Interoperability of IEEE 802.1AS and Fault-Tolerant Clock Synchronization

IEEE Plenary, Geneva, Jul/2013

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

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").

Proposed Failure Hypothesis in a broader context

Proposed AVB/TSN Failure Hypothesis is adequate for a large set of use cases, e.g., some industrial and automotive use cases, but is **not sufficient for other use cases**.

For example, it is common in the avionics world to assume that a chip may fail arbitrarily. This means, e.g., a chip may output arbitrary messages for an arbitrary number of times.

These failures are realistic, e.g., see "*Byzantine Fault Tolerance, from Theory to Reality*" Driscoll et al.

Are these other use cases relevant for AVB/TSN?

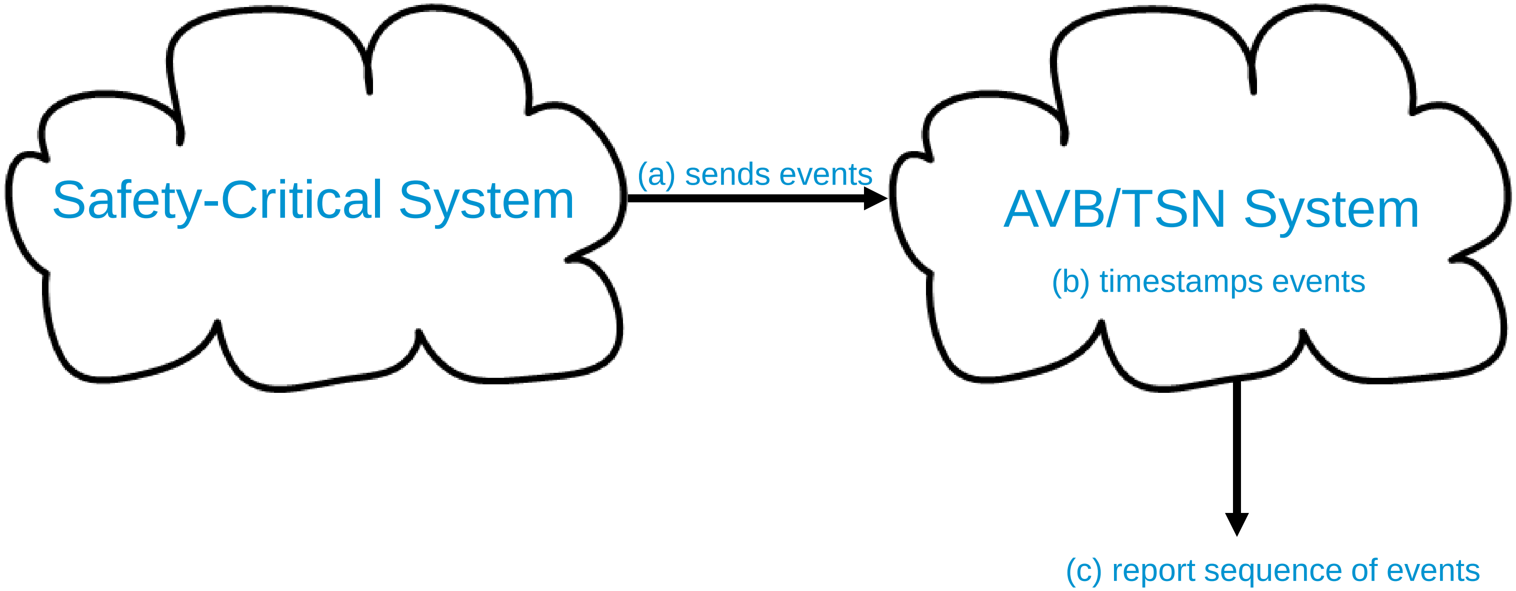
Ensuring Reliable Networks TTTech

At the IEEE 802.1 interim meeting in May/2013, I felt that there was a common understanding that these use cases are relevant, but the interest might be secondary for now.

Hence, I proposed that we should define the interaction between AVB/TSN and fault-tolerant clock synchronization algorithms.

Some examples of the use of these interaction are as follows.

Example 1: Monitoring



Safety-Critical System

(a) sends events

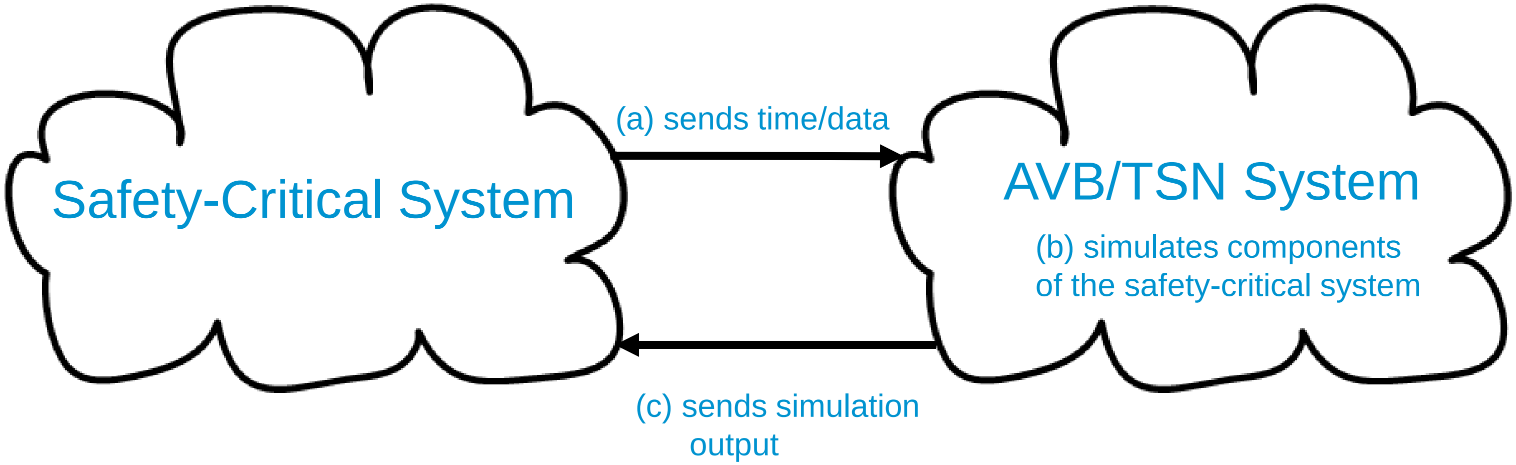
AVB/TSN System

(b) timestamps events

(c) report sequence of events

Example 2:
Restbus Simulation

Ensuring Reliable Networks TTTech



Safety-Critical System

(a) sends time/data

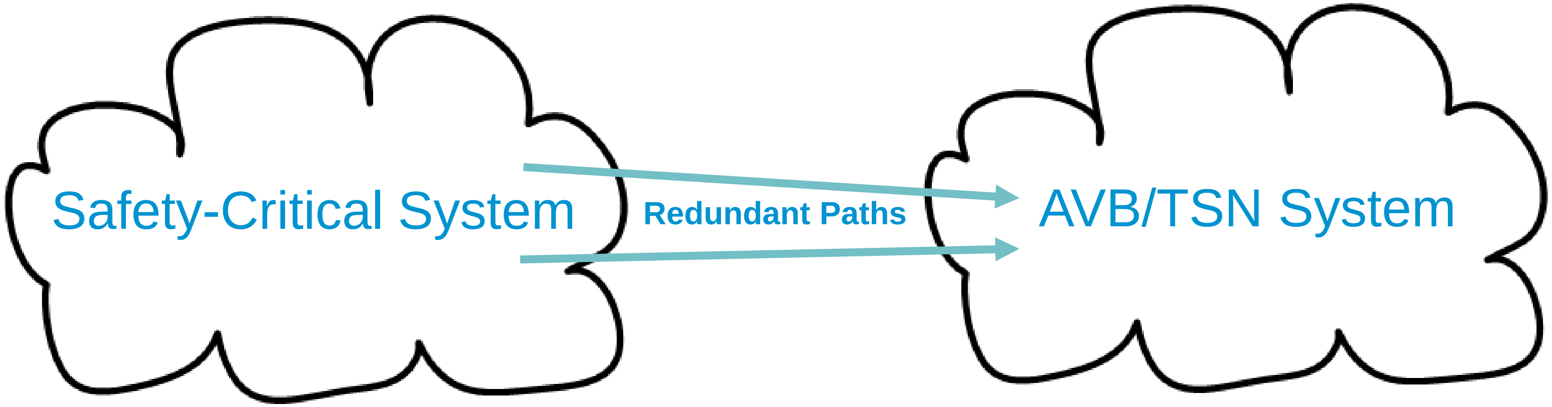
AVB/TSN System

(b) simulates components of the safety-critical system

(c) sends simulation output

Synchronization of AVB/TSN to a Safety-Critical System

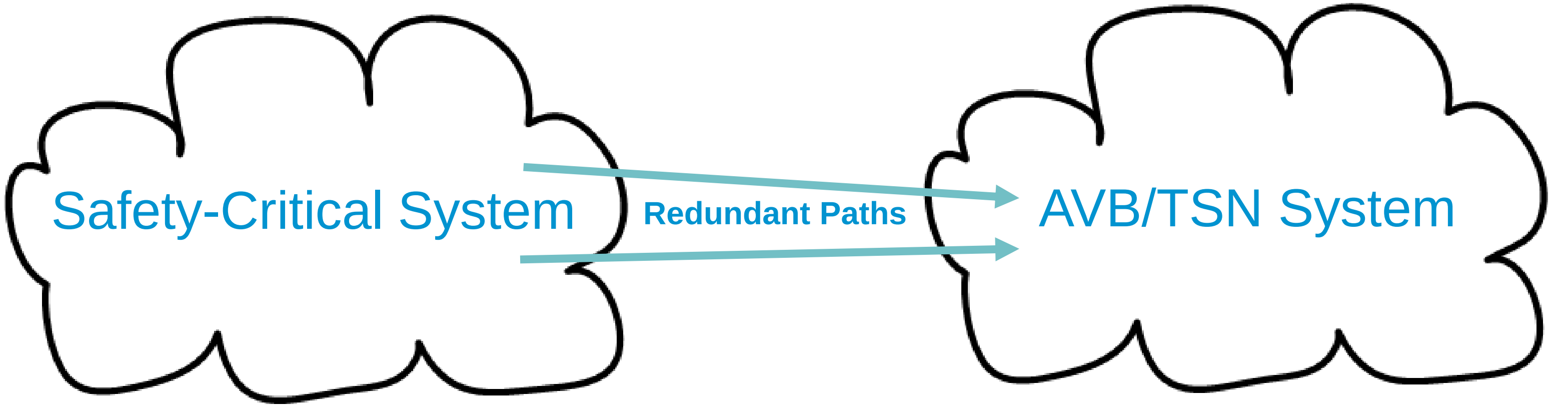
Ensuring Reliable Networks TTTech



This approach allows a system designer to use her preferred synchronous solution for the safety-critical system, e.g.:

- ARINC 659, used for example in the Boeing 777
- TTP, used for example in the Boeing 787, and Airbus A380
- FlexRay, used for example in several automotive serial production programs
- SAE AS6802, used for example in space programs and the green energy area
- other solutions: NASA Robus, Cesiumspray, Braided Ring (BRAIN), …

Synchronization of AVB/TSN to a Safety-Critical System



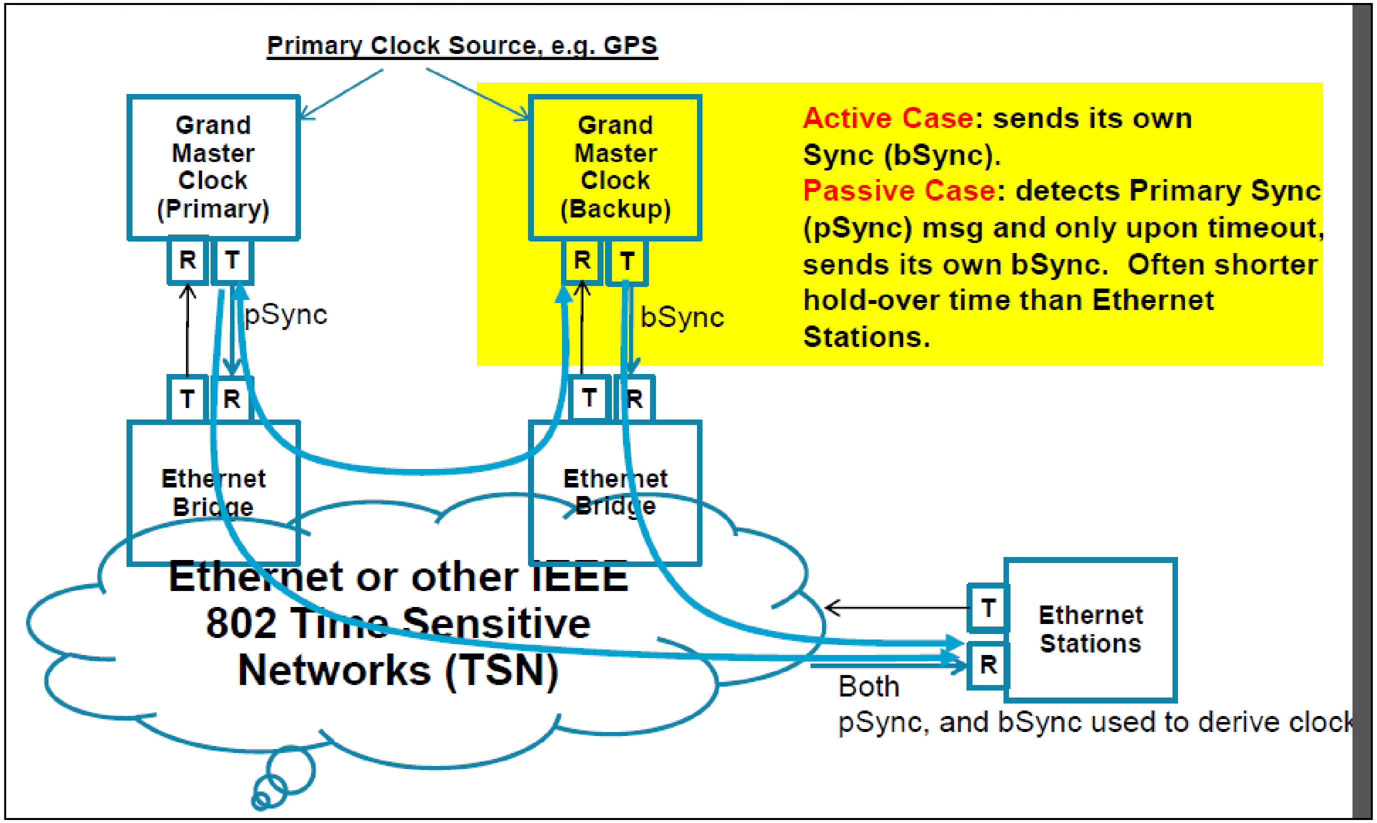
How about to standardize the quality of the clock synchronization messages (e.g., announce and synchronization messages) from redundant masters?

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.

802.1ASbt Clock Synchronization Improvement Proposals so far


Primary Clock Source, e.g. GPS
Grand Master Clock (Primary)
R
T
pSync
Grand Master Clock (Backup)
R
T
bSync
T
R
Ethernet Bridge
T
R
Ethernet Bridge
Ethernet or other IEEE 802 Time Sensitive Networks (TSN)
T
R
Ethernet Stations

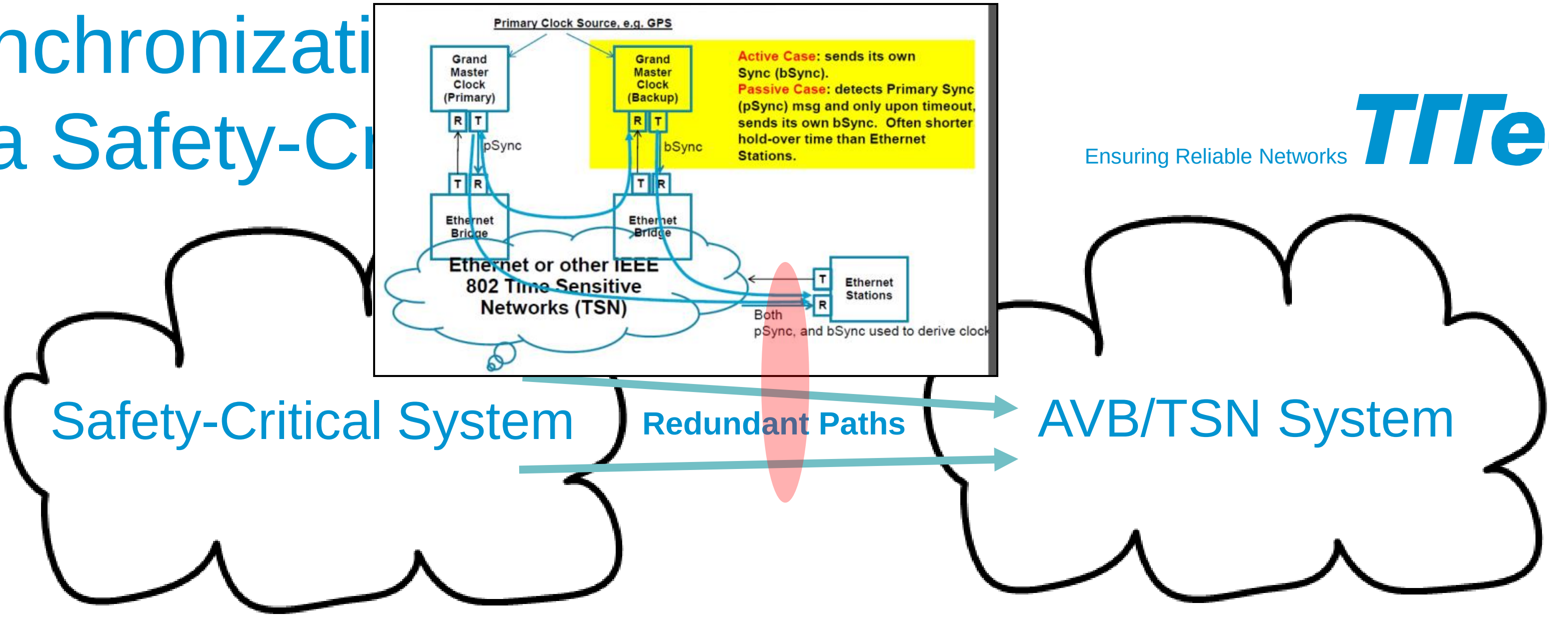
Active Case: sends its own Sync (bSync).
Passive Case: detects Primary Sync (pSync) msg and only upon timeout, sends its own bSync. Often shorter hold-over time than Ethernet Stations.

Both pSync, and bSync used to derive clock

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

Synchronizati
to a Safety-C

Ensuring Reliable Networks TTTech


Primary Clock Source, e.g. GPS
Grand Master Clock (Primary)
Grand Master Clock (Backup)
R
T
pSync
bSync
T
R
Ethernet Bridge
Ethernet Bridge
Ethernet or other IEEE 802 Time Sensitive Networks (TSN)
T
R
Ethernet Stations

Active Case: sends its own Sync (bSync).
Passive Case: detects Primary Sync (pSync) msg and only upon timeout, sends its own bSync. Often shorter hold-over time than Ethernet Stations.

Both pSync, and bSync used to derive clock

Safety-Critical System
Redundant Paths
AVB/TSN System

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.

IEEE 1588 Alternate Master

IEEE 1588-2008 clause 17.4 Alternate Master (optional):

“This option allows alternate masters that are not currently the best master to exchange PTP timing information with slave ports, and for a slave port to acquire knowledge of the characteristics of the transmission path between itself and each alternate master. This will allow a slave switchover to an alternate master with a small phase excursion when the best master fails.”

Complementary this concept may also be used by a slave to synchronize to a fault-tolerant timebase if present.

IEEE 1588 Alternate Master cont.

A slave will receive synchronization messages from several alternate masters.

In one configuration, the slave may use the mathematical average of the time information in these synchronization messages.

For more intelligent synchronization to a fault-tolerant timebase more information is needed in the Sync messages (and potentially also other messages), e.g.:

- the fault-tolerance Quality of Service of the Sync message

The new information not necessarily demands a modification of the existing frame formats, but it may be sufficient to use a different interpretation of the existing frame contents.

TTTech

Ensuring Reliable Networks

www.tttech.com