

# **TSN-Switch**

## **Anwenderhandbuch**

Version: **1.27 (Juli 2023)**  
Bestellnr.: **TSN-Switch**

**Originalbetriebsanleitung**

## **Impressum**

B&R Industrial Automation GmbH

B&R Straße 1

5142 Eggelsberg

Österreich

Telefon: +43 7748 6586-0

Fax: +43 7748 6586-26

[office@br-automation.com](mailto:office@br-automation.com)

## **Disclaimer**

Alle Angaben entsprechen dem aktuellen Stand zum Zeitpunkt der Erstellung dieses Dokuments. Jederzeitige inhaltliche Änderungen dieses Dokuments ohne Ankündigung bleiben vorbehalten. B&R Industrial Automation GmbH haftet insbesondere für technische oder redaktionelle Fehler in diesem Dokument unbegrenzt nur (i) bei grobem Verschulden oder (ii) für schuldhaft zugefügte Personenschäden. Darüber hinaus ist die Haftung ausgeschlossen, soweit dies gesetzlich zulässig ist. Eine Haftung in den Fällen, in denen das Gesetz zwingend eine unbeschränkte Haftung vorsieht (wie z. B. die Produkthaftung), bleibt unberührt. Die Haftung für mittelbare Schäden, Folgeschäden, Betriebsunterbrechung, entgangenen Gewinn, Verlust von Informationen und Daten ist ausgeschlossen, insbesondere für Schäden, die direkt oder indirekt auf Lieferung, Leistung und Nutzung dieses Materials zurückzuführen sind.

B&R Industrial Automation GmbH weist darauf hin, dass die in diesem Dokument verwendeten Hard- und Softwarebezeichnungen und Markennamen der jeweiligen Firmen dem allgemeinen warenzeichen-, marken- oder patentrechtlichen Schutz unterliegen.

Hard- und Software von Drittanbietern, auf die in diesem Dokument verwiesen wird, unterliegt ausschließlich den jeweiligen Nutzungsbedingungen dieser Drittanbieter. B&R Industrial Automation GmbH übernimmt hierfür keine Haftung. Allfällige Empfehlungen von B&R Industrial Automation GmbH sind nicht Vertragsinhalt, sondern lediglich unverbindliche Hinweise, ohne dass dafür eine Haftung übernommen wird. Beim Einsatz der Hard- und Software von Drittanbietern sind ergänzend die relevanten Anwenderdokumentationen dieser Drittanbieter heranzuziehen und insbesondere die dort enthaltenen Sicherheitshinweise und technischen Spezifikationen zu beachten. Die Kompatibilität der in diesem Dokument dargestellten Produkte von B&R Industrial Automation GmbH mit Hard- und Software von Drittanbietern ist nicht Vertragsinhalt, es sei denn, dies wurde im Einzelfall gesondert vereinbart; insoweit ist die Gewährleistung für eine solche Kompatibilität jedenfalls ausgeschlossen und hat der Kunde die Kompatibilität in eigener Verantwortung vorab zu prüfen.

<b>1 Sicherheitshinweise.....</b>	<b>6</b>
1.1 Bestimmungsgemäße Verwendung.....	7
1.2 Schutz vor elektrostatischen Entladungen.....	7
1.2.1 Verpackung.....	7
1.2.2 Vorschriften für die ESD-gerechte Handhabung.....	8
1.3 Transport und Lagerung.....	8
1.4 Montagerichtlinien.....	8
1.5 Betrieb.....	9
1.5.1 Schutz gegen Berühren elektrischer Teile.....	9
1.6 Gestaltung von Hinweisen.....	9
1.7 Reinigung des Geräts.....	9
1.8 Umweltgerechte Entsorgung.....	9
1.8.1 Werkstofftrennung.....	9
<b>2 Einleitung.....</b>	<b>10</b>
2.1 Anwendungsfälle.....	11
2.1.1 Gleichzeitiges Steuern von Ereignissen.....	11
2.1.2 Übertragungsgarantie am IT-Netzwerk.....	12
2.1.3 Big Data.....	13
2.2 Netzwerktopologien.....	14
<b>3 Technische Beschreibung.....</b>	<b>15</b>
3.1 Bestelldaten.....	15
3.2 Technische Daten.....	16
3.3 Bedien- und Anschlusselemente.....	17
3.3.1 Status-LED.....	17
3.3.2 Ethernet Anschluss.....	18
3.3.3 Resettaster.....	18
3.3.4 24 VDC Versorgung.....	19
3.4 Versorgung des TSN-Switchs.....	19
3.5 Einstellen der IP-Adresse.....	19
3.6 Abmessungen.....	20
3.7 Montage.....	21
3.7.1 Ummontieren der Hutschienehalterung.....	22
3.7.2 Einbaulagen und Derating.....	23
3.8 Blitz- und Überspannungsschutz.....	24
3.8.1 UL/CSA.....	24
<b>4 Erste Schritte.....</b>	<b>25</b>
4.1 Vorbereitung.....	25
4.2 Verbindungsaufbau.....	25
4.2.1 Verbindungsaufbau per Hostname.....	26
4.2.2 Verbindungsaufbau per IP-Adresse.....	28
4.3 Mit OPC UA Client verbinden.....	29
4.4 Anlegen des initialen Benutzers.....	30
4.5 Allgemeine Netzwerkeinstellungen über OPC UA.....	33
4.6 Zeitsynchronisation.....	34
4.7 Neustart und Reset.....	35
4.8 Aktualisierung des Self-Signed Zertifikats.....	35
4.9 TSN-Netzwerkconfiguration über NETCONF.....	36
4.9.1 Benutzerrechte.....	36
4.9.2 Konfigurationswerkzeuge.....	36
<b>5 Firmwareupdate über OPC UA.....</b>	<b>37</b>
5.1 Update durchführen.....	37

<b>6 Features / Funktionalität</b>	<b>40</b>
6.1 Verwendete Namespaces	40
6.2 Geräteinformation	41
6.3 Zeitsynchronisation und Zeitdomänen	42
6.4 Time Sensitive Networking (TSN)	42
6.4.1 Frame-Forwarding	42
6.4.2 Zeitgesteuerte Kommunikation (Scheduled Traffic)	43
6.4.3 Credit-based Shaping	43
6.4.4 Frame Preemption	43
6.5 Netzwerkmanagementprotokolle	44
6.5.1 Multiple Spanning Tree Protocol (MSTP)	44
6.5.2 Link Layer Discovery Protocol (LLDP)	44
6.6 Geräteeigenschaften	44
6.7 Port-Mirroring und Port-Isolation	45
<b>7 Konfiguration</b>	<b>46</b>
7.1 Konfiguration über OPC UA	46
7.1.1 Methoden	46
7.1.2 Allgemeine Netzwerkkonfiguration	47
7.1.3 Bridge-Konfiguration	47
7.1.4 Multiple Spanning Tree Protokoll	48
7.1.5 Port-Mirroring und Port-Isolation	48
7.1.6 Zeitsynchronisation	49
7.2 Integration im IT-Netzwerk	50
7.3 Konfiguration über NETCONF	51
7.3.1 Konfiguration mittels Automation Studio	51
7.3.2 Konfiguration mit TTTech Slate XNS	51
<b>8 Status</b>	<b>52</b>
8.1 Port-Status	52
8.2 Zeitsynchronisation	53
8.3 Netzwerk	53
<b>9 Cyber-Security</b>	<b>54</b>
9.1 Grundbegriffe und Grundlagen	54
9.1.1 Verschlüsselung	54
9.1.2 Integrität	55
9.1.3 Symmetrische und asymmetrische Schlüssel	55
9.1.4 Asymmetrischer Schlüsselaustausch	56
9.1.5 Vertrauenshierarchie und Autorität	56
9.2 Benutzerzugriffe	58
9.3 Schlüsselverwaltung für NETCONF	60
9.4 Zertifikatsmanagement	61
9.4.1 Zertifikatsanforderung erzeugen	61
9.4.2 Zertifikat mittels UpdateCertificate aktualisieren	61
<b>10 Diagnose</b>	<b>64</b>
10.1 Adressierung	65
10.2 Datenübertragung	66
10.3 Zeitsynchronisierung	67
10.4 Cyber-Security	68
<b>11 Lizenzen</b>	<b>69</b>
<b>12 Anhang</b>	<b>70</b>
12.1 OPC UA Informationsmodell	70

12.1.1 Benutzerverwaltung.....	70
12.1.2 Firmwareupdate.....	73
<b>13 OTB2103.9110.....</b>	<b>75</b>
13.1 Allgemeines.....	75
13.2 Bestelldaten.....	75
13.3 Technische Daten.....	75
13.4 Prüfzugang.....	76

# 1 Sicherheitshinweise

---

Speicherprogrammierbare Steuerungen, Bedien- und Beobachtungsgeräte (wie z. B. Industrie PCs, Power Panel, Mobile Panel usw.) wie auch die unterbrechungsfreie Stromversorgung sind von B&R für den gewöhnlichen Einsatz bzw. Einsatz mit erhöhten Sicherheitsanforderungen (Safety Technology) in der Industrie entworfen, entwickelt und hergestellt worden. Diese wurden nicht entworfen, entwickelt und hergestellt für einen Gebrauch, der verhängnisvolle Risiken oder Gefahren birgt, die ohne Sicherstellung außergewöhnlich hoher Sicherheitsmaßnahmen zu Tod, Verletzung, schweren physischen Beeinträchtigungen oder anderweitigem Verlust führen können. Solche stellen insbesondere die Verwendung bei der Überwachung von Kernreaktionen in Kernkraftwerken, von Flugleitsystemen, bei der Flugsicherung, bei der Steuerung von Massentransportmitteln, bei medizinischen Lebenserhaltungssystemen und Steuerung von Waffensystemen dar.

Sowohl beim Einsatz von Speicherprogrammierbaren Steuerungen als auch beim Einsatz von Bedien- und Beobachtungsgeräten als Steuerungssystem in Verbindung mit einer Soft-SPS (z. B. B&R Automation Runtime oder vergleichbare Produkte) bzw. einer Steckplatz-SPS (z. B. B&R LS251 oder vergleichbare Produkte) sind die für die industriellen Steuerungen geltenden Sicherheitsmaßnahmen (Absicherung durch Schutzeinrichtungen wie z. B. Not-Halt etc.) gemäß den jeweils zutreffenden nationalen bzw. internationalen Vorschriften zu beachten. Dies gilt auch für alle weiteren angeschlossenen Geräte wie z. B. Antriebe.

Alle Arbeiten wie Installation, Inbetriebnahme und Service dürfen nur durch qualifiziertes Fachpersonal ausgeführt werden. Qualifiziertes Fachpersonal sind Personen, die mit Transport, Aufstellung, Montage, Inbetriebnahme und Betrieb des Produktes vertraut sind und über die ihrer Tätigkeit entsprechenden Qualifikationen verfügen (z. B. IEC 60364-1). Nationale Unfallverhütungsvorschriften sind zu beachten.

Die Sicherheitshinweise, die Angaben zu den Anschlussbedingungen (Typenschild und Dokumentation) und die in den technischen Daten angegebenen Grenzwerte sind vor der Installation und Inbetriebnahme sorgfältig durchzulesen und unbedingt einzuhalten.

Die Verwendung der Produkte ist auf folgende Personen begrenzt:

- **Qualifiziertes Personal\***, das mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und Vorschriften vertraut ist.
- **Qualifiziertes Personal\***, das Sicherheitseinrichtungen für Maschinen und Anlagen plant, entwickelt, einbaut und in Betrieb nimmt.

\* **Qualifiziertes Personal** im Sinne der sicherheitstechnischen Hinweise dieses Handbuches sind Personen, die aufgrund ihrer Ausbildung, Erfahrung und Unterweisung sowie ihrer Kenntnisse über einschlägige Normen, Bestimmungen, Unfallverhütungsvorschriften und Betriebsverhältnisse berechtigt sind, die jeweils erforderlichen Tätigkeiten auszuführen und dabei mögliche Gefahren erkennen und vermeiden können. In diesem Sinne werden auch ausreichende Sprachkenntnisse für das Verständnis dieses Handbuches vorausgesetzt.

## 1.1 Bestimmungsgemäße Verwendung

Es sind in jedem Fall die einschlägigen nationalen und internationalen Fachnormen, Vorschriften und Sicherheitsmaßnahmen zu beachten und einzuhalten!

Die in diesem Handbuch beschriebenen B&R Produkte sind für den Einsatz in der Industrie und in Industrieanwendungen bestimmt.

Die bestimmungsgemäße Verwendung umfasst das Steuern, Bedienen, Beobachten, Antreiben und Visualisieren im Rahmen von Automatisierungsprozessen in Maschinen und Anlagen.

B&R Produkte dürfen nur im Originalzustand verwendet werden. Modifikationen und Erweiterungen sind nur dann zulässig, wenn sie in diesem Handbuch beschrieben sind.

B&R schließt die Haftung für Schäden jeglicher Art aus, die bei einem Einsatz der B&R Produkte außerhalb der bestimmungsgemäßen Verwendung entstehen.

B&R Produkte wurden nicht entworfen, entwickelt und hergestellt für einen Gebrauch, der verhängnisvolle Risiken oder Gefahren birgt, die ohne Sicherstellung außergewöhnlich hoher Sicherheitsmaßnahmen zu Tod, Verletzung, schweren physischen Beeinträchtigungen oder anderweitigem Verlust führen können.

B&R Produkte sind explizit nicht zum Gebrauch in folgenden Anwendungen bestimmt:

- Überwachung und Steuerung von thermonuklearen Prozessen
- Steuerung von Waffensystemen
- Flug- und Verkehrsleitsysteme für Personen- und Gütertransport
- Gesundheitsüberwachungs- und Lebenserhaltungssysteme

### Information:

Die in diesem Handbuch beschriebenen B&R Produkte sind als "offenes Betriebsmittel" (IEC 61010-1) und als "open type equipment" (UL) konzipiert und somit nur für den Einbau im geschlossenen Schaltschrank bestimmt.

## 1.2 Schutz vor elektrostatischen Entladungen

Elektrische Baugruppen, die durch elektrostatische Entladungen (**ElectroStatic Discharge**) beschädigt werden können, sind entsprechend zu handhaben.

### 1.2.1 Verpackung

- Elektrische Baugruppen mit Gehäuse  
... benötigen keine spezielle ESD-Verpackung, sie sind aber korrekt zu handhaben (siehe "[Elektrische Baugruppen mit Gehäuse](#)" auf Seite 8).
- Elektrische Baugruppen ohne Gehäuse  
... sind durch ESD-taugliche Verpackungen geschützt.

## 1.2.2 Vorschriften für die ESD-gerechte Handhabung

### Elektrische Baugruppen mit Gehäuse

- Kontakte von Steckverbindern auf dem Gerät nicht berühren (Bus-Datenkontakte)
- Kontakte von Steckverbindern von angeschlossenen Kabeln nicht berühren
- Kontaktzungen von Leiterplatten nicht berühren

### Elektrische Baugruppen ohne Gehäuse

Zusätzlich zu "Elektrische Baugruppen mit Gehäuse" gilt:

- Alle Personen, die elektrische Baugruppen handhaben, sowie Geräte, in die elektrische Baugruppen eingebaut werden, müssen geerdet sein.
- Baugruppen dürfen nur an den Schmalseiten oder an der Frontplatte berührt werden.
- Baugruppen immer auf geeigneten Unterlagen (ESD-Verpackung, leitfähiger Schaumstoff etc.) ablegen.

#### **Information:**

**Metallische Oberflächen sind als Ablageflächen nicht geeignet.**

- Elektrostatische Entladungen auf die Baugruppen (z. B. durch aufgeladene Kunststoffe) sind zu vermeiden.
- Zu Monitoren oder Fernsehgeräten muss ein Mindestabstand von 10 cm eingehalten werden.
- Messgeräte und -vorrichtungen müssen geerdet werden.
- Messspitzen von potenzialfreien Messgeräten sind vor der Messung kurzzeitig an geeigneten geerdeten Oberflächen zu entladen.

### Einzelbauteile

- ESD-Schutzmaßnahmen für Einzelbauteile sind bei B&R durchgängig verwirklicht (leitfähige Fußböden, Schuhe, Armbänder etc.).
- Die erhöhten ESD-Schutzmaßnahmen für Einzelbauteile sind für das Handling von B&R Produkten bei unseren Kunden nicht erforderlich.

## 1.3 Transport und Lagerung

Bei Transport und Lagerung müssen die Geräte vor unzulässigen Beanspruchungen (mechanische Belastung, Temperatur, Feuchtigkeit, aggressive Atmosphäre) geschützt werden.

Die Geräte enthalten elektrostatisch gefährdete Bauelemente, die durch unsachgemäße Behandlung beschädigt werden können. Es sind daher beim Ein- bzw. Ausbau der Geräte die erforderlichen Schutzmaßnahmen gegen elektrostatische Entladungen zu treffen (siehe "[Schutz vor elektrostatischen Entladungen](#)" auf Seite 7).

## 1.4 Montagerichtlinien

- Die Montage muss entsprechend der Dokumentation mit geeigneten Einrichtungen und Werkzeugen erfolgen.
- Die Montage der Geräte darf nur in spannungsfreiem Zustand und durch qualifiziertes Fachpersonal erfolgen.
- Die allgemeinen Sicherheitsbestimmungen sowie die national geltenden Unfallverhütungsvorschriften sind zu beachten.
- Die elektrische Installation ist nach den einschlägigen Vorschriften durchzuführen (z. B. Leiterquerschnitt, Absicherung, Schutzleiteranbindung). Falls das Gerät auf eine vom Hersteller unvorgesehene Weise verwendet wird, kann der durch das Gerät gebotene Schutz beeinträchtigt werden.
- Treffen Sie die erforderlichen Schutzmaßnahmen gegen elektrostatische Entladung (siehe "[Schutz vor elektrostatischen Entladungen](#)" auf Seite 7).

## 1.5 Betrieb

### 1.5.1 Schutz gegen Berühren elektrischer Teile

#### Gefahr!

Zum Betrieb der speicherprogrammierbaren Steuerungen sowie der Bedien- und Beobachtungsgeräte und der unterbrechungsfreien Stromversorgung ist es notwendig, dass bestimmte Teile unter gefährlichen Spannungen stehen. Werden solche Teile berührt, kann es zu einem lebensgefährlichen elektrischen Schlag kommen. Es besteht die Gefahr von Tod oder schweren gesundheitlichen oder materiellen Schäden.

Vor dem Einschalten der speicherprogrammierbaren Steuerungen, der Bedien- und Beobachtungsgeräte sowie der Unterbrechungsfreien Stromversorgung muss sichergestellt sein, dass das Gehäuse ordnungsgemäß mit Erdpotenzial (PE-Schiene) verbunden ist. Die Erdverbindungen müssen auch angebracht werden, wenn das Bedien- und Beobachtungsgerät sowie die unterbrechungsfreie Stromversorgung nur für Versuchszwecke angeschlossen oder nur kurzzeitig betrieben wird!

Vor dem Einschalten sind spannungsführende Teile sicher abzudecken. Während des Betriebs müssen alle Abdeckungen geschlossen gehalten werden.

## 1.6 Gestaltung von Hinweisen

### Sicherheitshinweise

Enthalten **ausschließlich** Informationen, die vor gefährlichen Funktionen oder Situationen warnen.

Signalwort	Beschreibung
<b>Gefahr!</b>	Bei Missachtung der Sicherheitsvorschriften und -hinweise werden Tod, schwere Verletzungen oder große Sachschäden eintreten.
<b>Warnung!</b>	Bei Missachtung der Sicherheitsvorschriften und -hinweise können Tod, schwere Verletzungen oder große Sachschäden eintreten.
<b>Vorsicht!</b>	Bei Missachtung der Sicherheitsvorschriften und -hinweise können leichte Verletzungen oder Sachschäden eintreten.
<b>Achtung!</b>	Bei Missachtung der Sicherheitsvorschriften und -hinweise können Sachschäden eintreten.

### Allgemeine Hinweise

Enthalten **nützliche** Informationen für Anwender und Angaben zur Vermeidung von Fehlfunktionen.

Signalwort	Beschreibung
<b>Information:</b>	Nützliche Informationen, Anwendungstipps und Angaben zur Vermeidung von Fehlfunktionen.

## 1.7 Reinigung des Geräts

#### Information:

Die Reinigung im Bereich des Aufklebers ist nur mit einem trockenen Tuch oder mit Wasser zulässig.

## 1.8 Umweltgerechte Entsorgung

Alle Steuerungskomponenten von B&R sind so konstruiert, dass sie die Umwelt so gering wie möglich belasten.

### 1.8.1 Werkstofftrennung

Damit die Geräte einem umweltgerechten Recycling-Prozess zugeführt werden können, ist es notwendig, die verschiedenen Werkstoffe voneinander zu trennen.

Bestandteil	Entsorgung
X20 Module, Kabel	Elektronik-Recycling
Karton/Papier-Verpackung	Papier-/Kartonage-Recycling

Tabelle 1: Umweltgerechte Werkstofftrennung

Die Entsorgung muss gemäß den jeweils gültigen gesetzlichen Regelungen erfolgen.

## 2 Einleitung

---

Mit dem TSN-Switch lassen sich modulare Maschinenkonzepte und Ethernet TSN-Netzwerke einfach umsetzen, zum Beispiel in Verbindung mit der herstellerunabhängigen Kommunikationslösung OPC UA over TSN. Der TSN-Switch ermöglicht Stern-, Baum-, Ring- oder vermaschte Topologien in OPC-UA-over-TSN-Netzwerken. Er ermöglicht Netzwerk-Zykluszeiten von weniger als 50  $\mu$ s und fügt sich hinsichtlich Design und Formfaktor in das B&R-Portfolio ein.

Ethernet-Netzwerkteilnehmer mit oder ohne TSN-Funktionalität können mit dem TSN-Switch gleichermaßen problemlos in das Netzwerk eingebunden werden. Der TSN-Switch funktioniert in allen Ethernet und Ethernet-TSN-Netzwerken und unterstützt dabei folgende TSN-Standards:

- IEEE 802.1Q
- IEEE 802.1AS-2020 - Precision Time Protocol (PTP)
- IEEE 802.1Qbv
- IEEE 802.1Qav
- IEEE 802.1Qbu

### Information:

Für genauere Informationen zu den verwendeten TSN-Standards siehe [OPC UA over TSN Technologiebeschreibung](#).

## 2.1 Anwendungsfälle

Die hier beschriebenen Szenarien zeigen, in welchen Anwendungsgebieten OPC UA over TSN bzw. Teile dieser Technologie eingesetzt werden können.

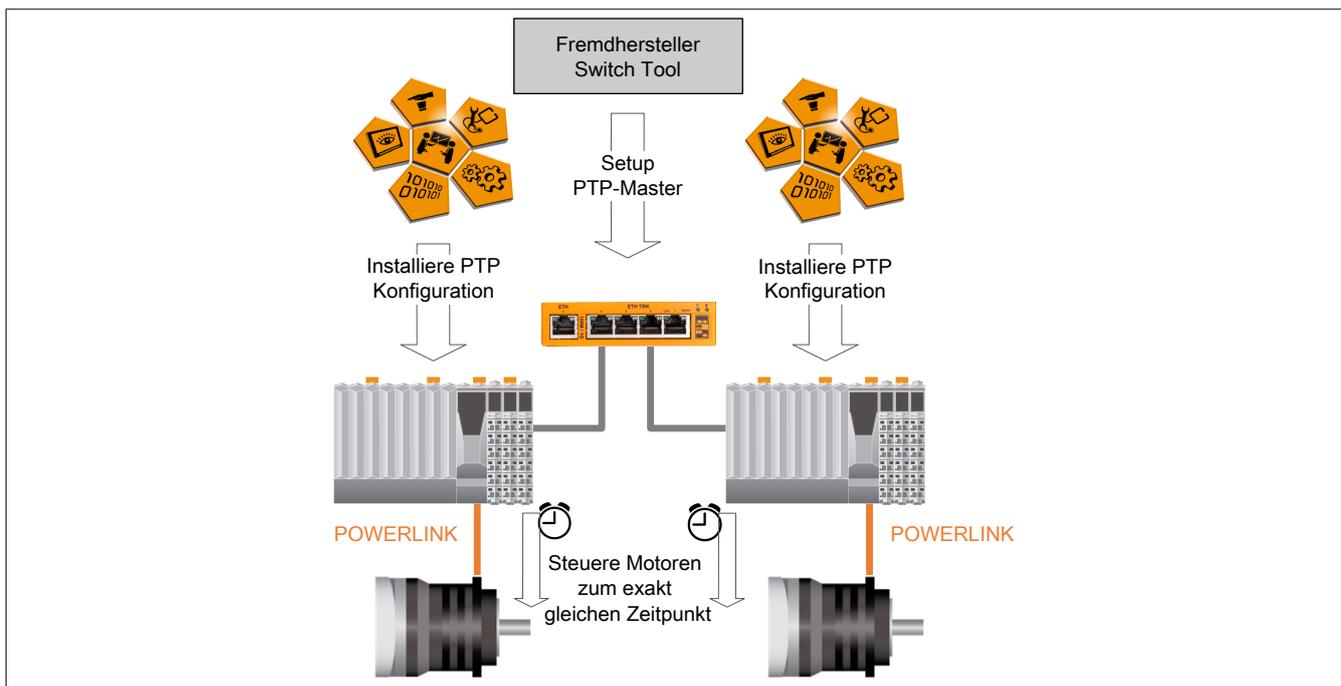
### 2.1.1 Gleichzeitiges Steuern von Ereignissen

IEEE 802.1AS (gPTP) ermöglicht eine sehr genaue Zeitsynchronisierung. B&R Steuerungen sind dadurch in der Lage den Systemtick auf PTP im Bereich weniger Mikrosekunden zu synchronisieren. Wenn auf den zu synchronisierenden B&R Steuerungen die gleiche Zykluszeit für die Taskklasse1 gewählt und diese Zykluszeit gleich dem Systemtick ist, dann sind auch die Zyklen der Taskklasse1 auf wenige Mikrosekunden synchron.

Mit der synchronisierten Taskklasse ist es möglich, auf verschiedenen B&R-Steuerungen zeitgleich ein Ereignis (z. B. Ansteuern eines Motors) auszulösen. Die Steuerungen können sich z. B. über PubSub austauschen, welche Ereignisse stattfinden sollen und wann sie stattfinden sollen. Auf den Steuerungen kann man während der Abarbeitung der Taskklasse1 die aktuelle PTP-Zeit auslesen und somit können beide Steuerungen zum exakt gleichen Zeitpunkt das geplante Ereignis durchführen.

Dadurch lassen sich auf unterschiedlichen Steuerungen zeitgleich Ereignisse ausführen, aber noch nicht in Echtzeit regeln. Dafür wäre zusätzlich eine deterministische Kommunikation zwischen den Steuerungen nötig, welche zurzeit noch nicht unterstützt wird. Aktuell kann man mit PubSub zwar – analog zu Modbus TCP, PROFINET oder Ethernet/IP – eine rasche und auf unausgelasteten Steuerungen mit hoher Wahrscheinlichkeit zuverlässige Kommunikation erreichen, aber harte Echtzeit kann nicht garantiert werden.

Auf den Steuerungen muss PTP aktiviert und als Zeitgeber für den Systemtick konfiguriert werden (Automation Help Abschnitt "PTP Konfiguration"). Zusätzlich muss ein PTP-Master (z. B. TSN-Switch) im Netzwerk vorhanden sein.

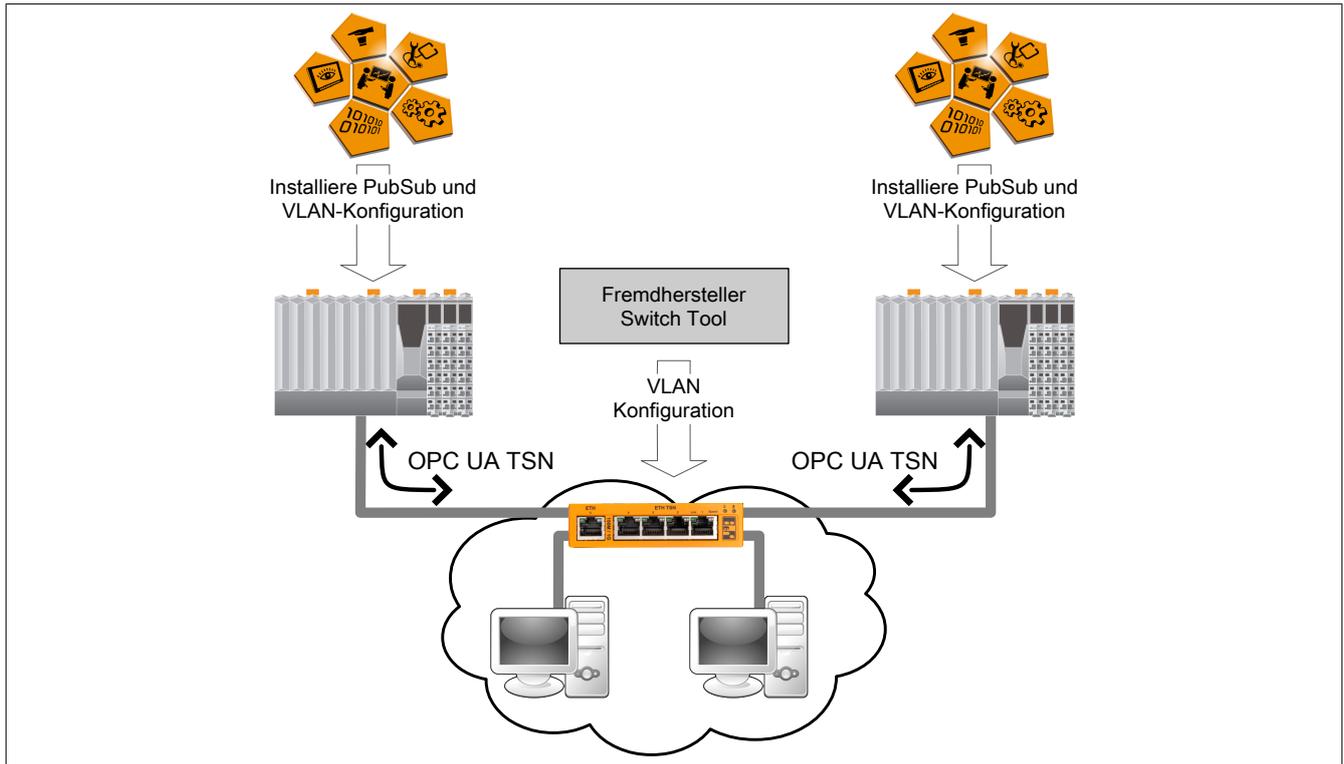


## 2.1.2 Übertragungsgarantie am IT-Netzwerk

Mit OPC UA over TSN bieten B&R-Steuerungen eine über konvergente TSN-Netzwerk-Infrastrukturen einsetzbare Kommunikationsmöglichkeit mit Übertragungsgarantie. Somit ist es möglich Maschinen, welche innerhalb einer Anlage an das bestehende TSN-Netzwerk angeschlossen sind, kommunizieren zu lassen ohne dass diese Kommunikation vom Best-Effort Verkehr im Netzwerk gestört wird. Dazu werden PubSub Nachrichten mit VLAN-Tags versehen, sodass ein TSN-fähiger Switch diese höherprior behandelt und dieser Verkehr somit nicht vom restlichen Best-Effort Verkehr behindert wird.

Die B&R-Steuerungen werden, wie in Automation Help Abschnitt "PubSub Konfiguration" beschrieben, hinsichtlich PubSub konfiguriert und es werden zusätzlich VLAN-Tags für die PubSub Nachrichten eingestellt. Für eine priorisierte Weiterleitung im Netzwerk muss diese VLAN-Information dann auch auf allen TSN-Switchs im Netzwerk konfiguriert werden.

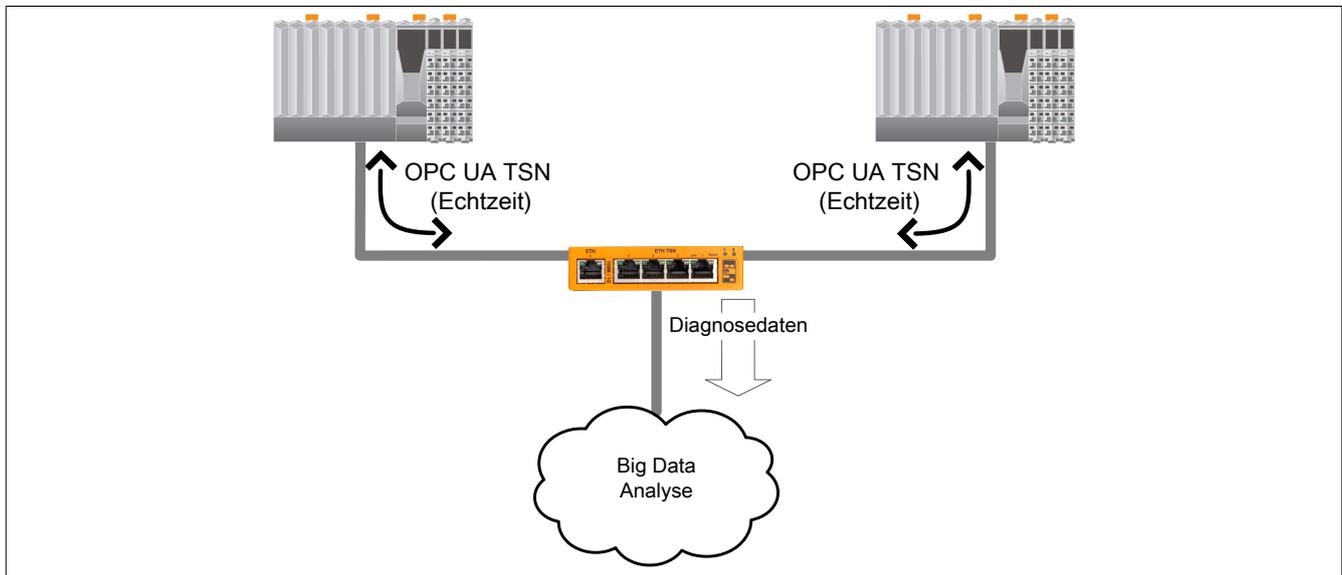
Um zeitgleiche Ereignisse auf den Steuerungen abzuarbeiten, kann auch in diesem Fall die Synchronisierung der Taskklasse1 durch PTP konfiguriert werden (Automation Help Abschnitt "PTP Konfiguration").



### 2.1.3 Big Data

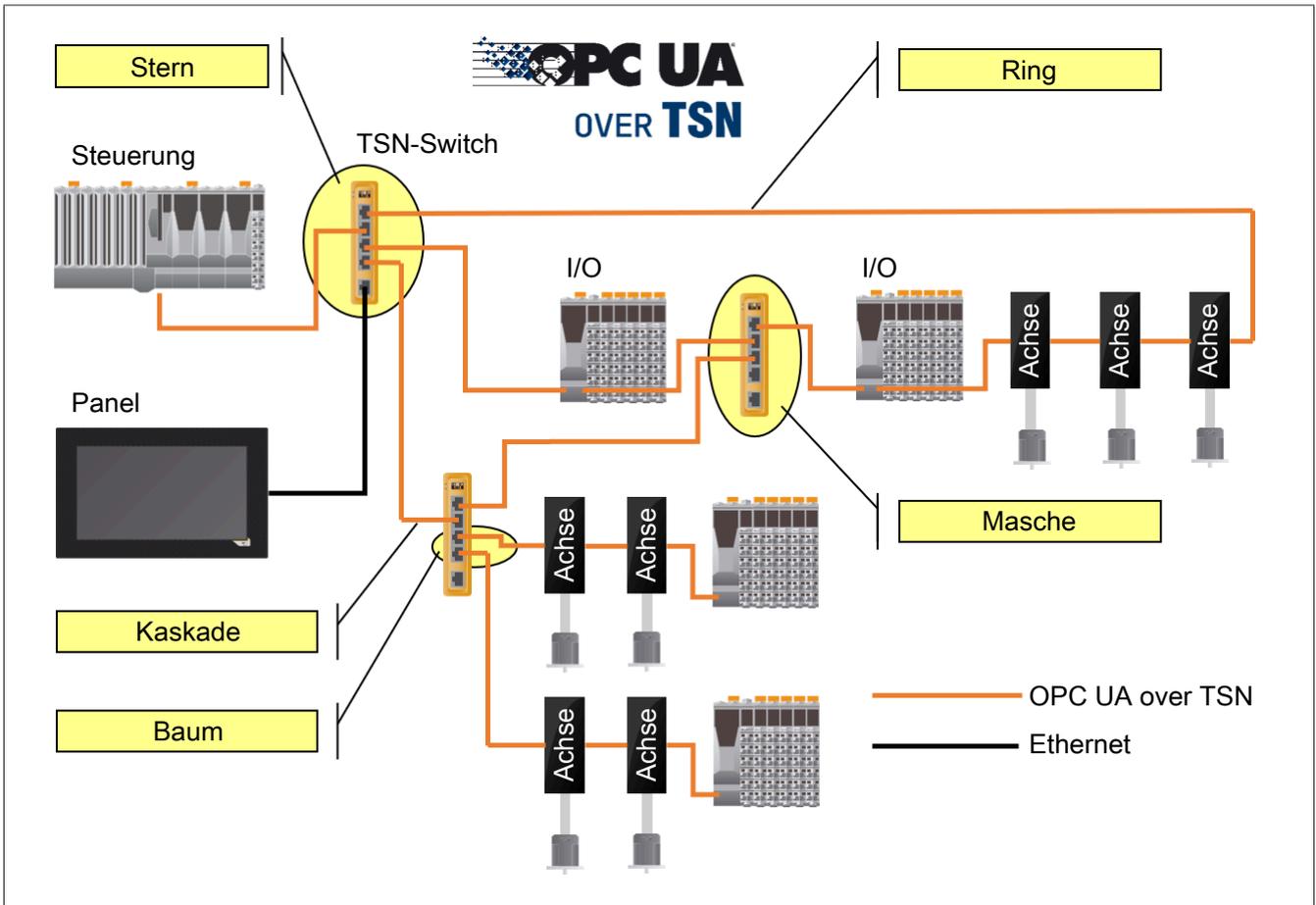
Mittels TSN-Mechanismen kann man die zu kommunizierenden Daten priorisieren. Es ist sowohl am Netzwerk als auch innerhalb der Steuerung möglich, zwischen wichtigen und weniger wichtigen Daten zu unterscheiden. Somit kann das Netzwerk durch Best-Effort Verkehr voll ausgelastet werden, bei gleichzeitiger Garantie der zeitgerechten Übertragung des Echtzeitverkehrs.

Das ist ein großer Unterschied im Vergleich zu bestehenden Kommunikationstechnologien, welche über Standard-Ethernet angeboten werden. Bei Technologien wie z. B. PROFINET oder Modbus TCP ist es möglich unter gewissen Voraussetzungen, wie z. B. sehr niedriger Netzwerklast sogenanntes "Soft Real Time" zu betreiben. Bei OPC UA over TSN hingegen ist es möglich "Hard Real Time" auch bei stark ausgelastetem Netzwerk zu betreiben.



## 2.2 Netzwerktopologien

Der TSN-Switch ermöglicht physikalisch Stern-, Baum-, Ring- oder vermaschte Topologien in OPC-UA-over-TSN-Netzwerken. Ebenso ist eine Kaskadierung mehrerer TSN-Switche realisierbar.



### Information:

Kabel- oder Ringredundanz in Ring- oder vermaschten Anordnungen wird vom TSN-Switch für OPC UA-over-TSN-Verbindungen nicht aktiv unterstützt.

Nur für Best-Effort Verbindungen ermöglicht der Multiple Spanning Tree Protocol (MSTP) Algorithmus eine entsprechende Redundanz.

## 3 Technische Beschreibung

### 3.1 Bestelldaten

Bestellnummer	Kurzbeschreibung	Abbildung
	<b>Switch</b>	
0ACST052.1	5-Port 100/1000 MBit Ethernet Layer 2 Industrie-Switch, 4-Port TSN, 1-Port Ethernet Uplink (RJ45, Layer 2), 24 VDC, Anschlussklemme 0TB2103.9110 beiliegend	

Tabelle 2: 0ACST052.1 - Bestelldaten

Für Details zur beiliegenden Anschlussklemme siehe [13 "0TB2103.9110"](#).

#### Optionales Zubehör

Bestellnummer	Kurzbeschreibung
<b>Verbindungskabel</b>	
X20CA0E61.xxxxx	POWERLINK/Ethernet-Verbindungskabel RJ45 auf RJ45, 0,2 bis 20 m
X20CA0E61.xxxx	POWERLINK/Ethernet-Verbindungskabel RJ45 auf RJ45, ab 20 m

#### Endklammerset bei Montage an senkrechter Hutschiene

Bestellnummer	Kurzbeschreibung	Abbildung
	<b>Endklammerset</b>	
X20AC0RF1	X20 Endklammerset für hohe Vibration	

Tabelle 3: X20AC0RF1 - Bestelldaten

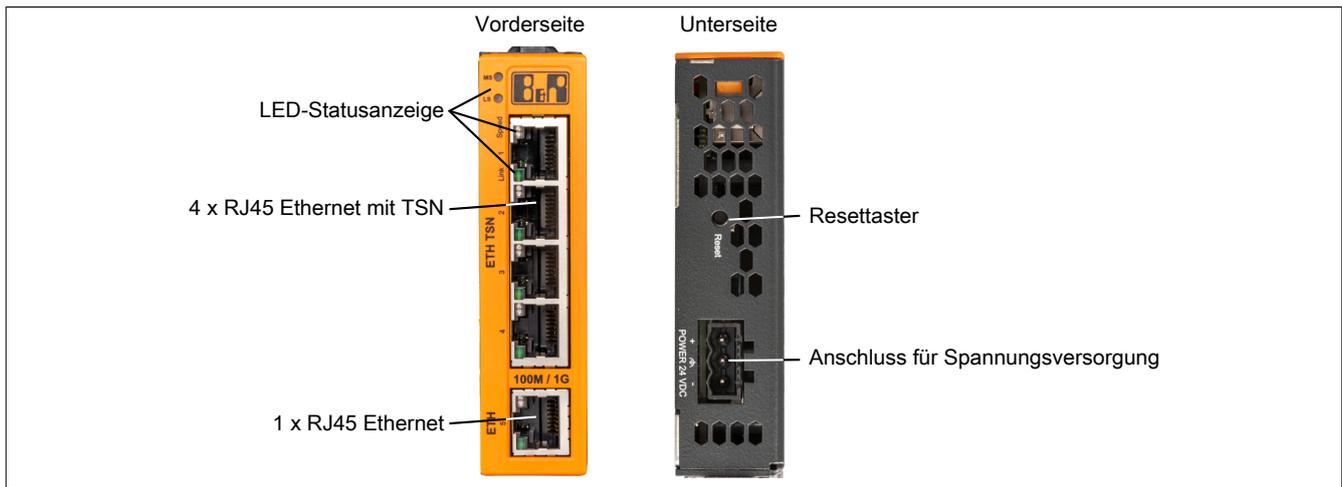
## 3.2 Technische Daten

Bestellnummer	0ACST052.1
<b>Allgemeines</b>	
B&R ID-Code	0x1404
Statusanzeigen	Modulstatus, Netzwerkstatus
Diagnose	
Modulstatus	Ja, per Status-LED und SW-Status
Netzwerkstatus	Ja, per Status-LED und SW-Status
Leistungsaufnahme	6,3 W
Zulassungen	
CE	Ja
UKCA	Ja
UL	cULus E115267 Industrial Control Equipment
<b>Schnittstellen</b>	
Typ	4x OPC UA over TSN 1x Ethernet
Standard (Compliance)	IEEE 802 (Standard Ethernet), IEEE 802.1Q (TSN), OPC UA
Ausführung	5x RJ45 geschirmt
Leitungslänge	max. 100 m zwischen 2 Stationen (Segmentlänge)
Übertragungsrate	100 MBit/s und 1 GBit/s
Übertragung	
Physik	100BASE-TX/1000BASE-T
Halbduplex	Nein
Vollduplex	Ja
Autonegotiation	Ja
Auto-MDI/MDIX	Ja
<b>Versorgung</b>	
Nennspannung	24 VDC, SELV/PELV
Spannungsbereich	20,4 bis 28,8 VDC
Sicherung	T 3 A
Verpolungsschutz	Ja
<b>Elektrische Eigenschaften</b>	
Potenzialtrennung	Ethernet zueinander und zu Versorgung getrennt
<b>Einsatzbedingungen</b>	
Einbaulage <sup>1)</sup>	
waagrecht	Ja
senkrecht	Ja
Aufstellungshöhe über NN (Meeresspiegel)	
0 bis 2000 m	Keine Einschränkung
>2000 m	Reduktion der Umgebungstemperatur um 0,5°C pro 100 m
maximal	4000 m
Verschmutzungsgrad nach EN 60664-1	2
Überspannungskategorie nach EN 60664-1	2
Schutzart nach EN 60529	IP20 <sup>2)</sup>
Betriebsposition	Nur im Innenbereich
<b>Umgebungsbedingungen</b>	
Temperatur	
Betrieb <sup>1)</sup>	
waagrechte Einbaulage	-25 bis 60°C
senkrechte Einbaulage	-25 bis 50°C
Derating	Siehe Abschnitt "Einbaulagen und Derating"
Lagerung	-40 bis 85°C
Transport	-40 bis 85°C
Luftfeuchtigkeit	
Betrieb	5 bis 95%, nicht kondensierend
Lagerung	5 bis 95%, nicht kondensierend
Transport	5 bis 95%, nicht kondensierend
<b>Mechanische Eigenschaften</b>	
Abmessungen	
Breite	25 mm
Länge	100 mm
Höhe	100 mm
Gewicht	280 g

Tabelle 4: 0ACST052.1 - Technische Daten

- 1) Für weitere Einbaulagen siehe Abschnitt "Einbaulagen und Derating".  
2) Nicht UL geprüft.

### 3.3 Bedien- und Anschlüsselemente



#### 3.3.1 Status-LED

In der folgenden Tabelle sind die Status-LEDs des TSN-Switchs beschrieben. Die genauen Blinkzeiten zeigt das Timingdiagramm im nächsten Abschnitt.

Direkt nach dem Einschalten blitzen die LEDs rot auf. Dies ist keine Fehlermeldung.

Abbildung	LED	Farbe	Status	Beschreibung
	MS <sup>1)</sup>	-	Aus	Modul nicht versorgt oder Modus RESET <sup>2)</sup>
		Grün	2 Pulse	Firmware-Update
			Ein	Modul OK
		Rot	1 Puls	Modus RESET: Neustart
			2 Pulse	Modus RESET: Konfiguration löschen
			3 Pulse	Modus RESET: Sicherheit-Konfiguration löschen
			4 Pulse	Modus RESET: Zurücksetzen auf Werkseinstellungen
	Ein	Fehlerzustand		
	Grün + Rot	Ein	Modus RESET: Bestätigung des Löschvorgangs	
	LS <sup>3)</sup>	Grün	1 Puls	Warten auf IP-Konfiguration
			2 Pulse	Warten auf PTP-Synchronisation
			3 Pulse	Warten auf NTP-Synchronisation
			Ein	Netzwerk OK
		Rot	1 Puls	Zeitüberschreitung IP-Konfiguration <sup>4)</sup>
			2 Pulse	Zeitüberschreitung PTP-Synchronisation <sup>5)</sup>
			3 Pulse	Zeitüberschreitung NTP-Synchronisation
	4 Pulse	Fehler PTP-Status <sup>6)</sup>		
	Ein	IP-Adressenkonflikt		
	Speed <sup>7)</sup>	Gelb	Ein	Übertragungsrate: 1 GBit/s
		Grün	Ein	Übertragungsrate: 100 MBit/s
Gelb + Grün		Aus	Übertragungsrate der Gegenstelle entspricht nicht 1 GBit/s oder 100 MBit/s	
Link	Grün	Aus	Kein Link zur Gegenstelle	
		Ein	Der Link zur Gegenstelle ist aufgebaut	
		Flackernd	Der Link zur Gegenstelle ist aufgebaut. Die LED flackert, wenn Ethernet Aktivität vorhanden ist.	

1) Modul-Status "MS": Diese LED ist eine grün/rote Dual-LED.

2) Siehe "Reset-taster" auf Seite 18.

3) LAN-Status "LS": Diese LED ist eine grün/rote Dual-LED.

Die LED wechselt vom grün gepulsten Zustand in den rot gepulsten Zustand, wenn der aktuelle "Warten auf"-Status länger als 15 s ansteht. Bei Statuswechsel wird diese Zeit zurückgesetzt.

4) Dem TSN-Switch wurde noch keine IP-Adresse zugewiesen.

5) Der TSN-Switch ist noch nicht über PTP synchronisiert. Mögliche Ursachen:

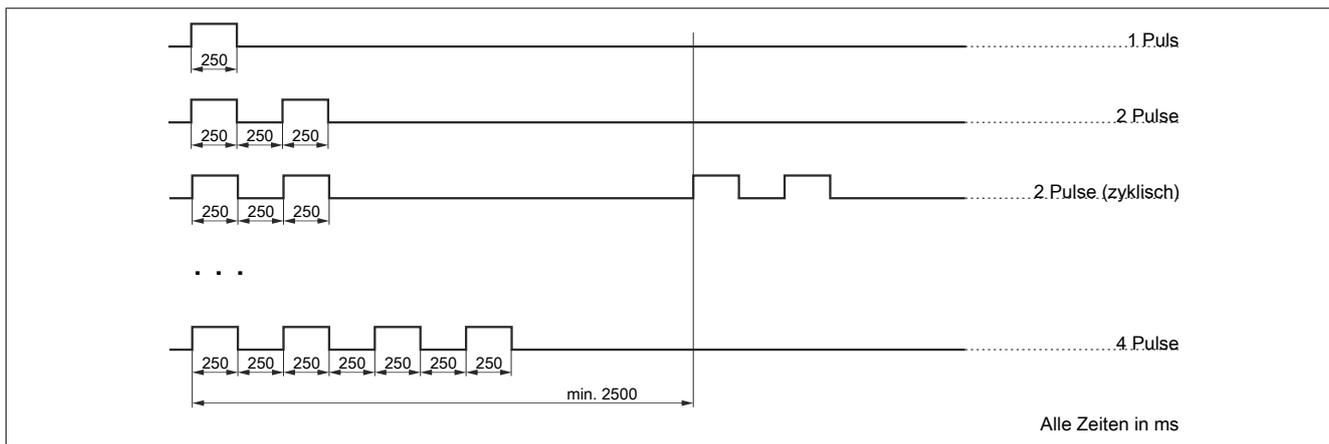
- Keine Verbindung zu einem PTP-Grandmaster
- Der Synchronisationsoffset zum PTP-Grandmaster ist außerhalb der Vorgabe ( $\text{abs}(\text{OffsetFromMaster}) > \text{SyncOffsetNs}$ ).
- PTP-Konfigurationsfehler

6) Mögliche Ursachen:

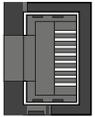
- Der TSN-Switch wurde als PTP-Grandmaster konfiguriert ( $\text{Priority1} < 128$ ), ist jedoch PTP-Slave.
- Der TSN-Switch wurde als PTP-Slave konfiguriert ( $\text{SlaveOnly} = \text{true}$ ), ist jedoch PTP-Grandmaster.

7) Netzwerkgeschwindigkeit: Diese LED ist eine grün/gelbe Dual-LED.

### Status-LEDs - Blinkzeiten



### 3.3.2 Ethernet Anschluss

Schnittstelle	Anschlussbelegung		
	Pin	Ethernet	
 Geschirmter RJ45 Port	1	D1+	Daten 1+
	2	D1-	Daten 1-
	3	D2+	Daten 2+
	4	D3+	Daten 3+
	5	D3-	Daten 3-
	6	D2-	Daten 2-
	7	D4+	Daten 4+
	8	D4-	Daten 4-

### 3.3.3 Resettaster

Auf der Unterseite des Moduls befindet sich ein Resettaster (roter Kreis).



#### Reset während Hochlauf

Anzeige des Hochlaufs: LED "MS" leuchtet noch nicht dauerhaft grün oder rot.

#### Information:

Während des Hochlaufs ist das Drücken des Resettasters nicht zulässig.

#### Reset während Betrieb

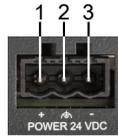
Während des Betriebs ist die ausgelöste Funktion von der Länge der Betätigungsdauer abhängig, welche der Resettaster gedrückt wird.

Funktion	Betätigungsdauer	LED-Anzeige <sup>1)</sup>	Bestätigung
Temporäre IP-Adresse setzen <sup>2)</sup>	1 s	LED "MS": Aus	-
Neustart	5 s	LED "MS": Nach 5 Sekunden 1 Puls	-
Konfiguration löschen	10 s	LED "MS": Nach 10 Sekunden 2 Pulse	Wird der Resettaster innerhalb von 5 s erneut betätigt, wird die Aktion ausgeführt und anschließend der TSN-Switch neu gestartet.
Sicherheitskonfiguration löschen	15 s	LED "MS": Nach 15 Sekunden 3 Pulse	
Zurücksetzen auf Werkseinstellungen	20 s	LED "MS": Nach 20 Sekunden 4 Pulse	

1) Siehe "Status-LEDs - Blinkzeiten" auf Seite 18.

2) Temporäre IP-Adresse 192.168.1.1; siehe "Einstellen der IP-Adresse" auf Seite 19.

### 3.3.4 24 VDC Versorgung



Klemme	Belegung
1	24 VDC
2	Funktionserde
3	0 V / GND

### 3.4 Versorgung des TSN-Switchs

Zur Versorgung des TSN-Switchs ist ein Netzteil mit einer Ausgangsspannung zwischen 20,4 bis 28,8 V notwendig. Es wird die Verwendung eines B&R 24 VDC-Netzteils empfohlen. B&R-Netzteile stellen sicher, dass der TSN-Switch selbst bei kurzfristigen Netzausfällen ( $\leq 10$  ms) zuverlässig versorgt wird.

#### **Achtung!**

**Primärstromkreise, aus denen die angeschlossenen Sekundärspannungen erzeugt werden, müssen auf die Überspannungskategorie II begrenzt sein und dürfen eine Systemspannung von maximal 300 V haben.**

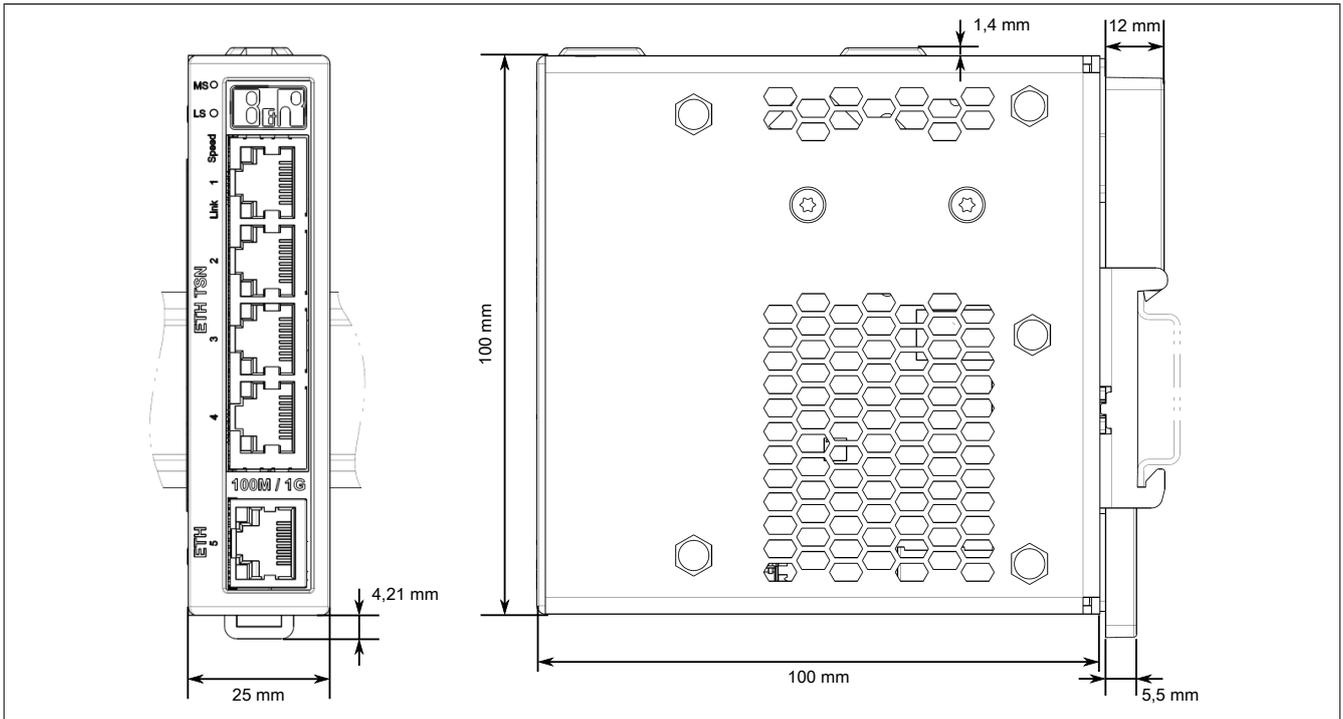
**Alle angeschlossenen Stromkreise müssen die Anforderungen an SELV/PELV-Stromkreise (Klasse III) gemäß UL/CSA/IEC 61010-1, 61010-2-201 erfüllen.**

### 3.5 Einstellen der IP-Adresse

Je nach verwendetem Einsatzgebiet kann eine IP-Adresse dem TSN-Switch auf verschiedene Arten zugewiesen werden.

- Automatische Zuweisung per DHCP-Server  
Standardmäßig ist der TSN-Switch für eine automatische IP-Adresszuweisung per DHCP-Server konfiguriert. In Maschinennetzwerken mit einer B&R-Steuerung wird die DHCP-Server-Funktion von der Automation Runtime bereitgestellt.  
PCs oder Laptops mit Desktop-Betriebssystemen, wie z. B. Windows oder Linux, bieten jedoch normalerweise keinen DHCP-Server an.
- Einstellen der temporären IP-Adresse (192.168.1.1) durch Betätigen des Resettaster. (Siehe Abschnitt "[Resettaster](#)" auf Seite 18)
- Konfiguration per OPC UA-Server
- Konfiguration im Automation Studio

### 3.6 Abmessungen



### 3.7 Montage

Der TSN-Switch wird mit der mitgelieferten Hutschienebefestigung im Schaltschrank montiert. Dabei sind folgende Einbaulagen möglich:

- Waagrechte Montage
- Senkrechte Montage
- Liegende Montage
- Schräge Montage

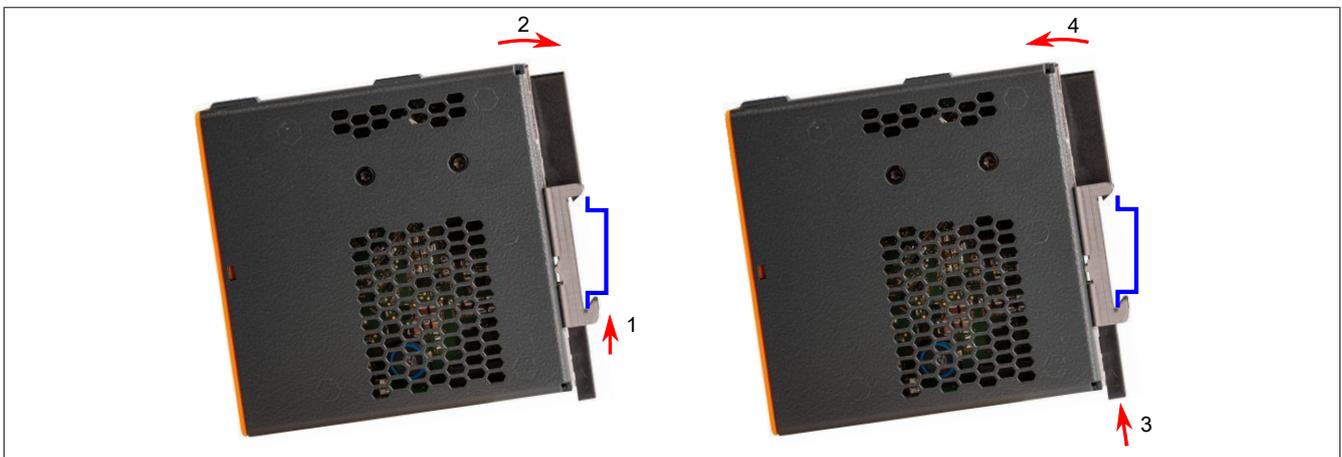
#### Achtung!

Das Modul muss in das endgültige Sicherheitsgehäuse eingebaut werden, das die Anforderungen nach UL/CSA/IEC 61010-1, UL/CSA/IEC 61010-2-201 aufweist und die geforderten Eigenschaften bezüglich Brandausbreitung erfüllt.

Es sind in jedem Fall die einschlägigen nationalen und internationalen Fachnormen, Vorschriften und Sicherheitsmaßnahmen zu beachten und einzuhalten

#### Modul (de-)montieren

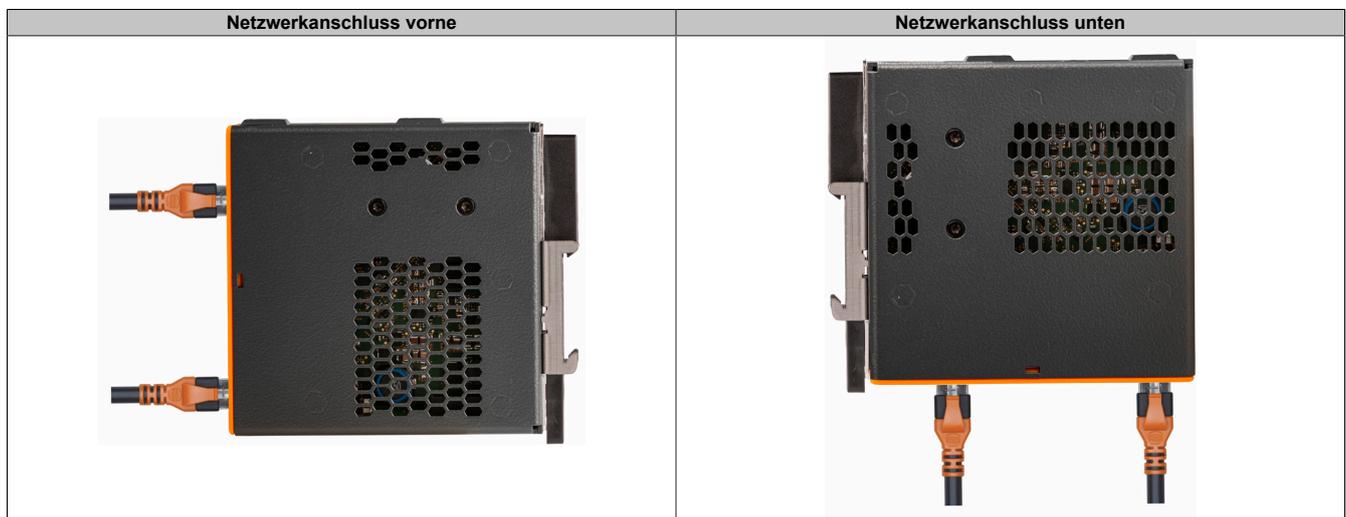
Zur Montage den TSN-Switch von unten in die Hutschiene einhängen (1) und Oberseite in Hutschiene einrasten (2). Zur Demontage Entriegelungshebel (3) drücken und den TSN-Switch von Hutschiene entfernen (4).



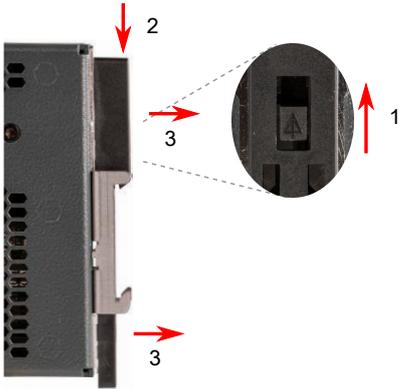
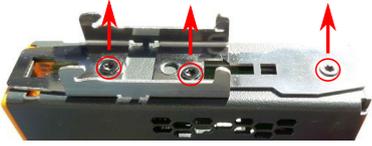
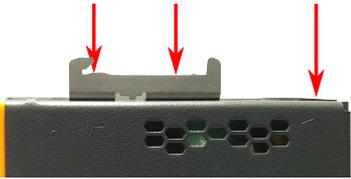
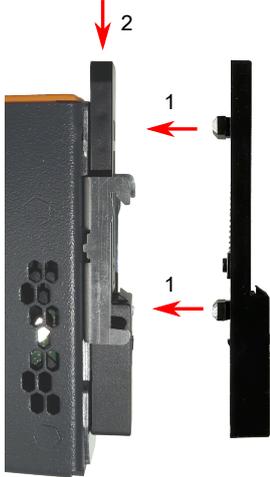
#### Optionen

Alle Einbaulagen verfügen über die Optionen "Netzwerkanschluss vorne" und "Netzwerkanschluss unten bzw. seitlich".

Die Hutschienehalterung ist bereits für die Option "Netzwerkanschluss vorne" vormontiert.



### 3.7.1 Ummontieren der Hutschienehalterung

<p>1. Sicherungshebel (1) ganz nach oben drücken und Hutschienehalterung anschließend nach unten schieben (2). Hutschienehalterung aus dem Gehäuse herausziehen (3).</p>	<p>2. M3-Schrauben entfernen und Hutschienehalterung abnehmen.</p>
	
<p>3. Seitliche Abdeckkappen entfernen.</p>	<p>4. Hutschienehalterung auflegen und M3-Schrauben mit einem Drehmoment von 0,55 Nm befestigen.</p>
	
<p>5. Haltebolzen des Hutschienehalters in Gehäuse einführen (1) und nach unten drücken (2).</p>	<p>6. Rückseitige Öffnungen mit Abdeckkappen verschließen.</p>
	

### 3.7.2 Einbautagen und Derating

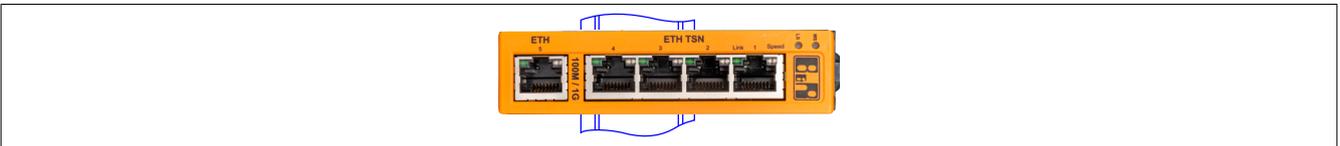
#### Waagrechte Montage



Ein Betrieb ist bis 60°C möglich. Bei der waagrechten Montage sind zwischen 2 Modulen folgende Abstände einzuhalten:

- Bis 50°C - Abstand 10 mm
- Ab 50°C - Abstand 20 mm

#### Senkrechte Montage



#### Information:

Bei einer senkrechten Montage muss der TSN-Switch mit einer **Endklammer** gegen Herabrutschen gesichert werden.

Ein Betrieb ist bis 50°C möglich. Bei der senkrechten Montage sind zwischen 2 Modulen folgende Abstände einzuhalten:

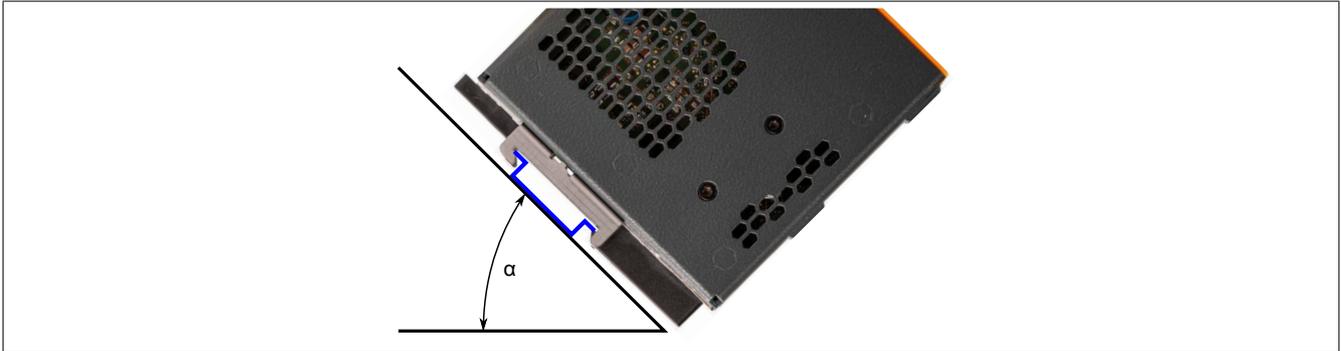
- Bis 40°C - Abstand 10 mm
- Ab 40°C - Abstand 20 mm

#### Liegende Montage



Ein Betrieb ist bis 45°C möglich. Bei der liegenden Montage ist zwischen 2 Modulen ein Abstand von 10 mm einzuhalten.

## Schräge Montage



Ein Betrieb ist bis 60°C möglich. Bei der schrägen Montage ist das zu verwendete Derating vom Winkel  $\alpha$  abhängig:

- $\alpha < 70^\circ$ : Entspricht liegender Montage
- $\alpha > 70^\circ$ : Entspricht waagrechter Montage

## 3.8 Blitz- und Überspannungsschutz

### Information:

Versehen Sie blitzschlaggefährdete Leitungen mit einem geeigneten Überspannungsschutz.

Die Stromkreise müssen auf die Überspannungskategorie II gemäß IEC 60664-1 begrenzt sein oder entsprechend anderslautender Informationen des Moduldatenblattes.

Für die Auslegung Ihrer elektrischen Anlage siehe ABB-Dokumentation "[Global guide to surge protection](#)".

### 3.8.1 UL/CSA

Die elektrischen Installationen müssen den jeweils relevanten Anforderungen des National Electrical Code® (ANSI/NFPA-70 (NEC®) und gegebenenfalls Canadian Electrical Code (CEC), CE Code, or CSA C22.1 entsprechen. Dies gilt speziell für elektrische Kommunikationsleitungen, welche außerhalb eines Gebäudes geführt werden und als blitzgefährdet gelten (siehe (ANSI/NFPA-70 (NEC®) 2020 Edition - Part III Protection 805.90 Protective Devices.

## 4 Erste Schritte

Der TSN-Switch wird mit Werkseinstellungen ausgeliefert. Das bedeutet, dass weder Gerätefunktionalität noch etwaige Sicherheitseinstellungen konfiguriert sind. Um die Inbetriebnahme sicher zu gestalten, soll dafür gesorgt werden, dass der TSN-Switch vorerst nur in einer sicheren Umgebung benutzt wird. Sichere Umgebungen sind z. B. von Unternehmensnetzwerk getrennte Netzwerke oder eine direkte Verbindung mit dem zur Konfiguration benutzten PC. Nach erfolgter Sicherheitskonfiguration kann der TSN-Switch auch in einer nicht sicheren Umgebung sicher betrieben werden.

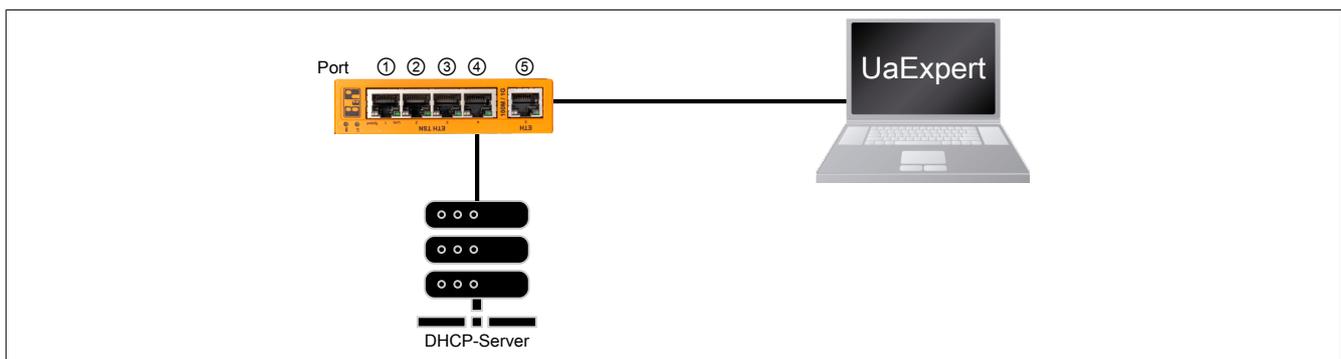
### 4.1 Vorbereitung

In den folgenden Beispielen wird die OPC UA Client-Software "UaExpert" für die Konfiguration verwendet. Sie kann aber auch mit anderen, vergleichbaren Tools durchgeführt werden.

Dabei sollte folgende Mindestversion verwendet werden:

- UaExpert ab Version 1.6  
Download: <https://www.unified-automation.com>

Zu Beginn kann der folgende Aufbau für eine Erstkonfiguration verwendet werden. Dieser besteht aus einem PC mit UaExpert-Software, einem direkt angeschlossenen TSN-Switch und einem DHCP-Server. Der DHCP-Server kann dabei auch Teil des PCs sein.



### 4.2 Verbindungsaufbau

#### Information:

Um Problem beim Verbindungsaufbau zu vermeiden, siehe auch Abschnitt 7.2 "Integration im IT-Netzwerk".

In der Werkseinstellung wird am TSN-Switch ein DHCP-Client gestartet und ein Hostname abhängig von Produktkennung und MAC-Adresse generiert. Ein im Netzwerk vorhandener DHCP-Server kann dadurch dem TSN-Switch eine IP-Adresse zuweisen. Zusätzlich ist am TSN-Switch Multicast-DNS (mDNS) aktiviert.

In der Werkseinstellung werden folgende Netzwerkeinstellungen vom DHCP-Server übernommen:

- IP-Adresse
- Subnetzmaske
- Gateway
- Hostname
- Domäne
- DNS-Server
- NTP-Server

Um die Werkseinstellungen zu ändern (siehe Abschnitt 4.5 "Allgemeine Netzwerkeinstellungen über OPC UA"), muss zuerst einer der folgenden, werkseitig vorhandenen Mechanismen für die erste Verbindung verwendet werden.

## 4.2.1 Verbindungsaufbau per Hostname

### 4.2.1.1 Hostnamen ermitteln

Für den Verbindungsaufbau muss zuerst der Hostname des TSN-Switchs bekannt sein. In den Werkseinstellungen wird dieser aus der Produktkennung und der TSN-Switch-MAC-Adresse generiert und hat folgendes Format:

0acst052-1-[MAC-Adresse]

#### Information:

**Nach einer Änderung des Hostnamens ist der Default-Hostname aus Produktkennung und Bus Controller-MAC-Adresse nicht mehr gültig.**

#### Beispiel

Für einen TSN-Switch mit MAC-Adresse 00:60:65:00:22:01 ergibt sich folgender Hostname:

0acst052-1-006065002201

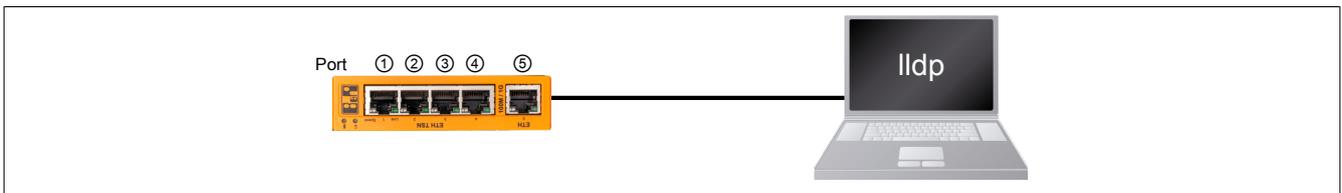
Um den Hostnamen zu ermitteln gibt es folgende Möglichkeiten:

#### 4.2.1.1.1 Hostname mit Gehäuseaufdruck ermitteln

Die TSN-Switch-MAC-Adresse ist, zusammen mit den MAC-Adressen der Ports, am Gehäuse aufgedruckt.

#### 4.2.1.1.2 Hostname mit LLDP und Direktverbindung ermitteln

Alternativ kann der Hostname über eine Netzwerkverbindung mit LLDP ermittelt werden. Der TSN-Switch veröffentlicht die MAC-Adresse des Endpoints im Netzwerk über das "Link Layer Discovery Protokoll (LLDP)" mit der Bezeichnung "ChassisID" an direkte Nachbargeräte. Diese lässt sich z. B. von einem PC mit Linux und direktem Geräteanschluss mithilfe von LLDP ermitteln:



#### Beispiel

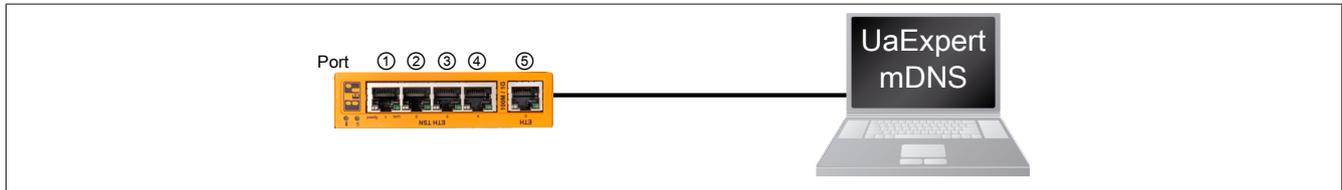
```
$ lldpctl
-----
Interface:   enx9cebe8ae5553, via: LLDP, RID: 42, Time: 0 day, 01:03:00
Chassis:
  ChassisID:   mac 00:60:65:00:22:01
  SysName:     0acst052-1-006065002201.home
  SysDescr:    B&R Industrial Automation GmbH, 802.1Q TSN Switch, 0ACST052.1,
               SW 1.0.0, HW C0
  MgmtIP:      192.168.0.128
  MgmtIP:      2a02:810d:6e3f:e9a0:260:65ff:fe00:2201
  Capability:  Bridge, on
  Capability:  Router, off
  Capability:  Wlan, off
  Capability:  Station, off
Port:
  PortID:      mac 00:60:65:00:22:03
  PortDescr:   sw0p3
  PMD autoneg: supported: yes, enabled: yes
  Adv:         100Base-TX, HD: no, FD: yes
  Adv:         1000Base-T, HD: no, FD: yes
  MAU oper type: 100BaseTXFD - 2 pair category 5 UTP, full duplex mode
-----
```

### 4.2.1.2 Hostnamen auflösen

Nachdem der Hostname ermittelt wurde, muss er durch die Netzwerk-Infrastruktur in eine IP-Adresse aufgelöst werden. Dafür gibt es folgende Möglichkeiten:

#### 4.2.1.2.1 Hostname-Auflösung per mDNS

Nachdem der Hostname bekannt ist, kann der TSN-Switch vom PC aus über diesen Namen angesprochen werden. Die Verbindung erfolgt in diesem Fall über den Hostnamen und der ".local"-mDNS-Domäne. Die IP-Adresse muss bei dieser Möglichkeit nicht bekannt sein.



Folgende "Endpoint-URL" kann im UaExpert für den Verbindungsaufbau verwendet werden (siehe 4.4 "Anlegen des initialen Benutzers"):

```
opc.tcp://<Produktkennung>-<MAC-Adresse>.local:4840
```

Bzw. für dieses Beispiel:

```
opc.tcp://0acst052-1-006065002201.local:4840
```

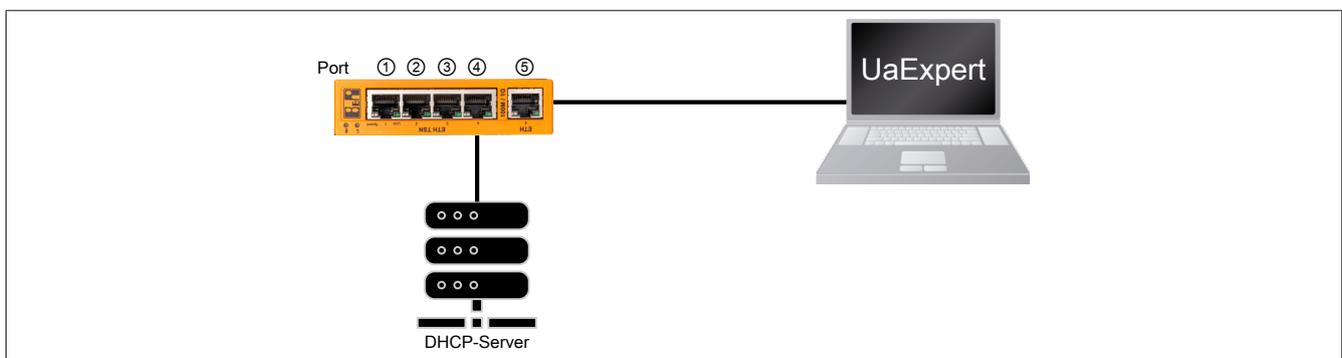
#### Information:

Der OPC UA Server am TSN-Switch erwartet eingehende Verbindungen auf Port 4840.

#### 4.2.1.2.2 Hostname-Auflösung per DNS

In großen Netzwerken mit vielen Teilnehmern oder wenn eine DHCP/DNS-Infrastruktur vorhanden ist und genutzt wird, besteht die Möglichkeit mDNS über das OPC UA Informationsmodell zu deaktivieren.

Die Verbindung erfolgt über den Hostnamen, da eine DHCP/DNS-Infrastruktur existiert. Die IP-Adresse muss bei dieser Möglichkeit nicht bekannt sein.



Folgende "Endpoint-URL" kann im UaExpert für den Verbindungsaufbau verwendet werden (siehe 4.4 "Anlegen des initialen Benutzers"):

```
opc.tcp://<Produktkennung>-<MAC-Adresse>:4840
```

Bzw. für dieses Beispiel:

```
opc.tcp://0acst052-1-006065002201:4840
```

## 4.2.2 Verbindungsaufbau per IP-Adresse

Je nach vorhandener Infrastruktur kann die Verbindung durch eine statische oder dynamischen IP-Adresse erfolgen.

### 4.2.2.1 Statische IP-Adresse

Für diese Methode wird kein DHCP-Server benötigt. Mit Hilfe des [Resettasters](#) wird die IPv4-Adresse für den aktuellen Bootvorgang auf den Wert "192.168.1.1" gesetzt.



Folgende "Endpoint-URL" kann im UaExpert für den Verbindungsaufbau verwendet werden (siehe [4.4 "Anlegen des initialen Benutzers"](#)):

```
opc.tcp://192.168.1.1:4840
```

Falls die IPv4-Adresse bereits konfiguriert und bekannt ist, ist der Resetvorgang nicht notwendig. In diesem Fall lautet die "Endpoint-URL" im UaExpert:

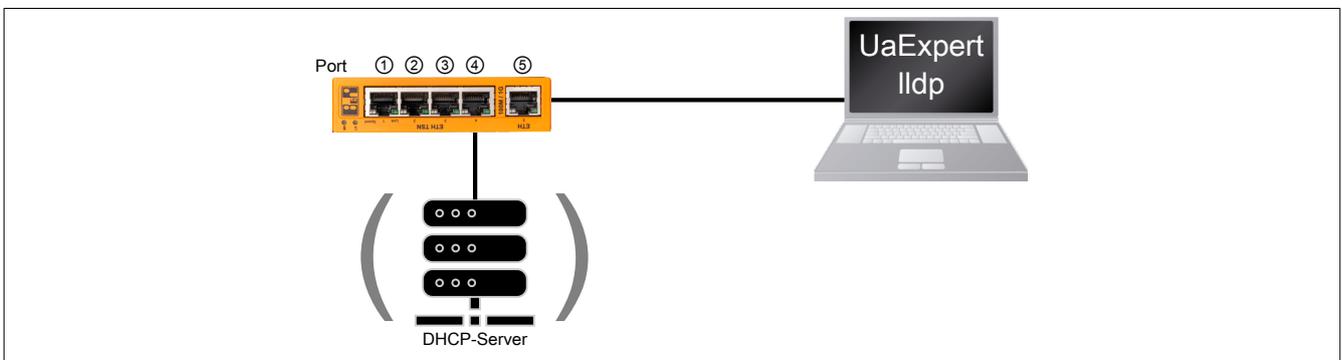
```
opc.tcp://<Bekannte IP-Adresse>:4840
```

### 4.2.2.2 Dynamische oder unbekannte IP-Adresse

Die Zuweisung einer IP-Adresse an den TSN-Switch kann auf mehrere Arten erfolgen:

- Durch den DHCP-Server
- Bekommt der TSN-Switch keine IP-Adresse per DHCP zugewiesen, wird vom TSN-Switch automatisch eine zufällige IPv4 Link-Local (IPv4LL) Adresse generiert

Diese zugewiesene IPv4-Adresse lässt sich per LLDP (siehe Abschnitt [Hostname mit LLDP und Direktverbindung ermitteln](#)) mit der Bezeichnung "MgmtIP" ermitteln.

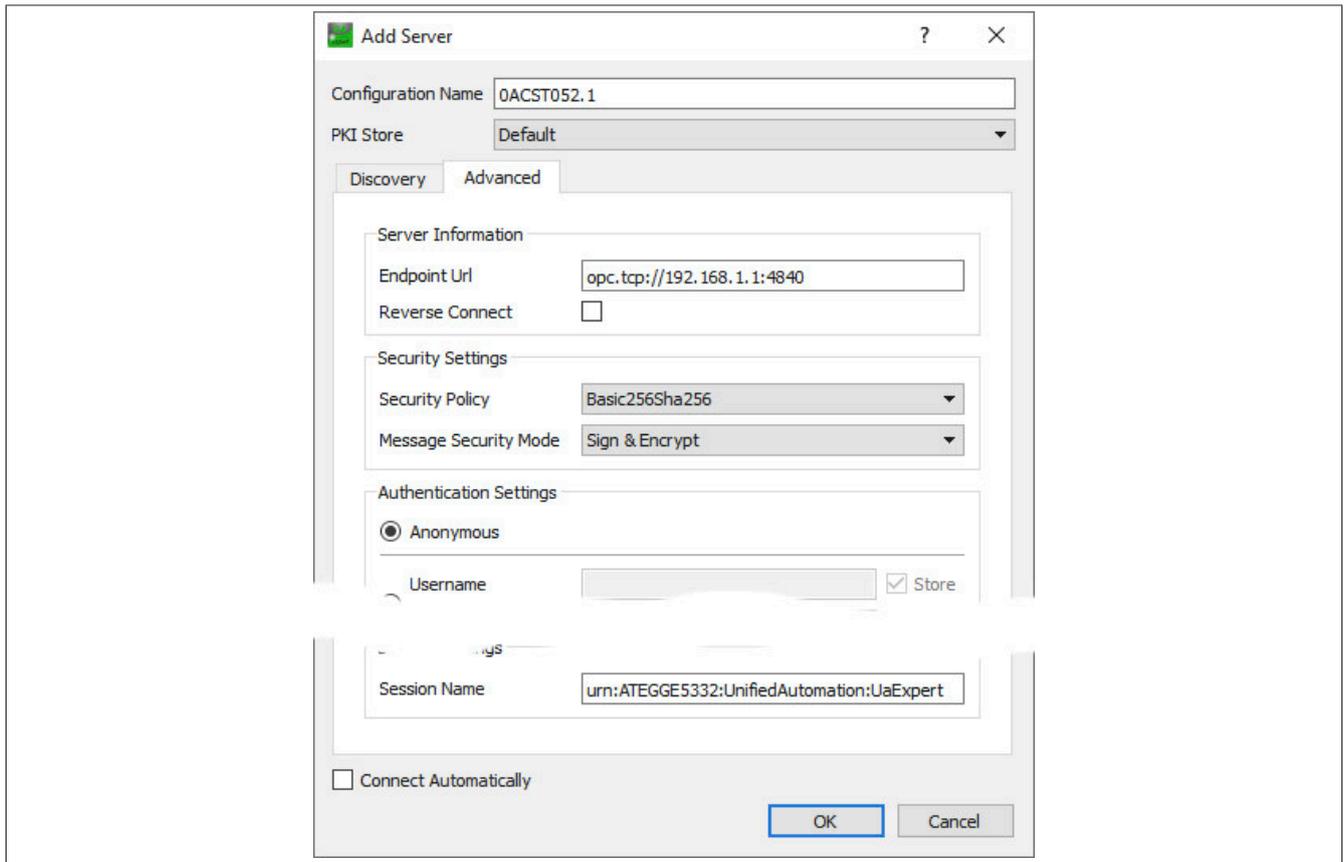


Folgende "Endpoint-URL" kann im UaExpert für den Verbindungsaufbau verwendet werden (siehe [4.4 "Anlegen des initialen Benutzers"](#)):

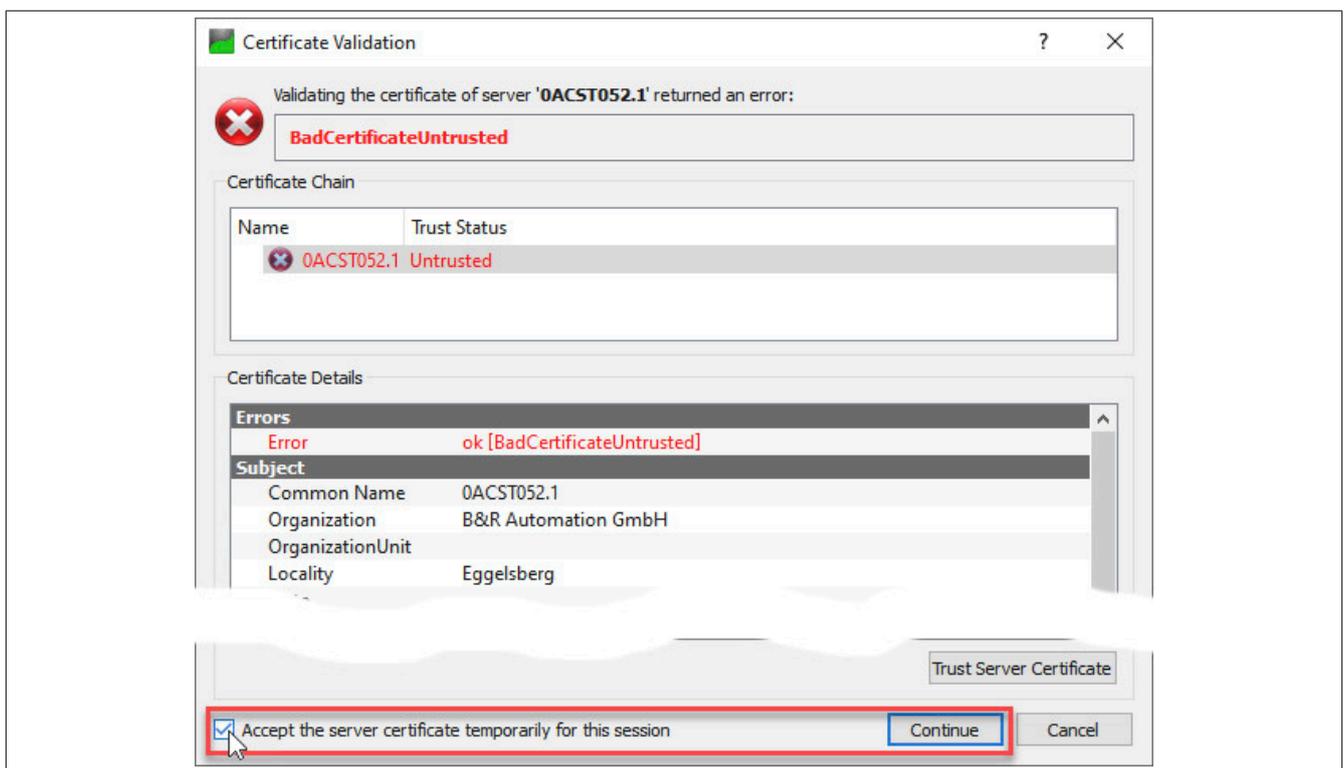
```
opc.tcp://<Ermittelte IP-Adresse>:4840
```

### 4.3 Mit OPC UA Client verbinden

- Für die erste OPC UA Verbindung ist die Einstellung *Anonymous* zu verwenden. Zusätzlich sollte eine angemessene Security-Policy wie *Basic256SHA256* ausgewählt werden, da sensible Daten übertragen werden.



- Der TSN-Switch ist initial noch nicht in eine Public-Key-Infrastruktur (PKI) eingebunden und hat daher lediglich ein selbst erzeugtes Zertifikat. Dieses Zertifikat ist korrekt, der Client kann dessen Herkunft aber nicht verifizieren und warnt daher. In einer vertrauenswürdigen Umgebung ist es aber sicher, dieses Zertifikat zu akzeptieren.



- Durch Auswahl von "Accept the server certificate temporarily for this session" und einen Klick auf *Continue* wird das Zertifikat akzeptiert.

### Information:

In einer nicht vertrauenswürdigen Umgebung kann durch das Akzeptieren eines solchen selbst erstellten Zertifikats ein gewisses Risiko entstehen. Ein Angreifer könnte sich als "Man-in-the-Middle" in die Kommunikation einklinken und den Datenverkehr trotz Verschlüsselung mitlesen und verfälschen.

## 4.4 Anlegen des initialen Benutzers

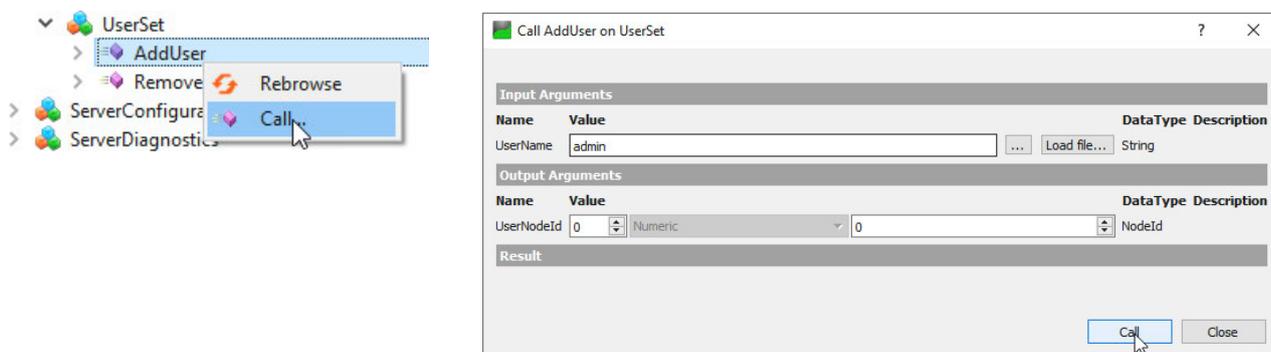
### Information:

Es muss zwingend ein Benutzer angelegt werden, ansonsten kann keine weitere Konfiguration durchgeführt werden.

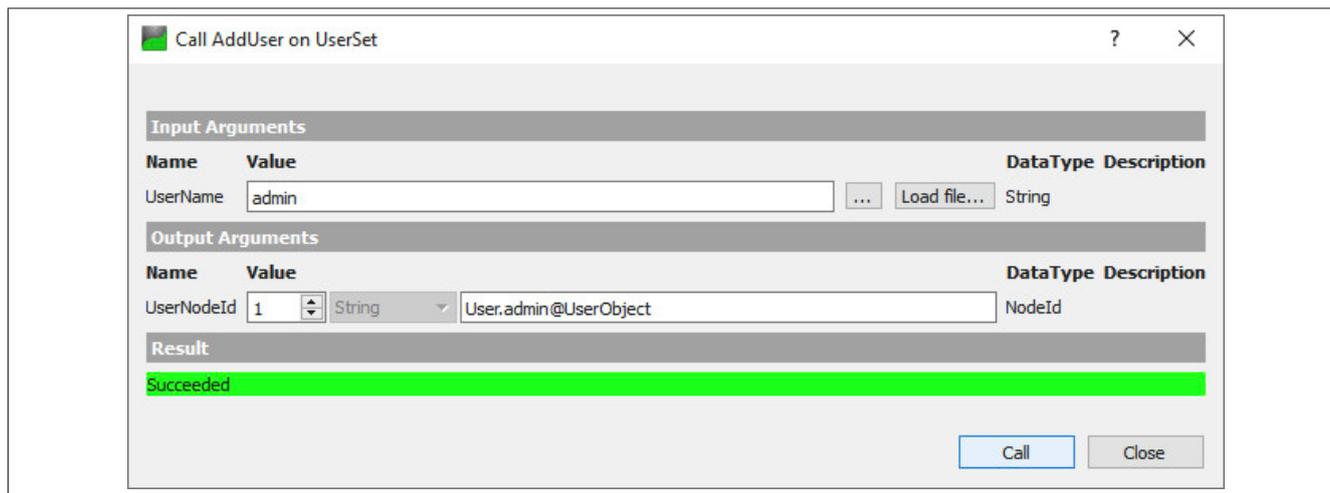
### Benutzer anlegen

Der TSN-Switch ist aktuell noch im Kommissionierungsmodus und erlaubt dem anonymen Client nur den Aufruf weniger Methoden. Diese enthalten das Anlegen des ersten Benutzers, das Setzen des Passworts und die Zuordnung zur Rolle *SecurityAdmin*.

- Als erster Schritt wird der Benutzer angelegt, der für die weitere Konfiguration zuständig ist. Dies geschieht durch Aufruf der Methode *Root/Objects/Server/ServerCapabilities/UserSet/AddUser*. Durch einen Klick auf *Call...* wird der Benutzerdialog angezeigt.

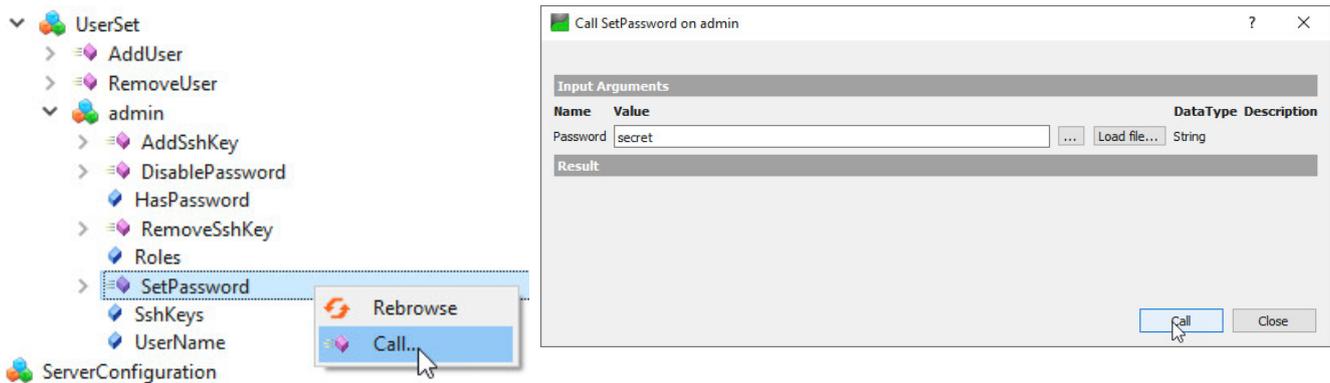


Ein erfolgreicher Aufruf wird unter "Result" angezeigt und die Knoten-ID des angelegten Benutzers zurückgegeben.



## Passwort zuordnen

- Der Name des neu angelegten Benutzers wird im Informationsmodell angezeigt. Um das Passwort zu konfigurieren, wird die Methode *Root/Objects/Server/ServerCapabilities/UserSet/<NAME>/SetPassword* aufgerufen. Durch einen Klick auf *Call...* wird der Passwortdialog angezeigt.

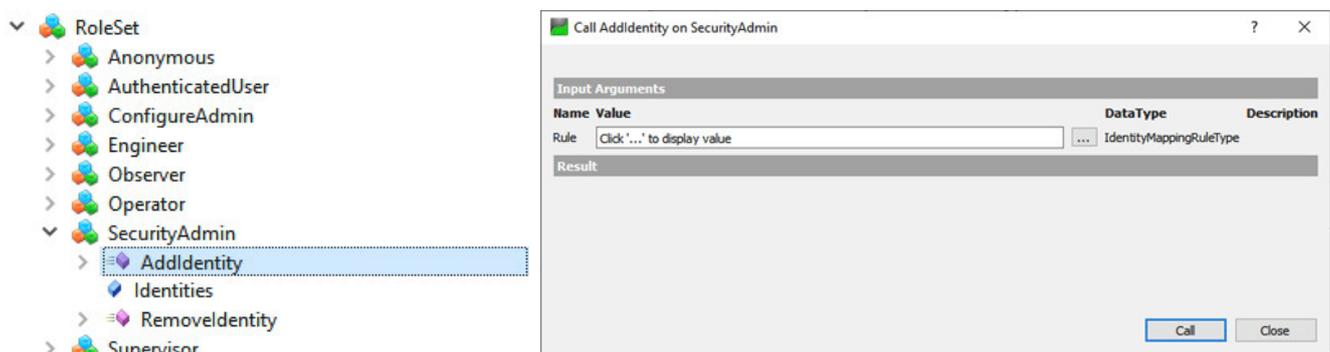


### Information:

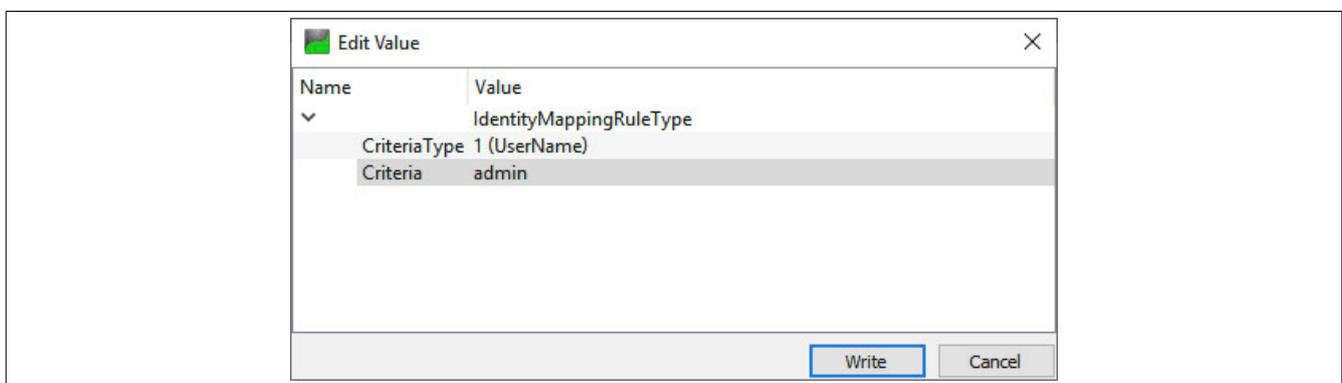
Das Passwort wird verschlüsselt vom Client zum TSN-Switch übertragen. Um ungewollte Zugriffe auf den TSN-Switch zu vermeiden, ist sicherzustellen, dass das Passwort während der Eingabe nicht von unbefugten Personen gesehen werden kann.

## SecurityAdmin-Rolle zuweisen

- Als nächstes ist dem Benutzer die für die weitere Konfiguration nötigen Berechtigungen als "Security Admin" zuzuweisen. Dazu wird die Methode *Root/Objects/Server/ServerCapabilities/RoleSet/SecurityAdmin/AddIdentity* aufgerufen.



Nach einem Klick auf "..." kann als *CriteriaType* der Eintrag "1 (UserName)" ausgewählt werden. Als "Criteria" wird der Benutzernamen angegeben.



Mit einem Klick auf *Write* werden die Daten übernommen und der Dialog geschlossen. Anschließend wird der SecurityAdmin-Dialog mit Klick auf *Call* geschlossen und der Benutzer damit als Security Admin angemeldet.

## Rollenzuordnung anzeigen

- Einem Benutzer können mehrere Rollen zugeordnet werden, bzw. mehrere Benutzer können dieselbe Rolle ausüben. Mit Hilfe der beiden Properties *Root/Objects/Server/ServerCapabilities/RoleSet* und *.../ServerCapabilities/UserSet* können diese eingesehen werden.

### Beispiel

Angabe aller Benutzer, welche als SecurityAdmin angemeldet sind.

- ▼ RoleSet
  - > Anonymous
  - > AuthenticatedUser
  - > ConfigureAdmin
  - > Engineer
  - > Observer
  - > Operator
  - ▼ SecurityAdmin
    - > AddIdentity
    - Identities
    - > RemoveIdentity
  - > Supervisor
  - ServerProfileArray
  - SoftwareCertificates

Value	
SourceTimestamp	03-Mar-21 16:01:29.198
SourcePicoseconds	0
ServerTimestamp	03-Mar-21 16:01:29.198
ServerPicoseconds	0
StatusCode	Good (0x00000000)
▼ Value	IdentityMappingRuleType Array[1]
▼ [0]	IdentityMappingRuleType
CriteriaType	1 (UserName)
Criteria	admin

### Beispiel

Angabe aller Rollen, welche dem Benutzer mit Namen "admin" zugeordnet sind.

- ▼ UserSet
  - > AddUser
  - > RemoveUser
  - ▼ admin
    - > AddSshKey
    - > DisablePassword
    - Password
    - > RemoveSshKey
    - Roles
    - > SetPassword
    - SshKeys

Value	
SourceTimestamp	03-Mar-21 16:06:27.937
SourcePicoseconds	0
ServerTimestamp	03-Mar-21 16:06:27.937
ServerPicoseconds	0
StatusCode	Good (0x00000000)
▼ Value	String Array[1]
[0]	SecurityAdmin

## Weitere Zuordnungen

Mit dem Anlegen des ersten Benutzers, dem Setzen des Passworts und der Zuordnung zur Rolle *SecurityAdmin* sind die Möglichkeiten des anonym angemeldeten Clients erschöpft.

- Um weitere Zuordnungen und Einstellungen vornehmen zu können, muss die Verbindung zum TSN-Switch getrennt und eine neue, mit Benutzernamen und Passwort authentifizierte Sitzung begonnen werden.

Security Settings

Security Policy: Basic256Sha256

Message Security Mode: Sign & Encrypt

Authentication Settings

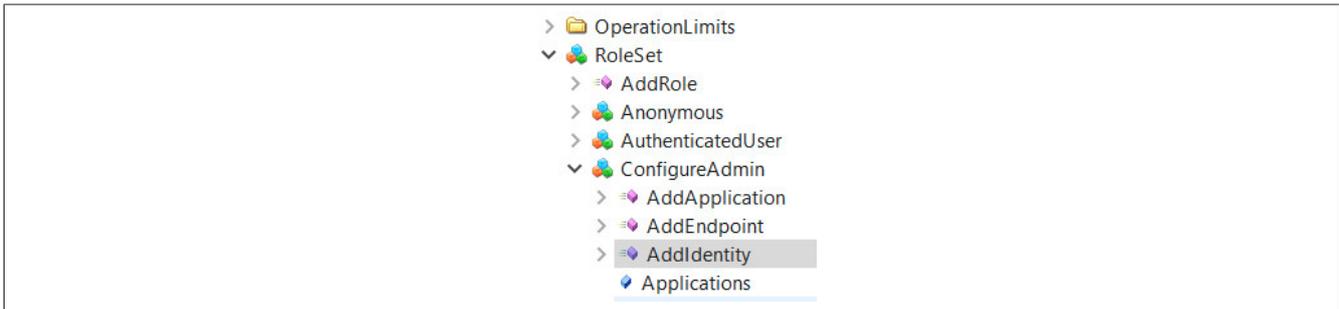
Anonymous

---

Username: admin  Store

    Password: .....

- Damit zusätzliche Einstellungen vorgenommen werden können, muss dem Benutzer zusätzlich die Rolle *ConfigureAdmin* zugewiesen werden. Dazu wird die Methode *Root/Objects/Server/ServerCapabilities/RoleSet/ConfigureAdmin/AddIdentity* aufgerufen und der Name, wie unter [SecurityAdmin-Rolle zuweisen](#) beschrieben, zugeordnet.



## 4.5 Allgemeine Netzwerkeinstellungen über OPC UA

Eine gültige Netzwerkkonfiguration kann über OPC UA durchgeführt werden.

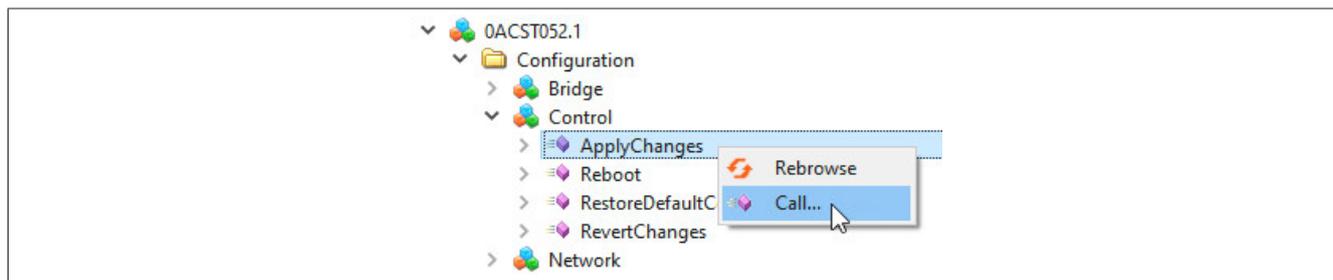
- Dafür werden die verschiedenen Parameter für die Netzwerk-Konfiguration unter *Root/Objects/DeviceSet/0ACST052.1/Configuration/Network* aufgerufen und entsprechend beschrieben.

The screenshot shows the configuration tree on the left and a data table on the right. In the tree, 'DeviceSet' is expanded to '0ACST052.1', then 'Configuration', and finally 'Network'. The 'IP-Address' parameter is selected and highlighted. The data table on the right shows the configuration details for the selected parameter.

UserRolePermissions	RolePermissionType Array[0]
AccessRestrictions	BadAttributeldInvalid (0x80350000)
Value	
SourceTimestamp	01.01.1970 02:23:28.219
SourcePicoseconds	0
ServerTimestamp	01.01.1970 02:23:28.219
ServerPicoseconds	0
StatusCode	Good (0x00000000)
Value	192.168.1.1
DataType	
NamespaceIndex	0
IdentifierType	Numeric
Identifier	12 [String]

Knotenname	Beschreibung
EnableDHCP	Aktiviert beziehungsweise deaktiviert die DHCP-Client-Funktionalität - Bei fehlender IP-Zuweisung durch einen DHCP-Server wird dem TSN-Switch eine zufällige Link Local Adresse aus dem Bereich 169.254.0.0/16 zugewiesen. IPv4LL (RFC3927). - Wenn der DHCP-Client aktiviert ist, werden die Parameter <i>Gateway</i> , <i>IP Address</i> , <i>Netmask</i> , sowie <i>Primary DNS</i> und <i>Secondary DNS</i> vom DHCP-Server bezogen.
Gateway	Konfiguration der Default-Gateway IP-Adresse - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, kann zusätzlich eine Gateway-Adresse vom DHCP-Server übermittelt werden. - Wenn der Parameter <i>Gateway</i> gesetzt ist, wird die manuelle Konfiguration verwendet und die vom DHCP-Server übermittelte Adresse ignoriert.
Hostname	Konfiguration des Hostnamens
IP-Address	Konfiguration einer statischen IP-Adresse - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, dann wird der Parameter ignoriert und die vom DHCP-Server übermittelte IP-Adresse verwendet.
Primary DNS Secondary DNS	Konfiguration eines primären bzw. sekundären DNS-Servers - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, können zusätzlich Adressen für DNS-Server vom DHCP-Server übermittelt werden. - Wenn mindestens 1 DNS-Server manuell gesetzt ist, wird die manuelle Konfiguration verwendet und die vom DHCP-Server übermittelten Adressen werden ignoriert.
Netmask	Einstellung der Subnetzmaske - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, wird dieser Parameter ignoriert und die vom DHCP-Server übermittelte Subnetzmaske verwendet.
EnableMulticastDNS	Aktiviert beziehungsweise deaktiviert Multicast DNS (mDNS) - In der Werkseinstellung ist mDNS aktiviert, um auch bei fehlender Netzwerkinfrastruktur den TSN-Switch über den Hostnamen ansprechen zu können.

- Damit die neue Konfigurationsdaten gespeichert werden, muss die Methode *Root/Objects/DeviceSet/0ACST052.1/Configuration/Control/ApplyChanges* aufgerufen werden.



### Information:

Die neue Netzwerkkonfiguration wird erst beim Neustart des TSN-Switchs übernommen.

## 4.6 Zeitsynchronisation

Für den Betrieb benötigt der TSN-Switch Informationen zur aktuellen Uhrzeit. Diese wird vor allem benötigt, damit digitale Zertifikate korrekt verarbeitet werden können und um die Zeitstempel von OPC UA Werten richtig zu setzen.

Im Folgenden wird beschrieben wie die sogenannte "WallClock" konfiguriert werden muss, damit eine Synchronisation über das Network Time Protocol (NTP) erfolgt. Die notwendigen Parameter befinden sich unter *Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WallClock*.

- Damit NTP für die Zeitsynchronisation verwendet wird, muss über Parameter *.../WallClock/TimeSyncProtocol* das Protokoll für die Synchronisation auf NTP eingestellt werden.

Property	Value																						
UserKolePermissions	KolePermission type Array[UI]																						
AccessRestrictions	BadAttributeldInvalid (0x80350000)																						
Value	<table border="1"> <tr> <td>SourceTimestamp</td> <td>01.01.1970 02:30:43.695</td> </tr> <tr> <td>SourcePicoseconds</td> <td>0</td> </tr> <tr> <td>ServerTimestamp</td> <td>01.01.1970 02:30:43.695</td> </tr> <tr> <td>ServerPicoseconds</td> <td>0</td> </tr> <tr> <td>StatusCode</td> <td>Good (0x00000000)</td> </tr> <tr> <td>Value</td> <td>0 (NONE)</td> </tr> <tr> <td>DataType</td> <td>0 (NONE)</td> </tr> <tr> <td>NamespaceIndex</td> <td>1 (PTP)</td> </tr> <tr> <td>IdentifierType</td> <td>2 (NTP)</td> </tr> <tr> <td>Identifier</td> <td>3012</td> </tr> <tr> <td>ValueRank</td> <td>-1 (Scalar)</td> </tr> </table>	SourceTimestamp	01.01.1970 02:30:43.695	SourcePicoseconds	0	ServerTimestamp	01.01.1970 02:30:43.695	ServerPicoseconds	0	StatusCode	Good (0x00000000)	Value	0 (NONE)	DataType	0 (NONE)	NamespaceIndex	1 (PTP)	IdentifierType	2 (NTP)	Identifier	3012	ValueRank	-1 (Scalar)
SourceTimestamp	01.01.1970 02:30:43.695																						
SourcePicoseconds	0																						
ServerTimestamp	01.01.1970 02:30:43.695																						
ServerPicoseconds	0																						
StatusCode	Good (0x00000000)																						
Value	0 (NONE)																						
DataType	0 (NONE)																						
NamespaceIndex	1 (PTP)																						
IdentifierType	2 (NTP)																						
Identifier	3012																						
ValueRank	-1 (Scalar)																						

- Der nächste Konfigurationsschritt ist von der Art des Netzwerks abhängig, in dem sich der TSN-Switch befindet.
  - Wenn im Netzwerk Zeitserver mittels DHCP übermittelt werden, muss kein Zeitserver eingestellt werden, sondern es werden die vom DHCP-Server übermittelten Zeitserver verwendet.
  - Wenn im Netzwerk kein Zeitserver mittels DHCP übermittelt wird, muss im Unterobjekt *NTP* mindestens 1 Zeitserver konfiguriert werden. Hierzu ist im Attribut *Value* des Knotens *TimeServer0x* der Hostnamen oder die IP-Adresse einzutragen.
- Damit die neuen Konfigurationsdaten gespeichert werden, muss die Methode *Root/Objects/DeviceSet/0ACST052.1/Configuration/Control/ApplyChanges* aufgerufen werden.

### Information:

Die neue Konfiguration wird erst beim Neustart des TSN-Switchs übernommen.

## 4.7 Neustart und Reset

Ein Neustart kann über die Methode *Root/Objects/DeviceSet/0ACST052.1/Configuration/Control/Reboot* ausgelöst werden. Vorher mittels der Methode *ApplyChanges* gespeicherte Konfigurationen werden beim Hochfahren des TSN-Switchs übernommen und angewendet.

Wurde die Netzwerkkonfiguration geändert, ist nach dem Neustart der TSN-Switch nur unter den neuen Einstellungen erreichbar. Bei Verbindungsproblemen sind daher im UaExpert die Verbindungseinstellungen entsprechend der neuen Konfiguration anzupassen.

## 4.8 Aktualisierung des Self-Signed Zertifikats

Der TSN-Switch verfügt im Informationsmodell über eine Methode, die verwendet werden kann, um auf einfache Weise ein neues selbstsigniertes Zertifikat zu erzeugen, das notwendige applikationsspezifische Informationen enthält.

- Für die Aktualisierung muss die Methode *UpdateSelfSignedCertificate* durch einen Klick auf *Call* unter *Root/Objects/Server/ServerConfiguration (1)* aufgerufen werden.

Im Methodendialog (2) werden die gewünschten Werte eingegeben. Die Methode verfügt über folgende Argumente:

Argument	Beschreibung																								
<b>Eingangsargumente</b>																									
ExpiryDate	Ablaufdatum, bis zu dem das Zertifikat gültig ist.  <b>Information:</b> Die Eingabe wird nur auf den Tag genau ausgewertet																								
Subject	Sequenz aus X.509 Name-Wert-Paaren die durch ein "/"-Zeichen getrennt werden. Die folgenden Namen sind vorgesehen: <table border="1" data-bbox="534 1429 1457 1639"> <thead> <tr> <th>Name</th> <th>Vollständiger Name</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>CN</td> <td>CommonName</td> <td>Name des Produkts oder vergleichbare Information</td> </tr> <tr> <td>O</td> <td>Organization</td> <td>Information Name der Organisation die den TSN-Switch betreibt</td> </tr> <tr> <td>OU</td> <td>Organization Unit</td> <td>Organisationseinheit</td> </tr> <tr> <td>DC</td> <td>Domain Component</td> <td>Domain der Organisation</td> </tr> <tr> <td>L</td> <td>Locality</td> <td>Ort oder Stadt</td> </tr> <tr> <td>S</td> <td>State</td> <td>Bundesstaat</td> </tr> <tr> <td>C</td> <td>Country</td> <td>2-Zeichen Ländercode</td> </tr> </tbody> </table> <b>Information:</b> Die Angabe der Werte /CN und /O ist verpflichtend. <b>Beispiel</b> "/O=B&R Industrial Automation GmbH/CN=0ACST052.1-OPCUA/DC=switch/DC=machine/DC=customer/DC=com"	Name	Vollständiger Name	Beschreibung	CN	CommonName	Name des Produkts oder vergleichbare Information	O	Organization	Information Name der Organisation die den TSN-Switch betreibt	OU	Organization Unit	Organisationseinheit	DC	Domain Component	Domain der Organisation	L	Locality	Ort oder Stadt	S	State	Bundesstaat	C	Country	2-Zeichen Ländercode
Name	Vollständiger Name	Beschreibung																							
CN	CommonName	Name des Produkts oder vergleichbare Information																							
O	Organization	Information Name der Organisation die den TSN-Switch betreibt																							
OU	Organization Unit	Organisationseinheit																							
DC	Domain Component	Domain der Organisation																							
L	Locality	Ort oder Stadt																							
S	State	Bundesstaat																							
C	Country	2-Zeichen Ländercode																							
DNS (optional)	Hostname oder Fully Qualified Domain Name (FQDN) des Switchs. Wenn bei diesem Parameter ein leerer String angegeben wird, wird der konfigurierte Hostname des TSN-Switchs in das Zertifikat eingetragen.																								
IncludeIPAddress	Gibt an, ob eine IP-Adresse in das Zertifikat eingetragen werden soll. Das Eintragen der IP-Adresse ist notwendig, wenn die IP-Adresse statisch vergeben ist und Clients mit Hilfe der IP-Adresse auf den TSN-Switch zugreifen (Zum Beispiel über die URL <code>opc.tcp://192.168.1.1:4840</code> ). Wird die IP-Adresse über einen DHCP-Server bezogen, ist es nicht sinnvoll eine IP-Adresse in das Zertifikat einzutragen, da sie dynamisch zugeteilt wird und nicht immer gleich ist.																								
IP Address (optional)	IP-Adresse, die in das Zertifikat eingetragen werden soll. Wenn hier ein leerer String übergeben wird und <i>IncludeIPAddress</i> gesetzt ist, dann wird die konfigurierte IP-Adresse in das Zertifikat eingetragen.																								
<b>Ausgangsargumente</b>																									
ApplyChangesRequired	Zeigt an, ob die Methode <i>Root/Objects/Server/ServerConfiguration/ApplyChanges</i> ausgeführt werden kann, um die Änderungen zu übernehmen.																								

- Wenn das Zertifikat erfolgreich erstellt werden konnte, muss im Anschluss die Methode *Root/Objects/Server/ServerConfiguration/ApplyChanges* (3) aufgerufen werden, um die Änderungen zu übernehmen.

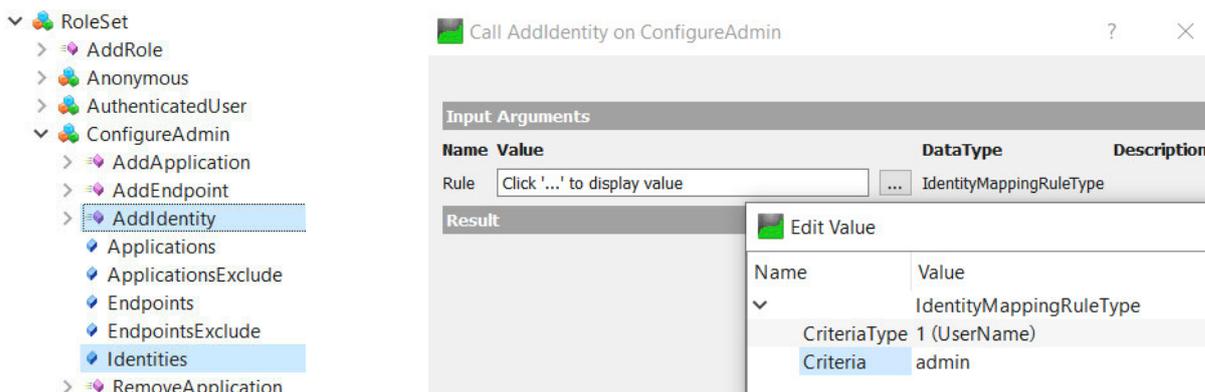
### Information:

Beim Aufruf der Methode *ApplyChanges* werden alle verbundenen Clients getrennt. Eine neue Verbindung ist erst wieder möglich, wenn dem neuen Zertifikat vertraut wird.

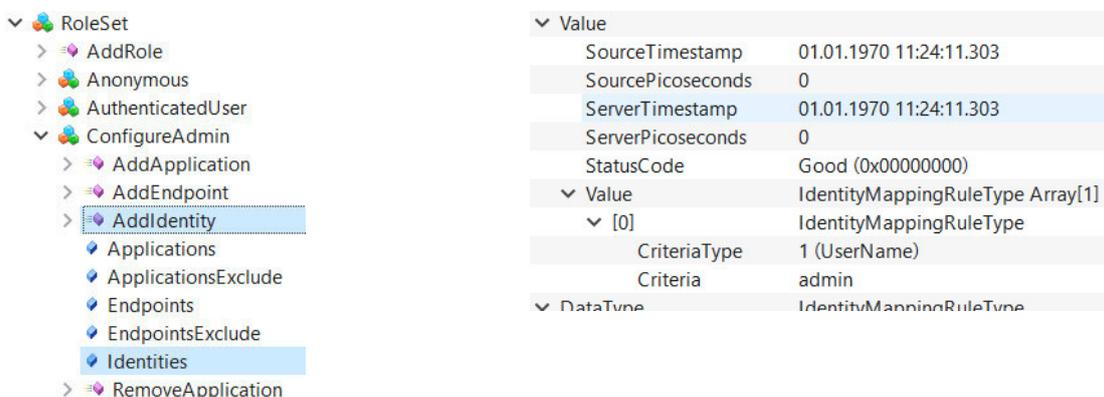
## 4.9 TSN-Netzwerkconfiguration über NETCONF

### 4.9.1 Benutzerrechte

- Damit eine Konfiguration über NETCONF möglich ist, muss einem existierenden Benutzer die Rolle *ConfigureAdmin* zugewiesen sein. Diese Rolle kann mit der Methode *Root/Objects/Server/ServerCapabilities/RoleSet/ConfigureAdmin/AddIdentity* hinzugefügt werden.



- Mit der Variable *Root/Objects/Server/ServerCapabilities/RoleSet/ConfigureAdmin/Identities* lässt sich das Ergebnis überprüfen.



### 4.9.2 Konfigurationswerkzeuge

Für die vereinfachte Durchführung von TSN-Netzwerkconfigurationen, ohne detaillierte Kenntnisse über NETCONF zu benötigen, stehen verschiedene Konfigurationswerkzeuge zur Verfügung. Für Beispiele dafür siehe [7.3 "Konfiguration über NETCONF"](#).

## 5 Firmwareupdate über OPC UA

Mit der Firmwareupdate-Funktionalität lässt sich über OPC UA die Firmware des TSN-Switchs auf einen beliebigen Versionsstand bringen. Dabei bleibt sichergestellt, dass auch bei einem Spannungsausfall oder einer Unterbrechung der Übertragung stets eine kommunikationsfähige Firmware geladen wird.

Der Updatemechanismus richtet sich nach der Spezifikation "OPC 10000-100 - UA Specification Part 100 - Devices 1.03.0" und verwendet die "Cached-Loading" Option, bei der die Firmwaredatei zuerst auf den Server geladen und in einem zweiten Schritt installiert wird. Zuletzt muss die installierte Firmware noch aktiviert werden.

Um ein Firmwareupdate durchzuführen wird ein UaExpert Client benötigt, der folgende OPC UA Typen unterstützt:

- FileType
- TemporaryFileTransferType
- OptionSet

Für Details zur Durchführung des Firmwareupdates mit UaExpert siehe Abschnitt 5.1 "Update durchführen".

Für eine detaillierte Beschreibung der Struktur des Firmwareupdate Objekts siehe 12.1.2 "Firmwareupdate".

### 5.1 Update durchführen

Alle benötigten Methoden und Statusinformationen für den Firmwareupdate befinden sich unter *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate*. Zusätzlich wird noch die Methode "Reboot" unter *Root/Objects/DeviceSet/0ACST052.1/Configuration/Control/Reboot* benötigt.

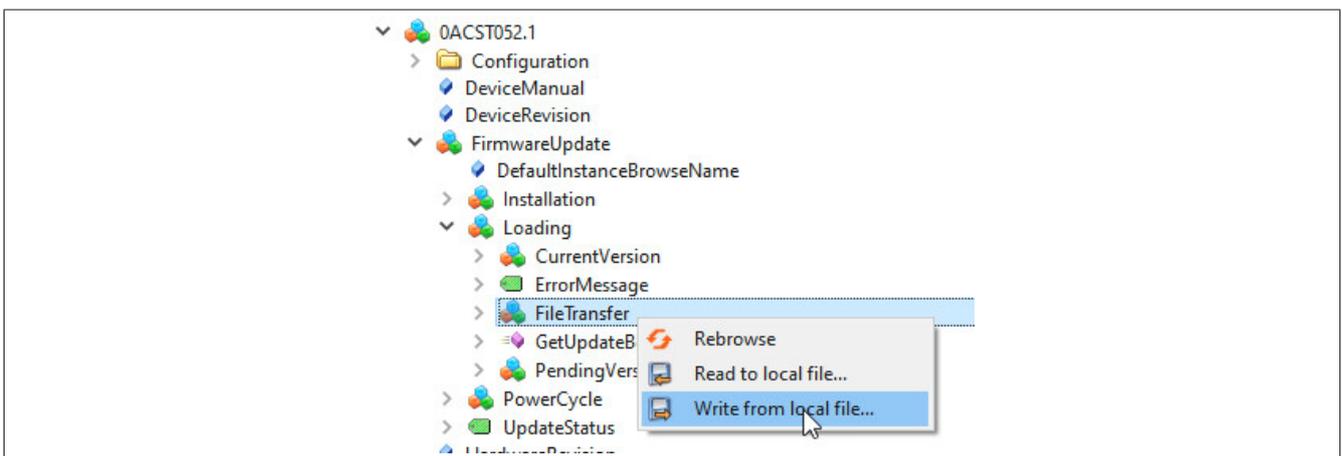
Ein Firmwareupdate kann mit UaExpert auf einfache Art durchgeführt werden. Dazu sind folgende Schritte nötig:

#### • Vorbereitung

Gewünschte Firmwareupdate-Datei von der [B&R Homepage \(https://www.br-automation.com\)](https://www.br-automation.com) herunterladen und entpacken.

#### • Übertragung

Nachdem eine Verbindung mit dem TSN-Switch hergestellt wurde, im Objekt *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/Loading/FileTransfer* einen Rechtsklick auf *Write from local file ...* durchführen und die entpackte Firmwareupdate Datei (\*.fw) auswählen.



• Die ausgewählte Datei wird von UaExpert auf den TSN-Switch übertragen. Zur Kontrolle kann die zu installierende Datei durch Aufruf der Methode *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/Loading/PendingVersion/SoftwareRevision* überprüft werden. Diese muss mit der gerade übertragenen Datei übereinstimmen und lässt sich anhand des letzten Teils des Dateinamens ermitteln:

- <Bestellnummer>\*V<SoftwareRevision>.zip

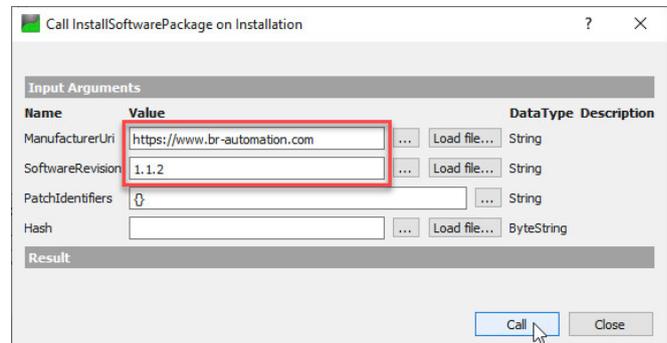
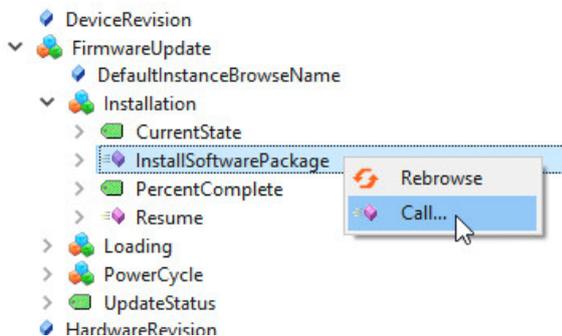
#### Beispiel

0ACST052.1\_FIRMWARE\_V1.0.0.zip → entspricht SoftwareRevision = 1.0.0

### • Installation

Im Objekt *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/Installation/InstallSoftwarePackage* einen Rechtsklick auf *Call* durchführen und die erforderlichen Parameter eintragen. Diese sind:

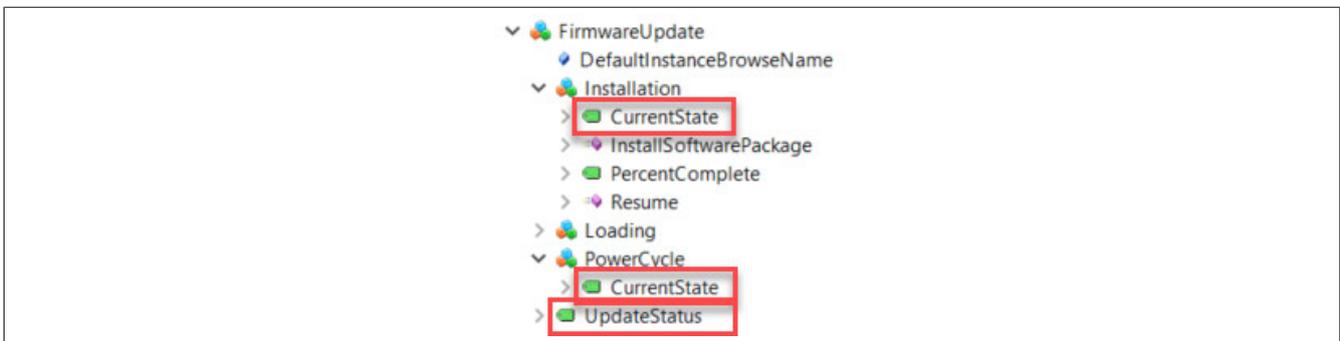
- ManufacturerURI: "https://www.br-automation.com"
- SoftwareRevision: entsprechend Beispiel oben



• Installation mit Klick auf *Call* abschließen und warten, bis die Installation abgeschlossen wurde. Der Status einer erfolgreichen Installation kann mit folgenden Parametern überprüft werden:

- Parameter *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/Installation/CurrentState* zeigt "Installing"
- Parameter *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/PowerCycle/CurrentState* zeigt "WaitingForPowerCycle"

Beide Parameter müssen den beschriebenen Wert anzeigen. Alternativ kann auch der Parameter *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/UpdateStatus* ausgewertet werden. Dieser sollte den Wert "[INFO] Installation successful, reboot required" enthalten.



### Information:

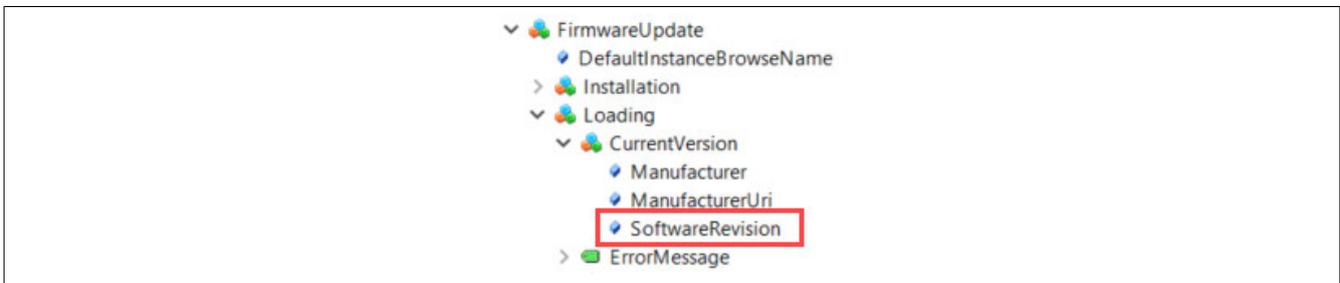
Die Firmware-Installation kann bis zu einer Minute dauern.

Der anschließende Neustart darf erst durchgeführt werden, wenn der Parameter *Root/Objects/DeviceSet/0ACST052.1/PowerCycle/CurrentState* den Status "WaitingForPowerCycle" anzeigt. Ansonsten wird das Firmware-Update abgebrochen und das Gerät bootet wieder mit der alten Version.

### • Neustart und Überprüfung

Einen Neustart durchführen. Dieser kann durch Aufruf der Methode *Root/Objects/DeviceSet/0ACST052.1/Configuration/Control/Reboot* oder durch ein Aus- und Einschalten der Spannungsversorgung erfolgen.

Nach dem Neustart kann die erfolgreiche Aktivierung des Firmwareupdates überprüft werden. Das geschieht durch Auslesen des Knotens *Root/Objects/DeviceSet/0ACST052.1/Loading/CurrentVersion/SoftwareRevision*. Die angezeigte Firmwareversion muss mit der SoftwareRevision der Firmwareupdate "\*.zip"-Datei identisch sein.



### • Fehlerbehandlung

Falls während des Firmwareupdates ein gravierender Fehler auftritt, muss dieser zurückgesetzt werden, da im Fehlerzustand kein weiterer Firmwareupdate möglich ist. Dies kann durch folgende Möglichkeiten geschehen:

- Quittierung des Fehlers mittels der Methode *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/Installation/Resume*
- Rücksetzen des Fehlerzustands durch einen Neustart. Dadurch wird wieder die ursprüngliche Firmware geladen.

Das fehlgeschlagene Firmwareupdate wird durch jede der beiden Methoden korrekt abgebrochen und beendet.

## 6 Features / Funktionalität

### 6.1 Verwendete Namespaces

Im TSN-Switch werden folgende Namespaces verwendet:

Index	Namespace URL	Beschreibung
0	http://opcfoundation.org/UA/	Adressraum für Typen und Objekte, welche in der OPC UA Spezifikation definiert sind
1	http://br-automation.com/OpcUa/0ACST052.1/<Seriennummer>/	Dieser Namespace-URL stellt den Adressraum des TSN-Switchs dar, auf dem der OPC UA Server läuft. Die <Seriennummer> entspricht der Seriennummer des TSN-Switchs
2	http://opcfoundation.org/UA/DI/	Adressraum für Typen und Objekte, welche in der OPC UA Companion Spezifikation für Geräteintegration (DI = Device Integration) definiert sind.
3	http://br-automation.com/OpcUa/BrDevice	Basis-Informationsmodell für B&R Feldgeräte
4	http://br-automation.com/OpcUa/io-system	Informationsmodell des TSN-Switchs

Die verwendeten Namespaces können auch im OPC UA Informationsmodell ausgelesen werden:

The screenshot shows the OPC UA Information Model tree on the left and the details of the selected 'NamespaceArray' object on the right.

**Information Model Tree (Left):**

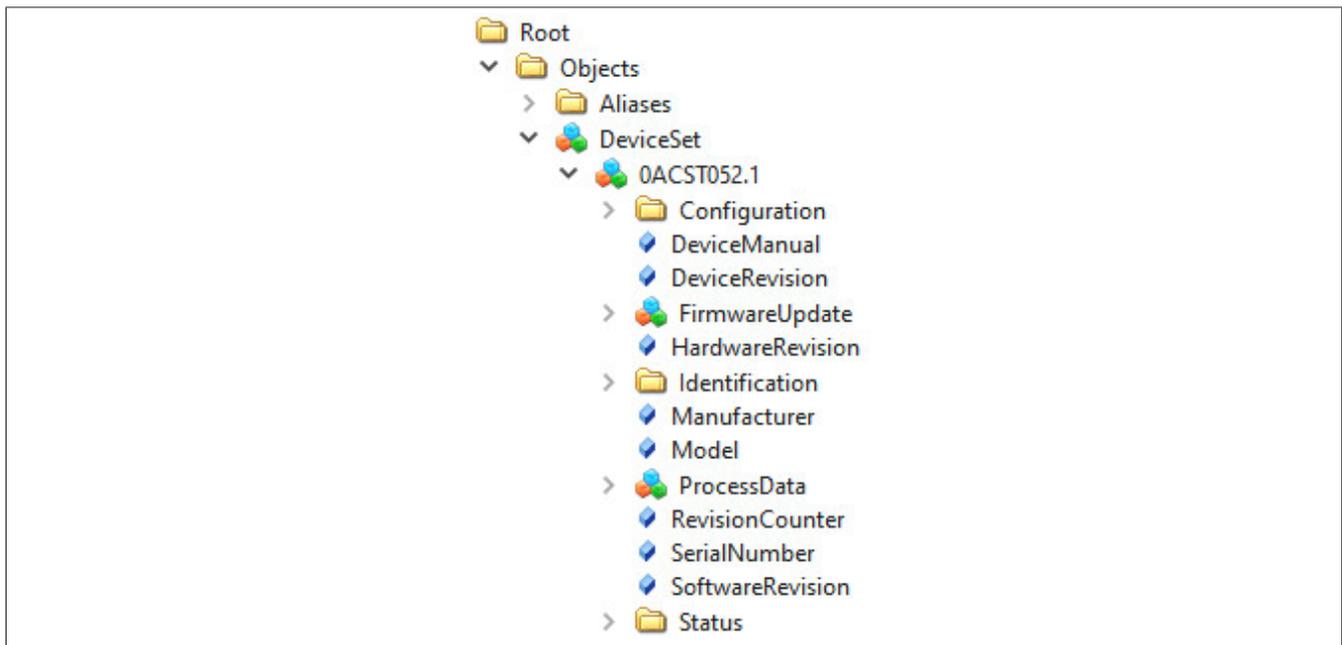
- Root
  - Objects
    - Aliases
    - DeviceSet
    - DeviceTopology
    - NetworkSet
    - Server
      - Auditing
      - Dictionaries
      - EstimatedReturnTime
      - GetMonitoredItems
      - LocalTime
      - NamespaceArray** (Selected)
      - Namespaces
      - PublishSubscribe

**Object Details (Right):**

- UserRolePermissions: RolePermissionType Array[2]
- AccessRestrictions: BadAttributeIdInvalid (0x80350000)
- Value:
  - SourceTimestamp: 25.03.2021 15:33:53.831
  - SourcePicoSeconds: 0
  - ServerTimestamp: 25.03.2021 15:33:53.831
  - ServerPicoSeconds: 0
  - StatusCode: Good (0x00000000)
  - Value: String Array[5]
    - [0]: http://opcfoundation.org/UA/
    - [1]: http://br-automation.com/OpcUa/0ACST052.1/
    - [2]: http://opcfoundation.org/UA/DI/
    - [3]: http://br-automation.com/OpcUa/BrDevice
    - [4]: http://br-automation.com/OpcUa/BC/io-system/
- DataType: String
  - NamespaceIndex: 0
  - IdentifierType: Numeric
  - Identifier: 12 [String]
  - ValueRank: 1 (OneDimension)

## 6.2 Geräteinformation

Unter dem Knoten *Root/Objects/DeviceSet/0ACST052.1* befinden sich weitere Knoten, durch die Basisinformationen des TSN-Switchs ausgelesen werden können:



Knotenname	Beschreibung
DeviceManual	URL, unter der weitere Informationen zum Modul zur Verfügung stehen
DeviceRevision bzw. Processdata/HardwareVariant	B&R Hardwarevariante
HardwareRevision	Hardwarerevision des TSN-Switchs
Manufacturer	Hersteller des TSN-Switchs
Model	Modulbezeichnung
RevisionCounter	Reserviert (immer -1)
SerialNumber	Vollständige Seriennummer als String
SoftwareRevision	Aktuelle Softwarerevision
Identification/ModuleID bzw. Processdata/ModuleID	Numerische Identifikationsnummer des Moduls
Processdata/SerialNumber	Seriennummer als 32 Bit Integer

## 6.3 Zeitsynchronisation und Zeitdomänen

Der TSN-Switch verfügt über 2 voneinander unabhängige Uhren, die mit unterschiedlichen Zeitdomänen synchronisiert werden können. Damit bekommen alle Netzwerkgeräte, welche zur gleichen Zeitdomäne synchronisiert sind, ein einheitliches Zeitverhalten. Das heißt, dass sowohl die Zeitwerte als auch die Frequenzen der Uhren miteinander abgestimmt werden. Dadurch lassen sich Aktivitäten auf diversen Geräten zeitlich exakt koordinieren und deren Zeitstempel in eine genaue Zeitabfolge bringen.

Für die Zeitsynchronisation am TSN-Switch kann entweder das Network Time Protocol (NTP) oder das IEEE 802.1AS-2020 Profil des Precision Time Protocol (PTP) verwendet werden.

Die beiden Uhren können wie folgt eingesetzt werden:

### WallClock

Die Wallclock entspricht der klassischen Systemuhr. Sie kann über NTP oder PTP mit der aktuellen UTC-Zeit synchronisiert und beispielsweise für Logging-Zeitstempel oder Zertifikatsvalidierung verwendet werden.

### WorkingClock

Die WorkingClock ist unabhängig von der UTC-Zeit und wird vor allem für das zeitgenaue Versenden der TSN-Ethernet-Frames verwendet. Im Vergleich zur WallClock wird bei der WorkingClock sichergestellt, dass nach der erstmaligen Synchronisation keine weiteren Sprünge im Zeitverlauf mehr erfolgen (z. B. durch Schaltsekunden, wie sie bei UTC-Zeit vorkommen). Um sicherzustellen, dass TSN-Ethernet-Frames ausreichend genau versendet werden, ist bei der WorkingClock die Anforderung an die Synchronisationsgenauigkeit viel höher. Aus diesem Grund steht für die WorkingClock nur PTP als Synchronisationsmethode zu Verfügung.

### Information:

**Es ist zu beachten, dass am TSN-Switch die PTP-Zeitsynchronisation für jede PTP-Zeitdomäne, die von verbundenen Netzwerkgeräten verwendet wird, aktiviert werden muss. Dies ist auch notwendig, wenn der TSN-Switch die entsprechende Domäne selbst nicht benutzt.**

## 6.4 Time Sensitive Networking (TSN)

Der TSN-Switch verfügt über 4 Ports, die Time Sensitive Networking (TSN) unterstützen (siehe [6.6 "Geräteeigenschaften"](#)). Zur Bereitstellung der TSN-Funktionalitäten sind am TSN-Switch folgende Standards implementiert:

- IEEE 802.1Q
- IEEE 802.1AS-2020 – Precision Time Protocol (PTP)
- IEEE 802.1Qbv
- IEEE 802.1Qav
- IEEE 802.1Qbu
- IEEE 802.3br

Die Nutzung der folgenden TSN-Funktionalitäten erfordert die Konfiguration des TSN-Switchs durch das NETCONF-Protokoll gemäß der hier aufgelisteten Standards und unter Nutzung der korrespondierenden YANG-Modelle. Diese Aufgabe kann durch geeignete Konfigurationswerkzeuge automatisiert und für den Anwender transparent erfolgen (siehe [7 "Konfiguration"](#)).

### 6.4.1 Frame-Forwarding

Geplante Kommunikation und speziell die TSN-Funktionalität erfordert, dass sich die richtigen Frames zum vorgegebenen Zeitpunkt in der korrekten Queue des vorbestimmten Ausgangsports befinden.

Um dies sicherzustellen, müssen entsprechende Weiterleitungsregeln in der Filtering Database (FDB) des TSN-Switchs eingetragen werden. Ein Eintrag in der FDB gibt dabei an, welche empfangenen Frames an welche Ports weitergeleitet werden müssen. Die Weiterleitung kann dabei auf unterschiedlichen Filtern beruhen. Beispielsweise können diese Regeln einzelne Zieladressen (Destination MAC-Adressen) oder VIDs betreffen. Schließlich ordnet das Portspezifische Priority Mapping, welches per NETCONF modifiziert werden kann, einen Frame einer entsprechenden Queue zu.

## 6.4.2 Zeitgesteuerte Kommunikation (Scheduled Traffic)

Bei der zeitgesteuerten Kommunikation werden Ethernet-Frames im Netzwerk zu festgelegten Zeitpunkten versendet. Dadurch lassen sich Kommunikationspfade im Netzwerk für festgelegte Zeiträume reservieren, um so die Einhaltung von Echtzeitanforderungen an den Datenaustausch garantieren zu können. Dies wird durch die Umsetzung der Standards IEEE 802.1Qbv und IEEE 802.1AS ermöglicht. Zur kollisionsfreien zeitgesteuerten Kommunikation ist eine erfolgreiche Zeitsynchronisation der WorkingClock (siehe Abschnitt 6.3 "Zeitsynchronisation und Zeitdomänen") erforderlich. Mit Hilfe dieser Zeitbasis steuert der TSN-Switch die Übertragung der Frames nach einem festgelegten Zeitplan, welcher in der sogenannten Gate-Control-List (GCL) im TSN-Switch hinterlegt ist. Entsprechend der Einträge in der GCL öffnet und schließt der TSN-Switch seine internen Queues periodisch zu den vorgegebenen Zeitpunkten.

Ein bereitstehender Frame wird dann übertragen, wenn er sich an erster Stelle einer geöffneten Queue befindet und eine vollständige Übertragung bis zum Schließen der Queue möglich ist. Wenn mehrere Queues gleichzeitig geöffnet sind, in denen sich Frames befinden, dann wird jener Frame in der Queue mit der höchsten Priorität übertragen.

## 6.4.3 Credit-based Shaping

Ein Credit-based Shaper (CBS) ist ein Mechanismus zur Begrenzung der Bandbreite für Ethernet-Frames bestimmter Prioritätsklassen. Dieser verhindert, dass ein Ethernet-Link durch Frames mit hoher Priorität dominiert wird und dadurch Frames mit niedrigerer Priorität nicht mehr weitergeleitet werden können. Der IEEE 802.1Qav Standard beschreibt die Umsetzung eines CBS.

Ein CBS ordnet einer Queue einen Creditwert zu, der beim Versenden von Frames aus der Queue reduziert wird. Die SendSlope definiert, wie viele Credits beim Versenden eines Frames mit bestimmter Größe verbraucht werden. Unterschreiten die Credits einer Queue den Wert 0, so wird diese Queue für eine bestimmte Zeit gesperrt und Frames aus den verbleibenden Queues (insbesondere auch Queues mit niedrigerer Priorität) können übertragen werden. Mit fortschreitender Zeit werden die Credits der Queues wieder erhöht. Durch Konfiguration der IdleSlope kann die maximale Bandbreite festgelegt werden. Diese gibt an, wie schnell sich die Credits wieder auffüllen, sodass die Queue mit höherer Priorität wieder für die Übertragung freigegeben wird. Credits können nur dann einen Wert größer 0 erreichen, wenn in der betreffenden Queue ein Frame zur Übertragung bereitsteht. Andernfalls kann maximal der Wert 0 erreicht werden.

CBS und Mechanismen zur zeitgesteuerten Kommunikation (siehe Abschnitt 6.4.2 "Zeitgesteuerte Kommunikation (Scheduled Traffic)") sind unabhängig voneinander und können kombiniert verwendet werden.

## 6.4.4 Frame Preemption

Durch Umsetzung der Standards IEEE 802.1Qbu und IEEE 802.3br stellt der TSN-Switch einen Frame Preemption Mechanismus zur Verfügung.

Dieser ermöglicht die Unterbrechung einer Frameübertragung auf einem Port, um den korrespondierenden Link für die Übertragung eines Expressframes freizugeben. Das kann einerseits zur Optimierung der Bandbreite genutzt werden, da die notwendigen Schutzbänder bei der Umschaltung der Zeitfenster stark reduziert werden können. Andererseits lässt sich dadurch die Latenz von Expressframes reduzieren, die ansonsten durch die Übertragung anderer, großer Frames lange verzögert werden könnten. Frame Preemption muss für jeden Port explizit konfiguriert werden und findet immer nur auf einem Link zwischen 2 benachbarten Netzwerkgeräten statt, die beide den Frame Preemption Standard unterstützen. Ein unterbrochener Frame kann am Nachbargerät erst dann weiterverarbeitet werden, wenn dieser dort wieder zusammengesetzt wurde.

Der Frame Preemption Mechanismus kann gemeinsam mit zeitgesteuerter Kommunikation (siehe Abschnitt 6.4.2 "Zeitgesteuerte Kommunikation (Scheduled Traffic)") eingesetzt werden.

## 6.5 Netzwerkmanagementprotokolle

Für das erweiterte Netzwerkmanagement unterstützt der TSN-Switch weitere Protokolle, die automatisch beim Hochlauf aktiviert werden.

### 6.5.1 Multiple Spanning Tree Protocol (MSTP)

Dieses Protokoll dient der logischen Auftrennung redundanter Verbindungen im Netzwerk, sodass Broadcast-Frames nicht mehrfach im Kreis gesendet werden können, was eine unnötige Belastung des Netzwerks darstellen würde. Durch Austausch von Konfigurationsnachrichten wird eine logische Baumtopologie erstellt, welche die Weiterleitung von Ethernet-Frames auf redundanten Pfaden verhindert. Im Falle von MSTP wird für alle vorhandenen Virtuellen Local Area Networks (VLANs) ein eigener logischer Baum aufgebaut.

Da sich die logischen Baumtopologien im Netzwerk dynamisch ändern können, sind diese für zeitgesteuerte Kommunikation ungeeignet. Daher ist es notwendig, Netzwerkpfade für zeitgesteuerte Kommunikation explizit mittels TSN-Konfiguration festzulegen. Das geschieht durch Konfiguration von Weiterleitungsregeln. Diese festgelegten Pfade werden nicht durch MSTP beeinflusst.

Detailinformationen zu MSTP können dem Standard IEEE 802.1Q entnommen werden. Die Konfiguration des MSTP Stacks oder Statusabfragen können via NETCONF durchgeführt werden. Die Konfigurationsparameter und Statuswerte sind dem entsprechenden YANG-Modell zu entnehmen.

### 6.5.2 Link Layer Discovery Protocol (LLDP)

LLDP wird dazu benutzt, um zwischen benachbarten Netzwerkgeräten Informationen zur Identität und zu unterstützten Funktionalitäten auszutauschen. Diese Informationen werden individuell für jeden Port gesammelt, an dem ein LLDP-fähiges Gerät angeschlossen ist.

Detailinformationen zu LLDP können dem Standard IEEE 802.1AB entnommen werden. Eine Statusabfrage ist via NETCONF, mit dem dazugehörigen YANG-Modell, möglich. Zu Diagnosezwecken sind einige der Statuswerte auch im OPC UA Informationsmodell aufgelegt (siehe dazu [8.1 "Port-Status"](#)).

## 6.6 Geräteeigenschaften

Die Ports des TSN-Switchs, deren Beschriftung auf der Vorderseite des TSN-Switchs (siehe Abschnitt [3.3 "Bedien- und Anschlusselemente"](#)), deren Bezeichnungen und TSN-Fähigkeit sind in der folgenden Tabelle aufgelistet.

Beschriftung	Bezeichnung im OPC UA Informationsmodell	Interne (LLDP, NETCONF)	Bezeichnung	TSN-fähig
ETH TSN 1	ETH1	sw0p2		Ja
ETH TSN 2	ETH2	sw0p3		Ja
ETH TSN 3	ETH3	sw0p4		Ja
ETH TSN 4	ETH4	sw0p5		Ja
ETH5	ETH5	sw0p6		Nein

### Information:

**Die internen Bezeichnungen sw0p1 und sw0ep werden jeweils für den Internen und den Management Port des TSN-Switchs verwendet. Diese haben keinen Bezug zu den externen Ports des TSN-Switchs.**

Die folgende Tabelle zeigt die Dimensionierung verschiedener Eigenschaften des TSN-Switchs. Wenn nicht explizit angegeben, gelten die angegebenen Werte global für den gesamten TSN-Switch.

Eigenschaft	Wert
Anzahl Filtering Database (FDB) Einträge	512
Maximale Anzahl VIDs	64
Anzahl Queues pro Port	8
Anzahl Gate Control List (GCL) Einträge pro Port	255

## 6.7 Port-Mirroring und Port-Isolation

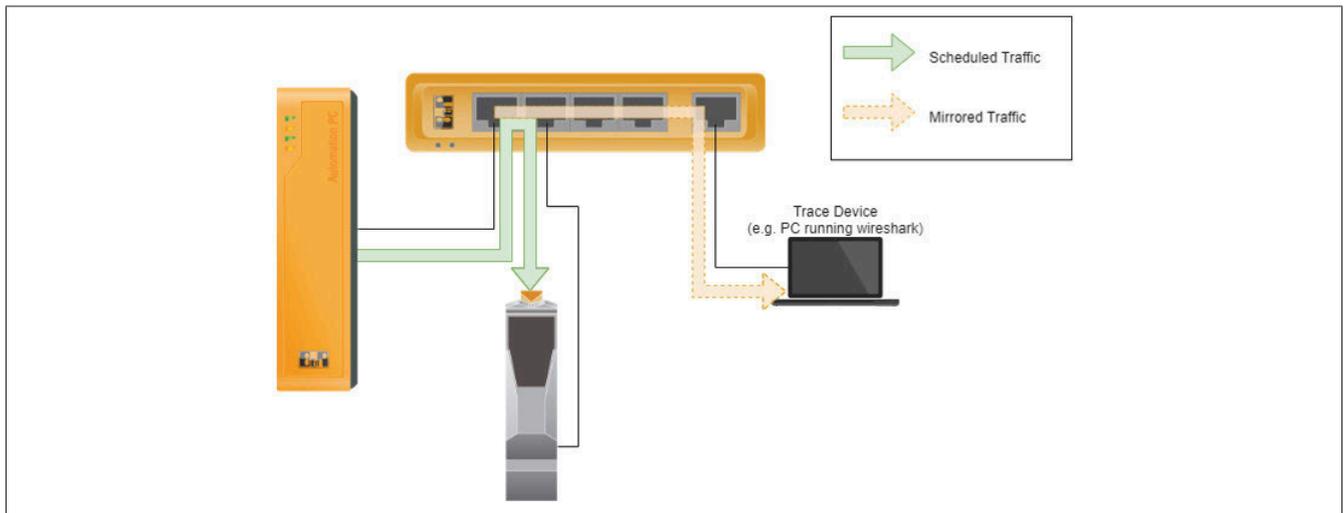
### Information:

Erst ab Firmwareversion 1.4.0

Das Port-Mirroring stellt eine Spezialvariante des Frame-Forwarding dar. Diese Funktionalität erlaubt es jeden einkommenden Ethernet-Frame eines Ports (Quell-Port), zusätzlich zum normalen Frame-Forwarding, zu duplizieren und über einen separaten Port (Ziel-Port) zu versenden.

Damit können übertragene Ethernet-Frames im Zuge einer Diagnose auf einem zusätzlich angeschlossenen Gerät aufgenommen und ausgewertet werden.

Im folgenden Beispiel wird gezeigt, wie die einkommenden Ethernet-Frames der geplanten Kommunikation zwischen APC und Bus Controller (Scheduled Traffic) dupliziert und zusätzlich an ein Trace Device weitergeleitet werden. (Mirrored Traffic)



Um eine derartige Diagnose zu vereinfachen und die duplizierten Ethernet-Frames von anderem Verkehr zu trennen gibt es die zusätzliche Funktionalität der Port-Isolation. Die Port-Isolation bietet die Möglichkeit den ausgehenden Standardverkehr auf einem ausgewählten Port zu deaktivieren. Dies verhindert sämtliche Ethernet-basierten Kommunikationen über diesen Port.

Folgende Limitierungen und Rahmenbedingungen sind bezüglich Port-Mirroring und Port-Isolation zu beachten:

- Es können nur einkommende Ethernet-Frames des Quell-Ports mittels Port-Mirroring weitergeleitet werden.
- Von einem Quell-Port ausgehend kann Port-Mirroring nur zu einem einzelnen Ziel-Port konfiguriert werden.
  - ⇒ Ein einzelner Ziel-Port kann jedoch sehr wohl für mehrere Quell-Ports verwendet werden. Auf Grund der Bandbreitenlimitierung beim Ziel-Port kann es dabei jedoch vorkommen, dass Ethernet Frames verworfen werden müssen.
- Port-Mirroring erfasst alle einkommenden Ethernet-Frames, außer jene mit einer Zieladresse (Destination MAC-Adresse) im Bereich 01:80:C2:00:00:00 bis 01:80:C2:00:00:1F
  - ⇒ Dieser Bereich inkludiert unter anderem die Protokolle PTP, LLDP und MSTP.
- Das Versenden über den Ziel-Port wird durch alle aktiven Ausgangsfunktionalitäten beeinflusst.
  - ⇒ Diese Funktionalitäten sind zum Beispiel Scheduled Traffic, Credit-based Shaping oder Frame Preemption.
- Wird die zusätzliche Funktionalität der Port-Isolation am Ziel-Port nicht verwendet, so werden über den Ziel-Port die duplizierten Ethernet-Frames und Ethernet-Frames der normalen Kommunikation versendet.
- Es gibt keine zeitlichen Garantien für die weitergeleiteten duplizierten Ethernet-Frames. Daher ist beispielsweise eine genaue zeitliche Vermessung der Sendezeitpunkte von Ethernet-Frames am Ziel-Port in den wenigsten Fällen sinnvoll.
- Sämtliche Ports des Gerätes (ETH1 bis ETH5) können sowohl als Quell-Port als auch als Ziel-Port konfiguriert werden.

# 7 Konfiguration

---

## 7.1 Konfiguration über OPC UA

### 7.1.1 Methoden

Die Konfiguration mittels OPC UA erfolgt, indem die gewünschten Konfigurationswerte auf entsprechende OPC UA Variablen Knoten geschrieben werden.

Die konfigurierten Werte werden erst durch den Aufruf der Methode *ApplyChanges* übernommen.

Position der Methoden im Informationsmodell: *Root/Objects/DeviceSet/0ACST052.1/Configuration/Control*

#### 7.1.1.1 ApplyChanges

Geänderte Werte werden erst durch einen Aufruf dieser Methode gespeichert und übernommen.

#### 7.1.1.2 RevertChanges

Die zuletzt mit *ApplyChanges* gespeicherten Werte werden wiederhergestellt.

#### 7.1.1.3 RestoreDefaultConfiguration

Die Default-Konfigurationswerte werden wiederhergestellt.

#### **Information:**

Durch den Aufruf der Methode werden die Default-Konfigurationswerte nur temporär in die Knoten geladen. Um die Default-Konfiguration zu Speichern bzw. zu Übernehmen ist zusätzlich ein Aufruf der Methode *ApplyChanges* notwendig.

#### 7.1.1.4 Reboot

Löst einen Neustart des TSN-Switchs aus.

## 7.1.2 Allgemeine Netzwerkkonfiguration

Die Konfiguration kann über das OPC UA Informationsmodell vorgenommen werden. Die entsprechenden Parameter befinden sich im Modell unter dem Knoten *Root/Objects/DeviceSet/0ACST052.1/Configuration/Network*.

Knotenname	Beschreibung
EnableDHCP	Aktiviert beziehungsweise deaktiviert die DHCP-Client-Funktionalität - Bei fehlender IP-Zuweisung durch einen DHCP-Server wird dem TSN-Switch eine zufällige Link Local Adresse aus dem Bereich 169.254.0.0/16 zugewiesen. IPv4LL (RFC3927). - Wenn der DHCP-Client aktiviert ist, werden die Parameter <i>Gateway</i> , <i>IP Address</i> , <i>Netmask</i> , sowie <i>Primary DNS</i> und <i>Secondary DNS</i> vom DHCP-Server bezogen.
Gateway	Konfiguration der Default-Gateway IP-Adresse - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, kann zusätzlich eine Gateway-Adresse vom DHCP-Server übermittelt werden. - Wenn der Parameter <i>Gateway</i> gesetzt ist, wird die manuelle Konfiguration verwendet und die vom DHCP-Server übermittelte Adresse ignoriert.
Hostname	Konfiguration des Hostnamens
IP-Address	Konfiguration einer statischen IP-Adresse - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, dann wird der Parameter ignoriert und die vom DHCP-Server übermittelte IP-Adresse verwendet.
Primary DNS Secondary DNS	Konfiguration eines primären bzw. sekundären DNS-Servers - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, können zusätzlich Adressen für DNS-Server vom DHCP-Server übermittelt werden. - Wenn mindestens 1 DNS-Server manuell gesetzt ist, wird die manuelle Konfiguration verwendet und die vom DHCP-Server übermittelten Adressen werden ignoriert.
Netmask	Einstellung der Subnetzmaske - Wenn der Parameter <i>EnableDHCP</i> gesetzt ist, wird dieser Parameter ignoriert und die vom DHCP-Server übermittelte Subnetzmaske verwendet.
EnableMulticastDNS	Aktiviert beziehungsweise deaktiviert Multicast DNS (mDNS) - In der Werkseinstellung ist mDNS aktiviert, um auch bei fehlender Netzwerkinfrastruktur den TSN-Switch über den Hostnamen ansprechen zu können.

Damit neue Konfigurationsdaten gespeichert werden, muss die Methode *Root/Objects/DeviceSet/0ACST052.1/Configuration/Control/ApplyChanges* aufgerufen werden.

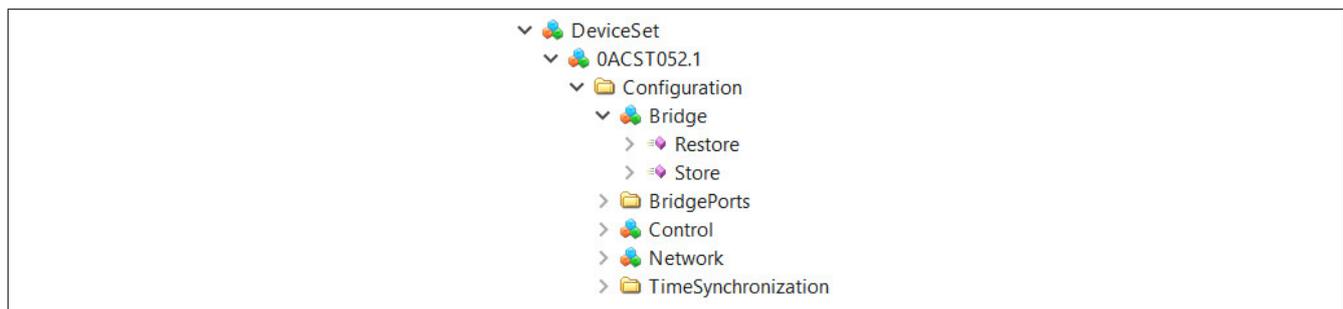
### Information:

Die Netzwerkkonfiguration wird erst beim Neustart des TSN-Switchs übernommen.

## 7.1.3 Bridge-Konfiguration

### 7.1.3.1 Methoden für Bridge-Konfiguration

Im OPC UA Informationsmodell werden 2 Methoden bereitgestellt, um die aktuelle Bridge-Konfiguration zu persistieren bzw. diese auf Werkseinstellungen zurückzusetzen.



### 7.1.3.2 Restore

Die aktuelle Bridge-Konfiguration wird gelöscht und auf Werkseinstellungen zurückgesetzt. Nach dem Ausführen dieser Methode ist ein Neustart des Geräts erforderlich.

### 7.1.3.3 Store

Die aktuelle Bridge-Konfiguration wird am Gerät persistiert.

## 7.1.4 Multiple Spanning Tree Protokoll

### Information:

Erst ab Firmwareversion 1.4.0

Unter dem Knoten *Root/Objects/DeviceSet/0ACST052.1/Configuration/BridgePorts/PORT\_NAME/MultipleSpanningTreeProtocol* im OPC UA Informationsmodell können Port spezifische Einstellungen konfiguriert werden.

Knotenname	Beschreibung
BDPU Filter enabled	Aktiviert oder deaktiviert den BPDU-Filter für den Port. Mögliche Werte : True                                   BPDU-Filter ist aktiv False                                   BPDU-Filter ist nicht aktiv

### Information:

Die Konfiguration wird erst durch den Aufruf der Methode *ApplyChanges* und anschließendem Neustart des TSN-Switchs übernommen.

## 7.1.5 Port-Mirroring und Port-Isolation

### Information:

Erst ab Firmwareversion 1.4.0

Die Funktionalitäten des Port-Mirroring und Port-Isolation können über das OPC UA Informationsmodell über die folgenden Knoten konfiguriert werden.

Position der Daten im Informationsmodell: *Root/Objects/DeviceSet/0ACST052/Configuration/BridgePorts/PORT\_NAME/PortMirroring*.

Knotenname	Beschreibung
IngressMirror	Auswahl des Ziel-Ports für die Port-Mirroring Funktionalität.
Isolation	Aktiviert die Port-Isolation für den Port. Mögliche Werte : True                                   Port-Isolation ist aktiv False                                   Port-Isolation ist nicht aktiv

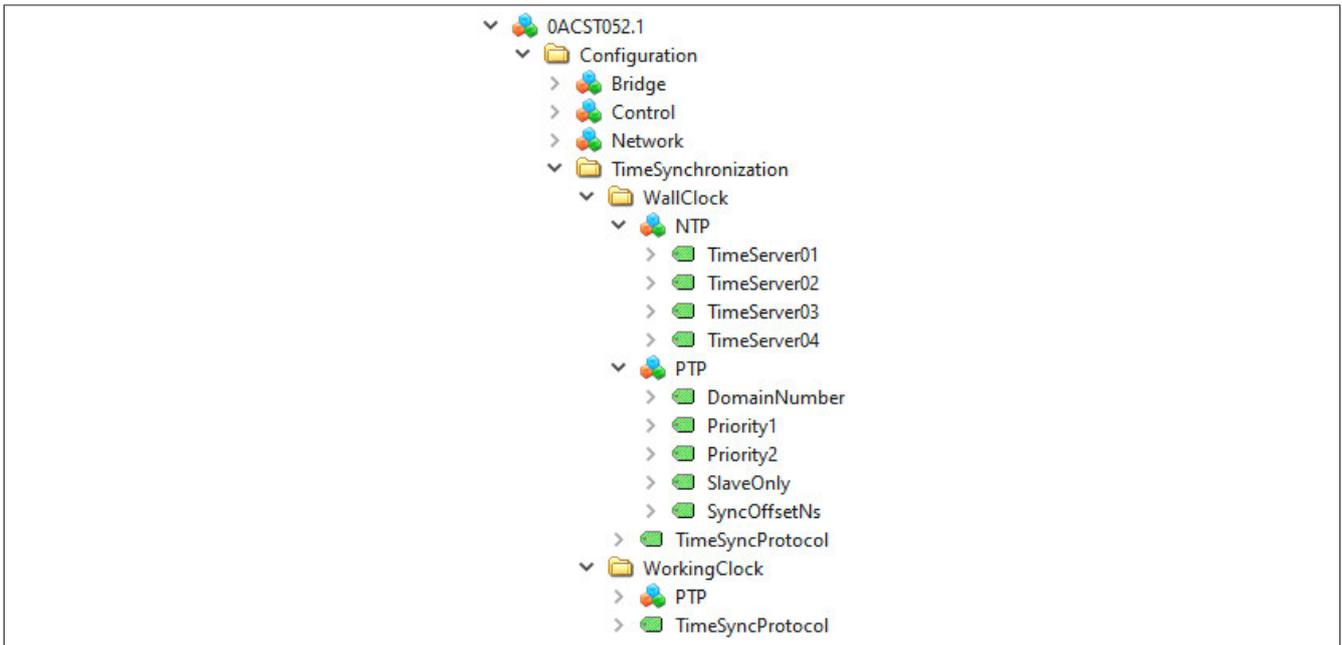
### Information:

Die Parameter zum Port-Mirroring und Port-Isolation werden erst durch den Aufruf der Methode *ApplyChanges* übernommen.

Die Parameter zum Port-Mirroring und Port-Isolation können nicht persistiert werden und werden daher durch jeden Neustart auf deren Standardwerte zurückgesetzt.

## 7.1.6 Zeitsynchronisation

Die verwendeten Protokolle zur Zeitsynchronisation müssen für die beiden Zeitdomänen *WallClock* und *WorkingClock* getrennt konfiguriert werden.



Position der Daten im Informationsmodell: *Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization*

### Information:

Die Parameter für die Zeitsynchronisation werden erst durch den Aufruf der Methode *ApplyChanges* und anschließendem Neustart des TSN-Switchs übernommen.

#### 7.1.6.1 NTP

Der NTP-Client kann für die *WallClock* aktiviert werden, indem der Konfigurationsparameter *TimeSyncProtocol* auf den Wert "2 (NTP)" eingestellt wird. Es können bis zu 4 Zeitserver angegeben werden. Optional ist es möglich, dass NTP-Server die Adressen durch den DHCP-Server zugewiesen bekommen. Wenn mehrere Zeitserver zur Verfügung stehen (entweder durch Konfiguration oder vom DHCP-Server bezogen), wird davon einer ausgewählt, der für die Zeitsynchronisation verwendet wird. Die anderen stehen als Redundanz zu Verfügung und werden verwendet, falls der aktuell aktive Zeitserver ausfällt.

Knotenname	Beschreibung
TimeServer0x	URL oder IP-Adresse von bis zu 4 Zeitservern, die manuell konfiguriert werden können. Bei Konfiguration von mehreren Zeitservern ist die Auswahl-Reihenfolge der Zeitserver nicht festgelegt.

### 7.1.6.2 PTP

PTP-Synchronisation kann sowohl für die *WallClock*, als auch die *WorkingClock* aktiviert werden. Dafür muss der Konfigurationsparameter *TimeSyncProtocol* der entsprechenden Uhr auf den Wert "1 (PTP)" eingestellt werden. Danach können weitere PTP-spezifische Parameter gesetzt werden, wie z. B. die Nummer der synchronisierten Zeitdomäne oder Parameter, die für die Auswahl der Zeitquelle (dem PTP-Grandmaster) relevant sind.

Knotenname	Beschreibung
DomainNumber	Nummer der Zeitdomäne, auf welche die betreffende Uhr synchronisiert werden sollte. Standardwerte WallClock 0 WorkingClock 20
Priority1	Übergeordneter Prioritätswert der lokalen Uhr bei der automatischen Auswahl des PTP-Grandmasters durch den Best Master Clock Algorithmus (BMCA), gemäß IEEE Std 802.1AS-2020. Ein kleinerer Wert repräsentiert eine höhere Priorität. Bei gleicher Priority1 werden weitere Faktoren ausgewertet (z. B. die Genauigkeit der Uhr). Wertebereich 1 bis 255 Standardwert 246
Priority2	Untergeordneter Prioritätswert der lokalen Uhr bei der automatischen Auswahl des PTP-Grandmasters durch den Best Master Clock Algorithmus (BMCA), gemäß IEEE Std 802.1AS-2020. Ein kleinerer Wert repräsentiert eine höhere Priorität. Dieser Wert ist nur relevant, wenn bei mindestens 2 Uhren sowohl Priority1, als auch alle Faktoren zur Uhrengenauigkeit identisch sind. Wertebereich 2 bis 255 Standardwert 247
SlaveOnly	Durch dieses Flag kann die lokale Uhr von der Master Clock Auswahl im Netzwerk ausgeschlossen werden. Wertebereich False Die lokale Uhr kann als PTP-Grandmaster ausgewählt werden. True Die lokale Uhr kann nicht als PTP-Grandmaster ausgewählt werden (Priority1 und Priority2 werden ignoriert) Standardwert False
SyncOffsetNs	Offsetwert in Nanosekunden zur Signalisierung, dass die erforderliche Synchronisationsgenauigkeit erreicht wurde. Wenn der Absolutwert des berechneten Offsets zum ausgewählten Grandmaster kleiner als dieser Parameter ist, so wird die korrespondierende Uhr als zeitsynchron angenommen. Wertebereich 0 bis $2^{32}$ Standardwert 1000

#### Information:

Bei der Nutzung von PTP in Kombination mit TSN-Zeitfenstern ist darauf zu achten, dass auch ein offenes Zeitfenster für den Netzwerkmanagementverkehr konfiguriert sein muss, damit PTP-Zeitsynchronisationsnachrichten nicht blockiert werden. Standardmäßig wird am Switch der Netzwerkmanagementverkehr der Verkehrsklasse 7 (höchste Priorität) zugeordnet.

### 7.1.6.3 TimeSyncProtocol

Die Konfigurationsparameter für NTP bzw. PTP sind nur dann gültig, wenn das entsprechende Synchronisationsprotokoll ausgewählt wurde.

Knotenname	Beschreibung
TimeSyncProtocol	Über diesen Parameter kann die Synchronisation der jeweiligen Uhr aktiviert bzw. das Synchronisationsprotokoll ausgewählt werden. Mögliche Werte: 0 Kein Synchronisationsprotokoll ausgewählt 1 PTP-Protokoll ausgewählt 2 NTP-Protokoll ausgewählt

## 7.2 Integration im IT-Netzwerk

Beim Hochlauf des TSN-Switchs wird automatisch der Multiple Spanning Tree Protocol (MSTP) Stack gestartet (siehe 6.5.1 "Multiple Spanning Tree Protocol (MSTP)"). Bei der Ausführung dieses Stacks werden Konfigurationsnachrichten zwischen Netzwerkgeräten ausgetauscht, welche mittels Bridge Protocol Data Unit (BPDU) Frames übertragen werden.

Diese Konfigurationsdaten können die logische Topologie eines Netzwerks beeinflussen, was insbesondere im Fehlerfall oder im Falle bewusster Manipulation zu unerwünschtem Verhalten im Netzwerk führen kann. Um derartigen Problemen vorzubeugen, unterstützen viele handelsübliche Switches sogenannte BPDU-Filter, welche auf einzelne Ports angewandt werden können. Einerseits können diese Filter dazu genutzt werden, um BPDU-Pakete zu verwerfen. Andererseits ist es möglich, den Port, mit dem das verursachende Gerät verbunden ist, zu sperren.

Bei der Integration des TSN-Switchs in ein IT-Netzwerk sind die Vorgaben der IT-Administration zu beachten, damit es zu keinen Störungen kommt, z. B. durch automatischen Ausschluss des Ports, an dem der TSN-Switch angeschlossen wurde. Sind im IT-Netzwerk keine BPDU-Pakete erlaubt, so sollte an dem IT-Switch, welcher für den TSN-Switch als Zugang zum IT-Netzwerk dient, ein BPDU-Filter eingestellt werden, der entsprechende Pakete an der Weiterleitung hindert. Siehe 7.1.4 "Multiple Spanning Tree Protokoll".

## 7.3 Konfiguration über NETCONF

Der TSN-Switch unterstützt das zentrale Konfigurationsmodell nach dem Standard IEEE 802.1Qcc. Dabei werden sogenannte YANG-Modelle (IEEE 802.1Qcp) für die Darstellung der Konfigurations- und Statusparameter verwendet. Als Konfigurations- und Abfrageprotokoll wird NETCONF unterstützt. Die verwendeten YANG-Modelle entsprechen den aktuellen Versionen der entsprechenden Standards wie IEEE 802.1Qcw. Der TSN-Switch kann mit jedem Netzwerkkonfigurationstool, welches diesen Standards genügt, konfiguriert werden.

### 7.3.1 Konfiguration mittels Automation Studio

#### **Information:**

**Erst ab Firmwareversion 1.4.0**

Um sich nicht direkt mit dem NETCONF-Protokoll befassen zu müssen, bietet Automation Studio ein einfaches Werkzeug für die TSN-Netzwerkkonfiguration. Dazu ist die Installation des OPC UA FX Technologiepakets entsprechend der Automation Studio Hilfe erforderlich.

Wenn das OPC UA FX Technologiepaket installiert ist, befindet sich eine schrittweise Anleitung zur Nutzung von Automation Studio für die TSN-Netzwerkkonfiguration im Abschnitt "Kommunikation > OPC UA FX > TSN Netzwerkkonfiguration" der Automation Help.

#### **Information:**

**Für die TSN-Netzwerkkonfiguration wird ein OPC UA FX Technologiepaket  $\geq 1.1.0$  benötigt.**

### 7.3.2 Konfiguration mit TTTech Slate XNS

Slate XNS der Firma TTTech ist eine browserbasierte Software, mit der sich Topologien modellieren und Konfigurationen für TSN-Netzwerke erstellen lassen. Die Offline-Netzwerkkonfiguration wird über eine Benutzeroberfläche ermöglicht, die eine Topologieansicht oder einen tabellenbasierten Editor bietet. Netzwerkkomponenten werden dabei mit Hilfe offener YANG-Standardmodelle konfiguriert und per NETCONF übertragen.

Die Verwendung des TTTech Slate XNS Tools ist in der Evaluierungsversion (maximal 5 Netzwerkteilnehmer) kostenfrei. Der Zugang für den Download des TTTech Slate XNS Tools kann unter der Email-Adresse [slatexns@tttech-industrial.com](mailto:slatexns@tttech-industrial.com) beantragt werden.

#### **Information:**

**Als Mindestversion ist Slate XNS  $\geq 2.3$  zu verwenden.**

## 8 Status

Das OPC UA Informationsmodell des TSN-Switchs zeigt Statusinformationen, die der Information beziehungsweise Diagnose von auftretenden Funktionsstörungen dienen sollen. Diese sind:

- [Port-Status](#)
- [Zeitsynchronisation](#)
- [Netzwerk](#)

### 8.1 Port-Status

Die entsprechenden Knotennamen befinden sich im OPC UA Informationsmodell unter den Knoten *Root/Objects/DeviceSet/0ACST052.1/Status/BridgePorts*. Für jeden Port des TSN-Switchs befindet sich unter diesem Pfad ein Eintrag mit der Bezeichnung des Ports selbst (*ETHx*). Dieser entspricht der Beschriftung, die an der jeweiligen RJ45-Buchse angebracht ist. Die folgende Tabelle listet die für jeden Port verfügbaren Statusinformationen.

Knotenname		Beschreibung
InternalName		Systeminterner Name der Schnittstelle.
<b>FrameStatistics/</b>		
FcsErrorFrameCount		Anzahl der am jeweiligen Port empfangenen Ethernet-Frames mit fehlerhafter Ethernet FCS (Frame Check Sequence)
GeneralRxErrorFrameCount		Anzahl der am jeweiligen Port eingegangenen Ethernet-Frames, die aufgrund switchinterner Fehler nicht empfangen werden konnten.
GeneralTxErrorFrameCount		Anzahl der am jeweiligen Port zu sendenden Ethernet-Frames, die aufgrund switchinterner Fehler nicht gesendet werden konnten.
RxFrameCount		Anzahl der am jeweiligen Port erfolgreich empfangenen Ethernet-Frames.
SizeErrorFrameCount		Anzahl der am jeweiligen Port empfangenen Ethernet-Frames, die aufgrund ungültiger Länge (< 64 Byte oder > max. Ethernet Framelänge) verworfen wurden.
TxFrameCount		Anzahl der am jeweiligen Port erfolgreich gesendeten Ethernet-Frames.
<b>LinkPartner/</b>		
ChassisId		Bezeichnung der "Chassis"-Komponente des angeschlossenen Geräts, z. B. die MAC-Adresse.
ManagementAddress		Management-Adresse des angeschlossenen Geräts, z. B. die IP-Adresse.
PortId		Bezeichnung der "Port"-Komponente des angeschlossenen Geräts, z. B. interner Schnittstellename.
<b>LinkProperties/</b>		
Duplex		Duplexmodus des Ports. Mögliche Werte: Full                                      Port arbeitet im Full-Duplex Modus Half                                        Port arbeitet im Half-Duplex Modus Kein Eintrag                              Verbindung ist nicht aktiv
LinkStatus		Status der Verbindung. Mögliche Werte: UP    Verbindung ist aktiv DOWN                                        Verbindung ist nicht aktiv
Speed		Geschwindigkeit der Verbindung. Mögliche Werte: 100Mb/s                                    Verbindung arbeitet mit 100 Mbit/s 1000Mb/s                                    Verbindung arbeitet mit 1000 Mbit/s Kein Eintrag                                Verbindung ist nicht aktiv
<b>MultipleSpanningTreeProtocol</b>		
BPDU-Filter enabled		Status des BPDU-Filters. Mögliche Werte: True                                         BPDU-Filter ist aktiv False                                        BPDU-Filter ist nicht aktiv
<b>PortMirroring<sup>1)</sup></b>		
MirroringActive		Status der Port-Mirroring Funktionalität des Ports. Mögliche Werte: True                                         Port-Mirroring ist aktiv False                                        Port-Mirroring ist nicht aktiv

1) Erst ab Firmwareversion 1.4.0

Position der Daten im Informationsmodell: *Root/Objects/DeviceSet/0ACST052/Status/BridgePorts/PORT\_NAME/PortMirroring*

## 8.2 Zeitsynchronisation

Der Zustand der Zeitsynchronisierung kann über die Knoten im Objekt *Root/Objects/DeviceSet/0ACST052.1/Status/TimeSynchronization* abgefragt werden. Entsprechende Informationen stehen sowohl für die *WallClock*, als auch für die *WorkingClock* zur Verfügung.

Knotenname	Beschreibung
<b>WallClock/NTP/</b>	
SyncOK	Status der NTP-Synchronisation der WallClock. Mögliche Werte: True Die WallClock ist mit einem Zeitserver synchronisiert False Die WallClock ist mit keinem Zeitserver synchronisiert
TimeServer	URL oder IP-Adresse des Zeitservers, mit dem die WallClock synchronisiert wird.
<b>WallClock/PTP/</b>	
ClockIdentity	Eindeutiger Identifikator der PTP-Instanz der WallClock.
GrandmasterIdentity	Identität der PTP-Instanz, die im Netzwerk als Grandmaster für die WallClock dient.
OffsetFromMaster	Berechnete Zeitabweichung in 1/65536 Nanosekunden <sup>1)</sup> der lokalen WallClock zur Uhr des Grandmasters.
ParentPortIdentity	Identität des Ports jenes Nachbargeräts, über den die PTP-Synchronisationsnachrichten zur lokalen WallClock PTP-Instanz gesendet werden. Die Identität ist als Byte-String dargestellt. Wenn die lokale WallClock die Grandmaster-Instanz ist, entspricht dieser String der <i>ClockIdentity</i> gefolgt von 2 Null-Bytes.
<b>WallClock/PTP/ETHx/</b>	
PortIdentity	Eindeutiger Port Identifikator des Ethernet Ports <b>ETHx</b> bei aktivierter PTP-Synchronisation der WallClock an diesem Port. x korrespondiert mit der Nummer des Ports am Gehäuse des TSN-Switchs.
PortState	Status der WallClock PTP-Synchronisation am Ethernet Port <b>ETHx</b> . Mögliche Werte: 3 Port ist deaktiviert 6 Port ist Master für die WallClock 7 Port ist passiv 9 Port ist Slave für die WallClock  Detailinformationen siehe IEEE 802.1AS – 2020, Tabelle 14-7.
<b>WorkingClock/PTP/</b>	
ClockIdentity	Eindeutiger Identifikator der PTP-Instanz der WorkingClock.
GrandmasterIdentity	Identität der PTP-Instanz, die im Netzwerk als Grandmaster für die WorkingClock dient.
OffsetFromMaster	Berechnete Zeitabweichung in 1/65536 Nanosekunden <sup>1)</sup> der lokalen WorkingClock zur Uhr des Grandmaster.
ParentPortIdentity	Identität des Ports jenes Nachbargeräts, über den die PTP-Synchronisationsnachrichten zur lokalen WorkingClock PTP-Instanz gesendet werden. Die Identität ist als Byte-String dargestellt. Wenn die lokale WorkingClock die Grandmaster-Instanz ist, entspricht dieser String der <i>ClockIdentity</i> gefolgt von 2 Null-Bytes.
<b>WorkingClock/PTP/ETHx/</b>	
PortIdentity	Eindeutiger Port Identifikator des Ethernet Ports <b>ETHx</b> bei aktivierter PTP-Synchronisation der WorkingClock an diesem Port. x korrespondiert mit der Nummer des Ports am Gehäuse des TSN-Switchs.
PortState	Status der WorkingClock PTP-Synchronisation am Ethernet Port <b>ETHx</b> . Mögliche Werte: 3 Port ist deaktiviert 6 Port ist Master für die WorkingClock 7 Port ist passiv 9 Port ist Slave für die WorkingClock  Detailinformationen siehe IEEE 802.1AS – 2020, Tabelle 14-7.

1) Wert 65536 = 1 Nanosekunde.

## 8.3 Netzwerk

Die aktuell verwendete Netzwerkkonfiguration kann über die Knoten im Objekt *Root/Objects/DeviceSet/0ACST052.1/Status/Network* ausgelesen werden.

Knotenname	Beschreibung
CurrentDNS	Aktuell verwendete DNS-Server. Der String kann mehrere Einträge enthalten, wenn mehrere DNS-Server zur Verfügung stehen.
CurrentGateway	Aktuell verwendeter Default-Gateway
CurrentHostname	Aktuell verwendeter Hostname
CurrentIPConfig	Aktuelle IP-Konfiguration. Der String kann mehrere Einträge enthalten, falls mehrere IP-Adressen existieren (z. B. eine durch Drücken des Resetstasters hinzugefügte temporäre IP-Adresse).

# 9 Cyber-Security

---

Dieses Kapitel gibt eine kurze Einführung in das Thema der Cyber-Security. Die Beschreibung der Begriffe erfolgt dabei nur auf sehr allgemeiner Ebene. Daher können unter einem allgemeinen Begriff je nach Situation eine Reihe unterschiedlicher Aspekte gemeint sein.

Geräte werden mit Werkseinstellungen ausgeliefert. Das bedeutet, dass normalerweise weder Gerätefunktionalität noch Sicherheitseinstellungen konfiguriert sind. Um die Inbetriebnahme dieser Geräte sicher zu gestalten, sollte daher dafür gesorgt werden, dass sie vorerst nur in einer vertrauenswürdigen Umgebung benutzt werden. Das kann z. B. erreicht werden, indem das Maschinennetzwerk vom restlichen Unternehmensnetzwerk getrennt ist, oder die Geräte direkt mit dem zur Konfiguration benutzten PC verbunden werden.

OPC UA over TSN ermöglicht IT-OT konvergente Netzwerke, in denen man nicht davon ausgehen kann, dass alle Netzwerkteilnehmer vertrauenswürdig sind. Das setzt keinen bewussten Angriff voraus, sondern bereits Fehlkonfiguration von Steuerungen außerhalb des eigentlichen Maschinennetzwerks könnten zu unbeabsichtigten Störungen führen.

Fragen der Cyber-Security spielen daher in OPC UA over TSN eine wichtige Rolle und beide Basistechnologien, das heißt, sowohl OPC UA als auch TSN, enthalten alle dafür notwendigen Mechanismen.

## Security-Relevante Fehler und Benachrichtigungen

Cyber-Security lebt von einer offenen Fehlerkultur. Fehler einer Geräte-Firmware, die z. B. unberechtigten Zugriff erlauben, werden von B&R aktiv verfolgt und behandelt. Kritische Sicherheitslücken und deren Behebung werden gesammelt unter <https://www.br-automation.com/en/service/cyber-security/> zur Verfügung gestellt.

### Information:

**Alle Fehler, die die Sicherheit von B&R Geräten betreffen, sollen unverzüglich an die oben angegebene Webseite gemeldet werden.**

## 9.1 Grundbegriffe und Grundlagen

### 9.1.1 Verschlüsselung

Ziel der Verschlüsselung ist es, schützenswerte Daten für Außenstehende unlesbar zu machen. Selbst wenn ein Angreifer Zugriff auf die Daten hat, z. B. indem er mit Hilfe von Werkzeugen den Datenverkehr mitverfolgt, sollte es für ihn unmöglich sein, daraus wertvolle Informationen abzuleiten.

Zudem wird bei der Verschlüsselung unterschieden, ob Daten auf einem Computer, Gerät oder Datenträger gespeichert bleiben, oder ob sie über ein Kommunikationsmedium übertragen werden. Die grundlegenden Mechanismen sind in allen Fällen ähnlich.

Der Industriestandard für die Verschlüsselung ist die AES-Familie (Advanced Encryption Standard) und arbeitet mit Schlüssellängen von 128 oder 256 Bit. Sowohl OPC UA, als auch NETCONF unterstützen diesen Standard.

### 9.1.2 Integrität

Ein Angreifer muss geheime Daten nicht unbedingt entschlüsseln, um z. B. Störungen im Ablauf einer Maschine hervorzurufen. Vielmehr ist es oft schon ausreichend Daten zu verfälschen. Das gelingt selbst dann, wenn Daten verschlüsselt und eigentlich unlesbar sind.

Um diese Bedrohung zu verhindern, werden Daten daher um eine digitale Signatur erweitert. Die ist ähnlich einer CRC-Prüfsumme (Cyclic Redundancy Check). Die Algorithmen sind aber explizit darauf ausgelegt Verfälschungen durch einen Angreifer zu erkennen.

Häufig reicht es aus, lediglich die Integrität der Daten sicherzustellen zu können, ohne sie zu verschlüsseln zu müssen. Anwendungsfälle dafür sind zum Beispiel:

- Die Diagnose des Datenverkehrs mit Hilfe von Werkzeugen wie Wireshark. Die digitale Signatur verhindert die Diagnose nicht, wohingegen eine zusätzliche Verschlüsselung die Daten unlesbar und für eine Diagnose unbrauchbar machen würde.
- Sicherstellung der Integrität der Firmware von Geräten. Die Firmware bleibt auslesbar, es ist aber für einen Angreifer trotzdem nicht möglich Veränderungen durchzuführen.

Der Industriestandard für Signaturalgorithmen ist die SHA-Familie (Secure Hash Algorithm), mit Schlüssellängen von z. B. 256 Bit. Sowohl OPC UA, als auch NETCONF unterstützen diese Algorithmen.

### 9.1.3 Symmetrische und asymmetrische Schlüssel

Algorithmen wie die AES-Familie werden als "symmetrisch" bezeichnet, weil ein einziger Schlüssel sowohl für die Verschlüsselung als auch die Entschlüsselung verwendet wird. Falls 2 Geräte miteinander Daten verschlüsselt austauschen wollen, muss also zuvor sichergestellt sein, dass beide Geräte denselben Schlüssel besitzen. Das ist in der Praxis nicht immer einfach durchzuführen.

Algorithmen wie die RSA-Familie (benannt nach den Erfindern Rivest, Shamir und Adleman) werden dagegen als "asymmetrisch" bezeichnet. Diese Algorithmen verwenden 2 unterschiedliche Schlüsseln, um das Problem des Schlüsselaustauschs zu vereinfachen.

- Ein "privater" Schlüssel dient dazu, Daten zu entschlüsseln, bzw. die Signatur zu erstellen.
- Ein "öffentliche" Schlüssel dient dazu, Daten zu verschlüsseln, bzw. die Authentizität einer Signatur zu prüfen.

Der öffentliche Schlüssel darf – und soll – von jedem lesbar sein. Geräte, die miteinander kommunizieren wollen, stellen einander gegenseitig ihre öffentlichen Schlüsseln zur Verfügung. Da der private Schlüssel nicht übermittelt werden muss, kann er auf einfache Weise im Gerät geheim gehalten werden.

Ablauf der Datenübertragung mit asymmetrischen Algorithmen:

- Der Sender A signiert die Daten mit seinem privaten Schlüssel  $P_A$ .
- Der Sender A verschlüsselt die signierten Daten mit dem öffentlichen Schlüssel  $\ddot{O}_B$  des Empfängers B.
- Der Empfänger B entschlüsselt die verschlüsselten und signierten Daten mit seinem privaten Schlüssel  $P_B$ .
- Der Empfänger B prüfte die Echtheit der signierten Daten mit dem öffentlichen Schlüssel  $\ddot{O}_A$  des Senders A.

Der Nachteil der asymmetrischen Algorithmen besteht im wesentlich größeren Rechenaufwand. Da für RSA Schlüssel mit einer Länge von 2048 Bit verwendet werden, sind sie für den Austausch großer Datenmengen nicht geeignet. Symmetrische Algorithmen wiederum verwenden nur Schlüssellängen von 256 Bit, wodurch sich die Datenübertragung wesentlich einfacher durchführen lässt.

In der Praxis wird daher oft eine Kombination beider Verfahren eingesetzt. Asymmetrische Algorithmen werden verwendet, um einen, bloß temporär für die Kommunikationssitzung erzeugten, symmetrischen Schlüssel auszutauschen. Die eigentliche Kommunikation danach wird mit symmetrischen Algorithmen durchgeführt.

### 9.1.4 Asymmetrischer Schlüsselaustausch

Obwohl ein öffentlicher Schlüssel von jedem gelesen und benutzt werden darf, bedeutet das nicht, dass keine Vorsicht bei dessen Verwendung nötig wäre. Ein Sender A muss z. B. sicher sein, dass der öffentliche Schlüssel  $\bar{O}_B$  auch tatsächlich dem gewünschten Empfänger B gehört. Ohne eine derartige Versicherung wäre nämlich der folgende, als "Man-in-the-Middle" bekannte, Angriff möglich, bei dem sich der Angreifer in die Kommunikation einklinkt:

Sender A ↔ Angreifer C ↔ Empfänger B

- Der Sender A signiert die Daten mit seinem privaten Schlüssel  $P_A$ .
- Der Sender A verschlüsselt die signierten Daten fälschlicherweise mit dem öffentlichen Schlüssel  $\bar{O}_C$  des Angreifers C, an Stelle des öffentlichen Schlüssels  $\bar{O}_B$  des Empfängers B.
- Der Angreifer C entschlüsselt die verschlüsselten und signierten Daten mit seinem privaten Schlüssel  $P_C$ .
- Der Angreifer C liest die Daten und verfälscht sie eventuell.
- Der Angreifer C signiert die Daten mit seinem privaten Schlüssel  $P_C$ .
- Der Angreifer C verschlüsselt die signierten Daten mit dem öffentlichen Schlüssel  $\bar{O}_B$  des Empfängers B.
- Der Empfänger B prüfte die Echtheit der signierten Daten fälschlicherweise mit dem öffentlichen Schlüssel  $\bar{O}_C$  des Angreifers C, an Stelle des öffentlichen Schlüssels  $\bar{O}_A$  des Senders A.

Der Angreifer kann ebenso die umgekehrte Kommunikationsrichtung mitlesen und verfälschen.

Um sich vor einem Man-in-the-Middle-Angriff zu schützen existieren im Wesentlichen 3 Möglichkeiten:

- 1) Sicherstellen, dass zu Beginn des Kommunikationsaufbaus kein Angreifer anwesend sein kann, z. B. indem die Maschine vom Intra- und Internet getrennt ist. Die ausgetauschten Schlüssel sind danach sicher, auch wenn die Maschine wieder mit dem Intra- und Internet verbunden wird.
- 2) Sicherstellen, dass der empfangene öffentliche Schlüssel  $\bar{O}_X$  tatsächlich zum Kommunikationsteilnehmer X gehört. Das ist möglich, wenn es eine vertrauenswürdige dritte Stelle gibt, die garantiert, dass dieser Zusammenhang besteht.
- 3) Die öffentlichen Schlüssel auf eine geeignete Weise auf die jeweiligen Geräte verteilen. Dieser Weg bedeutet in der Regel manuelle Arbeit eines Benutzers oder Administrators.

NETCONF unterstützt – bei Verwendung des Kommunikationsprotokolls SSH (Secure Shell) – den ersten und dritten Weg. OPC UA unterstützt den zweiten und dritten Weg.

### 9.1.5 Vertrauenshierarchie und Autorität

Das auch im Internet angewandte Übertragungsprotokoll HTTPS (HyperText Transport Protocol Secure) basiert darauf, dass eine vertrauenswürdige dritte Stelle dafür bürgt, dass der öffentliche Schlüssel  $\bar{O}_X$  zu dem Kommunikationsteilnehmer X gehört.

Diese Garantie ist zusammen mit weiteren Informationen in einem sogenannten "Zertifikat" enthalten. Das Format der Zertifikate wurde durch die ITU (International Telecommunication Union) standardisiert und folgt dem Standard X.509. Die "bürgende" Stelle wird dementsprechend als Zertifizierungsstelle (engl. "Certificate Authority" CA) bezeichnet.

Ein Web-Browser akzeptiert z. B. das Zertifikat für <https://www.br-automation.com>, weil es beweisbar von der Zertifizierungsstelle "GlobalSign" ausgestellt wurde und der Web-Browser dieser Zertifizierungsstelle vertraut. Das Zertifikat von <https://www.br-automation.com> muss dafür vor Verfälschung geschützt sein, was wiederum über die [symmetrischen und asymmetrischen Verfahren](#) sichergestellt wird.

Während sich eine CA selbst durch eine höhere CA Zertifizieren lässt, gibt es einige CAs, denen Web-Browser und andere Geräte per Default vertrauen und die fest vorgegeben sind; die sogenannten Root-CAs. Diese stellen die höchste Certificate Authority im Internet dar.

- Eine Root-CA R erzeugt ein Zertifikat  $Z_R$  für sich selbst, das ihren öffentlichen Schlüssel  $\bar{O}_R$  enthält.
- Die Root-CA R signiert das Zertifikat  $Z_R$  mit ihrem privaten Schlüssel  $P_R$  (self-signed Certificate).
- Ein Gerät A (oder Web-Browser) importiert das Zertifikat  $Z_R$  und kann damit überprüfen, ob weitere Zertifikate gegebenenfalls von der Root-CA R ausgestellt wurden.
- Die Root-CA R erstellt ein Zertifikat  $Z_A$  für das Gerät A, das dessen öffentlichen Schlüssel  $\bar{O}_A$  enthält.
- Die Root-CA R signiert das Zertifikat  $Z_A$  mit ihrem privaten Schlüssel  $P_R$ .
- Ein Gerät B (oder Web-Browser) importiert das Zertifikat  $Z_R$  und kann damit überprüfen, ob weitere Zertifikate gegebenenfalls von der Root-CA R ausgestellt wurden.

- Die Root-CA R erstellt ein Zertifikat  $Z_B$  für das Gerät B, das dessen öffentlichen Schlüssel  $\ddot{O}_B$  enthält.
- Die Root-CA R signiert das Zertifikat  $Z_B$  mit ihrem privaten Schlüssel  $P_R$ .

Sobald Gerät A und Gerät B eine Kommunikationsverbindung eingehen, übermitteln sie einander zuerst ihre Zertifikate:

- Der Sender A sendet sein Zertifikat  $Z_A$  an den Empfänger B.
- Der Empfänger B überprüft die Integrität des Zertifikats  $Z_A$ , an Hand des öffentlichen Schlüssels  $\ddot{O}_R$ , das er dem Zertifikat  $Z_R$  der Root-CA R entnimmt.
- Der Empfänger B sendet sein Zertifikat  $Z_B$  an den Sender A.
- Der Sender A überprüft die Integrität des Zertifikats  $Z_B$ , an Hand des öffentlichen Schlüssels  $\ddot{O}_R$ , das er dem Zertifikat  $Z_R$  der Root-CA R entnimmt.
- Der Sender A signiert die Daten mit seinem privaten Schlüssel  $P_A$ .
- Der Sender A verschlüsselt die signierten Daten mit dem öffentlichen Schlüssel  $\ddot{O}_B$  des Empfängers B, den er aus dessen Zertifikat  $Z_B$  entnimmt.
- Der Empfänger B entschlüsselt die verschlüsselten und signierten Daten mit seinem privaten Schlüssel  $P_B$ .
- Der Empfänger B prüfte die Echtheit der signierten Daten mit dem öffentlichen Schlüssel  $\ddot{O}_A$  des Senders A, das er dessen Zertifikat  $Z_A$  entnimmt.

Die Verwendung einer Zertifizierungsstelle bedeutet anfangs einen erhöhten Aufwand. Jedoch entfällt dadurch bei größeren Systemen oder Maschinen die mühsame Verteilung von Zertifikaten auf die einzelnen Geräte.

### Information:

**In Unternehmen, welche eine eigene IT-Abteilung haben, sind meistens die nötigen Voraussetzungen für eine PKI (Public Key Infrastructure) bereits vorhanden.**

OPC UA verwendet grundsätzlich Zertifikate im X.509-Format. Selbst wenn keine Zertifizierungsstelle verwendet wird, muss der öffentlichen Schlüssel  $\ddot{O}_X$  für das Gerät X in das Zertifikat  $Z_X$  verpackt und vom Gerät mit seinem private Schlüssel  $P_X$  signiert werden.

Beim initialen Verbindungsaufbau kann der Empfänger B nicht sicherstellen, ob das Zertifikat  $Z_A$  tatsächlich vom Sender A stammt, oder von einem Man-in-the-Middle, und muss diesem Zertifikat blind vertrauen. Das ist der Grund für die Warnung, wenn man sich mit einem Programm wie UaExpert zum ersten Mal auf ein Gerät verbinden.

## 9.2 Benutzerzugriffe

### Zugriffsrechte zuweisen

Der TSN-Switch verfügt über ein Rechte- und Rollensystem, das festlegt, welche Aktionen ein angemeldeter Benutzer hat. In der Regel sind nicht alle Benutzer gleichberechtigt.

Vielmehr ist es üblich, nur einen oder mehrere Administratoren zu definieren, die sensitive Einstellungen am TSN-Switch vornehmen dürfen.

### Benutzer identifizieren

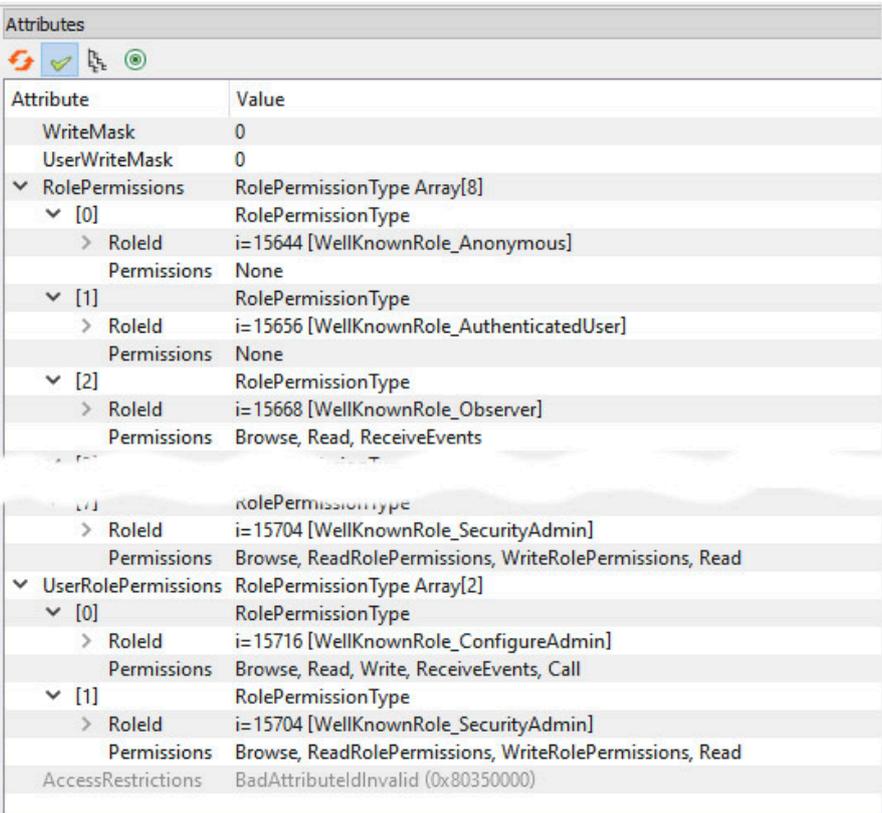
Der Zugriff auf den TSN-Switch erfolgt in der Regel authentifiziert. Die Identifizierung erfolgt entweder mit ihrem Benutzernamen und Passwort oder, im Falle von NETCONF, mittels einen SSH-Schlüssel.

Lediglich der erste Zugriff auf den TSN-Switch im Konfigurationsmodus erfolgt anonym, da zu diesem Zeitpunkt noch keine bekannten Benutzer am TSN-Switch existieren und diese erst angelegt werden müssen.

### Rollenzuweisung

OPC UA bietet 8 "bekannte Rollen", die unter dem Knoten *Root/Objects/Server/ServerCapabilities/RoleSet* aufgeführt sind. Benutzern können eine oder mehrere dieser Rollen zugewiesen werden (siehe "[SecurityAdmin-Rolle zuweisen](#)"). Jeder Knoten im Informationsmodell hat die Attribute *RolePermissions* und *UserRolePermissions*. *UserRolePermissions* zeigt die Berechtigungen für die Rollen eines Benutzers für diesen Knoten an. SecurityAdmins haben die Berechtigung, das Attribut *RolePermissions* zu lesen, das die Berechtigungen aller Rollen auf dem Knoten anzeigt.

### Beispiel für mögliche Werte der Attribute *RolePermissions* und *UserRolePermissions*:



Attribute	Value
WriteMask	0
UserWriteMask	0
RolePermissions	RolePermissionType Array[8]
[0]	RolePermissionType
RoleId	i=15644 [WellKnownRole_Anonymous]
Permissions	None
[1]	RolePermissionType
RoleId	i=15656 [WellKnownRole_AuthenticatedUser]
Permissions	None
[2]	RolePermissionType
RoleId	i=15668 [WellKnownRole_Observer]
Permissions	Browse, Read, ReceiveEvents
[3]	RolePermissionType
RoleId	i=15704 [WellKnownRole_SecurityAdmin]
Permissions	Browse, ReadRolePermissions, WriteRolePermissions, Read
UserRolePermissions	RolePermissionType Array[2]
[0]	RolePermissionType
RoleId	i=15716 [WellKnownRole_ConfigureAdmin]
Permissions	Browse, Read, Write, ReceiveEvents, Call
[1]	RolePermissionType
RoleId	i=15704 [WellKnownRole_SecurityAdmin]
Permissions	Browse, ReadRolePermissions, WriteRolePermissions, Read
AccessRestrictions	BadAttributeIdInvalid (0x80350000)

Die Knoten im Informationsmodell sind Gruppen zugeordnet. Alle Knoten innerhalb einer Gruppe haben die selben Berechtigungseinstellungen. Die Berechtigungseinstellungen sind fest eingestellt und nicht änderbar.

Die folgende Tabelle zeigt die möglichen Zugriffsrechte der Rollen für die Knoten innerhalb der verschiedenen Gruppen:

Gruppe	Knotenpfad	Rolle	Berechtigungen					
			B <sup>1)</sup>	R <sup>2)</sup>	RE <sup>3)</sup>	W <sup>4)</sup>	C <sup>5)</sup>	RP <sup>6)</sup>
Default	Alle Knoten, die in keiner der anderen Gruppen untergeordnet sind	Anonymous						
		AuthenticatedUser						
		Observer	✓	✓	✓			
		Operator	✓	✓	✓			
		Engineer	✓	✓	✓	✓	✓	
		Supervisor	✓	✓	✓		✓	
		ConfigureAdmin	✓	✓	✓	✓	✓	
		SecurityAdmin	✓	✓				✓
Security	Server/ServerConfiguration/* Server/ServerCapabilities/RoleSet/* Server/ServerCapabilities/UserSet/*	Anonymous						
		AuthenticatedUser						
		Observer						
		Operator						
		Engineer	✓	✓	✓			
		Supervisor	✓	✓	✓			
		ConfigureAdmin	✓	✓	✓			
		SecurityAdmin	✓	✓	✓	✓	✓	✓
Configuration	DeviceSet/0ACST02.1/Configuration/*	Anonymous						
		AuthenticatedUser						
		Observer	✓	✓	✓			
		Operator	✓	✓	✓			
		Engineer	✓	✓	✓	✓	✓	
		Supervisor	✓	✓	✓			
		ConfigureAdmin	✓	✓	✓	✓	✓	
		SecurityAdmin	✓	✓				✓
User	Server/ServerCapabilities/CurrentUser/*	Anonymous						
		AuthenticatedUser						
		Observer	✓	✓	✓	✓	✓	
		Operator	✓	✓	✓	✓	✓	
		Engineer	✓	✓	✓	✓	✓	
		Supervisor	✓	✓	✓	✓	✓	
		ConfigureAdmin	✓	✓	✓	✓	✓	
		SecurityAdmin	✓	✓	✓	✓	✓	✓
SoftwareUpdate	DeviceSet/0ACST02.1/FirmwareUpdate/*	Anonymous						
		AuthenticatedUser						
		Observer						
		Operator						
		Engineer	✓	✓	✓	✓	✓	
		Supervisor	✓	✓	✓			
		ConfigureAdmin	✓	✓	✓	✓	✓	
		SecurityAdmin	✓	✓	✓	✓	✓	✓

- 1) Browse
- 2) Read
- 3) ReceiveEvent
- 4) Write
- 5) Call
- 6) ReadRolePermissions und WriteRolePermissions

### 9.3 Schlüsselverwaltung für NETCONF

Damit ein NETCONF-Client mit dem TSN-Switch kommunizieren kann, sollten idealerweise SSH-Schlüssel verwendet werden. Grundsätzlich wäre zwar die Authentifikation über Benutzernamen und Passwort möglich, SSH-Schlüssel bieten aber bessere Sicherheit.

#### Information:

**Für das TTTech Slate XNS Tool ist dieser Schritt nicht möglich, da das Tool den Benutzernamen und das Passwort verwendet, aber keinen Schlüssel.**

- Zuerst muss am Gerät, auf dem der NETCONF-Client läuft, ein SSH-Schlüsselpaar erzeugt werden. Unter Linux bzw. Windows mit Cygwin geschieht das z. B. über das Kommandozeilen-Tool `ssh-keygen`:

```
$ ssh-keygen -q -N "" -f ~/.ssh/id_rsa
```

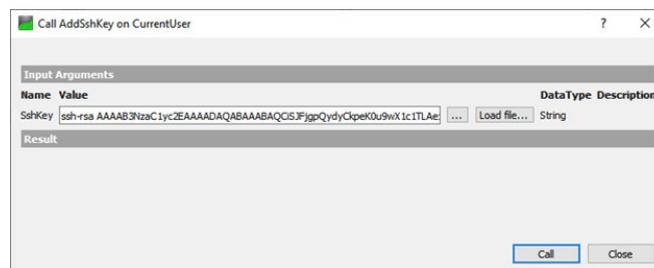
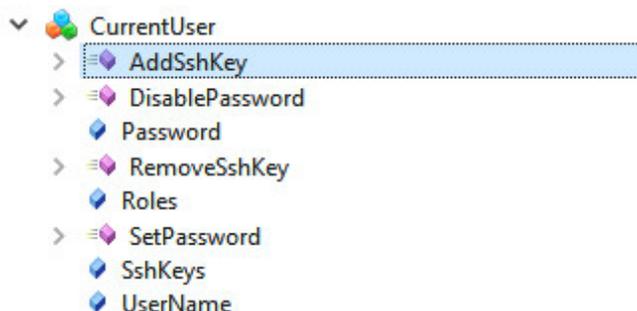
Dieser Aufruf erzeugt 2 Dateien:

```
~/.ssh/id_rsa
~/.ssh/id_rsa.pub
```

Die Datei `~/.ssh/id_rsa` enthält den privaten Schlüssel und muss geschützt am Gerät verbleiben. Die andere Datei `~/.ssh/id_rsa.pub` enthält den öffentlichen Schlüssel, der auf den TSN-Switch übertragen wird. Der Inhalt dieser Datei ist eine einzelne ASCII-Textzeile der folgenden Art:

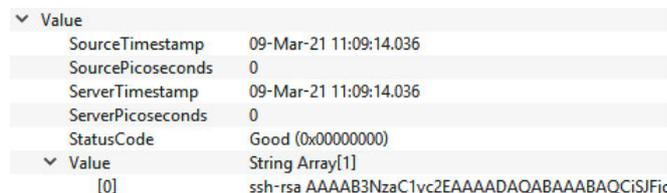
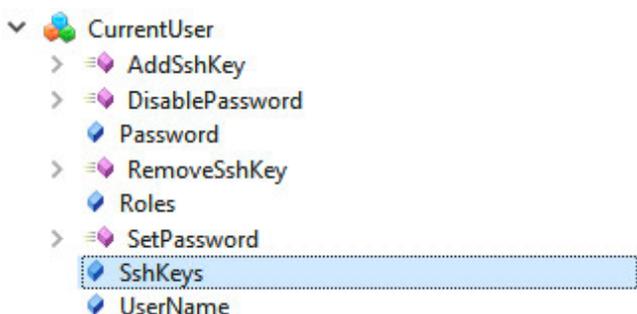
```
ssh-rsa AAAAB3NzaC1yc2EAAAADA...UmUCIxYc68QIw+OSoN admin@client
```

- Falls lediglich ein einziger Benutzer, wie der zuvor angelegte "admin" für sämtliche Verwaltungsaufgaben verwendet werden soll, kann der Schlüssel diesem Benutzer zugewiesen werden. Dazu muss die Methode `Root/Objects/Server/ServerCapabilities/CurrentUser/AddSshKey` aufgerufen und die gesamte Textzeile des öffentlichen SSH-Schlüssels hineinkopiert werden.



Falls unterschiedliche Geräte zur Switchverwaltung über NETCONF benutzen werden, kann für jedes dieser Geräte ein eigener SSH-Schlüssel hinzugefügt werden. Nicht mehr verwendete SSH-Schlüssel lassen sich analog über die Funktion `Root/Objects/Server/ServerCapabilities/CurrentUser/RemoveSshKey` wieder vom TSN-Switch entfernen.

Die Liste der SSH-Schlüssel ist beim jeweiligen Benutzer zu sehen:



- Bei Bedarf können unterschiedliche Benutzer mit eigenen Rollen definiert werden, die z. B. für unterschiedliche Verwaltungsaufgaben zuständig sind. Neben einem allgemeinen *SecurityAdmin* für die Benutzer- und Rollenverwaltung, wäre ein weiterer *ConfigureAdmin* denkbar, der für die Verwaltung der TSN-Funktionalität des TSN-Switchs zuständig ist. Dieser Benutzer würde mit dem TSN-Switch ausschließlich über NETCONF kommunizieren. In diesem Fall kann dessen Passwort deaktiviert und ihm somit der Zugang über OPC UA verwehrt werden.

## 9.4 Zertifikatsmanagement

### Information:

Siehe auch [4.8 "Aktualisierung des Self-Signed Zertifikats"](#).

### 9.4.1 Zertifikatsanforderung erzeugen

Will man Zertifikate verwenden, die von einer Zertifizierungsstelle (Certificate Authority, CA) signiert sind, dann sollte die notwendige Zertifikatsignierungsanforderung (Certificate-Signing-Request, CSR) direkt am Gerät erzeugt werden. Durch die Erzeugung des CSR am Gerät muss der private Schlüssel das Gerät nie verlassen, wodurch die Sicherheit erhöht wird. Der Prozess läuft folgendermaßen ab:

- Zum Erzeugen eines CSR gibt es unter *Root/Objects/Server/ServerConfiguration* die Methode *CreateSigningRequest*. Beim Aufruf der Methode wird optional ein neuer privater Schlüssel erzeugt. Sollte die Option nicht aktiviert sein, dann wird der bestehende Schlüssel verwendet. Der öffentliche Schlüssel, die Information über den Antragsteller, sowie weitere Informationen werden in einen "PKCS #10 DER" codierten Certificate-Request verpackt, der von der Methode zurückgegeben wird. Der Bytestring muss in eine entsprechende ".csr"-Datei gespeichert werden.
- Der CSR muss im Anschluss von einer Zertifizierungsstelle signiert werden, wobei noch zusätzliche Informationen in das Zertifikat eingetragen werden. Das Ergebnis ist ein gültiges Zertifikat.
- Das signierte Zertifikat kann im dann über die Methode *Root/Objects/Server/ServerConfiguration/UpdateCertificate* installiert werden.

### Information:

- **Der private Schlüssel für den CSR bleibt nur so lange am Gerät hinterlegt, bis ein neuer CSR generiert wird oder bis das Gerät neu gestartet wird. Ein signiertes Zertifikat kann nur dann installiert werden, wenn der dazu gehörige private Schlüssel noch vorhanden ist.**
- **UaExpert bietet im GDS Push View eine vereinfachte Möglichkeit den CSR zu erzeugen und zu speichern. Dadurch muss nicht direkt mit der Methode gearbeitet werden.**

Weiterführende Details zur OPC UA Methode *CreateSigningRequest* finden sich in der OPC UA Spezifikation, Teil 12

### 9.4.2 Zertifikat mittels UpdateCertificate aktualisieren

Über die Methode *Root/Objects/Server/ServerConfiguration/UpdateCertificate* können signierte Zertifikate auf dem TSN-Switch installiert werden. Dabei macht es keinen Unterschied, ob es sich um ein von einer Zertifizierungsstelle signiertes Zertifikat oder um ein selbstsigniertes Zertifikat handelt. Wenn das Zertifikat nicht aus einem CSR erzeugt wurde der vom TSN-Switch generiert wurde, dann muss zusätzlich der private Schlüssel übergeben werden.

Damit die Änderungen übernommen werden, muss zusätzlich die Methode *Root/Objects/Server/ServerConfiguration/ApplyChanges* aufgerufen werden. Dabei werden alle verbundenen Clients getrennt. Eine neue Verbindung ist erst wieder möglich, wenn dem neuen Zertifikat vertraut wird.

### Information:

- **Da beim Aufruf dieser Methode möglicherweise ein privater Schlüssel übertragen wird, ist der Aufruf nur möglich, wenn eine verschlüsselte Verbindung zwischen TSN-Switch und OPC UA Client besteht.**
- **UaExpert bietet im GDS Push View eine vereinfachte Möglichkeit Zertifikate zu aktualisieren. Dadurch muss nicht direkt mit der Methode gearbeitet werden.**
- **Zertifikate, die von anderen Zertifikaten abgeleitet sind, können nur installiert werden wenn alle übergeordneten Zertifikate bereits installiert wurden, (siehe [9.1.3 "Symmetrische und asymmetrische Schlüssel"](#)) sodass die vollständige Vertrauenskette überprüft werden kann.**

Weiterführende Details zur OPC UA Methode *UpdateCertificate* finden sich in der OPC UA Spezifikation, Teil 12.

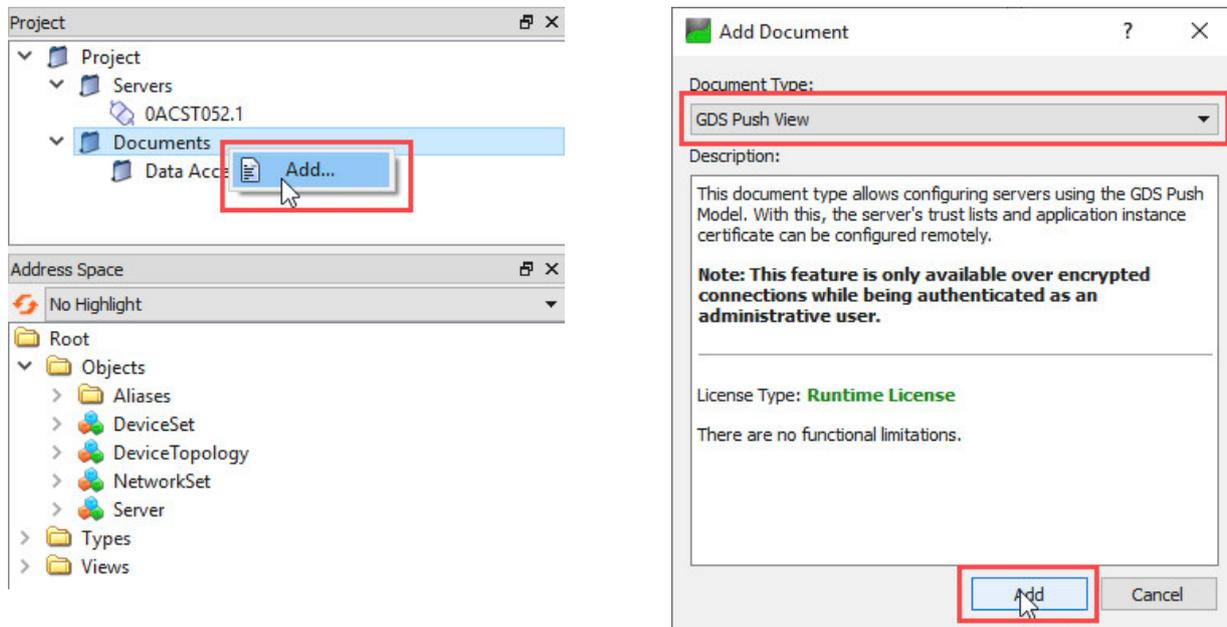
### 9.4.2.1 Aktualisierung des selbstsignierten Zertifikats mittels UaExpert

UaExpert verfügt über Werkzeuge mit dessen Hilfe Zertifikate auf einfache Weise aktualisiert werden können.

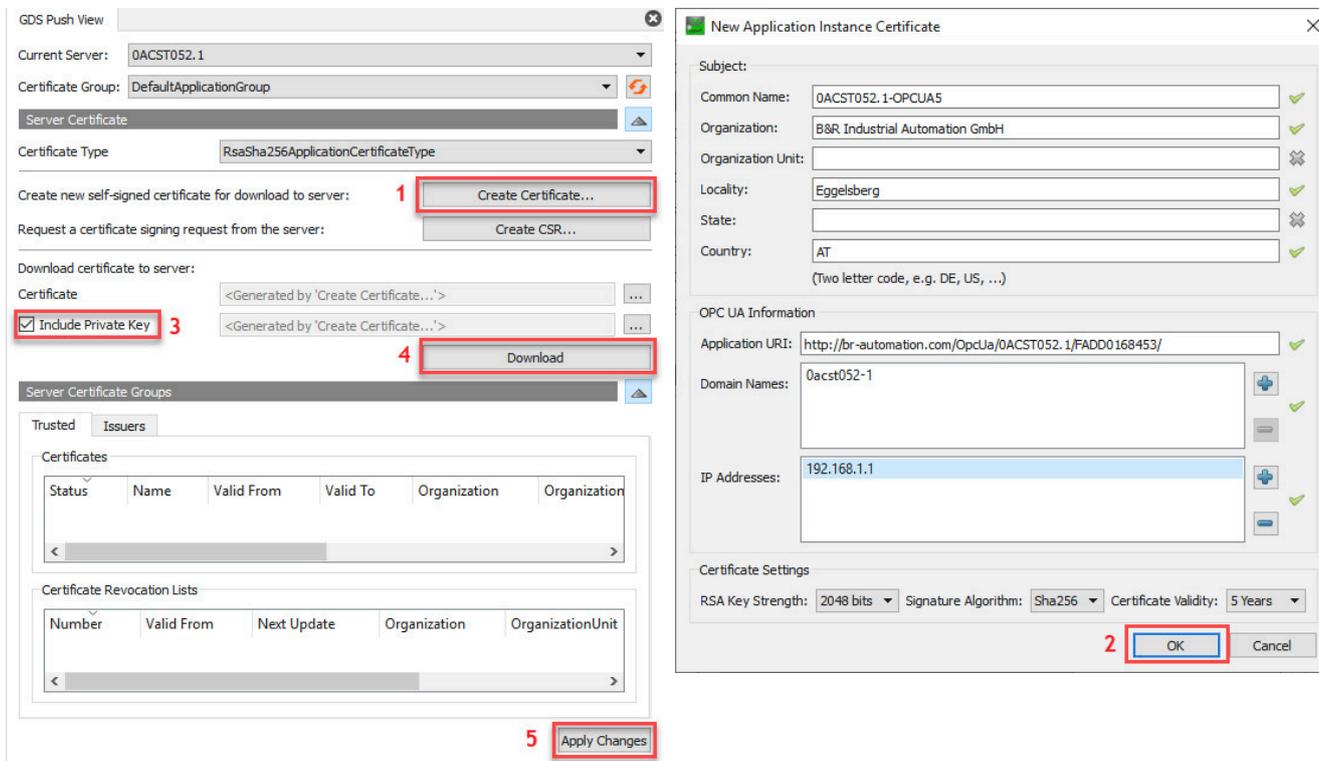
#### Information:

Da beim folgenden Ablauf ein privater Schlüssel übertragen wird funktioniert er nur, wenn eine verschlüsselte Verbindung zum TSN-Switch besteht.

- Im Projektfenster des UaExpert im Kontextmenü von *Documents* auf *Add...* klicken. Ein Dialog öffnet sich. In diesem Dialog den Dokument-Typ "GDS Push View" auswählen und durch Klick auf *Add* bestätigen.



- Das Zertifikat erstellen und übertragen.



- 1) Klick auf *Create Certificate*
- 2) Im folgenden Dialog werden die für das Zertifikat erforderlichen Daten eingegeben.

**Information:**

**Das Eintragen der IP-Adresse ist nur notwendig, wenn die IP-Adresse statisch vergeben ist und Clients mit Hilfe der IP-Adresse auf den TSN-Switch zugreifen (z. B. über die URL `opc.tcp://192.168.1.1:4840`). Wird die IP-Adresse über einen DHCP-Server bezogen, dann ist es nicht sinnvoll eine IP-Adresse in das Zertifikat einzutragen, da diese in der Regel dynamisch zugeteilt wird und sich ändern kann.**

- 3) Da für die Aktualisierung der private Schlüssel mit übertragen werden muss, ist die Option "Include Private Key" auszuwählen.
- 4) Durch Klick auf *Download* wird das vorher erstellte Zertifikat auf den TSN-Switch übertragen. Die folgende Abfrage, ob Issuer-Zertifikate spezifiziert werden sollen kann mit "Nein" bestätigt werden.
- 5) Durch Klick auf *ApplyChanges* wird das neue Zertifikat übernommen. Dabei werden alle verbundenen Clients getrennt. Eine neue Verbindung ist erst wieder möglich, wenn dem neuen Zertifikat vertraut wird.

# 10 Diagnose

---

Auftretende Fehlfunktionen oder das Beobachten von unerwartetem bzw. unerwünschtem Verhalten des TSN-Switchs kann vielfältige Ursachen haben. Insbesondere beim Einsatz in größeren Netzwerken im Verbund mit Netzwerkinfrastruktur unterschiedlicher Hersteller, gestaltet sich oft bereits die Lokalisierung möglicher Fehlerquellen schwierig. Das vorliegende Kapitel soll als Hilfestellung bei der Diagnose von Fehlfunktionen und der Lokalisierung ihrer Ursachen dienen. Es beschreibt kontextbezogene Fehler und zeigt mögliche Ursachen und deren Lösung auf. Diese umfassen:

- Fehler im Kontext der Adressierung
- Fehler im Kontext der Datenübertragung
- Fehler im Kontext der Zeitsynchronisierung
- Fehler im Kontext von Cyber-Security

## 10.1 Adressierung

Nr.	Fehlerbild	Mögliche Ursache	Lösung	Siehe
1	Verbindung über Hostname im Werkszustand nicht möglich.	Hostname unbekannt	Der TSN-Switch ist standardmäßig unter dem mDNS-Hostnamen "0acst052-1-<MAC-Adresse>.local" erreichbar <sup>1)</sup> .	- 4.2 "Verbindungsaufbau" - 7.1.2 "Allgemeine Netzwerkkonfiguration"
2	Verbindung über IP-Adresse im Werkszustand nicht möglich.	IP-Adresse unbekannt	<p>• <b>DHCP-Server ist im Netzwerk vorhanden<sup>2)</sup>:</b> Die dem TSN-Switch zugewiesene IP-Adresse beim zuständigen Netzwerkadministrator in Erfahrung bringen.</p> <p>• <b>DHCP-Server ist im Netzwerk nicht vorhanden:</b> Dem TSN-Switch zum Betrieb mit Hilfe des Resetters die statische IP-Adresse 192.168.1.1 zuweisen (Betätigen des Resetters für 1 s) und anschließend eine benutzerdefinierte Konfiguration über das OPC UA Informationsmodell durchführen.</p> <p>Falls der TSN-Switch direkt mit einem anderen Switch verbunden ist, welcher bereits über Hostname oder IP-Adresse erreichbar ist, dann kann die gesuchte IP-Adresse von dem Port ausgelesen werden, an dem der TSN-Switch angeschlossen ist. <i>Root/Objects/DeviceSet/0ACST052.1/Status/BridgePorts/ETHx/LinkPartner/ManagementAddress</i></p>	- 8.1 "Port-Status"  - 3.3.3 "Resettaster" - 3.5 "Einstellen der IP-Adresse" - 7.1.2 "Allgemeine Netzwerkkonfiguration"
3	In einem Netzwerk mit DHCP-Server ist die Verbindung zum TSN-Switch über IP-Adresse nicht möglich, nachdem eine statische IP-Adresse per Konfiguration über das OPC UA Informationsmodell gesetzt wurde.	Es besteht ein IP-Adressenkonflikt mit einem anderen Gerät im Netzwerk, das dieselbe Adresse dynamisch vom DHCP-Server bezogen hat.	Überprüfen, ob die statisch zugewiesene IP-Adresse außerhalb des vom DHCP-Server verwalteten Bereichs liegt.  • <b>Außerhalb des Bereichs:</b> Alle Geräte mit statischen Adresseinstellungen auf Adresskonflikte überprüfen.  • <b>Innerhalb des Bereichs:</b> Standard-Adresse 192.168.1.1 wiederherstellen und eine statischen IP-Adresse, die außerhalb des vom DHCP-Server verwalteten Bereichs liegt, konfigurieren.	- 3.3.3 "Resettaster" - 3.5 "Einstellen der IP-Adresse" - 7.1.2 "Allgemeine Netzwerkkonfiguration"
		Es wurde bei der Konfiguration über das OPC UA Informationsmodell eine Netzwerkmaske eines Subnetzes vergeben, das vom Client aus nicht erreicht werden kann.	Einstellungen des TCP/IP-Stacks auf dem Betriebssystem des Clients überprüfen.  • <b>Innerhalb desselben Subnetzes:</b> Befindet sich der Client im selben Subnetz, müssen die konfigurierten Netzwerkmasken am Client und am TSN-Switch identisch sein.  • <b>Nicht innerhalb desselben Subnetzes:</b> Befindet sich der Client nicht im selben Subnetz, sind die Routing-Einstellungen des Betriebssystems des Clients zu prüfen.	- 7.1.2 "Allgemeine Netzwerkkonfiguration"

### 1) Information

- Eine Adressierung des Geräts über den oben genannten Hostname erfordert eine entsprechende mDNS-Unterstützung auf dem Betriebssystem des zugreifenden Clients.
- Die zu verwendende MAC-Adresse im Hostname des TSN-Switchs, ist dem seitlich am TSN-Switch angebrachten Etikett zu entnehmen ("MAC1"), welches auch die Seriennummer enthält.

Ein benutzerdefinierter Hostname ist über das OPC UA Informationsmodell konfigurierbar.

- 2) Der TSN-Switch wird standardmäßig mit aktiviertem DHCP-Client ausgeliefert und eine IP-Adresse muss von einem DHCP-Server im Netzwerk zugewiesen werden.

## 10.2 Datenübertragung

Nr.	Fehlerbild	Mögliche Ursache	Lösung	Siehe	
1	Kompletter Kommunikationsausfall zwischen 2 oder mehr an den TSN-Switch angeschlossenen Geräten <sup>1)</sup> .	Ethernet Auto-Negotiation zwischen TSN-Switch und einem oder mehreren angeschlossenen Geräten ist fehlgeschlagen.	<p><i>LinkStatus</i> der betroffenen Ports im OPC UA Informationsmodell prüfen:  <i>Root/Objects/DeviceSet/0ACST052.1/Status/BridgePorts/ETHx/LinkProperties/LinkStatus</i>            Steht dieser Wert nicht auf <i>UP</i>, besteht auf Netzwerkebene kein Link zwischen TSN-Switch und angeschlossenenem Gerät.            Kabelverbindung kontrollieren:</p> <ul style="list-style-type: none"> <li>– Fester Sitz der Steckverbindung</li> <li>– max. Länge (100m) des Kabels nicht überschritten</li> <li>– Eventuelle Kabelschäden</li> </ul> <p>Eventuell vorhandene Log-Ausgaben des Switchs bzw. des angeschlossenen Geräts kontrollieren. Diese können Aufschluss über Hardwareprobleme geben.</p>	- 8.1 "Port-Status"	
		An der Kommunikation beteiligte Geräte senden keine oder fehlerhafte Ethernet-Frames, die vom TSN-Switch erkannt und verworfen werden.	<p>Fehlerzähler der betroffenen Ports im OPC UA Informationsmodell prüfen:  <i>Root/Objects/DeviceSet/0ACST052.1/Status/BridgePorts/ETHx/FrameStatistics/</i></p> <ul style="list-style-type: none"> <li>• <i>RxFrameCount</i> und <i>TxFrameCount</i>              Weisen diese Zähler den Wert 0 auf, werden von den angeschlossenen Geräten keine oder fehlerhafte Ethernet-Frames versendet.</li> <li>• <i>FcsErrorFrameCount</i>,  <i>GeneralRxErrorFrameCount</i>,  <i>GeneralTxErrorFrameCount</i> und  <i>SizeErrorFrameCount</i>              Bei fehlerfreiem Betrieb weisen diese Zähler den Wert 0 auf. Werte ungleich 0 deuten in den meisten Fällen auf Fehler in Netzwerkkomponenten der angeschlossenen Geräte oder dem TSN-Switch selbst hin.</li> </ul> <p>Eventuell vorhandene Log-Ausgaben des TSN-Switchs bzw. des angeschlossenen Geräts kontrollieren. Diese können Aufschluss über Hardwareprobleme geben.</p>		- 8.1 "Port-Status"
		Ethernet-Frames die mit einem VLAN-Tag versehen sind und/oder Multicast DMAC-Adressen wurden nicht am TSN-Switch konfiguriert.	Konfiguration zur Weiterleitung von Ethernet-Frames mit VLAN-Tag und/oder Multicast DMAC-Adressen im Konfigurationstool überprüfen.		
2	Datenempfang an einem an den TSN-Switch angeschlossenen Empfänger erfolgt nicht zum erwarteten Zeitpunkt <sup>2)</sup> .	Link-Geschwindigkeit zwischen TSN-Switch und angeschlossenenem Gerät entspricht nicht Erwartungshaltung (100 Mbit/s statt 1 Gbit/s).	<p>Knoten <i>Speed</i> und <i>Duplex</i> der betroffenen Ports im OPC UA Informationsmodell prüfen.  <i>Root/Objects/DeviceSet/0ACST052.1/Status/BridgePorts/ETHx/LinkProperties/Speed</i> bzw. <i>Duplex</i>            Entspricht die Geschwindigkeit oder der Duplex-Modus nicht der Erwartungshaltung, dann folgende Punkte überprüfen:</p> <ul style="list-style-type: none"> <li>– Unterstützt das angeschlossene Gerät die erwartete Geschwindigkeit/Duplex-Modus?</li> <li>– Wurde der korrekte Kabeltyp verwendet?              (Für Gigabit-Ethernet ist mindestens Cat 5 erforderlich)</li> <li>– Kabelverbindung kontrollieren:               <ul style="list-style-type: none"> <li>• Fester Sitz der Steckverbindung</li> <li>• Eventuelle Kabelschäden</li> <li>• Verlegung in der Nähe von potenziellen Einstreuungsquellen</li> </ul> </li> </ul>	- 8.1 "Port-Status"	
		Duplex-Mode zwischen TSN-Switch und angeschlossenenem Gerät entspricht nicht Erwartungshaltung (Half-Duplex anstatt Full-Duplex).			
		Geräte wurden nicht an den laut Systemdesign vorgesehenen TSN-Switch-Ports angeschlossen. Dadurch entsprechen die Übertragungslatenzen nicht der Erwartungshaltung.	<p>Knoten unter <i>LinkPartner</i> der betroffenen Ports im OPC UA Informationsmodell prüfen.  <i>Root/Objects/DeviceSet/0ACST052.1/Status/BridgePorts/ETHx/LinkPartner/</i></p>		

1) Beispielsweise, wenn Nachrichten eines OPC UA Publishers an einem OPC UA Subscriber nicht empfangen werden.

2) Beispielsweise, wenn ein OPC UA Subscriber verspätet eingetroffene oder ausgefallene Ethernet-Frames feststellt.

## 10.3 Zeitsynchronisierung

Nr.	Fehlerbild	Mögliche Ursache	Lösung	Siehe
1	Die PTP-Zeitsynchronisation am TSN-Switch angeschlossener Geräte funktioniert nicht.	Die PTP-Zeitsynchronisation am TSN-Switch ist nicht aktiviert.	PTP-Zeitsynchronisation im OPC UA Informationsmodell aktivieren <sup>1)</sup> .  <ul style="list-style-type: none"> <li>• <b>WallClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WallClock/TimeSyncProtocol</i></li> <li>• <b>WorkingClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WorkingClock/TimeSyncProtocol</i></li> </ul>	- 7.1.6 "Zeitsynchronisation"
		Es wurde die Zeitsynchronisation der falschen PTP-Domäne am TSN-Switch oder dem angeschlossenen Gerät konfiguriert.	Identische PTP-Domäne an allen beteiligten Geräten konfigurieren <sup>2)</sup> . Am TSN-Switch kann diese Einstellung im OPC UA Informationsmodell erfolgen.  <ul style="list-style-type: none"> <li>• <b>WallClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WallClock/PTP/DomainNumber</i></li> <li>• <b>WorkingClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WorkingClock/PTP/DomainNumber</i></li> </ul>	- 7.1.6 "Zeitsynchronisation"
		Es gibt keinen PTP-Grandmaster im Netzwerk.	Wenn der TSN-Switch als PTP Grandmaster fungieren sollte, Option <i>SlaveOnly</i> im OPC UA Informationsmodell deaktivieren.  <ul style="list-style-type: none"> <li>• <b>WallClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WallClock/PTP/SlaveOnly</i></li> <li>• <b>WorkingClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WorkingClock/PTP/SlaveOnly</i></li> </ul>	- 7.1.6 "Zeitsynchronisation"
		Für die Verkehrsklasse ('Traffic Class') des Netzwerkmanagementverkehrs wurde kein offenes Zeitfenster konfiguriert, wodurch Zeitsynchronisationsnachrichten blockiert werden.	Konfiguration eines offenen Zeitfensters für den Netzwerkmanagementverkehr. Standardmäßig wird der Netzwerkmanagementverkehr der Verkehrsklasse 7 (höchste Priorität) zugeordnet.	- 7.3 "Konfiguration über NET-CONF"
2	Der TSN-Switch sollte PTP-Grandmaster sein, es wurde aber ein anderes Netzwerkgerät ausgewählt.	Die Priorität der PTP-Uhr des TSN-Switches ist im Vergleich zum gewählten Netzwerkgerät zu niedrig.	Die <i>Priority1</i> Einstellung der PTP-Uhr im OPC UA Informationsmodell anpassen. Je niedriger der Wert eingestellt wird, desto höher ist die Priorität.  <ul style="list-style-type: none"> <li>• <b>WallClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WallClock/PTP/Priority1</i></li> <li>• <b>WorkingClock:</b> <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/TimeSynchronization/WorkingClock/PTP/Priority1</i></li> </ul>	- 7.1.6 "Zeitsynchronisation"
3	Datenempfang an einem an den TSN-Switch angeschlossenen Empfänger erfolgt nicht zum erwarteten Zeitpunkt <sup>3)</sup> .	Die an der Kommunikation beteiligten Geräte sind nicht, oder nicht den Anforderungen entsprechend, zeitsynchronisiert.	Überprüfen der korrekten Zeitsynchronisation der PTP-Domäne der WorkingClock aller Netzwerkgeräte zwischen Sender und Empfänger. Der Zustand der Zeitsynchronisation des TSN-Switches kann im OPC UA Informationsmodell überprüft werden: <i>Root/Objects/DeviceSet/0ACST052.1/Status/TimeSynchronization/WorkingClock/PTP</i>	- 8.2 "Zeitsynchronisation"

1) Standardmäßig ist am TSN-Switch die Zeitsynchronisation deaktiviert.

2) Standardmäßig wird die WallClock über Domäne 0 und die WorkingClock über die Domäne 20 synchronisiert.

3) Beispielsweise, wenn ein OPC UA Subscriber verspätet eingetroffene oder ausgefallene Ethernet-Frames feststellt.

## 10.4 Cyber-Security

Nr.	Fehlerbild	Mögliche Ursache	Lösung	Siehe
1	Der Aufbau einer sicheren Verbindung zum OPC UA Server des TSN-Switchs wird mit Hinweis auf ein abgelaufenes Zertifikat abgelehnt.	Gültigkeitsbereich des vom Client verwendeten Zertifikats liegt außerhalb des aktuellen Datums bzw. der aktuellen Uhrzeit des TSN-Switchs <sup>1)</sup> .	<p>• <b>Bei Verwendung von NTP</b> Sicherstellen, dass mindestens einer der konfigurierten NTP-Server erreichbar ist und die korrekte Uhrzeit verteilt.</p> <p>• <b>Bei Verwendung von PTP</b> Sicherstellen, dass der PTP-Grandmaster aktiv ist und mit der entsprechenden PTP-Domäne (für die WallClock) die korrekte Uhrzeit verteilt.</p> <p>Ist keine Quelle für die WallClock vorhanden oder funktional, Sicherheitseinstellungen des Geräts zurücksetzen. Nur in diesem Zustand kann eine unverschlüsselte Verbindung hergestellt werden.</p>	<ul style="list-style-type: none"> <li>- 4.5 "Allgemeine Netzwerkeinstellungen über OPC UA"</li> <li>- 6.3 "Zeitsynchronisation und Zeitdomänen"</li> <li>- 7.1.6 "Zeitsynchronisation"</li> <li>- 8.1 "Port-Status"</li> <li>- 3.3.3 "Resettaster"</li> </ul>

- 1) Maßgeblich ist hierfür der Wert der WallClock.  
Beim sicheren Verbindungsaufbau unter Verwendung von SSL/TLS, erfolgt sowohl Client- als auch Serverseitig eine Überprüfung der verwendeten Zertifikate.

# 11 Lizenzen

---

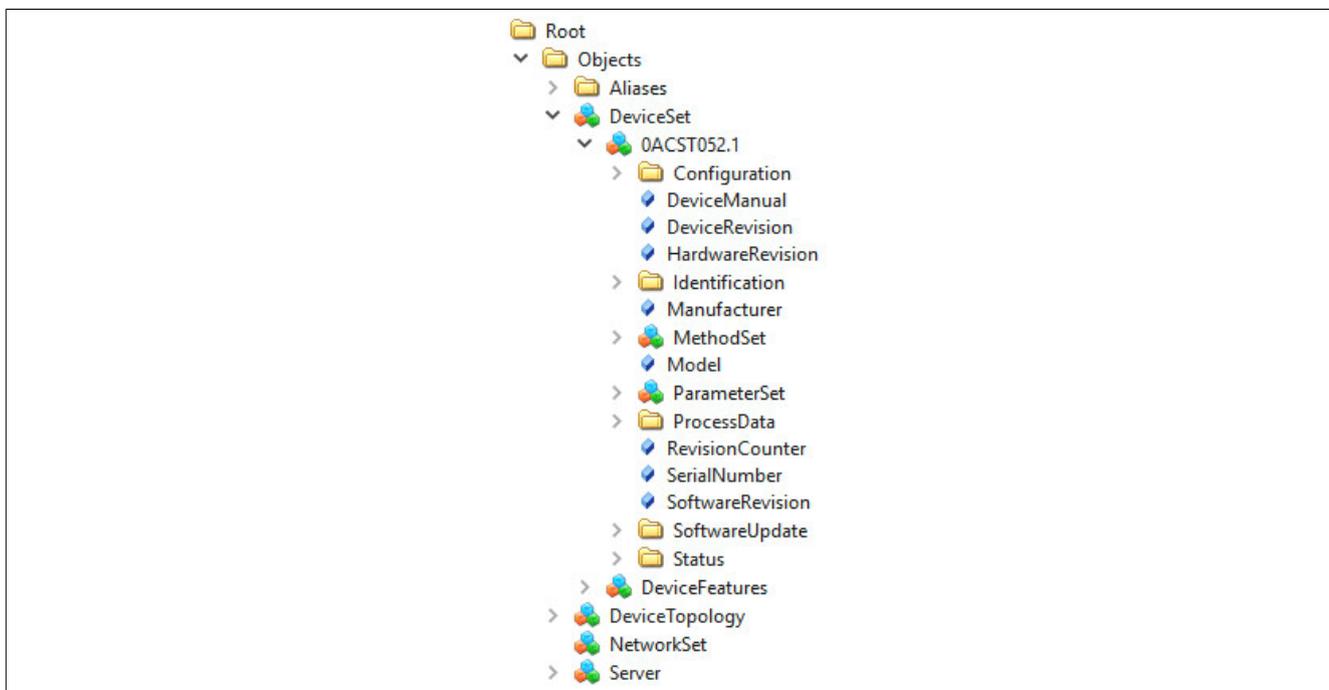
Mit Hilfe der Firmware-Upgrades, welche von der B&R Homepage ([www.br-automation.com](http://www.br-automation.com)) herunter geladen werden können, ist es möglich die Lizenzinformationen abzurufen.

1. Firmwareupgrade (ZIP-Datei) des Moduls von B&R Homepage herunterladen.
2. Das Firmwareupgrade in einen neuen Ordner entpacken.  
Es sollte danach eine ZIP-Datei licenses.zip vorhanden sein.
3. Die ZIP-Datei entpacken.  
Aus technischen Gründen können in der ZIP-Datei Dateien mit gleichem Namen enthalten sein. Dies sollte beim Entpacken der ZIP-Datei beachtet werden.
4. Nach dem Entpacken können die Lizenzdateien im Ordner ...*licenses* eingesehen werden.

## 12 Anhang

### 12.1 OPC UA Informationsmodell

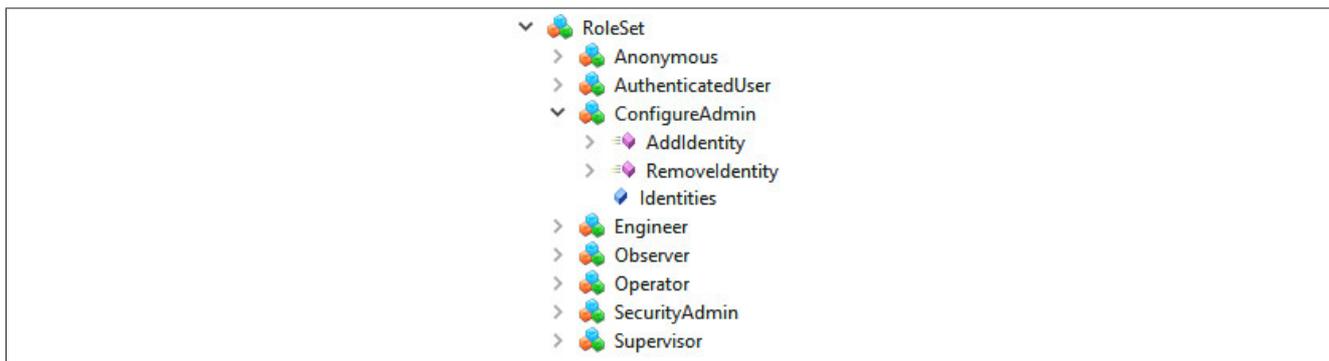
Der TSN-Switch bietet über das OPC UA Informationsmodell Zugang zur Konfiguration des TSN-Switchs. Auch OPC UA Clients können sich über dieses Informationsmodell Zugriff auf die vorhandenen Daten verschaffen.



Dem Hauptknoten *Root/Objects/DeviceSet/0ACST052.1* sind dabei über hierarchische Referenzen alle Knoten untergeordnet, die für den TSN-Switch verfügbar sind.

#### 12.1.1 Benutzerverwaltung

Der Zugriff auf den TSN-Switch ist im normalen Betrieb auf autorisierte Benutzer beschränkt. Benutzer wiederum haben unterschiedliche Rechte, entsprechend den ihnen zugewiesenen Rollen. Die dafür nötige Benutzer- und Rollenverwaltung erfolgt über das OPC UA Informationsmodell.



Der TSN-Switch kommt mit vordefinierten, standardisierten Rollen. Die Rollen unterscheiden sich strukturmäßig im Informationsmodell nicht, sondern besitzen alle die gleichen Methoden und Attribute. Beispielfähig wird hier die für Administrationsaufgaben zuständige Rolle *ConfigureAdmin* dargestellt.

Position der Daten im Informationsmodell: *Root/Objects/Server/ServerCapabilities/RoleSet*

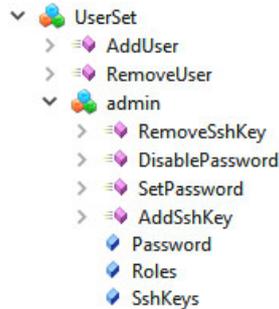
Knotenname	Beschreibung
AddIdentity	Hinzufügen eines Benutzers zu dieser Rolle
RemoveIdentity	Entfernen eines Benutzers aus dieser Rolle
Identities	Liste aller Benutzer in dieser Rolle



In der Werkseinstellung kommt der TSN-Switch ohne vordefinierte Benutzer. Diese können frei vergeben werden, bis auf wenige reservierte Namen, wie z. B. "root". Diese erscheinen dann unterhalb des *UserSet*-Objekts.

Position der Daten im Informationsmodell: *Root/Objects/Server/ServerCapabilities/UserSet*

Knotenname	Beschreibung
AddUser	Hinzufügen eines Benutzers
RemoveUser	Entfernen eines Benutzers



Angelegte Benutzer unterscheiden sich strukturmäßig im OPC UA Informationsmodell nicht, sondern besitzen alle die gleichen Methoden und Attribute. Beispielhaft wird hier der häufig verwendete Benutzer "admin" dargestellt.

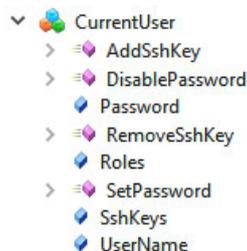
Benutzer können sich am TSN-Switch auf unterschiedliche Weise authentifizieren. Der Zugriff über OPC UA wird durch Passwörter, der Zugriff über NETCONF hingegen über SSH-Schlüssel gesichert. Es ist erlaubt, beide Arten gleichzeitig zu aktivieren.

Ein Benutzer kann höchstens ein Passwort haben. Es ist sinnvoll, ein Passwort von hinreichender Komplexität zu wählen. Der TSN-Switch überprüft allerdings das eingestellte Passwort nicht, wodurch auch das leere Passwort "" möglich ist.

Ein Benutzer kann beliebig viele SSH-Schlüssel haben. Das bietet sich an, wenn der Zugriff auf den TSN-Switch von unterschiedlichen Geräten aus erwünscht ist. Im Gegensatz zu Passwörtern sind SSH-Schlüssel grundsätzlich sicher und nicht zu erraten. Der TSN-Switch erlaubt die Verwendung von SSH-Schlüsseln allerdings nur für NETCONF. Der OPC UA Standard unterstützt SSH nicht.

Position der Daten im Informationsmodell: *Root/Objects/Server/ServerCapabilities/UserSet*

Beschreibung	Knotenname
Roles	Liste aller Rollen, die der Benutzer inne hat
Password	Anzeige, ob Passwortauthentifizierung für diesen Benutzer aktiv ist
SetPassword	Setzen eines Passworts
DisablePassword	Löschen des Passworts und Deaktivierung der Passwortauthentifizierung dieses Benutzers
SshKeys	Liste der öffentlichen SSH-Schlüssel
AddSshKey	Hinzufügen eines öffentlichen SSH-Schlüssels
RemoveSshKey	Entfernen eines öffentlichen SSH-Schlüssels



Der Zugriff auf die allgemeine Benutzer- und Rollenverwaltung ist beschränkt auf privilegierte Benutzer. Jeder Benutzer hat dagegen die nötigen Berechtigungen, um z. B. das eigene Passwort zu ändern. Der aktuelle Benutzer der Sitzung ist im Informationsmodell extra repräsentiert; dieser spiegelt dynamisch die Attribute und Methoden eines auch über die allgemeine Benutzerverwaltung erreichbaren Benutzers.

Position der Daten im Informationsmodell: *Root/Objects/Server/ServerCapabilities/CurrentUser*

Knotenname	Beschreibung
Roles	Liste aller Rollen, die der Benutzer dieser Sitzung inne hat
Password	Anzeige, ob Passwortauthentifizierung für diesen Benutzer aktiv ist
SetPassword	Setzen eines Passworts
DisablePassword	Löschen des Passworts und Deaktivierung der Passwortauthentifizierung dieses Benutzers

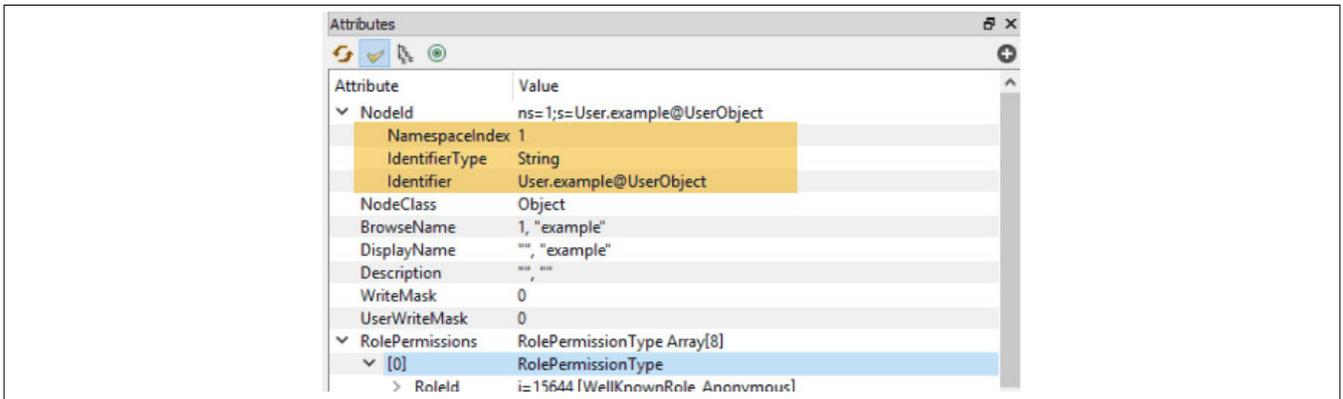
Knotenname	Beschreibung
SshKeys	Liste der öffentlichen SSH-Schlüssel
AddSshKey	Hinzufügen eines öffentlichen SSH-Schlüssels
RemoveSshKey	Entfernen eines öffentlichen SSH-Schlüssels
UserName	Name des aktuellen Benutzers der Sitzung

### 12.1.1.1 Angelegten Benutzer löschen

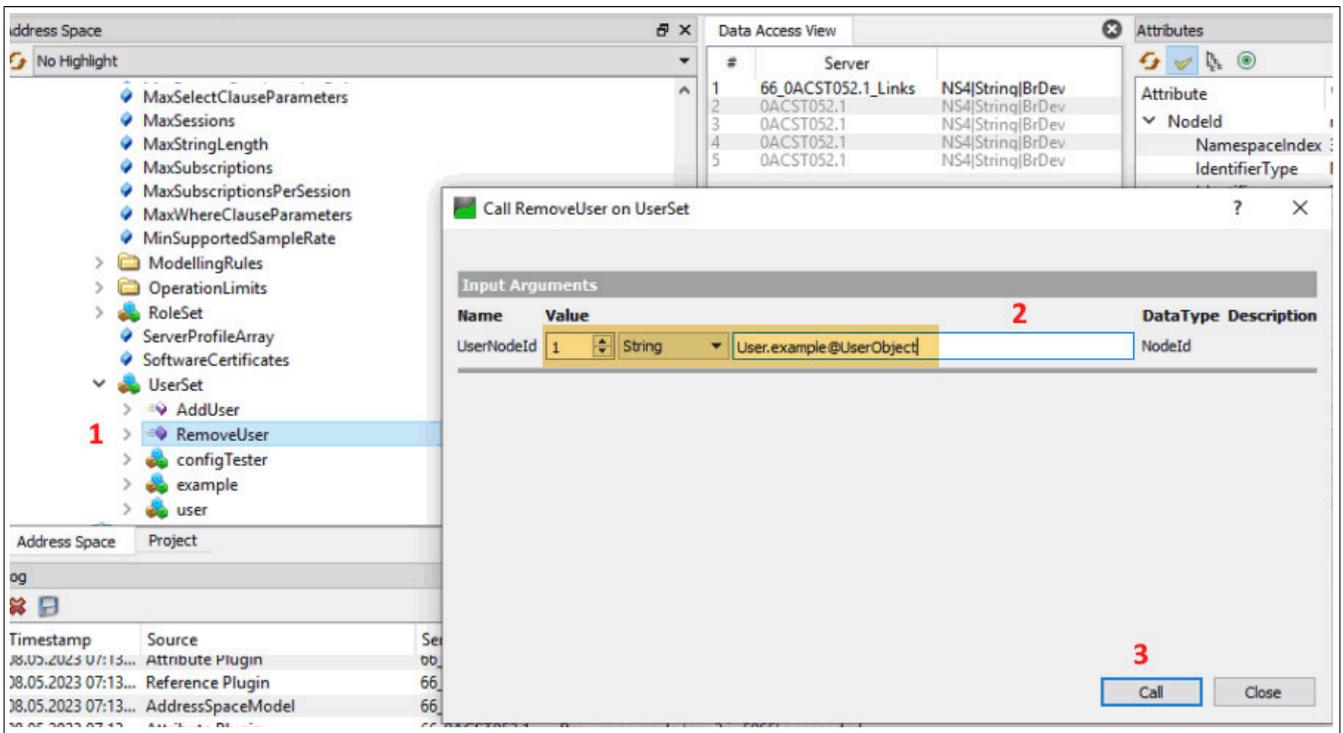
Um bereits angelegte Benutzer zu löschen, muss folgendes beachtet werden:

- Nur ein Benutzer mit *SecurityAdmin*-Rechten kann einen Benutzer löschen
- Benutzer können sich nicht selbst löschen

In diesem Beispiel soll der Benutzer "Example" gelöscht werden.



- 1) Zuerst muss die Methode 12.1.1 "RemoveUser" aufgerufen werden.
- 2) Als Eingangsargumente werden der *NamespaceIndex* und der *Identifier* des Benutzers übergeben
- 3) Zuletzt wird der Benutzer durch Klick auf "Call" gelöscht.



## 12.1.2 Firmwareupdate

Die Firmwareupdate-Funktionalität wird im OPC UA Informationsmodell dem TSN-Switch durch den Knoten *Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate* bereitgestellt. Die folgende Tabelle beschreibt die Hierarchie aller Unterknoten und deren Bedeutung:

Knotenname	Datentyp	Beschreibung
DefaultInstanceBrowseName	QualifiedName	Name des verwendeten Objekts. Festgelegter Standardname = "SoftwareUpdate"
<b>Installation</b>		
CurrentState	LocalizedText	Nutzer-lesbarer Installationsstatus Mögliche Werte Idle Installing Error
Id	Nodeld	Maschinen-lesbarer Installationsstatus Mögliche Werte 271 Idle Objekt 273 Installation Objekt 275 Error Objekt
InstallSoftwarePackage		Startet die Installation des zuvor geladenen Firmwarepakets
InputArguments	String ManufacturerUri String SoftwareRevision String[] PatchIdentifiers ByteString Hash	ManufacturerUri und SoftwareRevision; dient zur Identifikation des zu installierenden Firmwarepakets. Die Argumente <i>PatchIdentifiers</i> und <i>Hash</i> sind ohne Funktion und müssen leer bleiben. <b>Information:</b> Möchte man eine Firmware-Installation erzwingen, bei der eine identische, bereits installierte Version überschrieben werden soll, muss dem Argument <i>PatchIdentifiers[0]</i> der String "force" zugewiesen werden.
PercentComplete	Byte	Zeigt den Installationsfortschritt an. <b>Information:</b> Diese Methode ist nicht für die Erkennung einer abgeschlossenen Installation geeignet.
Resume		Setzt den Installationsstatus von "Error" zurück auf "Idle"
<b>Loading</b>		
CurrentVersion		Zeigt Eigenschaften der aktiven Firmware
Manufacturer	LocalizedText	Hersteller
ManufacturerUri	String	Hersteller-URI
SoftwareRevision	String	Version des Firmwarepakets
ErrorMessage	LocalizedText	Nutzerinformation für den Dateitransfer - siehe <a href="#">Fehlernachrichten</a>
FileTransfer		Gibt Informationen zum Dateitransfer des Firmwarepakets
ClientProcessingTimeout		Zeit in Sekunden, nach der der Server den Transfer beendet, sollte der Client keine für den Transfer erforderlichen Methodenaufrufe mehr ausführen.
CloseAndCommit		Beendet den Dateitransfer
GenerateFileForRead		Wird nicht unterstützt
GenerateFileForWrite		Generiert eine FileType Instanz, die für den Dateitransfer genutzt wird.
TransferState		Transferstatus Objekt
GetUpdateBehavior		Zeigt Update-Eigenschaften der geladenen Firmware
InputArguments	String ManufacturerUri String SoftwareRevision String[] PatchIdentifiers	ManufacturerUri und SoftwareRevision; dient zur Identifikation des vorher geladenen Firmwarepakets. Das Argument <i>PatchIdentifiers</i> ist ohne Funktion und muss leer bleiben.
OutputArguments	UInt32	Beschreibt, wie der TSN-Switch ein Update durchführen kann. Mögliche Werte 4 RequiresPowerCycle
PendingVersion		Zeigt Eigenschaften der geladenen Firmware <sup>1)</sup>
Manufacturer	LocalizedText	Hersteller
ManufacturerUri	String	Hersteller-URI
SoftwareRevision	String	Version des Firmwarepakets
<b>PowerCycle</b>		
CurrentState	LocalizedText	Nutzer-lesbarer Rebootstatus Mögliche Werte NotWaitingForPowerCycle WaitingForPowerCycle
Id	Nodeld	Maschinen-lesbarer Rebootstatus Mögliche Werte 299 NotWaitingForPowerCycle Objekt 301 WaitingForPowerCycle Objekt
UpdateStatus	LocalizedText	Nutzerinformation und Rückmeldung für den gesamten Updatevorgang, siehe <a href="#">Updatestatus</a>

1) Nur wenn die entsprechende Firmwareupdate-Datei bereits auf das Zielgerät übertragen wurde und bereit zur Installation ist.

### Fehlernachrichten

Nr.	Text	Bedeutung
0	[ERROR] File invalid or not loaded	Wird angezeigt, wenn der Knoten <i>Root/Objects/DeviceSet/0ACST052.1/FirmwareUpdate/Loading/PendingVersion</i> ausgelesen wird, das Firmwarepaket jedoch ungültig ist oder fehlt.

**Updatestatus**

Nr.	Text	Bedeutung
0	[ERROR] Requested version not present or file invalid	Eingabeparameter der Methode <i>GetUpdateBehavior</i> oder <i>InstallSoftwarePackage</i> passen nicht zum geladenen Firmwarepaket. Die angefragte Version ist nicht vorhanden, oder das Firmwarepaket ist ungültig.
1	[ERROR] Installation failed. See FirmwareIn-stall.log in system dump archive.	Die von der Methode <i>InstallSoftwarePackage</i> ausgelöste Installation des Firmwarepakets wurde gestartet, ist jedoch fehlgeschlagen. Weiterführende Informationen sind im "SystemDump" Objekt, in der Datei "FirmwareInstall.log", zu finden.
2	[ERROR] Action not allowed in current state	Methodenaufruf wurde verwehrt, da dieser im aktuellen Status nicht erlaubt ist.
3	[INFO] Installation successful, reboot required	Der TSN-Switch benötigt einen Neustart, um die installierte Firmware zu aktivieren. Dieser kann durch Aufruf der Methode <i>Root/Objects/DeviceSet/0ACST052.1/Configuration/Control/Reboot</i> oder durch ein Aus- und Einschalten der Spannungsversorgung erfolgen.

# 13 OTB2103.9110

## 13.1 Allgemeines

Die einreihige 3-polige Feldklemme wird als Spannungsversorgungsklemme verwendet.

## 13.2 Bestelldaten

Bestellnummer	Kurzbeschreibung	Abbildung
	<b>Feldklemmen</b>	
OTB2103.9110	Zubehör Feldklemme, 3-polig, Push-in-Klemme 2,5 mm <sup>2</sup>	

Tabelle 5: OTB2103.9110 - Bestelldaten

## 13.3 Technische Daten

Bestellnummer	0TB2103.9110
<b>Allgemeines</b>	
Zulassungen	
CE	Ja
UL	cULus E115267 Industrial Control Equipment
<b>Feldklemme</b>	
Anmerkung	Nennwerten nach UL
Anzahl der Pole	3
Art der Klemmung	Ausführung als Push-in-Klemme <sup>1)</sup>
Kabelart	Nur Kupferdrähte (keine Aluminiumdrähte!)
Rastermaß	5,08 mm
<b>Anschlussquerschnitt</b>	
AWG-Leiter	AWG 24 bis 12
Aderendhülse mit Kunststoffkragen	0,25 bis 2,50 mm <sup>2</sup>
eindrätig	0,20 bis 2,50 mm <sup>2</sup>
feindrätig	0,20 bis 2,50 mm <sup>2</sup>
mit Aderendhülse	0,25 bis 2,50 mm <sup>2</sup>
<b>Elektrische Eigenschaften</b>	
Nennspannung	300 V
Nennstrom <sup>2)</sup>	10 A / Kontakt
Durchgangswiderstand	≤5 mΩ

Tabelle 6: OTB2103.9110 - Technische Daten

- 1) Die Feldklemme in Push-in-Ausführung ist nicht anreihbar.
- 2) Die jeweiligen Grenzdaten der Geräte sind zu berücksichtigen!

### 13.4 Prüfzugang

Jeder Kontakt ist mit 2 zusätzlichen Öffnungen für die Benutzung einer Prüfspitze versehen.

Prüfzugänge Vorne an der Feldklemme	Prüfzugänge Oben an der Feldklemme
