# Overview of TSN use cases

*Japan Automotive Software Platform and Architecture*

2019.11.14

Takumi Nomura (Honda)

Hideki Gotoh (Toyota)

Yoshihiro Ito

(Nagoya Institute of Technology)

# Objective

- Provide use case study examples to create the Automotive Profile.
  - ✓ Create use cases (We are here)
  - ✓ Extract Requirements
  - ✓ Profiling

| | Use cases from JASPAR |
|---|---|
| UC1 | Connected-Car with 5G network |
| UC2 | Functional Safety |
| UC3 | Real-time communication |
| UC4 | Security |
| UC5 | In-Vehicle Traffic Types |

# UC1. Connected-Car with 5G network

- We recommend to investigate the requirement for In-Vehicle Network as a part of End-2-End (E2E) system for Connected-Car with 5G network.

- Use cases for Connected-Car with 5G network should be carefully discussed in 802.1DG because 5G network continues dynamically evolving and requires the updatability and upgradability of In-Vehicle Network which should be able to support additional new service applications after market.

- Use cases for Connected-Car will use the sophisticated network performance of 5G network as a part of E2E system from ECU to Server in Cloud.
  5G network includes the specification of eMMB and URLLC which can enable attractive E2E service applications if there is no bottle-neck part of In-Vehicle Network.

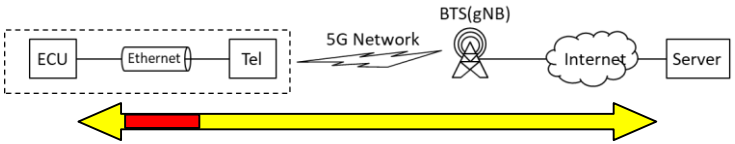

| | Data rate (5G Network) | Latency (5G Network) | Reliability (5G Network) |
|---|---|---|---|
| 5G (Sub 6GHz) | Depends on Category | < 1ms | 99.999 % |

Specification of 5G Network

eMMB: enhanced Mobile Broadband
URLLC: Ultra Reliable Low Latency Communications

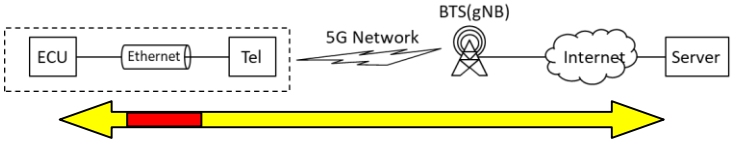
# UC1. Connected-Car with 5G network

- **High data rate** of 5G Network should be kept on all part of E2E system to avoid the bottleneck of low data rate so that In-Vehicle Network should have the same capability of High data rate.
- **Latency** is cumulative total of the latencies of all part so that we need to know them completely in order to define the requirement of latency for In-Vehicle Network part.
- **Reliability** is the total multiplication value of the reliability of all part so that we need also to know the reliability of each part.




| Scenario | Max-allowed E2E Latency | Reliability | User experienced Data rate |
|---|---|---|---|
| ITS Infrastructure backhaul | 30ms | 99.999% | 10Mbps |

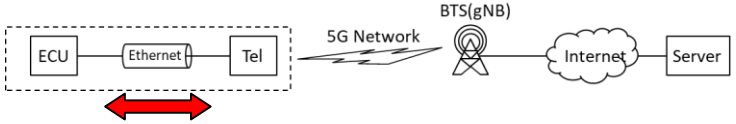
Use case defined in 3GPP TS 22.261 V15.8.0 (2019-09) (Rel.15)
" 7. Performance Requirements "




| Scenario | User experienced Data rate |
|---|---|
| 5 Dense Urban | DL: 300Mbps UL: 50Mbps |
| 6 Broadcast like service | DL: 200Mbps UL: n/a |
| 8 High Speed Vehicle | DL: 50Mbps UL: 25Mbps |
| (Ref) 3 Indoor hotspot (*1) | DL: 1Gbps UL: 500Mbps |

*1 : Not vehicle relevant use case, but can be hotspot in vehicle

**Requirements defined for In-Vehicle Network (Ethernet) (Draft)**




| 5G Scenario for Vehicle | Latency | Reliability | User experienced Data rate |
|---|---|---|---|
| ITS Infrastructure backhaul<br>5 Dense Urban | ?? ms | 100% ?<br>with redundant NW? | DL: 300Mbps UL: 50Mbps |

# UC2. Functional Safety

- Application of TSN standards for Functional Safety

We analyzed TSN standards from the “failure modes” of communication analyzed in functional safety (ISO 26262-5:2018) perspective.

Considered effective combinations of TSN standards for functional safety.

Extracts from ISO 26262-5:2018, Annex D, TableD.1－Analyzed failure modes

| Element | Analyzed failure modes |
|---|---|
| Data transmission | Loss of communication peer |
| | Message corruption |
| | Message unacceptable delay |
| | Message loss |
| | Unintended message repetition |
| | Incorrect sequencing of message |
| | Message insertion |
| | Message masquerading |
| | Message incorrect addressing |

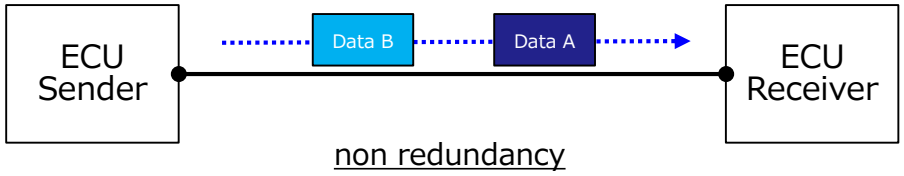
## Summary example

| Analyzed failure modes | Application of TSN standards for Functional Safety | | |
|---|---|---|---|
| | good | NOT good | Notes |
| Loss of communication peer | – | – | |
| Message corruption | – | **802.1AS** | **・Requires mechanisms such as CRC（FCS）<br>- Add CRC function (optional)** |
| Message unacceptable delay | 802.1CB | – | |
| Message loss | 802.1CB | – | |
| Unintended message repetition | – | – | |
| Incorrect sequencing of message | – | – | |
| Message insertion | – | – | |
| Message masquerading | – | – | |
| Message incorrect addressing | – | – | |

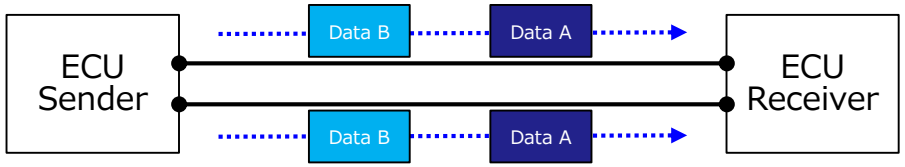
# Appendix: Application of 802.1CB for Functional Safety

- Extracts from ISO 26262-5:2018, Annex D, TableD.6－Communication Bus

| Safety mechanism/ measure | Typical diagnostic coverage considered achievable | Notes |
|---|---|---|
| Complete hardware redundancy | High | Common mode failures can reduce diagnostic coverage |
| Transmission redundancy | Medium | Depends on type of redundancy. Effective only against transient faults |

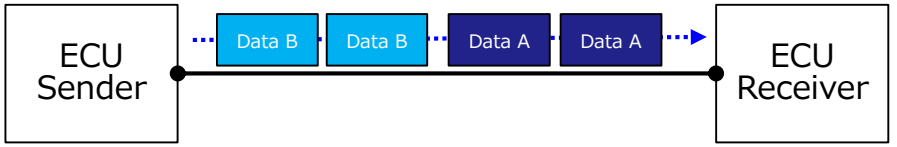



non redundancy




Complete hardware redundancy

Aim:
To detect failures during the communication by comparing the signals on two buses.
Description:
The bus is duplicated and the additional lines are used to detect failures.




Transmission redundancy

Aim:
To detect transient failures in bus communication.
Description:
The information is transferred several times in sequence.

802.1CB may be able to achieve **High/Medium diagnostic coverage**.
Considering application of TSN standards for Functional Safety.

# UC3. Real-time communication

## Use Case: FlexRay features

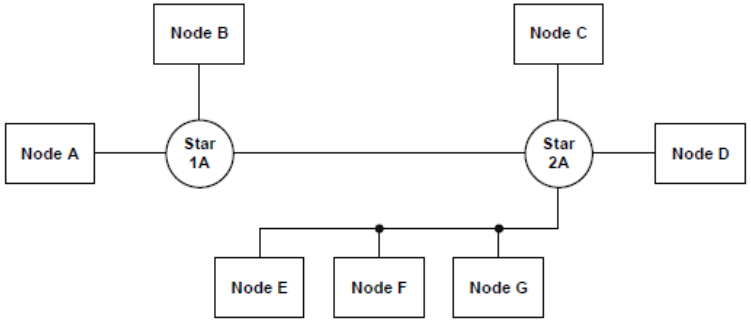



Figure 10 — Single channel hybrid example

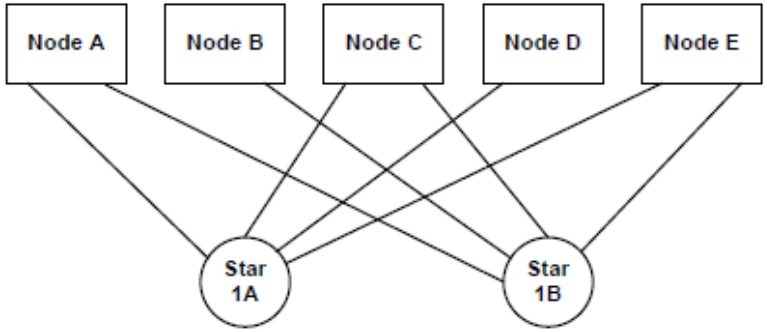



Figure 7 — Dual channel single star configuration

Referenced from ISO 174580-2:2013

## Requirement:

| | |
|---|---|
| R x.1 | Requirements to enable FlexRay like functionality |
| R x.2 | |
| R x.3 | |
| R x.4 | |
| R x.5 | |

## Useful 802.1 mechanisms:

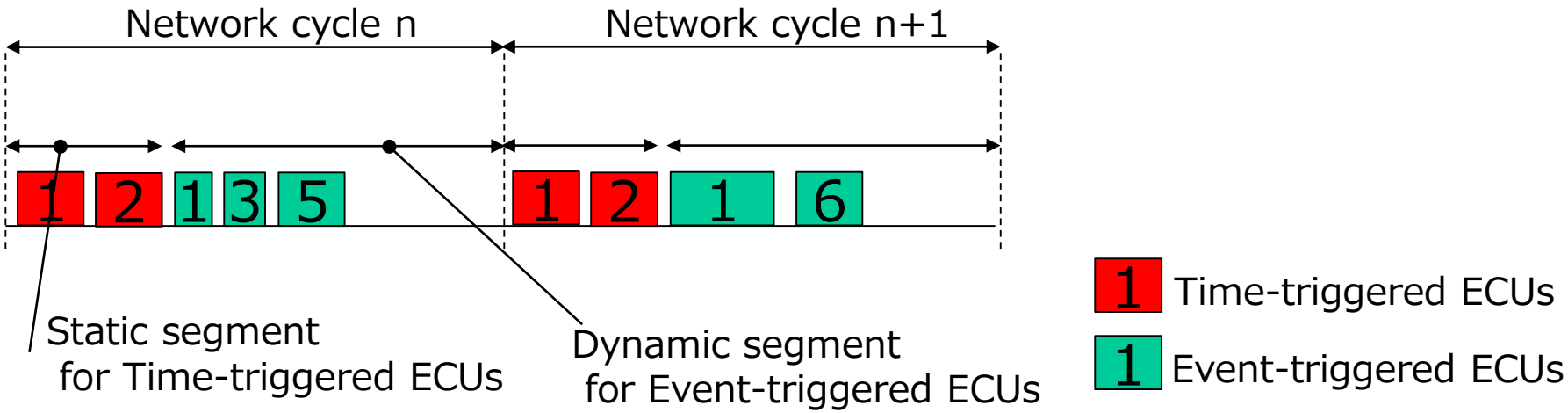
**TSN protocols/subset proposals to realize above requirements**

# UC3. Real-time communication

## Useful aspects of TSN (under discussion)

| Requirement | Function | Standard |
|---|---|---|
| Periodic traffic Bounded low latency | Clock synchronization | 802.1AS |
| | Scheduled traffic | 802.1Q 8.6.8.4 : Qbv |
| Traffic classification | TCP/IP-based stream identification | 802.1 CBdb |
| | Ingress Policing | 802.1Q 8.6.5.1 : Qci |
| Configuration | | 802.1Qcc, 802.1ABcu etc. |

## Example of traffic scheduling

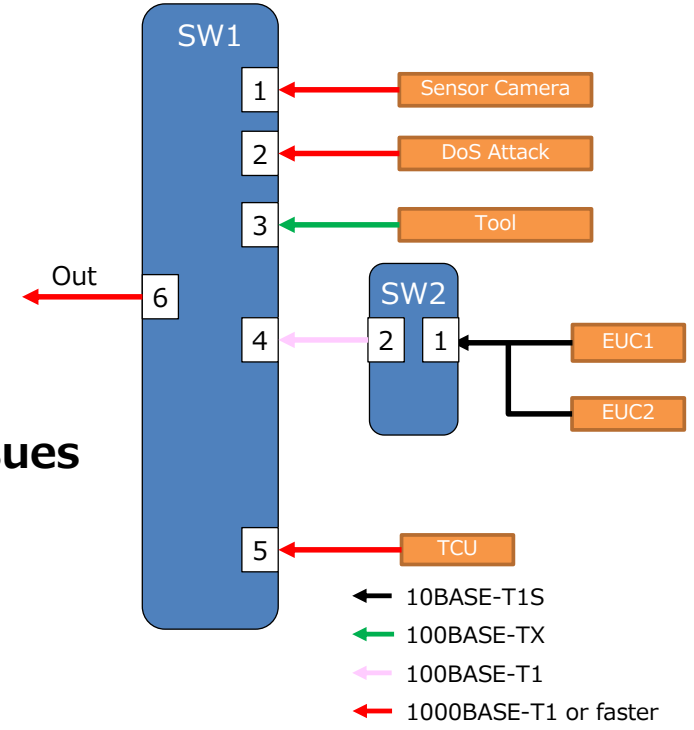


# UC4. Security

- **Goal**
  1. Define an IVN profile which can provide protection of high priority traffic
  2. Ensure low latency with this IVN profile for ECUs communication(Scheduled Traffic) against DDoS attacks
  3. Detect DDoS attacks immediately and protect the IVN and ECUs from them

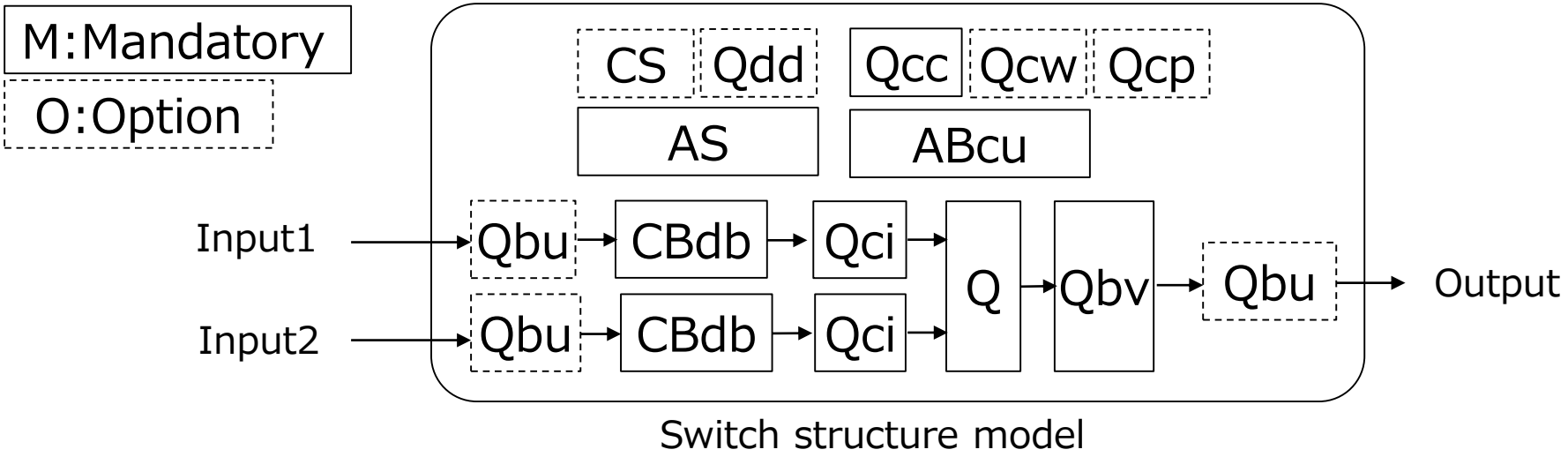
- **Potential Security Issues**
  1. DDoS attacks bring bandwidth exhaustion and disturbances to traffic prioritization on switch
  2. IVN is exposed to unauthorized access due to Brute-force attack

- **Example approach of using Qci to Security Issues**
  1. Block misbehaving streams by Per-Stream Filtering and Policing
  2. Detect unknown nodes or streams by Per-Stream Filtering and Policing
  3. Protect high-priority traffic from DDoS attacks and keep low latency




Example IVN in this use case

# Appendix : Definition the TSN model




Switch structure model

## TSN Function (1/2)

| Function | Standard | Convention |
|---|---|---|
| Clock synchronization | 802.1AS | M |
| Preemption | 802.1Q 6.7.2 | O: 802.1Qbu |
| Ingress Policing | 802.1Q 8.6.5.1 | M: 802.1Qci |
| VLAN | 802.1Q 6.9 | M |
| Transmission selection control | 802.1Q 8.6.8 | M |
| Scheduled traffic | 802.1Q 8.6.8.4 | M: 802.1Qbv |
| Extended Stream identification | 802.1CBdb | M |

## TSN Function (2/2)

| Function | Standard | Convention |
|---|---|---|
| Link-local registration Protocol | P 802.1CS | O |
| Resource allocation protocol | P 802.1Qdd | O |
| YANG for Qbv, Qbu, Qci | P 802.1Qcw | O |
| YANG for Bridge | 802.1Qcp | O |
| LLDP Neighbor discovery | P 802.1ABcu | M |
| Centralized configuration | 802.1Qcc | M |

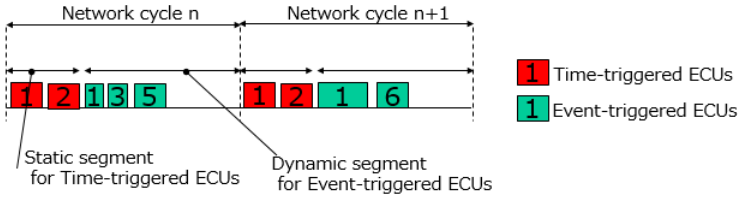
# Appendix: Example of TSN model for Real Time

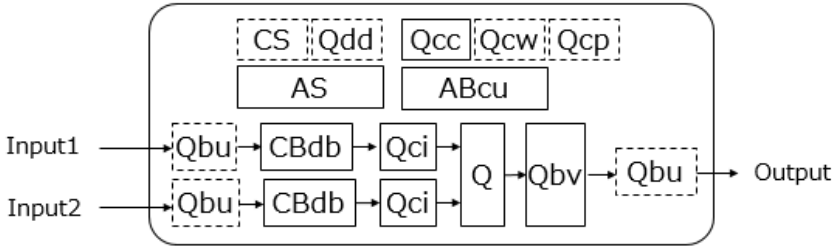
## UC3. Real-time communication

**Useful aspects of TSN**

| Requirement | Function | Standard |
|---|---|---|
| Periodic traffic Bounded low latency | Clock synchronization | 802.1AS |
| | Scheduled traffic | 802.1Q 8.6.8.4 : Qbv |
| Traffic classification | TCP/IP-based stream identification | 802.1 CBdb |
| | Ingress Policing | 802.1Q 8.6.5.1 : Qci |
| Configuration | | 802.1Qcc, 802.1ABcu etc. |

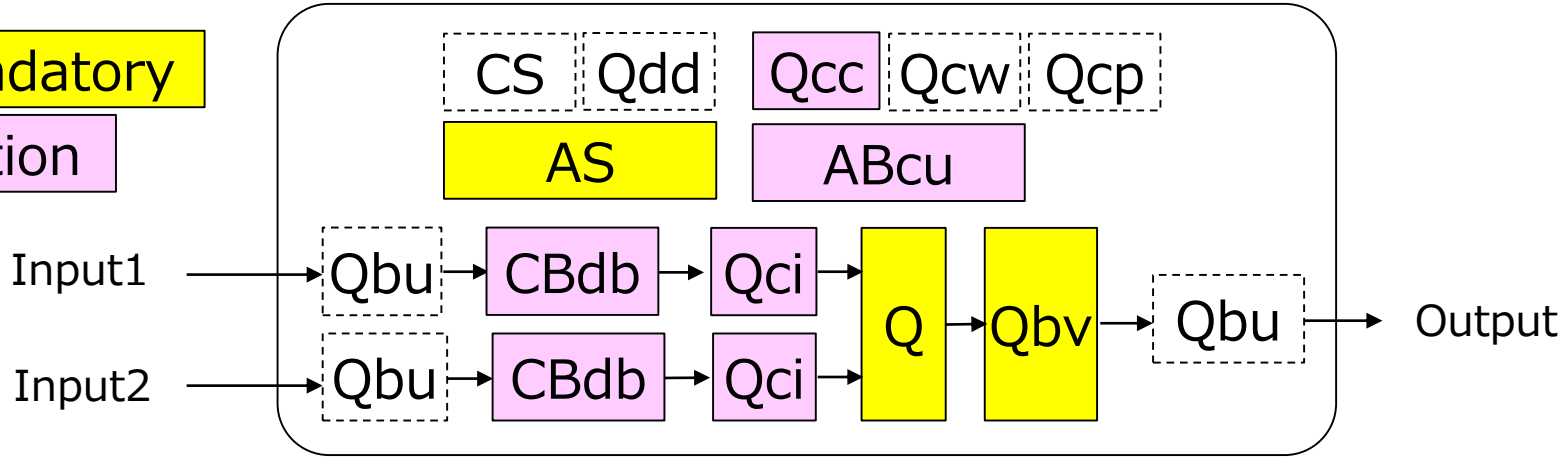
**Example of traffic scheduling**




M:Mandatory

O:Option




**Describe the Profile like a “Coloring” for easy understanding**

# UC5. In-Vehicle Traffic Types

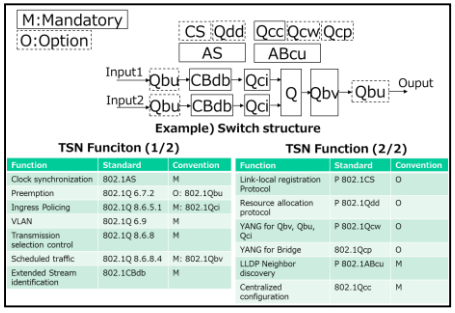
- Add a supplement to Auto Use Case 04 of「dg-pannell-automotive-use-cases-0719-v04.pdf」

Need for consideration of higher layer protocols (L3-L7)

| Traffic Type | Period | Guarantee[4] | Tolerance to Loss[5] | Frame Size | Criticality | L2 | L3 | L4 | L5~L7 |
|---|---|---|---|---|---|---|---|---|---|
| Safety-relevant Control: see 3.4.1.2 | <= 20ms | Deadline based Reserved w/Latency < 1ms | No | 64 bytes | High | | IP | UDP | |
| Safety-relevant Media: see 3.4.1.3 | <= 10ms | Bandwidth based Reserved w/Latency < 1ms | No | 64 to max frame size[6] (w/1500 data bytes) | High | | IP | UDP | |
| Network Control: see 3.4.1.4 | 50ms to 1s | Sporadic Highest priority Non-Reserved | Yes | 64 to 512[7] bytes | High | | IP OSPF | None, UDP | |
| Event: see 3.4.1.5 | N/A | Sporadic 2nd Highest priority Non-Reserved | Yes | 64 to max frame size (w/1500 data bytes) | Medium | | IP | TCP, UDP | |
| Safety-irrelevant Control see 3.4.1.6 | < 200ms | Bandwidth based Reserved w/Latency < 50ms | Yes | 64 bytes | Medium | | IP | UDP | |
| Safety irrelevant Media: see 3.4.1.7 | Defined by the media type | Bandwidth based Reserved w/Latency < 300ms | Yes | 64 to max frame size (w/1500 data bytes) | Medium | | IP | UDP | |
| Best Effort: see 3.4.1.8 | N/A | None | Yes | 64 to max frame size (w/1500 data bytes) | Low | | IP ARP | TCP, UDP, None | |

See next slide

Requirement from Application / Service




L2 Colum shows in diagram of TSN functions.

Add protocol example

The traffic type MUST be decided according to the L3 / L4 protocols

# UC5. In-Vehicle Traffic Types

## An Example of Application-based Categorization (Just a concept model without correctness)

| L5-L7 | Latency | Reliability | L4 | Traffic type |
|---|---|---|---|---|
| HTTP | < 1s | N/A | TCP | Best Effort |
| NFS | < 200ms | 99.99% | UDP | Safety-irrelevant media |
| | | | TCP | Best Effort |
| SNMP | < 1s | N/A | UDP | According to MIB |
| FTP | < 1s | N/A | TCP | Best Effort |
| TFTP | < 1s | 99.999% | UDP | Safety-irrelevant media |
| SSH | < 500ms | N/A | TCP | Safety-irrelevant control |
| Application-A (for Safety) | < 10ms | 99.999% | UDP | Safety-relevant control |
| Application-B (for no-safety) | < 1s | 99.99% | TCP | Best Effort |

# Thank You