4.2 Traffic Type Characteristics

The following application-centric communication characteristics enable the identification of a number of distinct traffic types that are shared among sets of industrial applications:

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.
Data transmission time is synchronized to network cycle	Denotes the capability of application to select the data transmission time of a periodic traffic to a specific point in time within the network cycle. Applications 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: • *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. Please note that the requested data delivery guarantee takes as a reference, the point in time of frame transmission at the talker • *deadline*: data delivery of each packet in a stream is guaranteed to occur at all registered receivers at or before a predictable time. Please note that the requested data delivery guarantee takes as a reference, the point in time of the start of a communication cycle. From the network point of view the deadline requirement can be expressed as latency (if talker sending point in time is known), but from an application point of view it is the point in time when frames are received at the listener • *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*.
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.

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 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.