Time Sensitive Networks for Flexible Manufacturing Testbed - Description of Converged Traffic Types

An Industrial Internet Consortium Results White Paper

IIC:WHT:IS3:V1.0:PB:20180417

Table of Contents

This white paper describes application traffic types that are 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 I lists traffic types as a means to structure network transmission priority and packet drop preference. We enhance those traffic types by adding those found in typical manufacturing Industrial Automation and Control Systems (IACS), with a list of characteristics to describe them precisely. We intend later to recommend IEEE 802.1 TSN mechanisms to support those traffic types.

We write for those working on establishing TSN as a core communication technology for industrial automation and control and therefore expect the reader to be familiar with terms of art in these domains. Readers should have a basic understanding of manufacturing applications and IACS. We intend to share the white paper with the various standards organizations and consortia working on TSN adoption, including but not limited to the Institute of Electrical and Electronics Engineers (IEEE), International Electrotechnical Commision (IEC), Avnu Alliance, CC-Link Partner Organization (CLPA), Labs Network Industrie 4.0 (LNI4.0), ODVA, OPC Foundation, Profinet International and Sercos International.

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

The Industrial Internet Consortium (IIC), with over 250 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 authorized 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. Currently, the testbed has over 25 participants with a range of companies including chip vendors, IACS vendors, network infrastructure/testing vendors and testing/certification organizations. The testbed liaises with many 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 variety of functions and capabilities to Ethernet to make it more suitable to industrial applications that require more deterministic characteristics than were possible in previous Ethernet implementations. The following table summarizes these enhancements.

Standard	Title
IEEE 802.1Qav	Forwarding and Queuing Enhancements for Time-Sensitive Streams
IEEE 802.1AS-Rev	Timing and Synchronization for Time-Sensitive Applications
IEEE 802.1Qbu & IEEE 802.3br	Frame preemption
IEEE 802.1Qbv	Enhancements for Scheduled Traffic
IEEE 802.1Qca	Path Control and Reservation
IEEE 802.1Qcc	Stream Reservation Protocol (SRP) Enhancements and Performance Improvements
IEEE 802.1Qci	Per-Stream Filtering and Policing
IEEE 802.1CB	Frame Replication & Elimination for Reliability

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 Testbed 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 devices and 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.

This white paper focuses on that last and describes the traffic patterns in a manufacturing environment that converge onto a single, open TSN network. A future revision of the whitepaper will map 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 may rely on the QoS they receive from the network and how that may affect the QoS of other traffic types. The specific traffic 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 or used for audio services provided in the manufacturing zone,
- *Video*, which may be part of an IACS or used for video services provided in the manufacturing zone and
- *Best Effort*.

And 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
- *Alarms 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 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, and *horizontal* communication between the automation and control devices. Horizontal communication can be broken down to controller-to-controller and controller-to-field-equipment (a.k.a. input and outputs or I/O). Historically, various types of fieldbuses, besides the Ethernet-based communication, support these diverse communication requirements and thereby segmenting the IACS traffic flows in separate networks.

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) that

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 where standard Ethernet is used.

Vertical communication traffic comprises 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 controllers, I/O equipment, drives, encoders and other field-level communication. We may distinguish here these traffic types:

Isochronous: with small frame sizes (often no more than 84 bytes), very short cycle times (usually less than 1 millisecond or ms) and a low jitter requirement. An example is turbine control in a power generation hydro plant, or a controller to drive an encoder.

Cyclic controller-controller: where controllers exchange variables as a part of shared applications, usually with maximum frame sizes 1500 bytes and cycle times between 100microseconds (µs) up to 1 second. There is more tolerance to jitter and frame loss than isochronous communication.

Cyclic controller-IO or controller-drive for automation applications: where sensors and actuators exchange data with controllers with smaller frame sizes up to 600 bytes and cycle times up to 60ms. There is a tolerance to jitter and to frame loss.

Alarms and events: where sensors, actuators and controllers communicate change-of-state, warnings when thresholds are exceeded or operator commands. These are acyclic with variable frame sizes and are tolerant to jitter and frame loss.

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	
Characteristic	**Description**
Data transmission periodicity	Traffic types consist of data streams that can either be transmitted in a *cyclic/periodic* (e.g. signal transmission) or *acyclic/sporadic* (e.g. event-driven) manner.
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 *acylcic/sporadic* traffic types, 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 in a stream is guaranteed to occur at all registered receivers at or before a predictable time (i.e. in a communication cycle), • *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 *"n.a." or not applicable*.

Traffic Types	
Characteristic	**Description**
Tolerance to interference	Denotes the application's tolerance of a certain amount of *communication jitter* (the latency variation of the packet's transmission) 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 to be specified. Other sources of jitter in application processing besides network communication 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 *acylcic/sporadic* data transmission periodicity types, this characteristic does not apply (n.a.) and jitter need not be specified.
Tolerance to loss	Denotes the application's tolerance to a certain amount of consecutive packet loss in network transmission. 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.
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* (the data is sent with variable size, 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 vary exceedingly or cannot be determined at design or configuration time, *data volume estimates* (e.g. required bandwidth) is provided.

Traffic Types	
Characteristic	**Description**
Criticality	Describes the criticality of the data for the operation of the critical parts of the system. Application criticality is used to guide the selection of the appropriate QoS/TSN mechanisms 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. Unmet QoS guarantees (e.g. latency, jitter or data loss) of this traffic type may cause critical system malfunction and data 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. Unmet QoS guarantees of this traffic type 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. These traffic types typically don't have specific latency or jitter guarantees. 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.

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

ISOCHRONOUS

The 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 100µs. For tight control loops, communication 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 type can be used for controller-to-controller and controller-to-I/O-communication 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).

Traffic Type I: Isochronous		
Characteristics		**Notes**
Periodicity	Cyclic/periodic	
Period	100µs ~ 2ms	
Application synchronized to network	Yes	
Data delivery guarantee	Deadline	Usually within one data transmission period
Tolerance to interference	0	
Tolerance to loss	No (0 frames)	Seamless redundancy is required
Application Data size	Fixed (30 ~ 100 bytes)	
Criticality	High	

CYCLIC

This 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 will be distributed over the cycle time. 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 and controller to I/O 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 1500 bytes and
- fast *diagnostic data* for drives that produce 1500 bytes samples at a rate up to every 4 ms that is used to verify drive functionality,
- *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 1500 bytes;

Traffic Type II: Cyclic		
Characteristics		**Notes**
Periodicity	Cyclic/periodic	
Period	2 ~ 20ms	
Application synchronized to network	No	
Data delivery guarantee	Latency	Typically 50% of the period is worst case and lower network latency improves control.
Tolerance to interference	Yes, <= latency guarantee	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).
Application Data size	Fixed (50 ~ 1000 bytes)	
Criticality	High	

ALARMS AND EVENTS

In a system when an input or output variable change occurs that requires attention, Alarm and Event messages are generated. Depending upon the change, this might be a single message, or a flurry of messages (domino effect). While the messages may be directed to different end devices, typically, they are directed at a single device, like an HMI or SCADA system. The network must be able to handle a burst of messages without loss, up to a certain number of messages or data size over a defined period.

After this period, messages can be lost until the allowed bandwidth quantity has been restored.

Examples include

- *process alarms and events* that create traffic that may require 1 to 2 seconds latencies and is acyclic but prone to flooding when issues arise in the process being controlled. Maximum frame size varies by vendor and application but may reach 1500 bytes and
- *operator commands* create another type of alarm and event traffic that is acyclic and has a latency up to 1 second. Maximum frame sizes vary following each vendor but are usually smaller than the previous ones, reaching 500 ~ 600 bytes.

Traffic Type III: Alarms and Events		
Characteristics		**Notes**
Periodicity	Acyclic/sporadic	
Period	n.a.	
Application synchronized to network	No	
Data delivery guarantee	Latency (100ms ~ 1s)	A bandwidth guarantee is also implied as stated above.
Tolerance to interference	n.a.	To be defined by the application.
Tolerance to loss	Yes	For example, alarm showers of up to 2000 alarms per second must be guaranteed, after which some packet loss is acceptable. The number is application dependent.
Application data size	Variable (50 ~1500 bytes)	
Criticality	High	

CONFIGURATION & DIAGNOSTICS

This type is used for the transport of configuration 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.

IACS configuration, maintenance and operator triggered diagnostics use this traffic type. Network and system management and configuration (e.g. SNMP, RESTCONF/NETCONF, firmware updates) protocol traffic also belongs to this traffic type.

Examples include:

- configuration activities create traffic with maximum frame sizes (1500 bytes) 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, and
- process information from the application, such as order scheduling and production.

Traffic Type IV: Configuration & Diagnostics		
Characteristics		**Notes**
Periodicity	Acyclic/sporadic	Some process supervision/diagnostic data may be sent periodically with higher periods (500ms ~2s).
Period	n.a.	
Application synchronized to network	No	
Data delivery guarantee	Bandwidth	
Tolerance to interference	n.a.	
Tolerance to loss	Yes	No seamless redundancy is required.
Application Data size	Variable	Can be large packets of 500 ~ 1500 bytes
Criticality	Medium	

NETWORK CONTROL

This type contains network control messages, like those for synchronizing time (IEEE 802.1AS a.k.a. Precision Time Protocol or PTP), for network redundancy (e.g. MSTP, RSTP), topology detection (e.g. LLDP). 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. PTP traffic due to its small size and the nature of the time-stamping shall not be preempted.

Traffic Type V: Network Control		
Characteristics		**Notes**
Periodicity	Cyclic/periodic	
Period	50ms ~ 1s	
Application synchronized to network	No	
Data delivery guarantee	Bandwidth	Typically 1 ~ 2 Mbps.
Tolerance to interference	Yes	Transmission of PTP frames should not be interrupted. Communication 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).
Application data size	Variable (50 ~ 500 bytes)	
Criticality	High	

BEST EFFORT

Best effort traffic follows one of two rules: either it suffers from data loss when higher priority traffic uses all the allocated bandwidth (default), or it can use a guaranteed bandwidth allocation. Best effort provides no delivery guarantees in the former case, and bandwidth guarantees in the latter.

Traffic Type VI: Best Effort		
Characteristics		**Notes**
Periodicity	Acyclic/sporadic	
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	
Application data size	Variable (30 ~1500 bytes)	
Criticality	Low	

VIDEO

Video traffic is the streaming of video data between end-points. 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 10ms delay and, hence, maximum jitter (one way transmission through the LAN infrastructure of a single campus)."

Traffic Type VII: Video		
Characteristics		**Notes**
Periodicity	Acyclic/sporadic	
Period	n.a.	
Application synchronized to network	No	
Data delivery guarantee	Latency	Less than 10ms depending on the application
Tolerance to interference	n.a.	
Tolerance to loss	Yes	Loss of packets may lead to decreased quality, but not necessarily application failure
Application Data size	Variable	Large packets (1000 - 1500 bytes)
Criticality	Low	

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 100ms delay, or other applications with low latency as the primary QoS requirement".

Traffic Type VIII: Audio/Voice		
Characteristics		**Notes**
Periodicity	Acyclic/sporadic	
Period	n.a.	
Application synchronized to network	No	
Data delivery guarantee	Latency	Less than 100ms depending on the application
Tolerance to interference	n.a.	
Tolerance to loss	Yes	Loss of packets may lead to decreased quality, but not necessarily application failure.
Application Data size	Variable	Large packets (1000 - 1500 bytes)
Criticality	Low	

CONCLUSION

This white paper outlined the types of traffic found in typical manufacturing IACS and the network performance characteristics they need. In a future release, the paper will be expanded to include mappings of the traffic types and performance characteristics to QoS capabilities, including the enhanced TSN capabilities. This mapping should help the underlying standards organizations to 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 can converge devices and applications onto a single, open, standard network in ways not possible before. This convergence will lead to greater openness to IIoT 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 Networks for Flexible Manufacturing Testbed chaired by Paul Didier (Cisco).

Authors: The following persons contributed substantial written content to this document:

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

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

- Florian Frick (ISW)
- Jeff Lund (Belden/Hirschmann)

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