

OPC UA over TSN

Technologiebeschreibung

Version: **1.00 (Mai 2021)**
Bestellnr.:

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

Disclaimer

Alle Angaben entsprechen dem aktuellen Stand zum Zeitpunkt der Erstellung des Handbuches. Jederzeitige inhaltliche Änderungen dieses Handbuches ohne Ankündigung bleiben vorbehalten. B&R Industrial Automation GmbH haftet insbesondere für technische oder redaktionelle Fehler in diesem Handbuch 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 Handbuch 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 Handbuch 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 Handbücher dieser Drittanbieter heranzuziehen und insbesondere die dort enthaltenen Sicherheitshinweise und technischen Spezifikationen zu beachten. Die Kompatibilität der in diesem Handbuch 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.

1 Einleitung	4
2 Szenarien	5
2.1 Ausbaustufe PubSub.....	5
2.1.1 PubSub-Kommunikation zwischen B&R Steuerungen.....	5
2.1.2 PubSub-Kommunikation mit Fremdherstellern.....	6
2.1.3 PubSub und Companion Specifications.....	7
2.1.4 Übertragungsgarantie am TSN Netzwerk.....	8
2.2 Ausbaustufe PTP.....	9
2.2.1 Gleichzeitiges Steuern.....	9
2.3 Ausbaustufe PubSub Echtzeit.....	10
2.3.1 Echtzeitkommunikation zwischen B&R Steuerungen.....	10
2.3.2 Echtzeitkommunikation mit Fremdgeräten.....	11
2.3.3 Achskopplung.....	12
2.3.4 Big Data.....	13
2.4 Ausbaustufe Switch-Konfiguration.....	14
2.5 Ausbaustufe PubSub Features.....	14
3 Unterstützte Produkte	15
4 OPC UA	16
4.1 Was ist OPC?.....	16
4.2 OPC UA Client Server.....	16
4.2.1 Funktionale Äquivalenz.....	17
4.2.2 Plattformunabhängig.....	17
4.2.3 Sicherheit.....	17
4.2.4 Erweiterbar.....	18
4.2.5 Informationsmodell und Zugriff.....	18
4.3 OPC UA PubSub.....	19
4.3.1 Was ist PubSub?.....	19
4.3.2 PubSub für Echtzeitkommunikation.....	20
5 TSN	21
5.1 Einführung.....	21
5.2 ISO/OSI-Modell.....	22
5.3 Zeitsynchronisierung.....	24
5.4 Traffic Types.....	26
5.5 Quality of Service (QoS).....	27
5.6 Mechanismen.....	28
5.6.1 IEEE 802.1Qbv.....	28
5.6.2 IEEE 802.1Qav.....	29
5.6.3 IEEE 802.1Qci.....	30
5.6.4 Konfiguration (IEEE 802.1Qcc).....	31
5.6.5 IEEE 802.1CB.....	32
5.7 Optimierungen.....	33
5.7.1 Cut/Trough.....	33
5.7.2 Pre-Emption.....	34
6 OPC UA Field Level Communication	35
6.1 Hintergrund.....	35
6.2 FLC Initiative.....	36
6.3 System Architecture Outline.....	36

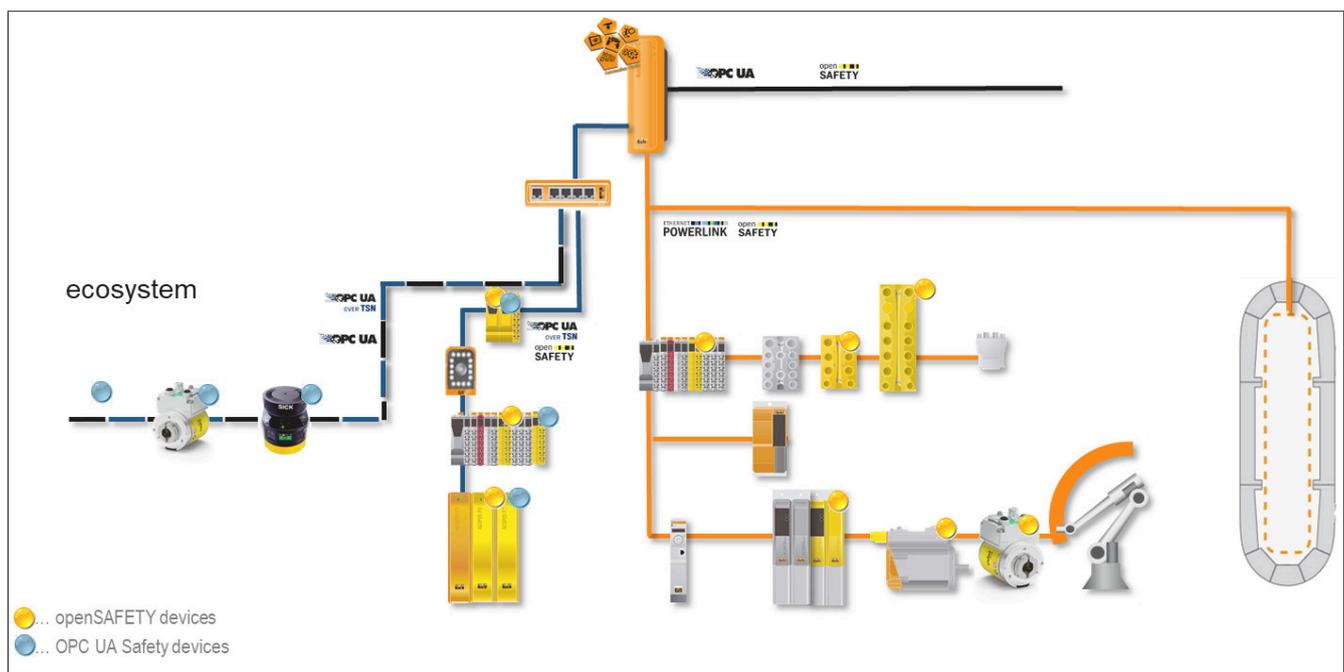
1 Einleitung

B&R setzt bei der industriellen (Echtzeit-) Kommunikation auf OPC UA over TSN und verwendet den Standard seit 2021 für die Controller-zu-Controller-Kommunikation. OPC UA over TSN ermöglicht es, OT- und IT-Netzwerke zusammenzuführen. Dabei werden die folgenden OT-relevanten Kommunikationseigenschaften erweitert:

- Höchste deterministische Echtzeit-Performance
- Bandbreite (nicht Echtzeit) maximal ausnutzbar
- Integrierte Security-Lösung
- Integrierte Safety-Lösung
- Selbstbeschreibende Geräteinformationen
- OPC UA 100% standardkonform
- IEEE Ethernet TSN 100% standardkonform
- Anwendungsprofile und Companion-Spezifikationen
- Riesiges Ökosystem

Typische OPC-UA-over-TSN-Geräte verfügen über einen OPC-UA-Server. Auf diesem wird ein Informationsmodell gehostet, das Geräteinformationen darstellt, z. B. Identifikationseigenschaften, Asset Model, Konfigurationsparameter, verfügbare Kanäle, Diagnoseinformationen und gerätespezifische Funktion. Zudem sind die Geräte mit einer oder mehreren Ethernet-Netzwerkschnittstellen ausgestattet, die TSN unterstützen. Geräte mit mehr als einer Schnittstelle verfügen über einen internen TSN-Switch, dessen Funktionen und Konfigurationsparameter in standardisierten YANG-Modellen aufgelegt und mit dem NETCONF-Protokoll konfiguriert werden. Ethernet TSN bildet somit die Netzwerkinfrastruktur, um OPC-UA-Geräte einheitlich verbinden zu können. Die Field Level Communications Initiative der OPC Foundation definiert, wie verschiedene TSN-Mechanismen hersteller- und protokollunabhängig genutzt und konfiguriert werden (für Netzwerke gemäß IEC/IEEE 60802).

Mögliche Topologie eines B&R-Systems



2 Szenarien

Die in diesem Kapitel beschriebenen Szenarien zeigen Anwendungsgebiete, in denen OPC UA over TSN bzw. Teile davon eingesetzt werden können.

2.1 Ausbaustufe PubSub

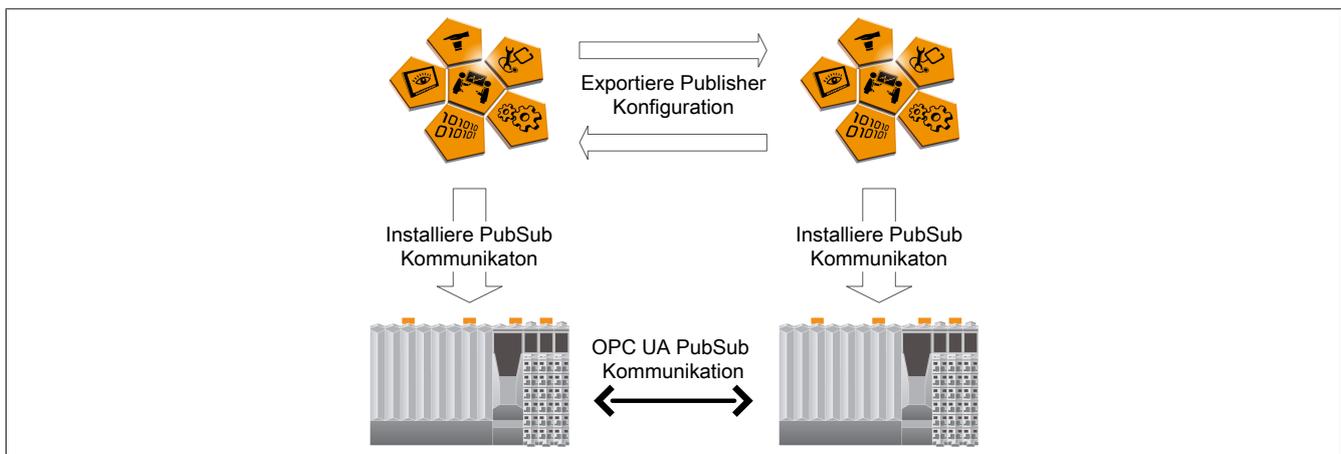
2.1.1 PubSub-Kommunikation zwischen B&R Steuerungen

OPC UA PubSub kann verwendet werden, um in einem bestehenden Ethernet-Netzwerk zwischen unterschiedlichen Maschinen, welche B&R Steuerungen einsetzen, nicht-echtzeitkritische Daten auszutauschen. PubSub kann z. B. in all jenen Anwendungsbereichen eingesetzt werden, welche bisher durch Modbus TCP, PROFINET oder Ethernet/IP abgedeckt wurden. Gegenüber OPC UA Client/Server-Verbindungen verringert sich speziell bei mehreren Kommunikationspartnern die CPU-Auslastung deutlich. Zudem wird die Echtzeitfähigkeit verbessert.

Es ist auch mögliche echtzeitnahe Kommunikation nur durch OPC UA PubSub, ohne Verwendung spezieller TSN-Mechanismen, auf einem nicht ausgelasteten Netzwerk und auf nicht ausgelasteten Steuerungen zu erreichen. Wenn es für den durch die Steuerungen zu regelnden Prozess ausreichend ist, dass die Kommunikation mehrere Millisekunden dauert und keine harte Echtzeit erforderlich ist, dann kann OPC UA PubSub ohne TSN auch für solche Anwendungsbereiche eingesetzt werden.

Zur Umsetzung dieses Szenarios werden beide B&R Steuerungen mit dem Automation Studio konfiguriert, wobei zwischen den Automation Studio Konfigurationen der beiden Steuerungen die Publisher Konfigurationen über einen Export/Import-Mechanismus ausgetauscht werden.

Die nötigen Konfigurationsschritte werden im Detail in der Automation Help im Abschnitt "PubSub Konfiguration" beschrieben.

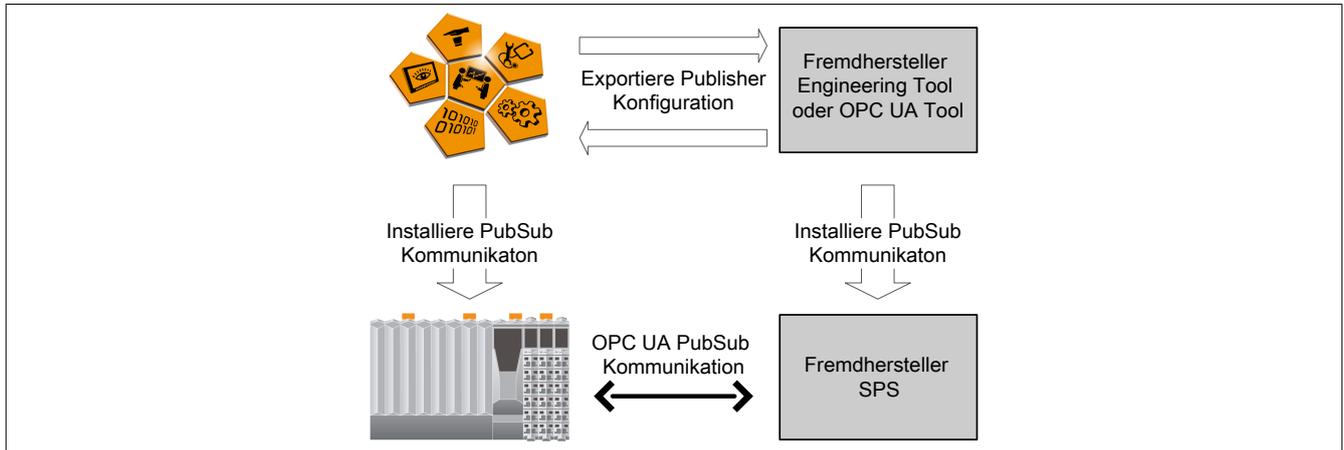


2.1.2 PubSub-Kommunikation mit Fremdherstellern

OPC UA PubSub kann, wie beim Szenario zur OPC UA PubSub Kommunikation zwischen B&R Steuerungen, auch zur Kommunikation mit Fremdherstellergeräten eingesetzt werden.

Das Fremdgerät wird mit dem Engineering Tool des Fremdgeräteherstellers oder mit anderen OPC UA Tools konfiguriert. Die PubSub Konfiguration wird mit Automation Studio über ein standardisiertes Dateiformat ausgetauscht, sodass in Automation Studio vom Fremdherstellergerät angebotene Daten für eine Subscriber-Konfiguration herangezogen werden können und das Fremdherstellergerät die von Automation Studio erstellte Publisher-Konfiguration interpretieren kann.

Die nötigen Konfigurationsschritte für den Automation Studio Anteil werden im Detail in Automation Help im Kapitel "PubSub Konfiguration" beschrieben.

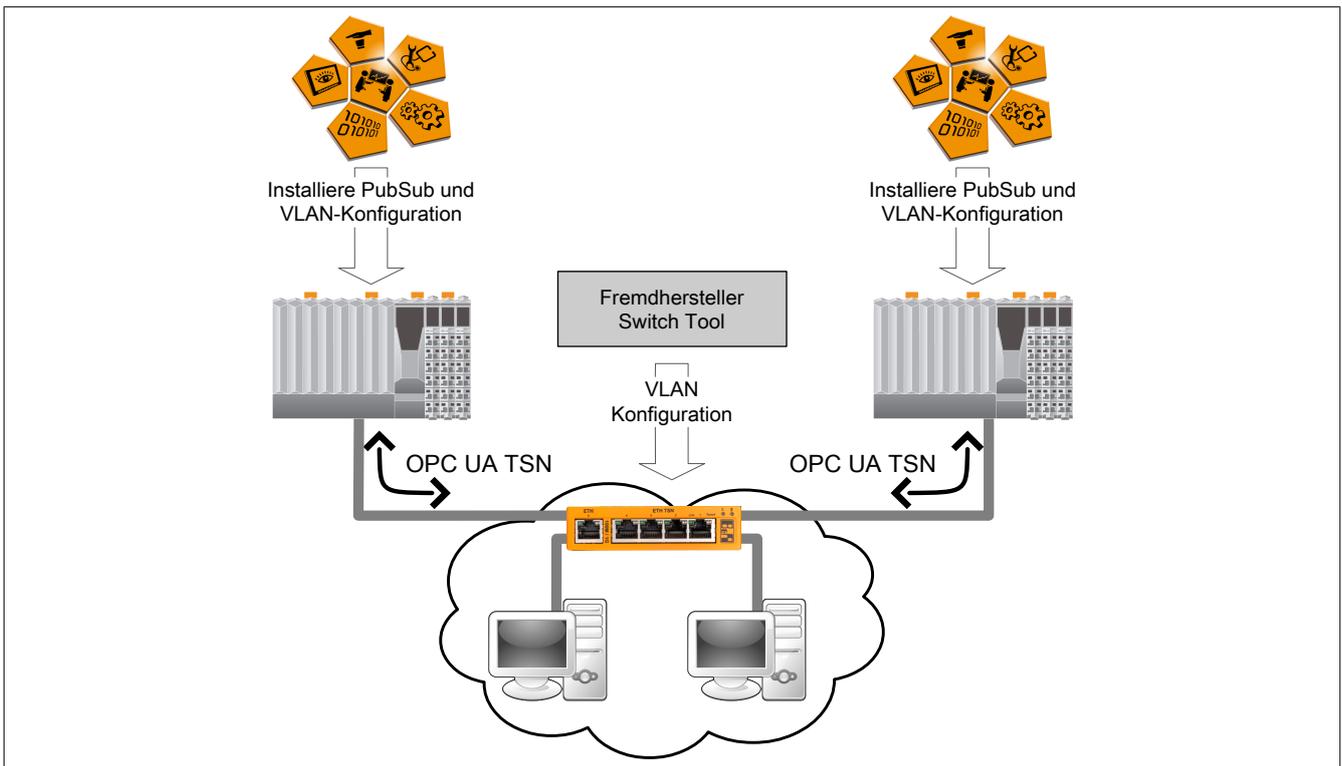


2.1.4 Übertragungsgarantie am TSN Netzwerk

Mit OPC UA over TSN bieten B&R-Steuerungen eine über konvergierte TSN-Netzwerkinfrastrukturen 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 am Netzwerk gefährdet wird. Dazu werden PubSub Nachrichten mit VLAN-Tags markiert, sodass ein TSN-fähiger Switch diese höherprior behandelt und dieser Verkehr somit nicht vom restlichen Best-Effort Verkehr gestört 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. Diese VLAN Information muss dann auch auf dem TSN Switch konfiguriert werden, damit diese die PubSub Nachrichten dann höher priorisiert und somit anderer Netzwerkverkehr diese Nachrichten nicht behindert.

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



2.2 Ausbaustufe PTP

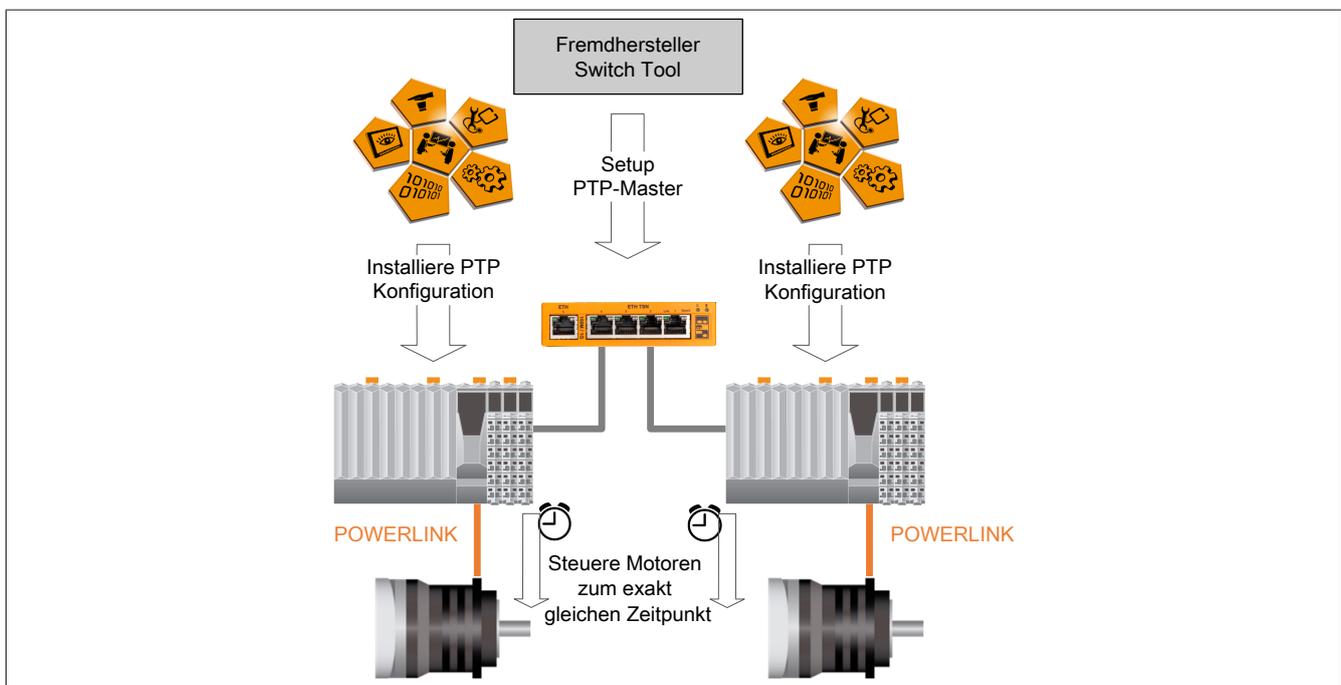
2.2.1 Gleichzeitiges Steuern

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

Mit der synchronisierten Taskklasse ist es dann 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 dann in der Abarbeitung der Taskklasse1 die aktuelle PTP-Zeit auslesen und somit können beide Steuerungen dann 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, was durch die aktuelle Implementierung 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 (siehe "[PubSub für Echtzeitkommunikation](#)" auf Seite 20).

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



2.3 Ausbaustufe PubSub Echtzeit

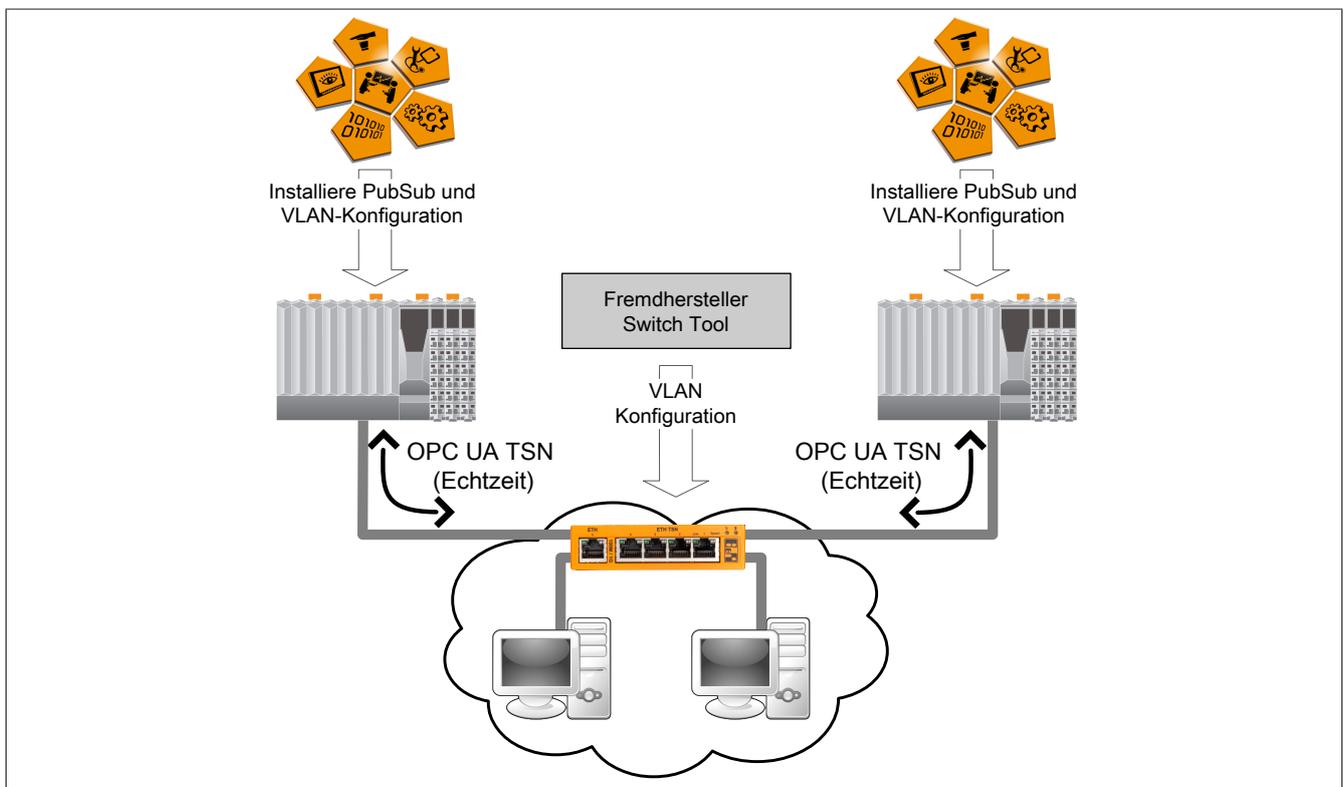
2.3.1 Echtzeitkommunikation zwischen B&R Steuerungen

Durch den definierten Aufbau der PubSub Frames¹⁾ und die Verwendung von standardisierten TSN-Mechanismen wird eine echtzeitfähige und performante Kommunikation über Standard-Ethernet-Hardware ermöglicht. Somit können Anwendungsfälle, welche bisher nur mit spezieller Hardware-Unterstützung, wie z. B. bei POWERLINK, möglich waren nun auch ohne solche Hardwareunterstützung umgesetzt werden.

Mittels PubSub kann somit eine echtzeitfähige Kommunikation zwischen Steuerungen ("Controller to Controller Kommunikation") umgesetzt werden. Im Vergleich zu POWERLINK iCN bietet PubSub den Vorteil, dass die Kommunikation über ein Netzwerk erfolgen kann, auf welchem zusätzlicher Ethernet-Verkehr möglich ist und es bietet den Vorteil, dass mehrere Fremdhersteller die PubSub Technologie unterstützen.

Um die hoch-prioren PubSub Daten von den restlichen Daten im Netzwerk unterscheiden zu können, werden die PubSub Daten mit einem VLAN-Tag versehen, sodass ein TSN-fähiger Switch diese höher-prior behandelt und dieser Verkehr somit nicht vom restlichen Verkehr gestört wird.

Der Austausch der PubSub Konfigurationen erfolgt (Automation Help Abschnitt „PubSub Konfiguration“) über den Export und Import der Konfigurationen zwischen den beteiligten Kommunikationspartnern. Die Konfiguration des TSN Switch erfolgt durch ein beliebiges Fremdhersteller Tool zur Switch-Konfiguration.



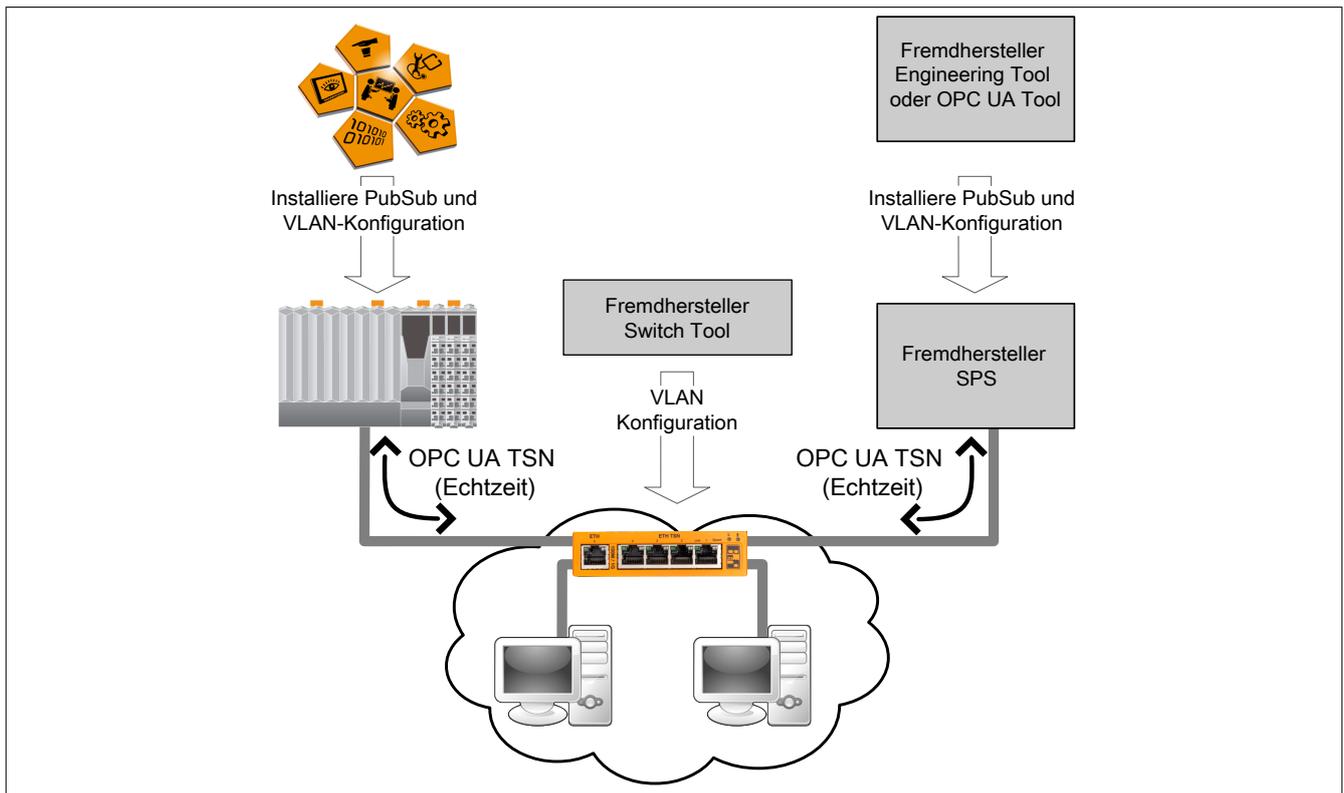
¹⁾ Im "Periodic Fixed Frame Format"

2.3.2 Echtzeitkommunikation mit Fremdgeräten

Durch die standardisierte PubSub Technologie ist es möglich mit Steuerungen von Fremdherstellern zu kommunizieren. Sofern diese Hersteller ebenso eine echtzeitfähige Kommunikation zur Verfügung stellen, ist es möglich über eine standardisierte Technologie und über ein Standard-Ethernet-Netzwerk in Echtzeit mit deren Geräten zu kommunizieren.

Insbesondere in Kombination dieser Fähigkeit mit OPC UA PubSub Companion Specifications eröffnen sich dadurch neue Möglichkeiten. So ist es möglich, dass herstellerunabhängig Maschinen, welche Teil eines echtzeitkritischen Prozesses sind, sehr einfach kombiniert und ausgetauscht werden können.

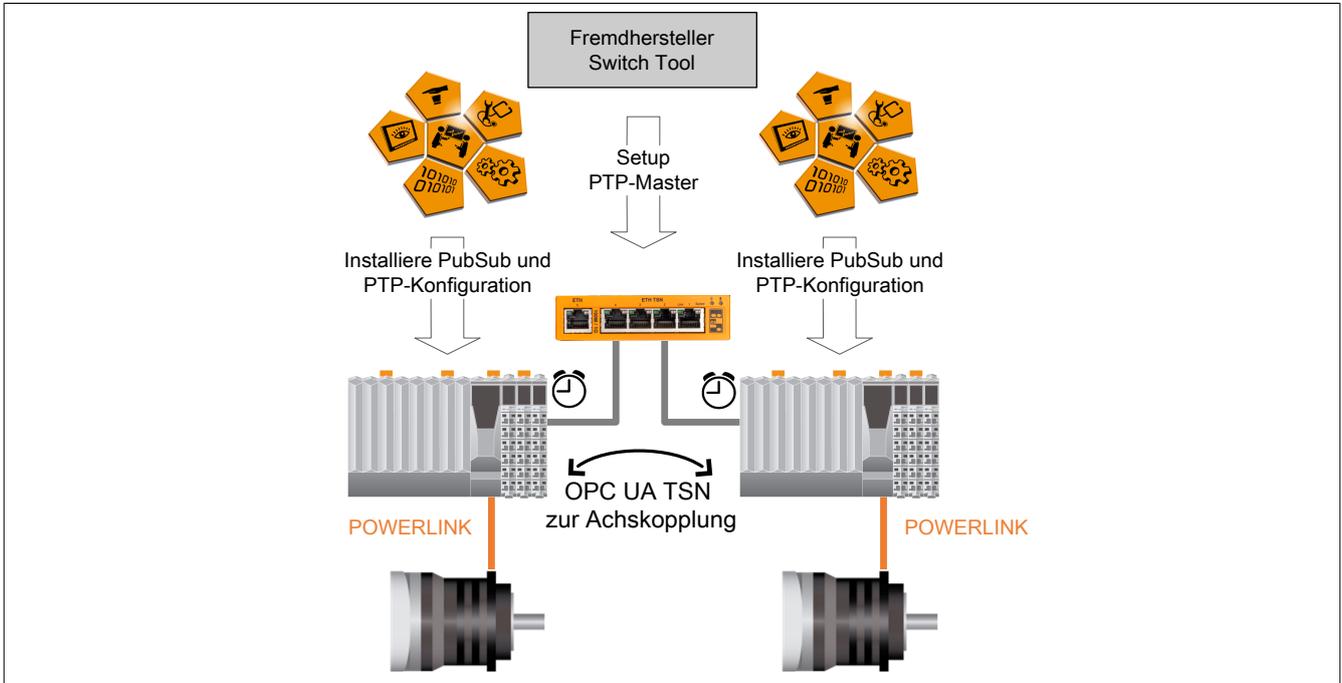
Die PubSub Konfiguration erfolgt wie im vorherigen Kapitel zur Echtzeitkommunikation zwischen B&R Steuerungen beschrieben. Das gilt auch für die die Konfiguration des TSN Switch bzw. kann diese auch durch die Fremdhersteller-Steuerung erfolgen.



2.3.3 Achskopplung

Mit der performanten PubSub Echtzeitkommunikation und durch die Möglichkeit die Steuerungen über IEEE 802.1AS (gPTP) zu synchronisieren ist es möglich POWERLINK Achsen an unterschiedlichen Steuerungen zu koppeln.

Die PubSub Kommunikation ermöglicht Zykluszeiten ab 400 μ s mit einer Latenz von nur 4 Zyklen. Durch PTP können die kommunizierenden Steuerungen auf einige Mikrosekunden genau synchronisiert werden und auch die an den Steuerungen angeschlossenen POWERLINK-Geräte werden so genau synchronisiert. Somit ist es möglich, Achsen mit gleicher Zykluszeit zwischen den Steuerungen zu synchronisieren.

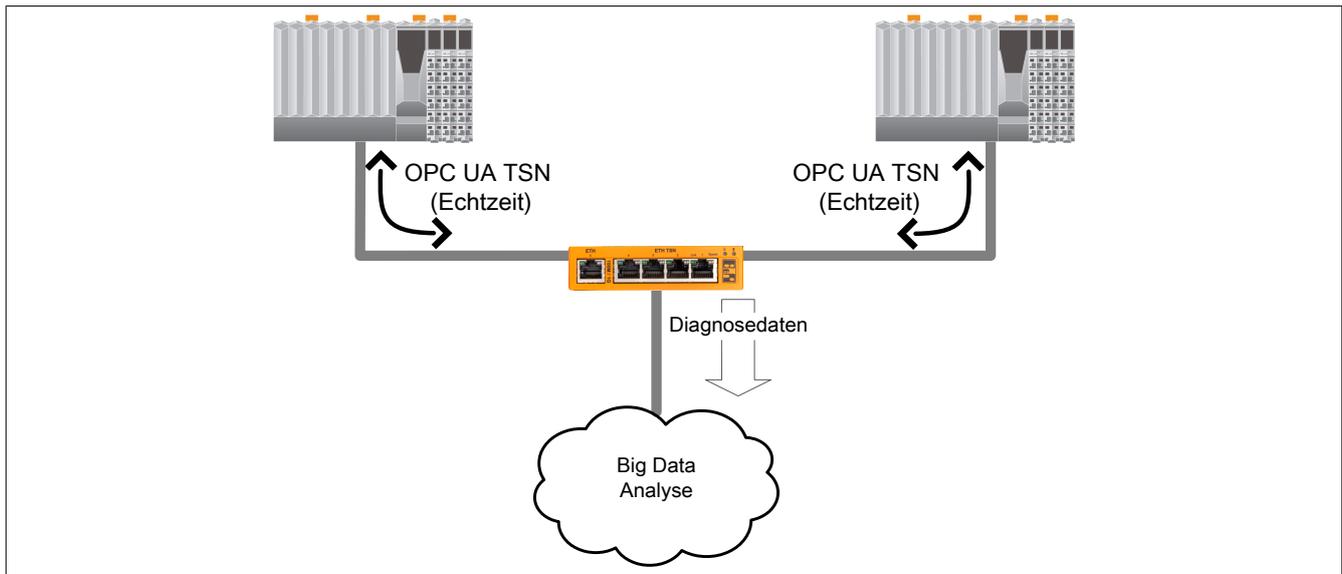


2.3.4 Big Data

Mittels TSN-Mechanismen kann man die kommunizierten 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, wobei noch immer der korrekte Echtzeitverkehr garantiert werden kann.

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 TSN hingegen ist es möglich "Hard Real Time" zu betreiben, auch wenn das Netzwerk stark ausgelastet ist.

Somit sind Anwendungsfälle denkbar, bei denen man sehr viele Daten von Steuerungen abgreift, welche gleichzeitig echtzeitkritische Kommunikation betreiben.

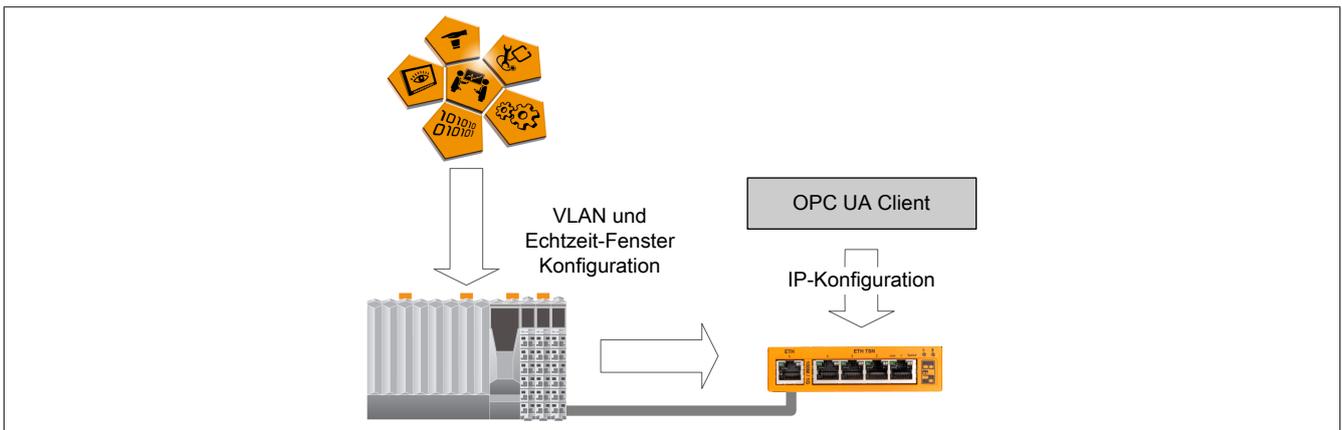


2.4 Ausbaustufe Switch-Konfiguration

Um die Konfiguration der Timing-Parameter des TSN Switch für den Anwender zu vereinfachen, soll diese mittels Automation Studio erstellt werden können. Eine im Automation Studio erstellte Konfiguration wird dann an das Automation Runtime übertragen und das Automation Runtime konfiguriert den Switch. Durch diesen Weg der Konfiguration ist es sogar möglich, dass eine defekte Switch-Hardware ausgetauscht und die neue Hardware wieder in Betrieb genommen werden kann, ohne dass dafür Automation Studio benötigt wird.

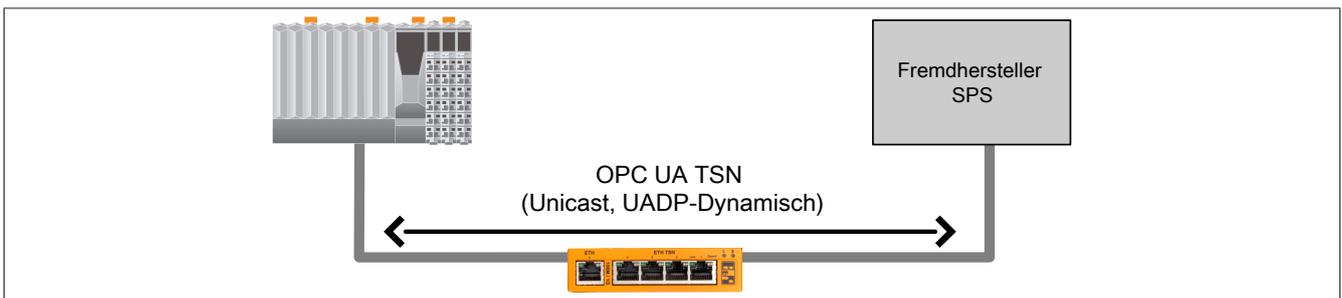
Es ist möglich für den TSN Switch Zeitfenster zu konfigurieren, bei welchen nur der hoch-priore mit VLANs markierte PubSub Verkehr weitergeleitet wird. Somit kann sichergestellt werden, dass dieser Verkehr nicht gestört wird. Damit der TSN Switch identifiziert werden kann, muss er eine eindeutige IP-Adresse haben. Diese IP-Adresse muss im Vorfeld mittels OPC UA Client am Switch konfiguriert werden.

Mit dem zusätzlichen Feature der Konfiguration der TSN Switch Zeitfenster sind die in den vorherigen Kapiteln aufgeführten Anwendungsfälle, welche Netzwerke betreffen die auch Best-Effort Teilnehmer beinhalten, nun leichter umzusetzen. Für die Konfiguration der Zeitfenster ist es nun nicht mehr nötig ein Fremdhersteller-Tool heranzuziehen.



2.5 Ausbaustufe PubSub Features

Um die PubSub Kommunikation mit möglichst vielen Fremdherstellern zu unterstützen, werden weitere PubSub Features wie die Kommunikation über Unicast Adressen oder die Kommunikation mit dem UADP-Dynamic Fixed Profile unterstützt. Durch diese breitere Unterstützung der von PubSub standardisierten Features ist es nun auch möglich mit verschiedenen Fremdherstellern zu kommunizieren, welchen jeweils nur einen kleinen Teil der PubSub Features unterstützen.



3 Unterstützte Produkte

OPC UA wird ab SG4 Automation Runtime Version 4.0 unterstützt.

OPC UA PubSub wird ab SG4 Automation Runtime Version 4.90²⁾ unterstützt.

IEEE 802.1AS (gPTP) wird ab SG4 Automation Runtime Version 4.92 unterstützt.

Hochpräzise Zeitsynchronisation (<5 µs) wird vom Produkt 0ACST052.1 und den folgenden Zielsystemen unterstützt: X20CPx86x, xPC2200, xPC3100, PPC900, C80.

OPC UA PubSub TSN wird ab SG4 Automation Runtime Version 4.92 unterstützt.

Die hochpräzise, zeitgetriggerte Steuerung von Sende- und Empfangsfenstern wird auf den folgenden Zielsystemen unterstützt: X20CPx86x, xPC2200, xPC3100, PPC900, C80.

²⁾ Die folgenden Zielsysteme/Funktionen werden nicht unterstützt: Controller-Redundanz, CiR, Hypervisor und Anwendungsmodule.

4 OPC UA

Die Abschnitte 4.1 bis 4.3.1 wurden der Website der OPC Foundation ³⁾ entnommen und übersetzt.

4.1 Was ist OPC?

OPC ist ein Interoperabilitäts-Standard für den sicheren und zuverlässigen Austausch von Daten in der industriellen Automatisierung sowie in anderen Branchen. OPC ist plattformunabhängig und gewährleistet den nahtlosen Informationsfluss zwischen Geräten verschiedener Hersteller. Die OPC Foundation hat den Standard entwickelt und ist auch für dessen Pflege verantwortlich.

Der OPC-Standard beinhaltet eine Reihe von Spezifikationen, die von Anbietern, Endanwendern und Softwareentwicklern entwickelt wurden. Diese Spezifikationen definieren die Schnittstellen für die Client-Server-Kommunikation sowie die Server-Server-Kommunikation. Zudem beinhalten sie wichtige Teilspezifikationen für den Austausch von Echtzeitdaten, die Überwachung von Alarmen und Ereignissen sowie den Zugriff auf historische Daten.

Als der Standard 1996 zum ersten Mal veröffentlicht wurde, bestand sein Zweck darin, SPS-spezifische Protokolle (Modbus, Profibus etc.) in eine standardisierte Schnittstelle zu abstrahieren. Dadurch kommunizierten HMI-/SCADA-Systemen mit einer Zwischenstation, die generische SPS-Lese-/Schreibanfragen in gerätespezifische Anfragen umwandelte und umgekehrt. Darauf aufbauend entstand eine Reihe von Produkten, die es Endanwendern ermöglichten, Systeme zu implementieren, in denen alle Komponenten nahtlos miteinander über OPC kommunizierten.

Ursprünglich war der OPC-Standard auf Windows beschränkt. Das Akronym OPC leitet sich von OLE (Object Linking and Embedding) for Process Control ab. Diese Spezifikationen sind jetzt als OPC Classic⁴⁾ bekannt und haben sich in vielen Branchen durchgesetzt. Zum Beispiel in der Fertigungsindustrie, Gebäudeautomatisierung, Öl- und Gasindustrie, im erneuerbaren Energiesektor und in Versorgungsunternehmen.

Mit der Integration serviceorientierter Architekturen in Fertigungssysteme veränderten sich auch die Anforderungen an die Sicherheit und Datenmodellierung. Um diese Anforderungen erfüllen zu können, entwickelte die OPC Foundation die OPC-UA-Spezifikationen⁵⁾ und schaffte damit eine technologieoffene Architektur, die nicht nur über viele Funktionen verfügt, sondern auch zukunftssicher, skalierbar und erweiterbar ist.

Heute steht das Akronym OPC für Open Platform Communications.

4.2 OPC UA Client Server

OPC UA (Unified Architecture) wurde 2008 auf den Markt gebracht. Dabei handelt es sich um eine plattformunabhängige, serviceorientierte und erweiterbare Architektur, in der die gesamten Funktionen der einzelnen OPC-Classic-Spezifikationen zusammengefasst sind.

Mit dem neuen Standard konnten die ursprünglichen Ziele der Designspezifikation erfolgreich realisiert werden:

- **Funktionale Äquivalenz:** Alle auf COM basierenden OPC-Classic-Spezifikationen werden auf UA abgebildet
- **Plattformunabhängig:** Vom eingebetteten Mikrocontroller bis in die Cloud
- **Sicherheit:** Sicher: Verschlüsselung, Authentifizierung und Auditing
- **Erweiterbar:** Neue Funktionen können hinzugefügt werden, ohne bestehende Anwendungen zu beeinträchtigen
- **Informationsmodell und Zugriff:** Definition komplexer Informationen

³⁾ <https://opcfoundation.org/about/what-is-opc>

⁴⁾ <https://opcfoundation.org/about/opc-technologies/opc-classic/>

⁵⁾ <https://opcfoundation.org/about/opc-technologies/opc-ua/>

4.2.1 Funktionale Äquivalenz

Mit OPC UA wurden die Funktionen der OPC-Classic-Spezifikationen nicht nur erweitert, sondern sogar übertroffen:

- **Discovery:** Ermittlung von verfügbaren OPC-Servern auf lokalen PCs und/oder in Netzwerken
- **Address space:** Hierarchische Darstellung aller Daten (z. B. Dateien und Ordner), wodurch einfache und komplexe Strukturen von OPC-Clients erkannt und genutzt werden können
- **On-demand:** Lesen und Schreiben von Daten/Informationen basierend auf Zugriffsrechten
- **Subscriptions:** Überwachung von Daten/Informationen und zeitgerechte Benachrichtigung, wenn sich ein Wert basierend auf Kundenkriterien ändert
- **Events:** Benachrichtigung über wichtige Informationen basierend auf Kundenkriterien
- **Methods:** Clients können Programme gemäß den auf dem Server definierten Methoden ausführen

OPC-UA-Produkte und OPC-Classic-Produkte können auf einfache Weise verbunden werden. Dazu wird entweder ein COM-Wrapper oder ein Proxy-Wrapper benötigt. Diese stehen im Downloadbereich zur Verfügung.

4.2.2 Plattformunabhängig

Plattformunabhängigkeit ist im Hinblick auf die große Bandbreite an Hardwareplattformen und Betriebssystemen unerlässlich. Auf den folgenden ist OPC UA lauffähig:

- **Hardwareplattformen:** Traditionelle PC-Hardware, cloudbasierte Server, SPS, Mikrocontroller (ARM etc.)
- **Betriebssysteme:** Microsoft Windows, Apple OSX, Android oder eine beliebige Linux-Distribution, sowie SPS-Laufzeitumgebungen wie Automation Runtime, CoDeSys etc.

OPC UA bietet Interoperabilität innerhalb des gesamten Unternehmens – von Maschine zu Maschine, von Maschine zum Unternehmen und für alles dazwischen.

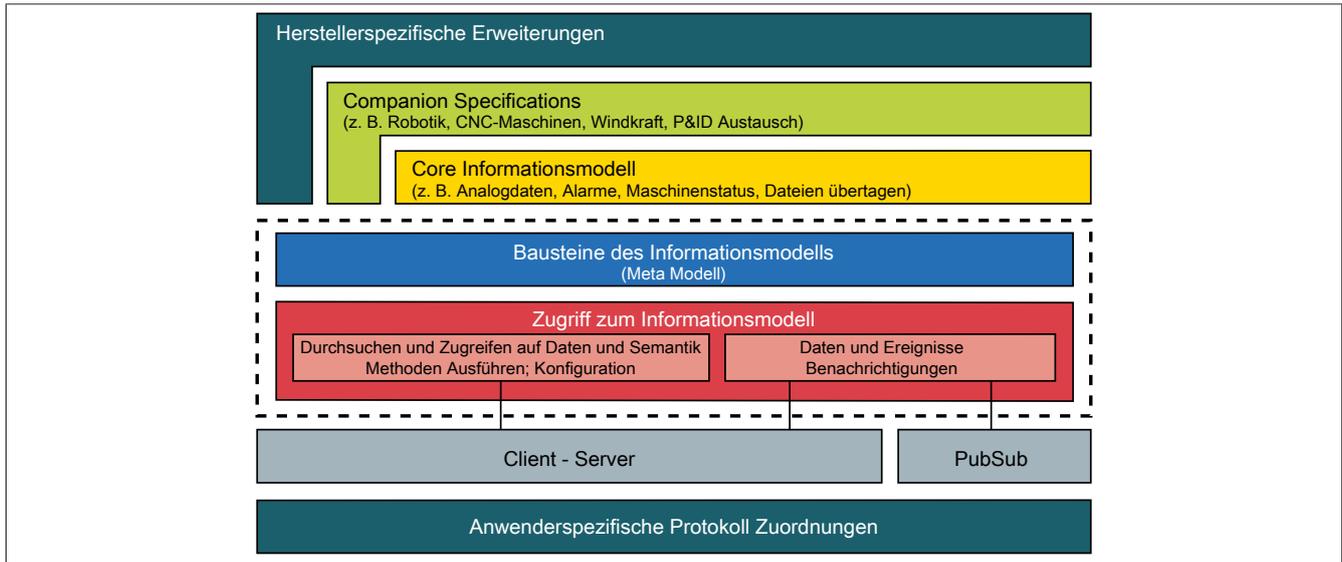
4.2.3 Sicherheit

Sicherheit ist einer der wichtigsten Überlegungen bei der Auswahl einer Technologie. OPC UA ist Firewall-freundlich und bietet mit einer Reihe von Funktionen ein Höchstmaß an Sicherheit:

- **Transport:** Zahlreiche definierte Protokolle bieten Optionen wie den ultraschnellen OPC-Binärtransport oder das universell kompatible JSON über WebSockets.
- **Verschlüsselung von Sitzungen:** Nachrichten werden in verschiedenen Verschlüsselungsstufen sicher übertragen.
- **Nachrichtensignatur:** Der Empfänger kann die Herkunft und Integrität der empfangenen Nachrichten mittels Signatur verifizieren.
- **Sequenzierung von Datenpaketen:** Die Anfälligkeit für Replay-Angriffe wird durch Sequenzierung eliminiert.
- **Authentifizierung:** Jeder UA-Client und UA-Server wird durch X509-Zertifikate identifiziert, die kontrollieren, welche Anwendungen und Systeme sich miteinander verbinden dürfen.
- **Benutzerkontrolle:** Anwendungen können Benutzer auffordern, sich zu authentifizieren (Anmeldedaten, Zertifikat, Web-Token etc.) und deren Zugriffsrechte und Adressraum-Ansichten einschränken oder erweitern.
- **Auditing:** Die Aktivitäten eines Benutzers und/oder des Systems werden in einem Audit Trail protokolliert.

4.2.4 Erweiterbar

Die vielschichtige Architektur von OPC UA bietet einen zukunftssicheren Rahmen für innovative Technologien und Methoden. Neue Transportprotokolle, Sicherheitsalgorithmen, Codierungsstandards oder Anwendungsdienste können jederzeit hinzugefügt werden. Die Rückwärtskompatibilität für bestehende Produkte bleibt dabei erhalten. UA-Produkte von heute sind mit denen von morgen kompatibel.



4.2.5 Informationsmodell und Zugriff

Die Informationsmodellierung in OPC UA ermöglicht es, Daten in Informationen umzuwandeln. Durch den objektorientierten Ansatz können selbst die komplexesten Strukturen modelliert und erweitert werden.

Das Framework für die Informationsmodellierung ist das zentrale Element von OPC UA. Es definiert die Regeln und wesentlichen Bausteine, die notwendig sind, um ein Informationsmodell mit OPC UA darzustellen. OPC UA definiert mehrere Kernmodelle, die in vielen Branchen angewendet werden können. Andere Organisationen bauen ihre Modelle darauf auf und stellen spezifischere Informationen mit OPC UA dar.

OPC UA definiert auch die notwendigen Zugriffsmechanismen auf Informationsmodelle.

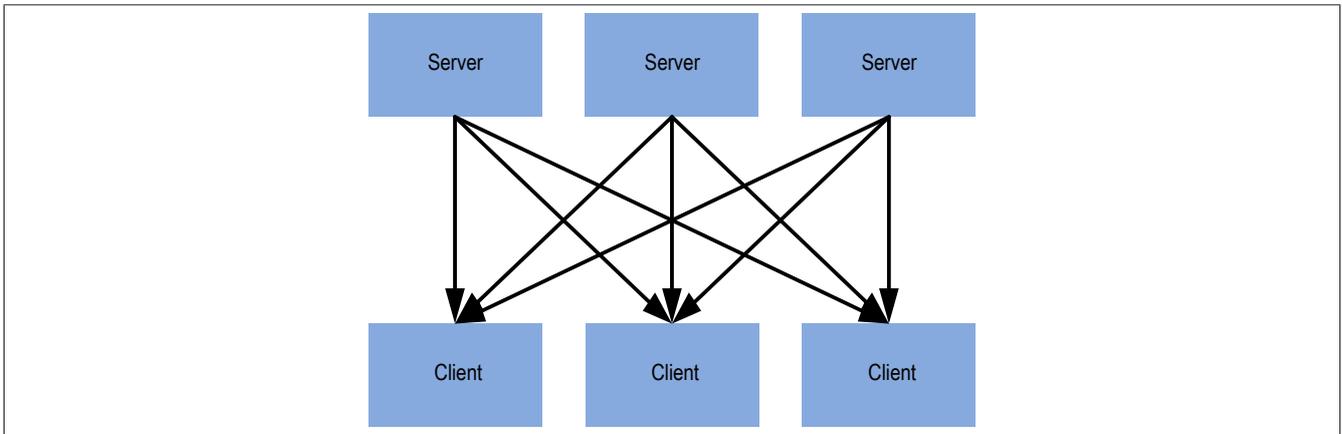
- Look-up-Mechanismus (Browsing) zum Lokalisieren von Instanzen und deren semantischer Bedeutung
- Lese- und Schreiboperationen für aktuelle und historische Daten
- Methodenausführung
- Benachrichtigung für Daten und Ereignisse

Für die Client-Server-Kommunikation steht der vollständige Informationsmodellzugriff mithilfe von Diensten zur Verfügung. Das entspricht dem Design-Paradigma der serviceorientierten Architektur (SOA), bei der ein Serviceanbieter Anfragen empfängt, sie verarbeitet und die Ergebnisse mit der Antwort zurücksendet.

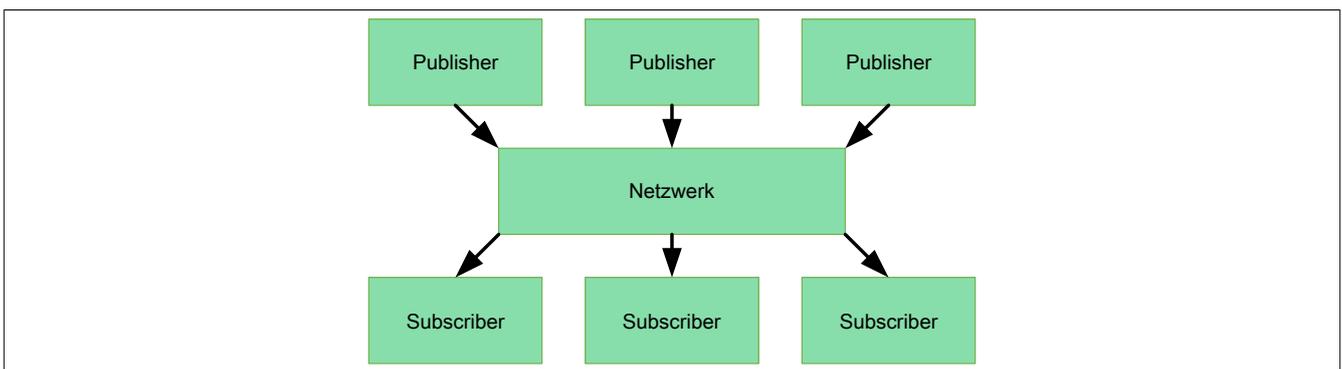
4.3 OPC UA PubSub

4.3.1 Was ist PubSub?

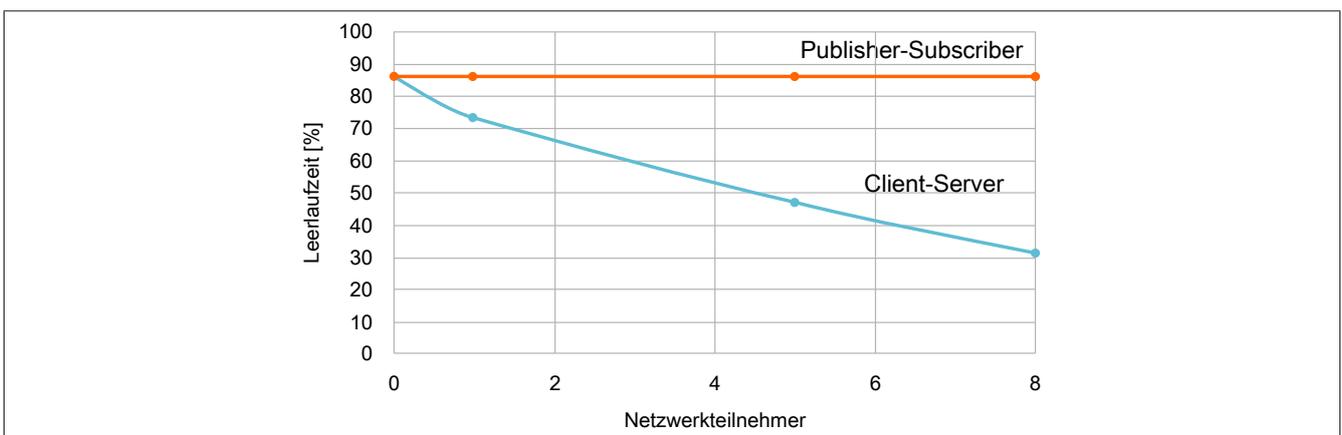
Publish-Subscribe (PubSub) bietet einen alternativen Mechanismus für die Daten- und Ereignisbenachrichtigung. Während in der Client-Server-Kommunikation jede Benachrichtigung für einen einzelnen Client mit garantierter Zustellung gilt, wurde PubSub für viele-zu-viele-Konfigurationen optimiert.



Mit PubSub tauschen OPC UA-Anwendungen Anforderungen und Antworten nicht direkt aus. Stattdessen senden Publisher Nachrichten an eine nachrichtenorientierte Middleware, ohne zu wissen, welche Subscriber es gegebenenfalls gibt. In ähnlicher Weise zeigen Subscriber Interesse an bestimmten Datentypen und verarbeiten Nachrichten, die diese Daten enthalten, ohne wissen zu müssen, woher sie stammen.

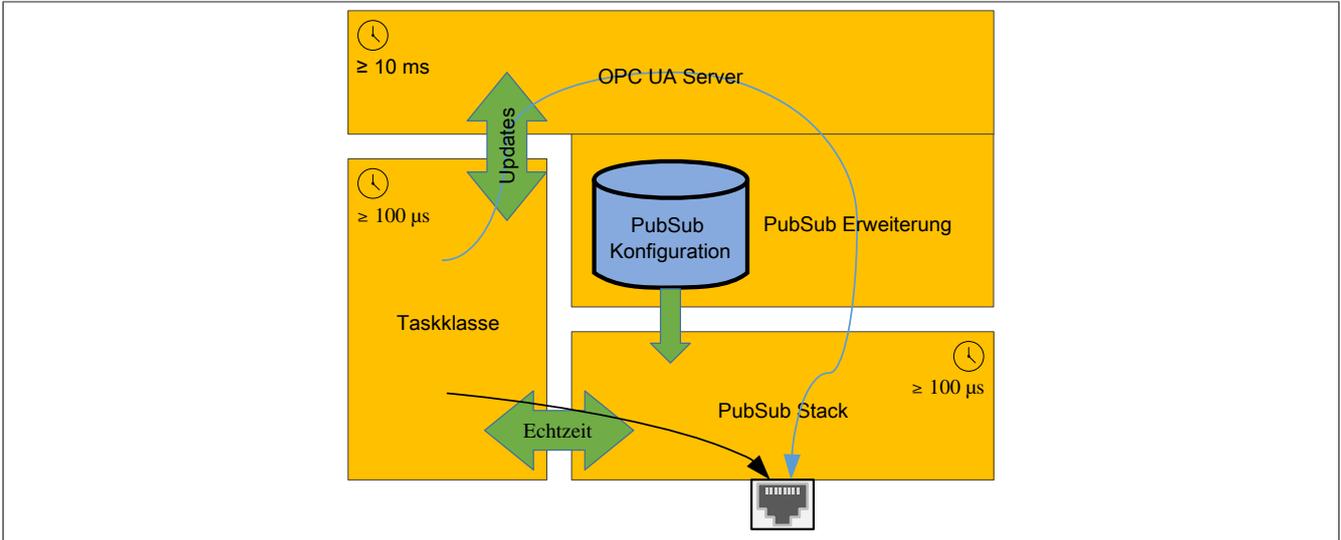


Auf diese Weise benötigt ein Publisher, der mit mehreren Subscriber kommuniziert, viel weniger Rechenressourcen als ein Server, der mit mehreren Clients kommuniziert.



4.3.2 PubSub für Echtzeitkommunikation

Neben der Unterstützung für viele-zu-viele Kommunikationsbeziehungen bringt OPC UA PubSub auch signifikante Verbesserungen bei der Echtzeitfähigkeit in der Kommunikation. Der PubSub Stack ist als eigener Prozess ausgeführt, der sowohl an den OPC UA Server, als auch an spezielle "Data Provider" angebunden ist. Bei der Anbindung an den Server sind die Updates der Daten von der Geschwindigkeit des Servers abhängig, der im B&R System in der Restzeit ausgeführt wird. Als eigener Data Provider kann dagegen das Taskklassensystem angesehen werden, wodurch eine Kommunikation mit der Echtzeitqualität wie bei POWERLINK erreicht wird. Der OPC UA Server erhält ebenfalls Updates zu den Prozessvariablen vom Data Provider, sodass auch auf diesem Weg relativ aktuelle Werte zur Verfügung stehen.



Jedes PubSub Frame kann mit einer eigenen Zykluszeit und einem zeitlichem Offset innerhalb des Zyklus versendet werden. Um diese harten Echtzeitanforderungen auch auf der Empfängerseite im Netzwerk zu garantieren, muss das Netzwerk entsprechende Mechanismen zur Verfügung stellen.

Diese Mechanismen werden im folgenden Kapitel über TSN beschrieben.

5 TSN

5.1 Einführung

Unter TSN versteht man Echtzeiterweiterungen des Ethernet Standards durch die IEEE. Die IEEE ist eine weltweite Organisation von hauptsächlich Experten der Elektrotechnik, die wissenschaftliche Konferenzen abhält, Journal-Publikationen herausgibt und Standardisierung betreibt. Das wohl bekannteste Standardisierungsprojekt ist IEEE Std. 802, unter dessen Schirm alle Themen der lokalen Netze (LANs) zusammengefasst sind. IEEE Std. 802.3 definiert Ethernet (einzelne Ports) und IEEE Std. 802.11 definiert Wireless LAN, während IEEE Std. 802.1 sich mit "LAN/MAN bridging and management", umgangssprachlich "Switches" beschäftigt.

Time Sensitive Networking (TSN) ist eine Arbeitsgruppe (AG) der IEEE 802.1⁶⁾.

Die ersten Echtzeiterweiterungen für Ethernet wurden für professionelle Audio- und Videotechnik erarbeitet und von 2009 bis 2011 veröffentlicht. Als die sich eröffnenden Möglichkeiten in der Standardisierung immer deutlicher wurden, wurde 2012 aus der Audio Video Bridging (AVB) AG die TSN AG. Sie hatte bis Ende 2019 ca. 10 Standards und 4 AVB-Standards veröffentlicht. Die Standards und Projekte lassen sich in 5 große Bereiche gliedern:

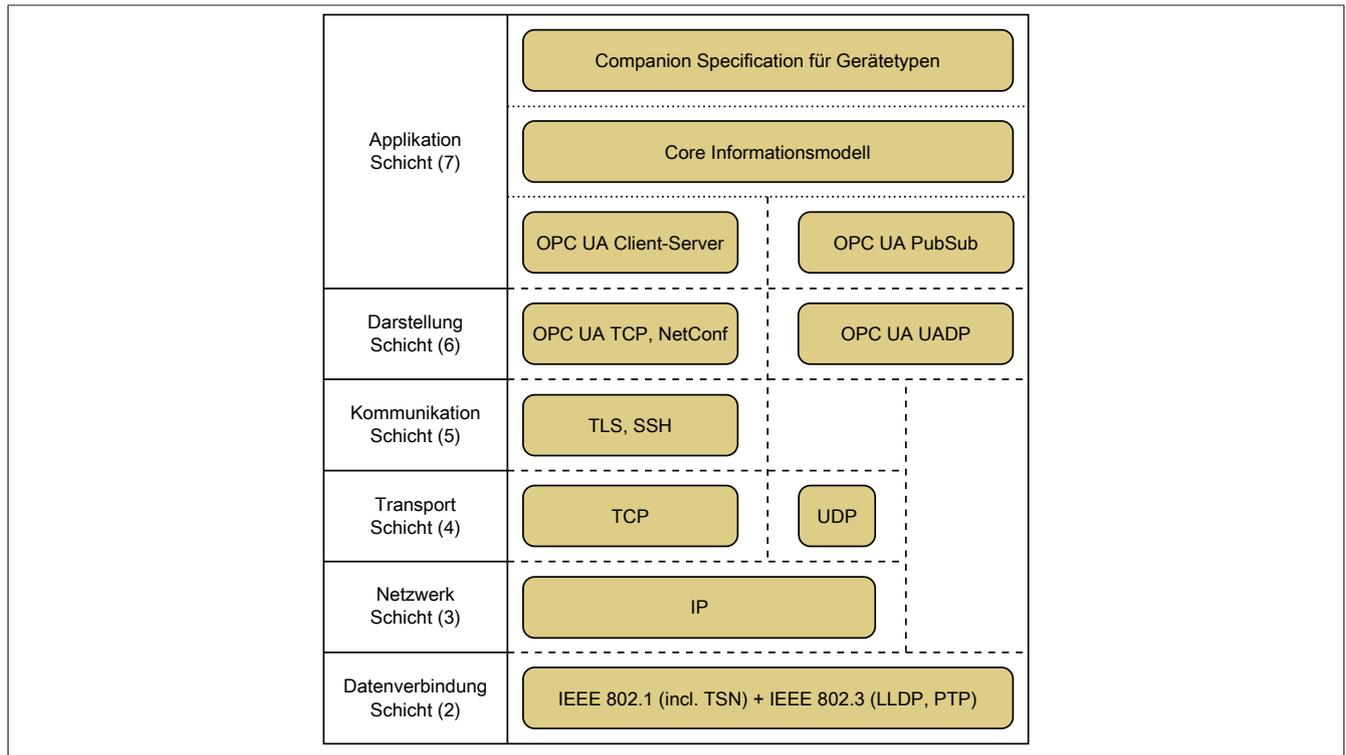
- Zeitsynchronisierung
- Redundanz
- Kurze, nach oben beschränkte Latenz
- Ressourcenverwaltung
- TSN-Profile

Zusammen erlaubt die Verwendung von TSN einen Grad an Determinismus in der Datenübertragung, der bisher nur Industrial Ethernet vorbehalten war. Darüber hinaus sind die TSN-Erweiterungen so spezifiziert, dass sie interoperabel im gleichen Netzwerk betrieben werden können. Harter Echtzeitverkehr, weicher Echtzeitverkehr, jeweils reservierte Bandbreiten für Videostreams, Ereignissen und Konfiguration, sowie Hintergrundverkehr uvm. sind mit jeweils individuellen Garantien am selben Kabel gleichzeitig umsetzbar (siehe dazu [5.4 "Traffic Types"](#)). Um eine Netzwerkkonfiguration planen und Garantien vergeben zu können, wird der Traffic in TSN-Netzen in Stream und non-Stream Traffic unterschieden. Ein Stream ist dabei ein gerichteter Informationsfluss von einem sogenannten "Talker" zu einem oder mehreren "Listeners" über einen definierten Pfad im Netzwerk (Switches). Üblicherweise werden solche Streams mit ihren gewünschten Echtzeiteigenschaften bei der Konfigurationsinstanz des Netzwerks angefordert. Diese kann den Stream zulassen, die Infrastruktur entsprechend konfigurieren und Talker und Listener die zu verwendenden Kommunikationsparameter mitteilen. Non-Stream Traffic kann - wie bei Ethernet mit QoS - in Klassen aufgeteilt werden. Die Klassen können dann als Ganzes eine Garantie bekommen (z. B. reservierte Bandbreite für Konfigurationsdaten), oder eine relative Priorität zueinander.

⁶⁾ <https://1.ieee802.org/tsn/>

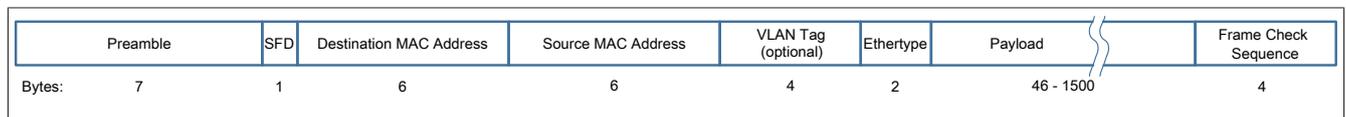
5.2 ISO/OSI-Modell

Im ISO/OSI-Referenzmodell für Kommunikationssysteme werden bei OPC UA over TSN alle verfügbaren Schichten ausgenutzt.



Datenverbindung - Schicht 2

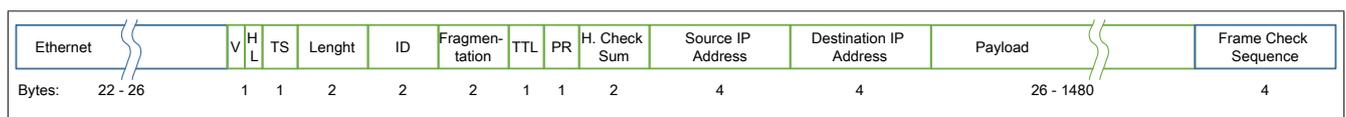
Ethernet (mit TSN) bildet Schicht 2. Auf dieser Schicht werden sogenannte Ethernet-Frames (oft auch nur als Frames bezeichnet) versendet, die über einen Ethernet-Header mit optionalem VLAN-Tag am Anfang des Frames identifiziert werden⁷⁾.



Für (TSN-) Streams ist der VLAN-Tag verpflichtend, hier wird die Kombination aus Destination MAC⁸⁾ und VLAN-ID (Teil des VLAN-Tags) als Stream ID verwendet und interpretiert. Der EtherType ist ein 16 Bit-Wert, der angibt, welches Protokoll auf der nächsten Schicht verwendet wird (z. B. IP). Die jeweils nächste Schicht ist im ISO/OSI-Modell immer in die Payload der darunterliegenden eingebettet (engl. encapsulated), siehe nächstes Bild. Für PubSub Frames gibt es die Möglichkeit, eine Nachricht (Network Message) direkt in einen Frame zu verpacken und mit eigenem EtherType zu kennzeichnen. Dadurch wird der Overhead der IP und UDP Header vermieden, wenn sie nicht benötigt werden.

Netzwerk - Schicht 3

Auf Schicht 3 wird das Internet Protokoll (IP-Protokoll) verwendet. Auf dieser Schicht werden sogenannte IP-Pakete (oft auch nur als Pakete bezeichnet) versendet, die über einen IP-Header am Anfang identifiziert werden. Der IP-Header beinhaltet unter anderem die IP-Adressen von Sender und Empfänger, das Protocol Field (PR) gibt an, welches Protokoll auf der nächsten Schicht verwendet wird (z. B. UDP).



Solche Pakete können über Router hinweg verschickt werden, welche die DMAC-Adresse des Ethernet-Frames entsprechend verändern (nächster Router am Pfad oder Empfänger).

⁷⁾ Nicht benötigte/beschriebene Felder von ETH- und IP-Header werden nur in ihren Abkürzungen erwähnt.

⁸⁾ Per Konvention verwenden TSN Streams Multicast DMACs, um sie leichter von physikalisch verfügbaren Adressen zu unterscheiden (auch wenn der Stream nur an einen Listener adressiert ist und damit eigentlich einem Unicast Frame entspricht).

Transport - Schicht 4

Auf Schicht 4 kommen die beiden Transportprotokolle UDP und TCP zum Einsatz. UDP ist ein verbindungsloses Protokoll, das sogenannte Datagramme versendet, die über einen UDP-Header (8 Bytes) am Anfang verfügen, der unter anderem Quell- und Zielport der Verbindung beinhaltet. Bei UDP gibt es keine Information, ob Datagramme vom Empfänger empfangen wurden. Diese Überprüfung muss daher, wenn notwendig, auf höheren Schichten erfolgen. TCP ist ein verbindungsorientiertes Protokoll, das sogenannte Segmente versendet, die über einen TCP-Header (20 Bytes) am Anfang verfügen, der unter anderem Quell- und Zielport der Verbindung sowie Informationen über das Segment beinhaltet. Bei TCP wird (innerhalb definierter Grenzen) sichergestellt, dass ein Segment beim Empfänger ankommt und die Segmente in der richtigen Reihenfolge rekonstruiert werden können. Aufgrund dieses Mechanismus ist TCP für echtzeitkritische Datenübertragung mit kurzen Latenzen nicht geeignet, sondern wird hauptsächlich für asynchrone Dienste eingesetzt, bei welchen die sichere Zustellung im Vordergrund steht. TCP wird auch für die meisten Security-Protokolle als Transportschicht gewählt.

Kommunikation - Schicht 5

Auf Schicht 5 kommen Security-Protokolle zum Einsatz. Für OPC UA over TSN ist TLS ein wichtiges Protokoll. Es kümmert sich zuerst um den Verbindungsaufbau, wobei die Identität der Kommunikationspartner mittels eindeutiger Schlüssel geprüft wird. Dafür können Zertifikate oder Benutzer/Passwort-Angaben verwendet werden. Für die eigentliche Datenübertragung kann der Kanal dann signiert und/oder verschlüsselt⁹⁾ werden.

Darstellung - Schicht 6

Schicht 6 beinhaltet das Encoding der Inhalte der Nachrichten, welches je nach verwendetem Protokoll auf der Applikationsschicht (OPC UA, NETCONF etc.) unterschiedlich sein kann.

Applikation - Schicht 7

Auf Schicht 7 schließlich findet die Interaktion mit der Applikation oder dem Applikationsprotokoll statt.

Eine Nachricht, die von einer Applikation zu einer anderen Applikation verschickt wird, enthält also gleichzeitig Informationen aller ISO/OSI Schichten. Sie ist damit gleichzeitig z. B. Frame, Packet und Segment, je nachdem, welche Schicht im ISO/OSI-Modell gerade Betrachtung findet.

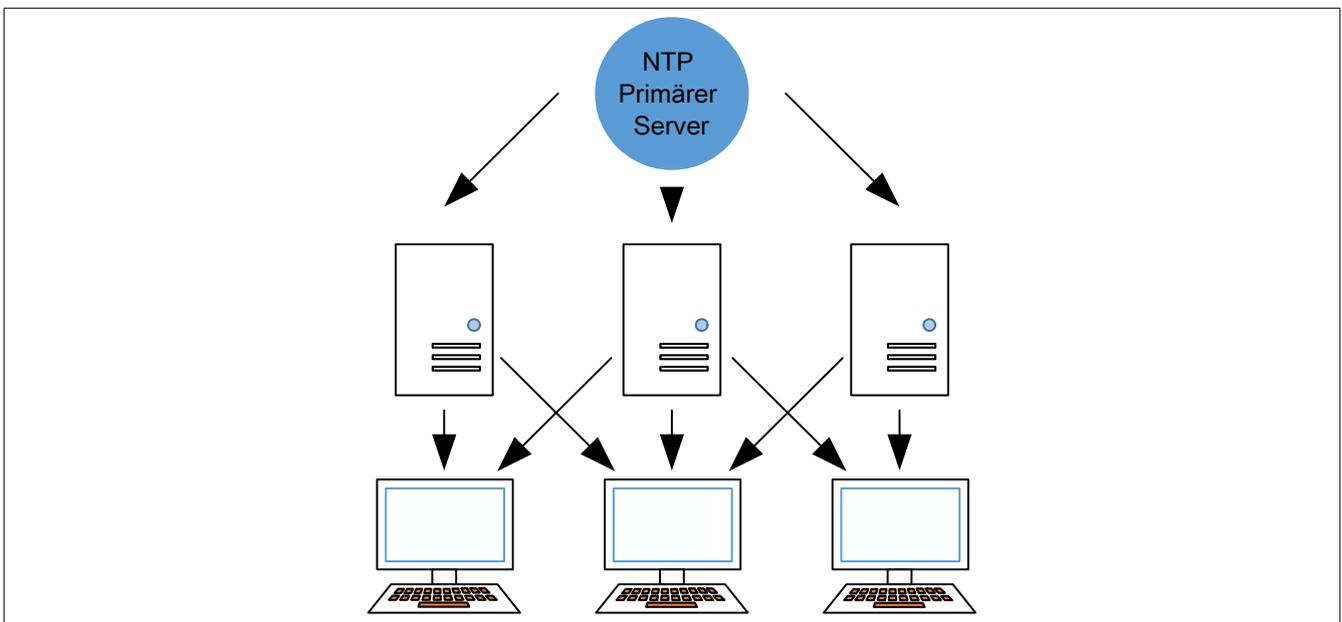
⁹⁾ Mittels eines Sitzungsschlüssels, der regelmäßig erneuert wird.

5.3 Zeitsynchronisierung

Zeitsynchronisierung bildet das Fundament von TSN. Viele der sogenannten Traffic Shaper, mit denen sich verschiedene Garantien am Netzwerk durch Shaping (Regulierung) des Verkehrs implementieren lassen, brauchen eine möglichst exakte, gemeinsame Zeitbasis auf allen Infrastrukturkomponenten, um zu funktionieren. Die Zeit wird dabei für Sende- und Weiterleitungszeitpunkte, sowie der Berechnung von Bandbreite und Framerraten verwendet. Für die beiden Berechnungen reicht ein gemeinsames Verständnis vom Fortschreiten der Zeit ohne Kenntnis von Absolutwerten (Synthonsation). Zeitsynchronisierung in Ethernet-Netzwerken ist ein relativ altes Problem mit entsprechend vielen Lösungen, die unterschiedlichen Anforderungen Rechnung tragen. Die wichtigsten verfügbaren Lösungen sind:

- (S)NTP – (Simple) Network Time Protocol
- IEEE Std. 1588 – Precision Time Protocol
- IEEE Std. 802.1AS – generalized Precision Time Protocol
- Industrial Ethernet

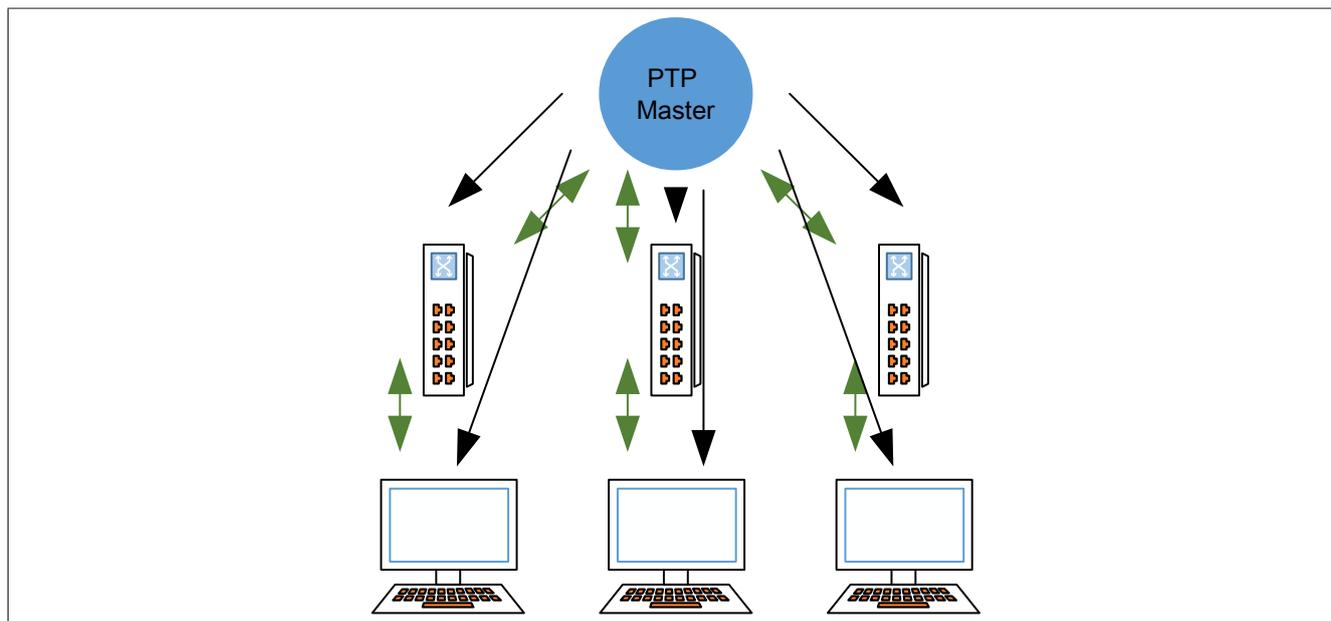
NTP bzw. früher SNTP wird hauptsächlich bei Anwendungen verwendet, wo eine für menschliche Begriffe gute Genauigkeit ausreichend ist (Desktop-PCs, Mobiltelefone) und eine globale Zeitbasis synchronisiert werden soll. Dabei wird von einem hochgenauen Master über verschiedene Zwischenschichten die Information über die aktuelle Zeit an die Endgeräte verteilt, wobei jeweils die schnellste Verbindung gesucht wird. Für industrielle Anwendungen mit Anforderungen an die Zeitgenauigkeit von $\geq 5 - 10$ ms (z. B. Prozessautomatisierung) ist es aufgrund der einfachen und effizienten Implementierung ebenfalls weit verbreitet¹⁰⁾.



Für industrielles Echtzeit-Ethernet mit Genauigkeitsanforderungen im μs - und $\text{sub-}\mu\text{s}$ -Bereich ist NTP jedoch nicht geeignet, daher verwenden die meisten Technologien eigene Mechanismen zur Zeitsynchronisierung. POWER-LINK verwendet zum Beispiel den ersten Frame im Zyklus (SoC), der vom Master zu hochpräzisen, äquidistanten Zeitpunkten versendet wird, zum Synchronisieren der Teilnehmer. In anderen Technologien (z. B. PROFINET, CIP Sync bei EtherNet/IP) wird IEEE 1588 eingesetzt.

¹⁰⁾ Die angegebenen 5 bis 10 ms beziehen sich auf Synchronisierung über das Internet. In lokalen Netzen sind auch Werte $< 500 \mu\text{s}$ erreichbar.

IEEE 1588 wurde für messtechnische Anwendungen entwickelt und zeichnet sich dadurch aus, dass neben der Verteilung der Zeit des lokalen Masters auch die Laufzeit der Nachrichten sehr genau kompensiert wird¹¹⁾, wodurch die Genauigkeit gegenüber NTP deutlich erhöht werden kann. Wenn die Empfangs- und Sendezeitpunkte der Synchronisationsframes und Frames zur Laufzeitmessung hardwareunterstützt gemessen werden können, sind Genauigkeiten von $< 1 \mu\text{s}$ möglich, bei reiner Software-Verarbeitung $\sim 1 \text{ ms}$.



IEEE 1588 ist ein sehr umfangreicher Standard mit vielen Optionen und Protokollmappings, was zur Spezifikation diverser Profile geführt hat (Power, Telekom, Messtechnik, Audio/Video, ...), die zueinander nicht kompatibel sind.

IEEE 802.1AS ist ebenfalls ein Profil von IEEE 1588 speziell für AVB LANs mit nur wenigen konfigurierbaren Optionen, um Interoperabilität in Multi-Vendor-TSN-Netzwerken zu ermöglichen. In der Version 802.1AS-2020 werden erstmals mehrere Time Domains (eine Working Clock für zeitgesteuerte Kommunikation und Motion-Anwendungen¹²⁾ und eine Global Time¹³⁾ für Logging) und Grand Master-Redundanz unterstützt. Darüber hinaus wurde 802.1AS für große Ethernet-Netzwerke optimiert, wohingegen bei IEEE 1588 regelungstechnische Fading-Effekte auftreten können, die die Synchronisierungsgenauigkeit beeinflussen¹⁴⁾. IEEE 1588 ist im Feld schon länger verbreitet als 802.1AS, daher werden am Markt Time Gateway-Funktionen angeboten, um Netzwerke mit den beiden Synchronisierungsvarianten in eine gemeinsame Zeitbasis aufnehmen zu können.

¹¹⁾ Im Bild grün gezeichnet. Jede Zeitinformation vom Master an einen Slave "sammelt" die Angaben über die Laufzeit auf, wodurch der Slave sehr genau auf die Zeit des Masters zurückrechnen kann.

¹²⁾ Ein streng monoton steigender Zähler, der nicht springen darf

¹³⁾ Entspricht der Weltzeit UTC

¹⁴⁾ Bei IEEE 1588 wird die residence Time der Frames am Gerät mit der schon geregelten Software-Uhr gemessen, während diese bei 802.1AS mit der freilaufenden Hardware-Uhr gemessen wird. Die absoluten Unterschiede sind absolut verschwindend, jedoch gibt es einen gegenseitigen Einfluss zwischen Laufzeitkorrektur und ausgerechneter Zeit bei IEEE 1588, wodurch in größeren Netzwerken normale Messungsgenauigkeiten immer wieder Schwebungseffekte verursachen.

5.4 Traffic Types

Die meisten Industrial Ethernet Technologien unterstützen jeweils 2 Arten der Datenübertragung:

- Echtzeitkritische
- Nicht-echtzeitkritische

Echtzeitkritische Datenübertragung lässt sich in harte und weiche Echtzeit unterscheiden, wobei bei harter Echtzeit die Zeitpunkte des Sendens, Weiterleitens und Empfangens von Nachrichten im Zyklus immer gleich sind. Bei weicher Echtzeit gibt es an diesen Stellen Jitter im Netzwerk, es wird jedoch davon ausgegangen, dass ein Frame pro Zyklus versendet und empfangen werden kann.

Bei nicht-echtzeitkritischer Datenübertragung gibt es je nach Anwendung die Notwendigkeit, Nachrichten zu priorisieren, wofür es ebenfalls unterschiedliche Implementierungen bei Industrial Ethernet gibt. Im IIC - TSN Testbed wurden 2017 erstmals die unterschiedlichen Arten von Traffic in industriellen Anwendungen, die sich historisch etabliert haben, und ihre Anforderungen systematisch untersucht und in einem White Paper zusammengefasst¹⁵⁾. Folgende Traffic Types wurden identifiziert:

Typen	Periodizität	Periode	Mit Netzwerk synchronisiert	Datenübertragungsgarantie	Toleranz gegenüber Störungen	Tolerance gegenüber Datenverlust	Typische Datengröße der Applikation	Kritikalität
Isochron	Periodisch	< 2 ms	Ja	Deadline	0	Keine	Fest: 30 bis 100 Bytes	Hoch
Zyklisch	Periodisch	2 bis 20 ms	Nein	Latenz	≤ Latenz	1 bis 4 Frames	Fest: 50 bis 1000 Bytes	Hoch
Ereignisse	Sporadisch	n.a.	Nein	Latenz	n.a.	Ja ¹⁾	Variabel: 100 bis 1500 Bytes	Hoch
Netzwerküberwachung	Periodisch	50 ms bis 1 s	Nein	Bandweite	Ja	Ja ¹⁾	Variabel: 50 bis 500 Bytes	Hoch
Konfiguration & Diagnose	Sporadisch	n.a.	Nein	Bandweite	n.a.	Ja ¹⁾	Variabel: 500 bis 1500 Bytes	Mittel
Best-Effort	Sporadisch	n.a.	Nein	Keine	n.a.	Ja ¹⁾	Variabel: 30 bis 1500 Bytes	Niedrig
Video	Periodisch	Frame-Rate	Nein	Latenz	n.a.	Ja ¹⁾	Variabel: 1000 bis 1500 Bytes	Niedrig
Audio/Stimme	Periodisch	Samplezeit	Nein	Latenz	n.a.	Ja ¹⁾	Variabel: 1000 bis 1500 Bytes	Niedrig

1) Auch bei den nicht-zyklischen Traffic Types ist aus Applikationssicht sehr oft kein Spielraum für Paketverluste (z. B. bei Ereignissen, die nur einmal übertragen werden). Diese Verluste werden jedoch durch Protokolle auf höheren Schichten (mit entsprechenden Latenzen) ausgeglichen, daher wird grundsätzlich auf Schicht 2 keine Maßnahme zur Vermeidung von Paketverlust gefordert.

Es ist davon auszugehen, dass in industriellen Anwendungen zumindest die folgenden Traffic Typen verwendet werden:

- Typen für periodischen Prozessdatenaustausch (isochron oder zyklisch; im B&R-System isochron)
- Netzwerküberwachung (Nachrichten, die für die Aufrechterhaltung der Netzwerkfunktion erforderlich sind, wie Zeitsynchronisierung, LLDP etc.)
- Konfiguration und
- Best-Effort¹⁶⁾

Je nach Anwendung können dann auch andere Traffic Types notwendig sein, für die das Netzwerk Übertragungsgarantien geben soll.

¹⁵⁾ https://www.iiconsortium.org/pdf/IIC_TSN_Testbed_Char_Mapping_of_Converged_Traffic_Types_Whitepaper_20180328.pdf

¹⁶⁾ Nachrichten ohne Übertragungsgarantie, die die restliche freie Bandbreite nutzen können

5.5 Quality of Service (QoS)

Quality of Service (QoS) ist eine allgemeine Bezeichnung, um zu beschreiben, dass man gewisse Daten in einem Netzwerk speziell auszeichnen und nach definierten Regeln (besser als Best Effort) behandeln möchte. Sowohl auf Schicht 2, als auch Schicht 3 des ISO/OSI-Modells, kennt man heute bereits QoS-Mechanismen, welche zur Klassifizierung und Priorisierung von Datenströmen zur Anwendung kommen (z. B. für die Priorisierung von Voice over IP). Mit TSN QoS bezeichnet man nun jene von der IEEE TSN-Arbeitsgruppe neu spezifizierten Mechanismen zur Regulierung der Datenübertragung auf Schicht 2 des ISO/OSI-Modells (zum Beispiel 802.1Qbv oder 802.1Qch). Die Klassifizierung erfolgt dabei über einen sogenannten VLAN-Tag¹⁷⁾, der dem Ethernet Header zusätzliche 16 Bit hinzufügt, wovon 12 Bit die sogenannte VLAN ID (VID) und 3 Bit den Priority Code Point (PCP) darstellen, das 16. Bit wird nicht verwendet.

Mit Hilfe des PCP lassen sich 8 Prioritäten abbilden, die dazu verwendet werden, dass ein Switch an jedem Ausgangsport (Egress Port; im Gegensatz zu Ingress für die Eingangsseite) die weiterzuleitenden Frames in bis zu 8 Queues einsortieren kann. Im Normalfall werden diese Queues dann ihrer Priorität nach geleert (höchste Priorität = 7 zuerst; wenn diese Queue leer ist, dann Priorität 6 etc.) und die Frames über den entsprechenden Egress Port versendet. Man spricht von "Strict Priority Transmission Selection". Über diese Prioritätssteuerung wird z. B. Voice over IP oder in manchen Industrial Ethernet Netzwerken Prozessdatenverkehr oder Alarme höher priorisiert als Best-Effort Traffic.

Die VID wird verwendet, um Ethernet-Netzwerke virtuell zu segmentieren. So muss eine Ethernet-Schnittstelle konfiguriert werden, um an bestimmten VLANs teilzunehmen, andernfalls wird einkommender, getaggeter Verkehr verworfen. Eine beliebte Variante von VLANs ist Port-based VLAN, bei welchem an einem managed Infrastruktur-Switch konfiguriert wird, dass alle an einem bestimmten Port angeschlossenen Geräte einem VLAN zugeordnet werden sollen. Der Traffic zwischen den Geräten in diesem Segment ist davon nicht beeinflusst (wenn z. B. mehrere Geräte in Linie an diesem Port angeschlossen sind), wenn allerdings Frames aus dem Segment an den Switch geleitet werden, fügt der Switch automatisch einen VLAN-Tag vor dem Weiterleiten hinzu. Geräte außerhalb des Segments müssten jetzt ebenfalls dieser VLAN ID zugeordnet sein, um mit Geräten im VLAN kommunizieren zu können. Kommunikation ist nur möglich zwischen Teilnehmern im selben VLAN (identische VLAN ID), andernfalls sind diese Geräte sozusagen unsichtbar.

Das Konzept der TSN Streams ist eine logische Weiterentwicklung des VLAN-Konzepts. Ein Stream muss mit einer Stream Reservation Methode in alle Switches konfiguriert werden, über die er versendet werden soll. Überall sonst wird er verworfen. Ein Stream bildet sozusagen ein VLAN für einen einzigen Frame (eine unidirektionale Datenübertragung von einem Absender (TSN "Talker") zu einem oder mehreren Empfängern (TSN "Listener")).

¹⁷⁾ Siehe auch https://de.wikipedia.org/wiki/IEEE_802.1Q

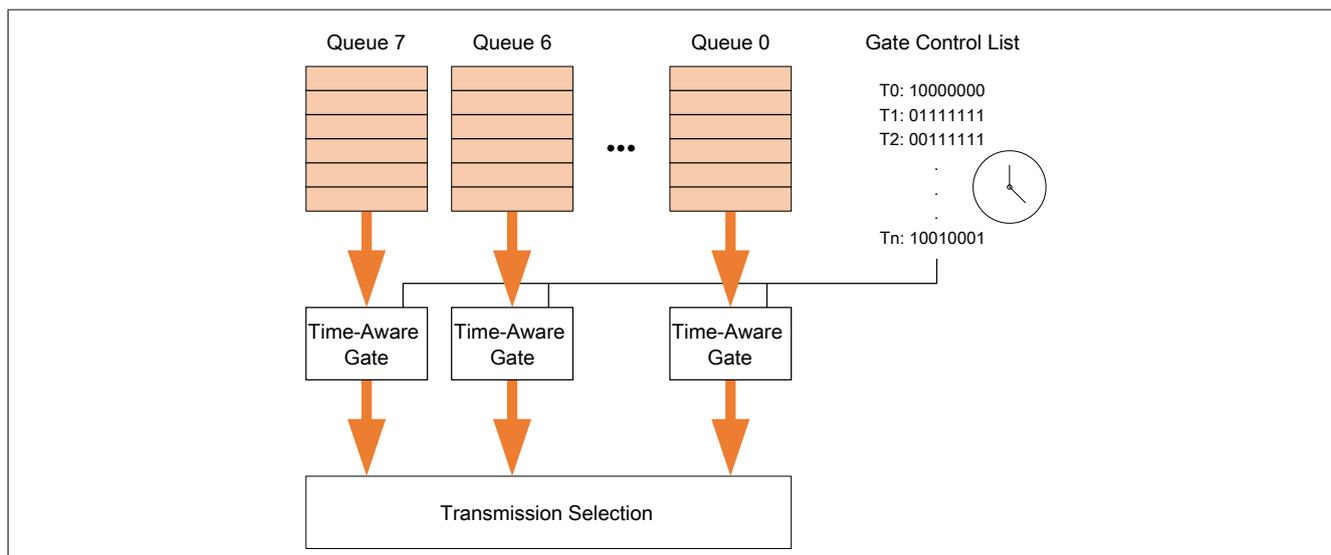
5.6 Mechanismen

Die TSN-Arbeitsgruppe beschäftigt sich mit einer Vielzahl an unterschiedlichen Mechanismen, um die Ziele in den oben genannten Bereichen zu erfüllen. Für industrielle Anwendungen ist nur ein kleiner Teil davon relevant, wie in den folgenden Kapiteln beschrieben. Man könnte theoretisch ein Netzwerk ausschließlich entweder über Ingress- oder Egress-Shaping definieren, daher haben auch alle entsprechenden Standards für sich relativ viel Funktionsumfang. In der Standardisierung der Anwendung von TSN¹⁸⁾ herrscht jedoch Einigkeit, dass ein Profil mit sowohl Ingress- als auch Egress-Mechanismen am zielführendsten ist und einige optionale Features der Standards nicht verwendet werden müssen.

5.6.1 IEEE 802.1Qbv

IEEE 802.1Qbv¹⁹⁾ stellt neben der Zeitsynchronisierung wohl das Herz von TSN und auch den bekanntesten Standard dar. IEEE 802.1Qbv wird auch als scheduled Traffic bezeichnet und spezifiziert den sogenannten Time-Aware Shaper (TAS). Im Wesentlichen definiert der TAS ein zeitgesteuertes Öffnen und Schließen von Switch Queues an einem Egress Port eines Switches. Man spricht von Qbv-Fenstern, die für Queues konfiguriert werden. Der TAS ist der eigentlichen Auswahl des zu sendenden Frames vorgelagert und kann damit mit den bekannten Auswahlmechanismen wie Strict Priority (siehe Abschnitt 5 "TSN") und Credit-Based Shaper (siehe Abschnitt 5.6.2 "IEEE 802.1Qav") kombiniert werden.

Ohne TAS werden Frames, die für einen bestimmten Egress Port bestimmt sind, in die entsprechende Queue für den Port zur Zustellung geleitet. Wenn mehrere Queues Frames vorrätig haben, werden diese ihrer Priorität nach entnommen und versendet. Mittels TAS wird jetzt ein Zyklus eingeführt, innerhalb dessen die einzelnen Queues individuell geöffnet bzw. geschlossen werden können (Gate Control List, GCL). Sind mehrere Queues geöffnet (in der GCL auf "1" gesetzt) und haben Frames vorrätig, werden diese wieder ihrer Priorität nach entnommen und versendet.



Wenn zu einem Zeitpunkt nur eine Queue geöffnet ist, spricht man von "exclusive network access". Damit erhält Traffic in der betreffenden Queue reservierte Bandbreite am entsprechenden Port ohne potentielle Beeinflussung durch Traffic in den anderen Queues am selben Port (Inter-Class Interference). Werden in allen Switches in einem Netzwerk die Queues dieser exklusiven Traffic-Klasse entsprechend aneinander ausgerichtet, können Frames dieser Traffic-Klasse ohne zusätzliche Verzögerung (Intra-Class Interference) übertragen werden und damit harte Echtzeitfähigkeit und kürzest mögliche Latenz erreicht werden.

Information:

Im B&R System wird IEEE 802.1Qbv verwendet, um isochronen Echtzeitverkehr ohne Beeinflussung von anderem Traffic zu ermöglichen. Zusätzlich wird IEEE 802.1Qbv verwendet, um für die weiteren Traffic Types Bandbreiten zu reservieren.

¹⁸⁾ IEC/IEEE 60802 und OPC Field Level Communications Initiative

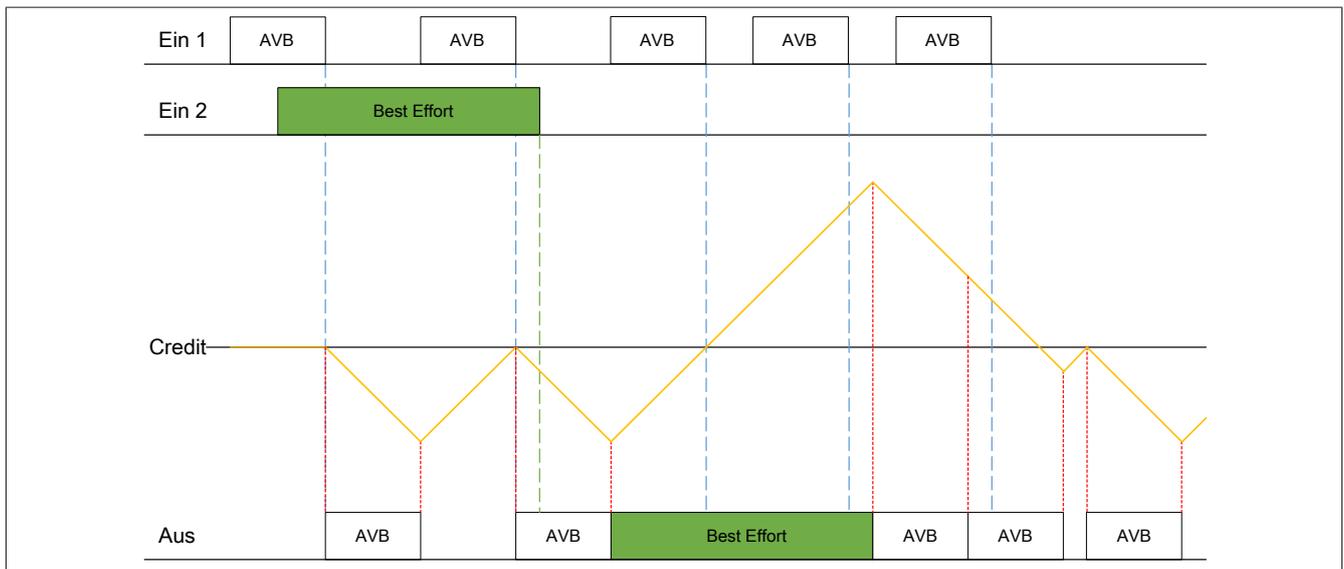
¹⁹⁾ Im 802.1Q Standard integriert und nicht einzeln verfügbar

5.6.2 IEEE 802.1Qav

An IEEE 802.1Qav²⁰⁾ wurde zur Zeit der AVB-Arbeitsgemeinschaft entwickelt und dieser Standard spezifiziert den sogenannten Credit-based Shaper (CBS). Mittels CBS können mehrere Ziele erreicht werden:

- Bandbreitenbegrenzung eines Senders
- garantierte maximale Latenz für versendete Frames
- definiertes Burst-Verhalten eines Senders.

Der Credit-based Shaper wird so implementiert, dass für das Versenden eines Frames je nach Größe eine gewisse Menge an Credits notwendig ist (≥ 0). Sind keine Credits mehr vorhanden (< 0), darf kein Frame gesendet werden. Wenn gerade keine Frames gesendet werden, "verdient" das Egress Port neue Credits bis zu einem oberen Limit von 0. Wenn das Egress Port gerade durch ein anderes gesendetes Frame blockiert ist und sich Qav-Frames in der Queue befinden (also stauen), "verdient" der CBS am Port zusätzliche Credits (bis zu einem weiteren Maximum), so dass er den Rückstand an Frames in seiner Queue wieder abbauen kann und damit über die Zeit seine zugewiesene Bandbreite ausnutzen kann. Dieses Maximum, zusammen mit der maximalen Frame-Länge, legt nun fest, wie lange eine CBS Queue das Netzwerk durchgehend belegen darf (Burst). Typische Anwendungsfälle für IEEE 802.1Qav sind Audio/Video und Ereignisse.



Information:

Im B&R System steht IEEE 802.1Qav zur Verfügung, um Audio, Video oder anderen Traffic kundenspezifisch im Netzwerk planen zu können.

²⁰⁾ Im 802.1Q Standard integriert und nicht einzeln verfügbar

5.6.3 IEEE 802.1Qci

IEEE 802.1Qci²¹⁾ ist ein umfangreicher Standard, mit dem man Filterregeln für das Verwerfen von eingehendem Traffic definieren kann. IEEE 802.1Qci wird auch als "Ingress Policing" bezeichnet. Im Wesentlichen definiert IEEE 802.1Qci rate-based und time-based Filtering auf Stream- und Port-Basis.

Wenn in einem Netzwerk zusätzlich entsprechende Egress Port Mechanismen konfiguriert sind, handelt es sich bei IEEE 802.1Qci "nur" um Mechanismen zur Steigerung der Robustheit und Diagnosefähigkeit. Beispielsweise kann auf einem Switch am Egress IEEE 802.1Qbv konfiguriert sein und am direkt angeschlossenen nächsten Switch IEEE 802.1Qci am Ingress. Man spricht dann von "reverse Qbv", wenn die Filterregeln so eingestellt sind, dass sie die Funktion von IEEE 802.1Qbv am Nachbarswitch überprüfen, also Frames, die nicht der Erwartungshaltung entsprechen, filtern.

IEEE 802.1Qci kann natürlich auch ohne IEEE 802.1Qbv verwendet werden, um den eingehenden Traffic zu kontrollieren, z. B. eben mit "reverse Qbv", mit dem Ziel die eigenen Egress Queues vor nicht gewolltem Traffic zu bewahren. Der Unterschied liegt darin, dass bei IEEE 802.1Qci Frames verworfen werden, bei denen eine Filterregel anschlägt, bei IEEE 802.1Qbv am Egress bleiben die Frames in der Queue, wenn das Gate geschlossen ist und warten auf das nächste Öffnen des Gates und können damit theoretisch über viele Zyklen hinweg Probleme bereiten.

Wenn sich alle angeschlossenen Geräte im obigen Qbv-Qci Beispiel immer richtig verhalten, werden die IEEE 802.1Qci Regeln nie ausgelöst. Wenn man allerdings annimmt, dass ein Gerät zum Beispiel fehlerhafterweise 2 Frames in einem Zyklus versenden kann (anstatt Einem), müsste man die Qbv-Fenster entsprechend größer dimensionieren, um den fehlerhaften Frame nicht dauerhaft in der Queue zu behalten und nachfolgende Zyklen zu stören. Mittels IEEE 802.1Qci am nächsten Switch kann der überzählig gesendete Frame dann erkannt und verworfen werden. Ein weiterer Anwendungsfall für IEEE 802.1Qci ist die Bandbreitenbegrenzung. Dadurch kann das Netzwerk vor zu viel Traffic von außen oder einem fehlerhaften Teilnehmer oder einem Teilnehmer ohne eigene Bandbreitenbegrenzung geschützt werden. Auch DoS-Attacken lassen sich auf diese Weise abmildern oder ganz verhindern.

Information:

Im B&R System wird IEEE 802.1Qci verwendet, um isochronen Echtzeitverkehr robuster gegen Fehler zu machen und Fehler gezielt lokalisieren zu können. Zusätzlich wird IEEE 802.1Qci verwendet, um ansonsten unkonfigurierten (offenen) Ports die Bandbreite ins System zu begrenzen.

²¹⁾ Im 802.1Q Standard integriert und nicht einzeln verfügbar

5.6.4 Konfiguration (IEEE 802.1Qcc)

IEEE 802.1Qcc definiert 3 verschiedene Konfigurationsmodelle für TSN Netzwerke: zentral, verteilt und hybrid. Die Unterscheidung beruht darauf, wo das Wissen über die reservierten Streams im Netzwerk vorgehalten wird.

Beim verteilten Modell, der direkten Weiterentwicklung der Konfiguration von AVB Streams melden sowohl Talker als auch Listener ihre Bedarfe an Streams an ihre jeweiligen Nachbarn an. Diese Information propagiert durch das Netzwerk bis irgendwann die Anforderungen von zumindest einem Talker und Listener zusammenfinden. Jeder Switch gibt dann bekannt, ob er den angeforderten Stream mit den angeforderten QoS-Parametern auf diesem Pfad zusätzlich reservieren kann. Wenn alle Switche bestätigen, wird der Stream etabliert und kann verwendet werden. Diese Methode ist insbesondere für CBS Traffic (siehe Abschnitt 5.6.2 "IEEE 802.1Qav") einfach und effizient umsetzbar. Für andere Traffic Shaper stößt die verteilte Konfiguration an ihre Grenzen, weshalb die beiden anderen Modelle entwickelt wurden.

Beim zentralen Modell wird eine zentrale Instanz, der CNC (Central Network Configuration), eingeführt, der die Topologie des Netzwerks und die aktuelle Stream-Konfiguration kennt. Ein zusätzlich benötigter Stream kann beim CNC angefordert werden, der über alle Informationen verfügt, um die Anfrage bestätigen oder ablehnen zu können und dann auch alle Infrastrukturkomponenten umkonfiguriert. Der CNC ist insbesondere gut geeignet, um Frames mit harten Echtzeitanforderungen netzwerkweit zu planen. Darüber hinaus kann der CNC auch effizient weitere Mechanismen wie Pre-Emption (siehe Abschnitt 5.7.2 "Pre-Emption") und Per-Stream Filtering and Policing (siehe Abschnitt "IEEE 802.1Qci" auf Seite 30) netzwerkweit verwalten.

Eine direkte Kommunikation mit einem CNC für jedes Anwendungsprotokoll ist nicht effizient, da es viele unterschiedliche Abbildungen vom QoS-Verständnis der Applikation zum zur Verfügung stehenden Netzwerk-QoS geben kann. Daher wurde in Qcc neben dem CNC noch die Rolle des CUC (Central User Configuration) eingeführt. Der CUC ist spezifisch für das im Netzwerk eingesetzte Anwendungsprotokoll. Beispielsweise wurde für OPC UA PubSub Kommunikation der PTCC als ein TSN CUC spezifiziert. Jeder CUC kann über übliche Konfigurationsmechanismen "seines" Applikationsprotokolls (der PTCC über OPC UA Client/Server) angesprochen werden und übersetzt diese Anforderungen in Anfragen an den CNC²²).

Das hybride Modell kombiniert die zentrale Instanz des CNCs mit Streamanforderungen an die benachbarten Switche. In der Praxis wird dieser Ansatz nicht verfolgt.

Im B&R System wird zentrale Konfiguration verwendet, wobei die Netzwerkkonfiguration von Automation Studio errechnet wird und das Ergebnis zur Laufzeit von Automation Runtime im Netzwerk verteilt wird.

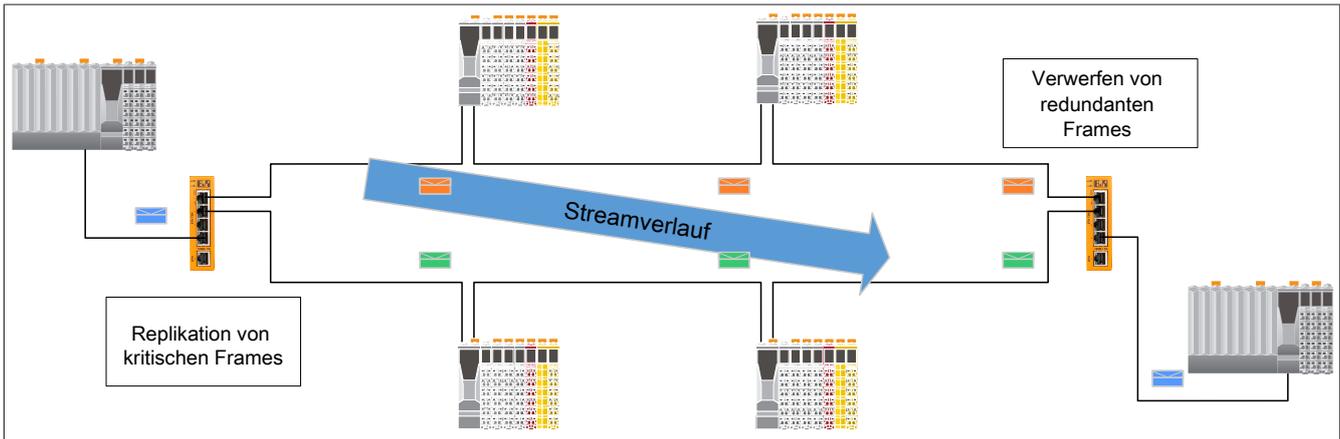
Information:

Im B&R System wird IEEE 802.1Qcc zur Konfiguration der TSN-Parameter in den Geräten verwendet.

²² Um einen PubSub-Frame zu konfigurieren, parametrisiert man direkt Publisher und Subscriber. Um einen "gleichen" PubSub over TSN-Stream zu konfigurieren, schickt man die gleiche Anfrage (erweitert um die QoS-Wünsche) an den CUC. Dieser fragt beim CNC die notwendigen Netzwerkressourcen an, die dann vom CNC auch gleich reserviert werden. Der CUC parametrisiert dann Publisher und Subscriber, jeweils erweitert um die notwendigen QoS-Parameter (wie Stream ID).

5.6.5 IEEE 802.1CB

IEEE 802.1CB definiert Mechanismen zur Duplizierung von Streams und dem Zusammenführen der redundanten Duplikate, um in einem Netzwerk stoßfreie, redundante Übertragung von Streams zu ermöglichen. Die Mechanismen sind transparent für alle Geräte, die diesen Standard nicht unterstützen, d. h. jeder Switch im Netzwerk der diesen Standard nicht unterstützt, wird die redundanten Kopien in der gleichen Weise weiterleiten wie normale Streams. Als einfaches Beispiel kann man sich einen zentralen Switch vorstellen, an dem einerseits an einem Port eine Steuerung angeschlossen wird und auf 2 weiteren Ports ein Ring von Feldgeräten. Der Switch kann alle (konfigurierten) Streams von der Steuerung auf beide Ports replizieren und die Feldgeräte werden jeweils die erste empfangene Kopie verarbeiten und die Zweite (so eine Zweite empfangen wird) verwerfen. Umgekehrt können auch die Feldgeräte ihre Streams auf beide Ports replizieren und der zentrale Switch kann dann jeweils die erste Kopie an die Steuerung weiterleiten (und weitere Kopien verwerfen). Da jeweils nur das Duplizieren und Zusammenführen konfiguriert wird, kann ein Anwender beliebige Redundanztopologien definieren und mit Switchen aufbauen. Das Bild zeigt ein anschauliches Beispiel mit 2 Infrastrukturswitchen, die mit CB konfiguriert sind.



Der Vorteil von CB liegt in der Anwendung auf Streams und der Vorkonfiguration, d. h. es gibt keine Switch-Overzeiten im Falle eines Ringbruchs oder einer Wiederherstellung eines Rings. Weiters können nur jene Nachrichten redundant übertragen werden, bei denen die Verfügbarkeit ohne Paketverlust wichtiger ist als die zusätzlich benötigte Bandbreite für die Duplikate im Netz. Nicht-Stream-Traffic kann/muss mittels anderer Mechanismen behandelt werden. In industriellen Anwendungen reichen außer für zyklische Prozessdaten die Umschaltzeiten von SpanningTree Varianten völlig aus, kurzfristiger Paketverlust (bis ein neuer Spanning-Tree aufgebaut ist) werden auf der Transportschicht von TCP durch wiederholtes Senden ausgeglichen.

In speziellen Anwendungen können außer den Prozessdaten noch weitere Daten hohe Verfügbarkeitsanforderungen haben (Ereignisse, Konfiguration). In diesen Fällen kann man auch diese Streams redundant auslegen. CB stellt daher einen minimal-invasiv, zielgerichtet einsetzbaren Mechanismus für Redundanz dar.

Im B&R System werden im Falle redundanter Verbindungen zyklische Prozessdaten standardmäßig redundant übertragen.

Information:

Im B&R System wird IEEE 802.1CB für stoßfreie Redundanz von kritischen Prozessdaten verwendet.

5.7 Optimierungen

5.7.1 Cut/Trough

Ethernet ist darauf ausgelegt, dass Frames von einem Switch vollständig empfangen, analysiert, traffic-geshaped und dann entsprechend weitergeleitet werden. Dieses Verhalten erlaubt es jedem Switch, die Prüfsumme (am Ende) eines Frames zu analysieren, um durch Bitfehler korrumpierte Nachrichten verwerfen zu können. Da erst mit dem vollständigen Empfangen eines Frames die Framegröße bekannt wird, können auch viele IEEE 802.1Qci-Filter erst mit dieser Information sinnvoll betrieben werden.

Dieses sogenannte Store/Forward Verhalten induziert jedoch eine Latenz in jedem Switch, die ungefähr der Übertragungsdauer eines Frames am Kabel entspricht. Ein maximaler Ethernet-Frame benötigt bei einer Bandbreite von 100 MBit ca. 127 μ s, bei Gigabit ca. 12,7 μ s, um von einem Switch vollständig empfangen zu werden. Haben die Frames im Netzwerk alle vergleichbare Größe, kann auch mit diesem Verhalten die Bandbreite sehr gut ausgenutzt werden (da gleichzeitig ein Frame weitergeleitet und ein weiterer empfangen werden kann). Wenn sich die Frames in der Größe jedoch merklich unterscheiden, dann "laufen" kürzere Frames auf längere Frames im Netzwerk "auf" bzw. umgekehrt entstehen Lücken, wenn kürzere Frames schneller durch Switches weitergeleitet werden als Längere.

Für viele regelungstechnische Anwendungen in großen industriellen Netzwerken würden die aufsummierten Latenzen im Store/Forward-Betrieb des Netzwerks in Konflikt mit der angepeilten Zykluszeit bzw. Reaktionszeit stehen.

Daher gibt es alternativ die Betriebsart Cut/Through, bei welcher ein Switch möglichst früh, also nach dem Empfang der Zieladresse bzw. der TSN Stream ID die Weiterleitungsentscheidung trifft und den Frame dann sofort an das Egress Port zur Weiterleitung übergibt. In dieser Betriebsart ist die aufsummierte Latenz minimal, es kann jedoch passieren, dass korrupte Frames weitergeleitet werden bzw., dass spezifische Filterregeln in Einzelfällen verletzt werden (bei Bandbreitenfiltern). Entsprechend muss das Netzwerk so ausgelegt sein, dass die Nachteile von Cut/Through auf andere Art behandelt werden.

Im B&R System wird Cut/Through²³⁾ für deterministische Echtzeitkommunikation verwendet. Korrupte Frames können sich im Netzwerk ausbreiten, werden jedoch beim Empfänger verworfen. Qci wird für diesen Traffic Type für die Kontrolle des Sende- bzw. Weiterleitungszeitpunkts verwendet, daher wird die Information der Framelänge nicht benötigt. Alle anderen Traffic-Types werden per Store/Forward behandelt. Die Latenz der B&R-Geräte beträgt <800 ns bei Gigabit und <3 μ s bei 100 Mbit.

Information:

Im B&R System wird Cut/Through für eine minimale Latenz bei isochronem Echtzeitverkehr von <800 ns pro Hop²⁴⁾ bei Gigabit verwendet.

²³⁾ Cut/Through wird von den B&R Feldgeräten implementiert, nicht vom TSN-Switch. Dieser arbeitet in Store/Forward.

²⁴⁾ Die angegebenen <800 ns inkludieren PHY-Verzögerungen und gelten für B&R Feldgeräte, nicht für den TSN-Switch.

5.7.2 Pre-Emption

IEEE 802.1Qbu für Switches im Verbund mit 802.3br für Endgeräte (single Ports) wird als Pre-Emption bezeichnet und definiert eine Methode, wie hochprioritäre Frames schneller durchs Netzwerk geleitet werden können indem sie niedriger prioritäre Frames am Egress unterbrechen. Im oben beschriebenen Fall des kurzen, "auflaufenden" Frames, würde der kurze Frame bei entsprechender Konfiguration dann nicht in jedem Switch die längere Latenz des vor ihm befindlichen längeren Frames erfahren, sondern könnte diesen gewissenmaßen überholen. Pre-Emption wird jeweils zwischen 2 Netzwerknachbarn konfiguriert und kann daher sehr spezifisch im Netzwerk eingesetzt werden.

Jede der 8 Queues an einem Egress wird entweder "express" oder "pre-emptive" konfiguriert. Wenn ein pre-emptiver Frame gerade gesendet wird und ein express Frame zur Zustellung am Egress einlangt, kann der pre-emptive Frame alle 64 Bytes unterbrochen (und entsprechend markiert) werden und der express Frame sehr zeitnahe weitergeleitet werden. Das angefangene Fragment wird beim Nachbarn gespeichert bis alle weiteren Fragmente empfangen wurden und wird erst dann weiter behandelt.

Mit Pre-Emption kann auf einfache Weise Echtzeitverhalten ohne Stream-basierte Netzwerkplanung erreicht werden, da ein Frame pro Switch auf seinem Pfad maximal 127 Bytes (der größte nicht-unterbrechbare Frame) zusätzliche Latenz erfahren kann, wenn nur ein express Traffic Type verwendet wird.

Im B&R System wird Pre-Emption nicht verwendet, da Echtzeit mittels IEEE 802.1Qbv ohne zusätzliche Latenzen sicher gestellt wird. B&R-Geräte mit TSN-Switch bieten jedoch Pre-Emption an, um in anderen Umgebungen verwendet werden zu können.

Information:

Im B&R System steht Pre-Emption für den kundenspezifischen Einsatz zur Verfügung.

6 OPC UA Field Level Communication

Die Abschnitte 6.1 bis 6.3 wurden der Website der OPC Foundation²⁵⁾ entnommen und übersetzt.

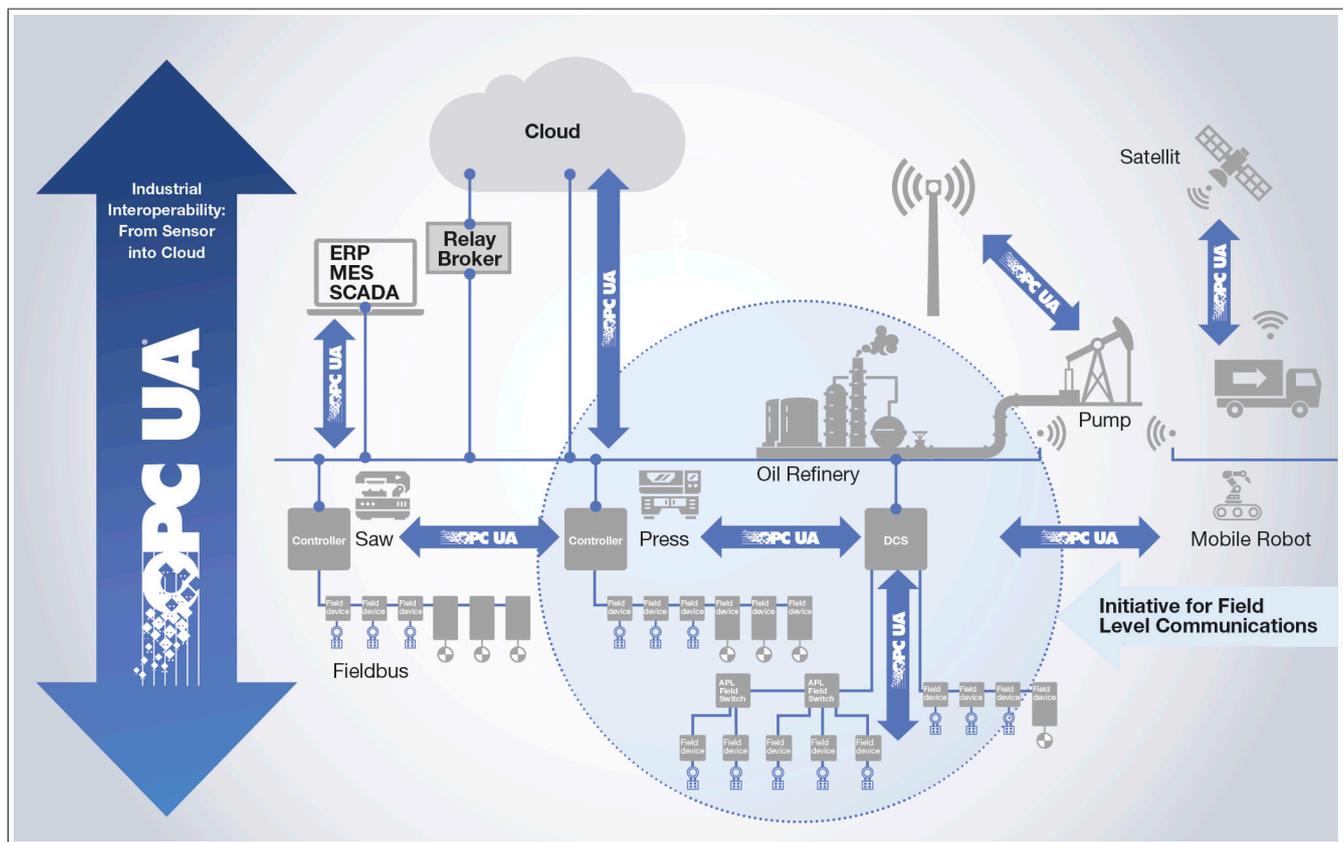
6.1 Hintergrund

Digitalisierung hat das Ziel, IT-Technologien und OT-Produkte, -Systeme, -Lösungen und -Dienstleistungen entlang ihrer gesamten Wertschöpfungskette zu vernetzen – von der Entwicklung über die Produktion bis hin zur Wartung. Dadurch eröffnen sich neue Möglichkeiten wie die Digitalisierung von Produkten und Systemen, neue und erweiterte Softwarelösungen und neue digitale Dienstleistungen.

Das Internet of Things (IoT) vereint eine breite Palette von Technologien, die bisher nicht über IP-basierte Netzwerke verbunden waren. Dinge könne sich über Ethernet zwar erreichen, benötigen aber dennoch eine einheitliche Kommunikation. Genau das wird durch standardisierte Datenkonnectivität und Interoperabilität ermöglicht.

Das Industrial Internet of Things (IIoT) mit standardisierter Datenkonnectivität ermöglicht die Kommunikation auf der vertikalen und horizontalen Ebene. Ein Beispiel für horizontale Kommunikation ist die Maschine-zu-Maschine-Kommunikation (M2M) in der Fertigung. Wenn Daten zwischen Geräten und der Cloud übertragen werden, spricht man hingegen von vertikaler Kommunikation.

In beiden Fällen bietet der OPC-UA-Standard eine sichere, zuverlässige und robuste Grundlage für standardbasierte Datenkonnectivität und Interoperabilität. Für die Entwicklung dieses Standards arbeiten viele Unternehmen und Partnerorganisationen seit Jahren unter dem Dach der OPC Foundation zusammen. Diese Kooperation wird es auch in Zukunft geben. Ein Schlüsselaspekt, um die horizontale und vertikale Datenkonnectivität zu optimieren, ist die IT-/OT-Konvergenz. Gemäß IEEE 802.1 unterstützt Ethernet mit Time-Sensitive Networking (TSN) nicht nur die Kommunikation mit beschränkter Latenz und Jitter. Es ist zudem möglich, verschiedene Datenströme und Datenverkehrstypen über eine gemeinsame Netzwerkinfrastruktur zu übertragen und gleichzeitig die verschiedenen Anforderungen an Bandbreite, Latenz, Jitter und Zuverlässigkeit zu erfüllen. Daher spielt TSN also eine zentrale Rolle für die IT-/OT-Konvergenz. Eine weitere Schlüsseltechnologie im Hinblick auf Netzwerkkonvergenz ist Ethernet Advanced Physical Layer (APL). Sie ermöglicht die nahtlose Ethernet-Konnectivität zu Sensoren und Aktuatoren in der Prozessautomatisierung – auch in Gefahrenbereichen.



²⁵⁾ <https://opcfoundation.org/wp-content/uploads/2020/11/OPCF-FLC-Technical-Paper-C2C.pdf>

6.2 FLC Initiative

Auf der SPS IPC Drives 2018 in Nürnberg hat die OPC Foundation die Field Level Communications (FLC) Initiative gegründet. Das Ziel dieser Initiative ist, OPC UA bis in die Feldebene zu erweitern. Dadurch soll eine offene, einheitliche, standardbasierte IIoT-Kommunikation zwischen Sensoren, Aktuatoren, Steuerungen und der Cloud ermöglicht werden, die alle Anforderungen der Fabrik- und Prozessautomatisierung erfüllt (siehe Abbildung in Abschnitt 6.1 "Hintergrund"). Die Erweiterung von OPC UA bis in die Feldebene rückt die Vision eines weltweiten, industriellen Interoperabilitätsstandards in greifbare Nähe. Die herstellerunabhängige End-to-End-Interoperabilität für Feldgeräte wird für alle relevanten Anwendungsfälle der industriellen Automatisierung, für die ein gesicherter Informationsaustausch erforderlich ist, verfügbar. Darunter fallen zum Beispiel Echtzeitkommunikation, funktionale Sicherheit und Antriebstechnik.

6.3 System Architecture Outline

Die Arbeit der FLC-Initiative umfasst die folgenden Themen:

- Definition eines Basismodells ("Automatisierungskomponenten") für alle FLC-konformen Steuerungen und Geräte
- Definition von Systemverhalten und Abläufen für gängige Funktionen, z. B. Bootstrapping, Verbindungsaufbau etc.
- Harmonisierung und Standardisierung von Anwendungsprofilen wie I/O, Antriebstechnik, funktionale Sicherheit, Systemredundanz
- Standardisierung von OPC-UA-Informationsmodellen für Feldgeräte im Online- und Offline-Betrieb, z. B. Gerätebeschreibung, Diagnose etc.
- Unterstützung von Ethernet TSN für deterministische Kommunikation und IT-/OT-Konvergenz
- Abbildung von Anwendungsprofilen für Echtzeitvorgänge auf Ethernet-Netzwerken mit TSN
- Definition von Konformitätseinheiten/Profilen, die getestet werden können, um herstellerübergreifende Interoperabilität zu gewährleisten
- Definition von Zertifizierungsverfahren

In der ersten Spezifikationsfreigabe (Version 1) steht die Controller-to-Controller-Kommunikation (C2C) im Mittelpunkt. Diese bezieht sich auf den Austausch von Standard- und Sicherheits-Echtzeitdaten über OPC UA Client/Server und OPC UA PubSub in Kombination mit einer Peer-to-Peer-Verbindung und einer einfachen Diagnose. Die Zielnetzwerkarchitektur ist in der folgenden Abbildung dargestellt.

