Use Cases – IEEE P802.1DG V0.1

Contributor group

This document is created by Don Pannell. If you wish to be a Contributor to this document, whether or not you wish your name to be listed below, please contact Don at donald.pannell@nxp.com. Feedback is welcome! Please e-mail corrections/issues with suggested text.

Dorr, Josef <josef.dorr@siemens.com> - for the source format of this document
Pannell, Don <donald.pannell@nxp.com> - this document creator
Potts, Mike <mike.potts@gm.com> - for Use Case presentations
Zinner, Helge <helge.zinner@conti.de> - for Use Case presentation

Abstract

This document summarizes use cases relevant to Automotive Time Sensitive Networking (TSN), along with their associated requirements. It will be used by the IEEE P802.1DG editor to create the standard. The IEEE P802.1DG project's title is: "TSN Profile for Automotive In-Vehicle Ethernet Communications."

The enclosed use cases are intended to guide the specification process: WHAT shall be part of the standard and WHY. Then the content of IEEE P802.1DG standard specifies the HOW to achieve these use cases.

Some use cases are on a system level of an automotive system, even if the scope of IEEE P802.1DG does not cover the overall system level. The IEEE P802.1DG should enable or at least do not prevent the features described in this use case document. Example use cases that are currently outside the scope of the P802.1DG standard are those using wireless interfaces, but these uses clearly impact the "Ethernet Communications" use in the vehicle.

This document is intended an aide to the formation of the IEEE P802.1DG standard.

THIS DOCUMENT IS NOT THE STANDARD!!

Log

V0.1	2019-May-20	First version – to show structure and flow only.
		-
		-
		-

Content

Figures

Tables

1 Definitions and Terms

<<creator's note: The Definitions & Terms listed below are some Automotive specific definitions that have been added along with examples as listed in the Industrial Use Case document. This list will be updated & added to as needed. The intended edits for the next revision are marked. Suggestions of what should be kept or deleted is requested.>>

1.1 Definitions

ADAS	Adaptive Driver Assistance System – needed for autonomous driving
ADAS Level	Autonomous driving capability levels as defined by the Society of Automotive Engineers (SAE) Level 0: Driver controls it all, to Level 5: Fully autonomous in all environments/scenarios (no steering wheel necessary). See: https://www.techrepublic.com/article/autonomous-driving-levels-0-to-5-understanding-the-differences/
CAN(-FD)	Controller Area Network - a vehicle bus standard, '-FD' stands for the Flexible Data-rate extension
DC	Domain Controller
ECU	Electronic Control Unit
LIN	Local Interconnect Network - a vehicle bus standard
OEM	Original Equipment Manufacturer – In Automotive: The Car Maker
Tier 1	In Automotive: typically, a subsystem/ECU supplier
Tier 2	In Automotive: typically, a silicon supplier
Reconfiguration	Any intentional modification of the system structure or of the device-level content, including updates of any type
Operational state	Normal state of function of a unit
Maintenance state	Planned suspension or partial suspension of the normal state of function of a unit
Stopped state	Full non-productive mode of a unit
Convergent network concept	All LAN devices (wired or wireless) can exchange data over a common infrastructure, within defined QoS parameters <<creator's note: TSN over wireless media is outside the scope of IEEE P802.1DG (it's title specifically states Ethernet Communications), the include of wireless devices in use cases may be needed to show the system level need.>>

Device	End station, bridged end station, bridge, access point
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, requires transmission latency to be bounded.[1)]
TSN domain	A quantity of commonly managed 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. 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	Devices of a common working clock domain with a common setup for the isochronous cyclic real-time traffic type
cyclic real-time domain	Devices 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 Figure 13); values are specific to a TSN domain and specify a repetitive behavior of the network interfaces belonging to that TSN domain;
Stream forwarding	Forwarding of stream data along the stream path including TSN domain boundary crossings

226
1.2 IEEE 802.1 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

227

---

[1] taken from 802.1Q-2018

2 TSN in Automotive

<<creator’s note: The Industrial Use Case document used this section to describe Cyber-Physical Systems. I propose this section can be a brief overview of non-Ethernet in-vehicle networks and where & why Ethernet came into the Automotive picture. If people feel this is not needed, this section would just be an overview of what comes below.>>

2.1 Interoperability

<<creator’s note: What parts of this section from the Industrial Use Case document are applicable to Automotive? Clearly there is a desire for interoperability of devices. But Automotive is historically static in its network construction, even if the flows of streams are altered by firmware updates.>>

Interoperability may be achieved on different levels. Figure 1 and Figure 2 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 1).

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.

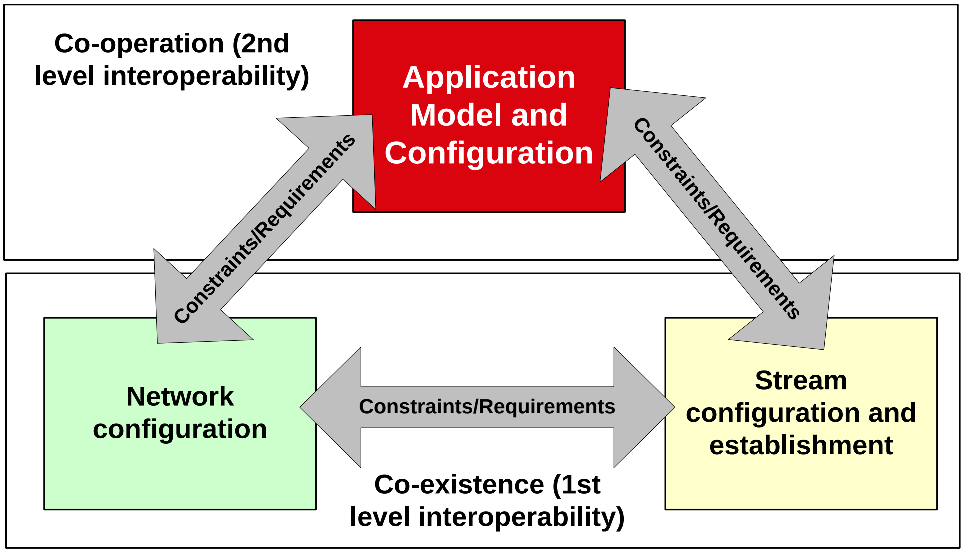


Figure 1 – Principle of interoperation

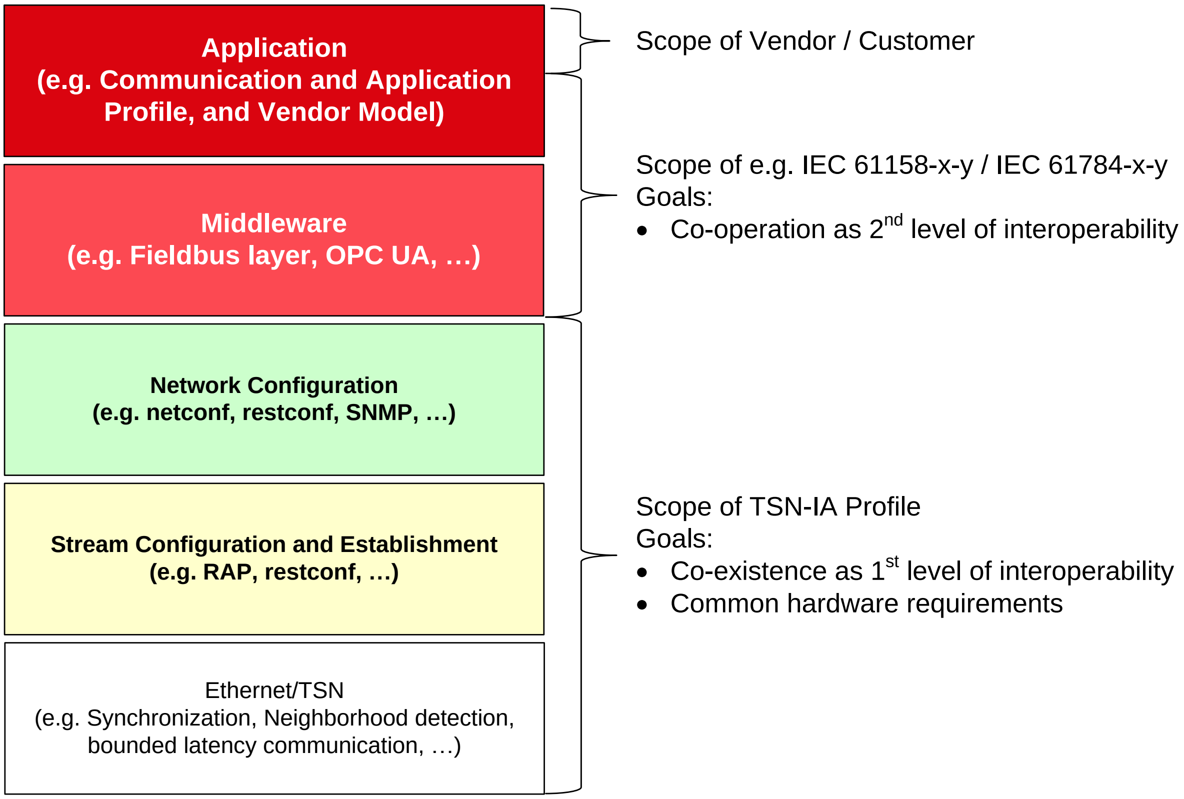


Figure 2 – Scope of work

2.2 TSN Domain

<<creator's note: What parts of this section from the Industrial Use Case document are applicable to Automotive? Is this concept needed for Automotive?>>

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 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 3 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.

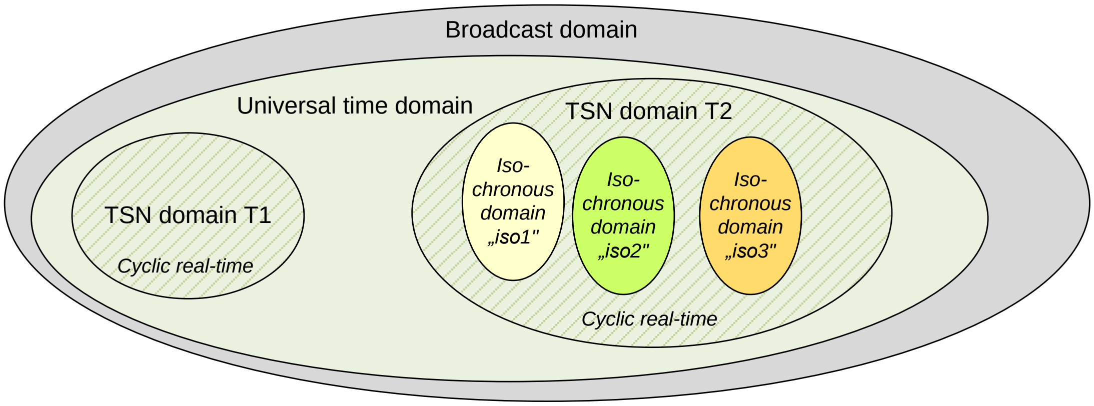


Figure 3 – Different Types of Domains

Interconnections between TSN domains are described in 2.2.2 and 3.8.1.

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 4 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.

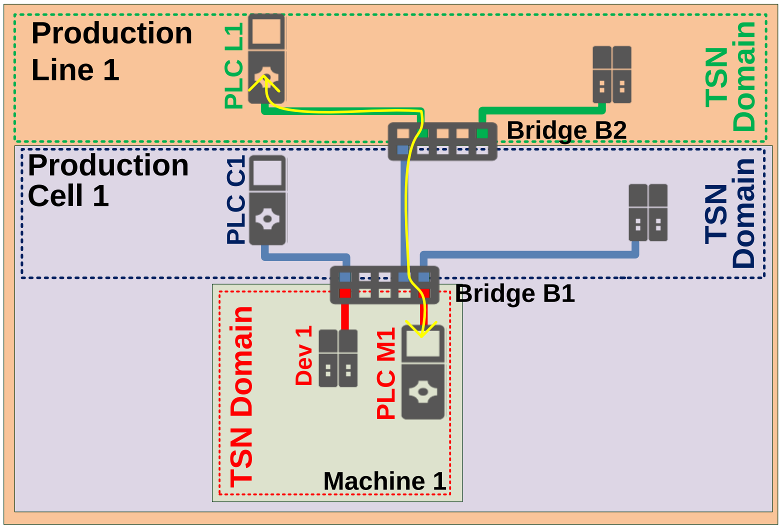


Figure 4 – Three TSN domains connected by Bridges

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 5 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.

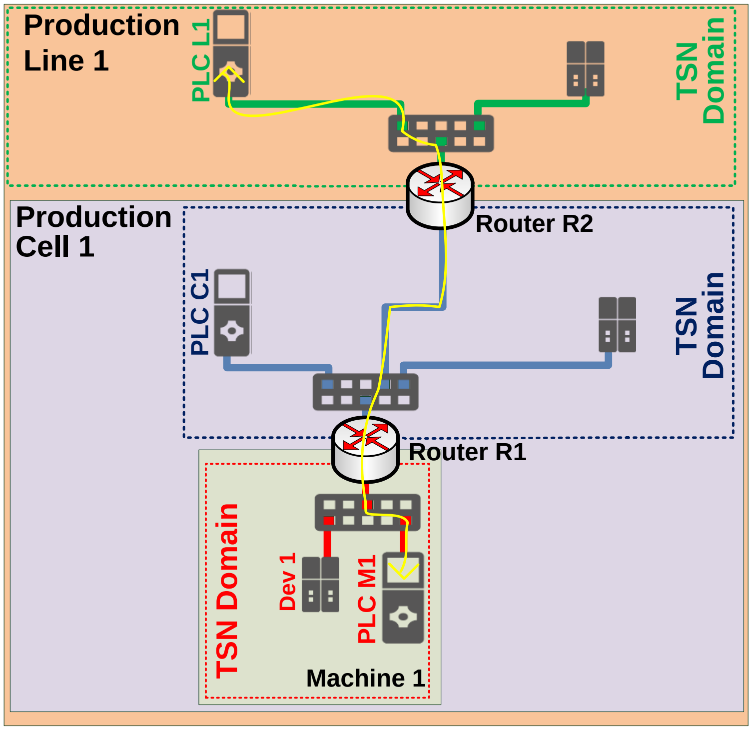


Figure 5 – Three TSN domains connected by Routers

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 6 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.

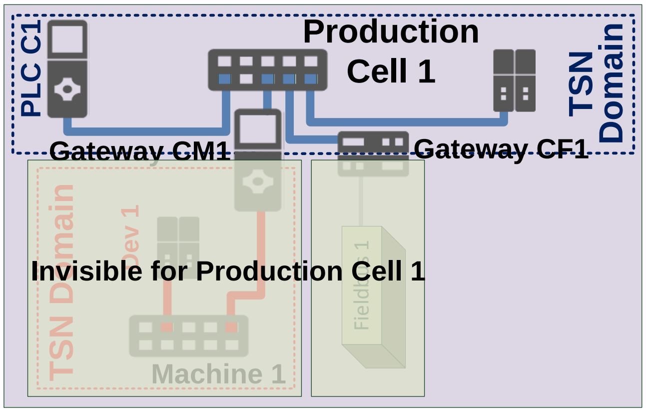


Figure 6 – Gateways with two TSN domains and an attached Fieldbus

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 6 and see also Use case 11: Fieldbus gateway).

2.3 Synchronization

<<creator's note: What parts of this section from the Industrial Use Case document are applicable to Automotive?>>

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 7 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.

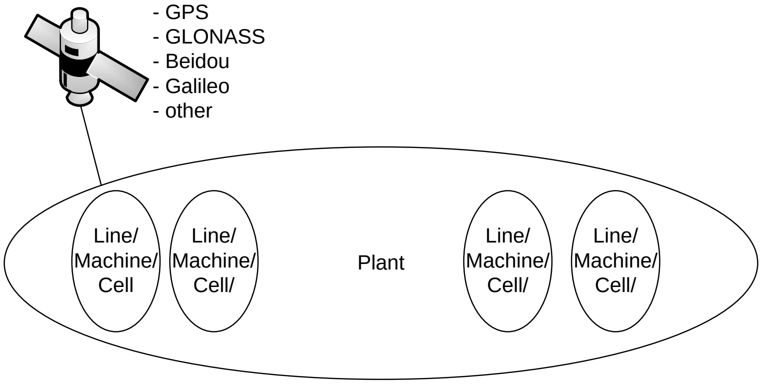


Figure 7 – plant wide time synchronization

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 8 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.

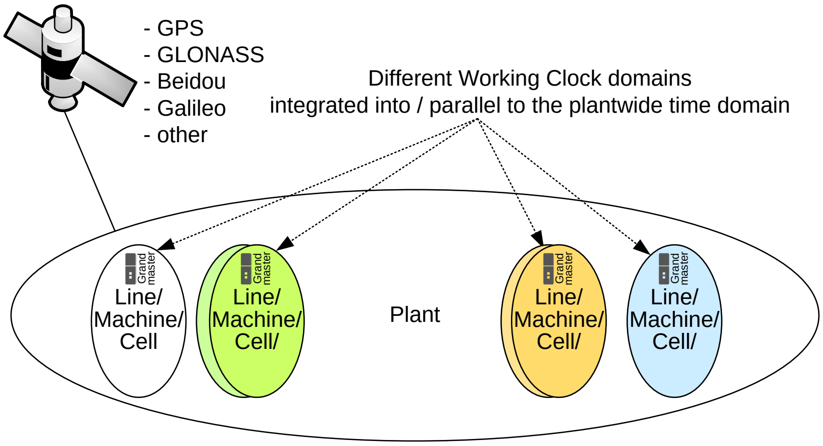


Figure 8 – line/cell/machine wide working clock synchronization overlapping with a universal time domain

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 3.1).

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 Sequence of events

Sequence of events (SOE) is a mechanism to record timestamped events from all over a plant in a common database.
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 7) 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 Redundancy

<<creator's note: Redundancy section was added.>>

2.5 Security

<<creator's note: Security section was added. What other sections are needed. As the Uses Cases are added to, this will become clearer.>>

2.6 Automotive traffic types

<<creator's note: I have moved the Use Cases section (data from presentations made at meetings/calls) into a separate major heading section below. And I moved the Automotive Traffic Types here. The Traffic Types is a very important topic that needs to be separated out. I see these use cases as the back-up material that needs to be referenced by the summary/conclusions listed here & above.>>

2.6.1 General

<<creator's note: This section has not been updated. It is unchanged from the Industrial document. This information has been left here so that readers can see the kinds of information we may need to document and how the Use Cases drive decisions here (as show via references to the appropriate Use Cases).>>

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 – 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 4 and 3.1
cyclic real-time	P	deadline/ bounded latency (e.g. n-times network cycle)/ bandwidth	bounded	up to seamless$^{1)}$	see Table 8 and 3.3
network control	S	Priority	-	up to seamless$^{1)}$ as required	see 2.2.2 and 3.7.1
audio/video	P	bounded latency/ bandwidth	bounded	up to seamless$^{1)}$ as required	-
brownfield	P	bounded latency/ bandwidth	-	up to regular$^{2)}$	see 3.7.6
alarms/ events	S	bounded latency/ bandwidth	-	up to regular$^{2)}$	see 2.3.4
configuration/ diagnostics	S	Bandwidth	-	up to regular$^{2)}$	see 3.10.1
Internal / Pass-through	S	Bandwidth	-	up to regular$^{2)}$	see 3.8.2
best effort	S	-	-	up to regular$^{2)}$	-

$^{1)}$ almost zero failover time;

$^{2)}$ larger failover time because of network re-convergence

Isochronous:

→ see section 2.3.3

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 *Use case 03: Non-Isochronous Control Loops with bounded* latency

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 07: Redundant networks*

Audio/video:

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

Brownfield:

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

Alarms/events:

→ see *Sequence of events*

Configuration/diagnostics:

→ see *Use case 29: Network monitoring and diagnostics*

Internal:

→ see *Use case 18: Pass-through Traffic*

Best effort:

→ see Use case 03: Non-Isochronous 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.

Property	Description
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) synchronized 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).

2.6.2 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.

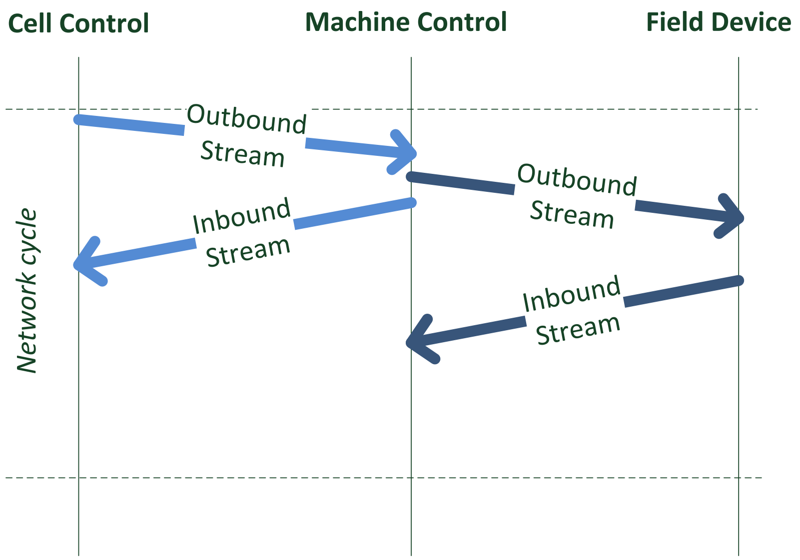


Figure 9 – Bidirectional Communication

<u>Requirements</u>:

- Support of bidirectional streams;
- Sequence of actions how to establish such streams;

<u>Useful 802.1 mechanisms:</u>

- IEEE 802.1Q (usage of streams)

2.6.3 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 3.3) network transfer quality.

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

There are 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.

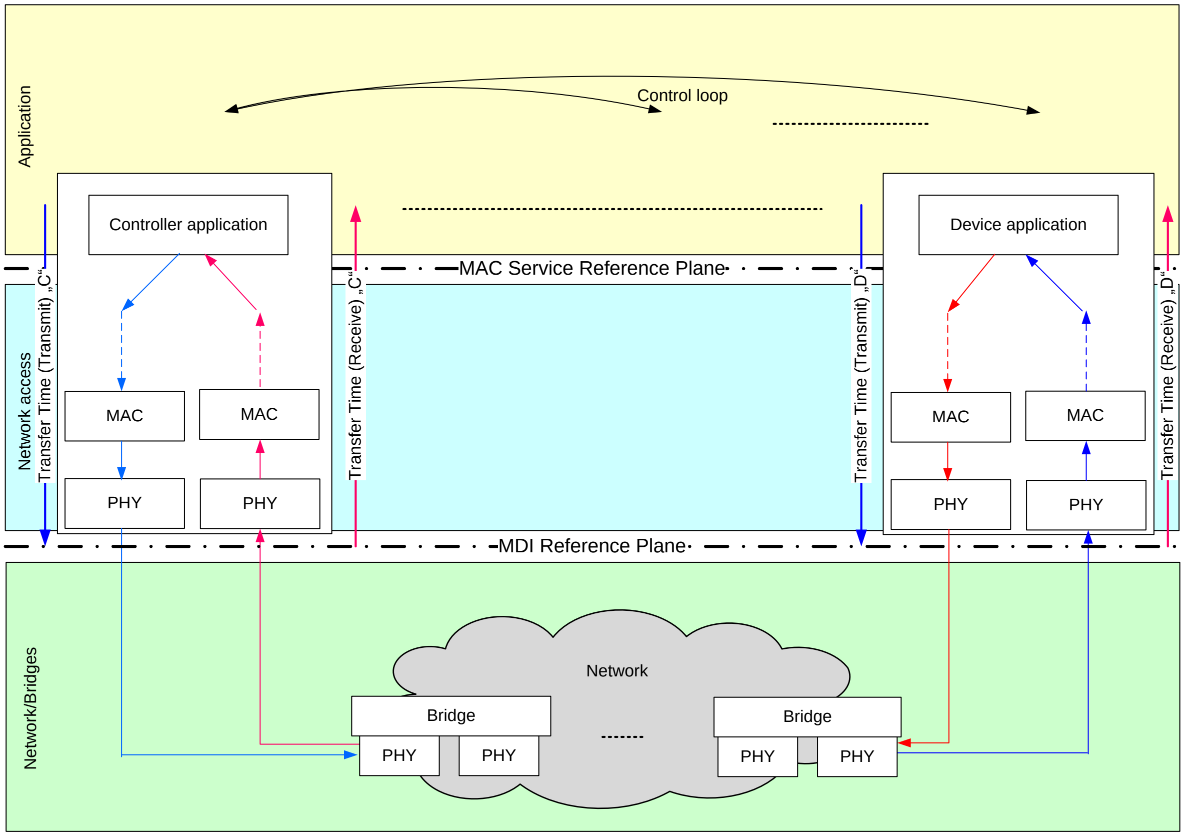


Figure 10 – Principle data flow of control loop

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 13).

Table 3 – Application types

Level	Isochronous Application		Non-isochronous Application		
Application	Synchronized to network access		Synchronized to local timescale		
Network access	Synchronized to working clock, Stream Class based scheduling, Preemption				Synchronized to local timescale, Stream Class based scheduling, Preemption
Network/Bridges	Synchronized to working clock	Free running	Synchronized to working clock	Free running	Free running
	Scheduled traffic + Strict Priority + Preemption	Strict Priority or other Shaper + Preemption	Scheduled traffic + Strict Priority + Preemption	Strict Priority or other Shaper + Preemption	Strict Priority or other Shaper + Preemption

3 Automotive modes of operation – the Use Cases

Each use case below, starts with a link to its source material (if available). The words in each use case are the interpretations of the creator of this document. It is up to the author of the source material to make sure that this interpretation is correct. If so, it will be marked as 'Reviewed by original author'.

3.1 Use case 01: Example Automotive Networks

Source material: http://www.ieee802.org/1/files/public/docs2019/dg-zinner-automotive-architecture-evolution-0319-v02.pdf <<Reviewed by original author – goes here>>

3.1.1 Traditional Model

A traditional, or present day automotive network architecture for many can makers, is shown in Figure 11. These networks typically contain a Central Gateway ECU (top box in the figure) with point-to-point communion between all the application specific ECUs. Most ECU's are connected using non-Ethernet connections such as CAN, LIN, etc.

Ethernet links are limited to only those that require higher bandwidth (shown as the bold blue lines in the figure).

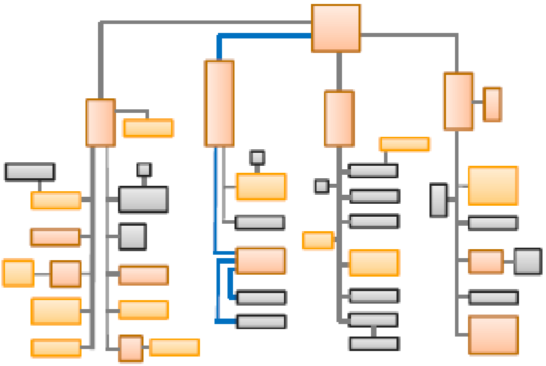


Figure 11 – Example of a Traditional or Central Gateway Automotive Network

3.1.2 Domain Model

An example of Domain automotive network architecture, is shown in Figure 12. Domain networks are the focus of many OEMs today. Ethernet is a clear enabler for these types of networks due to Ethernet's speeds and its support for the OSI Layer model.

Many OEMs want their ECU applications to communicate using IP so that the underlying physical connections are abstracted from the application. This allows a fully working ECU & application in one car model to be reused in another car model even if the underlying network is of a different speed and/or topology.

Domain networks can also work modularly. This allows a common architecture to work for full feature high-end cars, mid-range cars and low-end of a given model. For example, the ADAS ECU can be easily removed for those models that won't support autonomous driving. And/or the infotainment ECU can be scaled in quality/performance to meet the desired price point of the car.

Ethernet links can be used to connect the Domain Controllers (large top boxes in the figure) together (depending upon the link's needed bandwidth) where the figure shows possible redundancy support via the dotted line connection making a ring. Ethernet may be used more extensively below each Domain Controller as well (shown as the bold blue lines in the figure). Multiple connections to some ECU's are also shown. These connections could be for redundancy or one set of the connections could be from an ADAS ECU so that it can autonomously drive the car.

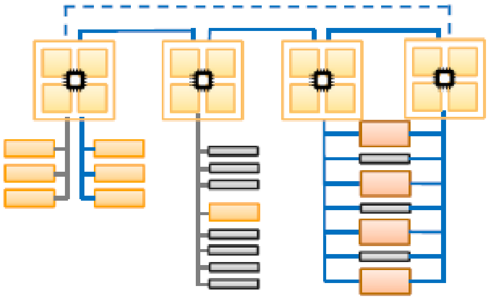


Figure 12 – Example of a Domain Automotive Network

<<creator's note: This Use Case summary is not completed yet!>>

3.1.3 Requirements from this use case (or Summary?)

<<creator's note: It is the intention that the Requirements for each Use Case will be listed at the end of each Use Case. This way it acts as a summary. This approach may need to be adjusted as this document progresses.>>

<<creator's note: From here down, this section has not been updated. It is unchanged from the Industrial Use Case document. This information has been left here so that readers can see the kinds of information we may need in the form of Use Cases.>>

3.2 Use case 02: Isochronous Control Loops with guaranteed low latency

Control loops with guaranteed low latency implement an isochronous traffic pattern for isochronous applications, which are synchronized to the network access. It is based on application cycles, which consists of an IO data Transfer time and an Application time wherein the control loop function is executed. Figure 13 shows the principle how Network cycle, Transfer time and Application time interact in this use case.

Application cycle time and Network cycle time are identical in the example of Figure 13 (RR=1/see 3.4), whereas Figure 14 shows examples where the Application cycle time is longer than the Network cycle time (RR>1/see 3.4).

The control loop function starts for controllers and devices at a fixed reference point 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 shall 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.

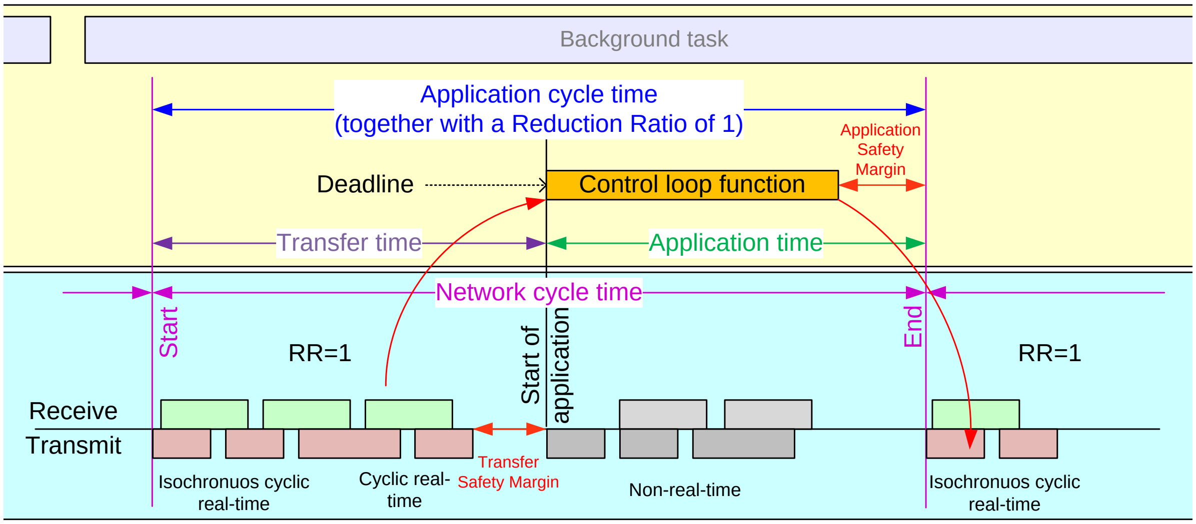


Figure 13 – network cycle and isochronous application (Basic model)

Transfer Safety Margin is the maximum time, which is needed to transfer received data from the MDI reference plane (see Transfer Time (Receive)) to the application.

Application Safety Margin is the maximum time, which is needed to transfer the produced data from the application to the MDI reference plane (see Transfer Time (Transmit)).

Figure 14 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 3.4), 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 14).

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 cyclic background task can additionally run, whenever spare Transfer or Application time is available.

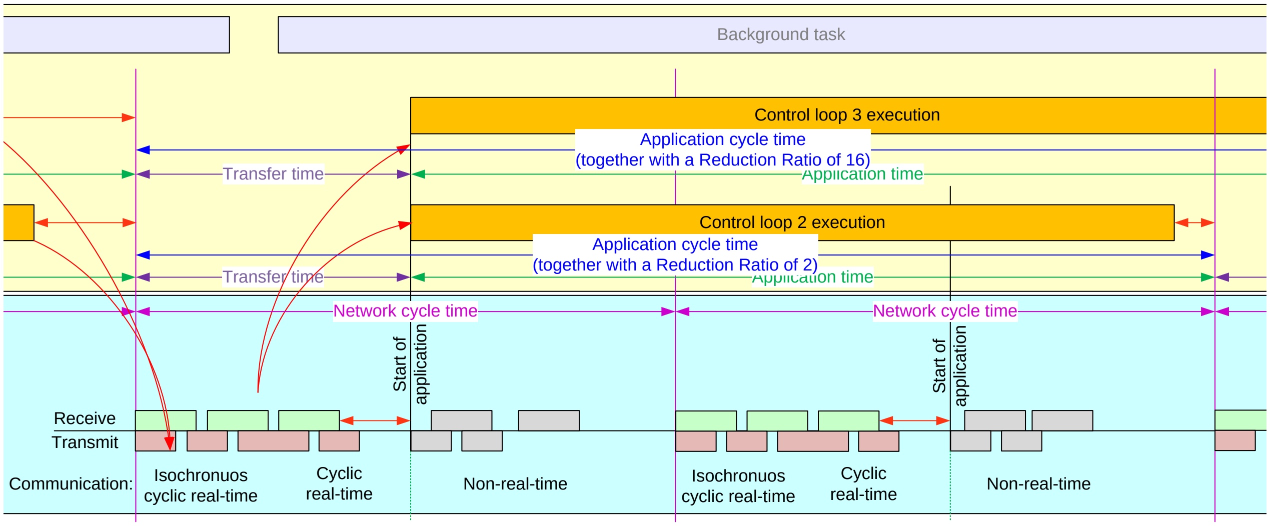


Figure 14 – Multiple concurrent isochronous control loops (Extended model)

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-, MAC-, cable-, 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-, cable- and bridge-delay contributions.

Figure 15 to Figure 20 show variations of the basic model of Figure 13:

In existing technologies some of the models are used in optimized ways to reduce the network cycle time and/or the IO-reaction time (sometimes also called ’makespan’ or ‘roundtrip delay time’).

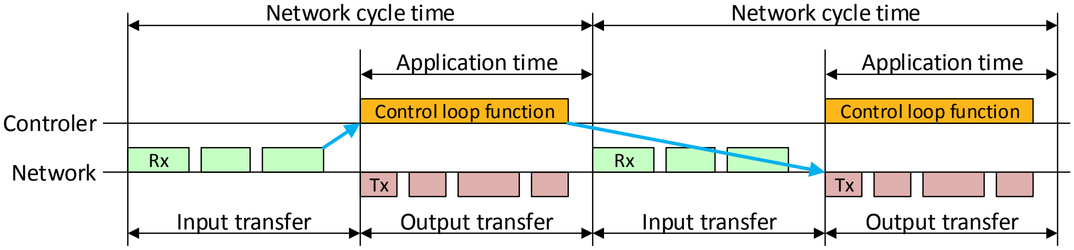


Figure 15 – Variation 1: two cycle timing model

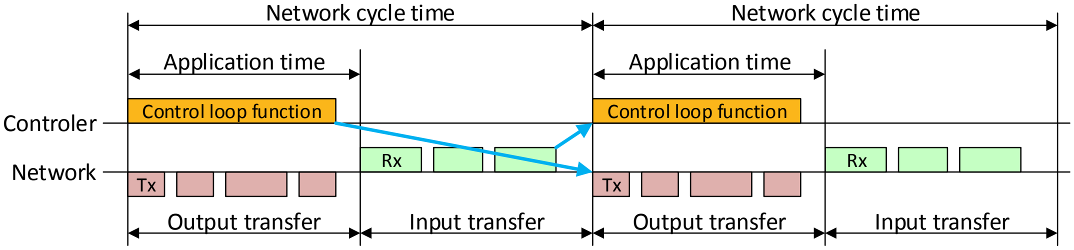


Figure 16 – Variation 2: two cycle timing model - shifted by 180°

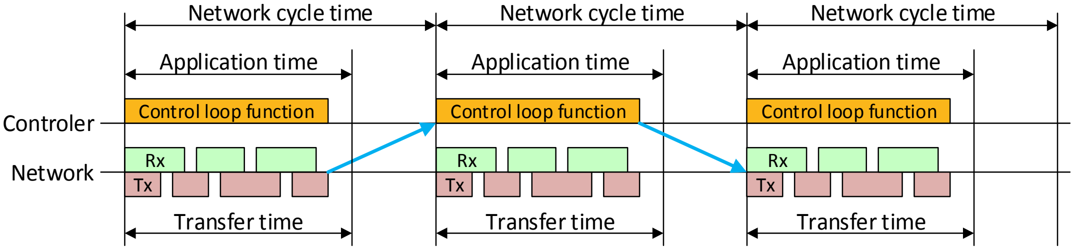


Figure 17 – Variation 3: three cycle timing model

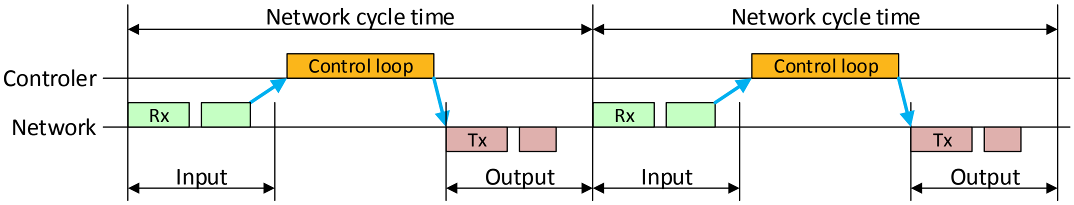


Figure 18 – Variation 4: one cycle timing model

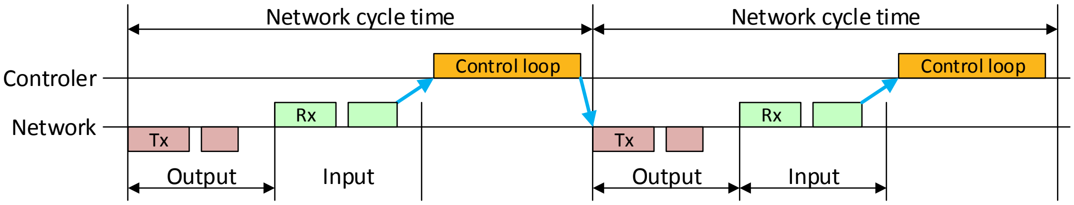


Figure 19 – Variation 5: one cycle timing model – changed sequence

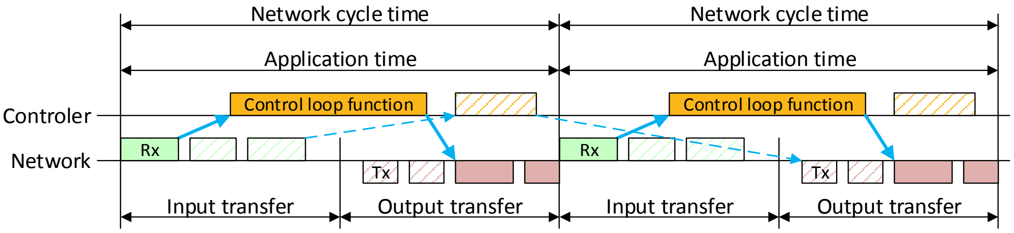


Figure 20 – Variation 6: further optimizations

The extended model of Figure 14 may be applied to these variations as well.

3.2.1.1 Isochronous cyclic operation model

Figure 21 shows the isochronous cyclic operation model for guaranteed low latency.

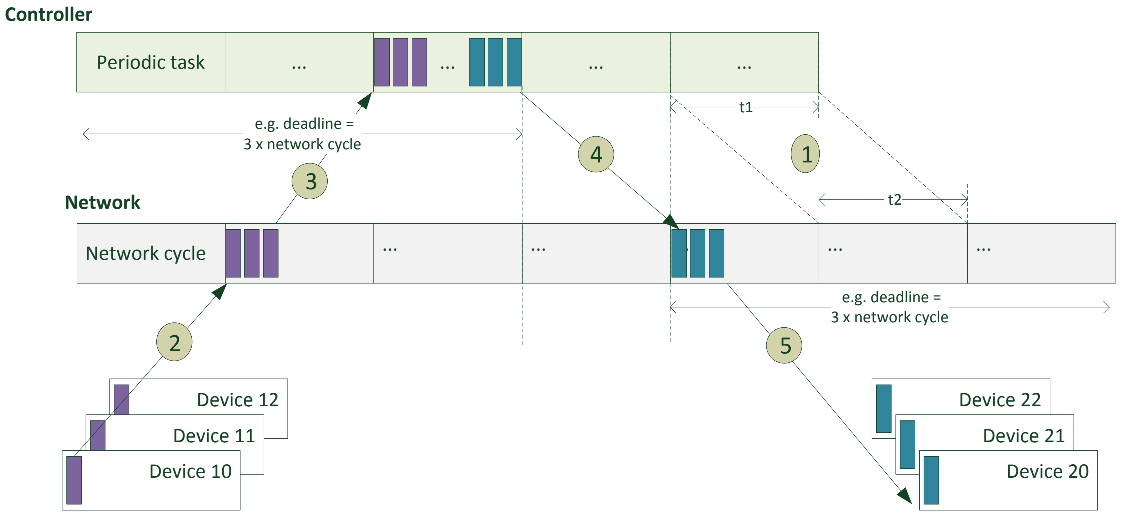


Figure 21 – isochronous cyclic operation model

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 shall 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 shall 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 shall 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 shall 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.

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

<u>isochronous cyclic real-time</u>: transfer time less than 20% (at link speeds > 100 Mbit/s) / 50% (at link speeds <= 100 Mbit/s) of network cycle and applications are coupled to the working clock.

Table 4 – isochronous traffic pattern properties

Characteristics		Notes
Data transmission scheme	periodic	
Data transmission constraints	deadline	End-to-end one-way latency[2] less than 20% (link speeds > 100 Mbit/s) / 50% (link speeds <= 100 Mbit/s) of network cycle
Data period	1µs .. 1ms 250µs ..4ms	
Network access (data transmission) synchronized to working clock network cycle	Yes	
Application synchronized to network access	Yes	
Acceptable jitter	n.a.	Deadline shall be kept

---

[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-2018).

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

<u>Requirements on network cycle times</u>:

– 1 µs to 1 ms	at link speed 1 Gbit/s (or higher)
– 250 µs to 4 ms	at link speed 100 Mbit/s
– 2 ms to 8 ms	at link speed 10 Mbit/s

3.2.1.2 Delay requirements

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 5.
- MAC delays shall meet the upper limits of Table 6.
- Bridge delays shall be independent from the frame size and meet the upper limits of Table 7.

Figure 22 shows the definition of PHY delay, MAC delay and Bridge delay reference points.

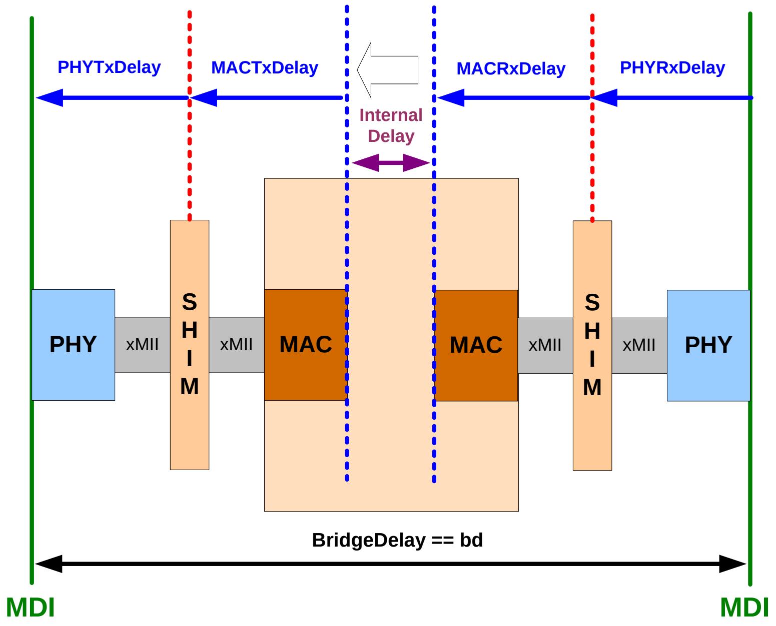


Figure 22 – delay measurement reference points

Strict numbers such as those proposed hereafter in Table 5, Table 6 and Table 7 are necessary to approach the problem of short control loop times. The numbers have to be agreed on in the profile. Specifying these numbers, however, doesn't eliminate the need to publish exact values through 802.1 standardized mechanisms as applicable.

Table 5 – 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	tdb	tdb
25 Gbit/s to 1 Tbit/s	tdb	tdb	tdb

[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 6 – 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	tdb	tdb

Table 7 – 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)
1 Gbit/s	< 1 µs	Bridge delay measure from RGMII to RGMII 1)
2,5 Gbit/s	< 1 µs	Bridge delay measure from XGMII to XGMII 1)
5 Gbit/s	< 1 µs	Bridge delay measure from XGMII to XGMII 1)
10 Gbit/s	< 1 µs	Bridge delay measure from XGMII to XGMII 1)
25 Gbit/s – 1 Tbit/s:	tdb	Bridge delay measure from XGMII to XGMII 1)

1) first bit in, first bit out

<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 3.7.11.4 *“Fast” process applications*.

3.3 Use case 03: Non-Isochronous Control Loops with bounded latency

Control loops with bounded latency implement a cyclic traffic pattern for non-isochronous applications, which are not synchronized to the network access but are synchronized to a local timescale.

Figure 23 shows the principle how network cycle, transfer time and application time interact in this use case. The control loop function starts at an application defined time, which is not synchronized to the network access but to a local timescale. The network cycle, which describes the repetitive behavior of the network interface, may be synchronized to a common working clock or to a local timescale.

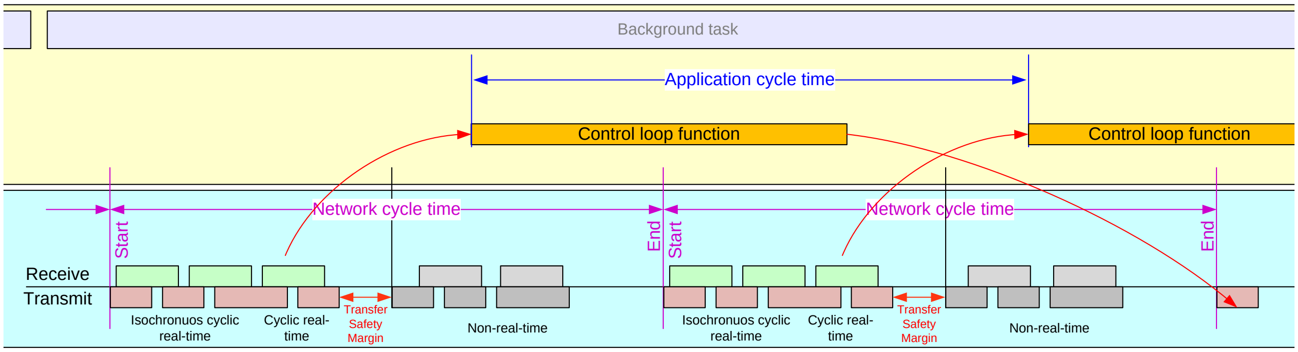


Figure 23 – network cycle and non-isochronous application (Basic model)

Extensions of this model analogous to Figure 14 (multiple applications with differing application lengths) are also possible.

3.3.1.1 Cyclic operation model

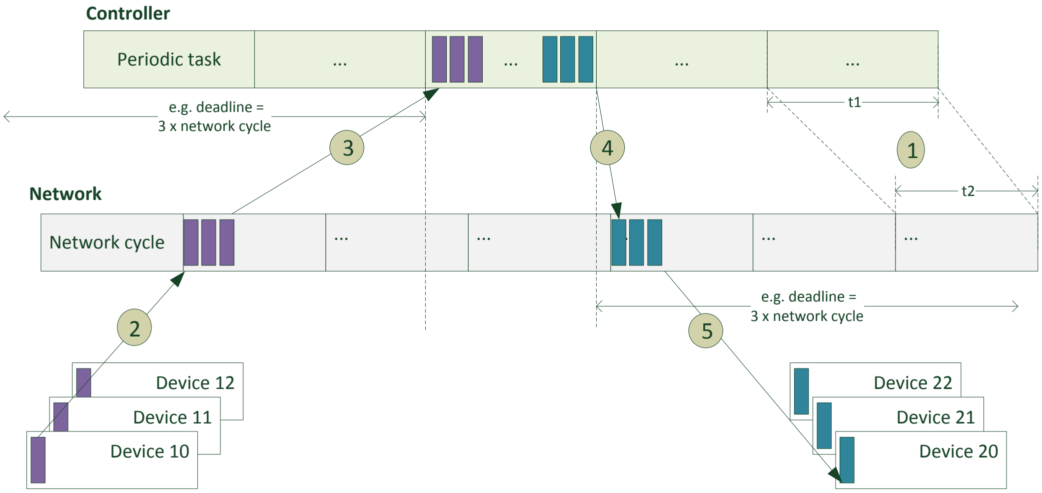


Figure 24 – cyclic operation model

Cyclic operation characteristics:

Multiple applications with different application periods are supported.
Applications synchronized to a common working clock or a local timescale:

- Devices: √
- Controller: √

Multiple update times based on different reduction ratios are supported.
Network access 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 shall 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 shall 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.

3.3.1.2 Cyclic traffic pattern

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

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

Table 8 – cyclic traffic pattern properties

Characteristics		Notes
Data transmission scheme	periodic	
Data transmission constraints	deadline	End-to-end one-way latency[3] less than X * network cycle (X | 1 .. n)
Data period	X * network cycle (X | 1 .. n)	
Network access (data transmission) synchronized to working clock (network cycle)	Optional	May be synchronized to local timescale instead
Application synchronized to network access	No	synchronized to local timescale
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 bytes)	Data size negotiated during connection establishment

---

[3] 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-2018).

Requirements:

3.4 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

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

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

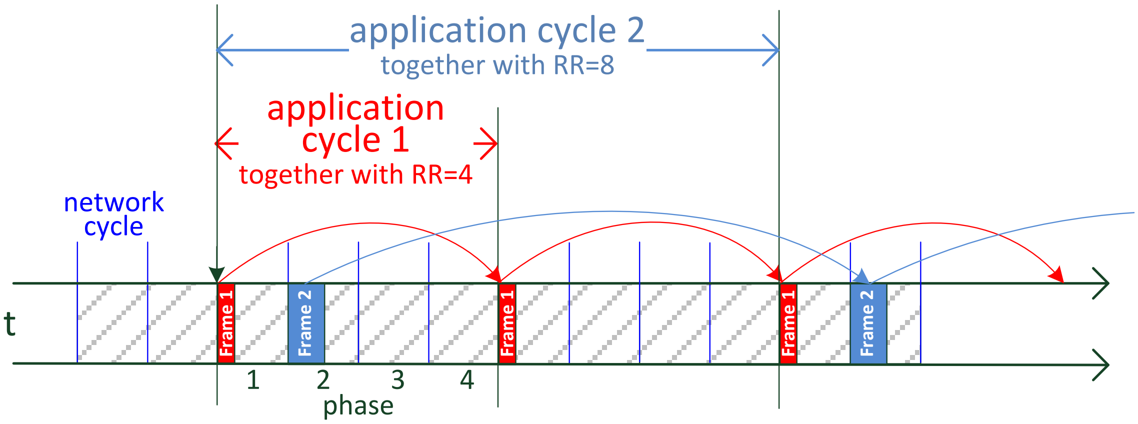


Figure 25 – network cycle and application cycle

Use case 06: Drives without common application cycle but common network cycle is an example of multiple different application cycles, which are based on a common network cycle.

Figure 26 shows another example use case where all drives are connected in a line and every drive needs direct data exchange to the Controller and additionally to its direct neighbor. Some similar applications might even be more complex when the physical topology does not match the logical order of drives.

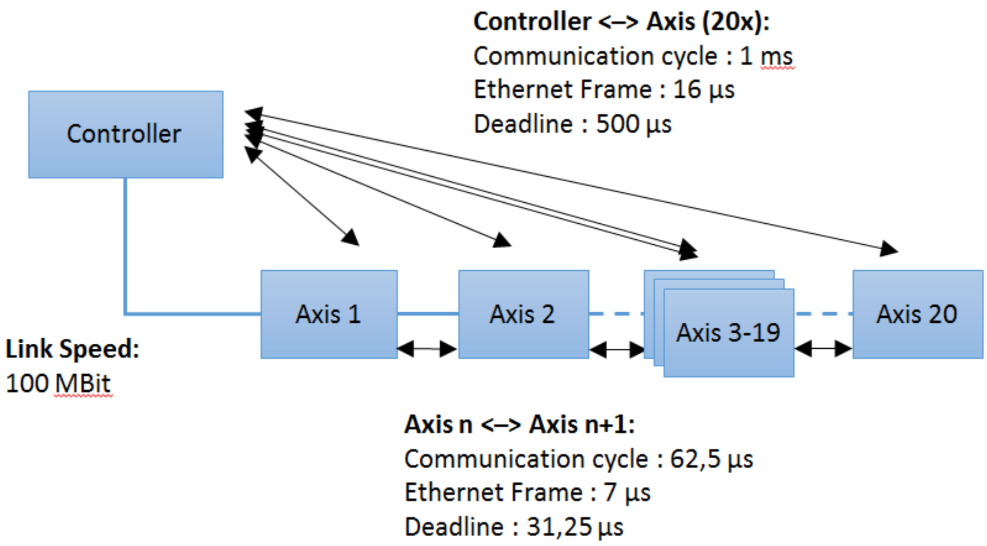


Figure 26 – isochronous drive synchronization

Requirements:

…

Useful 802.1 mechanisms:

- …

3.5 Use case 05: Drives without common application cycle

3.5.1.1 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 27 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 shall 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.

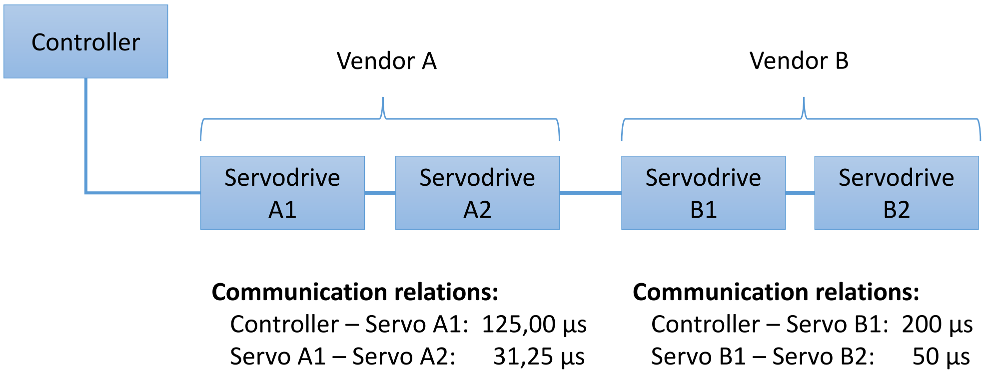


Figure 27 – network with different application cycles

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
- …

3.5.1.2 Controller communication

The Usecase concentrates on the communication between the devices A1 and B1, and the Controller as shown in Figure 28. Nevertheless the communication between A1/A2 and B1/B2 has to be solved as well.

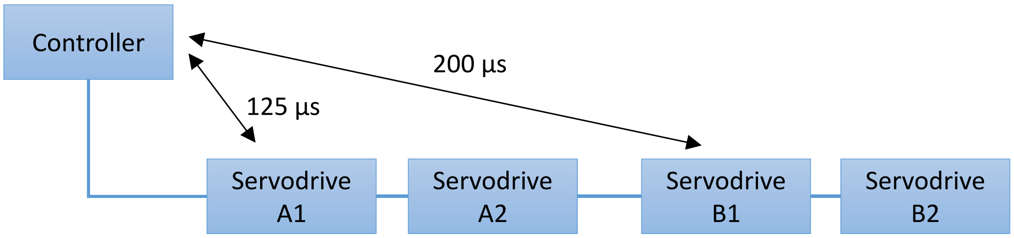


Figure 28 – Multivendor Motion – Controller communication

3.5.1.3 Timing Requirements

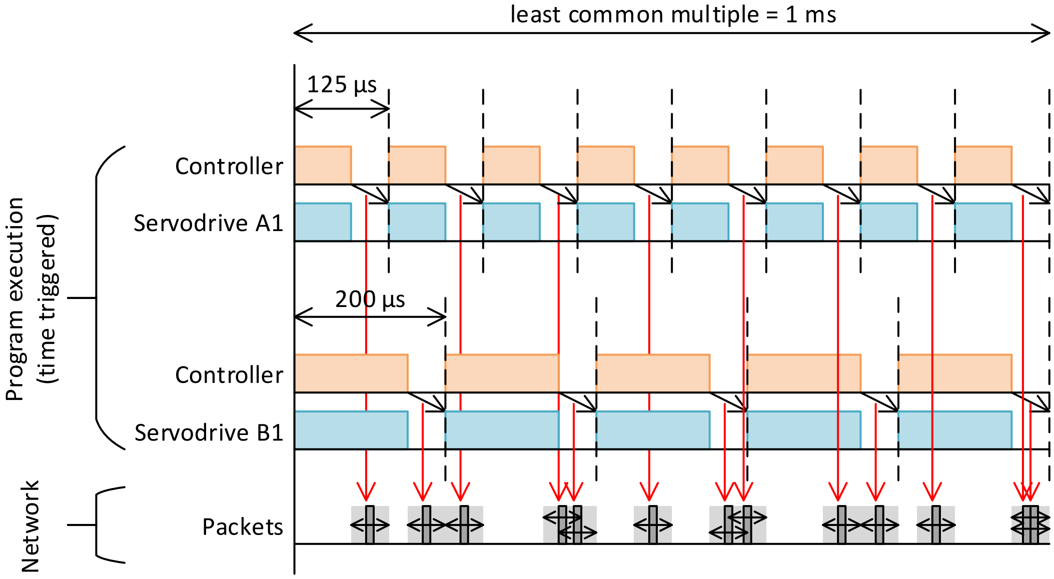


Figure 29 – Multivendor Motion – Timing Requirements

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.

3.6 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 8 for motor speed control loop,
- 1 ms, i.e. reduction ratio 32 for position control loop,
- 16 ms, i.e. reduction ratio 512 for remote IO.

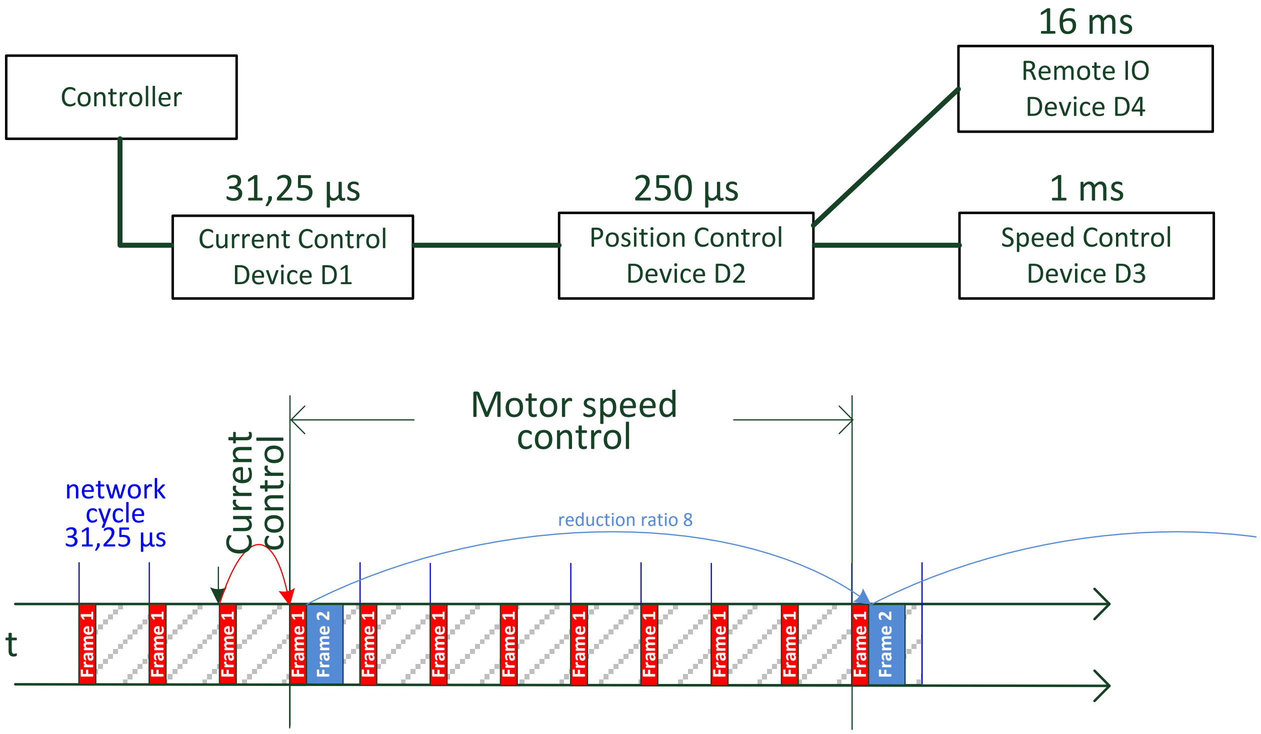


Figure 30 – different application cycles but common network cycle

3.7 Industrial automation networks

3.7.1 Use case 07: Redundant networks

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

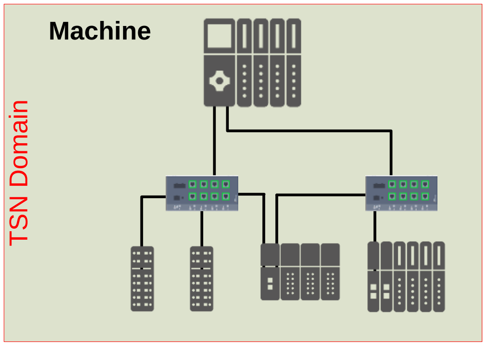


Figure 31 – ring topology

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 32):

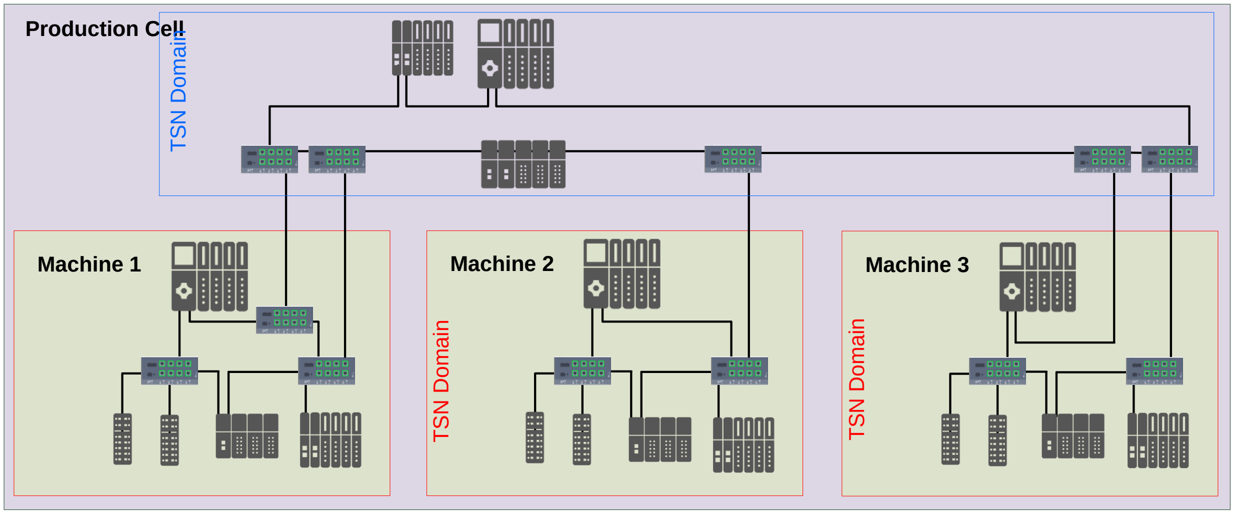


Figure 32 – connection of rings

<u>Requirement</u>:

Support redundant topologies with rings.

<u>Useful 802.1 mechanisms:</u>

- …

3.7.2 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.

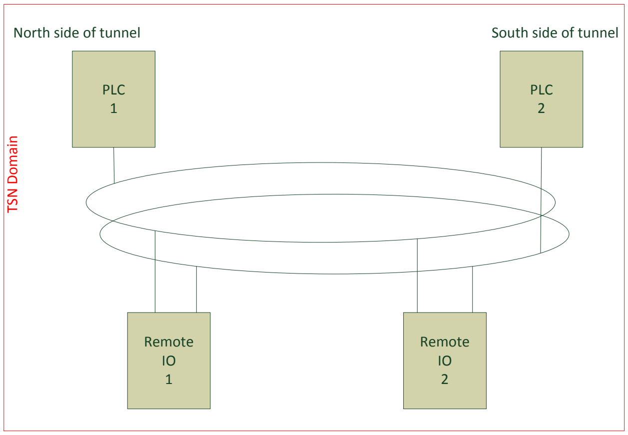


Figure 33 – example topology for tunnel control

Tunnel control may also include video surveillance as parallel application on the same network, replacing dedicated analogue CCTV systems. This includes image processing applications like speed section control, detecting lost cargo or traffic in wrong direction with minimized detection time.

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
- …

3.7.3 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 ITU/3GPP (5G). Even functional safety applications over wireless connections are supported (see Use case 25: Functional safety).

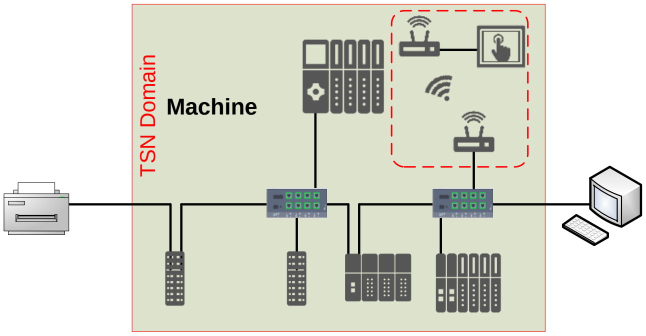


Figure 34 – HMI wireless connected using cyclic real-time

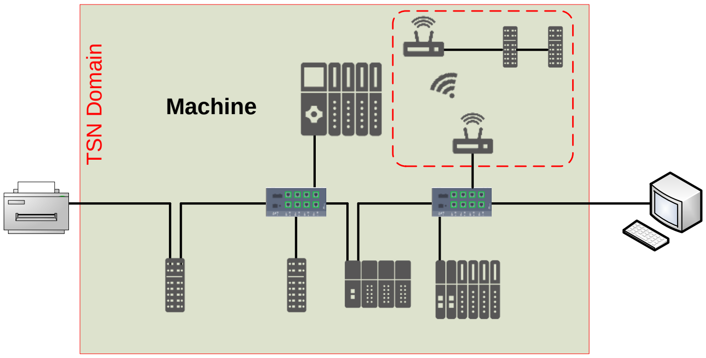


Figure 35 – Remote IO wireless connected using cyclic real-time

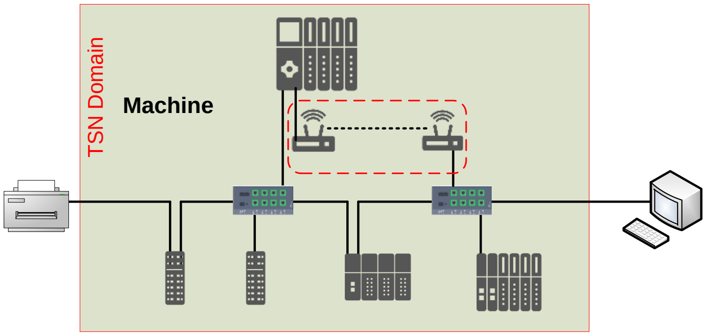


Figure 36 – Ring segment wireless connected for media redundancy

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:

- …

3.7.4 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.

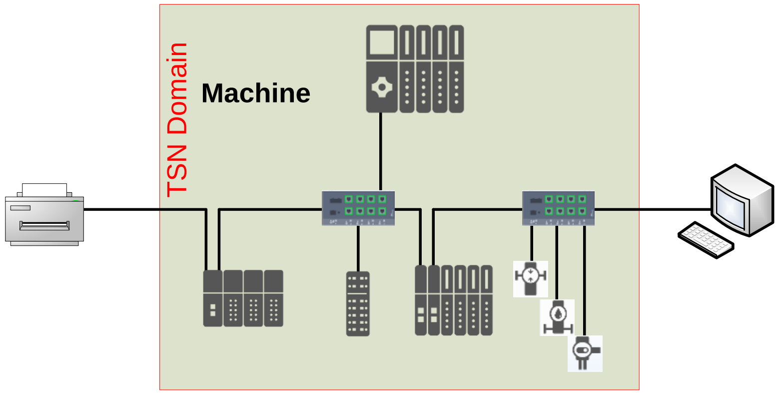


Figure 37 – Ethernet sensors

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:

- …

3.7.5 Use case 11: Fieldbus gateway

Gateways are used to integrate non-Ethernet and Ethernet-based fieldbusses into TSN domains.

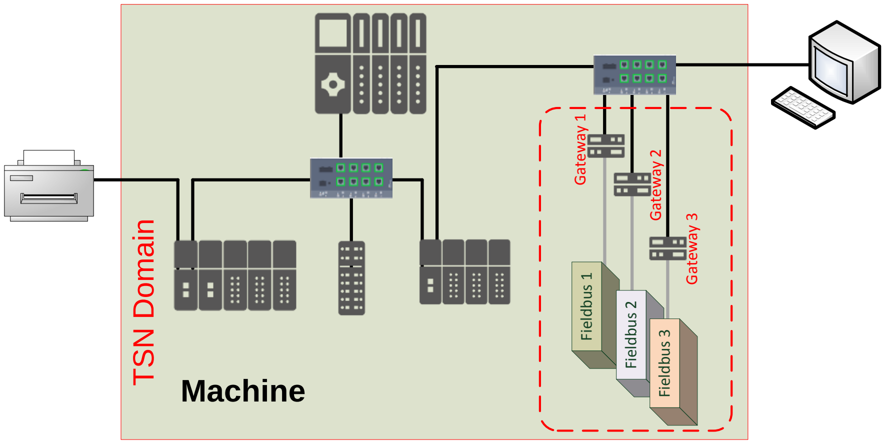


Figure 38 – fieldbus gateways

Many systems have at least one merging unit (e.g gateway, multiplexer) between the sensors and actuators assigned to a single machine control. The clustering is typically done with some infrastructure elements (slices) that require a backplane communication. The fieldbus communication is in many cases the third level of communication. Thus, it is assumed that TSN is not the first communication network between the sensors/actuators and a machine control unit. This means that TSN should be capable to adapt an existing communication infrastructure regardless of the size of those networks. The networks behind a gateway have their own timing constraints. A machine level network may take into account that the lower level networks e.g. behind a gateway have their own local timing. The timing of a TSN network has impact to sub-ordinated structures. An optimal timing requires taking into account the gateway behavior for the TSN configuration (see Figure 39).

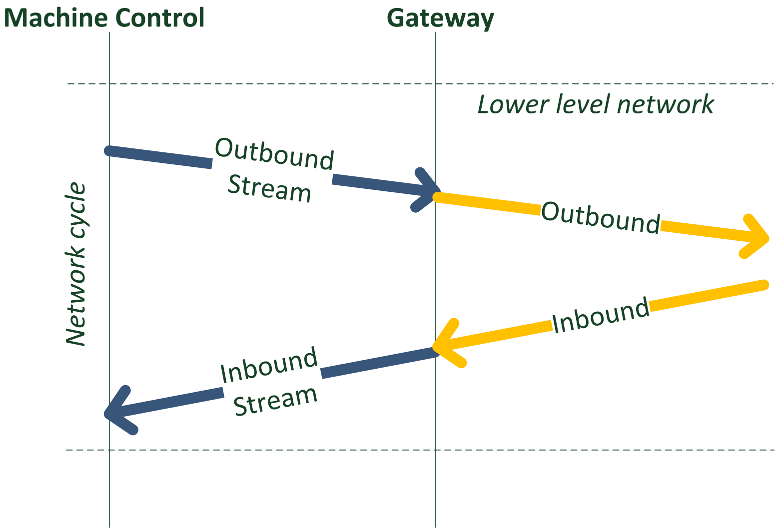


Figure 39 – Embedded non TSN communication

Requirement:

- Support of non-Ethernet and Ethernet-based fieldbus devices via gateways either transparent or hidden;

- TSN scheduling may need configuration to meet the requirements of subordinate systems;

3.7.6 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 40 gives an example of a machine with brownfield devices.

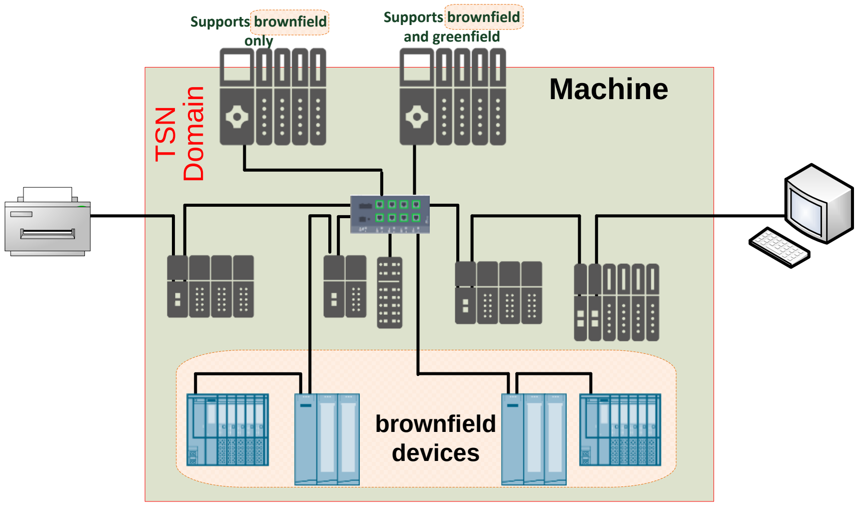


Figure 40 – New machine with brownfield devices

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.

Figure 41 shows a different use case where a TSN machine is attached to an existing brownfield machine. In this case only non-TSN traffic is possible between the two machines.

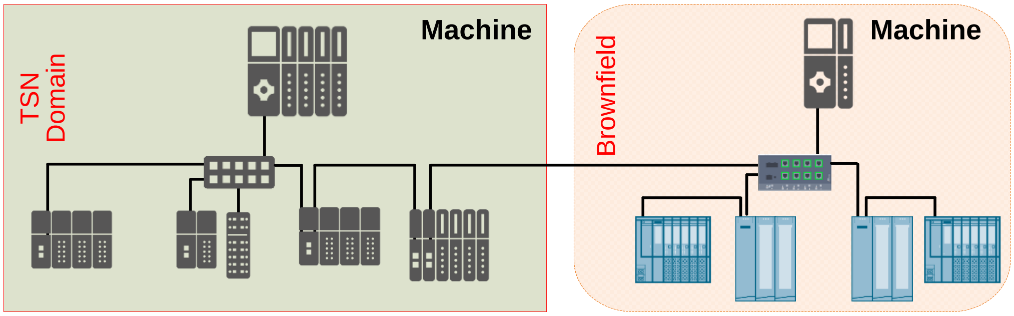


Figure 41 – Add TSN machine to brownfield machine

3.7.7 Use case 13: Mixed link speeds

Industrial use cases refer to link speeds, as shown in Table 9, 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 9 – 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.
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 42 and Figure 43 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 a 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.

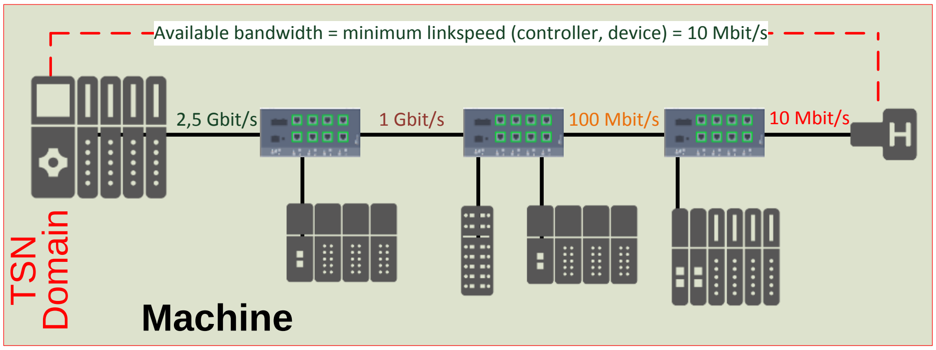


Figure 42 – mixed link speeds

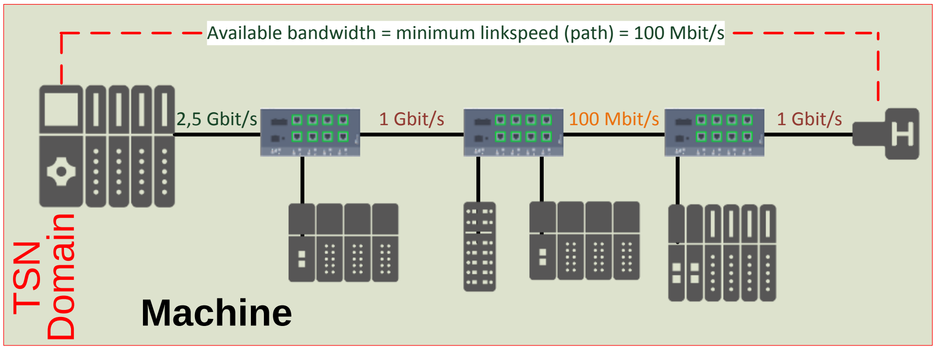


Figure 43 – mixed link speeds without topology guideline

<u>Requirement</u>:

Links with different link speeds as shown in Figure 42 share the same TSN-IA profile based communication system at the same time.
Links with different link speeds without topology guideline (Figure 43) may be supported.

<u>Useful 802.1 mechanisms:</u>

- …

3.7.8 Use case 14: Multiple isochronous domains

Figure 44 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.

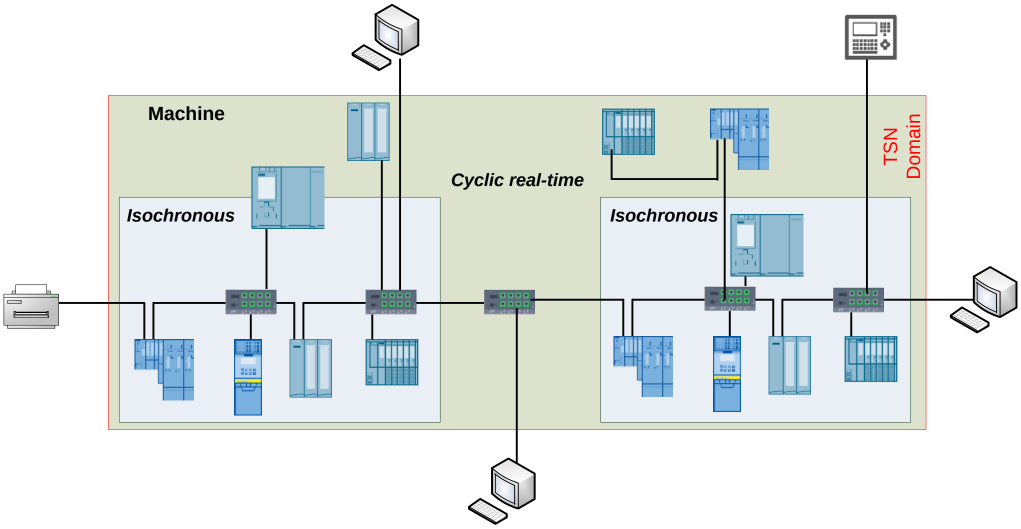


Figure 44 – multiple isochronous domains

Some kind of coupling (e.g. shared synchronization) between the isochronous domains / Working Clocks may be used (see Figure 45).
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.

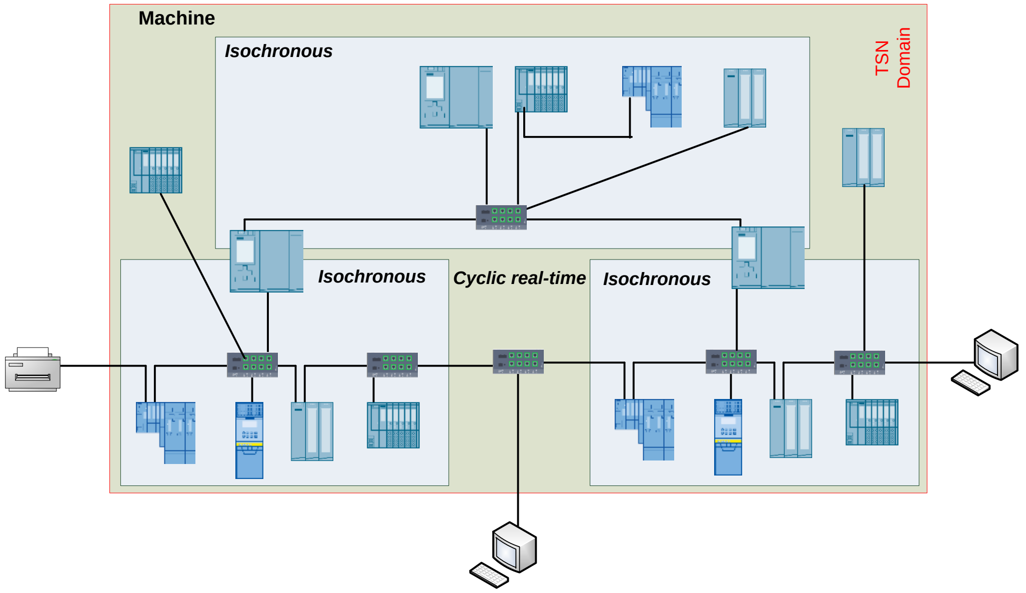


Figure 45 – multiple isochronous domains - coupled

Requirements:

Isochronous real-time domains may run independently, loosely coupled (start of network cycle is synchronized) or tightly coupled (shared working clock). 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,
- ...

3.7.9 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.

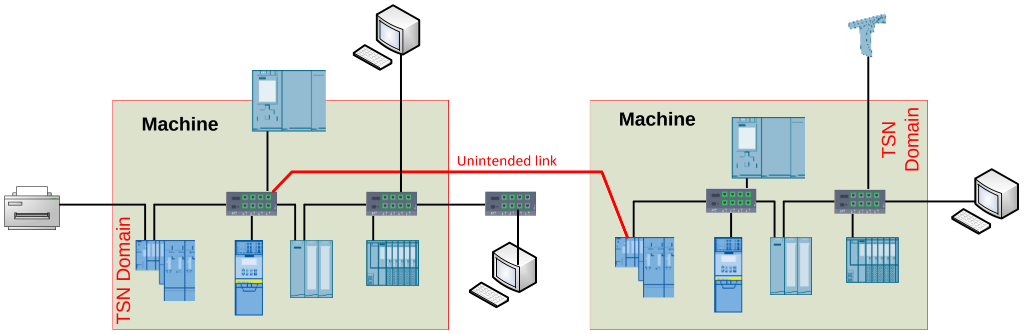


Figure 46 – Auto domain protection

Requirement:

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

Useful 802.1Q mechanisms:

- Priority regeneration
- …

3.7.10 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]

Further representative examples of required quantities are provided in 3.7.11.1 and 3.7.11.2.

Requirement:

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.

Useful 802.1 mechanisms:

- …

3.7.11 Minimum required quantities

3.7.11.1 A representative example for VLAN requirements

Figure 47 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 47.

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 real-time streams
❹	Cyclic RT „R”	VLAN for redundant cyclic real-time streams
❺	Isochronous cyclic RT 1	VLAN for isochronous cyclic real-time streams
❻	Isochronous cyclic RT 1 „R”	VLAN for redundant isochronous cyclic real-time streams
❼	Isochronous cyclic RT 2[4]	VLAN for isochronous cyclic real-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

---

[4] The isochronous cyclic RT 2 „R“ is not applied in this example but can be made available additionally

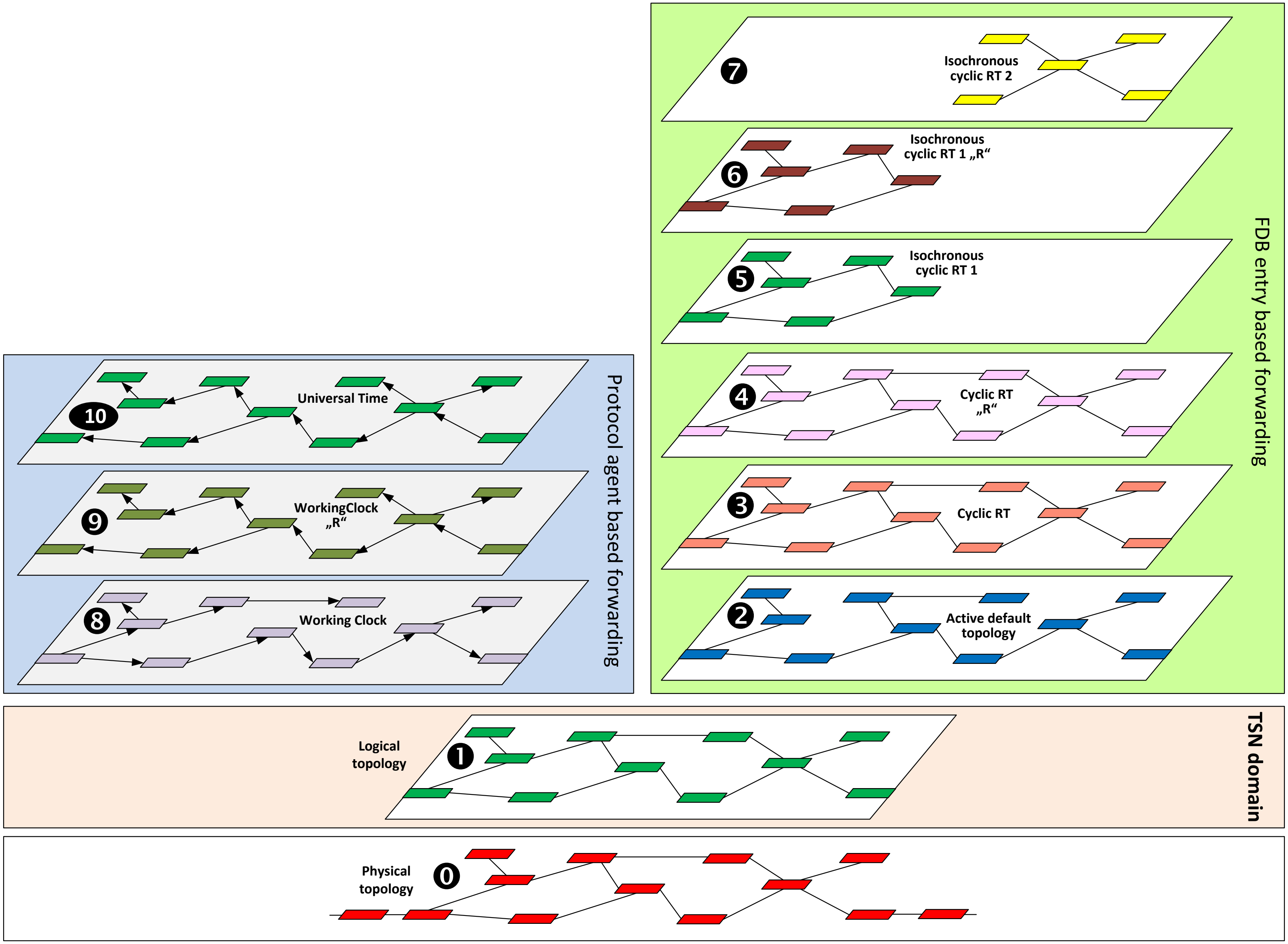

7
Isochronous cyclic RT 2
6
Isochronous cyclic RT 1 „R“
5
Isochronous cyclic RT 1
4
Cyclic RT „R“
3
Cyclic RT
2
Active default topology
FDB entry based forwarding
10
Universal Time
9
WorkingClock „R“
8
Working Clock
Protocol agent based forwarding
Logical topology
1
TSN domain
Physical topology
0

Figure 47 – 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 10 and Table 11.

Table 10 may be implemented as FDB table with a portion of DA-MAC address (e.g. 12 bits of Identifier and TSN-IA profile OUI) as row and the VLANs as column to ensure availability of a dedicated entry.

Table 10 – 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 1024 together with the 50% saturation due to hash usage rule. Table 11 shows the expected number of possible FDB entries.

Table 11 – 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 12.

Table 12 – Neighborhood for hashed entries

Neighborhood	Usage
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.

3.7.11.2 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; 1024 producer and 1024 consumer data flows in case of seamless redundancy.
  - 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; 4 producer and 4 consumer data flows in case of seamless redundancy.
  - 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; 128 producer and 128 consumer data flows in case of seamless redundancy.
  - 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.

3.7.11.3 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

3.7.11.4 “Fast” process applications

The structure shown in **Error! Reference source not found.** applies. Figure 48 provides a logic station view.

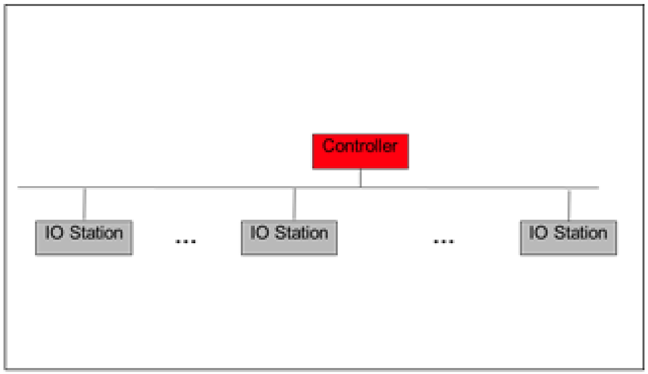


Figure 48 – Logical communication concept for fast process applications

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)

3.7.11.5 Server consolidation

The structure shown in **Error! Reference source not found.** applies. Figure 49 provides a logic station view.

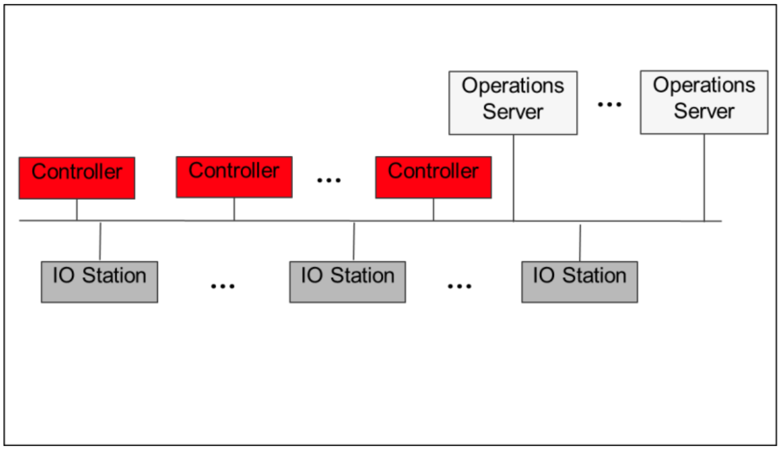


Figure 49 – Server consolidated logical connectivity

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

3.7.11.6 Direct client access

The structure shown in **Error! Reference source not found.** applies. Figure 50 provides a logic station view.

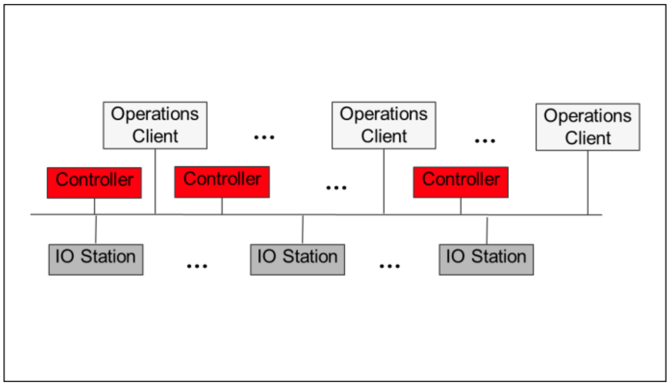


Figure 50 – Clients logical connectivity view

Data access to Operations Functionalities directly by Clients

- Max 20 direct access clients

Data subscriptions (vertical):

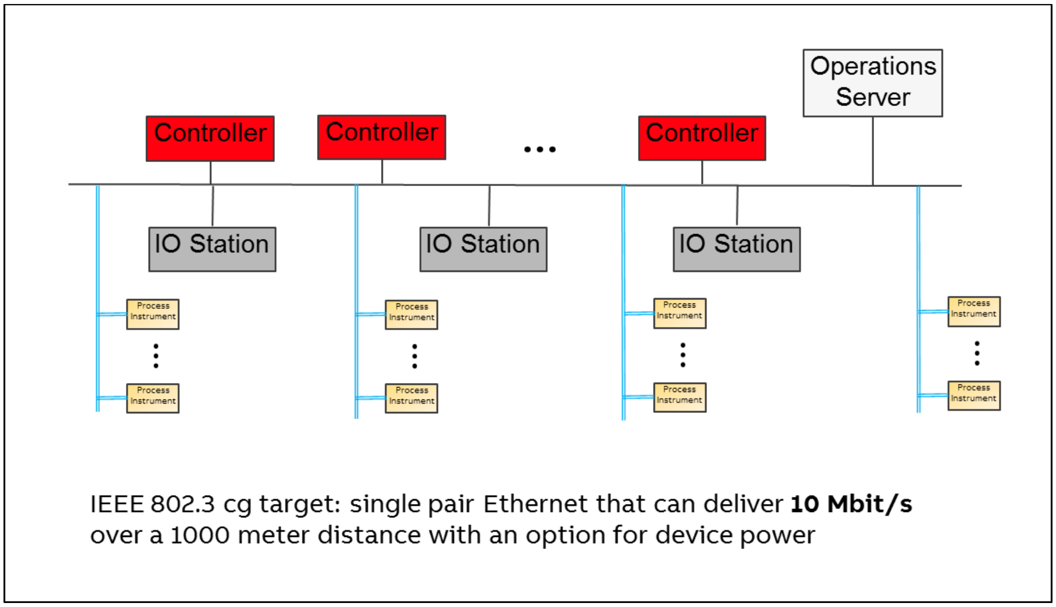
- Up to 3000 subscribed items per client
- 1s update rate
- Worst case 60000 items/second per controller in classical Client/Server setup
- 50% analog items -> 30% change every sec

Different physical topologies

- Rings, stars, redundancy

3.7.11.7 Field devices

The structure shown in **Error! Reference source not found.** applies. Figure 51 provides a logic station view.



IEEE 802.3 cg target: single pair Ethernet that can deliver **10 Mbit/s** over a 1000 meter distance with an option for device power

Figure 51 – 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

3.7.12 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. These 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.

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

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 13, Table 14, Table 15, and Table 16 shows the resulting values for different link speeds and fully utilized links.

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 13 – 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 14 – 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 15 – 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.

# of ports	MinimumFrameMemory [KBytes]	Comment
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 16 – 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 reduces 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 management”:

100 Mbit/s, 2 Ports, and 6 queues
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 its local bridge resources. Local network access shall conform to the TSN-IA profile defined model with management defined limits and cycle times (see e.g. row Data period in Table 4).

3.8 Industrial automation machines, production cells, production lines

3.8.1 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 Operations Control HMI (with its own TSN domain).

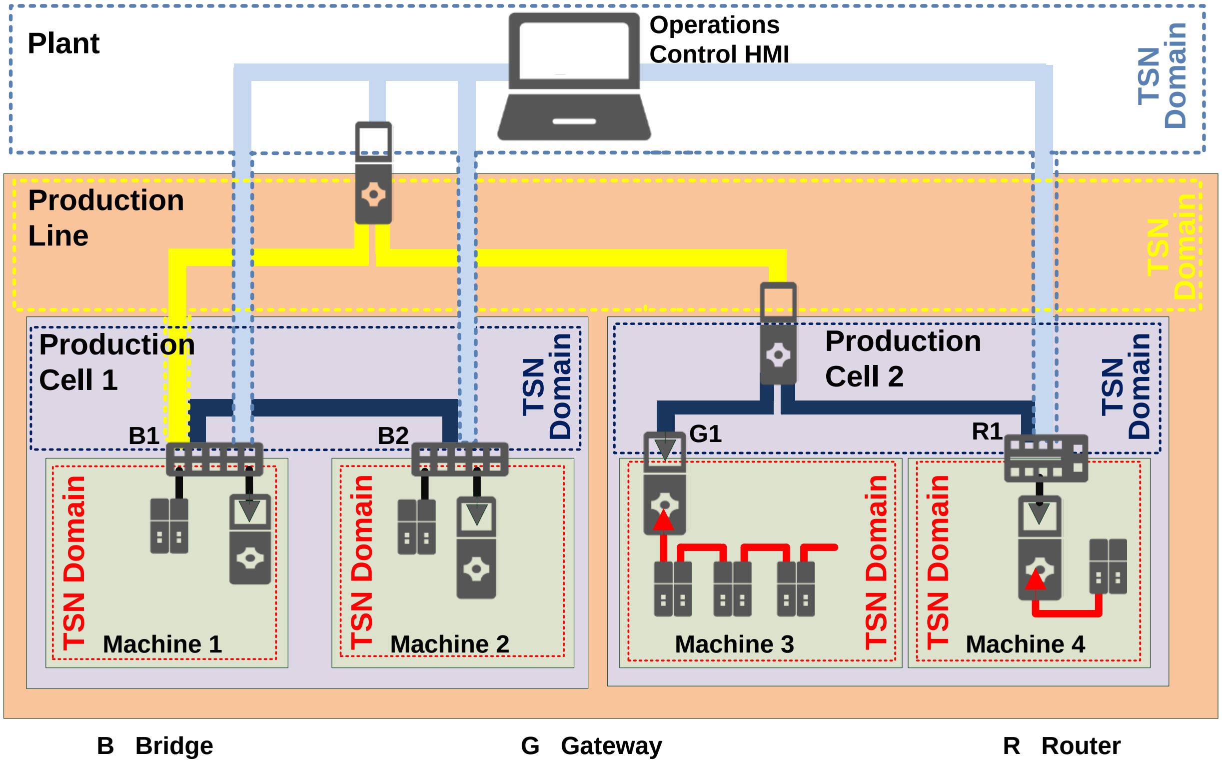


Figure 52 – M2M/C2C between TSN domains

Figure 52 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>:

1225

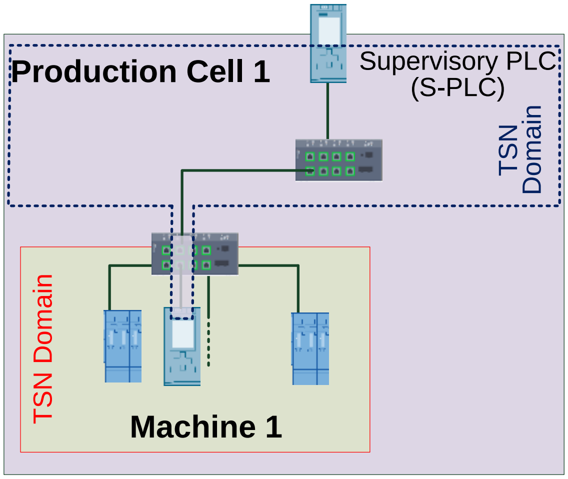


Figure 53 gives an example of M2M communication to a supervisory PLC.

Figure 54 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 53 – 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 55 shows an example where M2M communication is used to connect a PC for diagnostics/monitoring.

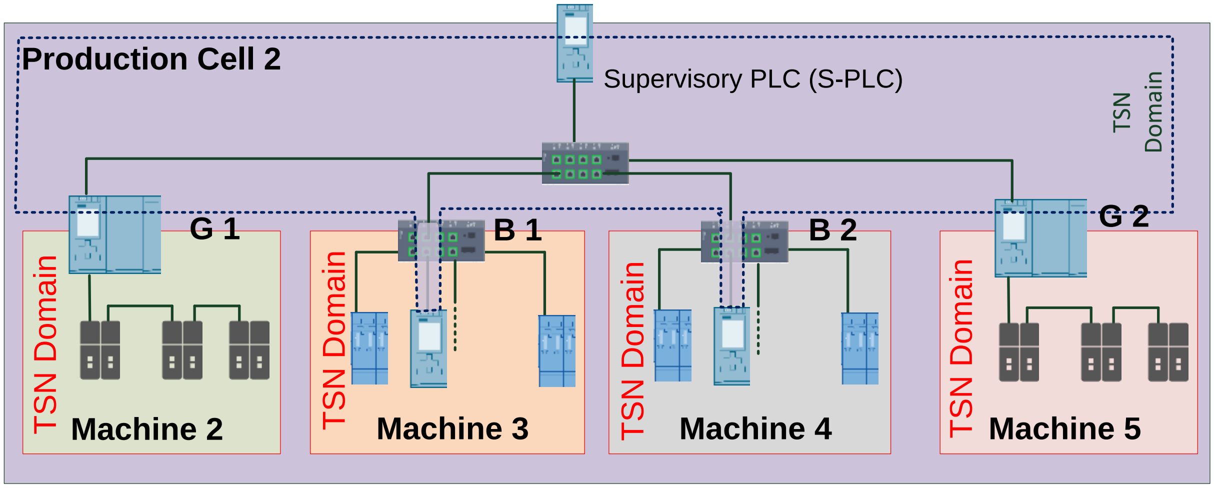


Figure 54 – M2M with four machines

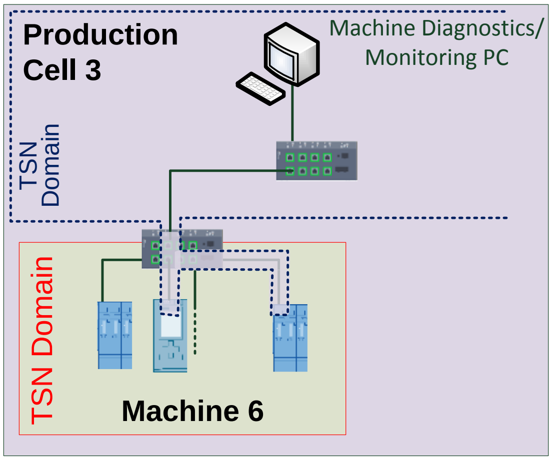


Figure 55 – M2M with diagnostics/monitoring PC

Figure 55 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 54 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.

3.8.2 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 56, Figure 57 and Figure 58 give some examples of pass-through traffic installations in industrial automation.

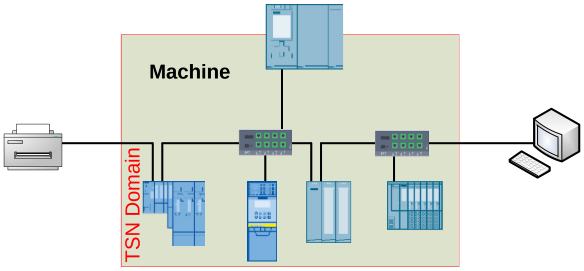


Figure 56 – pass-through one machine

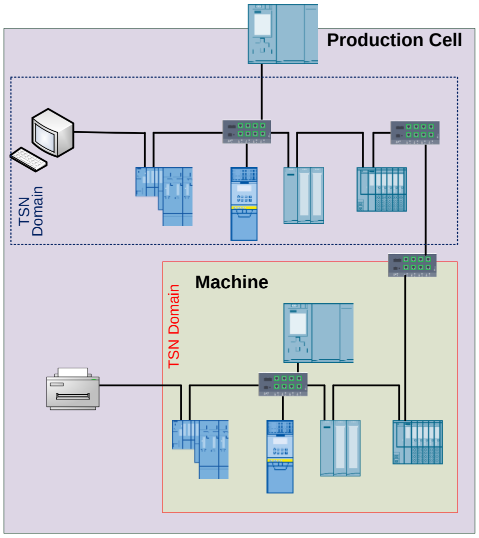


Figure 57 – pass-through one machine and production cell

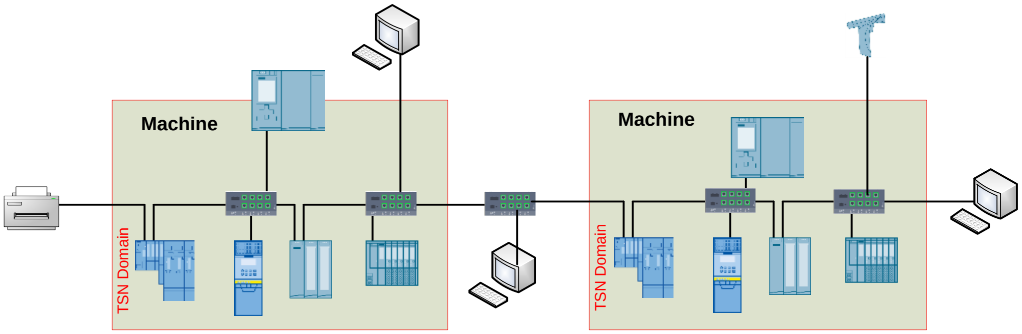


Figure 58 – pass-through two machines

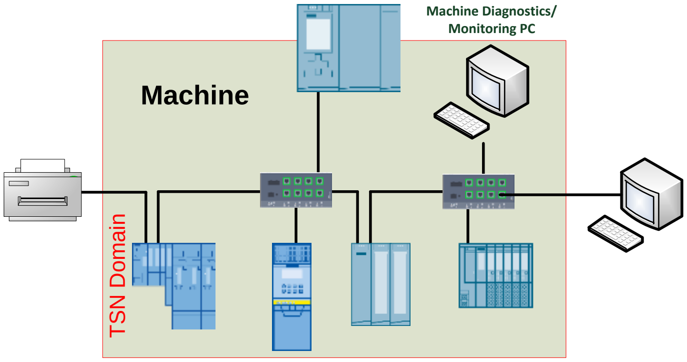


Figure 59 – machine with diagnostics / monitoring PC

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.

3.8.3 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 60 may have relaxed latency requirements, but the machine in Figure 61 needs to work with very high speed and thus has very demanding latency requirements.

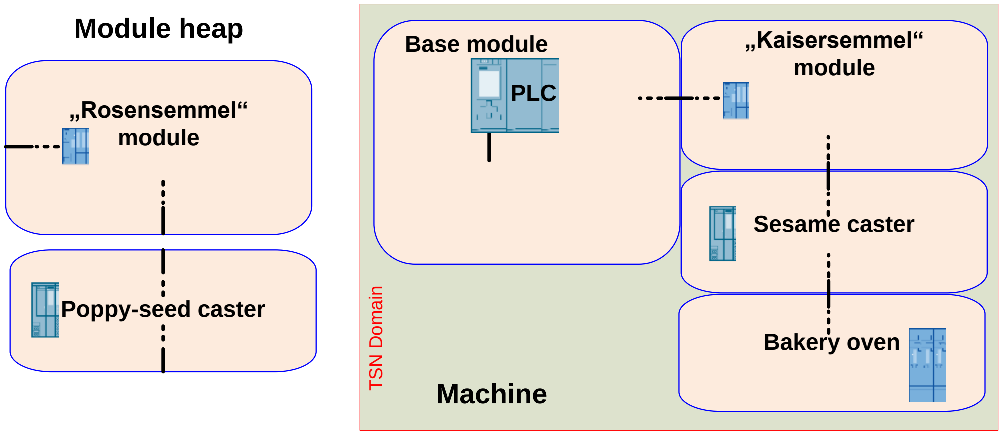


Figure 60 – modular bread-machine

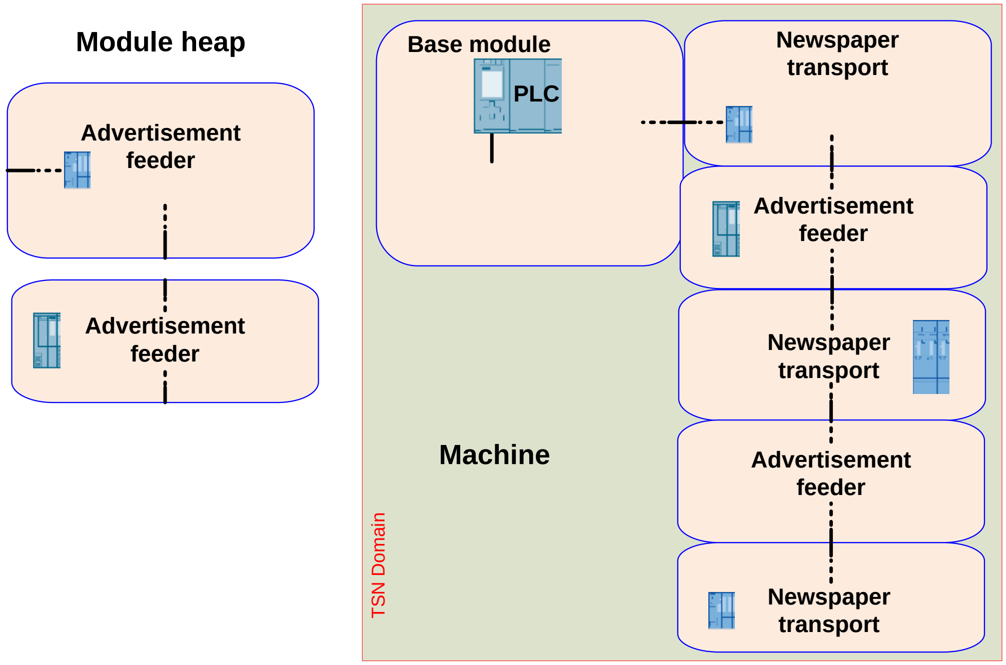


Figure 61 – modular advertisement feeder

Requirement:
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.

3.8.4 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.

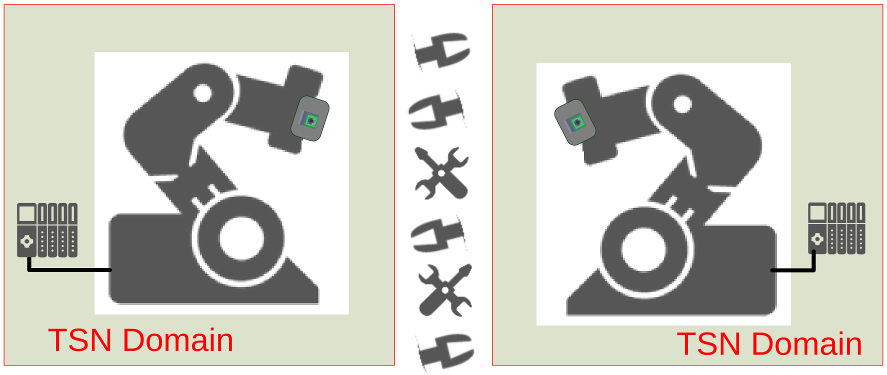


Figure 62 – tool changer

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
- …

3.8.5 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.

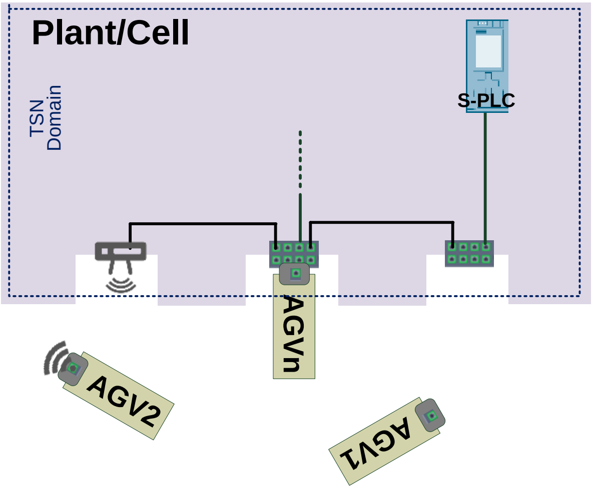


Figure 63 – AGV plug and unplug

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
- …

3.8.6 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.

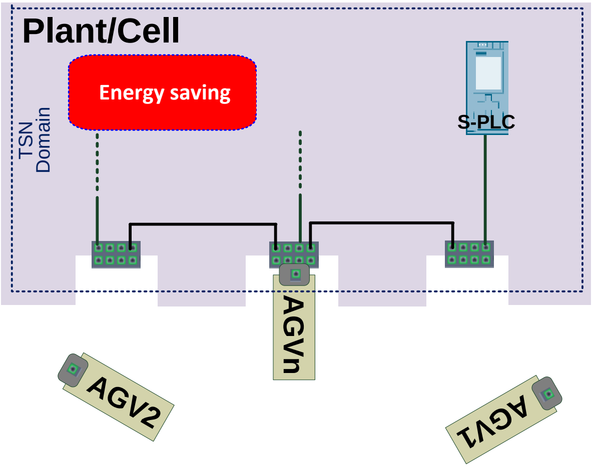


Figure 64 – energy saving

<u>Requirement</u>:

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.

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

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

3.8.7 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.

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.

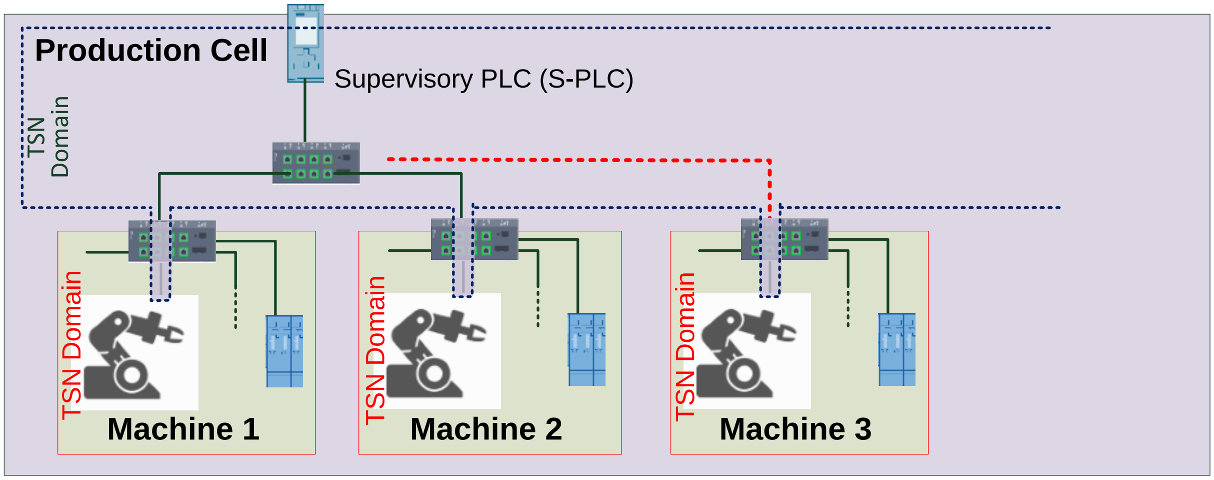


Figure 65 – add machine

<u>Requirement</u>:

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

<u>Useful mechanisms:</u>

- …

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

Technology A and B are implemented in PLC and devices.

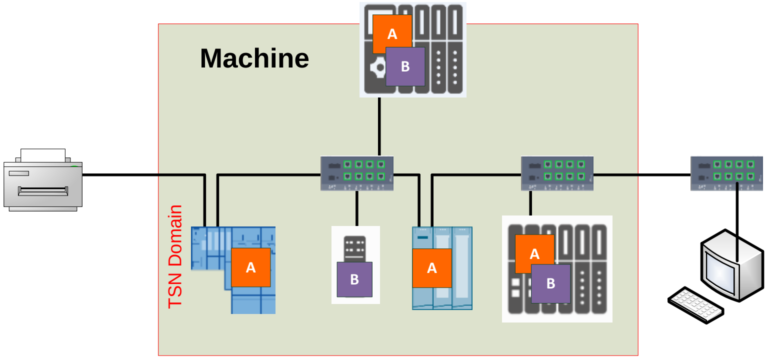


Figure 66 – two applications

<u>Requirement</u>:

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

<u>Useful 802.1 mechanisms:</u>

- …

3.8.9 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.

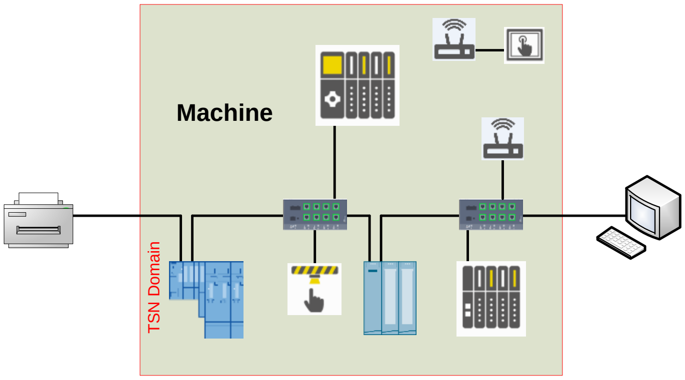


Figure 67 – Functional safety with cyclic real-time

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:

- …

3.8.10 Use case 26: 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 68). 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.

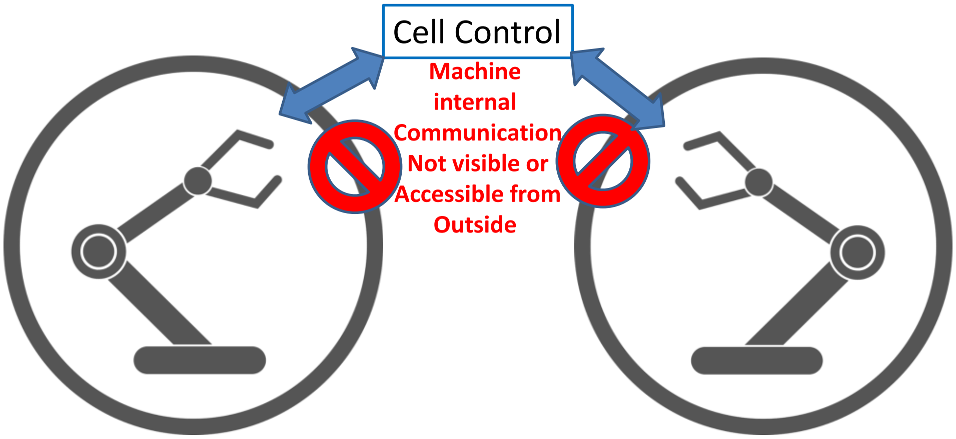


Figure 68 – Machine internal communication with isolated logical infrastructure

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;

Useful 802.1 mechanisms:

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

3.9 DCS Reconfiguration

3.9.1 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.

3.9.2 Use case 27: DCS Device level reconfiguration

The structure shown in **Error! Reference source not found.** applies. Figure 69 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).
- 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

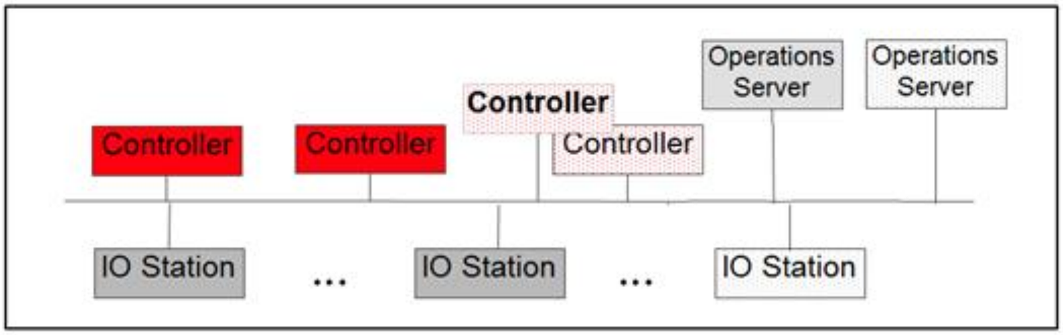


Figure 69 – Device level reconfiguration use cases

3.9.3 Use case 28: DCS System level reconfiguration

The structure shown in **Error! Reference source not found.** applies. Figure 70 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"

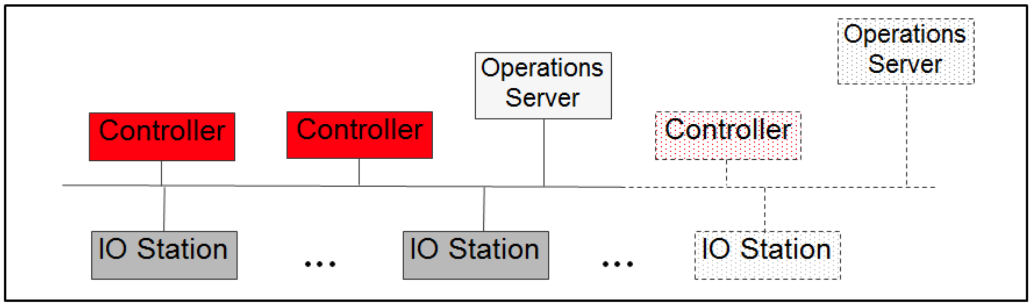


Figure 70 – System level reconfiguration use cases

3.10 Further Industrial Automation Use Cases

3.10.1 Use case 29: Network monitoring and diagnostics

Diagnostics plays an important role in the management of systems and of devices. Industrial automation requires a method for quick reaction to failures. The error reaction shall limit the damage caused by the error and minimize the machine downtime.

The error detection shall be done within a few cycles (exact value is depending on the application) and reaction shall be specified precisely in the case of an error. Machine stop is not always the right reaction on errors. This reaction can be located at the talker and listener.

Repairs are done by the service persons on site which have no specific communication knowledge. The indication of the components which have to be repaired shall occur within a few seconds. Machines are powered down during the repair. A typical repair time goal is below 15 min. This includes the restart of a machine and the indication that the problem is solved.

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 (see also Sequence of events).
- 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 shall 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;
- Reporting of detailed diagnostics information for TSN features shall be supported.

Useful 802.1 (ietf) mechanisms:

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

3.10.2 Use case 30: 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
- …

3.10.3 Use case 31: 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:

- …

3.10.4 Use case 32: 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 71 and Figure 72 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.

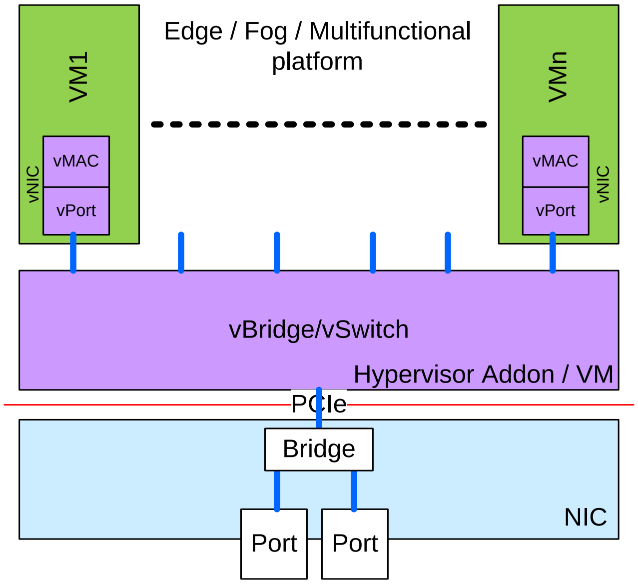


Figure 71 – Ethernet interconnect with VM based vBridge

Figure 71 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.

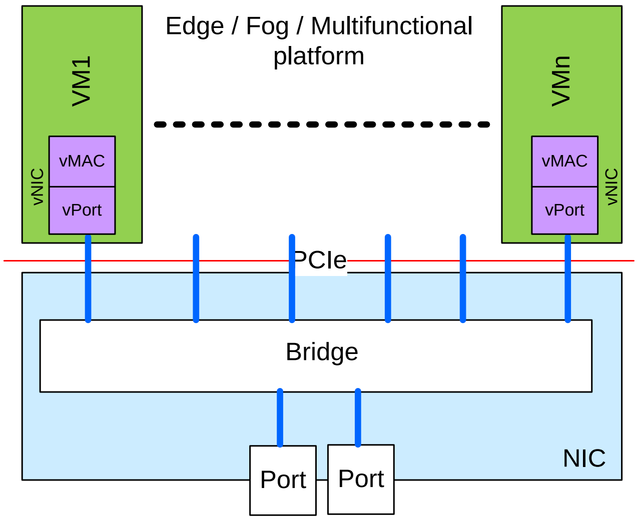


Figure 72 – Ethernet interconnect with PCIe connected Bridge

Figure 72 fits for a limited amount of VMs, because it saves the additional vSwitch/vBridge VM. For a given amount of VMs, e.g. PCIe 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:

- …

3.10.5 Use case 33: Offline configuration

The configuration of a machine is typically done before the machine is actually built. This is necessary for checking the availability of all components and as input for the machine programming. This requires an electronic data sheet of the field devices. Bridging components and talker listener behavior shall be described in these files. The talker and listener parameters are deduced from the application configuration as well as the communication intervals. The bridge description may include the port properties and the amount of streams supported for the individual purposes. Performance parameters are also required to set up the system. XML based textual description is used currently to describe the capabilities of field devices used in machinery. The individual elements are combined and additional parameters are defined resulting in another file which describes a machine configuration. This file is given to the machine control unit after machine setup and used to verify the commissioning. Protocols are needed to compare the real machine elements with the configured ones. Topology discovery is an important feature as well as the access to bridges to read and write management data.

Latency requirements restrict usable topologies and vice versa. Some applications can be handled with the description of an upper bound for latency. In this case the configuration may not use the accumulated latency from the bridge description but a limit which has to be checked during setup.

Another parameter for real time communication is the quality of time synchronization which depends upon several parameters of the components used in the synchronization path. YANG models of IEEE 802 components may be suitable for that purpose as offline database for individual bridge components and for the IEEE 802 network. It is not necessary for a machine configurator to handle the YANG related protocols but use the models. YANG means a completely different language as used today and implies two databases and some transformation and consistency issues between the two descriptive units. Thus, it is recommended to provide a mapping between XML and YANG.

Requirements:

- Device type description of IEC/IEEE 60802 components containing all necessary managed objects needs to be defined
- Means to store machine configuration offline in a textual form (e.g. XML);
- Offline - Online comparison of machine configuration shall be supported;

Useful 802.1 mechanisms:

- IEEE 802.1 YANG models;

3.10.6 Use case 34: 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:

- …

3.10.7 Use case 35: 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: 3.9.2 Use case 27: 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:

- …

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