Use Cases IEC/IEEE 60802 V0.7

Contributor group

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

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

Enzinger, Thomas <thomas.enzinger@inchstone.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>

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

Abstract

This document describes use cases for industrial automation, which have to be covered by the joint IEC/IEEE TSN-IA Profile for Industrial Automation.

Log

V0.1-V0.3		working drafts
V0.4	2018-03-02	Revised after circuit meeting
V0.5	2018-03-07	Revised and presented during Chicago meeting
V0.6	2018-04-12	Elaborated additional use cases from Chicago Added new use cases: - Control loops with bounded latency - Drives without common application cycle but common network cycle - Redundant networks - Vast number of connected stations

		- Digital twin Presented at ad-hoc meeting Munich
V0.61	2018-04-30	Revised after Munich ad-hoc review - Added Interoperability clause (2.1) - Reworked industrial automation traffic patterns clause (2.3.1) - Added VLAN requirements clause (2.4.11.1) - Added private machine domains sub-clause (2.5.2)
V0.7	2018-06-09	Comment resolution Interim Pittsburgh May 2018

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 to be 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 to be 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 Ethernet-based devices are able to exchange data over a common infrastructure, within defined QoS parameters
Device	End station, bridged end station, bridge
DCS	Distributed Control System
TSN domain	a quantity of commonly managed industrial automation devices; 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
Network cycle	transfer time including safety margin, and application time including safety margin (see Figure 8); values are specific to a TSN domain and specifies 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";

1.2 IEEE802 terms

Priority regeneration	See IEEE 802.1Q-2014 clause 6.9.4 Regenerating priority
Ingress rate limiting	See IEEE 802.1Q-2014 clause 8.6.5 Flow classification and metering

2 TSN in Industrial Automation

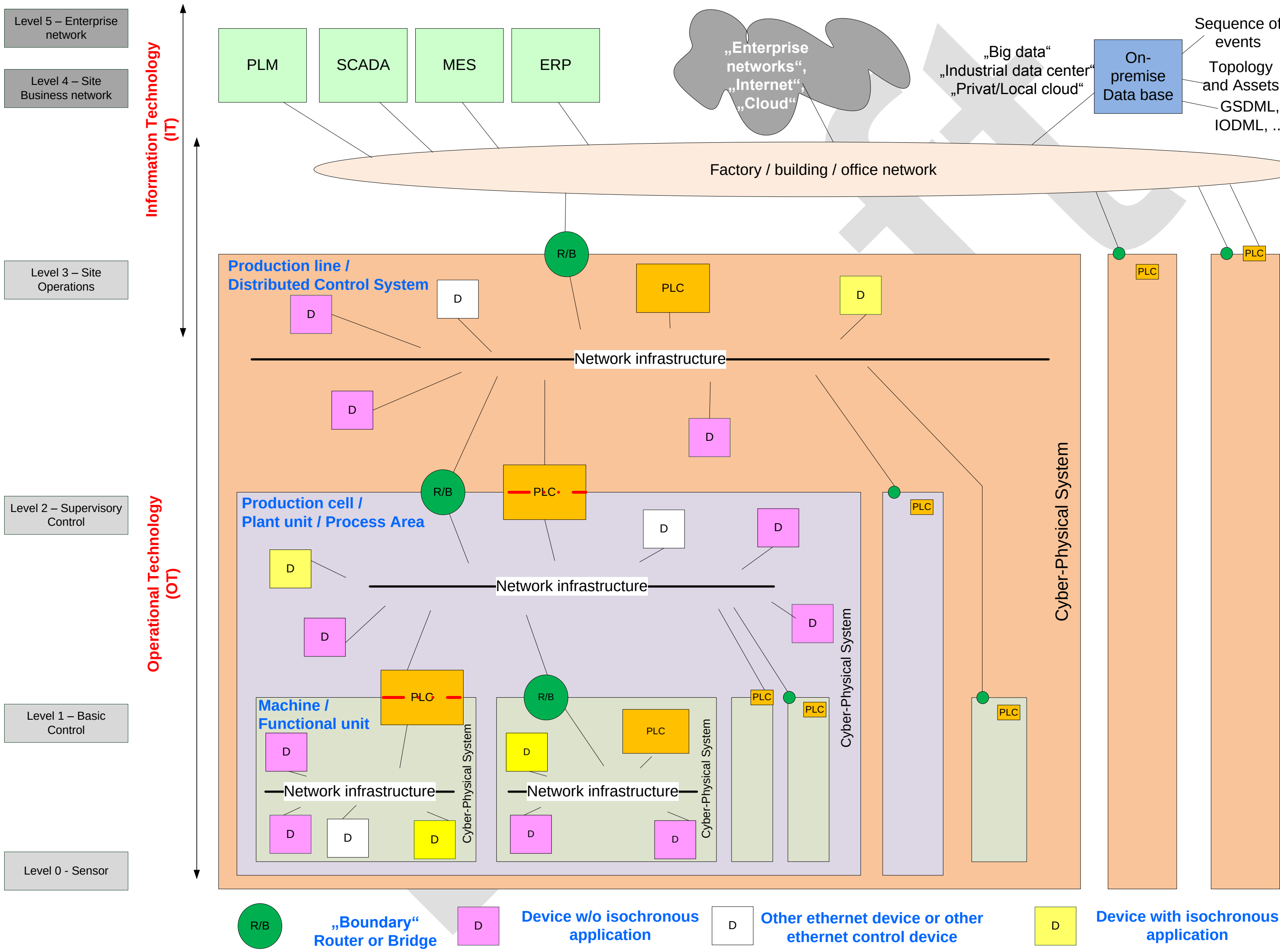

Figure 1 – Hierarchical structure of industrial automation

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. Ethernet provides the mechanisms (e.g. TSN features) for connectivity to time critical industrial applications on converged networks in operational technology control levels.

Ethernet 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 Ethernet 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.

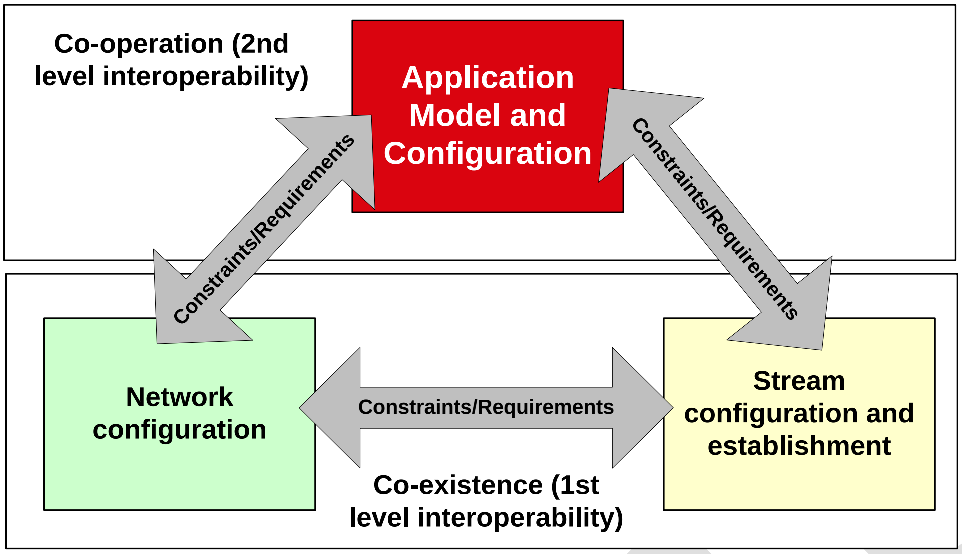

Figure 2 – Principle of interoperation

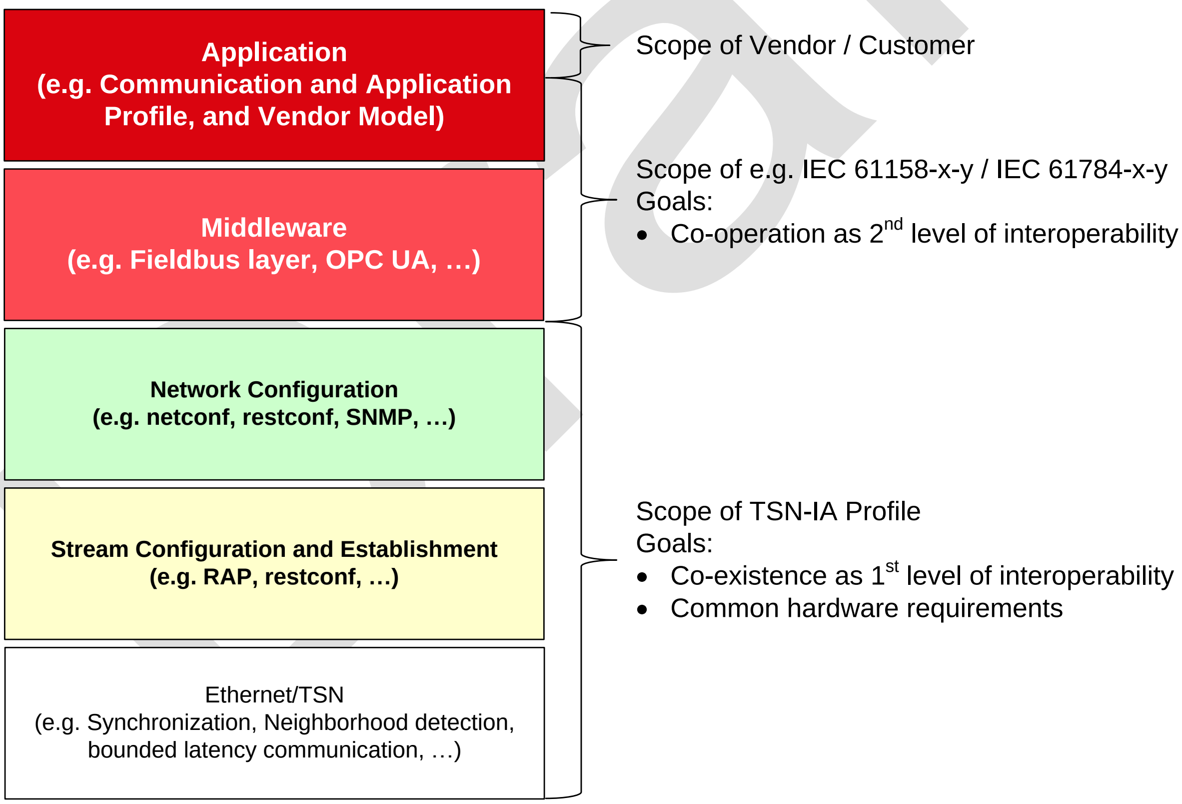

Figure 3 – Scope of work

2.2 TSN Domain

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

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.

Connections between TSN domains are described in 2.6.1.

Figure 4 shows an example TSN domain of multiple isochronous cyclic real-time domains, which overlap a common cyclic real-time domain.

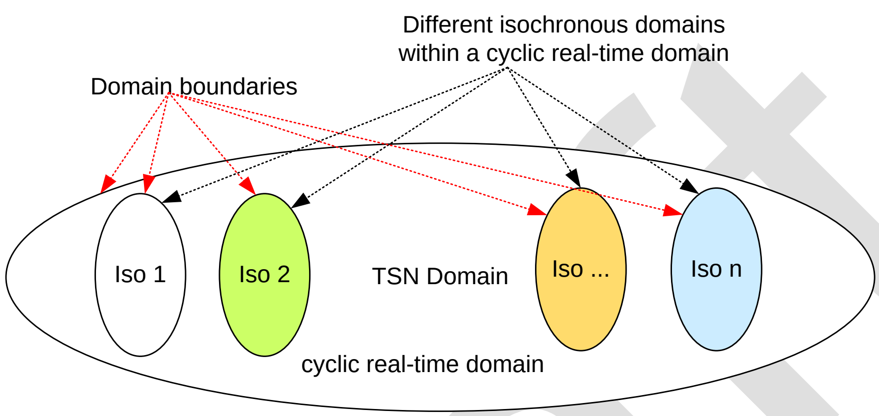

Figure 4 – TSN Domain

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.

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.

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 5 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.

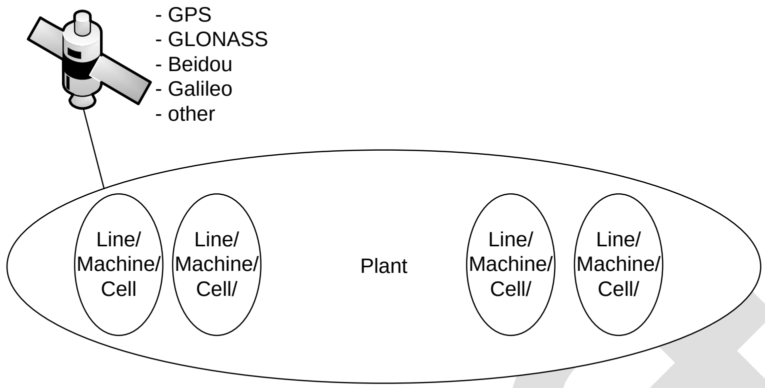

Figure 5 – plant wide time synchronization

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 6 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, an all-time active station must be used as Working Clock source, also known as Grandmaster.

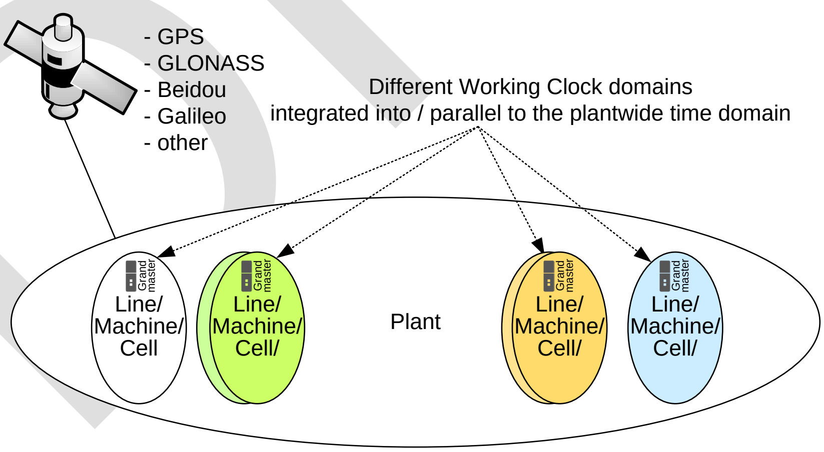

Figure 6 – line/cell/machine wide working clock synchronization overlapping with a universal time domain

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

2.3.4 Use case 01: Sequence of events

Sequence of events (SOE) is a mechanism to record timestamped events from all over a plant in a common database (on-premise database in Figure 1).
Application defined events are e.g. changes of digital input signal values. Additional data may be provided together with the events, e.g. universal time sync state and grandmaster, working clock domain and value …

SOE enables root-cause analysis of disruptions after multiple events have occurred. Therefore SOE can be used as diagnostics mechanism to minimize plant downtime.

Plant-wide precisely synchronized time (see Figure 5) is a precondition for effective SOE application.

SOE support may even be legally demanded e.g. for power generation applications.

Requirements:

- Plant wide high precision Universal Time synchronization;
- Maximum deviation to the grandmaster time in the range from 1 µs to 100 µs;
- Optional support of redundant sync masters and domains;
- Non-zero failover time in case of redundant universal time domains;

Useful 802.1 mechanisms:

- IEEE 802.1AS-Rev

2.4 Industrial automation mode of operation

2.4.1 Industrial automation traffic types

2.4.1.1 General

Industrial automation applications concurrently make use of different traffic schemes/patterns for different functionalities, e.g. parameterization, control, alarming. The various traffic patterns have different characteristics and thus impose different requirements on a TSN network.
Table 1 subsumes the industrial automation relevant traffic patterns to traffic types with their associated properties (see also: http://www.ieee802.org/1/files/public/docs2018/new-Bruckner-LNI-traffic-patterns-for-TSN-0118.pdf).

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 Table 3 and 2.4.2
cyclic real-time	P	deadline/ bounded latency (e.g. n-times network cycle)/ bandwidth	bounded	up to seamless[1)]	see Table 7 and 2.4.3
network control	S	Priority	-	up to seamless[1)] as required	see 2.3 and 2.5.1
audio/video	P	bounded latency/ bandwidth	bounded	up to regular[2)]	-
brownfield	P	bounded latency/ bandwidth	-	up to regular[2)]	see 2.5.6
alarms/ events	S	bounded latency/ bandwidth	-	up to regular[2)]	see 2.3.4
configuration/ diagnostics	S	Bandwidth	-	up to regular[2)]	see 2.8.1
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 *Use case 02: Control Loops with guaranteed low latency*

Cyclic:

→ see *Use case 03: Control Loops with bounded latency*

Network control:
→ see *Use case 07: Redundant networks*

Audio/video:

→ NOTE: Non-AVB – need to follow TSN-IA profile rules!

- Machine vision applications: counting, sorting, quality control, video surveillance, augmented reality, motion guidance, …
- based on TSN features and stream establishment, and not on AVB…

Brownfield:

→ see *Use case 12: New machine with brownfield devices*

Alarms/events:

→ see *Use case 01: Sequence of events*

Configuration/diagnostics:

→ see *Use case 28: Network monitoring and diagnostics*

Internal:

→ see *Use case 18: 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 Use case 02: Control Loops with guaranteed low latency and Use case 03: Control Loops with bounded latency.

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, • *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.
Data transmission synchronized to network cycle	Indicates whether the data transmission of sender stations is synchronized to the network cycle. Available property options are: *yes* or *no.*

Property	Description
Application synchronized to working clock	Indicates whether the applications, which make use of this traffic pattern, are synchronized to the working clock. 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 Use case 02: Control Loops with guaranteed low latency

2.4.2.1 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 2.4.3) network transfer quality.

To achieve the needed quality for Control loops the roundtrip delay (sometimes called makespan, too) of the exchanged data is essential.
Figure 7 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.

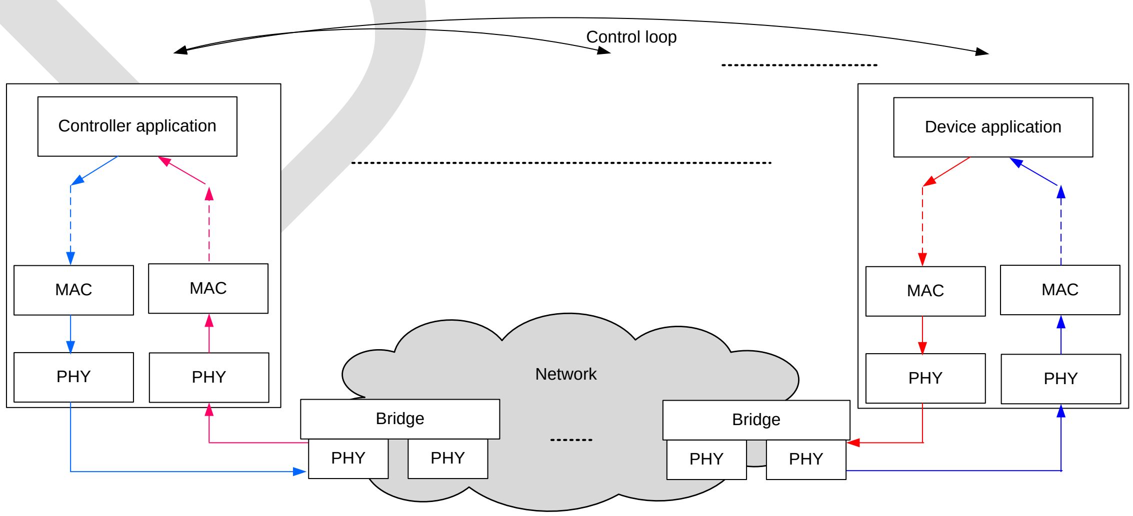

Figure 7 – Principle data flow of control loop

Control loops with guaranteed low latency implement an isochronous traffic pattern based on a network cycle, which consists of an IO data Transfer time and an Application time wherein the control loop function is executed. Figure 8 shows the principle how network cycle, transfer time and application time interact in this use case. The control loop function starts for controllers and devices after the transfer time when all necessary buffers are available. A single execution of a control loop function ends before the next transfer time period starts. Thus, all frames must be received by the addressed application within the transfer time. An optimized local transmit order at sender stations is required to achieve minimal transfer time periods.

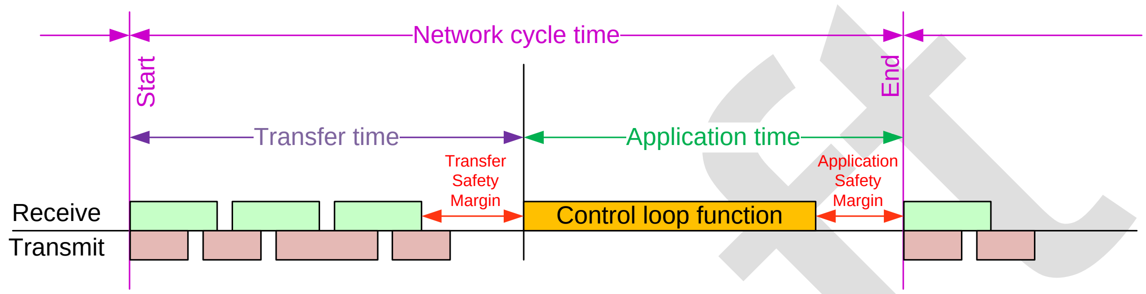

Figure 8 – network cycle and control loop (principle)

Figure 9 shows how this principle is used for multiple concurrent applications with even extended computing time requirements longer than a single application time within the network cycle time. When reduction ratio >1 is applied (see 2.4.4), the control loop function can be expanded over multiple network cycles (Control loop 2 with reduction ratio 2 and Control loop 3 with reduction ratio 16 in Figure 9).

Maximum available computation time for a Control loop with reduction ratio X:

X * network cycle time – Transfer time – Application safety margin

Transfer of isochronous cyclic real-time, cyclic real-time and non-real-time data is processed in parallel to the various control loop functions - preserving the deadline requirement of the control loops.

A background task can additionally run, when free compute time is available.

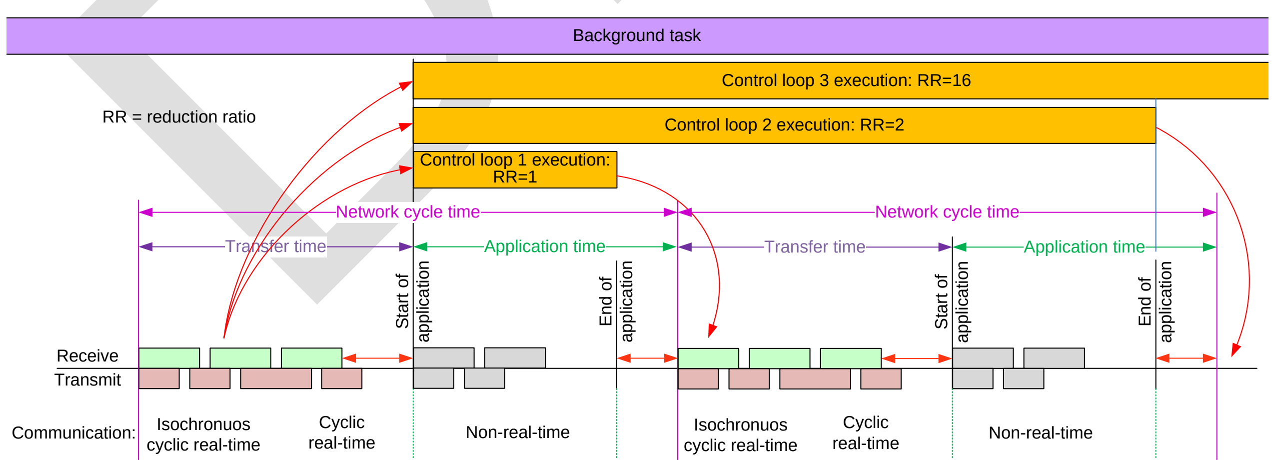

Figure 9 – Multiple concurrent control loops

Network cycle: transfer time (including safety margin) and application time (including safety margin)

Transfer time: period of time, wherein all necessary frames are exchanged between stations (controller, devices); the minimum transfer time is determined by the e2e latencies of the necessary frames; the e2e latency depends on: PHY-delays, MAC-delays, bridge-delays and send ordering. The transfer time is a fraction of the network cycle time.

For a given target transfer time the number of possible bridges on the path is restricted due to PHY-, MAC- and bridge-delay contributions.

2.4.2.2 Isochronous cyclic operation model for guaranteed low latency

Figure 10 shows the isochronous cyclic operation model for guaranteed low latency.

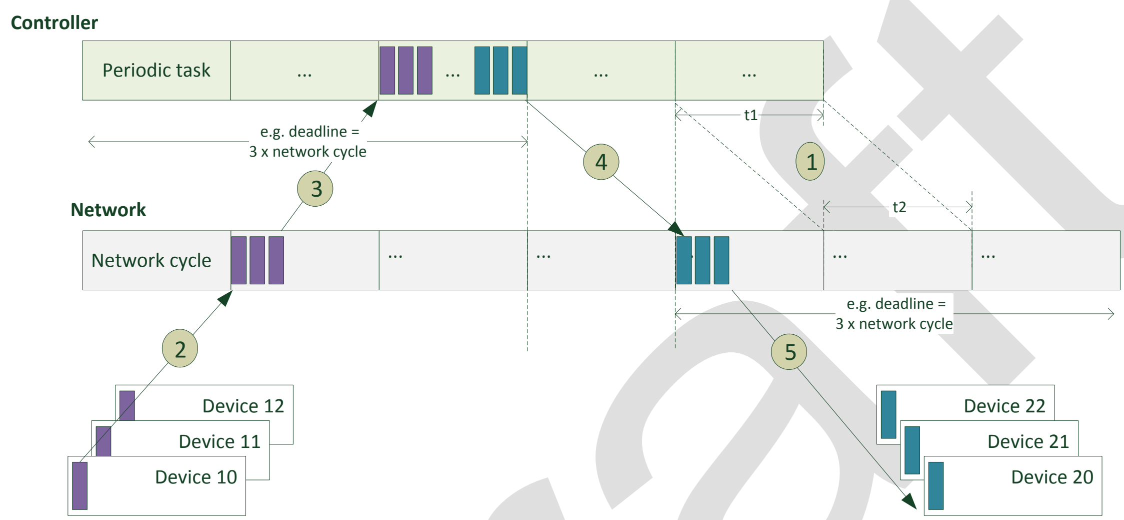

Figure 10 – isochronous cyclic operation model

Isochronous cyclic operation characteristics:

Multiple applications (periodic tasks) with different application periods are supported. Applications are synchronized to working clock:

- Devices: √
- Controller: √

Multiple application update times based on different reduction ratios are supported. Data transmission is synchronized to network cycle (WorkingClock):

- Devices: √
- Controller: √

The single steps of the isochronous cyclic operation model are:

1	Controller periodic tasks are synchronized to the working clock. Example: Periodic task_01 period (t1) == network cycle period (t2). Periodic task_02 period == 8 * network cycle period (t2). Periodic task_03 period == 32 * network cycle period (t2).
2	Device data transmission is synchronized to network cycle (Working Clock).
3	Device input data must reach controller within an application defined deadline. Controller application may check the timeliness (by means of additional data in the payload, e.g. LifeSign model).

	Controller application operates on local process image data. Local process image decouples communication protocol from application. Additional: Device input data must reach controller within a communication monitoring defined deadline (communication protocol). Communication disturbances are recognized and signaled asynchronously by communication protocol to application.
4	Controller output data transmission is synchronized to network cycle (Working Clock).
5	Controller output data must reach device within an application defined deadline. Device application may check the timeliness (by means of additional data in the payload, e.g. PROFINET Isochronous Mode SignOfLife model – see [3]). Device application operates on local process image data. Local process image decouples communication protocol from application. Additional: Controller out data must reach device within a communication monitoring defined deadline (communication protocol). Communication disturbances are recognized and signaled asynchronously by communication protocol to application.

High control loop quality is achieved by:

- Short network cycle times to minimize reaction time (dead time),
- equidistant network cycle times based on a synchronized working clock to ensure a defined reaction time,
- device signal processing and transfer coupled to synchronized working clock, and
- device and controller application (function) coupled to synchronized working clock.

isochronous mode: coupling of device and controller application (function) to the synchronized working clock

isochronous cyclic realtime: transfer time less than 20%/50% of network cycle and applications are coupled to the working clock.

Table 3 – isochronous traffic pattern properties

Characteristics		Notes
Data transmission scheme	periodic	
Data transmission constraints	deadline	End-to-end one-way latency[1] less than 20%/50% of network cycle
Data period	1µs .. 1ms	20% of network cycle at link speeds > 100 Mbit/s
	125µs .. 2ms	50% of network cycle at link speeds <= 100 Mbit/s
Data transmission synchronized to network cycle	Yes	
Application synchronized to working clock	Yes	
Acceptable jitter	n.a.	Deadline shall be kept

[1] The end-to-end one-way latency is measured from the arrival of the last bit at the ingress edge port of the bridged network to the transmission of the last bit by the egress edge port of the bridged network (see, e.g., Annex L.3 in IEEE Std 802.1Q-2014).

Characteristics		Notes
Acceptable frame loss	0..n frames	Media redundancy requirements according to the required tolerance; e.g. seamless redundancy for value 0
Payload	1 .. IEEE Std 802.3 maximum data payload size (i.e. 1500 bytes)	Data size negotiated during connection establishment

isochronous domain: All stations, which share a common

- working clock,
- network cycle, and
- traffic model (traffic class definition).

Requirements on network cycle times:

- 1 µs to 1 ms at link speed 1 Gbit/s (or higher)
- 125 µs to 4 ms at link speed 100 Mbit/s (or lower, e.g. 10 Mbit/s)

To make short control loop times feasible PHY, MAC and bridge delays shall meet upper limits:

- PHY delays shall meet the upper limits of Table 4.
- MAC delays shall meet the upper limits of Table 5.
- Bridge delays shall be independent from the frame size and meet the upper limits of Table 6.

Figure 11 shows the definition of PHY delay, MAC delay and Bridge delay reference points.

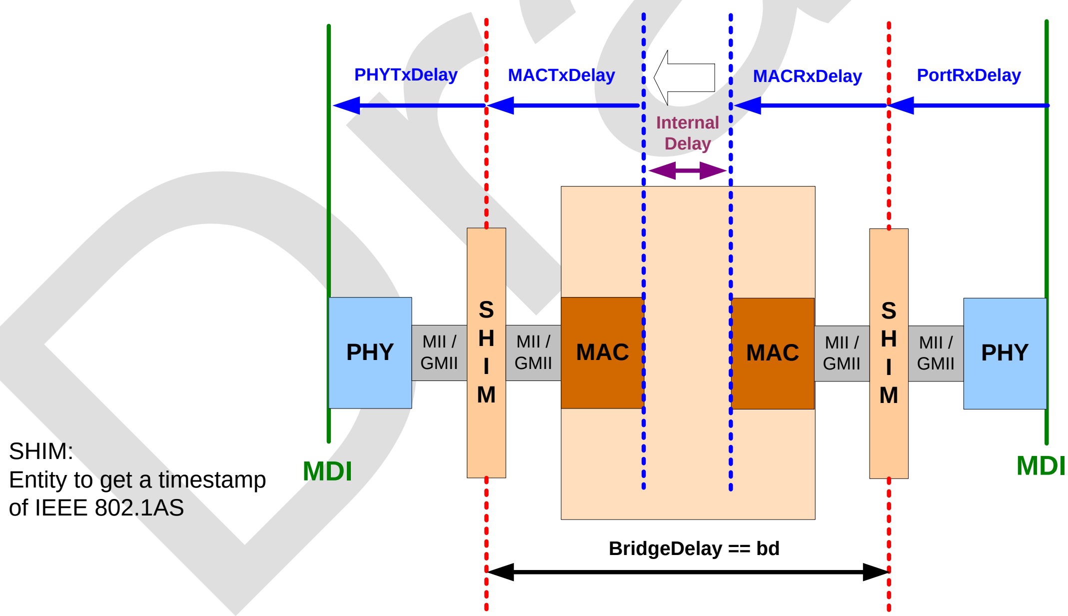

Figure 11 – delay measurement reference points

Table 4 – Expected PHY delays

Device	RX delay [c]	TX delay [c]	Jitter
10 Mbit/s	<< 1 µs	<< 1 µs	< 4 ns
100 Mbit/s MII PHY	210 ns (Max. 340 ns) [a]	90 ns (Max. 140 ns) [a]	< 4 ns
100 Mbit/s RGMII PHY	210 ns [b]	90 ns [b]	< 4 ns
1 Gbit/s RGMII PHY	<< 500 ns [b]	<< 500 ns [b]	< 4 ns
2,5 Gbit/s RGMII PHY	<< 500 ns [b]	<< 500 ns [b]	< 4 ns
5 Gbit/s RGMII PHY	<< 500 ns [b]	<< 500 ns [b]	< 4 ns
10 Gbit/s	Tdb	tbd	tbd
25 Gbit/s – 1 Tbit/s	n.a.	n.a.	n.a.

[a] According IEEE 802.3 for 100 Mbit/s full duplex with exposed MII.

[b] Values from 100 Mbit/s PHYs (or better) are needed to allow substitution even for Gigabit or higher.

[c] Lower values mean more performance for linear topology.

Table 5 – Expected MAC delays

Link speed	Maximum RX delay	Maximum TX delay
10 Mbit/s	<< 1 µs	<< 1 µs
100 Mbit/s	<< 1 µs	<< 1 µs
1 Gbit/s	<< 1 µs	<< 1 µs
2,5 Gbit/s	<< 1 µs	<< 1 µs
5 Gbit/s	<< 1 µs	<< 1 µs
10 Gbit/s	<< 1 µs	<< 1 µs
25 Gbit/s – 1 Tbit/s	n.a.	n.a.

Table 6 – Expected Ethernet Bridge delays

Link speed	Value	Comment
10 Mbit/s	< 30 µs	No usage of bridging expected
100 Mbit/s	< 3 µs	Bridge delay measure from MII to MII
1 Gbit/s	< 1 µs	Bridge delay measure from RGMII to RGMII
2,5 Gbit/s	< 1 µs	Bridge delay measure from XGMII to XGMII
5 Gbit/s	< 1 µs	Bridge delay measure from XGMII to XGMII
10 Gbit/s	< 1 µs	Bridge delay measure from XGMII to XGMII
25 Gbit/s – 1 Tbit/s:	n.a.	No covered by this specification

<u>Useful 802.1 mechanisms:</u>

- …

<u>Example</u>:

A representative example of a "Control loop with guaranteed low latency" use case is given in clause 2.5.11.4 *"Fast" process applications*.

2.4.3 Use case 03: Control Loops with bounded latency

2.4.3.1 Cyclic operation model

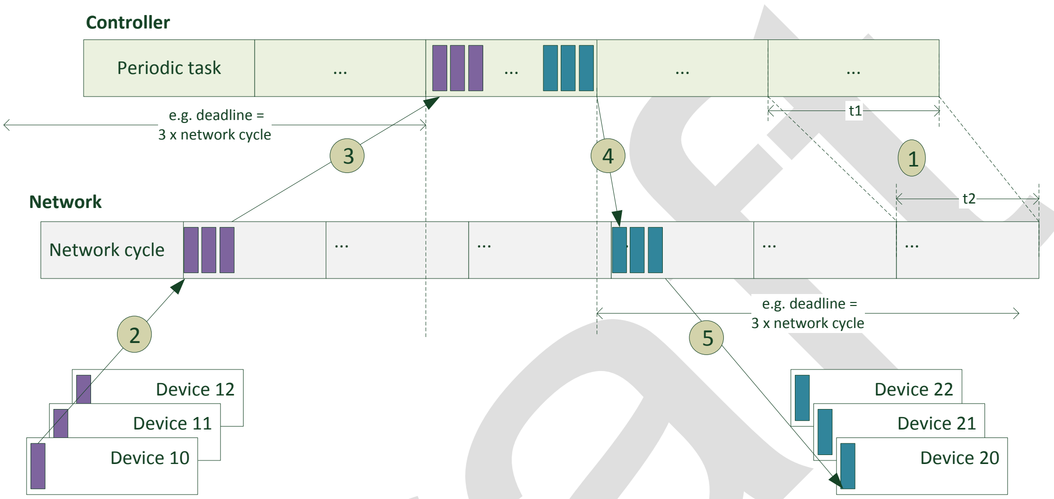

Figure 12 – cyclic operation model

Cyclic operation characteristics:

Multiple applications with different application periods are supported.
Applications don't need to be synchronized to working clock, but may be synchronized:

- Devices: √
- Controller: √

Multiple update times based on different reduction ratios are supported.
Data transmission is synchronized to network cycle (WorkingClock):

- Devices: √
- Controller: √

The single steps of the cyclic operation model are:

1	Controller periodic tasks don't need to be synchronized to working clock, but may be synchronized. Periodic task period (t1) != network cycle period (t2).
2	Data transmission is synchronized to network cycle (Working Clock)
3	Device input data must reach controller within a communication monitoring defined deadline (communication protocol). Controller application assumes a kept update interval but doesn't know whether it is

	kept or not. Communication disturbances are recognized and signaled asynchronously by communication protocol to application. Controller application operates on local process image data. Local process image decouples communication protocol from application.
4	Controller output data transmission is synchronized to network cycle (Working Clock).
5	Controller output data must reach device within a communication monitoring defined deadline (communication protocol). Device application assumes an kept update interval but doesn't know whether it is kept or not. Communication disturbances are recognized and signaled asynchronously by communication protocol to application. Device application operates on local process image data. Local process image decouples communication protocol from application.

2.4.3.2 Control Loop

Control loops with bounded latency implement a cyclic traffic pattern. More relaxed control reaction time requirements (e.g. 10 ms - 10 s) allow free running applications instead of isochronous applications. In consequence transfer time requirements are more relaxed as well. The transfer time may be longer than the network cycle in this use case.

For a given target transfer time the number of possible bridges on a communication path is restricted due to PHY-, MAC- and bridge-delay contributions, but can be much higher compared to Use case 02: Control Loops with guaranteed low latency

<u>Cyclic real-time:</u> transfer time may be longer than network cycle and applications are decoupled from the working clock.

Table 7 – cyclic traffic pattern properties

Characteristics		Notes
Data transmission scheme	periodic	
Data transmission constraints	deadline	End-to-end one-way latency[2] less than X * network cycle (X | 1 .. n)
Data period	X * network cycle (X | 1 .. n)	
Data transmission synchronized to network cycle	Yes	
Application synchronized to working clock	No	
Acceptable jitter	n.a.	Deadline shall be kept
Acceptable frame loss	0..n frames	Media redundancy requirements according to the required tolerance; e.g. seamless redundancy for value 0
Payload	1 .. IEEE Std 802.3 maximum data payload size (i.e. 1500	Data size negotiated during connection establishment

[2] The end-to-end one-way latency is measured from the arrival of the last bit at the ingress edge port of the bridged network to the transmission of the last bit by the egress edge port of the bridged network (see, e.g., Annex L.3 in IEEE Std 802.1Q-2014).

Characteristics	Notes
bytes)	

<u>Cyclic real-time domain:</u> All stations, which share a common

- traffic model (traffic class definition).

<u>Requirements</u>:

Stations shall be able to implement Use case 02: Control Loops with guaranteed low latency and Use case 03: Control Loops with bounded latency concurrently.

Transmission paths shall be able to handle different

- working clocks, and
- network cycles.

<u>Useful 802.1 mechanisms:</u>

- …

2.4.4 Use case 04: Reduction ratio of network cycle

Application needs may limit the in principle flexible network cycle time to a defined granularity. E.g. in case of network cycle granularity 31,25 µs the possible network cycles are:

>= 1Gbit/s: 31,25 µs * $2^{\wedge n}$ | n=0 .. 5
< 1Gbit/s: 31,25 µs * $2^{\wedge n}$ | n=2 .. 7

Application cycle times are the result of the used network cycle times together with reduction ratios:

- 31,25 µs to 512 ms

<u>Reduction ratio</u>: The value of “reduction ratio” defines the number of network cycles between two consecutive transmits.

<u>Phase</u>: The value of “phase” in conjunction with “reduction ratio” defines the starting network cycle for the consecutive transmits.

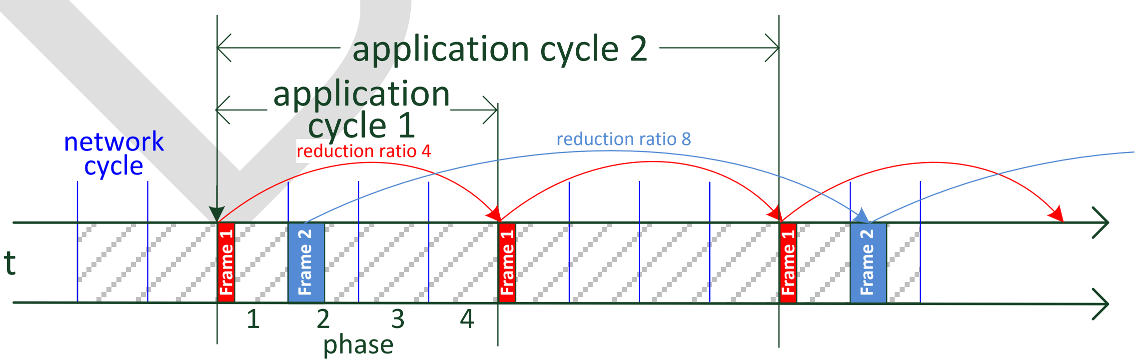

Figure 13 – network cycle and application cycle

Examples: see Use case 06: Drives without common application cycle but common network cycle.

<u>Requirements</u>:

…

Useful 802.1 mechanisms:

- …

2.4.5 Use case 05: Drives without common application cycle

2.4.5.1 Background information

The cycle time requirements of different vendors may be based on their technology, which cannot be changed with reasonable effort. These requirements may be based on hardware dependencies, independent of the capabilities of the communication part of the device.

Figure 14 shows an example, where Vendor A needs to communicate with 31,25 µs between its devices (A1 with A2), and Vendor B needs to communicate with 50 µs (between B1 and B2). The communication with the controller which has to coordinate both of them must be a multiple of their local cycles. A1 needs to exchange data every 125µs with the Controller, B1 needs to exchange data every 200µs with the Controller.

Servo drives from different vendors (Vendor A and Vendor B) are working on the same network. For specific reasons the vendors are limited in the choice of the period for their control loop.

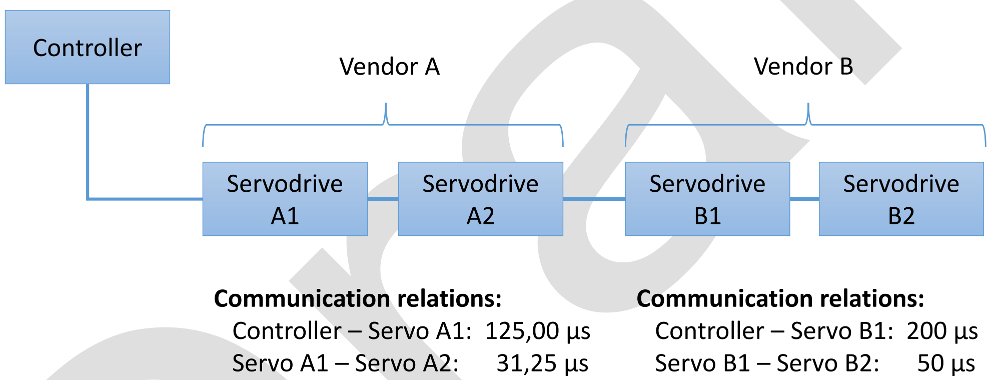

Figure 14 – network with different application cycles

The following Communication Relations are expected to be possible:

Servodrive A1 ←→ Servodrive A2: 31,25 µs
Servodrive B1 ←→ Servodrive B2: 50 µs

Controller ←→ Servodrive A1: 125 µs
Controller ←→ Servodrive B1: 200 µs

Servodrive A1 ←→Servodrive B1: 1 ms

Requirements:

- Isochronous data exchange
- Different cycles for data exchange, which are not multiples of each other (cycles are not multiple of a common base, but fractions of a common base, here for instance 1 ms)

Useful 802.1Q mechanisms:

- Whatever helps
- …

2.4.5.2 Controller communication

The Usecase concentrates on the communication between the devices A1 and B1, and the Controller as shown in Figure 15. Nevertheless the communication between A1/A2 and B1/B2 has to be solved as well.

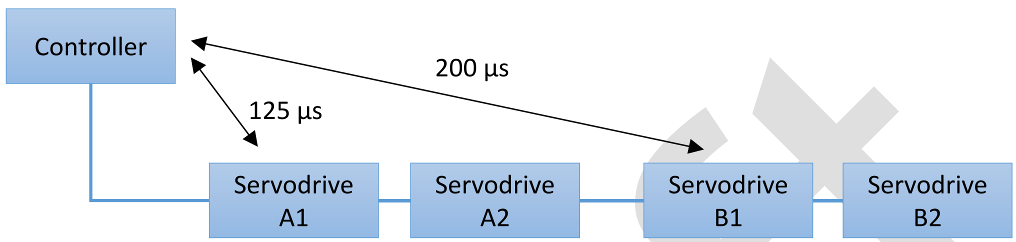

Figure 15 – Multivendor Motion – Controller communication

2.4.5.3 Timing Requirements

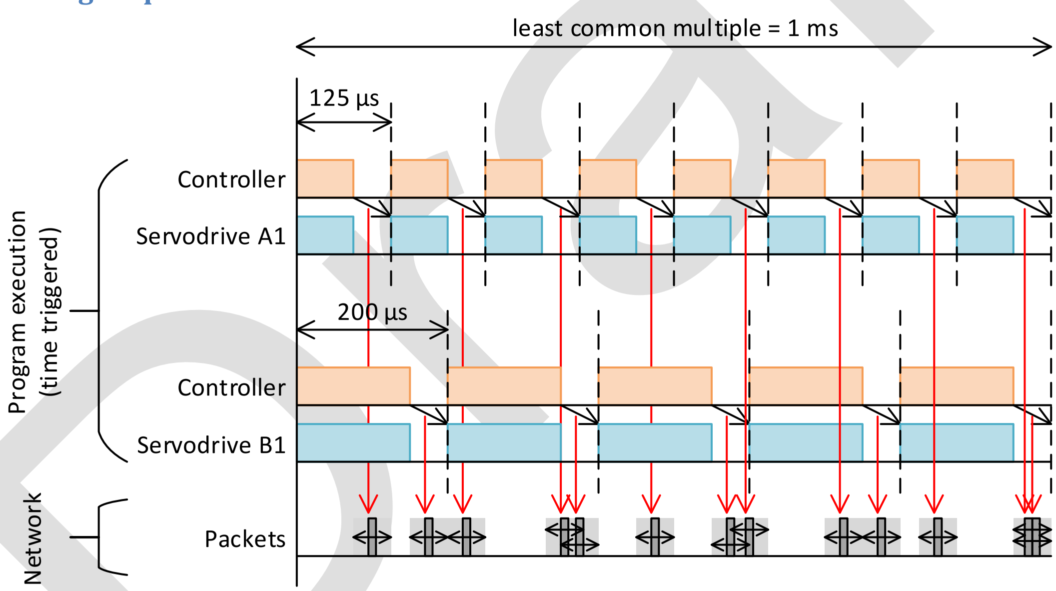

Figure 16 – Multivendor Motion – Timing Requirements

The Controller runs 2 parallel programs in multitasking, one program with 125 µs cycle, and another with 200 µs cycle. Alternatively there might also be 2 independent controllers on the same network, one of vendor A and one of vendor B.

After every program execution, data needs to be exchanged between Controller and Servodrive. The time window for this exchange is application specific.

The actual data exchange on the wire can happen at any time in this window, the devices are not dependent on any exact transmission or reception timing, as long as the packet is in the scheduled window.

2.4.6 Use case 06: Drives without common application cycle but common network cycle

The concept of multiple different application cycles which are based on a common network cycle is described in Use case 04: Reduction ratio of network cycle.

Examples with different application cycle times but common network cycle time 31,25 µs:

- 31,25 µs, i.e. reduction ratio 1 for current control loop,
- 250 µs, i.e. reduction ratio 4 for position control loop,
- 1 ms, i.e. reduction ratio 16 for motor speed control loop,
- 16 ms, i.e. reduction ratio 256 for remote IO.

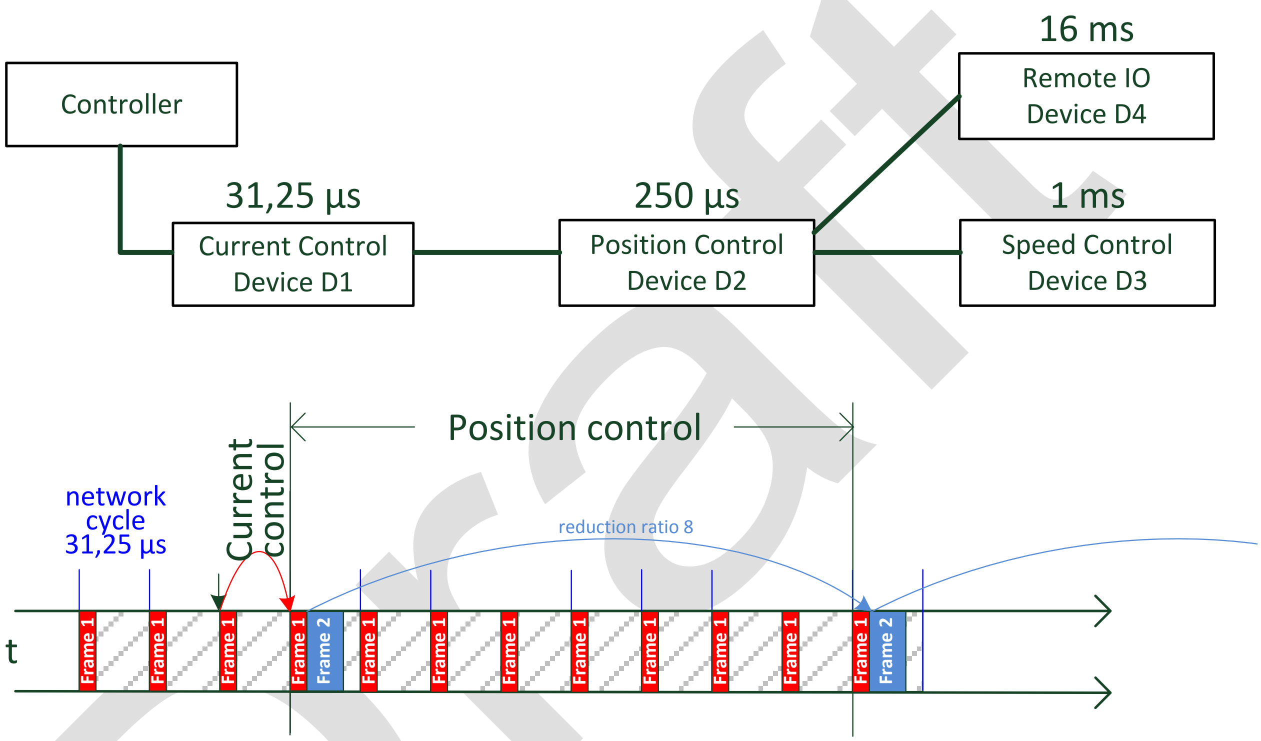

Figure 17 – different application cycles but common network cycle

2.5 Industrial automation networks

2.5.1 Use case 07: Redundant networks

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

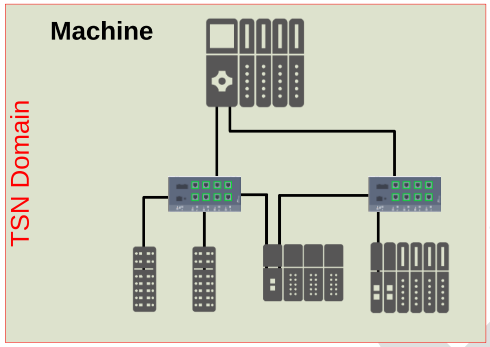

Figure 18 – ring topology

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

To even improve availability of the connection from the production cell into the machines this link can be arranged redundantly as well (machine 1 in Figure 19):

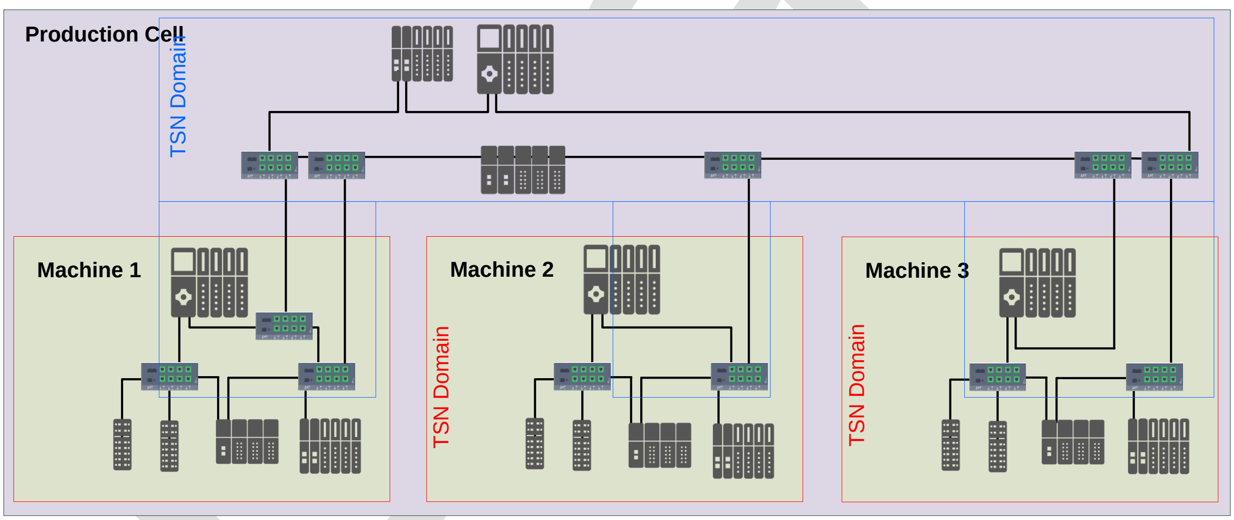

Figure 19 – connection of rings

<u>Requirement</u>:

Support redundant topologies with rings.

<u>Useful 802.1 mechanisms:</u>

- …

2.5.2 Use case 08: High Availability

High availability systems are composed of:

- Redundant networks, and
- Redundant stations.

E.g. tunnel control:

Tunnels need to be controlled by systems supporting high availability because airflow and fire protection are crucial for the protection of people's lives. In this case PLC, remote IO and network are installed to support availability in case of failure.

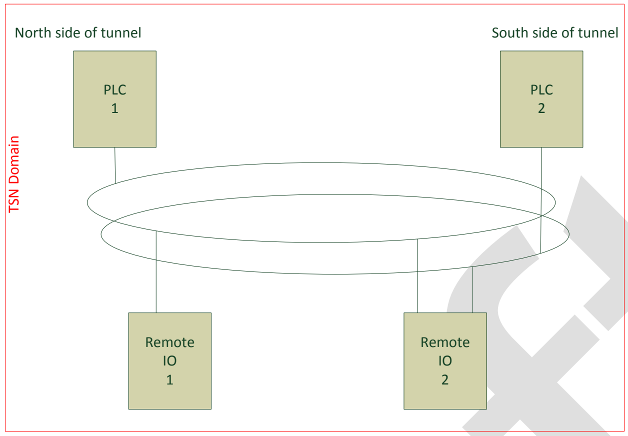

Figure 20 – example topology for tunnel control

Requirement:
Failure shall not create process disturbance – e.g. keep air flow active / fire control active.
The number of concurrent active failures without process disturbance depends on the application requirements and shall not be restricted by TSN profile definitions.
Parameter, program, topology changes need to be supported without disturbance.

Useful 802.1Q mechanisms:

- Redundancy for PLCs, Remote IOs and paths through the network
- …

Further high availability control applications:

- Ship control
- Power generation
- Power distribution
- …

2.5.3 Use case 09: 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 5G.

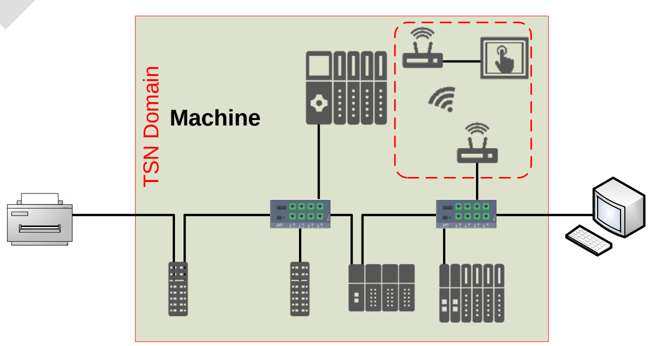

Figure 21 – HMI wireless connected using cyclic real-time

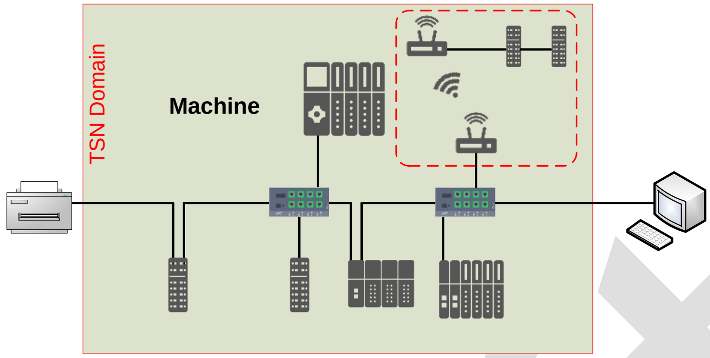

Figure 22 – Remote IO wireless connected using cyclic real-time

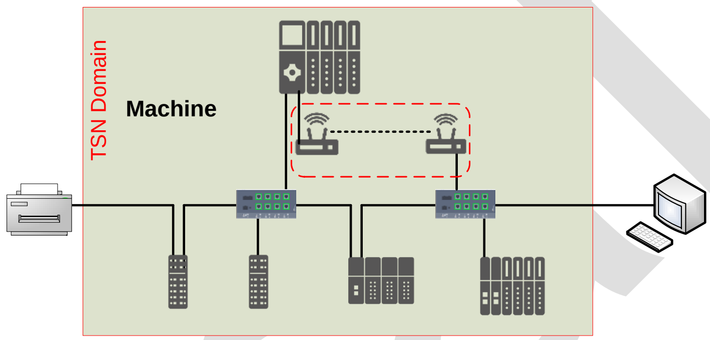

Figure 23 – Ring segment wireless connected for media redundancy

Requirement:

Support of wireless for

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

Useful 802.11 mechanisms:

- Synchronization support
- Extensions from .11ax
- …

Useful 802.15.1 mechanisms:

- …

Useful 802.1Q mechanisms:

- …

2.5.4 Use case 10: 10 Mbit/s end-stations (Ethernet sensors)

Simple and cheap sensor end-stations are directly attached via 10 Mbit/s links to the machine internal Ethernet and implement cyclic real-time communication with the PLC.

The support of additional physics like “IEEE 802.3cg APL support” is intended.

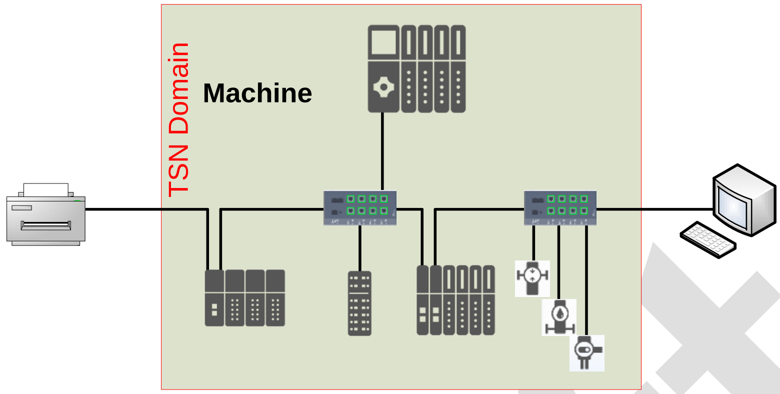

Figure 24 – Ethernet sensors

Requirement:

Support of 10 Mbit/s or higher link speed attached sensors (end-stations) together with POE and SPE (single pair Ethernet).

Useful 802.1Q mechanisms:

- …

2.5.5 Use case 11: Fieldbus gateway

Gateways are used to integrate non-Ethernet fieldbuses into TSN domains.

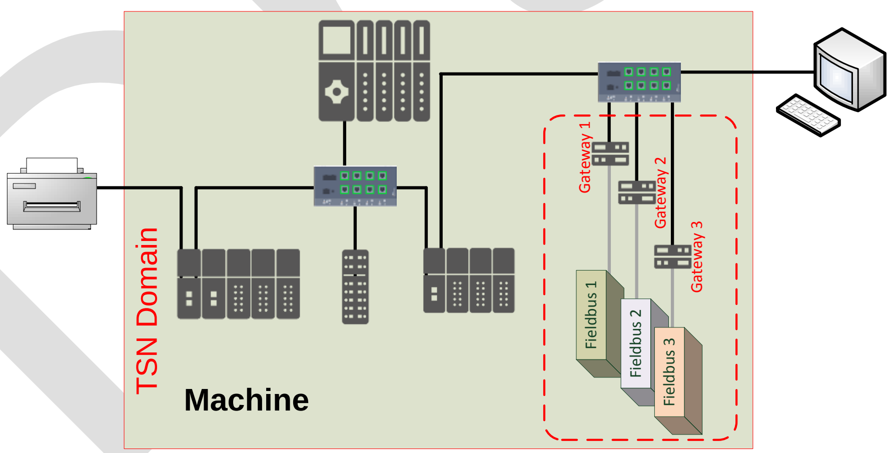

Figure 25 – fieldbus gateways

Requirement:

Support of non-Ethernet fieldbus devices via gateways either transparent or hidden.

Useful 802.1Q mechanisms:

- …

2.5.6 Use case 12: New machine with brownfield devices

Brownfield devices with real-time communication are attached to a PLC, which supports both brownfield and greenfield, within a machine. This allows faster deployment of devices supporting the TSN-IA profile into the field. Figure 26 gives an example of a machine with brownfield devices.

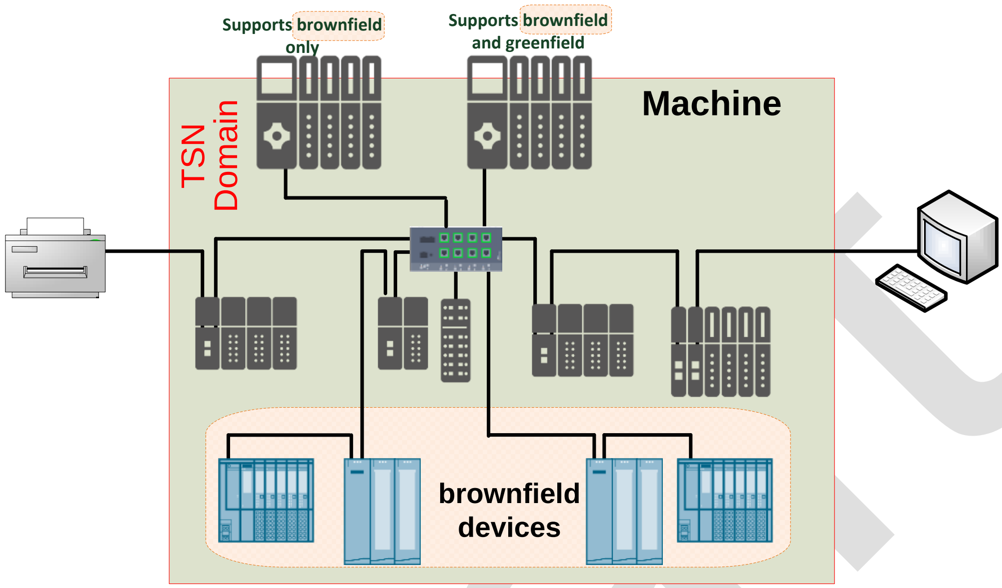

Figure 26 – new machine with brownfield devices

Requirement:
All machine internal stream traffic communication (stream traffic and non-stream traffic) is decoupled from and protected against the brownfield cyclic real-time traffic.
Brownfield cyclic real-time traffic QoS is preserved within the TSN domain.

Useful 802.1Q mechanisms:

- Priority Regeneration,
- separate "brownfield traffic queue".
- Queue-based resource allocation.

2.5.7 Use case 13: Mixed link speeds

Industrial use cases refer to link speeds, as shown in Table 8, in the range from 10 Mbit/s to 10 GBit/s for Ethernet and additional Wi-Fi, Bluetooth and 5G. Thus, the TSN domains need to handle areas with different link speeds.

Table 8 – Link speeds

Link speed	Media	Comments
100 kbit/s – 3 Mbit/s	Radio Bluetooth	These devices are connected thru a Bluetooth access point. They may be battery powered.
1 Mbit/s – 1 Gbit/s	Radio Wi-Fi	These devices are connected thru a Wi-Fi access point. They may be battery powered.
1 Mbit/s – 10 Gbit/s (theoretical/expected)	Radio 5G	These devices are connected thru a 5G access point. They may be battery powered.

Link speed	Media	Comments
10 Mbit/s	Copper or fiber	May be used for end station "only" devices connected as leafs to the domain. Dedicated to low performance and lowest energy devices for e.g. process automation. These devices may use PoE as power supply.
100 MBit/s	Copper or fiber	Historical mainly used for Remote IO and PLCs. Expected to be replaced by 1 GBit/s as common link speed.
1 GBit/s	Copper or fiber	Main used link speed for all kind of devices
2,5 GBit/s	Copper or fiber	High performance devices or backbone usage
5 GBit/s	Copper or fiber	Backbone usage, mainly for network components
10 GBit/s	Fiber	Backbone usage, mainly for network components
25 GBit/s – 1 Tbit/s	tbd	Backbone usage, mainly for network components

Mixing devices with different link speeds is a non-trivial task. Figure 27 and Figure 28 show the calculation model for the communication between an IOC and an IOD connected with different link speeds.

The available bandwidth on a communication path is determined by the path segment with the minimum link speed.

The weakest link of the path defines the usable bandwidth. If the topology guideline ensures that the connection to the end-station always is the weakest link, only these links need to be checked for the usable bandwidth.

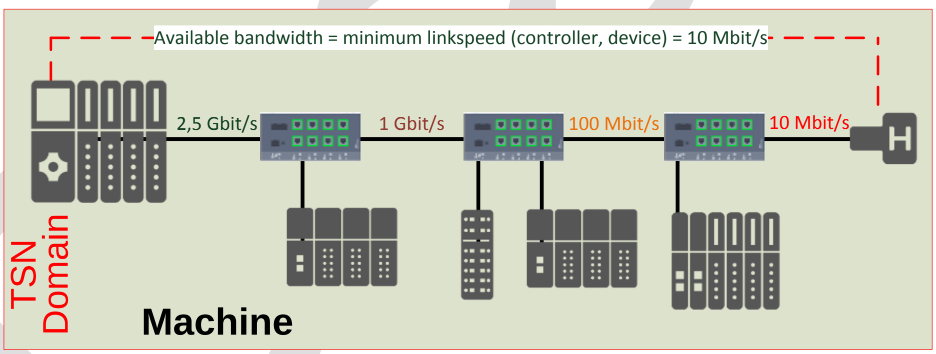

Figure 27 – mixed link speeds

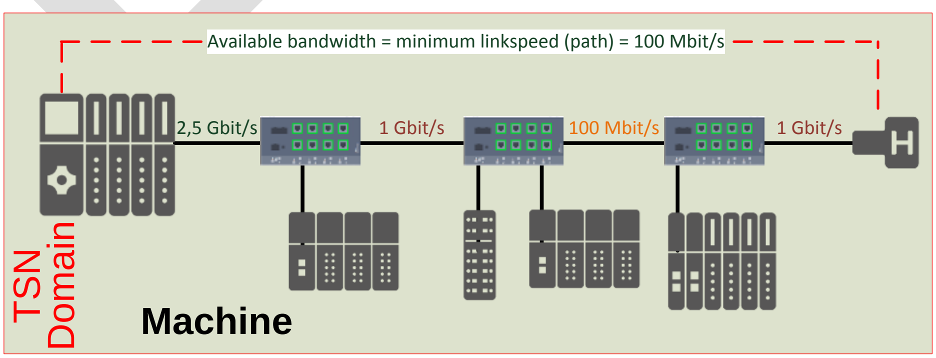

Figure 28 – mixed link speeds without topology guideline

Requirement:

Links with different link speeds as shown in Figure 27 share the same TSN-IA profile based communication system at the same time.
Links with different link speeds without topology guideline (Figure 28) may be supported.

Useful 802.1 mechanisms:

- …

2.5.8 Use case 14: Multiple isochronous domains

Figure 29 shows a machine which needs due to timing constraints (network cycle time together with required topology) two or more separated isochronous real-time domains but shares a common cyclic real-time domain.
Both isochronous domains may have their own Working Clock and network cycle. The PLCs need to share remote IOs using cyclic real-time traffic.

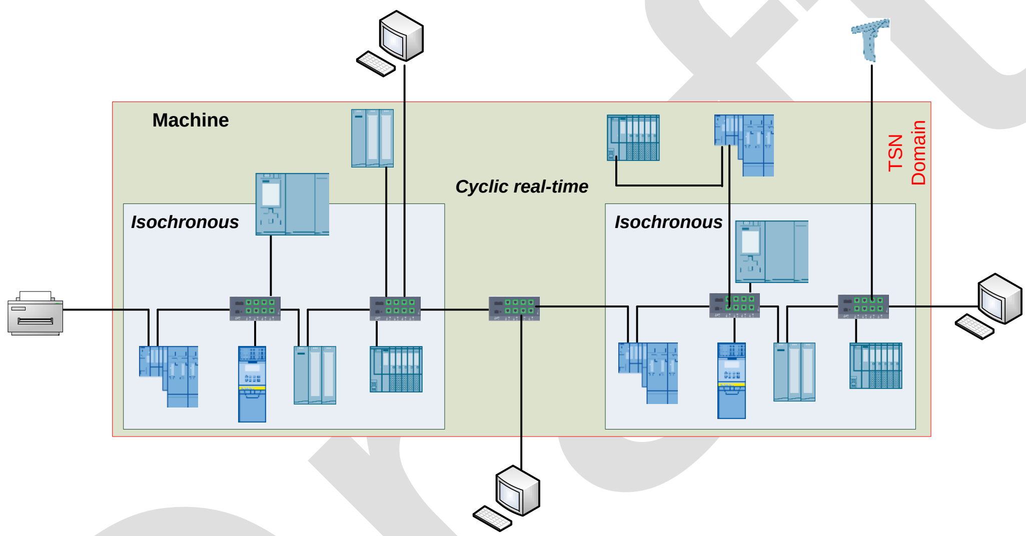

Figure 29 – multiple isochronous domains

Some kind of coupling (e.g. shared synchronization) between the isochronous domains / Working Clocks may be used (see Figure 30).
All isochronous domains may have different network cycle times, but the cyclic real-time data exchange shall still be possible for PLCs from both isochronous domains.

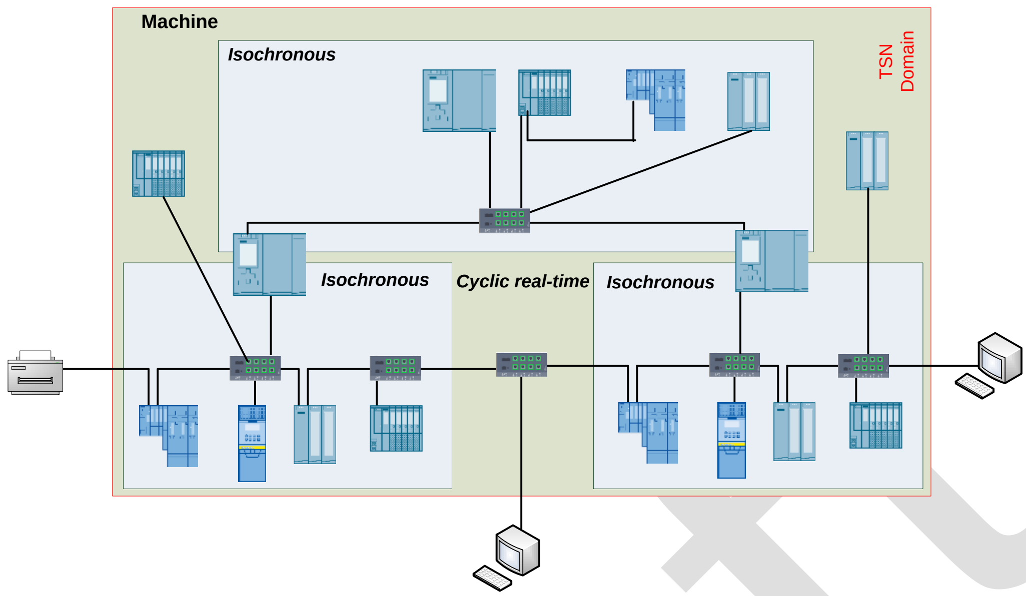

Figure 30 – multiple isochronous domains - coupled

Requirements:

All isochronous real-time domains may run independently, loosely coupled or tightly coupled. They shall be able to share a cyclic real-time domain.

Useful 802.1 mechanisms:

- separate “isochronous” and “cyclic” traffic queues,
- Queue-based resource allocation in all bridges,
- ...

2.5.9 Use case 15: Auto domain protection

Machines are built in a way that not always all devices are really attached either due to different machine models/variants or repair. In this use case a TSN domain shall not expand automatically when e.g. two machines get connected via an unplanned and unintended link.

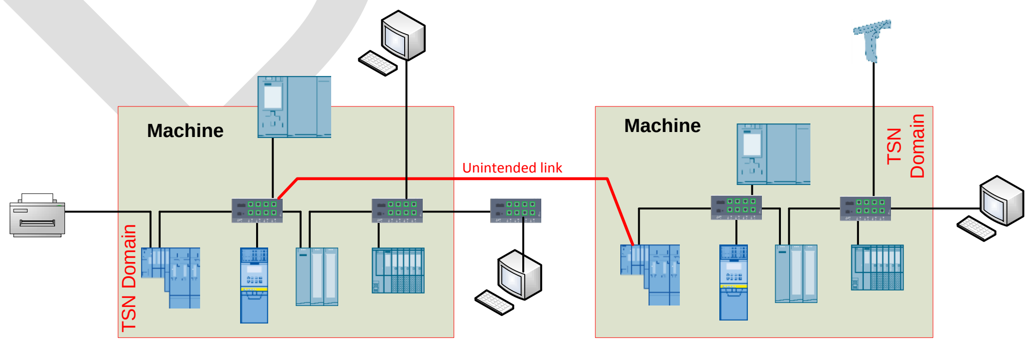

Figure 31 – auto domain protection

Requirement:

Support of auto domain protection to prevent unintended use of traffic classes

<u>Useful 802.1Q mechanisms:</u>

- Priority regeneration
- …

2.5.10 Use case 16: Vast number of connected stations

Some industrial applications need a massive amount of connected stations like

- Car production sites
- Postal, Parcel and Airport Logistics
- …

Examples for “Airport Logistics”:

- Incheon International Airport, South Korea
- Guangzhou Baiyun International Airport, China
- London Heathrow Airport, United Kingdom
- Dubai International Airport, UAE
- …

Dubai International Airport, UAE
Technical Data:

- 100 km conveyor length
- 222 check-in counters
- car park check-in facilities
- Max. tray speed: 7.5 m/s
- 49 make-up carousels
- 14 baggage claim carousels
- 24 transfer laterals
- Storage for 9,800 Early Bags
- Employing 48 inline screening
- Max. 8-stories rack system
- 10,500 ton steel
- 234 PLC’s
- 16,500 geared drives
- [xxxx digital IOs]

<u>Requirement</u>:

Make sure that even this massive amount of stations works together with the TSN-IA profile. This kind of applications may or may not require wireless support, too.

<u>Useful 802.1 mechanisms:</u>

- …

2.5.11 Minimum required quantities

2.5.11.1 A representative example for VLAN requirements

Figure 32 shows the IEEE 802.1Q based stacked physical, logical and active topology model. This principle is used to build TSN domains.

It shows the different active topologies driven by either VID (identified by VLAN) or protocol (identified by DA-MAC and/or protocol type).

Additionally the number of to be supported VIDs per bridge is shown. The number of protocol agent defined active topologies is just an example because e.g. LLDP, RSTP or MST is missing.

The following topologies, trees and VLANs are shown in Figure 32.

⓿	Physical network topology	all existing devices and links
❶	Logical network topology	**TSN domain**: administrative selection of elements from the physical topology
❷	Active default topology	Default VLAN: result of a spanning tree algorithm (e.g. RSTP)
❸	Cyclic RT	VLAN for cyclic rea-time streams
❹	Cyclic RT „R”	VLAN for redundant cyclic rea-time streams
❺	Isochronous cyclic RT 1	VLAN for isochronous cyclic rea-time streams
❻	Isochronous cyclic RT 1 „R”	VLAN for redundant isochronous cyclic rea-time streams
❼	Isochronous cyclic RT 2	VLAN for isochronous cyclic rea-time streams
❽	Working clock	gPTP sync tree used for the synchronization of a working clock
❾	Working clock „R”	Hot standby gPTP sync tree used for the synchronization of a working clock
❶⓿	Universal time	gPTP sync tree used for the synchronization of universal time

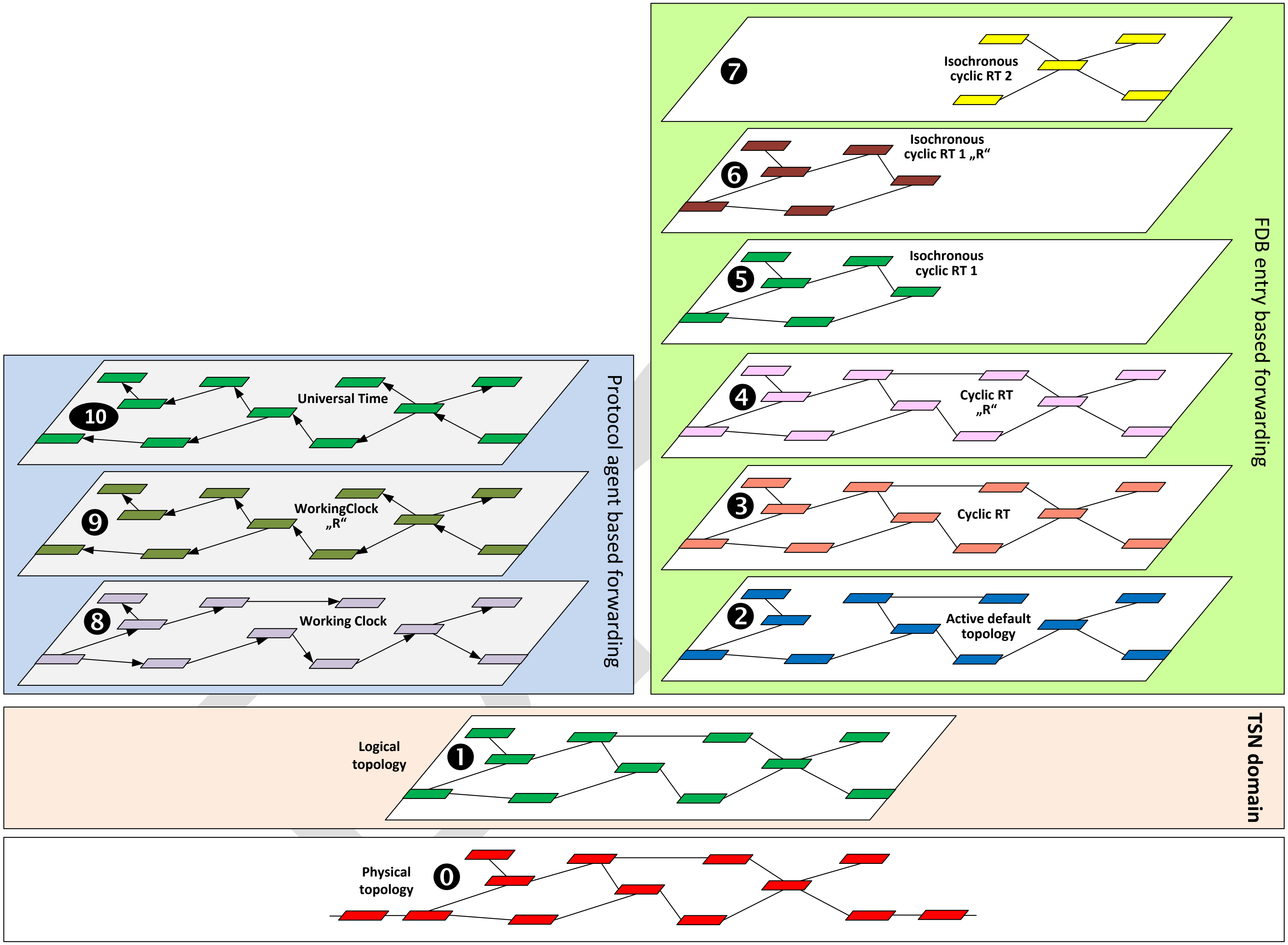

Figure 32 – Topologies, trees and VLANs

Expected numbers of DA-MAC address entries used together with five VLANs (Default, High. High Redundant, Low and Low Redundant) are shown in Table 9 and Table 10.

Table 9 – Expected number of stream FDB entries

# of VLANs	# of DA-MACs	Usage
4	4 096	Numbers of DA-MAC address entries used together with four VLANs (High, High Red, Low and Low Red)

Expected number of entries is given by the maximum device count of 1 024 together with the 50% saturation due to hash usage rule.

Table 10 shows the expected number of possible FDB entries.

Table 10 – Expected number of non-stream FDB entries

# of VLANs	# of entries	Usage
1	2 048	Learned and static entries for both, Unicast and Multicast

The hash based FDBs shall support a neighborhood for entries according to Table 11.

Table 11 – Neighborhood for hashed entries

Neighborhood	Usage
4	Optional A neighborhood of four entries is used to store a learned entry if the hashed entry is already used. A neighborhood of four entries for the hashed index is check to find or update an already learned forwarding rule.
8	Default A neighborhood of eight entries is used to store a learned entry if the hashed entry is already used. A neighborhood of eight entries for the hashed index is check to find or update an already learned forwarding rule.
16	Optional A neighborhood of sixteen entries is used to store a learned entry if the hashed entry is already used. A neighborhood of sixteen entries for the hashed index is check to find or update an already learned forwarding rule.

2.5.11.2 A representative example for data flow requirements

TSN domains in an industrial automation network for cyclic real-time traffic can span multiple Cyber-physical systems, which are connected by bridges. The following maximum quantities apply:

- Stations: 1024
- Network diameter: 64
- per PLC for Controller-to-Device (C2D) – one to one or one to many – communication:
  - 512 producer and 512 consumer data flows
  - 64 kByte Output und 64 kByte Input data

- per Device for Device-to-Device (D2D) – one to one or one to many – communication:
  - 2 producer and 2 consumer data flows
  - 1400 Byte per data flow
- per PLC for Controller-to-Controller (C2C) – one to one or one to many – communication:
  - 64 producer and 64 consumer data flows
  - 1400 Byte per data flow
- Example calculation for eight PLCs
  - → 8 x 512 x 2 = 8192 data flows for C2D communication
  - → 8 x 64 x 2 = 1024 data flows for C2C communication
  - → 8 x 64 kByte x 2 = 1024 kByte data for C2D communication
  - → 8 x 64 x 1400 Byte x 2 = 1400 kByte data for C2C communication
- All above shown data flows may optionally be redundant for seamless switchover due to the need for High Availability.

Application cycle times for the 512 producer and 512 consumer data flows differ and follow the application process requirements.

E.g. 125 µs for those used for control loops and 500 µs to 512 ms for other application processes. All may be used concurrently and may have frames sizes between 1 and 1440 bytes.

2.5.11.3 A representative example of communication use cases

IO Station – Controller (input direction)

- Up to 2000 published + subscribed signals (typically 100 – 500)
- Scan interval time: 0,5 ..100ms (typical 10ms)

Controller – Controller (inter-application)

- Up to 1000 published + subscribed signals (typically 100 – 250)
- Application task interval time: 10..1000ms (typical 100ms)
- Resulting Scan interval time: 5 … 500 ms

Closing the loop within/across the controller

- Up to 2000 published + subscribed signals (typically 100 – 500)
- Application task interval time: 1..1000ms (typical 100ms)
- Resulting Scan interval time when spreading over controllers: 0,5 … 500 ms

Controller – IO Station (output direction)

- Up to 2000 published + subscribed signals (typically 100 – 500)
- Application task interval time: 10..1000ms (typical 100ms
- Resulting Scan interval time: 5 … 500 ms

2.5.11.4 "Fast" process applications

The structure shown in Figure 1 applies. Figure 33 provides a logic station view.

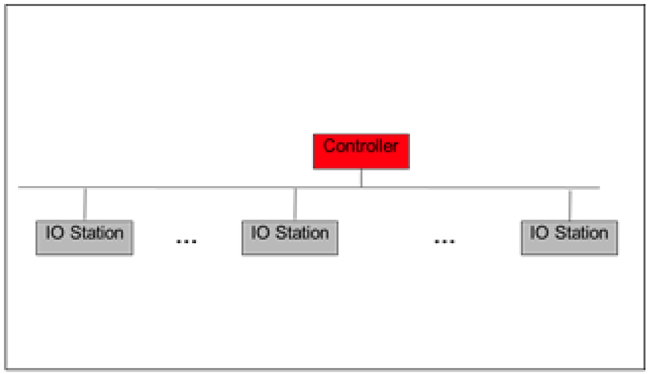

Figure 33 – Logical communication concept for fast process applications

Specifics:

- Limited number of nodes communicating with one Controller (e.g. Turbine Control)
- Up to a dozen Nodes of which typically one is a controller
- Data subscriptions (horizontal):
  - 270 bytes published + subscribed per IO-station
  - Scan Interval time 0,5 to 2 ms
- Physical Topology: Redundant (as path and as device)

2.5.11.5 Server consolidation

The structure shown in Figure 1 applies. Figure 34 provides a logic station view.

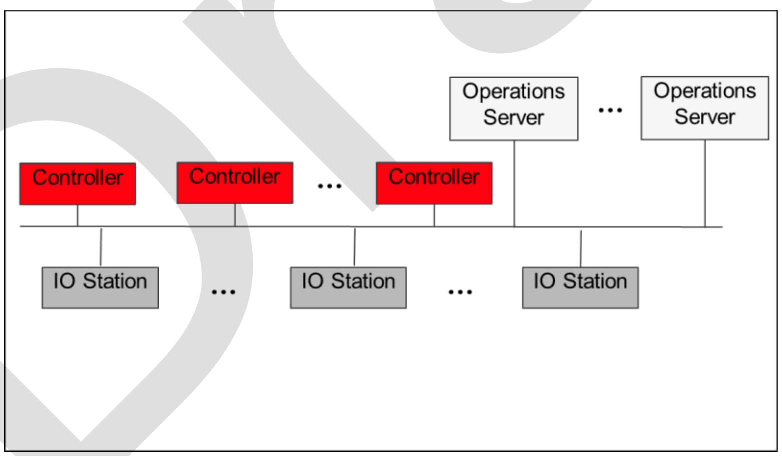

Figure 34 – Server consolidated logical connectivity

Data access to Operations Functionalities consolidated through Servers

- Up to 100 Nodes in total
- Out which are up to 25 Servers

Data subscriptions (vertical):

- Each station connected to at least 1 Server
- max. 20000 subscribed items per Controller/IO-station
- 1s update rate
- 50% analog items -> 30% change every sec

Different physical topologies

- Rings, stars, redundancy

2.5.11.6 Direct client access

The structure shown in Figure 1 applies. Figure 35 provides a logic station view.

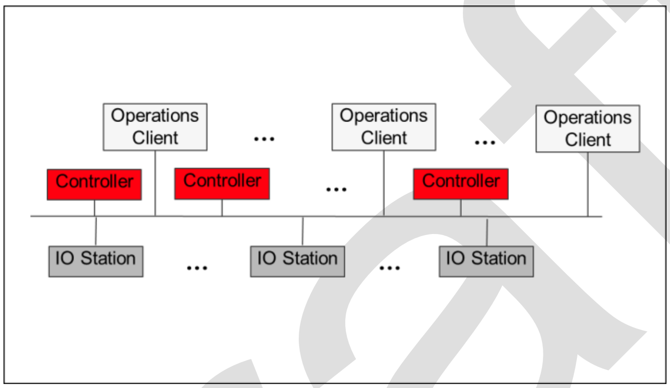

Figure 35 – Clients logical connectivity view

Data access to Operations Functionalities directly by Clients

- Max 20 direct access clients

Data subscriptions (vertical):

- Up to 3000 subscribed items per client
- 1s update rate
- Worst case 60000 items/second per controller in classical Client/Server setup
- 50% analog items -> 30% change every sec

Different physical topologies

- Rings, stars, redundancy

2.5.11.7 Field devices

The structure shown in Figure 1 applies. Figure 36 provides a logic station view.

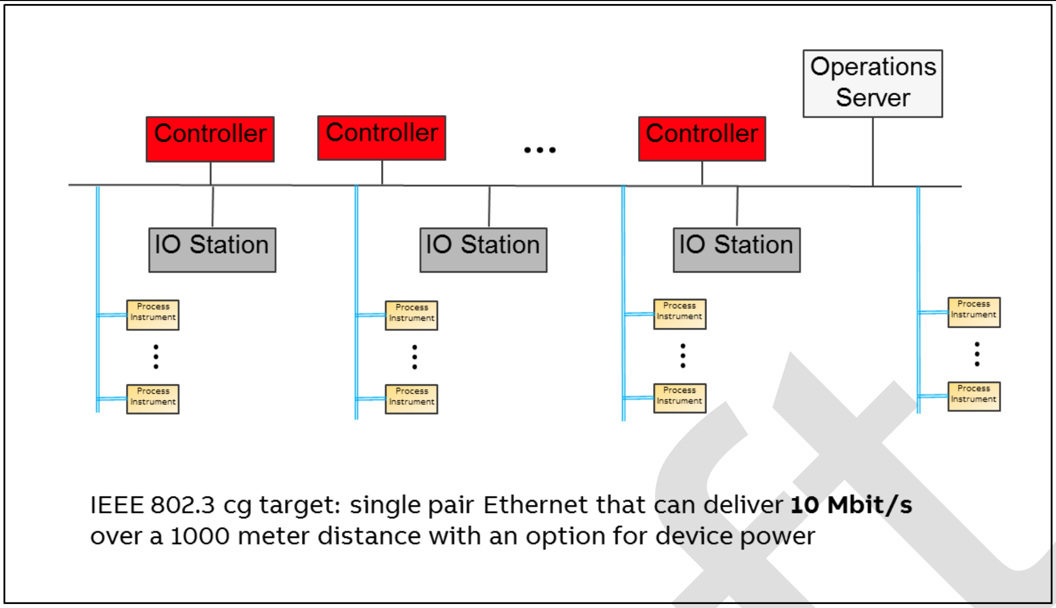

Figure 36 – Field devices with 10Mbit/s

Field Networks integrated with converged network

- Up to 50 devices per field segment
- Scan interval 50ms … 1s, typical 250ms
- Mix of different device types from different vendors
- Many changes during runtime

2.5.12 Bridge Resources

The bridge shall provide and organize its resources in a way to ensure robustness for the traffic defined in this document as shown in Formula (1).

The queuing of frames needs resources to store them at the destination port. This resources may be organized either bridge globally, port globally or queue locally.

The chosen resource organization model influences the needed amount of frame resources.

For bridge memory calculation Formula (1) applies.

$$\text{MinimumFrameMemory} = (\text{NumberOfPorts} - 1) \times \text{MaxPortBlockingTime} \times \text{Linkspeed} \qquad (1)$$

Where

MinimumFrameMemory	is minimum amount of frame buffer needed to avoid frame loss from non stream traffic due to streams blocking egress ports.
NumberOfPorts	is number of ports of the bridge without the management port.
MaxPortBlockingTime	is intended maximum blocking time of ports due to streams per millisecond.
Linkspeed	is intended link speed of the ports.

Formula (1) assumes that all ports use the same link speed and a bridge global frame resource management. Table 12, Table 13, Table 14, and Table 15 shows the resulting values for different link speeds.

The traffic from the management port to the network needs a fair share of the bridge resources to ensure the required injection performance into the network. This memory (use for the real-time frames) is not covered by this calculation.

Table 12 – MinimumFrameMemory for 100 Mbit/s (50%@1 ms)

# of ports	MinimumFrameMemory [KBytes]	Comment
1	0	The memory at the management port is not covered by Formula (1)
2	6,25	All frames received during the 50%@1 ms := 500 µs at one port needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
3	12,5	All frames received during the 50%@1 ms := 500 µs at two ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
4	18,75	All frames received during the 50%@1 ms := 500 µs at three ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
other	tbd	tbd

Table 13 – MinimumFrameMemory for 1 Gbit/s (20%@1 ms)

# of ports	MinimumFrameMemory [KBytes]	Comment
1	0	The memory at the management port is not covered by Formula (1)
2	25	All frames received during the 20%@1 ms := 200 µs at one port needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
3	50	All frames received during the 20%@1 ms := 200 µs at two ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
4	75	All frames received during the 20%@1 ms := 200 µs at three ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
other	tbd	tbd

Table 14 – MinimumFrameMemory for 2,5 Gbit/s (10%@1 ms)

# of ports	MinimumFrameMemory [KBytes]	Comment
1	0	The memory at the management port is not covered by Formula (1)
2	31,25	All frames received during the 10%@1 ms := 100 µs at one port needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
3	62,5	All frames received during the 10%@1 ms := 100 µs at two ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
4	93,75	All frames received during the 10%@1 ms := 100 µs at three ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
other	tbd	tbd

Table 15 – MinimumFrameMemory for 10 Gbit/s (5%@1 ms)

# of ports	MinimumFrameMemory [KBytes]	Comment
1	0	The memory at the management port is not covered by Formula (1)
2	62,5	All frames received during the 5%@1 ms := 50 µs at one port needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
3	125	All frames received during the 5%@1 ms := 50 µs at two ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
4	187,5	All frames received during the 5%@1 ms := 50 µs at three ports needed to be forwarded to the other port are stored during the allocation of this port due to stream transmission.
other	tbd	tbd

A per port frame resource management leads to the same values, but reduced the flexibility to use free frame resources for other ports.

A per queue per port frame resource management would increase (multiplied by the number of to be covered queues) the needed amount of frame resources dramatically almost without any benefit.

Example “per port frame resource”:

100 Mbit/s, 2 Ports, and 6 queue
Needed memory := 6,25 KOctets * 6 := 37,5 KOctets.

No one is able to define which queue is needed during the “stream port blocking” period.

Bridged End-Stations need to ensure that their local injected traffic does not overload the bridge resources. Dedicated resources for local injection and forwarding can solve this topic.

2.6 Industrial automation machines, production cells, production lines

2.6.1 Use case 17: 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 OS (Operator System) (with its own TSN domain).

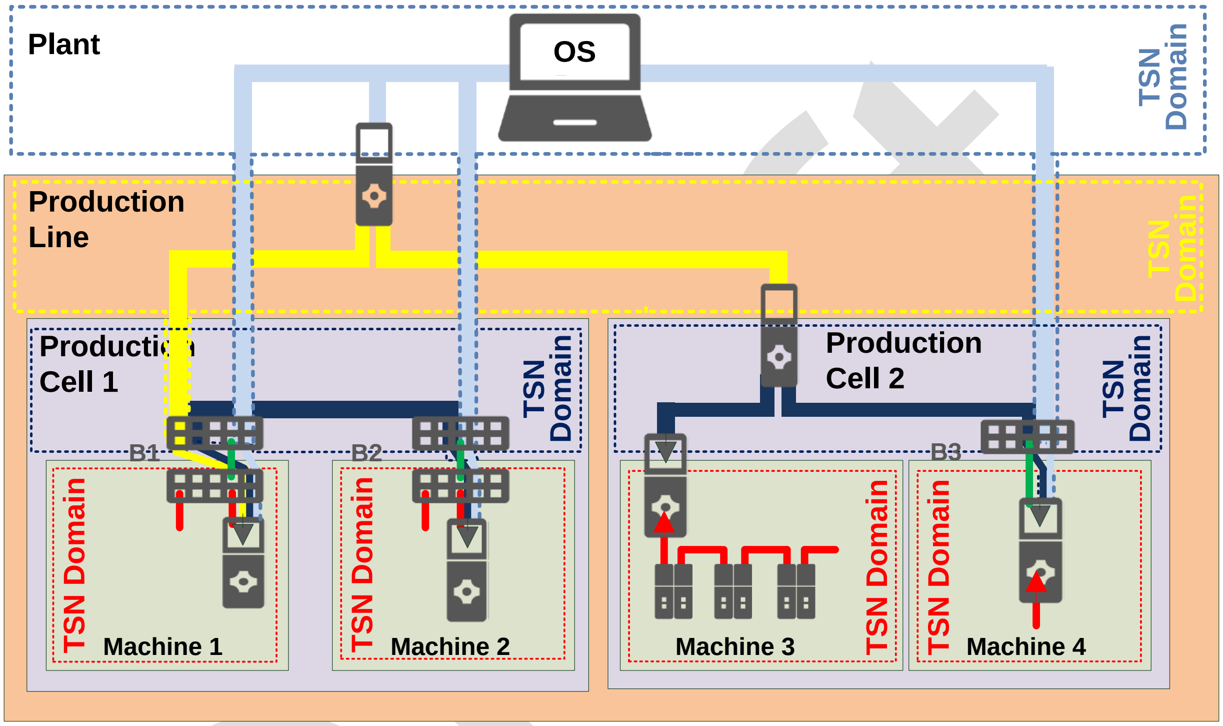

Figure 37 – M2M/C2C between TSN domains

Figure 37 shows that multiple 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.

Examples:

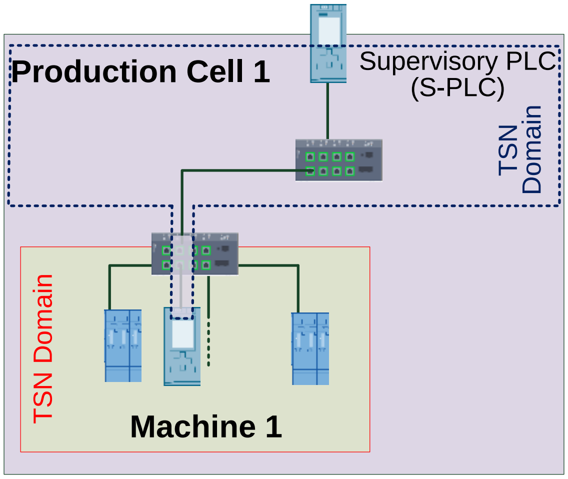

Figure 38 – M2M with supervisory PLC

Figure 38 gives an example of M2M communication to a supervisory PLC.

Figure 39 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 overlapping TSN domains.

Additionally Figure 40 shows an example where M2M communication is used to connect a PC for diagnostics/monitoring.

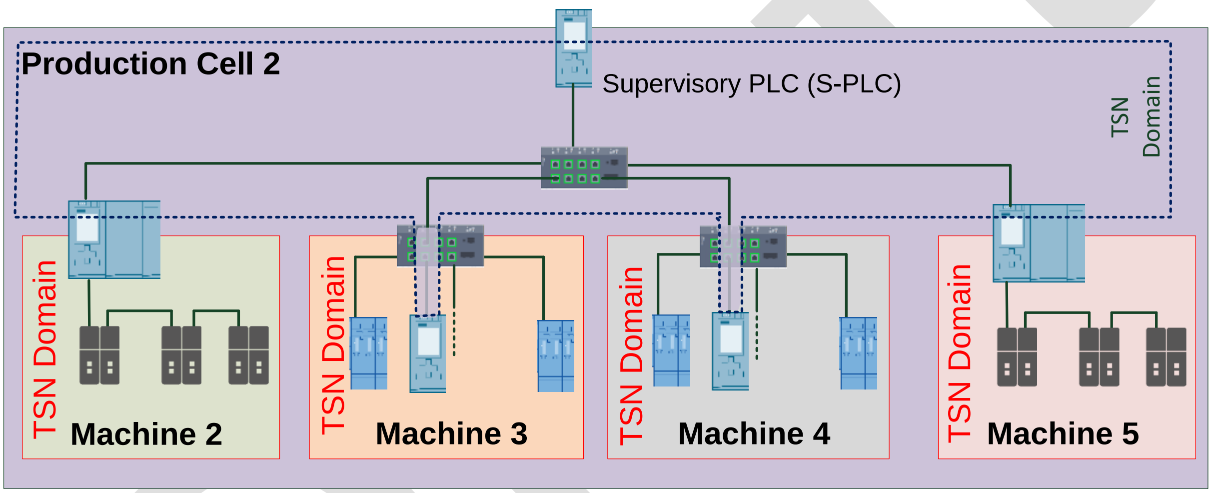

Figure 39 – M2M with four machines

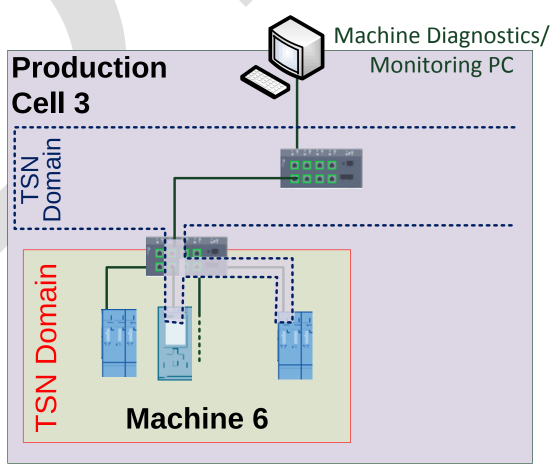

Figure 40 – M2M with diagnostics/monitoring PC

Figure 40 shows a M2M diagnostics related use case: communication is cyclic and must 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 must 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 39 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.

Useful 802 mechanisms:

- 802.1Qbu, 802.1Qbv, 802.1Qci, Fixed priority, 802.3br
- Priority Regeneration,
- Queue-based resource allocation,
- VLANs to separate TSN domains.

2.6.2 Use case 18: 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 41, Figure 42 and Figure 43 give some examples of pass-through traffic installations in industrial automation.

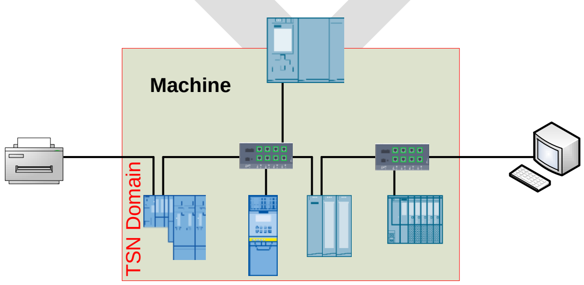

Figure 41 – pass-through one machine

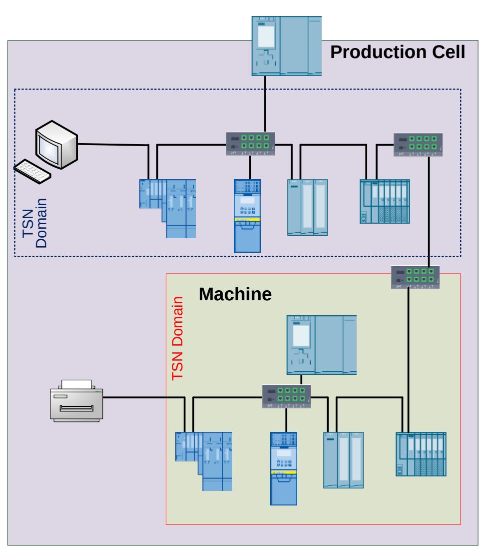

Figure 42 – pass-through one machine and

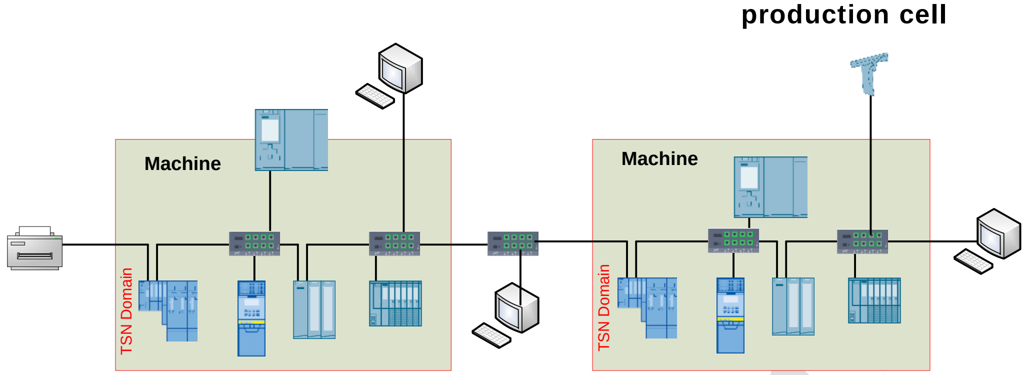

Figure 43 – pass-through two machines

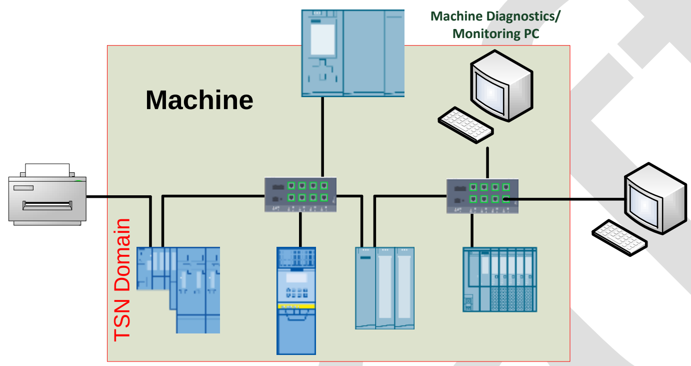

Figure 44 – machine with diagnostics / monitoring PC

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.

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 19: Modular machine assembly

In this use case machines are variable assemblies of multiple different modules. Effective assembly of a machine is executed in the plant dependent on the current stage of production, e.g. bread-machine with the modules: base module, 'Kaisersemmel' module, 'Rosensemmel' module, sesame caster, poppy-seed caster, baking oven OR advertisement feeder for newspapars.

Figure 45 may have relaxed latency requirements, but the machine in Figure 46 needs to work with very high speed and thus has very demanding latency requirements.

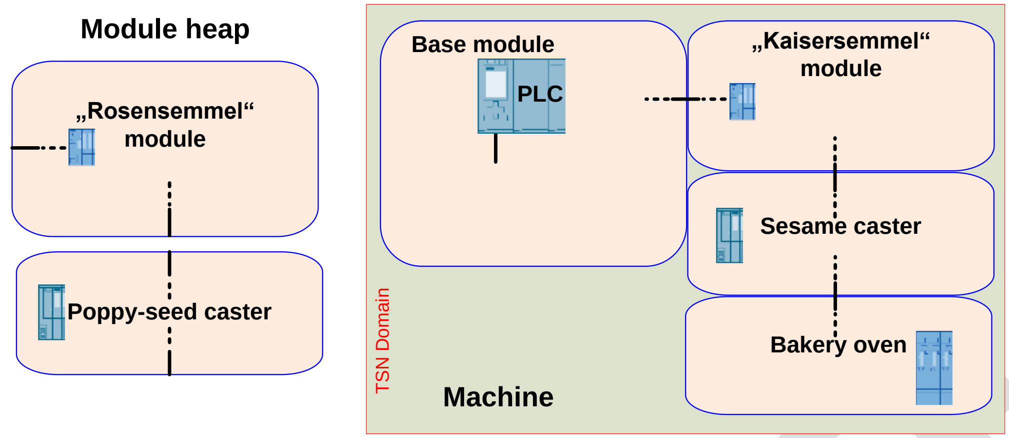

Figure 45 – modular bread-machine

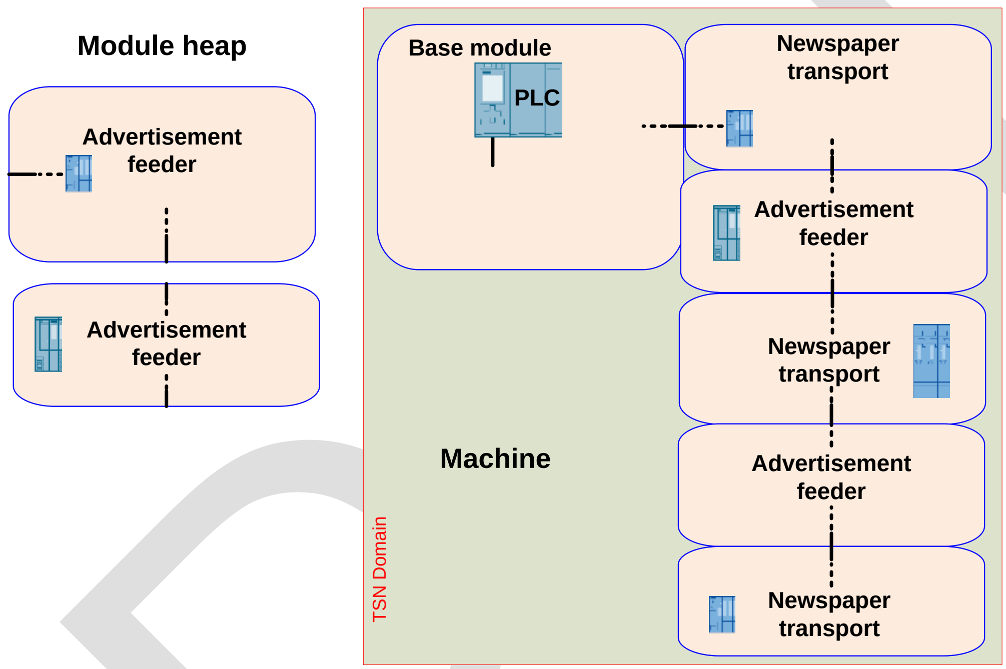

Figure 46 – modular advertisement feeder

<u>Requirement</u>:
Modules can be assembled to a working machine variably on-site (either in run, stop or power down mode) as necessary (several times throughout a day). The machine produces the selected variety of a product. Communication relying on TSN features is established automatically after the modules are plugged without management/ configuration interaction.

2.6.4 Use case 20: Tool changer

Tools (e.g. different robot arms) are in power off mode. During production a robot changes its arms for different production steps.

They get mechanically connected to a robot arm and then powered on. The time till operate influences the efficiency of the robot and thus the production capacity of the plant. Robots may share a common tool pool. Thus the “tools” are connected to different robots during different production steps.

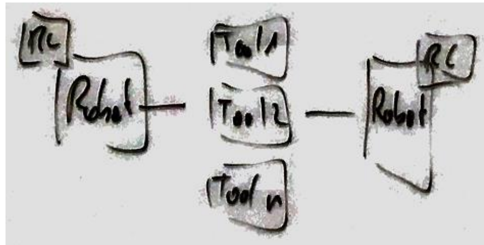

Figure 47 – tool changer

Requirement:

- Added portion of the network needs to be up and running (power on to operate) in less than 500ms.
- Extending and removing portions of the network (up to 16 devices) in operation
    - by one connection point (one robot using a tool)
    - by multiple connection points (multiple robots using a tool)

Useful 802.1Q mechanisms:

- preconfigured streams
- …

2.6.5 Use case 21: 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.

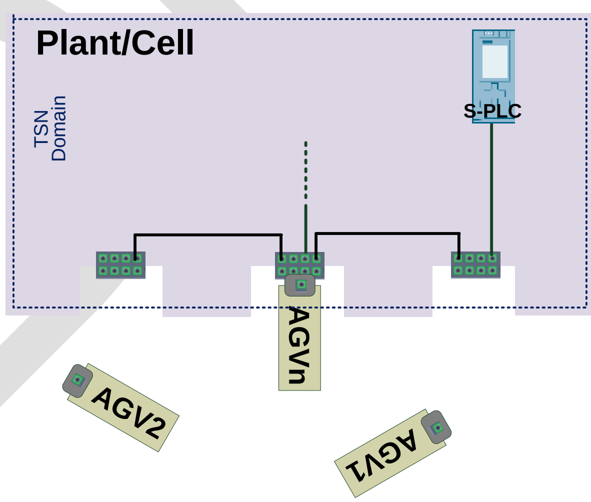

Figure 48 – AGV plug and unplug

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.

Useful 802.1Q mechanisms:

- preconfigured streams
- …

2.6.6 Use case 22: Energy Saving

Complete or partial plant components are switched off and on as necessary to save energy. Thus, portions of the plant are temporarily not available.

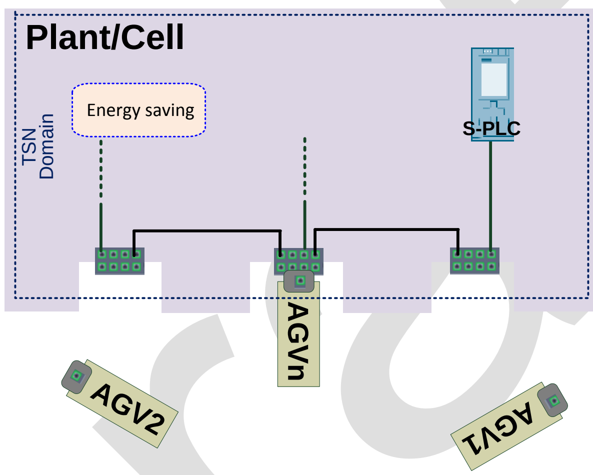

Figure 49 – energy saving

Requirement:
Energy saving region switch off/on shall not create process disturbance.
Communication paths through the energy saving area between end-stations, which do not belong to the energy saving area, shall be avoided.

Useful 802.1Q mechanisms:

- Appropriate path computation by sorting streams to avoid streams passing through energy saving region.

2.6.7 Use case 23: 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.

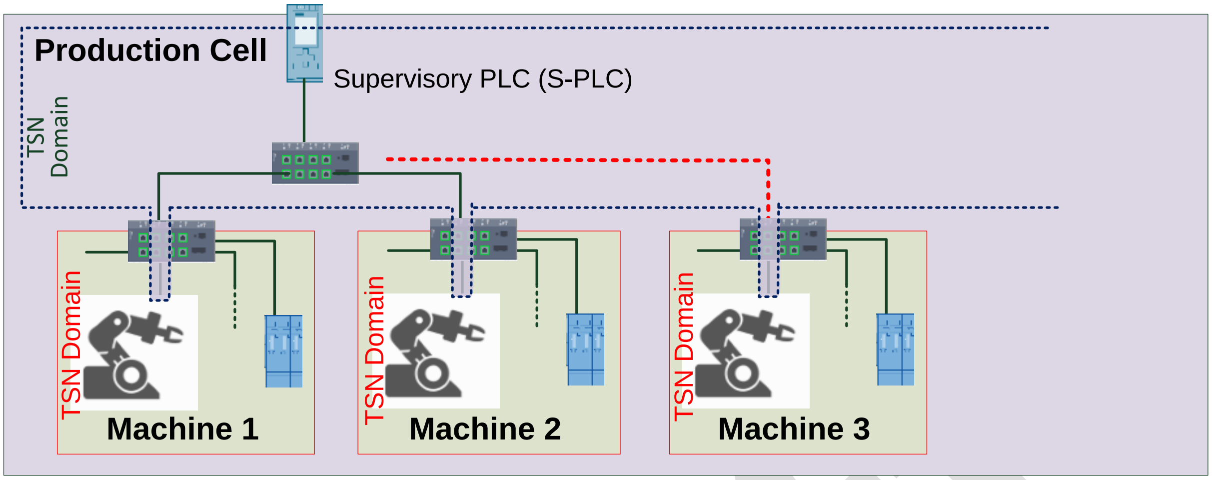

Figure 50 – add machine

Requirement:
Adding a machine/cell/production line shall not disturb existing installations

Useful mechanisms:

- …

2.6.8 Use case 24: Multiple applications in a station using the TSN-IA profile

E.g. Technology A and B in PLC and devices.

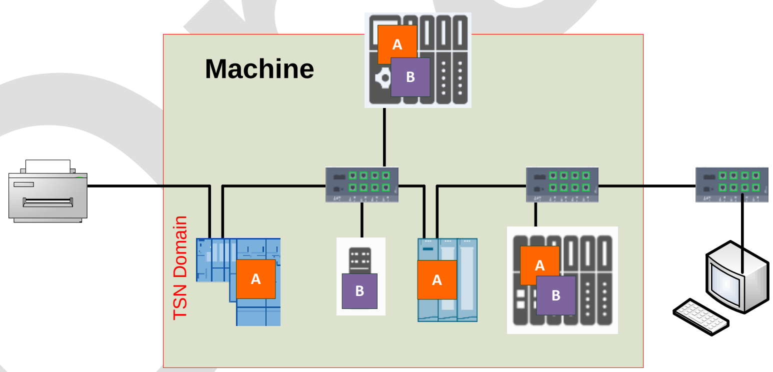

Figure 51 – two applications

Requirement:
Stations with multiple applications using TSN traffic classes shall be supported.

Useful 802.1 mechanisms:

- …

2.6.9 Use case 25: Functional safety

Functional safety is defined in IEC 61508 as "*part of the overall safety relating to the EUC [Equipment Under Control] and the EUC control system that depends on the correct functioning of* *the E/E/PE [electrical/electronic/programmable electronic] safety-related systems and other risk reduction measures*"

IEC 61784-3-3 defines a safety communication layer structure, which is performed by a standard transmission system (black channel), and an additional safety transmission protocol on top of this standard transmission system.

The standard transmission system includes the entire hardware of the transmission system and the related protocol functions (i.e. OSI layers 1, 2 and 7).

Safety applications and standard applications are sharing the same standard communication systems at the same time.

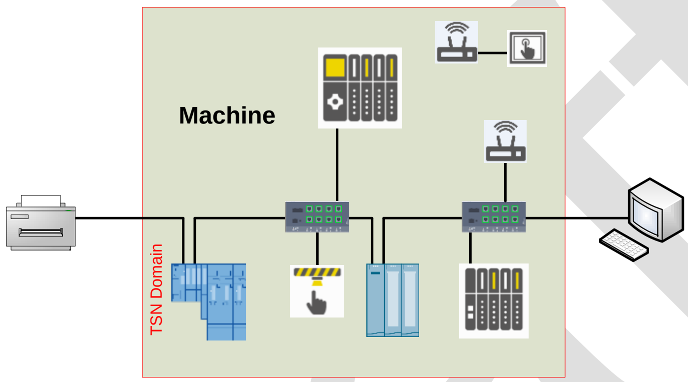

Figure 52 – Functional safety with cyclic real-time

Requirement:

Safety applications (as black channel) and standard applications share the same TSN-IA profile based communication system at the same time.

Useful 802.1 mechanisms:

- …

2.7 DCS Reconfiguration

2.7.1 Challenges of DCS Reconfiguration Use Cases

The challenge these use cases bring is the influence of reconfiguration on the existing communication: all has to happen without disturbances to the production!

We consider important the use case that we can connect any number of new devices wherever in the system and they get connectivity over the existing infrastructure supporting TSN features without a change to the operational mode of the system.

2.7.2 Use case 26: DCS Device level reconfiguration

The structure shown in Figure 1 applies. Figure 53 provides a logic station view.

- SW modifications to a device
  - A change to the device's SW/SW application shall happen, which does not require changes to the SW/SW application running on other devices (incl. firmware update): *add examples*
- Device Exchange/Replacement

- The process device is replaced by another unit for maintenance reason, e.g. for off-process calibration or because of the device being defective (note: a “defective device may still be fully and properly engaged in the network and the communication, e.g. if just the sensor is not working properly anymore):
- Use case: repair

- Add/remove additional device(s)
  - A new device is brought to an existing system or functionality, which shall be used in the application, is added to a running device, e.g. by enabling a SW function or plugging in a new HW-module. Even though the scope of change is not limited to a single device because also the other device engaged in the same application
  - For process devices, servers: BIOS, OS and applications updates, new VMs, workstations
  - Use cases: replacement with upgrade/downgrade of an existing device, simply adding new devices, removal of device, adding connections between devices
- Influencing factors relative to communication
  - Communication requirements of newly added devices (in case of adding)
  - Existing QoS parameters (i.e. protocol-specific parameters like TimeOuts or Retries)
  - Device Redundancy
  - Network/Media Redundancy
  - Virtualization
  - For servers: in-premise or cloud
  - Clock types in the involved process devices
  - Universal time and working clock domains
  - Cycle time(s) needed by new devices
  - Available bandwidth
  - Existing security policies

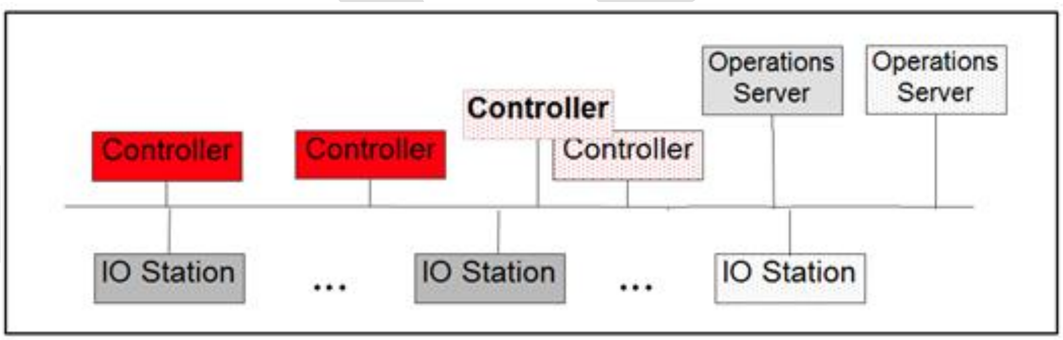

Figure 53 – Device level reconfiguration use cases

2.7.3 Use case 27: DSC System level reconfiguration

The structure shown in Figure 1 applies. Figure 54 provides a logic station view.

- Extend an existing plant
  - Add new network segment to existing network
    - Existing non-TSN / Newly added is TSN
    - Existing TSN / Newly added is TSN
- Update the system security policy
  - [New key lengths, new security zones, new security policy]
  - To be defined how and by whom to be handled
- Influencing factors

- Same as for “device-level”

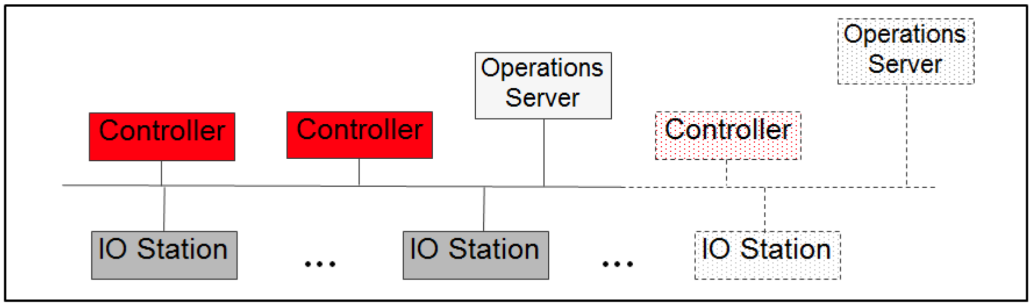

Figure 54 – System level reconfiguration use cases

2.8 Further Industrial Automation Use Cases

2.8.1 Use case 28: Network monitoring and diagnostics

Diagnostics plays an important role in the management of systems and of devices. Generally speaking the mechanisms used in this context are acyclic or having large cycle times so that they could perhaps be considered, from a networking perspective as sporadic. Most of the use cases related to diagnostics will be included in this category.

- Quick identification of error locations is important to minimize downtimes in production.
- Monitoring network performance is a means to anticipate problems so that arrangements can be planned and put into practice even before errors and downtimes occur.
- Identification of devices on an industrial Ethernet network must be done in a common, interoperable manner for interoperability on a converged TSN network. This identification both needs to show the type of device, and the topology of the network. IEEE 802.1AB, the Link Layer Discovery Protocol (LLDP), provides one possible mechanism for this to be done at layer two, but provides a large degree of variability in implementation.

Requirement:

Minimize downtime

Monitoring and diagnostics data including used TSN features shall be provided, e.g. established streams, failed streams, stream classes, bandwidth consumption, …

A discovery protocol such as IEEE 802.1AB shall be leveraged to meet the needs of TSN-IA.

Useful 802.1 (ietf) mechanisms:

- MIBs (SNMP)
- YANG (NETCONF/RESTCONF)

2.8.2 Use case 29: 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

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

Useful mechanisms:

- 802.1X
- IEC62443
- …

2.8.3 Use case 30: Firmware update

Firmware update is done during normal operation to make sure that the machine e.g. with 1000 devices is able be updated with almost no down time.

With bump: separate loading (space for 2 FW versions required) and coordinated activation to minimize downtime

Bumpless: redundant stations with bumpless switchover – the single device may lose connection (bump)

Requirement:

Stations shall be capable to accept and store an additional fw version without disturbance.

Useful 802.1 mechanisms:

- …

2.8.4 Use case 31: Virtualization

Workload consolidation is done by virtualizing the hardware interfaces. Even in such kind of environment the TSN features according to the TSN-IA profile shall be available and working.

vSwitch / vBridge

Figure 55 and Figure 56 show the two principle setups for an Ethernet communication concept allowing both, communication VM to Ethernet and VM to VM. The applications inside the VM shall not see, whether they communicate to another VM or an Ethernet node.

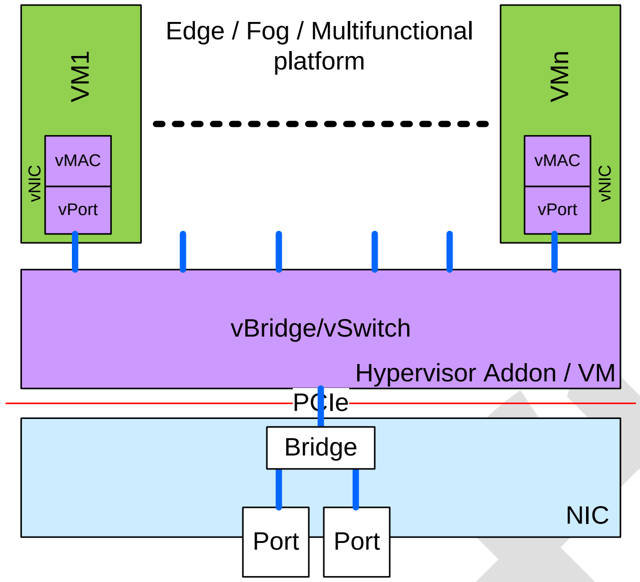

Figure 55 – Ethernet interconnect with VM based vBridge

Figure 55 scales for an almost infinite amount of VMs, because the memory bandwidth and the compute power of the vMAC/vPort and vSwitch/vBridge VM are much higher than the PCIe bandwidth to the NIC.

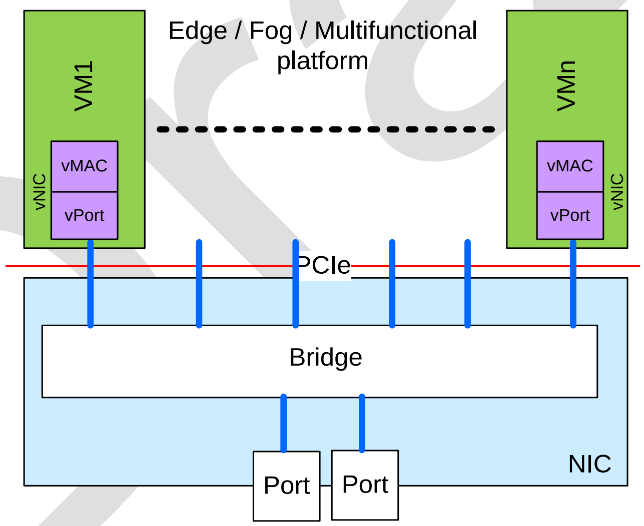

Figure 56 – Ethernet interconnect with PCIe connected Bridge

Figure 56 fits for a limited amount of VMs, because it saves the additional vSwitch/vBridge VM. For a given amount of VMs, e.g. Gen3 x4 or Gen4 x4, seems to be sufficient.

Requirement:

vBridge and vPort should behave as real Bridge and real Port: data plane, control plane, ...
vBridge and vPort can become members of TSN domains.
Should work like use case "multiple applications"

Useful 802.1 mechanisms:

- …

2.8.5 Use case 32: Digital twin

Virtual pre-commissioning of machines can save a lot of time and money.
Up to 30 % time-saving in the development of new machines are foreseen by an increased engineering efficiency due to the implementation and usage of digital twins.
Faster development, delivery and commissioning of new machines at customer locations should be possible.

A digital twin shows the real machine in as much detail as possible and allows simulation of its operation. With the help of digital twins machines can gradually and virtually be developed – in parallel to the real production and commissioning process of the machines at customer locations.

Requirement:

Reliable planning, development, testing, simulation and optimization results shall be possible

Useful 802.1 mechanisms:

- …

2.8.6 Use case 33: Device replacement without engineering

Any device in a plant, i.e. end-station, bridged end-station or bridge, may get broken eventually. If this happens fast and simple replacement of a broken device is necessary to keep production disturbance at a minimum (see also: 2.7.2 Use case 26: DCS Device level reconfiguration).
Support of “mechanical” replacement of a failed device with a new one without any engineering effort (i.e. without the need for an engineering tool) is a prerequisite for minimal repair downtime.

Requirement:

In case of repair it shall be possible to replace end-stations, bridged end-stations or brides without the need of an engineering tool.

Useful 802.1 mechanisms:

- …

3 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