Time Sensitive Networks for Flexible Manufacturing Testbed Characterization and Mapping of Converged Traffic Types

Version 1.0

2019-03-28

Table of Contents

The IIC's Time-Sensitive Networks for Flexible Manufacturing Testbed 4
TSN Overview 4
TSN Benefits 5
Overview of Traffic Types 6
Vertical and Horizontal 6
Traffic Type Characteristics 8
Traffic Type Descriptions 11
Isochronous 11
Cyclic 12
Events 15
Events—Alarms and Operator Commands 16
Events—Control 17
Configuration & Diagnostics 17
Network Control 19
Best Effort 20
Video 21
Audio/Voice 22
Traffic Type Characteristics Summary 23
Mapping Traffic Types 24
Mapping Overview 24
Recommendation Types 25
TSN Mechanisms 25
Mapped Device Types 30
Traffic Types Mappings 31
Mapping Traffic Type: Network Control 31
Mapping Traffic Type: Isochronous 32
Mapping Traffic Type: Cyclic 35
Mechanisms for Implementing Option Strict Priority: 37
Mechanisms for Implementing Option Scheduled Traffic: 38
Mapping Traffic Type: Events 38
Traffic Type: Events—Control Events 38
Traffic Type: Events—Alarms and Operator Commands 39
Mapping Traffic Type: Configuration & Diagnostics 40
Mapping Traffic Type: Best Effort 41
Mapping Traffic Types: Video & Audio 41
Mapping Summary 42
Summary 43
Authors and Legal Notice 43

Figures

Figure 1: Exclusive gating for Isochronous traffic. 35

Figure 2: Exclusive gating for Cyclic traffic. 37

Tables

Table 1: Table: Set of IEEE TSN Enhancements 5

Table 2: Traffic Type Characteristic 11

Table 3:Traffic Type Characteristics - Isochronous 12

Table 4:Traffic Type Characteristics - Cyclic 14

Table 5: Traffic Type Characteristics – Events – Alarms and Operator commands 16

Table 6: Traffic Type Characteristics – Events - Control 17

Table 7: Traffic Type Characteristics – Configuration & Diagnostics 18

Table 8: Traffic Type Characteristics – Network Control 19

Table 9: Traffic Type Characteristics – Best Effort 20

Table 10: Traffic Type Characteristics - Video 21

Table 11: Traffic Type Characteristics – Audio/Video 22

Table 12: Summary of Traffic Type characterizations 23

Table 13: Description of TSN Mechanisms 30

Table 14: Summary of Traffic Type Mappings 42

This document describes application traffic types that are found in industrial and process control systems and supported in the Industrial Internet Consortium's *Time Sensitive Networks for Flexible Manufacturing* testbed, including different types of critical control traffic and other traffic that may be in a manufacturing network. The IEEE 802.1Q specification, Annex lists traffic types as a means to structure network transmission priority and packet-drop preference. We enhance those traffic types by adding types found in typical manufacturing Industrial Automation and Control Systems (IACS), with a list of characteristics to describe them precisely. We then recommend IEEE 802.1 TSN mechanisms to support these traffic types in a converged network.

THE IIC'S TIME-SENSITIVE NETWORKS FOR FLEXIBLE MANUFACTURING TESTBED

The Industrial Internet Consortium (IIC), with over 200 members, aims to deliver a trustworthy Industrial Internet of Things (IIoT) in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes. The IIC has three main areas of activity: engage IIoT communities (ecosystem), develop guidance with technology and security architectures and drive innovation through testbeds. In 2015, the IIC Steering Committee approved the establishment of the Time-Sensitive Networks for Flexible Manufacturing testbed to display the value and readiness of time-sensitive networks to support real-time control and synchronization of high-performance machines. It has over 25 participants from a range of companies including chip vendors, IACS vendors, network infrastructure vendors, testing vendors and certification organizations. The testbed liaises with a range of standard development organizations including the IEEE, Avnu Alliance, OPC Foundation, IEC, ODVA, LNI4.0 and others. By aligning adopters, technology providers and standards developers, the testbed accelerates the adoption of this beneficial technology.

TSN OVERVIEW

Time-Sensitive Networking (TSN) enhances Ethernet (specifically IEEE 802.1 and 802.3), a foundational piece of the "internet of things." TSN adds a range of functions and capabilities to Ethernet to make it more applicable to industrial applications that require more deterministic characteristics than possible in previous Ethernet implementations. The table below summarizes those enhancements.

Standard	Title
IEEE 802.1Qav	Forwarding and Queuing Enhancements for Time-Sensitive Streams Incorporated in IEEE 802.1Q since 2009 clause 8.6.8.2 and Annex L.
IEEE 802.1AS-Rev	Timing and Synchronization for Time-Sensitive Applications The -Rev version is in progress.
IEEE 802.1Qbu & IEEE 802.3br	Frame preemption Incorporated in IEEE 802.1Q since 2016 clause 6.7.2
IEEE 802.1Qbv	Enhancements for Scheduled Traffic Incorporated in IEEE 802.1Q since 2015 clause
IEEE 802.1Qcc	Stream Reservation Protocol (SRP) Enhancements and Performance Improvements. Approved in 2018 and to be incorporated in October 2018
IEEE 802.1Qci	Per-Stream Filtering and Policing Incorporated in IEEE 802.1Q since 2017 clause 8.6.5.1.2.
IEEE 802.1CB	Frame Replication & Elimination for Reliability Approved in 2017

Table 1: Table: Set of IEEE TSN Enhancements

Automation and control systems comprise a large part of the estimated 50 billion things in IIoT, and these systems require the various devices, including the network, to perform in a deterministic way. The IIC's TSN Testbed for Flexible Manufacturing applies TSN technology to a manufacturing system to support the type of manufacturing application found in production environments and to display its capabilities and value.

TSN Benefits

TSN provides benefits to automation and control vendors as well as end customers, including:

- robust, reliable delivery of data,
- guaranteed latency,
- increased availability of network services for end-devices,
- accessibility of data driving IIOT big-data analytics and machine-learning applications,
- automated system configuration and management,
- system composability to add sub-systems and functions to existing systems with significantly reduced testing
- easy integration of innovations from open networks (more bandwidth, reliability and options) and
- ability to converge applications and traffic on a single, open network.

The first section of this whitepaper describes the traffic types in an industrial environment that converge onto a single, open TSN network. The second section maps the defined traffic types to the existing and recently updated Ethernet Quality of Service (QoS) mechanisms, such as TSN traffic-shaping mechanisms.

OVERVIEW OF TRAFFIC TYPES

Annex I.1 of the *IEEE Standard for Local and metropolitan area networks: Bridges and Bridged Networks (802.1Q)* lists eight traffic types. Of those listed, in particular, network control, voice, video, critical applications, excellent effort and best effort have direct relevance to IACS, while internetwork control and background traffic generally do not.

We focus on the types of traffic flows that IACS use that are reliant on the QoS they receive from the network and how that may affect the QoS of other traffic types. The specific types are:

- *Network Control*, which includes Precision Time Protocol (PTP) traffic critical to the IACS and the network's ability to provide TSN services,
- *Excellent Effort*, which includes IACS configuration and diagnostics traffic,
- *Voice* (audio), which may be part of an IACS systems or used for Audio services provided in the manufacturing zone,
- *Video*, which may be part of an IACS systems or used for video services provided in the manufacturing zone and
- *Best Effort*.

The following three new types that may be considered sub-types of Critical Application, but have specific characteristics:

- *Isochronous*, where IACS devices need to exchange data synchronously at a defined periodic rate,
- *Cyclic*, where IACS devices exchange data at a defined rate, and
- *Events*, where IACS devices create messages that need to be received and acted upon in a defined time period without loss.

VERTICAL AND HORIZONTAL

In a discrete factory or process automation plant there are various traffic types with different delivery requirements. Generally speaking, there is *vertical* communication between the automation control devices and the plant-level systems and applications, e.g. Scada, Manufacturing Execution Systems (MES) and Human-Machine Interfaces (HMI), and *horizontal* communication between the automation and control devices. Horizontal communication can be broken down to controller-to-controller and controller-to-field-equipment (e.g. actuators, sensors and drives), a.k.a. input and outputs (I/O). Historically various types of fieldbuses support these diverse communication requirements and thereby segment the IACS traffic flows onto separate networks. This significantly limits the type and volume of data available for IoT applications.

Current, pre-TSN Ethernet (IEEE 802.1 and 802.3) QoS capabilities include traffic-shaping mechanisms, bandwidth allocation, prioritization and queue management techniques, but lack the ability to guarantee latency (the amount of time to transmit a packet in the network), jitter

(the latency variation of the packet's transmission) or packet delivery. Without these guarantees, Ethernet is predominantly used for vertical communication, such as management, configuration, backup, historical data, diagnostics, alarms and process graphics updates, usually taking place between the controllers and the plant management and historian servers.

Horizontal communication is where real-time traffic types exist, either as controller-to-controller communication or controller-to-field-equipment, and are often supported by specific industrial Ethernet solutions (e.g. EtherNet/IP, Sercos, Powerlink, Profinet IO, Ethercat, CC-Link). Many of these worked around the precise QoS guarantees of pre-TSN Ethernet by including existing standard QoS mechanisms of prioritization and queue management, or by proprietary enhancements to Ethernet for synchronization and time-based bandwidth utilization. Alternatively, real-time traffic types may use legacy fieldbuses (e.g. Profibus, Foundation Fieldbus, DeviceNet, CAN, Interbus, etc.) in special local networks. The use of proprietary enhanced, segmented Ethernet protocols or fieldbus technologies hinder access to and sharing of data in those networks as opposed to when standard Ethernet is used.

Vertical communication traffic types comprise communication between the controllers, the local plant management servers and cloud services. It may include:

Alarms and events: the controllers, after processing data received from I/O field devices, report breaches of the process variable range (an event) or larger breach of such ranges (an alarm) to the servers and thus to the operators of the plant,

Process graphics update information: the operators monitor the status of the process equipment and current process values in the industrial process,

Historian information: to observe the behavior of the process using various complex analysis where process variables evolution over time must be taken into account,

Operator commands: the operators must be capable of intervening on the various process devices,

Configuration: the files and commands used to configure the various automation and control devices,

Server backup: the application servers and critical devices in the plant usually backed up for recovery purposes regularly, which can create bandwidth utilization peaks and

Diagnostics: to perform maintenance and analysis of reported alarms and diagnostics on field equipment.

Horizontal communication comprises communication between IACS devices (such as controllers, I/O equipment, drives, encoders and other field-level communication), including:

Isochronous: cyclic traffic streams from synchronized applications with very short cycle times and a low jitter requirement.

Cyclic controller-controller: where controllers exchange variables as a part of shared applications. There is more tolerance to jitter and frame loss than isochronous communication.

Cyclic controller-IO or controller-drive: where sensors and actuators exchange data with controllers

Events: where IACS devices communicate change-of-state, alarms/warnings when thresholds are exceeded or operator commands.

TRAFFIC TYPE CHARACTERISTICS

TSN lets information technology (IT) and operational technology (OT) applications share the same physical network infrastructure without influencing the other by introducing a toolbox of mechanisms, such as scheduled traffic (IEEE 802.1Qbv), to provide new levels of Data Delivery Guarantees to Ethernet-based communication. The following application-centric communication characteristics enable the identification of a small number of distinct traffic types that are shared among sets of industrial applications:

Traffic Types Characteristics	
Characteristic	**Description**
Data Transmission Periodicity	Traffic types comprise data streams that can either be transmitted in a *cyclic/periodic* (e.g. signal transmission) or *acyclic/sporadic* (e.g. event-driven) manner.
Typical period	For traffic types that transmit *cyclic/periodic* data streams, period denotes the *planned data transmission interval* (often also called "cycle") at the application layer. The interval is provided as a typical *range in orders of magnitude of time*, i.e. 80% of the industrial applications in scope of the given traffic type are within the provided range. For the traffic types with *acyclic/sporadic* data transmission periodicity this characteristic does not apply.
Application Synchronized to Network	Denotes whether an application producing a traffic type is synchronized to the network time at the application layer. Applications that are synchronized to the network time can align their sending behavior to mechanisms provided by the network (e.g. scheduling) for reduced latency and jitter in the network communication. Available options are: *yes* or *no.*
Data Delivery Guarantee	Denotes the application's delivery constraints of the network for unimpaired operation. To guide the selection of appropriate Ethernet QoS mechanisms including the enhancements from IEEE 802.1 TSN, the scope of this characteristic is limited to the application's data transmission requirements. Any non-application-related requirements and any impact from the application itself and the sending and receiving device's communication stack are out of scope. Three Data Delivery Guarantees are defined: • Deadline: data delivery of each packet or set of packets in a stream is guaranteed to occur at all registered receivers at or before a specified time (i.e. relative to the start of a communication cycle) and is applicable only to traffic types with *cyclic/periodic* data transmission periodicity, • Latency: data delivery of each packet in a stream is guaranteed to occur at all registered receivers within a predictable timespan starting when the packet is transmitted by the sender and ending when the packet is received and • Bandwidth*:* data delivery of each packet in a stream is guaranteed to occur at all registered receivers if the bandwidth utilization is within the resources reserved by the sender. For each option, a typical *quantification* shall be provided with the Data Delivery Guarantee, i.e. 80% of the industrial applications in scope of the given traffic type are within the provided quantification. In the case that a packet cannot be delivered within the given latency or deadline requirement, that packet may be considered as lost or discarded by the application. In the case of traffic types with no special Data Delivery Guarantee requirements, the available option is *"none."*

Traffic Types Characteristics	
Characteristic	**Description**
Tolerance to Interference	Denotes the application's tolerance of a certain amount of latency variation of the packet's transmission (i.e. jitter) for the traffic types with *cyclic/periodic* data transmission periodicity. In the case of a highly jitter-sensitive application, no jitter is expected and is to be indicated with the jitter value of zero, meaning that this jitter must be negligible. If the application can cope with jitter, the response is *yes* and the amount of jitter is specified in a range. Other sources of jitter in application processing besides network transmission jitter exist, e.g. stemming from local OS scheduling or time synchronization. These additional sources of jitter commonly have effects beyond individual traffic types and need to be considered separately. For traffic types with *none* or bandwidth Data Delivery Guarantees the response is *yes* and jitter is not specified.
Tolerance to Loss	Denotes the application's tolerance to a certain amount of consecutive packet loss from an IACS device in network transmission. Industrial applications may consider a packet lost if not received within the Data Delivery Guarantee. In this case, a *quantifiable number of tolerable lost packets* shall be provided. Alternatively, the option *"yes"* can be provided for applications that tolerate packet loss to the extent that basic redundancy protocols such as Spanning Tree suffice to recover from potential network interruptions. In the case of a highly loss-sensitive application, where no single packet may be lost, *"no (0 frames)"* is the only available option. Packet loss can occur from network congestion and network error. In the mapping of required features, both cases should be considered. It should also be noted that the Transmission Control Protocol (TCP) provides a form of protection from data loss, but many of the Industrial applications consider the packet lost sooner than this mechanism can respond.
Typical Application Data Size	Denotes the *size* of application data (payload) to be transmitted in the Ethernet frames. The size can be *fixed* (the data is always with the exact same size) or *variable* (data size varies from packet to packet, but not exceeding the given maximum size). The application data size provides a typical *range in orders of magnitude of bytes*, i.e. 80% of the industrial applications in scope of the given traffic type in the provided range. Where individual packet sizes widely fluctuate or cannot be determined at design or configuration time, *data volume estimates* (e.g. required bandwidth) is provided.

Traffic Types Characteristics	
Characteristic	**Description**
Criticality	Describes the criticality of the data for the operation of the critical parts of the system. Application criticality is used as a criterion to guide the selection of the appropriate QoS/TSN mechanisms and bandwidth reservations in case of conflicting requirements. The following categories of criticality are defined: • *high*: for traffic types used either by application or the network services that are highly critical for the operation of the system. Data loss of this traffic type may cause critical system malfunction and cannot be repeated or retransmitted by the application, • *medium*: for traffic types used either by application or the network services that are relevant but not continuously needed for the operation of the critical part of the system. Data loss of these traffic types may cause degraded operation but not a system malfunction. Data loss can be compensated by repeating/retransmitting the same data and • *low*: for traffic types used either by application or the network services that are not relevant for the operation of the critical part of the system. Data loss can be compensated by repeating/retransmitting the same data. Note that the criticality of the data is not to be confused with the traffic class priority. Traffic class priority is one mechanism to address the criticality, but not the only one. TSN provides additional mechanisms, such as frame preemption, scheduled traffic, to address the criticality of the traffic.

Table 2: Traffic Type Characteristic

NOTE: Solution-specific characteristics including any type of traffic-class prioritization, coordination or dependencies (e.g. offsets between flows) among the traffic streams and types are out-of-scope for the above.

NOTE: Application data streams may be based on 1:1 transmissions between the sender and receiver or 1:many (a.k.a. multicast) between a sender and multiple receivers. It is not expected that the cardinality of application traffic (i.e. 1:1 or 1:many) has an immediate influence on the QoS mechanisms (beyond stream configuration) and is therefore out-of-scope of this whitepaper.

TRAFFIC TYPE DESCRIPTIONS

This section describes the traffic types including a table of specific traffic type characteristics (as described above) for each.

ISOCHRONOUS

For the isochronous traffic type, applications in each device are synchronized to a common time, which is strictly monotonic and steadily increasing, without jumps or leaps. Devices synchronously sample inputs and apply outputs by exchanging data at a defined periodic rate or

cycle. When applied to motion applications, this rate can be fast, in some cases, under 100 microseconds. For tight control loops, transmission jitter must be minimal, with no interference from other traffic. Messages need a guaranteed delivery time. If they arrive later than this deadline, they are ignored for that cycle or discarded, thus potentially affecting the control loop. Message sizes are fixed at design time and remain constant for each cycle. Payload sizes are typically under 100 bytes per device. This traffic type can be used for controller-to-controller, controller-to-I/O-communication and device-to-device in synchronous exchanges.

Examples include:

- *time-synchronized applications* where data must be produced and delivered consistently and where packets are delivered with a bounded latency, in other words before or by the deadline and
- *applications with implicit synchronization* where devices act on reception of a frame and therefore lack Tolerance to Interference and require very low jitter to produce an *on-time* delivery (at a specific point in time).

An example is turbine control in a power generation hydro plant, drive to drive in a master-follower application or a drive to an encoder.

Traffic Type Isochronous		
Characteristic	**Value**	**Notes**
Periodicity	Cyclic/periodic	
Typical Period	< 2ms	
Application synchronized to network	Yes	
Data Delivery Guarantee	Deadline	Usually within one data transmission period
Tolerance to Interference	0	Least possible jitter is required
Tolerance to Loss	None	Seamless redundancy is required
Typical Application Data size	Fixed (30 ~ 100 bytes)	
Criticality	High	

Table 3:Traffic Type Characteristics - Isochronous

CYCLIC

This traffic type involves cyclic/periodic communication between devices. The applications in each device are not synchronized to a common time. Devices sample inputs and apply outputs

cyclically, which may or may not be the same as the data transmission period. When applied to a client-server protocol (e.g. PROFINET IO), messages will be clustered while in a publish/subscribe environment (e.g. EtherNet/IP) messages may be distributed over the cycle time (e.g. from devices) or clustered together (e.g. controller to devices). For best control, the time between a device sending a message and its reception should be minimized, with predictable interruptions from other traffic. Messages need a defined maximum latency time. Data message sizes are fixed at design time and remain constant for each cycle. This type can be used for controller-to-controller, controller to I/O and device-to-device communication.

Examples include:

- *input/output* updates sent to/from actuators and sensors and a programmable logic controller in a discrete manufacturing facility with request packet interval (RPI) times usually measured in milliseconds and cycle times usually 3 to 4 times the RPI,
- *process graphic updates* that need to be updated on a cyclic polling basis, with up to 1 second cycle times; the process controllers send this information to the servers of the plant; maximum frame size varies following each vendor but may reach the Ethernet Maximum Transmission Unit (MTU) 1500 bytes,
- *historian information* where process controllers create data traffic which is cyclic, but with an update rate or cycle time of around one second. Maximum frame size varies following each vendor but may reach the Ethernet MTU and
- *cyclic diagnostics* where a diagnostic computer checks the functionality of a follower drive in a master-follower application, i.e. by 1500 bytes (Ethernet MTU) each 4 ms.

Traffic Type: Cyclic		
Characteristic	**Value**	**Notes**
Periodicity	Cyclic/periodic	
Typical Period	2 ~ 20ms	
Application synchronized to network	No	
Data Delivery Guarantee	Latency	Typically it is less than 90% of the period, e.g. may be 100µs ~ 2ms.
Tolerance to Interference	<= latency	The jitter is constrained by the latency requirement.
Tolerance to Loss	1 ~ 4 frames	Applications are designed to tolerate the loss of one to 4 successive frames (1 ~ 4 periods).
Typical Application Data size	Fixed (50 ~ 1000 bytes)	
Criticality	High	

Table 4:Traffic Type Characteristics - Cyclic

EVENTS

In a system when an input or output variable change occurs that requires attention, event messages are generated. Events may be a change-of-state, operator commands, or an alarm or warning that thresholds were exceeded. Depending upon the change, this might be a single message, or a flurry of messages (domino effect).

The network must be able to handle a burst of messages without loss, up to a certain number of messages or bandwidth. After this period messages can be lost until the allowed bandwidth quantity has been restored.

Examples include:

- Alarms or Operator Commands that create traffic that may tolerate up to 2 seconds latencies and are acyclic. Alarms are prone to flooding when issues arise in the system being controlled. Maximum frame size varies by application but may reach 1500 bytes.
- Control Event*s* create another type of event traffic that is acyclic and has a typical latency requirement from 10 to 50 milliseconds. Maximum frame sizes vary but are usually smaller than the previous ones, reaching 100 ~ 200 bytes.
- Human-machine interface *cyclic data* that is not critical enough or does not have direct impact on the application may also be considered under this traffic type.

Due to the significantly different requirements, characteristics for “Alarms and Operator Commands” and “Control” events will be separately described. While both application categories send the data in non-periodic manner, some per-device and upper bound for the worst-case bandwidth usage shall be given by the application.

EVENTS—ALARMS AND OPERATOR COMMANDS

Traffic Type: Events—Alarms and Operator commands		
Characteristic	**Value**	**Notes**
Periodicity	Acyclic/sporadic	
Typical Period	n.a.	
Application synchronized to network	No	
Data Delivery Guarantee	Latency (~ 2s)	
Tolerance to Interference	<= latency	Jitter is not a concern as long as the latency guarantees are maintained.
Tolerance to Loss	Yes	Alarm showers of up to 2000 alarms per second should be guaranteed, after which some packet loss is acceptable. The number is application dependent.
Typical Application data size	Variable (100 ~ 1500 bytes)	
Criticality	Medium	

Table 5: Traffic Type Characteristics – Events – Alarms and Operator commands

EVENTS—CONTROL

Traffic Type: Events - Control		
Characteristic	**Value**	**Notes**
Periodicity	Acyclic/sporadic	
Typical Period	n.a.	
Application synchronized to network	No	
Data Delivery Guarantee	Latency (10ms ~ 50ms)	
Tolerance to Interference	<= latency	Jitter is not a concern as long as the latency guarantees are maintained.
Tolerance to Loss	Yes	Applications are designed to tolerate the loss of some frames but may degrade system integrity.
Typical Application data size	Variable (100 ~ 200 bytes)	
Criticality	High	

Table 6: Traffic Type Characteristics – Events - Control

CONFIGURATION & DIAGNOSTICS

The Configuration & Diagnostics traffic type is for the transport of configuration and diagnostic data, such as device configuration and firmware downloads. This data is traditionally sent using TCP/IP-based protocols that contain lost message recovery capabilities. This data is not time critical, but it must eventually be delivered.

Examples include:

- Configuration activities create traffic with maximum frame sizes up to the Ethernet MUT in an acyclic manner. This traffic type may occasionally create peaks of bandwidth utilization with a latency of up to 1 second.
- Diagnostic activities to monitor equipment health that creates acyclic traffic type.
- Process information from the application, such as order scheduling and production.
- Network and system management and configuration (e.g. SNMP, RESTCONF/NETCONF, firmware updates) protocol traffic are also considered part of this traffic type.

Traffic Type: Configuration & Diagnostics		
Characteristic	**Value**	**Notes**
Periodicity	Acyclic/sporadic	
Typical Period	n.a.	
Application synchronized to network	No	
Data Delivery Guarantee	Bandwidth	Additionally, the latency is in the range of 100ms
Tolerance to Interference	n.a.	
Tolerance to Loss	Yes	No seamless redundancy is required.
Typical Application Data size	Variable	Can be large packets of 500 ~ 1500 bytes
Criticality	Medium	

Table 7: Traffic Type Characteristics – Configuration & Diagnostics

NETWORK CONTROL

The network control traffic type contains network control messages. These messages are low in volume but have critical delivery requirements. Many of the messages are cyclic, but not relative to any TSN network cycle times.

Examples of network control include:

- clock synchronization (e.g. PTP),
- network redundancy (e.g. MSTP, RSTP) and
- topology detection (e.g. LLDP).

Traffic Type: Network Control		
Characteristic	**Value**	**Notes**
Periodicity	Cyclic/periodic	
Typical Period	50ms ~ 1s	
Application synchronized to network	No	
Data Delivery Guarantee	Bandwidth	Typically 1 ~ 2 Mbps.
Tolerance to Interference	Yes	Transmission jitter should not exceed the period.
Tolerance to Loss	Yes	Excessive loss of network control frames can lead to loss of network functions (e.g. link-down state or grand master fail-over).
Typical Application data size	Variable (50 ~ 500 bytes)	
Criticality	High	

Table 8: Traffic Type Characteristics – Network Control

BEST EFFORT

The Best Effort traffic type is the default for the transport of any application data that does not require a better service guarantee from the network than "as good as possible." In other words, best effort applications are not provided bandwidth or timing guarantees beyond a potential generic bandwidth reservation for the entire best effort traffic in the network. Best effort traffic follows may suffer from data loss when higher priority traffic uses does not leave sufficient bandwidth.

Examples include:

- Non-critical retrieval of telemetry data
- Non automation and control application data.

Traffic Type: Best Effort		
Characteristic	**Value**	**Notes**
Periodicity	Acyclic/sporadic	
Typical Period	n.a.	
Application synchronized to network	No	
Data Delivery Guarantee	None	Typically networks are configured to provide some bandwidth to best effort.
Tolerance to Interference	n.a.	
Tolerance to Loss	Yes	
Typical Application data size	Variable (30 ~ 1500 bytes)	
Criticality	Low	

Table 9: Traffic Type Characteristics – Best Effort

VIDEO

Video traffic is the streaming of video data between endoints. IACS often include video systems, but this traffic will be mapped to previous types such as *Cyclic* or potentially *Isochronous* data depending on the criticality of the application. The characteristics below describe video for human consumption. Video streaming for human consumption tends to have lower performance requirements and is reflected in the IEEE 802.1Q, where Video "traffic is characterized by less than 10 ms delay and, hence, maximum jitter (one-way transmission through the LAN infrastructure of a single campus)."

Examples include:

- Video Surveillance traffic used to monitor production conditions visually but are not part of any control process.

Traffic Type VII: Video		
Characteristics	**Value**	**Notes**
Periodicity	Cyclic/periodic	
Typical Period	Frame Rate	
Application synchronized to network	No	
Data Delivery Guarantee	Bandwidth	Latency greater than 10ms may impact application performance
Tolerance to Interference	n.a.	
Tolerance to Loss	Yes	Loss of packets may lead to decreased quality, but not necessarily application failure
Typical Application Data size	Variable	Large packets (1000 - 1500 bytes)
Criticality	Low	

Table 10: Traffic Type Characteristics - Video

AUDIO/VOICE

Audio traffic is the streaming of audio or voice traffic between end-points. As with video traffic, IACS systems often include sound sensors and actuators, but such end-devices treat the streaming data as *cyclic* or potentially *isochronous* data depending on the criticality of the application. Audio streaming for human consumption tends to have lower performance requirements and is reflected in the IEEE 802.1Q where audio traffic is "characterized by less than 100 ms delay, or other applications with low latency as the primary QoS requirement."

Traffic Type: Audio/Voice		
Characteristic	**Value**	**Notes**
Periodicity	Cyclic/periodic	
Typical Period	Sample Rate	
Application synchronized to network	No	
Data Delivery Guarantee	Bandwidth	Latency greater than 40ms may impact application performance
Tolerance to Interference	n.a.	
Tolerance to Loss	Yes	Loss of packets may lead to decreased quality, but not necessarily application failure.
Typical Application Data size	Variable	Large packets (1000 - 1500 bytes)
Criticality	Low	

Table 11: Traffic Type Characteristics – Audio/Video

TRAFFIC TYPE CHARACTERISTICS SUMMARY

The table below summarizes the traffic types and their characteristics.

Types	Periodicity	Typical Period	Synchronized to network	Data Delivery Guarantee	Tolerance to Interference	Tolerance to Loss	Typical Application data size (Bytes)	Criticality
Isochronous	Periodic	< 2ms	Yes	Deadline	0	None	Fixed: 30 ~ 100	High
Cyclic	Periodic	2 ~ 20ms	No	Latency	<= latency	1 ~ 4 Frames	Fixed: 50 ~ 1000	High
Events: Alarms & Operator Commands	Sporadic	n.a.	No	Latency	<= latency	Yes	Variable: 100 ~ 1500	Medium
Events: Control	Sporadic	n.a.	No	Latency	<= latency	Yes	Variable: 100 ~ 200	High
Network Control	Periodic	50ms ~ 1s	No	Bandwidth	Yes	Yes	Variable: 50 ~ 500	High
Config & Diagnostics	Sporadic	n.a.	No	Bandwidth	n.a.	Yes	Variable: 500 ~ 1500	Medium
Best Effort	Sporadic	n.a.	No	None	n.a.	Yes	Variable: 30 ~1500	Low
Video	Periodic	Frame Rate	No	Latency	n.a.	Yes	Variable: 1000 ~ 1500	Low
Audio/Voice	Periodic	Sample Rate	No	Latency	n.a.	Yes	Variable: 1000 ~ 1500	Low

Table 12: Summary of Traffic Type characterizations

MAPPING TRAFFIC TYPES

We have so far identified and characterized different types of traffic that may be in a converged industrial network. The remaining sections describe the enhanced set of IEEE 802 TSN/QoS mechanisms and maps that are needed to support each of them. The purpose of this mapping is to establish common application requirements so that customers and implementers have confidence their requirements will be met regardless of traffic type mix, topology or type of network infrastructure used, so long as the mapped mechanisms are available in the network infrastructure and end-devices. These mappings are not a "profile", but are input to standards organizations that may develop them. The configuration of these TSN mechanisms and networks is generally out of scope of this document.

The goal of this paper is to describe a set of mappings that is intended to support all the traffic types in a broad range of deployments. Different mappings for specific traffic types may sufficiently support that traffic type in limited situations. They are not included.

Different TSN/QoS mechanisms may also affect each other, for example, time-aware-shaping and credit-based-shaping, and the TSN mechanisms applied to one traffic type can influence other traffic types, such as frame preemption. For this reason, the analysis considers the interaction of different mechanisms and traffic types in a *converged* network. The choice of mechanisms for any traffic type suffice even when some traffic types are not available. The selection of mechanisms and configuration options for a traffic type does not invalidate the quality of service traffic types with same or higher criticality receive.

We assume the reader has a solid understanding of Ethernet (i.e. Layer 2) networking concepts, such as quality-of-service, input and output queueing, policing of network traffic and more.

MAPPING OVERVIEW

This section provides an overview of the mappings for each traffic type that are detailed later. The mappings that support each specific traffic type are structured and include:

- the recommendation type,
- the TSN mechanism,
- configuration considerations that are relevant to the use of the mechanism,
- the type of device the mechanism would be implemented upon and
- context and reasoning behind the recommendation.

The sections below give more detail and context regarding these parameters. The TSN Mechanism section describes the TSN mechanisms applied and also gives a general overview of what the mechanism provides. Later, in each traffic type mapping, specific reasons the mechanism is mapped are described in the context of that traffic type.

RECOMMENDATION TYPES

The recommendation types are:

- Mandatory (M): the type of device(s) must support the capability on some or all of the network ports,
- Recommended (R): the device(s) should support the capability on some or all of the network ports,
- Optional (O): the device(s) may support the capability on some or all of the network ports or
- Conditional (C): the device(s) support for the capability on some or all ports is conditional, where conditions are explained in the subsequent context section for each mapping.

TSN MECHANISMS

Each of the TSN mechanisms presented in “Table: Set of IEEE TSN Enhancements” are used to some extent in the mappings. We describe the mechanism and how it is used to support key traffic type characteristics. Because some latency-based Data Delivery Guarantees may require lower latency than standard “store and forward” network infrastructure can provide we describe an additional mechanism: cut-through switching. This concept is not currently an IEEE standardized feature.

TSN Mechanisms	
Mechanism	**Description and Comments**
IEEE 802.1Q Strict Priority	**Strict Priority Forwarding** The 802.1Q standard lays out a mechanism of identifying traffic forwarding priority and drop eligibility with the Priority Code Point (PCP) in the VLAN tag as outlined in IEEE 802.1Q 2018 Section 6.9.3. It also specifies Traffic Class as the means to place a frame in an output queue. Strict Priority Forwarding suggests that packets are assigned to outbound queues identified by a Traffic Class (respectively in bridges) by their PCP value. If a bridge supports more than 1 outbound queue, frames in queues with a higher Traffic Class are forwarded before frames in queues with a lower Traffic Class, if other mechanisms such as Traffic Scheduling (.1Qbv) or Credit-based Shaping (.1Qav) are not in place. This mechanism is considered a mandatory default feature for all bridges supporting IEEE 802.1Q. Each of the traffic types are assigned at least a Traffic Class value to indicate which QoS mechanisms the networking queuing and forwarding functions should apply to the packet. We do not recommend the number of queues a bridging device must have, but assume that two or more queues are required to support traffic scheduling and separate scheduled traffic from unscheduled traffic.
IEEE 802.1Qav	**Forwarding and Queuing Enhancements for Time-Sensitive Streams** Credit-based shaping was formally included in IEEE 802.1Q—Section 34. It identifies a means to reserve bandwidth along a network path through a Stream-Reservation protocol and enforced via a queue management mechanism that ensures an amount of bandwidth is available for certain specified traffic. It was designed for Audio/Video traffic types. This mechanism ensures specified traffic types receive requested and allocated bandwidth over lower priority traffic types, but does not meet all Data Delivery Guarantees outlined, such as Deadline or Latency. Credit-based shaping queues can also be used to limit a traffic type's use of bandwidth as the credit is used and only replenished over time.

TSN Mechanisms	
Mechanism	**Description and Comments**
IEEE 802.1AS-Rev	**Timing and Synchronization for Time-Sensitive Applications** This mechanism is based on the Precision Time Protocol (a.k.a. PTP) referred to as Clock Synchronization**. It** is used to ensure that the synchronization requirements are met for time-sensitive applications, such as audio, video, and control across networks. It is a profile or derivation of the IEEE 1588 Precision Timing Protocol. Clock synchronization is required to support scheduled traffic (IEEE 802.1Qbv), ensuring that the network infrastructure and end-devices can transmit on a schedule based on a common sense of time. Therefore, in the mapping considerations, it receives the same recommendation type as 802.1Qbv. IACS applications often require time synchronization, but that is not reflected in the mappings.
IEEE 802.1Qbv	**Enhancements for Scheduled Traffic** Scheduled Traffic enables support for scheduled network traffic as specified in IEEE 802.1Q 2018 section 8.6.8.4. This enhancement enables traffic streams to be communicated in the network without interference and with little jitter. This feature can be used to meet all the Data Delivery Guarantees (deadline, latency and bandwidth). Bandwidth guarantees may be met with other mechanisms, such as .1Qav Credit-based Shaping, but their ability to maintain bandwidth guarantees diminishes with the presence of Scheduled Traffic as the exclusive time-based queueing takes priority. Scheduled Traffic queues can be used to limit a traffic types use of bandwidth as the queue is only open a certain amount of time. We recommend this mechanism include a concept of Exclusive Gating, which suggests that only one queue (i.e. Traffic Class) has access to forwarding mechanisms at scheduled times. This is used for the Iscohronous traffic type Mapping.

TSN Mechanisms	
Mechanism	**Description and Comments**
IEEE 802.1Qbu & IEEE 802.3br	**Frame preemption** Frame Preemption standards allow higher priority “express” frames to interrupt a lower-priority preemptible frames currently in transmission and resume the preempted frame’s transmission after higher priority frames are transmitted. The 802.1Qbu portion has been incorporated into the IEEE 802.1Q standard (see sections 6.7.1, 6.7.2, 8.6.8 and Annex S). The Ethernet-specific specifications are defined in IEEE 802.3br. Frame preemption has two key capabilities. First, in the absence of Scheduled Traffic (802.1Qbv), frame preemption can be used to reduce latency and jitter of packet transmission to help meet deadline and latency Data Delivery Guarantees for express frames in the presence of potentially interfering preemptible frames. It cannot guarantee delivery to the same degree as with Scheduled Traffic due to the presence of other express traffic and traffic transmission delays due to transmitting frames too small to be preemptible thus causing delays and jitter. Second, in the presence of Scheduled Traffic, frame preemption is beneficial to lower priority preemptible traffic by freeing utilizable bandwidth for transmission. Preempting lower priority traffic allows the passage of non-express frames that might otherwise be too large to egress in the time allotted, thereby increasing the amount of usable bandwidth for lower priority traffic.
IEEE 802.1Qcc	**Stream Reservation Protocol (SRP) Enhancements and Performance Improvements** This standard has been approved and will be incorporated into IEEE 802.1Q in the next revision. It provides enhancements to the configuration of time-sensitive streams into the SRP. SRP includes the following: • description of three configuration models: centralized, decentralized, hybrid, • specification of MSRPv1 and MIBs for hybrid model, • definition of bridge-managed objects and MIBs for centralized configuration model and • YANG module with four core structures to be used for CNC/CUC API SRP contains multiple signaling protocols. This enhancement specifies the Multiple Stream Registration Protocol (MSRP) as a signaling protocol that enables the ability to reserve network resources for devices that will guarantee the transmission and reception of data streams across a network with the requested QoS capability. These end-devices are called Talkers (devices that produce data streams) and Listeners (devices that consume data streams). SRP also specifies the use of different configuration models and mechanisms to communicate required flows. Considerations for management and configuration are out of the scope. This mechanism is used to provide consistent QoS behavior across the network.

TSN Mechanisms	
Mechanism	**Description and Comments**
IEEE 802.1Qci	**Per-Stream Filtering and Policing (PSFP and a.k.a. Ingress Policing)** This enhancement to PSFP establishes time-based policing and has been included into IEEE 802.1Q-2018. *Per stream filtering and policing* (PSFP) is used to filter frames at the ingress port that do not meet the configured policies. PSFP supports the following policing actions: • *Time-based policing*: This allows detection of incoming frames during periods when the stream gate is in the closed state. The intent is to support applications where the transmission and reception of frames across the network is coordinated such that frames are received only when the stream gate is open, and hence, a frame received by the stream gate when it is in the closed state represents an invalid receive condition [IEEE 802.1Q §8.6.5.1.2]. The Stream Gate Instance applies to one or more Streams. This complements 1Qbv, which applies to egress port. • *Rate-based policing*: This is supported by the Flow meter instances. This enables specification of the Committed Information Rate and Excess Information Rate. These meters apply to one or more streams and allow policing of streams that exceed the configured rate. • *Burst-based policing***.** This is supported by the *Flow meter instances*, indicating the length of supported burst (back-to back sending of streams). • *Frame length-based policing***.** Flow Meter instance allows the specification of filtering criteria based on the maximum frame lengths. *Stream filter instance table* (IEEE 802.1Q-2018 §8.6.5.1.1) specifies which filtering actions shall be applied to network traffic with varying granularity. It allows the application of policers (Stream Gate Instance and Flow meters*)* • per stream and • by Traffic Class. The PSFP in 802.1Q refers to the 802.1CB standard for identifying a stream. This specification allows for a variety of granularity levels in the policing. For example, use of null-stream stream identification could be used to police a whole Traffic Class. Or specifying a unique stream identification can be used to create a more granular policy. As this specification affects hardware resources, further work should be specified in TSN profiles. This mechanism is used to protect queues from unwarranted traffic and to maintain the established quality of service for specified traffic and streams. The recommendations below include a type of policing to be applied. To limit the bandwidth usage for a traffic type either by a single device or through the accumulation of traffic, policing traffic utilization at both ingress (through PSFP) and egress (through either IEEE 802.1Qav Credit-Based Shaping or IEEE 802.1Qbv Traffic Scheduling) should be used.

TSN Mechanisms	
Mechanism	**Description and Comments**
IEEE 802.1CB	**Frame Replication & Elimination for Reliability** This mechanism is part of the formal TSN set of enhancements and supplies a critical function for industrial networking systems –seamless redundancy from connection or network infrastructure outage. As stated in IEEE 802.1CB "This standard specifies procedures, managed objects, and protocols for bridges and end systems that provide identification and replication of packets for redundant transmission, identification of duplicate packets, and elimination of duplicate packets." When applied on a network with redundant, non-congruous paths, it ensures that the packets arrive at their destination without interruption even if link or network infrastructure occurs. Loss of packets through congestion is eliminated in a properly functioning TSN network via the Scheduled Traffic function. The loss of packets due to network or link outages is mitigated through the Frame Replication and Elimination function. The Per-Stream Filtering and Policing mechanisms specifies that the stream identification portion of this standard is applicable when PSFP is used. For this reason, it is not mentioned in the recommendations for PSFP. Recommendations for PSFP below therefore only reference the frame replication and elimination aspects of this mechanism.
Cut-through	**Cut-Through Switching** Cut-through switching is not an IEEE standard nor is there a working group at IEEE working on this. Cut-through switching is a means to further reduce latency as a bridge can transmit frames before the frame is fully received. In other words, it begins transmitting as soon as enough header information is received to determine to which outbound port the frame should be transmitted. Store and Forward bridges must wait until a frame is fully received before transmitting thereby increasing latency. This mechanism is used to reduce latency. To ensure the outbound queue is available, this feature is best used in combination with Traffic Scheduling. To protect the capability from mis-use or inappropriate frames, the PSFP mechanism should also be engaged. Standardization is required before interoperability between bridges and end-points can be expected.

Table 13: Description of TSN Mechanisms

MAPPED DEVICE TYPES

We recommend two type of devices: end-devices and bridges. The mappings recommend TSN features for each. In many industrial and manufacturing networks, end-devices are combined with end-devices in multi-port end-devices capable of bridging communication. In this case, the multiport end-device should be seen as both a bridge and an end-device with a virtual link

between the end-device and the bridge. The recommendation for end-devices or bridges would then apply to this device.

TRAFFIC TYPES MAPPINGS

Each section below maps TSN Mechanisms to the relevant traffic types. The order in which those are presented are in a priority that reflects the Traffic Class mappings recommended for the traffic type. Traffic scheduling with time-based exclusive gating introduces a superseding form of priority over the Priority Code Point/Traffic Class and Strict Priority mechanisms. Therefore, Network Control is presented as the first traffic type, but any scheduled traffic (i.e. IEEE 802.1Qbv) by default of exclusive gating, is given priority regardless of the traffic class.

MAPPING TRAFFIC TYPE: NETWORK CONTROL

This traffic type requires bandwidth and latency guarantees. Additional constraints need to be considered for this traffic type, for example clock synchronization (i.e. IEEE 802.1AS-Rev) frames shall not be preempted. The timestamp integrity of the clock synchronization mechanism or other network control protocols may be invalidated by the frame preemption.

The following mechanisms can be used to implement this traffic type:

1. *Mandatory*: QoS Strict priority, treated with highest priority Traffic Class 7 applicable to bridges.

   Frames from this traffic type are usually small, sporadic and the bandwidth requirements are low. The highest priority (traffic class [IEEE 802.1Q]) ensures that these frames are minimally delayed by other traffic types. When Qbv scheduling mechanisms are in place, the strict priority has an effect only in the case when scheduled queues are closed and multiple other non-scheduled queues are opened at the same time—and have a frame ready for transmission at the same time. In this case, Strict Priority queueing gives Network Control packets priority. Clock Synchronization (IEEE 802.AS-Rev clause 8.4.4) specifies that PTP frames do not carry VLAN-Tags, but they shall be identified by the PTP-Ether Type and treated with a specific priority (still under discussion).

   No user application should send data associated with the highest Traffic Class.

2. *Conditional*: If Frame Preemption is in effect, then network control traffic (i.e. IEEE 802.1AS-Rev) queues are considered Express Traffic, applicable to bridges.

   Typically, Precision Time Protocol (PTP), i.e. IEEE 802.1AS-Rev, frames are too small to be considered for pre-emption, but that may change. The standard does not specify any considerations for preemption. If PTP is preempted without specifications on how, implementations may vary and could cause PTP integrity issues.

   Therefore, PTP traffic should not be preempted as that may interfere with the time-synchronization function. Therefore, if preemption (IEEE 802.1Qbu) is used, the traffic class

associated with this traffic type shall be configured as express and not preemptable. This recommendation may be changed if PTP frame size is limited so that they may not be preempted or the standard specifies how PTP frames are preempted to avoid impacting PTP functionality.

3. *Conditional*: Cut-through switching, Store-and-Forward handling, applicable to bridges.

   If switches with cut-through capabilities are used, network control traffic shall be configured to use the store-and-forward mechanism. Network control traffic is typically exchanged between the neighboring bridging devices and therefore not appropriate for cut-through transmission.

MAPPING TRAFFIC TYPE: ISOCHRONOUS

Data Delivery Guarantees and no Tolerance to Interference are key characteristics of isochronous traffic. These deadline guarantees are dependent on the application cycle time. Networks with fewer hops naturally can support smaller cycle times. Additionally, scheduling or network analysis mechanisms ("network calculus") are needed to determine whether a set of applications' requirements regarding Data Delivery Guarantees and Tolerance to Interference can be met. Regardless of those mechanisms or tools, a set of TSN quality of service capabilities in the networking infrastructure is required to meet those requirements while still maintaining guarantees for other traffic types.

To guarantee negligible jitter or interference, there shall be a guarantee of no interfering frames from frames from other traffic types delay Isochronous traffic along its transmission path. This can be achieved by guaranteeing that no traffic class other than the one used for Isochronous traffic is allowed to transmit during the period when this traffic type is scheduled for communication. The following mechanisms can be used to implement this traffic type:

1. *Mandatory*: QoS–Strict priority, treated with high priority (Traffic Class 6) applicable to bridges.

   Exclusive gating supersedes the priority suggested by Traffic Class. As isochronous traffic uses exclusive gating (see Figure 1) the selection of the priority has no effect. Although Isochronous traffic has a higher priority than network control, we recommend using traffic class 6 instead of 7 as network control is assumed to always be present in a network whereas isochronous may not. In that case, other traffic types may use this traffic class.

2. *Mandatory*: Scheduled Traffic mechanism (802.1Qbv) applicable to bridges and end-devices.

   Exclusive gating is needed to satisfy the above defined Data Delivery Guarantee (deadline) and Tolerance to Interference (no jitter) for Isochronous traffic by ensuring no interference from other traffic types. End-devices should send the isochronous frames at a specific time with negligible jitter. Although Scheduled Traffic (802.1Qbv) is meant for bridges, the mechanism (or something similar) is needed on end-devices too.

Note: Other mechanisms, for example Frame Preemption, in specific scenarios may achieve similar or sufficient results, but are not the focus of this paper as they would not achieve the guarantees in a converged network scenario. A “Mandatory” recommendation therefore ensures the requirements are fulfilled.

3. *Mandatory*: Clock Synchronization (IEEE 802.1AS-Rev) applicable to bridges and end-devices.

   Clock synchronization is necessary for the coordination of the scheduled events (e.g. IEEE 802.Qbv gate-events and message-transmission times on end-devices).

4. *Mandatory*: Per-Stream Filtering and Policing (IEEE 802.1Qci) with Time-based policing applicable to bridges.

   Mechanisms are needed to protect the Scheduled Traffic from interference by messages introduced by misconfigured or faulty devices at ingress points for the network infrastructure. PSFP provides mechanisms to protect against following error scenarios:

   - more traffic is sent than specified either because of a misconfiguration or device behavior,
   - traffic is sent outside the time window as a result of a clock synchronization error and
   - stops other traffic types or unexpected frames (e.g. Denial of Service attacks) from using the Scheduled Traffic queues. This may be because of legacy configurations or incorrectly configured devices.

   Note that PSFP has options to drop frames or reassign the frame’s Traffic Class.

5. *Mandatory*: Stream Reservation (IEEE 802.1Qcc) is applicable to bridges.

   A network configuration function is needed that will receive information from applications and end-devices about the traffic types that will be supported. This function must have knowledge of the topology (or at least neighbors) and capabilities of the infrastructure. With this information, it will determine if requirements can be met and generate a schedule for its particular area of responsibility. This network configuration function may be implemented by using the centralized, distributed or hybrid configuration model. We do not address these implementations here.

   The configuration function will ensure:

   - The schedule of the time windows within each bridge device shall be done such that the forwarding of these frames along the transmission path can be conducted with required latency and negligible jitter. For example, between any two neighboring devices, the sending time of Scheduled Traffic must match the receiver’s PSFP (“ingress policing”).
   - Consistent exclusive gating (see Figure 1) shall be configured. Exclusive gating closes all other queues during the gate open and gate close events for the queue assigned to this traffic type. Gate open intervals shall be calculated so that all engineered Scheduled Traffic can be forwarded within the interval (i.e. at least 100% of the required bandwidth

for Scheduled Traffic is reserved). Traffic scheduling (IEEE 802.1Q-2018 section 8.6.8.4**)** specifies that the device shall check if there is enough time interval left to transmit the frame completely before the gate closes, before start of transmission of an unscheduled frame the device. This is called “guard-banding” (described in more detail in IEEE 802.1Q Annex Q).

- Prohibit collisions or overlapping between multiple isochronous streams in an unintended manner. These scheduled streams should be separated in time within the same queue.
- Ensure exclusive gating for Scheduled Traffic does not significantly delay the frames from the Network Control traffic, which includes PTP for clock synchronization. In other words, exclusive gates must be open less than the timeout intervals used by network control protocols.

6. *Optional: Frame Replication and Elimination* (IEEE 802.1CB) for redundancy applicable to bridges and end-devices

   Depending on network topology and an application’s Tolerance to Loss requirements, it is optional whether replication and elimination of frames on redundant, non-congruous paths in the network is used.

7. *Optional: Cut-Through switching* is applicable to bridges

   When applications require cycles in the range of < 250 µsec and medium-to-large line topologies with more than 25 bridged endpoints, cut-through functionality may be required to meet latency requirements. This depends on the frame size, number of bridges, topology and link speed. This feature is needed to overcome the latency limitations caused by the store-and-forward delay and may even be required in case of 1Gbit/s link speeds.

   Cut-through propagation is guaranteed only in combination with the exclusive gating feature of scheduled traffic, otherwise there are no guaranties that a cut-through frame is using a switch port which is occupied (in use) by another frame.

   If Cut-Through forwarding is employed, it is not possible for a switch implementation to determine frame length before transmitting. It is thus possible that a Cut-Through frame violates a gate-close event of its assigned queue by being too large. Faulty devices or misconfiguration can lead to such scenarios and it is highly recommended a switch implement mechanisms to prevent fault propagation, such as truncating the transmission of the frame, thereby invalidates the offending frame.

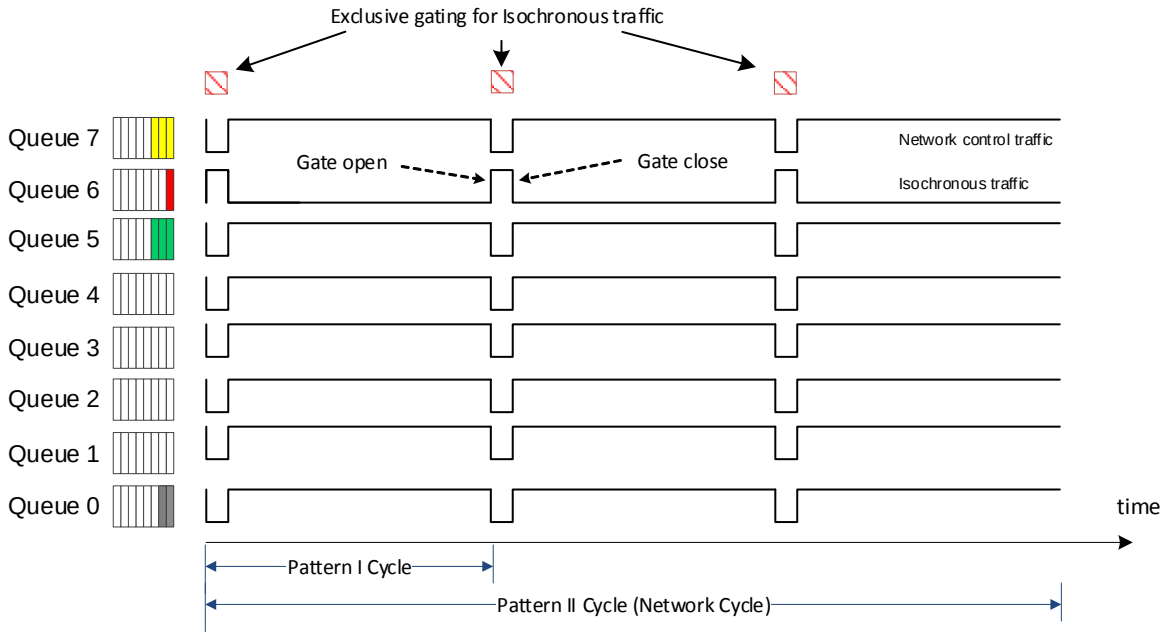

Figure 1: Exclusive gating for Isochronous traffic.

MAPPING TRAFFIC TYPE: CYCLIC

The Cyclic traffic type requires bounded latency where a limited amount of interference can be tolerated.

The mapping recommendations assume that isochronous traffic will be present in the network and therefore traffic scheduling (.1Qbv) is required and present in the network infrastructure, though isochronous traffic may not be present, as typically found in existing deployments. Therefore, other traffic shaping mechanisms may be used to achieve the traffic type requirements without the use of traffic scheduling (.1Qbv). This is reflected in the two options outlined for the Cyclic traffic type.

Depending on the parameters (period, latency and bandwidth) the following alternative implementation options are possible:

- *Strict Priority.* This option uses strict priority QoS in the network by assigning Cyclic Traffic to the queue with the second highest traffic class (out of the queues that do not use exclusive gating) where only Network Control and Isochronous traffic types have higher priority. In this case, it is assumed that a network configuration function can analyze (e.g., network calculus) the expected worst-case latency that Cyclic traffic may experience with knowledge of all the traffic in the network. The network calculus shall analyze the effect of different datastreams of the same traffic type, the Isochronous traffic, the Network

Control traffic type and the interference from lower priority traffic already in transmission.

Optionally frame preemption mechanisms may be deployed to help satisfy the latency requirements by reducing the interference from lower priority traffic classes in transmission.

Advantages: No oversampling (see below) is used –bandwidth reservation is not wasted

Disadvantages: Strong impact on communication latency from traffic types of numerically equal or higher Traffic Class. Adding streams of type Network Control (e.g. extending the network), isochronous or cyclic (e.g. potential future application updates) affect the maximum latency and communication jitter.

- *Scheduled Traffic*. Traffic Scheduling may be used for Cyclic traffic to guarantee bandwidth and bounded latency. As end-devices may not be time synchronized for the purpose of message (or frame) exchange although they may use time synchronization for the timestamping of events at the application level. Therefore, the network cannot assume arrival of the packets in a timely manner. A schedule can be created whereby exclusive gates are opened frequently enough (gating cycle is time between gate open and the next gate open) where latency would be bounded to the network communication latency plus 1 gating cycle. In this case the network from the first switch (edge switch) through to the listeners will forward the traffic as scheduled. Oversampling, where the gating cycle is less than the application cycle, may be required to achieve the application's required bounded latency. Oversampling leads to unused bandwidth as the exclusive gates are not always used.

  Advantages: This approach delivers guaranteed bandwidth, and no interference from other traffic types. Optionally, the Traffic Class gate may be left open beyond the exclusive gate to lower the latency for a portion of the Cyclic frames. But the bounded latency is still dependent on the gating cycle and the implied oversampling defines the amount of unused bandwidth. Figure 2 shows an example of the configuration, where exclusive gating is used and the gate left open for cyclic traffic (Traffic Class 5).

  Disadvantages: Depending on the configured gating cycle, this option leads to either:

  - bounded latency is greater than application cycle time if the gating cycle is equivalent to the application cycle time (i.e. no unused bandwidth) or
  - unused bandwidth when the gating cycle is smaller than the application cycle.

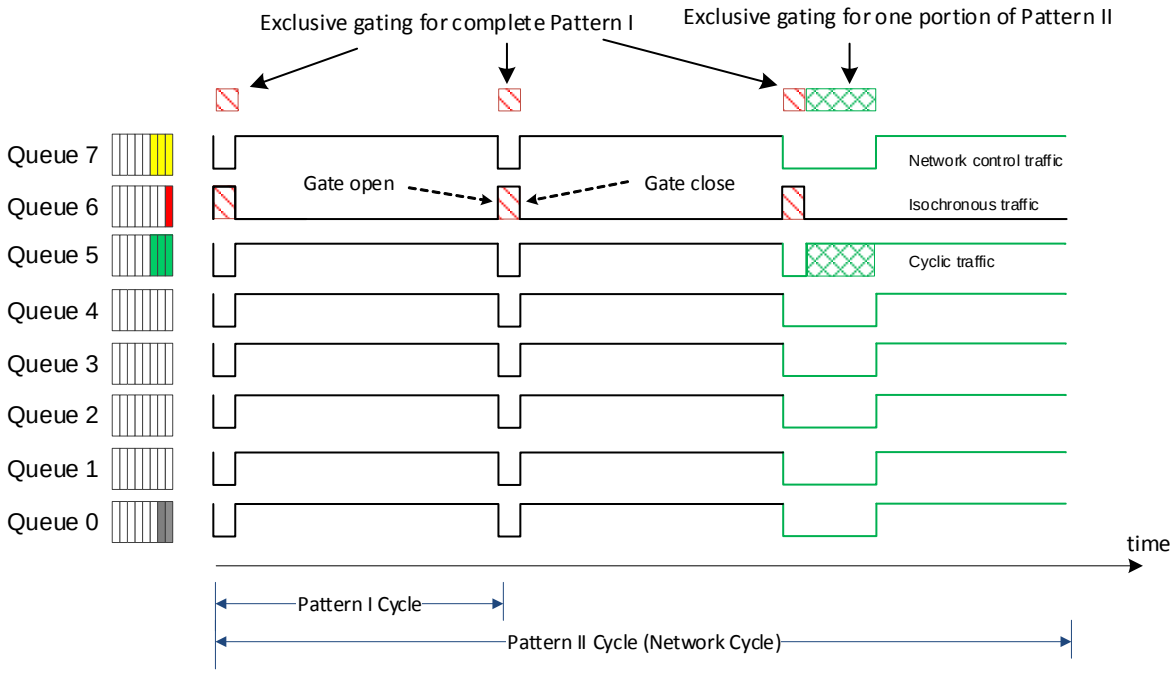

Figure 2: Exclusive gating for Cyclic traffic.

MECHANISMS FOR IMPLEMENTING OPTION STRICT PRIORITY:

1. *Mandatory: QoS—Strict priority, treated with priority Traffic Class 5 applicable to bridges:* First and second highest traffic classes are used for Network Control and Isochronous traffic. Cyclic traffic receives priority over all other traffic except Network Control or when Isochronous traffic is in-use.

2. *Mandatory: Per-Stream Filtering and Policing* (IEEE 802.1Qci) with Rate-based policing is applicable to bridges: This mechanism is needed to protect the traffic potential interference by:
   - policing traffic if more traffic is sent than specified for a specific data stream and
   - policing or retagging to best-effort (or lower priority) if non-configured data streams use the same traffic class (PCP).

3. *Mandatory: Stream Reservation* (IEEE 802.1Qcc) is applicable to bridges: A “network configuration” function is needed which will receive information from applications and/or end-devices about the traffic types that will be supported for PSFP configuration.

4. *Recommended: Frame preemption (IEEE 802.1Qbu),* where cyclic queues are marked as Express Traffic is applicable to bridges and end-devices: Frame preemption can be used to limit the interference from lower traffic classes with frames in transmission at the time Cyclic traffic is available for transmission. Isochronous traffic uses exclusive gating and is not

affected by preemption. End-devices must also support this as they may receive pre-empted frames.

5. *Optional: Frame Replication and Elimination* (IEEE 802.1CB) for redundancy applicable to bridges and end-devices Depending on network topology and an application's Tolerance to Loss requirements, the replication and elimination of frames so as to conduct them on redundant, non-congruous paths within the network is optional.

We recommended that a configuration mechanism is applied to analyze network traffic requirements (i.e. Network Calculus) to determine whether the latency requirements can be met.

MECHANISMS FOR IMPLEMENTING OPTION SCHEDULED TRAFFIC:

These are the union of mechanisms for Cyclic Traffic-Option and mechanisms needed for Isochronous traffic when applicable to bridges, with the following exceptions:

Per-Stream Filtering and Policing (IEEE 802.1Qci) with Rate-based policing should be used. It may be applicable to use Time-based policing on interlinks between bridges after the traffic has been Rate-based policed on ingress to the network.

Cut-through should not be applied to this traffic type. Depending on network topology and an application's Tolerance to Loss requirements, a means to guarantee packet delivery should be considered. Therefore, the replication and elimination of frames so as to conduct them on redundant, non-congruous paths within the network (IEEE 802.1CB) is considered optional.

MAPPING TRAFFIC TYPE: EVENTS

The Event traffic type contains traffic with the same characteristics, but there are two application categories that differ in the latency and Tolerance to Loss requirements:

- Applications that send "Alarms and Operator Commands"—tolerate latency up to 2 seconds and can contain large frames up to 1500 bytes. In case of alarm showers, a relatively high number of frames are issued. Forwarding of up to 2000 frames per second should be guarantee-able, even though more frames may be generated. The applications can tolerate frame loss in such scenarios.
- Applications that send Control Events—require latency in the range of 10 ~ 50ms and have short frames up to 200 bytes. Frame loss is to be minimized.

As the Data Delivery Guarantee (latency) requirement of the application categories differ significantly, and to guarantee the latency of the Control Event traffic under the condition that a shower of alarm traffic is active, two Traffic Classes shall be used, one for the Control Events and second for Alarms and Operator Commands.

TRAFFIC TYPE: EVENTS—CONTROL EVENTS

Mechanisms for implementing this traffic type for Control Event applications are:

1. *Mandatory: QoS—Strict priority*, treated with priority Traffic Class 4 applicable to bridges.
2. *Mandatory: Per-Stream Filtering and Policing* (IEEE 802.1Qci) with Rate-based policing is applicable to bridges

   As Control Events data is sporadic, some upper bound for accumulated the worst case bandwidth usage shall be given by the application.
3. *Mandatory: Stream Reservation* (IEEE 802.1Qcc) is applicable to bridges.

   A "network configuration" function is needed which will receive information from applications and/or end-devices about the traffic types that will be supported for PSFP configuration.
4. *Optional: Frame Replication and Elimination* (IEEE 802.1CB) for redundancy applicable to bridges.

   Depending on network topology and an application's Tolerance to Loss requirements, the replication and elimination of frames so as to conduct them on redundant, non-congruous paths within the network is optional.
5. *Optional: Frame Preemption (IEEE 802.1Qbu),* where Control Event queues are "Express Traffic" is applicable to bridges and end-devices

   In case that preemption is available in the network components, the traffic class associated to Control Events shall be configured as Express Traffic and thereby non-preemptable. This traffic has small frames (up to 200 Bytes), and will not significantly affect the Network Control and Cyclic traffic types.

TRAFFIC TYPE: EVENTS—ALARMS AND OPERATOR COMMANDS

Mechanisms for implementing this traffic type for Alarms and Operator Commands applications are:

1. *Mandatory: QoS—Strict priority*, treated with priority Traffic Class 3 applicable to bridges

   In some cases, more bandwidth is intentionally generated than reserved. In such a case this traffic will utilize the bandwidth intended to be used by the traffic with lower traffic classes (priorities).
2. *Mandatory: Clock Synchronization* (IEEE 802.1AS-Rev) applicable to bridges and end-devices.

   Clock Synchronization is necessary for timestamping and observing sequence of events on end-devices.
3. *Mandatory: Per-Stream Filtering and Policing* (IEEE 802.1Qci) with Rate-based policing is applicable to bridges.

PSFP is used to manage the bandwidth of end-device data streams at their ingress into the network and the accumulated traffic type bandwidth utilization along the network path. For the case that alarm applications are designed to send more data than the bandwidth reservation (e.g., in case of alarm showers exceed the 2000 frames/second), the PSFP mechanism is *mandatory* to perform rate limitation. PSFP also allows for the re-marking of traffic exceeding bandwidth utilization rates allowing the traffic to be handled as lower priority traffic or to be dropped altogether. This option may be an advantage to other policing mechanisms.

4. *Mandatory: Stream Reservation* (IEEE 802.1Qcc) is applicable to bridges and end-devices.

   A network configuration function is needed that will receive information from applications and end-devices about the traffic types that will be supported for PSFP configuration.

5. *Optional: Credit-Based Shaping* (IEEE 802.1Qav) is applicable to bridges and end-devices.

   To maintain the reserved bandwidth, credit-based shaping may be used. This enables bridges and end-points to queue frames that exceed credits allocated. It provides end-device more flexibility on how to handle alarm bursts.

6. *Optional: Frame Preemption* (IEEE 802.1Qbu), where Alarms and Operator Command queues are “Preemptable”, is applicable to bridges.

   When frame preemption is available in the network components, the traffic class associated to Alarms and Operator Commands shall be configured as preemptable traffic to minimize the interference effect on Cyclic, Network Control and Control Events traffic types. This also increases available bandwidth for this traffic type as the packet can be distributed over small amounts of available time.

MAPPING TRAFFIC TYPE: CONFIGURATION & DIAGNOSTICS

This traffic type requires bandwidth guarantees. Due to the relaxed latency requirements (100ms) this traffic type can be considered as sporadic (non-cyclic) traffic.

Necessary mechanisms for implementing this traffic type:

1. *Mandatory: QoS—Strict priority*, treated with priority Traffic Class 2 applicable to bridges

   Maintains the higher priority of other traffic types.

2. *Mandatory: Per-Stream Filtering and Policing* (IEEE 802.1Qci) with Rate-based policing is applicable to bridges.

3. *Mandatory: Stream Reservation* (IEEE 802.1Qcc) is applicable to bridges.

4. *Optional: Frame Preemption* (IEEE 802.1Qbu), where the Configuration and Diagnostics queue(s) are “Preemptable”, is applicable to bridges

MAPPING TRAFFIC TYPE: BEST EFFORT

This traffic type uses all the remaining bandwidth. In some cases, it is required to have some bandwidth guarantees. Following mechanisms can be used to implementing this traffic type:

1. *Mandatory: QoS—Strict priority*, treated with priority Traffic Class 0 applicable to bridges
2. *Optional: Frame Preemption* (IEEE 802.1Qbu), where the Best Effort queue(s) are “Preemptable”, is applicable to bridges

MAPPING TRAFFIC TYPES: VIDEO & AUDIO

These two traffic types are intended for human consumption.

As this traffic is less critical than ICAS traffic, it will use a lower traffic class but higher than Best Effort.

As both traffic types have similar characteristics (the difference is on the absolute value of the latency requirement), there should be one Traffic Class for both these traffic types.

Mechanisms for implementing these two traffic types are:

1. *Mandatory: QoS - Strict priority*, treated with priority Traffic Class 1 applicable to bridges
2. *Recommended: Credit-Based Shaping* (IEEE 802.1Qav) is applicable to bridges and end-devices

   In professional audio/video-based systems credit-based shaping is used to maintain some latency upper bounds. The given guarantees are possible when these frames use traffic classes with higher priorities. In the case of converged industrial network, additional traffic with scheduling, and preemption is introduced, and these Audio-Video Bridging, AVB (IEEE 802.1QAV), guarantees are not achievable to the same degree. In this situation latencies for this traffic type depend on application-specific factors such as rate and length of scheduled data streams with exclusive gating, number of streams, network load and usage of preemption.

   In this case, credit-based shaping will contribute that one talker/sender (within this traffic type) will not monopolize the bandwidth left over for this traffic type (at least the video traffic will not cause longer latencies in the audio traffic).

3. *Mandatory: Per-Stream Filtering and Policing* (IEEE 802.1Qci) with rate-based policing is applicable to bridges.
4. *Mandatory: Stream Reservation* (IEEE 802.1Qcc) is applicable to bridges.

5. *Optional: Frame Preemption (IEEE 802.1Qbu), where the Video and Audio queue(s) are "Preemptable"*, is applicable to bridges.

MAPPING SUMMARY

This table summarizes the traffic type mappings described above.

Types	802.1Q Strict Priority	Traffic Class	802.1Qbv (exclusive gating)	802.1AS-Rev Clock Synch	Cut-Through	802.1CB—Frame Replication	802.1Qbu—Frame Preemption	802.1Qci—Ingress Policing	802.1Qav—Credit Based Shaping	Reservation/Scheduling
Isochronous	M	6	M	M	O	O		M^T		M
Cyclic—Option: Strict Priority	M	5				O	R	M^R		M
Cyclic—Option: Scheduled Traffic	M	5	M	M		O		M^R		M
Events—Control	M	4				O	O	M^R		M
Events—Alarms & Operator Commands	M	3		M			O	M^R	O	M
Config & Diag.	M	2					O	M^R		M
Network Control	M	7			C		C			
Video, Audio, Voice	M	1					O	M^R	R	M
Best Effort	M	0					O			

Table 14: Summary of Traffic Type Mappings

Legend:

- M: Mandatory
- O: Optional

- C: Conditional
- R: Recommended
- T: Time-based
- R: Rate-based

Our selection of the mechanisms for support of traffic types considers the presence of the traffic types in combination, e.g. Network Control type will always be present. As well, in some use cases there is no Isochronous traffic, nonetheless our selection considers it.

In case that there are devices that do not support eight (priority) queues, the mapping of the traffic types to the priority queues shall consider the following:

- *Mandatory:* Network Control shall have a separate queue and have the highest priority
- *Mandatory:* Isochronous shall have a separate queue
- *Recommended:* Cyclic shall have a separate queue (in case that Isochronous traffic is not present)
- Cyclic, Control Events, Alarms and Operator Commands and Configuration and Diagnostics Traffic Types can be mapped in one queue
- Best Effort, Audio and Video Traffic Types can be mapped in one queue

SUMMARY

We have documented the types of traffic found in typical manufacturing ICAS and the network performance characteristics they need. We presented a suitable mapping of the traffic types to QoS capabilities, including the TSN capabilities. This mapping should help vendors deliver interoperable and certifiable devices and network infrastructure to the industry overall.

With the enhanced QoS capabilities from IEEE 802.1 TSN, the manufacturing ecosystem has a chance to converge devices and applications onto a single, open, standard Ethernet network in ways not possible before. This convergence leads to greater openness to IoT innovations demanded by customers. That is the overall goal of the IIC and the companies working in this testbed.

AUTHORS AND LEGAL NOTICE

This document is a work product of the Industrial Internet Consortium Time-Sensitive Networking Testbed.

Authors: The following persons have written substantial portions of material content in this document:

- Astrit Ademaj (TTTech)
- David Puffer (B&R)
- Dietmar Bruckner (B&R)

- George Ditzel (Schneider Electric)
- Ludwig Leurs (Bosch Rexroth)
- Marius-Petru Stanica (ABB)
- Paul Didier (Cisco)
- René Hummen (Belden/Hirschmann)
- Richard Blair (Schneider Electric)
- Thomas Enzinger (B&R)

Contributors: The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document:

- Florian Frick (ISW)
- Jeff Lund (Cisco)
- Andreas Papa
- Paul Andrews

Technical Editor: Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors and Contributors into an integrated document.
