IEEE 802.1ASbt – Useful Synchronization Information for Fault-Tolerance

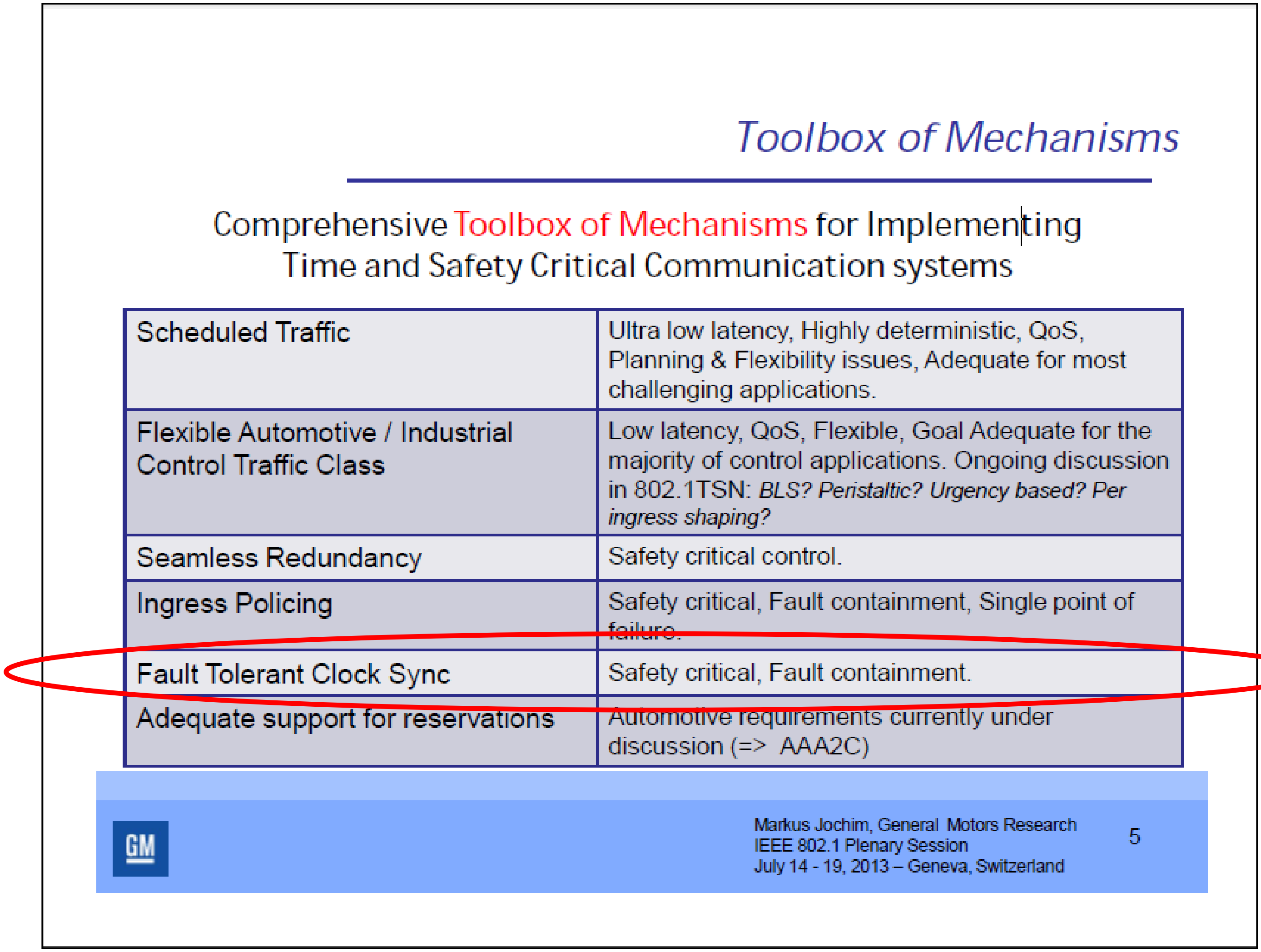
IEEE Plenary, Dallas, Nov/2013

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

Overview

- Background:
  - Industrial Need
  - Interfacing AVB/TSN to a Fault-Tolerant Clock Synchronization Protocol
- Interface Design
  - What interfaces are there?
  - Overview of the SAE AS6802 Fault-Tolerant Clock Synchronization Protocol
  - Elements of the interface descriptions
- Discussion of the Protocol Control Frames (PCF)

Background:
Industrial Need for FT Clock-Sync



Toolbox of Mechanisms

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

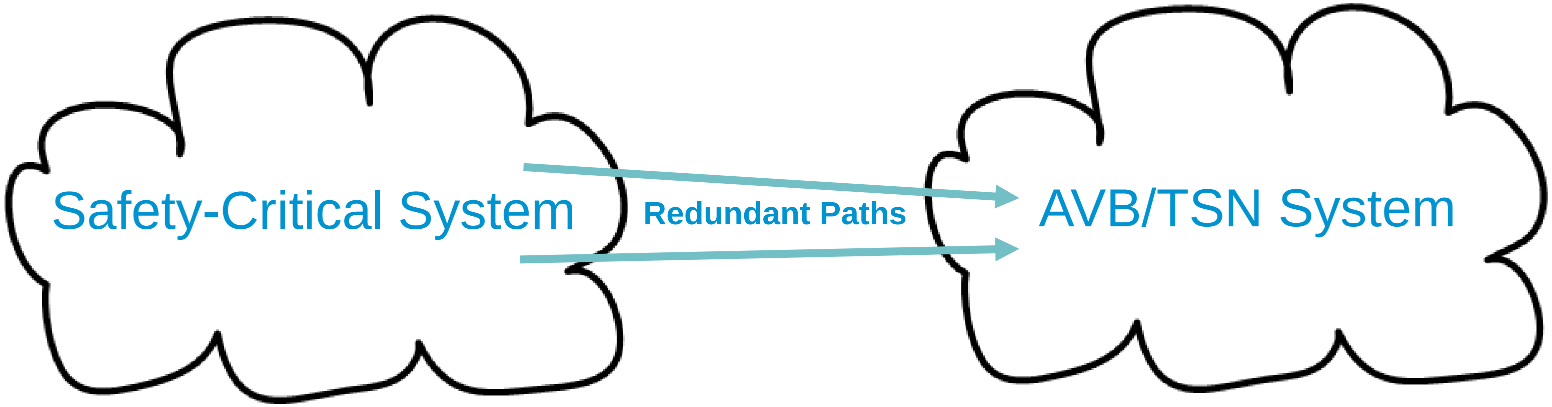
Scheduled Traffic	Ultra low latency, Highly deterministic, QoS, Planning & Flexibility issues, Adequate for most challenging applications.
Flexible Automotive / Industrial Control Traffic Class	Low latency, QoS, Flexible, Goal Adequate for the majority of control applications. Ongoing discussion in 802.1TSN: *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)

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

Background: Synchronization of AVB/TSN to a Safety-Critical System

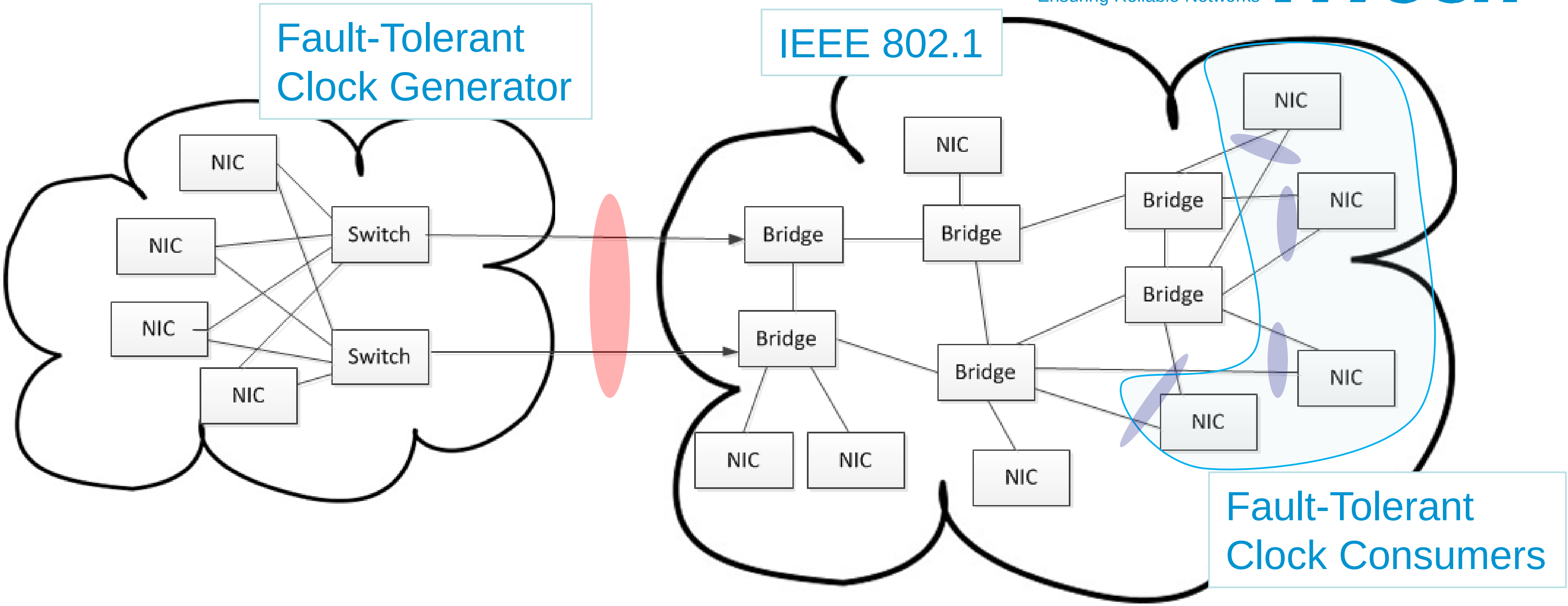


This approach allows a system designer to use her preferred synchronous solution for the safety-critical system, e.g.:

- 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 series production programs
- SAE AS6802, used for example in space programs and the green energy area
- other solutions: NASA Robus, Cesiumspray, Braided Ring (BRAIN), …

Interface Design

Ensuring Reliable Networks TTTech



"Architecture Design is Interface Design" [Kopetz]

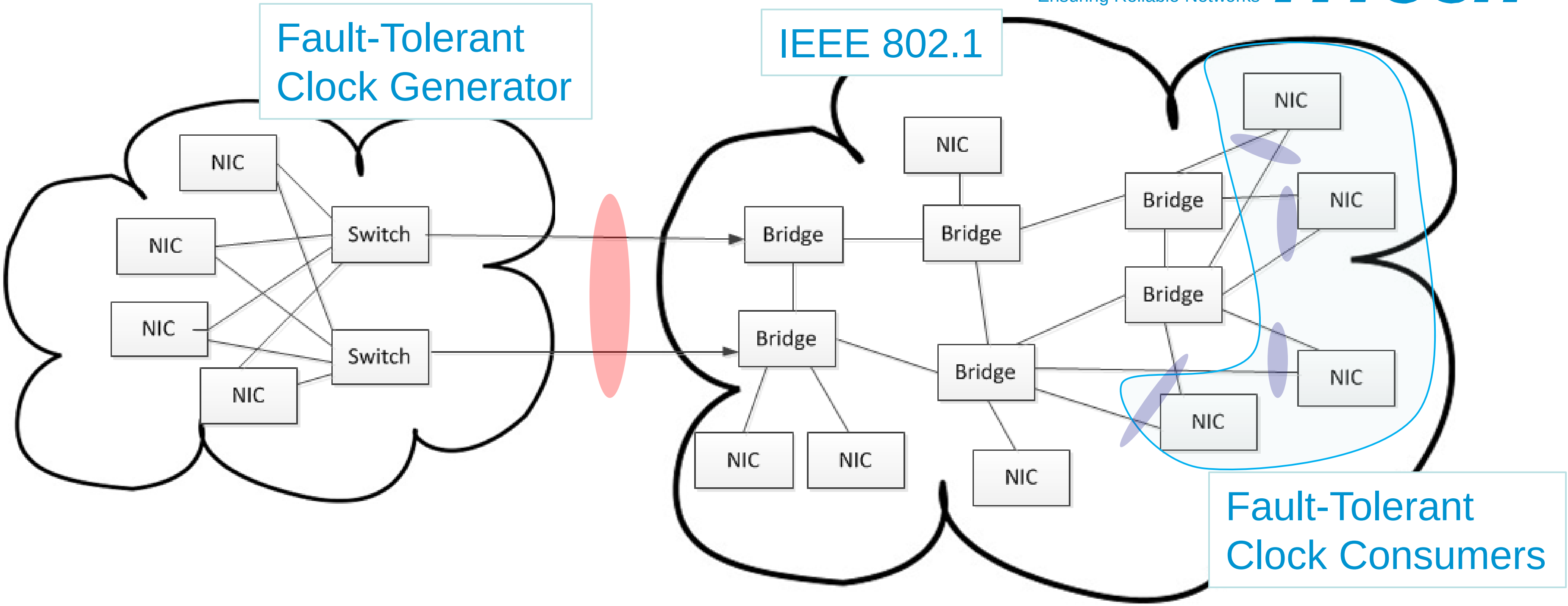
Red Interface specifies the behavior of the FT Clock Generator *as observed by the connecting bridges of the IEEE 802.1 network*.

Internal behavior of the FT Clock Generator may (and most likely will) *be much more complex* than as observed at the interface.

Blue Interface specifies the behavior of the FT Clock Generator *as observed by the FT Clock Consumers.*

Interface Design

Ensuring Reliable Networks TTTech

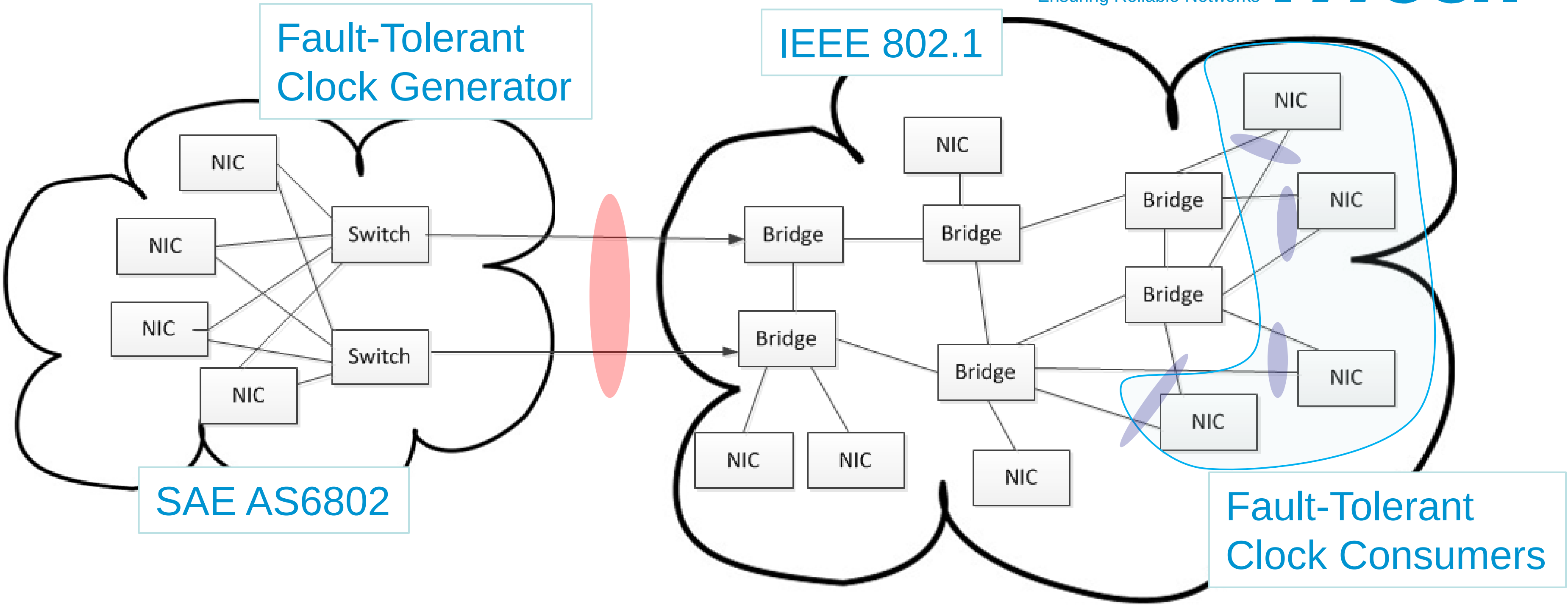


The red interface is different from the blue interfaces, because there *is additional behavior introduced by the IEEE 802.1 network* connecting the FT Clock Generator to the FT Clock Consumers.

Both, red and blue, interfaces need to be specified to enable the usage of a fault-tolerant timebase.

Example Realization

Ensuring Reliable Networks TTTech

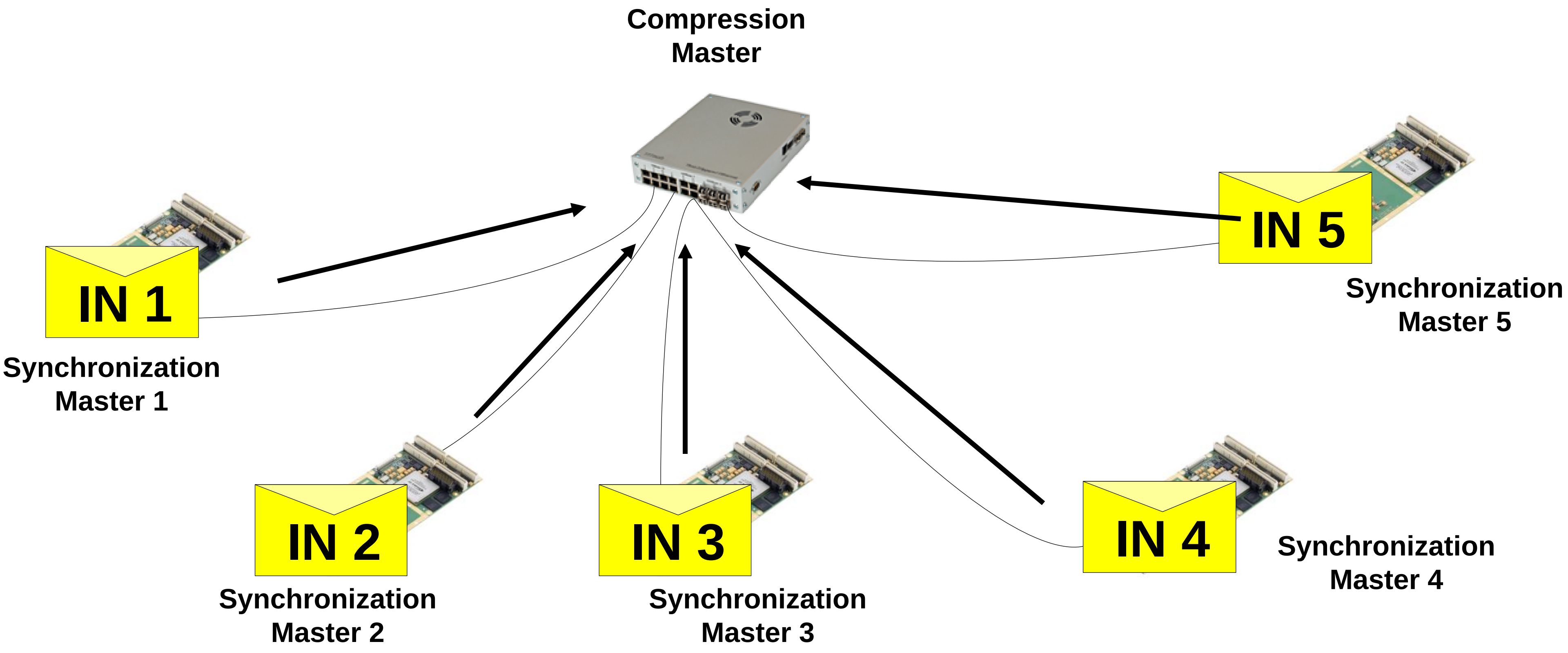


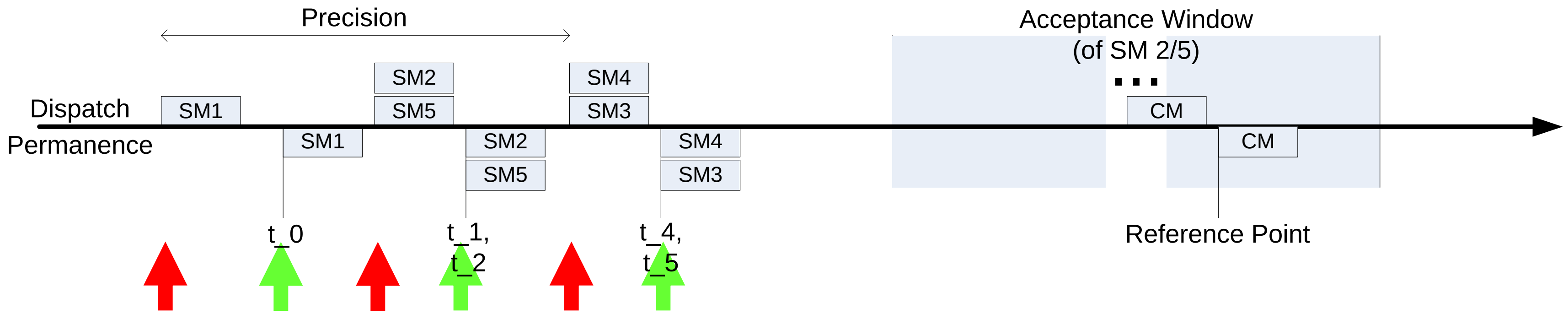
SAE AS6802 (“Time-Triggered Ethernet”) standardizes a fault-tolerant clock generator as depicted above.

It does so by combining the timing information of several “Synchronization Masters” in the switches, who implement a “Compression Master” functionality.

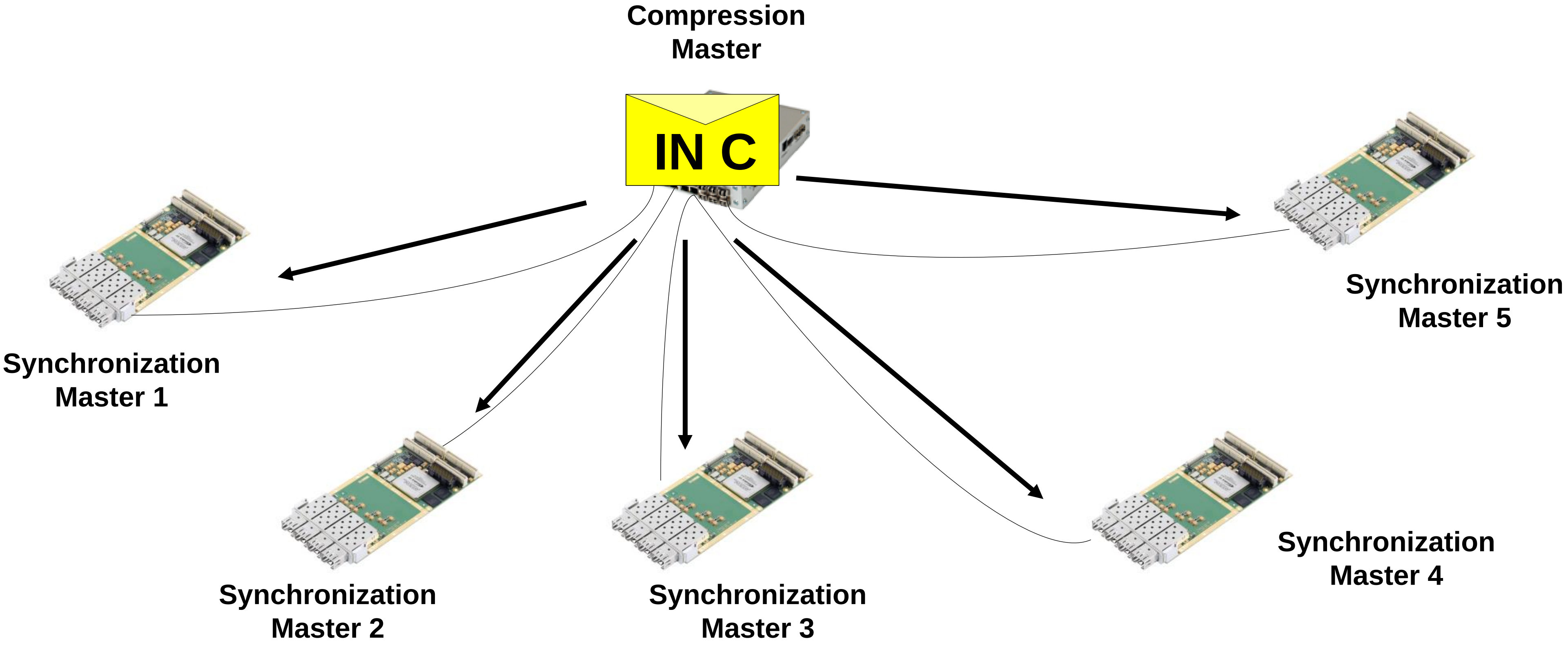
For the steady state operation mode, it looks a bit like in the following animations.

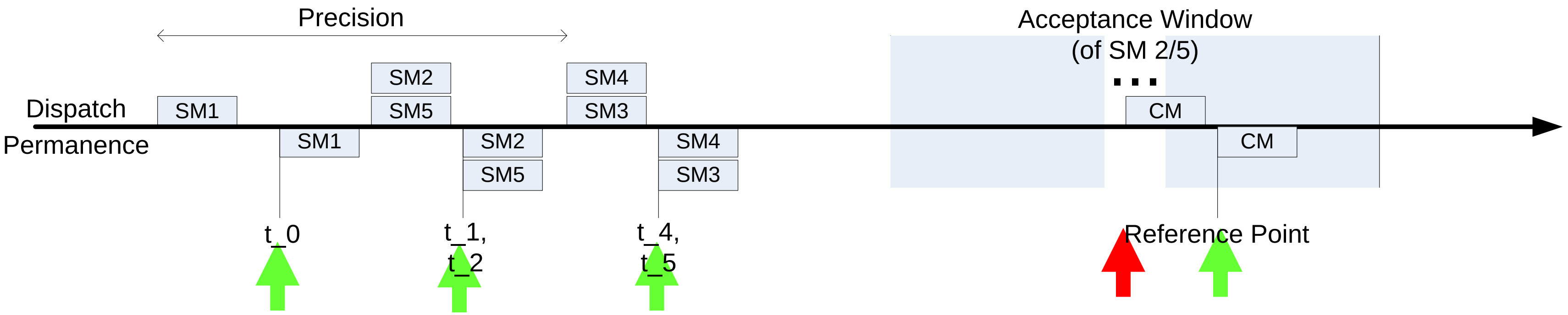
Step 1: ALL Synchronization Master Dispatch IN Frames at the SAME Scheduled Point in Time



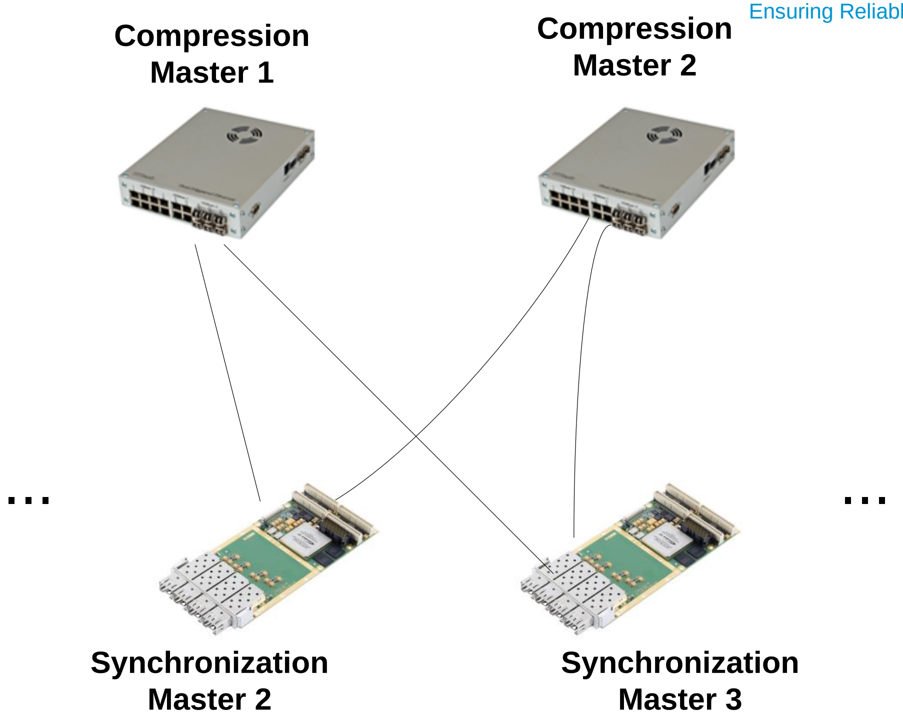


Step 2: Compression Master Dispatch Compressed IN Frame back to Synchronization Masters/Clients





Step 2: Multiple Channels/CMs



Compression Master 1

Compression Master 2

…

…

Synchronization Master 2

Synchronization Master 3

Multiple Channels/CMs are required for fault-tolerance.

Synchronization Masters (SMs) receive synchronization messages from all non-faulty Compression Masters (CMs)

SMs use either the median or the arithmetic mean on the redundant messages from the CMs.

Mandatory elements of the interface description of a FT Clock Generator

failure model: description of failure mode, number, frequency, etc.

precision: worst-case difference of any two non-faulty clocks in the system

accuracy: worst-case difference of the clocks in the system to an external time reference

startup time: worst-case time after startup of the time sources until the system is synchronized (with given precision and/or accuracy)

integration time: worst-case time for a non-synchronized component in the system to become synchronized

changeover time: worst-case time for the components in the system to change from one time source to another one (e.g., in the case that the original time source fails)

recovery time: worst-case time for the synchronized timebase to recover after global synchronization loss

Messages passing the interface

Sometimes the (clock synchronization) messages that pass an (red or blue) interface need to contain information regarding the current quality of the interface parameters (Quality of Fault Tolerance – QoFT).

Example: SAE AS6802 Protocol Control Frames

SAE AS6802 –
Protocol Control Frame Structure

“Membership New” field is filled by the Compression Master.

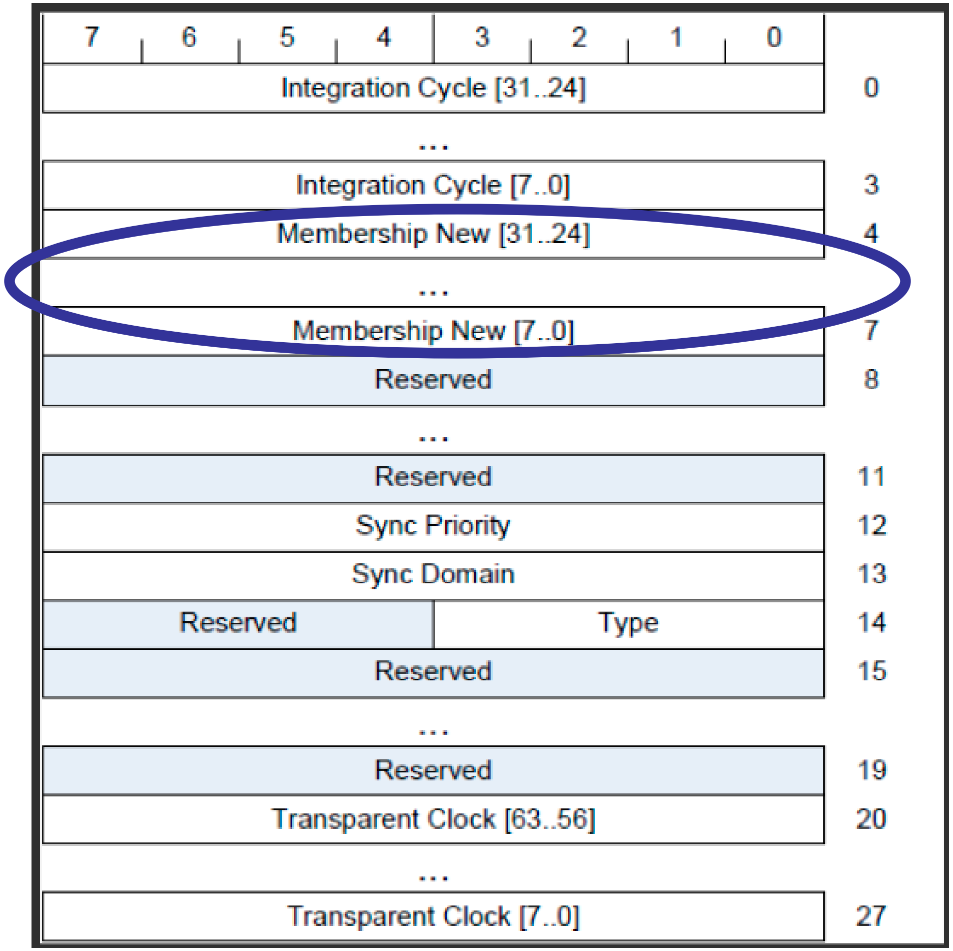
One-to-one mapping between Synchronization Masters (the NICs) and bits in the field.

Compression Master will set the bits from those NICs from which it received PCFs.

I am not advocating to add a field like this to the .1AS/1588 standards!

This detailed information should be hidden by the red interface.

A generic FT-quality field would make more sense (similar to a priority).



7 6 5 4	3 2 1 0	
Integration Cycle [31..24]		0
...		
Integration Cycle [7..0]		3
Membership New [31..24]		4
...		
Membership New [7..0]		7
Reserved		8
...		
Reserved		11
Sync Priority		12
Sync Domain		13
Reserved	Type	14
Reserved		15
...		
Reserved		19
Transparent Clock [63..56]		20
...		
Transparent Clock [7..0]		27

TTTech

Ensuring Reliable Networks

www.tttech.com