden Verbindung auf dem PTP-Port oder einer nicht synchronisierten Masteruhr nach einem Start gestoppt oder nicht gestartet.

Disabled Nicht in LANTIME-Systemen definiert.

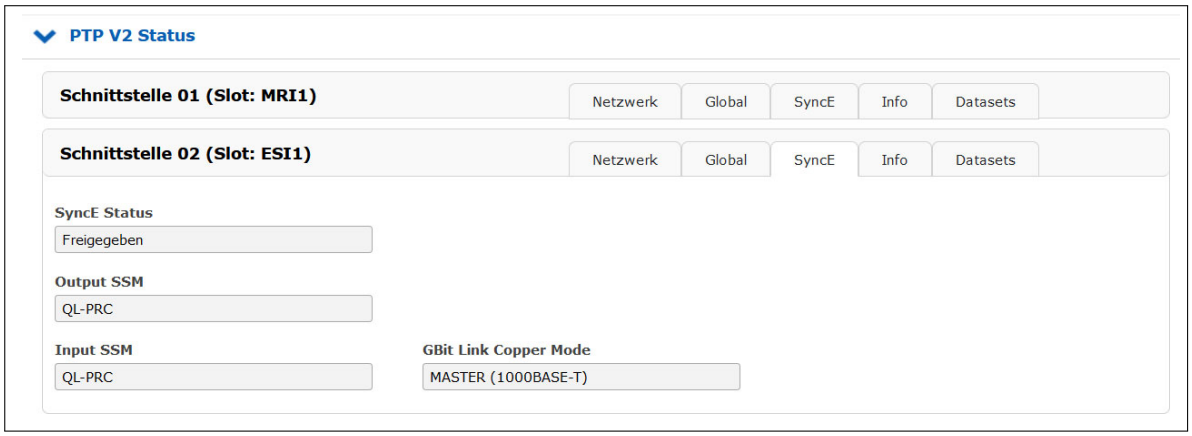
Listening Der Port wartet darauf, dass der *announceReceiptTimeout* abläuft oder dass er eine Announce-Nachricht von einem Master erhält.

preMaster Ein kurzer Übergangszustand, während der Port zum Master wird.

Master Der Port ist ein aktueller Master.

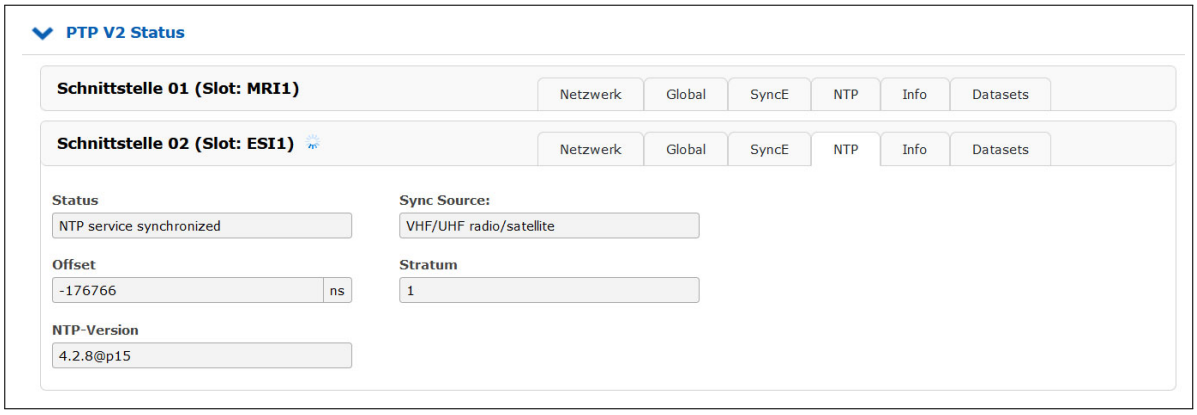
Passive	Der Port befindet sich im passiven Modus, d.h. es ist eine weitere Masterclock in der PTP-Domäne aktiv. Der Port kann in den Masterstatus wechseln, wenn er den BMCA (Best-Master-Clock-Algorithmus) aufgrund eines Ausfalls/Betriebsverschlechterung des aktuellen Masters gewinnt.
Uncalibrated	Der Port möchte ein Slave in der PTP-Domäne werden und hat bereits eine geeignete Grandmaster-Uhr gefunden. Die TSU wartet darauf, den „Path-Delay“ zu einem Grandmaster zu berechnen.
Slave	Der Port hat sich erfolgreich bei einem Master angemeldet und empfängt alle erwarteten Nachrichten. Es wurde auch erfolgreich der Path-Delay mit Hilfe von Delay-Request-Nachrichten gemessen.
Grandmaster MAC	Die MAC-Adresse des aktuellen Grandmasters.
Clock Accuracy	Die Taktgenauigkeit der aktiven Grandmaster-Uhr. Dieser Wert wird im Best-Master-Clock-Algorithmus verwendet, um den besten Master auszuwählen.
PTP Seconds	Aktueller Wert des reinen PTP-Sekundenwertes (Sekunden seit 1970).
UTC Offset	Dieser Wert stellt den aktuellen Offset zur PTP-Zeit basierend auf TAI zur Berechnung von UTC dar.
Domain Number	Eine PTP-Domäne ist eine logische Gruppe von PTP-Geräten innerhalb eines physikalischen Netzwerks, die durch die gleiche Domänennummer definiert ist. Slave-Geräte, die mit einem bestimmten Master im Netzwerk synchronisiert werden sollen, müssen mit einer eindeutigen Domänennummer konfiguriert werden, die derselbe wie für den Master ist.
Port Link up	Status 0: Der Port ist ausgefallen, überprüfen Sie die Link-LED und die Verbindung zum Link-Partner. Bei einem Defekt sollte die Netzwerkkarte ausgetauscht werden. Status 1: Der Port befindet sich im Normalbetrieb.
Delay Asymmetry	Wenn ein statischer Asymmetrieversatz im Netzwerk bekannt ist, kann dieser Wert (in ns) eingegeben werden, um ihn vor dem PTP-Start zu kompensieren.
Clock Class	PTP-Clock-Klasse des aktuell ausgewählten PTP-Grandmaster. Dieser Wert wird im Best-Master-Clock-Algorithmus verwendet.
Time Source	Der Typ einer Zeitquelle, welcher vom Grandmaster verwendet wird (nur informativ).
Leap Second	Schaltsekunden-Ankündigungs-Flag, die je nach GM-Implementierung bis zu 24 Stunden vor dem Schaltsekundenereignis eingerichtet wird.
TSU Time	Angezeigte Tageszeit in der ausgewählten PTP-Zeitskala.

13.1.7.4 SyncE Status



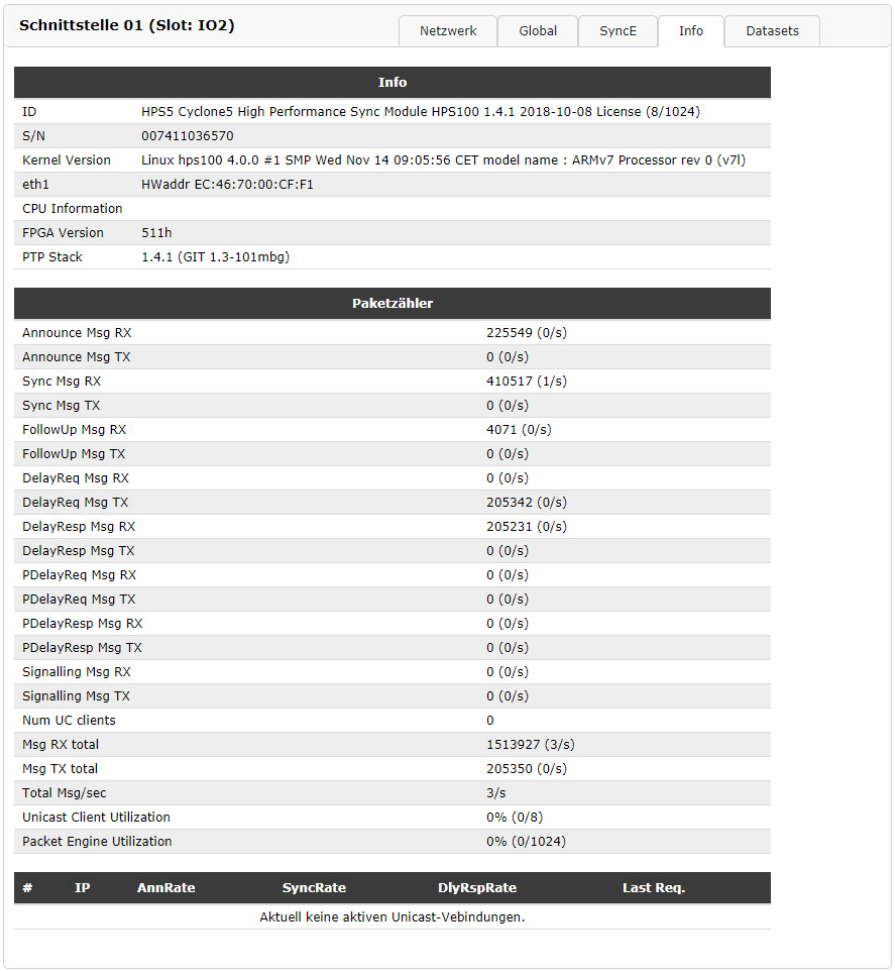
Sie können überprüfen, ob die SyncE-Funktionalität auf der Karte aktiviert ist oder nicht (falls vom PTP-Modul unterstützt).

13.1.7.5 Status NTP



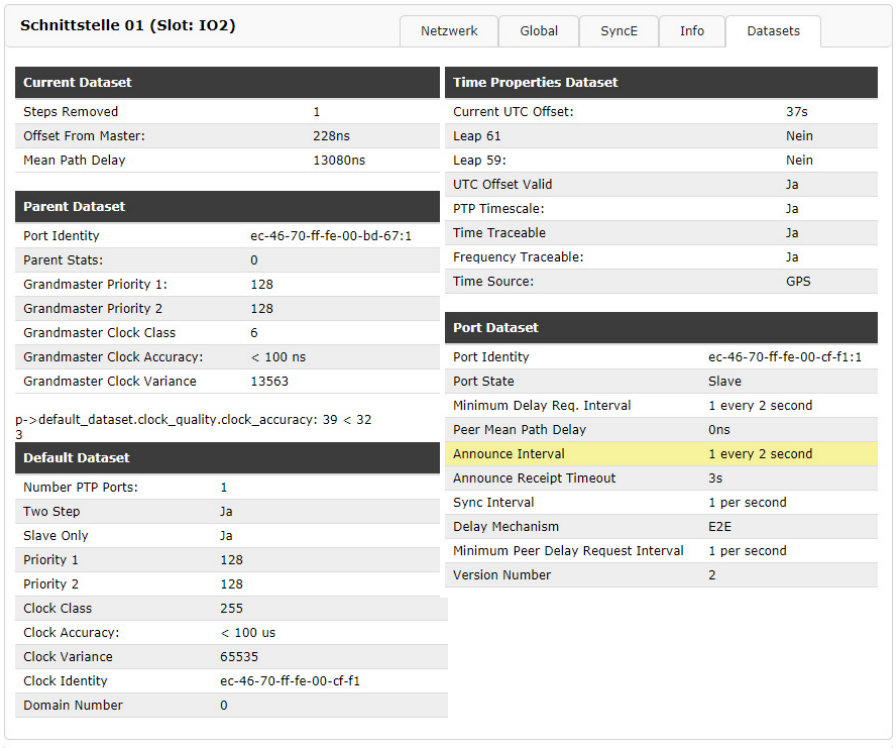
Der Reiter „NTP“ wird erst dann sichtbar, wenn zuvor im Menü „PTP V2 Konfiguration“ der **Software-NTP-Dienst** aktiviert wurde. Hier werden die Werte für Status (synchron oder nicht-synchron), Sync Source (z.B. der integrierte Empfänger), NTP-Offset vom Referenzempfänger (in Nanosekunden), der Stratum-Wert des Zeitservers und die verwendete NTP-Version angezeigt.

13.1.7.6 Menü PTP Status-Info



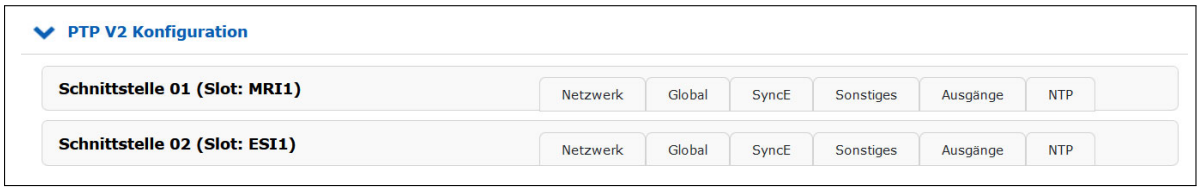
Unter diesem Menüpunkt finden Sie Informationen über das verwendete PTP-Modul, über die versendeten und empfangenen Pakete (Paketzähler) sowie Informationen über aktive Unicast-Verbindungen.

13.1.7.7 Menü PTP-Status Datasets



Clock Variance:
Eine logarithmisch skalierte Statistik, die den Jitter und die Wanderung des Taktoszillators über ein Sync-Nachrichtenintervall darstellt.

13.1.7.8 PTP-Konfigurationsmenü

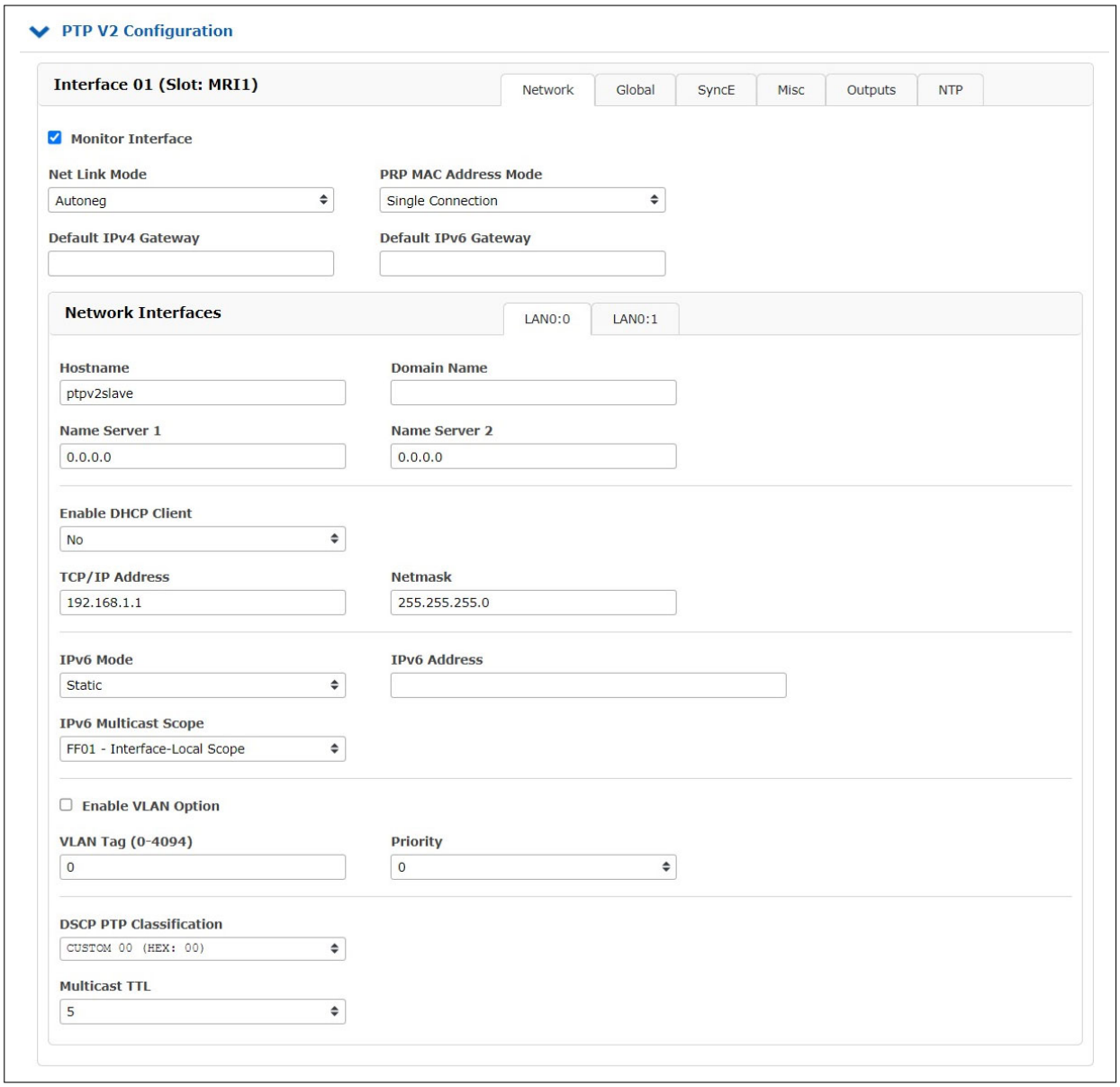


Alle im System verwendeten Parameter für den ordnungsgemäßen Betrieb jedes PTP-Ports (Schnittstelle) sollten entsprechend ihrer Funktion im PTP-Netzwerk separat konfiguriert werden. Wann immer eine Änderung übernommen werden soll, muss sie durch Bestätigen der Schaltfläche „Save Settings“ am Ende der Seite gespeichert werden.

Die Konfigurationsparameter sind in den Submenüs wie folgt gruppiert. Die mit * markierten Submenüs sind nur auf allen PTP-fähigen Modulen verfügbar, die mit ** markierten Registerkarten nur auf einem HPS- oder PSX-Modul.

- Netzwerk
- Global
- SyncE*
- Sonstiges*
- Ausgänge*
- NTP** (Software NTP-Dienst)

13.1.7.9 PTP-Netzwerkkonfiguration



Interface überwachen

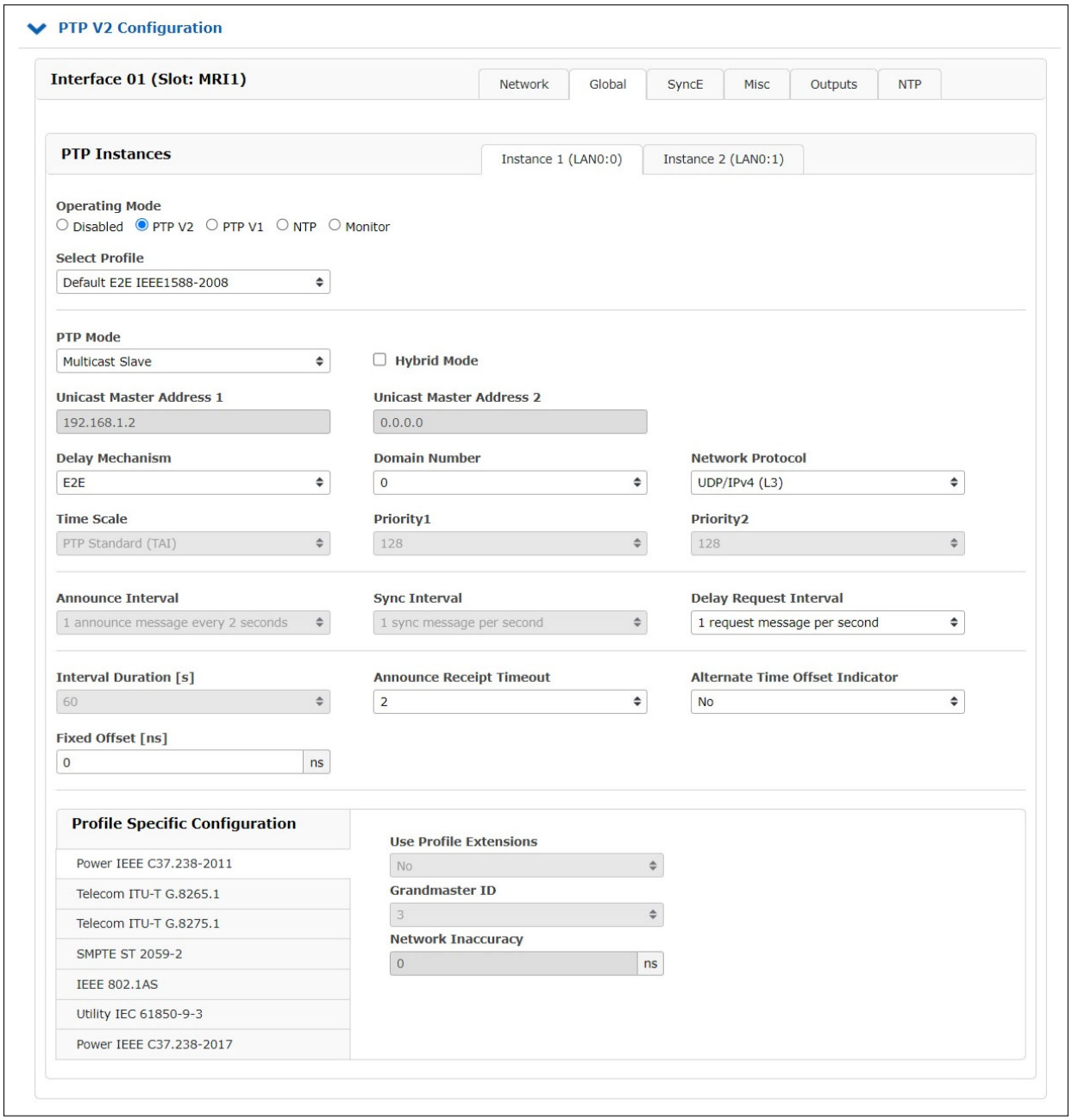
Überwachung des Verbindungsstatus des Netzwerkports. Sobald die ausgewählte PTP-Netzwerkverbindung eine Verbindung nicht mehr erkennt, löst dieser Zustand ein Ereignis „PTP Link Down“ aus. Dieses Ereignis wird im Menü „Benachrichtigung → Benachrichtigungsereignisse“ angezeigt.

Wenn das PTP-Modul nicht benötigt wird und somit nicht mit dem Netzwerk verbunden ist, kann das Kontrollkästchen „Interface überwachen“ deaktiviert werden. Es wird dann kein Fehlerereignis ausgelöst.

NET Link Mode	Auswählbare Werte sind: *Autonegotiation* *100 MBIT HALF DUPLEX* *100 MBIT FULL DUPLEX* *1000 MBIT HALF DUPLEX* *1000 MBIT FULL DUPLEX* *10000 MBIT FULL DUPLEX (nur mit PSX-Modul)*
MAC-Adresse im PRP-Mode	PRP ist ein redundantes Netzwerkprotokoll, welches dazu dient, die Verfügbarkeit eines Netzwerks zu sichern. PRP verwendet zwei voneinander unabhängige Pfade, um Datenpakete zu übertragen, so dass bei einem Ausfall eines Netzwerkpfades die Übertragung der Datenpakete weiterhin gewährleistet ist. Ein LANTIME mit zwei oder mehr PTP-Schnittstellen hat die Möglichkeit, als DAN zu arbeiten („Dual Attached Node" - ein Gerät, das an zwei unabhängige Netzwerke angeschlossen ist). PRP-Gruppen lassen sich im Menü „PTP → PTP V2 Konfiguration → Netzwerk" einstellen. Wählen Sie im Drop-Down-Menü „MAC-Adresse im PRP-Mode" für mindestens zwei Schnittstellen die gleiche PRP-Gruppe aus. **Hinweis:** Für eine PRP-Gruppe werden also mindestens zwei PTP-Module (HPS100) benötigt.
Hostname	Hostname, ein eindeutiges alphanumerisches Label, das den ausgewählten PTP-Port von anderen im Netzwerk unterscheidet, kann hier eingegeben werden.
Domainname	Der Domainname für die ausgewählte PTP-Schnittstelle kann zugewiesen werden.
Nameserver1	Nameserver 1 kann eingegeben werden, wenn er in einem Netzwerk verwendet wird.
Nameserver2	Nameserver 2 kann eingegeben werden, wenn er in einem Netzwerk verwendet wird.
DHCP-Client aktivieren	Aktivieren/deaktivieren des DHCP-Dienstes. Wenn ein DHCP-Client aktiviert ist, wird das Feld für die statische IP-Konfiguration deaktiviert. Das Gegenteil ist der Fall, wenn der DHCP-Client deaktiviert ist.
Zugewiesene DHCP-Adresse	Wenn ein DHCP-Dienst im Netzwerk gefunden wird, wird automatisch eine gültige IP für einen PTP-Port zugewiesen und hier angezeigt.
Zugewiesene Netzmaske	Wenn ein DHCP-Dienst im Netzwerk gefunden wird, wird automatisch eine gültige Netzmaske für einen PTP-Port zugewiesen.
Zugewiesener Gateway	Wenn ein DHCP-Dienst im Netzwerk gefunden wird, wird automatisch ein gültiges Gateway für einen PTP-Port zugewiesen.
TCP/IP-Adresse	Wenn der DHCP-Client deaktiviert ist, kann dieses Feld bearbeitet werden, um eine gültige statische IP-Adresse für die ausgewählte PTP-Schnittstelle zuzuweisen.
Netzmaske	Wenn der DHCP-Client deaktiviert ist, kann dieses Feld bearbeitet werden, um eine Netzmaske für die ausgewählte PTP-Schnittstelle zuzuweisen.
Default Gateway	Wenn der DHCP-Client deaktiviert ist, kann dieses Feld bearbeitet werden, um ein Standard-Gateway für die ausgewählte PTP-Schnittstelle zuzuweisen.
IPv6 Mode	IPv6-Adressierung über DHCPv6 / Statische Zuordnung / Router Advertisement sind verfügbar.
IPv6-Adresse	Ipv6 Adresse, die dem ausgewählten PTP-Port zugewiesen wurde. Wenn die Option

	„Static“ für den Ipv6-Modus aktiviert ist, kann in diesem Feld eine gültige statische IP-Adresse konfiguriert werden.
IPv6 Multicast Scope	Das Präfix von IPv6-Multicastadressen legt deren Umfang fest. Hier kann ein bestimmter Bereich für den Multicast-Modus ausgewählt werden.
VLAN-Funktion aktivieren	Aktivieren / Deaktivieren des Virtual LAN (IEEE 802.1Q) Dienstes auf der PTP-Schnittstelle.
VLAN-Tag (1-4094)	Ein 12-Bit-Wert, der eine VLAN-ID angibt, zu der ein PTP-Port gehört.
Priority	Werte 0 (Standard, niedrigste Priorität) bis 7 (höchste Priorität), mit denen der Netzwerkverkehr für verschiedene Datentypen priorisiert werden kann.
Disable SSH Service	Wenn diese Option aktiviert ist, wird der SSH-Zugang für diesen PTP-Port deaktiviert. Diese Auwahlmöglichkeit gibt es nur bei einem TSU-GbE-Modul.
DCSP PTP Klassifizierung	Differenzierter Service-Code-Point. Das ist ein QoS-Parameter im IP-Header des klassifizierten PTP-Pakets, um den Traffic zu priorisieren.
Multicast TTL	Time-To-Live. Standardmäßig wird der PTP-Multicast-Verkehr nicht geroutet und dieser Wert ist vom PTP-Standard als „1“ definiert. Hier kann jedoch eine benutzerdefinierte Konfiguration des TTL-Wertes eingegeben werden, um den Standardwert zu ändern.

13.1.7.10 PTP Globale Konfiguration

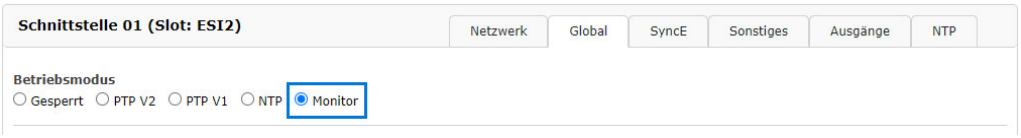


Betriebsmodus

PTP oder NTP
Wenn unterstützt ist es möglich, einen NTP-Dienst im Servermodus mit Hardware-Zeitstempel-Support auszuführen. In diesem Schritt wählen Sie zwischen PTP- und NTP-Modus. Es ist nicht möglich, beide Modi gleichzeitig auf einer TSU-Karte zu betreiben.

PTPv2 oder PTPv1 (nur HPS100 - Lizenz PL-C/D/E)
Die Karte kann im PTPv1-Modus betrieben werden, um als Kommunikationsschnittstelle zwischen PTPv1- und PTPv2-Netzelementen zu dienen.

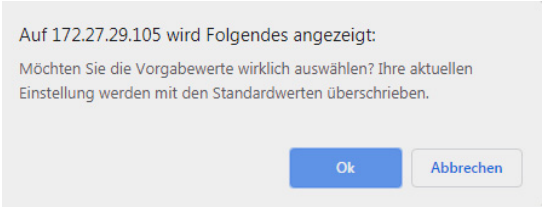
Monitor (nur HPS100 - Lizenz PL-D/E)



Um PTP-Netzwerkelemente zu überwachen und Statistiken zu erstellen, kann ein HPS100-Modul im Monitor-Modus betrieben werden. Nur wenn dieser Modus aktiviert ist, ist es möglich, PTP-Knoten im Netzwerk über das HPS100-Modul zu überwachen.

Aktuelles Profil
Der Benutzer kann zwischen vordefinierten PTP-Parametersätzen wählen, die in Profilen definiert sind, welche normalerweise in verschiedenen Branchen verwendet werden. Wenn die Standardeinstellung „Custom“ ausgewählt ist, kann der Benutzer jede beliebige Parameterkombination auswählen, die im Abschnitt „Globale Konfiguration“ verfügbar ist, sofern der PTP-Standard dies zulässt. Abhängig vom gewählten Profil stehen möglicherweise profilspezifische Parameter zur Verfügung, die Sie im Abschnitt „Profilspezifische Einstellungen“ unterhalb der Standard-PTP-Parameterbereiche finden.

Auf PTP-Karten werden derzeit zwölf verschiedene Voreinstellungssätze unterstützt:



Hinweis: Bei einem Wechsel auf ein anderes Profil werden Ihre aktuellen Einstellungen mit den Standardwerten des ausgewählten Profils überschrieben.

Beispiel: Bei der Auwahl des Profils Telecom ITU-T G.8275.1 wird SyncE automatisch aktiviert und der GBit Link Copper Modus im Reiter **SyncE** wird auf „Automatisch“ gesetzt.

Unicast Master / Slave Modus:

Telecom ITU-T G.8265.1

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “E2E“
- Network Prot: “Layer 3 (UDP/IPv4,v6)“

Telecom ITU-T G.8275.2

- Ann Msg Rate: 8/sec
- Sync Msg Rate: 128/sec
- Del Req Rate: 128/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “E2E“
- Network Prot: “Layer 3 (UDP/IPv4,v6)“

Unicast oder Multicast Master / Slave Modus:

Default E2E IEEE 1588-2008
Standardprofil mit End-to-End-Delay-Mechanismus gemäß der Norm IEEE 1588-2008, verfügbar im Multicast- und Unicast-Modus.

- Ann Msg Rate: 2 sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “E2E“
- Network Prot: “Layer 3 (UDP/IPv4,v6)“

SMPTE ST 2059-2

- Ann Msg Rate: 4/sec
- Sync Msg Rate: 8/sec
- Del Req Rate: 8/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “E2E“ or “P2P“
- Network Prot: “Layer 3 (UDP/IPv4,v6) or Layer 2 (IEEE 802.3)“

AES67 Media Profile

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 8/sec
- Del Req Rate: 8/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “E2E“ or “P2P“
- Network Prot: “Layer 3 (UDP/IPv4)“

Multicast Master / Slave Modus:

Custom P2P IEEE 1588-2008
Standardprofil mit P2P-Delay-Mmechanismus gemäß der Definition des Standards IEEE 1588-2008, verfügbar im Multicast-Modus.

- Ann Msg Rate: 2 sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"
- Network Prot: "Layer 3 (UDP/IPv4,v6) or Layer 2 (IEEE 802.3)"

Telecom ITU-T G.8275.1

- Ann Msg Rate: 8/sec
- Sync Msg Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot: "Layer 2 (IEEE 802.3)"

Power IEEE C37.238-2011

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"
- Network Prot: "Layer 2 (IEEE 802.3)"
- VLAN (802,1Q): enabled (VLAN ID:0, Prio:4)
- Power Profile: TLVs enabled

Power IEEE C37.238-2017

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “P2P or E2E“
- Network Prot: “Layer 3 (UDP/IPv4,v6) or Layer 2 (IEEE 802.3)“
- Power Profile: TLVs enabled

Utility IEC 61850-9-3

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “P2P“
- Network Prot: “Layer 2 (IEEE 802.3)“
- Power Profile: TLVs enabled

IEEE 802.1AS

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 8/sec
- Del Req Rate: 1/sec
- Priority 1: 248
- Priority 2: 248
- Delay Mech: “P2P“
- Network Prot: “Layer 2 (IEEE 802.3)“

DOCSIS 3.1

- Ann Msg Rate: 8/sec
- Sync Msg Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: “E2E“
- Network Prot: “Layer 2 (IEEE 802.3)“

PTP Mode:
Ein PTP-Port kann nur in einem Modus betrieben werden: Master oder Slave. Wenn der Modus ausgewählt ist, kann der Benutzer zwischen Multicast- oder Unicast-Only-Protokoll wählen. In der neuesten Firmware wird auch eine kombinierte Unicast-Multicast-Master Betriebsart unterstützt.

Hybrid-Mode:
In diesem Modus werden PTP-Nachrichten wie Sync, FollowUp und Announce im Multicast gesendet, während die DelayRequest- und DelayResponse-Nachrichten in Unicast gesendet werden.

Delay Mechanism:
Zwei Optionen sind möglich:

E2E (End-to-End): Verzögerungsmessnachrichten werden direkt von einem Slave an den Master (zwei Endknoten) gesendet.

P2P (Peer-to-Peer): Jedes Gerät (ein Peer) im Netzwerk tauscht Peer-Delay-Messages aus. Auf diese Weise kann jeder Knoten die Verzögerungen zwischen sich und seinem unmittelbar verbundenen Nachbarn im Auge behalten. Der P2P-Mechanismus kann nur in IEEE 1588-PTP-fähigen Netzwerken verwendet werden.

Domain Number:
Eine PTP-Domäne ist eine logische Gruppe von PTP-Geräten innerhalb eines physikalischen Netzwerks, die durch die gleiche Domänennummer definiert ist. Slave-Geräte, die mit einem bestimmten Master im Netzwerk synchronisiert werden sollen, müssen mit einer eindeutigen Domänennummer konfiguriert werden, der Master muss mit der selben Nummer konfiguriert werden.

Network Protocol:
Drei Optionen für das Netzwerkprotokoll sind möglich:

ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet-Frames mit MAC-Adressen von Slave und Master.
UDP/IPv4 oder UDP/IPv6 (Layer 3): User Data Protocol - eines der wichtigsten Protokolle für das Internet.

Timescale:
Zwei Optionen sind möglich:

PTP: Standardmäßig wird die TAI-Zeitskala im PTP-Timing verwendet. TAI ist eine lineare Zeitskala ohne Diskontinuitäten wie die eingefügten Schaltsekunden in der UTC-Zeitskala. Eine Zeiteinheit basiert auf der SI-Sekunde. Die TAI-Zeitskala begann am 1. Januar 1970 00:00:00 Uhr.

Arbitrary:
Ist Arbitrary ausgewählt, dann wird anstelle von TAI die UTC-Zeit über PTP verteilt. Die Timestamps in den PTP Nachrichten basieren dann auf UTC anstatt TAI. Darüber hinaus wird das UTC_OFFSET Feld in den Announce Messages von 37 (aktuelle Anzahl der Schaltsekunden Stand 12/2021) auf 0 gesetzt.

Priority 1:
Das Attribut wird bei der Ausführung des Best-Masterclock-Algorithmus (BMCA) verwendet. Niedrigere Werte haben Vorrang.

Konfigurierbarer Bereich: 0..255. Der Betrieb des BMCA wählt Uhren aus einem Satz mit einem niedrigeren Wert der Priorität 1 gegenüber Uhren aus einem Satz mit einem höheren Wert der „Priorität 1“.

Priority 2:
Das Attribut wird bei der Ausführung des BMCA verwendet. Niedrigere Werte tkae Priorität.

Konfigurierbarer Bereich: 0..255. Für den Fall, dass der Betrieb des BMCA die Uhren nicht nach den Werten basierend auf „Priority 1“, clockClass, clockAccuracy und scaledOffsetLogVariance ordnet, ermöglicht das „Priority 2“-Attribut die Erzeugung von bis zu 256 Prioritäten, die vor dem Tiebreaker ausgewertet werden. Der Tiebreaker basiert auf der clockIdentity. Die Werte clockClass, clockAccuracy und scaledOffsetLogVariance sind abhängig vom internen Zustand der Grandmaster-Clock und können nicht konfiguriert werden.

Nachrichten-Intervalle:
Geben Sie die Einstellungen für die PTP-Nachrichtenraten an.

Announce Interval:
Gibt die Rate für das Senden von „Announce-Messages“ zwischen Mastern an, um den aktuellen Grandmaster auszuwählen. Verfügbare Einstellungen sind: 16/s, 8/s, 4/s... 2s, 4s, 8s, 8s, 16s mit einem Standardwert von 2 Sekunden.

Sync Interval:
Gibt die Rate für das Senden von Synchronisationsnachrichten von einem Master zum Slave an.
Verfügbare Einstellungen sind: 128/s, 64/s... 64s, 128s, mit einem Standardwert von 1 Sekunde.

Delay Request Interval
Gibt die Rate an, wie oft Delay-Request-Messages von einem Slave an den Master gesendet werden. Delay-Request-Message-Intervalle sind 128/s, 64/s... 64s, 128s, mit einem Standardwert von 2 Sekunden.

Interval Duration [s]:
Gewünschte Dauer bis zum Timeout / Verlängerung.

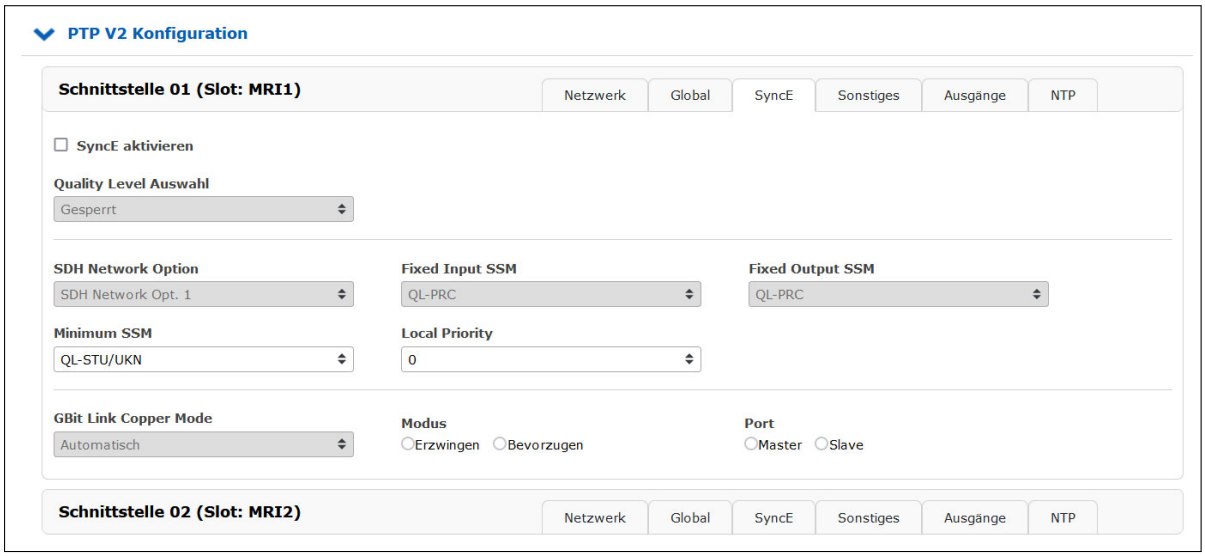
Announce Receipt Timeout:
Gibt die Quote für Timeout-Meldungen bei Ankündigungen an, die im Allgemeinen das 2 bis 10-fache der Quote für Ankündigungsintervalle beträgt, mit einem Standardwert von 3. in dieser Zeit sollte das BMCA-Verfahren den aktuellen Grandmaster auswählen.

Alternate Time Offset Indicator Extension:
Die TLV-Erweiterung Alternate Time Offset Indicator (ATOI) dient zur Übertragung von lokalen Zeitinformationen, wie z.B. lokaler Zeitzonenversatz und Sommerzeitumschaltung, von Master- zu Slave-Geräten. Dieses TLV verfügt über ein aktuelles Offset-Datenfeld und kann somit die Daten bereitstellen, die zur Umwandlung von TAI- oder UTC-basierten Zeitinformationen in lokale Zeit erforderlich sind.

Profilspezifische Einstellungen
Nur wenn das Custom-Profil ausgewählt wurde, kann diese Option genutzt werden. Es besteht hier die Möglichkeit, profilspezifische Parameter einfach für das eigenen „Custom-Profil“ auszuwählen. Dazu muss zuerst das Auswahlfeld „Use Profile Extensions“ auf **Ja** gestellt werden.

Grandmaster ID
Im Power-Profil C37.238-2011 muss dem Grandmaster eine 1-Byte-ID zugewiesen werden. Wählen Sie eine ID zwischen 3 und 254.

13.1.7.11 Option SyncE-Konfiguration



Dieses Submenü ermöglicht alle relevanten Einstellungen für die Synchronous-Ethernet-Funktionalität. SyncE ist ein ITU-T-Standard für Computernetzwerke, der die Übertragung von Taktsignalen über die physikalische Ethernet-Schicht ermöglicht.

Hinweis:
Das SyncE-Signal kann nur als Referenzeingangssignal verwendet werden, wenn eine TSU-GbE- oder HPS100-Karte in einem MRI-Steckplatz oder eine PSX210-Karte in einem beliebigen Steckplatz betrieben wird. (siehe Menü „Uhr → MRS-Einstellungen“).

SyncE aktivieren
Aktivierung / Deaktivierung wenn SyncE-Signal auf einem PTP-Port anliegt. SyncE läuft auf der PHY-Netzwerkebene und stört daher das PTP auf Layer 2 oder Layer 3 nicht. Beide können parallel auf dem gleichen Port laufen.

Quality Level Auswahl
Wenn SyncE aktiviert ist, wird die Qualitätsstufe einmal pro Sekunde innerhalb des ESMC (Ethernet Synchronization Message Channel) transportiert und automatisch, in Abhängigkeit vom Taktstatus, im Master-Modus bestimmt oder verwendet, da sie als Eingang im Slave-Modus empfangen wird. Wenn dieser Modus deaktiviert ist, werden die unter „Fixed Input SSM“ und „Fixed Output SSM“ gewählten Einstellungen dauerhaft als statische Werte verwendet.

SDH Network Option
Die ausgewählten Werte für die Qualitätsstufen hängen von den SDH-Netzwerkoptionen ab, die Option 1 (für SDH-, E1-basierte Systeme) oder Option 2 (für SONET-, T1-basierte Systeme) widergeben.

Fixed Input SSM Feste Qualitätsstufe des SyncE-Eingangssignals.
Fixed Output SSM Feste Qualitätsstufe des SyncE-Ausgangssignals.

Gbit Link Copper Mode
Wenn der „Kupfer-Modus“ für SyncE im Gbit-Modus verwendet wird, muss der Clock-Master oder Clock-Slave definiert werden. Das ist nicht notwendig, wenn optische Verbindungen über SFP verwendet werden, da diese dort automatisch ermittelt werden.

Modus
Der Benutzer kann wählen, ob der Kupferanschluss gezwungen werden soll, als Clock-Master oder Clock-Slave zu fungieren, je nachdem, welche Rolle (Master/Slave) dieser SyncE-Port haben soll. Eine Fehlkonfiguration kann zum Verlust der Verbindung führen, daher muss sich der Benutzer um die richtige Konfiguration der Link-Partner kümmern.

Port
Der Port kann in einem SyncE-Clock-Master- oder Clock-Slave-Modus betrieben werden. Eine Konfiguration ist nur für den Kupferport, nicht aber für Glasfaserverbindungen erforderlich.

13.1.7.12 Konfiguration Sonstiges

Abbildung: PTP-Konfiguration → Sonstiges mit HPS100-Modul und Performance-Level A oder B

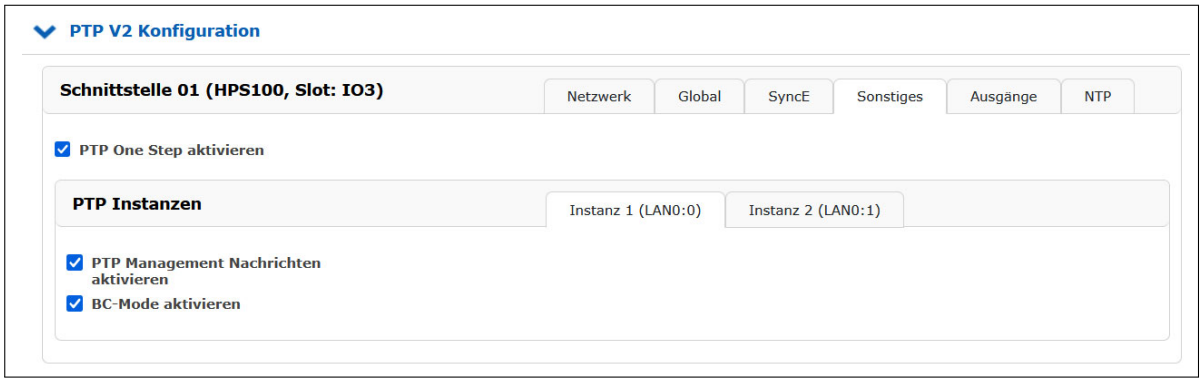


Abbildung: PTP-Konfiguration → Sonstiges mit HPS100 (Dual PTP-Stack, Performance-Level C, D, E) oder PSX-Modul

PTP One Step aktivieren:
Two-Step-Ansatz: Das PTP-Protokoll verlangt, dass der Master periodisch Sync-Nachrichten an Slave-Geräte sendet. Der Hardware-Zeitstempel-Ansatz von PTP erfordert, dass der Master den genauen Zeitpunkt aufzeichnet, zu dem ein solches Sync-Paket auf die Netzwerkleitung geht und diesen Zeitstempel an die Slaves übermitteln muss. Das kann erreicht werden, indem dieser Zeitstempel in einem separaten Paket (einer sogenannten Follow-Up-Nachricht) gesendet wird.

One-Step-Betrieb aktiviert: Die SYNC-Nachrichten selbst werden während der Übermittlung mit einem Zeitstempel versehen, kurz bevor sie den Netzwerkanschluss verlassen. Daher ist keine FOLLOW-UP-Meldung erforderlich.

Während im 2-Step-Betrieb eine Sync- und eine Follow-Up-Nachricht verwendet werden, um die Latenzzeit bei der Nachrichtengenerierung zu berücksichtigen, verwendet der 1-Step-Betrieb den genauen Zeitstempel, der in der Sync-Nachricht erzeugt wird, und lässt die Follow-Up-Nachricht aus.

PTP Management Nachrichten aktivieren
Ein Protokoll innerhalb von PTP, um die von den Hauptuhren gepflegten PTP-Datensätze abzufragen und zu aktualisieren. Diese Meldungen werden auch zur Anpassung eines PTP-Systems sowie zur Initialisierung und zum Fehlermanagement verwendet. Management-Nachrichten werden zwischen Management-Knoten und Uhren verwendet. Diese Funktion ist standardmäßig aktiviert.

BC-Mode aktivieren
Diese Einstellung ist für IMS-Systeme bestimmt, die mit mehreren PTP-Instanzen als Boundary-Clocks arbeiten.

Wenn *aktiviert*, überträgt dieses HPS100- oder PSX-Modul seinen übergeordneten Datensatz an alle anderen PTP-Uhren im System, die als Master operieren. Dies ermöglicht es allen nachgeschalteten Slave-Uhren, den vorgeschalteten Top-Level-Grandmaster im PTP-Netzwerk mit seiner Clock-ID, Clock-Class usw. zu identifizieren.

Wenn diese Option dagegen *deaktiviert* ist, wird dieses HPS100- oder PSX-Modul seine eigene Clock ID, Clock Class usw. an Slave-Uhren übermitteln. Damit stellt es sich fiktiv als den Grandmaster im PTP-Netzes dar.

13.1.7.13 Option: Konfiguration Ausgänge

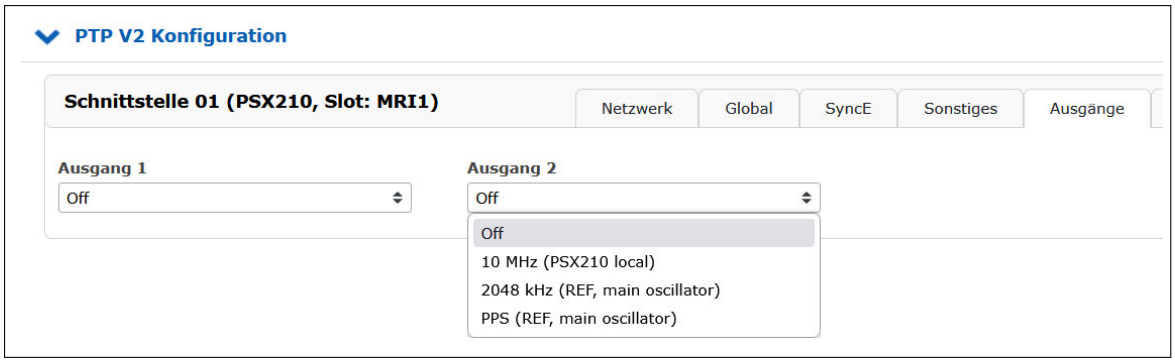


Abb.: Konfiguration der Ausgänge bei einem PSX210-Modul

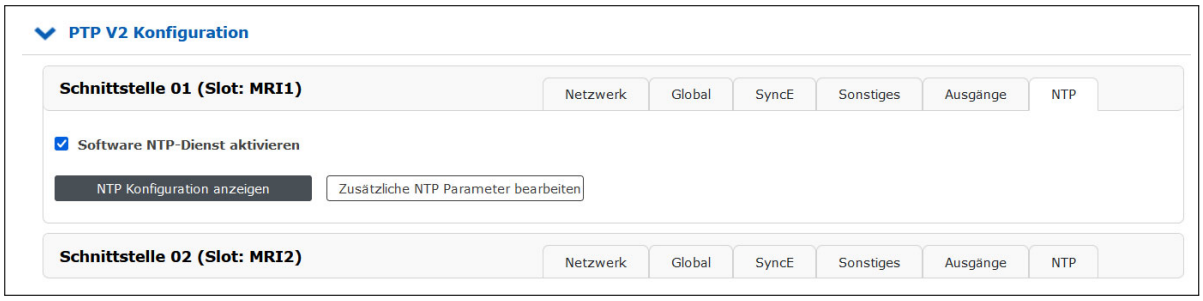
Unsere PTP-Module verfügen neben einem Gigabit Ethernet SFP/RJ45 Combo Port (TSU-GbE und HPS100) beziehungsweise zwei 10-Gigabit SFP-Ports bei einem PSX210-Modul auch über zwei konfigurierbare Ausgänge mit den folgenden Signalauswahlmöglichkeiten:

- PPS - lokal auf dem PTP-Modul erzeugt (TSU-GbE und HPS100)
- 10 MHz - lokal auf dem PTP-Modul erzeugt (TSU-GbE, HPS100 und PSX210)
- 2048 kHz - entnommen aus dem aktiven internen Clock-Modul (TSU-GbE, HPS100 und PSX210)
- 10 MHz - entnommen aus dem aktiven internen Clock-Modul (TSU-GbE und HPS100)
- PPS - entnommen aus dem aktiven internen Clock-Modul (TSU-GbE, HPS100 und PSX210)

Hinweis:

Standardmäßig sind beide Ausgänge bei allen PTP-Modulen deaktiviert.

13.1.7.14 Konfiguration NTP



Software-NTP-Dienst
Dieses Feature wird ausschließlich von PTP Modulen des Typs HPS100 mit HPS-Firmware-Version $\geq$ 1.4.1 und der PSX210 unterstützt. Der Typ und die Firmware Version eines verbauten PTP-Moduls kann unter „PTP → PTPv2 Status → Info“ überprüft werden.

Software NTP Dienst aktivieren:
Wenn aktiviert, wird zusätzlich ein Software-NTP-Dienst ***„ntpd“*** auf dem PTP-Modul gestartet. Dieser Service arbeitet genauso wie der NTP-Software Dienst auf der LAN-CPU und kann dementsprechend parametriert werden. Der Software-NTP-Dienst kann parallel zu allen anderen im Reiter „Global“ einstellbaren Betriebsarten des PTP-Moduls verwendet werden. Symmetrische Schlüssel, die auf dem Hauptsystem unter „NTP → NTP Symmetrische Schlüssel“ konfiguriert sind, werden automatisch mit in die NTP-Konfiguration des PTP-Moduls übernommen. Falls das PTP-Modul im „Global“ Reiter als NTP-Server konfiguriert wurde, werden alle NTP-Anfragen ohne Symmetric-Key-Authentication weiterhin vom Hardware-NTP-Responder des PTP-Moduls beantwortet. NTP-Anfragen mit Symmetric-Key-Authentication werden vom Software-NTP-Dienst beantwortet.

NTP Konfiguration anzeigen:
Über diese Schaltfläche kann die aktuelle NTP-Konfiguration angezeigt werden. Die initiale Konfiguration wird automatisch beim Aktivieren des Software-NTP-Dienstes generiert.

Zusätzliche NTP Parameter bearbeiten:
Über diese Schaltfläche können zusätzliche NTP-Parameter, wie z.B. Restrictions oder Trusted Keys, konfiguriert werden. Bei der Syntax muss sich an die Standardkonfigurationssyntax des *ntpd* gehalten werden. Konfigurierte Zeilen werden nach dem Speichern automatisch an die vom PTP-Modul generierte NTP-Konfiguration angehangen.

13.1.7.15 PTP Dual Stack Modus

Ab der HPS100-Firmwareversion 2.0.3 mit PL-C als minimaler Perfomance Level und einer PSX210 können zwei unabhängige PTP-Instanzen pro Port konfiguriert werden. LANTIME Firmware ≥7.04 unterstützt die Konfiguration dieser beiden PTP Instanzen und kann den Status der beiden PTP Instanzen getrennt voneinander anzeigen.

PSX210-Module haben zwei voneinander unabhängige Netzwerkschnittstellen mit PTP-Unterstützung. Für beide Schnittstellen können jeweils zwei PTP-Instanzen konfiguriert werden. Diese Funktion wird ab der LTOS Firmwareversion 7.08.001 unterstützt.

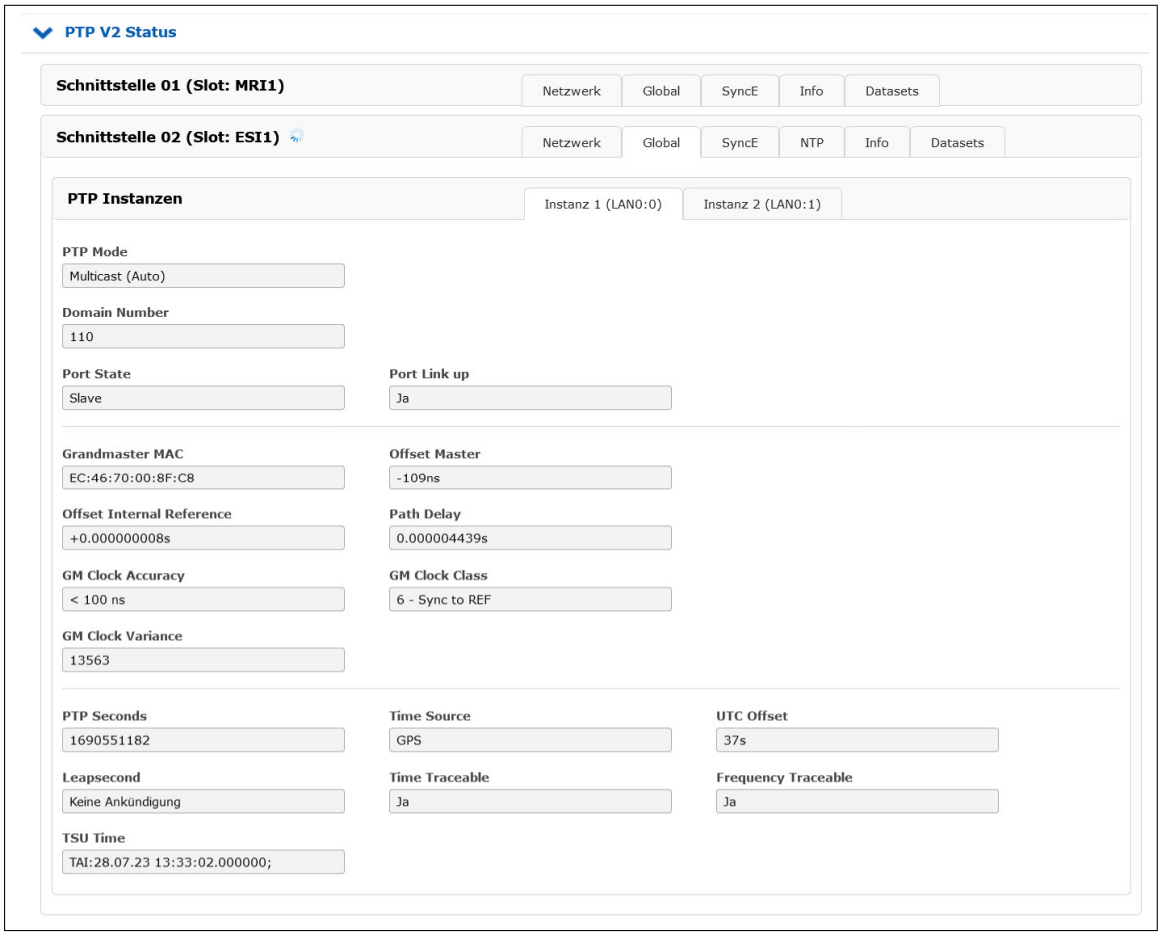
So können z. B. auf einem PTP-fähigen Port zwei PTP-Grandmaster-Instanzen sowohl für den IPv4- als auch für den IPv6-Modus oder für den Layer-2- und Layer-3-Betrieb parallel gestartet werden.

Wenn eine PTP-Slave-Instanz konfiguriert ist, ist eine zweite Instanz nicht möglich. Weitere Einschränkungen zu den möglichen Konfigurationsoptionen finden Sie nachfolgend.

Leistungshinweise
Die beiden PTP-Instanzen verfügen über unterschiedliche Client-Kapazitäten. Die erste Instanz (Instanz 1) verfügt über die volle Kapazität an PTP-Clients oder DelayRequests pro Sekunde, welche die gewählte Leistungsstufe zulässt (d. h. 1024 Unicast-Clients mit PL-D).

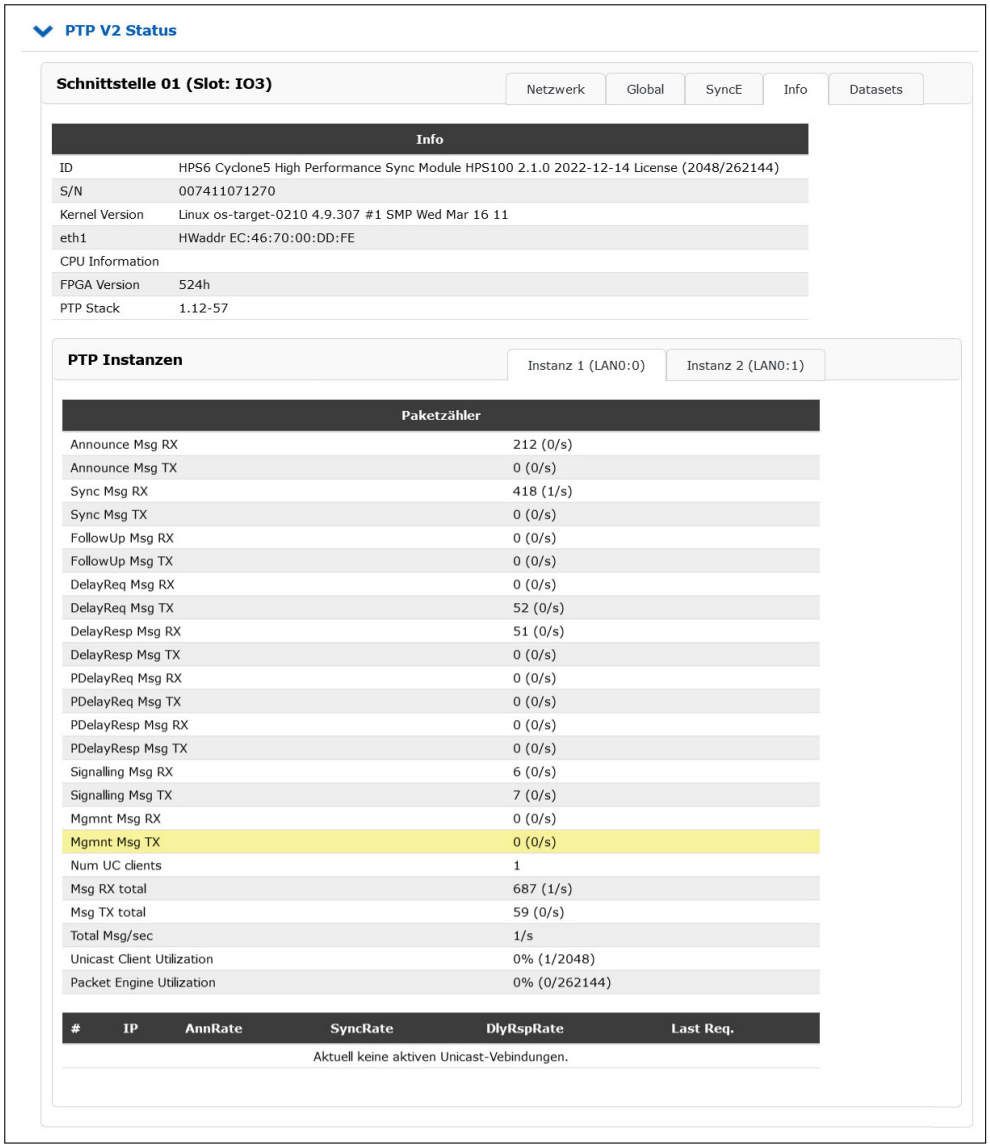
Bei der zweiten PTP-Instanz, die parallel zur ersten läuft, ist jedoch die CPU-Leistung der begrenzende Faktor. Die Gesamtkapazität der PTP-Packet-Engine liegt bei ca. 15.000 PTP-Transaktionen pro Sekunde.

Webinterface: PTP → Status → Global
Falls die Funktion von der HPS-Karte bereitgestellt wird, zeigt das Web-UI den Status der beiden PTP-Instanzen auf zwei unabhängigen Registerkarten auf der Seite Netzwerk, Global, Info und Datensätze an:

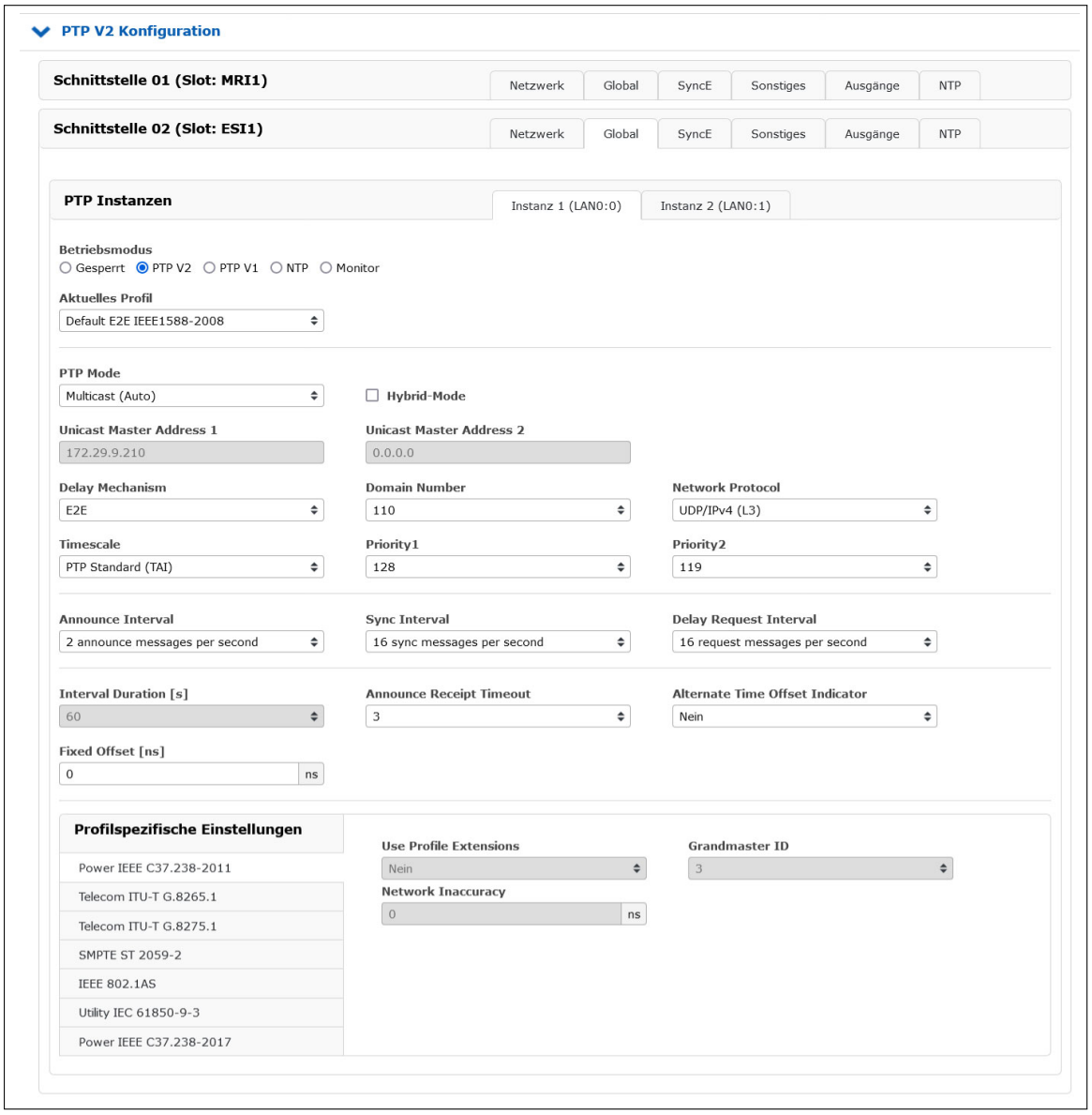


Webinterface: PTP → Status → Info

Der PTP-Paketzähler für beide Instanzen kann unabhängig voneinander angezeigt werden.



Webinterface: PTP → Konfiguration → Global
Auf der Seite PTP-Konfiguration können die beiden Instanzen des PTP-Daemons unabhängig voneinander konfiguriert werden, wobei jedoch einige Einschränkungen zu beachten sind (siehe unten).

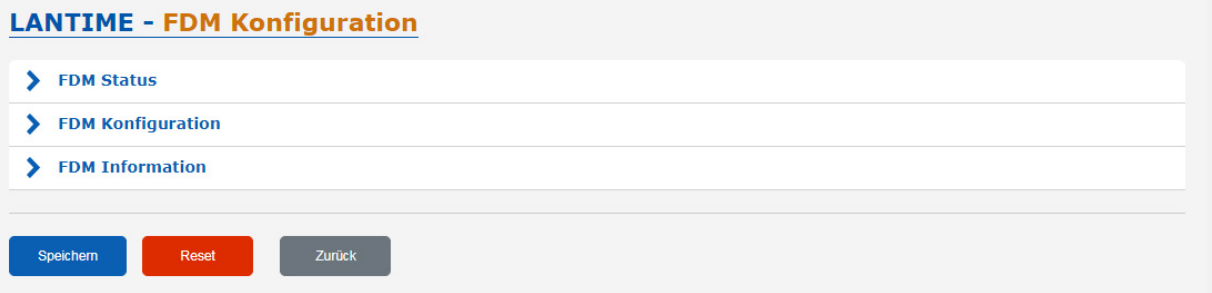


Einschränkungen und Regeln bei der Konfiguration einer PTP-Karte im Dual-Stack-Modus

(zwei aktive PTP-Instanzen)

- Beide Instanzen müssen PTPv2 sein (ab HPS100-Firmware 2.0.4 kann für die Instanz-1 PTPv1 und für die Instanz-2 PTPv2 ausgewählt werden).
- Beide Instanzen müssen Master Only sein.
- Über die Registerkarte „Verschiedenes“ muss der 1-Step-Clock-Betrieb aktiviert werden (im PTPv1/PTPv2-Mischbetrieb wird diese Einstellung deaktiviert).
- Die Konfigurationsparameter der beiden PTP-Instanzen müssen sich mindestens in einem der folgenden Parameter unterscheiden:
  - Domänennummer
  - Netzwerkprotokoll L2 oder L3
  - VLAN-Tag aktiviert

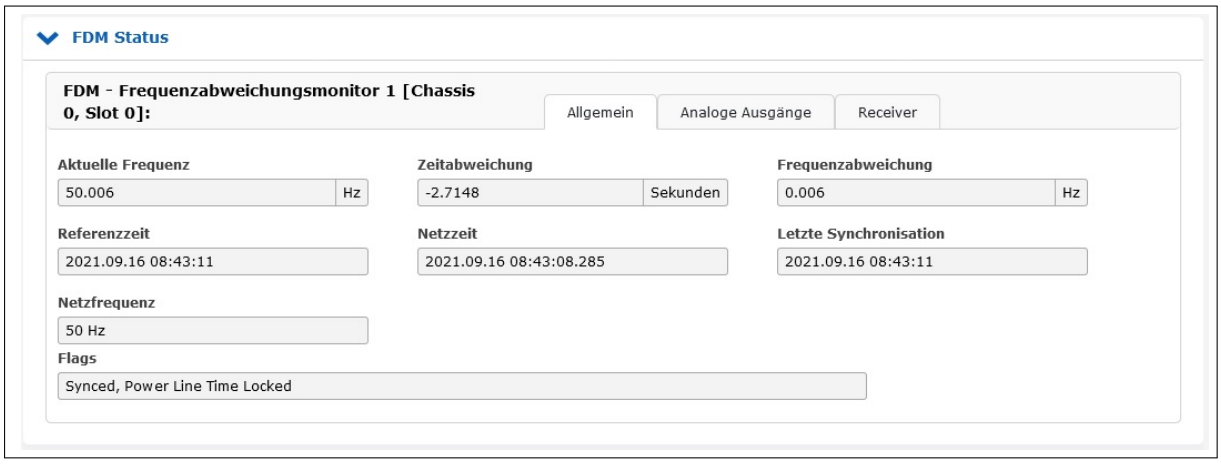
13.1.8 FDM - Frequenzüberwachung in Stromnetzen



Eine vorgeschaltete Referenz ist erforderlich, um eine serielle Zeitfolge, ein PPS-Signal (Puls pro Sekunde) und eine 10 MHz - Frequenz bereitzustellen. Aus diesen Signalen wird die Genauigkeit der Messungen abgeleitet.

Das Modul berechnet die Frequenz sowie die Zeit - basierend auf der Netzfrequenz. Die Zeitabweichung (TD Time Deviation) ist die Differenz dieser berechneten Zeit (PLT) zur Referenzzeit (REF). Diese Zeitabweichung sowie die Frequenz selbst werden über die serielle Schnittstelle ausgegeben oder in einen analogen Spannungsausgang umgewandelt, der von einem DAC geliefert wird.

13.1.8.1 FDM - Aktueller Status



In diesem Menü werden die folgenden Werte angezeigt:

Aktuelle Frequenz: Die aktuelle Frequenz des überwachten Stromnetzes

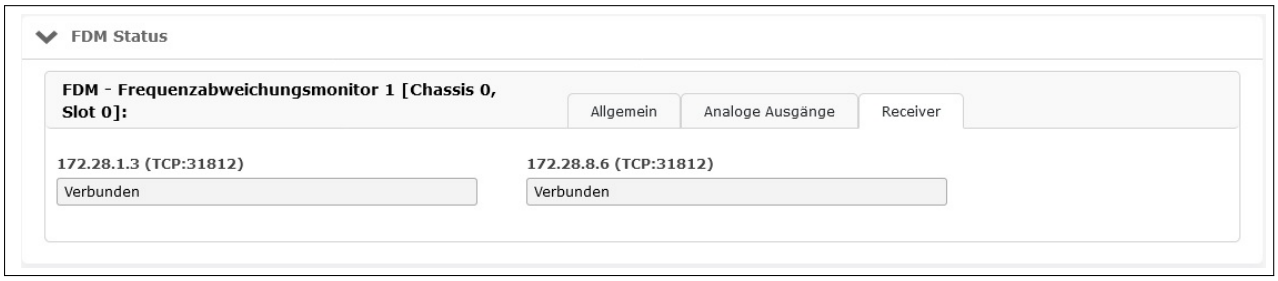
Referenzzeit: REF - die Zeit der Referenzuhr (z.B. GPS)

Netzzeit: PLT - die Zeit des überwachten Stromnetzes

Netzfrequenz: 50 Hz oder 60 Hz

Flags: Übertragene Flags per FDM (Error Bits)

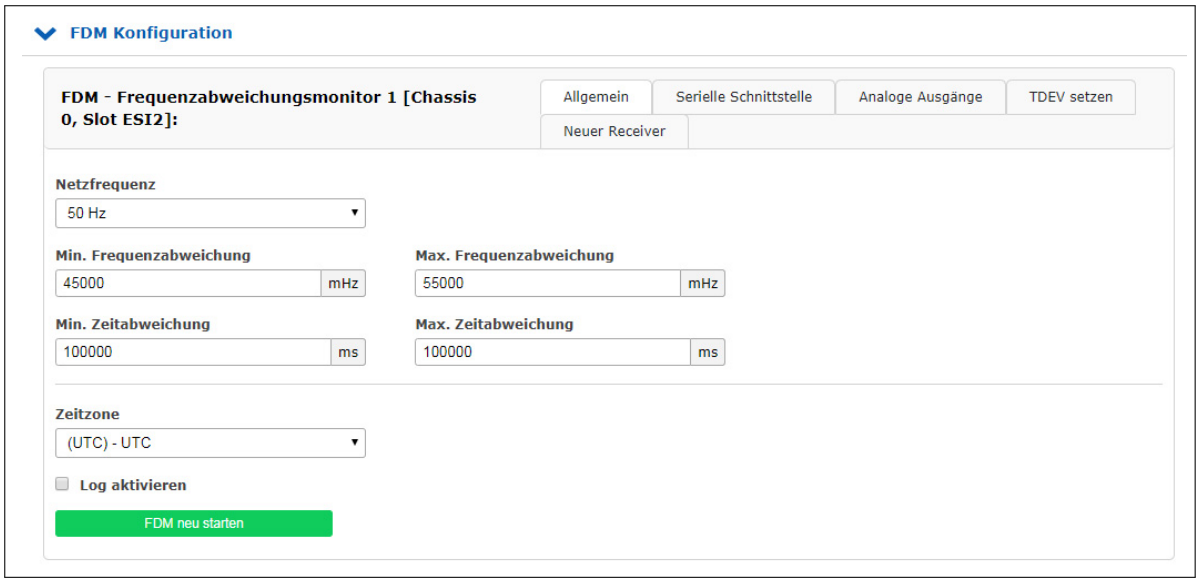
Empfängerstatus



Alle zuvor in der FDM-Konfiguration hinzugefügten Empfänger werden unter dem TAB „Receiver“ angezeigt.

13.1.8.2 FDM-Konfiguration

Automatische Überwachung der Netzfrequenz
Es ist möglich, eine Ober- und Untergrenze für die Netzfrequenz festzulegen und Alarmmeldungen (E-Mail, Syslog, SNMP-Traps) zu empfangen, wenn ein LANTIME erkennt, dass der Frequenzmesswert außerhalb des zulässigen Bereichs liegt.



Mit dem FDM-Konfigurationsmenü können folgende Parameter eingestellt werden:

Netzfrequenz: Frequenz der überwachten Stromleitung konfigurieren

Min. Frequenzabweichung: Ein Fehler tritt auf, wenn die Frequenz die minimale Frequenzabweichung erreicht.

Max. Frequenzabweichung: Ein Fehler tritt auf, wenn die Frequenz die maximale Frequenzabweichung erreicht.

Min. Zeitabweichung: Ein Fehler tritt auf, wenn die Frequenz die minimale Zeitabweichung erreicht.

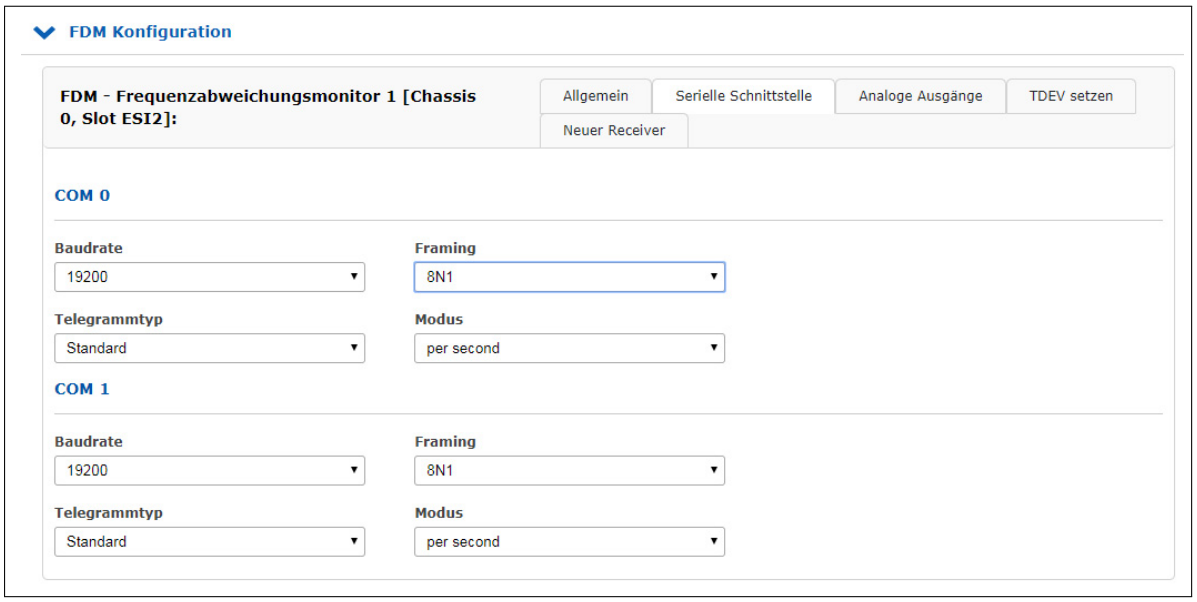
Max. Zeitabweichung: Ein Fehler tritt auf, wenn die Frequenz die maximale Zeitabweichung erreicht.

Zeitzone: Verwendete lokale Zeitzone für Referenz- und Netzfrequenz-Zeit

Log aktivieren: Protokollierung für FDM in XtraStats aktivieren

FDM neu starten Zum Neustart des Gerätes

Konfiguration der seriellen Schnittstelle



Baudrate: Zur Übertragung von seriellen Zeittelegrammen
600, 1200, 2400, 4800, 9600, 19200

Framing: 7N2, 7E1, 7E2, 7E2, 8N1 ,8N2, 8E1, 7O2 ,8O1

Telegrammtyp: Typ des erzeugten seriellen Zeittelegramms:
Standard, Short, Areva (TTM1), TPC (TTM2),
Standard 2, Computime, Fingrid, FDM III

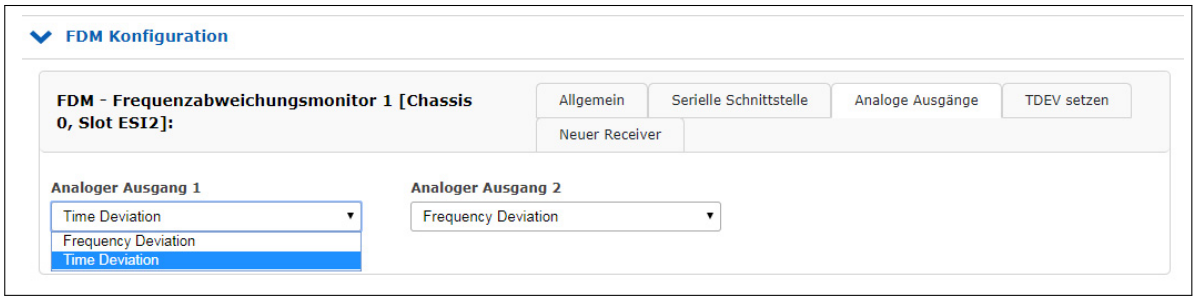
Das Standard-FDM-Telegrammformat enthält die folgenden Werte:
Netzfrequenz (FF.xxx Hz)
Frequenzabweichung (+-FF.xxx Hz)
Referenzzeit (HH:MM:SS)
Netzfrequenzzeit (HH:MM:SS.mmm)
Zeitabweichung (+-SS.mmm) - ab 99.999 ms (+-SSS.mmm)

Modus: Pro Sekunde, pro Minute oder auf Anfrage

Analoge Ausgänge

Die FDM180 stellt zwei analoge Ausgänge (A1/A2) zur Verfügung, welche je nach System über eine DFK-3 Buchse herausgeführt werden. Diese Ausgänge haben einen Spannungsbereich von -2,5 V ..... + 2,5 V, aufgeteilt in 65.536 Schritte (16-Bit-Auflösung).

Als Anzeigewert kann entweder die Frequenzabweichung oder die Differenzzeit jedes Analogausgangs gewählt werden.



Mode:

Zeitabweichung: Die Spannung am Ausgang hängt von den definierten Grenzen für die min. und max. Zeitabweichung ab.

Beispiel: Sind min: -100 s und max: +100 s eingestellt und wird eine Zeitabweichung von -100 s erreicht, liefert der Analogausgang eine Spannung von -2,5 V. Bei einer Abweichung von +100 s wird dagegen +2,5 V mit einer DAC-Auflösung von 16-Bit bereitgestellt.

Frequenzabweichung: Abhängig von den definierten Grenzen für die min. und max. Frequenzabweichung.

Beispiel: min: 45 Hz und max: 55 Hz bei 50 Hz Netzfrequenz. Wird eine Frequenz-abweichung von 45 Hz erreicht, liefert der Analogausgang eine Spannung von -2,5 V und bei 55 Hz, +2,5 V mit einer Auflösung von 16bit DAC.

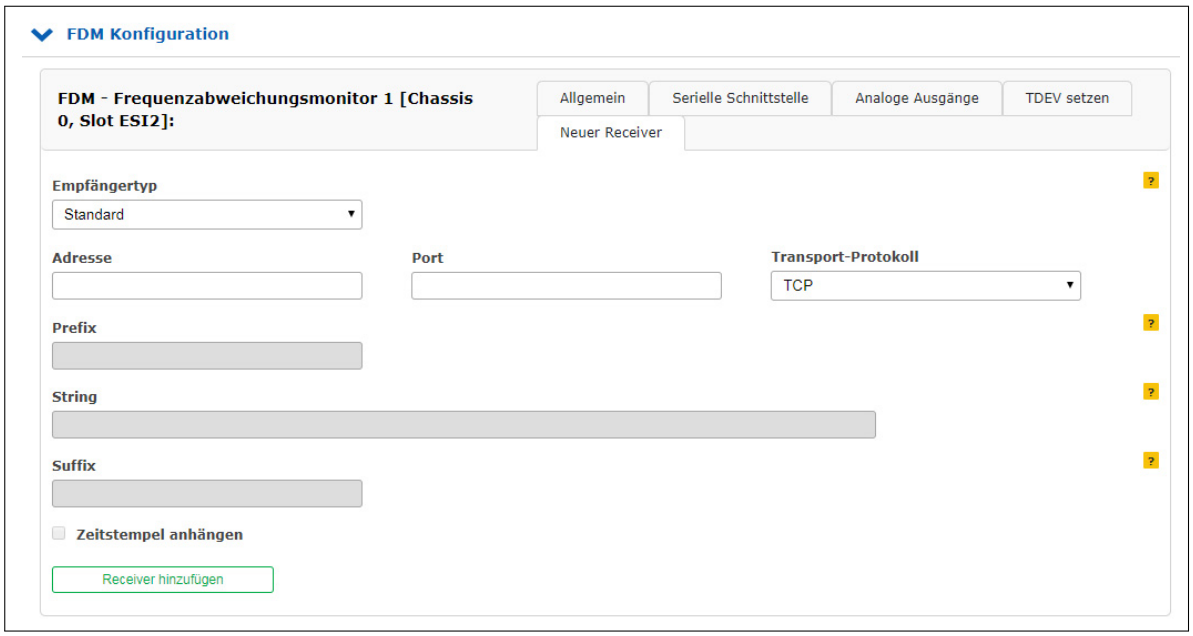
Submenü TDEV setzen

Zeitabweichung: Hier wird ein Wert (ggf. mit negativem Vorzeichen) eingetragen, um eine feste Zeitabweichung für die Power-Line-Zeit zu bestimmen.

Mit diesem Feld kann auch die aktuelle TDEV auch jederzeit auf Null zurückgesetzt werden, indem man hier einen Wert von 0 einträgt und **TDEV setzen** anklickt.

Diese (ggf. zurückgesetzte) Zeitabweichung wird angewendet, sobald die FDM180 synchron ist und eine Spannung vom Modul erfasst wird (bzw. wird sofort angewendet, wenn die FDM180 schon synchron ist und eine Spannung am Moduleingang bereits anliegt).

Submenü Neuer Receiver



In diesem Abschnitt kann der Benutzer einen neuen Empfänger für FDM-Telegramme hinzufügen. Hier können beliebig viele Empfänger (Netzwerkanzeigen und/oder PCs zur Analyse und Anzeige von Statusmeldungen oder Frequenzen) konfiguriert werden, die an das selbe Netzwerk angeschlossen sind.

Empfängertyp: Telegrammart für die Netzwerkübertragung
Standard: Standard-FDM-Zeittelegramm
Einmal pro Sekunde gesendet
z.B. „F:50.016 FD:+00.016 REF:15:17:57 PLT:15:17:57.056 TD:+00.056“

Extended: Erweitertes FDM-Zeittelegramm mit Zwischenmessungen und Sequenz-ID
Einmal pro Sekunde gesendet
z.B. „F:50.006 F:50.004 F:50.013 F:50.012 F:50.010 F:50.010 F:50.006 F:50.012 F:50.020“
oder „F:50.013 FD:+00.013 REF:15:19:10 PLT:15:19:10.071 TD:+00.071 SEQ:0000000004“

Intermediate: Abgeschnittenes FDM-Zeittelegramm mit Zwischenmessungen
Einmalig gesendet alle 100ms
M1:49.997 SEQ:0000000053
M2:49.996 SEQ:0000000054
M3:50.000 SEQ:0000000055
M4:49.999 SEQ:0000000056
M5:49.996 SEQ:0000000057
M6:49.996 SEQ:0000000058
M7:49.997 SEQ:0000000059
M8:49.995 SEQ:0000000060
M9:49.996 SEQ:0000000061
M9:49.996 SEQ:0000000062

Custom: Benutzerspezifisches FDM-Zeittelegramm, das aus Präfix, Zeichenkette und Suffix besteht. Einmal pro Sekunde gesendet.

Adresse: Adresse oder Hostname des Nachrichtenempfängers (Display oder Computer)

Port: Benutzter TCP/UDP-Port für die Telegrammübertragung

Transport-Protokoll: Verwendete Protokolle für die Telegrammübertragung (TCP/UDP)

Nur wenn der Empfängertyp „Custom“ ausgewählt ist.

Prefix: Präfix von benutzerdefinierten Zeichenketten, Steuerzeichen können z.B. durch ihren Hex-Wert (ASCII) angegeben werden:
„\x01“ für SOH (Start of Header) oder „\x02“ für SOT (Start of Text)

String: Kundenspezifisches Zeittelegramm, das sich aus einem beliebigen Text und den folgenden Variablen zusammensetzen kann (gekennzeichnet durch das Präfix'%):

PLFRQ	Netzfrequenz (z.B. 50.023)
FRQDEV	Frequenzabweichung (z.B. +00.023)
REFTIME	Referenzzeit (z.B. 15:17:23)
POWERLNTIME	Stromnetzzeit (z.B.. 15:17:22.550)
PLTDEV	Stromnetzzeit-Abweichung (z.B. -00.450)
IDX	Zwischenmessung-Index (z.B. 1)
IMMFRQ1	Zwischenmessfrequenz mit Index 1 (z.B. 50.034)
IMMFRQ2	Zwischenmessfrequenz mit Index 2 (z.B. 50.034)
...	
SEQID	Sequenz-ID (z.B. 0000000061)
SYSTIME	Systemzeit (z.B. 15:17:23)
SYNCSTATE	Synchronisations-Status (“ = synchron, '*' = nicht synchron)
SYNCTEXT	Synchronisations-Text („OK“ = synchron, „NO“ = nicht synchron)
TIMESTAMP	Aktueller Zeitstempel (z.B. 2016-03-15 16:03:10.042)
TIMESTRING	Zeittelegramm zum Einstellen der Display-Zeit (z.B. S16:04:37;15.03.16S)

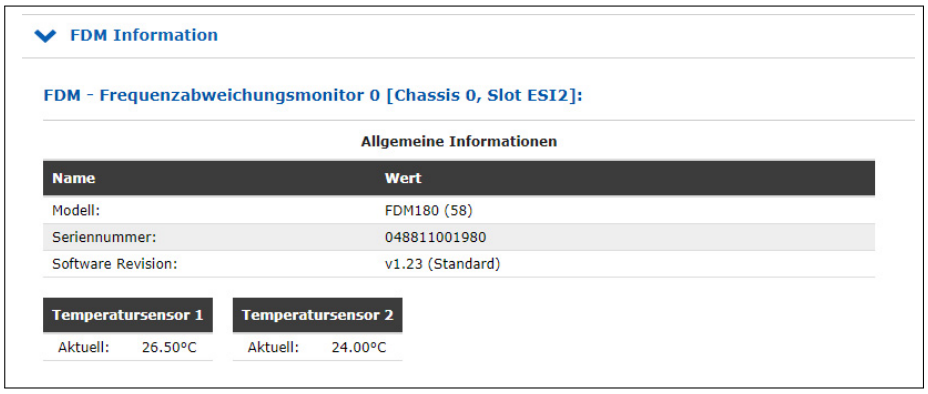
Eine Auto-Toggle-Funktion ermöglicht es, eine Folge von Formaten zu definieren, indem kommagetrennte Formatstrings eingerichtet werden. Zusätzlich kann die Dauer einer Formatzeichenkette über das Format *FORMATSTR@DURATION* definiert werden.

Das folgende Beispiel zeigt die Netzfrequenz für 20 Sekunden, dann die Referenzzeit für 30 Sekunden und dann die Frequenzabweichung für 10 Sekunden. Danach beginnt es von vorne mit der PLF-Anzeige: *PLF %PLFRQ Hz@20,REF %REFTIME@30,FDV %FRQDEV@10*

Suffix: Suffix von benutzerdefinierten Zeichenketten, Steuerzeichen können z.B. durch ihren Hex-Wert (ASCII) angegeben werden:
„\x0A“ für LF (Line Feed) oder „\x0D“ für CR (Carriage Return)

Angehängte Zeitstempel: Gibt an, ob ein Zeitstempel an die Nachricht angehängt werden soll.

13.1.8.3 FDM Informationen



Die Tabelle „FDM Informationen → Allgemeine Informationen“ zeigt die folgenden Werte an:

Modell: Der Modelltyp der FDM

Seriennummer: Die Seriennummer des FDM-Moduls

Software Revision: Die Firmware-Version der FDM

Temperatursensor 1/2: Die aktuell gemessene Betriebstemperatur der FDM

13.1.8.4 Serielle FDM Telegramme

13.1.8.5 Standard FDM-Telegramm

Das Standard-FDM-Telegramm ist eine Folge von 62 ASCII-Zeichen, die die Frequenz *F*, die Frequenzabweichung *FD*, die Referenzzeit *REF*, die Power-Line-Zeit *PLT* und die Zeitabweichung *TD* enthält, wobei jedes Feld durch ein Leerzeichen (ASCII-Code 20h) getrennt ist. Das Telegramm endet mit dem Carriage-Return Zeichen (<CR>, ASCII-Code 0Dh) und dem Line-Feed-Zeichen (<LF>, ASCII-Code 0Ah).

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

F:49.984 FD:*-00.016* REF:*15.03.30* PLT:*15.03.30.378* TD:*+00.378*<CR><LF>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

F:*49.984*	Die gemessene Netzfrequenz, Auflösung: 1 mHz.
FD:*-00.016*	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz
REF:*15.03.30*	Die Referenzzeit von der vorgeschalteten Uhr (Stunden:Minuten:Sekunden)
PLT:*15.03.30.378*	Die auf Basis der Netzfrequenz geführte Power-Line-Zeit, (Stunden:Minuten:Sekunden.Millisekunden) Zeitsprünge wie Sommer-/Winterzeit Umschaltung oder Schaltsekunden werden auf der Power-Line-Zeit nicht angewendet!
TD:*+00.378*	Die Abweichung der Power-Line-Zeit von der Referenz-Zeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms, maximum: +-99,999 s

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und die terminierenden Zeichen „<CR><LF>“ werden zu jedem Referenzzeit-Sekundenwechsel gesendet.

13.1.8.6 Standard 2 FDM-Telegramm

Das FDM-Telegramm „Standard 2“ ist identisch mit dem Standard-FDM-Telegramm, unterscheidet sich jedoch in der Übertragungsfrequenz, die vom konfigurierten Übertragungsmodus abhängig ist.

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an sowie bei jedem 500 ms-Intervall zwischen Sekunden.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request ‘?’ only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Nicht unterstützt.

13.1.8.7 Short FDM-Telegramm

Das Short-FDM-Telegramm ist eine Sequenz von 23 ASCII-Zeichen, die vereinfachte Informationen über die Frequenzabweichung *FD* und die Zeitabweichung *TD* enthält, wobei jedes Feld durch ein Leerzeichen (ASCII-Code 20h) getrennt sind. Das Telegramm endet mit dem Carriage-Return Zeichen (<CR>, ASCII-Code 0Dh) und dem Line-Feed-Zeichen (<LF>, ASCII-Code 0Ah).

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

FD:*-00.016*_TD:*+00.378*<CR><LF>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

FD:*-00.016*	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz, Maximum: +-09,999 Hz
TD:*+00.378*	Die Abweichung der Power-Line-Zeit von der Referenzzeit (Time Deviation), Auflösung: 1 ms, maximum: +-99,999s

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request ‘?’ only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und die terminierenden Zeichen „<CR><LF>“ werden zu jedem Referenzzeit-Sekundenwechsel gesendet.

13.1.8.8 Areva (TTM1) FDM-Telegramm

Das Areva-FDM-Telegramm besteht aus einer Folge von 71 Zeichen und beinhaltet die Frequenz *020*, die Frequenzabweichung *021*, die Zeitabweichung *022*, die Power-Line-Zeit *023* und die Referenzzeit *024* (letzterem wird der dreistellige Tag des Jahres vorangestellt). Diese Datenfelder sind jeweils getrennt durch die Zeichen Carriage-Return (<CR>, ASCII-Code 0Dh) und Line-Feed (<LF>, ASCII-Code 0Ah).

Jedem der fünf Datenfelder wird eine eindeutige dreistellige Adresse (020 ... 024) vorangestellt.

Das Telegramm als Ganze wird mit dem Zeichen Start-of-Text (<STX>, ASCII-Code 02h) eingeführt und mit dem Zeichen End-of-Text (<ETX>, ASCII-Code 03h) terminiert.

Die kursiv gedruckten Zeichen werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil des Telegramms sind:

```
<STX>02049.984<CR><LF>
021-0.016<CR><LF>
022+00.378<CR><LF>
02315 03 30.378<CR><LF>
024068 15 03 30 <CR><LF>
<ETX>
```

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

02049.984	Die gemessene Netzfrequenz, Auflösung: 1 mHz
021-0.016	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz.
022+00.378	Die Abweichung der Power-Line-Zeit von der Referenz-Zeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms.
02315_03_30.378	Die auf Basis der Netzfrequenz geführte Power-Line-Zeit, (Stunden_Minuten_Sekunden.Millisekunden) Zeitsprünge wie Sommer-/Winterzeit Umschaltung oder Schaltsekunden **nicht** auf der Power-Line-Zeit nicht angewendet!
024068_15_03_30	Die Referenz-Zeit von der vorgeschalteten Funkuhr, (Jahrestag_Stunden_Minuten_Sekunden). Ein Leerzeichen (ASCII-Code 20h) wird vor dem abschließenden <CR><LF> angehängt.

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Nicht unterstützt.

13.1.8.9 TPC (TTM2) FDM-Telegramm

Das TPC-FDM-Telegramm besteht aus einer Folge von 29 ASCII-Zeichen und beinhaltet die Referenzzeit (mit dreistelliger Jahrestag), die Zeitabweichung und die Frequenzabweichung *F*. Die Ausgabe beginnt mit dem Zeichen Start-of-Header (<SOH>, ASCII-Code 01h) und endet mit den Zeichen Carriage-Return (<CR>, ASCII-Code 0Dh) und Line-Feed (<LF>, ASCII-Code 0Ah).

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

<SOH>*288:10:11:29?-00.03*F*+50.01*<CR><LF>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

288:10:11:29	Referenzzeit von der vorgeschalteten Uhr, (Jahrestag:Stunden:Minuten:Sekunden).
?	Ist die Referenzuhr nicht synchron, wird an dieser Stelle ? (ASCII-Code 3Fh). Ist sie synchron, wird an dieser Stelle ein Leerzeichen (ASCII-Code 20h) sein.
-00.03	Die Netzfrequenzabweichung vom Sollwert, Auflösung 1 mHz.
F:*50.01*	Die gemessene Netzfrequenz, Auflösung: 10 mHz.

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Nicht unterstützt.

13.1.8.10 Computime Extended FDM-Telegramm

Das Computime Extended FDM-Telegramm besteht aus einer Folge von 42 ASCII-Zeichen, die die Referenz-Zeit (mit Datum und Wochentag), die Zeitabweichung D und die Frequenz F enthält. Es endet mit den Zeichen Carriage-Return (<CR>, ASCII-Code 0Dh) und Line-Feed (<LF>, ASCII-Code 0Ah).

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

T:*10:03:09:02:15:03:30*D:*+000.378*F:*49.984*<CR><LF>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

T:*10:03:09:02*:	Das Datum von der vorgeschalteten Referenzuhr, (Jahr:Monat:Tag:Wochentag / Montag = 01, Sonntag = 07)
15:03:30	Die Referenzzeit von der vorgeschalteten Uhr, (Stunden:Minuten:Sekunden)
D:*+000.378*	Die Zeitabweichung zwischen Referenzzeit und Power-Line-Zeit, mit Vorzeichen (+/-), Auflösung: 1 ms, maximum: +-99,999 s (immer mit einer führenden Null!)
F:*49.984*	Die gemessene Netzfrequenz, Auflösung: 1 mHz.

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und die terminierenden Zeichen „<CR><LF>“ werden zu jedem Referenzzeit-Sekundenwechsel gesendet.

13.1.8.11 Fingrid FDM-Telegramm

Das Fingrid FDM-Telegramm besteht aus einer Folge von 34 ASCII-Zeichen und beinhaltet die Referenzzeit, die Zeitabweichung *T* und die Frequenzabweichung *F*. Das Telegramm endet mit dem Carriage-Return Zeichen (<CR>, ASCII-Code 0Dh) und dem Line-Feed-Zeichen (<LF>, ASCII-Code 0Ah).

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

079:08:13:55.000 T*+6.780*F*+0.012*<CR><LF>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

079:08:13:55.000	Referenzzeit von der vorgeschalteten Uhr, (Jahrestag:Stunden:Minuten:Sekunden:Millisekunden).
T*+6.780*	Die Abweichung der Power-Line-Zeit von der Referenz-Zeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms.
F*+0.012*	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz.

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) oder „T“ (ASCII-Code 54h) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Nicht unterstützt.

13.1.8.12 FDM III-Telegramm

Das FDM III-Telegramm besteht aus einer Folge von 52 ASCII-Zeichen und beinhaltet die Referenzzeit (mit dreistelliger Jahrestag), die Zeitabweichung *T*, die Frequenzabweichung *F*, die gemessene Netzfrequenz *SF* und die Power-Line-Zeit *ST*. Es endet mit den Zeichen Carriage-Return (<CR>, ASCII-Code 0Dh) und Line-Feed (<LF>, ASCII-Code 0Ah).

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

068:12:17:55?T*-1.537*F*+0.123*SF*+60.095*ST*12:17:53.463*<CR><LF>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

068:12:17:55	Referenzzeit von der vorgeschalteten Uhr, (Jahrestag:Stunden:Minuten:Sekunden).
?	Ist die Referenzuhr nicht synchron, wird an dieser Stelle ? (ASCII-Code 3Fh). Ist sie synchron, wird an dieser Stelle ein Leerzeichen (ASCII-Code 20h).
T*-1.537*	Die Abweichung der Power-Line-Zeit von der Referenzzeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms.
F*+0.123*	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz.
SF*+60.095*	Die gemessene Netzfrequenz, Auflösung: 1 mHz.
ST*12:17:53.463*	Die auf Basis der Netzfrequenz geführte Power-Line-Zeit, (Stunden:Minuten:Sekunden.Millisekunden). Zeitsprünge wie Sommer-/Winterzeit Umschaltung oder Schaltsekunden werden auf der Power-Line-Zeit **nicht** angewendet!

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) oder „T“ (ASCII-Code 54h) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und die terminierenden Zeichen „<CR><LF>“ werden zu jedem Referenzzeit-Sekundenwechsel gesendet.

13.1.8.13 FDM III XLi-Telegramm

Das FDM III-XLi-Telegramm besteht aus einer Folge von 52 bzw. 56 ASCII-Zeichen (je nach Übertragungsmodus, siehe unten) und beinhaltet die Referenzzeit (mit dreistelliger Jahrestag), die Zeitabweichung *T*, die Frequenzabweichung *F*, die gemessene Netzfrequenz *SF* und die Power-Line-Zeit *ST*. Das Telegramm endet mit dem Carriage-Return Zeichen (<CR>, ASCII-Code 0Dh) und dem Line-Feed-Zeichen (<LF>, ASCII-Code 0Ah).

Im Gegensatz zum FDM III-Telegramm enthält die Zeitabweichung *T* eine zusätzliche führende Null und enthält nicht das Vorzeichen der Frequenzmessung *F*.

Bei eingestelltem Übertragungsmodus *per second*, *per minute* oder *per second <CR> on second change* ist das Telegramm wie folgt strukturiert:

068:12:17:55?T*-01.537*F*+0.123*SF*60.095*ST*12:17:53.463*<CR><LF>

Bei eingestelltem Übertragungsmodus *on request '?' only* enthält das Telegramm die Referenzzeit mit Millisekunden-Genauigkeit wie folgt:

068:12:17:55.000?T*-01.537*F*+0.123*SF*60.095*ST*12:17:53.463*<CR><LF>

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

068:12:17:55	Referenzzeit von der vorgeschalteten Uhr, (Jahrestag:Stunden:Minuten:Sekunden). Ist *on request '?' only* als Übertragungsmodus eingestellt, hat dieses Feld die Struktur (Jahrestag:Stunden:Minuten:Sekunden.Millisekunden).
?	Ist die Referenzuhr nicht synchron, wird an dieser Stelle ? (ASCII-Code 3Fh). Ist sie synchron, wird an dieser Stelle ein Leerzeichen (ASCII-Code 20h).
T*-01.537*	Die Abweichung der Power-Line-Zeit von der Referenzzeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms.
F*+0.123*	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz.
SF*60.095*	Die gemessene Netzfrequenz, Auflösung: 1 mHz.
ST*12:17:53.463*	Die auf Basis der Netzfrequenz geführte Power-Line-Zeit, (Stunden:Minuten:Sekunden.Millisekunden). Zeitsprünge wie Sommer-/Winterzeit Umschaltung oder Schaltsekunden **nicht** auf der Power-Line-Zeit nicht angewendet!

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) oder „T“ (ASCII-Code 54h) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und die terminierenden Zeichen „<CR><LF>“ werden zu jedem Referenzzeit-Sekundenwechsel gesendet. Im Gegensatz zu den anderen Übertragungsmodi wird die Referenzzeit hier nicht mit Sekunden-Genauigkeit, sondern mit Millisekunden-Genauigkeit ausgegeben.

13.1.8.14 SIE-TSF-FDM-Telegramm

Das SIE-TSF-FDM-Telegramm besteht aus einer Folge von 32 ASCII-Zeichen und beinhaltet die Referenzzeit *R*, die Zeitabweichung *D* und die gemessene Netzfrequenz *F*. Jedes Feld wird mit den Zeichen Line-Feed (<LF>, ASCII-Code 0Ah) und dann Carriage-Return (<CR>, ASCII-Code 0Dh) terminiert.

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

R:*13:11:19*<LF><CR>D:*+000.575*<LF><CR>F:*49.981*<LF><CR>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

R:*13:11:19*	Referenzzeit von der vorgeschalteten Uhr, (Jahrestag:Stunden:Minuten:Sekunden).
D:*+000.575*	Die Abweichung der Power-Line-Zeit von der Referenzzeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms.
F*+0.123*	Die gemessene Netzfrequenz, Auflösung: 1 mHz.

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und die terminierenden Zeichen „<CR><LF>“ werden zu jedem Referenzzeit-Sekundenwechsel gesendet.

Hinweis:

Bei dem SIE-TSF-Telegramm wird nicht mit dem Standard <CR><LF>, sondern mit der Sequenz <LF><CR> die ersten beiden Felder einzeln und das Telegramm als Ganzes terminiert.

Bei einer Einstellung von *per second, <CR> on second change* im Zusammenhang mit diesem Telegrammtyp wird das Telegramm allerdings als Ganzes (nach dem Feld *F*) doch mit der sonst üblichen Sequenz <CR><LF> terminiert. Die ersten beiden Felder werden weiterhin mit <LF><CR> terminiert. Das letzte Feld wird mit <CR><LF>terminiert. Das heißt, dass das Gesamttelegramm beispielsweise wie folgt aussehen würde:

R:13:11:19<LF><CR>D:+000.575<LF><CR>F:49.981<CR><LF>

13.1.8.15 Vorne-Anzeigetelegramm

Das Vorne-Anzeige-Telegramm besteht aus einer Folge von 90 ASCII-Zeichen und beinhaltet die Referenzzeit, die Frequenzabweichung (in 2 unterschiedlichen Formen), die Power-Line-Zeit sowie die gemessene Netzfrequenz. Jedes Feld endet mit dem Carriage-Return Zeichen (<CR>, ASCII-Code 0Dh) und dem Line-Feed-Zeichen (<LF>, ASCII-Code 0Ah) und das Telegramm als Ganze mit einem Bell-Zeichen (<BEL>, ASCII code 07h).

Das Vorne-Protokoll wird von einem proprietären Zeigermessgerät (PMU) verwendet, und die Implementierung in der FDM ermöglicht eine weitere Verwendung bestehender Empfänger. Es ist allerdings zu beachten, dass die FDM keine vollständige PMU ist: Auch wenn die Phase- und Stärke-Felder zwecks Kompatibilität im Zeittelegramm beibehalten werden, betragen diese Felder in der Ausgabe von der FDM immer Null.

Das Vorne-Protokoll spezifiziert ebenfalls ein Async-Feld (Out-of-Lock), mit dem zu erkennen sein soll, seit wann die Referenzuhr von der vorgeschalteten Referenzquelle getrennt ist. Dieses wird auch nicht von der FDM umgesetzt: Sollte Ihr Meinberg-System die Synchronisation mit der Referenzquelle verlieren und damit in den Holdover-Modus übergehen, wird die Telegrammausgabe der FDM ausgesetzt. Auch hier bleibt das Out-of-Lock-Feld auf Null, selbst wenn die Referenzuhr in den Simulationsmodus versetzt wird.

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

1100<CR><LF>44*10110 3*<CR><LF>22*+00016*<CR><LF>33*+015*<CR><LF>34*+ 0156*<CR><LF>
66*10110 3*<CR><LF>77*50016*<CR><LF>8800000<CR><LF>8900000<CR><LF>55*164*<CR><LF><BEL>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

1100	Eine fiktive „Async"-Zeit, die sonst die Holdover-Dauer der Referenzuhr bei Original-Systemen übermittelt. Hier lautet es immer 11 (der Feld-Code) und dann 00 (die Platzhalter-Zeit) bei einem Meinberg-System.
15:03:30	Die Referenzzeit von der vorgeschalteten Uhr, (StundenMinutenSekunden)
22-00016	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz. Die erste Stelle ist der Ganzzahlwert die letzten drei Zahlen sind die 3 Dezimalstellen.
33*+015*	Die Abweichung der Power-Line-Zeit von der Referenz-Zeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 10 ms. Die ersten beiden Stellen sind der Sekunden), die letzten beiden Zahlen sind die ersten und zweiten Dezimalstellen. Übersteigt die Abweichung einen Wert von *+9,99* bzw. unterschreitet sie *-9,99*, sind hier die letzten beiden Dezimalstellen stellvertretend Leerzeichen (d. h. +9.<SP><SP><CR><LF>). Achtung: Es findet keine Auf- oder Abrundung statt, d. h. +089 kann einen Wert zwischen *+0,890* und *+0,899* darstellen.
34*+0156*	Die Abweichung der Power-Line-Zeit von der Referenz-Zeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms. Das ist hier ein sechstelliger Wert: Die ersten 3 Stellen nach dem Vorzeichen sind der ganzzahlige Wert, die letzten 3 Zahlen sind die 3 Dezimalstellen. Führende Nullen im Ganzzahlbereich werden mit Leerzeichen dargestellt (d. h. 34+<SP><SP>1500<CR><LF> stellt 1 Sekunde und 500 Millisekunden dar. Übersteigt die Abweichung einen Wert von *+9,99* bzw. unterschreitet sie *-999,999*, sind hier alle Zahlstellen stellvertretend Leerzeichen (d. h. +<SP><SP><SP><SP><SP><SP><CR><LF>). Die Über- bzw. Unterschreitung bleibt durch das Vorzeichen (+/-) angegeben.
66101103	Die auf Basis der Netzfrequenz geführte Power-Line-Zeit, (StundenMinutenSekunden) Zeitsprünge wie Sommer-/Winterzeit Umschaltung oder Schaltsekunden werden

	nicht auf der Power-Line-Zeit nicht angewendet!
*77**50016***	Die gemessene Netzfrequenz, Auflösung: 1 mHz. Die ersten beiden Stellen sind der Ganzzahlwert, die letzten 3 Zahlen sind die 3 Dezimalstellen.
*88**00000***	Ein fiktiver Phasenwert für den Netzsinus, der ansonsten die Phase des Wechselstroms zum Messzeitpunkt. Hier beträgt dieser Wert immer 88 (der Feld-Code) und dann 00000 (als Platzhalterwert) bei einem Meinberg-
*89**00000***	Ein fiktiver Stärkewert für den Netzsinus, der ansonsten die Amplitude dessen Wechselstroms zum Messzeitpunkt. Hier lautet es immer 89 (der Feld-Code) und Feld-Code) und dann 00000 (der Platzhalter-Wert) bei einem Meinberg-System.
*55**164***	Der Jahrestag (1 ... 366) von der vorgeschalteten Uhr.

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?“ (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und das terminierende Zeichen <BEL> wird zu jedem Referenzzeit-Sekundenwechsel gesendet.

13.1.8.16 Altes Standard FDM-Telegramm

Das alte Standard-FDM-Telegramm ist eine Folge von 62 ASCII-Zeichen, die die Frequenz *F*, die Frequenzabweichung *FD*, die Referenzzeit *REF*, die Power-Line-Zeit *PLT* und die Zeitabweichung *TD* enthält, wobei jedes Feld durch ein Leerzeichen (ASCII-Code 20h) getrennt ist. Das Telegramm endet mit dem Carriage-Return Zeichen (<CR>, ASCII-Code 0Dh) und dem Line-Feed-Zeichen (<LF>, ASCII-Code 0Ah).

Das aktuelle „Standard FDM"-Telegrammformat hat das alte Format Ende 2023 abgelöst, wird aber weiterhin unterstützt, damit die Kompatibilität mit entsprechenden Empfängern erhalten bleibt. Es unterscheidet sich lediglich dadurch, dass die Stunden, Minuten, Sekunden und Millisekunden der Referenzzeit und Power-Line-Zeit im aktuellen Telegrammformat durch einen Punkt getrennt werden, während bei dem alten Format die Werte durch einen Doppelpunkt getrennt werden.

Die kursiv gedruckten Buchstaben werden durch die Messwerte ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind:

F:49.984 FD:*-00.016* REF:*15:03:30* PLT:*15:03:30:378* TD:*+00.378*<CR><LF>

Die Bedeutung der verschiedenen Werte wird im Folgenden beschrieben:

F:*49.984*	Die gemessene Netzfrequenz, Auflösung: 1 mHz.
FD:*-00.016*	Die Abweichung der Frequenz vom Sollwert (Frequency Deviation), mit Vorzeichen (+/-), Auflösung: 1 mHz
REF:*15:03:30*	Die Referenzzeit von der vorgeschalteten Uhr (Stunden:Minuten:Sekunden)
PLT:*15:03:30:378*	Die auf Basis der Netzfrequenz geführte Power-Line-Zeit, (Stunden:Minuten:Sekunden:Millisekunden) Zeitsprünge wie Sommer-/Winterzeit Umschaltung oder Schaltsekunden werden auf der Power-Line-Zeit **nicht** angewendet!
TD:*+00.378*	Die Abweichung der Power-Line-Zeit von der Referenzzeit (Time Deviation), mit Vorzeichen (+/-), Auflösung: 1 ms, Maximum: +-99,999 s

Übertragungsmodus-Verhalten

Per second	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Sekundenwechsel an.
Per minute	Die Übertragung eines Telegramms fängt bei jedem Referenzzeit-Minutenwechsel an.
On request '?' only	Die Übertragung eines Telegramms wird durch den Empfang des Zeichens „?" (ASCII-Code 3Fh) am RxD-Pin ausgelöst.
Per second, <CR> on second change	Die Übertragung eines Telegramms ist vorauseilend, so dass die Übertragung schon vor dem Sekundenwechsel anfängt, und die terminierenden Zeichen „<CR><LF>" werden zu jedem Referenzzeit-Sekundenwechsel gesendet.

13.1.8.17 Error-Bits

Die Baugruppe FDM180 registriert Fehler und Überläufe und setzt bzw. löscht daraufhin acht Error-Bits. Auf diese Weise kann der Anwender herausfinden, ob z.B. ein „Overflow“ aktiv ist. Diese Fehlerbits dokumentieren verschiedene Fehlerursachen die während des Betriebes aufgetreten sind.

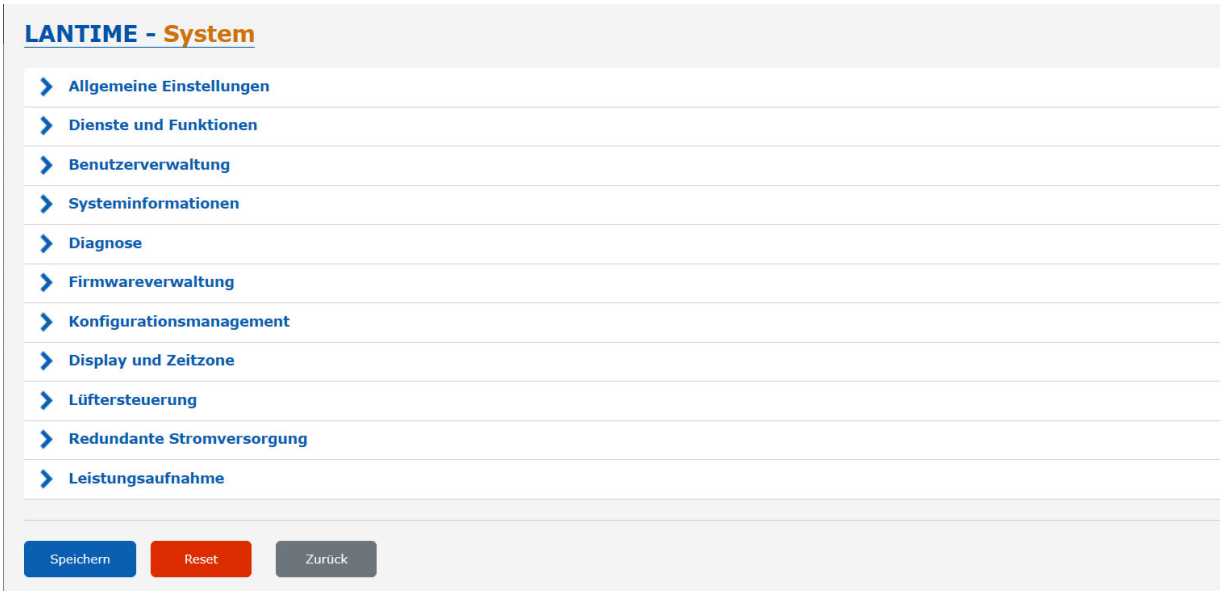
Die Anzeige hat das Format: *X8 X7 X6 X5 X4 X3 X2 X1*

X8: A2 Overflow, Analogausgang 2 hat seinen Endwert erreicht
X7: A1 Overflow, Analogausgang 1 hat seinen Endwert erreicht
X6: Time Deviation Overflow, die Zeitdifferenz ist größer +-99,999s
X5: Frequency Overflow, die Frequenzabweichung ist größer als die eingestellten max./min Werte
X4: REF Free, kein Sekundenimpuls von der Referenz
X3: Power Line Time Free, keine Netzfrequenz (Netzzeit bleibt auf dem letzten Wert stehen)
X2: No Time String, kein serielles Zeittelegramm erhalten
X1: No Power Line Time Init, die Netzzeit ist (noch) nicht initialisiert worden

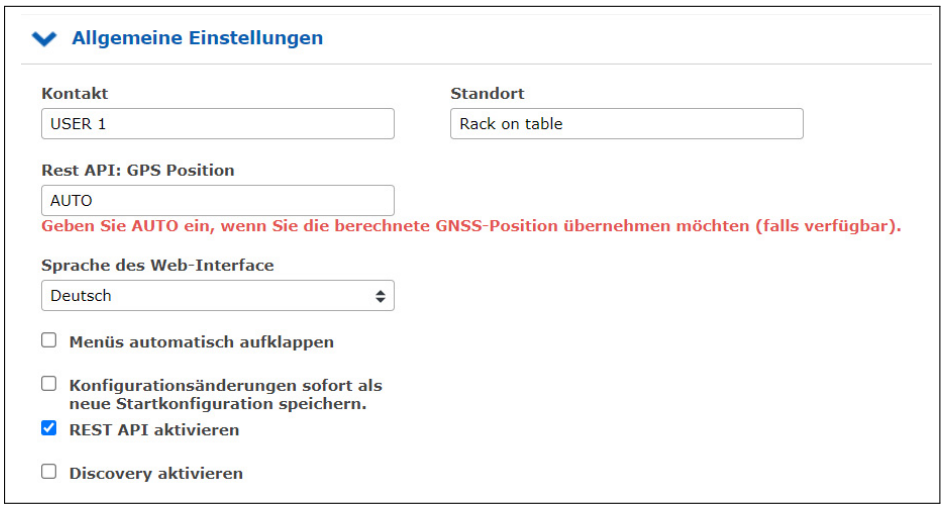
Die Fehlerbits können seriell auf Anfrage durch ein „E“ (ASCII-Code 45h) über die Schnittstellen COM 0/1 ausgelesen werden.

Das Format des Antwort-Strings ist:
ERROR:X8X7X6X5X4X3X2X1<CR><LF>

13.1.9 System



13.1.9.1 Allgemeine Einstellungen



Kontakt:
Ein Eingabefeld zum Speichern der Kontaktinformationen. Diese Information wird auch auf der Hauptseite des Webinterfaces angezeigt und kann über SNMP abgefragt werden.

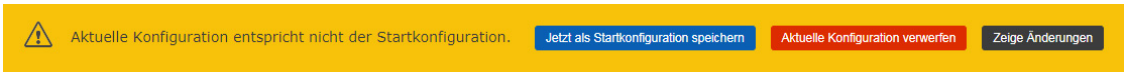
Ort:
Ein Eingabefeld zum Speichern des Gerätestandortes. Diese Information wird auch auf der Hauptseite des Webinterfaces angezeigt und kann über SNMP abgefragt werden.

Rest API: GPS Position
Der eingetragene Wert wird als GPS-Position des LANTIME über die REST API ausgegeben.

Sprache des Web-Interface:
Spracheinstellung des Webinterface.

Menüs automatisch aufklappen:
Wenn diese Funktion aktiviert ist, werden in jedem Konfigurationsdialog alle Untermenüs geöffnet.

Konfigurationsänderungen sofort als neue Startkonfiguration speichern:
Wenn diese Option aktiviert ist, wird jede Konfigurationsänderung sofort in die Startkonfiguration des LANTIME übernommen (die Startkonfiguration ist die Konfiguration, die beim Booten des LANTIME verwendet wird). Wenn die Option nicht aktiviert ist, wird nach jeder Konfigurationsänderung der folgende Hinweis im Kopf des Web-Interface angezeigt:



Jede Konfigurationsänderung kann dann als Startkonfiguration gespeichert werden, indem Sie mit der Schaltfläche „Jetzt als Startkonfiguration“ bestätigen.

REST API Support

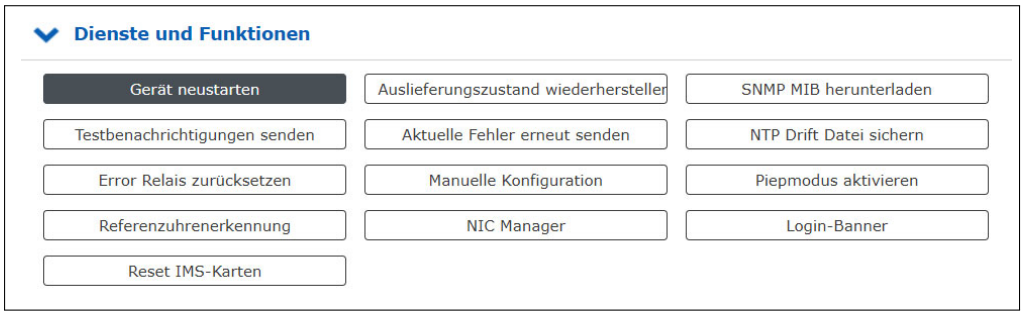
In der 7.04 Version wird erstmalig eine REST API Schnittstelle angeboten um Statusinformationen abzurufen und Konfigurationsanpassungen von externen Managementsystemen über eine sichere HTTPS Verbindung durchführen zu können. Die verfügbaren Objekte sind in einer auf JSON-basierenden Syntax als Baumstruktur abgelegt. Die REST API kann als Dienst per Konfiguration aktiviert und deaktiviert werden.

Eine Beschreibung aller verfügbaren Objekte ist in einer Online Hilfe verfügbar, die als ZIP-Archiv hier heruntergeladen werden kann: http:mbg.link/clihelp

Discovery aktivieren

Der LANTIME stellt Informationen für eine bessere Zuordnung in dem Meinberg Network Management System (mbgNMS) zur Verfügung.

13.1.9.2 Dienste und Funktionen



Gerät neustarten:
Leitet einen Neustart des LANTIME-Betriebssystems ein. Der eingebaute Referenztakt und die vom Taktgeber erzeugten Ausgangssignale bleiben davon unberührt.

SNMP MIB herunterladen:
Laden Sie die Meinberg SNMP MIB-Dateien herunter. Die Archivdatei enthält alle Meinberg SNMP-MIB-Dateien. Um einen LANTIME-Zeitserver mit V7-Firmware über SNMP zu überwachen, werden nur die MBG-SNMP-ROOT-MIB.mib und MBG-LANTIME-NG-MIB.mib-Dateien aus der Archivdatei benötigt.

Aktuelle Fehler erneut senden:
Mit dieser Schaltfläche können Sie dem Benutzer die LANTIME-Fehlerprotokolle per E-Mail oder SNMP-Trap zusenden. Um diese Funktion nutzen zu können, müssen die Fehlerereignisse auf der Seite „Benachrichtigung“ unter „Benachrichtigungsereignisse“ für den gewünschten Kanal (z.B. E-Mail oder SNMP) aktiviert werden. Zusätzlich muss ein E-Mail-Empfänger oder SNMP-Trap-Empfänger konfiguriert werden.

Error Relais zurücksetzen:
Mit dieser Taste kann das Fehlerrelais in einen fehlerfreien Zustand gesetzt werden.

Piepmodus aktivieren:
Diese Funktion kann verwendet werden, um ein LANTIME-Gerät zu finden. Nach dem Betätigen der Taste beginnt der LANTIME einmal pro Sekunde zu piepen und die Alarm-LED auf der Frontplatte blinkt rot. Die Funktion wird durch Drücken der Taste „F2“ auf der Frontplatte beendet. Sollte Ihr LANTIME-System nicht über Funktionstasten und Display verfügen, dann kann der Piepmodus auch über eine Konsolenverbindung mit dem Befehl **‘fpc‘** beendet werden. Drücken Sie im angezeigten Startmenü einach die F2-Taste auf Ihrer Tastatur. Für eine Terminalverbindung benötigen Sie Ihre Zugangsdaten (Benutzer und Passwort).

Auslieferungszustand wiederherstellen:
Setzt den LANTIME auf die Werkseinstellungen zurück. **Achtung:** Die Netzwerkeinstellungen bleiben während des Zurücksetzens über die Weboberfläche erhalten. Sollen auch die Netzwerkeinstellungen zurückgesetzt werden, muss der Reset über die Frontplatte ausgelöst werden. Während des Resets startet der LANTIME neu. Nach dem Neustart kann der LANTIME mit dem Standardbenutzer „root“ und dem Passwort „timeserver“ erneut konfiguriert werden.

Testbenachrichtigung senden:
Senden einer Testbenachrichtigung an die konfigurierten E-Mail-Empfänger und / oder SNMP-Trap-Empfänger.

NTP Drift Datei sichern:
Der NTP-Dienst ermittelt zur Laufzeit die Offsets der Systemuhr und speichert sie in der sogenannten NTP-Driftdatei. Diese Datei wird vom NTP-Dienst verwendet um die Systemuhr automatisch anzupassen, auch wenn kurzfristig keine Zeitquelle verfügbar ist.

Die Funktion „NTP Drift Datei sichern" speichert die aktuelle NTP-Driftdatei */etc/ntp.drift* auf der internen Compact-Flash-Karte unter */mnt/flash/data/ntp.drift*. Beim Neustart des LANTIME kann der Wert aus der gespeicherten Driftdatei vom NTP-Dienst ausgelesen werden, was die anfängliche Zeiteinstellung beschleunigt.

Manuelle Konfiguration:
Die Schaltfläche „Manuelle Konfiguration" ermöglicht einen direkten Zugriff auf die Konfigurationsdateien des LANTIME. Diese Funktion sollte nur von erfahrenen Administratoren genutzt werden.

NIC Manager
Der NIC Manager prüft das System auf die physikalischen Netzwerkschnittstellen. Das betrifft die zusätzlichen Schnittstellen, die über LNE-Module dem System hinzugefügt werden können. Nach dem Einbau und der Initialisierung einer LNE-Karte muss die Funktion ausgeführt werden, damit die Datei „etc/mbg/net.cfg" neu geschrieben wird. Der Netzwerkport-Status kann danach auf der Startseite im Webinterface angezeigt werden.

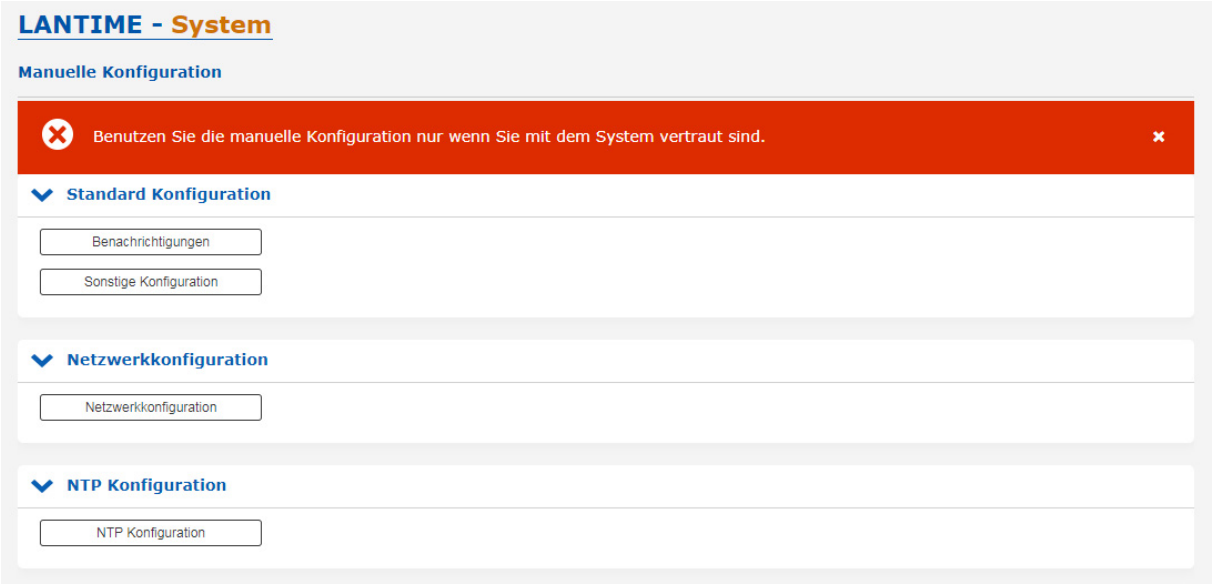
Auch nach dem Entfernen oder dem Austausch einer LNE sollte die Funktion NIC Manager ausgeführt werden. Das System prüft anhand der MAC-Adressen der einzelnen Netzwerkports, ob diese vorhanden sind, ob sich deren Position (Slot) im System verändert hat oder ob neue Schnittstellen vorhanden sind.

Referenzuhrenerkennung
Diese Funktion muss dann ausgeführt werden, wenn bei IMS-Systemen eine zweite Uhr nachträglich eingebaut wird um eine redundante Empfängerkonfiguration zu erhalten. Das System merkt sich nach dem Hochfahren die serielle Verbindung der eingesetzten Referenzuhr. Wird zum Beispiel bei einem M3000- oder M1000-System mit eingebauter RSC während des Betriebs (Hot-Plug) eine zweite Uhr nachträglich eingebaut, dann muss zur Registrierung der neuen Uhr die Taste „Referenzuhrenerkennung" betätigt werden, damit die serielle Verbindung der zweiten Uhr auf dem System gespeichert wird.

Login-Banner
Mit der Schaltfläche Login-Banner öffnet sich ein Dialog, um ein eigenes Login-Banner zu erstellen. Das Banner wird, auf der Login-Seite integriert. Somit kann einem Benutzer vor der Anmeldung ein Hinweis zur Nutzung des Gerätes angezeigt werden. Es ist möglich HTML (im begrenzten Umfang) und Text in dem Textfeld zu hinterlegen.

Reset IMS-Karten
Mit dieser Funktion können alle eingesetzten IMS-Module auf den Auslieferungszustand zurückgesetzt werden.

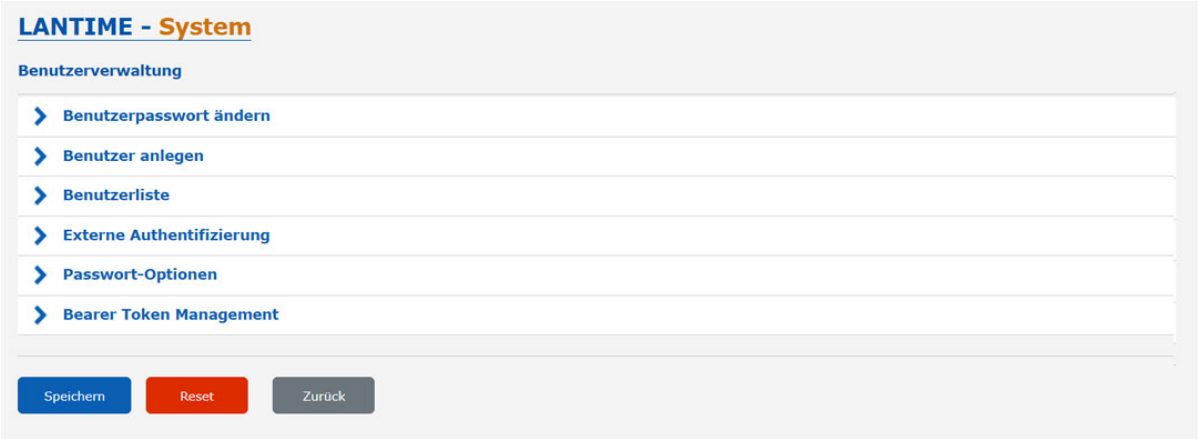
13.1.9.3 Manuelle Konfiguration



- Benachrichtigungseinstellungen
- Verschiedene Konfigurationen
- Netzwerkkonfiguration
- NTP-Konfiguration
- NTP-Broadcast-Konfiguration

Mit „Manuelle Konfiguration“ können Sie die Hauptkonfiguration ändern, indem Sie die Konfigurationsdatei von Hand bearbeiten. Nach der Bearbeitung klicken Sie auf die Schaltfläche „Datei speichern“, um Ihre Änderungen zu speichern, danach werden Sie gefragt, ob Ihre Änderungen durch erneutes Laden der Konfiguration aktiviert werden sollen (dies führt zum erneuten Laden mehrerer Subsysteme wie NTPD, HTTPD usw.).

13.1.9.4 Benutzerverwaltung



Benutzerpasswort ändern

Hier kann der angemeldete Benutzer sein Passwort ändern. Das neue Passwort muss durch zweimaliges Eingeben bestätigt werden. Zusätzlich muss auch das aktuelle Passwort mit angegeben werden.

Benutzer anlegen

Es ist möglich, mehrere Benutzerkonten auf einem LANTIME-System zu erstellen. Jedem Konto kann eine von drei Zugriffsebenen zugewiesen werden: Die Super-User-Ebene hat vollen Lese-/Schreibzugriff auf die Konfiguration des LANTIME-Systems, sie kann alle Parameter ändern und hat vollen Shell-Zugriff auf das System, wenn sie sich über Telnet, SSH oder den seriellen Konsolenport anmeldet. Konten auf Administratorebene können Parameter nur über die WEB-Schnittstelle ändern, haben aber keinen Shell-Zugriff. Die Zugriffsebene „Info“ kann nur Status- und Konfigurationsoptionen einsehen, darf aber keine Parameter oder Konfigurationsdateien ändern.

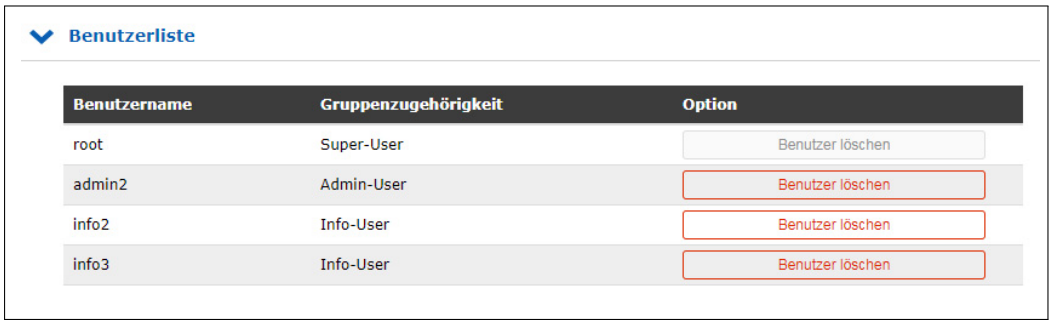
Die folgende Tabelle zeigt die Benutzerrechte der einzelnen Zugriffsebenen im Detail.

	Super User	Admin User	Info User
Vollständiger Zugriff auf die Befehlszeile	✓		
Ändern der Gerätekonfiguration durch das Webinterface	✓	✓	
Bearbeitung der zusätzlichen Konfigurationsdateien, die über das Webinterface* verfügbar sind.	✓		
Ausführen eines Firmware-Updates	✓		
Erstellen einer Diagnosedatei	✓		
Erstellen eines neuen Superuser-Accounts	✓		
Überprüfung aller Konfigurationswerte des Webinterfaces	✓	✓	✓

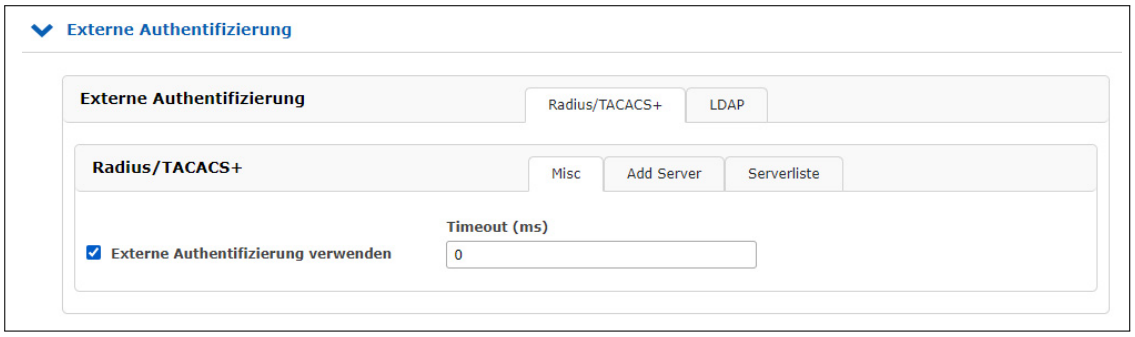
* Zusätzliche Netzwerkkonfiguration, zusätzliche NTP-Konfiguration, benutzerdefinierte Benachrichtigungen

Benutzerliste

Dieses Untermenü gibt Ihnen einen Überblick über alle konfigurierten LANTIME-Benutzer. Durch Anklicken von „Benutzer löschen“ kann ein einzelner Benutzer gelöscht werden.



13.1.9.5 Authentifizierung



Der LANTIME unterstützt Radius und TACACS+ als externe Authentifizierungsmethoden.

Externe Authentifizierung verwenden:
Über dieses Kontrollkästchen können Sie die externe Authentifizierungsfunktion des LANTIME aktivieren oder deaktivieren.

Timeout (ms):/b>
Zeitraum, in dem auf ein Paket „access accept“ von einem Authentifizierungsserver gewartet wird.

Sie können zwischen mehreren Authentifizierungsverfahren wählen:
1. LDAP
2. RADIUS
3. TACACS+

13.1.9.6 LDAP / LDAPS

Lightweight Directory Access Protocol
LDAP basiert auf dem Client-Server-Modell und wird für sogenannte Verzeichnisdienste verwendet. LDAP beschreibt die Kommunikation zwischen dem LDAP-Client und dem Verzeichnisserver. Aus einem solchen Verzeichnis können objektbezogene Daten, wie z.B. Personendaten oder Rechnerkonfigurationen, ausgelesen werden.

13.1.9.7 LDAP Setup

Beispiel LDAP-Einrichtung in Verbindung mit dem Microsoft-Active-Directory (AD)

Dieses Kapitel beschreibt ein Beispiel zur Einrichtung einer LDAP-Verbindung mit dem Microsoft-Active-Diretory mit vom Standard abweichenden Attributen eines Admin-Benutzers. Bitte beachten Sie, dass dies nur ein Beispiel ist und evtl. nicht direkt auf Ihre Verzeichnisstruktur anwendbar ist. Bitte kontaktieren Sie Ihren für den Verzeichnisdienst zuständigen Administrator, um Abweichungen auszumachen und nötige Anpassungen vorzunehmen.

Über den ADSI-Editor des Microsoft-Active-Directory werden in diesem Beispiel folgende Attribute eines LDAP-Benutzers angepasst:

- gidNumber = 4
- sAMAccountName = ldap-ad
- uidNumber = 10020
- unixHomeDirectory = /home/ldap-ad
- loginShell = /bin/false

Der Name des Benutzers (ldap-ad) die uidNumber und der „HomeDirectory"-Name sind frei wählbar. Dies sind lediglich Beispielwerte. Auch die Attribute (wie z.B sAMAccountName) können durch das Mapping frei gewählt werden. Wichtig ist nur, dass ein Mapping des im Verzeichnisdienst gewählten Attributes durch das dafür im RFC vorgesehenen Attribut definiert wird („shadow uid sAMAccountName" für dieses Beispiel).

Die **gidNumber** kann auch in einer Gruppe des Verzeichnisdienstes angegeben werden (Sekundäre Gruppen-Unterstützung). Der Benutzer benötigt dann dennoch eine primäre Gruppe, die jedoch keine Bedeutung für einen LANTIME hat. Dazu kann der Benutzer z.B. die **gidNumber** auf das AD-Attribut **primaryGroupID** mappen.

Nachdem „LDAP-Benutzer", „LDAP-Passwort", „Search-Scope" und „Search Base" angegeben wurden, können die Filter und Mappings definiert werden. Der LDAP-Benutzer wird benötigt, um Informationen aus dem AD auslesen zu können und ist im Normalfall kein Benutzer, der sich anschließend an dem System anmelden soll.

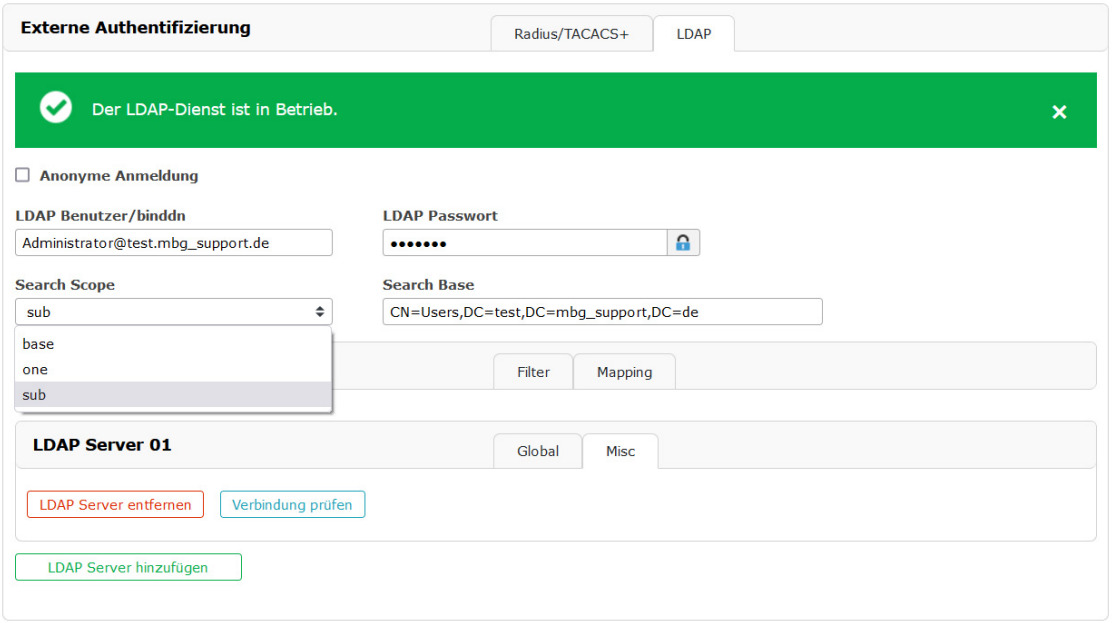


Abb.: Webinterface Menü „System → Benutzerverwaltung → Externe Authentifizierung → LDAP"

In der Beispiel-Domäne test.mbg.de wurde die „Search Base“ „CN=Users,DC=test,DC=mbg_support“ gewählt und der „Search-Scope“ auf „sub“ eingestellt.

Folgende Filter und Mappings müssen bei dieser Beispielkonfiguration über das Webfrontend des LTOS hinzugefügt werden.

Filter:
- passwd (&(objectClass=user)(unixHomeDirectory=*))
- shadow (&(objectClass=user)(uidNumber=*)(unixHomeDirectory=*))

Abb.: LDAP-Submenü „Erweiterte LDAP Konfiguration → Filter“

Mappings:
- passwd uid sAMAccountName
- passwd homeDirectory unixHomeDirectory
- shadow uid sAMAccountName

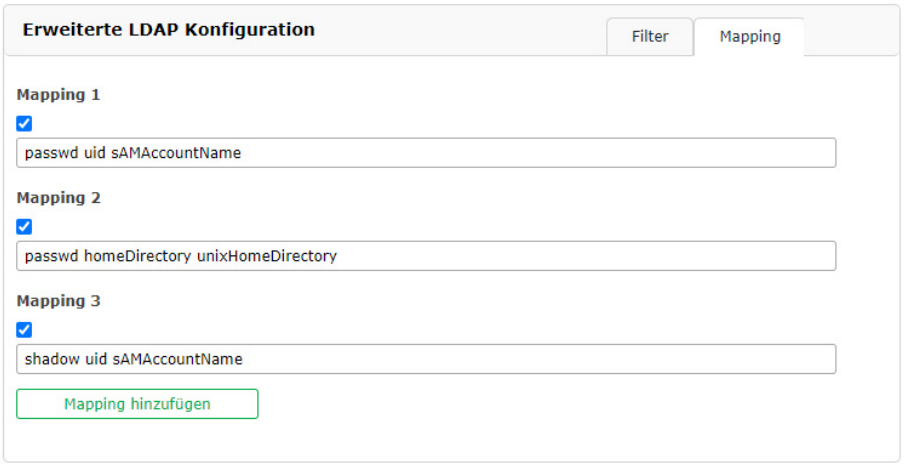
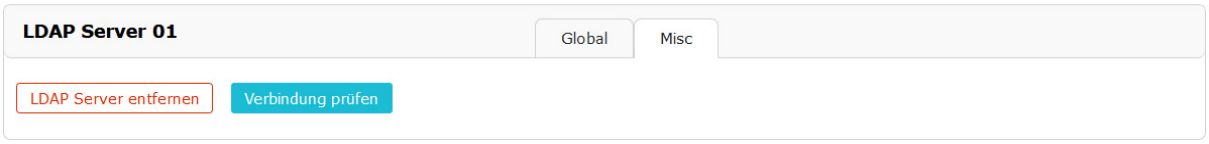


Abb.: LDAP-Submenü „Erweiterte LDAP Konfiguration → Filter“

Die gidNumber kann manchmal mit der Gruppenzugehörigkeit auf anderen Systemen kollidieren. Sprechen Sie mit Ihrem für den Verzeichnisdienst zuständigen Administrator über mögliche Vermeidungsstrategien.

Nachdem die URI des LDAP-Servers vergeben wurde, können die Einstellungen gespeichert werden. Wird LDAP als Protokoll ausgewählt, können sich die konfigurierten LDAP-Benutzer über das Webfrontend (und die CLI sofern eine loginShell für den Super-User vergeben wurde) anmelden. Wird LDAPS als Protokoll ausgewählt muss zuvor das rootca-Zertifikat, dass den LDAP-Server eindeutig identifiziert (siehe → Kapitel 13.1.5.5, „CA Zertifikate“) hinzugefügt werden.

Bei Problemen kann unter „Misc“ des jeweiligen LDAP-Server-Eintrags die Verbindung überprüft werden. Hierbei wird die grundsätzliche Verbindungsmöglichkeit mit den zwingend erforderlichen Werten URI, bind dn und search base überprüft. Der Status über die LDAP-Funktionalität wird in dem Banner des Reiters LDAP wiedergegeben.



13.1.9.8 RADIUS

Radius steht für „Remote Authentication Dial In User Service“ und bietet eine zentrale Authentifizierung für LANTIME-Geräte. RADIUS ist ein Client/Server-Protokoll, das in der Anwendungsschicht läuft und UDP als Transportprotokoll verwendet.

Die LANTIME RADIUS-Authentifizierung erfordert, dass für jedes Konto, das sich am LANTIME anmelden kann, ein Vendor Specific Attribute (VSA) namens MBG-Management-Privilege-Level konfiguriert ist. Diese VSA muss der RADIUS-Konfiguration eines externen Authentifizierungsservers hinzugefügt werden. Hier einige zusätzliche Informationen zum Attribut:

```
Name = MBG-Management-Privilege-Level
Datatype = Integer
Vendor-Code = 5597
Vendor assigned attribute number = 1
Value range = 100, 200, 300
```

Zusätzlich müssen Sie für dieses Attribut für jeden RADIUS-Benutzer, der sich am LANTIME anmelden kann, einen Wert von 100 (Super User), 200 (Admin User) oder 300 (Info User) vergeben.

13.1.9.9 TACACS

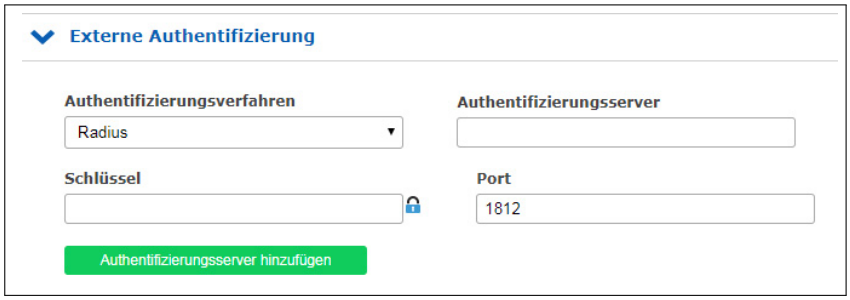
„Terminal Access Controller Acc-Control System“ ist ein Fernauthentifizierungsprotokoll, das dem LANTIME die Möglichkeit gibt, mit einem TACACS-Authentifizierungsserver zu kommunizieren.

Die LANTIME TACACS-Authentifizierung erfordert, dass jedes Konto, das sich am LANTIME anmelden können soll, ein Attribut namens „priv-lvl“ konfiguriert hat. Dieses Attribut muss auf dem TACACS-Server konfiguriert werden.

Für ein Superuser-Konto muss das Attribut „100“, für ein Admin-Konto „200“ und für ein Info-Benutzerkonto „300“ sein. Im Folgenden ein Beispiel für eine tac_plus Server-Konfigurationsdatei:

```
# This is the shared secret that clients have to use to access Tacacs+
key = meinberg

# User Groups

group = lantime_super_user {
        service = lantime_mgmt {
                priv-lvl = 100
                }
}

group = lantime_admin_user {
        service = lantime_mgmt {
                priv-lvl = 200
                }
}

group = lantime_info_user {
        service = lantime_mgmt {
                priv-lvl = 300
                }
}

# User

# LANTIME Super User
user = tacacs_su {
        member = lantime_super_user
        pap = cleartext „tacacs_su“ # User Password
}

# LANTIME Admin User
user = tacacs_au {
        member = lantime_admin_user
        pap = cleartext „tacacs_au“ # User Password
}

# LANTIME Info User
user = tacacs_iu {
        member = lantime_info_user
        pap = cleartext „tacacs_iu“ # User Password
}
```

Authentifizierungsserver hinzufügen



Über dieses Formular können Sie der LANTIME-Konfiguration einen externen Authentifizierungsserver hinzufügen. Die externe Authentifizierung muss zuerst im Menü „Authentifizierung-Optionen“ aktiviert werden.

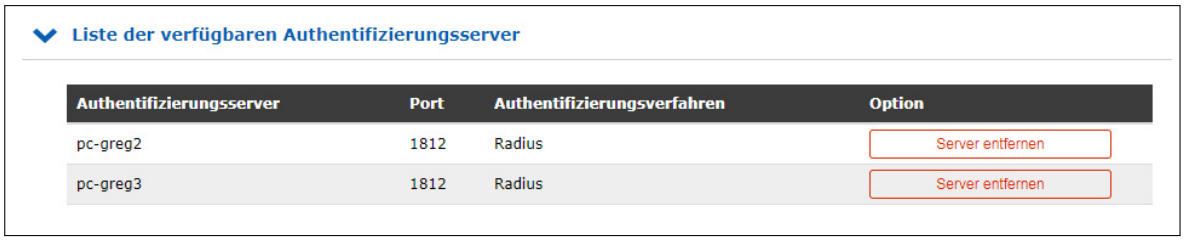
Authentifizierungsverfahren:
Konfiguration der zu verwendenden Authentifizierungsmethode, entweder Radius oder TACACS+. Detaillierte Informationen zu beiden Methoden finden Sie im oberen Teil dieses Kapitels.

Authentifizierungsserver:
Die IP oder der Host des ausgewählten Authentifizierungsservers (IPv4 und IPv6 werden unterstützt).

Schlüssel:
Ein gemeinsamer Schlüssel wird für eine grundlegende Authentifizierung zwischen einem LANTIME und dem Authentifizierungsserver verwendet. In diesem Feld muss das „Shared Secret“ des externen Authentifizierungsservers eingetragen werden. Eine Liste der zulässigen Zeichen, die für den gemeinsame Schlüssel verwendet werden können, finden Sie im Kapitel „Vor dem Start → Text- und Syntaxkonventionen“).

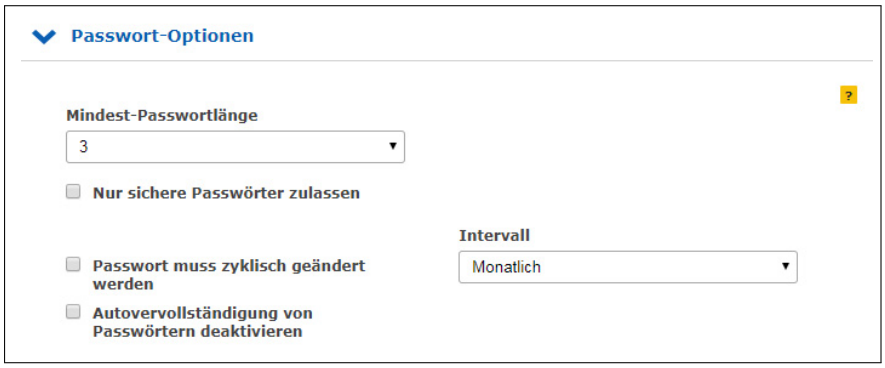
Port:
Abhängig von der Authentifizierungsmethode ist hier bereits der Standard-Port konfiguriert. Bei Bedarf kann der Port geändert werden.

Liste der verfügbaren Authentifizierungsserver



Diese Tabelle gibt Ihnen einen schnellen Überblick über die konfigurierten Authentifizierungsserver. Jeder Server kann entweder von einem Super- oder Admin-Benutzer entfernt werden, indem Sie auf die Schaltfläche „Server entfernen“ klicken.

13.1.9.10 Passwort - Optionen



Dieses Untermenü enthält einige allgemeine Passworteinstellungen.

Mindest-Passwortlänge:
Dieser Parameter legt die Mindestanzahl von Zeichen eines Passworts fest, bevor es vom System als gültiges Passwort akzeptiert wird. Dieser Wert wird sowohl beim Anlegen eines neuen Benutzers als auch beim Ändern eines aktuellen Benutzerkennworts verwendet. Bereits erstellte Passwörter sind davon nicht betroffen. Die maximale Länge eines Passworts beträgt 64 Zeichen.

Nur sichere Passwörter zulassen:
Wenn diese Option aktiviert ist, werden nur sichere Passwörter erlaubt. Ein sicheres Passwort benötigt mindestens:

- einen Kleinbuchstaben[a-z]
- einen Großbuchstaben [A-Z]
- eine Zahl [0-9]
- ein Sonderzeichen

Eine Liste der zulässigen Zeichen, die als Sonderzeichen verwendet werden können, finden Sie im Kapitel „Vor dem Start → Text- und Syntaxkonventionen“.

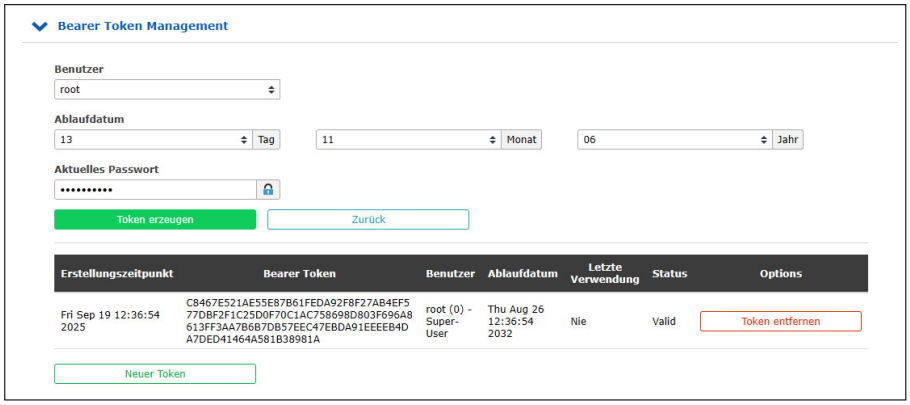
Passwort muss zyklisch geändert werden:
Die Benutzer werden gezwungen sein, in regelmäßigen Abständen Passwörter zu ändern. Wenn ein Passwort abgelaufen ist, kann sich der Benutzer nicht am Gerät anmelden, bevor er sein aktuelles Passwort geändert hat. Mögliche Intervalle sind:

- Monatlich
- Quartalsweise
- Halbjährlich
- Jährlich

Autovervollständigung von Passwörtern deaktivieren:
Nachdem diese Funktion aktiviert ist, wird Ihr Browser die Anmeldeinformationen eines LANTIME nicht automatisch vervollständigen.

13.1.9.11 Bearer Token Management

Ein „Bearer-Token“ ist ein Geheimnis (Secret), das einer Person oder Anwendung („dem Träger“) Zugang zu einer geschützten Ressource ermöglicht. Diese werden in der Regel automatisch generiert und sind meistens wesentlich länger als Passwörter (128 Zeichen). Bearer-Token lassen sich zwar nicht leicht merken, haben aber durch ihre Länge den Vorteil, dass sie im Allgemeinen sicherer sind. Für automatisierte Abfragen einer geschützten Ressource spielt die Länge des Secrets nur eine untergeordnete Rolle. Aus diesem Grund wurde die Möglichkeit geschaffen, einem normalen Benutzer ein Passwort und ein Bearer-Token oder einem Service-Benutzer ausschließlich ein Bearer-Token zur Verfügung zu stellen.



Zugriffskontrolle:
Ein Token muss einem Benutzer zugewiesen werden. Das Token erhält dadurch die Rechte der Gruppe des Benutzers.

Verwendung über HTTPS:
Da das Token Anmeldedaten enthält, sollte die Kommunikation immer über TLS/HTTPS erfolgen, um das Abhören dieser Daten zu verhindern.

Gültigkeitsdauer:
Bearer Token sind temporäre Zugriffstoken mit einer begrenzten Gültigkeitsdauer. Die Gültigkeitsdauer kann in dem Menü „Bearer Token Management“ eingestellt werden (Ablaufdatum).

Die folgenden Parameter können konfiguriert werden:

Benutzer: Der Benutzer aus der Liste der eingestellten Benutzer, für den das Token erzeugt werden soll.

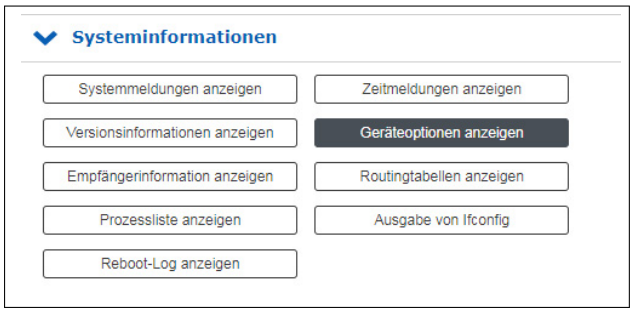
Ablaufdatum: Das Datum, an dem das Token seine Gültigkeit verliert.

Aktuelles Passwort: Das aktuelle Passwort des Benutzers, der das Token erzeugt.

Hinweis:

Nur Super-User haben die Berechtigung, ein Bearer Token zu erzeugen.

13.1.9.12 Systeminformationen



Das Menü „Systeminformationen“ bietet die Möglichkeit, wichtige Protokolldateien und Einstellungen des LANTIME anzuzeigen.

Systemmeldungen anzeigen: Anzeigen der LANTIME SYSLOG-Datei, die in */var/log/messages* gespeichert ist.

Versionsinformationen anziegen: Anzeige der zusätzlichen Geräteinformationen (Modell, Firmware, Seriennummer, eingebaute Hardwarekomponenten, etc.)

Empfängerinformation anzeigen: Anzeige der zusätzlichen Statusinformationen der eingebauten Referenzuhr.

Prozessliste anzeigen: Anzeige aller aktuell laufenden Prozesse.

Reboot Log anzeigen: Anzeigen der in */mnt/flash/data/reboot.log* gespeicherten Reboot-Logs. Die Protokolldatei enthält Informationen über frühere Systemneustarts.

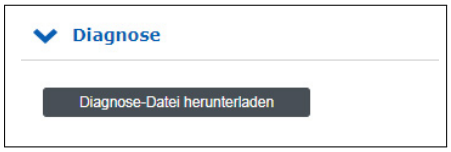
Zeitmeldungen anzeigen: Anzeige der Datei */var/log/lantime_messages*.

Geräteoptionen anzeigen: Anzeige zusätzlicher Systemparameter.

Routingtabelle anzeigen: Anzeige der Netzwerk-Routingtabelle.

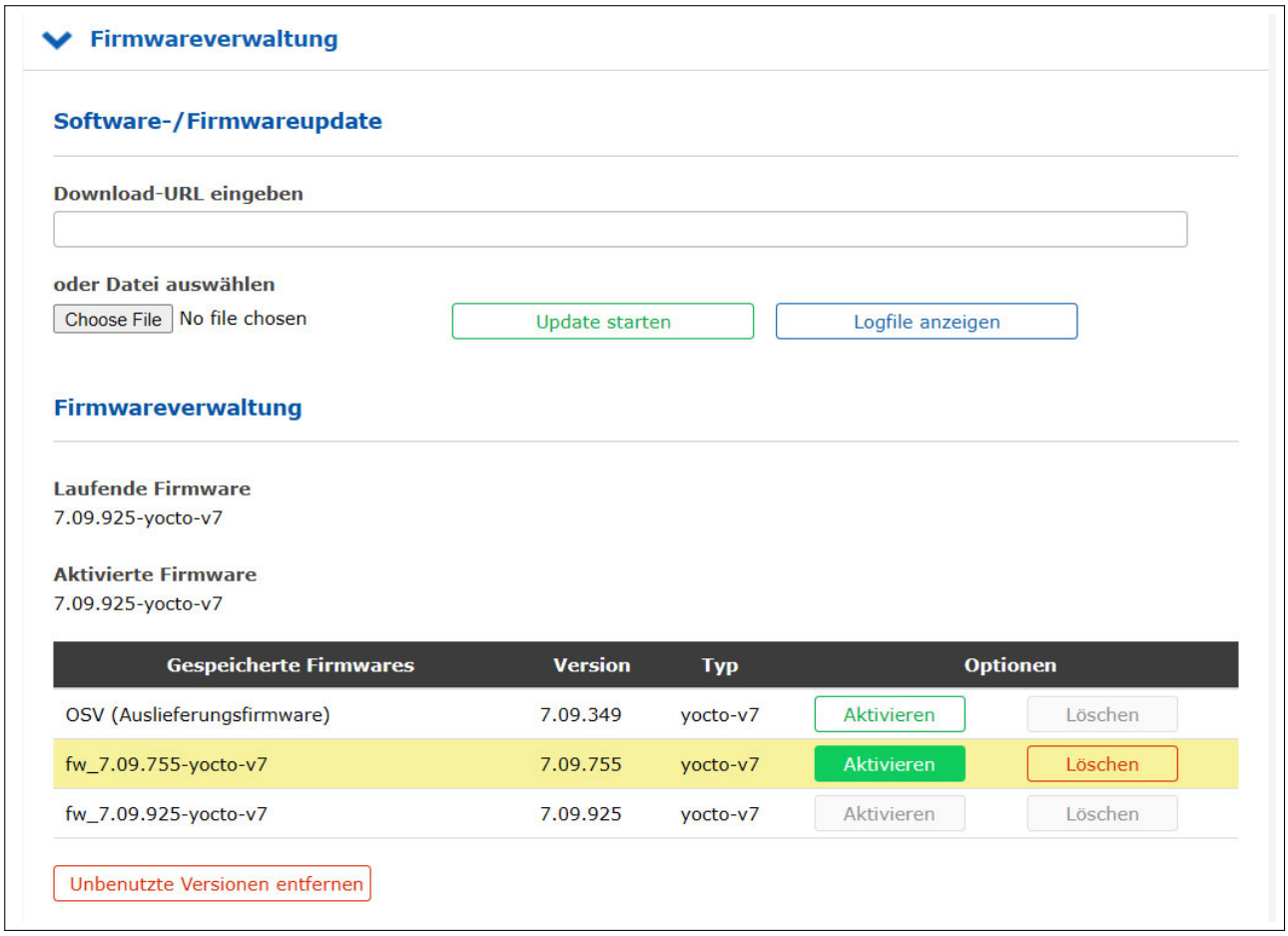
Ausgabe von Ifconfig: Anzeige von Informationen für alle Netzwerkschnittstellen (Ausgabe des Befehls „ifconfig -a“)

13.1.9.13 Download Diagnosedatei



Eine Diagnosedatei, die alle Statusdaten eines, seit dem letzten Neustart protokollierten, LANTIME-Systems enthält, kann von allen LANTIME-Servern heruntergeladen werden. Das Dateiformat der Diagnosedatei ist ein tgz-archiv. Das Archiv enthält alle wichtigen Konfigurationen und Logfiles. In den meisten Support-Fällen ist es die erste Aktion, den Benutzer aufzufordern, die Diagnose-Datei herunterzuladen, da es sehr hilfreich ist, den aktuellen Zustand des LANTIME zu identifizieren um mögliche Fehler zu finden.

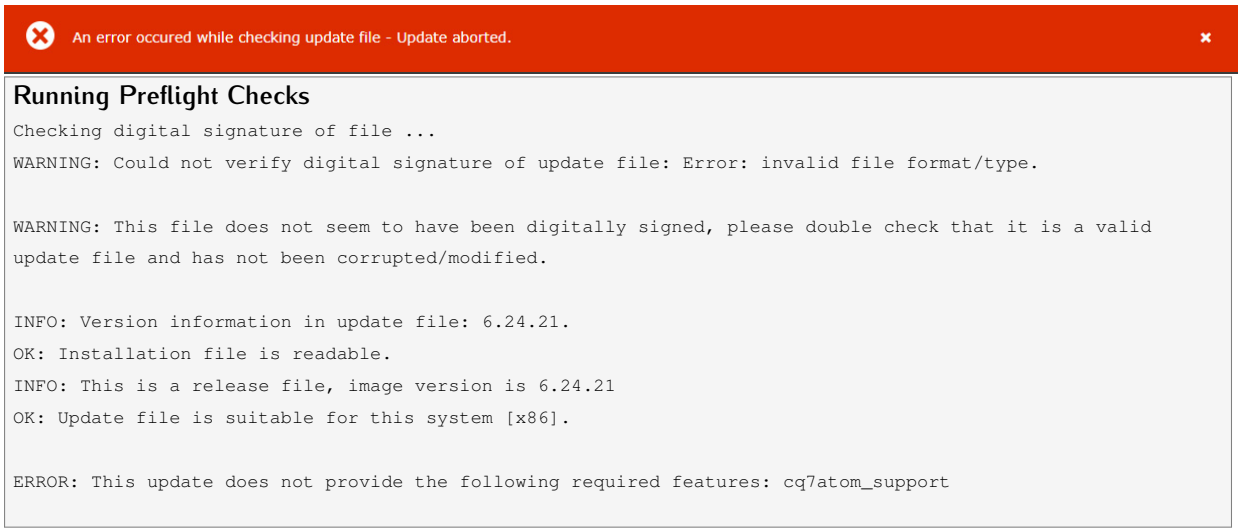
13.1.9.14 Firmwareverwaltung



Wenn Sie die Firmware Ihres LANTIME aktualisieren müssen, benötigen Sie eine bestimmte Aktualisierungsdatei. Sie können die neueste LANTIME-Firmwareversion von unserer Website herunterladen:
https://www.meinberg.de/german/sw/firmware.htm

Die Firmware-Update-Datei kann auf den LANTIME hochgeladen werden, indem Sie zuerst die Datei auf Ihrem lokalen Computer mit der Schaltfläche „Durchsuchen“ auswählen und dann auf „Update starten“ klicken. Danach werden Sie aufgefordert, den Start des Aktualisierungsprozesses zu bestätigen.

Es werden bei der Installation möglicherweise Fehler festegestellt, wie z.B. ein unbrauchbares Update-File oder eine fehlende Signatur der Update-Datei. Aus Sicherheitsgründen werden bei der Installation einige Informationen angezeigt. Nachfolgend ein Auszug von möglichen Warn- bzw. Infomeldungen:



In diesem Beispiel wird versucht ein Update-Paket zu installieren, welches den Q7-Prozessor der CPU nicht unterstützt.

LANTIME-Updates für Referenzuhren und HPS-Module

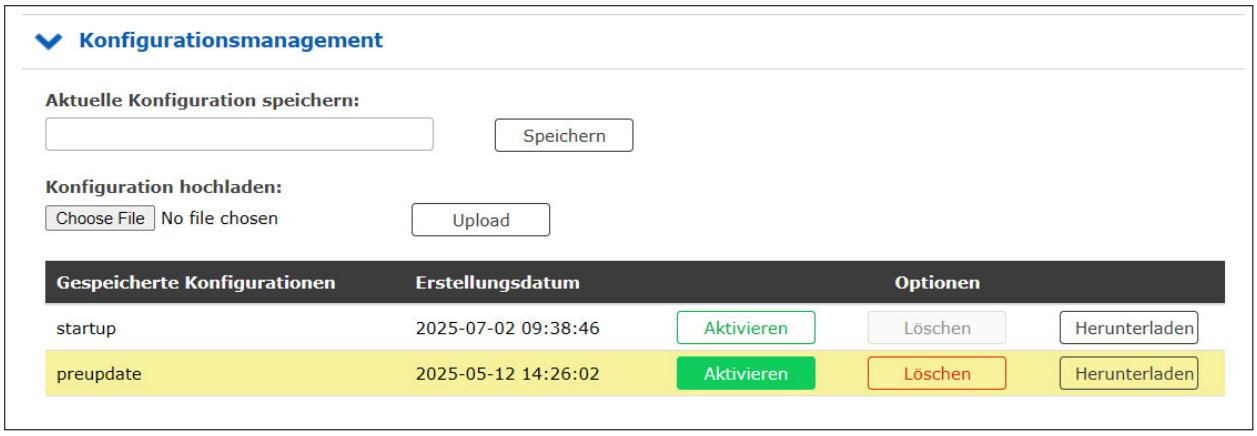
Bitte beachten Sie, dass *„Refclock Updates“* und *„HPS100 Firmware Updates“* nur auf Systemen durchführbar sind, die mit einer LANTIME Firmware LTOS > 6.24.013 laufen.

Auf dieser Seite finden Sie die aktuellsten Firmware-Update Pakete:
https://www.meinberg.de/german/sw/refclock-updates.htm

Hinweis:

Nach einem erfolgten Modul-Update wird keine neue Firmware-Version im Firmware-Management angezeigt. Refclock- und HPS100-Updates sind sofort nach dem Reboot aktiv.

13.1.9.15 Konfigurationsmanagement



Mit diesem Menü können Sie verschiedene Konfigurationsdateien zur Sicherung auf Ihrem LANTIME speichern. Mit der entsprechenden Schaltfläche **„Aktivieren“** kann eine gespeicherte Konfiguration geladen werden, mit der Schaltfläche **„Löschen“** kann eine nicht mehr benötigte Konfigurationsdatei gelöscht werden.

Mit der Schaltfläche **„Speichern“** können Sie die aktuell aktive Konfiguration des LANTIME speichern. Tragen Sie dazu in das Feld **Aktuelle Konfiguration speichern** einen eindeutigen Namen für diese Konfiguration ein und betätigen danach die **„Spechern“**-Schaltfläche. Damit erhalten Sie eine Sicherungskopie der aktuell auf Ihrem LANTIME verwendeten Konfiguration, die Sie auch auf anderen LANTIME-Systemen verwenden können. Um die aktuelle Konfiguration auf Ihren lokalen PC herunterzuladen, verwenden Sie die entsprechende Schaltfläche **„Herunterladen“**.

Konfigurationen speichern und hochladen
Um eine Konfiguration auf Ihr LANTIME-System hochzuladen, klicken Sie bitte auf die Schaltfläche **„Datei auswählen“** und wählen Sie die heruntergeladene Konfigurationsdatei auf Ihrem lokalen PC aus. Starten Sie den Upload-Vorgang mit der Schaltfläche **„Upload“**. Sobald Sie eine gültige Konfigurationsdatei auf Ihr LANTIME-System hochgeladen haben, können Sie diese Konfiguration sofort aktivieren.

13.1.9.16 Display

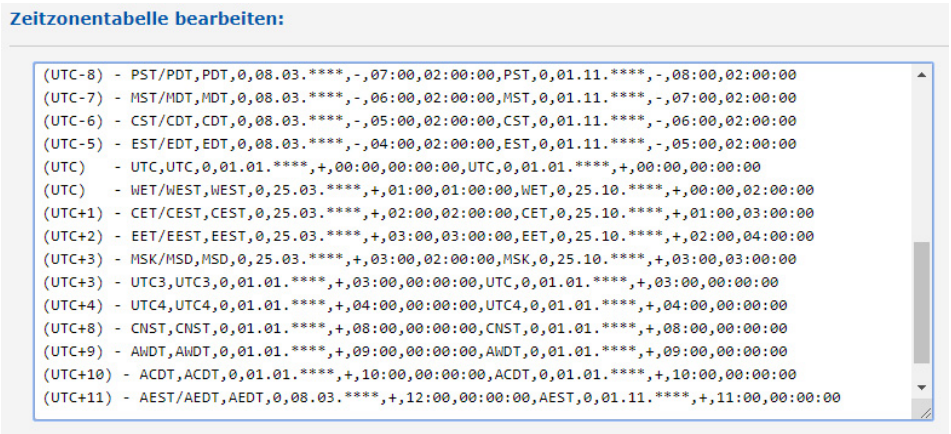
Displaybeleuchtung dauerhaft aktivieren:
Über dieses Kontrollkästchen kann die Displaybeleuchtung der Frontplatte dauerhaft eingeschaltet werden.

Zeitzone:
Zeit- und Zeitzoneneinstellung für das LANTIME-Display, die im Abschnitt „Datum/Uhrzeit“ auf der Startseite der Weboberfläche angezeigt wird.

Hinweis: Diese Einstellung hat keinen Einfluss auf die Zeit, die vom LANTIME über NTP, PTP, serielle Zeitstrings oder IRIG bereitgestellt wird.

Ausnahme:
Falls NTP so konfiguriert ist, dass es anstelle von UTC eine Ortszeit bereitstellt, müssen Sie hier in der Einstellung der Anzeigezeitzone die genaue Ortszeitzone konfigurieren. Diese Einstellung wird dann auch für NTP verwendet.

Zeitzonentabelle bearbeiten:
Mit der Schaltfläche „Zeitzonentabelle bearbeiten“ können Sie neue Zeitzonendefinitionen hinzufügen.



Beispiel:

```
(UTC+1) - CET/CEST,CEST,0,25.03.****,+,02:00,02:00:00,CET,0,25.10.****,+,01:00,03:00:00
```

Diese Zeichenkette ist die Zeitzonendefinition für Mitteleuropa. Wenn Sie eine neue Zeitzoneneinstellung benötigen, muss diese im gleichen Format konfiguriert werden. Die Zeichenkette enthält verschiedene Informationen, jede Information ist durch ein Komma getrennt. Eine detaillierte Beschreibung der verschiedenen Zeichenkettenteile am Beispiel der Zeitzoneneinstellung für Mitteleuropa ist wie folgt:

1. Feld: Anzeigename der Zeitzone. Dieser Name wird in der Liste der verfügbaren Zeitzonen angezeigt → (UTC+1) - CET/CEST

2. Feld: Abkürzung der Zeitzone mit Sommerzeit (max. 4 Buchstaben) → CEST

3. Feld: Wochentag der Umstellung auf Sommerzeit → 0 = (Sonntag)

4. Feld: Datum der Umstellung auf Sommerzeit (dd.mm.****) → 25.03.****
(Die Umstellung erfolgt am ersten Sonntag ab dem 25.03.)

5. Feld: Vorzeichen (+ oder -), addieren oder subtrahieren des Offsets von UTC → +

6. Feld: UTC-Offset Sommerzeit (hh:mm) → 02:00

7. Feld: Umschaltzeitpunkt → 02:00

8. Feld: Abkürzung der Standardzeitzone → CET

9. Feld: Wochentag der Umstellung auf Standardzeit → 0 (Sonntag)

10. Feld: Datum der Umstellung auf die Standardzeit (dd.mm.****) →
25.10.**** (Die Umstellung auf die Normalzeit erfolgt am ersten Sonntag ab dem 25.10.)

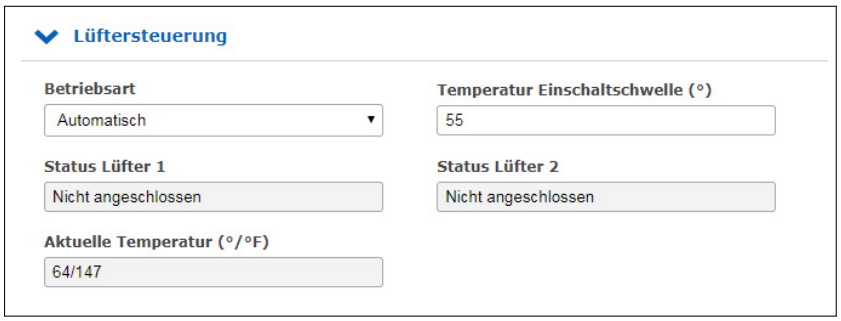
11. Field: Vorzeichen (+ oder -), addieren oder subtrahieren des Offsets von UTC → +

12. Field: UTC-Offset (hh:mm) → 01:00

13. Field: Zeitpunkt der Umstellung → 03:00

13.1.9.17 Lüftersteuerung

Diese Parameter sind nur bei LANTIME IMS-Geräten mit eingebautem Lüftermodul konfigurierbar.



Betriebsart: Einstellung der Betriebsart. Die folgenden Optionen stehen zur Verfügung:

Automatisch: In diesem Modus schalten sich die Lüfter automatisch ein, sobald die aktuelle Systemtemperatur den eingestellten Temperaturschwellenwert überschreitet.

Ein: In diesem Modus laufen die Lüfter permanent.
Aus: In diesem Modus sind die Lüfter dauerhaft ausgeschaltet.

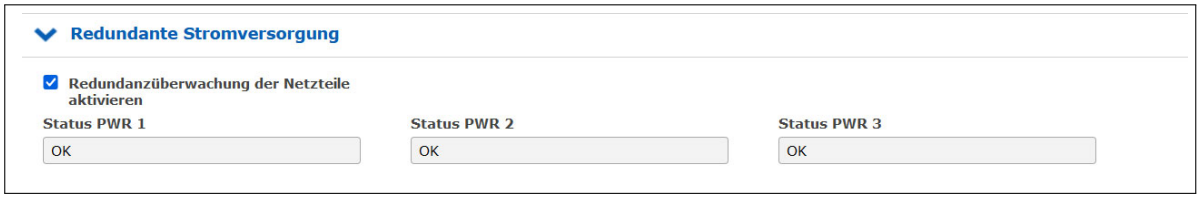
Temperatur Einschaltschwelle (°): Angabe der Systemtemperaturschwelle in Grad Celsius. Der konfigurierte Temperaturwert wird bei der Steuerung des Lüfters berücksichtigt, wenn der Lüftermodus „Automatisch“ gewählt ist.

Status Lüfter 1: Statusanzeige des 1. Lüfters.
Status Lüfter 2: Statusanzeige des 2. Lüfters.

Aktuelle Temperatur (°/°F): Anzeige der aktuellen Temperatur in Grad Celsius und Fahrenheit.

13.1.9.18 Redundante Stromversorgung

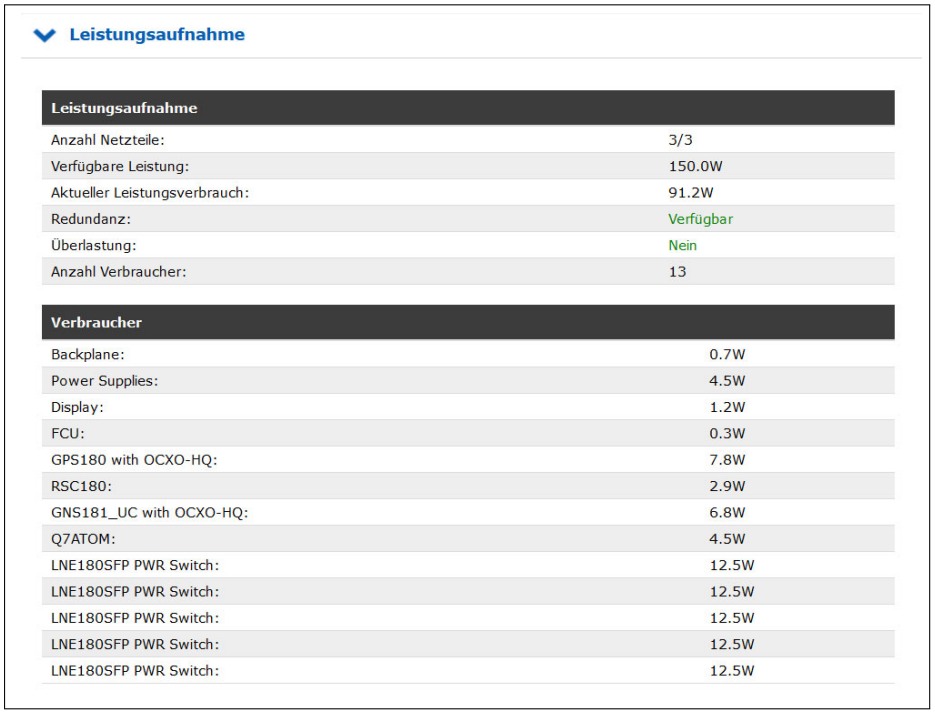
Falls es sich bei Ihrem LANTIME um ein IMS System handelt, wird in diesem Untermenü der Status der verfügbaren Netzteile angezeigt.



Redundanzüberwachung
Ist der Haken bei „Redundanzüberwachung der Netzteile aktivieren“ gesetzt, dann wird eine Benachrichtigung über die eingestellten Kanäle gesendet, falls eine redundante Spannungsversorgung in diesem System nicht mehr sichergestellt wird (zum Beispiel durch Trennen der Stromversorgung eines Netzteils). Siehe auch Kapitel Benachrichtigung.

13.1.9.19 Leistungsaufnahme

Handelt es sich bei Ihrem LANTIME um ein IMS-System, werden in diesem Untermenü alle eingesetzten Stromverbraucher angezeigt und ausgewertet.



Leistungsaufnahme	
Anzahl Netzteile:	3/3
Verfügbare Leistung:	150.0W
Aktueller Leistungsverbrauch:	91.2W
Redundanz:	Verfügbar
Überlastung:	Nein
Anzahl Verbraucher:	13

Verbraucher	
Backplane:	0.7W
Power Supplies:	4.5W
Display:	1.2W
FCU:	0.3W
GPS180 with OCXO-HQ:	7.8W
RSC180:	2.9W
GNS181_UC with OCXO-HQ:	6.8W
Q7ATOM:	4.5W
LNE180SFP PWR Switch:	12.5W
LNE180SFP PWR Switch:	12.5W
LNE180SFP PWR Switch:	12.5W
LNE180SFP PWR Switch:	12.5W
LNE180SFP PWR Switch:	12.5W

Leistungsaufnahme
Die verfügbare Leistung ergibt sich aus der Anzahl der eingesetzten Netzteile. Im Beispiel haben wir drei Netzteile mit jeweils 50 Watt Leistung - das ergibt in der Summe 150 Watt wenn alle Netzteile mit Spannung versorgt werden.

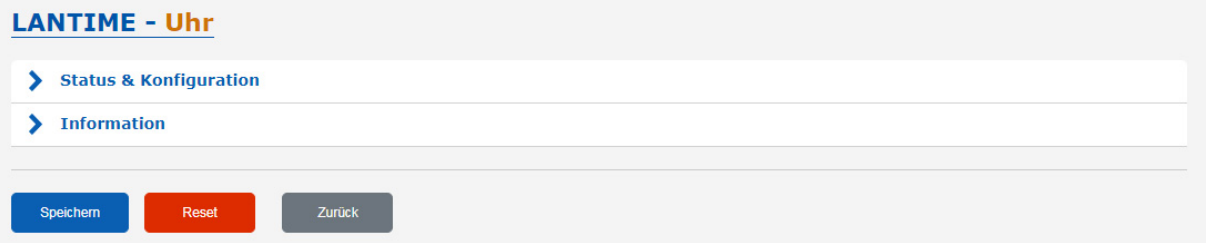
Solange, wie in diesem Beispiel, in der Reihe „Aktueller Leistungsverbrauch“ ein Wert kleiner 50W angezeigt wird, reicht ein Netzteil aus um das System zu versorgen. Bei einem Wert größer oder gleich 50W werden zwei Netzteile zur Versorgung bzw. drei aktive Netzteile benötigt um Redundanz zu gewährleisten.

Das Feld „Redundanz“ steht auf „verfügbar“, wenn die „Verfügbare Leistung“ minus dem „Aktuellen Leistungsverbrauch“ größer oder gleich 50W ist. Das Feld „Überlastung“ zeigt immer „Nein“ an, solange der „Aktuelle Leistungsverbrauch“ kleiner oder gleich der „Verfügbaren Leistung“ ist.

Verbraucher
In dieser Tabelle werden alle Verbraucher des Systems aufgelistet. Die Backplane, die CPU, die Netzteile, die Empfänger und alle anderen eingesetzten Module. Die Summe aller Verbraucher ergibt den Wert, der als „Aktueller Leistungsverbrauch“ angezeigt wird.

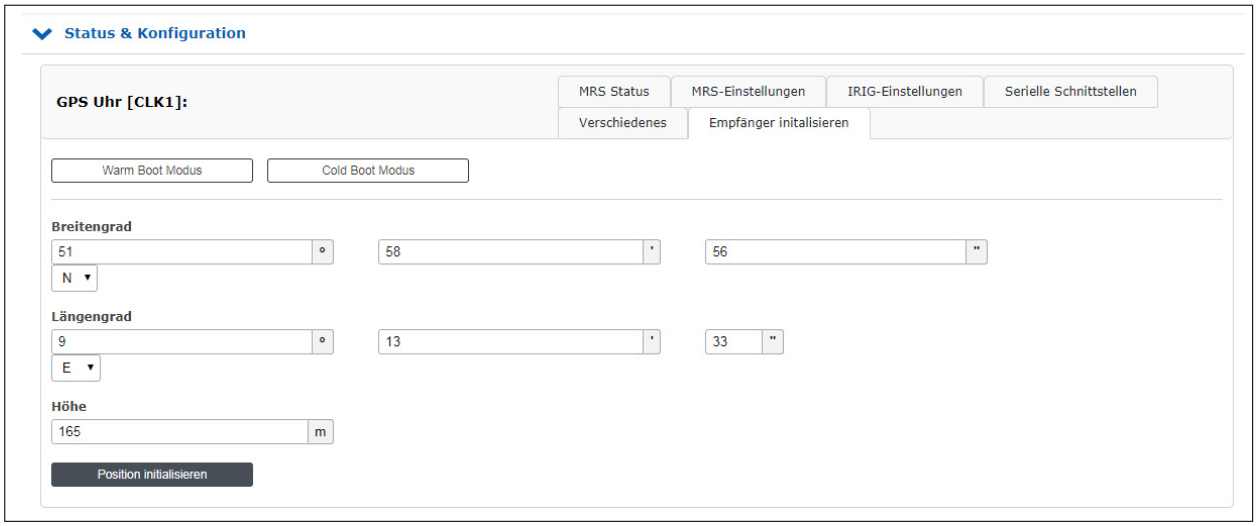
13.1.10 Menü Uhr

Im Menü „Uhr“ der Web-Oberfläche können Konfigurationen an den jeweils installierten Referenzuhren oder der RSC-Umschaltkarte vorgenommen werden.



Je nach Aufbau des Systems, d.h. ob es sich um eine einzelne Referenzuhr oder ein System mit zwei installierten Referenzuhren und einer Umschaltkarte handelt, baut sich das Web-Interface entsprechend auf. Diese Menüstruktur ist auch abhängig vom Typ der Referenzuhr und deren Optionen. Bei einer Konfiguration mit redundanten Referenzuhren erscheinen im Menü „Umschaltkarte“ die üblichen Einstellungen für „IRIG Timecode Ausgang“, „Zeitzone“, „Freigabe der Ausgänge“, „Programmierbare Impulse“ und „Synthesizer“.

Einstellungen für „MRS (Prioritäten, Offset)“, „IRIG“, „Serielle Schnittstellen“, „Satellitennavigationsmodus“, „Antennenkabellänge“, „GNSS Simulationsmodus“ und „Empfänger-Initialisierung“ werden direkt über die ausgewählte Referenzuhr vorgenommen.



13.1.10.1 Synchronisation über GNSS (GXL-Empfänger)

In diesem Kapitel wird beschrieben, wie Sie den GXL-Referenzempfänger schnell für die Synchronisation mit GNSS-Diensten einrichten können.

Hinweis:

Diese Funktion steht ab der LTOS Firmware-Version 7.08.007 zur Verfügung.

Schritt 1: Verbindung des GXL-Empfängers mit der GNSS-Multiband-Antenne

Stellen Sie sicher, dass der GXL-Empfänger an eine korrekt installierte GNSS-Multibandantenne angeschlossen ist.

Schritt 2: Auswählen der Satellitenkonstellationen

Der GXL-Empfänger ist in der Lage, Signale der Satellitenkonstellationen GPS, Galileo, BeiDou und GLONASS gleichzeitig zu empfangen.

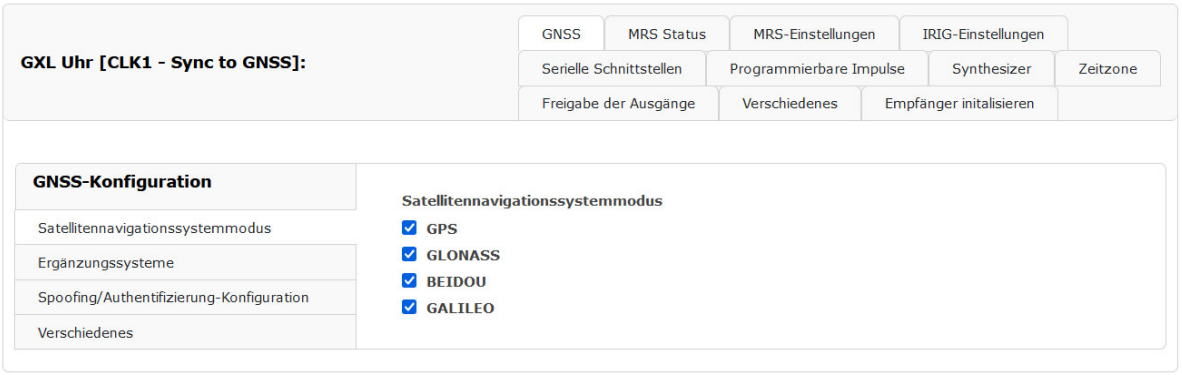


Abbildung: Festlegen der zu verwendenden Satellitenkonstellationen

Der GXL-Empfänger unterstützt auch die japanische QZSS-Konstellation und eine Reihe nationaler satellitengestützter Erweiterungssysteme (SBAS). Die folgenden Ergänzungssysteme werden unterstützt:

- Europäischer geostationärer Navigations-Overlay-Dienst (EGNOS) - Europa
- Wide Area Augmentation System (WAAS) – Vereinigte Staaten, Kanada, Mexiko
- GPS-gestützte Geo Augmented Navigation (GIGAN) - Indien
- Multifunktionales satellitengestütztes Erweiterungssystem (MSAS) – Japan
- System für differentielle Korrekturen und Überwachung (SDCM) – Russland

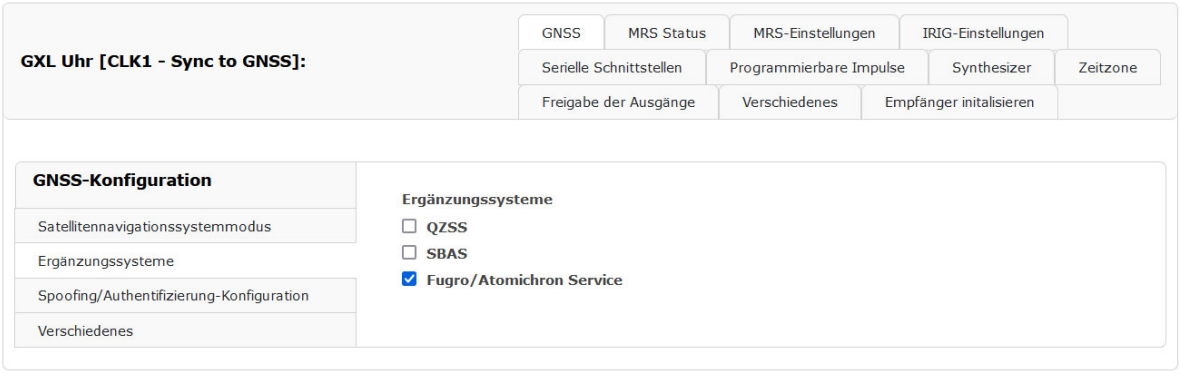


Abbildung: Unterstützung für die japanische QZSS-Konstellation und nationale SBAS-Konstellationen.

Sie können festlegen, welche Konstellationen verwendet und welche ausgeschlossen werden sollen, indem Sie sich in das Webinterface Ihres LANTIME-Systems einloggen und wie folgt vorgehen:

1. Öffnen Sie das Menü „**Uhr**“ → „**Status & Konfiguration**“.
2. Wählen Sie das entsprechende Uhrenmodul aus.
3. Klicken Sie auf die Registerkarte „GNSS“.
4. Wählen Sie die Konstellationen mit Hilfe der Kontrollkästchen unter „Satellitennavigationssystemmodus“ aus.
5. Falls gewünscht, aktivieren Sie die Unterstützung für regionale Erweiterungssysteme unter „Ergänzungssysteme“.

Hinweis:

Wenn Sie die Fugro NMA Spoofing-Erkennung verwenden möchten, stellen Sie sicher, dass „**Fugro AtomiChron® Service**“ unter „**Ergänzungssysteme**“ aktiviert ist.

Schritt 3: Konfigurieren der Signallaufzeit

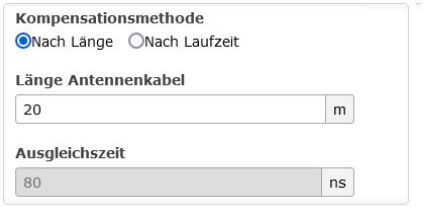
Die Signallaufzeit des Satellitensignals wird durch die Kabellänge beeinflusst und kann zu einer Verzögerung des Signalempfangs von ca. 4 ns/m Kabellänge führen (bei Verwendung des Antennenkabels H155).

Damit die angeschlossene Referenzuhr die kabelbedingte Laufzeit des Signals kompensieren kann, müssen Sie entweder die Länge des Antennenkabels in Metern angeben (von der Antenne bis zum Meinberg-System) oder in den Konfigurationseinstellungen Ihrer Referenzuhr die ermittelte Offset-Zeit in Nanosekunden eintragen.

Gehen Sie dazu wie folgt vor:

1. Von der selben Seite wie oben Schriit 1 (**Uhr** → **Status und Konfiguration**), wählen Sie die Registerkarte „**Verschiedenes**“ des jeweiligen Empfängemoduls aus.

2. Unter „**Kompensationsmethode**“ wählen Sie die Kompensationsmethode und geben Sie den entsprechenden Wert ein (Kabellänge oder Laufzeit).



Hinweis:

Der voreingestellt Wert in diesem Feld beträgt 20 m oder 80 ns. LANTIME OS unterstützt einen Maximalwert von 2000 m oder 8000 ns.

Die Verzögerungszeit kann automatisch als Kabellänge multipliziert mit 4 geschätzt werden. Dabei wird davon ausgegangen, dass Sie ein H155-Antennenkabel verwenden. Dies liefert eine vernünftige Schätzung der Laufzeitverzögerung durch das Antennenkabel.

Wenn Sie einen anderen Kabeltyp oder eine andere Übertragungsmethode verwenden, muss die Laufzeitverzögerung manuell berechnet und in Nanosekunden eingegeben werden. Eine manuelle Angabe der Laufzeitverzögerung wird auch empfohlen, wenn Sie die Zeitgenauigkeit im Vergleich zu einem Zeitstandard wie UTC weiter verbessern wollen.

Schritt 4: Konfiguration des Positionssperrverhaltens

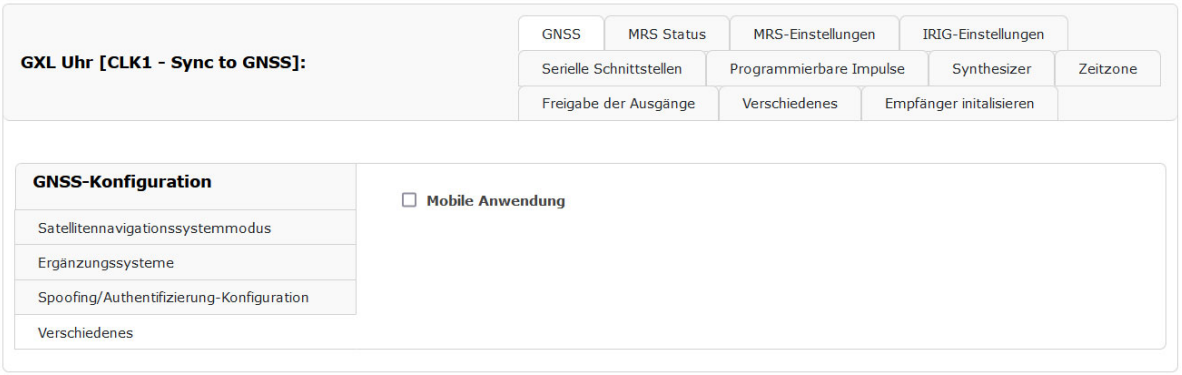


Abbildung: Mobil-Modus aktivieren

Wenn Ihr GXL-Empfänger mobil betrieben werden soll (z.B. an Bord eines fahrenden Fahrzeugs), sollten Sie „**Mobile Anwendung**“ unter „**Verschiedenes**“ aktivieren. Der mobile Modus ermöglicht es, die Position des Empfängers dynamisch zu halten, was auf Kosten einer gewissen Genauigkeit der Uhr und der Zuverlässigkeit der Spoofing-Erkennung geht.

Wenn Ihr GXL-Empfänger an einem festen Standort eingesetzt wird, stellen Sie sicher, dass diese Option deaktiviert ist, um die Genauigkeit der Uhr und die Zuverlässigkeit der Spoofing-Erkennung zu maximieren.

Schritt 5: Konfiguration der Authentifizierung von Navigationsnachrichten

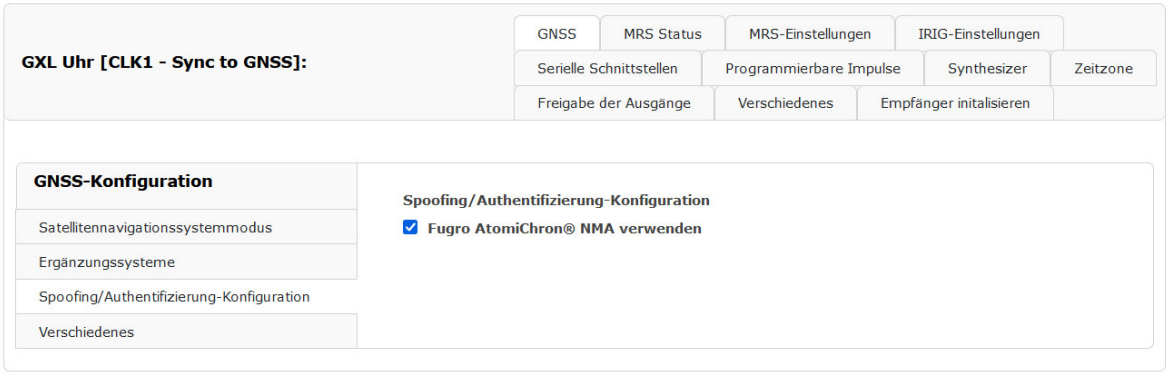


Abbildung: Konfigurieren der Authentifizierung von Navigationsnachrichten (Spoofing-Erkennung)

Um die Navigation Message Authentication (NMA) für die Spoofing-Erkennung zu aktivieren, sollten Sie „**Fugro NMA verwenden**“ entsprechend aktivieren.

Für den AtomiChron®-Service von Fugro ist ein aktives Abonnement erforderlich. Weitere Informationen zur Verwaltung eines AtomiChron®-Abonnements finden Sie in Kapitel 13.1.10.2, Aktivierung des AtomiChron®-Dienstes (GXL-Empfänger).

Weitere Informationen über die Authentifizierung von Navigationsnachrichten im Allgemeinen finden Sie in Kapitel 16.8, Funktionsweise von Navigation Message Authentication (NMA).

Hinweis:

Stellen Sie sicher, dass der Galileo- und Fugro/AtomiChron-Empfang entsprechend aktiviert ist, wie in Schritt 2 oben beschrieben!

Schritt 6: MRS-Konfiguration

Wenn Sie nur den GNSS-Empfang konfigurieren möchten, fahren Sie mit dem MRS-Konfigurationsprozess fort, der in Kapitel MRS Einstellungen, „MRS Einstellungen“ beschrieben wird.

Andernfalls fahren Sie mit der Konfiguration der anderen Referenzquellen fort.

Letzte Schritte

Nach dem Anschluss der Antenne und der Stromversorgung ist die Referenzuhr betriebsbereit.

Nach etwa zwei Minuten nach dem Einschalten der Anlage ist der Oszillator warmgelaufen und hat damit die für den Empfang von Satellitensignalen erforderliche Basisgenauigkeit erreicht. Sind im batteriegepufferten Speicher der Referenzuhr gültige Almanach- und Ephemeridendaten vorhanden und hat sich die Position des Empfängers seit dem letzten Einschalten nicht verändert, kann die CPU der Anlage berechnen, welche Satelliten aktuell empfangbar sein sollten.

In diesem Fall muss nur ein einziger Satellit empfangen werden, damit sich der Empfänger synchronisieren kann. Andernfalls wechselt das System in den Warmstart- oder Kaltstartmodus, wie unten beschrieben.

Warm Boot

Wenn sich der Standort des Empfängers seit dem letzten Einschalten der Anlage um mehrere hundert Meilen verändert hat, stimmen die Elevation und die Dopplerverschiebung der Satelliten nicht mit den berechneten Werten überein. Dies führt dazu, dass das System in den Modus „Warm Boot“ wechselt, in dem es systematisch nach Satelliten für den Empfang sucht.

Der Empfänger kann anhand der gültigen Almanachdaten die Identifikationsnummern der vorhandenen Satelliten ermitteln. Wenn vier Satelliten empfangen werden können, kann die neue Position des Empfängers bestimmt werden und das Gerät wechselt in den Modus „**Normal Operation**“.

Cold Boot

Wenn keine Almanachdaten verfügbar sind (z. B. weil der batteriegepufferte Speicher gelöscht oder beschädigt wurde), startet die GNSS-Referenzuhr im „Cold Boot“-Modus, in dem der Empfänger nach einem Satelliten sucht und den gesamten Almanach liest. Der Almanach wird alle 12,5 Minuten vollständig übertragen, aber der Empfänger muss möglicherweise auf den Beginn der nächsten Übertragung warten. Dieser Vorgang kann bis zu 25 Minuten dauern, danach schaltet das System in den „Warm Boot“-Modus.

13.1.10.2 Aktivierung des AtomiChron®-Dienstes (GXL-Empfänger)

Der GXL-Empfänger unterstützt den AtomiChron®-Service von Fugro, mit dem die Integrität und Authentizität eingehender GNSS-Nachrichten von allen wichtigen GNSS-Konstellationen überprüft werden kann. Die zur Authentifizierung Ihrer GNSS-Signale erforderlichen Daten werden über eine separate L-Band-Satellitenfrequenz übertragen, die von der Inmarsat-Konstellation gesendet wird, die Ihr GXL-Empfänger zusätzlich zu den eigentlichen GNSS-Signalen empfängt.

AtomiChron® ist ein kostenpflichtiger Abonnementdienst und die Lizenz dafür muss daher aktiviert und danach gelegentlich erneuert werden. Die Regelmäßigkeit der Lizenzverlängerung hängt von der Dauer Ihres Dienstleistungsvertrags ab.

Da das IMS LANTIME-System, in dem Ihr GXL-Empfänger installiert ist, aus Gründen der Praktikabilität oder der Betriebssicherheit vom öffentlichen Internet isoliert sein sollte, wird das Signal, das zur Aktivierung oder Erneuerung einer AtomiChron®-Lizenz erforderlich ist, über das gleiche L-Band-Satellitensignal übertragen, über das es die Authentifizierungsdaten empfängt. Sobald ein Abonnementvertrag abgeschlossen und bezahlt ist (oder ein kostenloses Abonnement in Anspruch genommen wird), wird das Aktivierungssignal über einen bestimmten Satellitenstrahl (Beam) übertragen.

Zu diesem Zweck muss in Ihrem IMS LANTIME-System der GXL-Empfänger installiert, aktiviert und mit einer funktionierenden und betriebsbereiten GNSS-Multiband-Antenne verbunden sein.

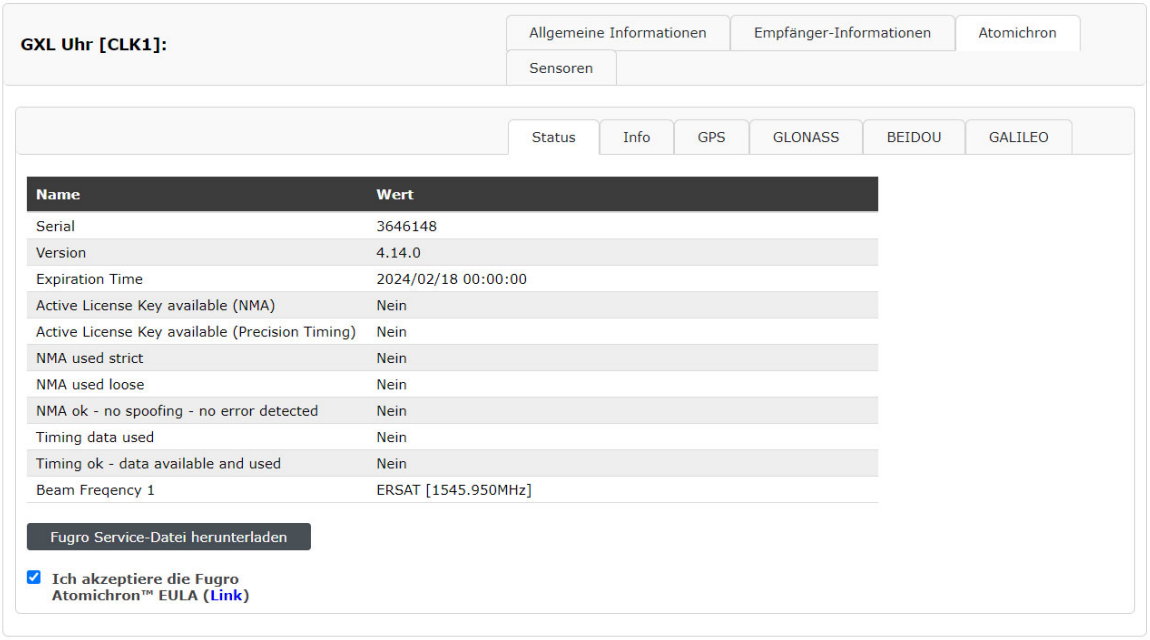


Abbildung: Anzeige von AtomiChron®-bezogenen Informationen in der LTOS-Webschnittstelle

Bestimmte Informationen werden von Meinberg und Fugro benötigt, damit Ihre GXL-Referenzuhr die entsprechenden Aktivierungsdaten erhält. Diese Informationen können bequem von der Weboberfläche Ihres IMS LANTIME-Systems heruntergeladen werden, indem Sie den Menüpunkt „**Uhr**“ auswählen, das Feld „**Informationen**“ öffnen, die Registerkarte „AtomiChron“ für das GXL-Empfängermodul („GXL Uhr“) auswählen, die Fugro AtomiChron® EULA einsehen und akzeptieren und auf die Schaltfläche „**Fugro Service-Datei herunterladen**“ klicken.

Dadurch wird der Download einer Textdatei gestartet, die alle von Meinberg und Fugro benötigten Informationen enthält. Diese Datei sollte dann als Anhang an atomichron@meinberg.de gesendet werden, wenn Sie von Meinberg dazu aufgefordert werden (d.h. wenn die Zahlung für Ihr Abonnement eingegangen ist oder wenn Sie einen Anspruch auf ein kostenloses Abonnement geltend machen).

Sobald Meinberg diese Datei erhalten und verarbeitet hat, sollten die Aktivierungsdaten innerhalb von drei Arbeitstagen über die, in der Fugro Servicedatei angegebenen, Frequenzen übertragen werden. Wenn Sie einen besonderen Wunsch bezüglich der Terminierung der Aktivierungsdatenübertragung haben, teilen Sie dies bitte ebenfalls in der E-Mail mit, wenn Sie die Fugro Service Datei an Meinberg senden. Bitte beachten Sie jedoch, dass Meinberg nicht garantieren kann, dass ein bestimmter Terminwunsch berücksichtigt werden kann.

Sobald Sie die Fugro Servicedatei an Meinberg gesendet haben, ist es wichtig, dass Sie Ihr IMS LANTIME-System betriebsbereit und mit einer korrekt positionierten und funktionierenden GNSS Multi-Band Antenne verbunden lassen, bis die Aktivierungsdaten empfangen werden. Sie können überprüfen, ob der AtomiChron® Service korrekt aktiviert wurde, indem Sie den Menüpunkt „**Uhr** → **Informationen** → **GXL-Uhr** → **AtomiChron** → **Status**“ wie oben beschrieben öffnen. Falls aktiviert, steht in der Zeile „*Aktiver Lizenzschlüssel verfügbar (NMA)*“ **Ja**, während in der Zeile „Ablaufzeit“ das Datum und die Uhrzeit des Ablaufs Ihrer aktuellen AtomiChron®-Lizenz angezeigt wird.

Achtung!

Bitte beachten Sie, dass die Aktivierungsdaten in der Regel nur einmal übertragen werden und normalerweise nicht an Wochenenden oder niederländischen Feiertagen übermittelt werden.

Wenn Ihr GXL-Empfängermodul immer noch nicht anzeigt, dass die Aktivierung innerhalb von 72 Stunden nach Versand der Fugro-Service-Datei (oder innerhalb von 24 Stunden nach einem angeforderten Aktivierungsdatum) erfolgt ist, wurde das Aktivierungssignal möglicherweise übersehen.

Überprüfen Sie in diesem Fall, ob die Antenne korrekt installiert und angeschlossen ist und ob sie korrekt empfängt. Dies kann im Webinterface erfolgen, indem Sie das Menü „**Uhr** → **Informationen** → **GXL-Uhr** → **AtomiChron** → **Info**“ auswählen. Der Eintrag „LBAND SV Information available“ (LBAND SV-Informationen verfügbar) sollte „*Yes*“ (Ja) anzeigen, um darauf hinzuweisen, dass das Gerät auf die Inmarsat-Satelliten ausgerichtet ist, die für die Übertragung der AtomiChron®-Daten verwendet werden. Stellen Sie sicher, dass die Antenne nicht an einem Ort installiert ist, an dem sie Störungen durch andere L-Band-Emissionen oder Signalreflexionen ausgesetzt sein könnte (insbesondere in bebauten Gebieten).

Sobald Sie sicher sind, dass die Uhr das Signal zuverlässig empfangen kann, wenden Sie sich bitte an den Technischen Support von Meinberg unter *techsupport@meinberg.de*, um eine weitere Übertragung des Aktivierungssignals zu planen.

Die rechtzeitige Erneuerung Ihrer AtomiChron®-Lizenz sicherstellen

Atomichron License Expired	Fehler	Zuletzt: Thu Jan 18 11:30:42 2024	☐	☐	☐	☐	☐	☐
Atomichron License Expiration Warning	Warnung	Letztes Event: Sun Jan 21 00:00:28 2024	☐	☐	☐	☐	☐	☐
Atomichron receiver report spoofing detected	Fehler	Letztes Event: Thu Jan 18 11:30:42 2024	☐	☐	☐	☐	☐	☐
Atomichron receiver report spoofing stopped	Info		☐	☐	☐	☐	☐	☐

Abbildung: Konfiguration der Benachrichtigungen, um sicherzustellen, dass die AtomiChron®-Lizenz nicht abläuft

Ein AtomiChron®-Abonnement wird nicht automatisch verlängert. Eine Verlängerung muss daher explizit bei Meinberg erworben werden.

Bitte achten Sie darauf, dass Ihre AtomiChron®-Lizenz rechtzeitig verlängert wird, damit der Dienst nicht durch das Ablaufen der Lizenz unterbrochen wird. Meinberg wird sich bemühen, Sie zu kontaktieren, um Sie an den bevorstehenden Ablauf zu erinnern, kann aber nicht garantieren, dass wir in der Lage sein werden, die jeweils zuständige Person zu erreichen.

Meinberg empfiehlt daher, dass Sie auch:

- eine Art organisatorische Erinnerung (Kalendersoftware o.ä.) einrichten, um sicherzustellen, dass Sie an die Notwendigkeit der Erneuerung Ihrer AtomiChron®-Lizenz erinnert werden,
- Ihre LTOS-Benachrichtigungen so konfigurieren, dass Sie benachrichtigt werden (per E-Mail, SNMP, etc.), wenn Ihre AtomiChron®-Lizenz demnächst (in 28 Tagen) abläuft und wenn sie abgelaufen ist.

Weitere Informationen zur Konfiguration von Benachrichtigungen finden Sie im Kapitel Benachrichtigung.

13.1.10.3 MRS Status

Hier werden die Status der Referenzeingänge angezeigt:

Priorität: Anordnung der Zeitquelle nach Ihrer Priorisierung.

Quelle: Art der Referenzquelle.

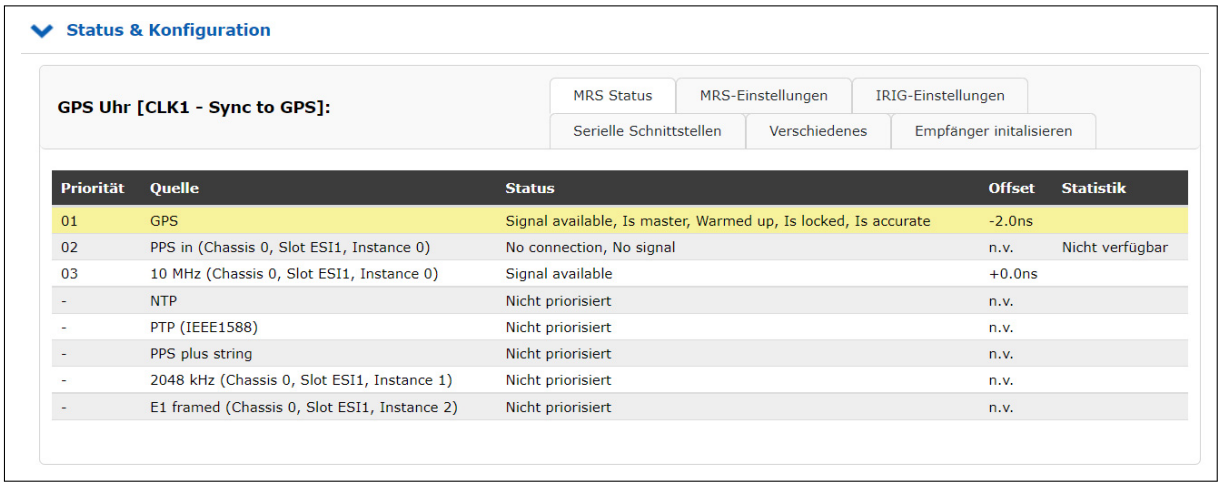
Status:

Keine Verbindung, kein Signal	→	die Referenzquelle ist nicht verfügbar
Signal verfügbar	→	die Referenzquelle ist verfügbar
ist Master	→	die Referenzquelle wird zur Systemsynchronisation verwendet
ist gesperrt	→	Das System synchronisiert sich mit der Referenzquelle
ist exakt (akkurat)	→	Grundgenauigkeit der Synchronisation ist erreicht

Offset: Zeitdifferenz der Referenzuhr zur vorgegebenen Zeitquelle.

Statistik:

Spanne	→	Wenn die Differenz zwischen dem Min./Max.-Wert der Zeitquelle über einem definiertem statistischen Intervall liegt
Step-Kompensation	→	Zeigt einen großen Sprung der Referenzquelle an (derzeit nur für PTP verfügbar).
Auto-Bias	→	Bestimmter Zeitversatz für die Quelle gegenüber einer versatzfreien Zeitquelle.



Priorität	Quelle	Status	Offset	Statistik
01	GPS	Signal available, Is master, Warmed up, Is locked, Is accurate	-2.0ns	
02	PPS in (Chassis 0, Slot ESI1, Instance 0)	No connection, No signal	n.v.	Nicht verfügbar
03	10 MHz (Chassis 0, Slot ESI1, Instance 0)	Signal available	+0.0ns	
-	NTP	Nicht priorisiert	n.v.	
-	PTP (IEEE1588)	Nicht priorisiert	n.v.	
-	PPS plus string	Nicht priorisiert	n.v.	
-	2048 kHz (Chassis 0, Slot ESI1, Instance 1)	Nicht priorisiert	n.v.	
-	E1 framed (Chassis 0, Slot ESI1, Instance 2)	Nicht priorisiert	n.v.	

Abbildung: Ein Beispiel für verfügbare Referenzsignale in der Reihenfolge der Priorität.

Die Tabelle zeigt die möglichen Referenzquellen - die Verfügbarkeit hängt von der Hardwarekonfiguration des Systems ab.

Signal	**bereitgestellt durch**
GPS	eingebauter GPS-Empfänger
GNSS	eingebauter GNS-Empfänger
PPS plus string	externer Signalgenerator
NTP	externer NTP Server
PTP (IEEE1588)	HPS / TSU Zeitstempelmodul
SyncE	HPS Zeitstempelmodul
E1 framed PPS In Fixed Freq.	IMS ESI - Eingangsmodul für 2.048 MHz, 2.048 MBit/s, 1PPS und variable Frequenzen
IRIG PPS in 10 MHz	IMS MRI - IRIG, 1PPS, 10 MHz Eingangsmodul
Video In LTC In Freq. In PPS In	IMS VSI - Video-Signaleingangsmodul

13.1.10.4 MRS Einstellungen

MRS steht für „Multi Reference Source“. Das ist eine spezielle Funktionalität des Empfängers, der neben GNSS auch andere Eingangssignale als Referenz für die Synchronisation verwenden kann.

13.1.10.5 Bevorzugte Quellen

In den MRS-Einstellungen können Sie eine Prioritätenliste der Eingangssignale konfigurieren, wie die Umschaltung erfolgen soll, falls eine Master-Referenz nicht verfügbar ist. Die Auswahl der Signale in der Liste wird vom LANTIME entsprechend der Hardwarekonfiguration automatisch generiert. Die Prioritätenliste der Eingangssignale sollte in absteigender Reihenfolge bezüglich der Genauigkeit der Signale konfiguriert werden.

Hier ein Beispiel, wie Sie eine Prioritätenliste in absteigender Reihenfolge konfigurieren können:
1. Quelle: GNSS / GPS
2. Quelle: PPS + String
3. Quelle: PTP – IEEE1588
4. Quelle: external NTP Server

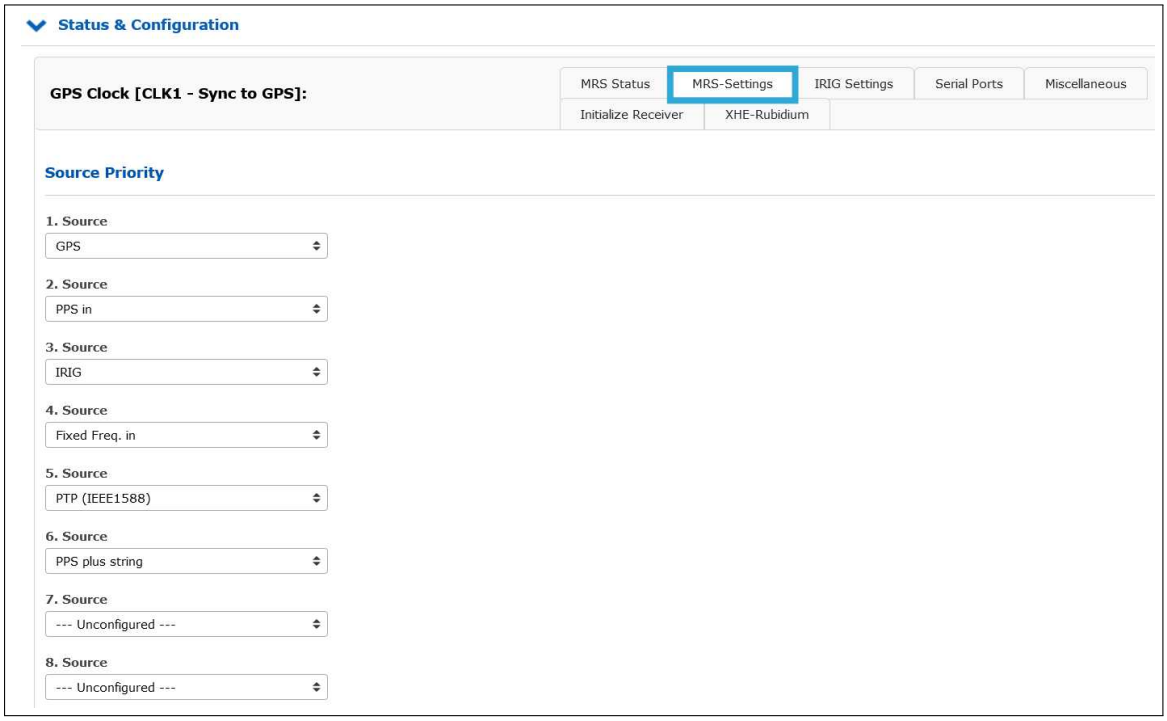


Abbildung: Konfigurationsbeispiel für Referenzsignale in absteigender Reihenfolge.

PTP als Referenzsignal

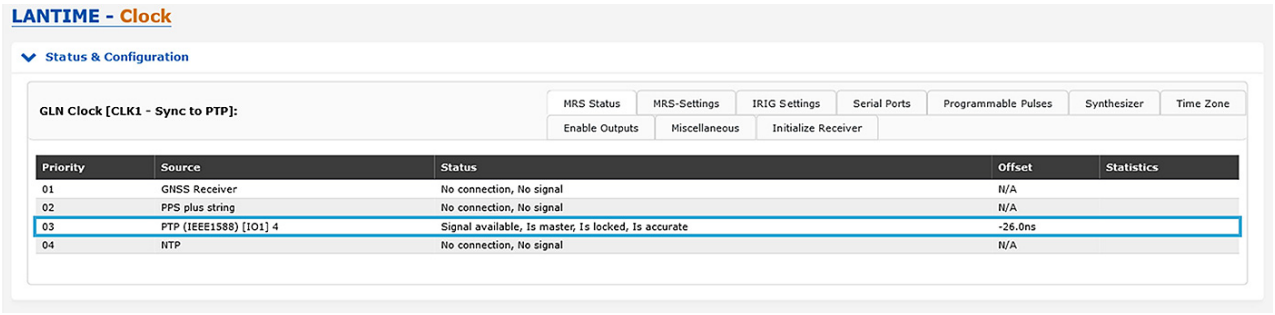


Abbildung: IMS-HPS100 auf IO1 als PTP-Referenz

HPS100-Module (mit FW ≥1.4.1) und PSX-Module können im I/O Slot im PTP Master- oder Slave-Modus arbeiten. So kann das PTP-Modul für das System als hochpräziser PTP-Referenzeingang (siehe Abbildung) arbeiten.

Kommen mehrere PTP-Module in einem System zum Einsatz und befinden diese sich im Slave Modus, wird mittels BMCA-Verfahren (Best Master Clock Algorithm) ein Slave ausgewählt, welcher dann in der MRS-Prioritätenliste aufgeführt wird (siehe Abbildung). Als Master-Referenz kann dieser dann seine Korrekturdaten an die im System verbauten Clock-Module (CLK1 u. CLK2) senden.

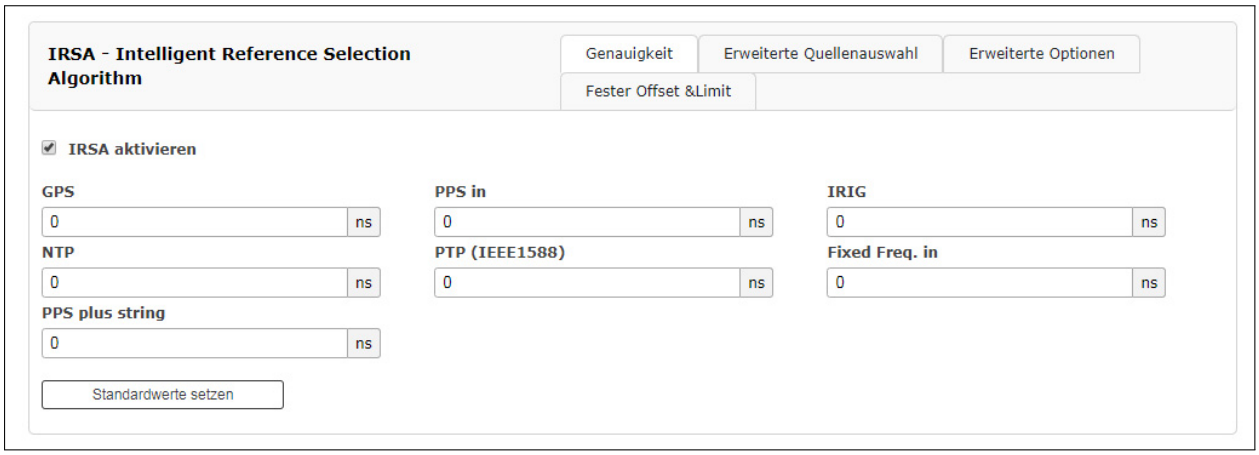
Hinweis:

Die TSU GbE unterstützt die oben beschriebene Funktion nicht.

Bei einer redundanten Empfängerkonfiguration und dem Einbau der HPS100 in einem **ESI/MRI-Slot** funktioniert der Master/Slave-Modus nur für die zugeordnete Clock. Soll der Empfänger **CLK1** über eine HPS100 synchronisiert werden, dann muss sich diese entweder in einem IO-Slot befinden, oder im **MRI1/ESI1-Slot** verbaut sein.

13.1.10.6 IRSA - Intelligent Reference Selection Algorithm

IRSA steht für einen intelligenten Referenzauswahlalgorithmus. Fällt ein Master-Signal aus, sorgt IRSA dafür, dass das Umschalten auf das nächste Referenzsignal in der Prioritätenliste automatisch und reibungslos erfolgt. IRSA berücksichtigt auch die sehr stabile Holdover-Performance des lokalen Oszillators. Der Auswahlalgorithmus stellt sicher, dass das Umschalten von dem höheren Referenzsignal zu dem weniger genauen verzögert wird, solange der hochstabile Oszillator eine bessere Holdover-Genauigkeit bietet, als das nächste verfügbare Referenzsignal in der Prioritätenliste bereitstellen kann.



Gehen Sie folgendermaßen vor um sicherzustellen, dass IRSA ordnungsgemäß funktioniert:

1. Konfigurieren Sie eine Prioritätsliste der verfügbaren Referenzsignale in absteigender Reihenfolge von der übergeordneten zu der untergeordneten Referenz im Menü „MRS-Einstellungen“.

2. Aktivieren Sie IRSA im IRSA-Menü. Standardmäßig ist IRSA deaktiviert.

3. Geben Sie die geschätzten Präzisionswerte für die Eingangsreferenzsignale für diese aktivierten Präzisionsfelder ein. Der Genauigkeitswert bestimmt die Wartezeit beim Wechsel zur nächsten Referenzquelle, wenn der aktuelle Master nicht verfügbar ist.

   Hier sind einige geschätzte Präzisionswerte, die Sie als Standardwerte laden können:
   - GPS / GNSS als erste Priorität hat die höchste geschätzte Genauigkeit:100 ns
   - ext. Osc. (z.B. Rubidium): 120 ns
   - PTP IEEE 1588: 100 ns
   - PPS plus String: 100 ns
   - NTP: 100 us

13.1.10.7 MRS Optionen

Erweiterte Quellenauswahl
Die Firmware V6.24 und die folgenden Versionen unterstützen eine gemischte Kombination von Referenzsignalen für die Synchronisation. Im gemischten Modus können Sie eine Quelle nur für die ToD (Time of Day) -Synchronisation und eine andere Quelle für Phase und Frequenz auswählen. Die Phase und Frequenz kann durch eine sehr stabile und genaue Quelle, zum Beispiel eine Atomuhr, wie Rubidum oder Cäsium, bereitgestellt werden.

Die Uhrzeit (ToD) stellt eine „Wanduhrzeit" dar - eine bestimmte Zeit mit Stunden, Minuten, Sekunden und dem entsprechenden Datum. Die ToD-Information kann nicht durch eine Atomuhr allein geliefert werden. Wenn Sie die ToD in Ihrem System benötigen, müssen Sie daher eines der Referenzsignale auswählen, das die ToD-Informationen enthält, z. B. GPS, NTP, PTP, PPS plus String.

Wenn Sie den gemischten Modus verwenden, wird die Referenzuhr zuerst von einem Referenzsignal gesteuert, welches ToD-Informationen enthält. Der Oszillator wird grob eingestellt, bis er die höchste Genauigkeit erreicht, die mit dieser Referenz erreicht werden kann. Danach schaltet der Referenztaktgeber automatisch auf eine genauere Quelle um, zum Beispiel ein 1PPS, das von einer externen Atomuhr kommt, die eine hochstabile Phase liefert, oder ein 10MHz-Signal, um eine stabile Frequenz bereitzustellen.

Standardmäßig sind ToD und Phase für jede verfügbare Referenzquelle aktiviert. Wenn Sie den gemischten Modus verwenden möchten, wählen Sie die ToD für ein Referenzsignal und die Phase für ein anderes. Die Referenzquellen, die Sie verwenden möchten, sollten zuerst in der Liste „Bevorzugte Quellen" konfiguriert werden.

Hier ist ein Konfigurationsbeispiel für die erweiterte Quellenauswahl:

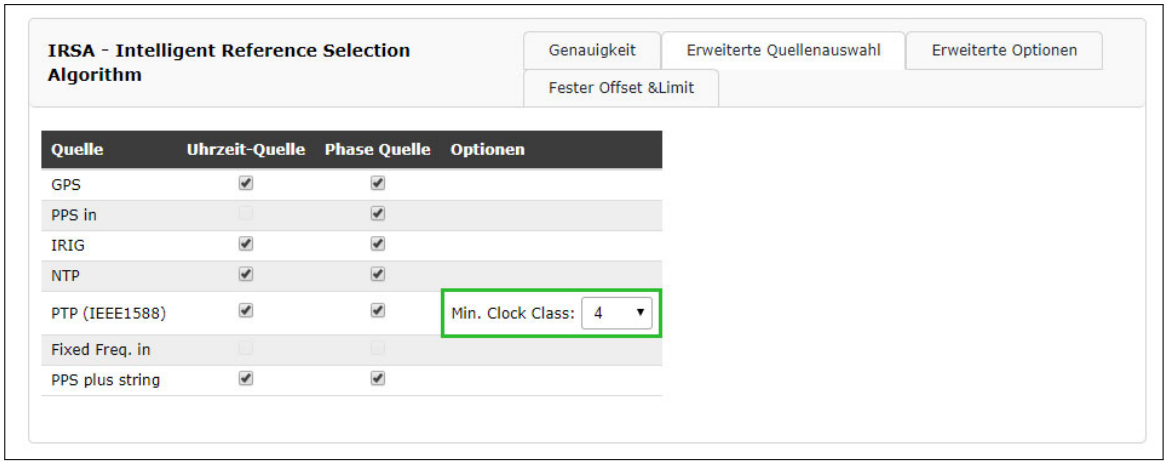


Abbildung: Ein Beispiel für eine gemischte Kombination aus ToD und Phasenquelle für gegebene Referenzsignale.

PTP Min. Clock Class
Das MRS-System sollte einen PTP Master nur zur Synchronisation der Uhr verwenden, wenn die gewünschte Clock-Class gegeben ist. Es soll verhindert werden, dass der Slave auf einen schlechten Master sychronisiert bleibt, obwohl eine weitere Quelle verfügbar ist.

13.1.10.8 Erweiterte Optionen

Die Trusted Source (TRS) -Funktion ist ein leistungsstarkes Tool zum Schutz der GNSS Empfänger[1] vor Spoofing-Attacken. Im Moment wird die Funktion „Vertrauenswürdige Quelle“ nur in Kombination mit einem Meinberg GPS- oder GNSS-Empfänger und einer Meinberg XHE (externe Rubidium-Holdover Erweiterung) unterstützt.

Um diese Funktion zu aktivieren, wählen Sie das Kontrollkästchen „Verwendet vertrauenswürdige Quelle“ für das GPS-Referenzsignal. Das bedeutet, dass die GPS-Referenz von einer anderen Referenzquelle, die als vertrauenswürdige Quelle anerkannt ist, auf Konsistenz geprüft wird. In unserem Fall ist die vertrauenswürdige Quelle eine Rubidium-Uhr. Es wird in der Tabelle der erweiterten Optionen als „ext.Osc“ bezeichnet (externer Oszillator). Aktivieren Sie daher das Kontrollkästchen „Vertrauenswürdige Quelle“.

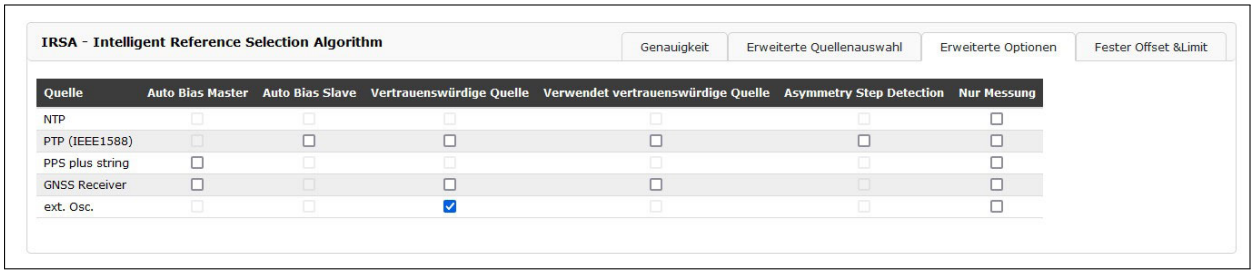


Abbildung: Ein Beispiel für den Betrieb einer vertrauenswürdigen Quelle mit einem externen Rubidium.

Das externe Rubidium fungiert als externer Oszillator, der vom GPS- oder GNSS-Master synchronisiert wird, solange der Master verfügbar ist und seine Präzision besser ist, als die Genauigkeit des XHE. Wenn der Master ausfällt oder aus irgendeinem Grund beschädigte oder manipulierte Daten verwendet, erkennt das TRS dieses als Offset-Grenzwertverletzung. Folglich verwirft der Referenzauswahlalgorithmus den aktuellen Master und die XHE Rubidium-Quelle wird der neue Master für die Synchronisation.

Sowohl GNSS- als auch Rubidium-Referenzsignale müssen zuerst in der Quellenprioritätenliste konfiguriert werden, GPS oder GNSS als „Quelle 1“ und externer Oszillator als „Quelle 2“. Alle anderen Positionen sollten leer bleiben. Zusätzlich sollte der IRSA Reference Algorithmus mit entsprechenden Genauigkeiten aktiviert werden.

Die Genauigkeit für GPS oder GNSS ist gleichzeitig auch das TRS-Limit, dem die Referenz entsprechen sollte. Wenn das TRS-Limit verletzt wird, verwirft der Referenzauswahlalgorithmus den aktuellen Master und schaltet automatisch auf die Trusted Source - XHE Rubidium um. Für den GPS- oder GNSS-Präzisionswert nehmen wir 250 ns, welches die maximale Zeitabweichung für den Empfänger ist.

Schließlich sollte die GPS- oder GNSS-Referenz „Uhrzeit-Quelle“ und „Phase-Quelle“ aktiviert haben, was bedeutet, dass der Empfänger eine Quelle sowohl für die Tageszeit als auch für die Phase ist. Am XHE Rubidium sollte nur die Phase-Quelle aktiviert sein, da die Atomuhr allein die ToD-Information nicht liefert.

Auto Bias Master / Auto Bias Slave
„Auto Bias“ bietet eine Technologie für eine Situation, in der ein konstanter Offset, der bei einem gegebenen Eingangssignal vorhanden ist, automatisch gemessen und gegen eine vertrauenswürdige Referenz kompensiert werden kann. Ein Grund für diesen konstanten Offset könnte eine Verzögerung durch die Kabellänge sein, die einen festen Offset (5ns pro m Koaxialkabel und 3ns für Glasfaserkabel) verursacht.

Darüber hinaus können noch andere Gründe für eine Offset verantwortlich sein: Eine Verzögerung, die durch einen IRIG-Generator entsteht, wenn IRIG als Eingangsreferenz verwendet wird oder ein konstanter Offset über PTP aufgrund von Netzwerkasymmetrien.

Wenn Sie also z.B. GPS als Referenzsignal mit Priorität 1 wählen, während Sie „Auto Bias Master“ für GPS aktiviert haben, dann wird GPS als Messreferenz für alle anderen Quellen verwendet, solange GPS verfügbar ist.

Wenn PTP bei aktiviertem „Auto Bias Slave“ als sekundäre Priorität konfiguriert ist, wird der konstante Offset des PTP-Eingangssignals gegenüber der aktuellen Referenz „Auto Bias Master“ (GPS) gemessen und automa-

[1] GPS / GNSS: Die Trusted Source (TRS) -Funktion arbeitet nur mit GPS und GNS-Empfängern.

tisch kompensiert.

Selbst wenn PTP zu einem Referenzsignal wird, falls ein Master nicht verfügbar ist, beinhalten die PTP-Offsets eine Kompensation für den anfänglichen Offset, der automatisch mit dem vorherigen Master gemessen wird. In dieser Betriebsart ist ein reibungsloser Übergang von GPS zu PTP ohne Zeitsprung möglich, falls GPS nicht verfügbar ist.

Ist PTP dann eine primäre Synchronisationsquelle und tritt plötzlich ein Asymmetriesprung im Netzwerk auf (z.B. durch Pfadänderungen), wird der auftretende Asymmetriesprung daher bei aktivierter „Asymmetrie-Step-Detection“ automatisch mit kompensiert.

Asymmetrie-Step-Detection
Wenn die Asymmetriesprung-Erkennung aktiviert ist, folgt der PTP-Slave keinen harten Zeitsprung. Die Soft-Synchronisation bleibt erhalten und der Zeitsprung wird in der MRS-Statistik als Offset angezeigt.

Mit aktivierter „Asymmetry Step Detection“ misst das System ca. 10 Minuten den Offset. Nach weiteren 10 Minuten wird ein ermittelter Wert bzw. Offset gesetzt, welcher dann auch unter MRS -> PTP-Status angezeigt wird [Step Compensated]:

```
Auto-Bias: 0.000000000s
Step-Comp.: -0.000010001s
Span: 0.000000025s
```

Nur Messung
Wenn das Feld aktiviert ist, wird diese Quelle nur für Messungen verwendet aber niemals als Synchronisationsquelle.

13.1.10.9 Fixed Offset and Limit

Die „Fixed Offsets“ und „Limits“ können über die entsprechenden Felder eingegeben werden. Der „Fixed Offset“ gibt für jeden Referenztakt einen festen Offset zur Referenzzeit an. Mit diesem Wert können bekannte und konstante Abweichungen einer Referenzzeitquelle kompensiert werden. Für GNSS-Referenzen kann kein konstanter Offset eingestellt werden - das kann nur indirekt mit der Kompensationszeit des Antennenkabels erfolgen.

Limit:
Hier können Sie einen Grenzwert konfigurieren. Überschreitet die Referenzquelle diese Grenze, wird eine Benachrichtigung ausgelöst. Eine Konfiguration im Web-Interface ist auf der Benachrichtigungsseite „Benachrichtigung → Ereignisse → MRS Limit Exceed“ erforderlich.

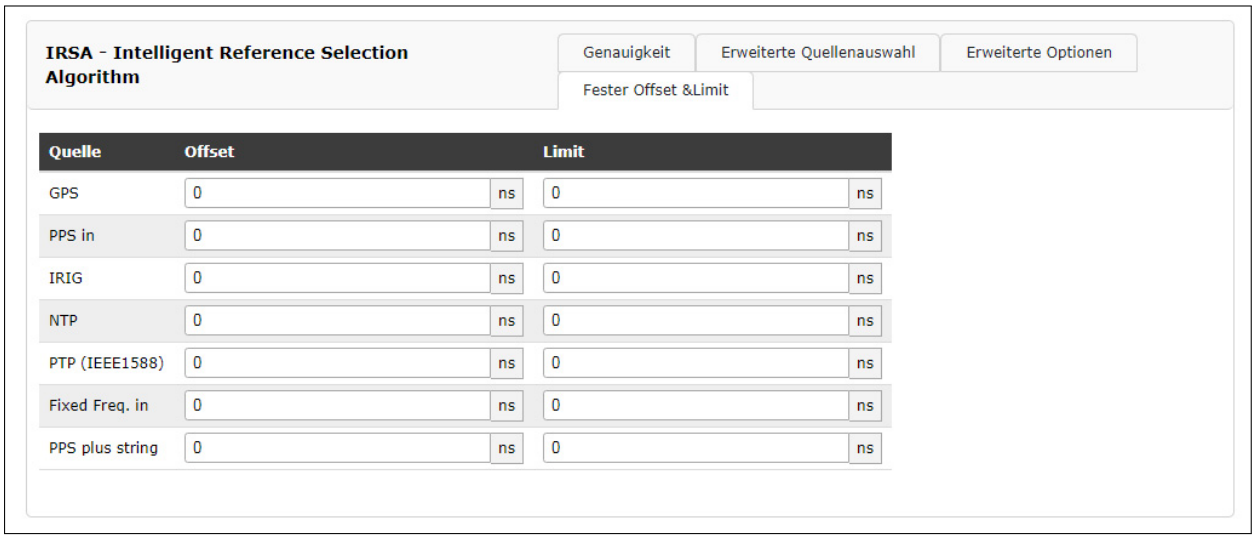
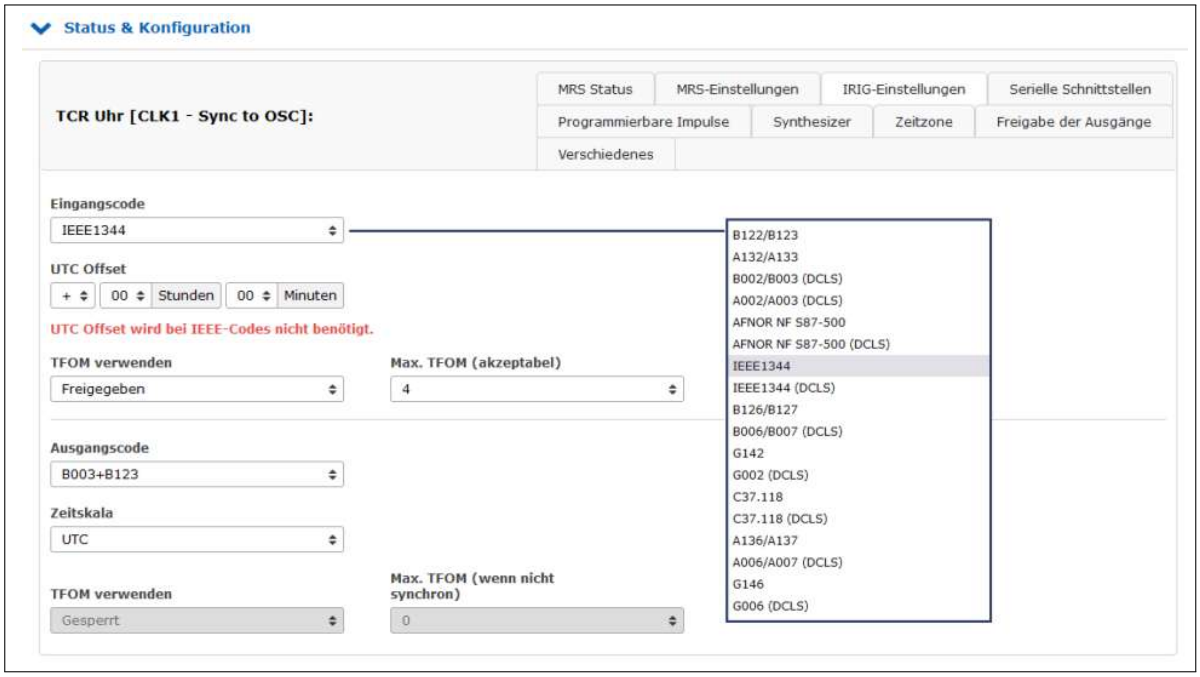


Abbildung: Konfiguration für bekannte Offsets und Limits.

13.1.10.10 IRIG-Einstellungen

Abhängig davon, welche Module in Ihrem System verbaut sind, können in diesem Menü die eingehenden und / oder ausgehenden Zeitcodes (Timecode = TC) konfiguriert werden. Dazu zählen u.a. die IMS-Ausgangsmodule der BPE-Reihe, welche als „passive" Module die von der Referenzuhr generierten Zeit- und Synchronisationssignale ausgeben.



Einstellung der Signalausgabe

1. Rufen Sie den Reiter „Uhr" auf.

2. Öffnen Sie den Abschnitt „Status & Konfiguration" mit einem Klick.

3. *Wenn Ihr LANTIME-System über eine Umschaltkarte (z.B. RSC-Modul) verfügt:*
   Im Bereich „Umschaltkarte", klicken Sie auf den Reiter „IRIG-Einstellungen".

   Wenn Ihr LANTIME-System über nur eine Referenzuhr (z.B. SPT-Modul) verfügt:
   Im Bereich „CLK1" (bzw. „CLK2", sofern die Uhrmodul sich dort befindet), klicken Sie auf den Reiter „IRIG-Einstellungen".

4. Wählen Sie den Reiter „IRIG-Einstellungen" aus.

5. Stellen Sie den gewünschten IRIG-Eingangs- oder Ausgangscode ein. Für detaillierte Informationen wird auf das Handbuch Ihres IMS-Gerätes verwiesen.

IRIG

Beispiel:	B002/B003	
	B002	100pps, PWM-DC-Signal, kein Träger, BCD time of year
	B003	100pps, PWM-DC-Signal, kein Träger, BCD time of year, SBS time of day mit Tagessekunde (0....86400)
AFNOR NF S87-500	AFNOR NF S87-500 Ist ein standardisierter französischer Zeitcode, ähnlich dem IRIG-Code. Code lt. NFS-87500, 100pps, AM-Sinussignal, 1kHz Träger, BCD time of year, vollständiges Datum, SBS-Time of Day	
IEEE1344	Code. lt. IEEE1344-1995, 100pps, AM-Sinussignal, 1kHz Träger, BCD time of year, SBS time of day, IEEE1344 Erweiterungen für Datum, Zeitzone, Sommer/Winterzeit und Schaltsekunde im Control Funktionssegment	

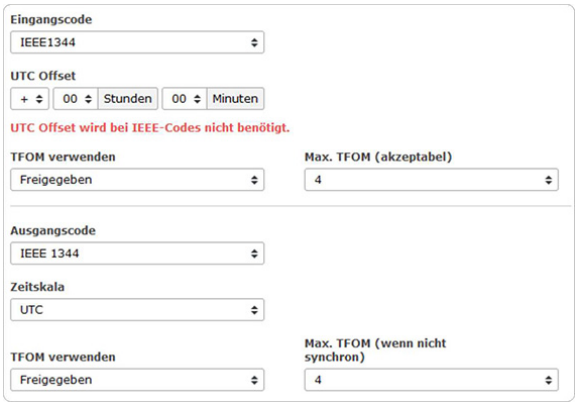
Eingangscode:
Es muss zunächst der passende Zeitcode eingestellt werden, damit das von der Referenzquelle kommende Time-Code-Signal korrekt dekodiert werden kann.

UTC Offset:
Wenn der angewendete Zeitcode mit einem konstanten Zeitversatz zu UTC beaufschlagt wird, muss dieser Zeitversatz hier eingestellt werden, damit die Uhr die empfangene Zeit in UTC umwandeln kann.

IRIG TFOM

Bei verbautem TCR-Modul sind im Menü „IRIG-Einstellungen“ die TFOM Parameter nach Auswahl der IEEE1344 oder C37.118 als Eingangs-Zeitcodes aktiv und konfigurierbar.

In den Control Bits der formatspezifischen Erweiterung dieser Zeitcodes sind 4 Bits für einen sog.„Time Figure of Merit“-Wert (TFOM) vorgesehen, mit dem eine zu erwartende Zeitgenauigkeit des Referenzsystem an das Empfängersystem übermittelt werden kann.



Befindet sich das System im Freilauf, kann der Wert des TFOMs auf Basis der zu erwarteten Oszillatordrift und der Freilaufzeit ermittelt werden. Wenn das System synchron zur Referenzquelle ist, wird der TFOM Wert auf 0 gesetzt. Stellt das Referenzsystem keine Informationen für die TFOM-Werte zur Verfügung, wird der TFOM auf 15 (undefiniert) gesetzt.

TFOM verwenden

Enabled	TFOM wird beachtet
Disabled	TFOM wird ignoriert

Max. TFOM (akzeptabel):

Wird dieses Signal (z.B. C37.118) als Referenzquelle verwendet, kann im Webinterface eingestellt werden, dass sich das System in Abhängigkeit des konfigurierten „Max. TFOM“ Wertes auf die Referenzquelle synchronisiert. Wird der voreingestellte Wert überschritten, wird das Eingangssignal nicht mehr als gültige Referenzquelle akzeptiert und das System geht in den Freilauf oder wechselt zur nächsten Referenzquelle in der Prioritätenliste.

TFOM-Wert	Estimated Time Error (ETE)	TFOM-Wert	Estimated Time Error (ETE)
0*	TQ_LOCKED_TO_UTC	8	ETE < 10 ms
1	ETE < 1 ns	9	ETE < 100 ms
2	ETE < 10 ns	10	ETE < 1 s
3	ETE < 100 ns	11	ETE < 10 s
4	ETE < 1 μs	12	ETE < 100 s
5	ETE < 10 μs	13	ETE < 1000 s
6	ETE < 100 μs	14	ETE < 10000 s
7	ETE < 1 ms	15	ETE undefiniert

Ausgangscode:
Wenn das System über eine Zeitcode Ausgabeoptionen verfügt, können die Parameter ähnlich wie die Eingangscodes konfiguriert werden.

Hinweis:

Bei redundanten Empfängersystemen wird die Konfiguration über das Umschaltkarten-Menü vorgenommen.

Zeitskala:
Die Ausgabe des ausgewählten Zeitcodes kann mit UTC oder der lokalen Zeit erfolgen. Wenn „LOCAL TIME“ verwendet wird, bezieht sich die Ausgabe auf die konfigurierte Zeitzone.

TFOM verwenden:

Enabled	TFOM aktiviert
Disabled	TFOM deaktiviert (fester TFOM-Wert ist 0)

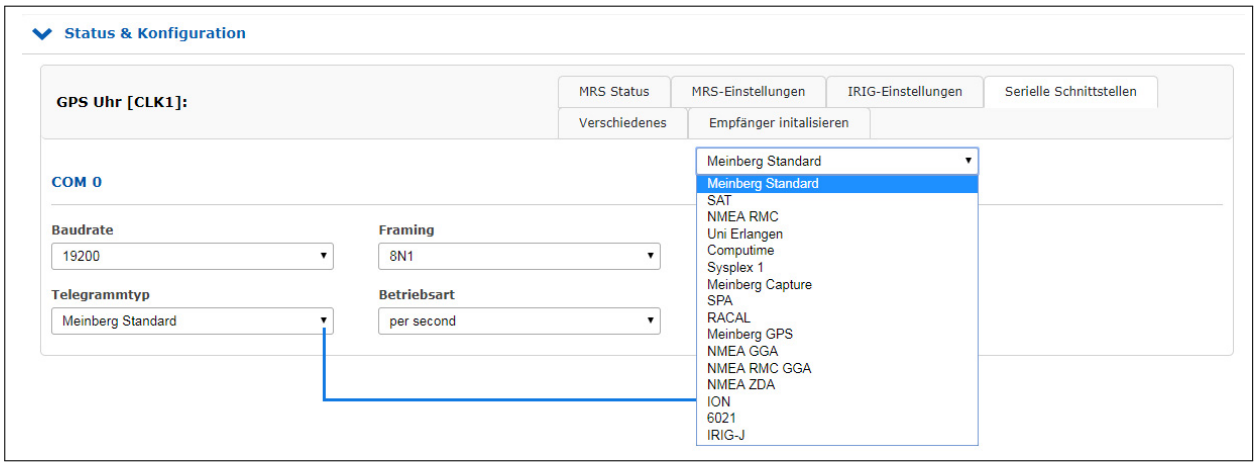
Hinweis:

Befindet sich das Modul im Simulationsmodus, wird der TFOM-Wert automatisch auf 0 gesetzt.

Max. TFOM (wenn nicht synchron)
Verfügt das System auch über einen IRIG Ausgang (z.B. BPE2000), kann hier ebenfalls ein „Max. TFOM“ konfiguriert werden. Dieser kann dafür genutzt werden, um den ausgegebenen TFOM-Wert zu begrenzen. Das Ausgangssignal ist weiterhin verfügbar, der in den IRIG eingefügte TFOM-Wert wird aber nicht weiter hochgezählt.

13.1.10.11 Serielle Schnittstellen

Abhängig von der Hardware und der Version des Systems können in diesem Menü die Parameter für die seriellen Schnittstellen konfiguriert werden.



Baudrate: Die Geschwindigkeit, mit der das serielle Telegramm übertragen werden soll:
300, 600, 1200, 2400, 4800, 9600, 19200

Framing: Aufbau des Telegramms:
7E1, 7E2, 7N2, 7O1, 7O2, 8E1, 8E2, 8N1, 8N2, 8O1

Telegrammtyp: Meinberg Standard, SAT, NMEA RMC, Uni Erlangen, Computime, Sysplex 1, Meinberg Capture, SPA, RACAL, Meinberg GPS, NMEA GGA, NMEA RMC GGA, NMEA ZDA, ION, 6021, IRIG-J

Betriebsart: Sie können Für die ausgehende Zeitzeichenfolge einen Intervall einstellen (per second, per minute, on request „?“ only). Wenn die Betriebsart auf ‘on request „?“ only‘ eingestellt ist, muss der Client ein „?“ senden um das Zeittelegramm als Antwort zu erhalten.

Optionen:

MRS PPS Plus String
Wenn das System die Option „MRS PPS plus string“ hat, muss die Baudrate und das Framing für die eingehende Zeitzeichenfolge über dieses Untermenü konfiguriert werden.

Meinberg Capture *only for specific units*
Diese Option ist für Systeme mit einem Capture-Eingang. Das Ereignis wird durch eine negative Flanke ausgelöst.

Für die Ausgabe der Capture-Zeitstempel stehen zwei Betriebsarten zur Verfügung, „on request ? only“ und „automatisch“.

on request „?“ only
Die ausgelösten Ereignisse werden in einem Puffer der Referenzuhr gespeichert. Sobald ein „?“ über die serielle Schnittstelle an den Referenzempfänger gesendet wurde, werden die gespeicherten Ereignisse aus dem Puffer heraus übertragen.

automatically
In diesem Modus werden die erfassten Ereignisse direkt an der seriellen Schnittstelle ausgegeben.

13.1.10.12 Zeitzone

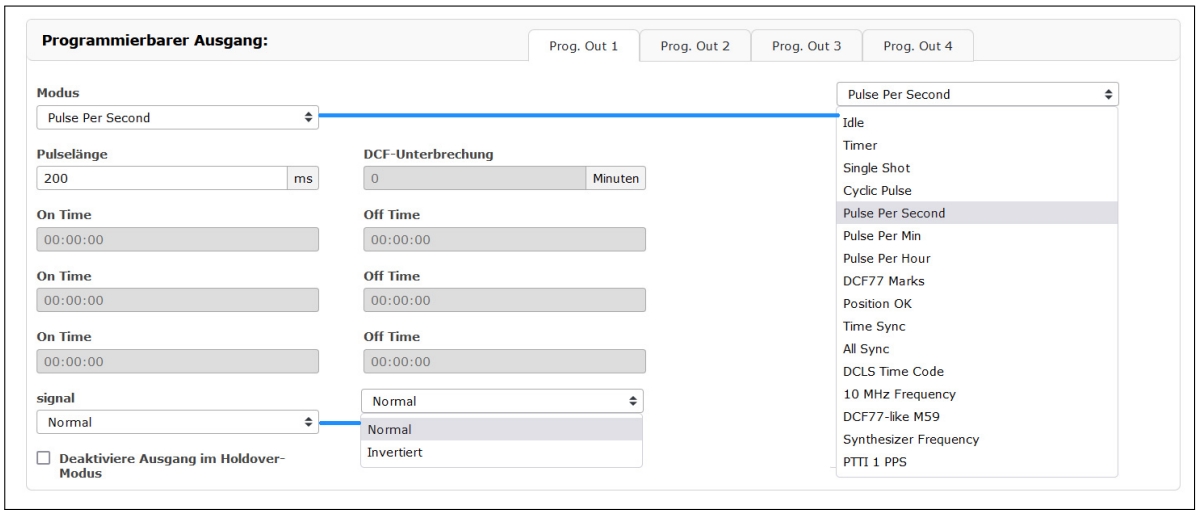
In diesem Menü können Sie die Zeitzonen (Offsets) für die Ausgangssignale (IRIG, serielle Schnittstelle, programmierbare Impulse) der Referenzuhr konfigurieren.

Die Daten der Zeitzone werden aus der Zeitzonentabelle verwendet (Menü „System → Display → Zeitzonentabelle bearbeiten“).

13.1.10.13 Freigabe der Ausgänge

Optional können die Ausgänge der Referenzuhr so eingestellt werden, dass sie immer ein Signal liefern, wenn das Gerät eingeschaltet ist oder nur wenn die interne Uhr synchron läuft.

13.1.10.14 Programmierbare Signale



Einstellung der Signalausgabe

1. Zur Konfiguration der programmierbaren Signale wählen Sie das Menü „Uhr“.

2. Öffnen Sie den Abschnitt „Status & Konfiguration“.

3. *Wenn Ihr LANTIME-System über eine Umschaltkarte (z.B. RSC-Modul) verfügt:*
   Klicken Sie im Bereich „Umschaltkarte“ auf den Reiter „Programmierbare Impulse“.

   Wenn Ihr LANTIME-System über nur eine Referenzuhr verfügt:
   Im Bereich „CLK1“ (bzw. „CLK2“, sofern die Referenzuhr sich dort befindet), klicken Sie auf den Reiter „Programmierbare Impulse“.

4. Es sind jetzt vier Reiter sichtbar: Prog. Out 1-4. Wählen Sie das zu konfigurierende Ausgangssignal aus.

5. Führen Sie jetzt alle Einstellungen für die gewünschte Signalausgabe durch.

6. Speichern Sie abschließend Ihre gewünschten Einstellungen.

Modus: Auswahl des Ausgangssignals
(siehe auch ➜ Kapitel 16.5, „Übersicht der programmierbaren Signale“)

Pulslänge (ms): Eingabe der Pulslänge.

Zyklus: Für den „Cycle Pulse“-Modus kann ein Intervall im Format *hh:mm:ss* konfiguriert werden.

Zeit: Im konfigurierten Modus „Single Shot“ kann die Zeit für den Puls parametriert werden, im Format *hh:mm:ss*.

DCF-Unterbrechung (min): Im Modus „DCF77 Marks“ können Sie eine Abschaltzeit für den Ausgangsport konfigurieren, so dass im Falle einer Asynchronität der Referenzuhr keine DCF-Marker am Ausgang zur Verfügung stehen.

On / Off Time: Für den „Timer“-Modus können Start- und Stoppzeiten im Format *hh:mm:ss* konfiguriert werden.

Signal: Konfiguration des Ausgangssignals in „Active high“ oder „Active low“.

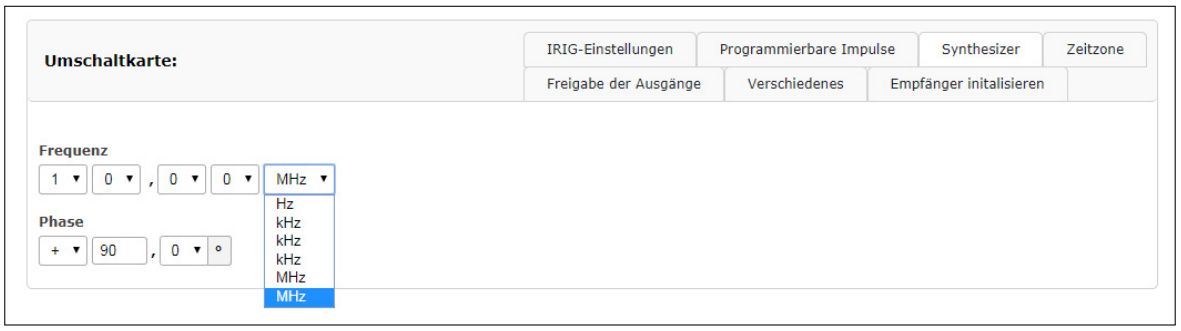
Deaktiviere Ausgang im Holdover-Modus: Wenn der Referenztakt asynchron ist, wird das Ausgangssignal sofort deaktiviert, falls das Kontrollkästchen aktiviert ist.

Hinweis:

Im Menü „Freigabe der Ausgänge“ muss bei Impulsausgänge die Auswahl „if sync“ getroffen werden, damit die Ausgänge im Holdover-Modus abgeschaltet werden können.

13.1.10.15 Synthesizer

Hier können die Ausgangsfrequenz und die Phase des integrierten Synthesizers eingestellt werden.

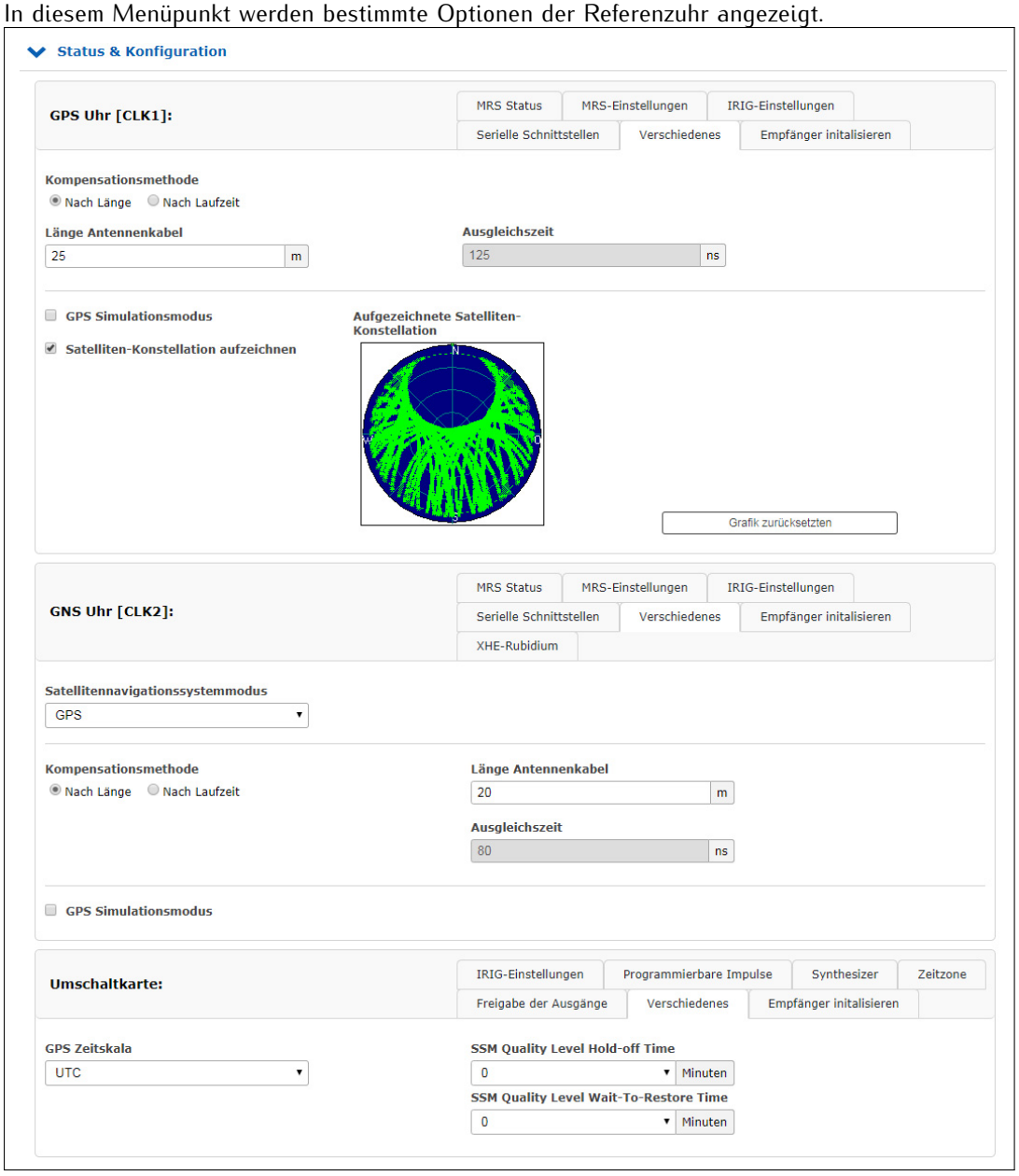


Frequenz: Frequenzen von 1/3 Hz bis 10 MHz können durch Eingabe von vier Ziffern und einem Frequenzbereich eingestellt werden. Durch Eingabe der Frequenz 0 Hz kann der Synthesizer abgeschaltet werden.

Phase: Mit Phase können Sie die Phasenlage der eingestellten Frequenz im Bereich von -180° bis + 180° mit einer Auflösung von 0,1 eingeben. Wenn der Phasenwinkel erhöht wird, wird die Verzögerung des Ausgangssignals wird größer. Ist eine Frequenz höher als 10 kHz eingestellt, kann die Phase nicht verändert werden.

13.1.10.16 Verschiedenes

In diesem Menüpunkt werden bestimmte Optionen der Referenzuhr angezeigt.



Länge Antennenkabel (m):
Die Signallaufzeit des Antennenkabels kann durch diesen Wert kompensiert werden. Das empfangene Zeitsignal wird um ca. 5ns/m bei Einsatz des RG58U und 4ns/m bei Einsatz des H155 Antennenkabel verzögert. Dieser Zeitfehler wird durch die Eingabe der Kabellänge automatisch kompensiert. Der Standardwert ist 20m. Der maximale Eingabewert darf 500m nicht überschreiten.

GPS Simulationsmodus:
Dieses Menü erlaubt dem Benutzer, den Zeitserver ohne Antenne zu betreiben. Normalerweise verliert der NTPD die Synchronisation, wenn die Antenne oder die externe Referenzquelle getrennt ist (rote FAIL-LED ist eingeschaltet). Durch Aktivierung des Simulationsmodus werden die entsprechenden Statusinformationen für den NTPD permanent auf SYNC gesetzt. Damit ist es auch möglich, andere Zeiten, die über den Menüpunkt „Initialisieren des Empfängers" eingegeben wurden, an den NTPD zu übermitteln. Im Normalfall sollte das Kontrollkästchen leer bleiben. Wenn diese Box aktiviert ist, wird im Hauptmenü unter „Info des Empfängers" der Status „Simulationsmodus" angezeigt.

GPS Zeitskala:

UTC Coordinated Universal Time (einschließlich der laufenden Schaltsekunden, die ständig aktualisiert werden)

GPS Seit 1. Januar 1980 - GPS Systemzeit: monotone Zeitskala ohne Schaltsekunden.
Enthält die Schaltsekunden von 1970-1980.

TAI Seit dem 1. Januar 1970 - Internationale Atomzeit: monotone Zeitskala ohne Schaltsekunden.
Unterschied zur GPS-Zeit: 19 Sekunden.

Wenn Sie die Zeitskala im Dropdown-Menü ändern, erscheint im Browserfenster eine Warnmeldung.

Bitte beachten Sie:
Wenn der GPS-Empfänger konfiguriert ist, um GPS- oder TAI-Zeitskala anstelle von UTC auszugeben, basiert die verteilte Zeit über NTP dann nicht auf UTC. Das ist eine Protokollverletzung und dieser Zeitserver kann nicht verwendet werden um Standard NTP Clients zu synchronisieren, die UTC Zeit erwarten.

Satelliten-Konstellation aufzeichnen (GPS Empfänger):
Wenn diese Option aktiviert ist, wird eine Grafik erzeugt, auf der die Konstellation der sichtbaren Satelliten angezeigt wird.

SSM Quality Level im GPS Lock Mode:
Wenn das System E1 / T1-Ausgänge hat, kann hier das SSM-Qualitätsniveau konfiguriert werden.

SNS Mode - Satellite Navigation System Mode (GNS Receiver):
Wenn Sie einen GNS-Empfänger (GNS oder GNS-UC mit Up-Converter) verwenden, dann können Sie mit diesem Drop-Down-Menü ein oder auch mehrere Satellitensysteme auswählen, die dann gleichzeitig verwendet werden.

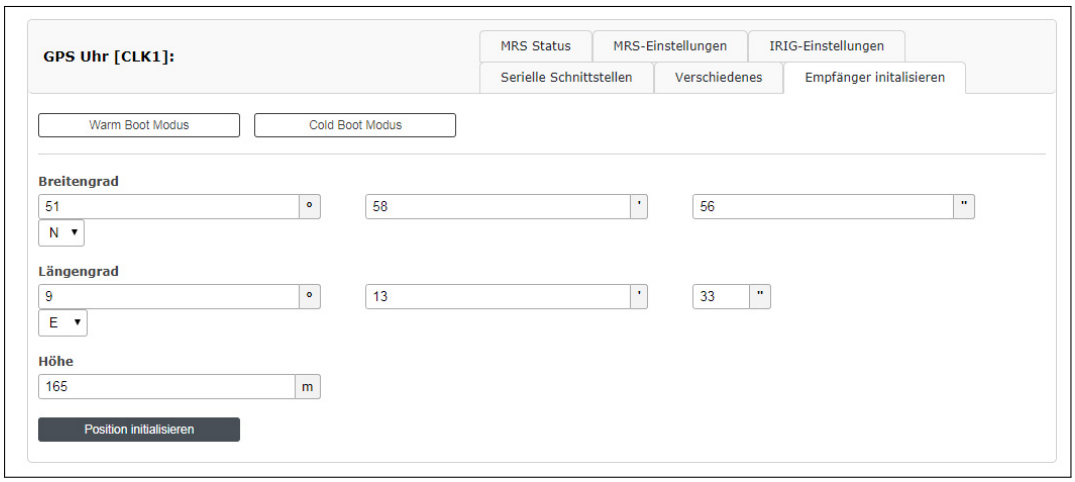
Folgende Kombinationen können ausgewählt und gleichzeitig empfangen werden:

GNS Empfänger	GNS-UC Empfänger	GNM Empfänger
GPS only	GPS only	GPS
GLONASS only	Galileo only	GLONASS
Galileo only	GPS/Galileo	Galileo
BeiDou only		BeiDou
GPS/GLONASS		(Alle verfügbaren Systeme
GPS/Galileo		können gleichzeitig empfangen
GPS/BeiDou		werden)
Galileo/GLONASS		
Galileo/BeiDou		
GLONASS/BeiDou		
GPS/Galileo/GLONASS		
GPS/Galileo/BeiDou		

Entfernung zum Sender (km) - nur PZF / AM Empfänger:
Im Menüpunkt „Distanz zum Sender“ können Sie den Senderabstand in km eingeben, der für die Verzögerungskompensation des eingehenden Langwellen-Signals verwendet wird. Die Einstellung der Distanz sollte so genau wie möglich erfolgen, da sie einen direkten Einfluss auf die absolute Genauigkeit des Zeitrasters hat.

PZF Simulationsmodus:
Dieses Menü erlaubt dem Benutzer, den Zeitserver ohne Antenne zu betreiben. Normalerweise verliert der NTPD die Synchronisation, wenn die Antenne oder die externe Referenzquelle getrennt ist (rote FAIL-LED ist eingeschaltet). Durch Aktivierung des Simulationsmodus werden die entsprechenden Statusinformationen für den NTPD permanent auf SYNC gesetzt. Damit ist es auch möglich, andere Zeiten, die über den Menüpunkt „Initialisieren des Empfängers“ eingegeben wurden, an den NTPD zu übermitteln. Im Normalfall sollte das Kontrollkästchen leer bleiben. Wenn diese Box aktiviert ist, wird im Hauptmenü unter „Info des Empfängers“ der Status „Simulationsmodus“ angezeigt.

13.1.10.17 Empfänger initalisieren



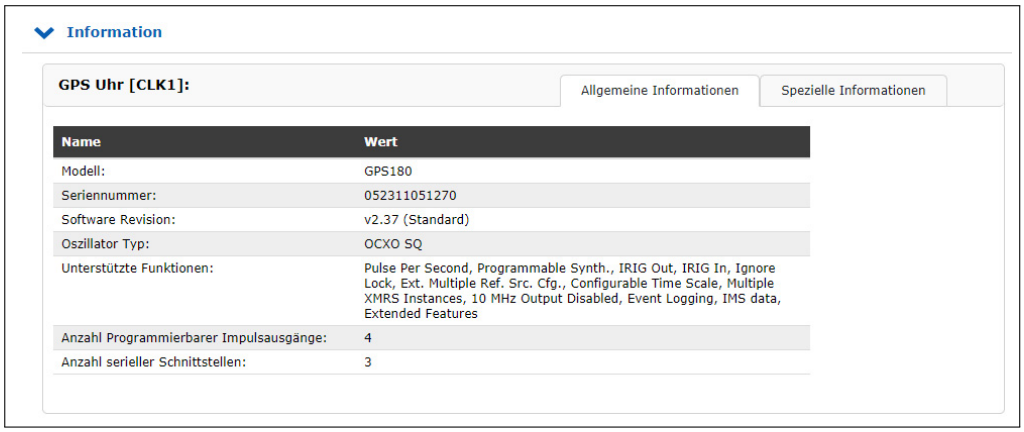
Warm Boot Modus - nur für GNSS-Empfänger:
In diesem Menü kann der Benutzer den Empfänger auf WARMBOOT MODE schalten. Das kann erforderlich sein, wenn die Satellitendaten im batteriegepufferten Speicher zu alt sind oder wenn das Gerät an einer Stelle betrieben wird, die mehrere hundert Kilometer von der letzten Betriebsstätte entfernt ist und die Berechnung der Sichtbarkeit der Satelliten neu durchgeführt werden muss.

Cold Boot Modus - nur für GNSS-Empfänger:
Dieses Menü erlaubt dem Benutzer, alle GPS-Systemwerte neu zu initialisieren, d.h. alle gespeicherten Satellitendaten werden gelöscht. Bitte beachten Sie, dass der Empfänger ca. 15 Minuten benötigt, um die Informationen der Satelliten wieder einzulesen und den Kaltstart zu vervollständigen!

Koordinaten (Breitengrad, Längengrad und Höhe) - nur für GNSS-Empfänger:
Hier kann die absolute Position der GPS-Antenne eingegeben und mit der „Initialisierungsposition“ an die GPS-Referenzuhr gesendet werden. Diese Option ist sinnvoll, wenn das System an einem anderen Ort betrieben wird und wenn es mit den zuvor batteriegepufferten Satellitendaten gestartet wird.

Uhrzeit/Datum:
Mit dieser Funktion kann die Referenzuhr manuell auf ein bestimmtes Datum und Uhrzeit eingestellt werden.

13.1.10.18 Empfänger-Informationen



Dieser Menüpunkt listet alle wichtigen Informationen und Optionen der Referenzuhr auf.

Erläuterung zu GPS-Satelliten-Status „Satellites in View“ und „Number of Good Satellites“
Die Satelliten des GPS-Systems und anderer GNSS-Navigationssysteme sind normalerweise nicht geostationär, sondern bewegen sich auf genau bekannten Bahnen um die Erde. Daher befinden sich zu einem bestimmten Zeitpunkt an einer bestimmten geographischen Position immer nur einige der Satelliten über dem Horizont, während die anderen unterhalb des Horizonts versteckt sind. Signale von Satelliten, die sich unterhalb des Horizonts befinden, können nicht empfangen werden. Deshalb berechnet der GPS-Empfänger aufgrund seiner letzten bekannten Position und der gespeicherten Satelliten-Bahndaten, welche Satelliten sich momentan über dem Horizont befinden und daher **„sichtbar“** („in view“) sein sollten.

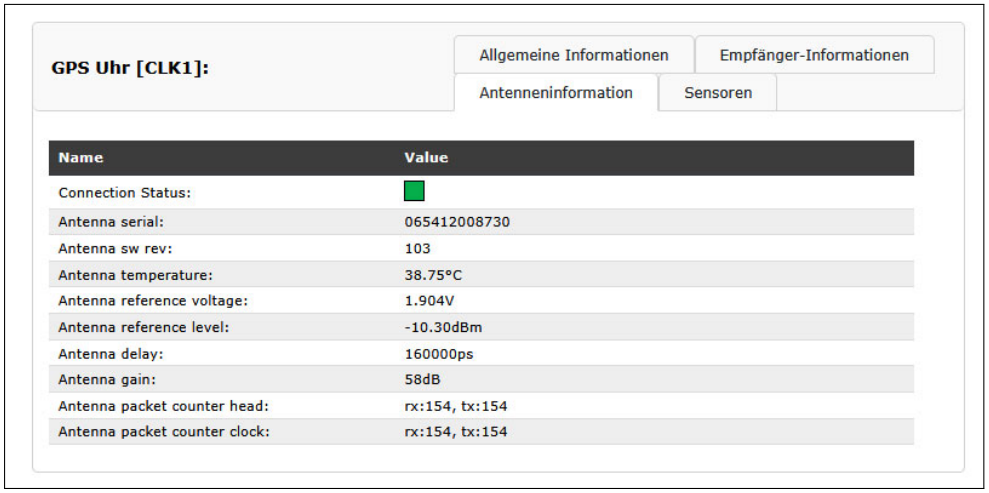
Allerdings ist es möglich, dass Signale von Satelliten, die eigentlich sichtbar sein sollten, tatsächlich nicht empfangen werden können, da die Satelliten durch hohe Gebäude, Berge usw. abgeschirmt werden. Außerdem können einzelne Satelliten vorübergehend in einen Wartungsmodus geschaltet worden sein, so dass man deren Signale zwar empfangen kann, aber nicht verwenden sollte. Nur Satelliten, deren Signal empfangen werden kann, und die sich nicht im Wartungsmodus befinden, werden als **„gut“** („good“, „tracked“) bezeichnet und zur Ortsbestimmung und Zeitsynchronisation herangezogen.

Aus diesem Grund kann die Anzahl der **„guten“** Satelliten niemals größer sein als die Anzahl der „sichtbaren“ Satelliten. Sie kann dagegen sogar erheblich geringer sein, wenn die Antenne an einem Ort mit eingeschränkter Sichtbarkeit des Himmels installiert ist und viele Satelliten abgeschirmt werden. Im schlimmsten Fall kann dadurch sogar die erreichbare Zeitgenauigkeit leiden, oder eine Synchronisation ist nur zeitweise möglich, wenn vorübergehend genügend Satelliten empfangen werden können.

13.1.10.19 Antenneninformationen

Anzeige der Antenneninformationenn im Webinterface

Meinberg GNSS-Empfänger ab der 183er Generation können aktiv mit einer angeschlossenen GPSANTv2 oder GNMANTv2 kommunizieren, um Betriebsdaten auszutauschen, die es der Uhr ermöglichen, bestimmte Betriebsparameter anzupassen. Lesen Sie mehr über das bidirektionale Kommunikationsframework von Meinberg (mbgARC) in dem ➜ Kapitel 16.9, „mbgARC: Antennen-Empfängerkommunikation“



Über das Menü „Uhr ...“ lassen sich alle gemessenen Werte der Antenne anzeigen. Die angezeigten Parameter haben die folgende Bedeutung:

Connection Status:	Zeigt den Verbindungsstatus der angeschlossenen Antenne an. Grün: Antenne ist aktiv aus: Antenne ist nicht verbunden oder die Verbindung ist unterbrochen
Antenna Serial:	Die Seriennummer der angeschlossenen Antenne
Antenna sw rev:	Die Firmware-Revision der Antenne
Antenna temperature:	Die gemessenen Innentemperatur der Antenne
Antenna reference voltage:	Die Spannung der vom Empfänger gesendeten 10 MHz an der Antenne
Antenna reference level:	Der Pegel der vom Empfänger gesendeten 10 MHz an der Antenne
Antenna delay:	Die Laufzeitverzögerung durch die Antenne (1)
Antenna gain:	Die Verstärkung der Antenne (2)
Antenna packet counter head:	Die gesendeten Nachrichten von der Antenne zum Empfänger und die von der Antenne empfangenen Nachrichten von dem Empfänger
Antenna packet counter clock:	Die gesendeten Nachrichten von dem Empfänger zur Antenne und die von der Uhr empfangenen Nachrichten von der Antenne

(1) Die Laufzeitverzögerung der Antenne muss im Menü „Uhr → Status & Konfiguration → Verschiedenes → Kompensationsmethode“ zu der Laufzeitverzögerung des Antennenkabels dazu addiert werden.

(2) Die benötigte Verstärkung des Antennsignals ist im Zusammenhang mit der Länge des Antennenkabels bzw. mit der Laufzeitverzögerung zu betrachten. Eine Kabellänge von 20 m benötigt eine wesentlich geringere Verstärkung des Signals als eine Kabellänge von 300 m.

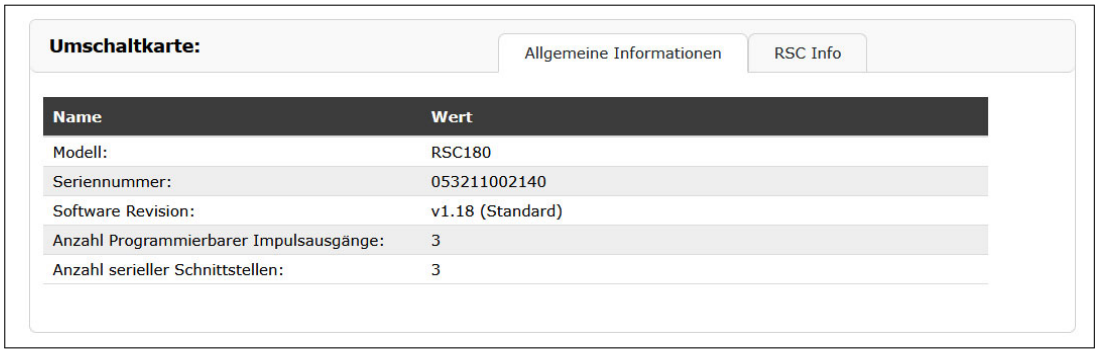
13.1.10.20 Umschaltkarte

Die RSC (SCU) Switch-Karte ist ein automatischer Multiplexer für redundante Systeme mit zwei Meinberg-Empfängern. Die Karte dient zur automatischen Umschaltung der Puls- und Frequenzausgänge sowie der seriellen Schnittstellen der angeschlossenen Uhren. Die Auswahl des jeweils aktiven Systems erfolgt auf der Grundlage des Zustands der TIME_SYNC-Signale der Uhr, die den synchronen Zustand der Uhren anzeigen.

Um unnötige Schaltvorgänge zu vermeiden, beispielsweise bei periodischem Freilauf eines Systems, wird bei jedem Umschalten die Reihenfolge des aktiven und des Reservesystems ausgetauscht. Wenn beispielsweise das aktive System in den Freilaufmodus wechselt, während das Reservesystem synchron arbeitet, wird auf das synchrone Reservesystem umgeschaltet. Ein Reset auf den alten Zustand erfolgt nur, wenn das nun aktive System (früher das Reservesystem) die Synchronisation verliert, während das Reservesystem (vorher aktives System) synchron arbeitet. Wenn beide Systeme im Freilaufbetrieb arbeiten, erfolgt keine Umschaltung und der aktuelle Zustand bleibt erhalten.

13.1.10.21 Information der Umschaltkarte

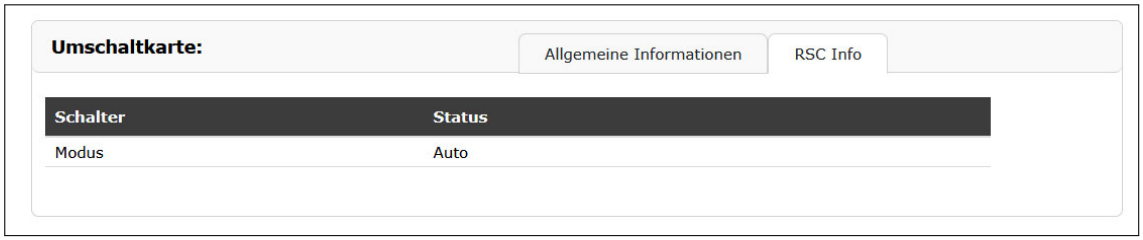
Allgemeine Informationen



In diesem Menüpunkt werden allgemeine Informationen der Umschaltkarte angezeigt:

Modell:	Die Typbezeichnung der RSC
Seriennummer:	Die Seriennummer der RSC-Umschaltkarte
Software-Revision:	Die Firmwareversion der RSC
Anzahl der Progr. Impulsausgänge:	Die verfügbaren programmierbaren Impulsausgänge, die über die RSC-Umschaltkarte konfiguriert werden können (Standard immer 4 Pulsausgänge)
Anzahl der seriellen Schnittstellen:	Die verfügbaren seriellen Schnittstellen (Standard immer eine Schnittstelle COM 0)

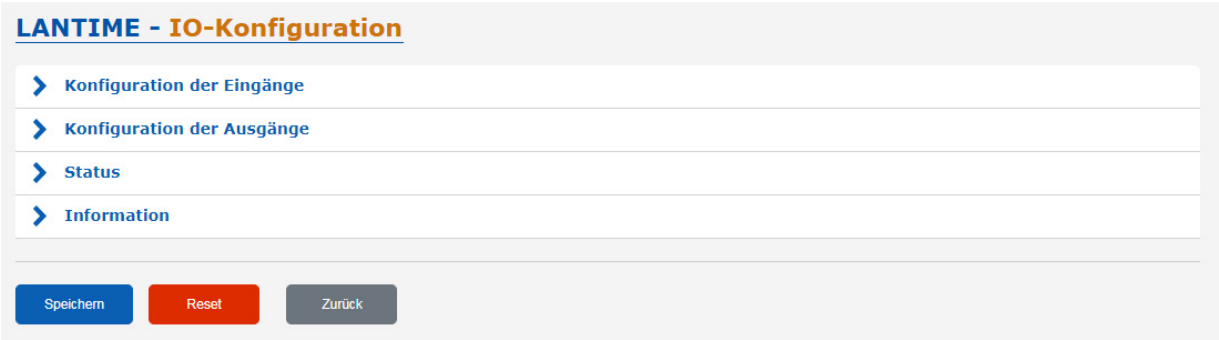
Status der Umschaltkarte



Über den Reiter „RSC Info“ kann der aktuelle Status der RSC-Umschaltkarte abgerufen werden.
Mögliche Einstellungen sind hier „Auto“ oder „Manual“. Diese Einstellung kann über den **Auto/Manual-Schalter** direkt am RSC-Modul durchgeführt werden (z.B. M3000). Bei RSC-Modulen ohne Schalter (z.B. M1000) kann ein Wechsel von „Auto“ zu „Manual“ nur über das Display-Menü durchgeführt werden.

13.1.11 I/O Konfiguration

Dieses Menü ist nur bei einem IMS-System verfügbar. Einzelne Ein- und Ausgangsmodule können hier konfiguriert werden.



13.1.11.1 Konfiguration der Eingänge

13.1.11.2 IMS-MRI (Multiple Reference Input)

Wenn eine Anwendung externe Synchronisationsquellen anstelle von Radio/GNSS-Signalen verwenden muss, ermöglicht eine MRI-Karte dem installierten Uhrenmodul die Synchronisation mit 1PPS-, 10MHz, DCLS- und AM-Timecodes.

Jede MRI-Karte ist einem Uhrenmodul zugeordnet. Benötigt eine redundante Lösung externe Synchronisationseingänge für beide Empfängermodule, dann müssen zwei MRI-Karten installiert werden. Die MRI-Karte ist mit 4x BNC- oder 4x FO-Anschlüssen verfügbar.

Allgemeine Referenzeingangssignale
- 1PPS
- 10 MHz
- IRIG-AM (B, AFNOR, IEEE1344 / C37.118)
- IRIG-DCLS (B, AFNOR, IEEE1344 / C37.118)

Weitere und detaillierte Konfigurationseinstellungen der MRI-Karte finden Sie im Kapitel 13.1.10 - „Das Webinterface → Uhr → MRS-Einstellungen“.

13.1.11.3 IMS-ESI (Extended Synchronization Interface)

Die ESI-Karte (External Synchronization Input) ist in der Lage, einem IMS-System zusätzliche Synchronisationsquellen hinzuzufügen. Die Karte akzeptiert E1- oder T1-Signale, sowohl als „framed" Signale (2.048 MBit/s - 1.544 MBit/s, SSM/BOC wird unterstützt) als auch als Takteingänge (Clock).

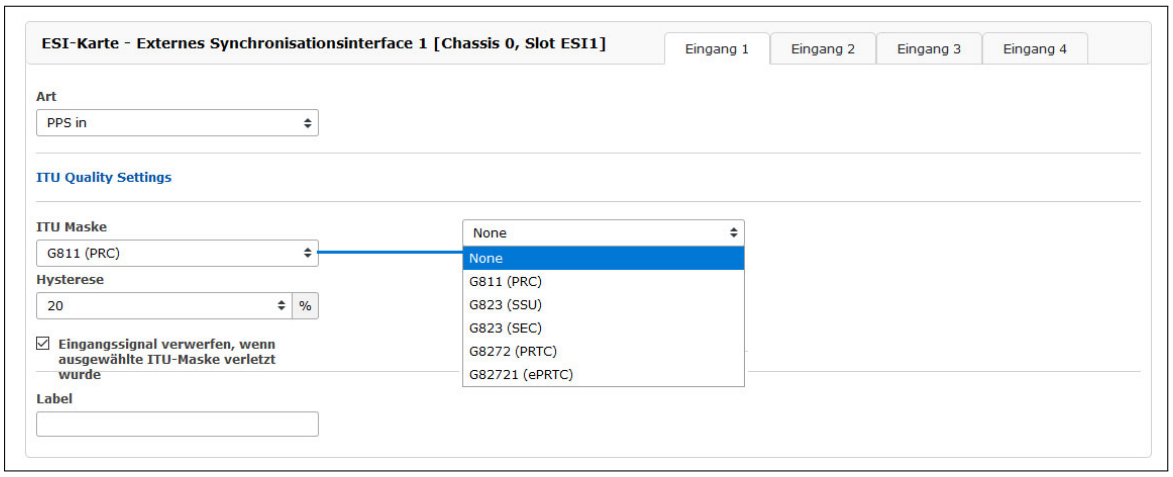
Die Takteingänge sind frei konfigurierbar (1 kHz - 20 MHz). Darüber hinaus ist auch ein 1PPS-Eingang vorhanden.

Eine ESI-Karte ist, wie die MRI-Karte, einem bestimmten Uhrenmodul zugeordnet (abhängig vom Steckplatz, in dem sie installiert ist) und kann sowohl in ESI- als auch in MRI-Slots installiert werden.

Erweiterte Referenzeingangssignale
- 1PPS, BNC
- var. Frequenzen (1 kHz - 20 MHz) unframed, BNC
- var. Frequenzen (1 kHz - 20 MHz) unframed, RJ45
- BITS E1/T1 framed, RJ45

Hinweis:
Wird der angegebene Frequenzbereich unter- bzw. überschritten, wird eine Fehlermeldung im Webinterface angezeigt und der eingetragene Wert wird in diesem Fall nicht übernommen.

Eingang 1: Der Eingang 1 ist für die 1PPS-Pulssynchronisation vorgesehen.



Signalart: – PPS In

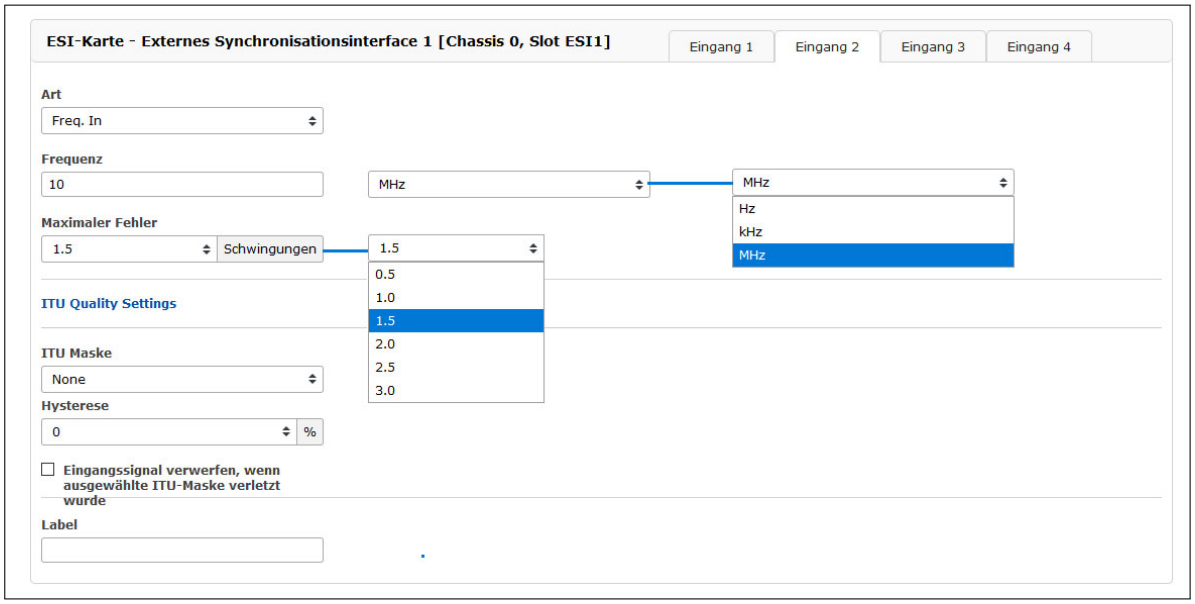
ITU Quality Settings
(diese Einstellungen können für die Eingänge 1 bis 4 einzeln vorgenommen werden)

ITU Maske
Hier können vordefinierte Masken ausgewählt werden, in denen Qualitätsanforderungen hinsichtlich Jitter und Wander der Eingangssignale festgelegt sind. Beim Überschreiten der Vorgabewerte wird der betroffene Signaleingang abgeschaltet.

Hysterese
Um ein fortlaufendes Ab- und Wiedereinschalten der Signaleingänge im Falle der Überschreitung der ITU-Maske zu vermeiden, kann eine Hysterese für das Wiedereinschalten definiert werden. Der Signaleingang wird erst wieder aktiviert, wenn alle Punkte der ausgewählten Maske um den definierten Prozentwert unter den Grenzwerten liegen.

Eingangssignal verwerfen, wenn ausgewählte ITU Maske verletzt wurde
Nur bei Anwählen dieser Box wird das Eingangssignal abgeschaltet, wenn eine ITU-Maske überschritten wird.

Eingang 2: Der Eingang 2 akzeptiert entweder 2.048/1.544 kHz Frequenz oder konfigurierbare Frequenz im Bereich zwischen 1 kHz und 20 MHz, bei Bedarf auch 1.544 kHz.



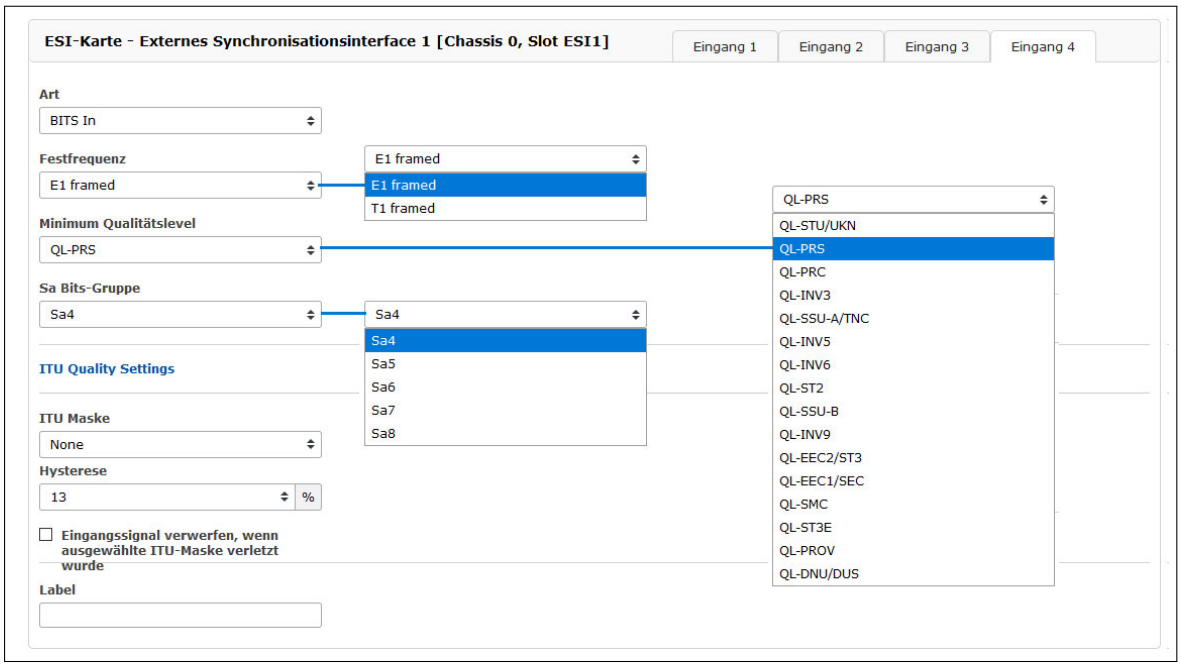
Signaltyp: Frequenzeingang

Frequenz: 1 kHz - 20 MHz des Eingangssignals, 10 MHz ist als Standard eingestellt.

Maximaler Fehler: Eine Diskontinuität einer ganzzahligen Anzahl von Zyklen in der gemessenen Übertragungsphase, die sich aus einem zeitweiligen Verlust des Eingangssignals ergibt. Die maximale Schlupfzahl kann im Bereich von 0,5 - 3 Zyklen gewählt werden, mit 1,5 als Standardwert.

Eingang 3:
Siehe Eingang 2, jedoch mit RJ45-Anschluss und standardmäßig Frequenzeingang mit 2.048 kHz.

Eingang 4: Als feste Frequenz können Sie zwischen E1-framed und T1-framed wählen.



Typ: BITS in.

Feste Frequenz: E1 framed (2,048 MHz), T1 framed (1,544 MHz).

Minimum Qualitätslevel: Synchronisationsstatusnachrichten (SSM), bitorientierter Code (BOC).

Sa Bits-Gruppe: Ort des übertragenen SSM/BOC

Qualität Maximum SSM / Maximum BOC (Qualitätsstufen für T1-framed Signal)
Die Synchronisationsstatusnachricht (SSM) gemäß dem Standard ITU G.704-1998 beinhaltet 4 Bit lange SSM-Qualitätsnachrichten, die über das eingehende E1-framed-Signal empfangen werden. Je niedriger die Bitfolge, desto höher ist die Qualität des Referenztaktes. Die Qualitätsstufen der Taktquellen nach G.704-1998 sind wie folgt:

0000	QL-STU/UKN:	Qualität unbekannt
0001	QL-PRS:	Primäre Referenzquelle
0010	QL-PRC:	Primärer Referenztakt
0011	QL-INV3:	nicht verwendet
0100	QL-SSU-A/TNC:	Synchronisations-Versorgungseinheit A oder Transitknoten-Uhr
0101	QL-INV5:	nicht verwendet
0110	QL-INV6:	nicht verwendet
0111	QL-ST2:	Stratum 2 Takt
1000	QL-SSU-B:	Synchronisations-Versorgungseinheit B
1001	QL-INV9:	nicht verwendet
1010	QL-EEC2/ST3:	Ethernet-Gerätetakt 2
1011	QL-EEC1/SEC:	Ethernet-Gerätetakt 1 / SDH Gerätetakt
1100	QL-SMC:	SONET Minimum-Takt
1101	QL-ST3E:	Stratum 3E Takt
1110	QL-PROV:	Vom Netzbetreiber bereitstellbar
1111	QL-DNU/DUS:	Nicht für die Synchronisation verwenden

Mit dem Feld „Minimum Qualitätslevel“ können Sie den minimalen SSM-Pegel des eingehenden Signals

auswählen, der als Eingangssignal noch akzeptabel ist. Wenn die Uhr eine niedrigere Qualitätsstufe als die konfigurierte minimale SSM-Stufe meldet, wird das System diese nicht zur Synchronisation verwenden.

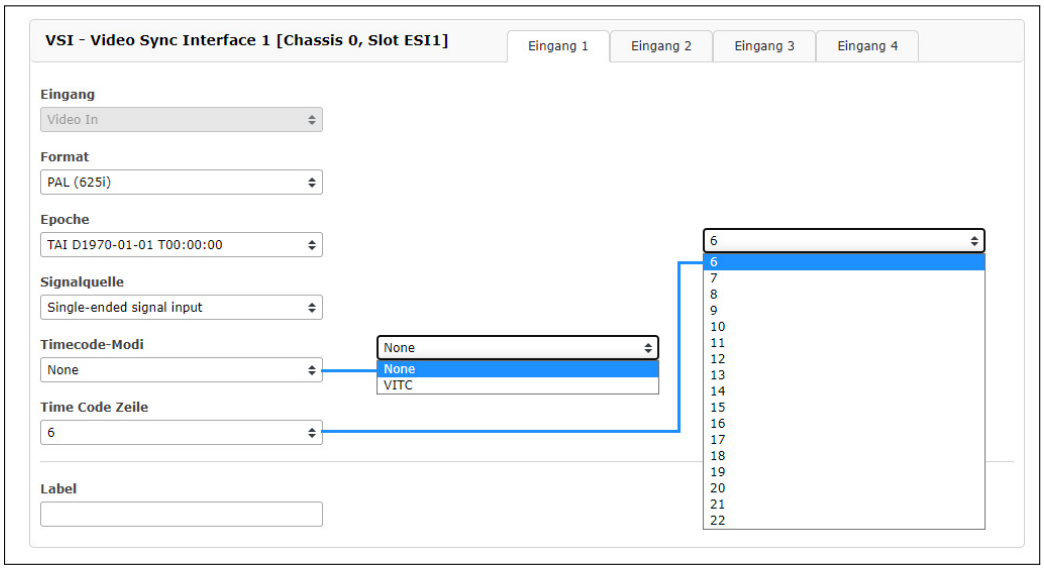
Beispiel:
Der Benutzer hat QL-SSU-B als Minimum-QL für sein System konfiguriert. Ein E1-Eingangssignal, das entweder QL-SSU-A oder QL-PRC meldet, wird zur Synchronisation zugelassen, während ein Signal mit dem Qualitätsniveau QL-EEC1/SEC nicht akzeptiert wird.

Sa Bit-Gruppe
Hier können Sie zwischen der Gruppe Sa4 bis Sa8 Bit wählen, um den Speicherort für SSM-Bits auszuwählen.

13.1.11.4 VSI-Konfiguration über das Webinterface

VSI - Videosignal-Eingangsreferenzen
Menü „IO Konfig → Konfiguration der Eingänge → VSI-Karte“

Konfigurierbare Eingänge



Eingang 1: Video Sync In

Format: PAL 625i

Epoche: TAI

Signalquelle: Single-ended signal input

Time Code Modus: VITC

Time Code Zeile: 6 - 22

Eingang 2: LTC In

Art: LTC 25 FPS (Frmaes pro Sekunde)

tägl. Jam-Zeit: Uhrzeit (hh:ii)

Eingang 3: Word Clk In

Portart: GPIO (General Purpose Input Output)

Richtung: Input

Betriebsart: Always enabled

Eingang 4: PPS In

Impulslänge: $\geq 5\mu$s, aktiv high

13.1.11.5 Konfiguration der Ausgänge

13.1.11.6 IMS BPE

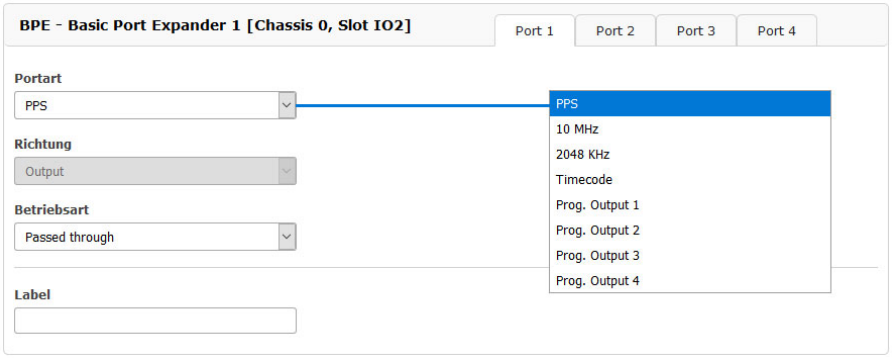
BPE (Basic Port Erweiterung)
Die Standard-BPE ist ein passives Modul und gehört zu den IMS-Ausgangsmodulen. Der Kunde wählt bei Bestellung zwischen verschiedenen physikalischen Anschlüssen und Signalpegeln welche von der Referenzuhr erzeugt werden.

Eine BPE kann mit den folgenden Signalen vorkonfiguriert werden:

- 1PPS, 10 MHz TTL
- 2048 kHz
- Programmierbare Pulse von der Referenzuhr
  (siehe auch → Kapitel 16.5, „Übersicht der programmierbaren Signale“)
- IRIG DCLS+AM (B, AFNOR, IEEE1344 / C37.118)
- ...

Es gibt keine weiteren Konfigurationsmöglichkeiten für ein Standard-BPE-Modul im I/O-Konfigurationsmenü. Für weitere detaillierte Einstellungsmöglichkeiten der Ausgangssignale einer BPE-Karte lesen Sie bitte das Kapitel Menü Uhr.

BPE8000-Serie: Schaltbare Ausgangssignale



Die BPE8000-Serie mit acht verschiedenen BNC- und ST-Anschlusskombinationen, bietet frei konfigurierbare Ausgangssignale über das Webinterface eines IMS-Systems. Ein elektronisch gesteuerter Schalter (Multiplexer) auf der Modulplatine ermöglicht die Auswahl der Signale, die vom Empfängermodul über die Backplane verteilt werden.

13.1.11.7 IMS CPE

Dieses Modul besteht aus einer Standard-Controllerkarte (Back-End) und einer daran angeschlossenen Port-Expanderkarte (Front-End), die eine große Vielfalt von physikalischen Steckverbindern, einschließlich verschiedener elektrischer und optischer Schnittstellen, ermöglicht.

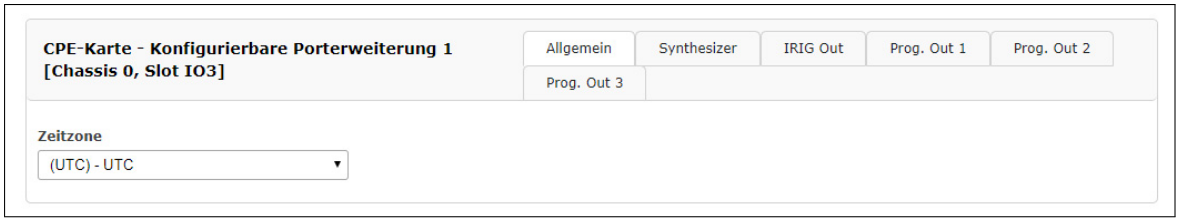
Über das Hauptmenü der CPE gelangen Sie zu spezifischen Untermenüs, in denen die verfügbaren Ausgangssignale konfiguriert werden können.

IMS–CPE - verfügbare Signale:

- Zeitcodes: IRIG A/B/E/G/AFNOR/IEEE1344/C37.118/NASA36
- Frequenz-Synthesizer (Sinuswelle + TTL)
- Programmierbare Impulse: 1PPS, 1PPM, 1PPH, Timer. Single Shot, etc.
- Zyklische Impulse; DCF77 Mark, Sync Status
- Serielle Zeitstrings (RS232 oder RS 422/485)

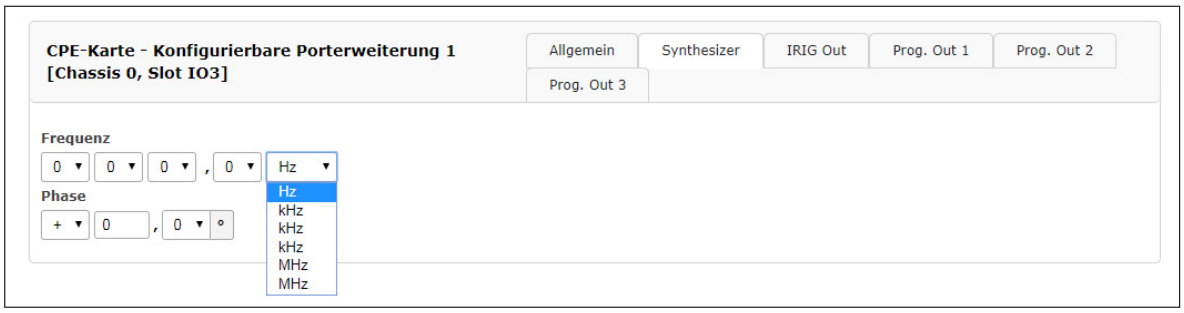
Untermenüs

Allgemein:



Zeitzone Wählen Sie Ihre lokale Zeitzone aus.

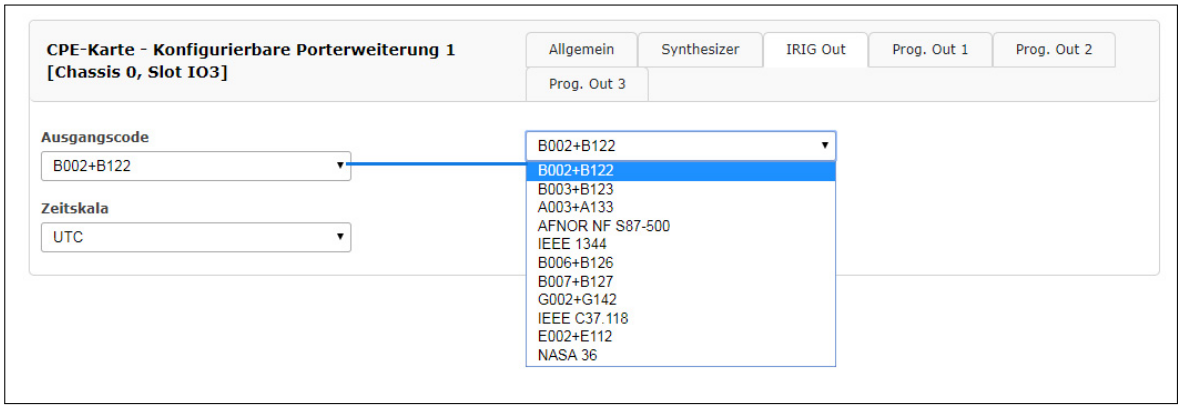
Synthesizer:



Frequenz 1/8 Hz bis 10 kHz: Phase synchron zu Puls pro Sekunde
10 kHz bis 10 MHz: Abweichung der Frequenz < 0,0047 Hz

Phase Bearbeiten Sie die Frequenz und Phase, die vom integrierten Synthesizer erzeugt werden sollen. Frequenzen von 1/8 Hz bis 10 MHz können mit vier Ziffern und einem Bereich eingegeben werden. Wenn die Frequenz auf 0 gesetzt ist, ist der Synthesizer deaktiviert. Mit „Phase“ ist es möglich, die Phase der erzeugten Frequenz von -360° bis +360° mit einer Auflösung von 0,1° einzugeben. Eine Erhöhung der Phase lässt das Signal später ausgeben. Die Phase beeinflusst nur Frequenzen unter 10,00 kHz!

IRIG-Ausgang:

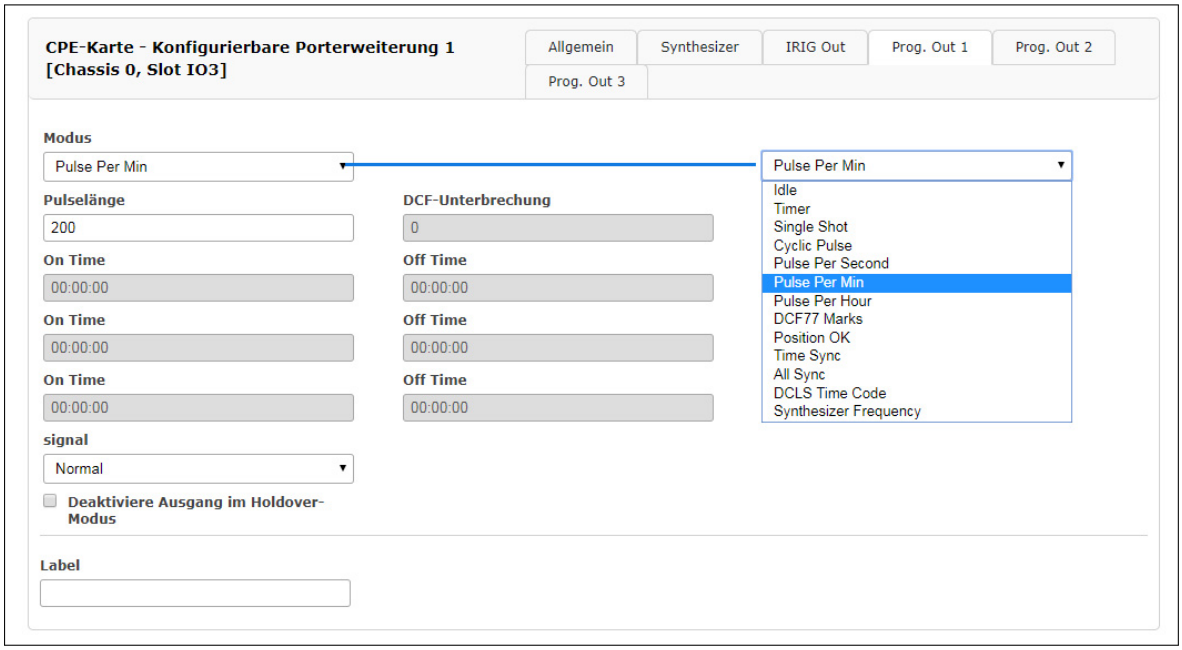


IRIG Ausgangscode Ausgabecode, der für die CPE ausgewählt wird.

Zeitskala Wählen Sie die Zeitskala (UTC oder Ortszeit) aus, welche für Signale mit Zeitinformationen (z.B. Time-Code-Signale) die Zeitbasis bildet.

Die einzelnen Time-Code-Formate werden im → Kapitel 16.4, „Zeitcode-Formate“ näher beschrieben.

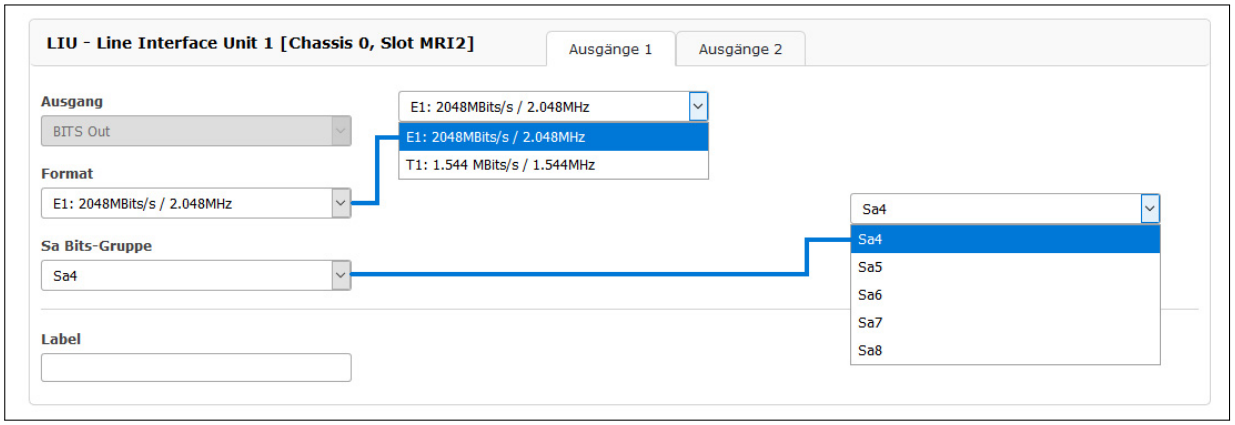
Programmierbare Ausgänge:



Die einzelnen programmierbaren Signale und Impulse werden im
→ Kapitel 16.5, „Übersicht der programmierbaren Signale“ näher beschrieben.

13.1.11.8 IMS - LIU (Line Interface Unit)

E1/T1 - Generator mit 4 oder 8 Ausgängen erhältlich
Erzeugung von Referenztakten für Synchronisationsaufgaben. Das Modul LIU (Line Interface Unit) erzeugt verschiedene Referenztaktimpulse, die vom GPS-Locked Masteroszillator einer vorgeschalteten GPS-Uhr abgeleitet werden. Die Ausgangssignale sind daher mit hoher Genauigkeit und Stabilität verfügbar.



Submenü Ausgang 1:

Ausgangstyp

Taktausgänge:	2,048 MHz (E1-Modus) oder 1,544 MHz (T1-Modus), G.703, 75 Ohm, unsymmetrisch oder 2,048 MHz (E1-Modus) oder 1,544 MHz (T1-Modus), G.703, 120 Ohm, symmetrisch.
BITS	framed Ausgänge mit SSM/BOC-Unterstützung: 2,048 Mbit/s (E1-Modus) oder 1,544 Mbit/s (T1-Modus), 75 Ohm unsymmetrisch oder 2,048 MPs (E1-Modus) oder 1,544 Mbit/s (T1-Modus), 120 Ohm, symmetrisch.
Format	E1 framed (2.048 kBit) oder T1 framed (1.544 kBit)

Mit dem Pulldown-Menü „Output Configuration“ können die verfügbaren Ausgänge der I/O-Slots konfiguriert werden:

Ausgangskonfiguration eines LIU-Moduls (Line Interface Unit):
In diesem Menü kann man zwischen dem E1- oder T1-Modus für die LIU-Ausgänge wählen. Der gewählte Modus ist für alle Ausgänge gleich.

T1 oder E1?
T1 ist ein digitales Trägersignal, das das DS - 1 Signal überträgt. Es hat eine Datenrate von ca. 1.544 Mbit/Sekunde. Das Signal enthält 24 digitale Kanäle und erfordert daher ein Gerät, das über eine digitale Verbindung verfügt.

E1 ist das europäische Äquivalent zu T1. T1 ist der nordamerikanische Standard, während E1 der europäischer Standard für die digitale Übertragung ist. Die Datenrate von E1 beträgt etwa 2 Mbit/Sekunde. Es verfügt über 32 Kanäle mit einer Geschwindigkeit von 64 Kbit/Sekunde. 2 von 32 Kanälen sind bereits reserviert.

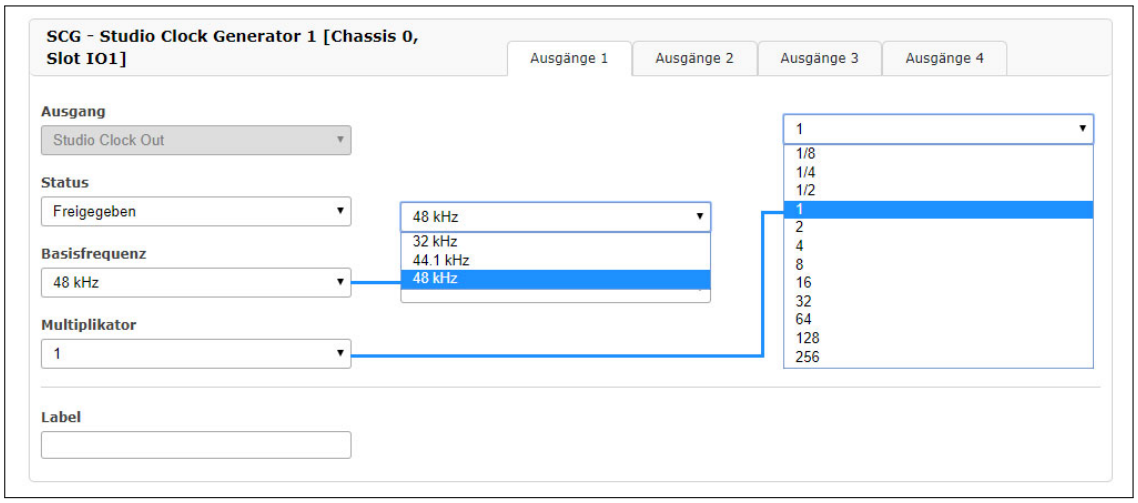
Ein Kanal wird für die Signalisierung und der andere für die Steuerung verwendet. Der Unterschied zwischen T1 und E1 liegt hier in der Anzahl der Kanäle.

Sa Bits
ITU-T-Empfehlungen ermöglichen die Verwendung der Bits Sa4 bis Sa8 in bestimmten Punkt-zu-Punkt-Anwendungen (z.B. Transcoder-Geräten) innerhalb der Landesgrenzen.

Das Sa4-Bit kann als nachrichtenbasierte Datenverbindung für Betrieb, Wartung und Leistungsüberwachung verwendet werden. Das SSM-Bit (Synchronization Status Message) kann im Web GUI für Informationen zur Referenzuhrqualität ausgewählt werden. Sa4 ist standardmäßig ausgewählt.

13.1.11.9 IMS - SCG Studio Clock Generator

SCG-U - Word Clock Generator, unsymmetrisch



Dieses Modul ist nicht nur für unsere IMS-Serie konzipiert und erzeugt verschiedene Tonfrequenzen für Studioanwendungen. Das SCG-Modul kann auch in unserem 19-Zoll-Rackmount- und 1HE-Multipac-Chassis betrieben werden.

- Programmierbare Wordclock-Raten: 24Hz - 12,888MHz
- Referenzeingänge: 1PPS, 10MHz, serieller Zeitstring

Ausgangstyp Studio Clock Out (Word Clock) oder Digital Audio Out (DARS)

Status An oder Aus

Basisfrequenz 32kHz, 44,1kHz, 48kHz

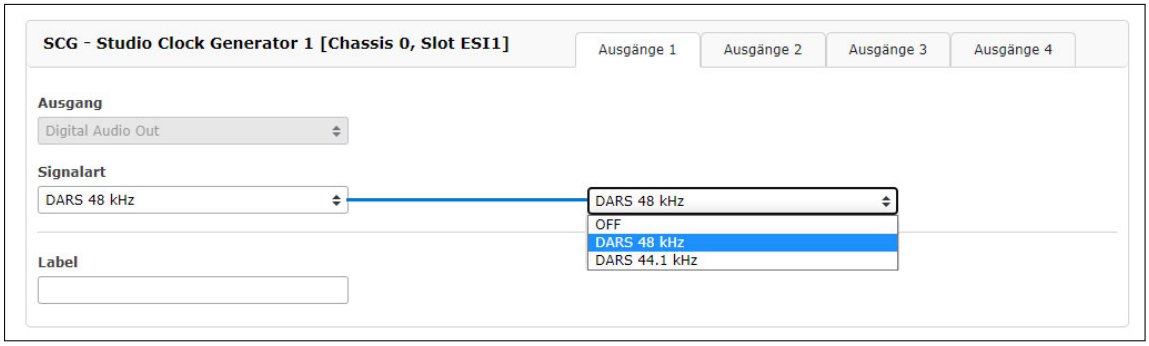
Scale mögliche Skalen sind abhängig von der Grundfrequenz
Wählen Sie eine Basisfrequenz und eine Skala, um die richtige Frequenz am Ausgang X zu erhalten

Beispiel: Ausgang 3 - Status Aktiviert, Basis 48kHz, Skala 1/8
Ausgang 3 = Basisfrequenz * Skala
48kHz * 1/8 = 6kHz am Ausgang 3

SCG-B - DARS Generator, symmetrisch

Die SCG-B ist eine Zusatzkarte zur Erzeugung von „Digital Audio Reference Signals“ für Studioanwendungen. Die 25-polige D-Sub-Buchse verfügt über vier DARS-Ausgänge, die hier im Menü IO Config konfiguriert werden können.

Beispielkonfiguration: SCG-B Ausgang 1



Im Menü „IO Konfiguration“ können Sie für jeden Ausgang der SCG-B den Ausgang auf DARS einstellen. Die vier verfügbaren Ausgänge können optional abgeschaltet werden.

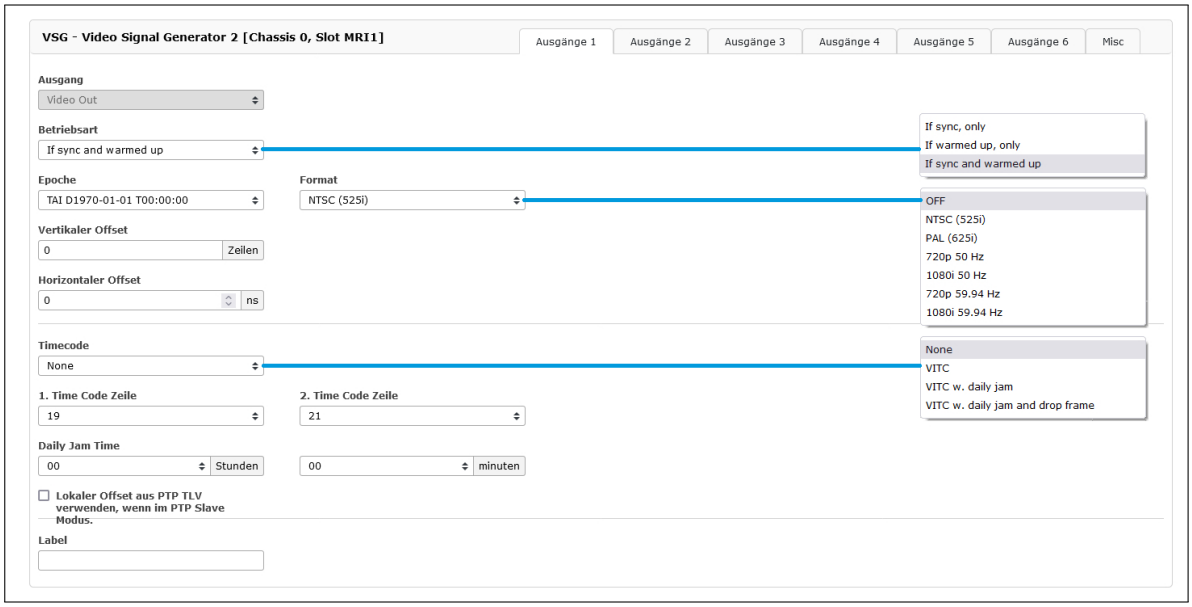
13.1.11.10 IMS - VSG

Die VSG-Module dienen als Video-Signal-Referenz für Studioequipment.

Die IMS-VSG181 stellt über 4x BNC-Buchsen ein analoges Black-Burst- oder Tri-Level-Sync-Signal, ein Linear-Time-Code-Signal (LTC), ein Digital-Audio-Reference-Signal (DARS) und ein Word-Clock-Signal bereit.

Die IMS-VSG181H stellt über 2x BNC-Buchsen ein analoges Black-Burst- oder Tri-Level-Sync-Signal und ein Digital-Audio-Reference-Signal sowie über eine 15-pol. D-Sub-GPIO-Buchse LTC- (symmetrisch und unsymmetrisch), DARS- (nur symmetrisch) und Word-Clock-Signale (nur unsymmetrisch) bereit.

Funktionsweise
Die Karte wird mit einem externen 10MHz Signal, 1PPS und einem Zeittelegramm synchronisiert und erzeugt konfigurierbare Video-Signale in verschiedenen Formaten. Die erzeugten Signale haben einen Phasenbezug zum 1PPS.



Erzeugte Signale:

Black-Out:	NTSC (525i) *(59,94 Hz, „Black-Burst", ITU-R BT.1700/SMPTE ST 170:2004)* PAL (625i) *(50 Hz, „Black-Burst", ITU-R BT.1700)* 720p 50 Hz *(Tri-Level-Sync, SMPTE ST 296)* 1080i 50 Hz *(Tri-Level-Sync, SMPTE ST 274)* 720p 59,94 Hz *(Tri-Level-Sync, SMPTE ST 296)* 1080i 59,94 Hz *(Tri-Level-Sync, SMPTE ST 274)*
DARS:	DARS 48 kHz DARS 44,1 kHz
LTC:	LTC 24 fps / 23,976 Hz LTC 24 fps LTC 25 fps LTC 30 fps LTC 30 fps Drop-Frame *(für NTSC-Inhalte mit einer Bildfrequenz von 29,97 fps)*
Word Clock:	Basisfrequenz - 44,1 kHz oder 48 kHz Multiplikator - 1/32, 1/16, 1/8, 1/4, 1/2, 1, 2, 4, 8, 16, 32

Hinweis:

Standardmäßig erfolgt die Ausgabe von allen unterstützten Signalen erst dann, wenn die Referenzuhr synchron läuft und der interne Oszillator eingeregelt ist. Diese Einstellung stellt die sicherste Signalausgabe dar. Allerdings kann es hier nach Start bzw. Inbetriebnahme u. U. mehrere Stunden dauern, bis die Signale bereitgestellt werden. Ein Teil dieses Prozesses kann übersprungen werden (mit dem entsprechenden Risiko von vorübergehenden Timing-Abweichungen), indem man das Modul so einstellt, dass die Signalausgabe schon bei einer synchronen Uhr ohne eingeregelten Oszillator erfolgt, oder auch bei eingeregeltem Oszillator ohne Synchronisation (Holdover).

13.1.11.11 IMS - LNO (Low Phase Noise Option)

Die IMS - LNO ist eine 10 MHz Generatorkarte, die 10 MHz Sinussignale mit geringem Phasenrauschen an 4 externe Ausgänge liefert. Die Karte verfügt über ein Mikroprozessorsystem, das die Ausgangssignale überwacht und entsprechend Statussignale für das übergeordnete Managementsystem erzeugt.

Es kann in unseren modularen IMS-Systemen eingesetzt werden und ist auch in der M900 Timeserver-Plattform und im GPS-basierten 3HE-Gehäuse einsetzbar, hier jedoch ohne Managementfunktionen.

Die Karte verfügt über einen hochwertigen Oszillator, der an ein externes 10 MHz-Signal gekoppelt ist. Der Mikroprozessor überwacht den Verriegelungszustand der PLL (Phasenregelschleife) und die Aufwärmphase des Oszillators. Er aktiviert die Ausgänge erst, wenn die Phase gesperrt ist. Dieser Zustand wird durch die LEDs angezeigt. Im „Phase Locked"-Zustand werden die Ausgangspegel der vier Ausgänge überwacht und im Fehlerfall durch eine zugeordnete LED signalisiert.

	Kein IMS-System	**IMS-System**
LED 1	**Status Ausgang 1** Grün: OK Rot: Error	**St - Status der LNO180-Karte** Grün: 10 MHz Referenz OK und PLL ist gesperrt Gelb: 10 MHz Referenz OK, aber PLL ist noch nicht gesperrt Rot: Keine 10 MHz Referenz erkannt
LED 2	**Status Ausgang 2** Grün: OK Rot: Error	**In - 10 MHz Referenz und PLL-Status** Grün: OK, 10 MHz an beiden Ausgängen verfügbar Rot: Fehler, kein Signal an einem oder beiden Ausgängen
LED 3	**Status Ausgang 3** Grün: OK Rot: Error	**A - Status Ausgang 1-2** Grün: Ok, 10 MHz an beiden Ausgängen verfügbar Rot: Fehler, kein Signal an einem oder beiden Ausgängen
LED 4	**Status Ausgang 4** Grün: OK Rot: Error	**B - Status Ausgang 3-4** Grün: OK, 10 MHz an beiden Ausgängen verfügbar Rot: Fehler, kein Signal an einem oder beiden Ausgängen

Der Ausgang kann nicht aktiv sein, bevor die PLL gesperrt ist.

13.1.11.12 Andere Ausgangsmodule

Netzwerkkarten:

LNE
Die LNE-Karte fügt der Management-CPU zusätzliche physikalische Netzwerkschnittstellen hinzu, wodurch die Anzahl der verfügbaren NTP- und Service-Ports erhöht wird.

Die zusätzlichen Ports können verwendet werden, um den Netzwerkverkehr auf physischen Netzwerksegmenten zu trennen. Weitere Konfigurationsmöglichkeiten finden Sie im Kapitel „13.1.3“.

Weitere detaillierte Konfigurationseinstellungen für diese Karte finden Sie im Kapitel 13.1.3, „Das Webinterface → Physikalische Netzwerkeinstellungen“.

HPS / TSU - IEEE 1588 Zeitstempel-Module
Die Meinberg Zeitstempelmodule bieten eine zukunftssichere Plattform für Ihre IEEE 1588/SyncE/Carrier Grade NTP Infrastruktur. Der leistungsstarke Dual-Core-Prozessor, die One-Step Masterclock und die 1GE-Schnittstelle mit SFP-Slot unterstützen eine große Anzahl von PTP-Clients.

Die Möglichkeit, Master- und Slave-Betrieb für Standard-, Power-, Telekommunikations- oder SMPTE-Profile auszuwählen, macht dieses Produkt zur flexibelsten PTP-Lösung auf dem Markt, die für eine Vielzahl von Anwendungen geeignet ist.

Viele IEEE 1588 Slave-Geräte oder NTP-Clients aus verschiedenen Marktsegmenten können synchronisiert werden, auch über IPv6-Netzwerke, z.B. eNodeBs für LTE-Basisstationen, Linux-Server mit hardwaregestützten Zeitstempeln für Hochfrequenz-Trading-Anwendungen, IEEE 1588-kompatible IEDs in Smart-Grid-Umgebungen oder IP-vernetzte Audio-/Video-Geräte in Rundfunkstudios.

Die Synchronous-Ethernet-Funktion ermöglicht einen hochgenauen Frequenztransport über Ethernet-Netzwerke. Die Karte kann entweder verwendet werden, um ein SyncE-Signal aus dem Netzwerk als Referenz zu beziehen oder SyncE als Master zu erzeugen.

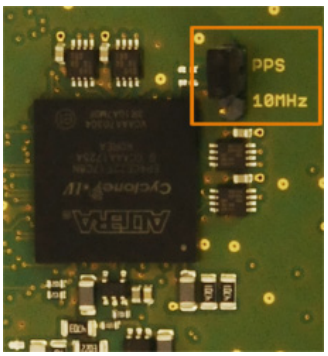
Weitere Informationen zu den PTP-Funktionen und eine detaillierte Konfigurationsanweisung dieser Module finden Sie im Kapitel 13.1.7, „Das Webinterface → PTP → Globale Konfiguration“.

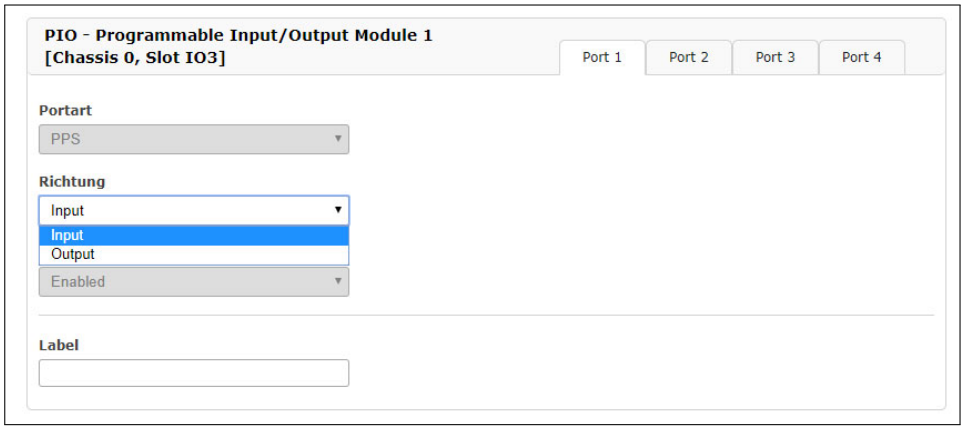
13.1.11.13 IMS Ein/Ausgangskarten

13.1.11.14 PIO - PPS / 10MHz Ein- Ausgangsmodul

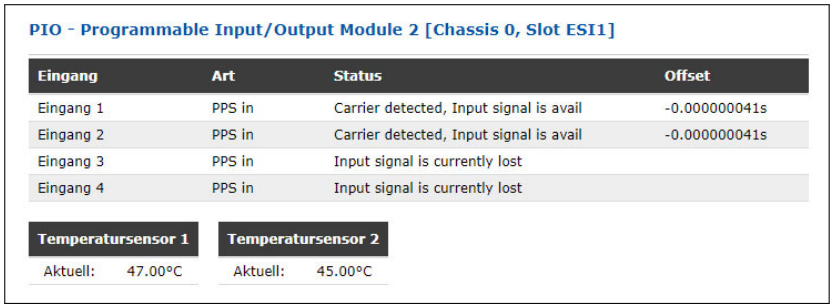
Das PIO Modul wird durch einen Jumper voreingestellt ausgeliefert. Alle Ports sind bei Auslieferung auf PPS (Pulse Per Second) vorkonfiguriert.

Soll diese Voreinstellung geändert werden (auf 10MHz), dann muss die Karte ausgebaut und die Jumperstellung angepasst werden.





Im Web Interface kann dann jeder Port einzeln auf „Input“ oder „Output“ eingestellt werden. Ist ein Port auf „Output“ eingestellt, dann wird der System-PPS bzw. die 10MHz Referenzfrequenz an diesem Anschluss ausgegeben. Wird ein Port auf „Input“ gestellt, dann wird das eingehende Signal mit dem System-PPS bzw. mit der 10MHz Referenzfrequenz verglichen. Die Offsetwerte werden im Statusfenster angezeigt.



13.1.12 SyncMon

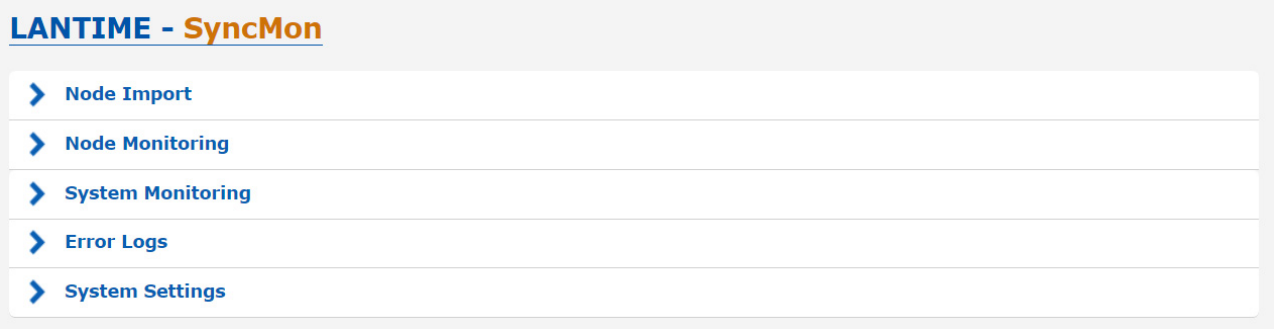


Abbildung: Der SyncMon-Dialog im LANTIME Webinterface.

13.1.12.1 Einleitung SyncMon

Die Funktion **SyncMon** (Sync Monitor) dient zum Messen, Überwachen und Berichten der Genauigkeit von Netzwerkknoten gegenüber einer UTC-rückverfolgbaren Quelle (z.B. einer GPS- oder Multi-GNSS-Uhr oder einem lokalen Zeitdienst wie NPL). SyncMon kann Knoten überwachen, die über die Netzwerkprotokolle PTP (sowohl IEEE 1588v1 als auch IEEE 1588v2) oder NTP (RFC1305) synchronisiert sind.

PTP-Knoten müssen den Meinberg-TLV-Ansatz oder Standard-PTP-Management-Meldungen unterstützen, da sie sonst nicht überwacht werden können. NTP-Knoten können nur überwacht werden, wenn sie so konfiguriert sind, dass sie auf NTP-Client-Anfragen reagieren.

Hinweis:

Ein NTP-Client, der den Windows Time-Service *W32Time* verwendet, reagiert nicht auf NTP-Client-Anfragen gemäß Standardkonfiguration. *W32Time* muss konfiguriert werden, um gleichzeitig als Client und Server zu fungieren. Andernfalls kann der Knoten nicht über SyncMon überwacht werden.

Es können aber auch alle konfigurierten MRS-, FDM-, PIO- und ESI-Eingänge (wie PPS- und Frequenz-Eingänge) überwacht werden, wenn eine ESI-Karte (External Synchronization Input) vorhanden ist. Die Funktion SyncMon ist ab sofort auf Meinberg IMS- und LANTIME-Systemen mit LTOS-Version 7.00 oder höher verfügbar. Für die PTP-Überwachung mit SyncMon muss eine IMS-HPS100 PTP-Karte mit einer Lizenz von mindestens 1024 Clients installiert sein.

Der SyncMon kann auch als Knoten unabhängig von einer Hauptuhr ausgeführt werden. In diesem Fall kann ein SyncMon-Knoten grundsätzlich überall im Netzwerk platziert werden, im Idealfall aber so nah wie möglich an den Slaves, um deren tatsächliche Genauigkeit messen zu können. Gleichzeitig können Sie auch die Leistung einer Grandmaster-Clock überwachen und die potenzielle Netzwerkasymmetrie messen, die in der Verbindung zwischen einem GM und dem SyncMon-Knoten vorhanden ist.

Es ist möglich, bis zu 1.000 Knoten für die Überwachung in der SyncMon-Schnittstelle zu konfigurieren, die auf einem Standard-LANTIME- oder IMS-System läuft. Sie können Anfragen- und Protokollierungsintervalle für jeden einzelnen Knoten separat festlegen. Außerdem kann für jeden Knoten eine Offset-Grenze konfiguriert werden, die bei Überschreitung des Grenzwertes für diesen Knoten eine Alarmmeldung auslöst (über SNMP, E-Mail oder einen anderen benutzerdefinierten Kanal). Für NTP-Knoten können Sie auch ein Stratum-Limit definieren, der auch bei Überschreitung des definierten Stratums eine Alarmierung auslösen kann.

Darüber hinaus ist es für jeden Knoten möglich, alle Überwachungsdaten und deren Protokolldateien herunterzuladen, die zur Erstellung eines Berichts oder für weitere statistische Analysen verwendet werden können. Die Daten jedes überwachten Knotens können online über das syslog-Protokoll mit verschiedenen Formaten gesendet werden oder anhand eines rsync-Dienstes auf einem externen Datenserver bei Änderungen aktualisiert werden. Die aktuellen Online-Daten eines jeden Knotens können anhand Programme wie *curl* oder *wget*

im JSON-Format abgerufen werden, um diese dann anderen Managementsystemen weiterzugeben.

Eine JSON-Datei für jeden Knoten ist verfügbar unter: */www/htdocs/syncmon/[alias].json*. Hier ist [alias] als Platzhalter mit dem eigentlichen Node-Alias zu ersetzen.

13.1.12.2 SyncMon - Erste Schritte

Beim ersten Start von SyncMon ist noch keine Überwachung aktiviert. Um die Überwachung zu aktivieren, muss mindestens ein Knoten hinzugefügt werden. Klicken Sie auf die Schaltfläche „**Add Node**“, um einen neuen Überwachungsknoten hinzuzufügen.

13.1.12.3 SyncMon Statusüberwachung und Konfiguration über Webinterface

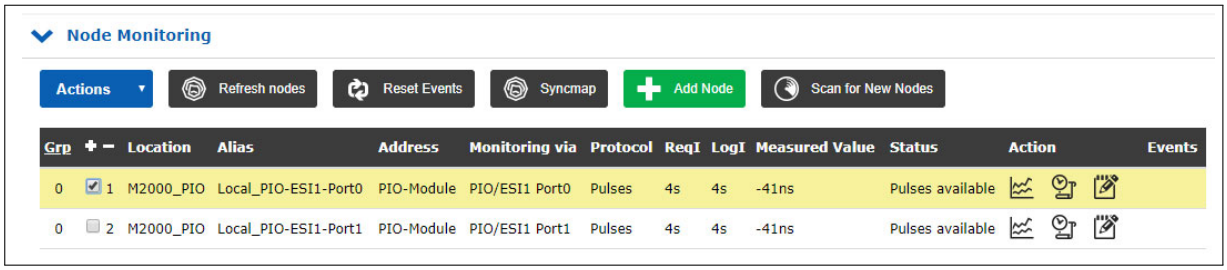
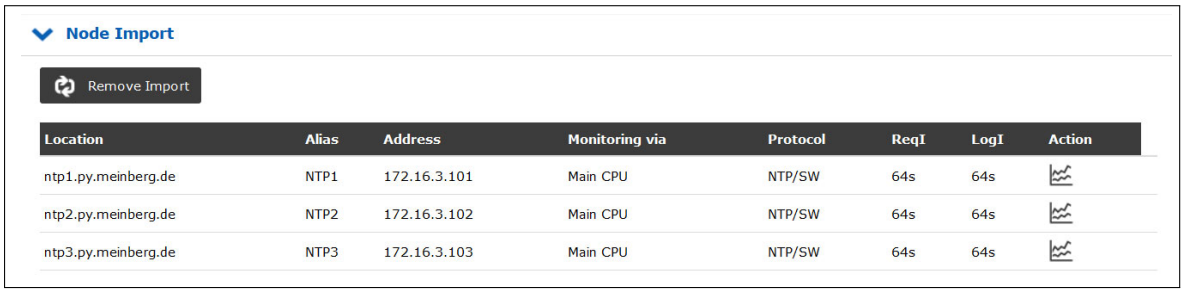


Abbildung: SyncMon-Benutzeroberfläche auf LANTIME-Systemen bei LTOS-Version 7.00 oder höher.

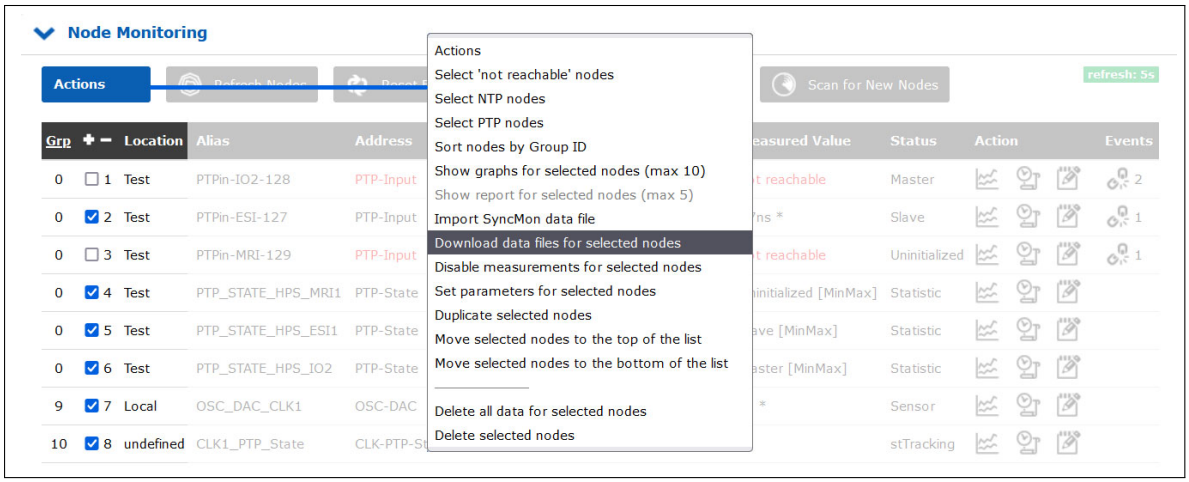
Der Bereich „Node Monitoring“ (Knotenüberwachung) zeigt den aktuellen Status und die Konfiguration aller überwachten Knoten an. Ein Überwachungsknoten kann entweder ein Gerät im Netzwerk wie ein NTP-Server oder PTP-Gerät, oder ein LANTIME-spezifisches Eingangsmodul für z.B. Impulse oder Frequenzen sein. Jede Zeile in der Tabelle repräsentiert einen überwachten Knoten oder eine Gruppe von Knoten. Die Tabelle kann im Flat- oder Gruppenmodus angezeigt werden. Im Flat-Modus werden nur Knoten in einer Zeile angezeigt. Zur Strukturierung der Tabelle kann der Gruppenmodus durch Klick auf die Überschrift „**Grp**“ in der ersten Spalte ausgewählt werden: So können alle Knoten mit dem gleichen Index gruppiert und als Gruppen geöffnet werden. Ein erneutes Klick auf die Überschrift „**Grp**“ wechselt zurück in den Flat-Modus.

Der Status im Webinterface wird alle 10 Sekunden automatisch aktualisiert.

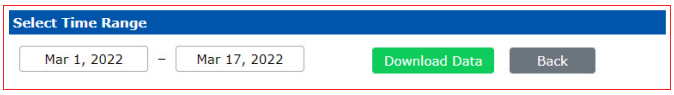
13.1.12.4 Node Import

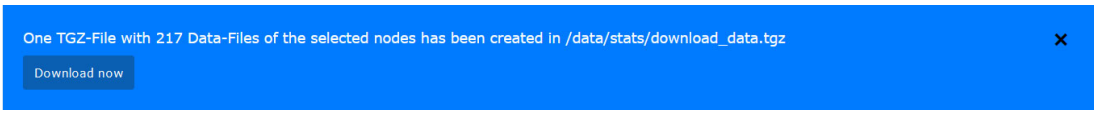


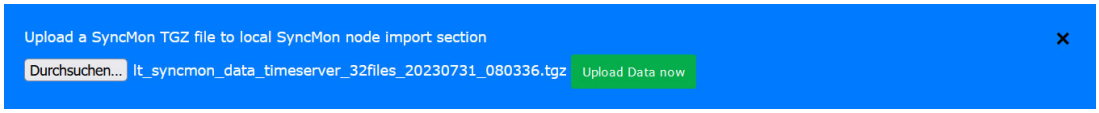
Das Menü „Node Import“ wird angezeigt, wenn vorher ein Satz an Knoten über die Funktion „Actions → Download Data Files for selected Nodes“ von einem LANTIME heruntergeladen wurde und danach über die „Actions → Import Sync Mon data files“ auf dem LANTIME importiert wurden. Es können auch Knoten von demselben LANTIME exportiert und wieder zurück importiert werden. Auf diesem Weg lassen sich zum Beispiel bestimmte Knoten zusammenhängend und übersichtlich gruppiert in der Liste der überwachten Knoten darstellen.



Wenn ein Satz an Dateien heruntergeladen werden soll, dann müssen zuerst die Knoten ausgewählt werden und im nächsten Schritt muss der gewünschte Zeitraum eingetragen werden, in dem die Knoten überwacht wurden. Nach dem Bestätigen wird eine TGZ-Datei generiert, die dann zum Download bereitgestellt wird.







Dieses Archiv kann dann wieder auf einen LANTIME über „Actions → Import Sync Mon data files“ hochgeladen werden.

Über den Button „Remove Import“ im Menü „Node Import“ können die importierten Knoten einfach wieder entfernt werden.

13.1.12.5 Node Monitoring

Im Bereich „Node Monitoring“ können Sie neue Knoten hinzufügen, um deren Genauigkeit zu messen und deren Synchronisationsleistung zu überwachen. Durch Auswahl der Schaltfläche **„+ Add Node“** (Knoten hinzufügen) gelangen Sie zu einem Konfigurationsdialog, um einen neuen Knoten zur Überwachung hinzuzufügen.

Schaltfläche „Refresh Nodes“ (Knoten aktualisieren):
Mit dieser Schaltfläche können Sie die Werte aktualisieren, auch wenn die automatischen Anfrageintervalle größer sind. Eine neue Messung wird dabei durchgeführt und der Status in der Tabelle der Knoten wird aktualisiert. Die aktualisierten Werte werden der Liste der Messwerte hinzugefügt, um den Mittelwert zu berechnen. Es wird keine Messung an allen HPS-Karten mit PTP durchgeführt.

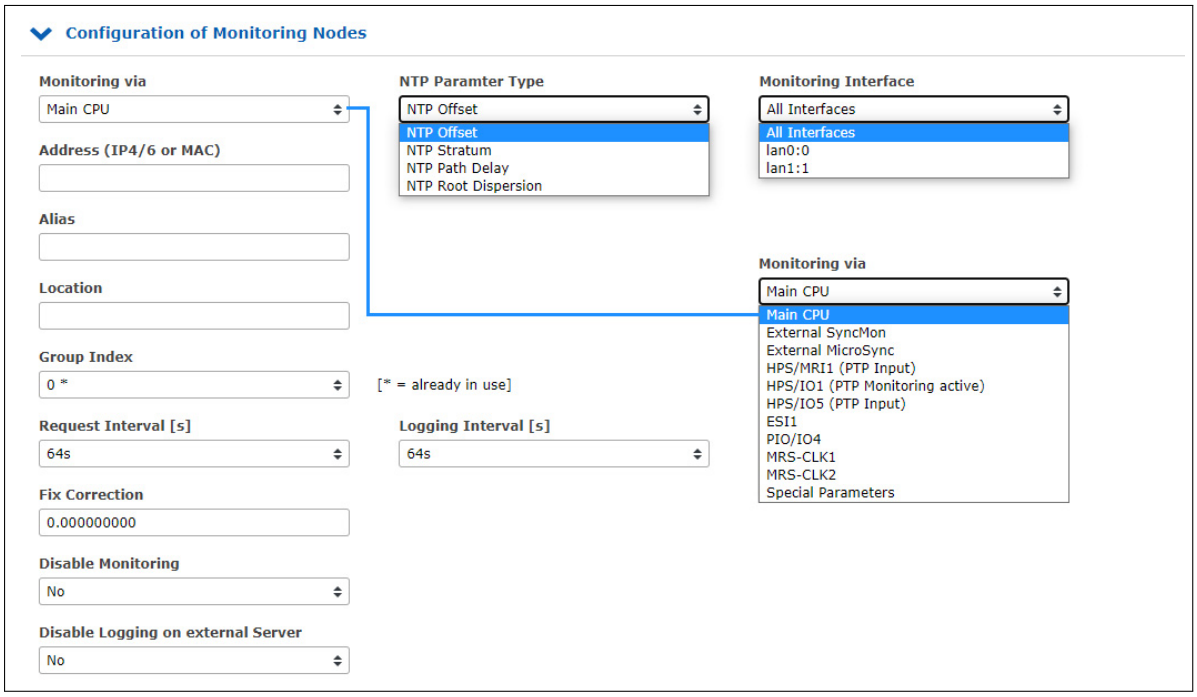
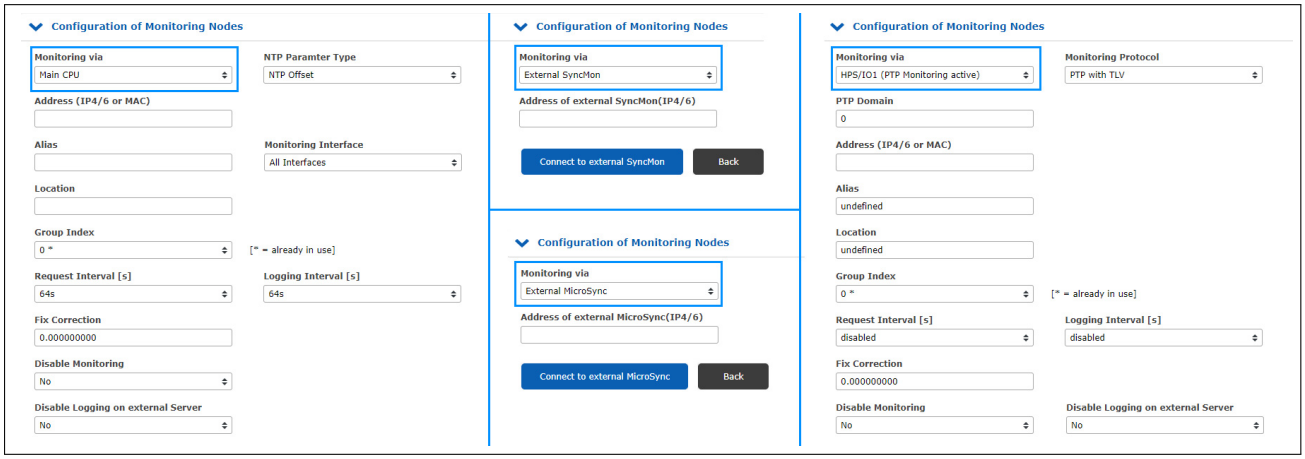


*Abbildung: Hinzufügen eines Knoten anhand „**Add Node**“.*

Die Funktionen im Konfigurationsdialog „**Add Node**“ hängen von der Auswahl des ersten Parameters „**Monitoring via**“ (Monitoring über) ab und liefern verschiedene Eingabemasken mit unterschiedlichen Optionen:



Monitoring via:
Wählen Sie eine Überwachungsinstanz aus der Dropdown-Liste aus. Die Dropdown-Liste erscheint in verschiedenen Hardwarekonfigurationen unterschiedlich. Die folgenden Optionen stehen ggf. zur Verfügung:

Main CPU: Diese Monitoring-Instanz ist immer verfügbar und unabhängig von der Hardware-Konfiguration des LANTIME-Systems. Es kann nur native NTP-Knoten überwachen, die auf NTP Client-Anfragen reagieren.

Hinweis:

Ein NTP-Client, der den Windows Time-Service *W32Time* verwendet, reagiert nicht auf NTP-Client-Anfragen gemäß Standardkonfiguration. *W32Time* muss konfiguriert werden, um gleichzeitig als Client und Server zu fungieren. Andernfalls kann der Knoten nicht über SyncMon überwacht werden.

Sie können alle zugeordneten Schnittstellen gleichzeitig überwachen lassen oder eine bestimmte Schnittstelle aus einer Liste auswählen, falls vorhanden.

Über das Dropdown-Menü „**NTP Parameter Type**“ kann ausgewählt werden, ob der „*NTP Offset*“, „*NTP Stratum*“, „*NTP Path Delay*“ oder „*NTP Root Dispersion*“ gespeichert werden soll.

Wenn mehrere Netzwerkschnittstellen vorhanden sind, kann über das Dropdown-Menü „**Monitoring Interface**“ eine spezifische Schnittstelle oder alle Schnittstellen („*All Interfaces*“) ausgewählt werden.

External SyncMon: Diese Überwachungsinstanz kann Knoten und Sensoren anderer LANTIME-Geräte mit aktiviertem SyncMon überwachen. Bei der Auswahl eines externen SyncMon per IP-Adresse wird eine Liste der verfügbaren Knoten von diesem externen SyncMon heruntergeladen. Konfiguration und Daten werden über die HTTP(S)-Schnittstelle mit *curl* übertragen.

External Microsync: Hiermit können MRS Referenzen von externen microSync-Geräten überwacht werden. Bei der Auswahl eines externen microSyncs per IP-Adresse wird eine Liste der verfügbaren Referenzen von diesem externen microSync heruntergeladen. Konfiguration und Daten werden über die HTTP/S-Schnittstelle (*curl*) übertragen.

HPS: IMS-HPS100-Karten können zur Überwachung von PTP-Instanzen oder NTP-Uhren über den eigenen Netzwerkanschluss verwendet werden.

Wenn ein HPS-Modul als PTP-Slave konfiguriert ist (siehe LANTIME PTP-Konfiguration), dann wird die HPS-Karte sich wie ein Standard-PTP-Slave verhalten, mit all seinen Optionen wie Profile und netzwerkspezifischen Konfigurationen. Pro HPS-Modul kann allerdings nur zur gleichen Zeit immer nur ein PTP-Master überwacht werden-

Wenn die HPS-Karte als Überwachungssystem konfiguriert werden soll (siehe LANTIME PTP- Konfiguration), dann muss sie mindestens mit einer 1024er-Client-Lizenz ausgestattet sein. Ist das der Fall, dann können mehrere PTP-Knoten über den Netzwerkanschluss der HPS-Karte überwacht werden. Diese Überwachungsinstanz kann PTP-Knoten überwachen, die die Protokolle „PTP with TLV“ (proprietär für einen Meinberg Sync Node), „PTP with MGMT“ (definiert im IEEE 1588v2 Standard), NTP mit Software-Zeitstempel oder „PTPv1 with MGMT“ (definiert im IEEE 1588v1 Standard) unterstützen.

Hinweis:

„PTPv1 with MGMT“ erfordert eine IMS-HPS100-Karte mit mind. Firmware-Version 2.1.0 und LTOS-Version 7.06.110. Prüfen Sie, welche Firmware-Version Ihre HPS-Karte hat, indem Sie „**System** → **Systeminformationen** → **Versionsinformationen**“ aufrufen. Die Versionsnummer steht unten bei der Auflistung der installierten Karten neben „ID“, z.B. „HPS6 Cyclone5 High Performance Sync Module HPS100 2.0.6 2022-06-30 License (2048/262144)“.

Wenn Sie mit SyncMon PTPv1-Instanzen überwachen möchten aber die Firmware-Version Ihres HPS100-Moduls nicht aktuell ist, kontaktieren Sie bitte den Technischen Support von Meinberg, der Ihnen gerne weiter hilft.

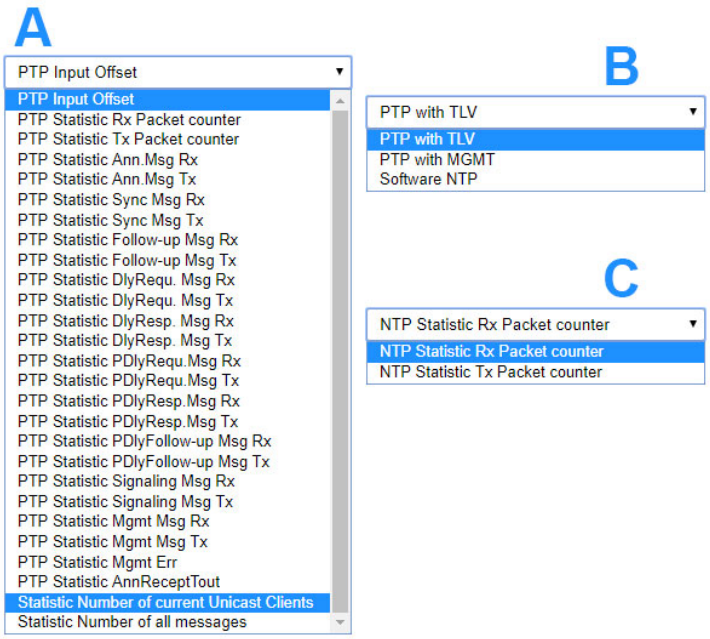
Das spezielle Protokoll „PTP with TLV“ ist wie ein umgekehrtes PTP: Ein PTP-Delay-Request-Paket mit einem speziellen TLV wird an das PTP-System gesendet und dieses antwortet mit einem Synchronisationspaket und einem Delay-Response-Paket. Mit diesem Verfahren kann der Offset von der internen Referenz auf dem PTP-Gerät gemessen werden, auch wenn sich dieses PTP-System im Master-, Slave- oder Passiv-Modus befindet.

Statistic Types:

Es ist möglich, diverse Statistiken über Knoten abzuleiten, die über eine HPS-Karte im PTPv2-Betriebsmodus, Überwachungsmodus oder NTP-Modus überwacht werden. Diese Statistiken werden vom Knoten abgefragt und als Antwort an SyncMon zurückgesendet.

Hinweis:

Die Aufzeichnung von berichteten Statistiken im PTPv1-Betriebsmodus ist nicht möglich, weil das Protokoll die Abfrage von Statistiken über Management-Nachrichten nicht vorsieht.



HPS-Karten im PTP- oder NTP-Modus unterstützen Paketstatistiken, die individuell überwacht werden können:

A: HPS im PTPv2 Betriebsmodus.
B: HPS im Überwachungsmodus.
C: HPS im NTP-Modus.

ESI: Diese Überwachungsinstanz kann PPS- und Frequenz-Knoten mit der ESI-Karte (Extension Signal Input) überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Verfügbare Optionen sind: PPS0, Freq In0, Freq In1, BITS In2.

MRS-CLK: Diese Überwachungsinstanz kann alle aktivierten MRS-Eingangssignale für jeden MRS-Referenztakt überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Verfügbare Optionen sind: GNSS/GPS, NTP, PTP, PPS, IRIG, 10MHz, E1, 2048kHz, je nach Hardware-Optionen (siehe Registerkarte „**Uhr**“ im Web-Interface).

PIO: Diese Überwachungsinstanz kann PPS- und Frequenz-Knoten mit einer PIO-Karte (Programmable Input/Output) überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Das hängt von der Konfiguration der PIO-Karte ab. Verfügbare Optionen sind: PPS0, PPS1, PPS2, PPS3, Freq In0, Freq In1, Freq In1, Freq In2, Freq In3.

FDM: Diese Überwachungsinstanz kann 50/60 Hz-Netzknoten mit einer FDM-Karte (Frequency Deviation Monitor) überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Die verfügbaren Optionen sind: Zeitabweichung oder Frequenzabweichung.

Special Parameters: Diese Überwachungsinstanz kann verschiedene Parameter überwachen, wenn diese aktiviert sind:

Process Memory: (Arbeitsspeicher des Prozesses)
Hiermit kann die Speicherauslastung von System-Prozessen überwacht werden. Dazu muss der Name des Prozesses angegeben werden und die Werte werden in **%** dargestellt.

Nach der Auswahl von „**Special Parameters** → **Process Memory**“ die Felder
NTP Parameter Type → **Special Parameter** und
Address (IPv4/IPv6 or MAC) → **Name of Process** werden angezeigt.

Hier muss in „**Name of Process**“ der Prozessname eingetragen werden: Das könnte z.B. *ntpd* oder *httpd* sein. Über eine SSH-Verbindung mit der LANTIME CLI können Sie sich eine Liste der ausgeführten Prozesse (mit Namen) mit dem Kommando *‘ps ax‘* ausgeben lassen.

ID of Selected HPS Card: (ID der ausgewählten HPS-Karte)
Diese Option erscheint nur, wenn im System eine HPS-Karte als PTP-Slave aktiv ist.
Wenn mehrere HPS-Karten im System als PTP-Slave vorhanden sind, dann wird die beste Karte über den internen PTP-BMCA (Best Master Clock Algorithm) ausgewählt und als MRS/PTP-Referenz benutzt. Mit diesem Parameter kann die ID der ausgewählten Karte überwacht werden.

ID of Selected NTP Server: (ID des ausgewählten NTP-Servers)
Diese Option erscheint nur, wenn im System externe NTP-Server konfiguriert wurden.
Sind mehrere externe NTP-Server konfiguriert, dann wird der beste externe NTP-Server über ein spezielles NTP-Selektierungsverfahren ausgewählt und als MRS/NTP-Referenz benutzt.
Mit diesem Parameter kann die ID des ausgewählten externen NTP-Servers überwacht werden.

Address (IP4/6 or MAC) (Adresse, IP4/6 bzw. MAC):
IPv4/IPv6 oder MAC-Adresse eines Knotens, den Sie über das Netzwerk überwachen möchten. Hostnamen sind nicht erlaubt.

Alias:
Aliasname für einen Überwachungsknoten, um ihn in der gesamten Tabellenübersicht leicht zu finden. Der Aliasname, der vom Benutzer festgelegt wird, bestimmt auch den Namen des Verzeichnisses auf dem gewählten Speichermediums („Data Storage Base Path“) jedes Knotens. Der Aliasname muss eindeutig, muss ohne Leerzeichen sein (Leerzeichen werden automatisch in‘_‘ umgewandelt) mit einer maximalen Länge von 63 Zeichen. Es ist möglich, den gleichen Knoten (z.B. die gleiche IP-Adresse) mit unterschiedlichen Aliasnamen zu überwachen: Dies kann nützlich sein, wenn Sie den gleichen Knoten von verschiedenen Überwachungsmodulen aus überwachen möchten (z.B. verschiedene IMS-HPS100-Karten mit getrennten Netzwerkpfaden).

Location (Standort):
Geben Sie einen physischen Standort eines Überwachungsknotens ein, damit Sie diesen Knoten leichter orten können. Der Ortsname muss ohne Leerzeichen (Leerzeichen werden automatisch in ‘_‘ umgewandelt) mit einer maximalen Länge von 63 Zeichen sein.

Group Index (Gruppenindex):
Sie können überwachte Knoten innerhalb einer logischen Gruppe anordnen, indem Sie ihnen den gleichen Index zuweisen. Beispielweise können Knoten mit einem gleichen Gruppenindex versehen werden, die von gleicher Art (NTP, PTP, PPS) oder am gleichen Ort sind, um die Organisation zu erleichtern. Knoten mit dem gleichen Gruppenindex werden automatisch in der Tabelle sortiert. Die Tabelle kann im Flat- oder Gruppenmodus angezeigt werden. Im Flat-Modus werden nur Knoten in einer Zeile angezeigt. Zur Strukturierung der Tabelle kann der Gruppenmodus durch Klick auf die Überschrift „**Grp**“ in der ersten Spalte ausgewählt werden: So können alle Knoten mit dem gleichen Index gruppiert und als Gruppen geöffnet werden. Ein erneutes Klick auf

die Überschrift „**Grp**“ wechselt zurück in den Flat-Modus.

Request Interval (s) (Anfrageintervall):
Intervall in Sekunden, in dem ein Überwachungsknoten Anfragen an die Slaves/Clients sendet. Das minimale Anfrageintervall beträgt 1 s, das maximale 3600 s. Das Standardintervall ist 64 s. Das Senden von Anfragen an die Knoten und die Protokollierung können mit der Einstellung „**Disabled**“ deaktiviert werden.

Logging Interval (s) (Aufzeichnungsintervall):
Intervall in Sekunden, in dem der gemessene Offset und Stratum in eine Protokolldatei geschrieben werden. Wenn das Aufzeichnungsintervall deaktiviert ist, werden keine Daten in der Logdatei gespeichert. Wenn das Anfrageintervall aktiviert und das Protokollintervall deaktiviert wurde, werden die Knoten überwacht und Grenzwerte und Benachrichtigungen überprüft (und entsprechende Alarms ausgelöst), aber keine Daten gespeichert. Wenn das Anfrageintervall kleiner als das Aufzeichnungsintervall ist, wird der Mittelwert der gemessenen Offsets im Anfrageintervall protokolliert und der Minimal- und Maximalwert im Protokollintervall zusätzlich festgehalten.

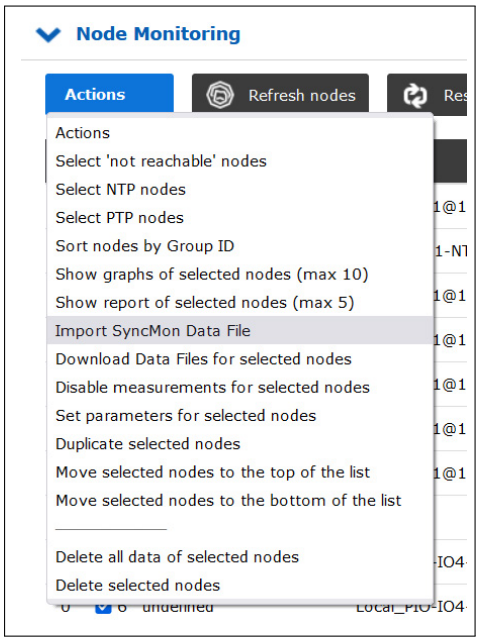
Request Delay (ms) (Anfragewartezeit):
Eine Wartezeit in Millisekunden, die der SyncMon-Knoten einhalten soll, bevor eine PTP-Nachricht mit TLV-Daten zu jedem Intervall versendet wird. Mit dieser Wartezeit soll vermieden werden, dass Knoten mit mehreren gleichzeitigen Anfragen von unterschiedlichen SyncMon-Instanzen überlastet werden. Wenn z.B. mehrere SyncMon-Instanzen bei identischen Request Intervals mit unterschiedlichen Request Delay-Werten belegt werden, so können die Anfragenachrichten in „gestaffelter“ Reihenfolge verschickt werden.

Fixed Offset Correction [s] (Korrektur eines festen Offsets):
Wenn ein fester Offset bekannt ist (z.B. durch Netzwerk-Asymmetrie), kann dieser Wert als Korrekturwert hier eingetragen werden. Der „Fixed Offset Correction“ wird beim gemessenen Wert (Measured Value) immer **aufgerechnet**. Möchten Sie einen Korrekturwert **abziehen**, ist hier einen **negativen** Wert einzutragen. Ein eingetragener fester Offset wird in der Übersicht mit einem * in der Spalte „**Measured Value**“ angezeigt.

Disable Monitoring (Überwachung deaktivieren):
Die Überwachung kann für jeden Knoten deaktiviert werden. Wenn der Knoten deaktiviert wurde, werden keine Überwachungsdaten an den Knoten gesendet und keine Daten gespeichert.

Disable Logging on External Server (Protokollierung auf externem Server deaktivieren):
Die gemessenen oder protokollierten Daten können über das syslog- oder rsync-Protokoll an einen externen Server gesendet werden. Dies kann für jeden Knoten deaktiviert werden (siehe Systemeinstellungen für externe Serverkonfiguration).

13.1.12.6 Schaltfläche "Actions"



Die Schaltfläche „Actions“ kann verwendet werden, um systematisch bestimmte Knoten in der SyncMon-Knotenliste auszuwählen und bestimmte Operationen an ihnen durchzuführen sowie die Reihenfolge in der Liste zu ändern:

Select 'Not Reachable' Nodes': Es werden alle nicht erreichbaren Knoten ausgewählt.

Select NTP Nodes: Es werden alle Knoten ausgewählt, die NTP-Nachrichten senden oder empfangen.

Select PTP Nodes: Es werden nur PTP-Grandmaster oder Slave-Systeme ausgewählt.

Sort Nodes by Group ID: Alle Knoten werden nach ihrer Gruppen-ID geordnet (aufsteigend).

Show Graphs of Selected Nodes: Die Graphen der ausgewählten Knoten werden angezeigt (max. 10).

Show Report of Selected Nodes: Die Reports der ausgewählten Knoten werden angezeigt (max. 5).

Import SyncMon Data File: Knoten und Daten werden aus einer Datendatei importiert.

Download Data Files for Selected Nodes: Eine Datendatei wird aus den ausgewählten Knoten erzeugt.

Disable Measurements for Selected Nodes: Die ausgewählten Knoten werden nicht mehr überwacht.

Set Parameters for Selected Nodes: Die ausgewählten Knoten können gemeinsam konfiguriert werden.

Duplicate Selected Nodes: Ausgewählte Knoten werden dupliziert.

Move Selected Nodes to the Top of the List: Die ausgewählten Knoten werden an das Ende der Liste verschoben.

Move Selected Nodes to the Bottom of the List: Die ausgewählten Knoten werden an den Anfang der Liste verschoben.

Delete All Data of Selected Nodes: Alle gespeicherten Daten der ausgewählten Knoten werden gelöscht.

Delete Selected Nodes: Alle ausgewählten Knoten werden gelöscht.

Show a Status Overview for Current Day: Zeigt eine Statusübersicht für jeden in der Liste angezeigten Knotenliste, einschließlich gemessener und gemeldeter Offsets und des zuletzt aufgezeichneten Fehler. Ermöglicht auch den Zugriff auf Diagramme und Fehlerprotokolle für jeden Knoten.

Diese Option wird nur angezeigt, wenn keine Knoten ausgewählt sind.

Show a Status Overview of Time Range: Fordert Sie auf, einen Zeitbereich für die Übersicht anzugeben. Wenn *Add SyncMap to Report* aktiviert ist, enthält die Übersicht eine Kopie der aktuellen SyncMap.

Sobald der Zeitbereich angegeben ist, wird eine Statusübersicht über jeden in der Liste angezeigten Knoten angezeigt, einschließlich der gemessenen und gemeldeten Offsets und des zuletzt aufgezeichneten Fehlers. Für jeden Knoten können auch Diagramme und Fehlerprotokolle abgerufen werden.

Diese Option wird nur angezeigt, wenn keine Knoten ausgewählt sind.

13.1.12.7 Export und Import von Daten im SyncMon

Über die Export/Import Funktion können gezielt Daten von einzelnen Nodes über einen gewählten Zeitraum exportiert werden. Dabei werden die Tages-Daten-Dateien in einem File (*.tgz*) gepackt, welches dann heruntergeladen werden kann. Die Export Funktion „Download Data Files for Selected Nodes" findet sich unter dem „Actions" Menü wenn vorher mindestens ein Node ausgewählt wurde. Es wird dann ein Zeitbereich abgefragt von wann bis wann die Daten gespeichert werden sollen. Der Name des TGZ-Files hat folgendes Format:

```
lt_syncmon_data_ + Hostname + Anzahl der enthaltenen Dateien + Datum +
Uhrzeit
```

Beispiel:

```
lt_syncmon_data_timeserver_6files_20220311_070714.tgz
```

In dem TGZ-File sind dann alle Datendateien von den selektierten Nodes über den ausgewählten Zeitraum gespeichert. Jeder Node wird mit einem Verzeichnis mit dem Alias Namen angelegt. Zusätzlich werden noch die entsprechenden Dateien der Local-Clock und die Konfigurationsdateien für die Nodes gespeichert. Die Anzahl der enthaltenen Dateien in dem Download-Namen sind nur die Datendateien der Nodes und der Local-Clock.

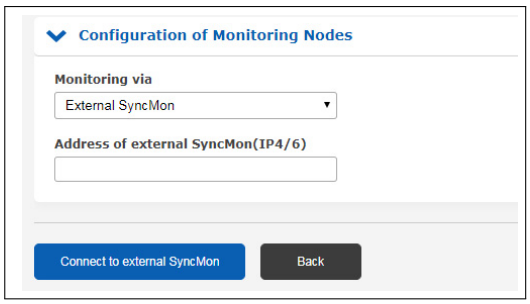
Beispiel für die Verzeichnisstruktur eines ausgepackten TGZ-Files:

```
172.27.100.57/
----> ntp_mon_stats.20220314
----> ntp_mon_stats.20220315
----> ntp_mon_stats.20220316
local_reference/
----> ntp_mon_stats.20220314
----> ntp_mon_stats.20220315
----> ntp_mon_stats.20220316
---------> syncmon_selected_nodes.cfg
---------> syncmon_selected_system_monitoring.cfg
```

Diese TGZ-Datei kann dann auf jedem SyncMon System über den Menü-Punkt „Import SyncMon Data File" wieder eingelesen werden – dies ist auch auf anderen Lantime Systemen möglich. Damit kann man die exportierten Daten direkt mit anderen Daten von SyncMon Systemen vergleichen.

13.1.12.8 External SyncMon

External SyncMon ist eine spezielle Überwachungsinstanz, die Knoten und Sensoren anderer LANTIME-Geräte mit aktiviertem SyncMon überwachen kann. Bei der Auswahl eines externen SyncMon per IP-Adresse wird eine Liste der verfügbaren Knoten von diesem externen SyncMon heruntergeladen. Konfiguration und Daten werden über die HTTP(S)-Schnittstelle mit *curl* übertragen.

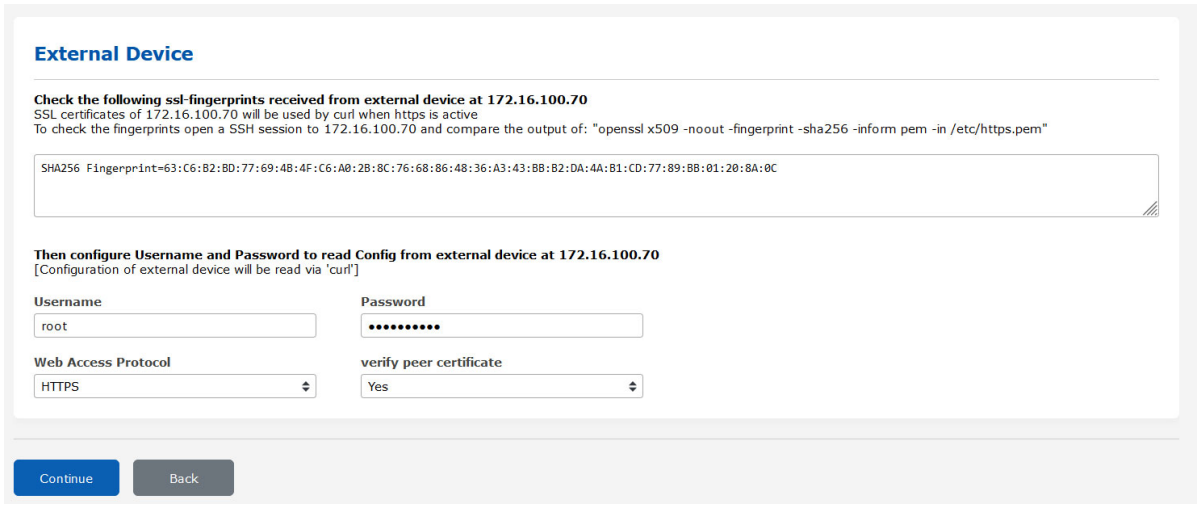


Klicken Sie auf „**Connect to External SyncMon**“, versucht das System, sich mit dem externen SyncMon zu verbinden und zeigt den SSL-Fingerabdruck des lokalen LANTIME an. Die SSL-Zertifikate werden von *curl* verwendet, sofern HTTPS aktiv ist.

Gleichen Sie die vom externen SyncMon empfangenen SSL-Fingerabdrücke mit dem SSL-Fingerabdruck des lokalen LANTIME ab. Um die Fingerabdrücke des externen SyncMon auszugeben, öffnen Sie eine SSH-Sitzung auf dem externen LANTIME und geben Sie folgendes Kommando ein:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem
```

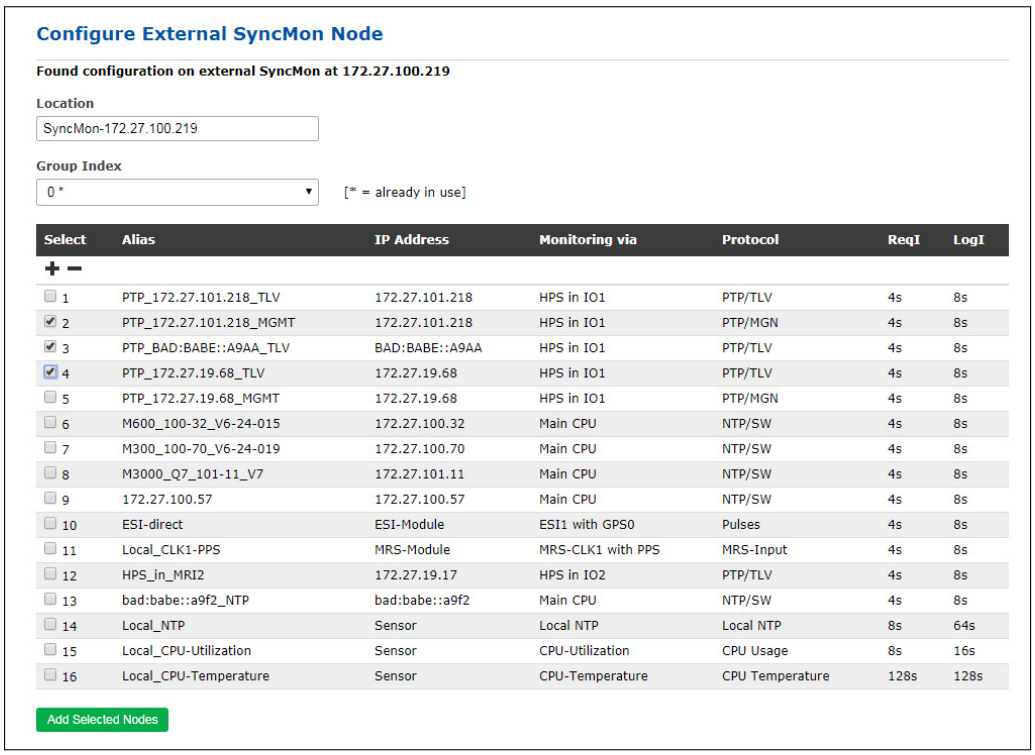
Auf diese Weise wird sichergestellt, dass es sich um das richtige Gerät handelt.



Geben Sie dann den Benutzernamen und das Passwort ein, um die Konfiguration des externen SyncMon zu lesen: Die aktuelle Konfiguration des externen SyncMon wird über *curl* ausgelesen. Außerdem müssen Sie das Web-Zugriffsprotokoll (HTTP oder HTTPS) konfigurieren, wenn Sie ein CA-Zertifikatspaket verwenden möchten, um Konfigurations- und Messdaten vom externen SyncMon zu erhalten.

Beachten Sie, dass bei der Verwendung von HTTPS alle Daten verschlüsselt und entschlüsselt werden müssen, was zu einer erhöhten CPU-Auslastung für jede Datenanforderung an das externe SyncMon führt.

Wenn Sie das HTTP-Zugriffsprotokoll verwenden möchten, dann müssen Sie den HTTP-Netzwerkdienst auf sowohl dem LANTIME der lokalen SyncMon-Instanz als auch dem der externen SyncMon-Instanz aktivieren. Das Gleiche gilt für das HTTPS-Protokoll.



Configure External SyncMon Node

Found configuration on external SyncMon at 172.27.100.219

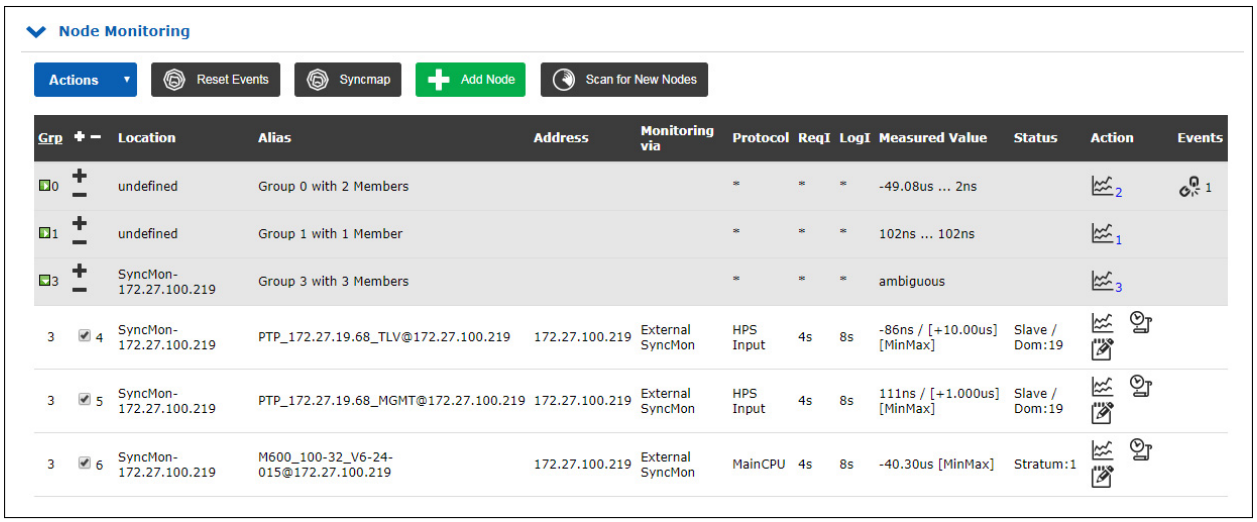
Location: SyncMon-172.27.100.219

Group Index: 0 * [* = already in use]

Select	Alias	IP Address	Monitoring via	Protocol	ReqI	LogI
1	PTP_172.27.101.218_TLV	172.27.101.218	HPS in IO1	PTP/TLV	4s	8s
2	PTP_172.27.101.218_MGMT	172.27.101.218	HPS in IO1	PTP/MGN	4s	8s
3	PTP_BAD:BABE::A9AA_TLV	BAD:BABE::A9AA	HPS in IO1	PTP/TLV	4s	8s
4	PTP_172.27.19.68_TLV	172.27.19.68	HPS in IO1	PTP/TLV	4s	8s
5	PTP_172.27.19.68_MGMT	172.27.19.68	HPS in IO1	PTP/MGN	4s	8s
6	M600_100-32_V6-24-015	172.27.100.32	Main CPU	NTP/SW	4s	8s
7	M300_100-70_V6-24-019	172.27.100.70	Main CPU	NTP/SW	4s	8s
8	M3000_Q7_101-11_V7	172.27.101.11	Main CPU	NTP/SW	4s	8s
9	172.27.100.57	172.27.100.57	Main CPU	NTP/SW	4s	8s
10	ESI-direct	ESI-Module	ESI1 with GPS0	Pulses	4s	8s
11	Local_CLK1-PPS	MRS-Module	MRS-CLK1 with PPS	MRS-Input	4s	8s
12	HPS_in_MRI2	172.27.19.17	HPS in IO2	PTP/TLV	4s	8s
13	bad:babe::a9f2_NTP	bad:babe::a9f2	Main CPU	NTP/SW	4s	8s
14	Local_NTP	Sensor	Local NTP	Local NTP	8s	64s
15	Local_CPU-Utilization	Sensor	CPU-Utilization	CPU Usage	8s	16s
16	Local_CPU-Temperature	Sensor	CPU-Temperature	CPU Temperature	128s	128s

Add Selected Nodes

Um die aktuelle Konfiguration aus dem externen SyncMon zu erhalten, müssen Sie die Knoten auswählen, die Sie von diesem LANTIME überwachen möchten. Es werden nur Knoten angeboten, die nicht deaktiviert und für die externe Protokollierung erlaubt sind. Die Parameter für Anfrage- und Protokollintervall werden von der externen Konfiguration übernommen. Der Standort und der Gruppenindex können für alle ausgewählten Knoten konfiguriert werden. Der Standardort ist „SyncMon-“ plus die IP-Adresse. Die Alias-Namen für die externen SyncMon-Knoten sind der ursprüngliche Alias-Name plus „@IP-Adresse“. Es wird empfohlen, für alle Knoten eines externen SyncMon eine nicht verwendete Gruppen-ID zu verwenden.

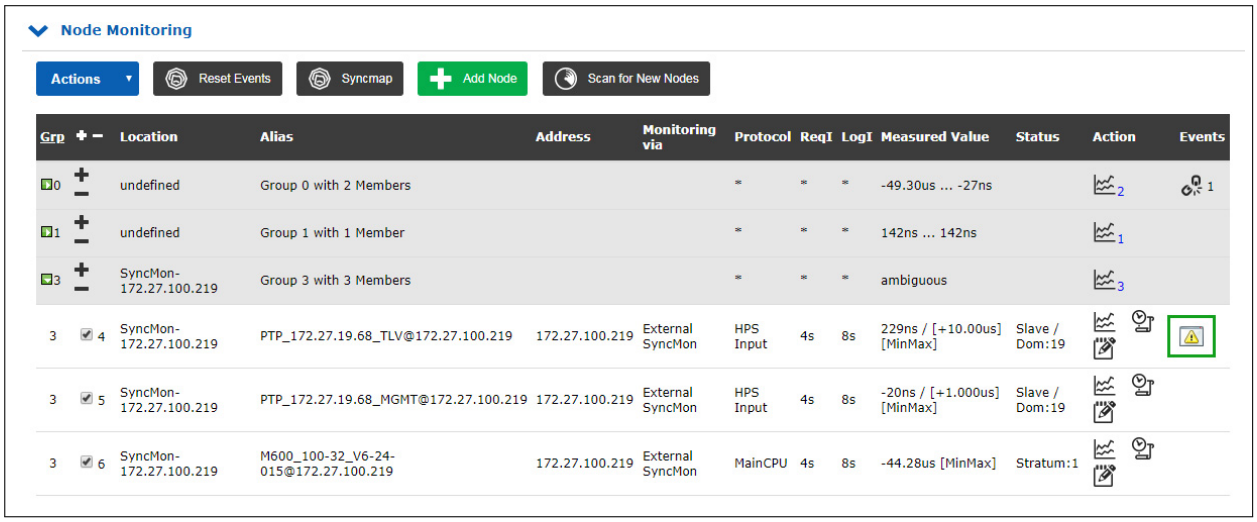


Node Monitoring

Actions | Reset Events | Syncmap | Add Node | Scan for New Nodes

Grp	Location	Alias	Address	Monitoring via	Protocol	ReqI	LogI	Measured Value	Status	Action	Events
0	undefined	Group 0 with 2 Members			*	*	*	-49.08us ... 2ns		2	1
1	undefined	Group 1 with 1 Member			*	*	*	102ns ... 102ns		1	
3	SyncMon-172.27.100.219	Group 3 with 3 Members			*	*	*	ambiguous		3	
3 4	SyncMon-172.27.100.219	PTP_172.27.19.68_TLV@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	-86ns / [+10.00us] [MinMax]	Slave / Dom:19		
3 5	SyncMon-172.27.100.219	PTP_172.27.19.68_MGMT@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	111ns / [+1.000us] [MinMax]	Slave / Dom:19		
3 6	SyncMon-172.27.100.219	M600_100-32_V6-24-015@172.27.100.219	172.27.100.219	External SyncMon	MainCPU	4s	8s	-40.30us [MinMax]	Stratum:1		

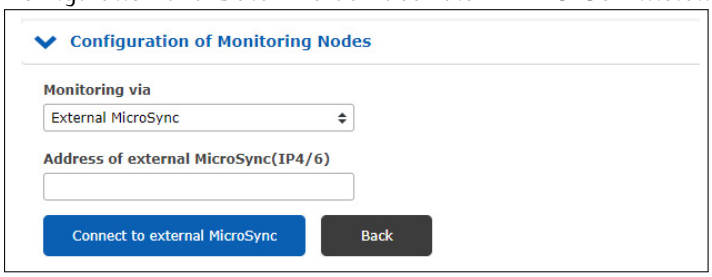
Wenn Änderungen an den Knoten der externen SyncMon-Konfiguration vorgenommen werden, die überwacht werden sollen, wird in der Haupttabelle in der Spalte **Events** für diesen Knoten ein Warnzeichen angezeigt. Dann müssen Sie die Parameter für diesen Knoten manuell ändern.



13.1.12.9 External MicroSync

External MicroSync ist eine spezielle Überwachungsinstanz, die MRS-Referenzen von externen microSync-Geräten überwachen kann. Bei der Auswahl eines externen microSyncs per IP-Adresse wird eine Liste der verfügbaren Referenzen von diesem externen microSync heruntergeladen.

Konfiguration und Daten werden über die HTTPS-Schnittstelle (*curl*) übertragen.



Klicken Sie auf „**Connect to External MicroSync**“, versucht das System, sich mit dem externen microSync zu verbinden und zeigt den SSL-Fingerabdruck des lokalen LANTIMEs an. Die SSL-Zertifikate werden von *curl* verwendet, sofern HTTPS aktiv ist.

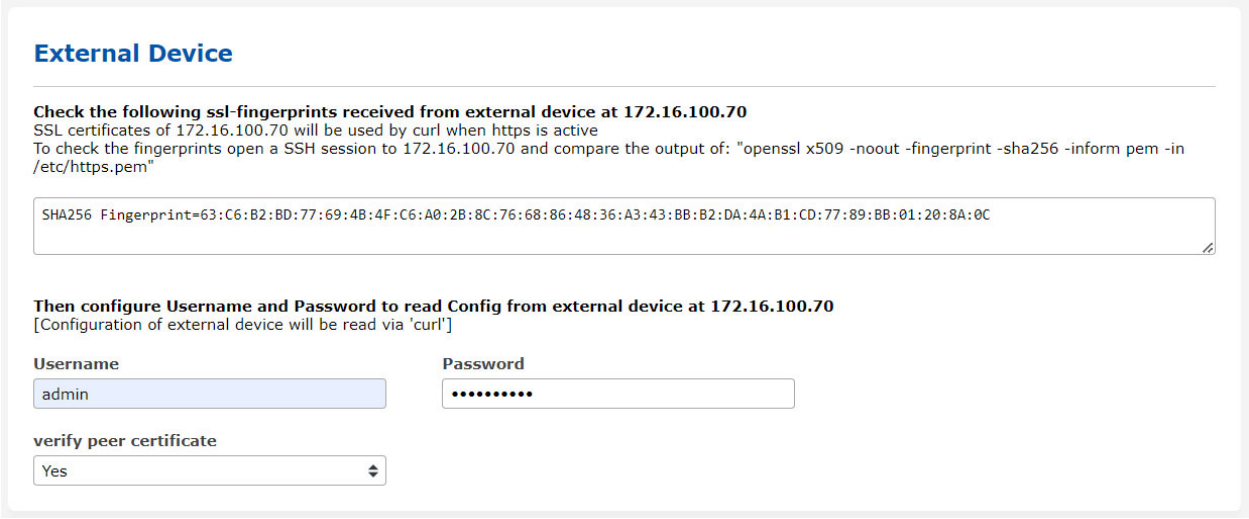
Gleichen Sie die vom microSync empfangenen SSL-Fingerabdrücke mit dem SSL-Fingerabdruck des lokalen LANTIME ab. Um die Fingerabdrücke des microSync zu überprüfen, öffnen Sie eine SSH-Sitzung auf dem externen microSync und geben Sie folgendes Kommando ein:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem
```

Auf diese Weise wird sichergestellt, dass es sich um das richtige Gerät handelt.

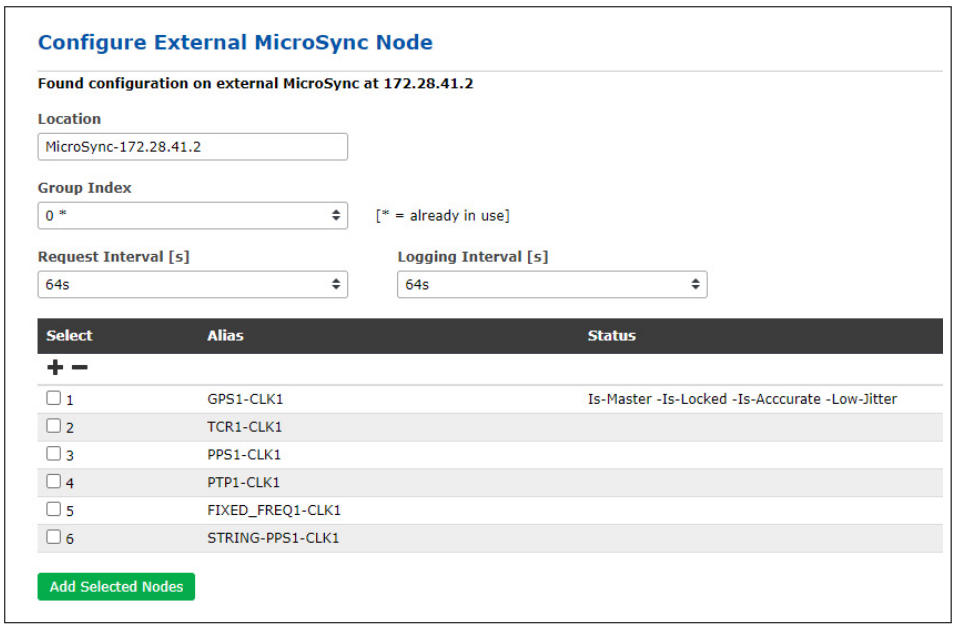
Geben Sie dann den Benutzernamen und das Passwort ein, um die Konfiguration des externen microSync zu lesen: Die aktuelle Konfiguration des externen microSync wird über *curl* ausgelesen.

Beachten Sie, dass bei der Verwendung von HTTPS alle Daten verschlüsselt und entschlüsselt werden müssen, was zu einer erhöhten CPU-Auslastung für jede Datenanforderung an das externe microSync führt.

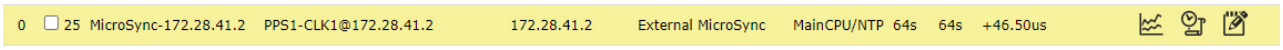


Um die aktuelle Konfiguration aus dem externen microSync zu erhalten, müssen Sie die MRS-Referenzen auswählen, die Sie von diesem LANTIME aus überwachen möchten. Die Parameter für Anfrage- und Protokollintervall werden für alle gleich eingestellt.

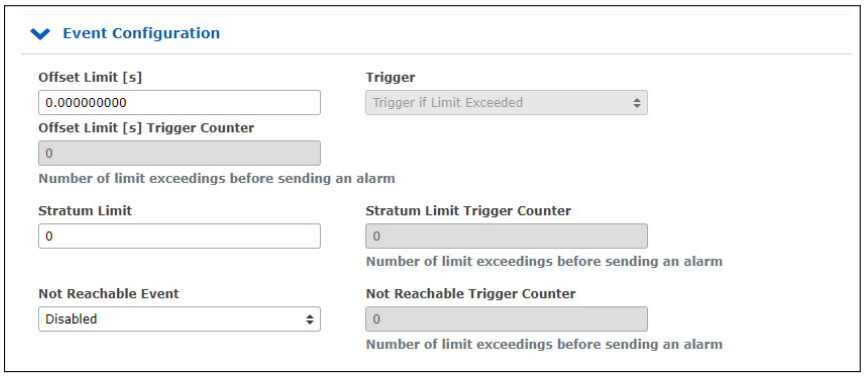
Der Standort und der Gruppenindex können für alle ausgewählten MRS-Referenzen konfiguriert werden. Der Standardort ist *MicroSync-** plus die IP-Adresse. Die Alias-Namen für die externen microSync-MRS-Referenzen sind der ursprüngliche Alias-Name plus *@IP-Adresse*. Es wird empfohlen, für alle MRS-Referenzen eines externen microSync eine nicht verwendete Gruppen-ID zu verwenden.



Wenn Änderungen an den Knoten der externen microSync-Konfiguration vorgenommen werden, die überwacht werden sollen, wird in der Haupttabelle in der Spalte Events für diesen Knoten ein Warnzeichen angezeigt. Dann müssen Sie die Parameter für diesen Knoten manuell ändern.



13.1.12.10 Ereignis-Konfiguration:

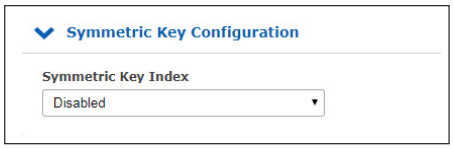


Offset Limit (s):
Offsetgrenze in Sekunden. Der gemessene Offset zwischen einem Knoten und der Referenz wird mit dem konfigurierten Schwellenwert verglichen. Wenn die berechnete Differenz größer als die konfigurierte Offsetgrenze ist, erzeugt der LANTIME einen SyncMon-Alarm (der als Benachrichtigungs-E-Mail, als SNMP-Trap oder als Nachricht an einen externen syslog-Server gesendet werden kann). Mit dem Dropdown-Menü „Trigger" kann die Richtung „Trigger if Limit Exceeded" (bei Überschreitung auslösen) oder „Trigger if Below Limit" (bei Unterschreitung auslösen) gewählt werden. Mit der Option „Offset Limit[s] Trigger Counter" (Offsetgrenze-Auslösezähler) wird das Event einmalig ausgelöst, nachdem die Anzahl der Limitüberschreitungen in einer Reihe überschritten wurde.

Stratum Limit:
Schwellenwert für ein NTP-Stratum. Wenn das Stratum eines überwachten Clients höher als das konfigurierte Stratum-Limit ist, wird ein Alarm ausgelöst (als Benachrichtigungs-E-Mail, als SNMP-Trap oder als Nachricht an einen externen syslog-Server). Mit der Option „Stratum Limit Trigger Counter" wird das Event einmalig ausgelöst, nachdem die Anzahl der Limitüberschreitungen in einer Reihe überschritten wurde.

Not Reachable Event:
Wenn ein konfigurierter Knoten für die Überwachung nicht erreichbar ist, erzeugt der LANTIME einen SyncMon-Alarm (als Benachrichtigungs-E-Mail, als SNMP-Trap oder als Nachricht an einen externen syslog-Server). Mit dieser Option kann das aktiviert oder deaktiviert werden. Mit der Option „Not Reachable Limit Trigger Counter" wird das Event einmalig ausgelöst, nachdem die Anzahl der nicht erreichbaren Knoten in einer Reihe überschritten wurde.

13.1.12.11 Symmetrische Schlüsselkonfiguration

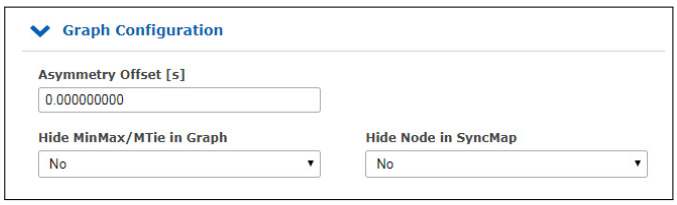


Symmetric Key Index:
Wenn Sie die symmetrische Schlüsselauthentifizierung für SyncMon verwenden möchten, wählen Sie einen Schlüsselindex aus der Liste der bereits verwendeten Schlüssel. Wenn die Schlüssel noch nicht definiert sind, fahren Sie mit dem NTP-Schlüssel-Dialog unter „**NTP → Symmetrische Schlüssel**“ fort und erzeugen Sie eine neue Schlüsseldatei, die auf dem überwachten Knoten gespeichert und aktiviert werden muss.

Für weitere Informationen zur Symmetrischen Schlüsselerzeugung, rufen Sie bitte den LTOS7-Konfigurationsbereich „**NTP → NTP Symmetrische Schlüssel**“ auf.

13.1.12.12 Grafische Parameter bearbeiten

Graph Offset Correction (Grafik-Offset-Korrektur):
Wenn eine konstante Asymmetrie der gemessenen Knoten bekannt ist, können die grafische Ausgabe entsprechend anpassen. Die protokollierten Werte werden hierbei nicht geändert: Der Grafik-Offset stellt lediglich ein fester Offset nur für die grafische Darstellung dar.



Hide MinMax/MTie in Graph (Ausblenden von MinMax in der Grafik):
Wenn das Anfrage-Intervall kleiner als das Protokoll-Intervall ist, werden zusätzliche Werte für Min und Max in den Protokolldateien gespeichert. Diese Min/Max-Werte werden als gefüllte Kurve in einer grauen Farbe hinter der aufgezeichneten Offset-Kurve angezeigt. Diese Funktion kann deaktiviert werden.

Hide This Node in SyncMap (Diesen Knoten im SyncMap ausblenden):
Der Knoten wird in der SyncMap nicht angezeigt.

Wenn Sie mit der Konfiguration eines neuen überwachten Knotens fertig sind, speichern Sie die aktuelle Konfiguration, indem Sie auf die Schaltfläche „**Save Member**“ klicken. Durch Anklicken der Schaltfläche „**Remove Member**“ entfernen Sie den aktuell ausgewählten Knoten aus der vollständigen Liste aller überwachten Knoten. Alle erfassten Daten für den jeweiligen Knoten gehen verloren, wenn Sie die gespeicherten Daten nicht vor dem Entfernen gesichert haben.

Durch Anklicken der Schaltfläche „**Remove Existing Data**“ werden alle Daten für nur diesen speziellen Knoten gelöscht.

13.1.12.13 Nach neuen Knoten suchen

Scan for New Nodes ist eine automatische Suche nach NTP- und PTP-Knoten in Ihrem Netzwerk. Die Suche nach PTP-Knoten wird von der HPS-Karte nur unterstützt, wenn die Lizenz und Überwachung für mindestens 1024 Clients aktiviert ist.

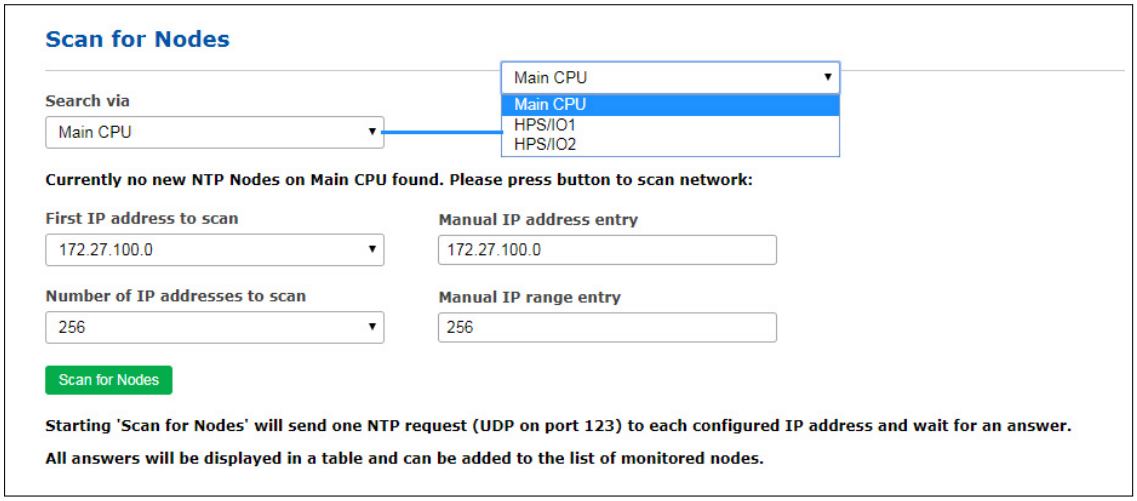


Abbildung: Dialogfeld „Scan for New Nodes". In dieser temporären Tabelle werden nur neu gefundene Knoten angezeigt, die nicht schon überwacht werden. Markieren Sie die Knoten, die Sie in der Tabelle aller überwachten Knoten hinzufügen möchten.

Search via (Suchen mit):
Wählen Sie zunächst eine Instanz aus der Dropdown-Liste aus, die Sie für die Suche nach neuen Knoten verwenden können. Mögliche Optionen sind „*Main CPU*" und, sofern mindestens eine HPS-Karte in Ihrem System installiert ist, einen „*HPS*"-Eintrag pro Karte. Mit der Option „*Main CPU*" können Sie nur nach NTP-Knoten suchen. Die Suche nach PTP-Knoten wird von der HPS-Karte nur unterstützt, wenn die Lizenz und Überwachung für mind. 1024 Clients aktiviert ist.

Suche über „Main CPU"

First IP Address to Scan (erste zu scannende IP-Adresse):
Legen Sie die Anfangs-IP-Adresse fest, unter der die Suche mit dem automatischen NTP-Scan beginnen soll. In der Dropdown-Liste finden Sie alle Teilnetzbereiche der einzelnen Netzwerkschnittstellen. Mit „**IP Scan Address - Manual Override**" (Manuelle IP-Adresseingabe) kann ein anderer Startpunkt definiert werden, der im Dropdown-Menü nicht angeboten wird,

Number of IP Addresses to Scan (Anzahl der zu scannenden IP-Adressen):
Dieser Parameter legt eine Anzahl von IP-Adressen fest, die gescannt werden. An jede IP-Adresse aus dem IP-Bereich wird ein separates NTP-Anforderungspaket gesendet. Wenn ein NTP-Client auf diese Anfrage antwortet und seine IP-Adresse noch nicht konfiguriert ist, erscheint dieser Knoten in der Tabelle. Mit „**IP Scan Range - Manual Override**" (Manuelle IP-Bereichseingabe) kann eine andere Größe des Bereichs definiert werden.

Scan for Nodes (Scannen nach Knoten):
Beim Start von **„Scan for Nodes"** über die Main-CPU wird eine NTP-Anfrage (UDP auf Port 123) an jede konfigurierte IP-Adresse (IP-Adressbereich) gesendet und auf eine Antwort gewartet.

Alle Antworten werden in einer Tabelle angezeigt und können der Liste der überwachten Knoten hinzugefügt werden, indem sie unter „**Select**" ausgewählt werden und mit „**Add Selected Nodes**" (ausgewählte Knoten hinzufügen) übernommen werden. Die Parameter für Standort, Gruppenindex, Anfrageintervall, Aufzeichnungsintervall, Offsetgrenze und Stratum-Limit können im nächsten Schritt definiert werden, bevor sie in die Tabelle mit den anderen überwachten Knoten aufgenommen werden.

Suche über eine HPS-Karte

Wird eine HPS-Karte im Überwachungsmodus ausgewählt (unterstützt von der HPS-Karte nur bei aktivierter 1024- oder 2048-Clients-Lizenz und Überwachung), muss die „PTP Domain“ eingerichtet werden, um PTPv2-Knoten zu erfassen.

PTPv1-Knoten müssen einer der PTPv1-Subdomains *_DFLT, _ALT1, _ALT2,* oder *_ALT3* angehören, damit sie vom SyncMon erfasst werden können.

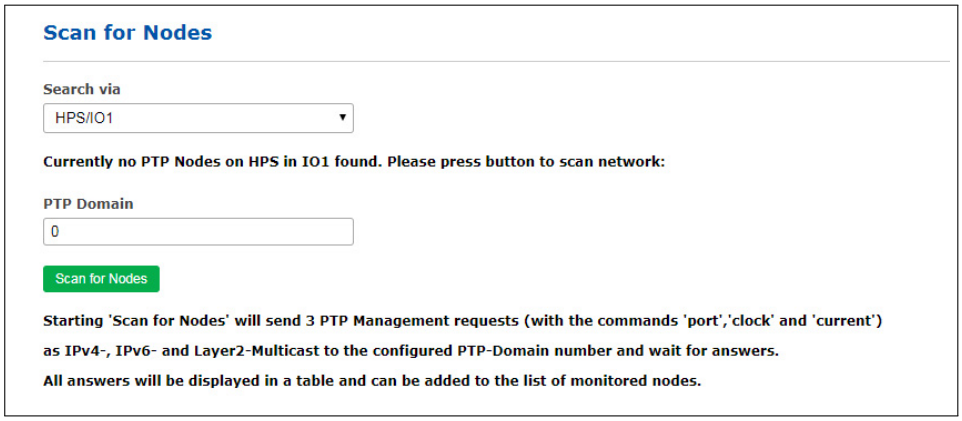


*Abbildung: Um das Netzwerk nach PTP-Knoten zu durchsuchen, muss zunächst in der Dropdown-Liste „***Search via***“ eine HPS-Karte mit aktiviertem Monitoring ausgewählt werden.*

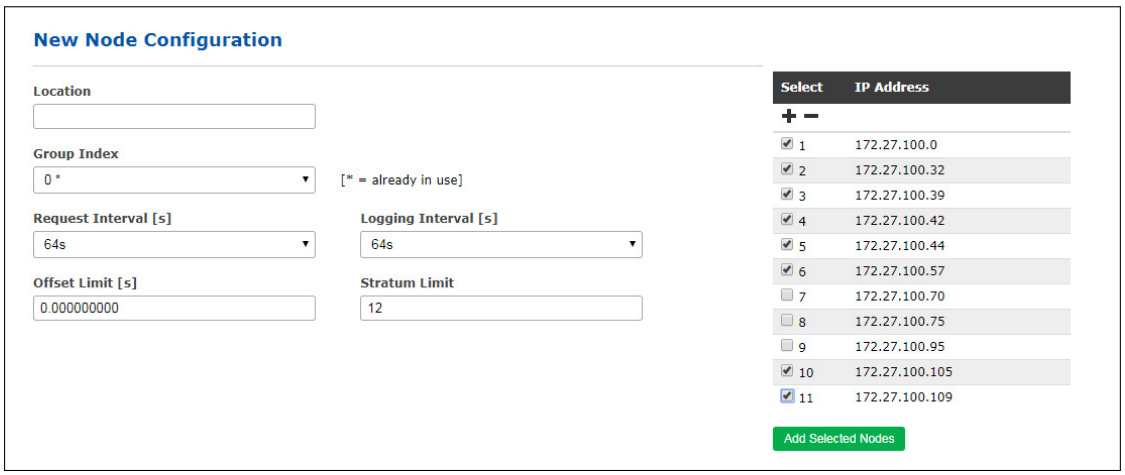
PTP Domain:
Das mit dieser HPS-Karte verbundene Netzwerk wird nach Geräten in der Domain bzw. Subdomain gescannt, die hier vom Benutzer definiert wurde. Die folgenden Geräteadressierungen gemäß IEEE 1588-2008 werden gescannt:

- UDP/IPv4/Ethernet,
- UDP/IPv6/Ethernet,
- Ethernet (IEEE 802.3, Layer 2).

Beim ersten Start des Scans wird eine PTP-Management-Nachricht im Broadcast-Modus gesendet, um den „Port-Status“ jedes PTP-Knotens zu erhalten: Dies geschieht bei IPv4, IPv6 und Layer 2.

Alle PTP-Knoten, die auf diese Anfrage antworten, fragen nach dem „aktuellen Status“ und dem „Uhrenstatus“ mit Managementmeldungen, die nachfolgend beschrieben werden. Das Ergebnis wird als Liste aller verfügbaren PTP-Knoten angezeigt. Jeder neue PTP-Knoten wird in eine Übersichtstabelle der verfügbaren Knoten eingetragen.

In der Tabelle werden nur neue Knoten angezeigt, die noch nicht konfiguriert wurden. Für jeden Knoten werden die PTP-UUID, PTP-Version, IP-Adresse, Herstellername, Knotentyp, PTPv2-Domänennummer bzw. PTPv1-Subdomain, Status (der aktuelle PTP-Status wie Slave, Master, Listening.....), Offset und Delay (aktuelle Messwerte aus der PTP-Verwaltung) automatisch in der Tabelle angezeigt. Mit den Auswahlfeldern können die ausgewählten neuen Knoten automatisch in die Liste der überwachten Knoten aufgenommen werden. Die Parameter für *Standort*, *Gruppenindex*, *Anfrageintervall*, *Aufzeichnungsintervall*, *Offsetgrenze* und *Stratum-Limit* können im nächsten Schritt definiert werden.



Die Überwachungs-Engine beginnt damit, PTP-/NTP-Requests in den konfigurierten Intervallen an jeden Knoten aus der Liste zu senden und misst die in den Antworten empfangene Zeit mit ihrer eigenen Zeit (die z.B. auf UTC, GNSS-Synchronisation zurückzuführen ist). Die aktuellen Offset- und Statusinformationen können in der Statusübersichtstabelle im Bereich „Node Monitoring“ eingesehen werden.

13.1.12.14 Knotenüberwachung

In der Statusübersichtstabelle der überwachten Knoten im Bereich „**Node Monitoring**“ (Knotenüberwachung) finden Sie neben den Statusinformationen 3 Schaltflächen unter der Überschrift „Action“: **Graph** (grafische Darstellung), **Error Logs** (Fehlerprotokolle) und **Edit** (Bearbeitung).

Durch Auswahl der **Grafik**-Schaltfläche wird ein grafisches Diagramm für den ausgewählten Knoten angezeigt. Auf dieser Seite finden Sie verschiedene Funktionen für verschiedene Darstellungsoptionen.

Schaltfläche „Graph“ (Grafische Darstellung)

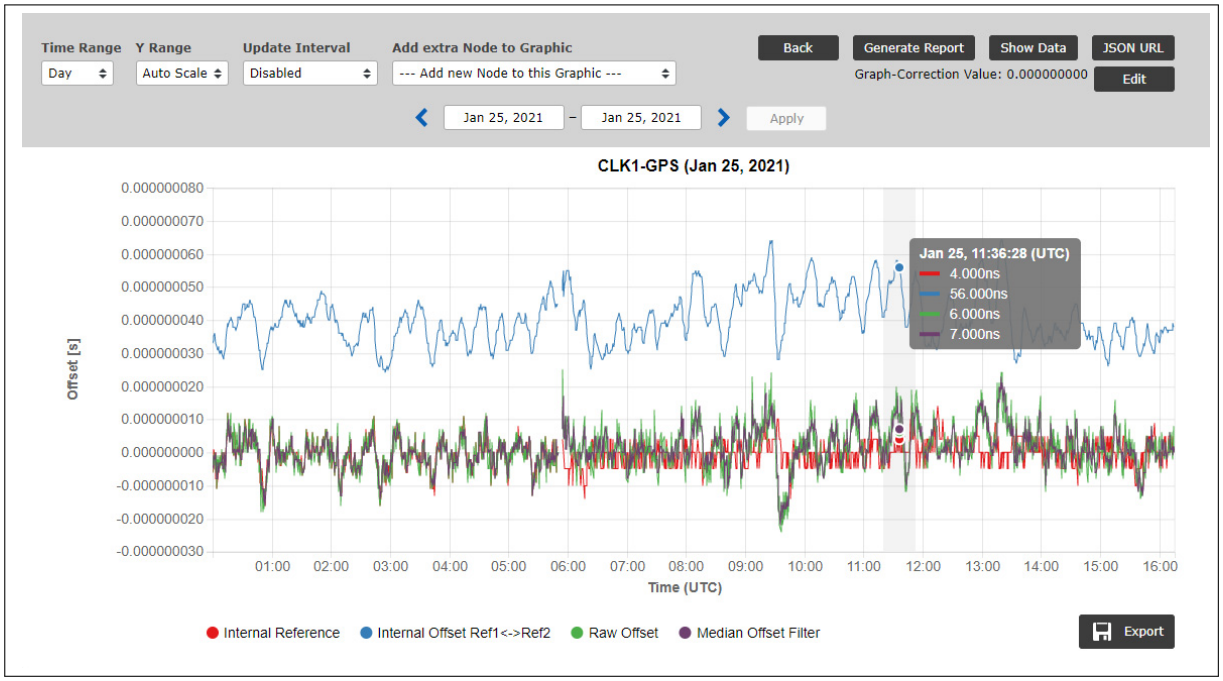
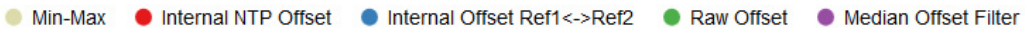


Abbildung: Grafische Darstellung der Offsetwerte für jeden Knoten, wählbar für verschiedene Zeitbereiche (Tag, Woche, Monat oder individuelle Auswahl). Mit den vorgegebenen Schaltflächen bei den Zeitbereich-Feldern können Sie für die grafische Darstellung entweder vergangene oder zukünftige Intervalle auswählen.

Offset-Daten werden für jeden NTP-/PTP- oder anderen überwachten Knoten gesammelt und können grafisch für wählbare Zeitintervalle in der Webinterface des SyncMon-Knotens dargestellt werden.

Die überwachten Daten werden kontinuierlich in der Sync-Knoten-Datei gespeichert und automatisch auf dem gewählten Speichermedium (unter „**Data Storage Base Path**“) bei Tageswechsel um 0:00 UTC gespeichert. Für die weitere statistische Verarbeitung stehen die Daten jederzeit zur Verfügung.

Am unteren Rand des Diagramms zeigt eine Legende, welche Farbe welche Daten darstellt. In diesem Fall stellt die rote Linie den internen NTP-Offset dar, der die Referenz für den überwachten NTP-Knoten ist. Die grüne Linie ist der Versatz zwischen einer Referenzzeit des Sync-Knotens und der gemessenen Zeit eines überwachten Systems.



Wenn Sie den Cursor auf ein Element in der Legende positionieren, wird nur dieses Element in der Grafik angezeigt und alle anderen Elemente werden ausgeblendet. Wenn Sie auf ein Element in der Legende klicken, wird dieses Element dauerhaft ausgeblendet, bis es mit einem weiteren Klick wieder eingeblendet wird.

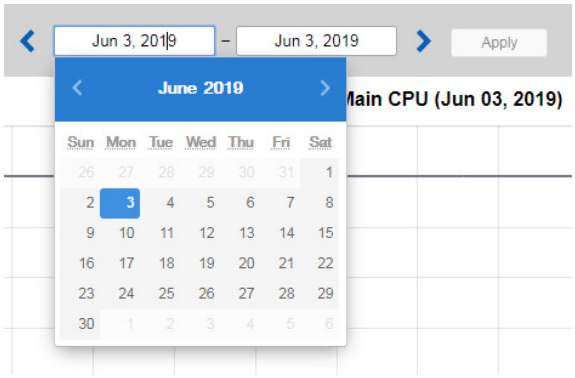
Bei PTP- und PPS-Signalen ist die Sync-Node-Referenz eine interne Referenzzeit vom Empfänger, z.B. GNSS (GPS, GLONASS, Galileo, BeiDou), externer UTC-Zeitdienst, IRIG-Zeitcode, Langwellenzeitreferenz (DCF77, MSF...). Die Referenz des Sync-Knotens wird als rote Linie dargestellt und wenn eine zweite Referenz vorhanden ist, dann stellt die blaue Linie den Versatz zwischen den beiden Referenzuhren dar.

Bei einer GNSS-Referenzuhr im Normalbetrieb zeigt die y-Achse der Referenzuhr-Linie generell Offset-Werte im unteren Nanosekundenbereich (typischerweise maximal 5 ns) mit einer Auflösung von 1 ns.

Für NTP-überwachte Signale wird der Sync-Knoten mit dem internen NTP synchronisiert, der durch eine interne Referenzuhr synchronisiert wird (die wiederum über GNSS, IRIG-Timecode, Langwelle usw. synchronisiert wird). In diesem Fall stellt die rote Linie im Diagramm die interne NTP-Systemzeit dar.

Time Range (Zeitskala):
Es gibt verschiedene Zeitskalen zur Auswahl: 1 Tag, 1 Woche, 1 Monat und ein benutzerdefinierter Bereich. Bei der Auswahl einer benutzerdefinierten Zeitskala klicken Sie auf **„Apply“**, um die Grafik mit der ausgewählten Zeitskala anzuzeigen.

Für jede Zeitskala können Sie mit den Pfeil-Schaltflächen den Zeitbereich anpassen, um vergangene Datensätze einzusehen. Die Zeitskala bleibt hierbei immer gleich, d.h. selbst bei einer individuellen Zeitskala von z.B. 2 Wochen wird mit den Pfeilschaltflächen den Zeitbereich entsprechend um 2 Wochen verschoben.



Y Range (Y-Skala):
Verschiedene Optionen sind verfügbar: automatische Skalierung oder feste Y-Bereiche in Dekadenintervallen: 100 ns, 1 μs, 10 μs, 100 μs, 1 ms, 10 ms und 100 ms.

Update Interval (Aktualisierungsintervall):
Die automatische Aktualisierung der aktuellen Grafik kann in einem Bereich von 1 Sekunde bis 1 Stunde aktiviert werden. Ansonsten können automatische Updates mit *Disabled* deaktiviert werden.

Für NTP-Knoten zeigt die Grafik den internen NTP-Offset (rote Linie), den rohen Offset (blaue Linie) sowie den Offset-Filter-Medianwert (grüne Linie).

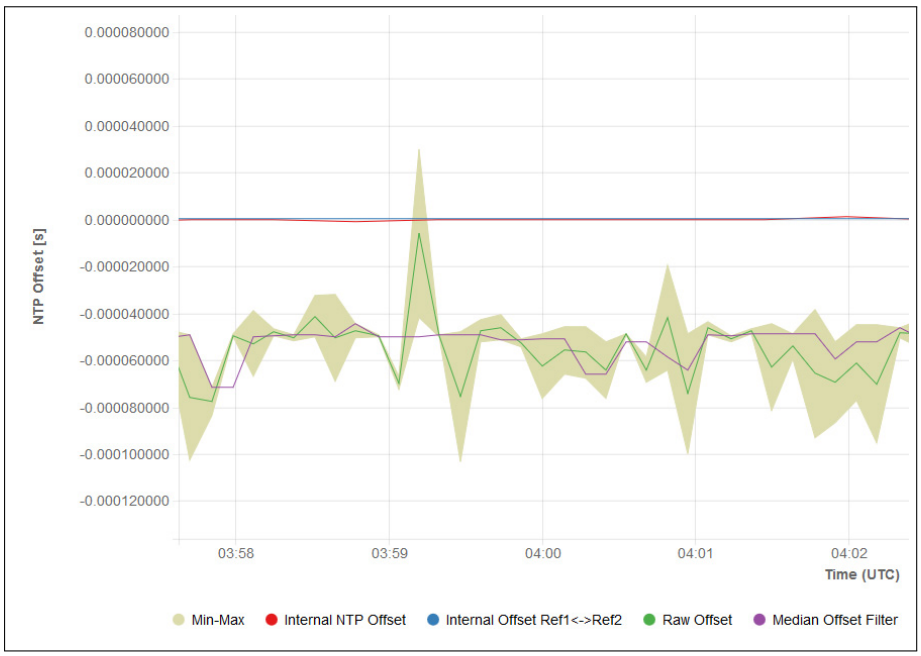
Für PTPv2-Knoten könnten folgende Werte in der Grafik aufgezeichnet werden:
Reported Values (gemeldete Werte): Daten, die von einem PTPv2-Knoten durch Standard-Management-Nachrichten erhalten wurden.

Measured Values (gemessene Werte): Offset eines PTPv2-Knoten gemessen gegen die interne Referenz. Messungen sind nur für PTPv2-Knoten verfügbar, die die Überwachung des PTPv2-Protokolls mit TLVs unterstützen. Der überwachte Knoten kann sich im Slave-, Master- oder Passivmodus befinden. Neben den durch Reverse-PTP erhaltenen Messwerten stehen auch die gemeldete Wertekurve und die MTie-gefüllte Kurve zur Verfügung, wenn die Min- und Max-Wertmessung auf dem überwachten Knoten unterstützt wird.

Für PTPv1-Knoten (nur LTOS 7.06.007 oder später) zeigt die Grafik den internen PTP-Offset (rote Linie) und den gemessenen Offset (blaue Linie).

Für PPS-Knoten, die über eine ESI- oder PIO-Eingangskarte am Sync-Knoten überwacht werden, zeigt die Grafik den internen Referenz-Offset (rote Linie), den rohen Offset (blaue Linie) sowie den Offset-Filter-Medianwert (grüne Linie).

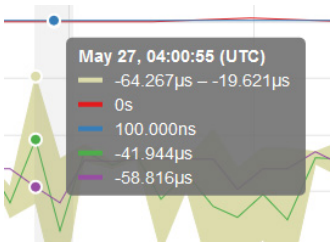
Wenn das Anfrage-Intervall kleiner als das Protokoll-Intervall ist, werden zusätzliche Werte für Min und Max in den Protokolldateien gespeichert. Diese Min/Max-Werte werden automatisch als gefüllte Kurve in einer grauen Farbe hinter der aufgezeichneten Offset-Kurve angezeigt und der Mittelwert wird als rote Linie in der gefüllten Min/Max-Kurve angezeigt.



X/Y-Bereich vergrößern:
Um den Y-Bereich ein- und auszuzoomen, positionieren Sie den Mauszeiger auf der Y-Achse und scrollen Sie mit dem Mausrad, um ein- und auszuzoomen. Durch einmaliges Drücken der Maustaste auf der Y-Achse wird diese auf den ausgewählten Y-Bereich zurückgesetzt. Indem Sie die Maustaste gedrückt halten und die Maus nach oben und unten bewegen wird die Y-Achse auf und ab bewegt.

Um den X-Bereich (Zeitachse) ein- und auszuzoomen, positionieren Sie den Mauszeiger im Diagramm selbst (nicht in der X-Achse) und scrollen Sie mit dem Mausrad, um ein- und auszuzoomen. Wenn Sie die Maustaste im Diagramm gedrückt halten und die Maus nach links und rechts bewegen, wird die Grafik nach links und rechts verschoben.

Wenn Sie mit der Maus über einen beliebigen Punkt des Diagramms fahren, zeigt eine Info-Ansicht alle Werte aller sichtbaren Diagramme an jenem Punkt an.



Schaltfläche „Show Data“ (Daten anzeigen):
Mit der Schaltfläche „**Show Data**“ können Sie von der grafischen Darstellung in eine Tabellenansicht der aktuell angezeigten Werte wechseln. Die erste Zeile zeigt die Beschreibung jeder Spalte. Mit der Schaltfläche „**Show Graph**“ (Grafik anzeigen) können Sie zur grafischen Ansicht zurückkehren. Der Datenbereich der Tabelle umfasst lediglich die in der Grafik sichtbaren Werte: ist die Grafik also eingezoomt, werden nur die in der eingezoomten Ansicht sichtbaren Daten aufgeführt.

#	Day	Sec	Julian_day_time	Meas_offset	Report_offs	Path_delay	Port_state	Min	Max			
58638	00002	2019-06-04T00:00:02+00:00	-0.000000002	0.000000173	0.000009348	9	M	-0.000000876	0.000000578	R	-0.000000036	0.000000031
58638	00010	2019-06-04T00:00:10+00:00	0.000000078	0.000000055	0.000009064	9	M	-0.000000876	0.000000578	R	-0.000000028	0.000000185
58638	00018	2019-06-04T00:00:18+00:00	-0.000000087	-0.000000001	0.000009067	9	M	-0.000000876	0.000000578	R	-0.000000359	0.000000185
58638	00026	2019-06-04T00:00:26+00:00	0.000000234	0.000000152	0.000009123	9	M	-0.000000876	0.000000578	R	-0.000000159	0.000000628
58638	00034	2019-06-04T00:00:34+00:00	0.000000497	0.000000104	0.000009059	9	M	-0.000000876	0.000000578	R	0.000000366	0.000000628
58638	00042	2019-06-04T00:00:42+00:00	0.000000084	-0.000000147	0.000009064	9	M	-0.000000876	0.000000578	R	0.000000045	0.000000124
58638	00050	2019-06-04T00:00:50+00:00	0.000000334	-0.000000237	0.000009015	9	M	-0.000000876	0.000000578	R	0.000000124	0.000000544
58638	00058	2019-06-04T00:00:58+00:00	0.000000136	-0.000000306	0.000009015	9	M	-0.000000276	0.000000352	R	-0.000000077	0.000000349
58638	00066	2019-06-04T00:01:06+00:00	0.000000247	-0.000000230	0.000008820	9	M	-0.000000276	0.000000352	R	0.000000145	0.000000349
58638	00074	2019-06-04T00:01:14+00:00	0.000000117	0.000000124	0.000008703	9	M	-0.000000276	0.000000352	R	0.000000117	0.000000117
58638	00083	2019-06-04T00:01:23+00:00	0.000000073	-0.000000322	0.000008846	9	M	-0.000000276	0.000000352	R	-0.000000216	0.000000362
58638	00232	2019-06-04T00:03:52+00:00	0.000000107	0.000000019	0.000008869	9	M	-0.000000486	0.000000387	R	-0.000000063	0.000000277

Schaltfläche „JSON URL“:
Mit der Schaltfläche „**JSON URL**“ erhalten Sie die HTTP(S)-URL, über die den letzten Messwert des ausgewählten Knotens zu erhalten ist. Damit können die aktuellen Werte über HTTP(S) aus einem externen Programm über ein geeignetes Tool (z.B. *wget*, *curl*) gelesen werden. Die JSON-Datei ist wie folgt formattiert:

```
{
   "SyncMon_Data": {
       "LastLogValues" :  {
       "NodeName"              : "172.27.100.57",
       "OffsetLimit"           :  0.000000000,
       "RawOffset"             : -0.000050076,
       "MedianOffset"          : -0.000048733,
       "PathDelay"             : -0.000002693,
       "Status"                : 1,
       "LastErrorCode"         : 0,
       "LastConfigChange"      : 0,
       "LogTime"               : 1559025024
  }
 }
}
```

Schaltfläche „Export“:
Mit dem Button „**Export**“ wird eine PNG-Datei des aktuellen Graphen erzeugt. Diese Ansicht kann zum Drucken und Speichern verwendet werden.

Schaltfläche „Generate Report“ (Bericht erzeugen):
Mit der Schaltfläche „**Generate Report**“ werden die aktuellen Daten des überwachten Knotens in Form eines Berichts aufbereitet. Sie können auch einen Zeitrahmen für erfasste Daten auswählen, aus dem ein Bericht erzeugt wird. Der Bericht enthält die aktuellen Statusdaten, die Monitorkonfiguration, statistische Trends über den ausgewählten Zeitraum, ein grafisches Diagramm und optional eine vollständige SyncMap für den überwachten Knoten, für die das Kontrollkästchen „**Add SyncMap to Report**“ (SyncMap in Bericht einbinden) aktiviert werden muss.

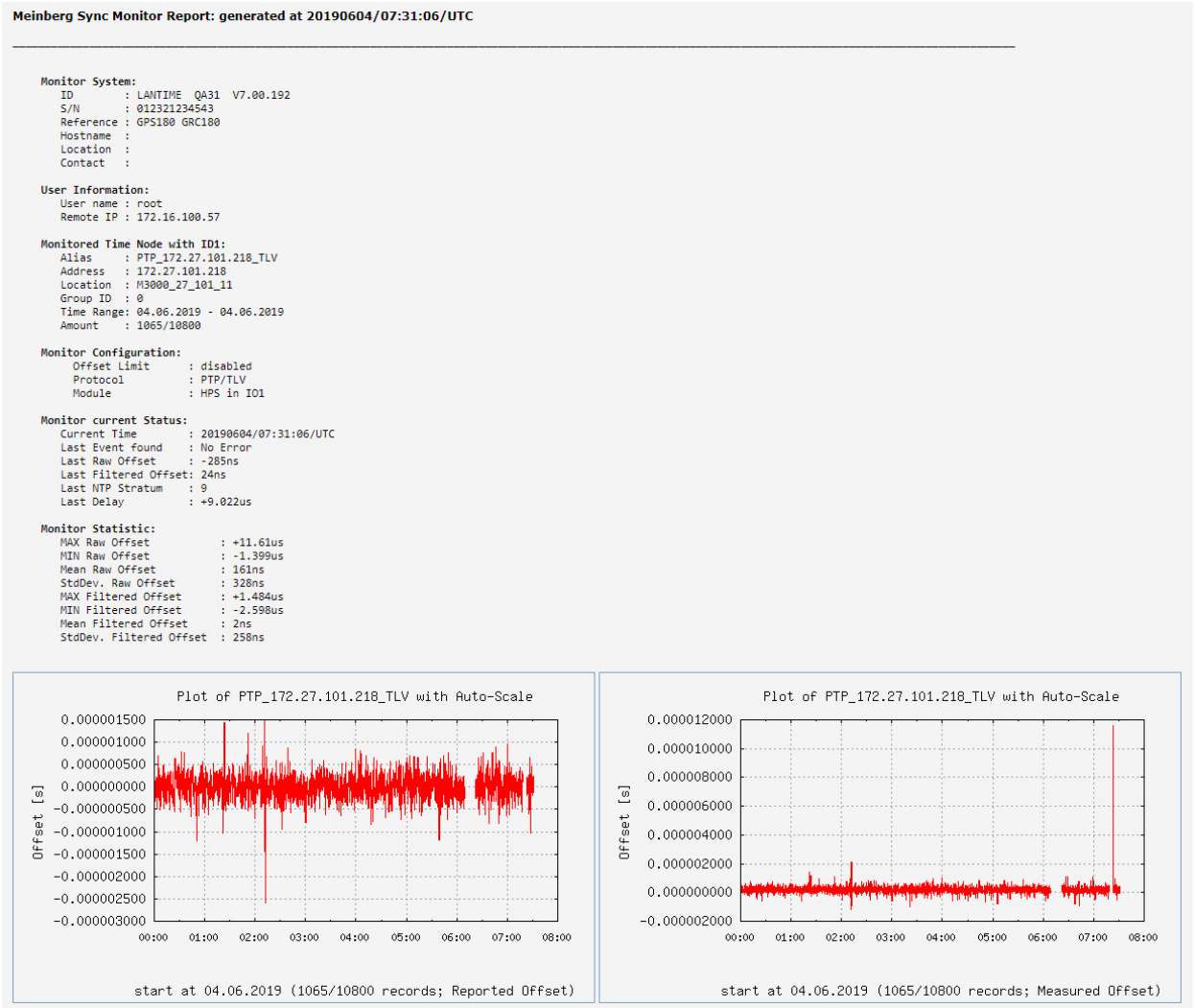


Abbildung: Generierter Bericht für einen ausgewählten Knoten. Der Bericht enthält Statusinformationen über die ausgewählten überwachten Knoten, die Monitorkonfiguration, die Hauptmonitorstatistiken und grafische Diagramme.

Schaltfläche „Back“:
Bei der Auswahl der Grafik-Ansicht führt die Schaltfläche „**Back**“ zurück zur Haupttabellenansicht und zeigt die Tabelle mit allen konfigurierten Knoten an.

Schaltfläche „Error Logs“ (Fehlerprotokolle)

Unter dem Bereich „Node Monitoring“ werden durch Anklicken der Schaltfläche „**Error Logs**“ den Bereich „Error Logs“ aufgeklappt und so gefiltert, dass nur die Protokollmeldungen zum ausgewählten überwachten Knotens angezeigt werden. Hier werden die Protokollmeldungen seit dem letzten Systemneustart angezeigt. Wenn die Flash-Speicherkarte voll ist, werden die älteren Protokolle überschrieben.

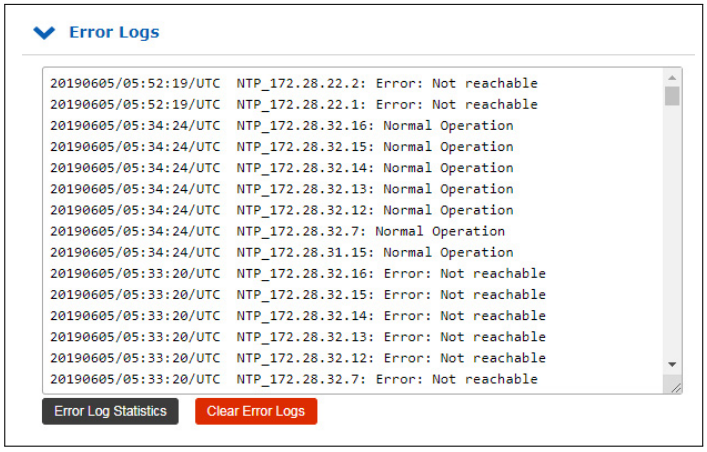
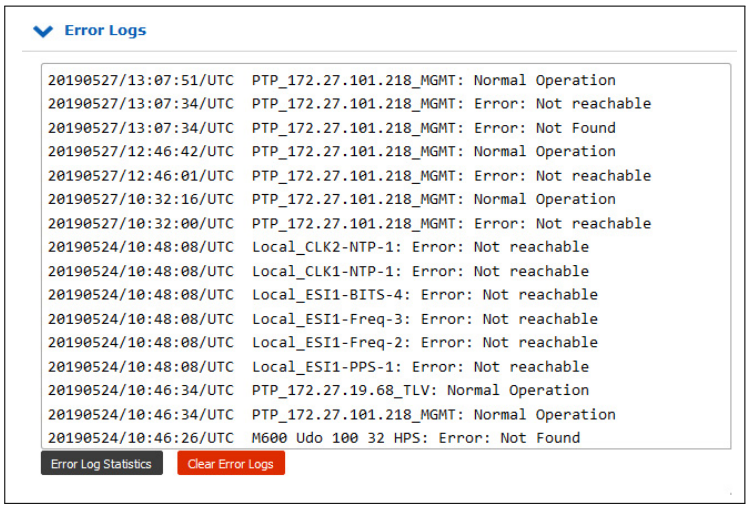
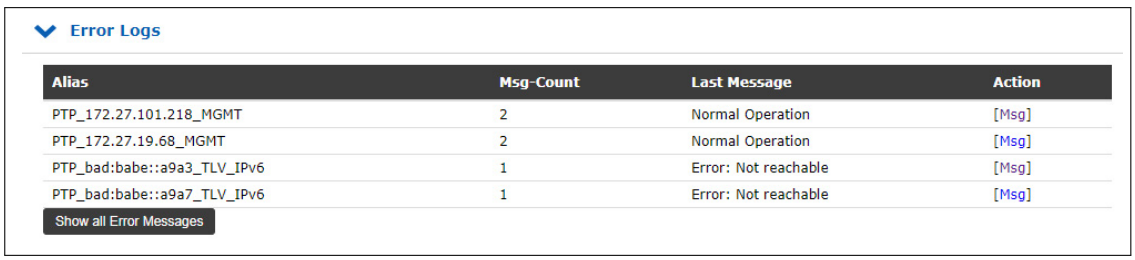


Abbildung: Fehlermeldungen für einen ausgewählten überwachten Knoten.

Am unteren Rand des Bereichs befindet sich die Schaltfläche „**Show All Error Messages**“ (alle Fehlermeldungen anzeigen), mit der Sie alle Fehlermeldungen von allen überwachten Knoten anzeigen können. Diese Schaltfläche erscheint nicht, wenn alle Fehlermeldungen schon in diesem „Error Logs“-Bereich angezeigt sind.



Mit „**Error Log Statistics**“ (Error-Log-Statistik) wird eine statistische Übersicht über die Protokolle aller Knoten angezeigt. Mit „**Clear Error Logs**“ (Error-Logs löschen) werden alle Log-Einträge entfernt.

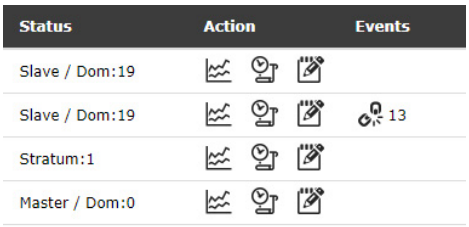


Schaltfläche „Edit“ (Bearbeiten)

Mit der Schaltfläche „**Edit**“ (Bearbeiten) können alle grafischen Parameter angezeigt und konfiguriert werden. Der „**Graph Offset Correction**“ (Korrekturwert eines Grafik-Offsets) in den Knoteneinstellungen kann verwendet werden, um die Grafik mit einem festen Offset anzupassen (um z.B. eine bekannte Asymmetrie in einem Netzwerk oder die Laufzeit einer Kabellänge zu kompensieren). Im Gegensatz zum „**Fixed Offset Correction**“ wird der „**Graph Offset Correction**“ nur auf die aktuelle Grafik angewandt und nicht auf die gespeicherten Daten.

13.1.12.15 Events

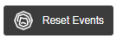
In der Übersichtstabelle der Knotenüberwachung werden unter die letzten Spalte „**Events**“ Alarme angezeigt, die für die entsprechenden überwachten Knoten definiert sind und alle 10 Sekunden automatisch aktualisiert werden:



Offset Limit Exceeded (Offset-Limit überschritten)
Dieser Alarm wird ausgelöst, wenn der in den Knoteneinstellungen festgelegte Offset-Limit (wiederholt) überschritten wird. Die Auslösung des Alarms bei der ersten Überschreitung oder erst bei mehreren Verletzungen hintereinander wird durch die entsprechende „Trigger Counter“-Einstellung in den Knoteneinstellungen festgelegt.

Not Reachable (nicht erreichbar)
Dieser Alarm wird ausgelöst, wenn der Knoten als nicht erreichbar bewertet wird. Die Auslösung des Alarms bei dem ersten Verbindungsfehlschlag oder erst bei mehreren erfolglosen Verbindungsversuchen in einer Reihe wird durch die entsprechende „Trigger Counter“-Einstellung in den Knoteneinstellungen festgelegt.

Diese Ereignisse werden auch in der SyncMap angezeigt.



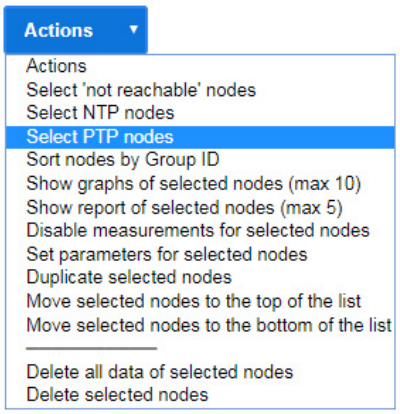
Bei „*Offset Limit überschritten*“ und „*Nicht erreichbar*“ wird in der Tabelle der überwachten Knoten in der Spalte Events neben dem Symbol die Anzahl der Ereignisse angezeigt. Mit der Schaltfläche „**Reset Events**“ (Ereignisse zurücksetzen), die sich oberhalb der Übersichtstabelle befindet, können Sie den aktuellen Zähler für die Events zurücksetzen.

13.1.12.16 Aktionen-Menü

Ab Firmware-Version 7.00 können Sie bestimmte Aktionen gleichzeitig auf eine Reihe von ausgewählten Knoten aus der Tabelle anwenden und Knoten systematisch auswählen, die bestimmte Bedingungen erfüllen.

Auswahl von Knoten

Aktivieren Sie zunächst die Knoten, die Sie verwalten möchten, entweder durch einzelnes Anklicken des Kontrollkästchens auf der linken Seite jedes Knoteneintrags oder durch Anklicken des „+"-Zeichens in der oberen Zeile der Tabelle, wenn Sie alle Knoten zusammen auswählen möchten. Um die Auswahl eines ausgewählten Knotens aufzuheben, klicken Sie entweder erneut in sein Kontrollkästchen, um ihm abzuwählen, oder klicken Sie auf das Symbol „-" in der oberen Zeile, um sie alle Knoten gleichzeitig abzuwählen.



Sie können auch alle Knoten aufgrund einer bestimmten Eigenschaft automatisch auswählen lassen: Klicken Sie auf der Schaltfläche „**Actions**", um ein Menü aufzurufen, und suchen Sie eine der folgenden Optionen aus:

Select 'Not Reachable' Nodes (alle „nicht erreichbaren" Knoten markieren):
Auswahl aller Knoten, deren Offset-Status „not reachable" anzeigt.

Select NTP Nodes (alle NTP-Knoten markieren):
Auswahl aller überwachten NTP-Knoten.

Select PTP Nodes (alle PTP-Knoten markieren):
Auswahl aller überwachten PTP-Knoten, ob über MGMT- oder TLV-Nachrichten.

Mit „**Sort Nodes by Group ID**" (Knoten nach Gruppen-ID sortieren) wird die vollständige Liste der Knoten nach Gruppen-ID sortiert.

Übersichten für alle Knoten

Die Optionen „**Show Overview for Current Day**" (Übersicht für aktueller Tag anzeigen) und „**Show Overview for Time Range**" (Übersicht für Zeitspanne anzeigen) sind nur sichtbar, solange keine Knoten ausgewählt sind. Diese Optionen zeigen eine statistische Übersicht der aufgezeichneten Werte und Eigenschaften von allen Knoten in der Tabelle an, inklusive grafische Darstellungen, für den aktuellen Tag bzw. die ausgewählte Zeitspanne.

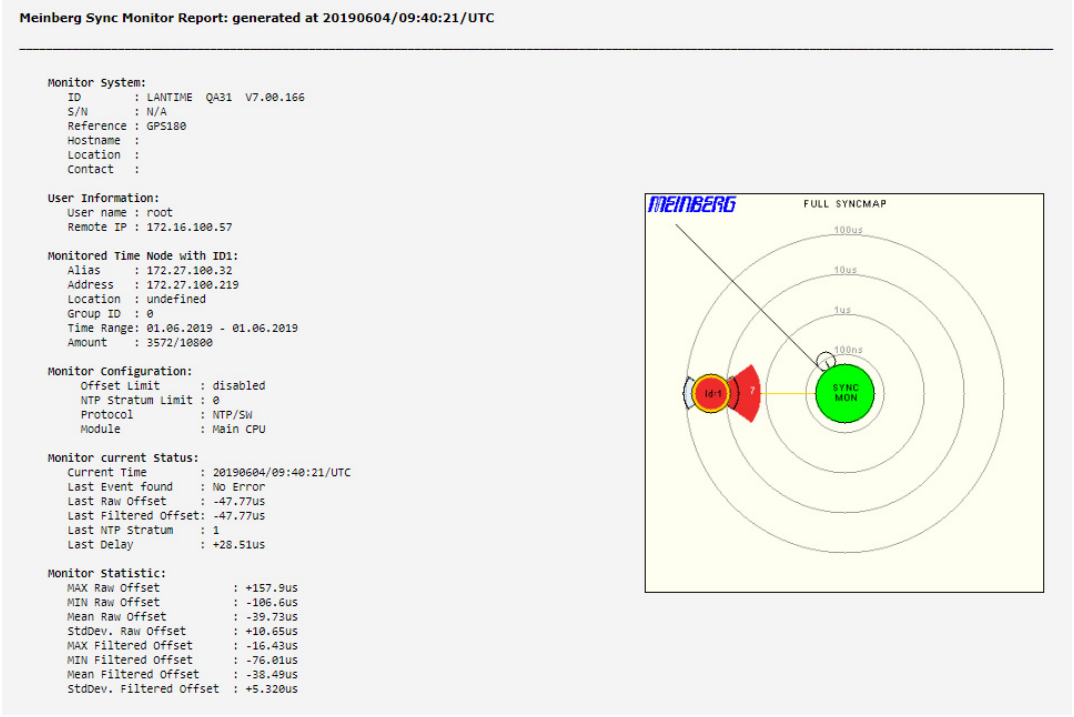
Aktionen für ausgewählte Knoten

Show Graphs of Selected Nodes (Max. 10) (grafische Diagramme für ausgewählte Knoten anzeigen):
Wenn Sie bis zu zehn Knoten in der Tabelle auswählen, können die Diagramme für diese angezeigt werden: Diese werden aufeinander überlagert. Die Standarddarstellung gilt für den aktuellen Tag: Sie können einen anderen Zeitraum auswählen, für den die grafischen Diagramme angezeigt werden.

Show Report of Selected Nodes (Max. 5) (Bericht für ausgewählte Knoten anzeigen):
Wenn Sie bis zu fünf Knoten in der Tabelle auswählen, werden mit dieser Option die aktuellen Daten der

ausgewählten Knoten in Form eines Berichts aufbereitet. Zuerst müssen Sie einen Zeitraum auswählen, für den der Bericht generiert wird. Der Bericht enthält die aktuellen Statusdaten, die Konfiguration des SyncMon, die Überwachung der statistischen Werte über den ausgewählten Zeitraum und ein grafisches Diagramm, das den Offset-Trend anzeigt.

Außerdem bietet der Bericht auch eine vereinfachte Version der SyncMap, die nur die ausgewählten Knoten aus der Tabelle enthält. In der SyncMap wird jeder einzelne Knoten hervorgehoben und der Rest im Hintergrund dargestellt, um einen Vergleich der Leistung des jeweiligen Knotens im Vergleich zu anderen im Bericht berücksichtigten Knoten zu erhalten.



Meinberg Sync Monitor Report: generated at 20190604/09:40:21/UTC

```
Monitor System:
   ID        : LANTIME  QA31  V7.00.166
   S/N       : N/A
   Reference : GPS180
   Hostname  :
   Location  :
   Contact   :

User Information:
   User name : root
   Remote IP : 172.16.100.57

Monitored Time Node with ID1:
   Alias     : 172.27.100.32
   Address   : 172.27.100.219
   Location  : undefined
   Group ID  : 0
   Time Range: 01.06.2019 - 01.06.2019
   Amount    : 3572/10800

Monitor Configuration:
      Offset Limit      : disabled
      NTP Stratum Limit : 0
      Protocol          : NTP/SW
      Module            : Main CPU

Monitor current Status:
   Current Time        : 20190604/09:40:21/UTC
   Last Event found    : No Error
   Last Raw Offset     : -47.77us
   Last Filtered Offset: -47.77us
   Last NTP Stratum    : 1
   Last Delay          : +28.51us

Monitor Statistic:
   MAX Raw Offset           : +157.9us
   MIN Raw Offset           : -106.6us
   Mean Raw Offset          : -39.73us
   StdDev. Raw Offset       : +10.65us
   MAX Filtered Offset      : -16.43us
   MIN Filtered Offset      : -76.01us
   Mean Filtered Offset     : -38.49us
   StdDev. Filtered Offset  : +5.320us
```


Abbildung: Generierter Bericht für ausgewählte Knoten in der Tabelle. Der Bericht enthält Statusinformationen über die ausgewählten überwachten Knoten, die SyncMon-Konfiguration, die Hauptmonitorstatistiken und grafische Diagramme.

Disable Measurements for Selected Nodes (Messungen für ausgewählte Knoten deaktivieren):
Die Knoten, für die Sie Messungen deaktivieren, erhalten den Status „Deaktiviert“. Die Messungen werden für diesen Knoten nicht mehr angefordert und protokolliert. Die Deaktivierung wird durch eine Setzung des Anfrageintervalls auf „*Disabled*“ umgesetzt: Um die Messungen daher erneut zu starten, rufen Sie die Konfigurationsseite des Knoten auf und setzen Sie das „Request Interval“ wieder auf den gewünschten Wert.

Set Parameters for Selected Nodes (Parameter für ausgewählte Knoten setzen):
Einzelne Überwachungsparameter können für die ausgewählten Knoten gleichzeitig bearbeitet werden. Wenn Sie diese Funktion auswählen, erscheint einen Konfigurationsdialog, in dem Sie jeden der Parameter neu konfigurieren können. Sobald Sie mit der Schaltfläche „**Save Selected Nodes**“ (Einstellungen für ausgewählten Knoten speichern) die Änderungen bestätigen, wird die neue Konfiguration wird auf alle Knoten angewendet, die Sie für diese Aktion ausgewählt haben. Es werden nur die Einstellungen angepasst, für die Sie eine Option ausgewählt haben: Wenn Sie ein Feld leer lassen, wird die entsprechende Einstellung der Knoten nicht angepasst.

Duplicate Selected Nodes (ausgewählte Knoten duplizieren):
Die von Ihnen ausgewählten Knoten werden kopiert und unter ihren Ursprungsknoten eingefügt. Anschließend können Sie deren Parameter bearbeiten.

Move Selected Nodes to the Top of the List (ausgewählte Knoten an den Anfang der Liste verschieben):
Die ausgewählten Knoten werden an den Anfang der Liste verschoben.

Move Selected Nodes to the Bottom of the List (ausgewählte Knoten an das Ende der Liste verschieben):
Die ausgewählten Knoten werden an das Ende der Liste verschoben.

Delete All Data of Selected Nodes (alle Daten der ausgewählten Knoten löschen):
Die protokollierten Messdaten der ausgewählten Knoten werden dauerhaft aus dem eingestellten Speichermedium gelöscht.

Delete Selected Nodes (markierte Knoten löschen):
Die ausgewählten Knoten werden aus der Knotenüberwachungstabelle gelöscht. Die bis zu diesem Zeitpunkt für die Knoten protokollierten Messungen bleiben erhalten; sollten diese Daten auch mitgelöscht werden, sollten Sie *zuerst* „**Delete All Data of Selected Nodes**“ auswählen. Die Knoten können bei Bedarf über eine Suche oder manuelle Eingabe wieder hinzugefügt werden.

13.1.12.17 SyncMap

Die SyncMap ist eine grafische Darstellung von überwachten Knoten in einem Netzwerk, die als Polardiagramm dargestellt wird. Die Idee der SyncMap ist es, einen schnellen Überblick über den Synchronisationsstatus aller überwachten Geräte in einer komplexen Netzwerkstruktur zu geben.

Die überwachten Geräte werden als Knoten bezeichnet. Knoten müssen eines der folgenden Signale unterstützen: NTP (RFC1305), PTP (IEEE 1588v1 and IEEE 1588v2) oder, in Verbindung mit einer IMS-ESI-Karte, PPS. Achtung: PTPv1-Knoten werden erst ab LTOS V7.06.007 in der SyncMap gezeigt.

Sie ermöglicht eine Visualisierung der absoluten Offset-Werte der überwachten Knoten innerhalb vordefinierten Offset-Grenzen. Die Daten können nach dem aktuellen Knoten-Status über einen wählbaren Zeitbereich (z.B. einen Tag) angezeigt werden. Es ist auch möglich, eine Animation über das dynamische Verhalten der überwachten Knoten über die letzten 60 Minuten zu generieren, wobei SyncMaps automatisch jede Minute generiert werden.

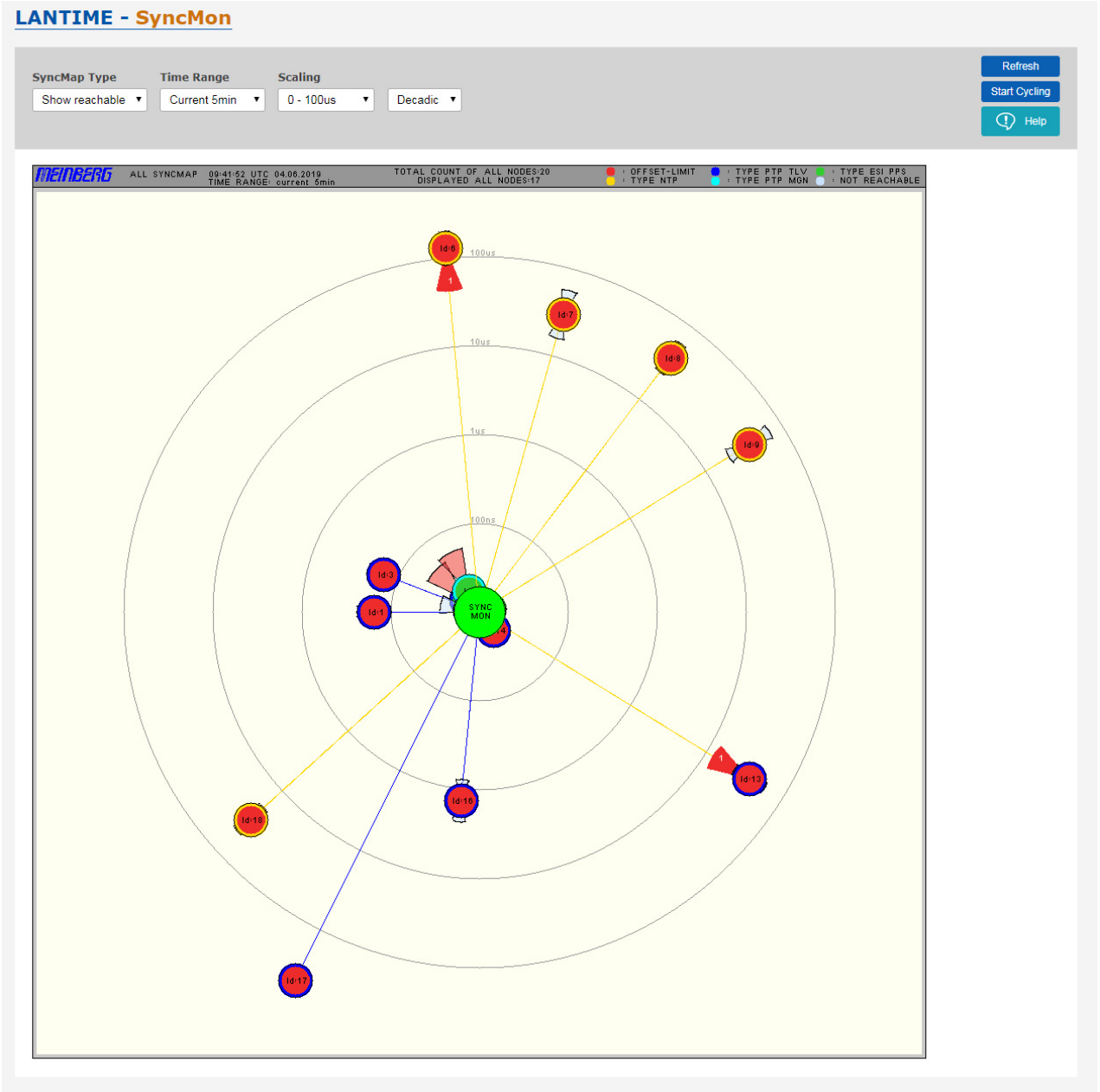


Abbildung: Die SyncMap als grafische Darstellung der überwachten Knoten in einem Netzwerk, visualisiert als Polardiagramm. Es kann Knoten anzeigen, die folgende Protokolle oder Signale unterstützen: NTP, PTP (IEEE 1588v1, IEEE 1588v2) oder PPS.

Jeder überwachte Knoten wird als Kreis mit unterschiedlichen statistischen Informationen angezeigt.

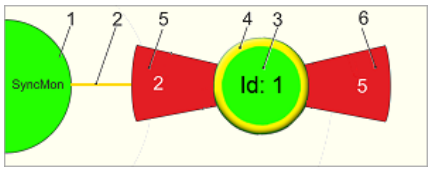


Abbildung: Eine Knoten-Darstellung in der SyncMap.

In der Mitte befindet sich die Referenzzeitüberwachung „SyncMon“ mit ihrer Referenzuhr [1]. Es stellt eine Zeitreferenz durch einen eingeregelten Oszillator zur Verfügung (synchronisiert durch GPS, GLN, DCF77, Galileo, BeiDou oder eine andere externe Taktung). Der SyncMon-Knoten in der Mitte [1] wird grün dargestellt, solange die Referenzuhr synchron ist.

Um den SyncMon-Knoten herum sind vier konzentrische Kreise gezeichnet, die die Skalierung des Polardiagramms darstellen. Alle „Satellitenknoten“ [3] sind durch eine Linie [2] vom zentralen SyncMon-Knoten aus verbunden. Der Abstand vom zentralen Konten zu den Satellitenknoten stellt den absoluten durchschnittlichen Zeitversatz zwischen dem Zeitmonitor „SyncMon“ und jedem einzelnen Knoten dar. Der Mittelwert wird über den gewählten Zeitraum berechnet. Jeder Satellitenknoten wird als Kreis mit einer Farbe im Inneren [3] dargestellt, die dem Status entspricht, und einem Außenring [4], der seinem Typ entspricht.

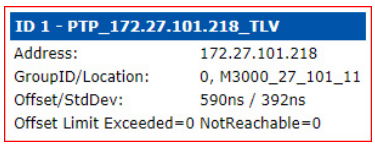
Status:	grün	= Offset hat Limit nicht überschritten
	rot	= Offset hat Limit überschritten bzw. maximale Skalierung ist überschritten worden
Typ:	gelb	= NTP
	dunkelblau	= PTP mit TLV (nur PTPv2)
	hellblau	= PTP mit Management-Nachrichten (PTPv1 oder PTPv2)
	grün	= ESI PPS
	grau	= nicht verfügbar

Die Satellitenknoten stellen grafisch auch einige statistische Werte dar. Die Standardabweichung, die den zeitlichen Jitter der Messwerte um den Mittelwert vermittelt, wird durch zwei „Flügel“ ([5] bzw. [6]) dargestellt: der **nach** SyncMon gerichtete Flügel [5] stellt die Anzahl der „nicht erreichbar“-Ereignisse dar. Der **weg** vom SyncMon gerichtete Flügel [6] repräsentiert dagegen die Anzahl der Überschreitungen des Offset-Limits des Knoten.

Wenn ein Flügel rot ist, dann ist die Abweichung von der Skalierung abhängig und überschreitet die Hälfte des Bereichs der Dekade. Beispiel: Liegt die mittlere Abweichung im Bereich von 1 μs - 10 μs und das größte gefundene Maximum ist > 5 μs, dann wird der einzelne Flügel rot, sonst blau gezeichnet.

Wenn ein Offset-Limit überschritten wird bzw. einen Knoten als „nicht erreichbar“ bewertet wird, dann wird der Flügel dunkelrot und ein Wert wird in weiß angezeigt, der die Anzahl der entsprechenden Ereignisse darstellt.

Fährt man mit dem Mauszeiger über einen Knoten ohne anzuklicken, werden in der SyncMap ein entsprechendes Infofensters den Namen und einige statistische Werte angezeigt:



Durch Auswahl eines bestimmten Knotens in der SyncMap mit einem linken Mausklick wird das folgende Kontext-Menü geöffnet:

„**Show Graphic**“ (Grafik anzeigen) öffnet das entsprechende grafische Diagramm.

„**Reset Event Counter**“ (Ereigniszähler zurücksetzen) setzt die Zähler der „nicht erreichbar“ und „Offset-Limit überschritten“-Ereignisse zurück und ändert die SyncMap entsprechend.

„**Edit Node Parameters**“ (Knotenparameter bearbeiten) öffnet die Konfigurationsseite für diesen Knoten (siehe SyncMon Statusüberwachung und Konfiguration über Webinterface für weitere Informationen).

„**Close This Menu**“ (Menü schließen) schließt dieses Kontext-Menü.

Beispiel für eine vollständige Sync-Map
Das folgende Bild zeigt eine SyncMap eines Netzwerks mit 250 überwachten NTP-Knoten, die auf einem Sync-Fire Server laufen. Es stellt eine echte Messung unseres Test-Netzwerks für Burn-In-Tests in der LANTIME-Produktion dar. Die rot markierten Knoten sind DCF77-Empfänger, bei denen die Entfernung zwischen einem Senderstandort und einem Empfänger nicht kompensiert wurde.

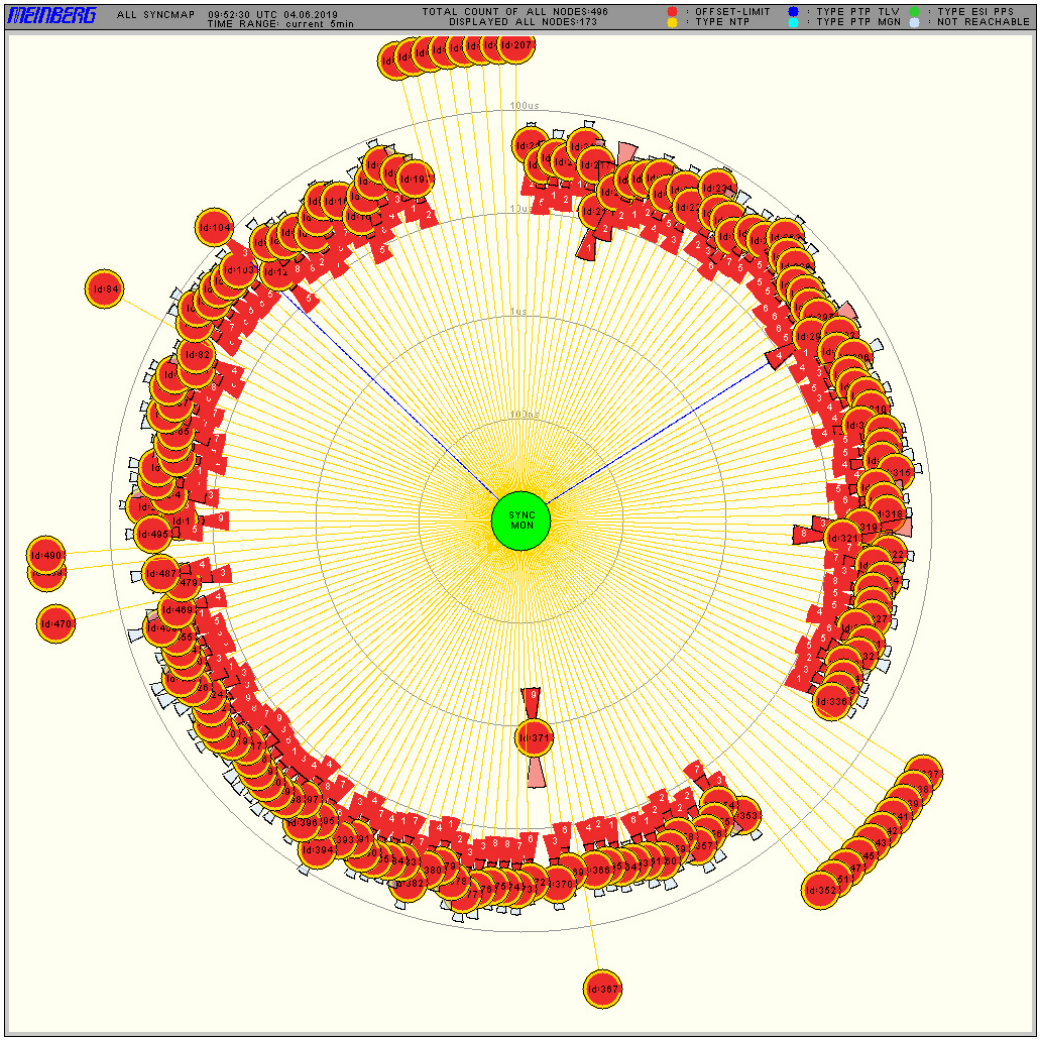


Abbildung: Ein Beispiel für eine SyncMap mit 250 Knoten.

SyncMap Type:

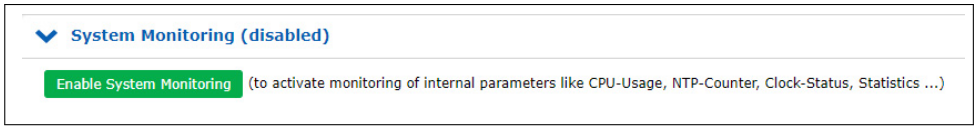
- **Show Reachable (erreichbare Knoten anzeigen):** Aktuell erreichbare Knoten werden in der SyncMap angezeigt.
- **Show All Nodes (alle Knoten anzeigen):** Alle in der Überwachungsliste konfigurierten Knoten werden in der SyncMap angezeigt, auch wenn sie nicht erreichbar sind.
- **Show NTP Only (nur NTP anzeigen):** In der SyncMap werden nur überwachte NTP-Knoten angezeigt. NTP-Knoten werden in der SyncMap mit einem gelben Außenring dargestellt.
- **Show PTP Only (nur PTP anzeigen):** In der SyncMap werden nur überwachte PTP-Knoten angezeigt. PTP-Knoten, die über TLV überwacht werden, sind in der SyncMap mit einem dunkelblauen Außenring dargestellt. PTP-Knoten, die über Management-Nachrichten überwacht werden, sind in der SyncMap mit einem hellblauen Außenring dargestellt.

Time Range (Zeitraum):	Die SyncMap kann aus den Überwachungsdaten erzeugt werden, die in den letzten 30 Min., 5 Min., 24 Stunden oder in einem manuell gewählten Zeitraum aufgenommen wurden. Auch die statistischen Werte werden aus den Daten des gewählten Zeitintervalls berechnet.
Scaling (Skalierung):	Skalierungen von 0–100 ns bis 0–10 ms, die in Dekadenschritten aufgesteigen, sind möglich. Darüber hinaus kann die Skalierung der SyncMap selbst auf linear (gleiche Schritte zwischen konzentrischen Kreisen) oder dekadisch (in Zehnerpotenzen aufsteigend) eingestellt werden. Für PTP-Knoten kann es sinnvoll sein, die Skalierung 0–10 μs zu verwenden, während sich für NTP die Bereiche 0–1 ms oder 0–10 ms bieten.
Refresh (Aktualisieren):	Aktualisiert sofort die SyncMap basierend auf den aktuell verfügbaren Statistiken der einzelnen Knoten. Es wird eine neue SyncMap mit dem gewählten Zeitraum generiert: Es hat die gleiche Wirkung wie ein Neuladen der Webseite mit den neuesten Messungen.
Start Cycling (Zyklusgenerierung starten):	Aktiviert den Sync-Map-Animationsmodus. In diesem Modus wird jede Minute eine neue SyncMap mit den neuesten Messungen generiert. Die letzten 60 SyncMaps werden dann als Animation angezeigt. Eine neue Sequenz beginnt mit einer leeren SyncMap. Der Statistikzeitbereich ist auf 5 Min. gesetzt. Die Anzahl der im RAM gespeicherten SyncMap-Bilder wird im automatischen Aktualisierungsmodus bei LANTIME-Systemen mit 2 GB RAM (z.B. IMS-CPU-C15G2-Modul) oder einem SyncFire-System auf 1000 beschränkt.
Help (Hilfe):	Zeigt die Online-Hilfeseite für die SyncMap-Funktion an.

13.1.12.18 System Monitoring

System Monitoring (Systemüberwachung) überwacht interne Signale im LANTIME-System, die nicht zu den überwachten Netzwerkknoten gehören: Dazu gehören z.B. CPU-Auslastung, lokale NTP-, ESI-Eingänge, MRS-Referenzen und Referenzuhrparameter. Die Anzahl und Art der internen Signale hängt von den integrierten Hardwarekomponenten in einem LANTIME-System ab.

Die Systemüberwachung ist eine optionale Funktion und ist standardmäßig deaktiviert. Sie kann im Menü „**SyncMon → System Settings → SyncMon Configuration**“ über das Dropdown-Menü „**Enable System Monitoring**“ oder direkt über den Reiter „**System Monitoring**“ aktiviert werden:



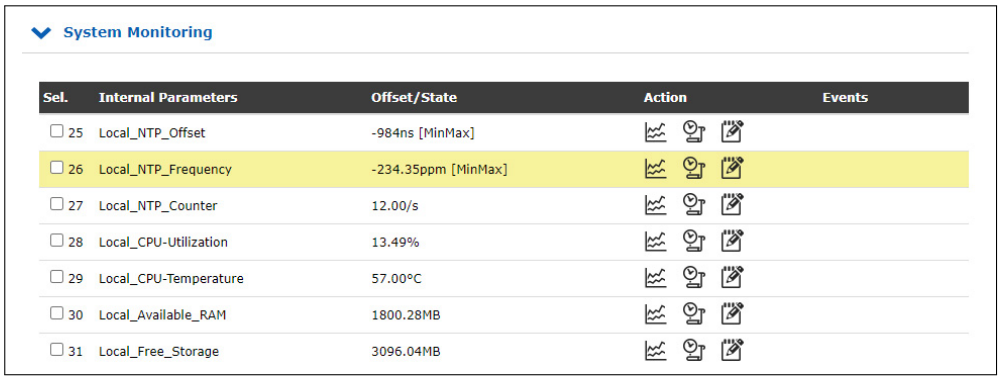
Um die Systemüberwachung wieder zu deaktivieren, sollte entsprechend über das Dropdown-Menü „**SyncMon → System Settings → SyncMon Configuration → Enable System Monitoring**“ wieder „*No*“ gewählt werden.

Wenn die Systemüberwachung aktiviert ist, werden alle Signale automatisch gemessen und protokolliert, wie bei der Netzwerk-Knotenüberwachung.

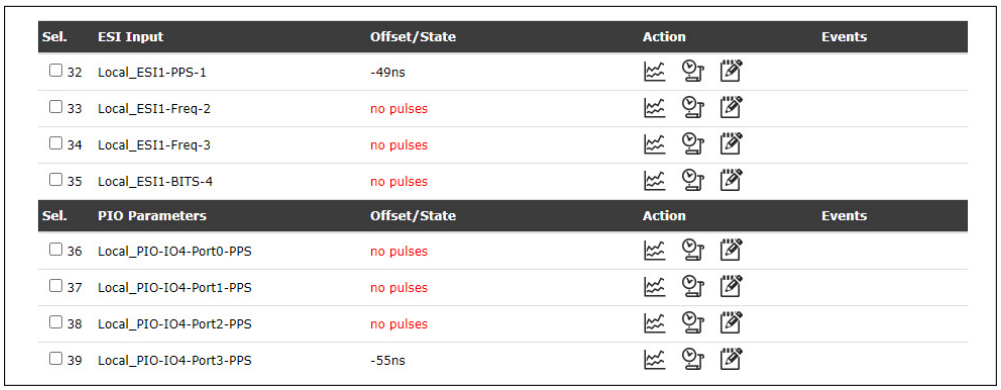
Die Anzahl der MRS-Referenzen (CLK1-GPS-0, CLK1-NTP-1, CLK1-PTP-2 ...) hängt von den aktivierten Quell-Prioritäten für jede Referenzuhr ab: Das kann über „**MRS-Einstellungen**“ im Webinterface-Menü „**Uhr**“ für jede eingesetzte Referenzuhr konfiguriert werden.

Jeder Knoten im Bereich „**System Monitoring**“ kann ausgewählt werden und gemeinsam mit überwachten Netzwerkknoten in einer Grafik dargestellt werden.

Liste der möglichen Sensoren in SyncMon:



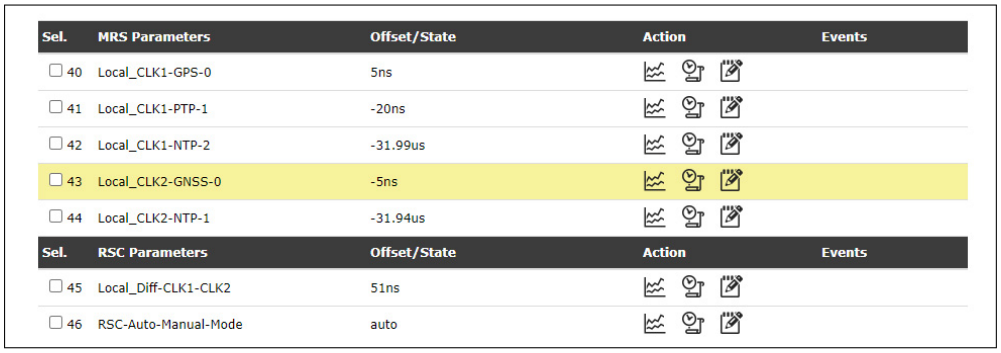
Interne Parameter:	Offset des lokalen NTP-Dienstes
	Frequenz des lokalen NTP-Dienstes
	Zähler für lokalen NTP-Dienst
	Eigene CPU-Auslastung
	Eigene CPU-Temperatur
	Eigene verfügbare RAM
	Eigener freier Flash-Speicher



Sel.	ESI Input	Offset/State	Action	Events
32	Local_ESI1-PPS-1	-49ns		
33	Local_ESI1-Freq-2	no pulses		
34	Local_ESI1-Freq-3	no pulses		
35	Local_ESI1-BITS-4	no pulses		
Sel.	**PIO Parameters**	**Offset/State**	**Action**	**Events**
36	Local_PIO-IO4-Port0-PPS	no pulses		
37	Local_PIO-IO4-Port1-PPS	no pulses		
38	Local_PIO-IO4-Port2-PPS	no pulses		
39	Local_PIO-IO4-Port3-PPS	-55ns		

ESI-Eingang:
ESI PPS In
ESI Freq In
ESI BITS In

PIO-Parameter:
PIO PPS In



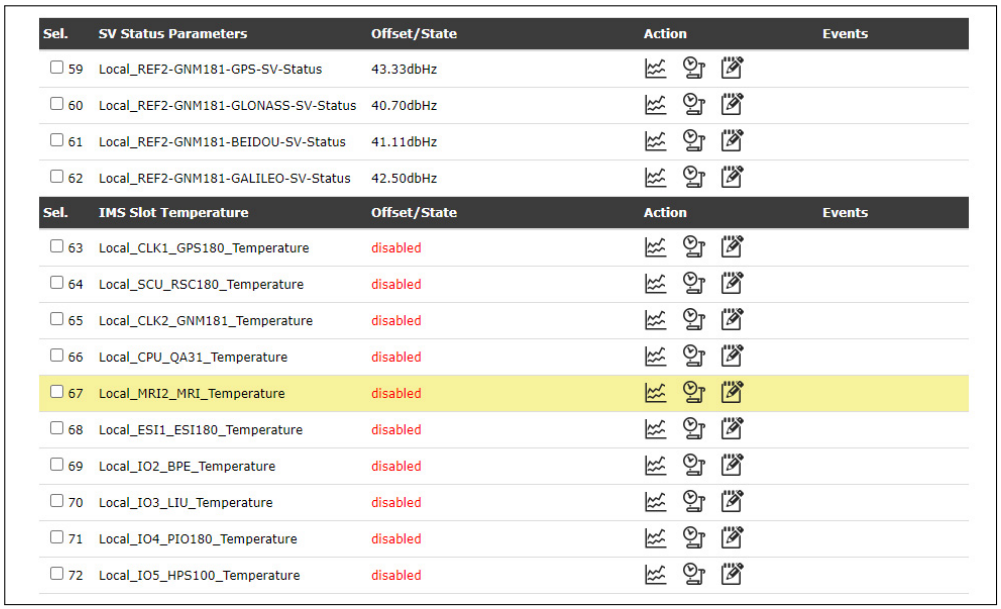
Sel.	MRS Parameters	Offset/State	Action	Events
40	Local_CLK1-GPS-0	5ns		
41	Local_CLK1-PTP-1	-20ns		
42	Local_CLK1-NTP-2	-31.99us		
43	Local_CLK2-GNSS-0	-5ns		
44	Local_CLK2-NTP-1	-31.94us		
Sel.	**RSC Parameters**	**Offset/State**	**Action**	**Events**
45	Local_Diff-CLK1-CLK2	51ns		
46	RSC-Auto-Manual-Mode	auto		

MRS-Referenzeingänge:
Standard-GPS
10 MHz Eingangsfrequenz
PPS-Eingangssignal
kombiniertes 10 MHz plus PPS
IRIG-Eingang
Network Time Protocol (NTP)
Precision Time Protocol (PTP/IEEE1588)
feste Frequenz
PPS zusammen mit Zeittelegramm
variable Eingangssignale über GPIO
DCF77 (Pseudozufallsfolge)
Langwellenempfänger z.B. DCF77 AM, WWVB, MSF, JJY
GNSS-Empfänger

RSC Parameter:
Lokale Differenz zwischen 2 Uhren
RSC Auto-/Manual-Modus

Für jede Referenzuhr:

- Refclock-State
- MRS-SubState
- Refclock-Usage
- Refclock-DCF-Field
- Refclock-DCF-Correlation
- Refclock-Sat-in-view
- Refclock-good-Sat
- Position change



Sel.	SV Status Parameters	Offset/State	Action	Events
59	Local_REF2-GNM181-GPS-SV-Status	43.33dbHz		
60	Local_REF2-GNM181-GLONASS-SV-Status	40.70dbHz		
61	Local_REF2-GNM181-BEIDOU-SV-Status	41.11dbHz		
62	Local_REF2-GNM181-GALILEO-SV-Status	42.50dbHz		
Sel.	**IMS Slot Temperature**	**Offset/State**	**Action**	**Events**
63	Local_CLK1_GPS180_Temperature	disabled		
64	Local_SCU_RSC180_Temperature	disabled		
65	Local_CLK2_GNM181_Temperature	disabled		
66	Local_CPU_QA31_Temperature	disabled		
67	Local_MRI2_MRI_Temperature	disabled		
68	Local_ESI1_ESI180_Temperature	disabled		
69	Local_IO2_BPE_Temperature	disabled		
70	Local_IO3_LIU_Temperature	disabled		
71	Local_IO4_PIO180_Temperature	disabled		
72	Local_IO5_HPS100_Temperature	disabled		

SV Status Parameter:

- GPS-SV-Status
- GLONASS-SV-Status
- BEIDOU-SV-Status
- GALILEO-SV-Status

IMS Slot-Temperatur: CLK, SCU, CPU, MRI, ESI, IO

13.1.12.19 NTP-Zugriffsstatistik

Der LANTIME zählt automatisch alle eingehenden Netzwerkpakete am UDP-Port 123 aller verfügbaren Netzwerkschnittstellen. Der aktuelle Wert wird in der Tabelle „**System Monitoring**“ unter „**Local_NTP_Counter**“ gezeigt und den Verlauf über Zeit kann mit einem Klick auf dem Grafik-Symbol grafisch dargestellt. Hier zeigt die rote Linie einen Wert der empfangenen NTP-Pakete innerhalb eines ausgewählten Zeitraums an.

13.1.12.20 Error Logs

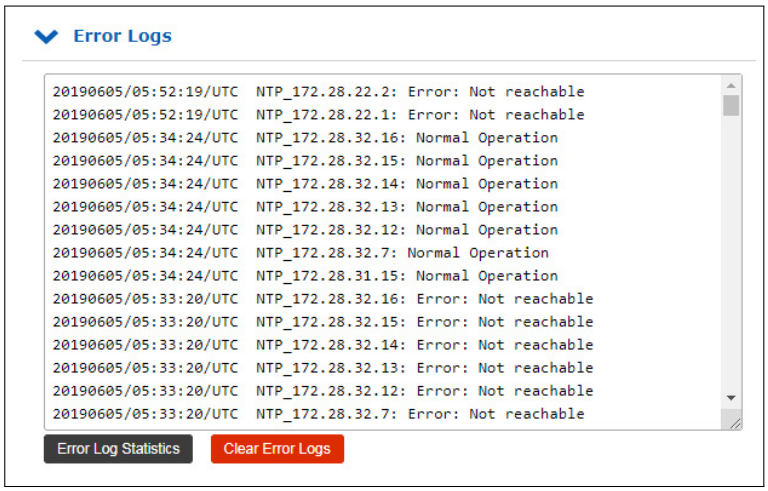


Abbildung: Protokollierte Meldungen von allen überwachten Knoten.

Das globale Fehlerprotokoll bietet die Möglichkeit, alle Fehlerereignisse für alle überwachten Knoten zu verfolgen.

Error Log Statistics (Fehlerprotokoll-Statistik): Hier werden die Meldungen des Fehlerprotokolls ausgewertet und ein statistischer Bericht angezeigt. So kann man erkennen, durch welche Knoten am häufigsten Fehlermeldungen erzeugt werden.

Clear Error Logs: (Fehlerprotokoll-Statistik): Mit dieser Schaltfläche werden alle bisherige Meldungen des Fehlerprotokolls gelöscht.

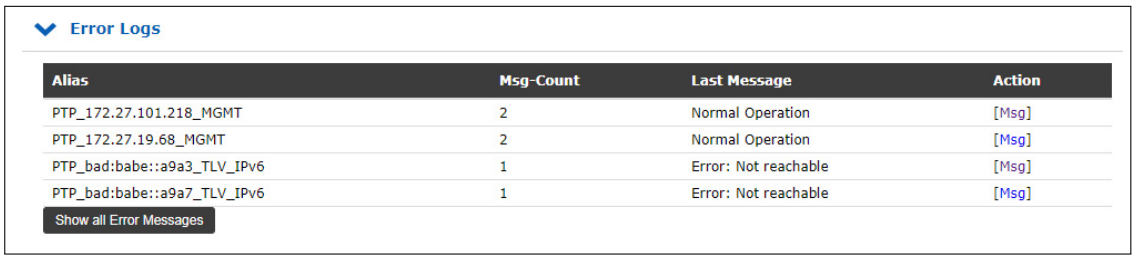


Abbildung: Fehlerprotokoll-Statistik.

13.1.12.21 Systemeinstellungen

Das Menü „**System Settings**“ (Systemeinstellungen) zeigt den aktuell verfügbaren Speicherplatz auf dem ausgewählten Speichermedium (intern oder extern) an und die berechnete Anzahl der Tage, die gespeichert werden können, abhängig von der Anzahl der überwachten Knoten und dem Protokollintervall. Darüber hinaus sind hier einige sonstige systemrelevante Funktionen und Einstellungen untergebracht.

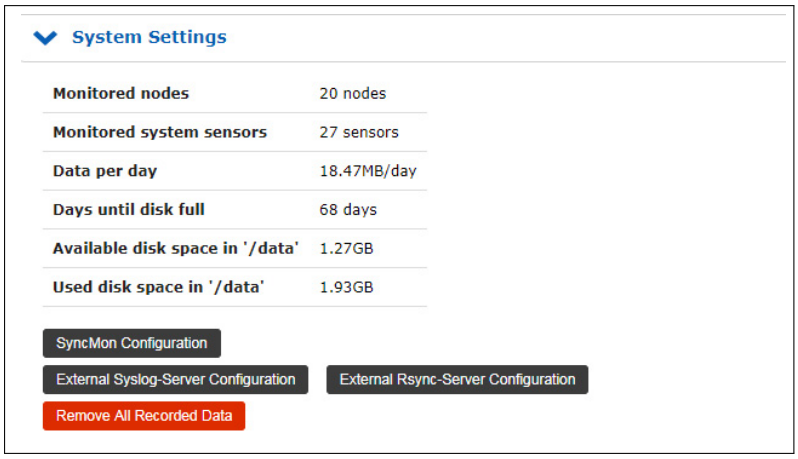


Abbildung: Status des Speichermediums, verfügbarer Speicherplatz und Archivierungsoptionen für Protokolldateien.

Monitored Nodes (überwachten Knoten) zeigt, wie viele externe Knoten aktuell überwacht werden.

Monitored System Sensors (überwachten Systemsensoren) zeigt, wie viele interne Systemknoten aktuell überwacht werden.

Data per Day (Daten pro Tag) zeigt, wie viele Daten voraussichtlich bei den aktuellen Überwachungseinstellungen von SyncMon gespeichert werden. Der entsprechende Wert „**Days Until Disk Full**“ (Tage bis Speicher voll) wird hiervon abgeleitet, damit man den voraussichtlichen Zeitraum erkennen kann, über die Daten auf dem ausgewählten Speichermedium gespeichert werden können.

„**Available Disk Space**“ zeigt, wie viel Speicherplatz auf dem ausgewählten Speichermedium noch verfügbar ist. „**Used Disk Space**“ zeigt dagegen, wie viel Speicherplatz auf dem ausgewählten Speichermedium schon belegt ist.

Je nach Anzahl der Knoten (bis zu 1.000 Knoten sind möglich) und den entsprechenden Anforderungs- und Protokollierungsintervallen wird die System-CPU unterschiedlich stark belastet.

Achtung!

Es ist wichtig, die Systemnutzung bei der Einstellung von SyncMon zu berücksichtigen. Bei hohen Knotenzahlen und häufigen Anforderungs- und Protokollierungsintervallen ist das Datenaufkommen besonders hoch. So kann auch die Leistung des NTP-Servers entsprechend beeinträchtigen.

Beispiele für Systemnutzung:

- Ein einziger Überwachungsknoten mit einem Protokollierungsintervall von 64s speichert ca. 110 KB pro Tag. Ein einziger Überwachungsknoten mit einem Protokollierungsintervall von 1s speichert 64 Mal so oft Daten und generiert demnach das 64-Fache an Daten, d.h. ca. 7 MB.
- 10 Überwachungsknoten mit einem Protokollierungsintervall von 1s speichern 70 MB pro Tag. Bei einem Speichermedium mit 400 MB freiem Platz können also 5 Tage auf dem ausgewählten Speichermedium gespeichert werden.
- 100 Überwachungsknoten mit einem Log-Intervall von 1s speichern 700 MB pro Tag. Bei einem Speichermedium mit 400 MB freiem Platz ist hier der Speicherplatz schon vor Ende des 1. Tags voll, so dass an diesem Punkt die Aufzeichnung angehalten wird. Die Log-Rotation für SyncMon wird um 00:00 UTC gestartet und löscht Dateien, die älter als 2 Tage sind. Die CPU-Auslastung wird um ca. 10 % steigen.
- 100 Überwachungsknoten mit einem Anforderungsintervall von 1s und Protokollierungsintervall von 64s speichern ca. 12 MB pro Tag: So können ca. 40 Tage auf dem ausgewähltem Speichermedium gespeichert werden. Die CPU-Auslastung wird um ca. 7 % steigen.
- 900 Überwachungsknoten mit einem Anforderungsintervall von 1s und Protokollierungsintervall von 64s speichern ca. 100 MB pro Tag: So können ca. 4 Tage auf dem ausgewähltem Speichermedium gespeichert werden. Die CPU-Auslastung wird um ca. 45 % steigen. Bei dieser Auslastung kann die NTP-Serverleistung des Geräts beeinträchtigt werden.

13.1.12.22 SyncMon Konfiguration

Mit der Schaltfläche „**SyncMon Configuration**“ können einige Systemkonfigurationsparameter eingestellt werden:

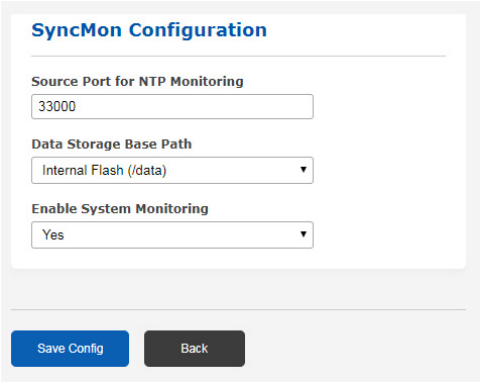


Abbildung: Systemparameter-Einstellungen für SyncMon. Hier können Sie u.a. den aktuellen Pfad einstellen, in dem die Daten gespeichert werden.

Source Port for NTP Monitoring (Quelle-Port für NTP-Überwachung): Dieser Parameter bestimmt den Port, über den ausgehende NTP-Pakete versendet werden. Standard ist 33000.

Data Storage Base Path (Basispfad für Datenspeicherung): Der Standardpfad ist die interne Compact-Flash mit */data*. Das kann durch Verwendung eines USB-Speichermediums (z.B: USB-Stick) in */mnt/usb-storage* geändert werden.

Enable System Monitoring (Systemüberwachung aktivieren): Aktiviert die Überwachung der systeminternen Parameter. Hierdurch werden interne Signalen wie CPU-Auslastung, lokale NTP-, ESI-Eingänge, MRS-Referenzen und Referenzuhrparameter, abhängig von der integrierten Hardware des Systems, überwacht. Standardmäßig ist die Überwachung des Systems deaktiviert.

Die Messdaten der überwachten Knoten werden in separaten Verzeichnissen auf dem ausgewählten Speicher gespeichert. Die Daten werden für jeden Tag und jeden überwachten Knoten separat gespeichert.

Achtung: Wenn das gewählte Speichermedium voll ist, werden die ältesten Daten überschrieben.

```
/data
    |   /stats
    |       |   /syncmon
    |       |       |   /alias-name1
    |       |       |       |   /ntp_mon_stats.20190501
    |       |       |       |   /ntp_mon_stats.20190502
    |       |       |       |   /ntp_mon_stats.20190503
    |       |       |       |   ...
    |       |       |   /alias-name2
    |       |       |       |   /ntp_mon_stats.20190501
    |       |       |       |   /ntp_mon_stats.20190502
    |       |       |       |   /ntp_mon_stats.20190503
    |       |       |       |   ...
```

Abbildung: Beispiel für die Standardpfadstruktur der Historie der Tagesdatendateien auf dem Speichermedium.

Das Format der Datendatei:

1. MJD: Modifiziertes julianisches Datum. Das ist die kontinuierliche Anzahl der Tage seit Beginn der Julianischen Periode (begonnen um 1858 Nov 17 - 0:00 Uhr).
2. Zeit nach Mitternacht in Sekunden
3. Zeitstempel (ISO von MJD und Zeit nach Mitternacht)
4. Roher gemessener Taktversatz (wenn das Anforderungsintervall kleiner als das Aufzeichnungsintervall ist, dann wird der Mittelwert der gemessenen Offsets im Anforderungsintervall gespeichert).
5. Bei NTP: Clock Offset Median (Median der 5 zuletzt gemessenen Offsets auf Anfrage)
   Bei PTP: Gemeldeter Offset
6. Pfadverzögerung in Sekunden
7. NTP-Stratum oder PTP-Status
8. 'R' (optionales Kennzeichen für Min/Max-Werte von Rohdaten: Wenn das Anforderungsintervall kleiner als das Protokollintervall ist, dann werden automatisch die Min- und Max-Werte der Rohdaten in den nächsten 2 Zeilen gespeichert.
9. Siehe 8. (optional)
10. Siehe 8. (optional)
11. 'M' (optionaler Indikator für Min/Max-Werte von MTie-Werten (Maximum Time interval error) von PTP-Knoten, die diese Option unterstützen: Wenn der PTP-Knoten MTie-Funktion mit erweiterten TLVs unterstützt, werden die Min- und Max-Werte in den nächsten 2 Zeilen gespeichert.
12. Siehe 11. (optional)
13. Siehe 11. (optional)

Auszüge von Überwachungsdaten, die in der Historie der Tagesdateien gespeichert sind:

Beispiel für NTP-Datendateien:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay Stratum
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 1
```

Beispiel für NTP-Datendateien mit Anfrageintervall kleiner als Protokollintervall:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay St Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.00000129 -0.000000053 0.000007667 1 R -0.01 0.01
```

Beispiel für PTP-Datendateien:

```
# Day Sec Modified_Julian_day_time Raw_offset Report_offs Path_delay Portstate
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 9
```

Beispiel für PTP-Datendateien mit Unterstützung der MTie-Funktionalität:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay St Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.00000129 -0.000000053 0.000007667 9 M -0.01 0.01
```

13.1.12.23 Externe syslog-Server-Konfiguration

Um die Überwachungsdaten zu sichern und für die spätere analytische Verarbeitung zu speichern, können Sie Daten über das syslog-Protokoll an bis zu 3 externe Datenbankserver automatisch übermitteln lassen.

Über die Schaltfläche „**External syslog Server Configuration**“ können Sie diese 3 Server konfigurieren, auf denen die Messdaten in jedem Protokollintervall über das syslog-Protokoll gesendet werden. Auf dem externen Server muss der entsprechende Dienst wie ein Standard-syslog-Server laufen. Jede in einem Protokollintervall verarbeitete Knotenmessung wird an diese Server gesendet, soweit die Protokollierung auf externe Server für einzelne Knoten nicht deaktiviert worden ist (**Disable Logging on External Server** unter den Knoteneinstellungen).

Im folgenden Dialog können Sie die Zielserver für die Daten konfigurieren:

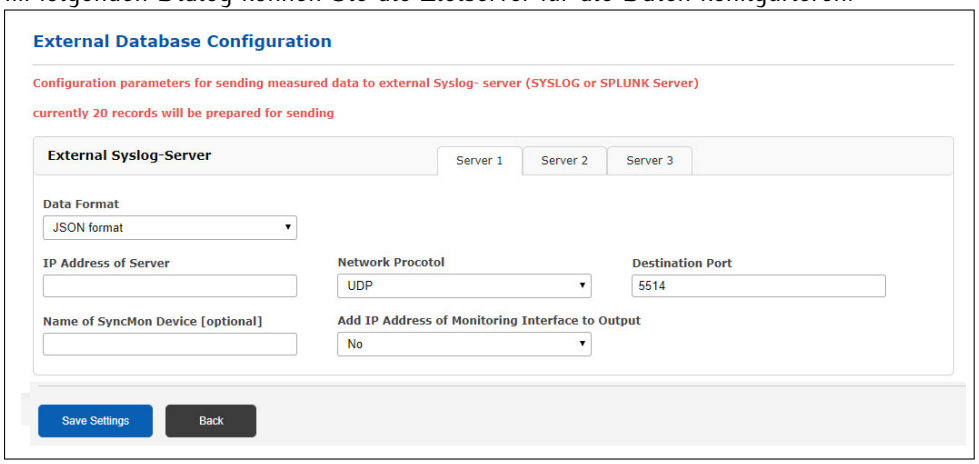


Abbildung: Konfigurationsoptionen für externe Datenbankserver, auf denen die Überwachungsdaten gespeichert werden können.

Für jeden dieser externen Server können die folgenden Parameter eingestellt werden:

Data Format (Ausgabeformat): Hier kann das Ausgabeformat der Daten festgelegt werden: MBG Data Format (das Meinberg-Standard-Format), SPLUNK-Friendly (Key-Value-Paare) oder JSON Format.

IP Address of Server: Die IP-Adresse des syslog-Servers ist hier einzugeben.

Network Protocol (Netzwerkprotokoll): Hier wird das Netzwerkprotokoll festgelegt (UDP oder TCP), das zur Kommunikation mit dem syslog-Server benutzt wird.

Destination Port (Zielport): Hier wird der Port des syslog-Servers festgelegt. Standardmäßig erwarten syslog-Dienste Daten über Port 514.

Name of SyncMon Device (Name des SyncMon-Gerätes): Hier können Sie optional dem SyncMon-Gerät einen Namen zuweisen. Dieser Name wird mit den Messdaten an den syslog-Dienst übermittelt und erleichtert die Zuordnung der Daten von dieser SyncMon-Instanz auf dem syslog-Server.

Add IP Address of Monitoring Interface to Output (IP-Adresse der Überwachungsschnittstelle in Ausgabe einfügen): Wenn Sie hier „*Yes*“ auswählen, wird auch die IP-Adresse der Netzwerkschnittstelle in die Ausgabe eingefügt, über die die Messdaten erhalten wurde.

Ein Auszug aus dem SyncMon-Format „Meinberg Standard“, das per syslog-Protokoll gesendet wird:

```
SyncMon 172.27.100.32 M3000_100_57_NTP_LAN0 58154 34813 2018-02-05T09:40:13+00:00
0.000000494 0.000041453 0.000073266 1 R -0.000011100 0.000041453
```

Für weitere Details zu den SyncMon-Formaten siehe Kapitel „Technischer Anhang → SyncMon Formate“.

13.1.12.24 Externe rsync-Server-Konfiguration

Über die Schaltfläche „**External rsync Server Configuration**“ (externe rsync-Server-Konfiguration) können Sie bis zu 3 externe Server konfigurieren, auf die die Messdaten stündlich oder einmal um 00:00 UTC über das rsync-Protokoll kopiert werden. Auf dem externen Server muss der entsprechende Dienst wie ein Standard-rsync-Server laufen.

Im folgenden Dialog können Sie die Zielserver konfigurieren, auf denen Sie Ihre Daten speichern möchten:

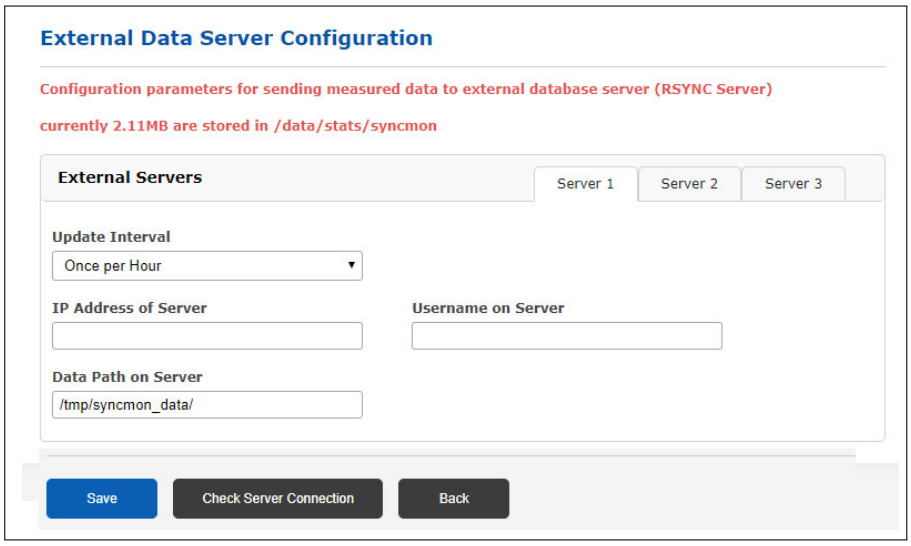


Abbildung: Externe rsync-Server-Konfiguration

Um Daten einmal stündlich oder täglich automatisch über *rsync* zu versenden, müssen Sie den ssh-Key für den externen rsync-Server vorbereiten:

1. Melden Sie sich über SSH bei dem LANTIME an.
2. Überprüfen Sie, ob Identität-Keys bereits in */root/.ssh/id_rsa.pub* verfügbar sind.
3. Wenn nicht, dann erstellen Sie eine Identität mit: *ssh-keygen -t rsa*.
4. Speichern Sie diese Identität für den dauerhaften Gebrauch mit: *saveconfig @*.
5. Kopieren Sie die Identität des LANTIME auf den externen rsync-Server mit: *ssh-copy-id ip-adresse-des-RSYNC-server*.

13.1.12.25 Alle Aufzeichnungen löschen

Mit der Schaltfläche „**Remove All Recorded Data**“ (alle Aufzeichnungen löschen) werden alle Messdaten für alle Knoten unwiderruflich gelöscht. Bei Betätigung dieser Schaltfläche werden Sie aufgefordert, den Vorgang einmal zu bestätigen.

13.1.12.26 Zugang zur SyncMon-Status-Datei über CLI

Der aktuelle Status der überwachten Knoten, wie er im Webinterface angezeigt wird, wird in einer ASCII-Datei */var/log/syncmon_node_status* gespeichert. Diese Datei wird nach jedem vollständigen Scan der konfigurierten Knoten aktualisiert und ist über CLI zugänglich.

```
#   Net Sync Monitoring Status with total 15 Nodes (updated  at  ...)

#   Node-Address    NTP:Offset     -filtered       Delay        NTP-Stratum   Auth  MTIE    CntErr     CntErr   Err    Message
#                   PTP:OffsNode   -measured                   PTP-Status                  Offset     Reach
#   ------------------------------------------------------------------------------------------------------------------------------
172.16.100.65:      -0.000113960    0.000055254   0.001663415   2             0     0       3          0        0      Normal Operation
172.16.3.11:        -0.005109100   -0.005896857   0.001891819   1             0     0       0          0        0      Normal Operation
172.16.3.12:        -0.028305041   -0.028305041   0.001669302   2             0     0       0          0        1      Error:Offset exceeded
172.27.101.90:      -0.000037604   -0.000002865   0.000352269   2             0     0       0          0        0      Normal Operation
172.27.100.32:       0.000008375    0.000008375   0.000209699   1             0     0       0          0        0      Normal  Operation
172.27.100.1:        0.000000899   -0.000027105   0.000416735   1             2     0       0          0        7      Error:Auth. Failed
ESI-Module:          0.000001819    0.000001839   0.000000000   0             0     0       0          0        0      Normal Operation
EC:46:70:00:8F:64:   0.000000000    0.000000000   0.000000000   0             0     0       0          0        6      Error:not active
172.27.19.68:        0.000000109   -0.000000013   0.000007451   9             0     0       0          0        0      Normal Operation
EC:46:70:00:8F:64:  -0.000000049   -0.000000171   0.000006273   9             0     0       0          0        0      Normal Operation
172.27.19.70:        0.000000030   -0.000000035   0.000007749   9             0     0       0          0        0      Normal Operation
172.27.19.98:        0.000000000    0.000000000   0.000000000   0             0     0       0          0        3      Error:Not reachable
172.27.101.143:      0.000000000    0.000000000   0.000000000   0             0     0       0          0        3      Error:Not reachable
172.27.19.11:       -0.000010202   -0.000090331   0.000052625   8             0     1       0          0        0      Normal Operation
172.27.101.90:       0.000000000    0.000000000   0.000352269   2             0     0       0          0        3      Error:Not reachable
```

Abbildung: Die Statusinformationstabelle, auf die über ein CLI zugegriffen werden kann.

13.1.12.27 SyncMon-Konfiguration über CLI

Die Konfiguration aller überwachten Knoten wird in einer zentralen Text-Datei */etc/mbg/syncmon.cfg* gespeichert. Jede Zeile repräsentiert die Konfiguration eines zu überwachenden Knotens.

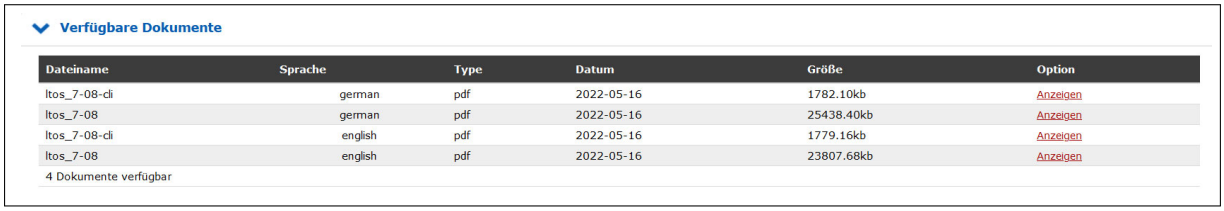
```
# Time Monitoring Node
Configuration
#
@ SourcePort: 33000
@ BaseLogPath: /data
@ BaseCurrDayPath: /data
# Supported Time Protocols: 0:NTP  1:MBG-PTP
# Support ESI Module: Protocol value define the input port
#
#   IP4-Address        CPU-Module   Interface     Protocol   Offset-Limit[s]   Stratum  Req-Intv  Log-Intv   Group  Alias                              Location
NtpKey   NtpKey       NtpKey
#   IPv6 or MAC        (MainCPU=-1)    Name         Index                       Domain                       Index
Index     Type        Secret
#
-------------------------------------------------------------------------------------------------------------------------------------------------------------------
addr=172.75.75.3          cpu=08   intf=all       prot=1  offs=0.000001000    domain=7  req=64    log=64    grp=0  alias=Master_TLV                   loc=M3000_training_rack
addr=172.75.75.3          cpu=08   intf=all       prot=2  offs=0.000001000    domain=7  req=64    log=64    grp=0  alias=Master_MGMT                  loc=M3000_training_rack
addr=172.75.75.1          cpu=08   intf=all       prot=1  offs=0.000001000    domain=7  req=64    log=64    grp=0  alias=Slave1_TLV                   loc=M3000_training_rack
addr=172.75.75.1          cpu=08   intf=all       prot=2  offs=0.000001000    domain=7  req=64    log=64    grp=0  alias=Slave1_MGMT                  loc=M3000_training_rack
addr=172.27.75.225        cpu=08   intf=all       prot=2  offs=0.000001000    domain=10 req=64    log=64    grp=0  alias=Boundary_Clock_1             loc=training_rack
addr=172.75.75.10         cpu=08   intf=all       prot=1  offs=0.000001000    domain=10 req=8     log=8     grp=0  alias=Slave2_TLV                   loc=M500_training
addr=172.75.75.10         cpu=08   intf=all       prot=2  offs=0.000001000    domain=10 req=8     log=8     grp=0  alias=Slave2_MGMT                  loc=M500_training
addr=172.27.100.194       cpu=-01  intf=lan0:0    prot=0  offs=0.001000000    strat=10  req=64    log=64    grp=0  alias=NTP_M500_unit                loc=M500_training
kidx=-1
addr=ESI-Module           cpu=10                  prot=1  offs=0.000001000              req=8     log=8     grp=0  alias=PPS_Slave2                   loc=training_rack
```

addr	:	IPv4/6- oder MAC-Adresse des zu überwachenden Knotens
CPU	:	ID der IMS-Karte: main cpu=-1 HPS100=0 - 9 ESI IMS-Karte=10-11
prot	:	Synchronisationsprotokoll für die Überwachung: NTP=0 PTP/TLV=1 PTP/Mngt=2
offs	:	Offset-Limit
stra	:	NTP-Stratum-Limit
domain	:	PTP-Domain
req	:	Anfragenintervall [s]
log	:	Protokollierungsintervall [s]
grp	:	Gruppen-ID
alias	:	Vom Benutzer definierter Aliasname
loc	:	Standort-String
kidx	:	NTP-Key-ID ('-1' wenn nicht verwendet)
ktyp	:	NTP-Schlüsseltyp (M=MD5 siehe NTP-Dokumentation)
ksecr	:	NTP Key Secret (siehe NTP-Dokumentation)

Diese Datei kann mit einem Texteditor (*vi*, *nano*) direkt in der Kommandozeile des Systems bearbeitet oder durch eine externe vorbereitete Datei ersetzt werden. SyncMon überprüft diese Konfigurationsdatei nach jedem vollständigen Scan der konfigurierten Knoten automatisch auf Änderungen.

13.1.13 Dokumentation und Support

Diese Seite bietet Ihnen Zugriff auf einige Dokumente, die auf Ihrem LANTIME-System gespeichert sind, insbesondere die aktuellsten Firmware-Handbücher. Die Liste enthält Dateiname, Sprache, Dateityp, Datum und Größe der Dokumente.


Verfügbare Dokumente

Dateiname	Sprache	Type	Datum	Größe	Option
ltos_7-08-cli	german	pdf	2022-05-16	1782.10kb	Anzeigen
ltos_7-08	german	pdf	2022-05-16	25438.40kb	Anzeigen
ltos_7-08-cli	english	pdf	2022-05-16	1779.16kb	Anzeigen
ltos_7-08	english	pdf	2022-05-16	23807.68kb	Anzeigen

4 Dokumente verfügbar

LT_CLI-Help
Für unsere LANTIME und SyncFire Zeitserver-Systeme steht Ihnen eine umfangreiche Dokumentation für das Command Line Interface und für die RestApi-Schnittstelle zur Verfügung. Darüber hinaus können Sie sich ein ZIP-Archiv mit einer Offline-Version dieser HTML-Hilfedateien auf Ihr lokales System herunterladen und sich die Hilfe auch „Offline“ ansehen.

CLI - REST API Dokumentation (Online)
https://www.meinberg.de/download/firmware/lantime/v7/lt-cli-help/

CLI - REST API Dokumentation (ZIP-Archiv zur Offline-Verwendung*)
https://www.meinberg.de/download/firmware/lantime/v7/lt-cli-help/lt-cli-help.zip

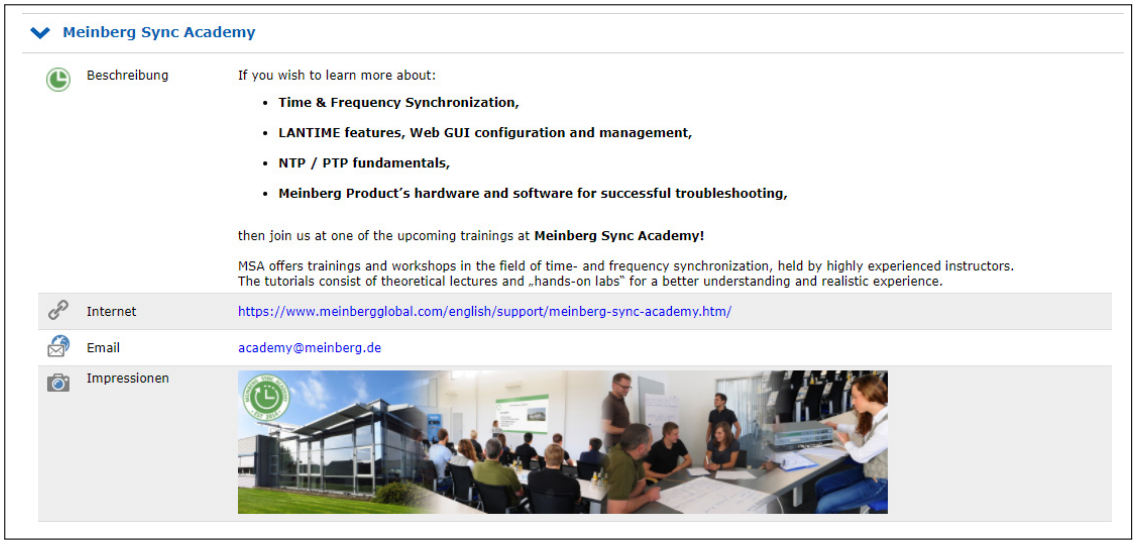
** Über diesen Link können Sie sich ein ZIP-Archiv der Hilfedateien auf Ihren lokalen PC herunterladen, entpacken und danach wie eine Webseite in Ihrem bevorzugten Internetbrowser ansehen.*

Im Submenü „Support-Informationen“ finden Sie alle notwendigen Informationen, wie Sie den technischen Support kontaktieren können. Darüber hinaus finden Sie hier einen Link zum Firmwareportal von Meinberg.


Support-Informationen

Telefon	+49(0)5281 9309888
Email	techsupport@meinberg.de
Firmware-Updates	https://www.meinberg.de/german/sw/firmware.htm
RMA	https://www.meinberg.de/german/support/rma.htm

Die Registerkarte „Docs & Support“ enthält auch einige wichtige Weblinks. Darüber hinaus erhalten Sie Informationen über die Meinberg Sync Academy (MSA).



Die Meinberg Sync-Academy bietet und entwickelt Tutorials im Bereich der Zeit- und Frequenzsynchronisation, wie NTP, PTP IEEE-1588 und viele mehr. Dieser Teil der LANTIME-Registerkarte „Dokumentation & Support“ enthält grundlegende Informationen über die Sync-Academy, gefolgt von einigen Links zu hilfreichen Informationen auf: https://www.meinberg.de/german/support/meinberg-sync-academy.htm

13.2 Über das Front-Panel-Display

13.2.1 LANTIME Displays

Für unsere LANTIME NTP Server gibt es vier unterschiedliche Displaytypen - das ist zum einen durch die Bauform bedingt und zum anderem durch den Funktionsumfang des jeweiligen Systems. Die Menüführung ist prinzipiell bei allen Displaytypen gleich, Unterschiede ergeben sich durch das verwendete Empfangssystem und über die verfügbaren Geräteoptionen.

Das hochauflösende VF-Display, welches im LANTIME M600 zum Einsatz kommt, bietet zudem eine grafische Darstellung der gemessenen Eingangssignale (NTP, PTP, IRIG, PPS ...). Das grafische VF-Display wird im nachfolgenden Kapitel beschrieben.

Die Darstellung der Konfigurationsmenüs wird mit einer vierzeiligen Grafik umgesetzt, die Menüs der jeweiligen Systeme können in der Anzeige davon abweichen (siehe Bild 1.0).

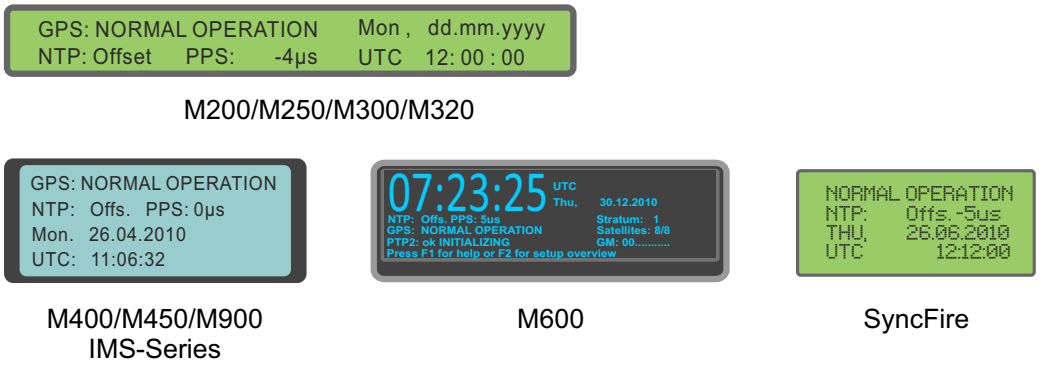


Bild 1.0 - LANTIME Displays

SyncFire	LC-Display, 4 x 20 characters
M200/M250/M300/M320	LC-Display, 2 x 40 characters
M400/M450/M900/IMS	LC-Display, 4 x 16 characters
M600	Vacuum Fluorescent Graphic Display (VFD), 256 x 64 Dots

13.2.1.1 Beschreibung des grafischen Menüs: VF-Display

Das grafische Display Menü dient zur graphischen Anzeige der Offset-Werte [1] zwischen dem ausgewählten Eingangssignal [2] und dem Oszillator der GPS-Karte. Das Programm kann über die ↑ - Taste in dem dazugehörigen Statusmenü gestartet werden. Weiterhin steht eine Auswahl der verschiedenen Offsets der jeweiligen Eingangssignale in der MRS Status Funktion zur Verfügung. Hierzu drücken Sie bitte die ↓ - Taste, wenn Sie sich im Hauptmenü befinden (aktuelle Uhrzeit wird angezeigt).

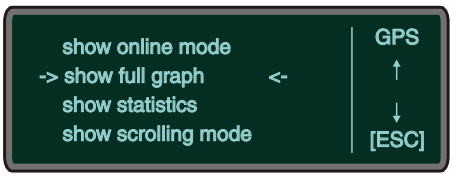
Hauptmenü des Lantime (Uhrzeit und Datum der gewählten Zeitzone wird dargestellt)

Wählen Sie Reference Time → MRS Management → MRS Status and Setup und schließlich MRS Status aus. Nun bleibt Ihnen die Wahl ob Sie sich die numerischen Offsets aller verfügbaren Eingangssignale anzeigen lassen oder das grafische Display Programm starten möchten. Wenn Sie den Graphical Status auswählen, haben Sie weiterhin die Möglichkeit ein Eingangssignal als Referenz auszuwählen.

Durch Drücken der Tasten ↑ und ↓ wechseln Sie die Referenzquelle und wählen diese mit der OK-Taste aus. In dem Graphic Menü haben Sie nun vier Auswahlmöglichkeiten sich den Offset der gewählten Referenzquelle anzeigen zu lassen (online mode, full graph, statistics, scrolling mode).

Mit den Tasten ↑ und ↓ wird die Cursorposition und somit die Auswahloptionen verändert. In der oberen rechten Ecke sehen Sie die ausgewählte Referenzquelle, zur der der grafische Offset angezeigt wird. Mit den Tasten OK oder → starten Sie den entsprechenden Modus.

Hauptmenü des grafischen Display Menüs mit den verschiedenen Auswahloptionen



In jedem dieser Modi steht Ihnen die Infotaste F1 zur Verfügung. Diese zeigt aktuelle Statusinformationen, sowie die wählbaren Tasten und Optionen des aktuelles Modus an. Mit der ESC-Taste gelangen Sie jederzeit in das vorherige Menü.

[1] Offset: Ein Offset ist die Zeitabweichung zweier Systeme. In unserem Fall ist der Offset die Zeitabweichung zwischen dem gewählten Eingangssignal und dem Oszillator, der die innere Uhr regelt.

[2] Eingangssignal: GPS, PTP, PPS, NTP, TCR, FRQ - Welche dieser Eingangssignale verfügbar sind, erfahren Sie im numerischen Status (Numerical Status)

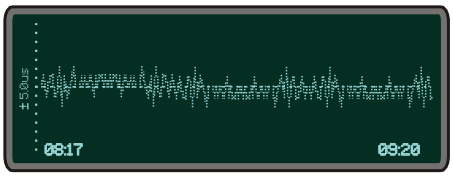
Zu jedem Graphen wird ein Wertebereich [3] angezeigt:

Anzeige des ausgewählten Modus (hier: SCROLLING MODE)

Nachdem einer der graphischen Menüpunkte auswählt wurde, erscheint für eine Sekunde sichtbar im Display der aktuelle Modus. In kleinerer Schrift steht unterhalb der Status von welcher Datei die Grafik erzeugt wird.

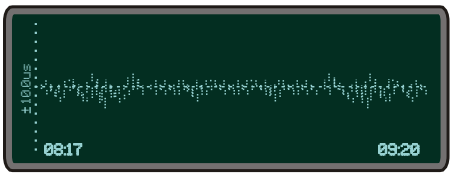
Der erste Modus ist der „ONLINE MODE“
Dieser zeichnet die letzten 255 Offsets und prüft ständig, ob weitere Offsets vorhanden sind. Ist dies der Fall, wird die Grafik zunächst um sechs Pixel nach links verschoben wenn diese am Displayende angekommen ist. Nun werden weitere Offsets gezeichnet. Zusätzlich wird der Wertebereich unten (Zeitachse) und am linken Rand (Größe des Offsets und Einheit) angezeigt.

Graph des Online Mode (ungezoomt)



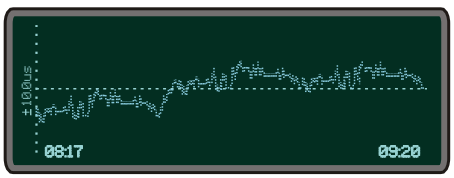
Mit den Tasten ↑ (zoom in) und ↓ (zoom out) kann jederzeit die Y-Achse des Wertebereichs verändert werden, um den Graphen größer oder kleiner darzustellen.

Graph des Online Mode (heraus gezoomt)



Der nächste Modus ist der „FULL GRAPHIC MODE“
Nachdem der Status angezeigt wurde, startet das Zeichnen des Graphen. Es werden alle Werte der Statistik-Datei dargestellt, solange nicht mehr als 255 Werte vorhanden sind. Sind mehr Werte als die Displaylänge (255 Punkte) vorhanden, so wird nur jeder Xte Offsetwert [4] gezeichnet. Es wird ein Durchschnittsgraph erzeugt, der so aussehen könnte:

Beispiel eines gezeichneten Graphen mit entsprechendem Wertebereich (hier: FULL GRAPHIC)

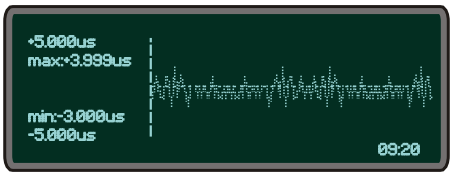


[3] Der Wertebereich hat eine X und Y Achse: Die Y-Achse stellt die Größeneinheit des Offsets dar. Es ist der größere Absolutwert von Minimum und Maximum und wird beim ersten Starten eines Menüs automatisch berechnet. Sie ist in folgenden Schritten eingeteilt: +- 1, 2, 5, 10, 20, ... (in den Einheiten von 30 Tagen [d] - eine Picosekunde [ps]). Die X-Achse ist die Zeitachse. Sie zeigt von und bis wann die jeweiligen Offsets aufgezeichnet wurden.

[4] Der Xte-Wert ist die Anzahl der Vorhandenen Werte dividiert durch die Displaylänge

Dabei wird der Wertebereich automatisch eingeordnet. Die X-Achse startet mit dem ersten zeitlichen Wert, der sich in der ausgelesenen Datei befindet. Der letzte Wert muss nicht zwingend der letzte Wert der ausgelesenen Datei sein, weil bei mehr als 255 Werte nur jeder Xte Wert genommen wird.

Mit der F2-Taste lässt sich die Legende anzeigen. Sie beinhaltet den Wertebereich, sowie das Minimum und Maximum der Grafik. Beim erneuten Drücken der F2-Taste verschwindet die Legende wieder.



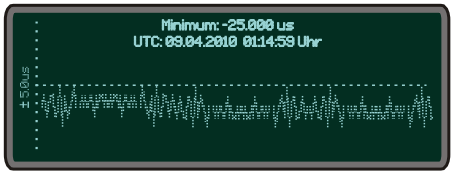
Beim Drücken der F1-Infotaste in dem „FULL GRAPHIC MODE“ wird das Hilfe-Menü aufgerufen. Es zeigt alle wählbaren Optionen in dem Modus. Von hier aus sind die Optionen teilweise wählbar. Um diese Funktion zu beenden, muss die ESC- Taste, OK-Taste oder erneut die F2 gedrückt werden.

In dem „FULL GRAPHIC MODE“ wird der Graph durch die Tasten ↑ (zoom in) und ↓ (zoom out) vergrößert bzw. verkleinert. Wird die Legende angezeigt, so wird beim Drücken der Zoom-Tasten die Y-Achse des Wertebereichs in den vordefinierten Schritten verändert und anschließend die Legende erneut angezeigt. Mit der ESC-Taste gelangt man zurück zum Hauptmenü des grafischen Programms, wenn die Legende nicht angezeigt wird. Andernfalls wird zum „FULL GRAPHIC MODE“ mit standardmäßigem Wertebereich zurückgesprungen.

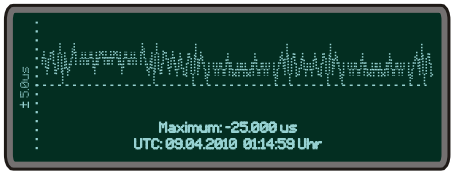
Die nächste Option in dem grafischen Menü ist die „Statistic“ - Option. Wählen Sie diese aus und bestimmen Sie ob Sie sich das Minimum oder Maximum der aktuellen Statistik-Datei anzeigen lassen möchten.

Nun wird das Minimum oder Maximum jeweils in der Displaymitte dargestellt, solange es mindestens 128 Werte (halbe Displaylänge) gibt. Zugleich wird eine Legende angezeigt, die neben dem Minimum bzw. Maximum auch den dazugehörigen UTC-Zeitpunkt [5] anzeigt.

Darstellung des Minimum incl. der Legende



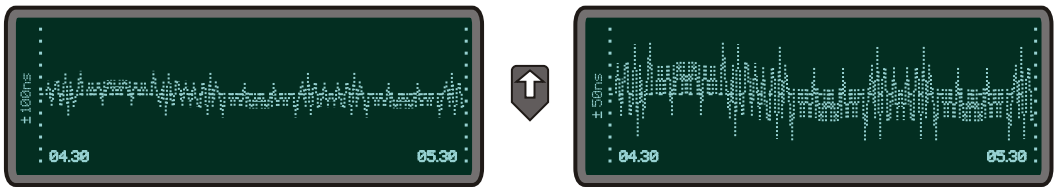
Darstellung des Maximum incl. der Legende



Der letzte Modus in dem Grafik Menü ist der „SCROLLING MODE“
Nach der Statusanzeige werden die gesamten vorhandenen Offsets gescrollt gezeichnet. Die Tasten ↑ oder ↓ verweisen im „SCROLLING MODE“ auf dessen vergrößerte bzw. verkleinerte Y-Achse des Wertebereichs. Hierbei startet der „SCROLLING MODE“ erneut von Anfang an. Mit den Tasten OK oder ← wird die Grafik angehalten. Optional lässt sich die Grafik jederzeit mit den Tasten OK oder → weiter scrollen. Wenn der Modus gestoppt ist (der Wertebereich wird angezeigt), wird mit den Tasten ↑ (vergrößert) und ↓ (verkleinert) die Y-Achse

[5] UTC: Universal Time Coordinated ist die einheitliche Weltzeit – diese kennt keine Sommer oder Winterzeitumstellung

des Wertebereichs in dem dargestellten Abschnitt verändert. Es wird nur bis zum Displayende gezeichnet und erst weiter gescrollt, wenn die Taste OK oder → gedrückt werden.



Mit der Taste ← wird die dargestellte Grafik um ein halbes Display nach links verschoben, wenn zuvor der SCROLLING MODE gestoppt wurde. Auch hier kann die Y-Achse des Wertebereichs verändert oder die Grafik um weitere Schritte nach links verschoben werden. Um das Scrollen fortzusetzen muss die Taste OK oder → gedrückt werden. Drücken Sie die ESC-Taste, und Sie gelangen zum Hauptmenü des graphischen Programms zurück.

13.2.2 Hauptmenü Front-Display

Das Hauptmenü wird angezeigt, wenn nach Einschalten des Geräts die Initialisierungsphase abgeschlossen ist. Über das Tastenfeld mit den 4 Pfeilen und den Tasten „OK“, „ESC“, „F1“ und „F2“ kann in der Anzeige durch die einzelnen Menüs navigiert werden. Das Hauptmenü kann immer durch längeres Drücken der „ESC“ Taste erreicht werden. Im Hauptmenü werden die wichtigsten Statusinformationen des Gerätes angezeigt. In der obersten Zeile wird die Betriebsart der Referenzuhr/Referenzzeit angezeigt:

Statt „NORMAL OPERATION“ kann auch „NOT SYNC“ erscheinen. Wenn eine verwendete Antennenleitung unterbrochen ist, kommt hier die Meldung „ANTENNA FAULTY“. Bei einem verwendeten Time Code Empfänger erscheint ggf. die Nachricht „NO DATA“ - in diesem Fall muss im Time-Code Parameter Menü der korrekte Wert eingestellt werden.

Mittels der mehrfarbigen LEDs werden Zustände des Zeitserver angezeigt:

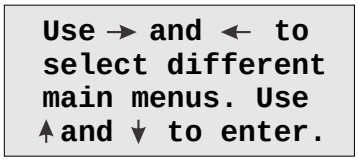
„Ref. Time“
grün: die Referenzuhr (z.B. eingebaute GPS, WWVB oder PZF) liefert eine gültige Zeit.
rot: die Referenzuhr liefert keine gültige Zeit (z.B. nicht synchron)

„Time Service“
grün: NTP ist synchron zur Referenzuhr (z.B. eingebaute GPS, WWVB oder PZF).
rot: NTP ist nicht synchron oder auf die „local clock“ geschaltet

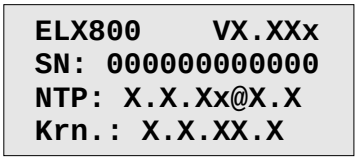
„Network“
grün: alle überwachten Netzwerkanschlüsse sind angeschlossen (Link up)
rot: mindestens einer der überwachten Netzwerkanschlüsse (siehe „Setup Device Parameter / Check Network Linkup“) ist nicht angeschlossen (kein Link)

„Alarm“
aus: kein Fehler
rot: allgemeiner Fehler – weitere Informationen auf dem Display.

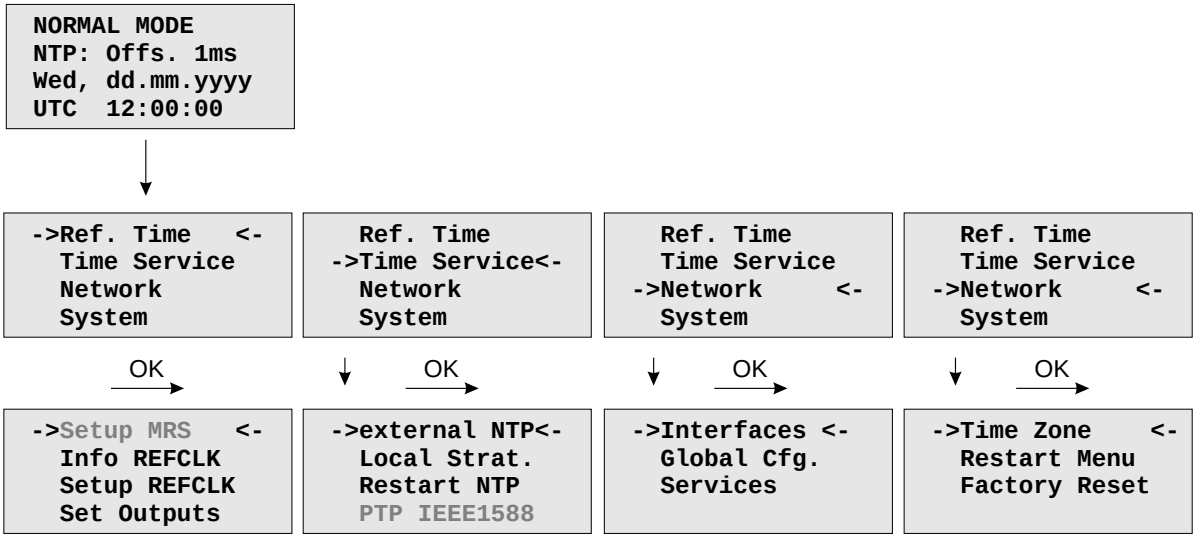
Wenn in der oberen rechten Ecke der Anzeige ein Symbol „F1“ angezeigt wird, kann mit der „F1“ Taste eine Seite mit zusätzlichen Informationen aktiviert werden. Mit „F1“ aus dem Hauptmenü wird eine kurze Beschreibung zur Navigation mit den Tasten durch die Menüs angezeigt.



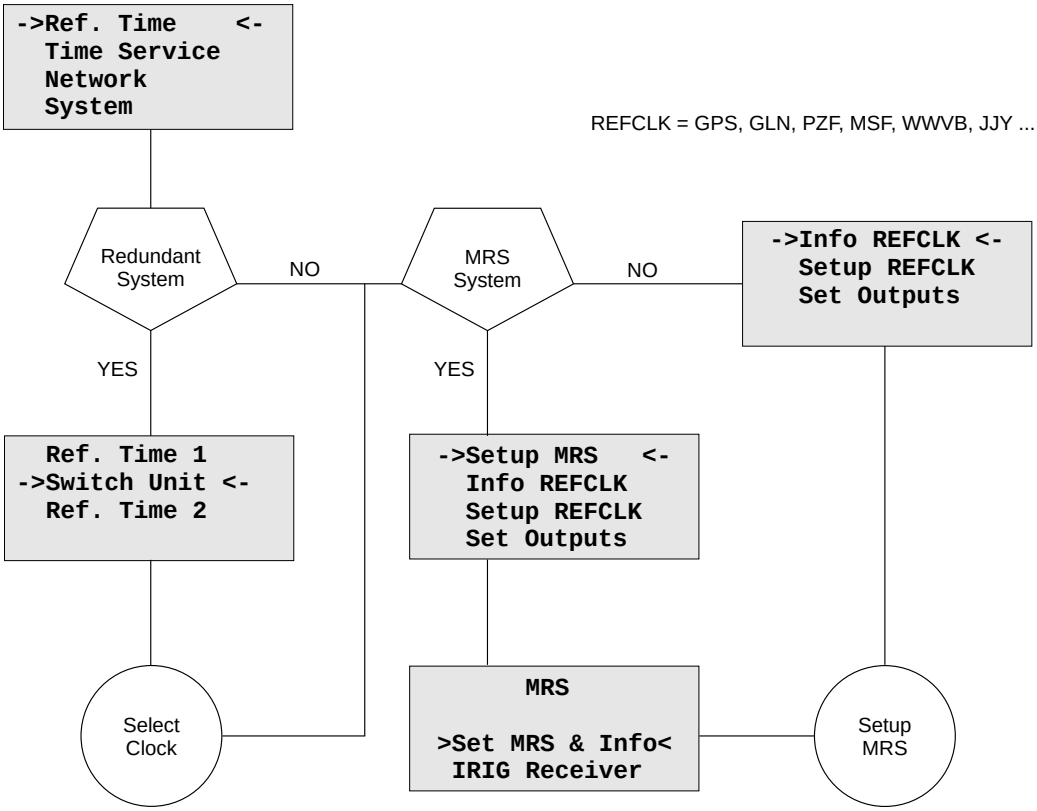
Durch Drücken der „OK“ Taste im Hauptmenü wird eine Seite mit den Software Versionen für den LANTIME, NTP und das Betriebssystem angezeigt.



Mit den Richtungstasten kann durch die einzelnen Hauptmenüs navigiert werden. Folgende Hauptmenüs stehen zur Verfügung:

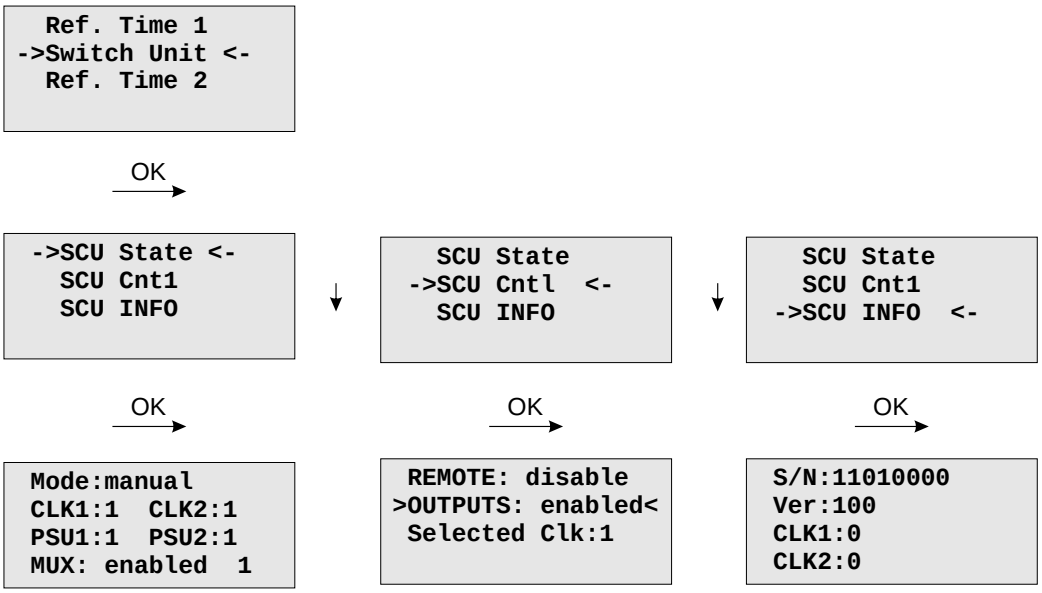


13.2.3 Menü: Reference Time



Mit der „OK“ Taste werden die Untermenüs geöffnet. Alle Statusinformationen und Einstellungen zur Referenzuhr werden über dieses Menü vorgenommen.

13.2.3.1 Optionales Menü Switch Unit



Mit diesem Menü können alle wichtigen Statusinformationen zur SCU abgefragt werden. Das Beispiel oben zeigt, dass beide Netzteile (PSU1 und PSU2) sowie beide Uhren (CLK1 und CLK2) im Betriebsmodus sind. Sollte zum Beispiel die CLK2 abgeschaltet sein oder sich im Freilauf befinden, dann wäre die Anzeige **CLK2:0** auf dem Display sichtbar. Ist das Netzteil 1 nicht an die Stromversorgung angeschlossen oder ist diese ausgefallen erscheint die Anzeige **PSU1:0** im Display des LANTIME.

Über das Untermenü **SCU Cntl** lassen sich die folgenden Einstellungen vornehmen:

REMOTE: disabled/enabled
mit diesem Parameter lässt sich der Fernzugriff via TELNET oder SSH (Putty) steuern

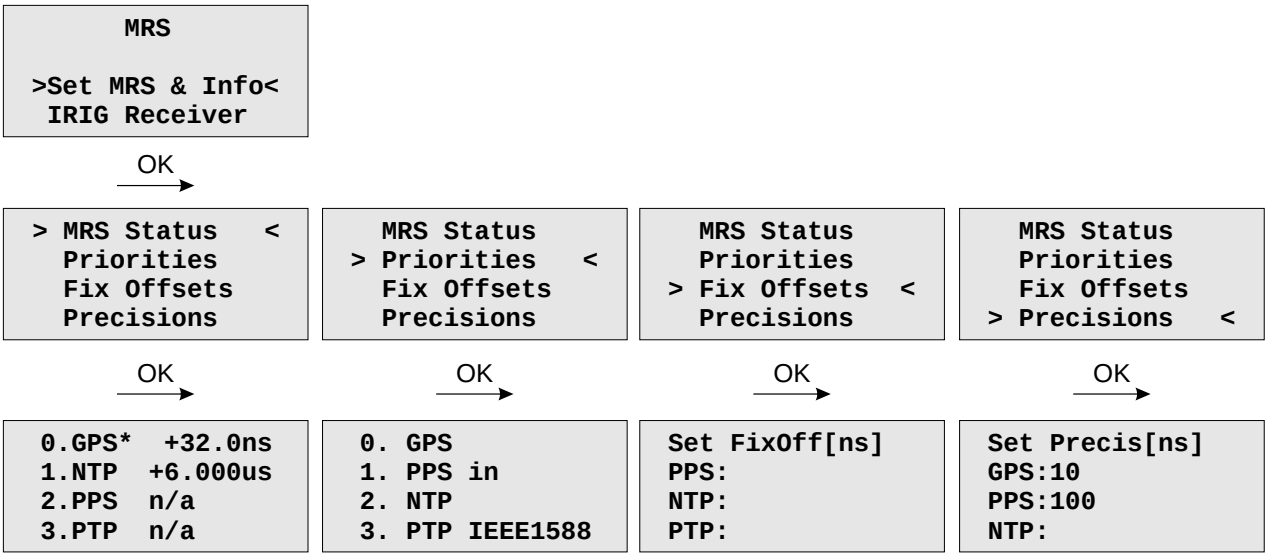
OUTPUTS: enabled/disabled
die Ausgänge der SCU werden aus- bzw. eingeschaltet

Selected Clk: Clk:1, Clk:2
die Referenzuhr kann hier über die Funktionstasten oder einem entfernten Computer ausgewählt werden - Vorraussetzung ist, der mechanische Schalter an der SCU muss sich in der Position „Auto“ befinden. In der Position „Manual“ ist das Umschalten der Uhr ausschließlich über den Schalter an der SCU möglich.

13.2.3.2 Optionales Menü Setup MRS

Mit diesem Menü können alle Parameter, für die zur Verfügung stehenden Eingangssignale, angezeigt und eingestellt werden.

Mögliche Referenzen sind:
- GPS
- PPS Pulse Per Second
- FRQ Frequenz - Standard 10MHz
- IRIG Time Code (AM, DCLS)
- PTP IEEE 1588 Grandmaster (M400, M600, M900)
- NTP - externe NTP Zeitserver



Mit dem Untermenü MRS Status werden die Offsets und die Verfügbarkeit der Referenzsignale angezeigt (n/a = nicht verfügbar):

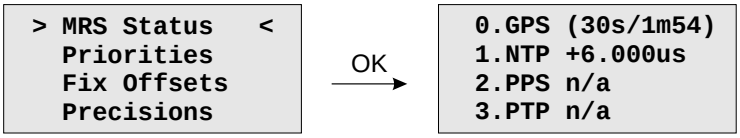
Die Prioritäten für die Referenzsignale, d.h., welche Referenz im Falle eines Ausfalls eines anderen Eingangssignals zur Steuerung des internen Oszillators verwendet werden soll, kann in dem nächsten Untermenü eingestellt werden:

Hier im Beispiel wird zuerst auf die GPS Uhr zugegriffen, danach auf das PPS Signal dann auf die NTP Zeit externer Zeitserver und zuletzt auf die PTP Nachrichten vom eingesetzten Grandmaster.

Der „Fixed Offset“ gibt für jede Referenzuhr einen festen Offset zur Referenzzeit an. Hiermit können bekannte und konstante Abweichungen einer Referenzzeitquelle kompensiert werden. Mit den Pfeil- und der OK Taste kann die Zeit für die einzelnen Referenzen eingestellt werden. Für die GPS Referenz kann kein konstanter Offset eingestellt werden – dies kann nur indirekt über die Antennenlänge gemacht werden.

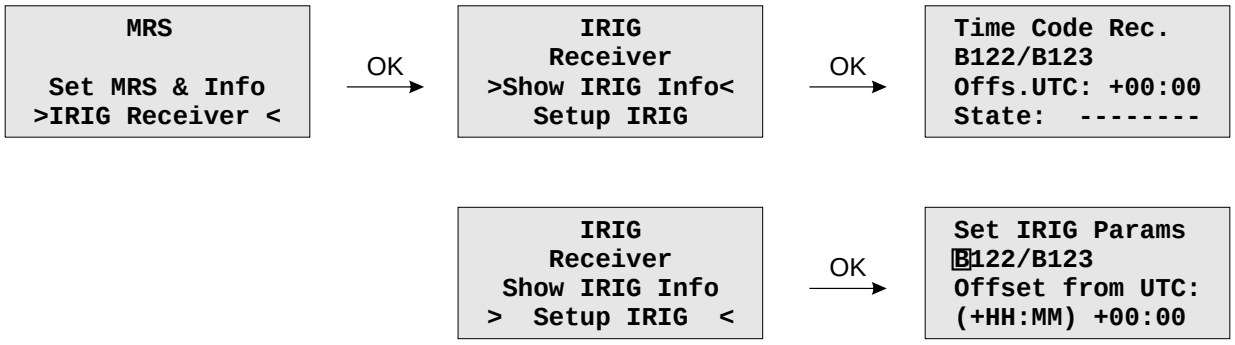
Die „Precison“ gibt die Genauigkeit einer Referenzquelle an. Anhand dieser Genauigkeit werden die Umschaltzeiten zwischen den einzelnen Referenzen berechnet. Die Umschaltzeit ist die Verzögerung (Holdover Time) wenn bei einem Ausfall des aktuellen Masters auf eine andere Referenzquelle umgeschaltet werden soll. Bei einem „Precision“ Wert von Null wird sofort auf die nächste Referenzuhr in der Reihenfolge (Priorität) umgeschaltet. Ansonsten wird die Verzögerung nach der Formel „(new_precision / old_precision) * const))“ berechnet.

Beispiel:
Wenn z.B. der GPS Receiver der aktuelle Master ist und gerade ausfällt wird auf PPS als Referenz weitergeschaltet, wenn dieses Signal verfügbar ist. Der GPS Empfänger hat eine eingestellte Genauigkeit von 10ns und PPS von 100ns. Intern wird nach der Formel (100ns / 10ns * 11.4) eine Verzögerung von 114 Sekunden berechnet. In der Online Darstellung „MRS Status“ wird die noch verbleibende- und die Gesamt- Wartezeit hinter dem Master angezeigt, falls von einer höheren Priorität auf eine potentiell ungenauere Quelle umgeschaltet wird. Sollte die GPS innerhalb dieser Zeit wieder ein Signal empfangen, wird der Umschaltvorgang nicht ausgeführt.

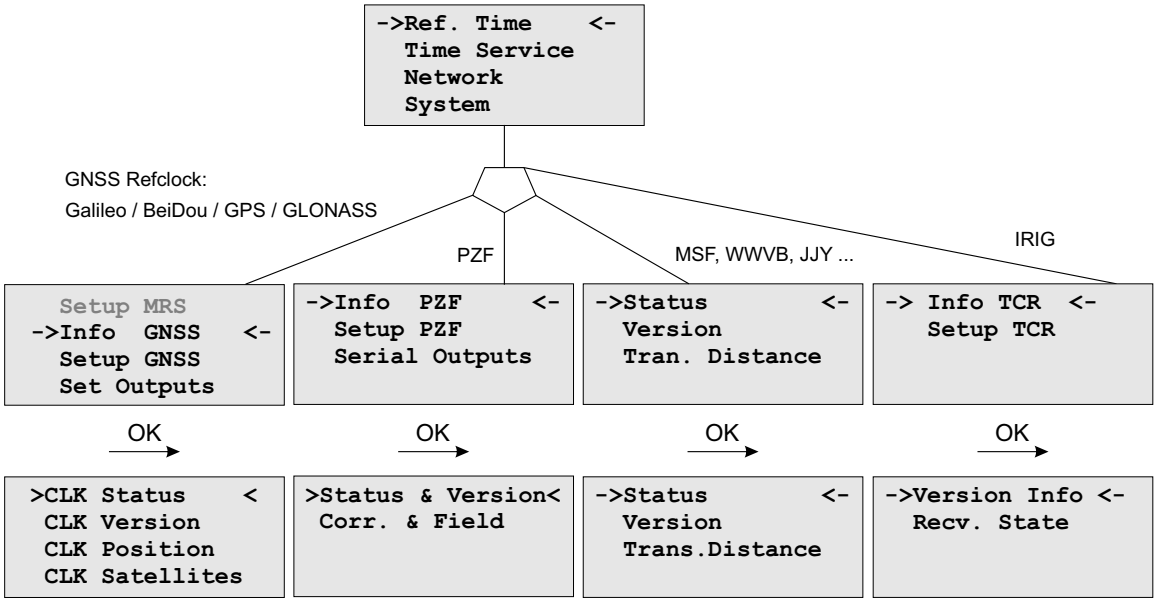


13.2.3.3 Optionales Menü Setup MRS - Time Code Receiver

Mit diesem Menü können die Parameter für die Zeitcode-Eingangssignale angezeigt und eingestellt werden.



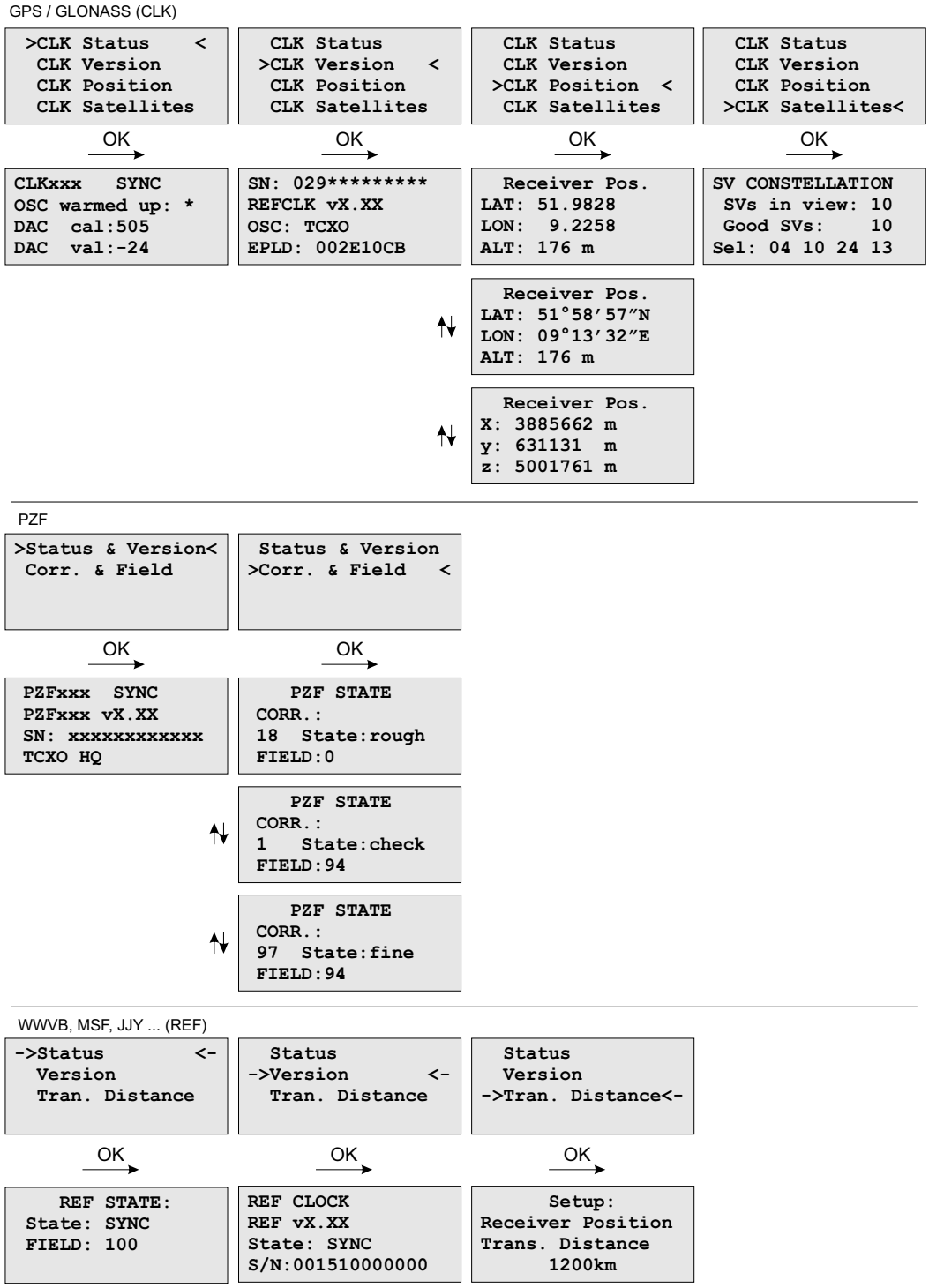
13.2.3.4 Menü: Info Receiver



In diesem Menü werden alle wichtigen Informationen zur verwendeten Referenzuhr, des internen Oszillators und im Falle eines GPS oder GLONASS Empfängers, die sichtbaren und gut zu empfangenden Satelliten angezeigt.

13.2.3.5 Empfänger Status und Version

Alle Statusinformationen zur Referenzuhr werden über dieses Menü angezeigt.

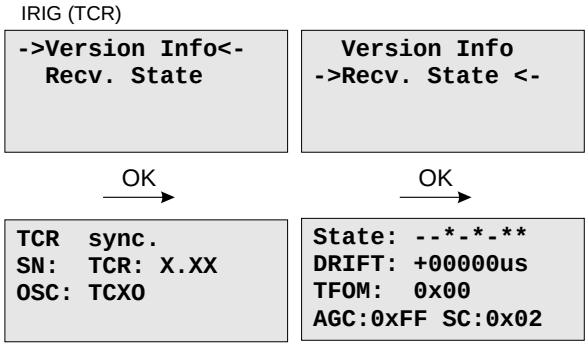


Der Typ der eingesetzten Referenzuhr wird mit dem aktuellen Status des Empfängers angezeigt. Darunter stehen die Versionsnummer der Firmware, die Seriennummer der Referenzuhr und der eingebaute Type des Oscillators.

13.2.3.6 Menü: IRIG Receiver Status

Unter diesem Punkt wird der Status der IRIG-Decodierung zur Anzeige gebracht. In der ersten Zeile wird der Systemstatus mit den 8 Zuständen wie unten beschrieben angezeigt. Ein '*'steht für aktiviert und ein '-'steht für ausgeschaltet. In der zweiten Zeile wird die Drift des internen Oszillators angezeigt. In der dritten Zeile wird der TFOM Wert (Time Figure of Merit: die Qualität des IRIG Signals, welche aber nur bei IEEE 1344 benutzt wird) ausgegeben und in der vierten Zeile wird der AGC Wert (Automatic Gain Control), also die Verstärkung

des Eingangsignals, als hexadezimaler Wert angezeigt.



IRIG System Status: Bit 7 ... 0
Bit 7: Ungültige UTC Parameter
Bit 6: TCAP zu groß, Jitter außerhalb des Wertebereiches
Bit 5: Lock an
Bit 4: Telegramm Fehler
Bit 3: Daten vorhanden
Bit 2: Ungültige Systemkonfiguration
Bit 1: Pulse eingeschaltet
Bit 0: Warmed up

Ungültige UTC Parameter: Dieses Bit ist auf eins gesetzt, wenn die Checksumme der „Offset from UTC" Parameter ungültig sind, (bei der Erweiterung IEEE 1344 möglich). Der Anwender muss einen neuen „Offset from UTC" eingeben, um dieses Bit zu löschen. Zu beachten ist, dass der IRIG-Empfänger den Freilauf Zustand verlassen wird, wenn IEEE 1344 abgeschaltet und die UTC Parameter ungültig sind.

TCAP zu groß: Wenn der Jitter zwischen zwei aufeinander folgenden IRIG-Telegramme größer als +/- 100 μs ist, schaltet der Empfänger in den Freilauf und das TCAP Bit wird gesetzt. Dieses Bit wird zurück gesetzt wenn der Jitter unter +/- 100μs geht.

Lock: Das Lock Bit wird gesetzt, wenn der Empfänger synchronisiert hat und die interne Oszillator - Korrektur eingeschwungen ist.

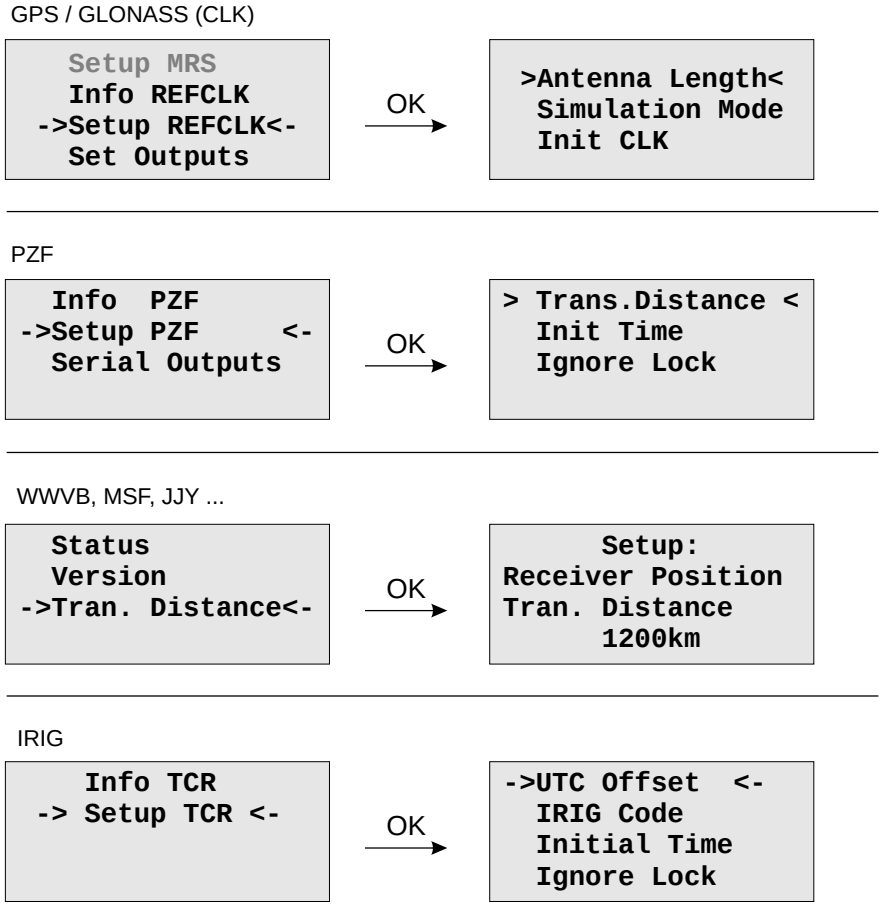
Telegramm Fehler: Dieses Bit wird gesetzt wenn zwei aufeinander folgende IRIG-Telegramme nicht konsistent sind. Der IRIG-Empfänger geht dann in den Freilauf.

Daten vorhanden: Wenn der IRIG-Empfänger den Zeitcode des Eingangssignals lesen kann.

Ungültige Systemkonfiguration: Dieses Bit wird gesetzt wenn die Checksumme der Systemkonfiguration ungültig ist. In diesem Fall wird der IEEE 1344 Modus abgeschaltet. Der Anwender muss das System neu starten oder eine neue Systemkonfiguration bei den IRIG-Parametern eingeben.

IRIG Systemkonfiguration Bit 2 ... 0
Bit 7 ... 4: Reserviert
Bit 3: Ignoriere Tag des Jahres
Bit 2: Ignoriere TFOM
Bit 1: Ignoriere SYNC
Bit 0: IEEE 1344 aktiv

13.2.3.7 Menü: Setup Meinberg Receiver



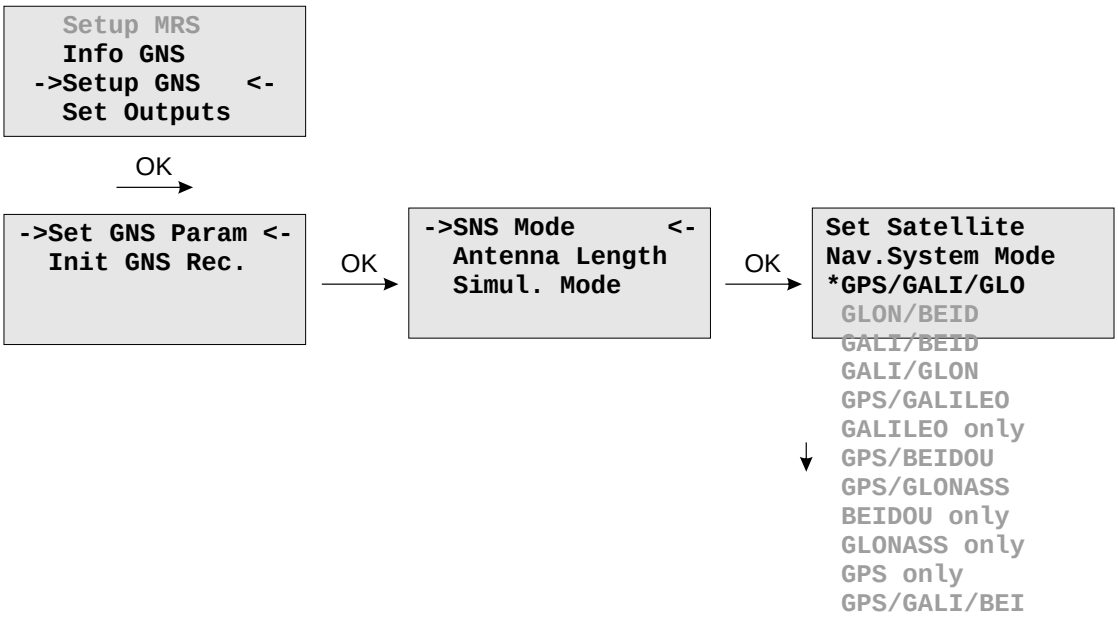
Im Menü Reference *Time -> Setup Clock* können alle relevanten Einstellungen des internen Empfängers vorgenommen werden. Bei satellitengestützen Systemen kann unter anderem die Antennenkabellänge eingetragen werden. Außerdem können die GPS und GLONASS Empfänger im Simulationsmodus betrieben werden.

Meinberg PZF Korrelationsempfänger könnnen über *Ignore Lock* ebenfalls im Simulationsmodus laufen. Zusätzlich muss in dem Setup Menü auch noch die Entfernung zum Sender eingestellt werden.

Für die Langwellenempfänger gibt es nur die Einstellung für „Transmitter Distance", diese ist im Menü **Info Refclock** verfügbar. Das Setup für unsere IRIG Zeitcode - Empfänger umfasst die Einstellungen für den UTC Offset und den entsprechenden Time Code. Die Zeitcodeempfänger können über Ignore Lock ebenfalls im Simulationsmodus betrieben werden. Über Initial Time bzw. Init Clock (GPS, GLONASS) wird die Zeit und das Datum für den Simulationsmodus gesetzt.

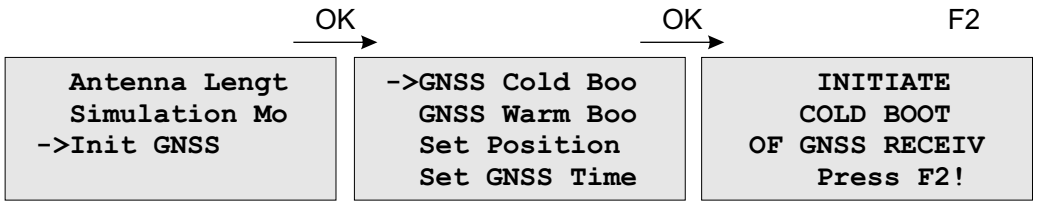
13.2.3.8 Setup Satelliten-Navigationssystem - SNS-Modus

Wenn Sie einen GNS-Empfänger (GNS oder GNS-UC mit Up-Converter) verwenden, dann können Sie mit diesem Drop-Down-Menü eins oder auch mehrere Satellitensysteme auswählen, die dann gleichzeitig verwendet werden. Folgende Kombinationen sind verfügbar:



13.2.3.9 Initiate Cold Boot

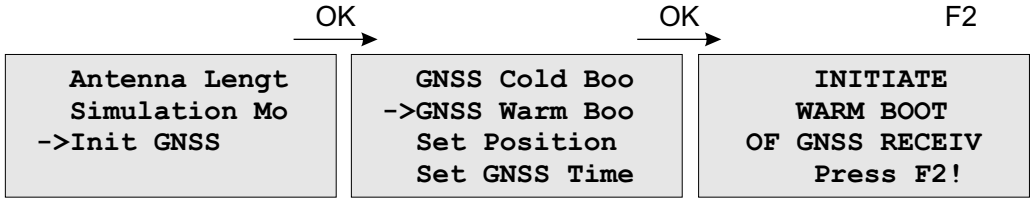
Dieses Menü erlaubt es dem Benutzer alle GNSS-Systemwerte zu initialisieren, d.h. alle gespeicherten Satellitendaten werden gelöscht. Bevor die Initialisierung erfolgt, wird nochmals eine Bestätigung des Bedieners erwartet. Anschließend geht das System in die Betriebsart COLD BOOT, um nach einem Satelliten zu suchen und von diesem die aktuellen Parameter einzulesen.



13.2.3.10 Initiate Warm Boot

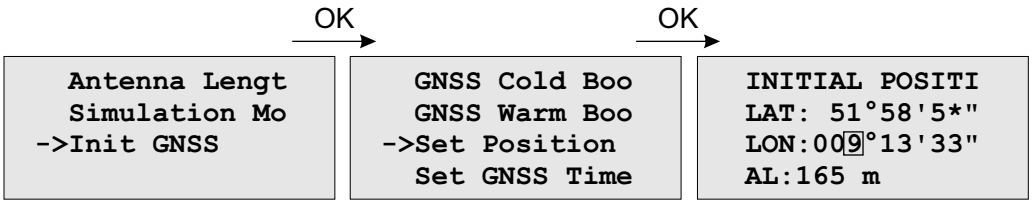
Dieses Menü erlaubt es dem Benutzer, den Empfänger in den **Warm Boot** Modus zu schalten. Das kann erforderlich sein, wenn die Satellitendaten im batteriegepufferten Speicher zu alt sind oder wenn das Gerät an einem Ort in Betrieb genommen wird, der mehrere hundert Kilometer vom letzten Betriebsstandort entfernt ist, da dann die Berechnung der Sichtbarkeit der Satelliten falsche Ergebnisse liefert.

Wenn der Benutzer in einem solchen Fall manuell in den **Warm Boot** Modus schaltet, kann die Zeitspanne bis zur Synchronisation wesentlich verringert werden, obwohl der Empfänger dieses nach einer Weile selbst tun würde, wenn keine Satelliten empfangen werden können. Nach Bestätigung der Auswahl geht das Gerät in die Betriebsart **Warm Boot**, wenn sich noch gültige Satellitendaten im Speicher befinden, ansonsten werden diese im **Cold Boot** neu eingelesen.



13.2.3.11 Init Receiver Position

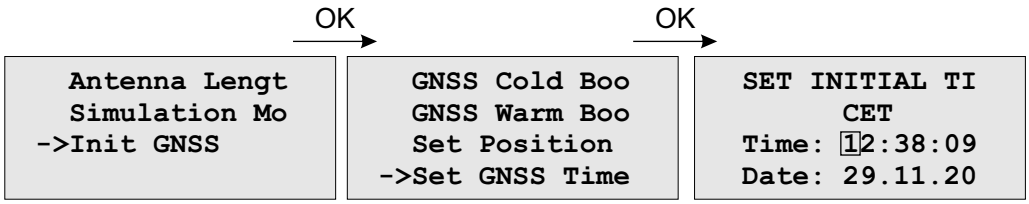
Wenn der Empfänger zum ersten Mal an einem neuen Standort in Betrieb genommen wird, der weit vom letzten Standort entfernt ist, muss der GNSS Empfänger im Warm Boot nach Satelliten suchen, da die berechneten Werte für Elevation und Doppler zu sehr von den tatsächlichen abweichen. Durch Eingabe der ungefähren neuen Position kann dies vermieden werden, wodurch die Zeit bis zur Synchronisation verkürzt wird.



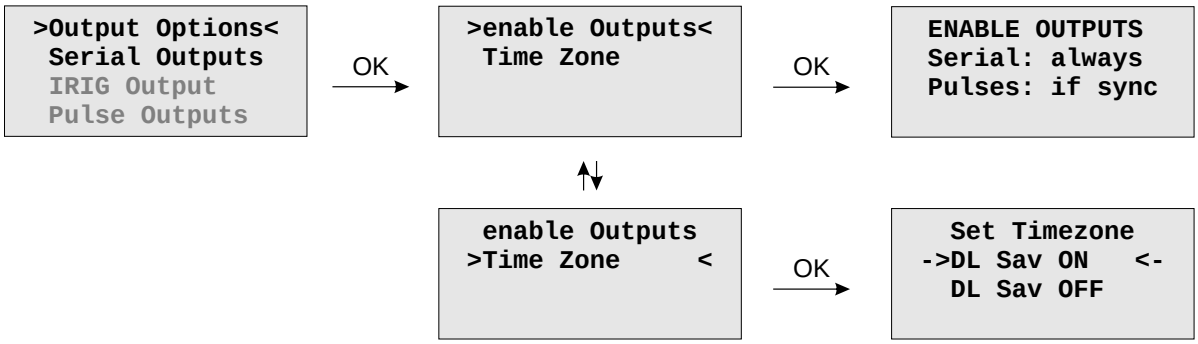
13.2.3.12 Init Receiver Time

Wenn die Hardware-Uhr des Systems falsch geht, berechnet der Empfänger ungültige Werte für Elevation und Doppler und muss im Warm Boot nach Satelliten suchen. Durch Eingabe der richtigen Zeit kann dies vermieden werden, wodurch die Zeit bis zur Synchronisation verkürzt wird.

Wenn das System ohne Antenne betrieben wird, können zu Testzwecken auch andere Zeiten eingestellt werden. Dabei ist zu beachten, dass zum einen der NTPD sich nicht mehr auf die GNSS Referenzuhr synchronisiert, wenn diese keinen Empfang hat und zum anderen sich der NTP automatisch beendet, wenn die Abweichung zwischen Systemzeit und Referenzuhr größer als 1024 Sekunden ist. Für einen solchen Test sollte der Punkt **Simulation Mode** aktiviert sein. Nach dem manuellen Setzen der Zeit wird die Systemzeit des Rechners auch gesetzt und der NTP neu gestartet.



13.2.3.13 Menü: Output Options



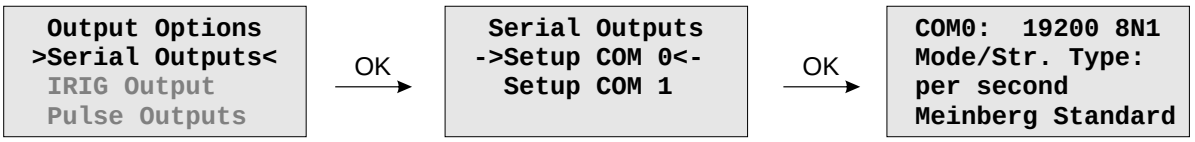
Enable Outputs:
Mit *Output Options -> Enable Outputs* wird festgelegt, zu welchem Zeitpunkt nach dem Einschalten die seriellen Schnittstellen und die Impuls/Frequenzausgänge freigeschaltet werden. Ausgänge, für die der Wert 'always' angezeigt wird, werden immer sofort nach der Initialisierungsphase des Systems freigegeben. Ausgänge, für die 'if sync' angezeigt wird, werden erst freigegeben, wenn die Systemzeit anhand der Satellitensignale überprüft und korrigiert wurde. Standardwert für alle Ausgänge ist 'if sync'.

Time Zone:
Siehe Kapitel „Set Time Zone of Serial Outputs".

13.2.3.14 Menü: Serial Outputs

Mit Hilfe dieses Untermenüs können Übertragungsgeschwindigkeit und Datenformat der seriellen Schnittstelle eingestellt werden. Standardwerte sind:

Baudrate:	300 bis 19200
Datenformat:	7E1, 7E2, 7N2, 7O1, 7O2, 8E1, 8E2, 8N1, 8N2, 8O1



COM0 gibt ein Zeittelegramm sekündlich, minütlich oder auf Anfrage aus. Auf Anfrage bedeutet, dass ein angeschlossener Client ein „?“ senden muss, um als Antwort das Zeittelegramm zu erhalten.

Defaulteinstellung COMx:	Speed	Framing	Mode	Signal Type
	19200 baud	8N1	pro Sekunde	Meinberg Standard

Es kann zwischen folgenden Zeittelegrammen gewählt werden. Die genaue Definition dieser Zeittelegramme ist im Anhang beschrieben.

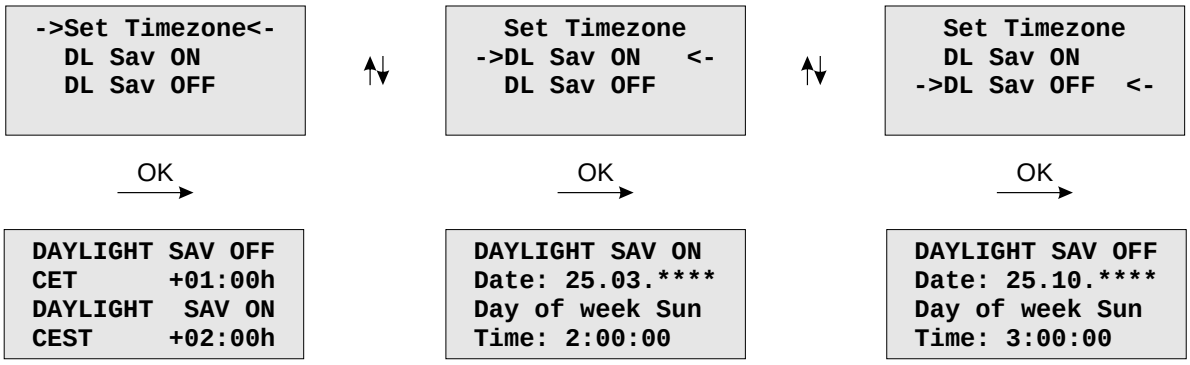
- Meinberg Standard
- SAT
- NMEA RMC (Rev. 2.2)
- Uni Erlangen
- Computime
- Sysplex 1
- Meinberg Capture
- SPA
- RACAL
- Meinberg GPS
- NMEA GGA (Rev. 2.2)
- NMEA RMC GGA (Rev. 2.2)
- NMEA ZDA (Rev. 2.2)
- ION
- 6021
- IRIG-J

13.2.3.15 Setup Output Time Zone

Die Zeitzone der Ausgänge kann entsprechend eingestellt werden. Diese Einstellungen wirken sich auf die seriellen Schnittstellen und die Timecode Ausgänge aus. Die interne Zeit des Zeitservers und die NTP Zeit bezieht sich immer auf UTC und ist unabhängig von diesen Einstellungen der Zeitzone. Die Anzeige im Display wird über ein anderes Menü eingestellt: Hauptmenü: *System->Set Time Zone*.

Im Untermenü *Daylight Saving OFF* werden die Einstellungen für die normale Ortszeit (Winterzeit) vorgenommen. Mit der Auswahl von *Daylight Saving ON* wird die lokale Sommerzeit konfiguriert.

Beispiel:
CET = UTC + 1h und CEST = UTC + 2h



In den Untermenüs *Daylight Saving ON* und *Daylight Saving OFF* gelangt man zu den Einstellmöglichkeiten der Sommer- bzw. Winterzeit. Die editierbaren Zeilen dienen der Eingabe der Umschaltzeitpunkte, in dem die Sommer buw. Winterzeit aktiviert werden. Unsere Funkuhren bieten zwei Möglichkeiten zur Eingabe von Sommer-/Winterzeit: Entweder werden Datum und Uhrzeit der Umschaltpunkte für ein Jahr exakt definiert oder es werden Randbedingungen gesetzt, mit deren Hilfe das Gerät automatisch für mehrere Jahre den Tag der Umschaltung bestimmen kann. Die Abbildungen zeigen den automatischen Modus: Wird die Jahreszahl als '****' angezeigt, muss ein Wochentag eingegeben werden; dann ist der Tag der Umschaltung der erste Tag ab dem eingegebenen Datum, der mit dem eingegebenen Wochentag übereinstimmt. In der Abbildung unten ist z.B. der 25.10. ein Samstag, am darauf folgenden Sonntag, den 26.10., zur angegebenen Uhrzeit *TIME*, findet die Umschaltung auf Winterzeit statt.

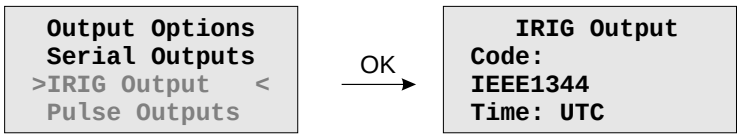
Die mitteleuropäische Sommerzeit wird jeweils an einem Sonntag beginnen und enden:

- Daylight Saving ON: Die Zeitumstellung auf Sommerzeit (CEST) findet am letzten Sonntag im März statt - Time = 2:00:00
- Daylight Saving OFF: Die Zeitumstellung auf Normalzeit (CET) findet am letzten Sonntag im Oktober statt - Time = 2:00:00

Für den Fall, dass keine Sommerzeitumstellung benötigt wird, sind unter beiden Menüpunkten (Daylight Saving ON / OFF) beliebige aber exakt gleiche Daten, Zeiten und Offsets zu setzen. Nach Eingabe dieser Werte sollte ein Restart des Gerätes erfolgen.

13.2.3.16 Menü: Setup Time Code

Der IRIG Time Code ist ein optionaler Ausgang.



In diesem Untermenü können die generierten Zeitcodes der Referenzuhr eingestellt werden. Die meisten Time-Codes beinhalten keine Zeitzoneninformation, somit wird standardmäßig UTC ausgegeben. Auf Wunsch kann durch Auswahl „TIME: Local“ die eingestellte Zeitzone der Uhr ausgegeben werden.

Folgende Codes können ausgewählt werden:

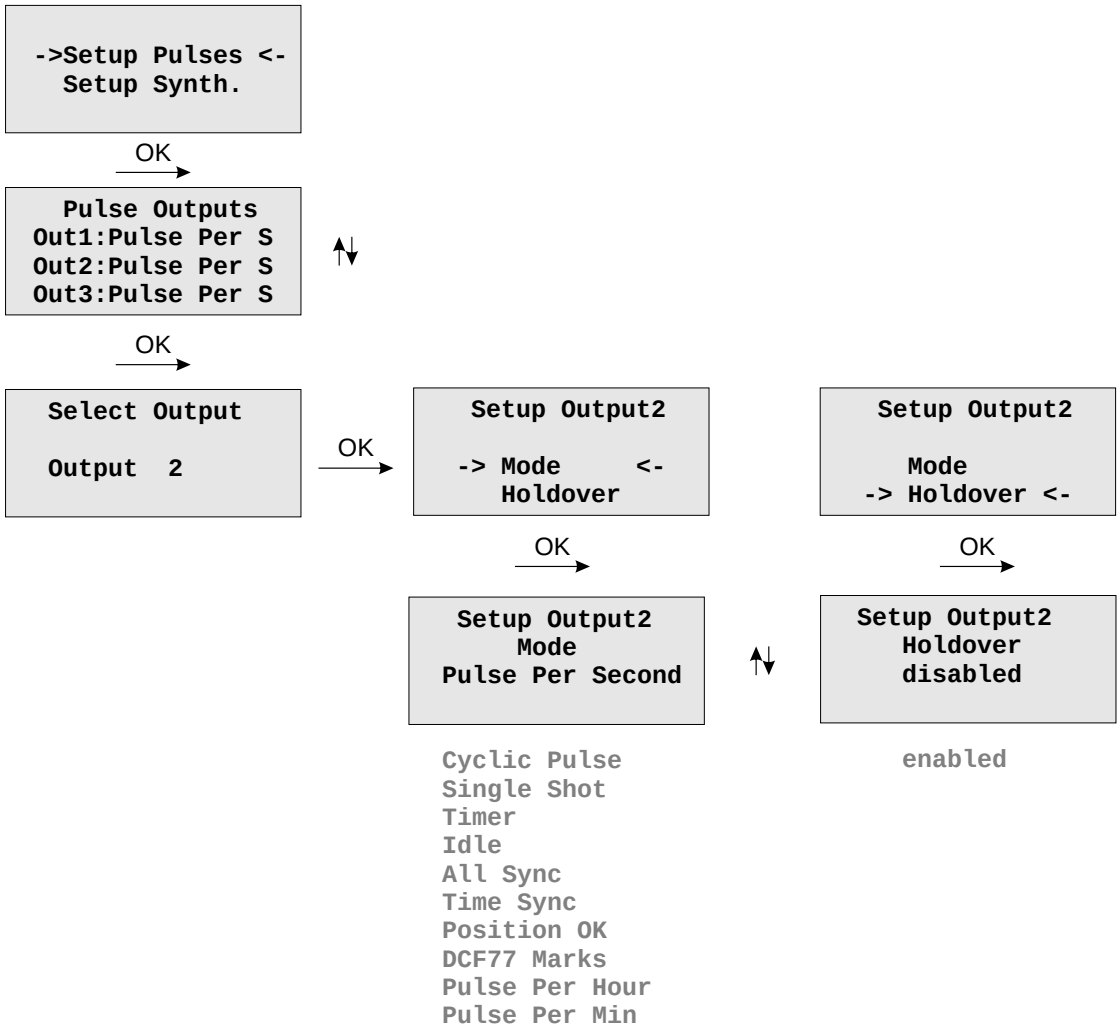
- IRIG B002+B122
- IRIG B006+B126
- IRIG B007+B127
- AFNOR NF S87-500
- C37.M8
- IEEE1344

Weitere Informationen zum IRIG-Zeitcode finden Sie im Anhang.

13.2.3.17 Option: Menü Setup Progr. Pulses

Stellt die angeschlossene Funkuhr programmierbare Impuls/Schaltausgänge zur Verfügung, so können deren Einstellungen hier verändert werden. Der Menüpunkt erscheint nicht im Menü Outputs, wenn von der angeschlossenen Funkuhr keine programmierbaren Ausgänge zur Verfügung gestellt werden.

Im Untermenü „Mode“ wird der Betriebsmodus des jeweiligen Ausgangs festgelegt. Verfügbare Betriebsmodi sind:
Timer, Single Shot, Cyclic Pulse, Pulse Per Second, Pulse Per Min, Pulse Per Hour, DCF77 Marks, Position OK, Time Sync, All Sync und Idle. Je nach gewähltem Modus und Bestätigung durch „OK“ werden unterschiedliche Steuerelemente im Display dargestellt.



Timer Modus
Im Timer Modus simuliert der Ausgang eine Schaltuhr mit Tagesprogramm. Auf jedem Ausgang der Funkuhr sind je drei Ein- und drei Ausschaltzeiten am Tag programmierbar. Soll eine Schaltzeit programmiert werden, so muss die Einschaltzeit „On“ und die zugehörige Ausschaltzeit „OFF“ eingetragen werden. Liegt der Einschaltzeitpunkt später als der Ausschaltzeitpunkt, so wird das Schaltprogramm derart interpretiert, dass der Auschaltzeitpunkt am darauffolgenden Tag liegt.

Ein Programm On Time 23.45.00, Off Time 0.30.00 würde demnach bewirken, dass am Tag n um 23.45 Uhr der Ausgang z.B. PORT1 aktiviert, und am Tag n+1 um 0.30 Uhr deaktiviert wird. Sollen eines oder mehrere der drei Programme ungenutzt bleiben, so müssen in die Felder On und Off nur gleiche Schaltzeiten eingetragen werden. Mit „active“ wird der Aktiv Zustand für die Schaltzeiten angegeben. Ist „active: high“ angewählt, liegt am entsprechenden Ausgang im inaktiven Zustand (außerhalb einer Schaltzeit) ein low - Pegel, und im aktiven Zustand ein high - Pegel an.

Cyclic Pulse - Erzeugung zyklisch wiederholter Impulse
Im Modus Cycle wird die Zeit zwischen zwei Impulsen eingegeben. Diese Zykluszeit muss immer in Stunden,

Minuten und Sekunden eingegeben werden. Zu beachten ist, dass die Impulsfolge immer mit dem Übergang 0.00.00 Uhr Ortszeit synchronisiert wird. Dies bedeutet, dass der erste Impuls an einem Tag immer um Mitternacht ausgegeben wird, und ab hier mit der gewählten Zykluszeit wiederholt wird. Eine Zykluszeit von 2sek würde also Impulse um 0.00.00Uhr, 0.00.02 Uhr, 0.00.04 Uhr etc. hervorrufen. Grundsätzlich ist es möglich jede beliebige Zykluszeit zwischen 0 und 24 Stunden einzustellen, jedoch machen meistens nur Impulszyklen Sinn, die immer gleiche zeitliche Abstände zwischen zwei Impulsen ergeben. So würden zum Beispiel bei einer Zykluszeit von 1Stunde 45min Impulse im Abstand von 6300 Sekunden ausgegeben. Zwischen dem letzten Impuls eines Tages und dem 0.00Uhr Impuls würden jedoch nur 4500 Sekunden liegen.

DCF77 Marks
Im Betriebsmodus DCF77 Marks wird der gewählte Ausgang in den DCF77 Simulationsmodus geschaltet, der Ausgang wird im Takt der für den DCF77 Code typischen 100 und 200 ms Impulse (logisch 0/1) aktiviert.

Im Feld 'Timeout' kann eingegeben werden, nach wieviel Minuten im Falle eines Freilaufes der Funkuhr der DCF-Simulationsausgang abgeschaltet werden soll. Wird hier der Wert Null eingegeben, ist die Timeout Funktion inaktiv.

Single Shot Modus
Der Single Shot Modus erzeugt pro Tag einen einmaligen Impuls definierter Länge.
Im Feld Time wird die Uhrzeit eingegeben, zu der ein Impuls erzeugt werden soll. Der Wert „Length" erlaubt die Einstellung der Impulslänge in 10ms Schritten zwischen 10ms und 10sek. Eingaben, die nicht im 10ms Raster liegen werden abgerundet.

Pulse Per Second, Per Min, Per Hour Modus
Diese Modi erzeugen Impulse definierter Länge pro Sekunde, pro Minute oder pro Stunde. Das angezeigte Menü ist für alle drei Betriebsarten gleich. Der Wert „Length" bestimmt die Impulslänge in 10ms Schritten zwischen 10ms und 10sek.

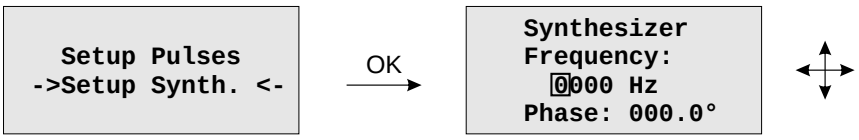
Position OK, Time Sync und All Sync
Zur Ausgabe des Synchronisationsstatus der Funkuhr sind drei verschiedene Modi auswählbar. Im Modus 'Position OK' wird der Ausgang aktiviert, wenn der GPS Empfänger genügend Satelliten empfängt um seine Position zu berechnen.

Der Modus 'Time Sync' aktiviert den Ausgang immer dann, wenn die interne Zeitbasis der Funkuhr mit dem Timing des GPS Systems synchronisiert wurde. Der Modus 'All Sync' führt eine UND Verknüpfung beider Zustände durch, d.H. der entsprechende Ausgang wird immer dann aktiviert, wenn die Position berechnet werden kann UND die interne Zeitbasis synchronisiert wurde.

Idle Modus
Über den Modus 'IDLE' können die programmierbaren Impulsausgänge einzeln deaktiviert werden.

Holdover
In der Betriebsart „enabled" bleibt der Ausgang eingeschaltet, im „disabled" Betrieb wird der Ausgang bei Verlust der Synchronisation abgeschaltet.

13.2.3.18 Option: Synthesizer Frequency Output

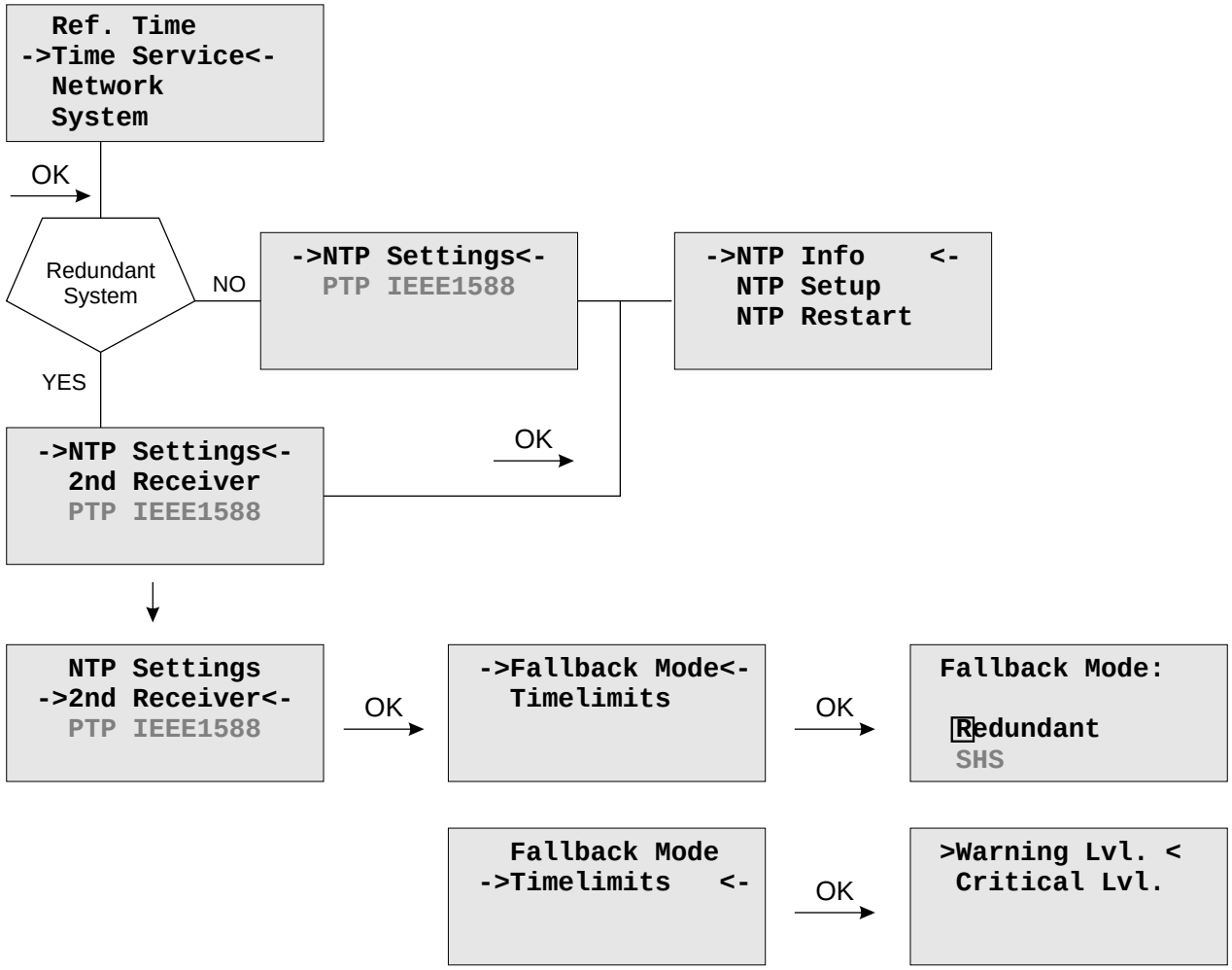


Mit Hilfe dieses Menüs kann die Ausgangsfrequenz und Phase des eingebauten Synthesizers eingestellt werden. Frequenzen von 1/3 Hz bis zu 12 MHz sind durch Eingabe von vier Ziffern und einem Frequenzbereich einstellbar. Der Frequenzbereich wird durch Betätigung der Pfeil-Tasten gewählt, wenn der Cursor auf der Einheit Hz, kHz oder MHz positioniert ist. Wenn der Bereich Hz eingestellt wurde, sind nur die Nachkommastellen 0.0, 0.1 (angezeigt als 1/8), 0.3 (angezeigt als 1/3), 0.5 und 0.6 (angezeigt als 2/3) erlaubt. Bei Einstellung von 1/8, 1/3 oder 2/3 werden echte Bruchteile von Hertz erzeugt, nicht etwa 0.33 Hz oder 0.66 Hz. Durch Eingabe der Frequenz 0 Hz kann der Synthesizer abgeschaltet werden.

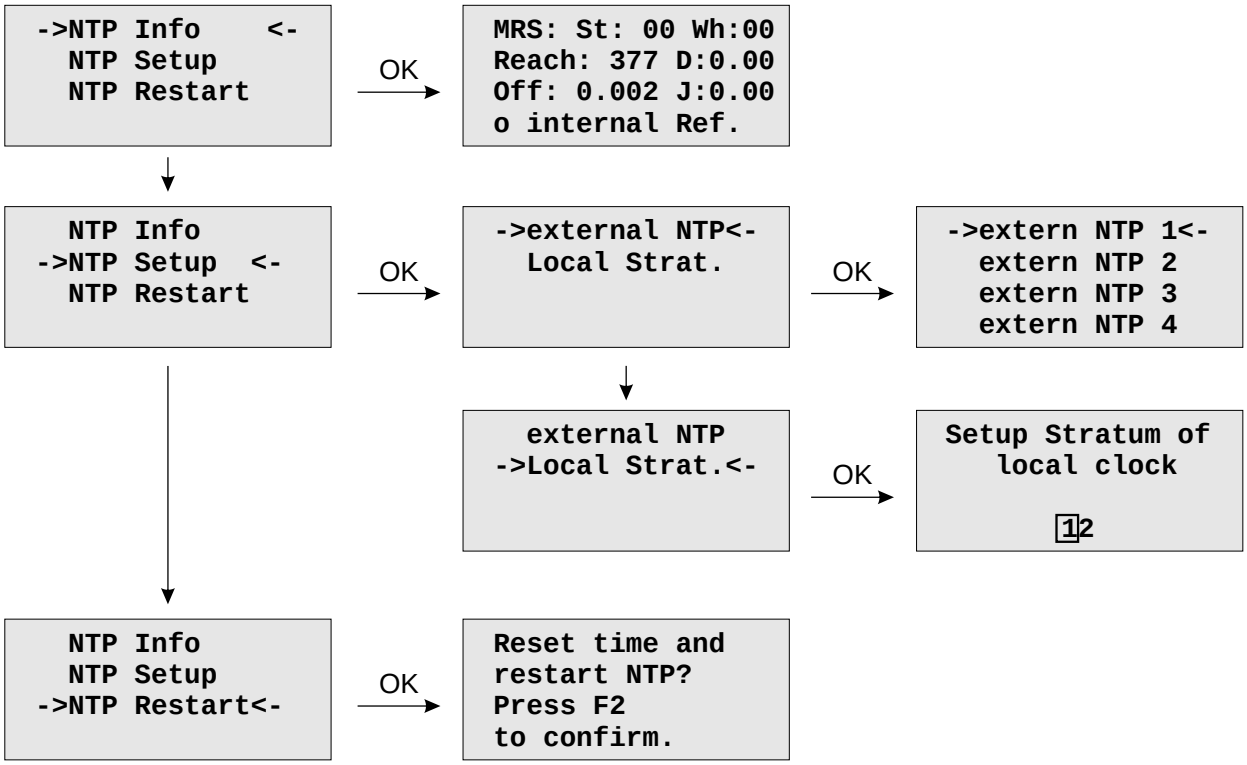
In der letzten Zeile des Displays kann die Phasenlage der eingestellten Frequenz im Bereich -360° bis +360° mit einer Auflösung von 0.1° eingegeben werden. Bei Vergrößerung des Phasenwinkels wird das Ausgangssignal mehr verzögert. Falls eine Frequenz größer als 10 kHz eingestellt wurde, kann die Phase nicht geändert werden.

13.2.4 Menü: Time Service

Alle Statusinformationen und Einstellungen zum NTP und die optional verfügbaren PTP Einstellungen werden über dieses Menü vorgenommen.

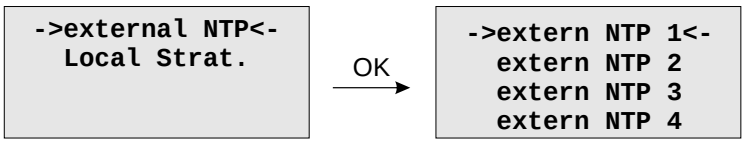


13.2.4.1 Menü NTP



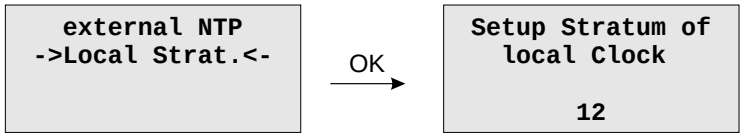
13.2.4.2 Menü: External NTP

Zu den internen Referenzuhren können zusätzlich externe NTP Server mit berücksichtigt werden. Die interne Referenzuhr hat immer Vorrang vor den externen NTP Servern. Wenn die interne Referenzuhr nicht synchron oder ausgefallen ist, schaltet der NTP automatisch auf eine der externen NTP Server um. Über diesen Menüpunkt können noch weitere NTP Server konfiguriert werden.



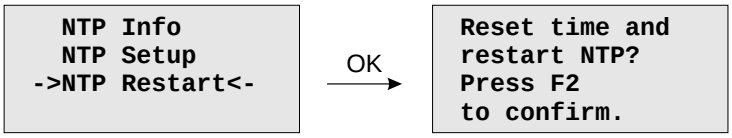
13.2.4.3 Menü: Stratum of local clock

Die „Local Clock“ wird vom NTP als eine Referenzuhr benutzt. Diese entspricht der Hardwareuhr des Rechners. Wenn keine Referenzuhr (interner Empfänger oder externe NTP Server) mehr zur Verfügung steht, schaltet der NTP auf diese „Local Clock“ zurück. Der Stratum-Wert der „Local Clock“ kann über dieses Menü eingestellt werden. Der Stratum-Wert unter NTP entspricht der Güte der Referenzuhr oder dem Abstand zur nächsten Referenzuhr.

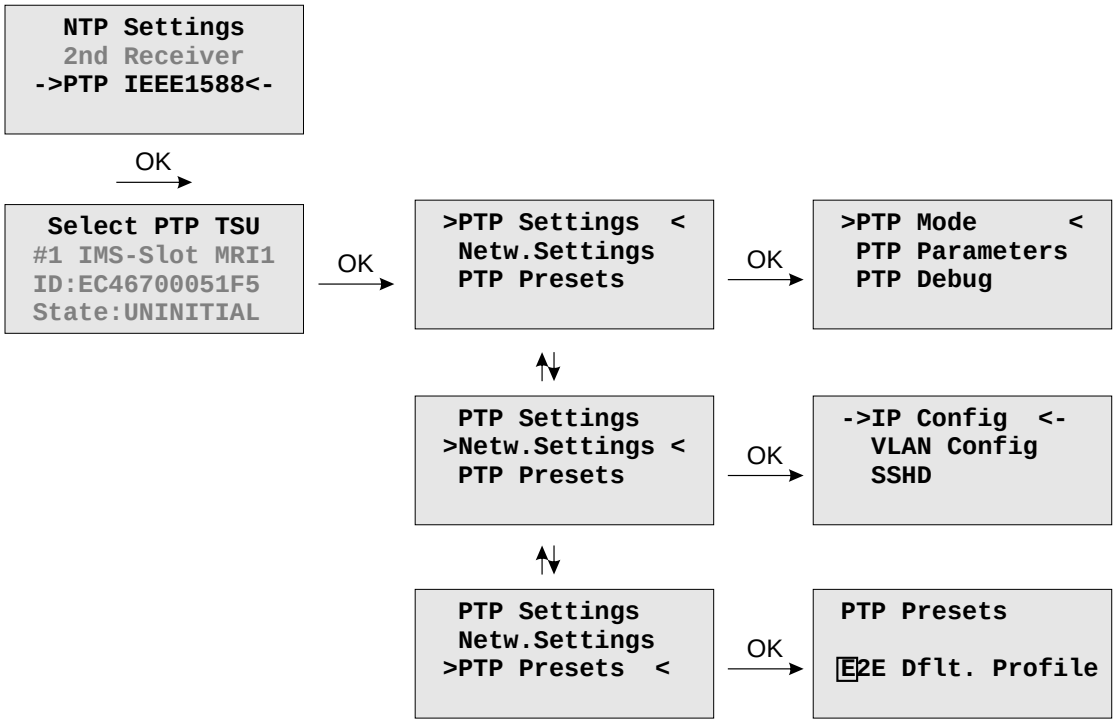


13.2.4.4 Menü: Restart NTP

Mit diesem Menüpunkt wird die Systemzeit einmalig mit der Referenzuhr gesetzt und der NTP neu gestartet.

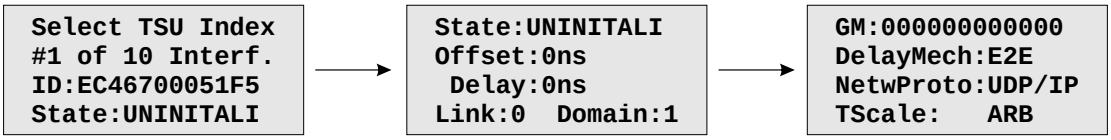


13.2.4.5 Option: Menü PTPv2 - IEEE 1588-2008



Das Menü für die PTP IEEE 1588 Konfiguration befindet sich unter der Hauptmenükategorie „Time Service“ und ist in die Abschnitte „TSU x Info“ und „TSU x Setup“ unterteilt. In einem Gerät mit mehr als einer PTPv2 Karte (auch TSU, Time Stamp Unit genannt), werden die Untermenüs für alle PTP Karten aufgelistet.

13.2.4.6 Menü TSU Info



Die Seite „TSU Info“ vermittelt einen Überblick über den Status der wichtigsten Parameter des PTP Subsystems. Die Zusammenstellung der Parameter ist abhängig vom eingestellten Modus. In der Betriebsart „Grandmaster“ wird hier der „MASTER“ Zustand dargestellt. Die Werte für Offset und Delay sind im Master-Modus auf 0 gesetzt. Darüber hinaus wird die MAC-Adresse des Grandmasters eingeblendet.

Bei MRS (Multi Reference Source) Geräten erscheint hier alternativ der Zustand der Betriebsart „Slave“.

Mögliche PTP Statusanzeigen:

uninitialized: Das PTP-Modul fährt hoch, der Software -Daemon ist noch nicht gestartet, und keine IP-Adresse ist zugeordnet.

initializing: In diesem Zustand initialisiert der Port seine Datensätze, Hardware und Kommunikationseinrichtungen.

faulty: Nicht definiert in LANTIME Systemen.

stopped: Der PTP-Dienst wurde angehalten oder nicht gestartet wegen einer fehlenden Verbindung mit dem PTP Port oder wegen eines nicht-synchronisierten Masters nach dem Systemstart.

disabled: Nicht definiert in LANTIME Systemen.

listening: Der Port wartet auf „announceReceiptTimeout“ um anzuhalten oder auf eine „Announce Message“ von einem Master.

preMaster: Ein kurzer Übergangszustand, während der Port zu einem Meister wird.

master: Der Port ist der aktuelle Master.

passive: Der Port ist im passiven Modus, was bedeutet, dass es einen anderen aktiven Master in der PTP-Domäne gibt. Falls der Dienst des aktiven Master ausfällt oder sich verschlechtert, kann dieser Port mittels BMCA (Best Master Clock Algorithm) den Master Modus übernehmen.

uncalibrated: Der Port will in der PTP-Domäne als Slave fungieren und hat bereits einen geeigneten Grandmaster gefunden. Die TSU wartet, um Netzwerk Delay-Messung zu dem Grandmaster zu berechnen.

slave: Der Port hat sich erfolgreich bei einem Master angemeldet und dadurch erhält er alle erwarteten Nachrichten. Auch die Netzwerk Delay-Messung wurde erfolgreich durch „delay_request“ Abfragen ermittelt.

Werte **Offset** und **Delay**

„Master“ Status: 0 ns nach dem Einstellen auf die interne Uhr.

„Slave“ Status: Zeigt den Offset zum Grandmaster und die mittlere Netzwerkverzögerung zwischen dem Master und Slave.

Link: Status 0: Wenn der angefragte Port nicht erreichbar ist, prüfen Sie die Link-LED. Wenn defekt, ersetzen Sie die Netzwerkkarte.

Status 1: Der angefragte Port arbeitet im Normalbetrieb.

Domain: Eine PTP -Domäne ist eine logische Gruppe von PTP-Geräten innerhalb eines physikalischen Netzwerkes, die durch die gleiche Domain-Nummer definiert ist. Slave-Geräte, die zu einem bestimmten Master im Netzwerk synchronisiert werden sollen, müssen mit einer eindeutiigen Domain-Nummer konfiguriert werden. Diese muss die gleiche wie bei dem Master sein.

GM: Die MAC Adresse von dem aktuellen Grandmaster.

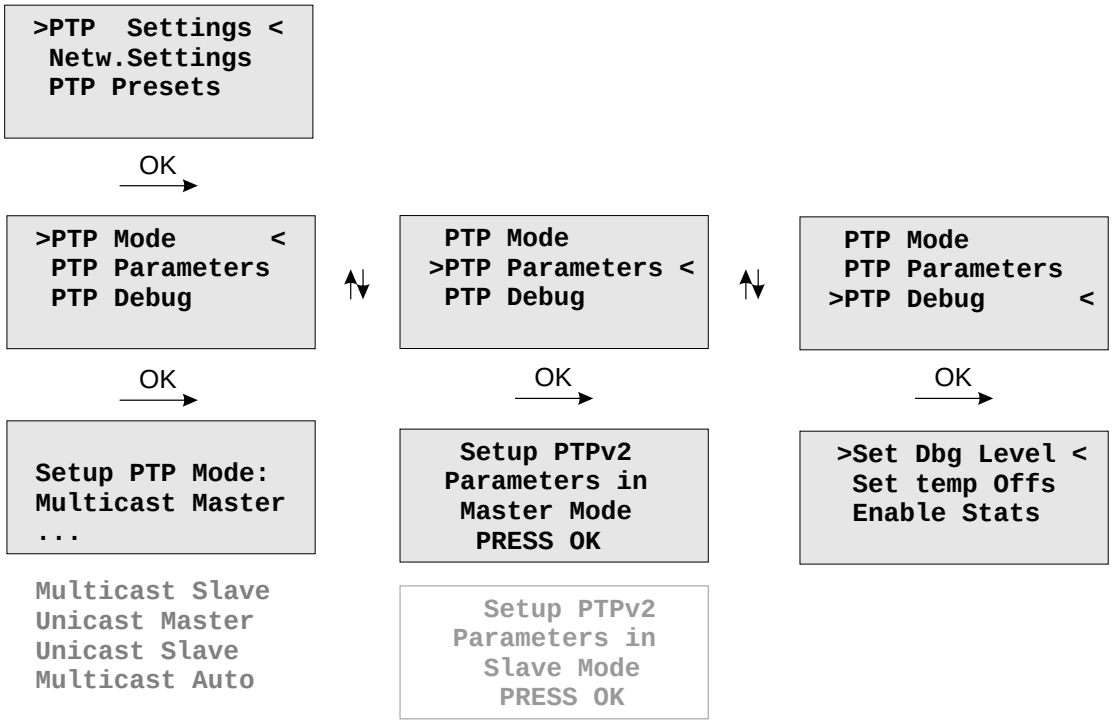
DelayMech: Zwei Optionen sind möglich:
E2E (End-to-End), wobei Delay-Messung Messages direkt vom Slave an den Master geschickt werden (Delay Messung zwischen 2 Endknoten).

P2P (Peer-to-Peer): jedes Gerät (ein Peer) tauscht die (Delay Request und Delay Response) Messages mit seinem unmittelbaren Nachbargerät (Peer) aus. Auf dieser Weise kennt jeder Knoten die Netzwerkverzögerung zu seinem direkten Nachbarn. Der P2P Mechanismus kann nur in IEEE-1588 PTP-fähigen Netzwerken eingesetzt werden.

NetwProto: Zwei Optionen für das PTP-Netzwerkprotokoll stehen zur Verfügung:
ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet-Frames einschließlich MAC-Adressen eines Slaves und Masters.

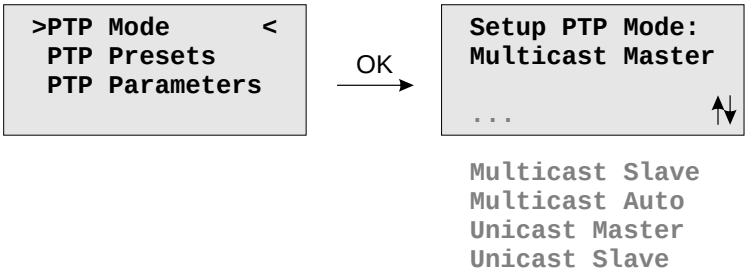
UDP-UDP/IPv4/IPv6 (Layer 3): Das User Data Protocol ist eines der wichtigsten Protokolle, die im Internet verwendet werden.

13.2.4.7 Menü TSU Setup



In diesem Menu können die Einstellungen für alle PTP Parameter für die ausgewählte PTP Schnittstelle vorgenommen werden.

13.2.4.8 Menü PTP Mode



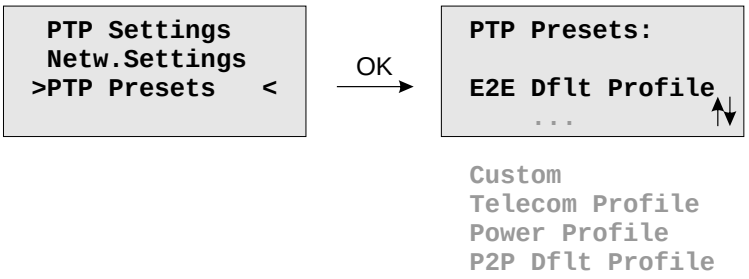
Die Anzahl der möglichen PTP Modi hängt von den Features des Gerätes ab.

Unterstütze Modi auf einem reinen GPS bzw. GPS/GLONASS System:
- PTPv2 Multicast Master
- PTPv2 Unicast Master

Unterstützte Modi auf einem MRS (Multi Reference Source) System:
- PTPv2 Multicast Slave
- PTPv2 Multicast Master
- PTPv2 Multicast Auto
- PTPv2 Unicast Slave
- PTPv2 Unicast Master

13.2.4.9 PTP Presets laden

Jedes „PTP Preset“ stellt einen Satz von PTP Parametern dar, mit dem man die PTP Einheit in einem Schritt auf ein bestimmtes PTP Profil umschalten kann. Nachdem ein bestimmtes Preset eingestellt wurde, besteht aber immer noch die Möglichkeit die einzelnen Parameter zu verändern.



Hinweis: Sobald ein PTP Preset ausgewählt ist, werden die vorher eingestellten PTP Parameter überschrieben!

Es werden sechs verschiedene Presets unterstützt:

Delay Request-Response Default Profile
- Sync Msg. Rate:1/sec
- Ann. Msg. Rate: 2 sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech.: „E2E“

Peer-to-Peer Default Profile
- Sync Msg. Rate:1/sec
- Ann. Msg. Rate: 2 sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech.: „P2P“

Power Systems Profile
- Sync Msg. Rate:1/sec
- Ann. Msg. Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech.: „P2P“
- VLAN (802.1Q) enabled (VLAN ID:0, Prio:4)
- Power Profile TLVs enabled

Telecom ITU-T G.8275.1
- Ann Msg. Rate: 8/sec
- Sync Msg. Rate:16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: „E2E“
- Netzwerkprotokoll: „Layer 2 (IEEE 802.3)“

In Unicast Master / Slave Modus:

Telecom ITU-T G.8265.1
- Ann Msg. Rate: 1/sec
- Sync Msg. Rate:16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: „E2E“
- Netzwerkprotokoll: „Layer 3 (UDP/IPv4)“

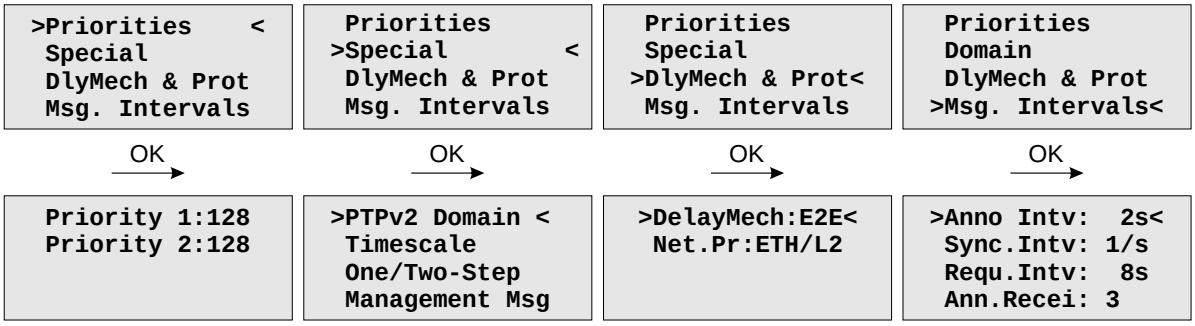
In Unicast oder Multicast Master / Slave Modus:

SMPTE ST 2059-2
-Ann Msg. Rate: 4/sec
-Sync Msg. Rate: 8/sec
-Del Req Rate: 8/sec
-Priority 1: 128
-Priority 2: 128
-Delay Mech: „E2E“ or „P2P“

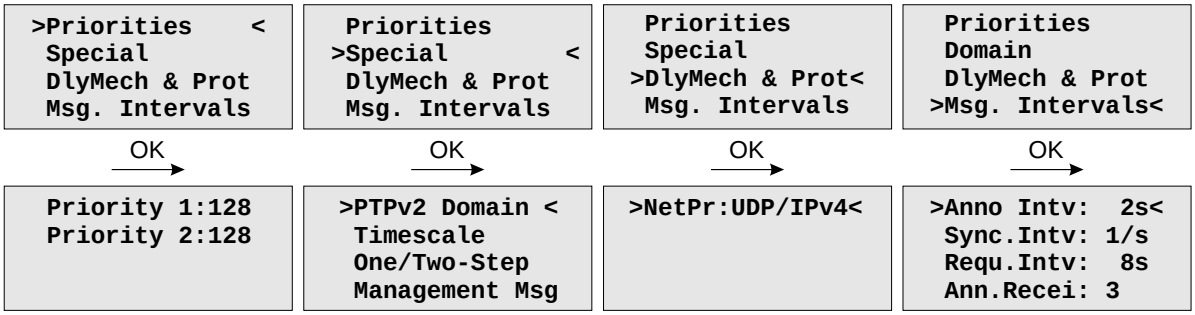
Custom Profile
Durch die Auswahl von „Custom“ werden alle Parameter zum Editieren freigeschaltet.

13.2.4.10 PTP Parameters

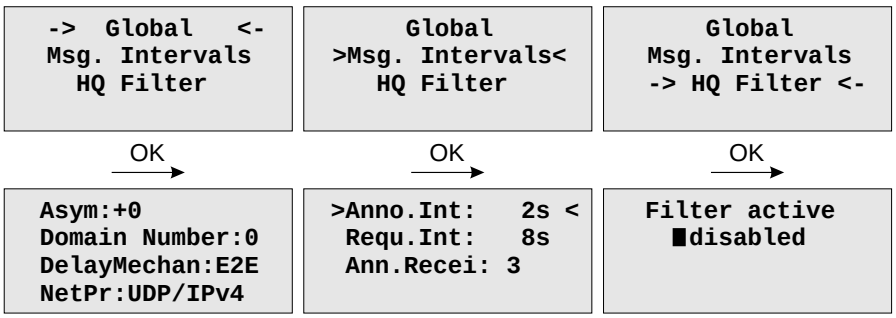
MULTICAST MASTER



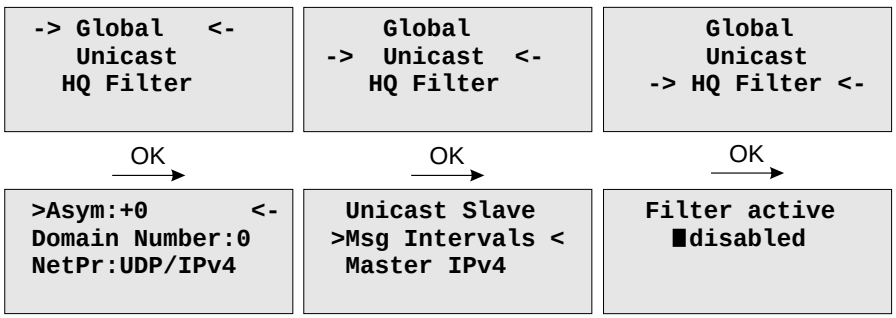
UNICAST MASTER



MULTICAST SLAVE



UNICAST SLAVE



In Abhängigkeit vom eingestellten PTP Mode werden im Untermenu „PTP Parameters“ verschiedene Untermenüs dargestellt.

Parameter für alle PTP Modis:

Priority1 (nur Master):
Das Attribut wird bei der Ausführung des Best-Master-Clock-Algorithmus (BMCA) verwendet. Geräte mit niedrigeren priority1 Werten haben bei der Wahl des besten Masters Vorrang gegenüber Geräten mit höheren priority1 Werten.
Konfigurierbarer Bereich: 0 .. 255.

Priority2 (nur Master):
Das Attribut wird bei der Ausführung des Best-Master-Clock-Algorithmus (BMCA) verwendet.
Für den Fall, dass der Best-Master-Clock-Algorithmus auch nach Auswertung der PTP Parameter priority1 und der Qualitätsparameter clockClass, clockAccuracy und scaledOffsetLogVariance keinen Master ermitteln konnte, ermöglicht das priority2 Attribut eine Bevorzugung von einem Gerät bevor der so genannte Tie-Break durchgeführt wird. Der Tie-Break basiert auf der clockIdentity (der MAC-Adresse des PTP Ports) und führt schließlich eine endgültige Entscheidung für einen Master herbei. Die Werte clockClass, clockAccuracy und scaledOffsetLogVariance sind vom Status des Grandmasters abhängig und können nicht konfiguriert werden.
Konfigurierbarer Bereich: 0 .. 255.

Domain Number:
Eine PTP Domain ist eine logische Gruppierung von PTP Geräten innerhalb eines physikalischen PTP Netzwerks. PTP Slaves, die sich mit einem bestimmten Master verbinden sollen, müssen alle die Domain Nummer des Masters konfiguriert haben.

Delay Mechanismus:
E2E - End-to-End (Delay Request-Response)
P2P - Peer-to-Peer (Pdelay Request-Response) - wird nur im Multicast Mode unterstützt

Netzwerkprotokoll:
UDP - UDP/IPv4 (Layer 3)
ETH - IEEE 802.3/Ethernet (Layer 2) - wird nur im Multicast Mode unterstützt

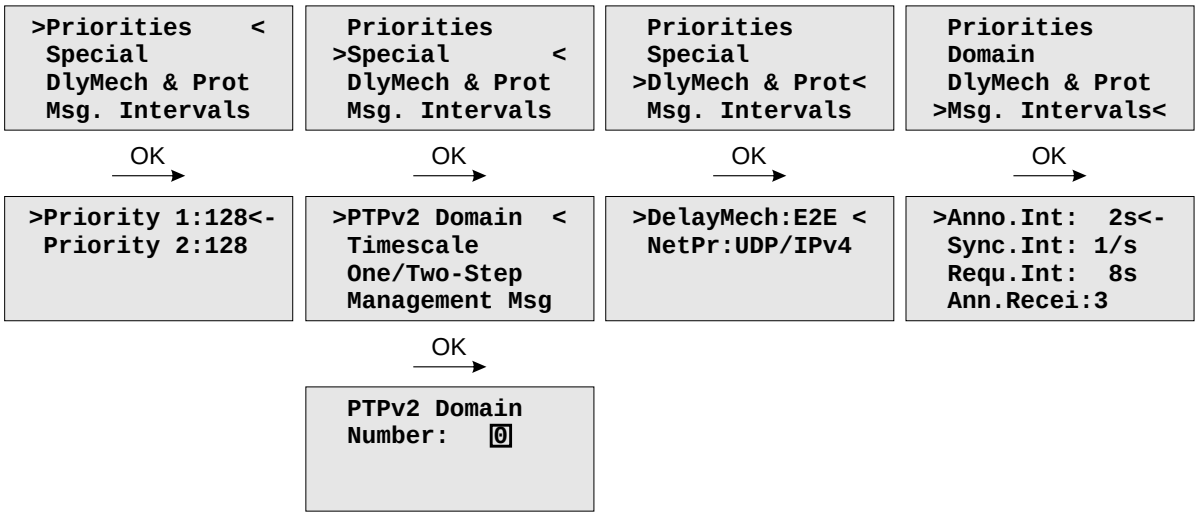
Nur für MRS:
Globale Parameter im PTP Slave Mode:

Asym: (Default Asymmetry Offset)
Falls innerhalb des Netzwerks ein konstanter Asymmetrieoffset bekannt ist, kann dieser Offset zur Kompensation dieses Asymmetrieoffsets eingetragen werden um einen potentiellen Zeitfehler zu korrigieren.

Achtung!

Verwenden Sie „Asym“ nur in Umgebungen mit bekanntem Asymmetrie-Offset.

13.2.4.11 Multicast Master



Für den Betrieb im Multicast Master Modus können die folgenden Einstellungen vorgenommen werden.

Domain Number:
Eine PTP Domain ist eine logische Gruppierung von PTP Geräten innerhalb eines physikalischen PTP Netzwerks. PTP Slaves, die sich mit einem bestimmten Master verbinden sollen, müssen alle die Domain Nummer des Masters konfiguriert haben.

Delay Mechanismus:
E2E - End-to-End (Delay Request-Response)
P2P - Peer-to-Peer (Pdelay Request-Response)

Netzwerkprotokoll:
UDP - UDP/IPv4 (Layer 3)
ETH - IEEE 802.3/Ethernet (Layer 2) - wird nur im Multicast Mode unterstützt!

Priority1:
Das Attribut wird bei der Ausführung des Best-Master-Clock-Algorithmus (BMCA) verwendet.
Geräte mit niedrigeren priority1 Werten haben bei der Wahl des besten Masters Vorrang gegenüber Geräten mit höheren priority1 Werten.
Konfigurierbarer Bereich: 0 .. 255.

Priority2:
Das Attribut wird bei der Ausführung des Best-Master-Clock-Algorithmus (BMCA) verwendet.
Konfigurierbarer Bereich: 0 .. 255.

Für den Fall, dass der Best-Master-Clock-Algorithmus auch nach Auswertung der PTP Parameter priority1, clockClass, clockAccuracy und scaledOffsetLogVariance keinen Master ermitteln konnte, ermöglicht das priority2 Attribut eine Bevorzugung von einen oder mehreren Geräten bevor der so genannte Tie-Break durchgeführt wird. Der Tie-Break basiert auf der clockIdentity und führt schließlich eine endgültige Entscheidung für einen Master herbei. Die Werte clockClass, clockAccuracy und scaledOffsetLogVariance sind vom Status des Grandmasters abhängig und können nicht konfiguriert werden.

Zeitskala (Timescale):

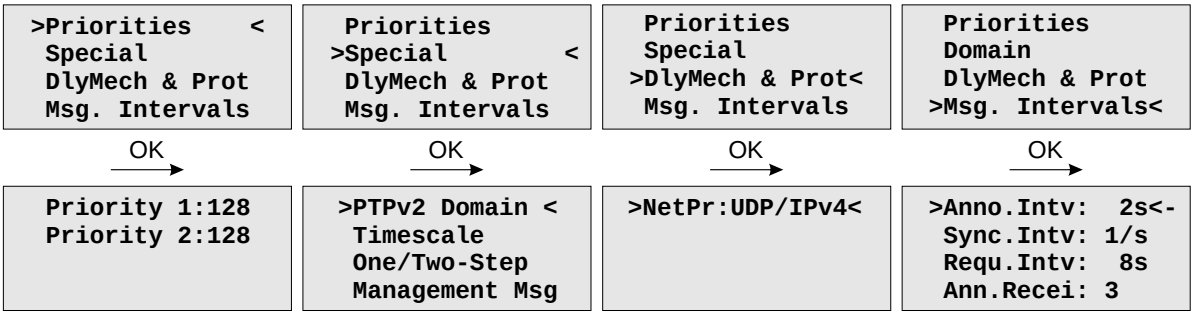
- **„1“:** PTP (TAI Zeitstempel in Sync Messages, Standardeinstellung) - PTP Slaves bestimmen die UTC Zeit, in dem sie den UTC Offset aus der Announce Message vom TAI-Zeitstempel der Sync Message subtrahieren. Die TAI Zeit ist die Internationale Atomzeitskala und wurde am 01.01.1970 synchron mit der UTC Zeit gestartet. Es wurden jedoch keine Schaltsekunden eingefügt, um eine monoton steigende Zeitskala zu realisieren. Im Jahre 2010 war daher die TAI Zeitskala der UTC Zeit um 34 Sekunden voraus.
- **„0“:** ARB (arbitrary): Benutzerdefinierte Zeitskala bei welcher der UTC Offset auf 0 gesetzt wird (für Testzwecke). Bei der Verwendung der ARB Zeitskala können die PTP Slaves die UTC Zeit nicht berechnen!

Message Intervalle:

- Sync Int: Paketrate der Sync Messages (64/sec...64 sec).
- Requ Int: Gibt das minimal erlaubte Interval zwischen zwei Delay Messungen vor (64/sec...64 sec).
- Ann. Int: Paketrate der Announce Messages (64/sec...64 sec).

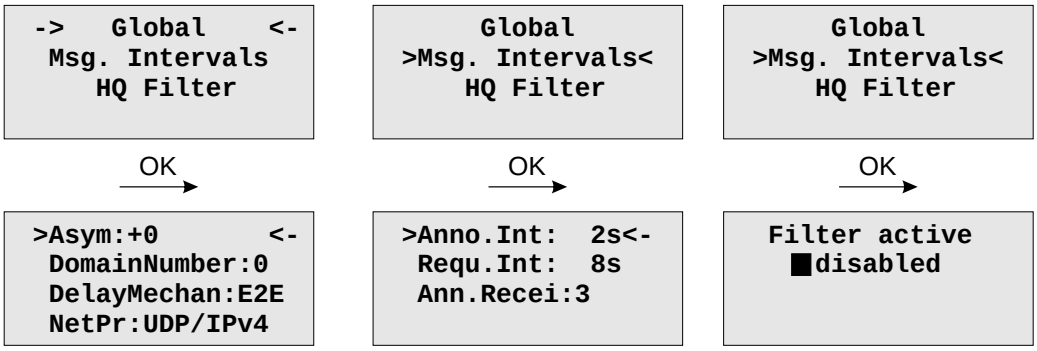
13.2.4.12 Unicast Master

Bei aktiviertem „Unicast“ Mode erscheint ein zusätzliches Untermenü zur Konfiguration von Unicast spezifischen Parametern.



Falls „Unicast Master“ eingestellt ist, kann nur die Priority1, Priority2 und die PTPv2 Domain für den Unicast Master eingestellt werden. Die notwendigen Einstellungen für die zu versendenden Nachrichten müssen im Rahmen des „Unicast Negotiation“ Verfahrens auf den Slaves vorgenommen werden.

13.2.4.13 Multicast Slave (nur MRS-Geräte)



Für den Betrieb im Multicast Slave Modus können zusätzlich zu den bereits beschriebenen Parametern aus dem Kapitel „Global Parameters“ die folgenden Einstellungen vorgenommen werden.

Asym: oder Standardasymmetrie ist ein anfänglicher Kalibrierungswert (in ns) und kann hier eingegeben werden, wenn vor dem Start der PTP-Einheit ein bestimmter Asymmetrie-Offset im Netzwerkpfad bekannt ist. Dies tritt beispielsweise in SDH-Netzwerken auf.

Max.Path Delay: Wenn eine gemessene Pfadverzögerung den Wert dieses Parameters (in ns) überschreitet, kann die PTP-Einheit eine Änderung des Asymmetrie-Offsets erkennen und diese bei ihren Verzögerungsmessungen berücksichtigen.

Note: Behalten Sie hier die Standardeinstellungen bei (0 ns für beide Parameter), es sei denn, es treten Probleme mit der Genauigkeit der Client-Synchronisation auf und nur, wenn der Asymmetrie-Offset zuvor gemessen werden kann.

PTPv2 Domain: Eine PTP-Domäne ist eine logische Gruppe von PTP-Geräten innerhalb eines physischen Netzwerks, die zur gleichen Domänennummer gehören. Slave-Geräte, die sich mit einem bestimmten Master innerhalb eines Netzwerks synchronisieren sollen, müssen eine eindeutige Domänennummer konfiguriert haben, die mit der des Masters übereinstimmt.

DelayMech: Zwei Optionen sind möglich:
E2E (End-to-End), bei dem Verzögerungsmessungsmeldungen vom Slave an den Master (die beiden Endknoten) gesendet werden.

P2P (Peer-to-Peer): Hier tauscht jedes Gerät (ein Peer) im Netzwerk Peer-Verzögerungs-messungsmeldungen aus. Auf diese Weise kann jedes Gerät die Verzögerungen zwischen sich selbst und seinen unmittelbar verbundenen Nachbarn (z. B. einem Switch oder Router) verfolgen. Der P2P-Mechanismus kann nur in 1588-PTP-fähigen Netzwerken verwendet werden.

NetPr: Zwei Optionen für das Netzwerkprotokoll möglich:
ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet-Frame einschließlich MAC-Adressen eines Ziels und einer Quelle.

UDP-UDP/IPv4/IPv6 (Layer 3): User Data Protocol, eines der wichtigsten Protokolle für das Internet.

Msg. Intervals: Spezifizieren der Einstellungen für die PTP-Timing-Meldungen.
Anno. Intv legt die Zeit für das Senden von Ankündigungsmeldungen zwischen den Mastern fest, um den Grandmaster auszuwählen.
Verfügbare Einstellungen sind:
16/s, 8/s, 4/s ... 2s, 4s, 8s, 16s mit einem Standardwert von 2 Sekunden.

Sync. Intv gibt die Zeit für das Senden von Synchronisationsmeldungen von einem Master an einen Slave an.
Verfügbare Einstellungen sind:
128/s, 64/s ... 64s, 128s, mit einem Standardwert von 1 Sekunde.

Requ. Intv gibt das Intervall an, in dem Verzögerungsanforderungsnachrichten vom Slave an den Master gesendet werden.
Intervalle für Verzögerungsanforderungs-Nachrichten:
128/s, 64/s, ... 64 s, 128 s, mit einem Standardwert von 2 Sekunden.

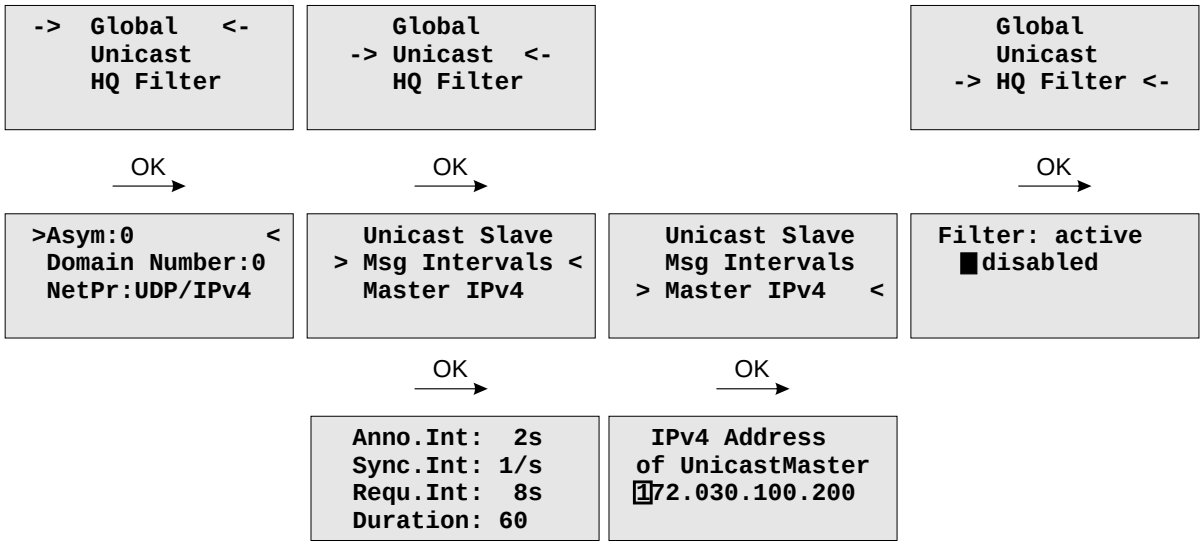
Der Wert „Ann. Recei“ gibt die Zeit für die Zeitüberschreitung bei der Ankündigung von Empfangsnachrichten an, die das 2- bis 10-fache des Ankündigungsintervalls beträgt, wobei der Standardwert 3 ist. Dies ist die Zeit, die ein BMCA benötigt, um einen Grand Master zu bestimmen.

HQ Filter: In stark ausgelasteten Netzwerken kann bei Verwendung von nicht PTP-kompatiblen Switches der „HQ-Filter“ aktiviert werden, um den Jitter zu reduzieren. In der Standardeinstellung ist der HQ-Filter deaktiviert.

Hinweis:

Seit der LANTIME-Firmware-Version 7.02 hat die Konfiguration des HQ Filters keine Auswirkung mehr. Ein sogenannter „Lucky Packet Filter“, der automatisch ab einem bestimmten Abfrageintervall aktiv wird, sorgt jetzt dafür, dass ein zu hoher Jitter durch nicht PTP-kompatible Systeme im Netzwerk entstehen kann. Mehr Informationen dazu im → Kapitel 8.6.1.10, „Lucky Packet Filter“.

13.2.4.14 Unicast Slave (nur MRS-Geräte)



Im Unicast Slave Modus kann wie im Multicast Modus ein **Asymmetrie Offset** vorgegeben werden. Der Asymmetrie Offset ist abhängig von der Netzwerk Topologie und muss manuell bestimmt werden - dieser Wert wird in Nanosekunden angegeben.

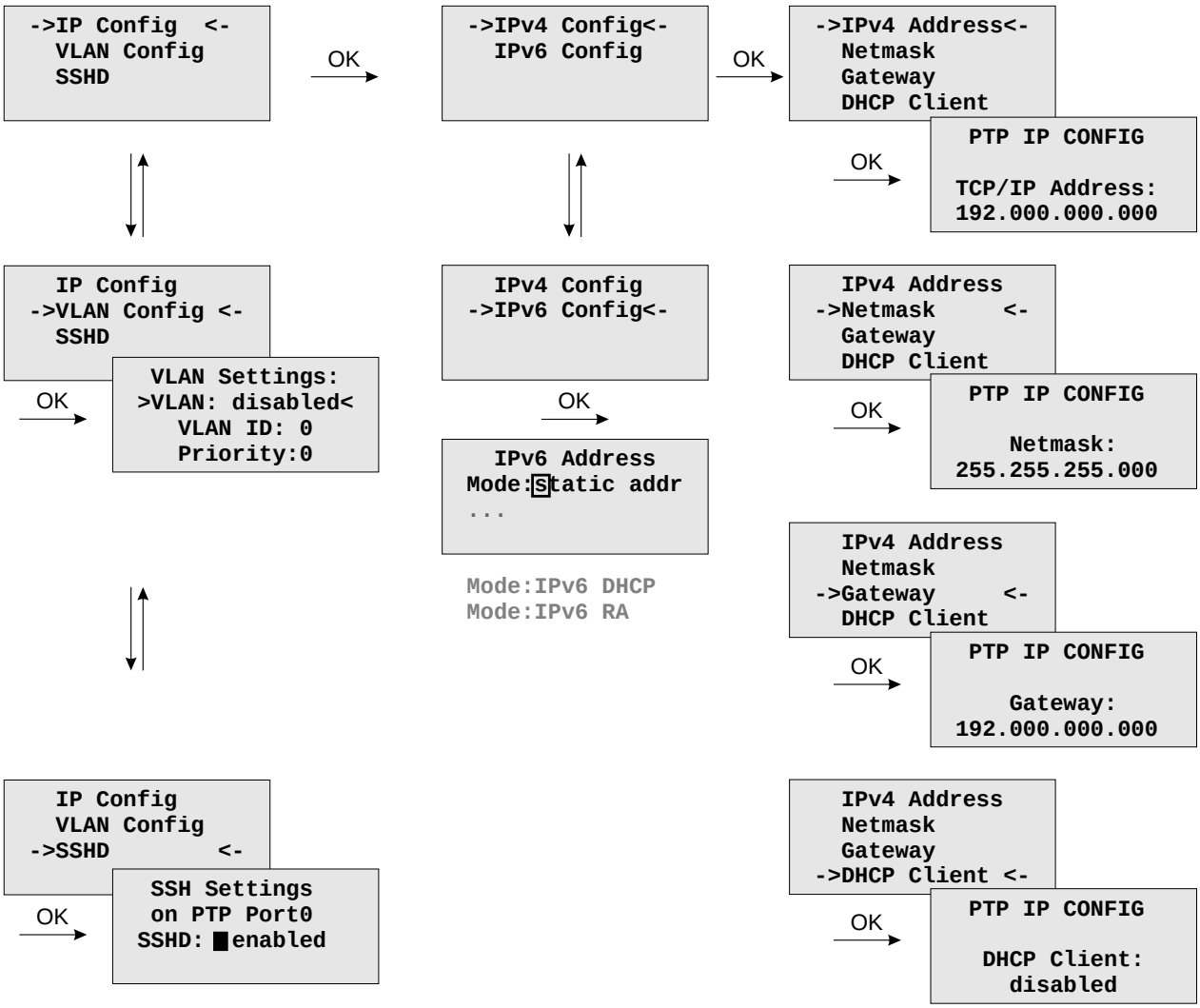
Unter **„Master Address“** muss die IP Adresse des PTP Ports des Grandmasters eingestellt sein.

Rate und Sendedauer für Sync, Announce und Delay Response Nachrichten
In diesen Untermenüs wird eingestellt, welche Nachrichten bei welcher Rate und mit welcher Dauer von einem Grandmaster angefordert werden sollen. Dies geschieht im Rahmen des „Unicast Negotiation“ Protokolls.

Mit **„Interval“** wird die Rate eingestellt, mit welcher eine bestimmte Nachricht vom Grandmaster zum Slave gesendet wird. Über die **„Duration“** wird bestimmt, wie lange der Master eine bestimmte Nachricht zum Slave senden soll. Um einen kontinuierlichen Empfang eines Nachrichtentyps sicher zu stellen, erneuert der Slave kurz vor Ablauf der „Duration“ seine Anfrage für einen bestimmten Nachrichtentyp. Dieser Vorgang wird im Rahmen des „Unicast Negotiation“ Protokolls automatisch sichergestellt. Die Duration bezieht sich auf alle Nachrichten Typen und sollte zwischen 10s und 300s eingestellt werden.

13.2.4.15 Menü PTP Network Settings

Konfigurationseinstllungen für die PTPx Netzwerkschnittstelle



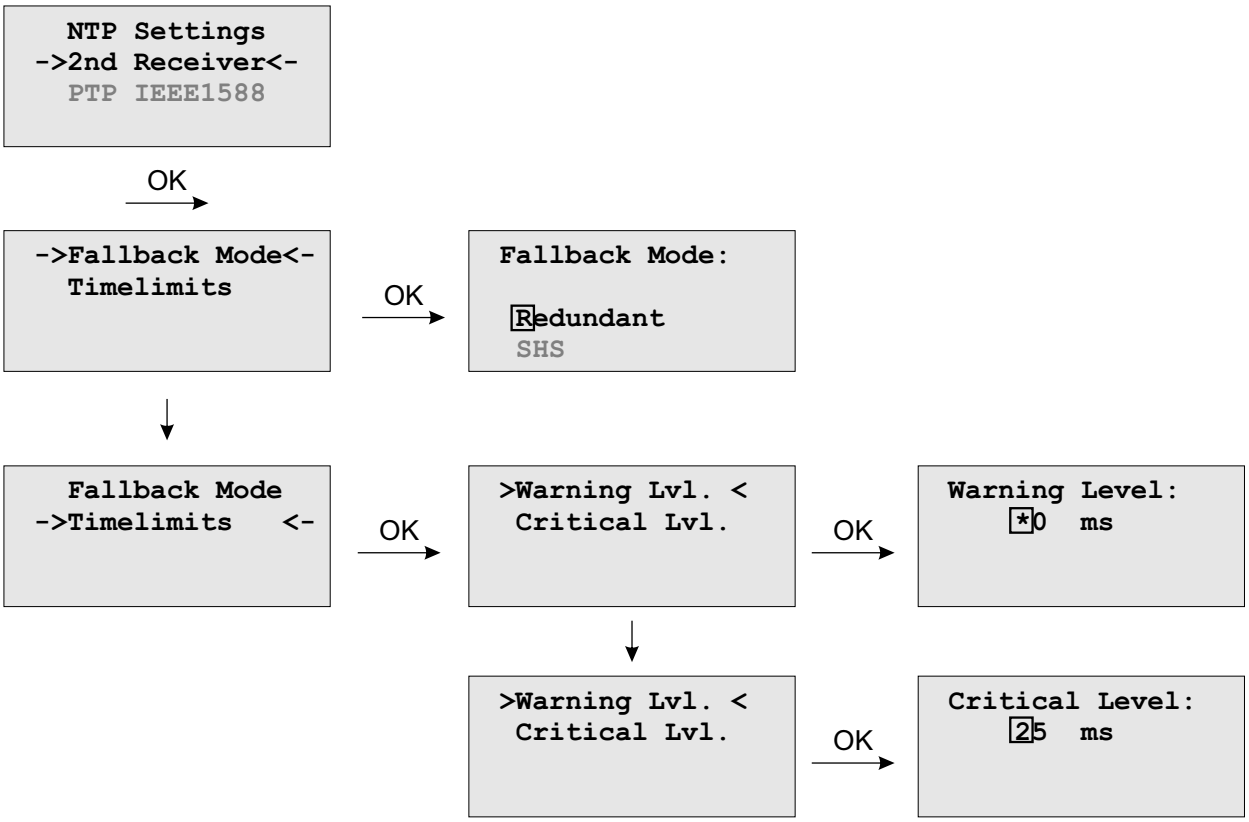
Hier kann die statische IP Konfiguration des PTPx Interfaces vorgenommen werden. Alternativ lässt sich für die PTPx Schnittstelle der DHCP Dienst aktivieren.

VLAN Config:
Virtual LAN (IEEE 802.1Q) Konfiguration für das PTPx Interface:

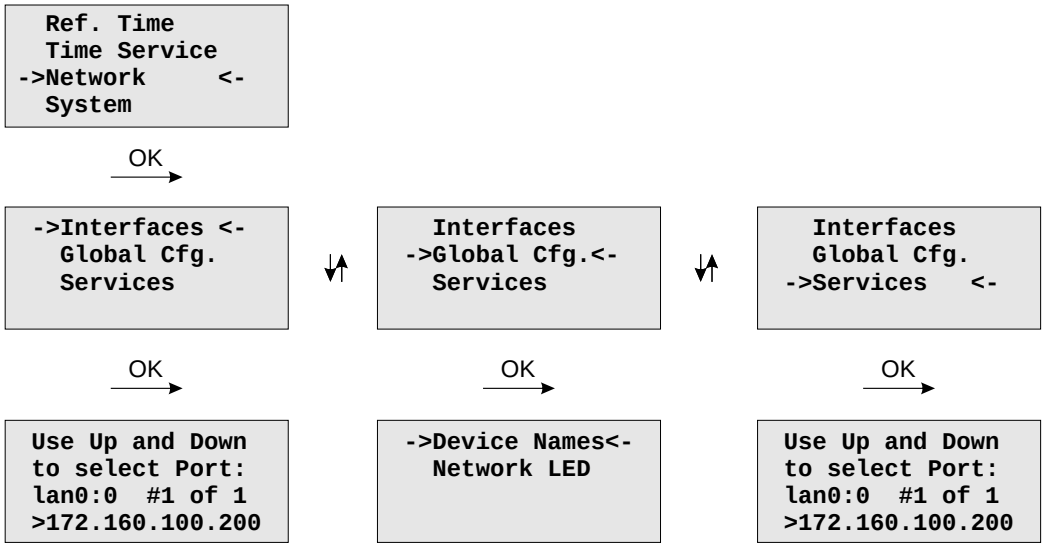
- VLAN ID: Ein 12-bit Wert (0..4096), der die Zugehörigkeit zu einem VLAN spezifiziert.
- Priority: Die Priorität gibt den „Frame Priority Level“ von 0 (niedrigster) bis 7 (höchster) an, der dazu verwendet wird bestimmte Klassen (Protokolle) des Netzwerkverkehrs zu priorisieren.

13.2.4.16 Optionales Menü: 2nd Receiver

Im Untermenü 2nd Receiver kann der Fallbackmode (Redundant oder SHS) gewählt werden und die entsprechenden Zeitlimits (Warning- und Critical-Level) können hier eingestellt werden.



13.2.5 Menü: Network

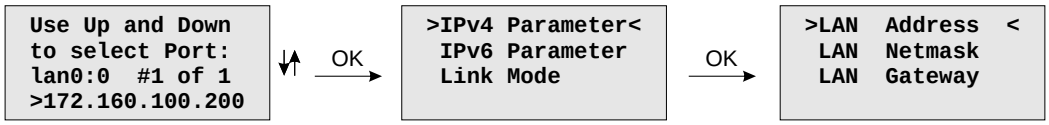


In diesem Untermenü werden die Netzwerkparameter festgelegt. Bei der Erstinstallation des LANTIME müssen diese Parameter an das vorhandene Netzwerk angepasst werden.

Differenzierte Einstellungen können dann später über den Netzwerkzugang mit TELNET, SSH oder das WEB Interface gemacht werden. Die Werte für diese Parameter sollten beim Netzwerk Administrator erfragt werden. Bei jeder Änderung der Netzwerkparameter wird die Konfigurationsdatei neu geschrieben und der NTPD neu gestartet. Alle Parameter für die Konfiguration des Zeitservers werden in der Datei „/mnt/flash/config/global_configuration“ auf der Flash-Disk abgespeichert und sind auch nach einem Neustart gültig. Es wird empfohlen diese Datei nicht manuell zu bearbeiten, sondern alle Änderungen über die Konfigurations-Schnittstellen (HTTP, CLI oder SNMP) durchzuführen. Falls diese Datei nicht vorhanden ist, wird automatisch eine leere Datei beim nächsten Abspeichern angelegt. Die Konfigurationsdatei wird im Anhang mit dem Auslieferzustand abgebildet.

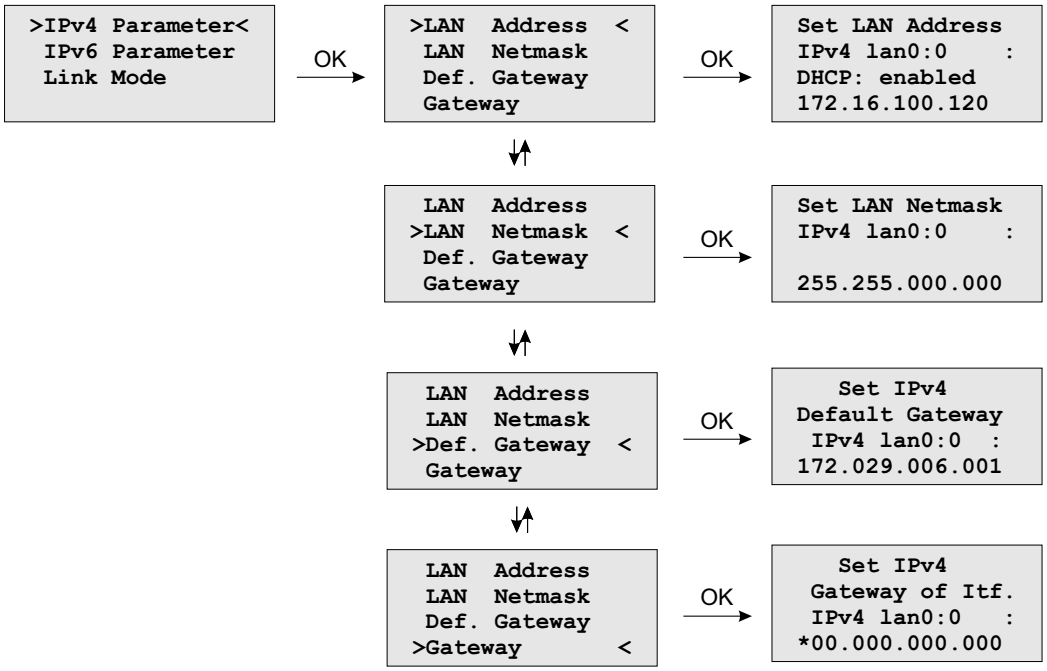
13.2.5.1 Menü: Network Interfaces

In diesem Untermenü werden die Netzwerkparameter festgelegt. Bei der Erstinstallation des LANTIME müssen diese Parameter an das vorhandene Netzwerk angepasst werden. Es können die folgenden Parameter eingestellt werden:



Differenzierte Einstellungen können dann später über den Netzwerkzugang mit TELNET, SSH oder das WEB Interface gemacht werden. Die Werte für diese Parameter sollten beim Netzwerk Administrator erfragt werden. Bei jeder Änderung der Netzwerkparameter wird die Konfigurationsdatei neu geschrieben und der NTPD neu gestartet.

13.2.5.2 Menü: Setup IPv4 LAN Parameter



Für jeden physikalischen Netzwerkanschluss (RJ45 Buchse) steht ein separater Abschnitt zur Verfügung. Ist kein DHCP Client Betrieb für IPv4 aktiviert, so kann manuell eine IP-Adresse für den jeweiligen Netzwerkanschluss eingestellt werden. IPv4-Adressen bestehen aus 32 Bit und werden mit 4 dezimalen Werten zwischen 0 bis 255 durch jeweils einen Punkt getrennt eingegeben:

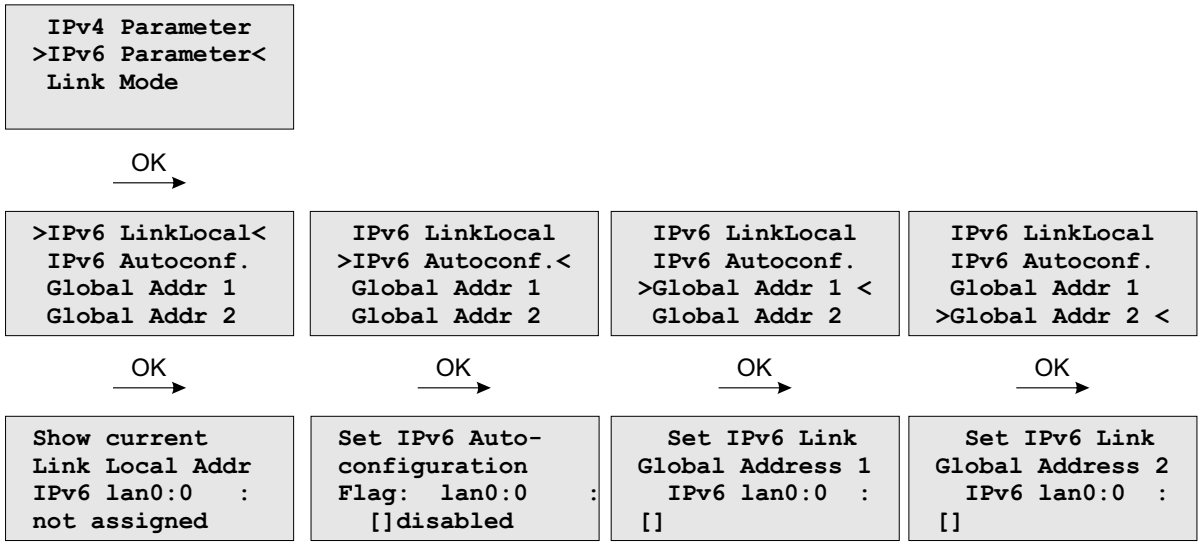
Beispiel: 172.160.100.200

Bitte wenden Sie sich an Ihren Netzwerk Administrator, der Ihnen eine gültige IPv4-Adresse speziell für Ihr Netzwerk vergibt. Ebenso verfahren Sie mit der Netzmaske.

Abhängig von der Anzahl der integrierten Netzwerkschnittstellen werden entsprechende Auswahlmöglichkeiten für die Netzwerkkonfiguration bereitgestellt. Falls sich ein DHCP Server (Dynamik Host Configuration Protocol) im Netz befindet, kann die Netzwerkeinstellung auch automatisch vorgenommen werden. Die Netzwerkeinstellungen werden dann automatisch von einem DHCP-Server (muss sich bereits im Netzwerk befinden) vorgenommen. Die so vergebenen Werte werden dann in den entsprechenden Untermenüs (IPv4-Adresse, Netmask, Default Gateway) angezeigt.

Der DHCP-Client vom LANTIME ist nur für das IPv4 Netzwerk Protokoll einsetzbar.

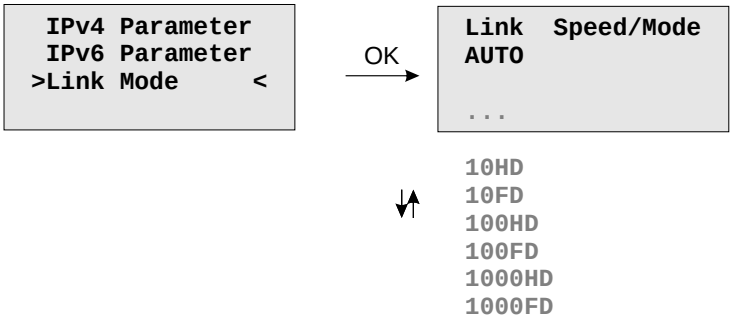
13.2.5.3 Menü: Setup IPv6 Parameter



Über das Frontpanel können die Parameter für IPv6 nur für die erste Schnittstelle eingestellt werden. Dabei sind drei globale IPv6 Adressen möglich, zwei davon sind über das Front Panel einstellbar, eine weitere dritte über das WEB-Interface. IPv6-Adressen haben 128 Bits und werden als Kette von 16-bit-Zahlen in Hexadezimal-Notation geschrieben, die durch Doppelpunkte getrennt werden. Folgen von Nullen können einmalig durch „::“ abgekürzt werden.

Ist das IPv6-Netzwerkprotokoll aktiviert, wird dem LANTIME automatisch immer eine Link-Local IPv6-Adresse in der Form „FE80::...“ zugewiesen, die die eigene Hardware-Adresse der Netzwerkkarte enthält. Befindet sich in dem IPv6 Netzwerk ein Router-Advertiser werden zusätzlich noch eine oder mehrere Link-Global IPv6 Adressen vergeben, wenn IPv6 Autoconf aktiviert wurde.

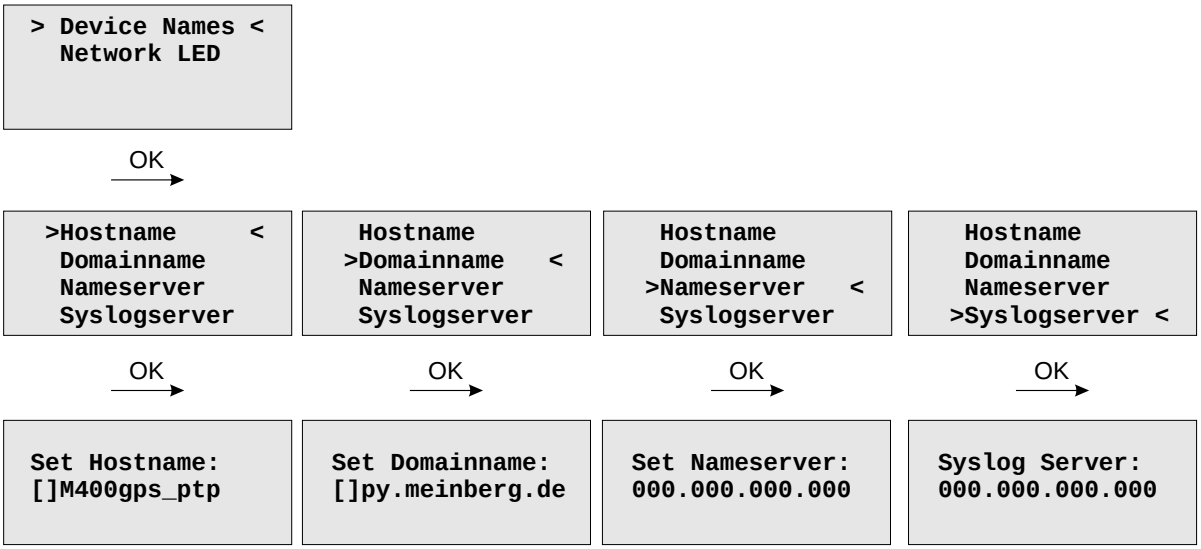
13.2.5.4 Menü: Link Mode



Über das Link Mode Untermenü können die Parameter für Geschwindigkeit und Duplex der ersten Netzwerkschnittstelle eingestellt werden. Es stehen 5 Modi zur Verfügung: Autosensing, 10 MBit/Halb-Duplex, 100 MBit/Halb-Duplex, 1000 MBit/Halb-Duplex (Gigabit Unterstützung), 10MBit/Voll-Duplex, 100 MBit/Voll-Duplex und 1000 MBit/Voll-Duplex (Gigabit Unterstützung).

Standardmäßig werden die Schnittstellen auf Autosensing eingestellt.

13.2.5.5 Menü: Global Configuration

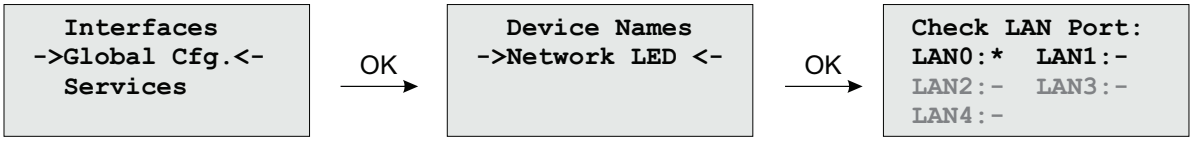


In diesem Untermenü werden Hostname, Domainname, Nameserver und Syslogserver eingestellt

Ein Nameserver und ein Syslogserver können eingetragen werden. Bei den Nameservern und Syslogservern sind nur IPv4 Adressen möglich. Jeweils ein weiterer Nameserver bzw. Syslogserver kann dann später über das WEB-Interface konfiguriert werden. Sind beide Adressen auf 0.0.0.0 gesetzt wird der REMOTE SYSLOG-Dienst nicht verwendet.

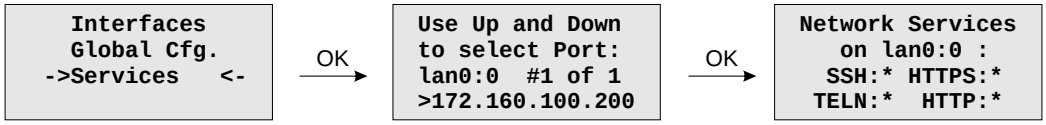
Alle Informationen die auf dem LANTIME in das SYSLOG (/var/log/messages) geschrieben werden, können auf einen entfernten Server umgeleitet werden. Der SYSLOG Dämon des entfernten Servers muss entsprechend auf Empfang geschaltet werden, z.B. unter LINUX mit „syslogd -r“, um die Syslog-Messages von anderen Servern empfangen zu können.

Beachten Sie, dass alle SYSLOG Ausgaben auf dem Zeitserver unter „/var/log/messages“ gespeichert werden und somit nach einem Neustart des Systems gelöscht sind. Ein täglich ausgeführtes Programm (CRON Job) prüft die Größe der Log-Dateien und löscht diese, wenn sie zu groß werden.



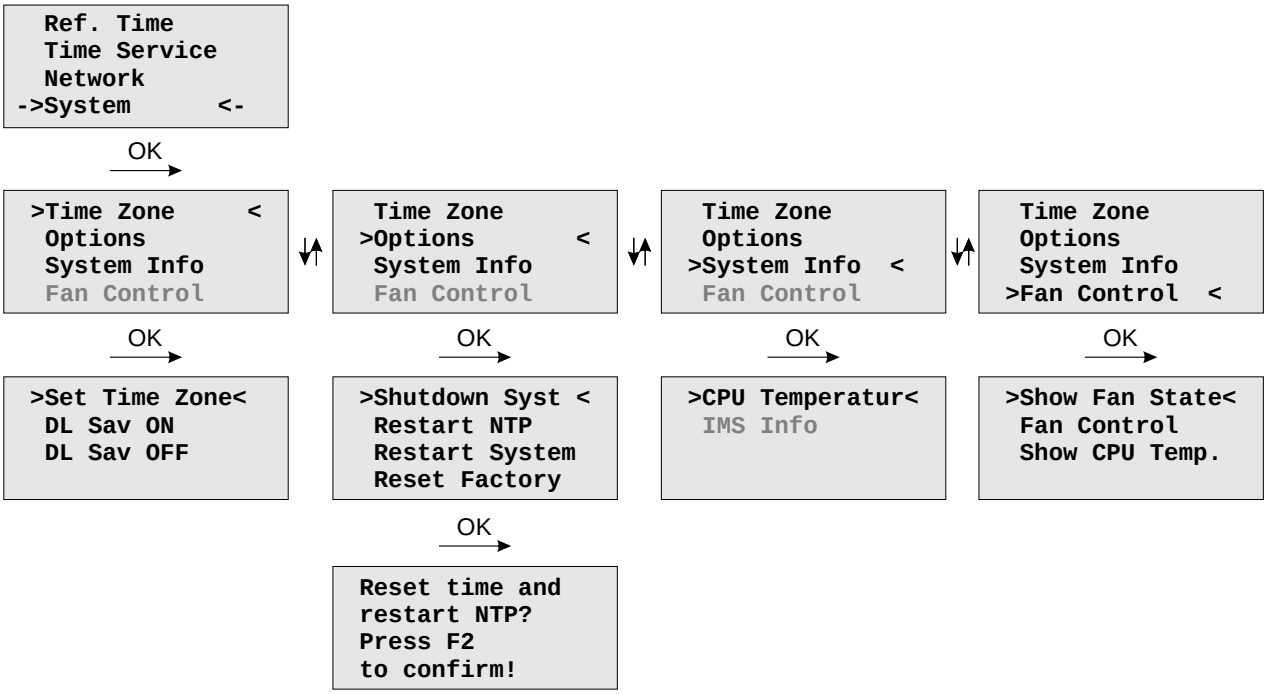
Über das Menü „Check Network Linkup“ kann eingestellt werden, welche Netzwerk Ports auf „LINK UP“ überprüft werden sollen. Wenn eine der ausgewählten Schnittstellen keinen LINK hat, wird die rote LED „Network“ an der Vorderseite des Gerätes eingeschaltet.

13.2.5.6 Menü: Network Services



Im Menü werden die möglichen Dienste angezeigt, die der LANTIME zur Verfügung stellt: SSH, TELNET, SNMP, FTP, IPv6, HTTP, HTTPS und NETBIOS. Die einzelnen Dienste können über die Auf/Ab Tasten aktiviert oder deaktiviert werden. Die Navigation durch die Liste erfolgt mit Hilfe der Rechts/Links Tasten. Die Dienste werden direkt nach dem Abspeichern mit OK entsprechend gestartet oder beendet.

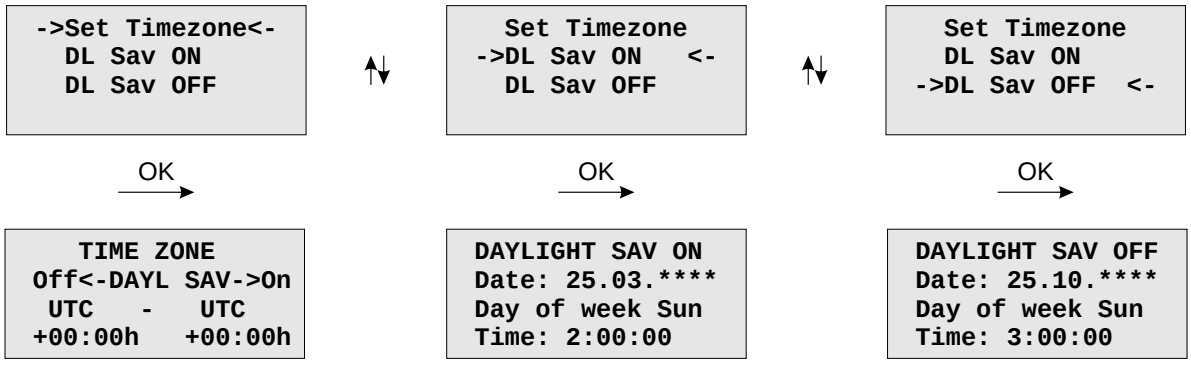
13.2.6 Menü: System



In diesem Untermenü werden systemspezifische Parameter festgelegt.

13.2.6.1 Menü: Set Time Zone (Display)

In diesem Menü wird die Zeitzone für die Anzeige im Display eingestellt. Diese Einstellungen wirken sich nicht auf die seriellen Schnittstellen und die Timecode Ausgänge aus. Die interne Zeit des Zeitservers und die NTP Zeit bezieht sich immer auf UTC und ist unabhängig von diesen Einstellungen der Zeitzone. Die Zeitzone für die seriellen Schnittstellen wird über ein anderes Menü eingestellt - **(Reference Time->Serial Outputs)**.



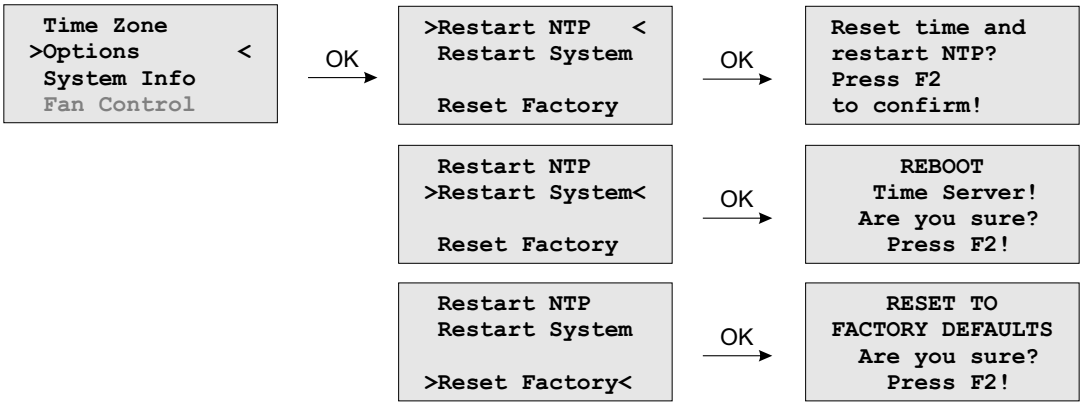
Im ersten Untermenü (Daylight Saving OFF) werden die Einstellungen für die normale Ortszeit (Winterzeit) vorgenommen. Im zweiten Untermenü (Daylight Saving ON) wird hingegen die Sommerzeit konfiguriert.

Nach der Auswahl einer von beiden Menüpunkten gelangt man hier zu den Einstellmöglichkeiten der Winter- bzw. Sommerzeit. Exemplarisch wird in der oben angegebenen Abbildung die Konfiguration der Winterzeit aufgezeigt.

In der ersten editierbaren Zeile werden Name und Abweichung für die normale Ortszeit angegeben (z.B.: MEZ = UTC + 1h).
Die beiden folgenden Zeilen dienen der Eingabe des Umschaltzeitpunktes, in dem die Winterzeit aktiviert wird. GPS bietet zwei Möglichkeiten zur Eingabe von Sommer-/Winterzeit: Entweder werden Datum und Uhrzeit der Umschaltpunkte für ein Jahr exakt definiert oder es werden Randbedingungen gesetzt, mit deren Hilfe das Gerät automatisch für mehrere Jahre den Tag der Umschaltung bestimmen kann. Die Abbildungen unten zeigen beide Varianten: Wird die Jahreszahl als '*' angezeigt, muss ein Wochentag eingegeben werden; dann ist der Tag der Umschaltung der erste Tag ab dem eingegebenen Datum, der mit dem eingegebenen Wochentag übereinstimmt. In der Abbildung unten ist z.B. der 25.10. im Jahr 2008 ein Samstag, am darauf folgenden Sonntag, den 26.10., zur angegebenen Uhrzeit, findet die Umschaltung auf Winterzeit statt. Wird eine bestimmte Jahreszahl eingegeben, ist der Tag der Umschaltung genau festgelegt und der Wochentag wird als '*' angezeigt.

Für den Fall, dass keine Sommerzeitumstellung benötigt wird, sind unter beiden Menüpunkten (DAYlight SAVING ON / OFF) beliebige aber exakt gleiche Daten, Zeiten und Offsets zu setzen.

13.2.6.2 Menü Options



Im Menü Optionen können folgende Einstellungen vorgenommen oder Einstellungsinformationen abgerufen werden:

Time Zone: Die für die konfigurierte Zeitzone umgerechnete Zeit (Offset zu UTC), die im Display angezeigt wird. Das hat keine Auswirkung auf die Zeittelegramme, die über die seriellen Schnittstellen ausgegeben werden.

Diese Einstellung kann über das Menü
„Ref. Time -> Set Outputs -> Output Options -> Time Zone“ vorgenommen werden.

Options: In diesem Untermenü kann das System mit „Reset Factory“ auf den Auslieferungszustan zurückgesetzt werden. Die Netzwerkeinstellungen bleiben hier unverändert.

Mit „Restart NTP“ wird der NTP Dienst neu gestartet und mit „Restart System“ das Linux Betriebssystem der CPU.

System Info: Mit „System Info“ kann die aktuelle Betriebstemperatur der CPU abgefragt werden. Sollte der LANTIME in einem IMS System eingesetzt sein, können hier auch noch Informationen über die Konfiguration des Systems, wie die Belegung der einzelnen Steckplätze, angezeigt werden.

Fan Control: Sollte eine aktive Kühlung eingebaut sein, wird über diesen Menüpunkt der Status der Kühlung angezeigt und über „Fan Control“ kann der Modus der aktiven Kühlung eingestellt werden:

Auto: (temperaturabhängig - der Schwellenwert kann über das Webinterface angepasst werden - Menü *„System -> Fan Control“*.

FAN ON: die Kühlung läuft immer.

FAN OFF: die Kühlung ist immer aus).

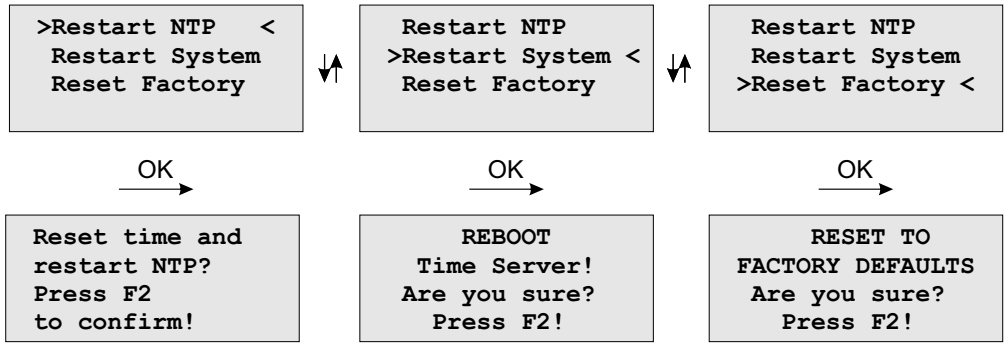
13.2.6.3 Shutdown System

Vor dem Ausschalten des Systems durch einen Netzschalter ist darauf zu achten, dass nicht Prozesse unterbrochen werden, die erst noch beendet werden müssen bevor das Gerät ausgeschaltet wird. Der Sync-Monitor kann zum Beispiel im Moment des Ausschaltens Daten auf der internen Flash speichern, die durch ein abruptes Ausschalten verloren gehen würden.

```
>Shutdown Syst <
 Restart NTP
 Restart System
 Reset Factory
```

Der „Shutdown“ stoppt den LANTIME-Daemon und Sync-Monitor und bereitet das System auf das Herunterfahren vor.

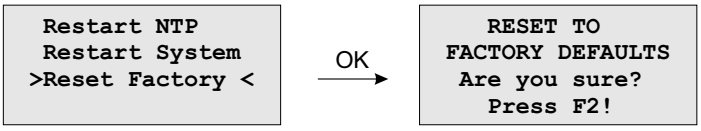
13.2.6.4 Menü: Restart System



Wenn zu Testzwecken die Uhrzeit der GPS verstellt wurde, muss die Uhrzeit des Systems ebenfalls gesetzt werden. Der NTP beendet sich, wenn die Zeitabweichung zwischen der Referenzuhr (GPS) und der Systemzeit mehr als 1000 Sekunden abweicht. Mit diesem Menüpunkt wird die Systemzeit einmalig mit der Referenzuhr gesetzt und der NTP neu gestartet.

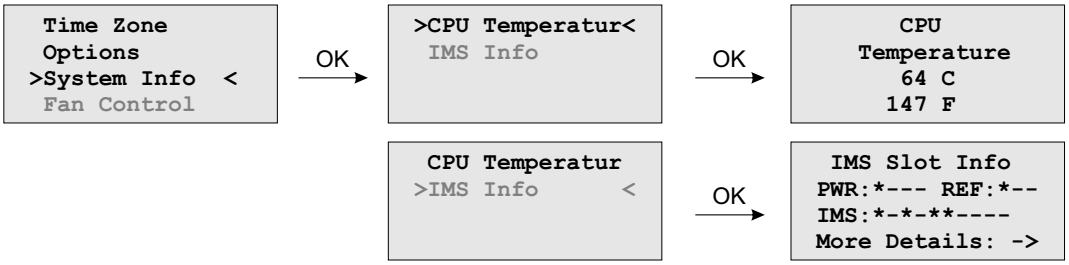
Über den Punkt **Reboot time server** wird das Betriebssystem neu gestartet – die eingebaute Referenz Uhr wird nicht neu gestartet.

13.2.6.5 Menü Factory Reset



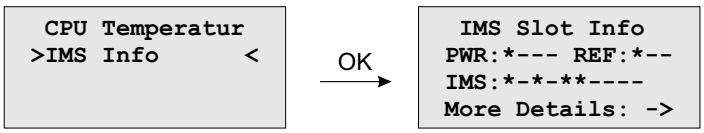
Wird der Menüpunkt **Reset to Factory Defaults** aufgerufen und bestätigt, werden alle Netzwerk Parameter und Systemparameter auf die Werkseinstellung zurückgesetzt.

13.2.6.6 Menü System Info



Im Menü System Info kann die CPU Temperatur abgefragt werden. Bei IMS Systemen kann hier auch eine detaillierte Übersicht über die Systemkonfiguration angezeigt werden.

13.2.6.7 Option: Menü IMS Slot Info

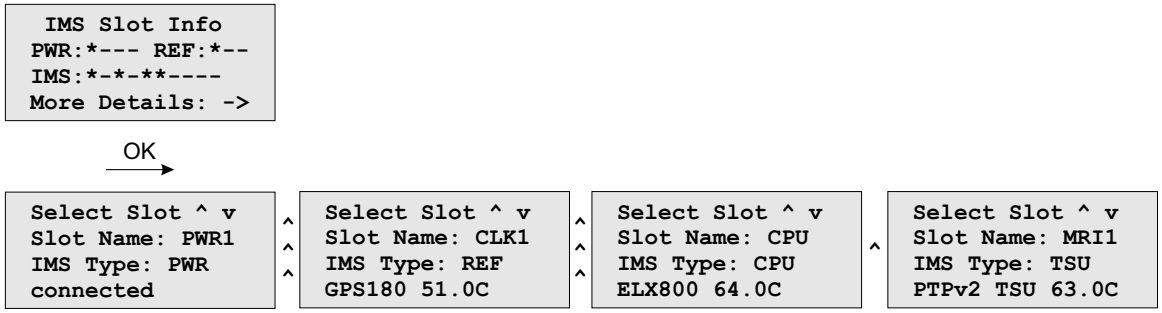


Hinweis: Dieses Menü ist nur bei IMS Systemen sichtbar. Hier wird eine detaillierte Übersicht über die verwendeten Module in den ausgewählten Söts aufgelistet.

Das Beispiel oben zeigt die Konfiguration eines LANTIME M3000:

PWR:*— Die Zeichenkette bedeutet, das PWR 1 aktiv belegt ist.
REF:*– CLK 1 ist belegt, CLK 2 und RSC (SCU Slot) sind frei.
IMS:*-*-**—- Zeigt an, dass die IMS I/O Slots MRI 1, ESI 1 sowie IO 1 und IO2 belegt sind.
More Details: ->Mit der OK Taste kann in das Untermenü „Select Slot“ ’gesprungen werden.

13.2.6.8 Option: IMS Menü Select Slots

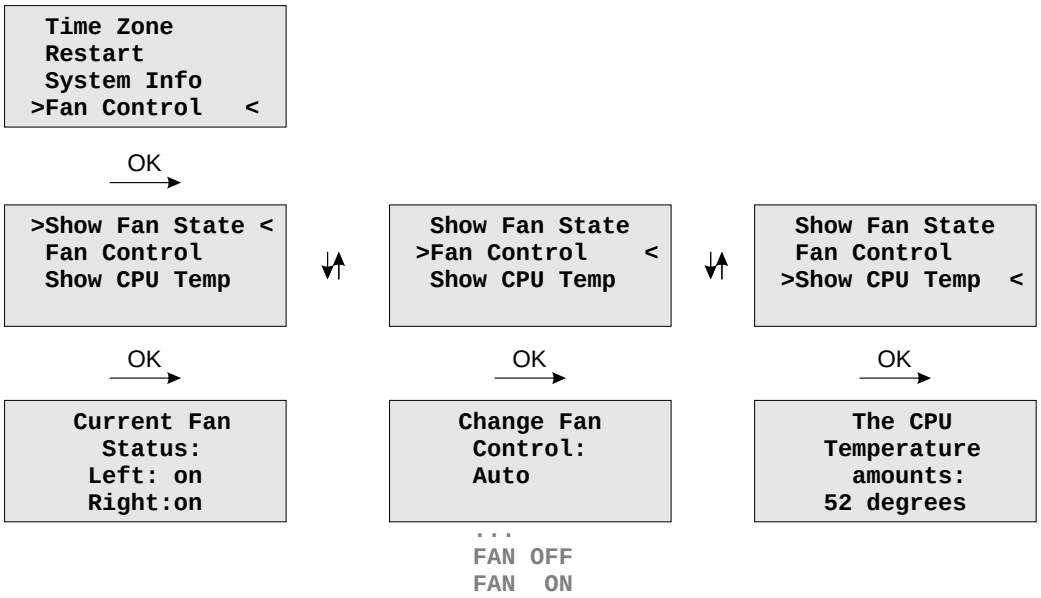


In diesem Menü wird angezeigt, welches Modul in dem ausgewählten Steckplatz eingesetzt ist.

Angezeigte Werte sind:
Slot Name: In diesem Beispiel PWR1, CLK1, CPU, MRI1, IO1 und IO2
IMS Type: PWR (Netzteil), REF (Empfänger), CPU (Prozessoreinheit), LIU (Telekom Ausgänge) ...

In der unteren Zeile wird noch die momentane Betriebstemperatur (Grad/Celsius) angezeigt.

13.2.6.9 Option: Fan Control



Mit dem optionalen Menü Fan Control wird der aktuelle Status der Ventilatoren angezeigt.
Außerdem kann im Untermenü „Fan CFontrol“ der Modus eingestellt werden:

FAN ON	Die Ventilatoren laufen immer
FAN OFF	Die Ventilatoren sind ausgeschaltet
Auto	Die Belüftung läuft ab der Temperatur an, die durch den Parameter „Temperature Threshold“ festgelegt wird (siehe „Das Web Interface“).Im Auslieferungszustand sind +55 Grad Celsius voreingestellt. Die Temperatur des Gerätes muss erst den festgelegten Wert um ca. 7 Grad Celsius unterschreiten, damit die Ventilation automatisch abgeschaltet wird.

13.2.7 USB Stick

LANTIME NTP-Server verfügen über eine USB-Schnittstelle zum Anschluss eines USB-Speichermediums. Der USB-Stick kann in Kombination mit dem LANTIME bzw. mit der LAN-CPU für verschiedene Aufgaben verwendet werden:

- Übertragung von Konfigurationen auf mehrere LANTIME-Server
- Key-Pad-Locking zur sicheren Nutzung der Tastatur des LCD-Bildschirms
- Übertragung von Protokolldateien
- Software-Updates installieren
- Hoch- und Herunterladen sicherer Zertifikate (SSL, SSH) und Passwörter

Beim Anschluss des USB-Sticks signalisiert das LC-Display nach einigen Sekunden, dass der USB-Stick erkannt wurde und ermöglicht es Ihnen, mit der Taste „OK“ in das USB-Menü zu gelangen.

```
USB Memory Stick
(OK to confirm)
```

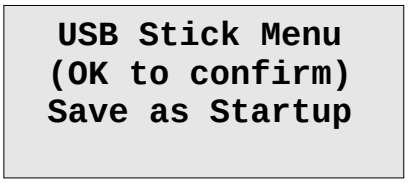
Die gewünschte Menüfunktion kann mit den Tasten ↑ und ↓ ausgewählt und mit der Taste „OK“ aktiviert werden. Sie können dieses Menü durch Entfernen des USB-Sticks oder mit der Taste „ESC“ verlassen.

Menü „Install Firmware“
Wenn eine Firmware-Update-Datei auf dem USB-Stick gespeichert ist, erscheint der Menüpunkt **„Install [Firmware Version]“** auf dem Display. Nun können Sie das Update-Paket auf dem LANTIME durch Drücken der OK-Taste installieren. Die Datei hat das Format *„firmware-7.00.007-x86.rel“*. Im Display wird jedoch nur die Version angezeigt, in diesem Beispiel die *7.00.007-x86*.

```
USB Stick Menu
(OK to confirm)
   Install
7.xx.xxx-x86
```

Hinweis:
Nach dem Hochladen der neuen Firmware auf den LANTIME, muss diese noch über das Webinterface (Menü System → Firmware/Software Update) oder das CLI (Command Line Interface) aktiviert werden.

Menü „Save as Startup“
Wird dieser Menüpunkt mit der OK-Taste bestätigt, wird die aktuell als „Startkonfiguration“ gespeicherte Firmware-Konfiguration des LANTIME auf dem USB-Stick gespeichert.



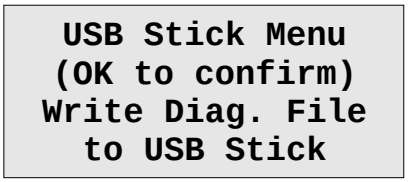
Hinweis:
Auch wenn Sie gerade Änderungen an einem LANTIME vornehmen, können Sie nur die Konfiguration auf dem USB-Stick speichern, welche Sie über die Weboberfläche als „Startup-Konfiguration“ bestätigt haben. Das hat den Vorteil, dass Sie auch bei umfangreichen Änderungen an den Einstellungen Ihres Systems eine Sicherung Ihrer „alten“ Konfiguration durchführen können.

Menü „Backup Configuration to USB Stick“
In diesem Untermenü können Sie die Konfigurationsdatei von Ihrem LANTIME auf das USB-Speichermedium kopieren, die Sie dann auf Ihrem USB-Stick unter */Lantime/Config/USB_Backup/xxxxxxxxxxxxx* finden (xxx.... = die 12-stellige Seriennummer Ihres LANTIME).

Hinweis:
Die auf den USB-Stick kopierte Konfiguration ist immer die aktuell gespeicherte „Start-Up-Konfiguration“ des Systems.

Wenn die Sicherung auf anderen LANTIMEs importiert werden soll, muss das Verzeichnis umbenannt werden: */Lantime/Config/USB_Backup/ANY_SN*

Menü „Write Diagnostic File to USB Stick“



Dieses Untermenü ist eine einfache Möglichkeit, den Inhalt der LANTIME-Diagnosedatei abzurufen. Nachdem Sie auf die Schaltfläche OK geklickt haben, kopiert das System ein Dateiarchiv auf Ihr USB-Speichemedium: */Lantime/Diag/ltdiag.tgz*

Keypad locking
Der USB-Stick kann zum Sperren der Funktionstasten des LANTIME LC-Displays verwendet werden. Bei Aktivierung dieser Funktion kann der Benutzer die Tasten nicht verwenden, ohne den USB-Stick mit dem LANTIME zu verbinden. Die Zugangsberechtigung wurde mit einer Passwortdatei auf dem USB-Stick */Lantime/keypad_lock* realisiert. Diese Passwortdatei wird mit */mnt/flash/config/keypad_lock* verglichen. So ist es möglich, verschiedene LANTIMEs mit nur einem USB-Stick zu verwalten.

Die Tastatursperre wird mit einem Untermenü vom USB-Stick-Menü aktiviert:

Bei Aktivierung dieses Untermenüs wird die Datei */mnt/flash/config/keypad_lock* in den internen Flash-Memory kopiert. Wenn Sie die Tastatursperre deaktivieren, wird diese Datei aus dem internen Flash entfernt.

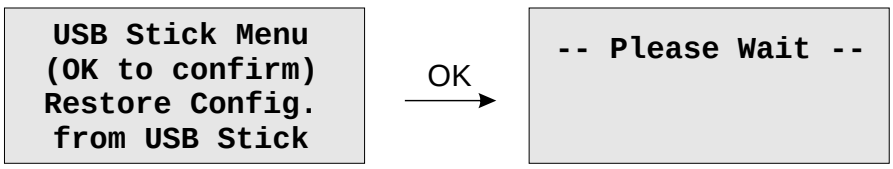
Hinweis:
Make sure, that you never loose the „Keypad_Lock" file or the USB storage device! If you have problems, please contact Meinberg Radio clocks: Mail to techsupport@meinberg.de .

Menü Restore Configuration
Dieser Befehl dient zur Wiederherstellung der LANTIME-Konfiguration. Nach diesem Vorgang startet der Zeitserver neu.

1. Es wird ein USB-Stick benötigt, auf dem eine Sicherungsdatei gespeichert ist.

2. Das Backup wird nur importiert, wenn ein Verzeichnis mit der entsprechenden SN verfügbar ist (oder „ANY_SN").

3. Nach „Restore" ist die Konfiguration noch nicht bootfähig. Um dies zu aktivieren, müssen Sie zunächst die Funktion *'saveconfig'* über eine CLI (Konsolenprogramm) oder über das Web-Interface ausführen. Im Webinterface drücken Sie am Ende die Schaltfläche „Als Startkonfiguration ausführen".



13.3 Über eine serielle Verbindung

Erste Inbetriebnahme: LANTIME Konfigurations-Assistent>
Nach der Bootphase des Gerätes müssen Sie eine serielle Verbindung mit der LAN-CPU herstellen. Über die Terminalverbindung ist es möglich, Parameter mit einer Kommandozeilenschnittstelle zu konfigurieren. Verwenden Sie ein NULL-Modem-Kabel oder ein CAB-CONSOLE-RJ45-Kabel, um Ihren PC oder Laptop anzuschließen. Sie können z.B. das Standardprogramm „Hyperterminal“ verwenden, das mit Ihrem Windows-Betriebssystem ausgeliefert wird. Konfigurieren Sie Ihr Terminalprogramm mit 38400 Baud, 8 Datenbits, No Parity und 1 Stopbit. Die Terminalemulation muss auf VT100 eingestellt sein. Nach dem Anschließen des LANTIME erscheint die Login-Meldung (drücken Sie RETURN für die Erstverbindung):

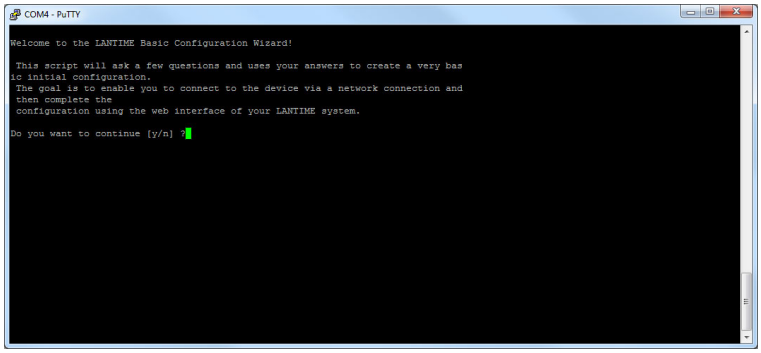
Nachdem die Verbindung erfolgreich hergestellt wurde, verwenden Sie Ihre Anmeldedaten im Begrüßungsbildschirm.

```
Welcome to Meinberg LANTIME
login: _
```

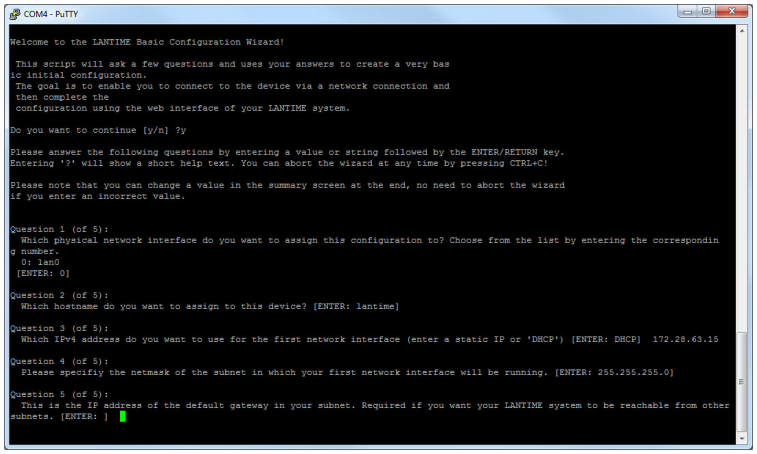
Die Standardeinstellungen sind:
Login: **root**
Passwort: **timeserver**
(Es kann vorkommen, dass Sie die ENTER-Taste erneut betätigen müssen).

Nach erfolgreicher Anmeldung ändern Sie den aktuellen Pfad zu */wizard/*. Starten Sie jetzt den LANTIME Basic Configuration Wizard mit dem Befehl „startwizard“.

Der folgende Willkommensbildschirm des Assistenten wird nun angezeigt:



Bestätigen Sie mit „y“, um die Konfiguration für alle folgenden Einstellungen zu starten.



Am Ende bestätigen Sie bitte Ihre Konfiguration.

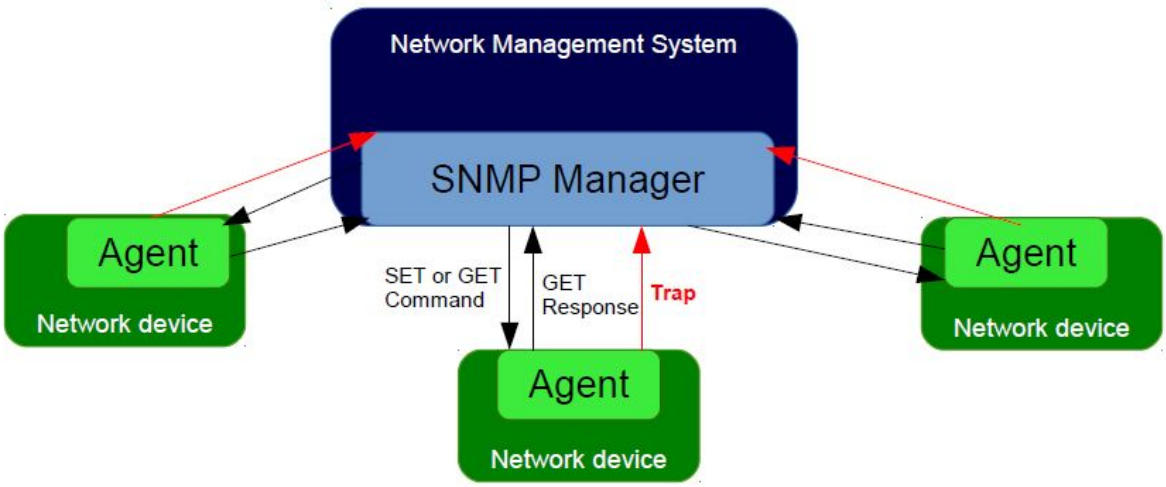
Nachdem dem LANTIME eine korrekte IP-Adresse zugewiesen wurde, können alle anderen Einstellungen über die umfangreiche und leistungsfähige Weboberfläche vorgenommen werden (siehe Kapitel Das Webinterface).

13.4 Monitoring über SNMP

13.4.1 Das Simple Network Managment Protocol

Die meisten vernetzten Geräte unterstützen eine Reihe von Verwaltungsoptionen, darunter das Simple Network Management Protocol (SNMP). SNMP ist ein Netzwerkprotokoll, das es einem einzelnen Netzwerkmanagementsystem ermöglicht, eine große Anzahl von Geräten im Netzwerk zu überwachen.

Die Funktionsweise ist, dass jedes Netzwerkelement einen „Agent“ hat, der mit dem Manager über SNMP kommuniziert. Jeder Agent verfügt über eine entsprechende „Management Information Base“, kurz MIB. Die MIBs organisieren Datenelemente in einer Baumstruktur. Es ist in einer standardisierten und strukturierten Sprache geschrieben, so dass die MIBs aller Geräte im Netzwerk im selben Manager vereint werden können.



MIB-Elemente werden als „Object Identifiers“ oder OIDs bezeichnet. Sie bestehen aus Konfigurationsvariablen, Statusvariablen, Baumstrukturbezeichnungen und Benachrichtigungen. Die OIDs können mit den Befehlen SNMP SET und GET gelesen oder geändert werden. Es gibt auch rekursive Befehle, mit denen der Manager nach allen OIDs in einem Zweig (Teilbaum) oder sogar dem gesamten Baum fragen kann. Dieser Prozess wird als „Walking the MIB“ bezeichnet. Ereignisbenachrichtigungen, allgemein als Traps bezeichnet, sind eine spezielle Art von OID. Ein Trap kann so konfiguriert werden, dass beim Statuswechsel des Geräts sofort eine Nachricht vom Agent an den Manager gesendet wird.

13.4.2 MIB Objekte eines LANTIME

Ein LTOS-Betriebssystem, das auf einem LANTIME-Servern läuft, unterstützt alle SNMP-Versionen (v1, v2c und v3) mit voller Funktionalität. Die properitären LANTIME-OIDs sind in Teilbäume gegliedert, die eine bestimmte Systemkomponente oder eine Betriebsart definieren. Der Hauptteilbaum mit den OIDs, die sich auf den LANTIME-Status verschiedener Modi beziehen, heißt „LantimeNGStatus“, NG steht für „Neue Generation der LANTIME-Features“ in der LANTIME-Firmware. Der „LantimeNGStatus“ besteht aus acht Teilbäumen, in denen Refclock, NTP, PTP, SystemHardware, Cluster und Misc die am wichtigsten zu überwachenden Teilbäume sind.

13.4.2.1 Refclock Subtree

Hier ist eine kurze Liste von OIDs aus dem Teilbaum NGStatus mit entsprechenden Beschreibungen:

mbgLtNgRefclockState
Diese OID beschreibt einen aktuellen Zustand einer LANTIME refclock (Hardware-Uhrenmodul), der sich auf GNSS oder ein anderes Zeitquellensignal im MRS (Multi Reference Source) Modell bezieht.

Status	Beschreibung
0:	*refclock is not available:* Siehe mögliche Fehlerbehebung: 1. Das Refclock-Modul kann nicht aufgerufen werden. 2. Überprüfen Sie, ob es beschädigt ist und ersetzen Sie es gegebenenfalls.
1:	*synchronized:* Die Referenzuhr Ihres Systems ist korrekt mit der ausgewählten Zeitquelle (GNSS oder MRS) synchronisiert. In einem MRS-System kann eine Refclock mit einer Referenzzeitquelle aus der Prioritätenliste synchronisiert werden. Siehe das Beispiel in der nächsten Abbildung. Das obige MRS-System synchronisiert sich zuerst mit GPS, aber wenn das GPS-Signal nicht verfügbar ist, wechselt die Referenzuhr zur nächsten Zeitquelle aus der Prioritätenliste (in unserem Fall PTP). Der Wechsel erfolgt erst nachdem eine „Trust-Time“ der nicht verfügbaren Zeitquelle (GPS-Signal) abgelaufen ist. Das soll verhindern, dass in zu kurzen Zeitperioden von einer Zeitquelle zur anderen gewechselt wird. Sobald GPS wieder verfügbar ist, schaltet die Uhr wieder auf GPS um, ohne auf den Ablauf der PTP-Trust-Tiem zu warten, weil die GPS-Referenz eine höhere Genauigkeit als PTP hat.
2:	*not synchronized:* Offensichtlich ist die refclock nicht mit ihrer Zeitquelle synchronisiert. Hier ist die mögliche Fehlerbehebung: A) Überprüfen Sie, ob die GPS-Antenne angeschlossen ist und die Referenzzeit empfangen wird. Mehr darüber, wie die Meinberg GPS-Antenne richtig zu montieren und zu positionieren ist, erfahren Sie hier. B) Wenn GPS die aktuelle Zeitquelle ist, überprüfen Sie die Anzahl der empfangenen Satelliten. Es sollte mindestens vier sein, um Synchronisationsinformationen bereitzustellen. C) Starten Sie „warm boot“, um die aktuelle Satellitenposition zu ermitteln. Dies ist besonders notwendig, wenn die physische Position Ihres LANTIME um mehr als 100 km von seiner Position verschoben wurde. Der vorherige Standort und die damit veralteten Satellitendaten werden weiterhin im System gespeichert. D) Starten Sie „cold boot“, um das Satelliten-Almanach zu aktualisieren. E) Wenn diese Maßnahmen nicht helfen, muss das GPS-Uhrenmodul ausgetauscht werden.

```
Es wird empfohlen, Ihre Netzwerkmanagement-Software so zu konfigurieren,
dass sie diesen Status regelmäßig, wenn möglich alle 60 Sekunden,
überprüft.
```

mbgLtNgRefclockLeapSecondDate
Diese OID übermittelt Informationen über das nächste Schaltsekundendatum. Wenn das bevorstehende Schaltsekundendatum noch nicht bekannt gegeben wurde, enthält die OID Informationen über das vorherige Schaltsekundenereignis.

Hier ist eine kurze Zusammenfassung der Schaltsekunden. Es gibt zwei verschiedene Zeitskalen, über die wir normalerweise in der Synchronisierungsumgebung sprechen: GPS - steht für Global Positioning System Time und UTC - steht für Universal Time Coordinated. UTC war früher bekannt als GMT (Greenwich Mean Time). Diese Zeitskalen unterscheiden sich voneinander durch die Anzahl der Schaltsekunden, die seit Beginn der GPS-Zeit am 6. Januar 1980 eingeführt wurden. Im Moment des Schreibens liegt das UTC 16 Sekunden hinter der GPS-Zeit. Das ist auf die ungleichmäßige Rotation der Erde zurückzuführen.

```
Da die Einführung einer neuen Schaltsekunde die Zeit im gesamten zu
synchronisierenden System beeinflusst, empfehlen wir, diesen Status
regelmäßig zu überprüfen, z.B. einmal pro Stunde.
```

Die nächsten in einer Reihe von OIDs sind diejenigen, die sich auf den NTP-Status beziehen. Sie befinden sich im Teilbaum „mbgLtNgNtp“.

13.4.2.2 NTP subtree

Hier ist eine kurze Liste von OIDs aus dem Teilbaum NGStatus mit entsprechenden Beschreibungen:

mbgLtNgNtpCurrentState
Eine der wichtigsten OIDs in diesem Teilbaum, die regelmäßig überprüft werden muss. Diese OID informiert über den NTP-Dienst Ihres LANTIME. Es sind drei Zustände möglich:

Status	Beschreibung

0: *not available:* Siehe die mögliche Fehlerbehebung:

A) Überprüfen Sie, ob der NTP-Dienst an einer bestimmten LAN-Schnittstelle tatsächlich aktiviert ist.

Um das zu überprüfen, melden Sie sich über das Webinterface an. Werkseitig voreingestellte Anmeldeinformationen: „root/timeserver“. Gehen Sie zum Menü: „Netzwerk → Netzwerkdienste“ und aktivieren Sie den Service der entsprechenden Schnittstelle (siehe Abbildung 3).

B) Überprüfen Sie, ob die Schnittstelle bzw. der Anschluss beschädigt ist und ersetzen Sie diesen gegebenenfalls.

1: *not synchronized:* Im Falle von „nicht synchronisiert“ ist der NTP-Dienst noch nicht auf einen Referenztakt synchronisiert. Mögliche Ursachen für diesen Zustand sind die folgenden:

A) Der NTP-Daemon befindet sich noch in der Initialisierungsphase, für die er ca. 3-5 Minuten benötigt. Warten Sie daher eine Weile, um zu sehen, ob sich hier der Status ändert.

B) Wenn eine Referenzuhr nicht synchronisiert wird, wird das im NTP-Status angezeigt. In diesem Fall wird der NTP-Daemon auf seine lokale Uhr synchronisiert und sein Stratumwert ändert sich auf 12. Bitte überprüfen Sie die mögliche Fehlerbehebung für einen Refclock-Status wie oben beschrieben.

2. *synchronized* : Der NTP-Dienst befindet sich im Normalbetrieb. Der LANTIME funktioniert nun einwandfrei.

```
Es wird empfohlen, den NTP-Status regelmäßig zu überprüfen,
jedoch nicht öfter als alle 64 s.
```

13.4.2.3 Hardware subtree

mbgLtNgSysPsStatus
Wenn ein LANTIME über ein redundantes Netzteil (RPS) verfügt, ist es wichtig, den Status beider RPS-Module regelmäßig zu überprüfen. Diese PowerSupplyStatus-OID befindet sich im Teilbaum System-Hardware. Die folgenden Zustände sind verfügbar:

Status	Beschreibung
0:	*notAvailable:* Das abgefragte Netzteil wird von einem System nicht erkannt. Überprüfen Sie, ob es beschädigt ist, und ersetzen Sie das Netzteil gegebenenfalls.
1:	*down:* Das abgefragte Netzteil ist nicht in Betrieb. Überprüfen Sie, ob es beschädigt ist, und ersetzen Sie das Netzteil gegebenenfalls.
2:	*up:* Das abgefragte Stromversorgungsmodul ist in Betrieb.

```
Es wird empfohlen, diese OID alle 60 s zu überprüfen.
```

13.4.2.4 Misc subtree

mbgLtNgEthPortLinkState
Im Teilbaum mbgLtNgMisc befindet sich eine „EthPortLinkState OID", die den Status jedes physikalischen Ethernet-Ports eines LANTIME identifiziert. Verfügbare Werte sind:

Status	Beschreibung
0:	*notAvailable:* Der abgefragte Port ist ausgefallen, überprüfen Sie die Link-LED. Bei einem Defekt ersetzen Sie die Netzwerkkarte.
1:	*up:* Der abgefragte Port befindet sich im Normalbetrieb.

```
Es wird empfohlen, diese OID alle 60 s zu überprüfen.
```

13.4.2.5 PTP subtree

Wenn Ihr LANTIME über eine IEEE 1588 PTPv2-Funktionalität verfügt, finden Sie die entsprechenden PTP-OIDs im Teilbaum „mbgLtNgPtp“. Hier sind die wichtigsten zu überwachenden OIDs:

mbgLtNgPtpPortState
Die folgenden PTP-Portzustände sind möglich:

Status	Beschreibung
0:	*uninitialized:* Der Port bootet, der Software-Daemon ist noch nicht gestartet, die IP-Adresse ist noch nicht vergeben.
1:	*initializing:* In diesem Zustand initialisiert der Port seine Datensätze, Hardware und Kommunikationseinrichtungen.
2:	*faulty:* Nicht in einem LANTIME definiert.
3:	*disabled:* Der PTP-Dienst wurde an diesem Port deaktiviert, entweder durch Benutzerkonfiguration oder weil sich das Modul im Standby-Modus befindet.
4:	*listening:* Der Port wartet darauf, dass der „announceReceiptTimeout“ abläuft oder dass er eine Announce-Nachricht von einem Master erhält.
5:	*preMaster:* Ein kurzer Übergangszustand, während der Port zum Master wird.
6:	*master:* Der Port ist ein aktueller Master.
7:	*passive:* Der Port befindet sich im passiven Modus, d.h. es ist eine weiterer Masterclock in der PTP-Domäne aktiv. Der Port kann in den Masterstatus wechseln, wenn er den BMCA aufgrund eines Ausfalls/Dienstabfalls des aktuellen Masters gewinnt.
8:	*uncalibrated:* Ein oder mehrere Master-Ports wurden in der Domäne erkannt.
9:	*slave:* Der Port hat sich erfolgreich bei einem Master angemeldet und empfängt alle erwarteten Nachrichten. Es wurde auch erfolgreich die Pfadverzögerung (Path Delay) mit Hilfe von „Delay Request Messages“ gemessen.

```
Es wird empfohlen, die PtpPortState OID alle 3 s zu überwachen.
```

13.4.3 SNMP Traps

SNMP Trap Name:	mbgLtNgTrapNTPNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.1
Schweregrad:	Warnung oder kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn NTP nicht synchron ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → NTP-Nachrichten → NTP Not Sync
Aufgehoben durch:	mbgLtNgTrapNTPSync

SNMP Trap Name:	mbgLtNgTrapNTPStopped
OID:	.1.3.6.1.4.1.5597.30.3.0.2
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn gestoppt ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → NTP-Nachrichten → NTP Stopped
Aufgehoben durch:	MbgLtNgTrapNTPSync or mbgLtNgTrapNTPNotSync

SNMP Trap Name:	mbgLtNgTrapServerBoot
OID:	.1.3.6.1.4.1.5597.30.3.0.3
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Zeitserver die Boot-Sequenz beendet hat
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapReceiverNotResponding
OID:	.1.3.6.1.4.1.5597.30.3.0.4
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der Empfänger nicht antwortet.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Rsponding
Aufgehoben durch:	MbgLtNgTrapReceiverNotSync or mbgLtNgTrapReceiverSync

SNMP Trap Name:	mbgLtNgTrapReceiverNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.5
Schweregrad:	Fehler
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der Empfänger nicht synchronisiert ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Sync
Aufgehoben durch:	mbgLtNgTrapReceiverSync

SNMP Trap Name:	mbgLtNgTrapAntennaFaulty
OID:	.1.3.6.1.4.1.5597.30.3.0.6
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, die gesendet werden soll, wenn die Verbindung zur Antenne unterbrochen ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Antenna Faulty
Aufgehoben durch:	mbgLtNgTrapAntennaReconnect

SNMP Trap Name:	mbgLtNgTrapAntennaReconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.7
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn die Antenne wieder angeschlossen ist
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapConfigChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.8
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Zeitserver seine Konfiguration neu geladen hat.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapLeapSecondAnnounced
OID:	.1.3.6.1.4.1.5597.30.3.0.9
Schweregrad:	Info-Warnung
Kurzbeschreibung:	trap to be sent when a leap second has been announced
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Leap Second Announced Managm./Mon. → NTP → Leap Second Handling
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitError
OID:	.1.3.6.1.4.1.5597.30.3.0.10
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der bei Überschreitung des SHS-Zeitlimits gesendet wird
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → SHS Time Limit Warning Managm./Mon. → Webinterface → Einleitung LTOS 6 Managm./Mon. → Webinterface → Sicherheit → SHS Modus LTOS 6 Managm./Mon. → Webinterface → Sicherheit → SHS Time Limit
Aufgehoben durch:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.11
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der sekundäre Empfänger nicht synchronisiert ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Sync
Aufgehoben durch:	mbgLtNgTrapSecondaryRecSync

SNMP Trap Name:	mbgLtNgTrapPowerSupplyFailure
OID:	.1.3.6.1.4.1.5597.30.3.0.12
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn eine der redundanten Stromversorgungen ausfällt.
Referenz zu anderen Kapitel:	Wichtige Sicherheitshinweise → Sicherheit bei der Installation Wichtige Sicherheitshinweise → Sicherheit im laufenden Betrieb
Aufgehoben durch:	mbgLtNgTrapPowerSupplyUp

SNMP Trap Name:	mbgLtNgTrapAntennaShortCircuit
OID:	.1.3.6.1.4.1.5597.30.3.0.13
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn eine angeschlossene Antenne aufgrund eines Kurzschlusses ausfällt.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Antenna Short Circuit
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapReceiverSync
OID:	.1.3.6.1.4.1.5597.30.3.0.14
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der bei synchronisiertem Empfänger gesendet wird
Referenz zu anderen Kapitel:	Antennen- und Empfängerinformationen → Referenzzeitquellen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPClientAlarm
OID:	.1.3.6.1.4.1.5597.30.3.0.15
Schweregrad:	Error
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein NTP Client Monitoring Alarm auftritt, z.B. wenn ein überwachter Client nicht erreichbar ist.
Referenz zu anderen Kapitel:	Überprüfen Sie die Netzwerkkonfiguration unter Managm./Mon. → Netzwerk
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPowerSupplyUp
OID:	.1.3.6.1.4.1.5597.30.3.0.16
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Netzteil wieder in einen korrekten Zustand versetzt wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNetworkDown
OID:	.1.3.6.1.4.1.5597.30.3.0.17
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn ein überwachter Netzwerk-Port ausgefallen ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Netzwerk-Nachrichten → Network Link Down
Aufgehoben durch:	mbgLtNgTrapNetworkUp

SNMP Trap Name:	mbgLtNgTrapNetworkUp
OID:	.1.3.6.1.4.1.5597.30.3.0.18
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn ein überwachtes Netzwerk-Port aktiv ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotRespp
OID:	.1.3.6.1.4.1.5597.30.3.0.19
Schweregrad:	Warnung oder kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn der sekundäre Empfänger nicht antwortet.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Responding
Aufgehoben durch:	mbgLtNgTrapSecondaryRecSync

SNMP Trap Name:	mbgLtNgTrapMrsLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.30
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Referenzoffset den konfigurierten Grenzwert überschreitet.
Referenz zu anderen Kapitel:	LTOS 6 Managm./Mon. → Webinterface → Clock → MRS Settings Troubleshooting und Alarmierungen → Referenzuhr → MRS Limit Exceed
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapMrsRefDisconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.31
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Referenzsignal verloren gegangen ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → MRS Reference Disconnected
Aufgehoben durch:	mbgLtNgTrapMRSRefReconnect

SNMP Trap Name:	mbgLtNgTrapMRSRefReconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.32
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Referenzsignal wiederhergestellt wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapFdmError
OID:	.1.3.6.1.4.1.5597.30.3.0.33
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein FDM-Modul einen Alarm erzeugt.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → FDM → FDM Konfiguration
Aufgehoben durch:	mbgLtNgTrapFDMOk

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitWarning
OID:	.1.3.6.1.4.1.5597.30.3.0.34
Schweregrad:	Warnung, kritisch
Kurzbeschreibung:	Trap, der bei Überschreitung der SHS-Warngrenze gesendet wird.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Einleitung Managm./Mon. → Webinterface → Security → SHS Konfiguration Managm./Mon. → Webinterface → Security → SHS Modus Troubleshooting und Alarmierungen → Referenzuhr → SHS Time Limit Warning
Aufgehoben durch:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecSync
OID:	.1.3.6.1.4.1.5597.30.3.0.35
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der sekundäre Empfänger synchronisiert ist.
Referenz zu anderen Kapitel:	Antennen- und Empfänger-Information → Referenzzeitquellen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPSync
OID:	.1.3.6.1.4.1.5597.30.3.0.36
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn NTP synchronisiert wird
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPtpPortDisconnected
OID:	.1.3.6.1.4.1.5597.30.3.0.37
Schweregrad:	Warnung oder kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn der PTP-Netzwerkanschluss getrennt wurde.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → PTP → PTP Globaler Status
Aufgehoben durch:	mbgLtNgTrapPtpPortConnected

SNMP Trap Name:	mbgLtNgTrapPtpPortConnected
OID:	.1.3.6.1.4.1.5597.30.3.0.38
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der PTP-Netzwerkanschluss verbunden wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPtpStateChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.39
Schweregrad:	Info-Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn sich der PTP-Zustand geändert hat (z.B. von „passiv“ auf „Master“).
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → PTP → PTP Globaler Status
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPtpError
OID:	.1.3.6.1.4.1.5597.30.3.0.40
Schweregrad:	Warnung, kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn PTP einen Fehler ausgelöst hat.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → PTP → PTP Globaler Status
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapLowSystemResources
OID:	.1.3.6.1.4.1.5597.30.3.0.41
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System mit geringen Ressourcen läuft.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapSufficientSystemResources

SNMP Trap Name:	mbgLtNgTrapFanDown
OID:	.1.3.6.1.4.1.5597.30.3.0.45
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Lüfter ausfällt.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Sonstige Meldungen → Fan Failure
Aufgehoben durch:	mbgLtNgTrapFanUp

SNMP Trap Name:	mbgLtNgTrapFanUp
OID:	.1.3.6.1.4.1.5597.30.3.0.46
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Lüfter hochfährt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapCertificateExpired
OID:	.1.3.6.1.4.1.5597.30.3.0.47
Schweregrad:	Info oder Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn das HTTPS-Zertifikat abläuft oder ablaufen wird.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Sicherheit → HTTPS-Zertifikat
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSufficientSystemResources
OID:	.1.3.6.1.4.1.5597.30.3.0.48
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System wieder genügend Ressourcen erhalten hat.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.49
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Oszillator aufgewärmt ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorNotWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.50
Schweregrad:	Information
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der Oszillator nicht aufgewärmt ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Oscillator not Adjusted
Aufgehoben durch:	mbgLtNgTrapOscillatorWarmedUp

SNMP Trap Name:	mbgLtNgTrapMRSRefChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.51
Schweregrad:	Info-Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn die MRS-Referenzquelle geändert wurde.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapClusterMasterChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.52
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Cluster-Modus aktiv ist und der Cluster geändert wurde.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Netzwerk → Netzwerkschnittstellen → Cluster
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerDetected
OID:	.1.3.6.1.4.1.5597.30.3.0.53
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der bei aktivem Cluster-Modus gesendet werden soll, und ein Cluster-Mitglied wird als Falseticker erkannt.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Netzwerk → Netzwerkschnittstellen - Cluster
Aufgehoben durch:	mbgLtNgTrapClusterFalsetickerCleared

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerCleared
OID:	.1.3.6.1.4.1.5597.30.3.0.54
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der bei aktivem Cluster-Modus gesendet werden soll, und ein Clustermitglied ist kein Falseticker mehr.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.55
Schweregrad:	Information
Kurzbeschreibung:	Trap, der gesendet wird, wenn der SHS-Zeitlimitfehler bestätigt wurde. oder die Zeitdifferenz fällt unter den Warngrenzwert.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Einleitung
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapIMSError
OID:	.1.3.6.1.4.1.5597.30.3.0.56
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein IMS-Modul nicht mehr reagiert - hat Temperaturprobleme, etc.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Sonstige Meldungen → IMS Error
Aufgehoben durch:	mbgLtNgTrapIMSOk

SNMP Trap Name:	mbgLtNgTrapIMSOk
OID:	.1.3.6.1.4.1.5597.30.3.0.57
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein IMS-Modul in einen normalen Zustand zurückkehrt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapFDMOk
OID:	.1.3.6.1.4.1.5597.30.3.0.58
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein FDM-Modul in einen normalen Zustand zurückkehrt.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → FDM → FDM Konfiguration
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.59
Schweregrad:	Error
Kurzbeschreibung:	Trap, der bei der Überwachung eines NTP-Clients und seiner Umgebung gesendet wird. Offset-Grenze wird überschritten.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → NTP-Nachrichten → NTP Offset Limit Exceeded
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.60
Schweregrad:	Info
Kurzbeschreibung:	Trap, der bei der Überwachung eines NTP-Clients und seiner Umgebung gesendet wird. Offset-Grenze ist wieder in einem gültigen Bereich.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapNTPOffsetLimitExceeded

SNMP Trap Name:	mbgLtNgTrapXheRubOk
OID:	.1.3.6.1.4.1.5597.30.3.0.61
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn externes Rubidium OK meldet.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapXheRubError
OID:	.1.3.6.1.4.1.5597.30.3.0.62
Schweregrad:	Error
Kurzbeschreibung:	Trap, der gesendet wird, wenn externes Rubidium einen Fehler meldet.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapXheRubOk

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.63
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System zu viel Strom verbraucht.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapPowerConsumptionOk

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionOk
OID:	.1.3.6.1.4.1.5597.30.3.0.64
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System über ausreichend Strom verfügt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyNotAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.65
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn kein Backup der Stromversorgung verfügbar ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapPowerRedundancyAvail

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.66
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn mindestens eine Stromnetzteil als Backup vorhanden ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapTrustedSourceError
OID:	.1.3.6.1.4.1.5597.30.3.0.67
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn die Zeitabweichung einer MRS-Quelle die konfigurierte Grenze überschreitet.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapTrustedSourceOk

SNMP Trap Name:	mbgLtNgTrapTrustedSourceOk
OID:	.1.3.6.1.4.1.5597.30.3.0.68
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn die Zeitabweichung einer MRS-Quelle zu ihrer konfigurierten Grenze zurückkehrt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNormalOperation
OID:	.1.3.6.1.4.1.5597.30.3.0.77
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System in den Normalbetrieb zurückkehrt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapHeartbeat
OID:	.1.3.6.1.4.1.5597.30.3.0.88
Schweregrad:	Information
Kurzbeschreibung:	Trap, der regelmäßig gesendet wird, um anzuzeigen, dass der Zeitserver noch arbeitet.
Referenz zu anderen Kapitel:	Managm./Mon. → Benachrichtigung → Verschiedenes - Heartbeat aktivieren
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapTestNotification
OID:	.1.3.6.1.4.1.5597.30.3.0.99
Schweregrad:	Information
Kurzbeschreibung:	Trap, der gesendet wird, wenn eine Testbenachrichtigung angefordert wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

14 Troubleshooting und Alarmierungen

14.1 NTP-Nachrichten

Fehler- und Systemmeldung / Beschreibung	Troubleshooting / Zusatzinformationen
NTP Not Sync / Der NTP-Dienst eines LANTIME ist nicht synchronisiert.	• Für LANTIMEs mit eingebauter Referenzuhr überprüfen Sie bitte den Status der Uhr auf der Startseite im Webinterface. Wenn der Referenztakt nicht synchronisiert ist, lesen Sie bitte die Fehlerbehebungsinformationen für „CLK Not Sync“. • Bei LANTIMEs, die von externen NTP-Servern synchronisiert werden sollen, ist darauf zu achten, dass die externen NTP-Server erreichbar sind. • Überprüfen Sie für MRS-Geräte, ob MRS-Referenzzeitquellen im Web-Interface konfiguriert sind („Das Webinterface → Uhr → MRS-Einstellungen) und entsprechende Signale verfügbar sind (“Das Webinterface → Uhr → MRS-Status)". • Wenden Sie sich an Ihren Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.
NTP Stopped / Der NTP-Dienst wurde angehalten	• Hinweis: Nach jeder für den NTP relevanten Konfigurationsänderung wird der NTP-Dienst gestoppt und neu gestartet. In diesem Fall wird eine Meldung ‘NTP Stopped‘ in das Systemprotokoll des LANTIME geschrieben. • Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn „NTP Stopped“ dauerhaft als NTP-Status auf der Frontplatte oder im Webinterface angezeigt wird.

NTP Offset Limit Exceeded
LANTIMEs erzeugen diese Meldung, wenn der interne Zeitversatz zwischen LANTIME-Systemzeit und Referenztakt größer als der konfigurierte Schwellenwert ist.

- Überprüfen Sie den konfigurierten Schwellenwert im Web Interface: „NTP → Spezielle Einstellungen → Max. Interner Offset (ms.)“.
- Hinweis: Nach dem Neustart des LANTIME dauert es je nach Referenzzeitquelle mehrere Minuten, bis der interne Offset $< \pm 1$ ms ist.
- Wenden Sie sich an Ihren Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

14.2 Referenzuhr-Nachrichten

Fehler- und Systemmeldung / Beschreibung	Fehlerbehebung / Zusatzinformationen
CLK Not Responding / Der LANTIME kann nicht mehr mit seiner internen Referenzuhr kommunizieren.	• Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.
CLK Not Sync / Leistungs- und Systemressourcen-problem des NTP	LANTIME mit GNSS-Referenzuhr (GPS/GLN/GNS): • Überprüfen Sie die Antennenposition: • Wenn der GPS-Referenztaktgeber an einen GPS-Antennenverteiler GPSAV4 (https://www.meinberg.de/german/products/gps-antennenverteiler.htm) angeschlossen ist, stellen Sie sicher, dass der Port „Clock 1“ des GPSAV4 angeschlossen ist, da der GPSAV4 und die Antenne über diesen Port mit Strom versorgt werden. LANTIME mit Langwellenempfänger (DCF77-PZF/WWVB/MSF/JJY): • Überprüfen Sie die Antennenposition LANTIME mit TCR-Referenztakt (IRIG): • Überprüfen Sie, ob der Timecode-Eingangsport auf der Rückseite des LANTIME korrekt mit einer IRIG-Quelle verbunden ist. Überprüfen Sie im Webinterface, ob der richtige IRIG-Eingabecode konfiguriert ist (Menü „Uhr → IRIG-Einstellungen → Timecode-Eingang“). Der Eingangs-Zeitcode ist der IRIG-Code, der dem LANTIME von der IRIG-Quelle zur Verfügung gestellt wird. • Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Antenna Faulty /
GNSS-Referenzuhr (GPS/GLN/GNS):
Die Antenne wurde nicht erkannt.

- Überprüfen Sie die Verbindungen zwischen der Antenne und einem LANTIME.
- Überprüfen Sie die Ausgangsspannung am LANTIME-Antennenanschluss.
- Trennen Sie dazu das Antennenkabel vom LANTIME-Antennenanschluss. Der folgende Spannungswert sollte
- zwischen Innen- und Außenleiter gemessen werden:
  - GPS-Empfänger → 15-18 V DC
  - GLN-Empfänger → 5 V DC
  - GNS-Empfänger → 5 V DC
- Wenn die Spannung 0 V DC beträgt, wenden Sie sich bitte an den Technischen Support von Meinberg.
- Wenn die gemessene Spannung am Antennenanschluss des LANTIME korrekt ist, schließen Sie das Antennenkabel wieder an und überprüfen Sie die Spannung am anderen Ende des Kabels.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Langwellenempfänger (DCF77-PZF/WWVB/MSF/JJY):
Entweder die Antenne oder ein anderes Eingangssignal wurde nicht erkannt.

- Überprüfen Sie die Verbindungen zwischen der Antenne und einem LANTIME.
- Überprüfen Sie den Status des empfangenen Antennensignals auf der Hauptseite im Webinterface. Der angezeigte Feldstärkewert sollte > 40 sein. Ist das nicht der Fall, überprüfen Sie bitte, wie die Antenne positioniert ist.
- Überprüfen Sie die Ausgangsspannung am LANTIME-Antennenanschluss.
- Trennen Sie dazu das Antennenkabel vom LANTIME-Antennenanschluss. Der folgende Spannungswert sollte zwischen Innen- und Außenleiter gemessen werden: Langwellenempfänger →] 5 V DC.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Antenna Short Circuit
Kurzschluss an der Antennenleitung.

- Trennen Sie das Antennenkabel vom LANTIME-Antennenanschluss.
- Durchführen eines Neustarts des Systems
- Wenn der LANTIME nach der Inbetriebnahme die Fehlermeldung nicht anzeigt, schließen Sie die Antenne wieder an. Andernfalls wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.

GPS Warm Boot
Im Warm-Boot-Modus führt die GPS-Referenzuhr die Positionsbestimmung durch. Um diesen Prozess erfolgreich abzuschließen, sollten mindestens 4 Satelliten empfangen werden. Nach erfolgreicher Positionsbestimmung wird die Position im batteriegepufferten Speicher der Uhr gesichert. Damit soll die Positionsbestimmung nach einem Neustart nicht erneut durchgeführt werden müssen.

- Wenn der LANTIME den GPS-Warmstartvorgang nicht abschließen kann, überprüfen Sie die Anzahl der „Guten Satelliten", die im Webinterface angezeigt werden: „Menü Uhr → GPS (GNSS-Uhr) → Empfängerinformationen → Anzahl der guten Satelliten".
- Wenn die Anzahl der guten Satelliten dauerhaft unter 4 liegt und der LANTIME die Positionsbestimmung nicht abschließen kann, dann lesen Sie den Fehlerbehebungsfall für „CLK Not Sync".
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

GPS Cold Boot
Im GPS Cold Boot-Modus versucht die GPS-Referenzuhr, das GPS-Almanach herunterzuladen, welches die Satellitenbahndaten für alle Satelliten enthält. Um diesen Prozess abzuschließen, sollte mindestens ein Satellit empfangen werden. Der Prozess dauert mindestens 12 Minuten. Nachdem der Kaltstart abgeschlossen ist, schaltet die Uhr automatisch auf den GPS-Warm-Boot um, um die Position zu bestimmen.

Das GPS-Almanach wird im batteriegepufferten Speicher der Uhr gesichert.

- Wenn der LANTIME den GPS Cold Boot-Betrieb nach mehr als 30 Minuten nicht abschließen kann, überprüfen Sie die Anzahl der „guten Satelliten" im Webinterface-Menü: „Uhr → GPS (GNSS-Uhr → Empfängerinformationen → Anzahl der guten Satelliten".
- Wenn die Anzahl der guten Satelliten 0 ist, lesen Sie bitte den Fehlerbehebungsfall für „CLK Not Sync".
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

SHS Time Limit Warning
LANTIME-Systeme mit zwei eingebauten Referenzuhren senden diese Meldung, sobald die Zeitdifferenz zwischen beiden Uhren die vorkonfigurierte Einstellung „Time Limit Warning Level“ überschreitet.

- Überprüfen Sie die aktuelle Zeitdifferenz zwischen den beiden Referenzuhren im Hauptmenü des Webinterfaces.
- Überprüfen Sie Ihre SHS-Konfiguration unter „Sicherheit → SHS-Konfiguration“. Sind die konfigurierten Schwellenwerte möglicherweise zu streng eingestellt?
- Überprüfen Sie den Status der beiden Referenzuhren im Hauptmenü des Webinterfaces. Wenn eine der beiden Uhren nicht synchronisiert ist, lesen Sie bitte den Fehlerbehebungsfall für „CLK Not Sync“.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Oscillator not Adjusted
Der interne Oszillator ist (noch) nicht vollständig diszipliniert. Sobald dieser Vorgang abgeschlossen ist, sendet der LANTIME eine Logmeldung „Oscillator Adjusted“. Die Zeit, die benötigt wird, um einen Oszillator zu disziplinieren, hängt von der Qualität des eingehenden Signals, der Alterung und den Umwelteinflüssen auf den Oszillator ab.

- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Leap Second Announced
LANTIME-Server mit GNSS-Referenztaktgeber (GPS / GLN / GNS) oder Langwellenempfänger (DCF77-PZF / WWVB / MSF / JJY) senden die Schaltsekunden-Benachrichtigungsmeldung „Leap Second Announced“, sobald sie die Durchsage durch das Referenzsignal erhalten haben. Die GPS-Satelliten kündigen die bevorstehende Schaltsekunde in der Regel etwa ein halbes Jahr im Voraus an. Langwellensender senden die Ansage in der Regel 1 Stunde im Voraus.

- Dies ist nur eine Info-Benachrichtigung, daher ist keine weitere Aktion erforderlich.

MRS Limit Exceed
Der LANTIME erzeugt diese Meldung, wenn der gemessene Zeitversatz einer MRS-Zeitquelle den konfigurierten Schwellenwert überschritten hat.

- Überprüfen Sie den aktuellen MRS-Zeitquellenstatus im Web-Interface unter „Uhr → GNSS-Uhr → MRS-Status".
- Überprüfen Sie die MRS-Konfiguration im Web-Interface unter „Uhr → GNSS-Uhr → MRS-Einstellungen". Sind die konfigurierten Schwellenwerte (Spalte „Limit" ankreuzen) möglicherweise zu streng konfiguriert?
- Wenden Sie sich an Ihren Meinberg TechSupport und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

MRS Source: No Signal
Der LANTIME erzeugt diese Meldung, wenn die konfigurierte MRS-Zeitquelle nicht mehr verfügbar ist.

- Wenden Sie sich an Ihren Meinberg TechSupport und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

MRS Source: Invalid Signal
Der Lantime erzeugt diese Meldung, wenn zwar ein MRS-Eingangssignal anliegt, aber z.B. die geforderten Qualitätsbedingungen nicht erfüllt sind. Beispiel: Das PTP-Signal eines PTP-GM liegt an, besitzt allerdings nicht die vom Slave vorgegebene Min. Clock-Class.

- Wenden Sie sich an Ihren Meinberg TechSupport und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

14.3 Netzwerk-Meldungen

Fehler- und Systemmeldung / Beschreibung	Troubleshooting / Zusatzinformationen
Network Link Down / Es wurde keine Verbindung an einer der Netzwerkschnittstellen des LANTIME erkannt.	• Überprüfen Sie, welche Ports physisch verbunden sind und ob der Link verfügbar sein sollte. • Überprüfen Sie, ob die Netzwerkeinstellungen am Switch und am LANTIME kompatibel sind. • Überprüfen Sie die Einstellungen zur Linküberwachung über das Web-Interface: „Netzwerk → Physikalische Netzwerkkonfiguration → Zeige Linkstatus an Front LED“. – Der LANTIME überwacht einen Verbindungsstatus für die Ports, bei denen die Option „Zeige Linkstatus an Front LED“ aktiviert ist. • Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

14.4 Sonstige Meldungen

Fehler- und Systemmeldung / Beschreibung>	Troubleshooting / Zusatzinformationen
Fan Failure / Der LANTIME hat einen Fehler an einem Lüftermodul erkannt oder ein Lüftermodul wurde während des Systembetriebs entfernt.	• Wenn das Lüftermodul nicht bewusst entfernt wurde, wenden Sie sich an den Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.
IMS Error / Entweder hat der LANTIME einen Fehler an einem IMS-Modul erkannt oder ein IMS-Modul wurde während des Betriebs aus dem LANTIME IMS-System entfernt.	**Troubleshooting / Zusatzinformationen** • Wenn das IMS-Modul nicht bewusst entfernt wurde, wenden Sie sich an den Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.
CPU No Response (Diese Fehlermeldung kann nur auf einem Display erscheinen) / Das Display erhält keine Informationen von der installierten LANTIME CPU-Einheit.	**Troubleshooting / Zusatzinformationen** • Überprüfen Sie, ob der LANTIME noch über das Netzwerk erreichbar ist (Ping, SSH, HTTP / HTTPS). • Löst ein System-Neustart dieses Problem (kurz von der Spannungszufuhr trennen)? • Wenn der LANTIME noch über HTTP / HTTPS erreichbar ist, laden Sie bitte eine Diagnosedatei über das Webinterface herunter und senden Sie diese an den Technischen Support von Meinberg. Wenn keine Verbindung zum LANTIME möglich ist, wenden Sie sich an unseren Support mit der Seriennummer Ihres LANTIME.
Certificate Expired / Ein LANTIME erzeugt diese Warnung 60 Tage, 30 Tage und 15 Tage vor dem Ende der Laufzeit des installierten SSL-Zertifikats für den HTTPS-Dienst.	**Troubleshooting / Zusatzinformationen** • Überprüfen Sie die Gültigkeit des installierten SSL-Zertifikats über das Web-Interface: „Sicherheit → HTTPS-Zertifikat → SSL-Zertifikat anzeigen“. • Laden Sie ein neues SSL-Zertifikat über das LANTIME Webinterface im Dialogfeld „Sicherheit → HTTPS Zertifikat → Upload SSL-Zertifikat“ hoch. • Wenden Sie sich an Ihren Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Low System Resource /
Ein LANTIME erzeugt diese Warnung:
Verzeichnis „/var“ <] 1MB frei
Verzeichnis „/var“ >] 90% Nutzung
RAM Speicher frei < 6MB

Troubleshooting / Additional information

- Wenden Sie sich an Ihren Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

15 Support-Informationen

In diesem Kapitel erfahren Sie mehr über die verschiedenen Support-Level der Firma Meinberg. Im Allgemeinen ist der „Basic Customer Support-Level“ im Gerätepreis enthalten, den Sie für Ihr Meinberg-Produkt bezahlen und verursacht keine zusätzlichen Kosten. Dieser Basis-Support beinhaltet kostenlose E-Mails, telefonischen Support und kostenlose Firmware-Updates für die gesamte Lebensdauer Ihres Produkts, d.h. solange Sie es verwenden.

Je nach Produkt beinhaltet diese Stufe auch eine 2- oder 3-jährige Hardwaregarantie. Sie können die Hardware-Garantiezeit nach Ablauf der Standardgarantie für Ihr Meinberg-Produkt verlängern.

Das Kapitel beschreibt:

- Basic Customer Support
- Support-Ticket-System
- So laden Sie eine Diagnosedatei herunter
- Selbsthilfe-Online-Tools
- NTP und IEEE 1588-PTP Online-Tutorials
- Vorstellung und Angebot der Meinberg Sync-Academy
- Meinberg Newsletter
- Meinberg Customer Portal

15.1 Standard Support-Service

Kontaktieren Sie Meinberg per E-Mail oder Telefon.

Technischer Support	
E-Mail	techsupport@meinberg.de
Service-Hotline	+49 (0) 5281 / 9309-888
Service-Zeiten	Mo. – Do. 8:00 – 17:00, Fr. 8:00 – 16:00 (MEZ/MESZ) Nicht erreichbar an Sa./So. und an gesetzl. Feiertagen

Büro (Vertrieb/Einkauf)	
E-Mail	info@meinberg.de
Service-Hotline	+49 (0) 5281 / 9309-888
Bürozeiten	Mo. – Do. 7:30 – 17:00, Fr. 07:30 – 15:00 (MEZ/MESZ) Nicht erreichbar an Sa./So. und an gesetzl. Feiertagen

MEINBERG Remote-Support

Um Sie bei der Konfiguration, Installation, Überwachung und Diagnose Ihrer Meinberg-Produkte zu unterstützen, können Sie eine Remote-Support-Software herunterladen, mit der der technische Support von Meinberg Fernzugriff auf Ihren Computer erhalten kann.

Wenn Sie diesem Link folgen:
https://www.meinberg.de/german/support/remote.htm
finden Sie alle notwendigen Informationen um den Remote-Support in Anspruch nehmen zu können.

LANTIME Firmware-Updates

Um zu überprüfen, ob ein Update für Ihre LANTIME verfügbar ist, besuchen Sie bitte:
https://www.meinberg.de/german/sw/firmware.htm

und füllen Sie das Formular aus. Verfügbare Firmware-Updates werden per E-Mail (LANTIME-Firmware V5 oder ältere Versionen) oder mit einem direkten Download-Link (LANTIME-Firmware V6 oder neuer) bereitgestellt.

15.2 Support-Ticket-System

Meinberg hilft Ihnen schnell und direkt bei Fragen zur Inbetriebnahme Ihrer Geräte, bei der Fehlersuche oder beim Update der Hard- oder Software. Wir bieten kostenlosen Support für die gesamte Lebensdauer Ihres Meinberg-Produkts.

- Senden Sie eine Mail an techsupport@meinberg.de mit einer kurzen Beschreibung Ihres Problems.
- Ein Support-Ticket wird danach automatisch erstellt.
- Unsere Support-Techniker werden sich so schnell wie möglich mit Ihnen in Verbindung setzen.
- Es ist immer hilfreich für unsere Ingenieure, beim Versenden eines Tickets eine Diagnosedatei zu erhalten.
- Die Diagnose-Datei enthält alle Statusdaten eines LANTIME-Systems, die seit dem letzten Neustart protokolliert wurden und von allen LANTIME-Zeitservern heruntergeladen werden können. Das Dateiformat der Diagnosedatei ist ein *tgz-archiv*. → Siehe Kapitel So laden Sie eine Diagnosedatei herunter wie Sie diese Datei auf Ihrem LANTIME-System erzeugen.

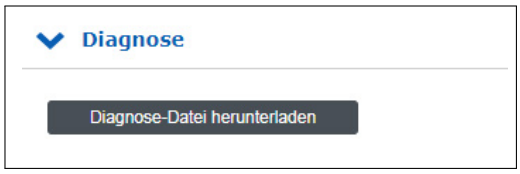
15.3 So laden Sie eine Diagnosedatei herunter

In den meisten Supportfällen ist die erste Maßnahme, den Kunden aufzufordern, die Diagnose-Datei herunterzuladen, da sie sehr hilfreich ist, um den aktuellen Zustand des LANTIME zu identifizieren und mögliche Fehler zu finden. Daher empfehlen wir Ihnen, Ihre Diagnosedatei als Anhang mitzusenden, wenn Sie ein Ticket an unseren Support senden.

Die Diagnose-Datei enthält alle Statusdaten eines LANTIME-Systems, die seit dem letzten Neustart protokolliert wurden. Es kann von allen LANTIME-Zeitservern heruntergeladen werden oder Sie können die Datei auf einem an das Gerät angeschlossenen USB-Speichermedium speichern. Das Dateiformat der Diagnosedatei ist ein tgz-Archiv. Das Archiv enthält alle wichtigen Konfigurationen und Logfiles.

15.3.1 Download über das Webinterface

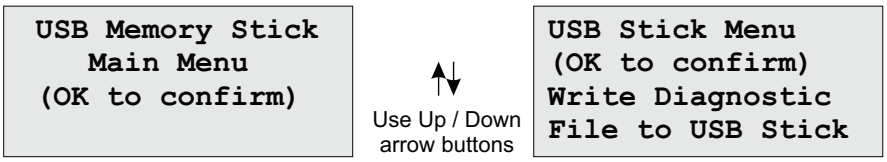
- Verbinden Sie sich mit dem LANTIME über das Webinterface, indem Sie die IP-Adresse in das Adressfeld Ihres Webbrowsers eingeben.
- Öffnen Sie die Seite „System“ und das Untermenü „Diagnose“.
- Drücken Sie die Taste „Diagnosedatei herunterladen“.



- Die Erstellung der Datei wird einige Zeit in Anspruch nehmen, da sie mehrere MB groß ist. Nachdem die Datei erstellt wurde, wird sie automatisch an Ihren Webbrowser gesendet. Speichern Sie die Datei dann auf Ihrer lokalen Festplatte.
- Die Diagnose-Datei heißt *„lt_diag_SERIALNUMBER.tgz“* und das Dateiformat ist ein tgz-Archiv. Sie können das tgz-Archiv z.B. mit 7Zip öffnen (https://www.7-zip.org/).

15.3.2 Herunterladen über ein USB-Speichermedium

- Das USB-Speichermedium muss in einem linuxkompatiblen Dateisystem wie FAT formatiert sein. Schließen Sie einen USB-Stick an den USB-Port des LANTIME an:
- Das USB Memory-Stick-Menü wird automatisch geöffnet. Zur Bestätigung „OK“ drücken.
- Mit den Pfeiltasten ↑ und ↓unten können Sie sich durch das Menü bewegen.
- Verwenden Sie die Option „Write diagnostic File to USB stick“, um die aktuelle Diagnosedatei auf dem USB-Speichermedium zu sichern.
- Sie können die Diagnose-Datei finden, indem Sie den Ordner LANTIME öffnen und mit dem Ordner „Diag“ fortfahren.



Achtung!

Das Herunterladen auf ein USB-Speichermedium ist nicht möglich, wenn das Frontpanel über das Webinterface-Menü „Security → Frontpanel“ gesperrt wurde. Sie ➜ Kapitel 13.1.5.2, „Frontplatte“

15.4 Selbsthilfe-Online-Tools

Hier ist die Liste einiger Websites, auf denen Sie verschiedene Informationen über die Meinberg-Systeme abfragen können.

1. Meinberg Homepage:
   https://www.meinberg.de

2. NTP Download:
   https://www.meinberg.de/german/sw/

3. NTP Client Download für Windows (NTP-time-server-monitor):
   https://www.meinberg.de/german/sw/ntp-server-monitor.htm

4. LANTIME Firmware-Updates:
   https://www.meinberg.de/german/sw/firmware.htm

5. Download-Seite für Meinberg-Software und Treiber:
   https://www.meinberg.de/german/sw/

6. Meinberg Handbücher (EN und DE Versionen):
   https://www.meinberg.de/german/docs/

7. Meinberg Kundenportal (systemspezifische Handbücher, Produktbilder, Software, ...):
   https://meinberg.support/

8. Meinberg Newsletter:
   https://www.meinberg.de/german/company/news.htm

9. NTP / IEEE 1588-PTP Online-Tutorials von Meinberg:
   https://blog.meinbergglobal.com

10. FAQs über Meinberg-Produkte:
    https://www.meinberg.de/german/faq/

11. Meinberg Knowledgebase:
    https://kb.meinbergglobal.com

12. GPS / GNSS Antenneninstallation:
    https://www.meinberg.de/german/info/gps-antenna-mount.htm
    https://www.youtube.com/watch?v=ZTJMKSI8OGY (YouTube Video)

13. Offizielle NTP-Support-Seite und Dokumentation:
    http://support.ntp.org/bin/view/Support/WebHome

15.5 NTP und IEEE 1588-PTP Online-Tutorials

Ein Team von Meinberg-Ingenieuren schreibt Online-Tutorials zu Themen wie IEEE-1588 PTP, NTP, Synchronisations-Setups und Konfigurationen, die in verschiedenen Branchen und Szenarien eingesetzt werden.

Die Tutorials finden Sie unter diesem Link:
https://blog.meinbergglobal.com/

Der Blog bietet Ihnen auch die Möglichkeit, unseren Experten einen Kommentar oder eine Frage zu schreiben und ihre Antwort zu erhalten.

Kategorien:
Konfigurationsrichtlinien, IEEE 1588, Industrieanwendungen, NTP und Sicherheit.

15.6 Die Meinberg Academy - Vorstellung und Schulungsangebote

Die Meinberg Sync Academy (MSA) ist eine Einrichtung innerhalb des Meinberg Unternehmens, die sich um die Ausbildung und Vermittlung von Expertenwissen im Bereich der Zeit- und Frequenzsynchronisation kümmert. Die Akademie bietet Tutorials und Kurse zu den neuesten Synchronisationstechnologien wie NTP, IEEE 1588-PTP und Synchronisationsnetzwerke für verschiedene Branchen an: Telekommunikation, Energie, Rundfunk, professionelle Audio/Video-Anwendungen, Finanzen und IT. Die MSA-Kurse umfassen sowohl theoretische Vorlesungen als auch praktische Übungen.

Wenn Sie die Synchronisation für Ihre Netzwerke planen oder neu gestalten und dabei zusätzliches Wissen benötigen, lesen Sie unsere Agenda für die kommenden Kurse.

Webseite:	https://www.meinbergglobal.com/english/support/meinberg-sync-academy.htm
Aktuelle Kurse:	Meinberg Produkttrainings, PTP- und NTP-Kompaktkurse kundenspezifisches Training sowie Online-Tutorials.
Telefon:	+49 (0) 5281 93093-0
E-Mail:	info@meinberg.de

15.7 Meinberg Newsletter

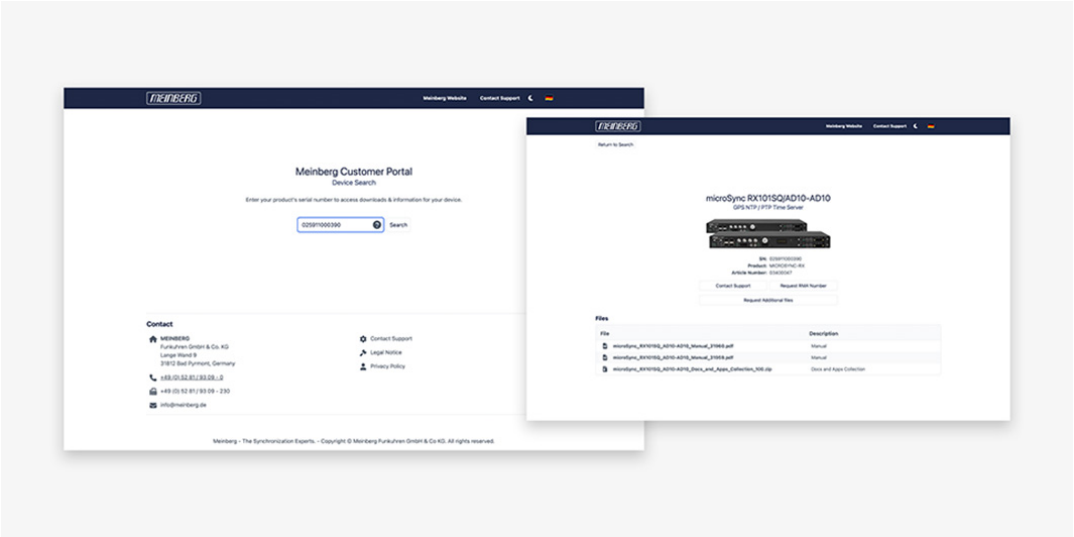
Meinberg veröffentlicht regelmäßig aktuelle Informationen, technische Neuerungen, Firmware-Updates und Sicherheitshinweise über den Meinberg Newsletter in englischer und deutscher Sprache.

Abonnieren Sie hier den Newsletter:

https://www.meinberg.de/german/contact/newslett.htm

15.8 Meinberg Customer Portal - Software und Dokumentation

Endnutzern von Meinberg-Produkten wird über unser Support Center technische Unterstützung, vollständige Dokumentationen und Software-Downloads zur Verfügung gestellt – alles an einem Ort: https://meinberg.support



Keine Registrierung notwendig
Geben Sie einfach die Seriennummer Ihres Produktes unter https://www.meinberg.support ein und Sie erhalten alles, was Sie für einen reibungslosen Einsatz Ihres Meinberg-Systems in Ihrer Umgebung benötigen. Aktuelle Handbücher für die initiale Inbetriebnahme und den laufenden Betrieb, Treiber-Downloads, Programme für die Überwachung und Konfiguration, SNMP MIBs, direkte Links zum Technischen Support von Meinberg und Online-Formulare zur einfachen Anforderung von zusätzlichen Dateien stehen für Sie in diesem Portal zur Verfügung.

Das Meinberg Customer Portal vereinfacht den Zugang zum Support, Software und zur Dokumentation erheblich und stellt sicher, dass Ihnen immer die neuesten Versionen unserer Programme und Handbücher zum Download angeboten werden.

16 Appendix

16.1 LANTIME - Central Processing Unit

Booten des Single Board Computers

Das LINUX-Betriebssystem wird aus einer gepackten Datei auf der Flash-Disk des Single-Board-Computers in eine RAM-Disk geladen. Alle Dateien der Flash-Disk werden nach dem Booten in der RAM-Disk gespeichert. Dadurch wird sichergestellt, dass sich das Dateisystem nach dem Neustart in einem definierten Zustand befindet. Dieser Bootvorgang dauert ca. zwei Minuten. Während dieser Zeit erscheint die folgende Meldung auf dem Display:

```
MEINBERG LANTIME
is booting  ...
please wait ...
......
```

Nach dem Start des LINUX-Systems wird die Netzwerkfunktion gestartet und das Programm zur Kommunikation mit der Refernzuhr und dem NTPD (NTP-Daemon) gestartet. Danach beginnt NTPD mit der Synchronisation mit den Referenzuhren (üblich ist die Hardwareuhr des Einplatinencomputers und des Referenz-Empfängers). Bis zum Abschluss der Synchronisation wird die folgende Meldung angezeigt:

```
CLK: Not Sync
NTP: Sync to OSC
Wed, dd.mm.yyyy
UTC  12:00:00
```

Für die Synchronisation des NTPD mit der Referenzuhr ist es notwendig, dass zum Beispiel der GPS-Empfänger mit der GPS-Zeit synchron ist. In diesem Fall wird die folgende Meldung auf dem Display angezeigt:

```
NORMAL OPERATION
NTP: Offs. 2ms
Wed, dd.mm.yyyy
UTC  12:00:00
```

Die zweite Zeile zeigt dem Benutzer, dass der NTPD mit der GPS mit einem Offset von 2ms synchronisiert hat. Aufgrund der internen Zeit von NTP, die über eine Software-PLL (Phase Locked Loop) eingestellt wird, dauert es eine gewisse Zeit, diesen Offset zu optimieren. Der NTPD versucht, den Offset unter +-128 ms zu halten; wenn der Offset zu groß wird, wird die Systemzeit mit der GPS-Zeit eingestellt. Typischerweise sind die Werte für den Offset +-5 ms, nachdem der NTPD bereits synchronisiert hat.

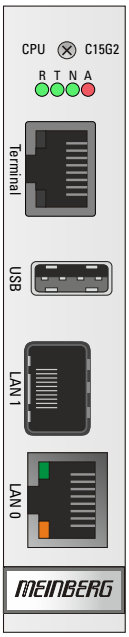
16.1.1 Technische Daten LAN-CPU

CPU Modul-Typ C05F1:

Prozessor:	AMD Geode™ LX 800 (500 MHz, 128 KB L2 Cache, 3.6 W)
Hauptspeicher:	Onboard 256 MByte
Flash-Disk:	1 GB
Netzwerk-Anschluss:	10/100 MBIT mit RJ45-Buchse
Stomversorgung:	5 V +- 5 %, @ 1 A
Frontpanel:	3HE / 4TE (128 mm hoch x 20,3 mm breit)
Umgebungs-temperatur:	0 ... 50 °C
Lager-temperatur:	-20 ... 70 °C
Luftfeuchtigkeit:	85 % max.

16.1.2 Technische Daten - IMS CPU-C15G2

Als zentrales Management- und Bedienelement ist das CPU-Modul in einem LANTIME-System für Management, Überwachung, Konfiguration und Alarmmeldungen zuständig. Es bietet zusätzlich NTP- und SNTP-Dienste auf seinen Netzwerkschnittstellen. Das CPU-Modell C15G2 ist mit zwei integrierten Netzwerk-Schnittstellen ausgerüstet, zusätzliche Netzwerk-Ports können durch die Installation von LNE-Modulen hinzugefügt werden.



Prozessor: Intel® Atom™ Processor E Series
(2 Cores, 1.33GHz, TDP 3W)

Hauptspeicher: onboard 2 GB

Cache-Speicher: 1MB 2nd Level Cache

Flashdisk: 4 GB

Netzwerk-anbindung:
1 x 10/100/1000 Base-T mit RJ45-Anschluss
1 x 1000Base-T mit SFP-Anschluss

Serielle: Schnittstelle:
RJ45 Anschluss
Konsole: 38400 / 8N1,
Anschluss über CAB-CONSOLE Kabel

USB Port:
Aufspielen von Firmware-Updates
Backup und Sichern von Konfigurationsdateien
Kopieren von Sicherheitsschlüsseln
Sperren / Entsperren von Funktionstastatur

Betriebssystem: GNU/Linux 4.x

Statusanzeige:

LAN 0 Interface
LED - Connect, Activity und Speed der Netzwerkverbindung

LAN-CPU
R - Reference Time
T - Time Service
N - Network
A - Alarm

Unterstützte Protokolle:

Network Time Protocol (NTP):	NTP v2 (RFC 1119), NTP v3 (RFC 1305), NTP v4 (RFC 5905) SNTP v3 (RFC 1769), SNTP v4 (RFC 4330)
OSI Layer 2 (Data Link Layer):	PRP (IEC 62439-3)
OSI Layer 3 (Network Layer):	IPv4, IPv6
OSI Layer 4 (Transport Layer):	TCP, UDP, TIME (RFC 868), DAYTIME (RFC 867), SYSLOG
OSI Layer 7 (Application Layer):	HTTP / HTTPS (RC 2616), DHCP, FTP, NTPv3 / NTPv4, SNTP, RADIUS, TACACS, FTP, SSH (incl. SFTP, SCP) - SSH v1.3 / SSH v1.5 / SSH v2 (OpenSSH), SNMPv1 (RFC 1157) / SNMPv2c (RFC 1901-1908) / SNMP v3 (RFC 3411-3418), Telnet (RFC 854-RFC 861)

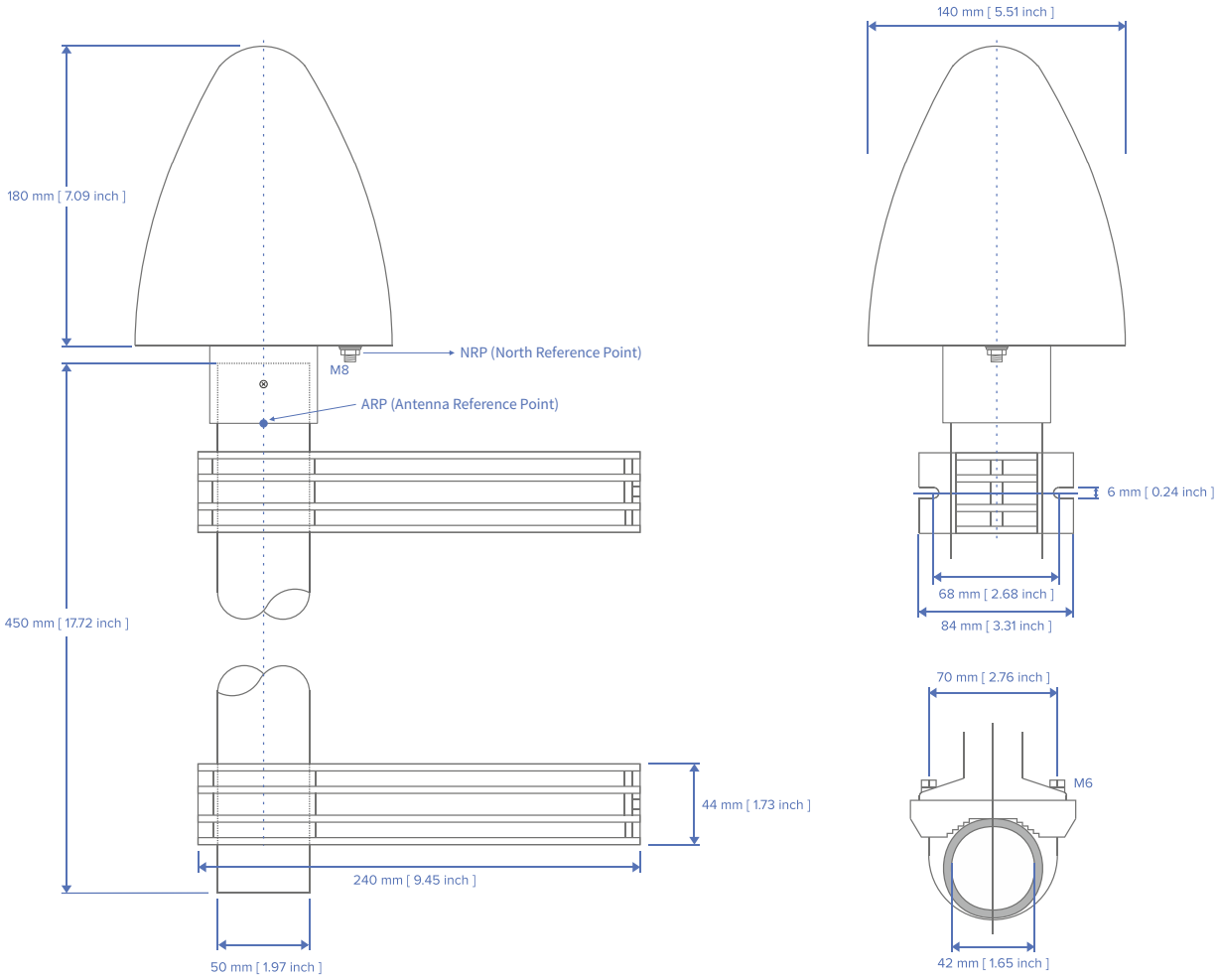
Umgebung:

Umgebungstemperatur:	0 ... 50°C
Luftfeuchtigkeit:	Max. 85%

16.2 Technische Daten - Antennen für LANTIME-Systeme

16.2.1 Technische Daten - GPSANTv2-Antenne

Abmessungen



Elektrische Spezifikationen

Spannungsversorgung: (über Antennenkabel)	15 V ± 3 V
Nennstromaufnahme: (über Antennenkabel)	ca. 100 mA bei 15 V, max. 115 mA

Signalempfang und -verarbeitung

Empfangsfrequenz:	1575,42 MHz (GPS L1/Galileo E1 band)
Achsenverhältnis:	≤ 3 dB im Zenith
Verstärkung:	typ. 5,0 dBic im Zenith
Mischfrequenz:	10 MHz
Zwischenfrequenz:	35,4 MHz
Weitabselektion:	≥ 70 dB @ 1555 MHz ≥ 55 dB @ 1595 MHz
Mischverstärkung: Antenneneingang bis ZF-Ausgang	59 dB ± 3 dB
Rauschzahl:	typ. 1,8 dB, max. 3 dB bei +25 °C
Überlebenspegel Eingangsfilter:	zerstörungsfrei bei > 13 dBm für 24 Stunden
Ausbreitungsverzögerung: (Anschluss Patch bis ZF-Ausgang)	typ. 152 ns ± 5 ns
Gruppenlaufzeitschwankung innerhalb der 2,4 MHz-Systembandbreite:	max. 15 ns
Polarisierung:	rechtsdrehend, kreisförmig
Frequenzabschirmung nach ETSI-Normen:	abgeschirmter Frequenzbereich auf 6 GHz erweitert
	–40 dBm
P1dB-Eingang:	
Empfangscharakteristik:	Vertikale Breite des 3 dB-Empfangsbereiches: 100° mit Azimut als Mitte

Anschluss

Anschluss:	N-Norm Buchse
Nennimpedanz:	50 Ω
Voltage Standing Wave Ratio (VSWR):	≤ 1,5 : 1
Erdungsanschluss:	M8-Gewindeschraube und Sechskantmutter passend zur entsprechenden Öse

Angaben zur Störfestigkeit

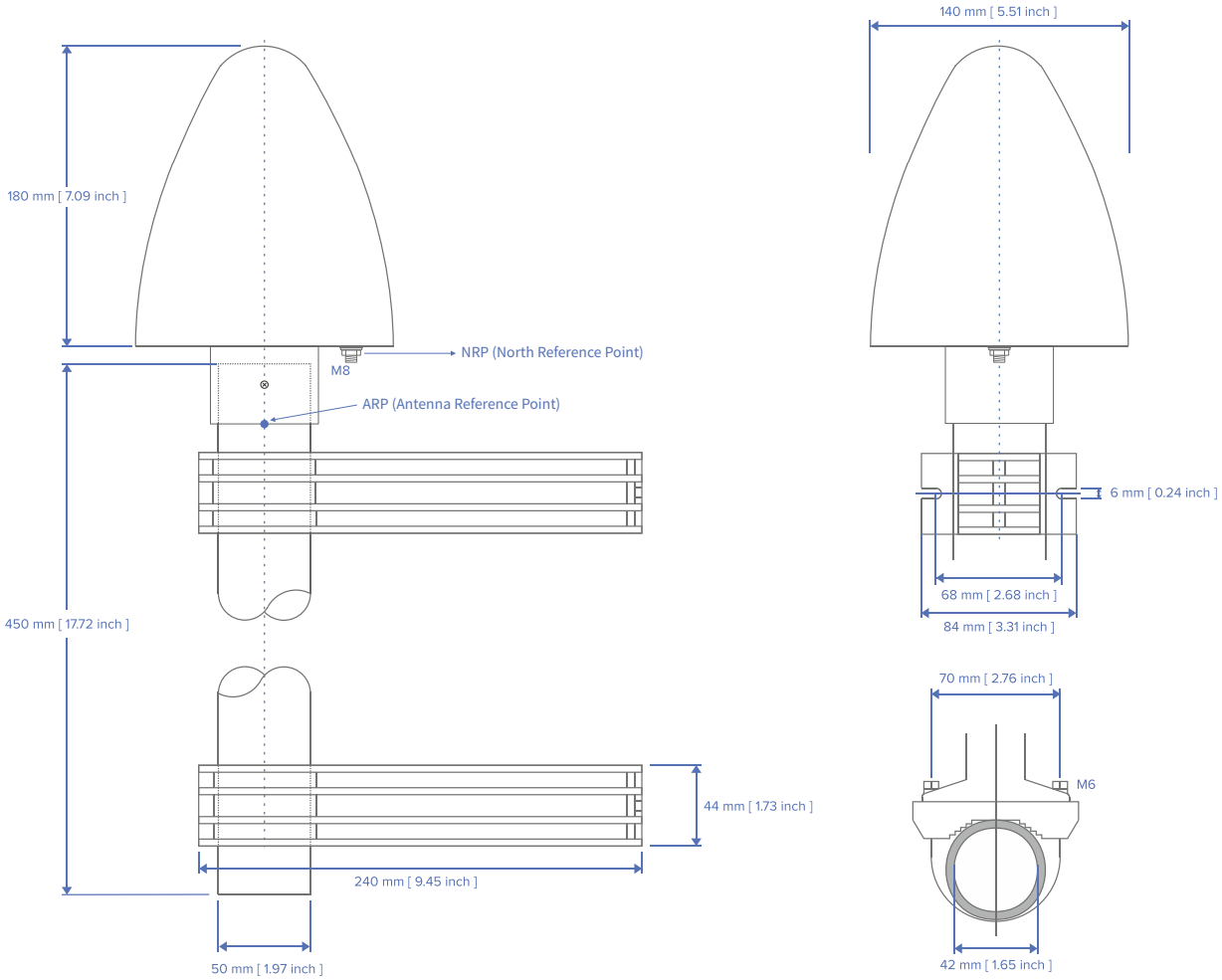
Stoßüberspannungsschutz:	Level 4 (nach IEC 61000-4-5) Prüfspannung: 4000 V Max. Spitzenstrom @ 2 Ω: 2000 A
ESD-Schutz:	Level 4 (nach IEC 61000-4-2) Kontaktentladung: 8 kV Luftentladung: 15 kV

Mechanische und umwelttechnische Spezifikationen

Gehäusematerial:	ABS Kunststoff-Spritzgussgehäuse
Spezifizierte Umgebung:	Außenbereich
IP-Schutzart:	IP65
Temperaturbereich (Betrieb):	–60 °C ... +80 °C
Temperaturbereich (Lagerung):	–20 °C ... +70 °C
Relative Luftfeuchtigkeit (Betrieb):	5 % ... 95 % (nicht kondensierend)
Gewicht:	1,4 kg mit Montagekit

16.2.2 Technische Daten - GNSS Multi-Band-Antenne

Abmessungen



Allgemeine Daten

Spannungsversorgung:	5 V ... 16 V ⎓, 24 mA (über Antennenkabel)
Anschluss:	N-Norm Buchse
Formfaktor:	ABS-Plastikgehäuse für Außeninstallation
IP-Schutzart:	IP66
Relative Luftfeuchtigkeit:	95 %
Temperaturbereich:	–40 °C ... +85 °C
Gewicht:	1,6 kg mit Montagekit
Frequenzbereiche:	1164 MHz ... 1254 MHz und 1525 MHz ... 1606 MHz
Gesamt LNA-Verstärkung:	35 dB min., 37 dB typ.
Rauschzahl:	2,5 dB typ. at 25 °C

Unterstützte Frequenzbänder

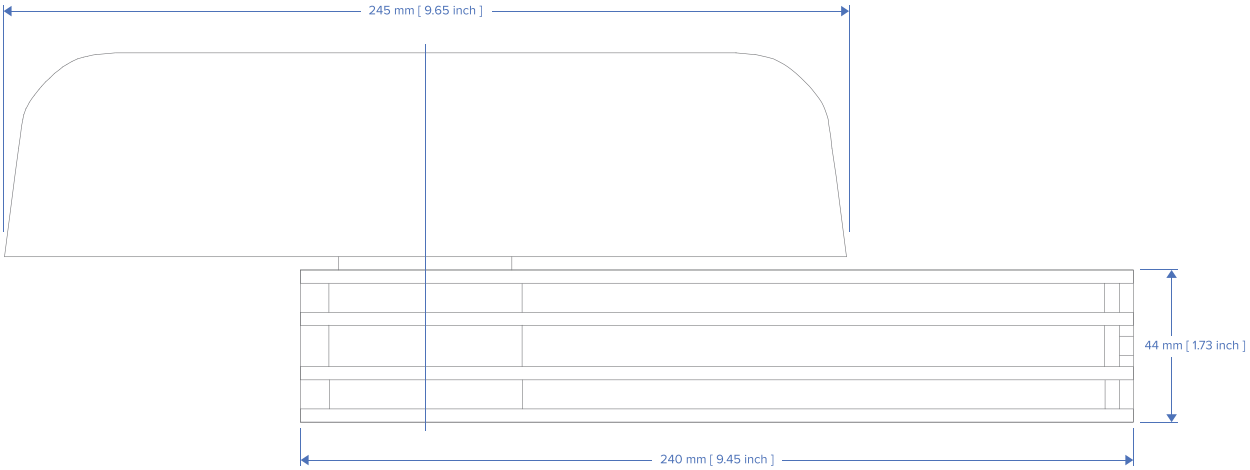
GPS:	L1/L2/L5
GLONASS:	G1/G2/G3
Beidou:	B1/B2/B3
Galileo:	E1/E5a+b plus L-band/E6

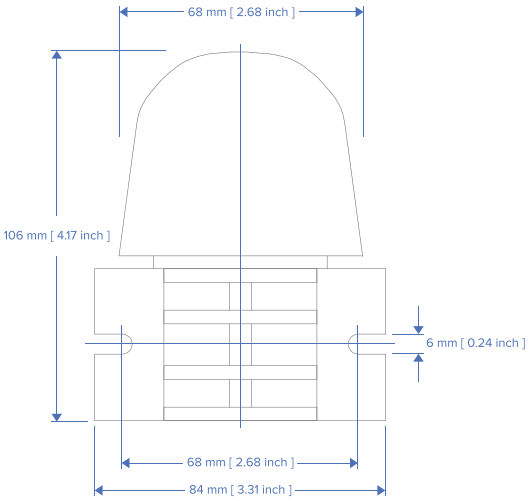
Weitabselektion

Freq. Band E5/L2/G2:	Frequenz	
	< 1050 MHz	> 45 dB
	< 1125 MHz	> 30 dB
	< 1350 MHz	> 45 dB
Freq. Band L1/E1/B1/G1:	Frequenz	
	< 1450 MHz	> 30 dB
	< 1690 MHz	> 30 dB
	< 1730 MHz	> 40 dB

16.2.3 Technische Daten - AW02-Antenne

Abmessungen





Elektrische Spezifikationen

Spannungsversorgung:	3,5 V ... 5 V ⎓
Bandbreite:	1 kHz
Signalpegel:	50 μV ... 5 mV

Mechanische und umwelttechnische Spezifikationen

Anschluss:	N-Norm Buchse
Gehäusematerial:	ABS Kunststoff-Spritzgussgehäuse
IP-Schutzart:	IP56
Umgebungstemperatur (im Betrieb)	-60 °C bis +80 °C (–76 °F to 176 °F)
Umgebungstemperatur (Lagerung):	-20 °C bis +70 °C (–4 °F to 158 °F)
Gewicht:	0,55 kg inkl. Montagesatz für Wandmontage

16.2.4 Technische Daten - MBG S-PRO Überspannungsschutz

Der MBG S-PRO ist ein Überspannungsschutzgerät von Phoenix Contact (Typenbezeichnung CN-UB-280DC-BB), das zum Schutz von Geräten, die über Koaxialkabel angeschlossen sind, entwickelt wurde. Er wird in die Antennenzuleitung eingebaut und besteht aus einem auswechselbaren Gasableiter, welcher nach dem Zünden die Energie vom Außenleiter des Kabels zum Erdungspotential ableitet. Der Erdanschluss ist auf möglichst kurzem Wege zu realisieren.

Der MBG S-PRO hat keinen dedizierten Eingang/Ausgang und keine bevorzugte Einbaulage.

Abbildung 16.1: Überspannungschutz MBG S-PRO (Phoenix CN-UB-280DC-BB)

Eigenschaften

- Hervorragende RF-Performance
- Mehrfaches Einschlagpotential
- 20-kA-Überspannungsschutz
- Schutz in zwei Richtungen

Lieferumfang:	Überspannungsschutz mit Montagewinkel und Zubehör
Produkttyp:	Überspannungsschutz für Sende- und Empfangsanlagen
Bauform:	Zwischenstecker
Anschlüsse:	N-Norm Buchse/N-Norm Buchse

Die Original-Produktseite des Lieferanten des Überspannungsschutzes CN-UB-280DC-BB stellt detaillierte technische Daten sowie diverse produktspezifische Unterlagen unter folgendem Link bereit:

Datenblatt zum Download:

https://www.meinberg.de/download/docs/shortinfo/german/cn-ub-280dc-bb_pc.pdf

16.3 Zeittelegramm-Formate

16.3.1 Meinberg Standard-Telegramm

Das Meinberg Standard Telegramm besteht aus einer Folge von 32 ASCII-Zeichen, eingeleitet durch das Zeichen <STX> (Start-of-Text) und abgeschlossen durch das Zeichen <ETX> (End-of-Text). Das Format ist:

<STX>D:*tt.mm.jj*;T:*w*;U:*hh.mm.ss*;*uvxy*<ETX>

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> — Start-of-Text, ASCII-Code 02h, wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.

tt.mm.jj — Das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
jj	Jahr ohne Jahrhundert	(00..99)

w — Der Wochentag (1..7, 1 = Montag)

hh.mm.ss — Die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)

uv — Status der Funkuhr (abhängig vom Funkuhrentyp):

u:	„#“	GPS: Uhr läuft frei (ohne genaue Zeitsynchronisation) PZF: Zeitraster nicht synchronisiert DCF77: Uhr hat seit dem Einschalten nicht synchr.
„ “	(Leerzeichen, ASCII-Code 20h)	GPS: Uhr läuft GPS synchron (Grundgenauig. erreicht) PZF: Zeitraster synchronisiert DCF77: Synchr. seit letztem Einschalten erfolgt
v:	„*“	GPS: Empfänger hat die Position noch nicht überprüft PZF/DCF77: Uhr läuft im Moment auf Quarzbasis
„ “	(Leerzeichen, 20h)	GPS: Empfänger hat seine Position bestimmt PZF/DCF77: Uhr wird vom Sender geführt

x — Kennzeichen der Zeitzone:

„U“	UTC	Universal Time Coordinated, früher GMT
„ “	MEZ	Mitteleuropäische Standardzeit
„S“	(MESZ)	Mitteleuropäische Sommerzeit

y — Ankündigung eines Zeitsprungs während der letzten Stunde:

„!“	Ankündigung Beginn oder Ende der Sommerzeit
„A“	Ankündigung einer Schaltsekunde
„ “	(Leerzeichen, 20h) kein Zeitsprung angekündigt

<ETX> — End-of-Text (ASCII-Code 03h)

16.3.2 Meinberg GPS-Zeittelegramm

Das Meinberg GPS-Zeittelegramm besteht aus einer Folge von 36 ASCII-Zeichen, eingeleitet durch das Zeichen <STX> (Start-of-Text) und abgeschlossen durch das Zeichen <ETX> (End-of-Text). Es enthält im Gegensatz zum Meinberg Standard-Telegramm keine lokale Zeitzone oder UTC, sondern die GPS-Zeit ohne Umrechnung auf UTC. Das Format ist:

<STX>D:*tt.mm.jj;T:w;U:hh.mm.ss;uvGy;lll*<ETX>

Die *kursivgedruckten* Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Start-of-Text, ASCII-Code 02h

tt.mm.jj Das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
jj	Jahr ohne Jahrhundert	(00..99)

w Der Wochentag (1..7, 1 = Montag)

hh.mm.ss Die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59 bzw. 60 während Schaltsekunde)

uv Status der Funkuhr:

u:	„#“	Uhr läuft frei (ohne genaue Zeitsynchronisation)
	„ “	(Leerzeichen, ASCII-Code 20h) Uhr läuft synchron (Grundgenauig. erreicht)
v:	„*“	Empfänger hat die Position noch nicht überprüft
	„ “	(Leerzeichen, ASCII-Code 20h) Empfänger hat seine Position bestimmt

G Kennzeichen der Zeitzone „GPS-Zeit“

y Ankündigung eines Zeitsprungs während der letzten Stunde:
vor dem Ereignis:

„A“	Ankündigung einer Schaltsekunde
„ “	(Leerzeichen, ASCII-Code 20h) kein Zeitsprung angekündigt

lll Anzahl der Schaltsekunden zwischen GPS-Zeit und UTC
(UTC = GPS-Zeit + Anzahl Schaltsekunden)

<ETX> End-of-Text (ASCII-Code 03h)

16.3.3 Meinberg Capture-Telegramm

Das Meinberg Capture-Telegramm besteht aus einer Folge von 31 ASCII-Zeichen und wird durch eine <CR><LF>-Sequenz (Carriage-Return/Line-Feed) abgeschlossen. Das Format ist:

CH*x*<*SP*>*tt.mm.jj_hh:mm:ss.fffffff*<CR><LF>

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

x	0 oder 1, Nummer des Eingangs		
<SP>	Leerzeichen, ASCII-Code 20h		
tt.mm.jj	Das Aufnahme-Datum:		
	tt	Monatstag	(01 ... 31)
	mm	Monat	(01 ... 12)
	jj	Jahr ohne Jahrhundert	(00 ... 99)
hh:mm:ss.fffffff	Die Aufnahme-Zeit:		
	hh	Stunden	(00 ... 23)
	mm	Minuten	(00 ... 59)
	ss	Sekunden	(00 ... 59, oder 60 während Schaltsekunde)
	fffffff	Bruchteile der Sekunden, 7 Stellen	
<CR>	Carriage-Return (ASCII-Code 0Dh)		
<LF>	Line-Feed (ASCII-Code 0Ah)		

16.3.4 ATIS-Zeittelegramm

Das ATIS Zeittelegramm besteht aus einer Folge von 23 ASCII-Zeichen, abgeschlossen durch das Zeichen <CR» (Carriage-Return). Die Standardeinstellung für die Schnittstelle bei diesem Telegramm ist 2400 Baud, 7E1). Das Format ist:

<GID><ABS><TSQ><CC><CS><ST>*jjmmtthhmmsswcc*<GID><CR>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind fester Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<GID>	Empfängeradresse, ASCII-Code 7Fh
<ABS>	Ursprung der Nachricht, „0“, ASCII-Code 30h
<TSQ>	Telegrammnummer, „0“, ASCII-Code 30h
<CC>	Befehlcode, „S“ (für ‘SETZEN’), ASCII-Code 53h
<CS>	Befehlcode, „A“ (für „ALLE“), ASCII-Code 41h
<ST>	Zeitstatus, „C“ (für gültige Zeit), ASCII-Code 43h
jjmmtt	Das Datum: jj Jahr ohne Jahrhundert (00..99) mm Monat (01..12) tt Monatstag (01..31)
hhmmss	Die Zeit: hh Stunden (00..23) mm Minuten (00..59) ss Sekunden (00..59, oder 60 wenn Schaltsekunde)
w	Der Wochentag (1..7, 1 = Montag)
cc	Checksumme (hexadezimal) aller Zeichen inkl. GID, ABS, TSQ, CC, ST, ...
<CR>	Carriage-Return, ASCII-Code 0Dh

16.3.5 SAT-Telegramm

Das SAT-Telegramm besteht aus einer Folge von 29 ASCII-Zeichen, eingeleitet durch das Zeichen <STX> (Start-of-Text) und abgeschlossen durch das Zeichen <ETX> (End-of-Text). Das Format ist:

<STX>*tt.mm.jj/w/hh:mm:ssxxxxuv*<ETX>

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Start-of-Text, ASCII-Code 02h, wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.

tt.mm.jj Das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
jj	Jahr ohne Jahrhundert	(00..99)

w Der Wochentag (1..7, 1 = Montag)

hh:mm:ss Die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)

xxxx Kennzeichen der Zeitzone:

„UTC“	Universal Time Coordinated, früher GMT
„CET“	European Standard Time, daylight saving disabled
„CEST“	Mitteleuropäische Sommerzeit

u Status der Funkuhr:

„#“	Uhr hat seit dem Einschalten nicht synchr.
„ “	(Leerzeichen, 20h) Synchr. seit letztem Einschalten erfolgt

v Ankündigung eines Zeitsprungs während der letzten Stunde vor dem Ereignis:

„!“	Ankündigung Beginn oder Ende der Sommerzeit
„ “	(Leerzeichen, ASCII-Code 20h) kein Zeitsprung angekündigt

<CR> Carriage-Return (ASCII-Code 0Dh)

<LF> Line-Feed (ASCII-Code 0Ah)

<ETX> End-of-Text (ASCII-Code 03h)

16.3.6 Uni Erlangen-Telegramm (NTP)

Das Zeittelegramm Uni Erlangen (NTP) besteht aus einer Folge von 66 ASCII-Zeichen, eingeleitet durch das Zeichen <STX> (Start-of-Text) und abgeschlossen durch das Zeichen <ETX> (End-of-Text). Das Format ist:

<STX>*tt.mm.jj; w; hh:mm:ss; voo:oo; acdfg i;bbb.bbbbn lll.lllle hhhhm*<ETX>

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Start-of-Text, ASCII-Code 02h, wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.

tt.mm.jj Das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
jj	Jahr (ohne Jahrhundert)	(00..99)

w Der Wochentag (1..7, 1 = Montag)

hh.mm.ss Die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)

v Vorzeichen des Offsets der lokalen Zeitzone zu UTC

oo:oo Offset der lokalen Zeitzone zu UTC in Stunden und Minuten

ac Status der Funkuhr:

a:	„#“	Uhr hat seit dem Einschalten nicht synchr.
	„ “	(Leerzeichen, ASCII-Code 20h) Synchr. seit letztem Einschalten erfolgt
c:	„*“	GPS-Empfänger hat die Position noch nicht überprüft
	„ “	(Leerzeichen, ASCII-Code 20h) GPS-Empfänger hat seine Position bestimmt

d Kennzeichen der Zeitzone:

„S“	MESZ	Mitteleuropäische Sommerzeit
„ “	MEZ	Mitteleuropäische Standardzeit

f Ankündigung eines Zeitsprungs während der letzten Stunden vor dem Ereignis:

„!“	Ankündigung Beginn oder Ende der Sommerzeit
„ “	(Leerzeichen, ASCII-Code 20h) kein Zeitsprung angekündigt

g Ankündigung eines Zeitsprungs während der letzten Stunde vor dem Ereignis:

„A“	Ankündigung einer Schaltsekunde
„ “	(Leerzeichen, ASCII-Code 20h) kein Zeitsprung angekündigt

i Schaltsekunde

„L“	Schaltsekunde wird momentan eingefügt (nur in 60. Sekunde aktiv)
„ “	(Leerzeichen, ASCII-Code 20h) Schaltsekunde nicht aktiv

bbb.bbbb Geographische Breite der Empfängerposition in Grad
Führende Stellen werden mit Leerzeichen (ASCII-Code 20h) aufgefüllt

n	Geographische Breitenhemisphäre, mögliche Zeichen sind: „N“ nördlich d. Äquators „S“ südlich d. Äquators
lll.llll	Geographische Länge der Empfängerposition in Grad Führende Stellen werden mit Leerzeichen (ASCII-Code 20h) aufgefüllt
e	Geographische Längenhemisphäre, mögliche Zeichen sind: „E“ östlich des Greenwich-Meridians „W“ westlich des Greenwich-Meridians
hhhh	Höhe der Empfängerposition über WGS84 Ellipsoid in Metern Führende Stellen werden mit Leerzeichen (ASCII-Code 20h) aufgefüllt
<ETX>	End-of-Text (ASCII-Code 03h)

16.3.7 NMEA 0183-Telegramm (RMC)

Das NMEA-0183-RMC-Telegramm besteht aus einer Folge von 65 ASCII-Zeichen, eingeleitet durch die Zeichenfolge „$GPRMC“ und abgeschlossen durch die Zeichenfolge <CR> (Carriage-Return) und <LF> (Line-Feed). Das Format ist:

$GPRMC,*hhmmss.ff*,A,*bbbb.bb*,n,*lllll.ll*,e,*0.0*,*0.0*,*ttmmjj*,*0.0*,a*hh*<CR><LF>

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

$ — Start-Zeichen, ASCII-Code 24h
Wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.

GP — Geräte-ID, in diesem Fall „GP“ für GPS

RMC — Datensatz-ID, um den Telegrammtyp zu beschreiben, in diesem Fall „RMC“

hhmmss.ss — Die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)
ff	Sekundenbruchteile	(1/10 ; 1/100)

A — Status (A = Zeitdaten gültig, V = Zeitdaten ungültig)

bbbb.bb — Geographische Breite der Empfängerposition in Grad
Führende Stellen werden mit Leerzeichen (ASCII-Code 20h) aufgefüllt

n — Geographische Breitenhemisphäre, mögliche Zeichen sind:

„N“	nördlich d. Äquators
„S“	südlich d. Äquators

lllll.ll — Geographische Länge der Empfängerposition in Grad
Führende Stellen werden mit Leerzeichen (ASCII-Code 20h) aufgefüllt

e — Geographische Längenhemisphäre, mögliche Zeichen sind:

„E“	östlich des Greenwich-Meridians
„W“	westlich des Greenwich-Meridians

0.0,0.0 — Geschwindigkeit in Knoten und die Richtung in Grad.
Bei einer Meinberg GPS-Uhr sind diese Werte immer 0.0.
Bei einer GNS-Uhr werden die Werte bei mobilen Anwendungen berechnet.

ttmmjj — Das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
yy	Jahr ohne Jahrhundert	(00..99)

a — magnetische Variation E/W

hh — Prüfsumme (XOR über alle Zeichen außer „$“ und „*“)

<CR> — Carriage-Return (ASCII-Code 0Dh)

<LF> — Line-Feed (ASCII-Code 0Ah)

16.3.8 NMEA-0183-Telegramm (GGA)

Das NMEA-0183-GGA-Telegramm besteht aus einer Zeichenfolge, eingeleitet durch die Zeichenfolge „$GPGGA“ und abgeschlossen durch die Zeichenfolge «CR» (Carriage-Return) und <LF> (Line-Feed). Das Format ist:

$GPGGA,*hhmmss.ff*,*bbbb.bbbbb*,*n*,*lllll.ll*,*e*,*A*,*vv*,*hhh.h*,*aaa.a*,M,
ggg.g,M,,*0***cs*<CR><LF>

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

$	Start-Zeichen, ASCII-Code 24h Wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.
GP	Geräte-ID, in diesem Fall „GP“ für GPS
GGA	Datensatz-ID, in diesem Fall „GGA“
hhmmss.ss	Die Zeit: *hh* Stunden (00..23) *mm* Minuten (00..59) *ss* Sekunden (00..59 bzw. 60 während Schaltsekunde) *ff* Sekundenbruchteile (1/10 ; 1/100)
bbbb.bbbbb	Geographische Breite der Empfängerposition in Grad Führende Stellen werden mit Leerzeichen (ASCII-Code 20h) aufgefüllt
n	Geographische Breitenhemisphäre, mögliche Zeichen sind: „N“ nördlich d. Äquators „S“ südlich d. Äquators
lllll.lllll	Geographische Länge der Empfängerposition in Grad Führende Stellen werden mit Leerzeichen (ASCII-Code 20h) aufgefüllt
e	Geographische Längenhemisphäre, mögliche Zeichen sind: „E“ östlich des Greenwich-Meridians „W“ westlich des Greenwich-Meridians
A	Position bestimmt (1 = yes, 0 = no)
vv	Anzahl der verwendeten Satelliten (0..12)
hhh.h	HDOP (Horizontal Dilution of Precision)
aaa.h	Mittlere Meereshöhe (MSL = WGS84 Höhe - Geoid Separation)
M	Einheit Meter (fester Wert)
ggg.g	Geoid Separation (WGS84 Höhe - MSL Höhe)
M	Einheit Meter (fester Wert)
cs	Prüfsumme (XOR über alle Zeichen außer „$“ und „*“)
<CR>	Carriage-Return (ASCII-Code 0Dh)
<LF>	Line-Feed (ASCII-Code 0Ah)

16.3.9 NMEA-0183-Telegramm (ZDA)

Das NMEA-0183-ZDA-Telegramm besteht aus einer Folge von 38 ASCII-Zeichen, eingeleitet durch die Zeichenfolge „$GPZDA“ und abgeschlossen durch die Zeichenfolge <CR> (Carriage-Return) und <LF> (Line-Feed). Das Format ist:

$GPZDA,*hhmmss.ss*,*tt*,*mm*,*jjjj*,*HH*,*II***cs*<CR><LF>

ZDA - Zeit und Datum: UTC, Tag, Monat, Jahr und lokale Zeitzone.

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

`$` Start-Zeichen (ASCII-Code 24h)
Wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.

`hhmmss.ss` UTC-Zeit:

`hh`	Stunden	(00..23)
`mm`	Minuten	(00..59)
`ss`	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)

`HH,II` Die lokale Zeitzone (Offset zu UTC):

`HH`	Stunden	(00..±13)
`II`	Minuten	(00..59)

`tt,mm,jj` Das Datum:

`tt`	Monatstag	(01..31)
`mm`	Monat	(01..12)
`jjjj`	Jahr	(0000..9999)

`cs` Prüfsumme (XOR über alle Zeichen außer „$“ und „*“)

`<CR>` Carriage-Return (ASCII-Code 0Dh)

`<LF>` Line-Feed (ASCII-Code 0Ah)

16.3.10 ABB-SPA-Telegramm

Das ABB-SPA-Zeittelegramm besteht aus einer Folge von 32 ASCII-Zeichen, eingeleitet durch die Zeichenfolge „>900WD:“ und abgeschlossen durch das Zeichen <CR> (Carriage-Return). Das Format ist:

>900WD:*jj-mm-tt*<*SP*>*hh.mm;ss.fff:cc*<CR>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

jj-mm-tt	Das Datum:		
	jj	Jahr ohne Jahrhundert	(00..99)
	mm	Monat	(01..12)
	tt	Monatstag	(01..31)
	<SP>	Leerzeichen (ASCII-Code 20h)	
hh.mm;ss.fff	Die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)
	fff	Millisekunden	(000..999)
cc	Prüfsumme. Die Berechnung erfolgt durch Exklusiv-Oder-Verknüpfung der vorhergehenden Zeichen, dargestellt wird der resultierende 8-Bit-Wert im Hex-Format als 2 ASCII-Zeichen („0“ bis „9“ oder „A“ bis „F“)		
<CR>	Carriage-Return (ASCII-Code 0Dh)		

16.3.11 Computime-Zeittelegramm

Das Computime-Zeittelegramm besteht aus einer Folge von 24 ASCII-Zeichen, eingeleitet durch das Zeichen `T` und abgeschlossen durch das Zeichen `<LF>` (Line-Feed, ASCII-Code 0Ah). Das Format ist:

`T:`*`jj:mm:tt:ww:hh:mm:ss`*`<CR><LF>`

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

`T` — Startzeichen
Wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.

`jj:mm:tt` — Das Datum:

`jj`	Jahr ohne Jahrhundert	(00..99)
`mm`	Monat	(01..12)
`tt`	Monatstag	(01..31)
`ww`	Der Wochentag	(01..07, 01 = Montag)

`hh:mm:ss` — Die Zeit:

`hh`	Stunden	(00..23)
`mm`	Minuten	(00..59)
`ss`	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)

`<CR>` — Carriage-Return (ASCII-Code 0Dh)

`<LF>` — Line-Feed (ASCII-Code 0Ah)

16.3.12 RACAL-Zeittelegramm

Das RACAL-Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch das Zeichen X und abgeschlossen durch das Zeichen <CR> (Carriage-Return, ASCII-Code 0Dh). Das Format ist:

XGU*jjmmtthhmmss*<CR>

Die *kursivgedruckten* Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

X	Startzeichen (ASCII-Code 58h) Wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.		
G	Kontrollzeichen (ASCII-Code 47h)		
U	Kontrollzeichen (ASCII-Code 55h)		
jjmmdd	Aktuelles Datum:		
	jj	Jahr ohne Jahrhundert	(00..99)
	mm	Monat	(01..12)
	tt	Monatstag	(01..31)
hh:mm:ss	Die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59 bzw. 60 wenn Schaltsekunde)
<CR>	Carriage-Return (ASCII-Code 0Dh)		

16.3.13 SYSPLEX-1-Zeittelegramm

Das SYSPLEX-1-Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch das ASCII-Kontrollzeichen <SOH> (Start-of-Header) und abgeschlossen durch das Zeichen **<LF>** (Line-Feed, ASCII-Code 0Ah).

Achtung!

Damit das Zeittelegramm über ein ausgewähltes Terminalprogramm korrekt ausgegeben und angezeigt werden kann, muss ein „C“ (einmalig, ohne Anführungszeichen) eingegeben werden.

Das Format ist:

<SOH>*ttt:hh:mm:ssq*<CR><LF>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<SOH>	Start-of-Header, ASCII-Code 01h wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
ttt	Jahrestag	(001..366)	
hh:mm:ss	die Zeit:		
	hh Stunden	(00..23)	
	mm Minuten	(00..59)	
	ss Sekunden	(00..59, oder 60 wenn Schaltsekunde)	
	q Status der Funkuhr:	Leerzeichen (ASCII-Code 20h)	Time Sync (GPS Lock)
		„?“ (ASCII-Code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage-Return, ASCII-Code 0Dh		
<LF>	Line-Feed, ASCII-Code 0Ah		

16.3.14 ION-Zeittelegramm

Das ION-Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch das ASCII-Kontrollzeichen <SOH> (Start-of-Header, ASCII-Code 01h) und abgeschlossen durch das Zeichen <LF> (Line-Feed, ASCII-Code 0Ah). Das Format ist:

<SOH>*ttt:hh:mm:ssq*<CR><LF>

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<SOH>	Start-of-Header (ASCII-Code 01h) Wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet.		
ttt	Jahrestag	(001..366)	
hh:mm:ss	Die Zeit:		
	hh Stunden	(00..23)	
	mm Minuten	(00..59)	
	ss Sekunden	(00..59 bzw. 60 während Schaltsekunde)	
	q Status der Funkuhr:	Leerzeichen (ASCII-Code 20h)	Time Sync (GPS Lock)
		„?“ (ASCII-Code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage-Return (ASCII-Code 0Dh)		
<LF>	Line-Feed (ASCII-Code 0Ah)		

16.3.15 ION-Blanked-Zeittelegramm

Das ION-Blanked-Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch das ASCII-Kontrollzeichen <SOH> (Start-of-Header, ASCII-Code 01h) und abgeschlossen durch das Zeichen <LF> (Line-Feed, ASCII-Code 0Ah). Das Format ist:

<SOH>*ttt:hh:mm:ssq*<CR><LF>

Achtung!

Das Blanking Intervall hat eine Länge von 2 Minuten 30 Sekunden und wird alle 5 Minuten eingefügt.

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<SOH>	Start-of-Header (ASCII-Code 01h) wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
ttt	Jahrestag	(001..366)	
hh:mm:ss	die Zeit:		
	hh Stunden	(00..23)	
	mm Minuten	(00..59)	
	ss Sekunden	(00..59, oder 60 wenn Schaltsekunde)	
	q Status der Funkuhr:	Leerzeichen (ASCII-Code 20h)	Time Sync (GPS Lock)
		„?“ (ASCII-Code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage-Return (ASCII-Code 0Dh)		
<LF>	Line-Feed, ASCII-Code 0Ah		

16.3.16 IRIG-J-Zeittelegramm

Der IRIG-J-Zeitcode besteht aus einer Folge von ASCII-Zeichen, welche im Format 701 gesendet wird, d. h.

- 1 Startbit
- 7 Datenbit
- 1 Paritätsbit (ungerade)
- 1 Stopbit

Die Sekundenwechsel wird im Telegramm durch die Vorderflanke des Startbits gekennzeichnet. Das Telegramm umfasst 15 Zeichen und wird sekündlich mit einer Baudrate von 300 oder größer gesendet. Das Format ist:

<SOH>*TTT:HH:MM:SS*<CR><LF>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<SOH>	„Start of Header“ (ASCII-Code 0x01h)
TTT	Tag des Jahres (Ordinaldatum, 1..366)
HH, MM, SS	Zeit des Startbits in Stunde (HH), Minute (MM), Sekunde (SS)
<CR>	„Carriage-Return“ (ASCII-Code 0Dh)
<LF>	„Line-Feed“ (ASCII-Code 0Ah)

16.3.17 6021-Telegramm

Das 6021-Telegramm besteht aus einer Folge von 18 ASCII-Zeichen, eingeleitet durch das Zeichen <STX> (Start-of-Text, ASCII-Code 02h) und abgeschlossen durch die Zeichenfolge <LF> (Line-Feed, ASCII-Code 0Ah), <CR> (Carriage-Return, ASCII-Code 0Dh), <ETX> (End-of-Text, ASCII-Code 03h).

Es ist mit dem ➜ „Freelance-Telegramm“ weitgehend identisch, hat aber eine andere Terminierungsfolge.

Das Format ist:

<STX>*C9hhmmsstt mmjj*<LF><CR><ETX>

Die kursiv gedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind: Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Start-of-Text, ASCII-Code 02h

C Clock-Status. Dieser Wert ist als ASCII-Nibble hinterlegt: hier haben die jeweiligen Bits in der Binärfolge die folgenden Bedeutungen:

Bit 0 (minderwertigstes Bit)	Schaltsekunde angekündigt (1) / nicht angekündigt (0)
Bit 1	Schaltsekunde aktiv (1) / nicht aktiv (0)
Bit 2	Zeit von der Echtzeituhr ist gültig (1) / nicht gültig (0)
Bit 3 (höchstwertiges Bit)	Clock läuft synchron (1) / nicht synchron (0)

Beispiel: Wird an dieser Stelle C (ASCII-Code 0x43h) ausgegeben, entspricht das einem Binärwert von *1100*: Damit ist zu entnehmen, dass die Zeit der Echtzeituhr gültig ist, die Uhr läuft synchron und eine Schaltsekunde ist weder angekündigt worden noch aktiv.

9 UTC-Status der Clock und Wochentag. Dieser Wert ist als ASCII-Nibble* hinterlegt: hier tragen die 3 minderwertigsten Bits den Wochentag und können einen Wert zwischen 1 und 7 darstellen 7 (d. h. Montag bis Sonntag). Das höchstwertige Bit stellt den UTC-Flag dar.
Es beträgt 1, sofern die Clock auf UTC gestellt ist, und 0, falls es sich um eine lokale Zeitzone handelt. D. h. der Wert liegt im Bereich 1 ... 7, wenn die Clock lokale (nicht-UTC) Zeit ausgibt, und im Bereich 9 ... F, sofern die Clock UTC-Zeit ausgibt.

Beispiel: Wird an dieser Stelle 9 (ASCII-Code 0x39h) ausgegeben, entspricht das einem Binärwert von *1001*. Das höchstwertige Bit *1* zeigt, dass die Clock auf UTC-Zeit läuft, und der 3-Bit-Wert der minderwertigsten Bits *001* vermittelt, dass der Tag Montag ist.

hhmmss Aktuelle Uhrzeit:

hh	Stunden	(00 ... 23)
mm	Minuten	(00 ... 59)
ss	Sekunden	(00 ... 59 bzw. 60 während Schaltsekunde)

ttmmjj Aktuelles Datum:

tt	Tag	(01 ... 31)
mm	Monat	(01 ... 12)
jj	Letzte 2 Stellen des Jahres	(00 ... 99)

<LF> Line-Feed (ASCII-Code 0Ah)

<CR> Carriage-Return (ASCII-Code 0Dh)

<ETX> End-of-Text (ASCII-Code 03h)

* Bei ASCII-Nibbles stellt das eigentliche ASCII-Zeichen (0 ... 9, A ... F, ASCII-Codes 0x30h ... 0x39h bzw. 0x41h ... 0x46h) direkt das hexadezimale Äquivalent einer 4-Bit-Binärfolge dar. Zum Beispiel: Wenn die Clock „A" an diesen Stellen ausgibt, ist es nicht als das binäre Äquivalent des ASCII-Codes *0x41h* direkt auszulegen, sondern das des hexadezimalen Wert *0x0Ah* (binäres Äquivalent: *0x1010b*).

16.3.18 Freelance-Telegramm

Das Freelance-Telegramm besteht aus einer Folge von 18 ASCII-Zeichen, eingeleitet durch das Zeichen <STX> (Start-of-Text, ASCII-Code 02h) und abgeschlossen durch die Zeichenfolge <CR> (Carriage-Return, ASCII-Code 0Dh), <LF> (Line-Feed, ASCII-Code 0Ah), <ETX> (End-of-Text, ASCII-Code 03h).

Es ist mit dem ➜ „6021-Telegramm“ weitgehend identisch, hat aber eine andere Terminierungsfolge.

Das Format ist:

<STX>*C9hhmmsstt mmjj*<CR><LF><ETX>

Die kursiv gedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Zeichen fester Bestandteil der Zeichenfolge sind: Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Start-of-Text, ASCII-Code 02h

C Clock-Status. Dieser Wert ist als ASCII-Nibble hinterlegt: hier haben die jeweiligen Bits in der Binärfolge die folgenden Bedeutungen:

Bit 0 (minderwertigstes Bit)	Schaltsekunde angekündigt (1) / nicht angekündigt (0)
Bit 1	Schaltsekunde aktiv (1) / nicht aktiv (0)
Bit 2	Zeit von der Echtzeituhr ist gültig (1) / nicht gültig (0)
Bit 3 (höchstwertiges Bit)	Clock läuft synchron (1) / nicht synchron (0)

Beispiel: Wird an dieser Stelle C (ASCII-Code 0x43h) ausgegeben, entspricht das einem Binärwert von *1100*: Damit ist zu entnehmen, dass die Zeit der Echtzeituhr gültig ist, die Uhr läuft synchron und eine Schaltsekunde ist weder angekündigt worden noch aktiv.

9 UTC-Status der Clock und Wochentag. Dieser Wert ist als ASCII-Nibble* hinterlegt: hier tragen die 3 minderwertigsten Bits den Wochentag und können einen Wert zwischen 1 und 7 darstellen 7 (d. h. Montag bis Sonntag). Das höchstwertige Bit stellt den UTC-Flag dar.
Es beträgt 1, sofern die Clock auf UTC gestellt ist, und 0, falls es sich um eine lokale Zeitzone handelt. D. h. der Wert liegt im Bereich 1 ... 7, wenn die Clock lokale (nicht-UTC) Zeit ausgibt, und im Bereich 9 ... F, sofern die Clock UTC-Zeit ausgibt.

Beispiel: Wird an dieser Stelle 9 (ASCII-Code 0x39h) ausgegeben, entspricht das einem Binärwert von *1001*. Das höchstwertige Bit *1* zeigt, dass die Clock auf UTC-Zeit läuft, und der 3-Bit-Wert der minderwertigsten Bits *001* vermittelt, dass der Tag Montag ist.

hhmmss Aktuelle Uhrzeit:

hh	Stunden	(00 ... 23)
mm	Minuten	(00 ... 59)
ss	Sekunden	(00 ... 59 bzw. 60 während Schaltsekunde)

ttmmjj Aktuelles Datum:

tt	Tag	(01 ... 31)
mm	Monat	(01 ... 12)
jj	Letzte 2 Stellen des Jahres	(00 ... 99)

<CR> Carriage-Return (ASCII-Code 0Dh)

<LF> Line-Feed (ASCII-Code 0Ah)

<ETX> End-of-Text (ASCII-Code 03h)

* Bei ASCII-Nibbles stellt das eigentliche ASCII-Zeichen (0 ... 9, A ... F, ASCII-Codes 0x30h ... 0x39h bzw. 0x41h ... 0x46h) direkt das hexadezimale Äquivalent einer 4-Bit-Binärfolge dar. Zum Beispiel: Wenn die Clock „A“ an diesen Stellen ausgibt, ist es nicht als das binäre Äquivalent des ASCII-Codes 0x41h direkt auszulegen, sondern das des hexadezimalen Wert 0x0Ah (binäres Äquivalent: 0x1010b).

16.3.19 ITU-G8271-Y.1366-Tageszeittelegramm

Der Norm ITU-G8271-Y.1366 schreibt eine Übertragung dieses Telegramms mit einer Übertragungsrate von 9600 Baud und einem Format von 8N1 vor. Die Telegrammdaten sind nicht früher als 1 ms nach der steigenden Flanke des PPS-Signals zu senden und die Übertragung ist innerhalb von 500 ms abzuschließen. Das Telegramm ist einmal pro Sekunde zu senden und bezeichnet die steigende Flanke des PPS-Signals.

Das ITU-G8271-Y.1366-Tageszeittelegramm selbst, wie es von Meinberg-Uhren ausgegeben wird, beträgt immer 21 Bytes. Auch wenn der Norm kurz die Verwendung von zwei ASCII-Zeichen an den ersten beiden Stellen erwähnt, ist anzumerken, dass das Telegramm streng genommen kein ASCII-String ist. Werte, die aus mehreren Oketten bestehen, sind als Big-Endian-Werte ausgegeben, und jedes Byte wird mit dem niedrigwertigsten Bit **zuerst** übertragen. Auch wenn die ersten beiden Zeichen in diesem Sinne als die ASCII-Zeichen „C“ (ASCII-Code 0x43h, Binär `00101011`) bzw. „M“ (ASCII-Code 0x4Dh, Binär `01001101`) gelten, werden diese als `11010100` und dann `10110010` übermittelt.

Die Standard-Bytereihenfolge (mit dem minderwertigsten Bit zuerst bei jedem Byte) ist wie folgt:

Byte-Nr.	Bedeutung
0–1	Immer 0x43h, dann 0x4Dh. Die sind als Sync-Zeichen 1 bzw. 2 bezeichnet und gelten als Trennzeichen zwischen Nachrichten.
2	Die Klasse des Telegramms. Beträgt immer 0x01h.
3	Die ID des Telegramms. Bei den Tageszeittelegrammen von Meinberg-Uhren beträgt dieser Wert immer 0x01h.
4–5	Die Länge der Nutzdaten, ohne Sync-Zeichen, Telegramm-Klasse, Telegramm-ID und Prüfsumme. Wird als 16-Bit-Ganzzahl ohne Vorzeichen ausgegeben. Bei den Tageszeittelegrammen von Meinberg-Uhren beträgt dieser Wert immer 0x0Eh.
6–11	PTP-Zeit bzw. die Anzahl der Sekunden in der TAI-Zeitskala. Wird als 48-Bit-Ganzzahl ohne Vorzeichen ausgegeben.
12	Dieses Byte ist für eine zukünftige Definition vorbehalten und wird auf 0x00h gesetzt.
13	Übermittelt einige Zeitstatus-Flags: **Bit 0:** Bevorstehende positive Schaltsekunde **Bit 1:** Bevorstehende negative Schaltsekunde **Bit 2:** UTC-Offset gültig **Bit 3:** Reserviert **Bit 4:** Die Zeit lässt sich auf eine primäre Referenz zurückverfolgen **Bit 5:** Die Frequenz lässt sich auf eine primäre Referenz zurückverfolgen **Bit 6:** Reserviert **Bit 7:** Reserviert
14–15	Aktueller Offset zwischen TAI und UTC in Sekunden, wird als 32-Bit-Ganzzahl ohne Vorzeichen ausgegeben.
16–19	Dieses Byte ist für eine zukünftige Definition vorbehalten und wird auf 0x00h gesetzt.
20	Eine 8-Bit-CRC-Prüfsumme, die auf Basis der Bytes 2 bis 19 berechnet wird.

16.3.20 CISCO ASCII-Zeittelegramm

Das CISCO-ASCII-Zeittelegramm besteht aus einer Folge von mindestens 73 ASCII-Zeichen. Das Format ist:

*.A.*mjdxx*,*jj/mm/tt*,*hh*:*mm*:*ss*,*+3600.0*,*12N34.567*,*123W45.678*,+1234,
EV<SP>GPS<SP>FLT

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

*	Sync-Status der Uhr: *: Uhr wird von der Referenz geführt !: Uhr ist nicht synchron
A	Die Version des Formats. Bei einer Meinberg Uhr ist dieser Wert immer „A“.
mjdxx	Das aktuelle Datum als Modifiziertes Julianisches Datum.
jj/mm/tt	Das aktuelle Datum als Gregorianisches Datum (*yy*/*mm*/*dd*).
hh:mm:ss	Die aktuelle Zeit im 24-Stunden-Format.
+3600	Der aktuelle lokale Zeitoffset in Sekunden. Gibt die Uhr UTC-Zeit aus, lautet dieser Wert 00000.0. Gibt die Uhr eine lokale Zeit aus dagegen, wird das 1. Zeichen das Vorzeichen – bzw. +) sein und und die nachfolgenden Zeichen bis zum Punkt stellen den Offset dar. Beispiel: Ist MEZ als Zeitzone eingestellt, wird hier +3600 ausgegeben.
0	Ankündigung einer Schaltsekunde.
12N34.567	Die aktuelle geographische Breite des GNSS-Empfängers. Ist die Zeitreferenz aber kein GNSS-Empfänger, lautet dieses Feld 00 00.000.
123W45.678	Die aktuelle geographische Länge des GNSS-Empfängers. Ist die Zeitreferenz aber kein GNSS-Empfänger, lautet dieses Feld 000 00.000.
+1234	Die aktuelle Höhe über dem Meerespegel des GNSS-Empfängers. Ist die Zeitreferenz aber kein GNSS-Empfänger, lautet dieses Feld +0000.
EV	Zeigt die Einstufung eines eventuellen Alarms bei der Uhr: EV: Ereignis, nicht als Fehler einzustufen MN: Geringfügiger Fehler MJ: Schwerwiegender Fehler CL: Betriebskritischer Fehler
GPS	Zeigt die Quelle des aktuellen Fehlers (z. B. „GPS“ bei GPS-Empfängern).
FLT	Zeigt die Ursache des aktuellen Fehlers (z. B. „FLT“ bei einem Hardware-Fehler).

16.3.21 NTP-Type-4-Zeittelegramm

Das NTP-Type-4-Zeittelegramm besteht aus einer Folge von 24 ASCII-Zeichen. Das Format ist:

?<SP>*jj*<SP>*ttt*<SP>*hh:mm:ss.SSS*L<SP>S

Die kursivgedruckten Buchstaben werden durch Zahlen in ASCII-Format ersetzt, während die anderen Bestandteil des Zeittelegramms sind. Die einzelnen Zeichengruppen haben folgende Bedeutung:

?	Sync-Status der Uhr:		
	Leerzeichen:	Uhr wird von der Referenz geführt	
	„?“:	Uhr ist nicht synchron	
jj	Jahr ohne Jahrhundert		(00..99)
ttt	Jahrestag		(001..366)
hh:mm:ss.SSS	Die Zeit:		
	hh	Stunden	(00 ... 23)
	mm	Minuten	(00 ... 59)
	ss	Sekunden	(00..59 bzw. 60 während Schaltsekunde)
	SSS	Millisekunden	(000..999)
L	Ankündigung einer Schaltsekunde:		
	Leerzeichen:	Keine bevorstehende Schaltsekunde	
	„L“:	Schaltsekunde steht bevor	
S	Sommerzeitindikator:		
	„S“:	Winterzeit (Standardzeit)	
	„D“:	Sommerzeit (Daylight Saving Time)	

16.4 Zeitcode-Formate

Die Bezeichnung eines IRIG-Formats besteht aus einem Buchstaben und 3 darauf folgenden Ziffern. Jeder Buchstabe sowie die Ziffer an jeder Stelle legt eine Eigenschaft des entsprechenden IRIG-Codes fest.

Abhängig von Ihrem Meinberg-Produkt werden mehr oder weniger Timecode-Formate unterstützt.

A002:	1000 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code)
A003:	1000 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code), Tagessekunden (SBS-Code)
A132:	1000 pps, AM-Sinussignal, 10-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code)
A133:	1000 pps, AM-Sinussignal, 10-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code), Tagessekunden (SBS-Code)
B002:	100 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code)
B003:	100 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code), Tagessekunden (SBS-Code)
B006:	100 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code), Kalenderjahr (BCD-Code)
B007:	100 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code), Kalenderjahr (BCD-Code), Tagessekunden (SBS-Code)
B122:	100 pps, AM-Sinussignal, 1-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code)
B123:	100 pps, AM-Sinussignal, 1-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code), Tagessekunden (SBS-Code)
B126:	100 pps, AM-Sinussignal, 1-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code), Kalenderjahr (BCD-Code)
B127:	100 pps, AM-Sinussignal, 1-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code), Kalenderjahr (BCD-Code), Tagessekunden (SBS-Code)
E002:	10 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code)
E112:	10 pps, AM-Sinussignal, 100-Hz-Trägerfrequenz Jahresuhrzeit (BCD-Code)
G002:	10000 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code)
G006:	10000 pps, DCLS-Signal, pulsbreitenmoduliert, kein Träger Jahresuhrzeit (BCD-Code), Kalenderjahr (BCD-Code)
G142:	10000 pps, AM-Sinussignal, 100-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code)
G146:	10000 pps, AM-Sinussignal, 100-kHz-Trägerfrequenz Jahresuhrzeit (BCD-Code), Kalenderjahr (BCD-Code)

Abkürzungen:
BCD = Binary-Coded Decimal, SBS = Straight Binary Seconds

Neben den IRIG-Standards existieren auch Spezifikationen durch andere Gremien, die spezielle Erweiterungen definieren.

AFNOR:	Code lt. NF S87-500, 100 pps, AM-Sinussignal, 1-kHz-Träger, Jahresuhrzeit in BCD-Code, vollständiges Datum, Tagessekunden in SBS-Code, Ausgangspegel vom Standard vorgegeben.
IEEE 1344:	Code. lt. IEEE 1344-1995, 100 pps, AM-Sinussignal, 1-kHz-Träger, Jahresuhrzeit in BCD-Code, Tagessekunden in SBS-Code, IEEE-1344-Erweiterungen für Datum, Zeitzone, Sommer-/Winterzeit und Schaltsekunde im Control Funktions Segment (CF) (s.a. Tabelle „Belegung des CF-Segmentes beim IEEE-1344-Code“)
IEEE C37.118:	Wie IEEE 1344, jedoch mit gedrehtem Vorzeichenbit für den UTC-Offset
NASA 36:	100 pps, AM-Sinussignal, 1-kHz-Träger, Auflösung: 10 ms (DCLS), 1 ms (modulierte Trägerwelle) Jahresuhrzeit in BCD-Code: 30 Bits - Sekunden, Minuten, Stunden und Tage

16.5 Übersicht der programmierbaren Signale

In Meinberg-Systemen mit programmierbaren Impulsausgängen, stehen Ihnen je nach System mehr oder weniger der folgenden Signaloptionen zur Verfügung:

Idle

Über den Modus „**Idle**“ können die programmierbaren Impulsausgänge einzeln deaktiviert werden.

Timer

Im „**Timer**“ Modus simuliert der Ausgang eine Schaltuhr mit Tagesprogramm. Auf jedem Ausgang der Funkuhr sind je drei Ein- und drei Ausschaltzeiten am Tag programmierbar. Soll eine Schaltzeit programmiert werden, so muss die Einschaltzeit „**ON**“ und die zugehörige Ausschaltzeit „**OFF**“ eingetragen werden. Liegt der Einschaltzeitpunkt später als der Ausschaltzeitpunkt, so wird das Schaltprogramm derart interpretiert, dass der Ausschaltzeitpunkt am darauffolgenden Tag liegt, so dass das Signal weiterhin über Mitternacht hinaus anliegt.

Ein Programm On Time *23:45:00*, Off Time *0:30:00* würde demnach bewirken, dass am Tag *n* um 23.45 Uhr der Ausgang aktiviert, und am Tag *n+1* um 0.30 Uhr deaktiviert wird. Sollen eines oder mehrere der drei Programme ungenutzt bleiben, so müssen in die Felder „**ON**“ und „**OFF**“ nur gleiche Schaltzeiten eingetragen werden. Mit „**Signal**“ wird der Aktiv-Zustand für die Schaltzeiten angegeben. Ist „*Normal*“ angewählt, liegt am entsprechenden Ausgang im inaktiven Zustand (außerhalb einer Schaltzeit) ein low-Pegel, und im aktiven Zustand ein high-Pegel an. Ist dagegen „*Inverted*“ angewählt, liegt im inaktiven Zustand ein high-Pegel und im aktiven Zustand ein low-Pegel an.

Single Shot

Der „**Single Shot**“ Modus erzeugt pro Tag einen einmaligen Impuls definierter Länge. Im Feld „**Time**“ wird die Uhrzeit eingegeben, zu der ein Impuls erzeugt werden soll. Der Wert „**Length**“ erlaubt die Einstellung der Impulslänge in 10 ms Schritten zwischen *10 ms* und *10000 ms* (10 Sekunden). Eingaben, die nicht im 10 ms Raster liegen, werden abgerundet.

Cyclic Pulse

Im Modus „**Cyclic Pulse**“ werden zyklisch wiederholter Impulse erzeugt. Die Zeit zwischen zwei Impulsen (die Zykluszeit) muss immer in Stunden, Minuten und Sekunden eingegeben werden. Zu beachten ist, dass die Impulsfolge immer mit dem Übergang 0.00.00 Uhr Ortszeit synchronisiert wird. Dies bedeutet, dass der erste Impuls an einem Tag immer um Mitternacht ausgegeben wird, und ab hier mit der gewählten Zykluszeit wiederholt wird. Eine Zykluszeit von *2 s* würde also Impulse um 0.00.00 Uhr, 0.00.02 Uhr, 0.00.04 Uhr etc. hervorrufen. Grundsätzlich ist es möglich jede beliebige Zykluszeit zwischen 0 und 24 Stunden einzustellen, jedoch sind meistens nur Impulszyklen sinnvoll, die immer gleiche zeitliche Abstände zwischen zwei Impulsen ergeben. So würden zum Beispiel bei einer Zykluszeit von *1 Stunde 45 Min* Impulse im Abstand von 6300 Sekunden ausgegeben. Zwischen dem letzten Impuls eines Tages und dem 0.00 Uhr Impuls würden jedoch nur 4500 Sekunden liegen.

Pulse-per-Second, Pulse-per-Minute, Pulse-per-Hour

Diese Modi erzeugen Impulse definierter Länge pro Sekunde, pro Minute bzw. pro Stunde. Die angezeigte Optionen sind für alle drei Betriebsarten gleich. Der Wert „**Pulse Length**“ bestimmt die Impulslänge zwischen *10 ms* und *10000 ms* (10 Sekunden).

DCF77 Marks

Im Betriebsmodus „**DCF77 Marks**“ wird der gewählte Ausgang in den DCF77-Simulationsmodus geschaltet: Der Ausgang wird im Takt der für den DCF77 Code typischen 100 und 200 ms Impulse (logisch 0/1) aktiviert.

Durch das Fehlen der 59. Sekundenmarke wird die Minutenmarke angekündigt.

DCF77-like M59

In der 59. Sekundenmarke wird ein 500 ms-Impuls gesendet.

Im Feld „**Timeout**“ kann eingegeben werden, nach wie vielen Minuten im Falle eines Freilaufes der Funkuhr der DCF77-Simulationsausgang abgeschaltet werden soll. Wird hier der Wert *Null* eingegeben, ist die Timeout-Funktion inaktiv, so dass die simulierte DCF77-Ausgabe nur manuell abgeschaltet werden kann.

Position OK, Time Sync und All Sync

Zur Ausgabe des Synchronisationsstatus der Funkuhr sind drei verschiedene Modi auswählbar. Im Modus „**Position OK**“ wird der Ausgang aktiviert, wenn der GNSS-Empfänger genügend Satelliten empfängt, um seine Position zu berechnen.

Der Modus „**Time Sync**“ aktiviert den Ausgang immer dann, wenn die interne Zeitbasis der Funkuhr mit der Zeitbasis der GNSS-Referenz synchron läuft. Der Modus „**All Sync**“ berichtet, ob beide Zustände zutreffen, d. h. der entsprechende Ausgang wird immer dann aktiviert, wenn die Position berechnet werden kann **und** die interne Zeitbasis mit der Zeitbasis der Referenzkonstellation synchronisiert wurde.

DCLS-Timecode

DC-Level-Shift Timecode. Die Auswahl des Timecodes wird über den Bereich „**Uhr** → **IRIG-Einstellungen**“ im Webinterface vorgenommen.

1 MHz Frequency, 5 MHz Frequency, 10 MHz Frequency

Bei diesen Modi wird eine feste Frequenz des programmierbaren Impulsausgangs von 1, 5 bzw. 10 MHz mit fester Phasenbeziehung zum PPS generiert (d. h. die fallende Flanke des Signals ist gekoppelt an die steigende Flanke vom PPS).

Synthesizer Frequency

Mit diesem Modus wird eine individuelle Frequenz ausgegeben. Die Ausgabe des Frequenzsynthesizers wird über den Bereich „**Uhr** → **Synthesizer**“ im Webinterface vorgenommen.

Time Slots per Minute

In diesem Modus wird jede Minute gleichmäßig in Zeit-Tranchen geteilt, die einzelne während den entsprechenden Sekunden der Minute zu- oder abgeschaltet werden können. Beispiel: Bei einer Auswahl von *sechs* Zeit-Tranchen kann der Benutzer bestimmen, ob der Ausgang in den Tranchen 0–10 Sekunden, 10–20 Sekunden, 20–30 Sekunden, 30–40 Sekunden, 40–50 Sekunden und 50–60 Sekunden aktiviert wird. Ist nur die Tranche *10–20 Sekunden* aktiviert, wird der Ausgang nur zwischen 10 und 20 Sekunde einer jeden Minute aktiviert. Ansonsten bleibt der Ausgang deaktiviert.

PTTI 1PPS

Bei diesem Modus wird ein PPS von 20 μs Pulsweite ausgegeben.

16.6 SyncMon Formate

SyncMon-Format für die Verwendung der LANTIME-Firmware:

```
SyncMon 172.27.100.32 M3000_100_57_NTP_LAN0_test 58154 34813 2018-02-05T09:
40: 13 + 00: 00 0.000000494 0.000041453 0.000073266 1 R -0.000011100
0.000041453
```

Schlüssel- und Wert-Paare
Das Format mit Schlüsselwertpaaren kann direkt von einem SPLUNK-Datenbankserver aus aufgerufen werden und hat folgendes Format:

isoTime	=	2018-02-05T09: 40: 13 + 00: 00
syncMonName	=	SyncMon
optInterfaceIp	=	172.27.100.32
utcTime	=	1517823613
node	=	M3000_100_57_NTP_LAN0_test
offset1	=	0.000000494
offset2	=	0.000041453
pathDelay	=	0.000073266
status	=	Stratum: 1 / [10]
offset1Min	=	-0.000011100
offset1Max	=	0.000041453
type	=	NTP / SW / CPU

JSON
Das JSON-Format kann von den meisten Datenbanken direkt verarbeitet werden und hat das folgende Format:

```
{
    „IsoTime“:          „2018-02-05T09: 40: 13 + 00: 00“,
    „syncMonName“:      „SyncMon“,
    „optInterfaceIp“:   „172.27.100.32“,
    „utcTime“:          1517823613,
    „node“:             „M3000_100_57_NTP_LAN0_test“,
    „offset1“:          0.000000494,
    „offset2“:          0.000041453,
    „pathDelay“:        0.000073266,
    „status“:           „stratum 1 / [10]“,
    „offset1Min“:       - 0.000011100,
    „offset1Max“:       0.000041453,
    „type“:             „NTP / SW / CPU“
}
```

16.7 IEC 61850 Grundlagen

IEC 61850 ist ein internationaler Standard für Kommunikationsprotokolle in elektrischen Umspannwerken und Stromversorgungssystemen.

Die Norm IEC 61850 bietet einen umfassenden Rahmen für den Austausch von Daten und Informationen zwischen verschiedenen Geräten und Systemen innerhalb einer Schaltanlage. Sie definiert eine einheitliche Kommunikationsarchitektur, Datenmodelle und Protokolle, die eine nahtlose Integration und Interoperabilität zwischen den Geräten verschiedener Hersteller ermöglichen.

Die wichtigsten Merkmale der Norm IEC 61850 sind:

- Kommunikationsarchitektur: Die Norm definiert eine mehrschichtige Architektur, die den Austausch von Informationen zwischen verschiedenen Ebenen eines Stationsautomatisierungssystems ermöglicht, wie z. B. der Prozess-, Feld- und Stationsebene. Sie legt die Rollen und Verantwortlichkeiten der verschiedenen Geräte und Komponenten im System fest.
- Datenmodellierung: IEC 61850 führt ein standardisiertes Datenmodell ein, das eine gemeinsame Sprache für die Beschreibung der Daten und Funktionen von Schaltanlagen bereitstellt. Dies ermöglicht eine einheitliche Darstellung und Interpretation von Daten über verschiedene Geräte und Systeme hinweg.
- Kommunikationsprotokolle: Die Norm definiert Protokolle für die Echtzeitkommunikation zwischen Geräten, darunter das Generic Object Oriented Substation Event (GOOSE) und Sampled Measured Values (SMV). Diese Protokolle ermöglichen einen schnellen und zuverlässigen Austausch von Steuerbefehlen, Statusinformationen und Messwerten.
- Konfiguration und Projektierung: IEC 61850 führt einen standardisierten Ansatz für die Systemkonfiguration und -entwicklung ein, der die Konfiguration, das Testen und die Wartung von Stationsautomatisierungssystemen erleichtert. Sie bietet Richtlinien für die Definition von Systemanforderungen, die Konfiguration von Geräten und die Verwaltung von Kommunikationsnetzwerken.
- Interoperabilität: Eines der Hauptziele der IEC 61850 ist die Förderung der Interoperabilität zwischen Geräten und Systemen verschiedener Hersteller. Durch die Verwendung von standardisierten Datenmodellen und Kommunikationsprotokollen erleichtert die Norm die nahtlose Integration und den Austausch von Informationen, unabhängig vom jeweiligen Anbieter oder der verwendeten Technologie.

16.7.1 Datensätze

Ein Datensatz in der IEC 61850 ist eine Liste von Variablen, die gemeinsam beobachtet und auf effizientere Weise übertragen werden können. Datensätze können durch CID/SCL-Dateien definiert werden oder von MMS-Clients über das MMS-Protokoll erstellt werden (Manufacturing Messaging Specification (definiert in IEC 61850-8-1).

Die Datensätze in der Norm IEC 61850 werden mit Hilfe des Common Information Model (CIM) definiert, das eine standardisierte Darstellung der Daten und Funktionen des Stromnetzes ist. Das CIM bietet eine gemeinsame Sprache für die Beschreibung der Datenelemente und ihrer Beziehungen innerhalb einer Substation.

Ein Datensatz besteht in der Regel aus einer Reihe von Datenattributen oder Parametern, die spezifische Informationen über ein Gerät definieren, z. B. seinen Status, seine Netzwerkadresse, oder seine Konfiguration. Diese Attribute sind innerhalb des Datensatzes in logischen Gruppen organisiert, um die Interpretation der Daten zu erleichtern.

Substation-Konfigurationssprache (SCL)

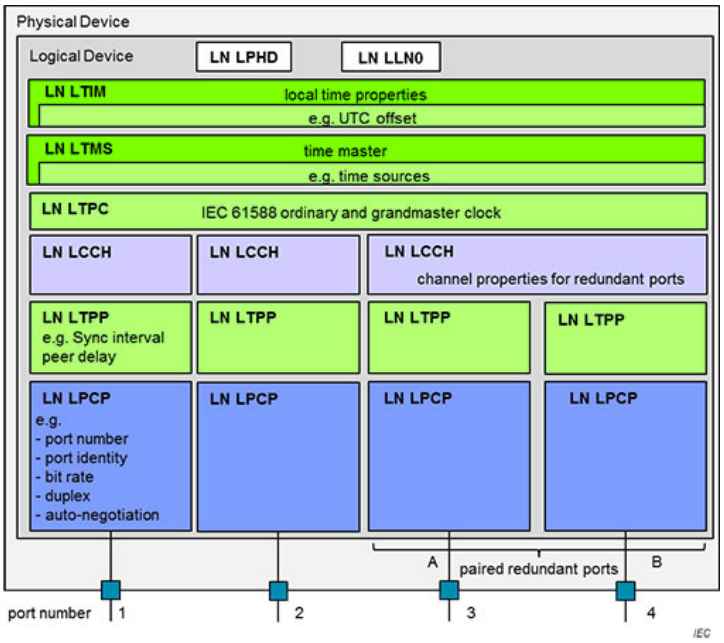
Die Substation Configuration Language ist ein XML-basiertes Dateiformat zur Beschreibung von IEDs und deren Beziehungen. Sie ist für die Beschreibung einer ganzen Substation und aller ihrer Kommunikationseigenschaften vorgesehen. SCL kann verwendet werden, um IEC 61850-konforme IEDs zu konfigurieren. Das Datenmodell (die Organisation der Daten eines Geräts) wird in den meisten Fällen in einer SCL-Datei definiert. Diese SCL-Datei kann dann von einem Werkzeug in eine Beschreibung umgewandelt werden, die von einem IEC 61850-Client- oder -Servergerät verwendet werden kann. Es gibt verschiedene Typen von SCL-Dateien. Die am häufigsten verwendeten Typen sind:

- **ICD (IED Capability Description):** ICD-Dateien enthalten eine Beschreibung der Eigenschaften eines Geräts. Es ist wie eine Vorlage, die eine generische Beschreibung aller Funktionen und Objekte enthält, die von einem bestimmten Gerät unterstützt werden können. Die ICD wird vom Entwickler/Hersteller erstellt. Die ICD-Datei dient als Eingabe für ein Systemkonfigurationswerkzeug (SCT), das der Anwender verwendet, um eine Konfigurationsbeschreibungsdatei für die Substation (SCD) zu erstellen.
- **SCD (Substation Configuration Description):** Die SCD enthält alle Geräte, die für das System benötigt werden. Das SCT kann verwendet werden, um eine Configured IED Description-Datei (CID) aus der SCD zu exportieren, die eine Beschreibung der Funktionen und Objekte enthält, die ein IED für dieses spezifische System benötigt.
- **CID (Configured IED Description):** enthält die vollständige Konfiguration für eine einzelne IED. Diese Datei wird normalerweise als Teil der endgültigen Gerätekonfiguration auf das IED geladen.

Die Konfiguration und Verwaltung von Datensätzen erfolgt in der Regel mit Engineering-Tools, die der Norm IEC 61850 entsprechen. Diese Werkzeuge ermöglichen es Systemintegratoren und Ingenieuren, Datensätze auf der Grundlage der spezifischen Anforderungen der Substation zu definieren und zu konfigurieren.

16.7.2 Aufbau einer IEC 61850 CID-Datei

In der IEC 61850 wird eine CID-Datei (Configured IED Description) verwendet, um die Konfiguration und das Datenmodell eines intelligenten elektronischen Geräts (IED) innerhalb eines Stationsautomatisierungssystems zu beschreiben. Die CID-Datei bietet eine strukturierte Darstellung der Eigenschaften, Datenattribute, Kommunikationsparameter und anderer relevanter Informationen des IED. Die Struktur einer CID-Datei entspricht in der Regel dem XML-Format (Extensible Markup Language).



Überblick über die Struktur einer IEC 61850 CID-Datei:

- **HEAD** - Kopfzeile: Der Kopfteil der CID-Datei enthält allgemeine Informationen über die Datei, wie z. B. die Version, das Erstellungsdatum und den Autor. Er kann auch zusätzliche Metadaten in Bezug auf das IED oder die Substation enthalten.
- **LD** - Logisches Gerät: Der Abschnitt „Logisches Gerät“ definiert die logische Darstellung des IED innerhalb der Substation. Er enthält Informationen wie den logischen Gerätenamen, die Identifikation und die Beschreibung. In diesem Abschnitt können auch die Kommunikationsadresse und die Netzwerkparameter für das IED angegeben werden.
- **LN** - Logische Knoten: Innerhalb des logischen Geräts stellen die logischen Knoten die funktionalen Komponenten oder Geräte des IED dar. Jeder logische Knoten entspricht einer bestimmten Funktion oder einem Gerätetyp, z. B. einem Leistungsschalter, einem Spannungswandler oder einem Schutzrelais. Der Abschnitt Logische Knoten definiert die Attribute, Datenobjekte und Dienste, die mit jedem logischen Knoten verbunden sind.
- **DO** - Datenobjekte: Die Datenobjekte stellen die Datenattribute und Funktionen der logischen Knoten dar. Sie definieren die spezifischen Parameter, Statusflags und Messwerte, die mit jedem Datenobjekt verbunden sind. Der Abschnitt Datenobjekte beschreibt das Datenmodell des IED, einschließlich seiner Struktur, Datentypen und Beziehungen zwischen Objekten.
- **Services** - Dienste: Der Abschnitt „Dienste“ der CID-Datei spezifiziert die vom IED unterstützten Dienste, wie z. B. Ereignisberichte, Steuerbefehle oder Dateiübertragung. Er definiert die Kommunikationsprotokolle, Nachrichtenformate und das Verhalten der einzelnen Dienste. Dieser Abschnitt kann auch die Zuordnung von Datenobjekten zu den in der Norm IEC 61850 definierten Diensten und Kommunikationsprotokollen enthalten.
- **Templates** - Substitutionsschablonen: Substitutionsvorlagen bieten eine Möglichkeit, wiederverwendbare Vorlagen für häufig verwendete Datenobjekte oder Konfigurationen zu definieren. Sie ermöglichen die effiziente Wiederverwendung von Konfigurationen über mehrere IEDs oder Umspannwerksprojekte hinweg, wodurch Doppelarbeit vermieden und das Konfigurationsmanagement vereinfacht wird.

- SCL-Version und Namespace: Die CID-Datei kann Informationen über die Version der IEC 61850-Norm enthalten, an die sie sich hält. Sie kann auch den mit der CID-Datei verbundenen Namensraum angeben, der ein eindeutiger Bezeichner ist, der zur Referenzierung und Identifizierung der IED innerhalb der Substation verwendet wird.

Die Struktur einer CID-Datei kann je nach der spezifischen Implementierung und den Anforderungen der IED und der Substation variieren. Die oben genannten Elemente geben jedoch einen allgemeinen Überblick über die Informationen, die typischerweise in einer IEC 61850 CID-Datei enthalten sind.

16.8 Funktionsweise von Navigation Message Authentication (NMA)

Spoofing ist definiert als die Manipulation von GNSS-Nachrichten mit dem Ziel, einem Empfänger vorzugaukeln, dass er ein legitimes Signal empfängt. Spoofing steht im Gegensatz zum *Jamming*, bei dem die GNSS-Signale in einer lokalen Umgebung einfach unterdrückt werden, indem Rauschen in die Bandfrequenzen eingebracht wird.

Arten von Spoofing

Spoofing-Strategien lassen sich im Wesentlichen in zwei Kategorien einteilen: Die Weiterleitung echter GNSS-Nachrichten, das so genannte *Meaconing*, und die Erzeugung künstlicher GNSS-Nachrichten auf der Trägerfrequenz, entweder in Phase mit dem ursprünglichen Signalträger (synchrones Spoofing) oder phasenverschoben (asynchrones Spoofing).

Meaconing ist die am wenigsten ausgefeilte Methode des Spoofing, bei der einfach eine echte GNSS-Nachricht von einem anderen Standort oder einem früheren Zeitpunkt weitergegeben wird.

Asynchrone und synchrone Spoofing-Techniken hingegen beinhalten die Verbreitung gefälschter GNSS-Nachrichten.

Asynchrone Angriffe sind vergleichsweise einfacher auszuführen, aber auch leichter zu erkennen. Da ein asynchrones Angriffssignal nicht in Phase mit dem echten GNSS-Signal ist, verlieren die Empfänger in der Regel die Verbindung zum echten Signal und benötigen eine gewisse Zeit, um das neue Signal zu erfassen. Dementsprechend kann der unerklärliche Verlust einer GNSS-Sperre auch ohne maßgeschneiderte Spoofing-Erkennung als Warnzeichen für einen Spoofing-Versuch gewertet werden.

Synchrones Spoofing ist natürlich viel schwieriger zu erkennen und auszuführen. Asynchrones Spoofing weist einen verräterischen Phasensprung auf, den die Empfänger erkennen können, um einen Alarm auszulösen, während synchrones Spoofing in der Regel auf der Phasensynchronisation mit dem echten Signal beruht und daher diese Phasendiskontinuität nicht aufweist. Als solches kann es aus Sicht des Angreifers sehr effektiv sein, insbesondere wenn es mit einer sehr subtilen und allmählichen Abweichung von der echten GNSS-Quelle kombiniert wird. Diese Technik ist aber logistisch schwierig durchzuführen und daher weniger häufig anzutreffen.

Abgesehen von einer begrenzten Anzahl von legitimen technischen und Testanwendungen gibt es nur wenige gutartige Anwendungen für Spoofing. Spoofing ist typischerweise eine Strategie bei kriminellen Aktivitäten, Spionage und militärischen Operationen, um kritische Anwendungen zu stören oder sich der Kontrolle zu entziehen. Sicherheitsorientierte Operationen, die darauf abzielen, kritische Infrastrukturen oder Operationen von der GNSS-Abdeckung abzuschirmen, haben keinen Bedarf an den durch Spoofing ermöglichten Täuschungsmanövern und verwenden stattdessen typischerweise Jamming-Strategien, um eine präzise Geopositionierung zu verhindern.

Schützen von GNSS-Signalen

Militärische GNSS-Anwendungen profitieren seit langem von den Vorteilen des Schutzes und der Authentifizierung von GNSS-Signalen. Da jedoch zivile Anwendungen, die in hohem Maße auf den genauen und echten GNSS-Empfang angewiesen sind - insbesondere kritische Infrastrukturen wie der Finanz- und der Energiesektor, in den letzten Jahren zunehmend unter Beschuss geraten sind, ist das Interesse daran gewachsen, zivile Anwendungen mit einem ähnlichen Schutz zu versehen.

Bei militärischen Anwendungen beinhalten solche Sicherheitsmechanismen typischerweise die Verschlüsselung von GNSS-Signalen von Anfang an und erfordern streng kontrolliertes Entschlüsselungsmaterial, um sie zu entschlüsseln, oder die Übertragung von Authentifizierungsdaten über einen sicheren Kanal, zu dem nur ein sehr begrenzter Kreis von autorisierten Benutzern Zugang hat. Aufgrund der öffentlichen Verfügbarkeit von zivilen GNSS-Diensten sind die logistischen und sicherheitstechnischen Herausforderungen bei einer solchen zivilen Implementierung etwas anders.

Die Grundlagen der Authentifizierung von Navigationsnachrichten

Jeder Sicherheitsmechanismus, der die Übertragung von Authentifizierungsdaten für GNSS-Navigationsnachrichten zur Überprüfung der Authentizität der Navigationsnachricht beinhaltet, wird als **Navigation Message Authentication** oder einfach als **NMA** bezeichnet. NMA-Implementierungen zielen darauf ab, Schutz gegen Spoofing zu bieten, indem sie es den Empfängern ermöglichen, betrügerische Nachrichten anhand von Korrelationsdaten aus einer vertrauenswürdigen Quelle zu identifizieren.

Während NMA ein seit langem etabliertes Feature des militärischen GNSS ist (z. B. das hochpräzise verschlüsselte P(Y)-Codesignal), sind NMA-Mechanismen für die zivile Nutzung noch relativ neu, und daher gibt es nur eine kleine Anzahl von Herstellern kommerzieller Empfänger, die sie bereits unterstützen. Meinberg ist einer dieser wenigen Anbieter.

NMA funktioniert in der Regel durch die Erzeugung einer digitalen Signatur oder einer Zusammenfassung von GNSS-Daten an einem hochsicheren Punkt der Kommunikationskette. Eine solche Signatur oder Zusammenfassung kann von den GNSS-Satelliten selbst oder von terrestrischen Referenzstationen erzeugt werden, wobei die Sicherheit durch Einwegkryptographie oder kontrollierten Zugriff auf das Schlüsselmaterial erreicht wird. Diese Signaturen oder Zusammenfassungen werden dann auf sichere Weise an den Empfänger gesendet - einige native Lösungen übertragen die Signatur auf ihren eigenen Frequenzbändern, während andere die Daten über einen separaten Satellitendienst auf einer anderen Frequenz innerhalb des L-Bandes übertragen. NMA-Lösungen können sich auch darin unterscheiden, wie sie ihre Signaturdaten und das zur Entschlüsselung oder Authentifizierung benötigte Schlüsselmaterial aufteilen - manche verteilen den Schlüssel über denselben Kanal wie die GNSS-Daten (wobei die Sicherheit durch eine verzögerte Übermittlung des Schlüssels erreicht wird), andere verwenden eine andere Frequenz oder ein anderes System, wieder andere einen völlig anderen Kanal wie das öffentliche Internet.

Theoretisch könnte jeder Kanal, der in der Lage ist, digitale Daten in Echtzeit und mit geringer Latenz zu übertragen, wie z.B. das öffentliche Internet oder der terrestrische Rundfunk, für die Übermittlung von Signaturen und Schlüsseln genutzt werden, obwohl die Sicherheit und Zuverlässigkeit solcher Methoden natürlich umstritten ist.

Aktuelle Implementierungen

Die Galileo-Konstellation ist derzeit die einzige GNSS-Konstellation, die native NMA für die zivile Nutzung bereitstellt. Die Implementierung wird als OSNMA (Open Service Navigation Message Authentication) bezeichnet und wurde erst kürzlich offiziell in Betrieb genommen. Der Nachteil von OSNMA ist, dass seine Nützlichkeit in einem Multi-GNSS-Empfänger-Kontext begrenzt ist, da nur die Galileo E1-Signale authentifiziert werden können. Dies bedeutet, dass die entsprechenden zivilen GPS-, BeiDou- und GLONASS-Signale ohne die Hilfe von Diensten Dritter nicht authentifiziert werden können.

Eine zukünftige zivile NMA-Implementierung für die GPS-Konstellation (derzeit noch in der Entwicklung) ist als Chimera (**Ch**ips **Me**ssage **R**obust **A**uthentication) bekannt und wird derzeit von keinem kommerziell erhältlichen Empfänger unterstützt.

BeiDou und GLONASS bieten noch keine bekannten NMA-Mechanismen für die zivile Nutzung, obwohl sich dies in Zukunft ändern könnte.

Reale kryptografische Verfahren

Wie oben beschrieben, verwenden NMA-Technologien in der Regel kryptografische Algorithmen, um eine robuste **digitale Signatur** oder einen **Message Authentication Code** (MAC) für eine Navigationsnachricht zu erzeugen. Die Nachricht kann dann durch Verifizierung der Signatur anhand eines entsprechenden Schlüssels authentifiziert werden. Eine solche Signatur kann mit Hilfe asymmetrischer oder symmetrischer Verschlüsselungsmethoden (oder einer Mischung aus beiden) erzeugt werden, wobei jede Methode ihre eigenen Vor- und Nachteile hat. Unabhängig von der Methode ist es wichtig, dass der Schlüssel *vertrauenswürdig* ist, d.h. es darf keine Anzeichen dafür geben, dass ein Angreifer den Schlüssel fälschen oder die Kryptographie fälschen könnte, um eine gültige Signatur zu erzeugen.

Rein symmetrische Verfahren eignen sich üblicherweise nicht für frei empfangbare NMA-Lösungen für zivile

GNSS, da sie auf einen einzigen Schlüssel für die Ver- und Entschlüsselung angewiesen sind (bekannt als „Shared Secret"). Wenn der Schlüssel öffentlich bekannt ist, könnte ein Angreifer einfach die Nachricht, den Schlüssel **und** den MAC fälschen. Dieser Schlüssel müsste daher über einen alternativen Kanal bereitgestellt werden, auf den ein Angreifer keinen Zugriff hat. Da zivile GNSS-Signale per Definition öffentlich zugänglich sind, wäre es unmöglich, einen solchen vertrauenswürdigen Schlüssel ohne Sicherheitsvorkehrungen bereitzustellen, die per Definition mit dem Grundsatz des freien öffentlichen Zugangs unvereinbar sind.

Aus diesem Grund eignen sich rein symmetrische Verfahren besser für Anwendungen auf staatlicher Ebene, wie z. B. das militärische GNSS, bei denen eine genauere Kontrolle der Schlüsselverteilung durch Beschränkung auf einen kleinen Kreis vertrauenswürdiger Benutzer erforderlich ist. Symmetrische Verfahren können auch durch eine zweite Sicherheitsebene geschützt werden, z. B. durch ein System zur Schlüsselrotation oder -erneuerung. Neue Schlüssel können in festen Zeitabständen aus einer Liste gezogen, pseudozufällig auf der Grundlage eines zeitindizierten Seed generiert (so dass der Algorithmus je nach aktuellem Zeitfenster immer denselben Schlüssel generiert) oder ad hoc über sichere Kanäle an vertrauenswürdige Nutzer übermittelt werden.

Asymmetrische Verfahren beruhen dagegen auf „privaten/öffentlichen" Schlüsselpaaren. Ein privater Schlüssel wird auf der Senderseite zur Erzeugung einer digitalen Signatur oder zur Verschlüsselung der gesamten Nachricht verwendet. Der entsprechende öffentliche Schlüssel ist, wie der Name schon sagt, öffentlich zugänglich und kann entweder zur Entschlüsselung von mit dem entsprechenden privaten Schlüssel verschlüsselten Navigationsnachrichten oder zur Authentifizierung von mit dem privaten Schlüssel erzeugten digitalen Signaturen verwendet werden. Er kann jedoch nicht verwendet werden, um gültige digitale Signaturen oder MACs zu erzeugen.

Einer der Nachteile rein asymmetrischer Methoden im Vergleich zur symmetrischen Kryptografie ist, dass Private/Public-Key-Lösungen rechenintensiv sein können: für die Authentifizierung oder Entschlüsselung verschlüsselter Daten sind beträchtliche Hardwareressourcen erforderlich. Da die Bitraten von GNSS-Signalen in der Regel recht niedrig sind, können asymmetrisch erzeugte MACs auch recht lang sein, was zu zusätzlichen Verzögerungen bei der Authentifizierung führt. Dementsprechend eignen sich asymmetrische Verfahren in der NMA besser für die Verschlüsselung als für Hash-basierte Signaturen.

In der Praxis verwenden viele reale NMA-Mechanismen hybride Lösungen oder neuartige Lösungen zur Schlüsselverteilung. Das OSNMA von Galileo beispielsweise nutzt quasi-asymmetrische Methoden, um den Algorithmus zu schützen, der zur Erzeugung der Kette öffentlicher Schlüssel verwendet wird, und ermöglicht es den Empfängern, die öffentlichen Schlüssel zu authentifizieren und die Kette rückwärts zu regenerieren.

16.8.1 Galileo OSNMA

Galileo OSNMA (**O***pen* **S***ervice* **N***avigation* **M***essage* **A***uthentication*) ist ein Mechanismus, bei dem Authentifizierungsdaten in die Galileo Open Service Navigationsnachrichten (I/NAV-Nachrichten) integriert werden, die von einer Teilmenge der Satelliten der Galileo-Konstellation im E1-Band übertragen werden, um kompatiblen Empfängern die Möglichkeit zu geben, die Integrität und Authentizität der empfangenen Nachrichten zu bestätigen.

Das Projekt wurde im Februar 2017 nach einer Entscheidung der Europäischen Kommission über die technischen und betrieblichen Spezifikationen der Galileo-Konstellation für die kommerzielle und industrielle Nutzung initiiert. Darin wurde insbesondere festgelegt, dass:

> *Die Authentifizierungskapazität soll die Sicherheit erhöhen und insbesondere Fälschungs- und Betrugsrisiken verhindern. Daher müssen zusätzliche Merkmale in die Satellitensignale integriert werden, um den Nutzern die Gewissheit zu geben, dass die empfangenen Informationen tatsächlich aus dem System im Rahmen des Galileo-Programms stammen und nicht aus einer unbekannten Quelle. So würde die Authentifizierungskapazität des kommerziellen Dienstes einerseits die Fähigkeit zur Authentifizierung von Daten im Zusammenhang mit der Geolokalisierung umfassen, die in den Signalen des offenen Dienstes enthalten sind und kostenlos angeboten werden, und andererseits im Hinblick auf einen besseren Schutz auch die eindeutige Identifizierung der Signale durch das Lesen verschlüsselter Codes umfassen, die ebenfalls in den Signalen enthalten sind und zu denen der Zugang gebührenpflichtig wäre.*
>
> *Durchführungsbeschluss (EU) 2017/224 der Kommission, vom 8. Februar 2017*

Die erste Testphase für OSNMA begann im November 2020 und endete im Jahr 2023.

Die Rückwärtskompatibilität mit bestehenden Empfängern wird durch die Verwendung des reservierten Feldes „`Reserved 1`“ der E1 I/NAV-Nachricht für die Aufnahme der OSNMA-Daten gewährleistet. Die Beibehaltung der spezifizierten Nachrichtenstruktur in dieser Weise stellt sicher, dass ältere Galileo-Empfänger trotz der Einbeziehung dieser Daten ohne Einschränkungen funktionsfähig bleiben. Jeder konforme ältere Empfänger ohne OSNMA-Unterstützung sollte den 40-Bit-Datenstrom in diesem Feld einfach ignorieren.

OSNMA verwendet einen Chain-of-Trust-Mechanismus, der als **T**imed **E**fficient **S**treamed **L**oss-Tolerant **A**uthentication oder einfach **TESLA** bekannt ist. Diese Vertrauenskette wird erreicht, indem sichergestellt wird, dass die zum Signieren der Authentifizierungscodes für Nachrichten verwendeten Schlüssel auf eine vertrauenswürdige Quelle zurückverfolgt werden können.

Die Wurzel dieser Vertrauenshierarchie besteht aus einer **Merkle Root-Datei**. Die Merkle Root-Datei wird als Referenzpunkt verwendet, um das Vorhandensein eines Wertes im entsprechenden *Merkle-Baum* zu überprüfen. Der Merkle-Baum ist eine Hierarchie von Werten, die die iterative Verkettung und das Hashing von zwei Werten über eine festgelegte Anzahl von Ebenen darstellen, bis alle Wertepaare zu einer gemeinsamen Merkle Root-Datei führen. Die aktuelle OSNMA Merkle Root-Datei ist auf Ihrem Empfängermodul von Meinberg vorinstalliert und wird voraussichtlich nur sehr selten erneuert werden. Falls eine Erneuerung notwendig wird, kann die Datei von der Website des European Union GNSS Service Center erworben werden. Die Merkle Root-Datei spezifiziert auch den **Hashing-Algorithmus** für den Merkle-Baum, der zum Zeitpunkt der Erstellung SHA-256 ist und nur mit Hilfe dieser Datei geändert werden kann. Benachrichtigungen, dass die Merkle Root ausgetauscht werden soll, werden Jahre im Voraus über das Galileo E1-Band ausgegeben und über die Verwaltungsschnittstellen Ihres Meinberg-Systems gemeldet. Die Merkle Root-Datei selbst muss jedoch manuell installiert werden.

TESLA erfordert auch einen vertrauenswürdigen öffentlichen Schlüssel (**Public Key**), der auf dem Empfänger installiert sein muss. Dieser öffentliche Schlüssel wird mit dem Schlüsseltyp und der Schlüssel-ID kombiniert, um einen Wert zu bilden, der zu dem angegebenen Blatt (Knoten) des aktuellen Merkle-Baums passen muss. Ein solcher Public Key ist auf Ihrem GXL-Empfänger von Meinberg vorinstalliert. Weitere Public Keys werden typischerweise über das Galileo E1-Band bezogen und können nur dann als vertrauenswürdig eingestuft werden, wenn sie ebenfalls gegen den lokal gespeicherten Merkle Root verifiziert wurden.

Sobald ein Empfänger mit einer vertrauenswürdigen Merkle Root und einem Public Key ausgestattet ist, kann

er den **Root Key** of the week (KROOT) aus den Galileo E1 I/NAV-Nachrichten erhalten. Beachten Sie, dass es sich hierbei nicht um die oben angegebene Merkle Root-Datei handelt. Der Root Key stellt das Ende einer bestimmten TESLA-Schlüsselkette dar, bei der es sich um eine Sequenz von Schlüsseln handelt, die algorithmisch erzeugt und zum Signieren von „Message Authentication Codes" verwendet werden. Dieser Root Key muss mit einem validen Public Key validiert werden, bevor die TESLA-Kette verwendet werden kann. Alle gültigen Schlüssel innerhalb der aktuellen TESLA-Kette sind über den in den KROOT-Daten mitgeteilten Hash-Algorithmus auf den Root Key rückführbar.

Sobald der Root Key der TESLA-Kette validiert wurde, kann er verwendet werden, um Schlüssel entlang der TESLA-Kette zurückzuverfolgen. Ein Empfänger, der sowohl über den Root Key KROOT einer Kette als auch über jeden nachfolgenden Schlüssel derselben Kette und den erforderlichen Hashing-Algorithmus verfügt, kann jeden Schlüssel zwischen dem Root Key und dem zuletzt empfangenen Schlüssel der Kette rekonstruieren und so Navigationsnachrichten mit MACs authentifizieren, für die die entsprechenden TESLA-Kettenschlüssel bei der Übertragung aus irgendeinem Grund (z. B. durch Interferenzen) verloren gegangen sein könnten.

Die Sicherheit von TESLA wird dadurch ermöglicht, dass es rechnerisch nicht möglich ist, den nächsten Schlüssel in der Kette vorherzusehen. Da die TESLA-Schlüsselkette im Voraus mit Hilfe einer Einwegfunktion mit einem „Seed" generiert wird, der nur dem Betreiber der Galileo-Konstellation bekannt ist, und da der anwendbare TESLA-Schlüssel für einen bestimmten MAC erst in der darauffolgenden Nachricht übertragen wird, verfügt ein Angreifer nicht über die notwendigen Schlüsselinformationen, um einen gültigen MAC zu generieren. Da alle TESLA-Schlüssel auf den validierten Root Key zurückgeführt werden müssen, kann der Angreifer nicht einfach eine Folge von gefälschten Nachrichten erzeugen. Ebenso kann der Root Key nicht gefälscht werden, da dem Angreifer die notwendigen Informationen (Funktion und Seed) für die Generierung des Merkle-Baums fehlen.

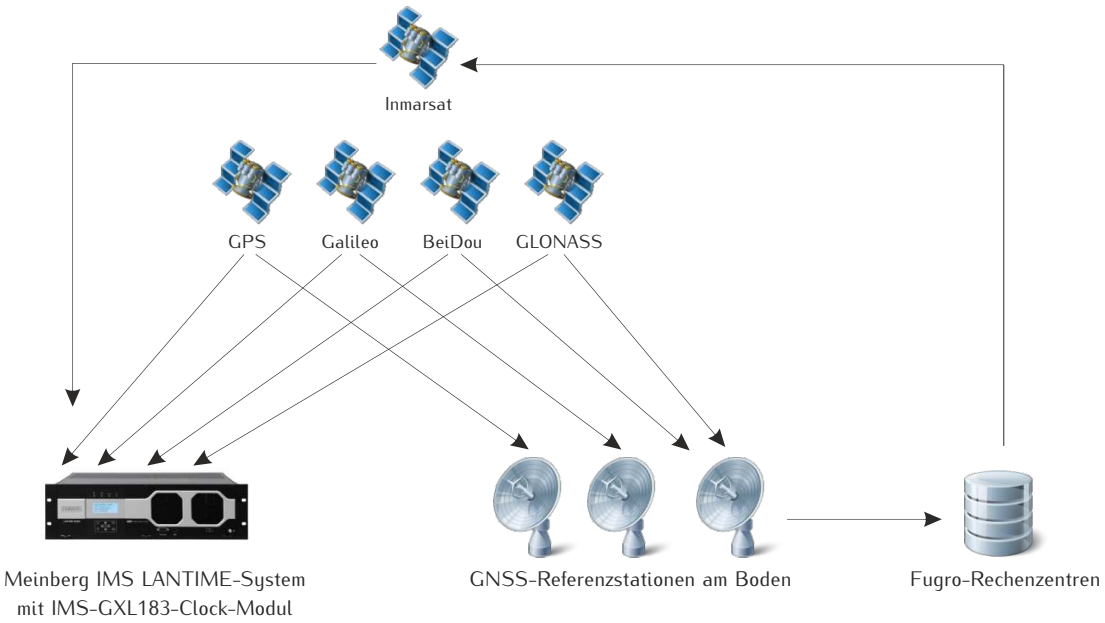
Eine TESLA-Kette besteht in der Regel aus Tausenden von Schlüsseln. Der zu einem bestimmten Zeitpunkt gültige Schlüssel ist von der Wochenzeit abhängig. Damit OSNMA den gültigen Schlüssel korrekt identifizieren kann, muss der Empfänger mit der Galileo-Systemzeit *locker* synchronisiert sein. Die erforderliche Genauigkeit beträgt hier 30 Sekunden, da die einzelnen Sub-Frames der I/NAV-Nachrichten mit einer Dauer von 30 Sekunden übertragen werden, so dass MACs und Schlüssel mit der gleichen Regelmäßigkeit übertragen werden. In der Folge ist jeder Schlüssel in der TESLA-Kette ebenfalls 30 Sekunden lang in Kraft.

Ein Empfänger kann feststellen, wann ein bestimmter Kettenschlüssel hätte übertragen werden müssen, indem er die Anzahl der iterativen Hash-Operationen zählt, die für die Regeneration des Root-Schlüssels erforderlich sind, und kann somit feststellen, ob eine authentifizierte Galileo I/NAV-Nachricht wahrscheinlich einfach eine *zeitverzögerte Reproduktion* einer früheren Nachricht ist.

Eine Uhr, die auf fünf Minuten genau geht, kann jedoch auch den „slow MAC"-Mechanismus nutzen, bei dem der öffentliche Schlüssel der 300 Sekunden zuvor übertragenen MAC erneut übertragen wird. Wenn die lokale Uhr einen Offset von mehr als fünf Minuten aufweist und die Uhr so konfiguriert ist, dass sie sich nur mit authentifizierten Galileo E1-Nachrichten synchronisiert, muss die Uhr manuell eingestellt werden.

Bei Verwendung eines entsprechend konfigurierten Empfängers ermöglicht OSNMA daher die Authentifizierung jeder Navigationsnachricht nicht nur in Bezug auf ihre Herkunft aus der echten Galileo-Konstellation, sondern auch in Bezug auf ihr Timing. Während die verzögerte Art der Schlüsselverteilung verhindert, dass subtile Manipulationen schnell aufgedeckt werden, schränkt die Signalüberwachungsfunktion auf Hardware-Ebene des Empfängers in Kombination mit Meinbergs verschiedenen anderen Anti-Spoofing-Funktionen wie „Trusted Source" die Möglichkeiten von Angreifern zur Fälschung von Zeitdaten in GNSS-Nachrichten erheblich ein.

16.8.2 Fugro AtomiChron®



Zwar sind native GNSS-NMA-Lösungen wie Galileo OSNMA und der GPS-Chimera-Mechanismus (letzterer befindet sich zum Zeitpunkt der Abfassung dieses Artikels noch in der Entwicklung) für die Sicherheit des zivilen GNSS-Empfangs in der Zukunft unerlässlich, doch weisen sie eine Reihe von Mängeln auf. Im Falle von OSNMA werden nur Galileo E1 OS-Signale authentifiziert. Signale auf den Bändern E5b oder E6 bleiben manipulierbar. Im Falle von Chimera befindet sich der Mechanismus noch in der Entwicklung, und ein Zeitrahmen für die Inbetriebnahme ist noch nicht absehbar. BeiDou und GLONASS bieten keine bekannte NMA-Lösung für die zivile Nutzung. Für Multi-GNSS-Empfänger sind diese nativen NMA-Lösungen daher nur von begrenztem Nutzen, da die ungeschützten Signale mögliche Angriffsvektoren darstellen.

AtomiChron® ist ein NMA-Abonnementdienst eines Drittanbieters, der vom niederländischen Geodatenspezialisten Fugro N.V. betrieben wird und diese Unzulänglichkeiten beseitigt. Er basiert auf Authentifizierungsdaten, die von den zahlreichen Referenzstationen von Fugro auf der ganzen Welt erzeugt werden, von denen jede GNSS-Daten von allen vier großen Satellitenkonstellationen (GPS, Galileo, BeiDou, GLONASS) sammelt und analysiert. Die Daten dieser Referenzstationen werden dann in den Netzwerkzentren von Fugro zusammengestellt und verglichen, die wiederum ihre Ergebnisse (und andere operative Daten) an die Inmarsat-Satellitenkonstellation übermitteln, um sie an einen AtomiChron®-fähigen Empfänger mit einem gültigen Abonnement weiterzuleiten.

Dies macht AtomiChron® zur idealen NMA-Lösung für Multi-GNSS-Produkte wie das GXL-Empfängermodul von Meinberg, da es den GNSS-Verkehr von jedem Signaltyp auf jedem von der Uhr unterstützten GNSS-Band authentifiziert.

Die globale Verteilung dieser Referenzstationen macht es für einen Angreifer fast unmöglich, die Referenzdaten an ihrer Quelle zu kompromittieren, da gefälschte Daten von einer oder zwei Referenzstationen leicht als Ausreißer erkannt werden.

Selbstverständlich sind die Übertragungen zu und von den Inmarsat-Satelliten verschlüsselt und kryptographisch signiert, so dass sie nur von einem Empfänger mit einer gültigen AtomiChron®-Lizenz entschlüsselt und authentifiziert werden können. Dadurch wird sichergestellt, dass eingehende AtomiChron®-Daten eindeutig authentifiziert werden können und das Risiko, dass das AtomiChron®-Signal selbst gefälscht wird, ausgeschlossen ist.

Der Zugang zum AtomiChron®-Dienst erfordert ein kostenpflichtiges Abonnement. Bei einem Abonnement für ein IMS-GXL-Empfängermodul wird dieses Abonnement direkt mit Meinberg abgeschlossen.

16.9 mbgARC: Antennen-Empfängerkommunikation

mbgARC ist das bidirektionale Kommunikationsframework von Meinberg für Antennen, das eine Empfängerinfrastruktur ermöglicht, in der die Antenne nicht mehr nur eine passive Komponente ist.

Mit **mbgARC** kommuniziert ein Meinberg-Empfänger aktiv mit einer angeschlossenen Antenne, um Betriebsdaten auszutauschen, die es der Uhr ermöglicht, bestimmte Betriebsparameter anzupassen. Beispielsweise kann ein Empfänger die lokale Betriebstemperatur der Antenne oder die aktuelle Betriebsspannung entlang des Kabelwegs zwischen der Antenne und dem Empfänger messen und die Ausgangsverstärkung der Antenne selbst steuern.

Die Kommunikation zwischen dem Empfänger und der Antenne erfolgt ausschließlich über das Koaxialkabel, das die beiden Komponenten verbindet. Der mbgARC-Datenstrom wird über das Referenzsignal gelegt und stört die Signalübertragung in keiner Weise.

Produktunterstützung

mbgARC wird von allen Meinberg Kybernion GNSS-Produkten (GPSANTv2-Antenne, GNMANTv2-Antenne, INA-20 Inline-Verstärker, INA-30 Inline-Verstärker) sowie den folgenden Zeitservern und Referenzuhren unterstützt:

- IMS-GXL183 Referenzempfänger-Module
- IMS-GNS183 Referenzempfänger-Module
- IMS-GNS183-UC Referenzempfänger-Module
- IMS-GPS183 Referenzempfänger-Module
- LANTIME M150 Zeitserver mit GNS, GNS-UC oder GPS-Referenzempfänger (1)
- LANTIME M250 Zeitserver mit GNS, GNS-UC oder GPS-Referenzempfänger (1)
- LANTIME M320 Zeitserver mit GNS, GNS-UC oder GPS-Referenzempfänger (1)
- LANTIME M450 Zeitserver mit GNS, GNS-UC oder GPS-Referenzempfänger (1)
- GNS183/DAHS Referenzempfänger
- GNS183/DHS Referenzempfänger
- GPS183/DAHS Referenzempfänger
- GPS183/DHS Referenzempfänger
- microSync Zeitserver (2)

(1) Nur LANTIME M-Serie-Modelle mit GNS183/GNS183-UC/GPS183-Referenzuhren, Herstellungsdatum Oktober 2023 oder später.

(2) Nur Modelle mit GNS183/GNS183-UC/GPS183-Referenzuhren, Herstellungsdatum März 2024 oder später.

16.10 Eingesetzte Software von Drittherstellern

Der LANTIME Netzwerk Zeitserver führt eine Reihe von Software aus, die auf der Arbeit von OpenSource Projekten basieren. Sehr viele Personen haben bei der Entwicklung und Realisierung dieser Software mitgearbeitet. Wir bedanken uns ausdrücklich für diese Arbeit.

Die eingesetzte OpenSource-Software unterliegt ihren eigenen Lizenzbedingungen, die wir im Folgenden aufführen. Sollte der Einsatz einer eingesetzten Software deren Lizenzbestimmungen verletzen, werden wir nach Mitteilung unverzüglich dafür sorgen, dass diese Lizenzbestimmungen wieder eingehalten werden.

Ist für eins der eingesetzten Software-Produkte vorgeschrieben, dass der zugrundeliegende Quellcode von der Firma Meinberg zur Verfügung gestellt werden muss, senden wir Ihnen auf Anfrage entweder einen Datenträger oder eine E-Mail zu oder wir stellen Ihnen einen Link zur Verfügungen, unter dem Sie die aktuellste Version des Quellcodes im Internet beziehen können. Bitte beachten Sie, dass wir bei Zusendung eines Datenträgers die dabei anfallenden Kosten in Rechnung stellen müssen.

16.10.1 Betriebssystem GNU/Linux

Die Weitergabe des GNU/Linux Betriebssystems unterliegt der GNU General Public License, die wir weiter unten abdrucken.

Mehr zu GNU/Linux finden Sie auf der GNU-Homepage
www.gnu.org

sowie auf der Homepage von GNU/Linux
www.linux.org

16.10.2 Samba

Die Samba Software Suite ist eine Gruppe von Programmen, die das Server Message Block (abgekürzt SMB) Protokoll für UNIX Systeme implementiert. Durch den Einsatz von Samba ist das Senden von Windows Popup Meldungen sowie die Abfrage der Zeit durch Clients mithilfe des NET TIME Befehls möglich.
Die Weitergabe von Samba unterliegt – wie bei GNU/Linux – der GNU General Public License, siehe Abdruck weiter unten.

Die Website des Samba – Projekts (bzw. einen Mirror) finden Sie unter:
www.samba.org

16.10.3 Network Time Protocol Version 4 (NTP)

Das von David L. Mills geleitete NTP-Projekt ist im Internet unter www.ntp.org erreichbar, dort finden sich eine Fülle von Informationen und Anleitungen zum Einsatz dieses Standard-Softwarepakets. Die Weitergabe und der Einsatz der NTP-Software ist erlaubt, solange der folgende Hinweis in der Dokumentation vorhanden ist:

16.10.4 lighttpd

Für die webbasierende Konfigurationsoberfläche (sowohl HTTP als auch HTTPS) setzen wir die Software lighttpd ein. Lighttpd ist ein freier Webserver, der vom deutschen Entwickler Jan Kneschke stammt und alle wesentlichen
Funktionen eines Webservers beinhalted.

Die Verwendung dieser Software ist durch folgende Lizenz abgedeckt:

16.10.5 GNU General Public License (GPL)

Version 2, June 1991 - Copyright (C) 1989, 1991

Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING,
DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The „Program", below, refers to any such program or work, and a „work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term „modification".) Each licensee is addressed as „you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in

either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and „any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions

are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM „AS IS“ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

16.11 Literaturverzeichnis

[**Mills88**] Mills, D. L., „Network Time Protocol (Version 1) - specification and implementation“, DARPA Networking Group Report RFC-1059, University of Delaware, July 1988

[**Mills89**] Mills, D. L., „Network Time Protocol (Version 2) - specification and implementation“, DARPA Networking Group Report RFC-1119, University of Delaware, September 1989

[**Mills90**] Mills, D. L., „Network Time Protocol (Version 3) - specification, implementation and analysis“, Electrical Engineering Department Report 90-6-1, University of Delaware, June 1989

Kardel, Frank, „Gesetzliche Zeit in Rechnernetzen“, Funkuhren, Zeitsignale und Normalfrequenzen, Hrsg. W. Hilberg, Verlag Sprache und Technik, Groß-Bieberau 1993

Kardel, Frank, „Verteilte Zeiten“, ix Multiuser-Multitasking-Magazin, Heft 2/93, Verlag Heinz Heise, Hannover 1993