Interoperability of IEEE 802.1AS and Fault-Tolerant Clock Synchronization

IEEE Interim Meeting, Victoria, May/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.

So, my question is:

Are these second use cases relevant for AVB/TSN?

And I can imagine three possible answers

Are these second use cases relevant for AVB/TSN?

1. No.

In which case we are done.

However, I hope that this is not the case.

And I can imagine three possible answers

Are these second use cases relevant for AVB/TSN?

2. Yes, these use cases are essential for AVB/TSN and need to be completely addressed in our standards.

This can be done, given that the group is willing to invest significantly into modifications and increments to IEEE 802.1AS and probably other standards.

However, I think answer 2 might also not be the case.

And I can imagine three possible answers

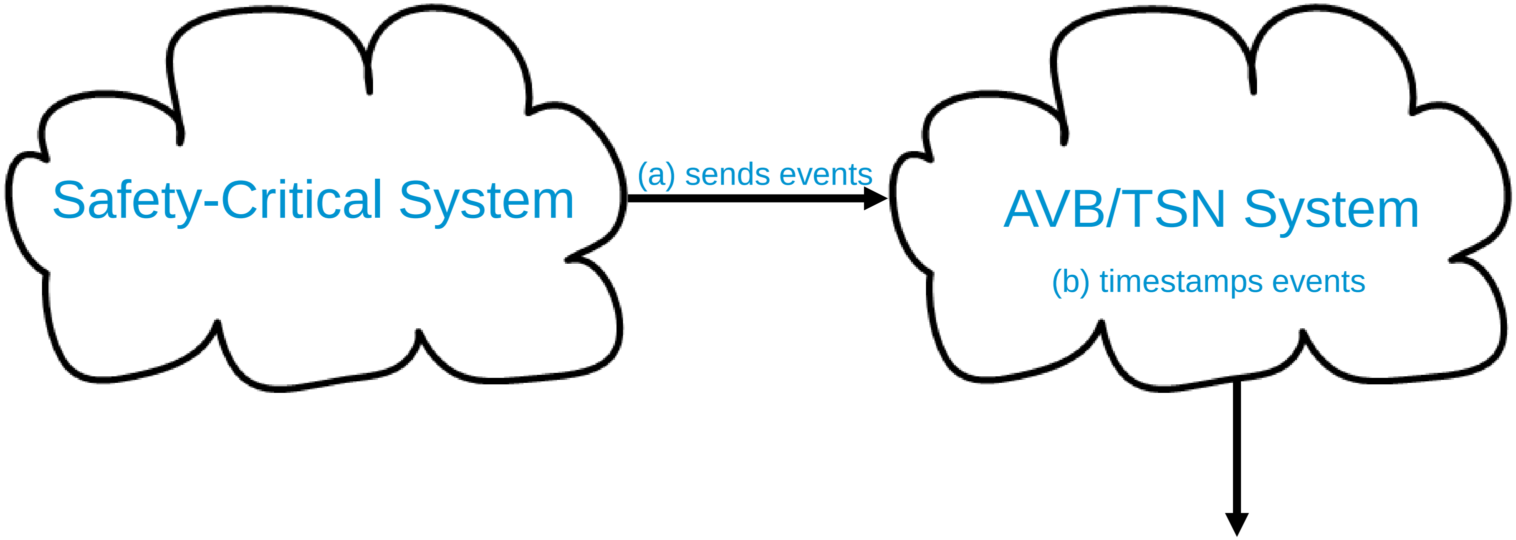
Are these second use cases relevant for AVB/TSN?

3. Yes, but the interest might be secondary for now.

In which case we should define the interaction between AVB/TSN and fault-tolerant clock synchronization algorithms.

→ I think this is the way to go and let me give some examples what I mean by that.

Example 1: Monitoring



Safety-Critical System

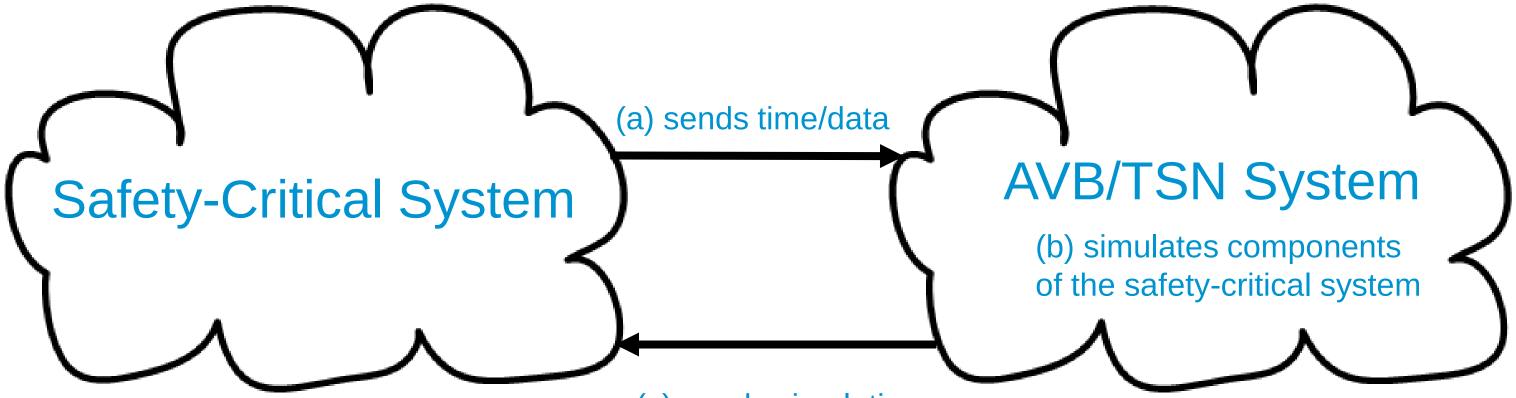
(a) sends events

AVB/TSN System

(b) timestamps events

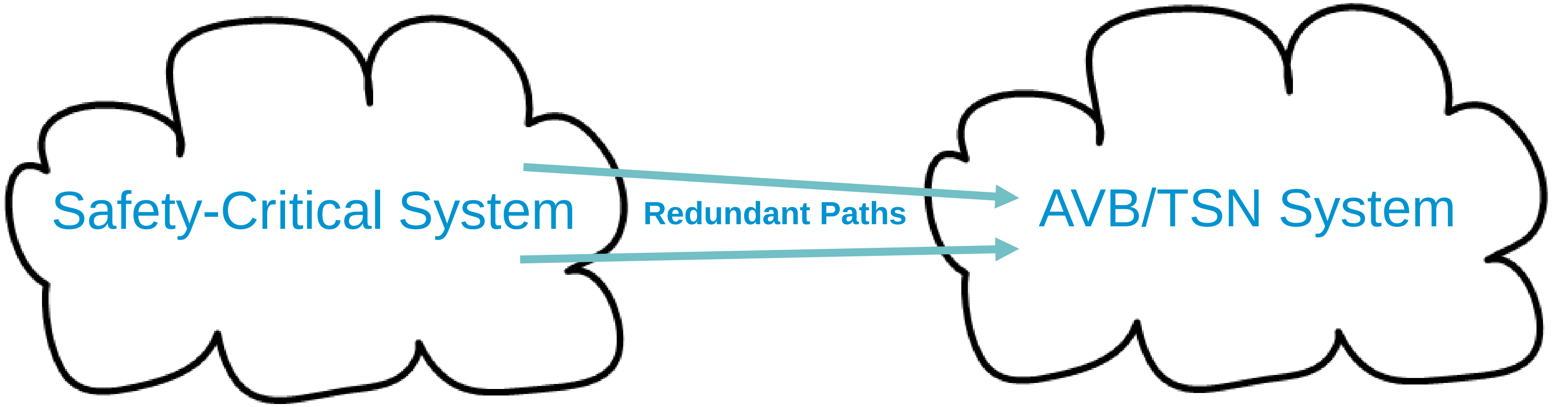
(c) report sequence of events

Example 2:
Restbus Simulation


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



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.

TTTech

Ensuring Reliable Networks

www.tttech.com