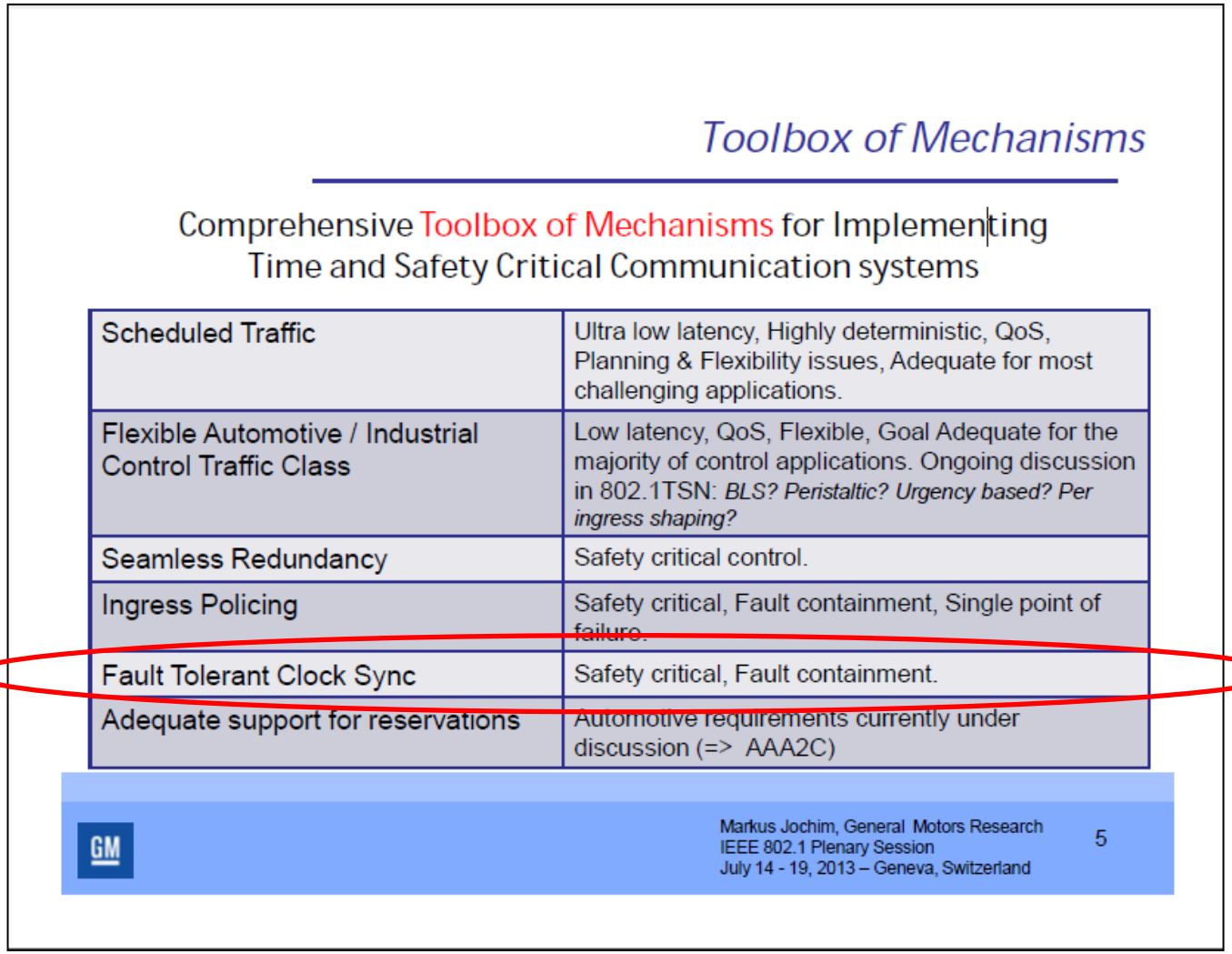
Interoperability of IEEE 802.1AS and Fault-Tolerant Clock Synchronization

IEEE Interim, York, Sep/2013

Wilfried Steiner, Corporate Scientist
wilfried.steiner@tttech.com

Industrial Need for FT Clock-Sync



Toolbox of Mechanisms

Comprehensive Toolbox of Mechanisms for Implementing Time and Safety Critical Communication systems

Scheduled Traffic	Ultra low latency, Highly deterministic, QoS, Planning & Flexibility issues, Adequate for most challenging applications.
Flexible Automotive / Industrial Control Traffic Class	Low latency, QoS, Flexible, Goal Adequate for the majority of control applications. Ongoing discussion in 802.1TSN: *BLS? Peristaltic? Urgency based? Per ingress shaping?*
Seamless Redundancy	Safety critical control.
Ingress Policing	Safety critical, Fault containment, Single point of failure.
Fault Tolerant Clock Sync	Safety critical, Fault containment.
Adequate support for reservations	Automotive requirements currently under discussion (=> AAA2C)

GM

Markus Jochim, General Motors Research
IEEE 802.1 Plenary Session
July 14 - 19, 2013 – Geneva, Switzerland

5

http://www.ieee802.org/1/files/public/docs2013/new-tsn-jochim-goals-of-802-1tsn-0713-v01.pdf

Which failures need to be tolerated?

Proposal – IEEE 802.1Q AVB/TSN Failure Hypothesis

Fault-Containment Regions (FCR):

- Communication Link
- End Station
- Bridge

→ A fault is local to either an end station or a bridge or a communication link.

→ If more than one bridge / one end stations / one link become faulty then we have also more than one fault.

Failure Mode for End Stations and Bridges

- Permanent, Consistent, and Fail-Silent

→ In the case of a failure, a faulty FCR will stop producing output (“Fail-Silent”).

→ A faulty FCR will behave the same on all ports, e.g., a faulty bridge will stop producing output on all ports (“Consistent”).

→ A faulty FCR will be faulty for the remaining mission time (“Permanent”).

Failure Mode for Communication Links

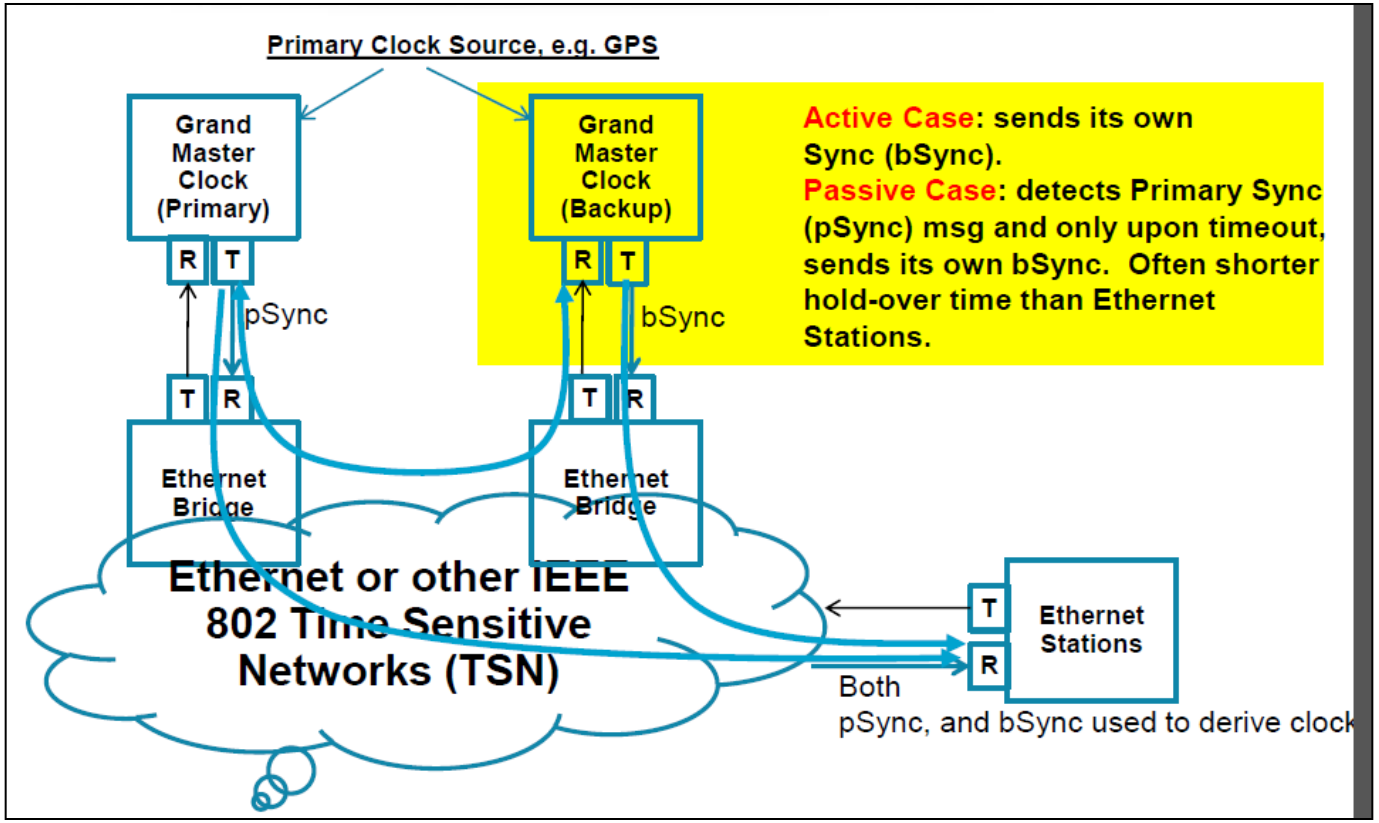
- Transient or Permanent, Detectably Faulty

→ The communication link may drop frames or invalidate the Ethernet FCS on a per frame basis (“Transient”).

→ The communication link may become unavailable for the remaining mission time (“Permanent”).

→ Each failure of the communication link results in either a loss of the frame or an invalidation of the frame’s FCS (“Detectably Faulty“).

802.1ASbt Clock Synchronization Improvement Proposals so far

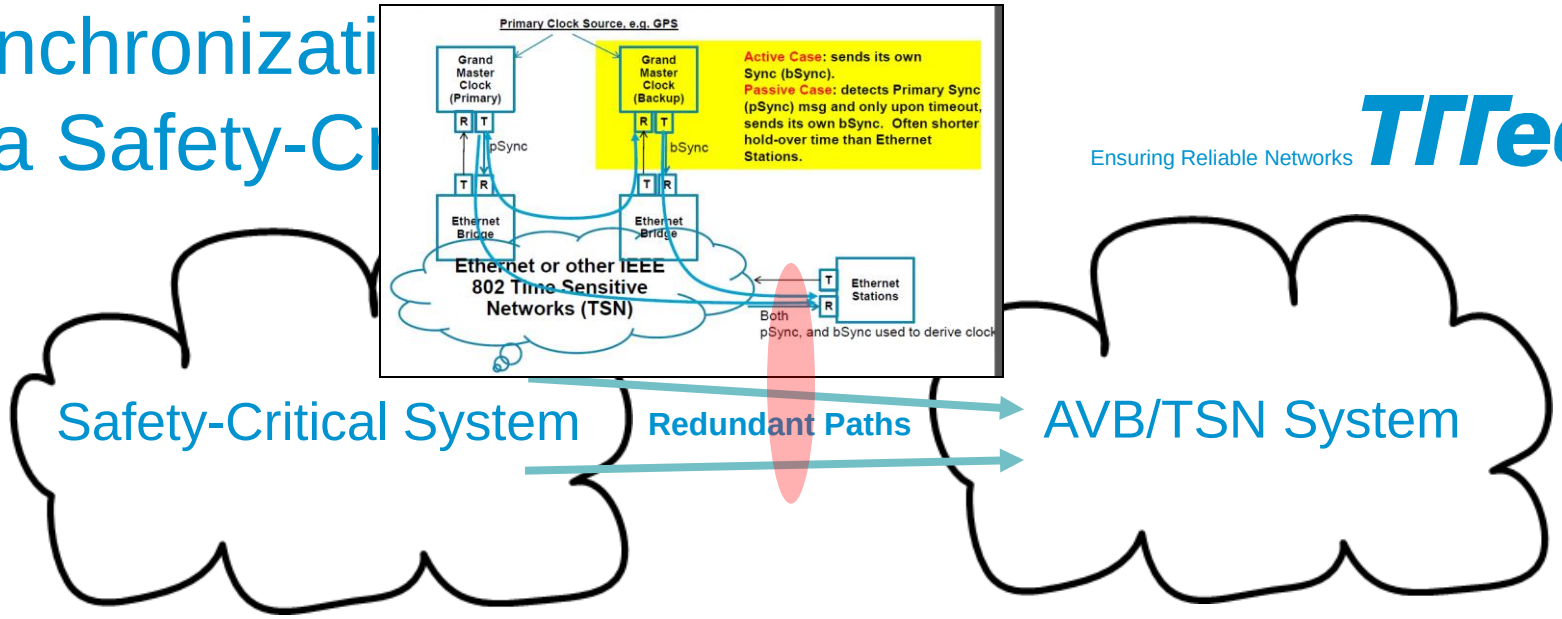


http://www.ieee802.org/1/files/public/docs2013/ASbt-Spada-Kim-Fault-tolerant-grand-master-proposal-0513-v1.pdf

The “Backup Grandmaster” proposal is likely to cover faults as outlined in the proposed “IEEE 802.1Q AVB/TSN Failure Hypothesis” (i.e., fail-silent failures).

For more severe failures we propose to define the interfaces to existing protocols rather than to define new protocols.

Synchronizati
to a Safety-Cr



How about to standardize the quality of the clock synchronization messages (e.g., announce and synchronization messages) from redundant masters?

Relevant quality parameters in the fault-tolerant clock synchronization domain are, e.g.:

- Failure modes of the clock synchronization inputs to the AVB/TSN domain
- Worst-case temporal deviation of two non-faulty clocks in the system (precision)
- Temporal communication blackout characteristics
- Mean Time To Repair (MTTR)

The IEEE 1588 alternative master mechanism may be usable as a basis.

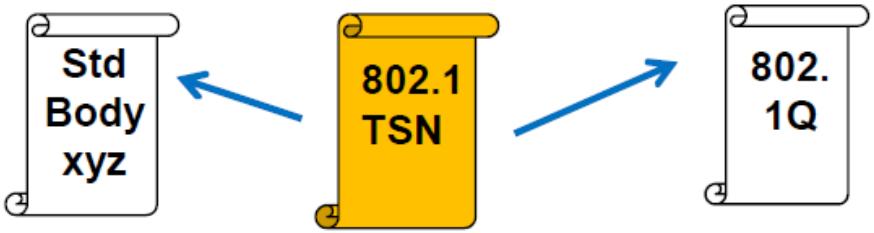
Where should these interfaces be standardized?

What needs to be done in .1 standards?

References to non-IEEE Standards

A single 802.1TSN Document

- Not all mechanisms in our toolbox need to be specified within the 802.1TSN document.



- Mechanisms can also be defined by reference to be mandatory for 802.1TSN compliant implementations.
- Goal: 802.1TSN as a single document that defines / bundles the set of mechanisms that need to be implemented to be "attractive" for time & safety critical control in Automotive and Industrial.

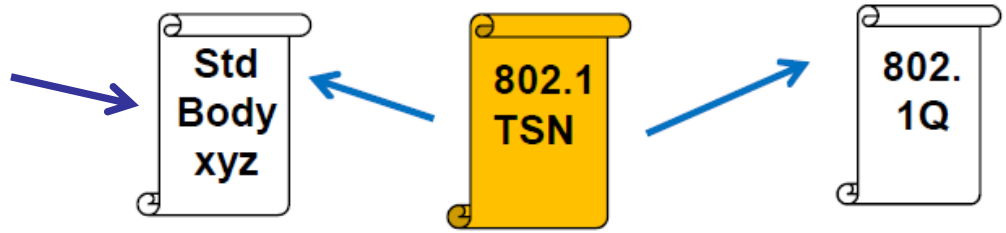
http://www.ieee802.org/1/files/public/docs2013/new-tsn-jochim-goals-of-802-1tsn-0713-v01.pdf

References to non-IEEE Standards

SAE AS6802 (FT Clock Sync)

A single 802.1TSN Document

- Not all mechanisms in our toolbox need to be specified within the 802.1TSN document.

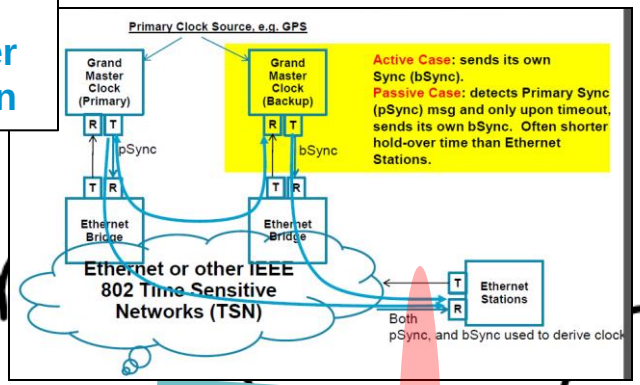


- Mechanisms can also be defined by reference to be mandatory for 802.1TSN compliant implementations.
- Goal: 802.1TSN as a single document that defines / bundles the set of mechanisms that need to be implemented to be "attractive" for time & safety critical control in Automotive and Industrial.

http://www.ieee802.org/1/files/public/docs2013/new-tsn-jochim-goals-of-802-1tsn-0713-v01.pdf

Synchronization of AVB/TSN to SAE AS6802

IEEE 802.1ASbt
- **backup grandmaster coordination**



Safety-Critical System

Redundant Paths

AVB/TSN System

SAE AS6802 (FT Clock Sync)

IEEE 802.1ASbt?
- **FT characteristics of the respective FT clock synch algorithm**

IEEE 802.1ASbt
- **how to transport synchronization information from redundant grandmasters through the network**

Ensuring Reliable Networks

www.tttech.com