Ensuring Reliable Networks TTTech

Time-Triggered Ethernet

CCSDS Meeting

Christian Fidi, Product Manager
Christian.Fidi@TTTech.com

March 23rd, 2015

Content

- Time-Triggered Approach
- Time-Triggered Ethernet Overview
- Application Examples in Space
- Patents & Licensing
- Cross-Industry use of Technology

No Backup – the 10^{-9} Challenge

- The system as a whole must be more reliable than any one of its components: e.g., System Dependability 1 FIT – Component dependability 1000 FIT (1 FIT: 1 failure in 109 hours)
- Architecture must be distributed and support fault-tolerance to mask component failures.
- System as a whole is not testable to the required level of dependability.
- The safety argument is based on a combination of experimental evidence about the expected failure modes and failures rates of fault-containment units (FCU) and a formal dependability model that depicts the system structure from the point of view of dependability.
- Independence of the FCUs is a critical issue.

Dependable Real-Time Systems are Distributed

There are four main reasons for the distribution of intelligence in dependable embedded systems:

1. Mask failures by the application of redundancy.
2. Partition a large system into a set of smaller subsystems in order to reduce the cognitive complexity.
3. Bring local intelligence to the sensors and actuators:
   - Complexity reduction by encapsulating subsystems
   - Reduce the number of cables and cabling points, thus reducing the weight and increasing the reliability
   - Simplification of Installation and Maintenance
4. Avoid spatial proximity: independent fault-containment regions.

. . . we must support the communication among subsystems of differing criticality over the same physical wire, otherwise we will be overwhelmed by wires.

Timeliness: Distinguish between

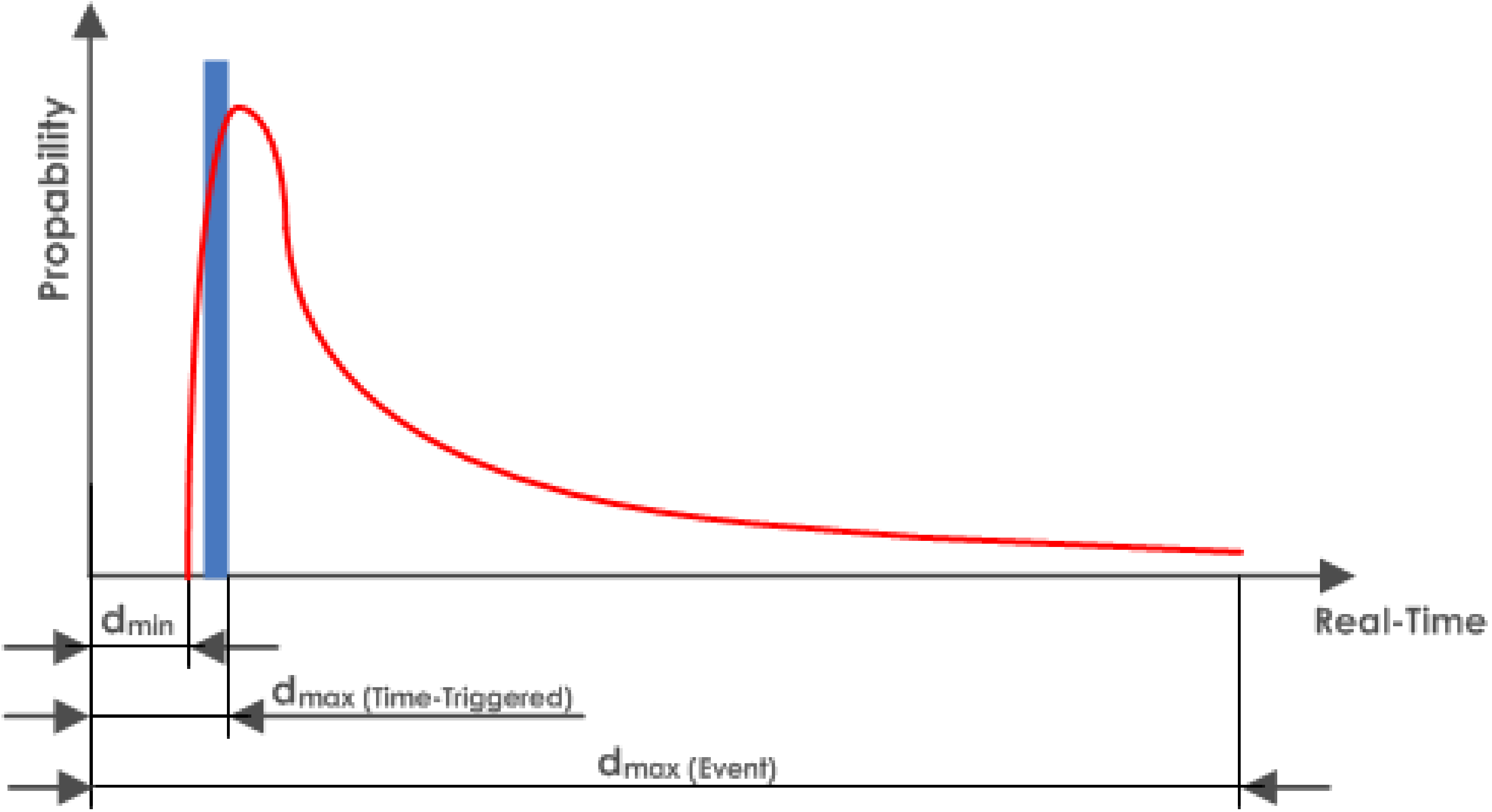
Event Triggered (ET)-Messages: (no global time needed)

- A message is sent, whenever a significant event occurs (e.g., completion of a task, arrival of an interrupt)
- Open World Assumption—possible conflicting send instants
- No Guarantee of Timeliness

Time-Triggered (TT)-Messages: (global time needed)

- An a priori planned cycle is associated with every TT message type. A TT message is sent, whenever the global time reaches the start instant of the cycle of this message type.
- Closed World Assumption—Preplanned conflict-free send instants.
- Guaranteed a priori known latency—Determinism.

Timeliness: Event vs Time-Triggered



Complexity Example:
Synchronous vs. Asynchronous

Active standby avionics system model with three components…

- **Synchronous model:** 185 reachable states (~$2x10^2$)
- **Asynchronous model & communication with no latency:** >$3x10^6$ states
- **Asynchronous model with varying communication latency:** The number of reachable states could not be calculated with 8Gb RAM…

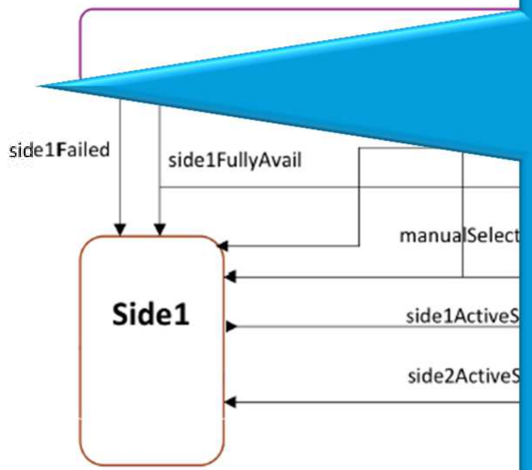


Fig. 5. The architecture of the active standby system.

>10^{8}-10^{10}

???

The number of system states in an integrated systems can be very high…
And this is still a relatively simple system…

https://www.ideals.illinois.edu/bitstream/handle/2142/17089/pals-formalization.pdf?sequence=2

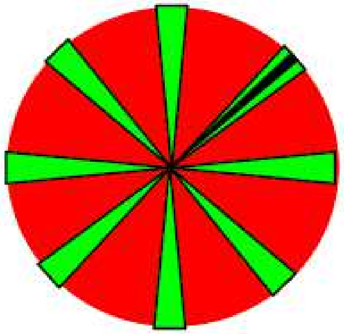
Models of Time

Dense

Physics

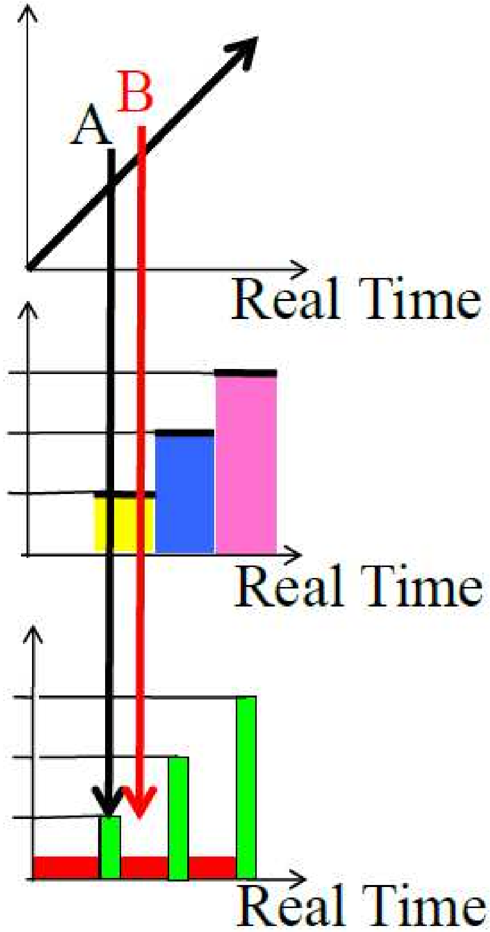
Discrete

Central Computer



Sparse

Distributed Computer



Replica Determinism: Example Stage Separation

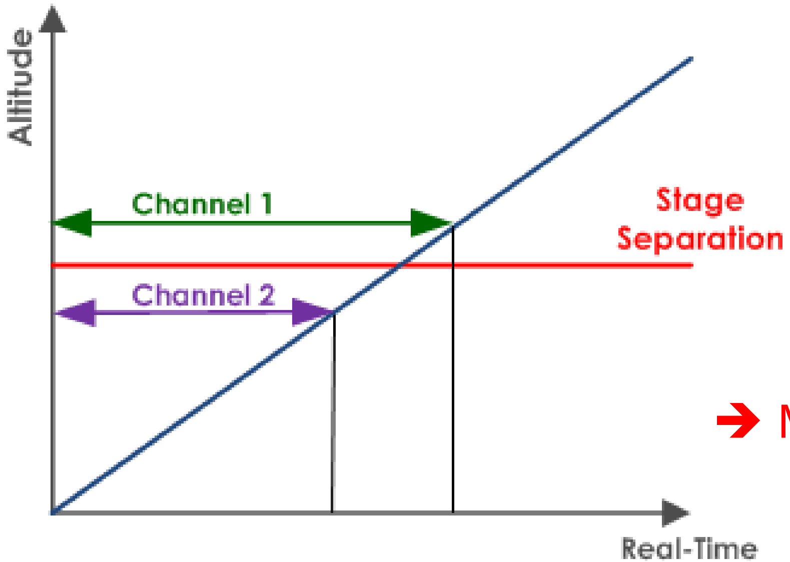
Consider a rocket launch.

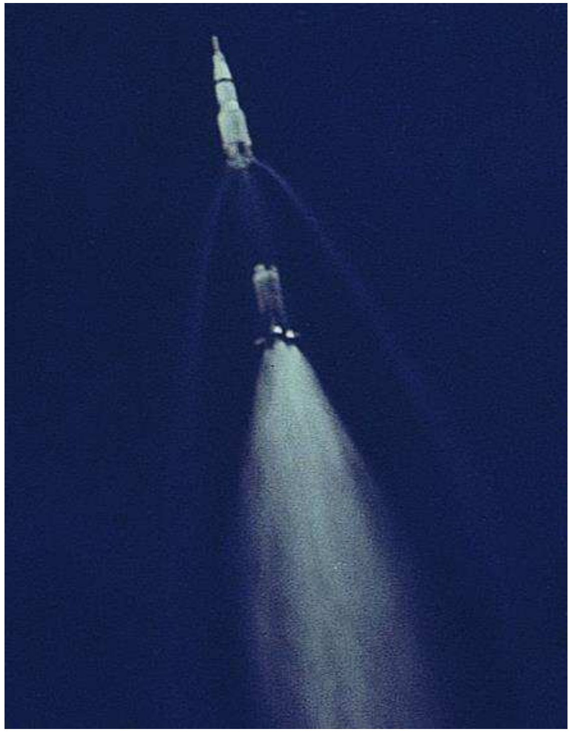
The real-time system, responsible for the stage separation system has three redundant channels:

Channel 1 – Separation and Fire Boosters

Channel 2 – No Separation and do not Fire Boosters

Channel 3 – No Separation and Fire Boosters (Fault)





➔ Majority – No Separation and Fire Boosters!!!

Motivation for Time-Triggered Ethernet

Statically Configured Communication

Performance guarantees:
real-time, dependability, safety

Standards:
- ARINC 664, ARINC 429, TTP,
- MOST, FlexRay, CAN, LIN, …

Applications:
- Flight control, powertrain, chassis,
- passive and active safety, ..

Validation & verification:
- Certification, formal analysis, ...

High cost

Free-Form Communication

No performance guarantees:
“best effort” plus some QoS

Standards:
- Ethernet, TCP/IP, UDP, FTP,
- Telnet, SSH, ...

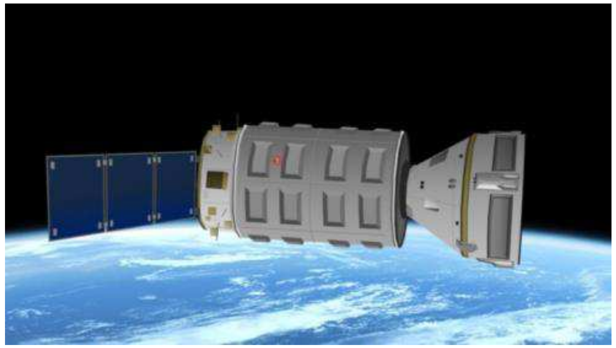
Applications:
- Multi-media, audio, video, phones,
- PDAs, internet, web, …

Validation & verification:
- No certification, test, simulation, ...

Low cost

Integration of functions from both worlds requires
a communication platform supporting both worlds

Space Programs Using Ethernet

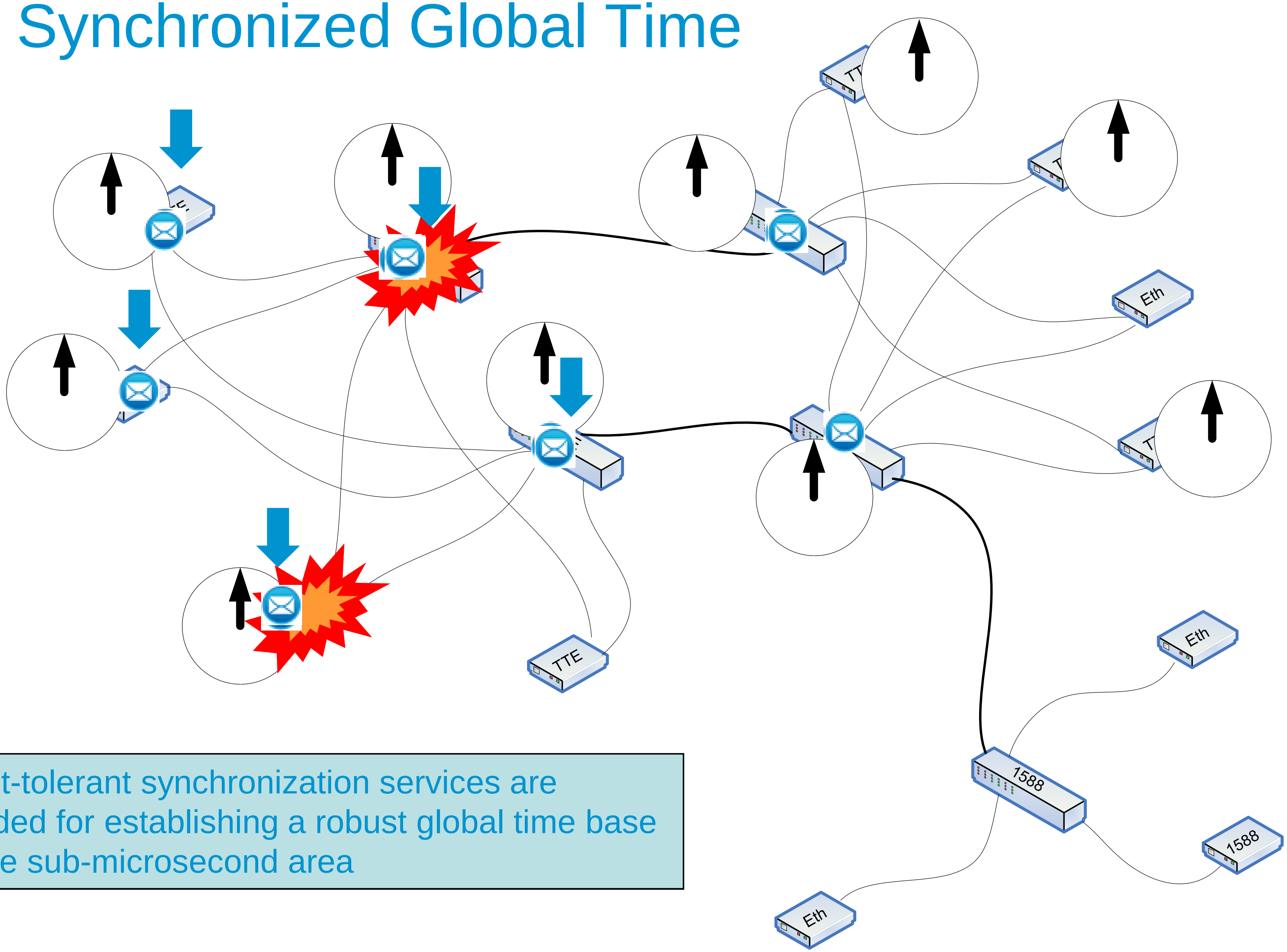


TTEthernet – Big Picture

TTEthernet = combination on the same network of

IEEE802.3	Rate-Constraint (ARINC664p7)	SAE AS6802
• best effort Ethernet • no performance guarantee	• asynchronous • jitter < 500 µs • latency typical 1-10 ms • If used as AFDX licensing from Airbus	• synchronous • jitter < 1 µs • latency < 12.5 µs/switch (1 GBit/s Ethernet) • very tight control loops

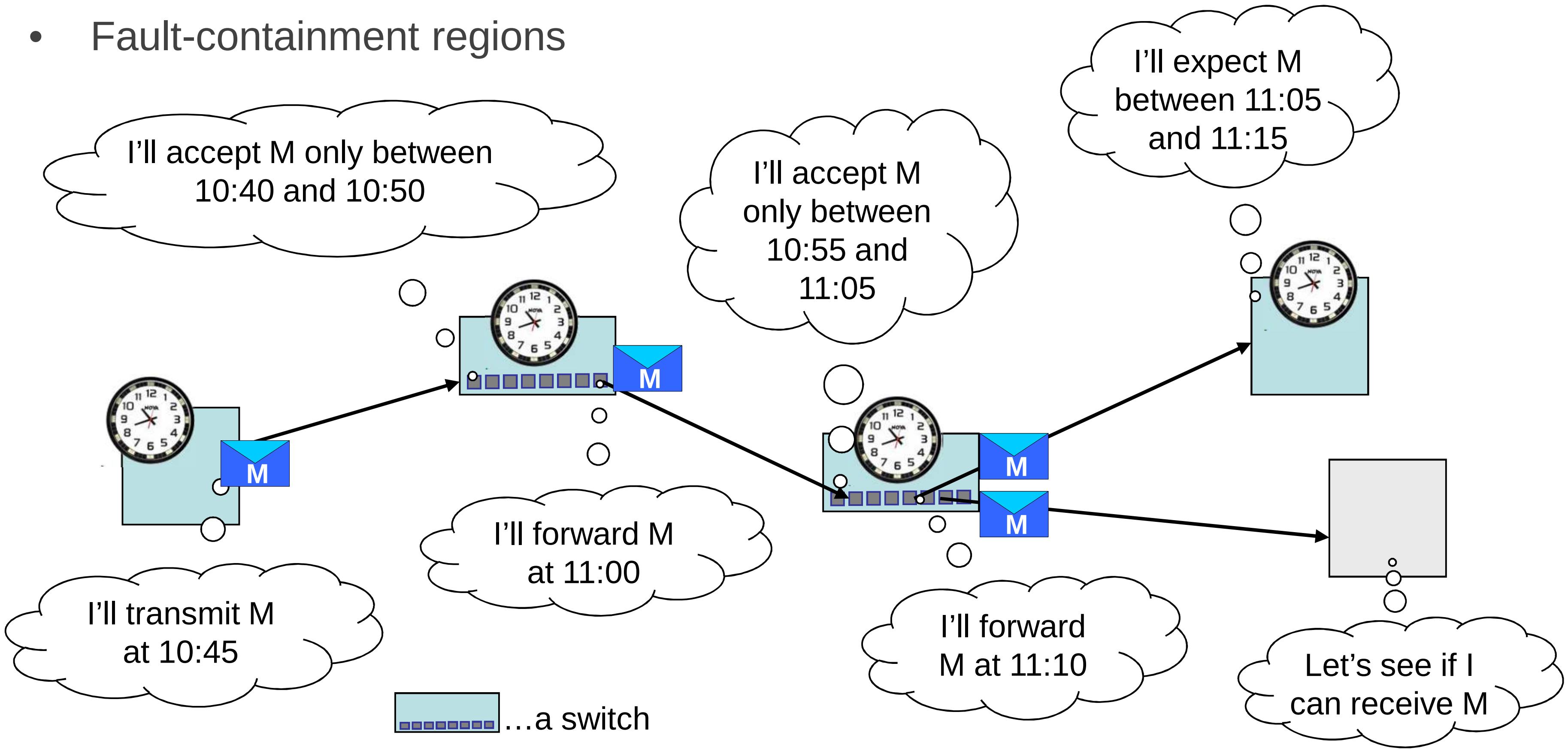
FT Synchronized Global Time



Fault-tolerant synchronization services are needed for establishing a robust global time base in the sub-microsecond area

Time-triggered Traffic Timing

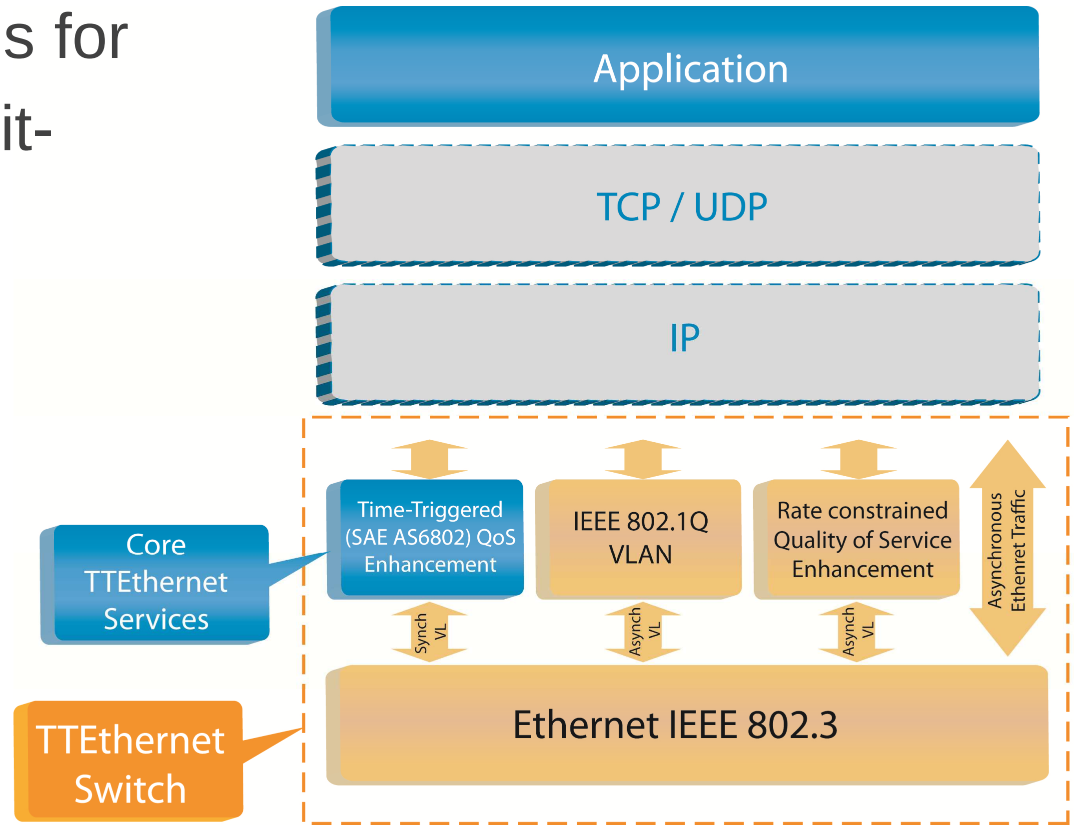
- Full control of timings in the system
- Defined latency and sub-microsecond jitter
- Minimum memory needs
- Fault-containment regions



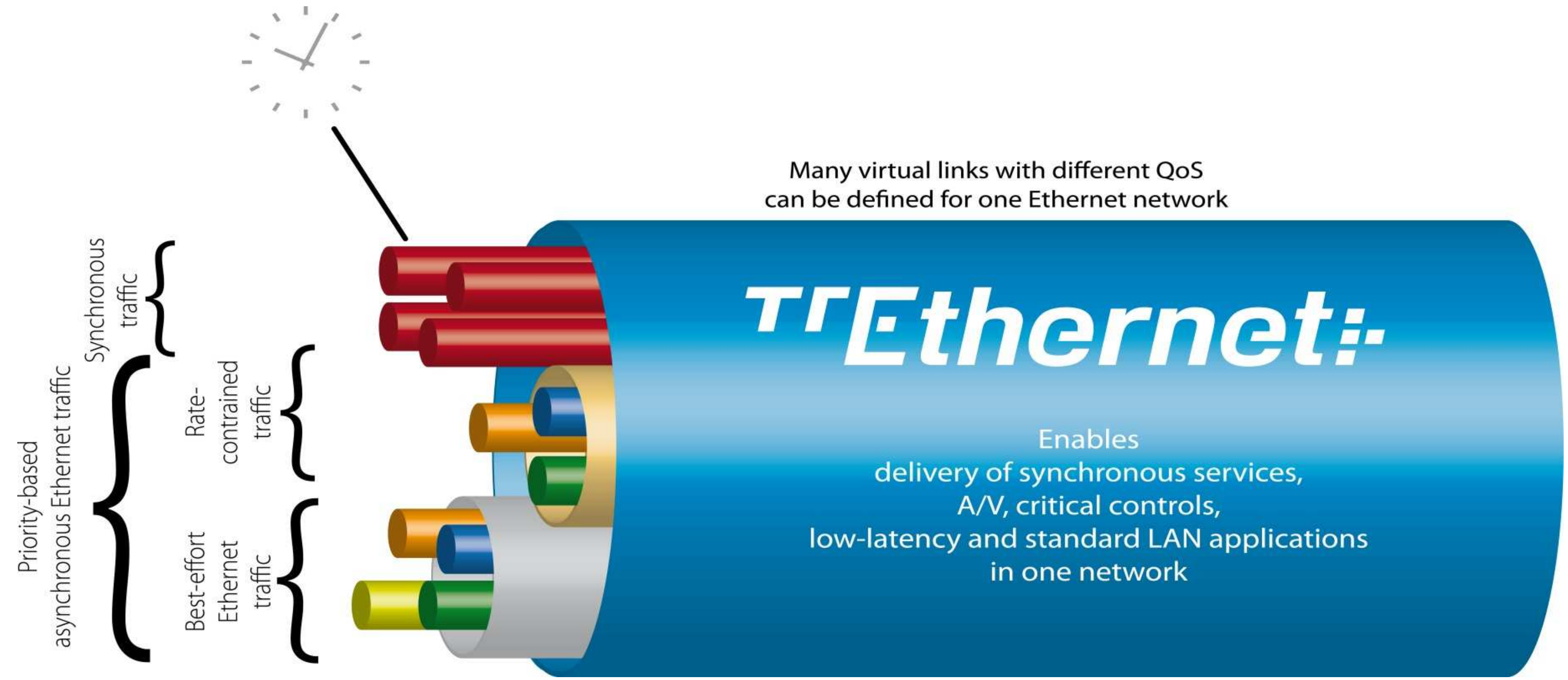
Extensions & Standard Ethernet

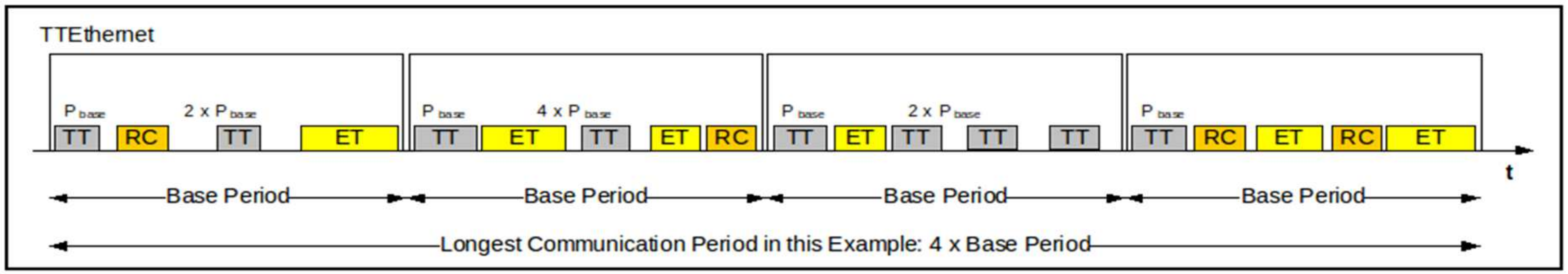
Time-triggered extensions for standard switched Gigabit-Ethernet

- Startup
- Recovery
- Robust fault-tolerant distributed clock
- Time-triggered Scheduling

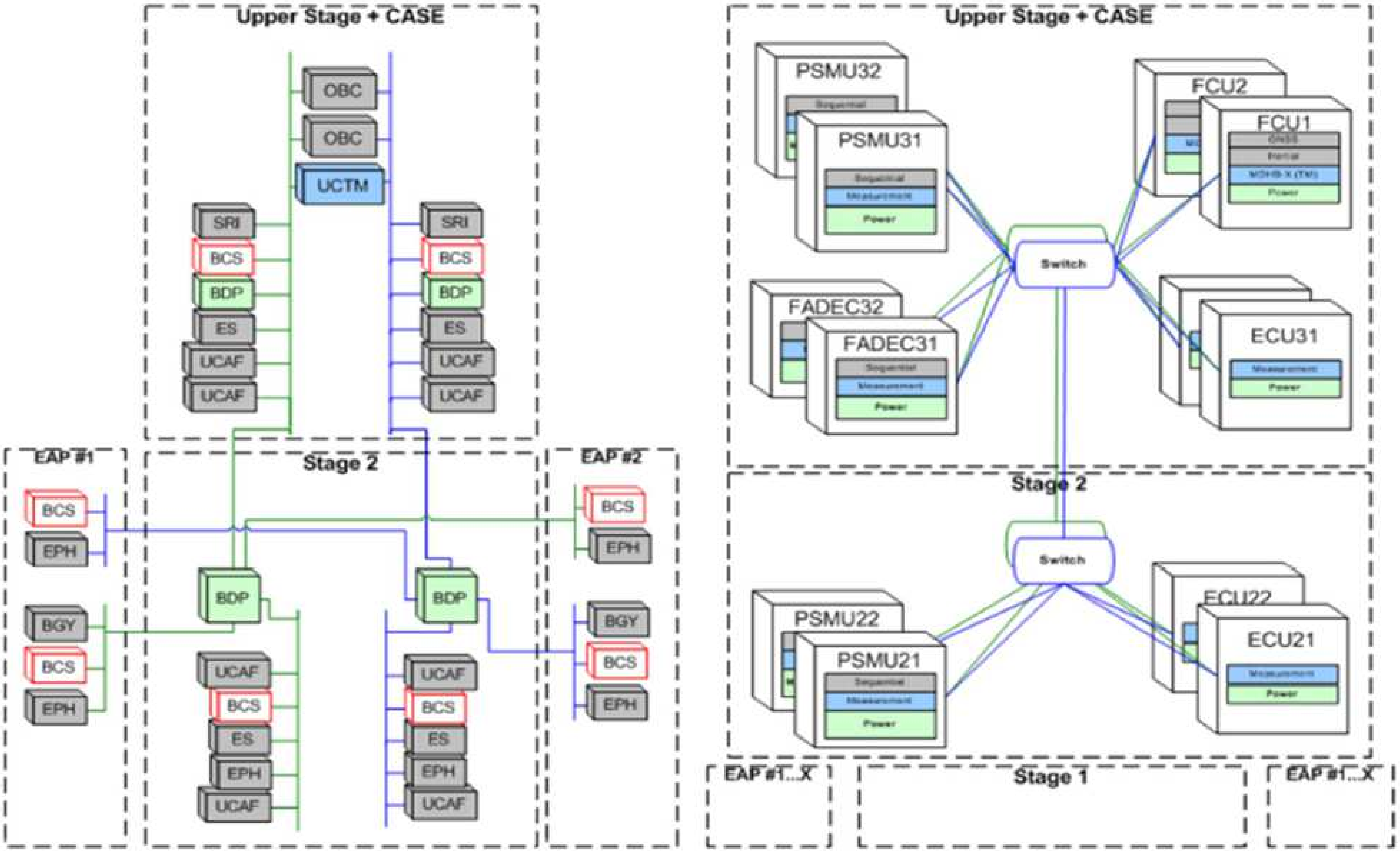


TTEthernet Traffic Partitioning





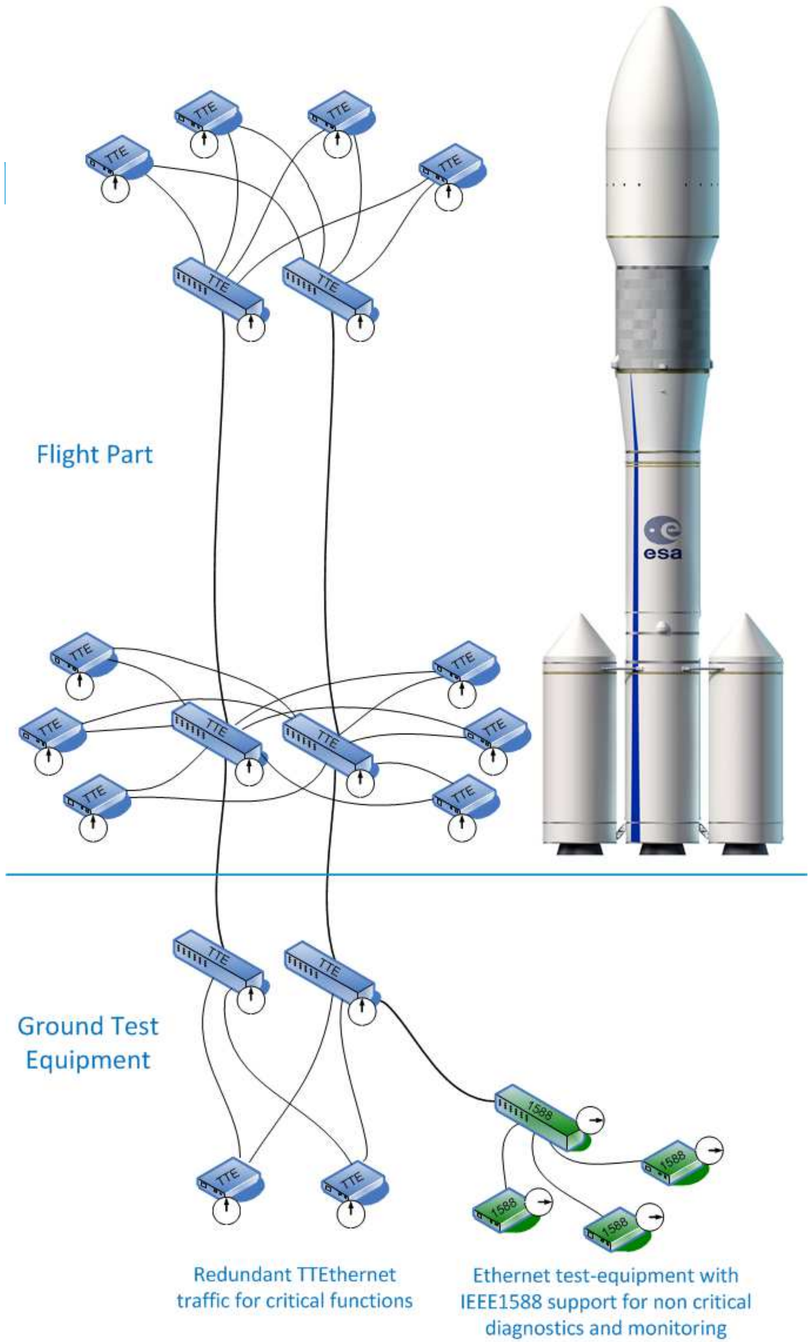
Launcher Application – Ariane 6



Launcher Application

- ❑ Single-fault-tolerance handled in the protocol (network level) ➔ Higly reliable
- ❑ One network configuration – different launcher configurations ➔ Modular
- ❑ Known latency and minimal jitter ➔ Fully deterministic
- ❑ Fault-tolerant synchronization
- ❑ Ethernet physical layer 100Base-TX ➔ Robust
- ❑ Seamless integration since the sub-systems are tested with the flight configuration ➔ Composeability
- ❑ Make use of standard Ethernet for development, testing and operations ➔ COTS based

Launcher Applicatio

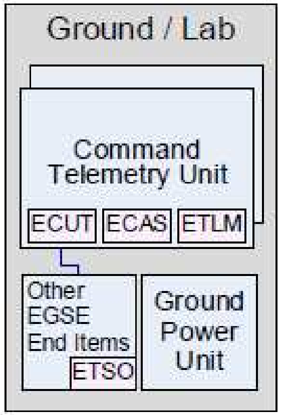


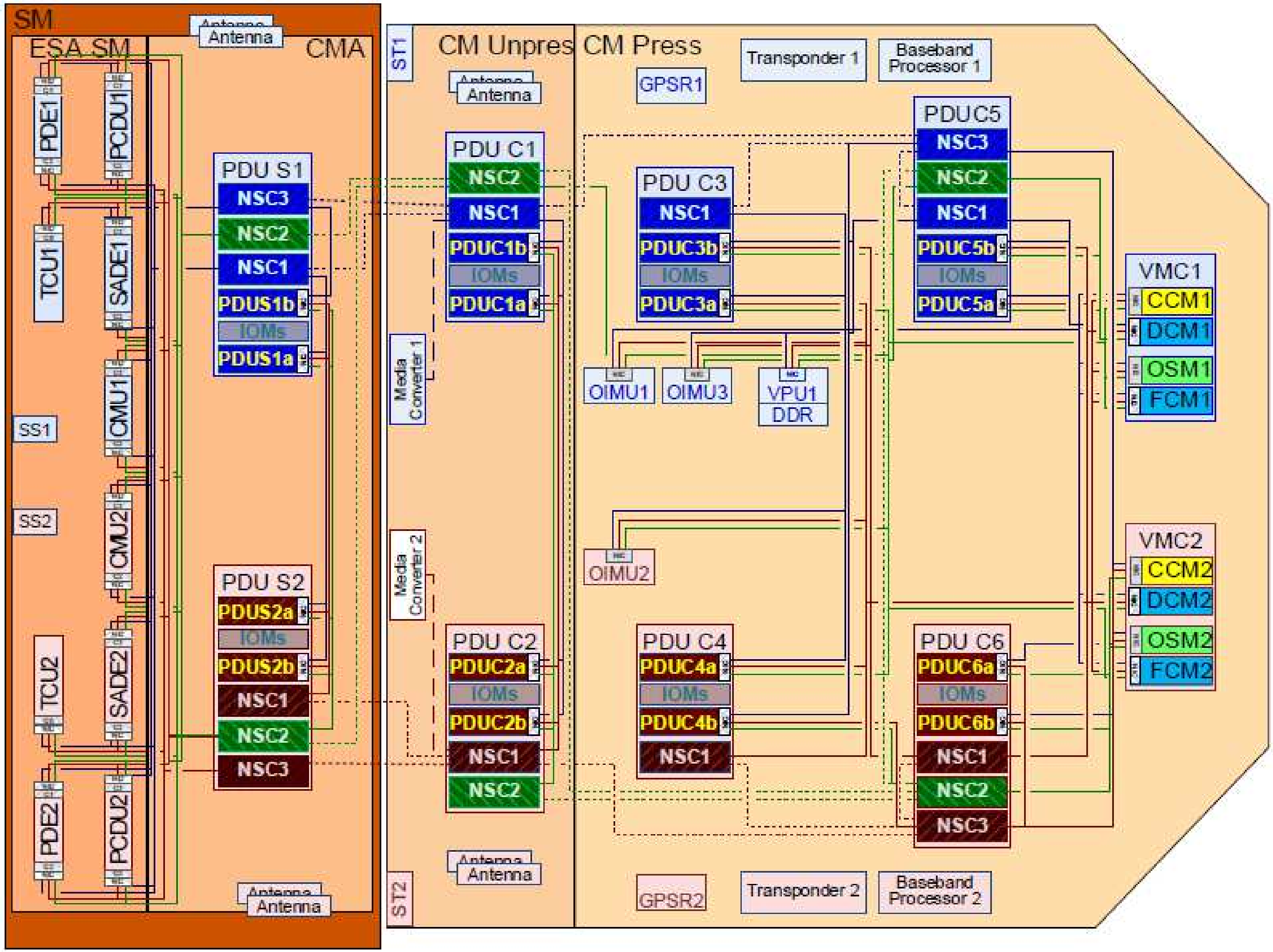
Human Space Flight Application – Example: Space Shuttle

Required Multiple Communications Functions

- ❑ Command & Status across 24 MIA Buses – MIL-STD-1553 like
- ❑ Displays across MIL-STD-1553
- ❑ Instrumentation across RS-422 (e.g. PCMMU to IDP)
- ❑ Audio for crew
- ❑ Time Distribution from MTU
- ❑ Video / Imagery (after Columbia) across IEEE-1394a
- ❑ Note: Shuttle implemented separate Communications Paths / Technologies

HSF Application – MPCV (Multi Purpose Crew Vehicle)





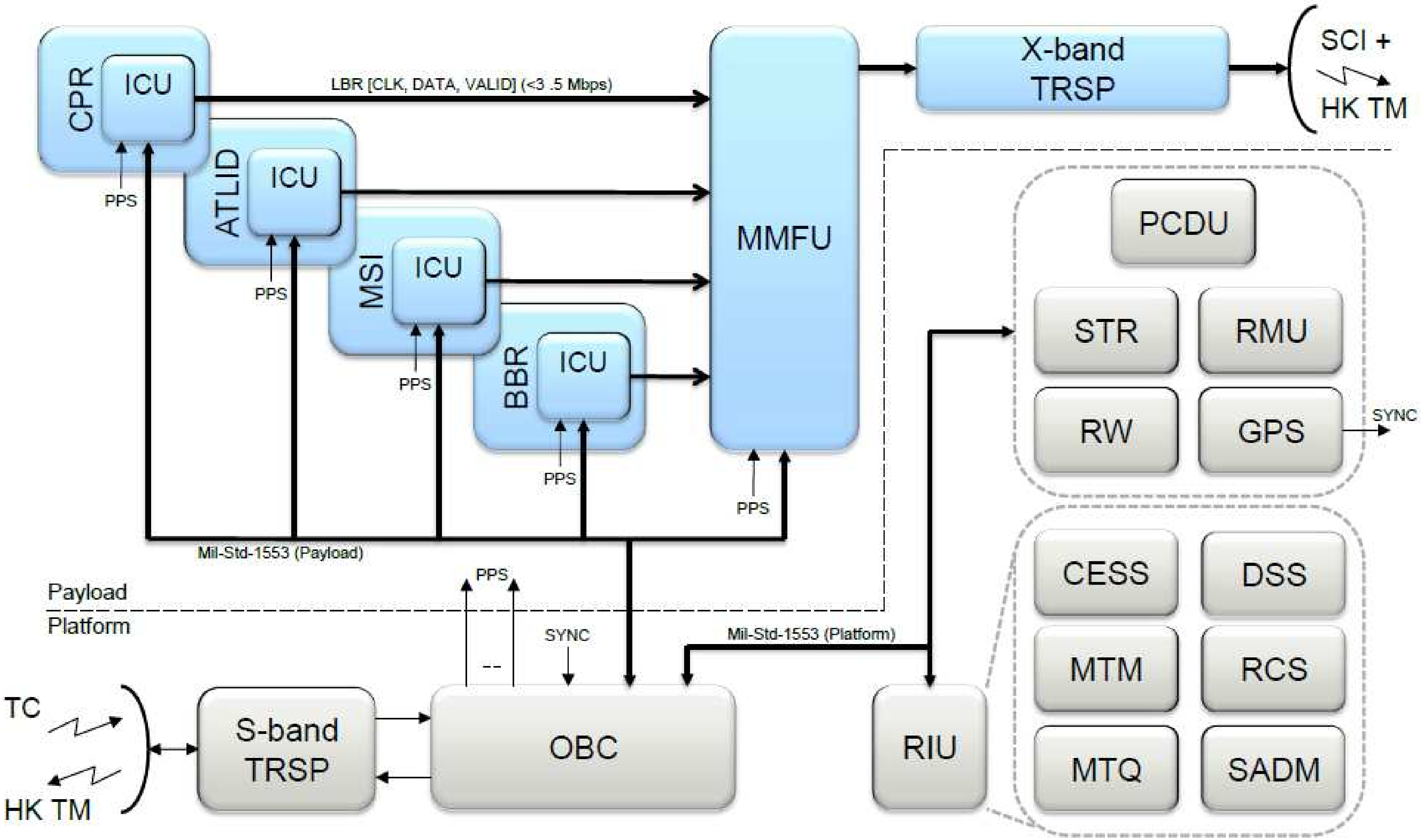
Notes:

- Only major components shown
- ODN
  - Plane 1 Blue
  - Plane 2 Red
  - Plane 3 Green
  - 18 Network Switch Cards (NSC)
  - 46 End System Network Interface Controllers (NIC)
- Serial/other – not shown
- LAS not shown

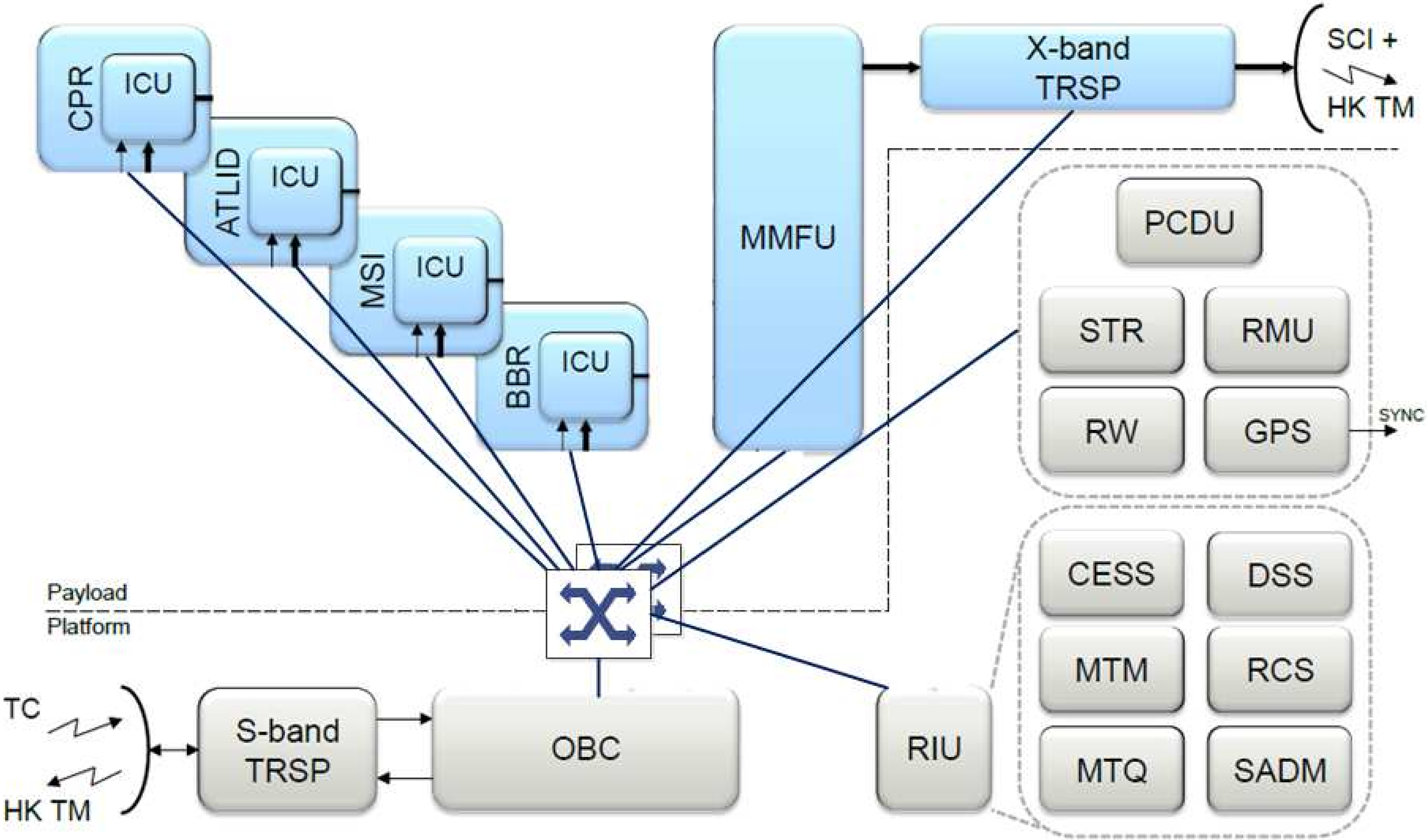
Human Space Flight Application

- ❑ Up to dual-fault-tolerance handled in the protocol (network level) ➔ Higly reliable
- ❑ Full determinism (known latency and minimal jitter) ➔ Highly deterministic
- ❑ Full traffic partitioning (combine platform and payload) ➔ Easy access to shared ressource e.g. TSP OS
- ❑ Fault-tolerant synchronization
- ❑ Seamless integration since the sub-systems are tested with the flight configuration ➔ Composeability

Satellite Application



Satellite Application



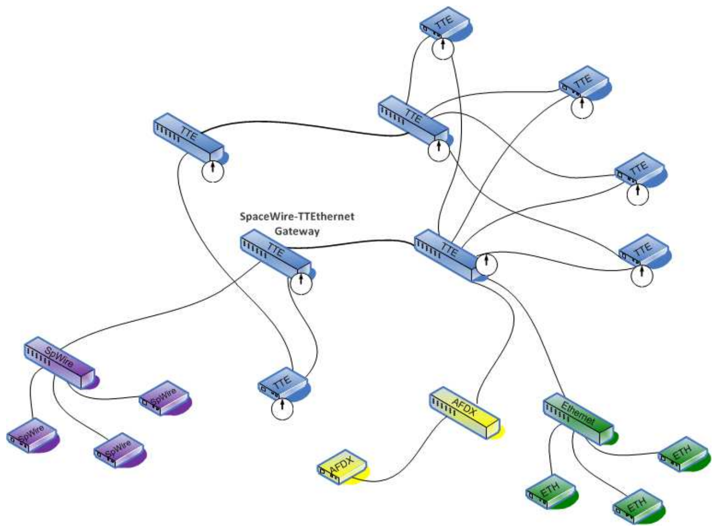
Satellite Application

- Globale synchronized time-base (important for platform and payload) ➔ One trusted timebase
- Synchronization to GPS (all data is timestamped with a precise absolutestamp) ➔ One absolute timebase
- Full determinism (known age of data important for platform an payload) ➔ Allows distributed computing
- Full traffic partitioning (combine platform and payload) ➔ Easy access to shared ressource e.g. TSP OS
- Seamless integration since the sub-systems are tested with the flight configuration ➔ Composeability
- Real-time ➔ Reduced memory needs (no buffering necessary)

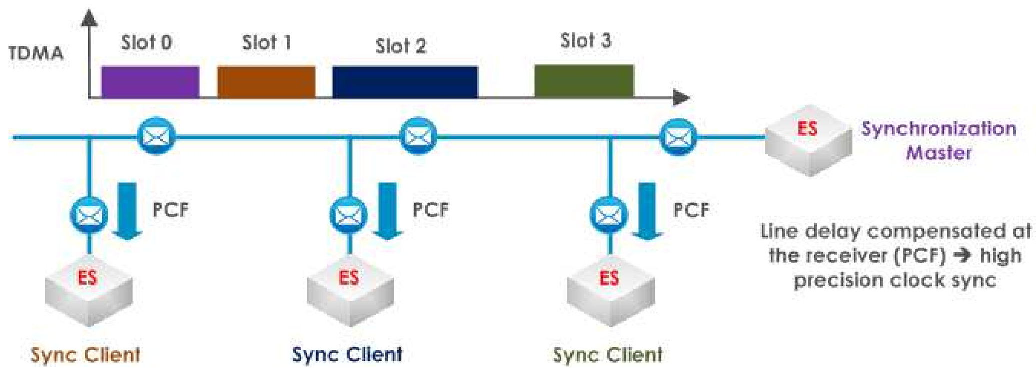
A Scalable Solution

TTEthernet is scalable concerning the architecture, the network speed, fault-tolerance and the degree of determinism

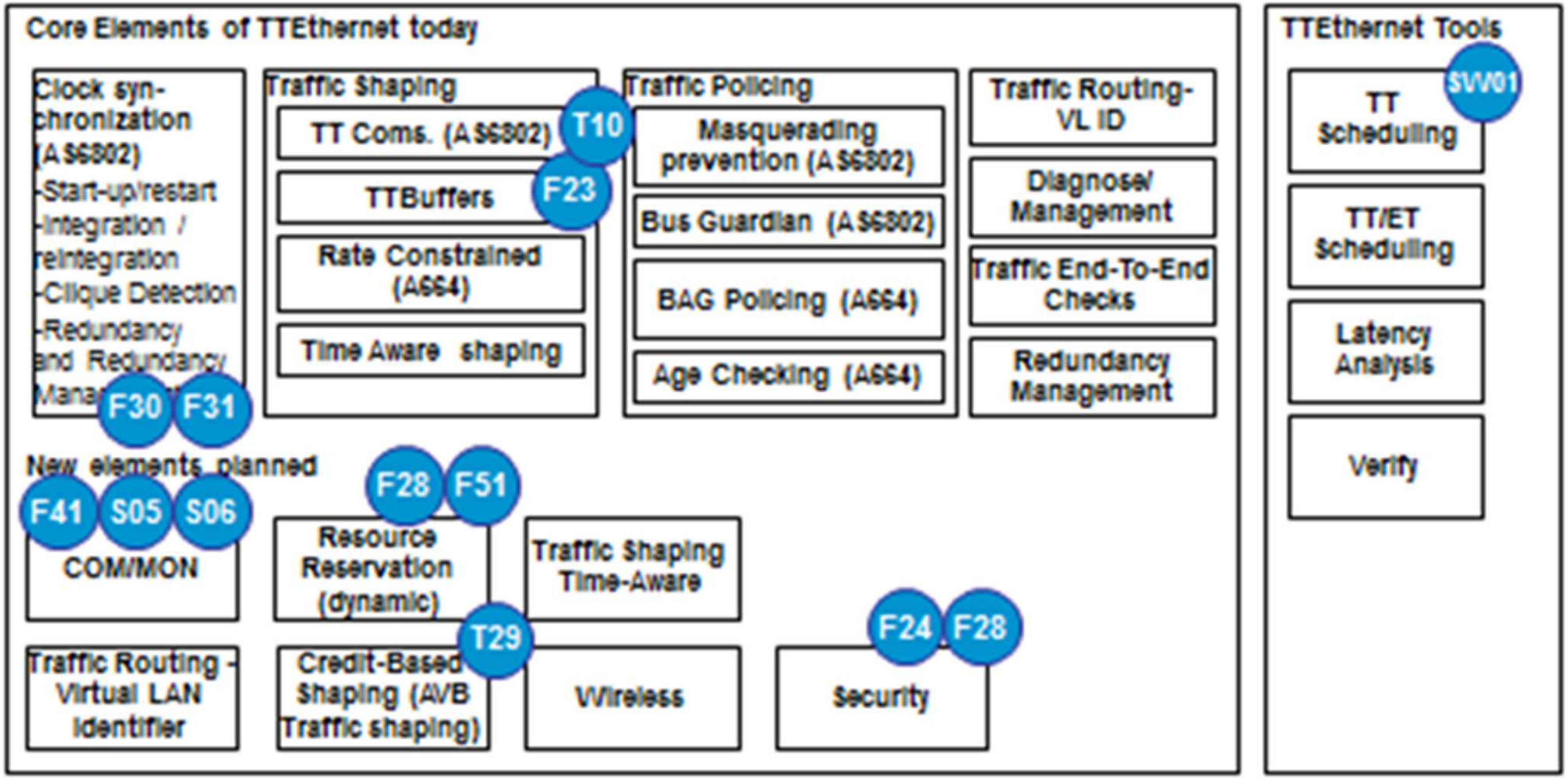
10/100/1000/10000Mbps via Ethernet



1Mbps via RS485



Patents Overview



CCSDS and other Standards

- TTTech is willing to license its patents under reasonable and non-discriminatory terms and conditions with applicants
- This has been also for SAE

LETTER OF ASSURANCE

Please return to: SAE IP Department
SAE International
400 Commonwealth Drive
Warrendale, PA 15096
USA

No License is implied by submission of this Letter of Assurance

PATENT OWNER/ORGANIZATION:

Legal Name of Organization: TTTech Computertechnik AG

PATENT OWNER'S CONTACT FOR LICENSE APPLICATION:

Name & Department: Georg Kopetz
Address: Schoenbrunnerstr. 7, A-1040 Wien
Telephone: +43 1 585 34 34 12 Fax: +43 1 585 34 34 90 E-mail: georg.kopetz@tttech.com

PROPOSED SAE TECHNICAL REPORT:

Number: AS6802
Title: Time-Triggered Ethernet

PATENT HOLDER'S POSITION REGARDING LICENSING ESSENTIAL PATENT RIGHTS

2. The Patent Holder is prepared to grant a *license** to an unrestricted number of applicants on a worldwide, non-discriminatory basis and on reasonable terms and conditions to comply with such Proposed SAE Technical Report.

- Does Patent Owner agree that its patent is required to comply with Proposed Technical Report?
- If Owner agrees its patent is required, please provide the patent number and claims affected.
  - Patent Number(s): ______
  - Claims Affected: ______

Licenses to an applicant denied on basis of pending or ongoing patent litigation with Patent Holder is not deemed discriminatory, nor is a license that includes a reciprocity requirement, field of use restrictions or termination upon withdrawal of Proposed Technical Report deemed unreasonable for such inclusion.

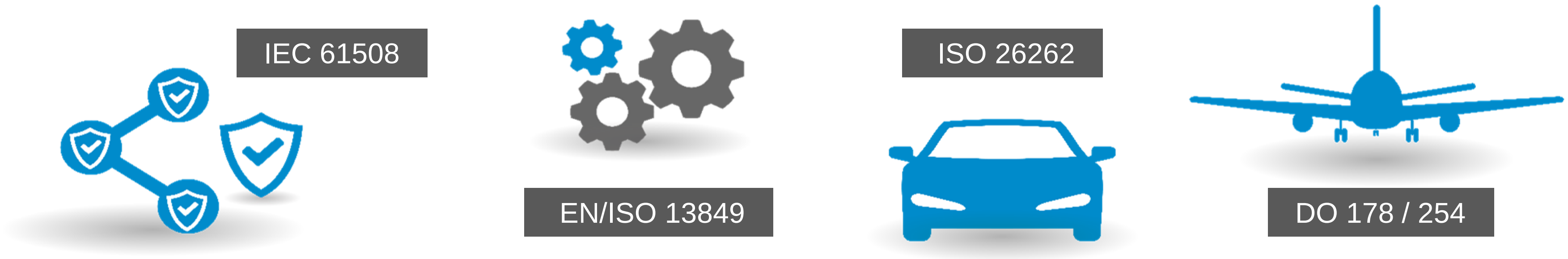
SIGNATURE
Print name of authorized person: GEORG KOPETZ
Title of authorized person: MEMBER OF THE EXECUTIVE BOARD
Signature of authorized person: [signature] Date: Sept. 6th 2011

Fail-Stop and Fail-Operational Requirements

TTTech

Strong trend towards fail-operational

Design assurance standards are similar across industries



Deterministic Ethernet

TTTech

Critical real-time traffic guaranteed in a converged network

Deterministic Ethernet Network Representation

Best-Effort IEEE 802.3	QoS / AVB IEEE 802.1Q	TSN IEEE 802.1Qbv	TTEthernet SAE AS6802
Low Criticality	Streaming	Scheduled	Deterministic
• Diagnostic over IP • Background Traffic	• Audio/Video • Sensor Fusion	• Real-time Control over IP	• Fault-Tolerant and Safety Systems

Guarantee of Service

Ensuring Reliable Networks

Vienna, Austria (Headquarters)
Phone +43 1 585 34 34-0
office@tttech.com

USA
Phone +1 978 933 7979
usa@tttech.com

Japan
Phone +81 52 485 5898
office@tttech.jp

China
Phone +86 21 5015 2925-0
china@tttech.com

www.tttech.com