TSN Industrial Automation Use Cases v0.2

Contributor group

This Use Case Document

McCall, David <david.mccall@intel.com>

Initial Use Case Document from 2019

Belliardi, Rudy <rudy.belliardi@schneider-electric.com>

Dorr, Josef <josef.dorr@siemens.com>

Enzinger, Thomas <thomas.enzinger@br-automation.com>

Essler, Florian <f.essler@beckhoff.com>

Farkas, János <janos.farkas@ericsson.com>

Hantel, Mark <mrhantel@ra.rockwell.com>

Riegel, Maximilian <maximilian.riegel@nokia.com>

Stanica, Marius-Petru <marius-petru.stanica@de.abb.com>

Steindl, Guenter <guenter.steindl@siemens.com>

Wamßer, Reiner <Reiner.Wamsser@boschrexroth.de>

Weber, Karl <karl.weber@beckhoff.com>

Zuponcic , Steven A. <sazuponcic@ra.rockwell.com>

Following discussion during the IEEE 802 Plenary, November 2025, consensus in the 802.1 TSN Task Group was **not** to develop a use case document for an IEC/IEEE 60802 follow-on project by editing the original use case document from 2018 (i.e. this document) but instead to start with a “clean sheet of paper”.

This new revision will import use cases from the original use case document (updated to match the language used in IEC/IEEE 60802) and add use cases from the various recent presentations listed in References.

The next version of this document (v0.3) will thus look very different.

Abstract

This document describes use cases for industrial automation, which may be covered by a future project or projects to add functionality to IEC/IEEE 60802 TSN Profile for Industrial Automation. These use cases can guide a specification process: a selection of these use cases would determine WHAT shall be enabled by a future project or projects that specifies HOW to achieve the use cases at the system level of an IA system. Even if a project does not cover the overall system level, the project can enable, or at least does not prevent, the features described in a use case.

In this first draft (v0.1) use case numbering (and Figure and Table numbering) from [1] (see References) is carried over to aid comparison with that document. New use cases are identified with a preceding “N”, e.g. N10. The intention is to renumber (and potentially reorder) the use cases in a future draft.

Log

v0.1	2025-11-10	Working Draft – Reviewed during Nov 2025 IEEE 802 Plenary
v0.2	2026-01-05	Working Draft – Following review during Nov 2025 IEEE 802 Plenary. Minor updates. Group consensus from meeting was to “start fresh” rather than try to edit the original Use Case document from 2018. There will therefore be a more major update prior to the next review.

References

[1] "Use Cases IEC/IEEE 60802 v1.3", group contribution to IEC/IEEE 60802, September 2018

[2] "Review of potential use cases for a potential amendment to IEC/IEEE 60802 version 2", contribution to IEC/IEEE 60802 by David McCall, September 2025

[3] "Security Use Cases IEC/IEEE 60802", group contribution to IEC/IEEE 60802, April 2022

[4] "IEC/IEEE 60802 amendment brainstorming: IA-Controller – Cloud Solution – Configuration Domain", contribution to IEC/IEEE 60802 by Günter Steindl and Dieter Proell, June 2025

[5] "IEC/IEEE 60802 Edition 2 Topics", contribution to IEC/IEEE 60802 by Mark Hantel, July 2025

[6] "Management proxies for ccA", contribution to IEC/IEEE 60802 by Thomas Enzinger, May 2025

[7] "60802 – Edition 2 – Some Topics", contribution to IEC/IEEE 60802 by Marius-Petru Stanica, May 2025

[8] "Kick-off for Brainstorming on Potential Amendment to IEC/IEEE 60802", contribution to IEC/IEEE 60802 by János Farkas, May 2025

[9] "Other considerations for IEC/IEEE 60802, Edition 2", contribution to IEC/IEEE 60802 by Jordon Woods, May 2025

[10] "Simplified Standardization Workflows, ISA/IEC 62443 Security for industrial automation and control systems and Mapping of Standards to 62443", contribution to IEC/IEEE 60802 by Dieter Proell, May 2025

Content

Figures

Tables

1 Terms and Definitions

1.1 Definitions

Reconfiguration	- Any intentional modification of the system structure or of the device-level content, including updates of any type - Ref: IEC 61158- Type 10, dynamic reconfiguration - Document provided by PI/PNO: Guidelines for high-availability
(Process) disturbance	- Any malfunction or stall of a process/machine, which is followed by production loss or by an unacceptable degradation of production quality - Ref: IEC 61158 – Failure - Ref. ODVA: Unplanned downtime - Document provided by PI/PNO: Guidelines for diagnosis
Operational state of a plant (unit)/machine	Normal state of function and production of a plant(unit)/machine
Maintenance state of a plant (unit)/machine	Planned suspension or partial suspension of the normal state of function of a plant(unit)/machine
Stopped state of a plant (unit)/machine	Full non-productive mode of a plant(unit)/machine
Convergent network concept	All LAN devices (wired or wireless) are able to exchange data over a common infrastructure, within defined QoS parameters
Device	End station, bridged end station, bridge, access point
DCS	Distributed Control System
Transmission selection algorithms	A set of algorithms for traffic selection which include Strict Priority, the Credit-based shaper and Enhanced Transmission Selection.[1)]
Preemption	The suspension of the transmission of a preemptable frame to allow one or more express frames to be transmitted before transmission of the preemptable frame is resumed.[1)]
Enhancements for scheduled traffic	A Bridge or end station may support enhancements that allow transmission from each queue to be scheduled relative to a known timescale.[1)]
Time-Sensitive Stream	A stream of traffic, transmitted from a single source station, destined for one or more destination stations, where the traffic is sensitive to timely delivery, and in particular, requires transmission latency to be bounded.[1)]
TSN domain	A quantity of commonly managed industrial automation devices; A set of devices, their Ports, and the attached individual LANs that transmit Time-Sensitive Streams using TSN standards which include Transmission Selection Algorithms, Preemption, Time Synchronization and Enhancements for Scheduled Traffic and that share a common management mechanism.

[1] taken from 802.1Q-2018

	It is an administrative decision to group these devices (see 2.2).
universal time domain	gPTP domain used for the synchronization of universal time
working clock domain	gPTP domain used for the synchronization of a working clock
isochronous domain	stations of a common working clock domain with a common setup for the isochronous cyclic real-time traffic type
cyclic real-time domain	stations with a common setup for the cyclic real-time traffic type - even from different working clock domains or synchronized to a local timescale
Network cycle	transfer time including safety margin, and application time including safety margin (see **Error! Reference source not found.**); values are s pecific to a TSN domain and specify a repetitive behavior of the network interfaces belonging to that TSN domain;
Greenfield	for the context of this document: greenfield refers to TSN-IA profile conformant devices; regardless if "old" or "new";
Brownfield	for the context of this document: brownfield refers to devices, which are not conformant to the TSN-IA profile; regardless if "old" or "new";
Stream forwarding	Forwarding of stream data along the stream path including TSN domain boundary crossings

126 1.2 IEEE802 terms

Priority regeneration	See IEEE 802.1Q-2018 clause 6.9.4 Regenerating priority
Ingress rate limiting	See IEEE 802.1Q-2018 clause 8.6.5 Flow classification and metering

127

2 TSN in Industrial Automation

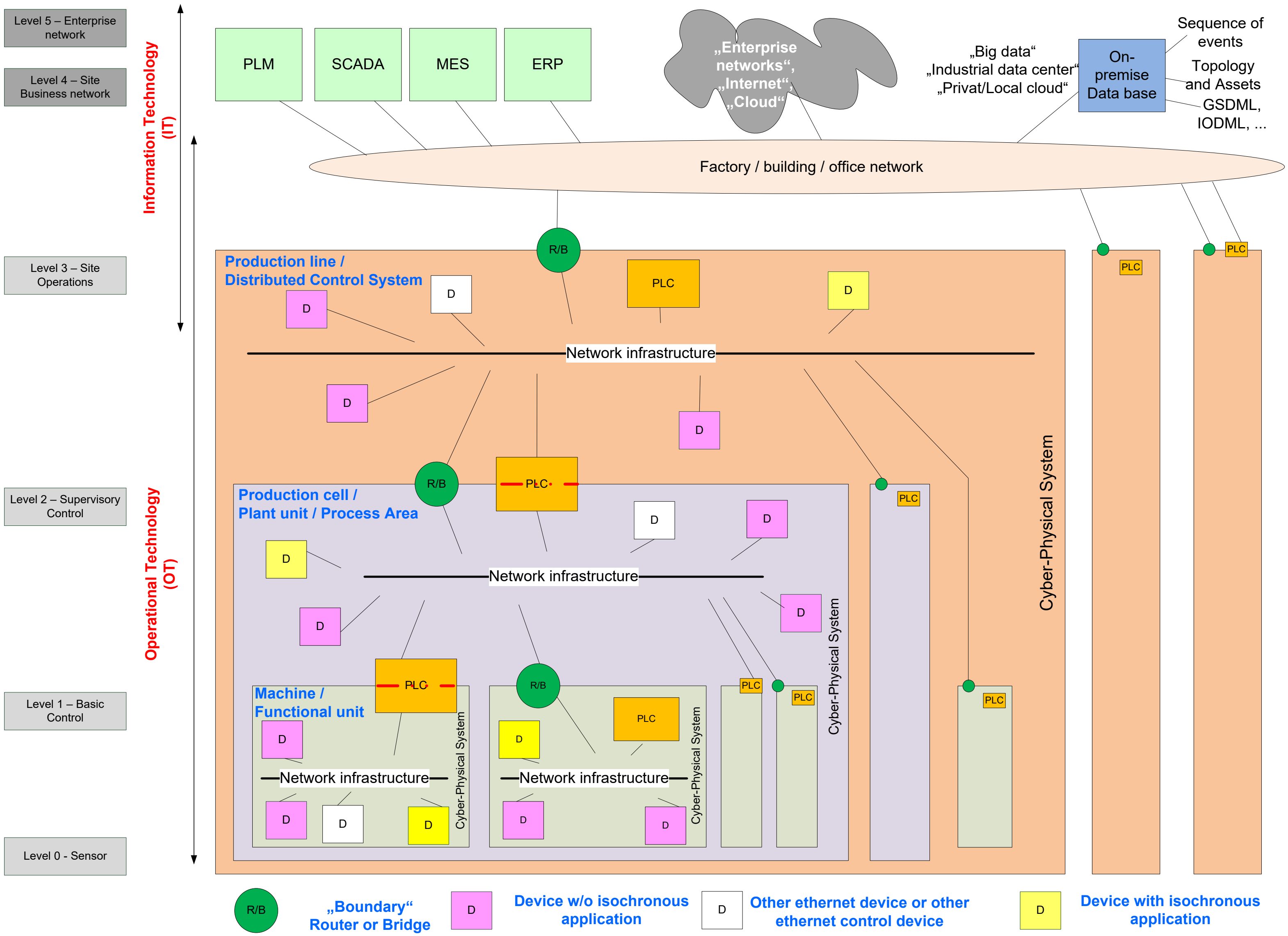

Figure 1 – Hierarchical structure of industrial automation

There is no generally accepted definition of the term “Cyber-Physical System (CPS)”. A report of Edward A. Lee [1] suitably introduces CPS as follows: „*Cyber-Physical Systems (CPS) are integrations of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa.*”

Cyber-Physical Systems are the building blocks of “smart factories” and Industry 4.0. IEEE 802 LAN technologies provide the mechanisms (e.g. TSN features) for connectivity to time critical industrial applications on converged networks in operational technology control levels.

IEEE 802 LANs with TSN features can be used in Industrial Automation for:

- Real-time (RT) Communication within Cyber-Physical Systems
- Real-time (RT) Communication between Cyber-Physical Systems

A CPS consists of:

- Controlling devices (typically 1 PLC),
- I/O Devices (sensors, actors),
- Drives,
- HMI (typically 1),
- Interface to the upper level with:
    - PLC (acting as gateway), and/or
    - Router, and/or
    - Bridge.
- Other Ethernet devices:
    - Servers or any other computers, be it physical or virtualized,
    - Diagnostic equipment,
    - Network connectivity equipment.

2.1 Interoperability

Interoperability may be achieved on different levels. Figure 2 and Figure 3 show three areas, which need to be covered:

- network configuration (managed objects according to IEEE definitions), and
- stream configuration and establishment, and
- application configuration.

The three areas mutually affect each other (see Figure 2).

Application configuration is not expected to be part of the profile, but the two other areas are.

The selection made by the TSN-IA profile covers IEEE 802 defined layer 2 and the selected protocols to configure layer 2.

Applications make use of upper layers as well, but these are out of scope for the profile.

Stream establishment is initiated by applications to allow data exchange between applications. The applications are the source of requirements, which shall be fulfilled by network configuration and stream configuration and establishment.

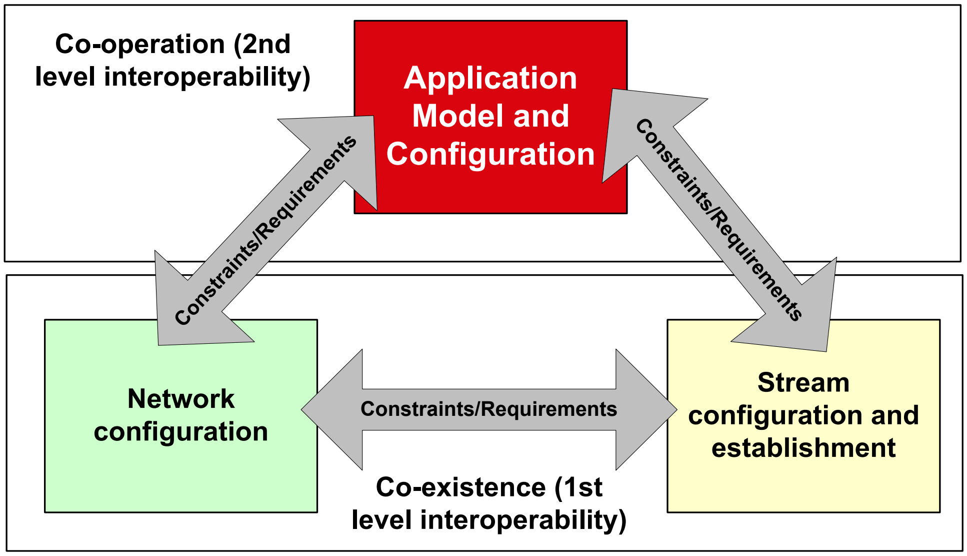

Figure 2 – Principle of interoperation

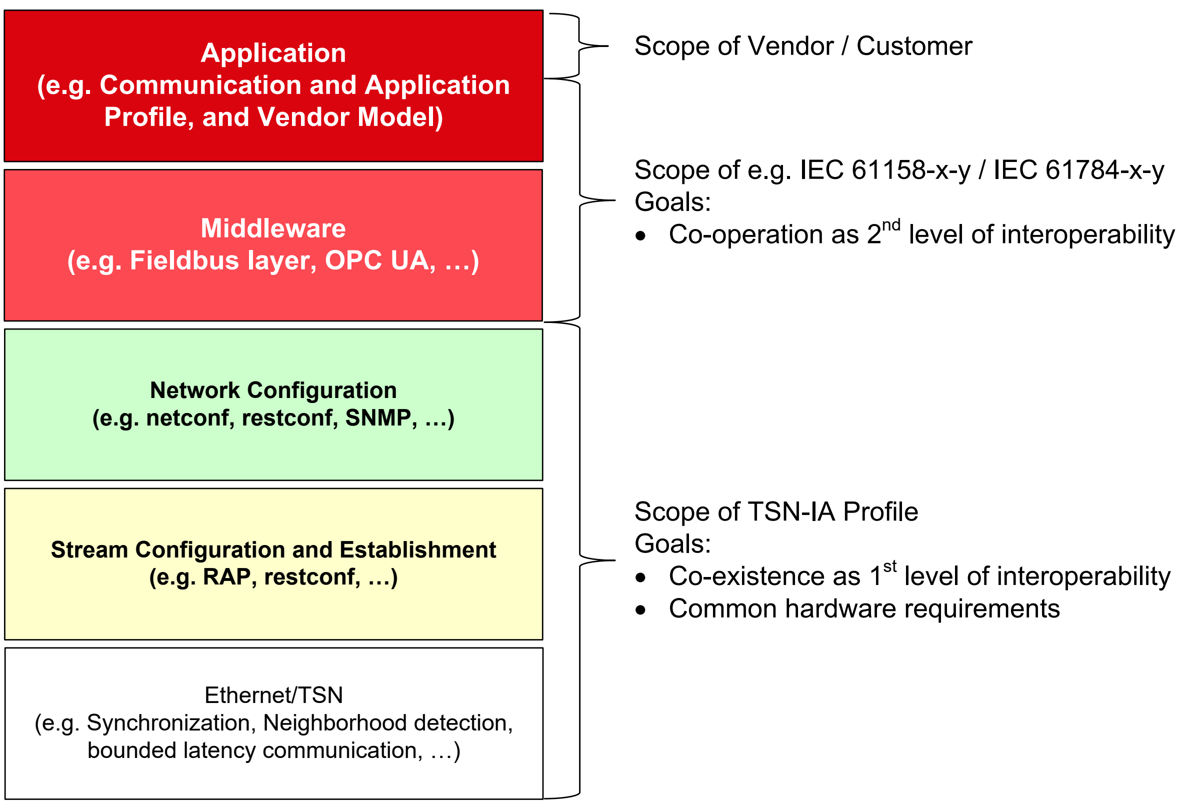

Figure 3 – Scope of work

2.2 TSN Domain

2.2.1 General

A TSN domain is defined as a quantity of commonly managed industrial automation devices; it is an administrative decision to group these devices.

TSN Domain Characteristics:

- One or more TSN Domains may exist within a single layer 2 broadcast domain.
- A TSN Domain may not be shared among multiple layer 2 broadcast domains.
- Multiple TSN Domains may share a common universal time domain.
- Two adjacent TSN Domains may implement the same requirements but stay separate.
- Multiple TSN domains will often be implemented in one bridge (see 2.2.2.2).
- Multiple TSN domains will often be implemented in one router (see 2.2.2.3).
- Multiple TSN domains will often be implemented in one gateway (see 2.2.2.4).

Typically machines/functional units (see Figure 1) constitute separate TSN domains. Production cells and lines may be set up as TSN domains as well. Devices may be members of multiple TSN domains in parallel.

Figure 4 shows two example TSN domains within a common broadcast domain and a common universal time domain. TSN domain 1 is a pure cyclic real-time domain, whereas TSN domain 2 additionally includes three overlapping isochronous domains.

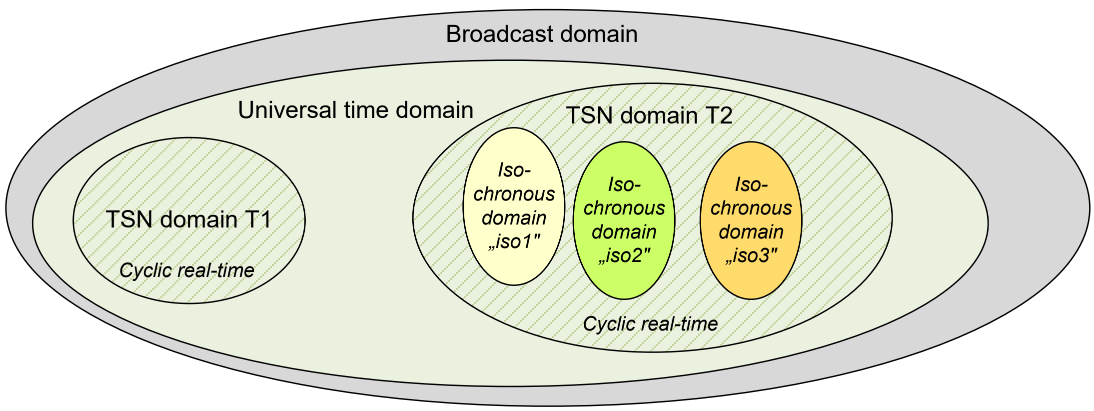

Figure 4 – Different Types of Domains

Interconnections between TSN domains are described in 2.2.2 and 2.6.1.

2.2.2 Interconnection of TSN Domains

2.2.2.1 General

TSN domains may be connected via

- Bridges (Layer 2), or
- Routers (Layer 3), or
- Application Gateways (Layer 7).

Wireless Access Points or 5G Base Stations may be used to connect TSN domains, too.

2.2.2.2 Bridges (Layer 2)

When a Bridge is member of multiple TSN domains, one bridge port must only be a member of a single TSN domain.

Figure 5 provides an example of two Bridges, which are members of two TSN domains each. Bridge B1 provides ports and connectivity in TSN domain Production Cell 1 and in TSN domain Machine 1, Bridge B2 for Production Line 1 and Production Cell 1.

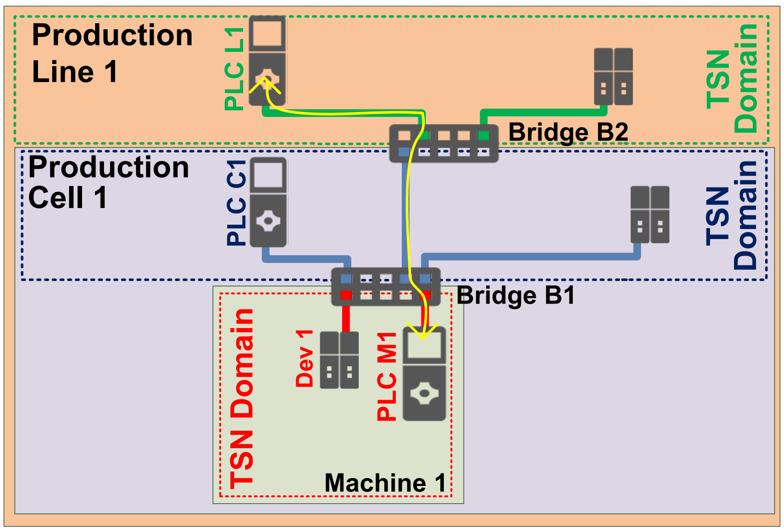

Figure 5 – Three TSN domains connected by Bridges

To support connectivity between multiple TSN domains (e.g. PLC L1 ↔ PLC M1) a method for reserving time-sensitive streams over multiple TSN domains needs to be specified, including:

- find the communication partner,
- identify the involved TSN domains,
- identify the involved management entities independent from the configuration model (centralized, hybrid, fully distributed),
- ensure the needed resources,
- parameterize the TSN domain connection points to allow stream forwarding if needed.

2.2.2.3 Routers (Layer3)

Together with routers, both intranet and internet are possible. In this sub-clause, however, only the intranet use case is addressed.

When a router is member of multiple TSN domains, one router interface/port must only be a member of a single TSN domain. Figure 6 provides an example of two routers, which are members of two TSN domains each. Router R1 provides ports and connectivity in TSN domain Production Cell 1 and in TSN domain Machine 1, Router R2 for Production Line 1 and Production Cell 1.

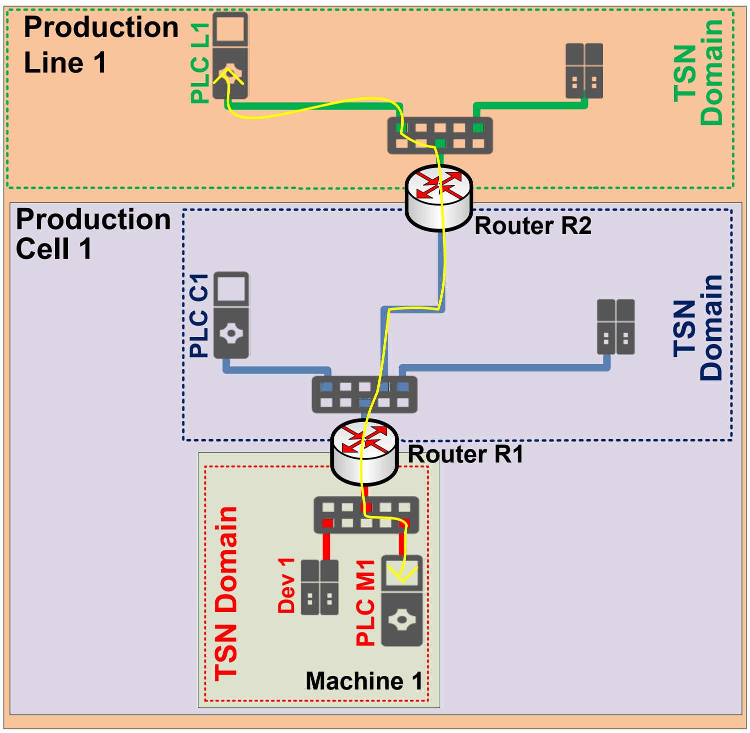

Figure 6 – Three TSN domains connected by Routers

To support connectivity between multiple TSN domains (e.g. PLC L1 ↔ PLC M1) a method for reserving time-sensitive streams over multiple TSN domains needs to be specified, including:

- find the communication partner,
- identify the involved TSN domains,
- identify the involved management entities independent from the configuration model (centralized, hybrid, fully distributed),
- ensure the needed resources,
- parameterize the TSN domain connection points to allow stream forwarding if needed.

2.2.2.4 Application Gateways (Layer7)

When an Application Gateway is member of multiple TSN domains, one gateway interface/port must only be a member of a single TSN domain.

Figure 7 provides an example of two application gateways:

- Gateway CM1 is member in the TSN domains Production Cell 1 and Machine 1;
- Gateway CF1 is member of the TSN domain Production Cell 1 and of Fieldbus 1.

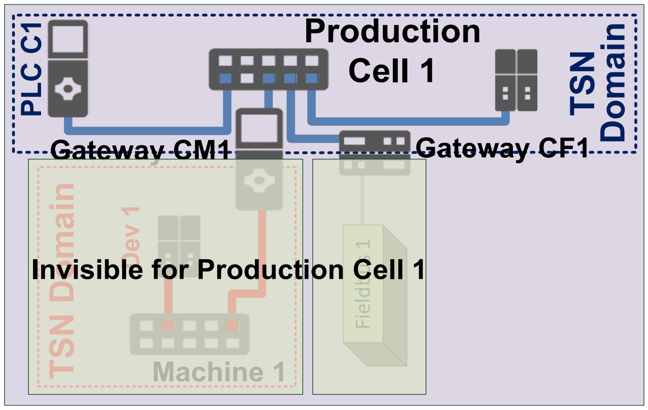

Figure 7 – Gateways with two TSN domains and an attached Fieldbus

Application level gateways do not provide direct access between devices of different TSN domains. Instead the application gateways act as end-stations for TSN domain egress and ingress communication.

An application specific translation of control and data to access adjacent TSN domains may be implemented in the application level gateway to realize TSN domain interconnections. The translation may even involve buffering, collecting and re-arranging of data and control. Thereby application level gateways decouple TSN domains, so that the internal structure and configuration of adjacent TSN domains is not visible respectively.

Application level gateways are also used to connect non-Ethernet- or Ethernet-based fieldbuses to TSN domains (see Gateway CF1 in Figure 7 and see also **Error! Reference source not found.**).

2.3 Synchronization

2.3.1 General

Synchronization covering both universal time (wall clock) and working clock is needed for industrial automation systems.

Redundancy for synchronization of universal time may be solved with “cold standby”. Support of "Hot standby" for universal time synchronization is not current practice - but may optionally be supported depending on the application requirements.

Redundancy for working Clock synchronization can be solved with “cold standby” or “hot standby” depending on the application requirements. Support of "hot standby" for working clock synchronization is current practice.

More details about redundancy switchover scenarios are provided in: http://www.ieee802.org/1/files/public/docs2018/60802-Steindl-TimelinessUseCases-0718-v01.pdf.

2.3.2 Universal Time Synchronization

Universal time is used to plant wide align events and actions (e.g. for “sequence of events”). The assigned timescale is TAI, which can be converted into local date and time if necessary. Figure 8 shows the principle structure of time synchronization with the goal to establish a worldwide aligned timescale for time. Thus, often satellites are used as source of the time.

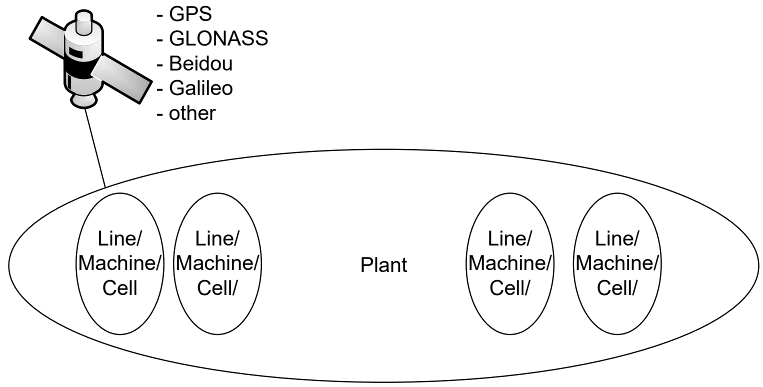

Figure 8 – plant wide time synchronization

Note: “Global Time” or “Wall Clock” are often used as synonym terms for “Universal Time”.

2.3.3 Working Clock Synchronization

Working Clock is used to align actions line, cell or machine wide. The assigned timescale is arbitrary. Robots, motion control, numeric control and any kind of clocked / isochronous application rely on this timescale to make sure that actions are precisely interwoven as needed. Figure 9 shows the principle structure of Working Clock synchronization with the goal to establish a line / cell / machine wide aligned timescale. Thus, often PLCs, Motion Controller or Numeric Controller are used as Working Clock source.

If multiple PLCs, Motion Controller or Numeric Controller need to share one Working Clock timescale (e.g. for scheduled traffic), an all-time active station shall be used as Working Clock source, also known as Grandmaster.

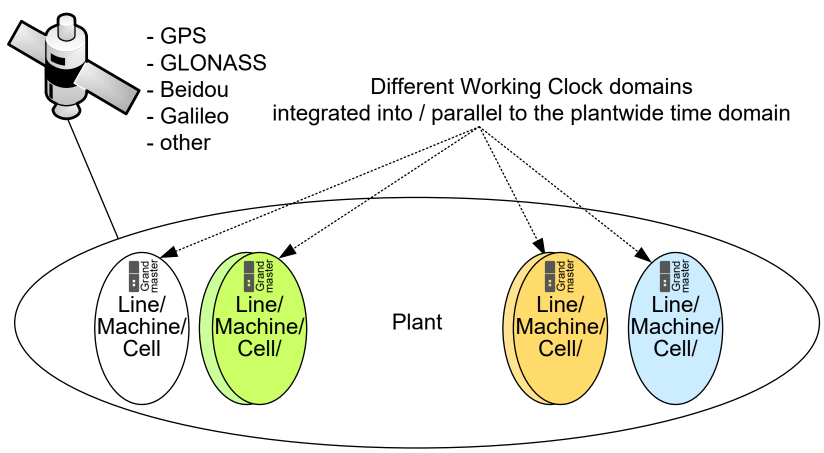

Figure 9 – line/cell/machine wide working clock synchronization overlapping with a universal time domain

Working Clock domains may be doubled to support zero failover time for synchronization.

High precision working clock synchronization is a prerequisite for control loop implementations with low latency (see 2.4.2).

Requirements:

- High precision working clock synchronization;
- Maximum deviation to the grandmaster time in the range from 100 ns to 1 µs;
- Support of redundant sync masters and domains;
- Zero failover time in case of redundant working clock domains;

Useful 802.1 mechanisms:

- IEEE 802.1AS-Rev

2.4 Industrial automation modes of operation

2.4.1 Industrial automation traffic types

Note: is this still necessary in the Use Cases document? Has the material in 60802 superseded it?

2.4.1.1 General

Industrial automation applications concurrently make use of different traffic types for different functionalities, e.g. parameterization, control, alarming. The various traffic types have different characteristics and thus impose different requirements on a TSN network. This applies for all use cases described in this document.
Table 1 subsumes the industrial automation relevant traffic patterns to traffic types with their associated properties (see also [4]).

Table 1 – Industrial automation traffic types summary

Traffic type name	Periodic/ Sporadic	Guarantee	Data size	Redundancy	Details
isochronous cyclic real-time	P	deadline/ bounded latency (e.g. 20%@1 Gbit/s / 50%@100 Mbit/s network cycle)/ bandwidth	bounded	up to seamless[1]	see **Error! Reference source not found.** and 2.4.2
cyclic real-time	P	deadline/ bounded latency (e.g. n-times network cycle)/ bandwidth	bounded	up to seamless[1]	see **Error! Reference source not found.** and **Error! Reference source not found.**
network control	S	Priority	-	up to seamless[1] as required	see 2.2.2 and 2.5.1
audio/video	P	bounded latency/ bandwidth	bounded	up to seamless[1] as required	-
brownfield	P	bounded latency/ bandwidth	-	up to regular[2]	see **Error! Reference source not found.**
alarms/ events	S	bounded latency/ bandwidth	-	up to regular[2]	see **Error! Reference source not found.**
configuration/ diagnostics	S	Bandwidth	-	up to regular[2]	see **Error! Reference source not found.**
Internal / Pass-through	S	Bandwidth	-	up to regular[2]	see 2.6.2
best effort	S	-	-	up to regular[2]	-

[1] almost zero failover time;

[2] larger failover time because of network re-convergence

All traffic types of Table 1 are referenced by the use cases, which are described in this document:

Isochronous:

→ see ***Error! Reference source not found.***

In addition, if an isochronous application interface is needed: Machine vision application use cases for counting, sorting, quality control, video surveillance, augmented reality, motion guidance …

Cyclic:

→ see ***Error! Reference source not found.***

In addition, if a cyclic application interface is needed: Machine vision application use cases for counting, sorting, quality control, video surveillance, augmented reality, motion guidance …

Network control:

→ see *Use case 01: Redundant networks*

Audio/video:

→ IEEE Std 802.1BA-2011 (AVB) may be supported in industrial automation as well

Brownfield:

→ see ***Error! Reference source not found.***

Alarms/events:

→ see ***Error! Reference source not found.***

Configuration/diagnostics:

→ see ***Error! Reference source not found.***

Internal:

→ see *Use case 04: Pass-through Traffic*

Best effort:

→ see …

2.4.1.2 Characterization of isochronous cyclic real-time and cyclic real-time

The following properties table is used to characterize in detail the traffic types of **Error! Reference source not found.** and **Error! Reference source not found.**.

Table 2 – isochronous cyclic real-time and cyclic real-time traffic type properties

Property	Description
Data transmission scheme	*Periodic* (P) - e.g. every N µs, or *Sporadic* (S) - e.g. event-driven
Data transmission constraints	Indicates the traffic pattern's data transmission constraints for proper operation. Four data transmission constraints are defined: • *deadline*: transmitted data is guaranteed to be received at the destination(s) before a specific instant of time, • *latency*: transmitted data is guaranteed to be received at the destination(s) within a specific period of time after the data is transmitted by the sending application, • *bandwidth:* transmitted data is guaranteed to be received at the destination(s) if the bandwidth usage is within the resources reserved by the transmitting applications,

Property	Description
	• *none:* no special data transmission constraint is given.
Data period	For traffic types that transmit *periodic* data this property denotes according to the *data transmission constraints*: *deadline*: application data deadline period, *latency*, *bandwidth* or *none*: data transmission period. The period is given as a *range* of time values, e.g. 1µs ... 1ms. For the *sporadic* traffic types, this property does not apply.
Network access (data transmission) synchro-nized to working clock (network cycle)	Indicates whether the data transmission of sender stations is synchronized to the working clock (network cycle). Available property options are: *yes, no* or *optional.*
Application synchronized to network access	Indicates whether the applications, which make use of this traffic pattern, are synchronized to the network access. Available property options are: *yes* or *no.*
Acceptable jitter	Indicates for traffic types, which apply data transmission with *latency* constraints, the amount of jitter, which can occur and must be coped with by the receiving destination(s). For traffic types with *deadline, bandwidth* or *none* data transmission constraints this property is not applicable (*n.a.*).
Acceptable frame loss	Indicates the traffic pattern’s tolerance to lost frames given e.g. as acceptable frame loss ratio range. The frame loss ratio value *0* indicates traffic types, where no single frame loss is acceptable.
Payload	Indicates the payload data *type* and *size* to be transmitted. Two payload types are defined: • *fixed:* the payload is always transmitted with exactly the same size • *bounded:* the payload is always transmitted with a size, which does not exceed a given maximum; the maximum may be the maximum Ethernet payload size (1500).

2.4.2 Bidirectional communication relations

The general behavior of field devices of process sensors and output signals is preconfigured and offers a set of services to a machine control unit. More complex field devices such as drives or machine parts have process data in both directions. If there are only outputs in a field device the stream back to the machine control is necessary for fast detection of problems in a field device. If there are only input process data the stream from the machine control to the field device is not necessary for normal operation.

The cell control communicates with the machine controls of the machines also in a bidirectional way.

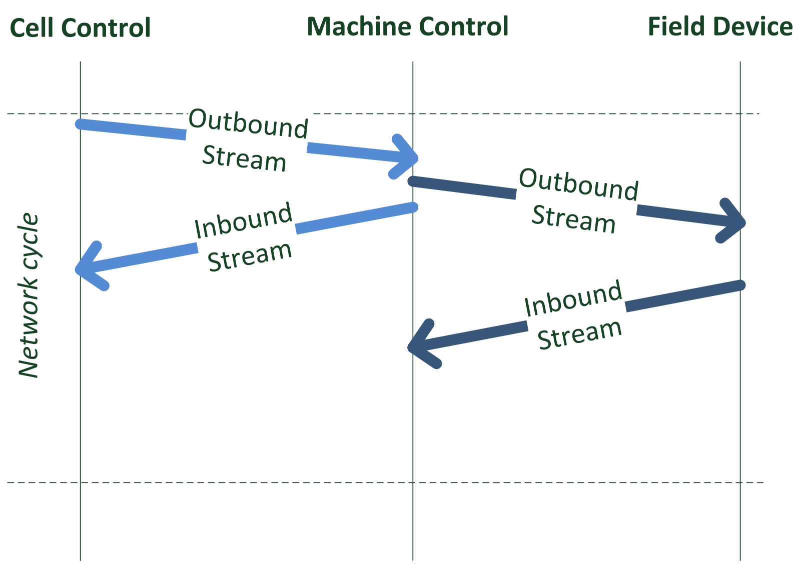

Figure 10 – Bidirectional Communication

Requirements:

- Support of bidirectional streams;
- Sequence of actions how to establish such streams (see Figure 10);

Useful 802.1 mechanisms:

- IEEE 802.1Q (usage of streams)

2.4.3 Control Loop Basic Model

Control loops are fundamental building blocks of industrial automation systems. Control loops include: process sensors, a controller function, and output signals. Control loops may require guaranteed low latency or more relaxed bounded latency (see **Error! Reference source not found.**) network transfer q uality.

To achieve the needed quality for Control loops the roundtrip delay (sometimes called makespan, too) of the exchanged data is essential.

Figure 11 shows the whole transmission path from Controller application to Device application(s) and back. The blue and red arrows show the contributions to the e2e (end-to-end) latency respectively.

Figure 11 and Table 3 show three levels of a control loop:

- Application - within Talker/Listener,
- Network Access - within Talker/Listener,
- Network Forwarding - within Bridges.

Network Access is always synchronized to a common working clock or to a local timescale.

Application may or may not be synchronized to the synchronized Network Access depending on the application requirements. Applications which are synchronized to Network Access are called “isochronous applications”. Applications which are not synchronized to Network Access are called “non-isochronous applications”.

Network Forwarding may or may not be synchronized to a working clock depending on whether the Enhancements for Scheduled Traffic (IEEE Std 802.1Q-2018) are applied.

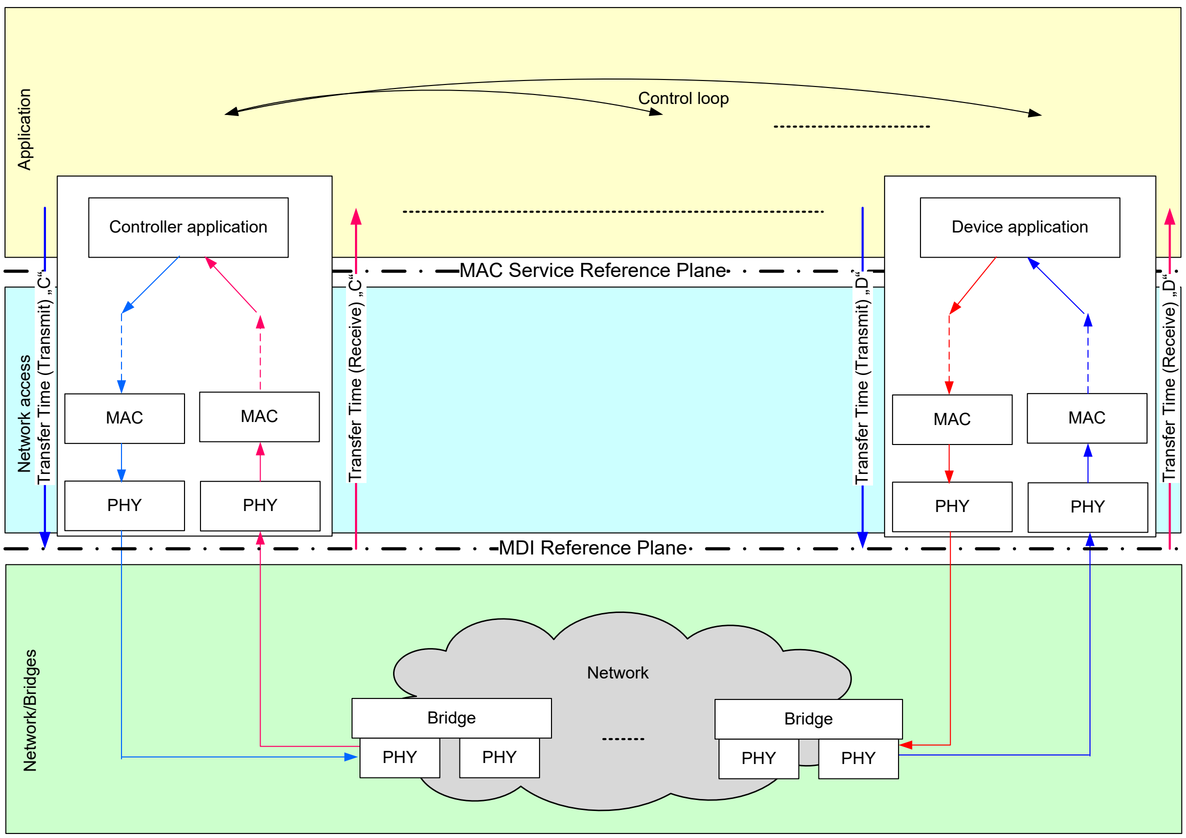

Figure 11 – Principle data flow of control loop

Transfer Times contain PHY and MAC delays. Both delays are asymmetric and vendor specific. Device vendors have to take into account these transfer times when their application cycle models are designed (see Figure 11 and **Error! Reference source not found.**).

Table 3 – Application types

<table>
<tr><th>Level</th><th colspan="2">Isochronous Application</th><th colspan="3">Non-isochronous Application</th></tr>
<tr><td>Application</td><td colspan="2">Synchronized to network access</td><td colspan="3">Synchronized to local timescale</td></tr>
<tr><td>Network access</td><td colspan="4">Synchronized to working clock,
Stream Class based scheduling, Preemption</td><td>Synchronized to local timescale,
Stream Class based scheduling, Preemption</td></tr>
<tr><td rowspan="2">Network/Bridges</td><td>Synchronized to working clock</td><td>Free running</td><td>Synchronized to working clock</td><td>Free running</td><td>Free running</td></tr>
<tr><td>Scheduled traffic + Strict Priority + Preemption</td><td>Strict Priority or other Shaper + Preemption</td><td>Scheduled traffic + Strict Priority + Preemption</td><td>Strict Priority or other Shaper + Preemption</td><td>Strict Priority or other Shaper + Preemption</td></tr>
</table>

2.5 Industrial automation networks

2.5.1 Use case 01: Redundant networks

Ring topologies are the basic industrial network architecture for switch-over or seamless redundancy.

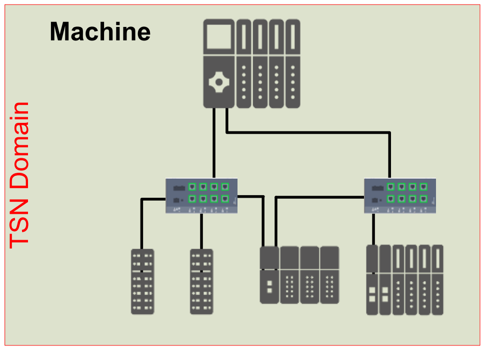

Figure 12 – ring topology

When a production cell is also arranged in a ring topology the resulting architecture of cell with attached machines is an interconnection of rings.

To even improve availability of the interconnection from the production cell into the machines this link can be arranged redundantly as well (machine 1 in Figure 13):

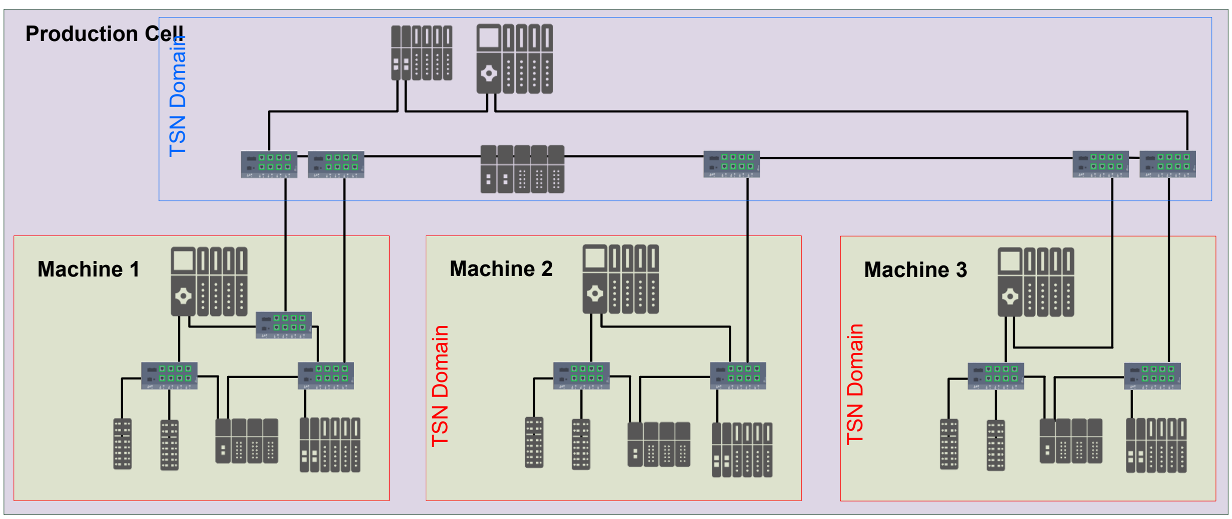

Figure 13 – connection of rings

Requirement:

Support redundant topologies with rings.

Note: FRER is part of 60802, but not all features. (End Station replication & elimination supported; but not for Relays.)

Useful 802.1 mechanisms:

- 802.1CB - FRER

2.5.2 Use case 02: Wireless

HMI panels, remote IOs, wireless sensors or wireless bridges are often used in industrial machines. Wireless connections may be based on IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 or ITU/3GPP (5G). Even functional safety applications over wireless connections are supported (see **Error! Reference source not found.**).

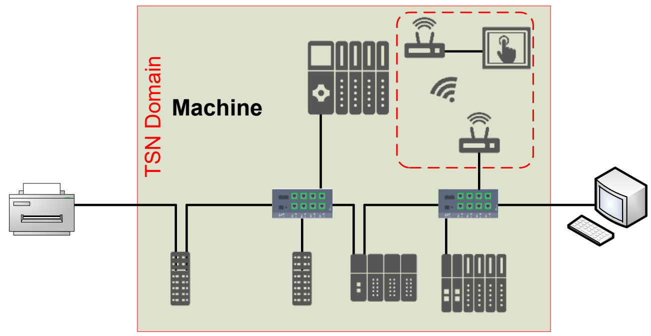

Figure 14 – HMI wireless connected using cyclic real-time

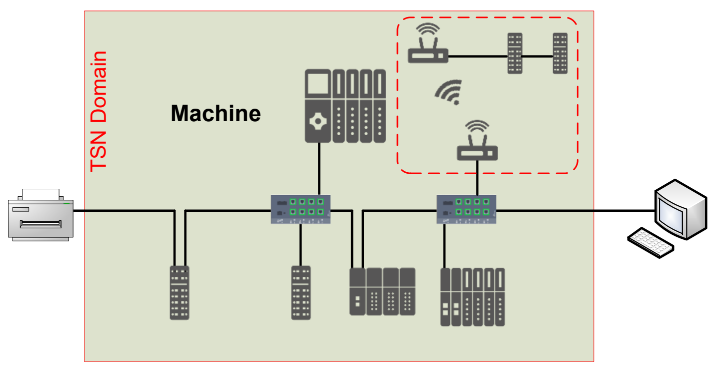

Figure 15 – Remote IO wireless connected using cyclic real-time

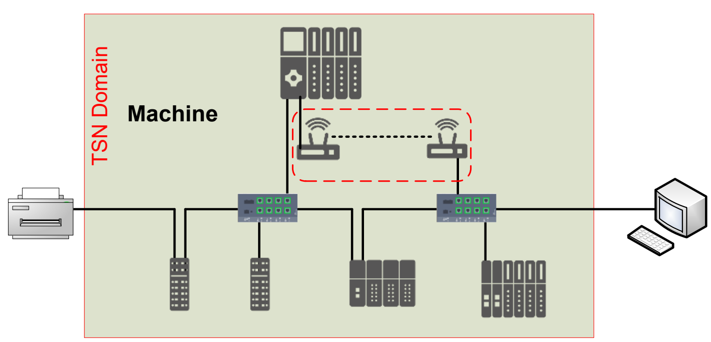

Figure 16 – Ring segment wireless connected for media redundancy

<u>Requirement</u>:

Support of wireless for

- cyclic real-time, and
- non-real-time communication

<u>Useful 802.11 mechanisms:</u>

- Synchronization support

- Extensions from .11ax
- …

Useful 802.15.1 mechanisms:

- …

Useful 802.1Q mechanisms:

- …

limits and cycle times (see e.g. row Data period in **Error! Reference source not found.**).

2.5.3 Use case N10: Multi-Subnet Operation

See [4].

2.6 Industrial automation machines, production cells, production lines

2.6.1 Use case 03: Machine to Machine/Controller to Controller (M2M/C2C) Communication

Preconfigured machines with their own TSN domains, which include tested and approved internal communication, communicate with other preconfigured machines with their own TSN domains, with a supervisory PLC of the production cell (with its own TSN domain) or line (with its own TSN domain) or with an Operations Control HMI (with its own TSN domain).

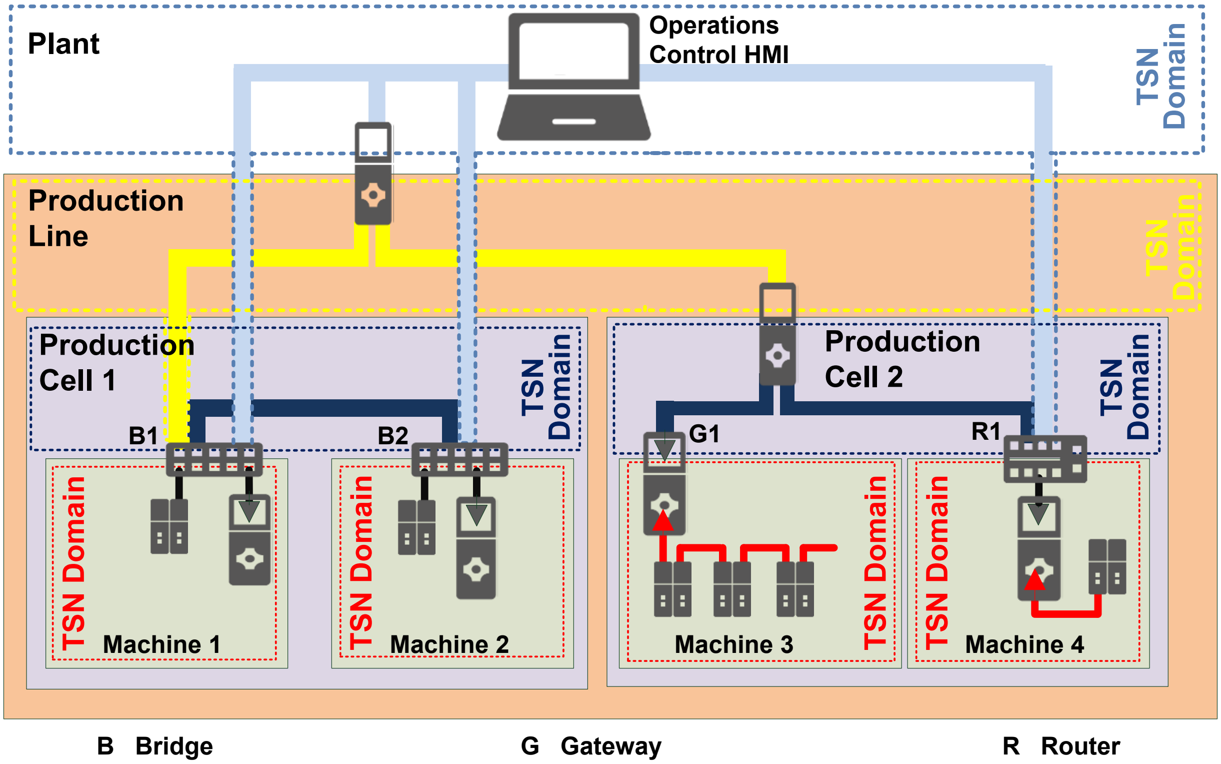

Figure 17 – M2M/C2C between TSN domains

Figure 17 shows that multiple logical overlapping TSN Domains arise, when controllers use a single interface for the M2M communication with controllers of the cell, line, plant or other machines. Decoupling of the machine internal TSN Domain can be accomplished by applying a separate controller interface for M2M communication.

Machine 1: the controller link to its connected cell bridge B1 is concurrently member of the TSN Domains of Machine 1, Production Cell 1, Production Line and Plant.

Machine 2: the controller link to its connected cell bridge B2 is concurrently member of the TSN Domains of Machine 2, Production Cell 1 and Plant.

Machine 3: the controller is directly attached to the PLC of Production Cell 2 and is therefore member of the TSN Domain of Production Cell 2. The machine internal TSN Domain is decoupled from M2M traffic by a separate interface.

Machine 4: the controller link to its connected cell bridge B3 is concurrently member of the TSN Domains of Production Cell 2 and Plant. The machine internal TSN Domain is decoupled from M2M traffic by a separate interface.

<u>Examples</u>:

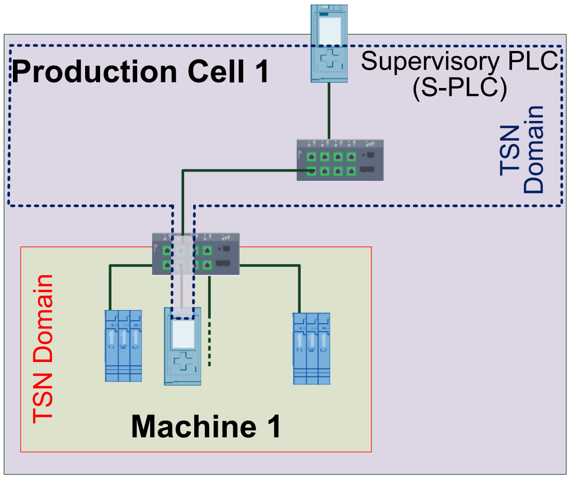

Figure 18 gives an example of M2M communication to a supervisory PLC.

Figure 19 shows an example of M2M communication relations between four machines.

PLCs with one single interface lead to overlapping communication paths of M2M and machine internal traffic. In this case two TSN domains (Machine / Production cell) need to share resources due to two logical overlapping TSN domains.

Figure 18 – M2M with supervisory PLC

There are quite a few constraints related to the machine internal networks. Each machine may run a different schedule and even the intervals may be different. It may be very complex or even impossible to find an optimal communication schedule down from the sensors and actuators to the cell control. The requirements for cascaded control loops require faster intervals for the lower control loops. The multiple machine intervals embedded in one cell interval can be mapped onto a sequence of intervals. Each step in the exchange of data between machine and cell control unit can be mapped into machine intervals:

- outbound cell communication,
- transfer outbound within machine network,
- transfer inbound within machine network,
- inbound cell communication.

Additionally Figure 20 shows an example where M2M communication is used to connect a PC for diagnostics/monitoring.

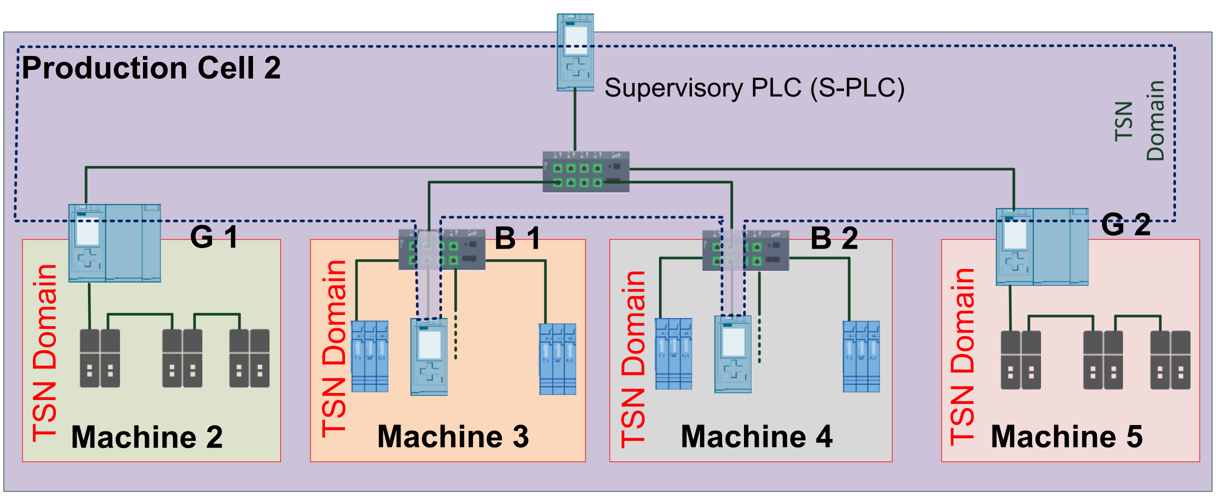

Figure 19 – M2M with four machines

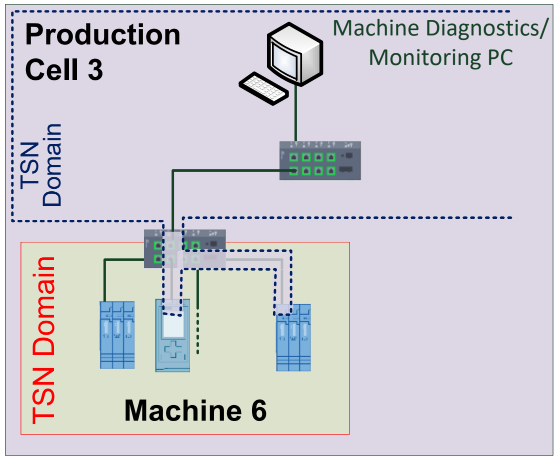

Figure 20 – M2M with diagnostics/monitoring PC

Figure 20 shows a M2M diagnostics related use case: communication is cyclic and shall happen within short application cycle times. An example of this use case is the verification of proper behavior of a follower drive, in a master-follower application. Today, the use case is covered by connecting a common PC to an interface of the follower drive. The various TSN mechanisms may now make it possible to connect such a PC network interface card anywhere in the system network and still gather the same diagnostics with the same guarantees, as the current direct connection.

The required guarantees are:

Each 4 ms a frame shall be sent from a follower drive and have its delivery guaranteed to the network interface of the PC used to perform the diagnostics. Of course, local PC-level processing of such frames has to be implemented such that the diagnostic application gets the required quality of service.

From the communication point of view the two types of machine interface shown in Figure 19 are identical. The PLC represents the machine interface and uses either a dedicated (machine 1 and 4) or a shared interface (machine 2 and 3) for communication with other machines and/or a supervisor PLC.

The communication relations between machines may or may not include or make use of a supervisory PLC.

Requirement:

- All machine internal communication (stream traffic and non-stream traffic) is decoupled from and protected against the additional M2M traffic and vice versa.
- 1:1 and 1:many communication relations shall be possible.
- Scheduling in a way that interleaved operation with machine intervals is possible.

Useful 802 mechanisms:

- IEEE Std 802.1Q-2018, Fixed priority, IEEE Std 802.3br
- Priority Regeneration,
- Queue-based resource allocation,
- VLANs to separate TSN domains.

2.6.2 Use case 04: Pass-through Traffic

Machines are supplied by machine builders to production cell/line builders in tested and approved quality. At specific boundary ports standard devices (e.g. barcode reader) can be attached to the machines. The machines support transport of non-stream traffic through the tested/approved machine (“pass-through traffic”) without influencing the operational behavior of the machine, e.g.

connection of a printer or barcode reader. Figure 21, Figure 22 and Figure 23 give some examples of pass-through traffic installations in industrial automation.

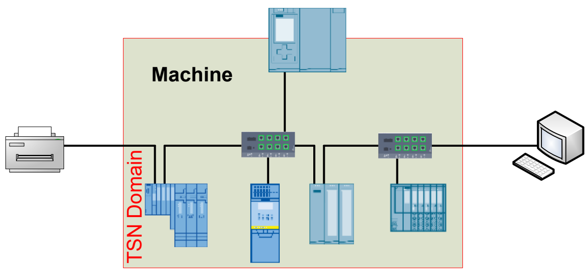

Figure 21 – pass-through one machine

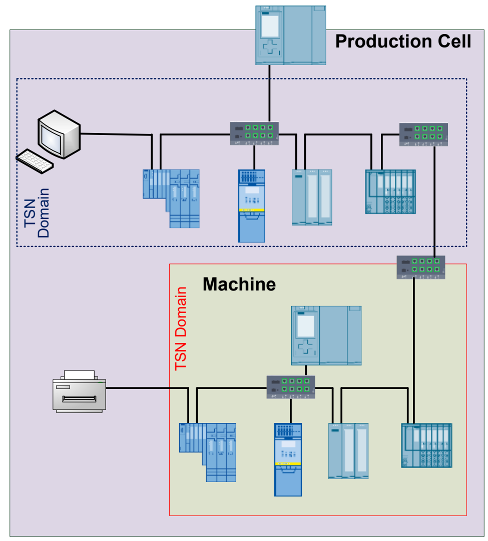

Figure 22 – pass-through one machine and production cell

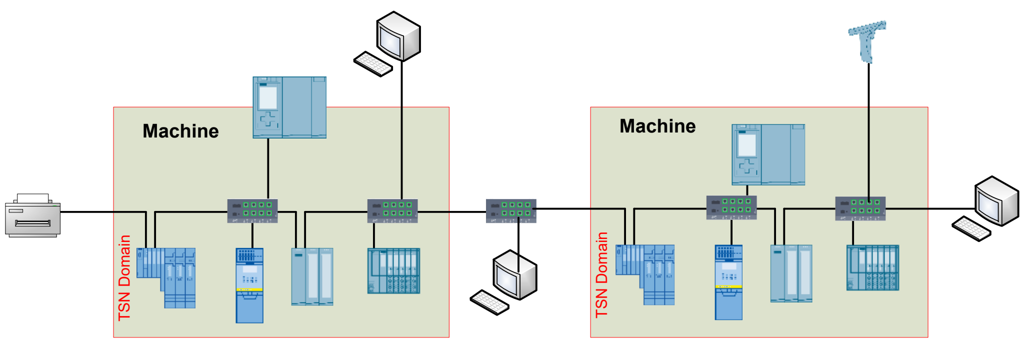

Figure 23 – pass-through two machines

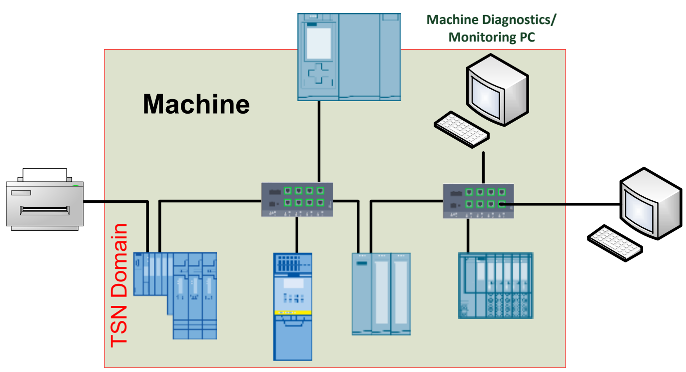

Figure 24 – machine with diagnostics / monitoring PC

Requirement:

All machine internal communication (stream traffic and non-stream traffic) is decoupled from and protected against the additional “pass-through” traffic.
“Pass-through” traffic is treated as separate traffic pattern.

Note: Boundary Port prevents pass-through traffic.

Useful 802.1Q mechanisms:

- Priority Regeneration,
- separate "pass-through traffic queue",
- Queue-based resource allocation in all bridges,
- Ingress rate limiting.

2.6.3 Use case 05: Dynamic plugging and unplugging of machines (subnets)

E.g. multiple AGVs (automatic guided vehicles) access various docking stations to get access to the supervisory PLC. Thus, an AGV is temporary not available. An AGV may act as CPS or as a bunch of devices.

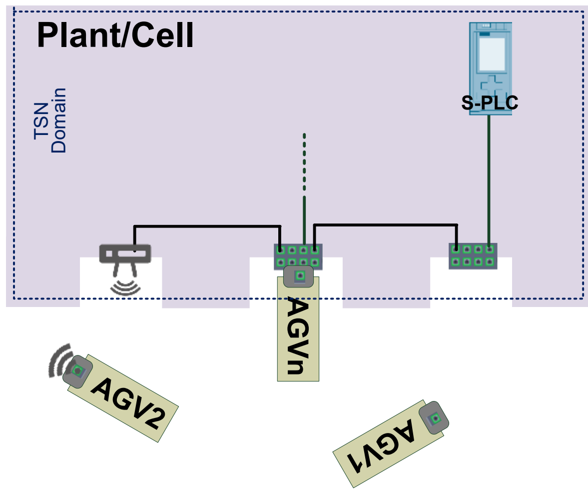

Figure 25 – AGV plug and unplug

Requirement:
The traffic relying on TSN features from/to AGVs is established/removed automatically after plug/unplug events.
Different AGVs may demand different traffic layouts.
The time till operate influences the efficiency of the plant.
Thousands of AGS may be used concurrently, but only a defined amount of AGVs is connected at a given time.

Note: Mechanisms to manage wireless connections are missing.

Useful 802.1Q mechanisms:

- preconfigured streams
- …

2.6.4 Use case 06: Add machine, production cell or production line

When production capacity is exhausted, additional machines, production cells or even production lines are bought and integrated into a plant.
E.g. an additional welding robot is added to a production cell to increase production capacity. The additional machine has to be integrated into the production cell control with minimal disturbance of the production cell process.

Another aspect is when a machine or a group of machines is tested in a stand-alone mode first before it is used in the combination with other machines or in combination with a supervisory system.

A flexible cell communication is needed to support this. Enabling and disabling of cell communication within a machine should be possible with minimal impact on production.

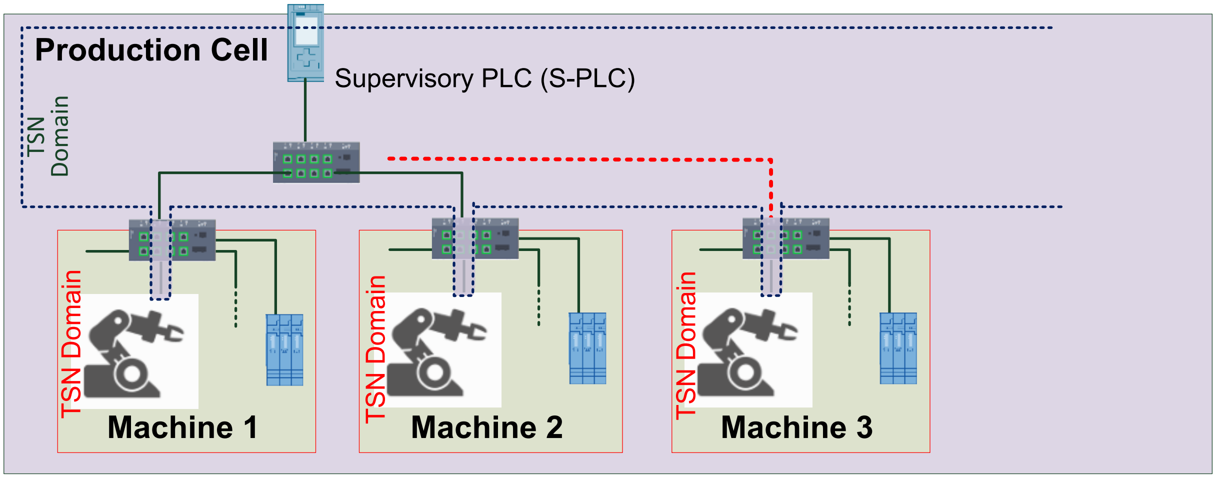

Figure 26 – add machine

Requirement:

Adding and removing a machine/cell/production line shall not disturb existing installations

Note: Only supported within a single configuration domain. Not supported across multiple domains.

Useful mechanisms:

- …

2.6.5 Use case 07: Machine cloning

The machines used in a cell can be identical but with a different task. Robots are a typical example of that kind of machines (see Figure 27). Thus, both machines have the same internal communication flows. The difference is just different machine identification for the external flow. The concept as of today is that the machine internal configuration has its identification and the cell system has its configuration but there is no dependency between both. The machine internal setup is done earlier and the cell identification is a result from a different configuration step and is done by a different organizational unit. Thus, it is difficult to propagate the cell level identification at the very beginning to the machine internal components. A worst case scenario is the startup of a machine and the connection to a cell in an ad hoc way with identification of the machine by the globally unique MAC address of the machine and the resolution of other addresses within the cell controller or above (e.g. for allocation of IP addresses). If there is a need to communicate with a few field device within the machine in a global way the machine subsystem has to be configured accordingly in advance. This configuration step could be done by a different organization as the stream configuration and not all machine internal elements may require a global address.

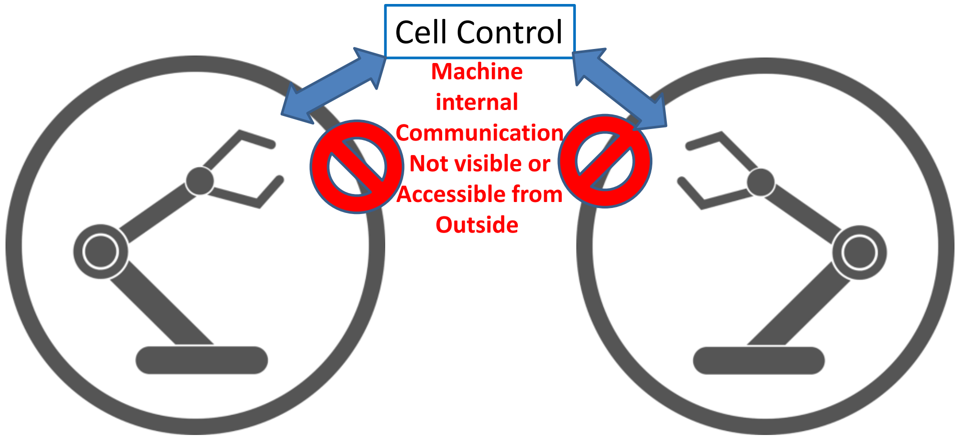

Figure 27 – Machine internal communication with isolated logical infrastructure

Requirements:

- TSN domains with unique addressing within the TSN domains;
- Unique TSN domain identification (e.g. using LLDP) also for cloned machines;
- Define handling of specific addresses (e.g. IP addresses) for global identification and how they are managed within the machine set-up procedures;

Note: Only supported within a single configuration domain. Not supported across multiple domains.

Useful 802.1 mechanisms:

- IEEE 802.1Q (usage of streams)
- IEEE 802.1 support for isolation is VLAN

2.7 Further Industrial Automation Use Cases

2.7.1 Use case 08: Security

Industrial automation equipment can become the objective of sabotage or spying.
Therefore all aspects of information security can be found in industrial automation as well:

- Confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes."
- Integrity means maintaining and assuring the accuracy and completeness of data.
- Availability implies that all resources and functional units are available and functioning correctly when they are needed. Availability includes protection against denial-of-service attacks.
- Authenticity aims at the verifiability and reliability of data sources and sinks.

Requirement:

Optional support of confidentiality, integrity, availability and authenticity.
Security shall not limit real-time communication

Note: Limited security for Control Plane only.

Protection against rogue applications running on authenticated stations are out of scope.

Note: No mechanisms identified for the Data Plane, so no guarantees. (It is expected that upper layer protocols will provide Data Plane security.)

Useful mechanisms:

- 802.1X
- IEC62443
- …

Abbreviations

AGV	Autonomous Guided Vehicle
CCTV	Closed Circuit Television
DCS	Distributed Control System
FW	Firmware
PA	Process Automation

Literature and related Contributions

Literature:

[1] "Cyber Physical Systems: Design Challenges", E. A. Lee, Technical Report No. UCB/EECS-2008-8; http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html

[2] Beckers, K. (2015). Pattern and Security Requirements: Engineering-Based Establishment of Security Standards; Springer; ISBN 9783319166643

[3] PI: Isochronous Mode – Guideline for PROFINET IO; V1.0; June 2016; available at http://www.ieee802.org/1/files/private/liaisons

Related contributions:

[4] LNI traffic patterns for TSN: http://www.ieee802.org/1/files/public/docs2018/new-Bruckner-LNI-traffic-patterns-for-TSN-0118.pdf

[5] Multivendor Motion Control: http://ieee802.org/1/files/public/docs2018/new-industrial-enzinger-multivendor-motion-control-0318-v01.pdf

[6] Hierarchical Domain based Network: http://www.ieee802.org/1/files/public/docs2018/60802-harima-industrial-use-case-0518-v04.pdf

[7] Process Automation System Quantities: http://www.ieee802.org/1/files/public/docs2018/60802-sato-pa-system-quantities-0718-v01.pdf

[8] TSN Interdomain Communications: http://www.ieee802.org/1/files/public/docs2018/60802-Hantel-TSN-Interdomain-Communications-0718.pdf

[9] Cycle Timing Models: http://www.ieee802.org/1/files/public/docs2018/60802-enzinger-cycle-timing-models-0718-v04.pdf

[10] Isochronous Drive Synchronization: http://www.ieee802.org/1/files/public/docs2018/60802-enzinger-use-case-isochronous-drive-synchronization-0718-v01.pdf

[11] Machine Internal and Machine to Cell Controller (M2C) Embedded Communication: http://www.ieee802.org/1/files/public/docs2018/60802-essler-additional-use-case-0718-v01.pdf

[12] Coexistence & Convergence in TSN-based Industrial Automation Networks: http://www.ieee802.org/1/files/public/docs2018/60802-stanica-convergence-coexistence-0718-v03.pptx

[13] Flexible Manufacturing System (FMS) for Small Batch Customized Production: http://www.ieee802.org/1/files/public/docs2018/60802-Bai-small-batch-customized-production-0718-v01.pdf

[14] Multi-traffic transmission in industrial backbone network: http://www.ieee802.org/1/files/public/docs2018/60802-chen-multi-traffic-transmission-on-backbone-0918.pdf