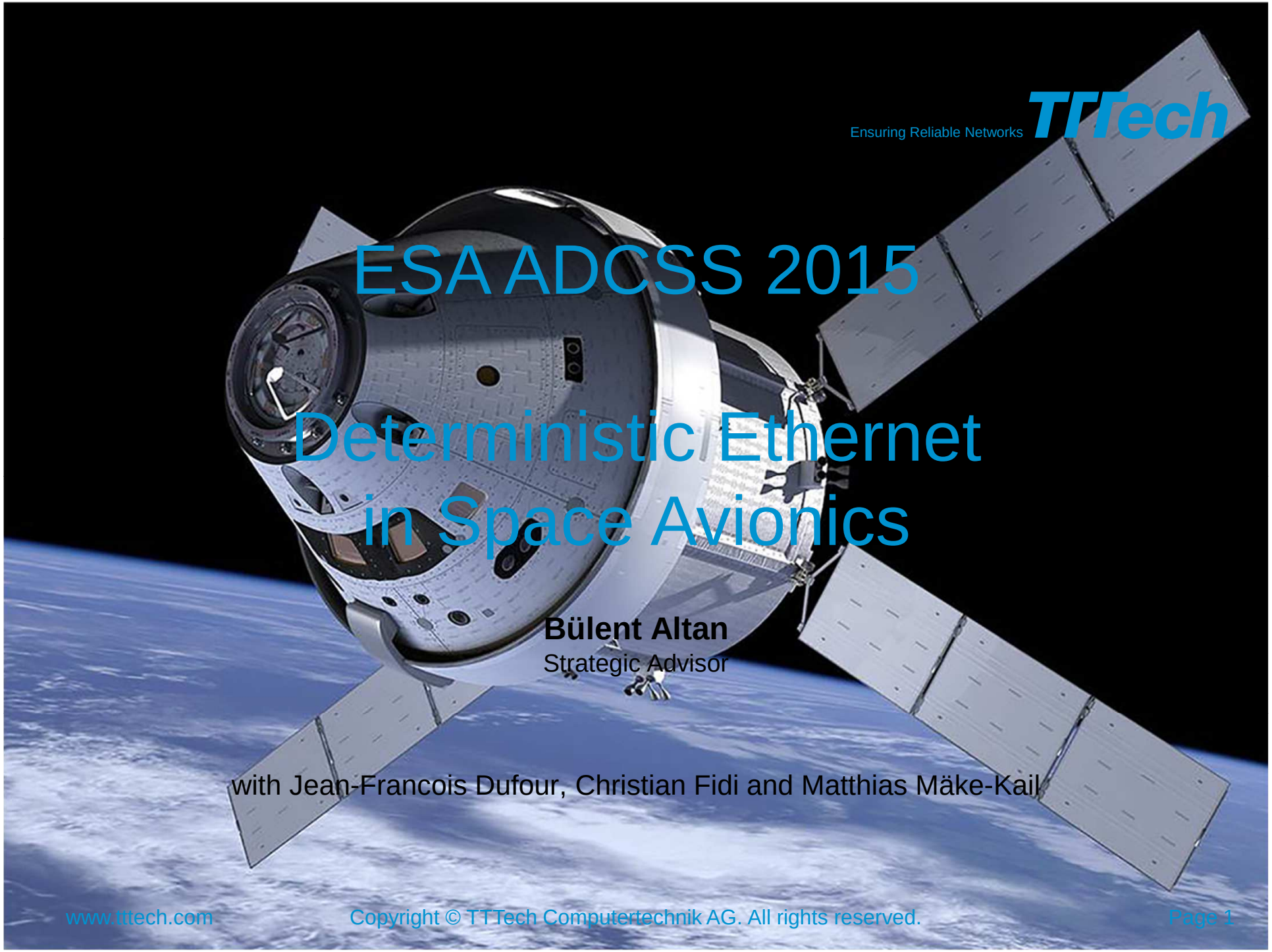


Ensuring Reliable Networks TTTech

ESA ADCSS 2015

Deterministic Ethernet in Space Avionics

Bülent Altan
Strategic Advisor

with Jean-Francois Dufour, Christian Fidi and Matthias Mäke-Kail

Content

- Space Avionics: Trends & Challenges
- Communication Requirements + Deterministic Ethernet
- Spin-in of Existing (Communication) Technology
- Federated Architectures / Distributed IMA
- Scalable, Modular Platforms + Related Savings
- Current R&D Status
- State-of-the Art Examples with TTEthernet
- Conclusions

Trends

- Globalization of space industry
- Emergence of “new space”
- Launchers used to be stable, “high-volume” platforms
- Nano-satellites and constellations are becoming the high-volume platforms
- …and drive the requirements for new launchers
- Automotive industry *drives* electronics innovation – particularly with autonomous driving
- …and this is of course being noted by space agencies and the space industry
- FPGAs become more affordable, ASIC designs more costly

Challenges

- Software has become the largest portion of spacecraft development cost (30-40%)
- Data rates and volumes increase drastically (new instruments and sensor technologies, new on-board functions and increased autonomy)
- While hardware costs decrease, more functionality is asked of avionics systems which creates even more pressure on software development
- …Yet shorter development times are needed for economic feasibility
- Software development widely seen as main schedule risk
- Can automotive or industrial solutions be re-used?
- …and how does this impact obsolescence management?
- Can one platform cover such diverse spacecraft as launch vehicles, earth observation satellites and human rated capsules or habitats?
- And of course the perennial challenge of weight reduction

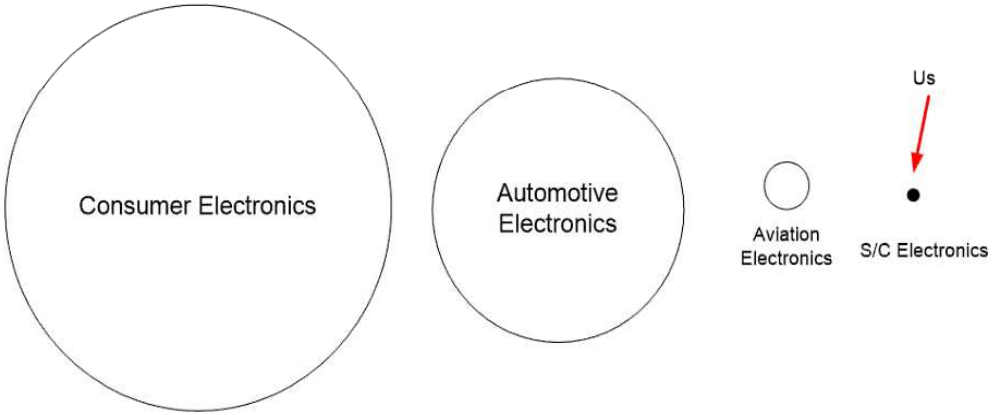
Challenge:
Tiny Space Electronics Market

CIF: Harness Reduction Workshop

Jet Propulsion Laboratory Div. 34

- The Avionics Development Dilemma
  - S/C Electronics Development vs. Industry
    - Business base for JPL avionics is actually very small

S/C Electronics Business Base



  - Need to employ collaboration, leverage and synergy to advance in this area

JAD - 12 Europa System Bus Trade

Space Data Handling Requirements

CIF: Harness Reduction Workshop

Jet Propulsion Laboratory Div. 34

- Real World Interconnect "Care-abouts" — Priority
  - **Must be serial** — **(0)**
  - Must have commercial COTS test equipment — (1)
  - Redundancy considerations built in — (2)
  - Must have programmatic legs — (3)
    - User base outside of JPL
  - Must have technical legs — (4)
    - Higher data rates possible
    - Fiber optic implementation possible
  - Must be dc isolated — (5)
  - Must be self-clocking protocol — (6)
  - **Must be 100 mbps or better** — **(7) → 100 times faster**
  - 20 meter length — (8)
  - Must support separation interfaces — (9)
  - Time Distribution Support — (10)
- Buses that failed these top criteria were deemed "Not Worthy"

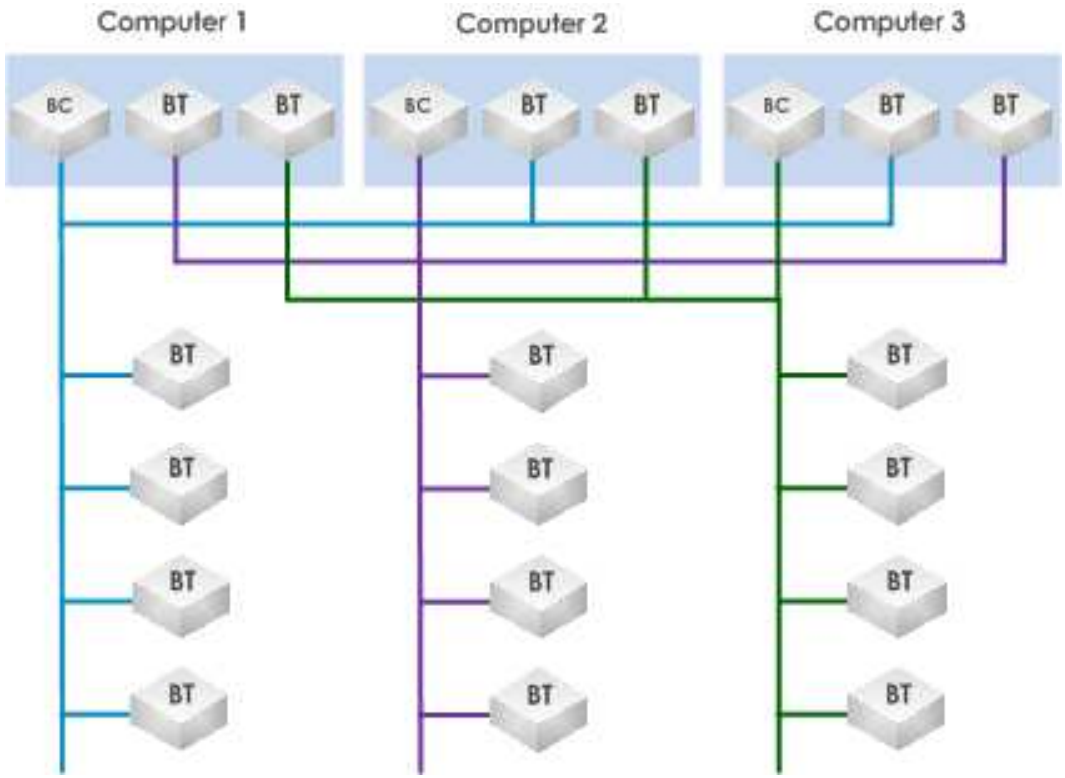
August 11th, 2013

JAD - 13

Europa System Bus Trade

Legacy Architecture – MIL1553 (TT)

- 3 redundant busses/lanes (1FT but not covering byzantine faults)
- Each computer has one bus master node (bus controller)
- All computers receive the messages from the other lanes where they are slave
- Precise synchronization has to be done between the lanes to be able to vote (state exchange)
- If one node fails than whole lane may be lost, voting is done in a two out of three manner
- Max. 1 Mbps



[© 2010 Data Device Corporation. Distributed and Reconfigurable Architecture for Flight Control System]

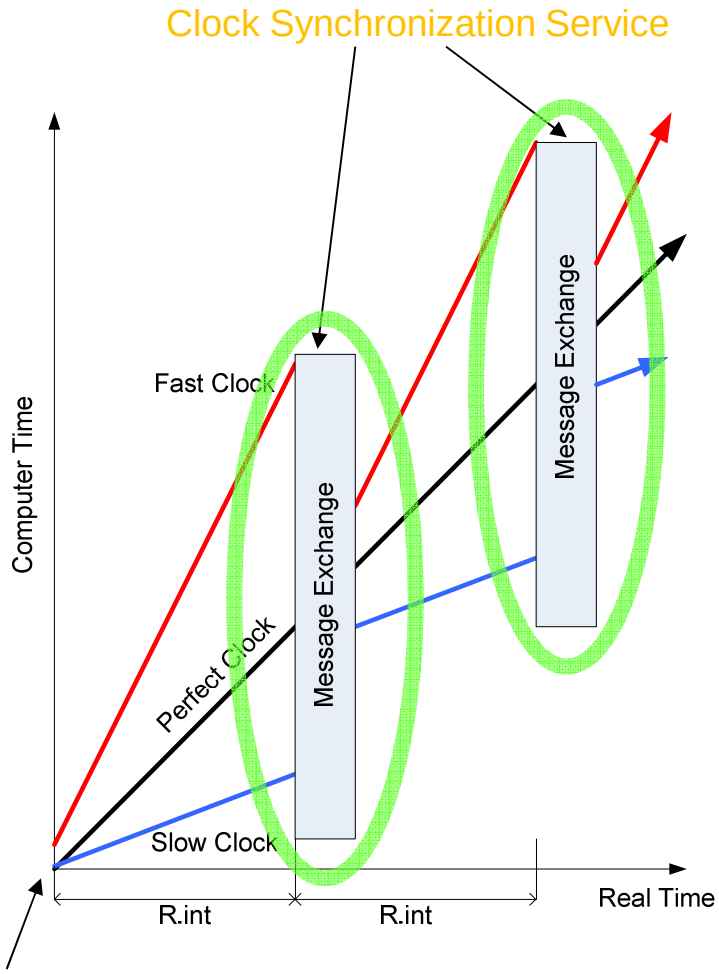
Using Non-Deterministic Ethernet

- Additional point to point needed to ensure low latency synchronization where needed for time critical control systems
- Multiple protocols needed which drive more hardware interfaces to be designed → standardization is not achieved
  - Synchronization
  - Deterministic data
  - High speed data
- Additional wiring needed on top of the Ethernet wiring (example ISS)
- Software needs to take care of:
  - Precise synchronization
  - Redundancy management
  - Driver support with different protocols
- This all leads to additional testing effort and hardware as each interface needs to be verified at each level and then all the different interfaces and protocols in their interaction with each other

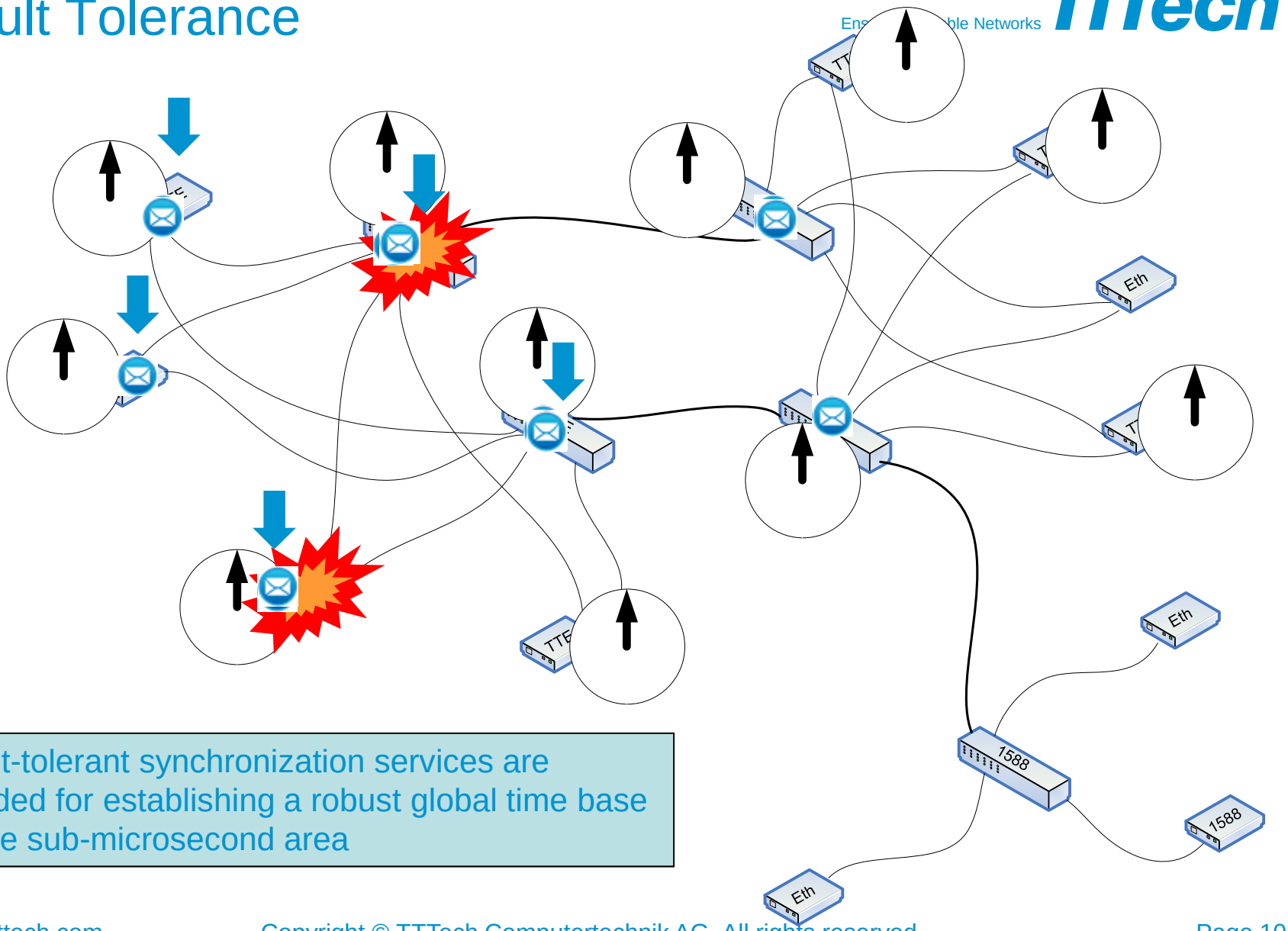
Requirement:
Clock Synchronization

Ensuring Reliable Networks TTTech

- Requirement is to have all computers within the control network work off a synchronized clock for purposes of time stamping, telemetry and control alignment and messaging de-conflict
- With TTEthernet Clock Synchronization:
  - Startup/restart service - initial synchronization of the local clocks is established
  - Integration-reintegration service to join components into an already synchronized system
  - Clique detection services to detect loss of synchronization and establishment of disjoint sets of synchronized components



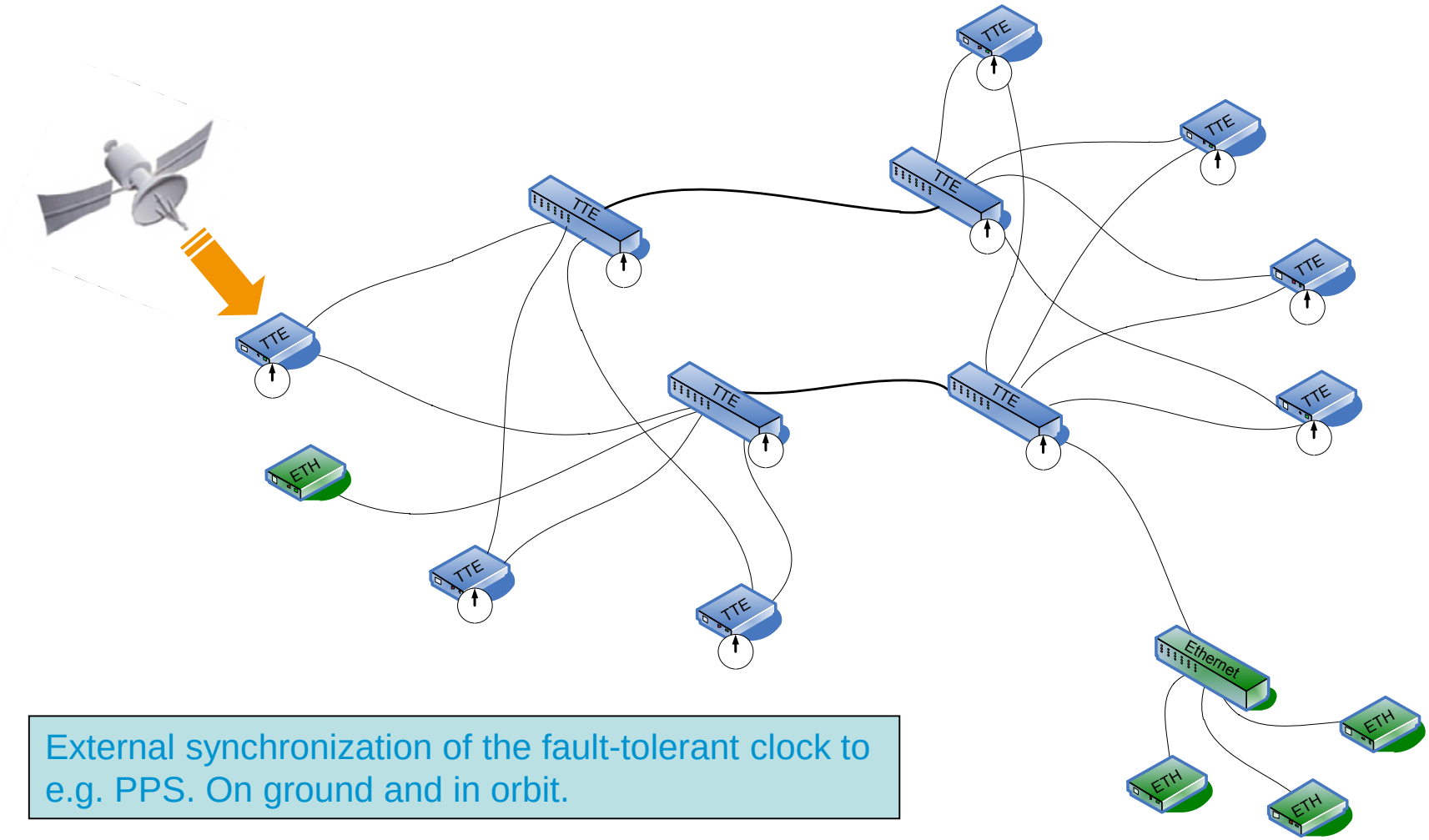
Requirement:
Fault Tolerance



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

Requirement:
External Clock Synchronization

Ensuring Reliable Networks TTTech



External synchronization of the fault-tolerant clock to e.g. PPS. On ground and in orbit.

Requirement:
Robust Partitioning

Ensuring Reliable Networks TTTech

Need to support multiple traffic classes over the same hardware and cabling.

TTEthernet = A network infrastructure that combines

IEEE802.3

- best effort Ethernet
- no performance guarantee (non-deterministic)

ARINC664p7

- asynchronous
- bandwidth guarantee
- jitter < 500 µs
- latency typical 1-10 ms
- TTTech AFDX licensee

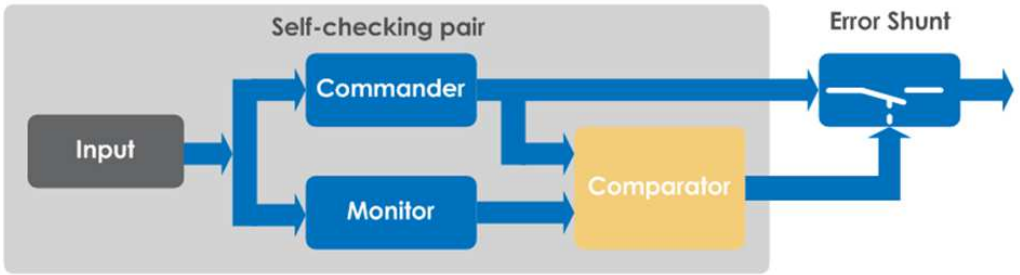
SAE AS6802

- synchronous
- fully deterministic
- jitter < 1 µs
- latency < 12.5 µs/switch (1 GBit/s Ethernet)
- very tight control loops

without interference!

Requirement:
Fail Silent

- To avoid designs which need a full two out of three voting architecture to deal with Byzantine behavior, network components need to be “fail silent”
- Therefore a high integrity design with a self checking pair is crucial
- Two processors that execute the same function in parallel
- Comparator checks output of both processors / switch cores
- If one processor fails (maliciously) and generates wrong data, second processor shuts down

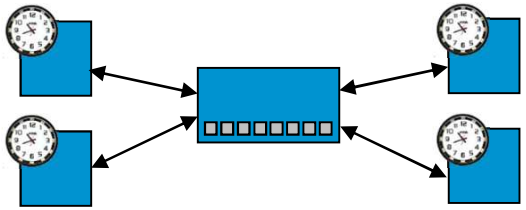


Self-checking pair ensures fail-silence !

Requirement:
(Hot) Redundancy

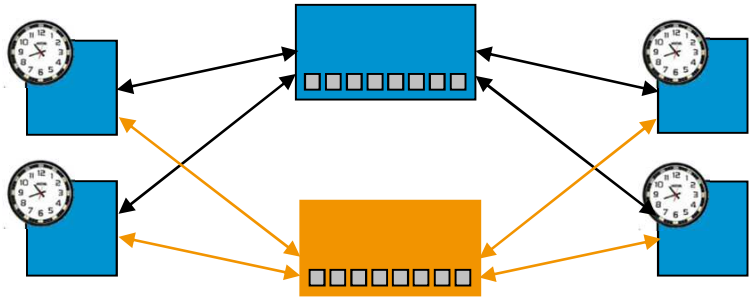
Ensuring Reliable Networks TTTech

The architecture should be immediately fail operational as many of the applications can not stay in a safe state (proxy operations, launch vehicle)



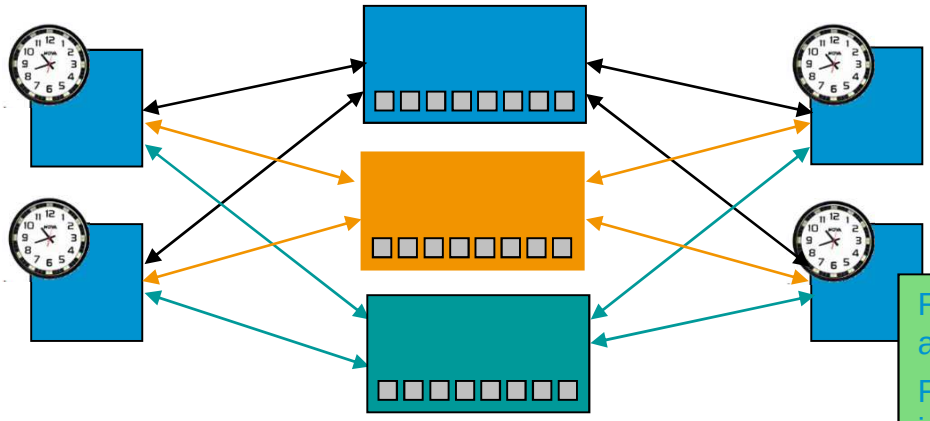
Regular network: No redundancy.

Fail-silent: Safe state in case of failure.



Regular network: Redundant to communication outage e.g. broken cable.

Fail-silent: Full single fault tolerance.

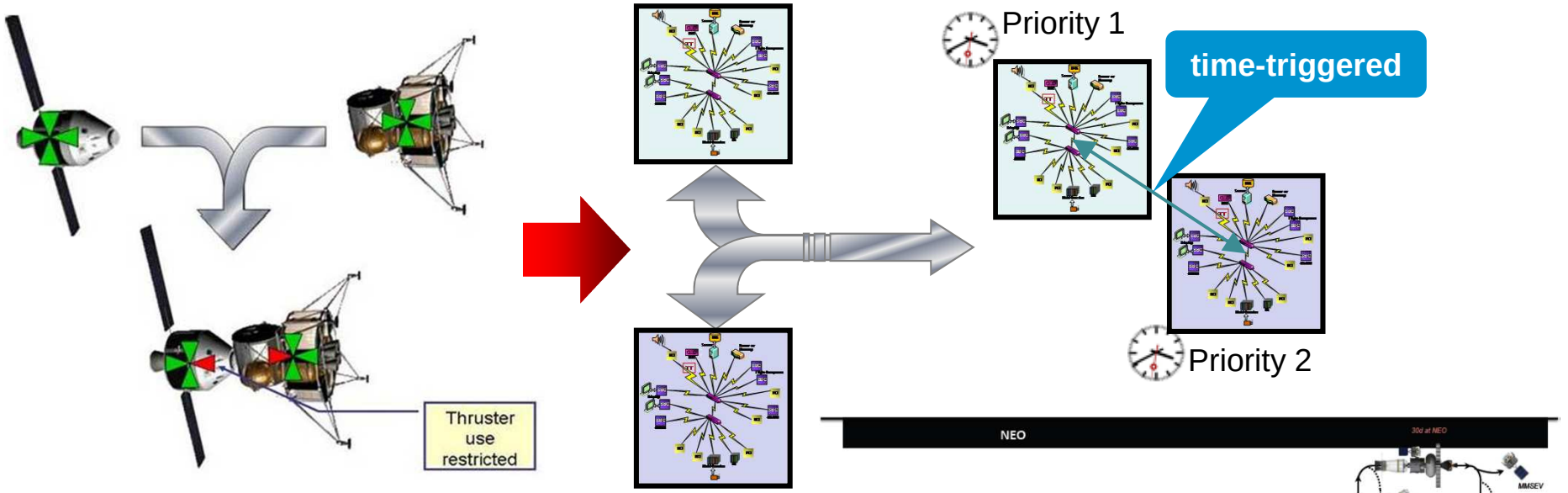


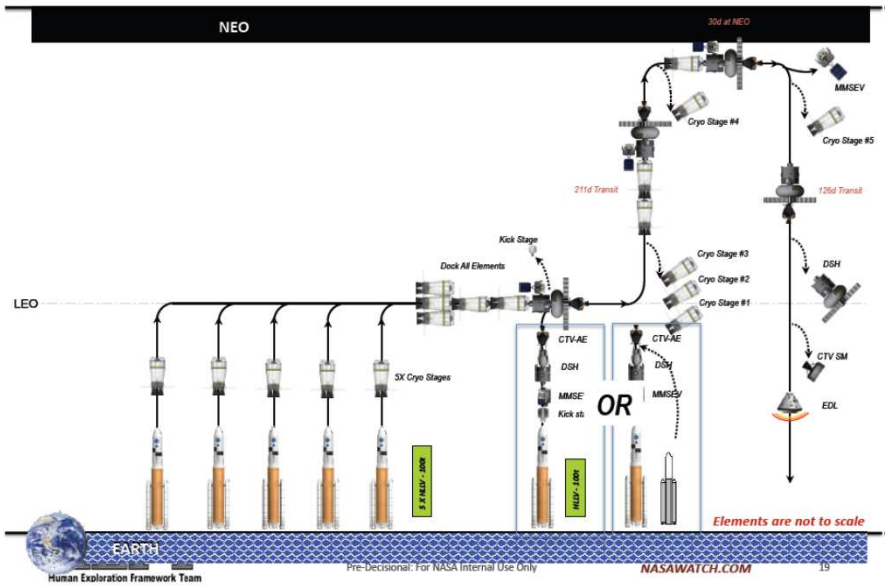
Regular network: Full single fault tolerance and tolerant to a 2nd communication outage.

Fail-silent: Full dual fault tolerance (except identical Byzantine failure).

Requirement:
Easy “System of Systems” Fusion

Ensuring Reliable Networks TTTech





SoS architecture with TTEthernet supports reconfiguration

Several separate vehicles or elements fuse into a new combined network configuration

Spin-in of Existing (Communication) Technologies

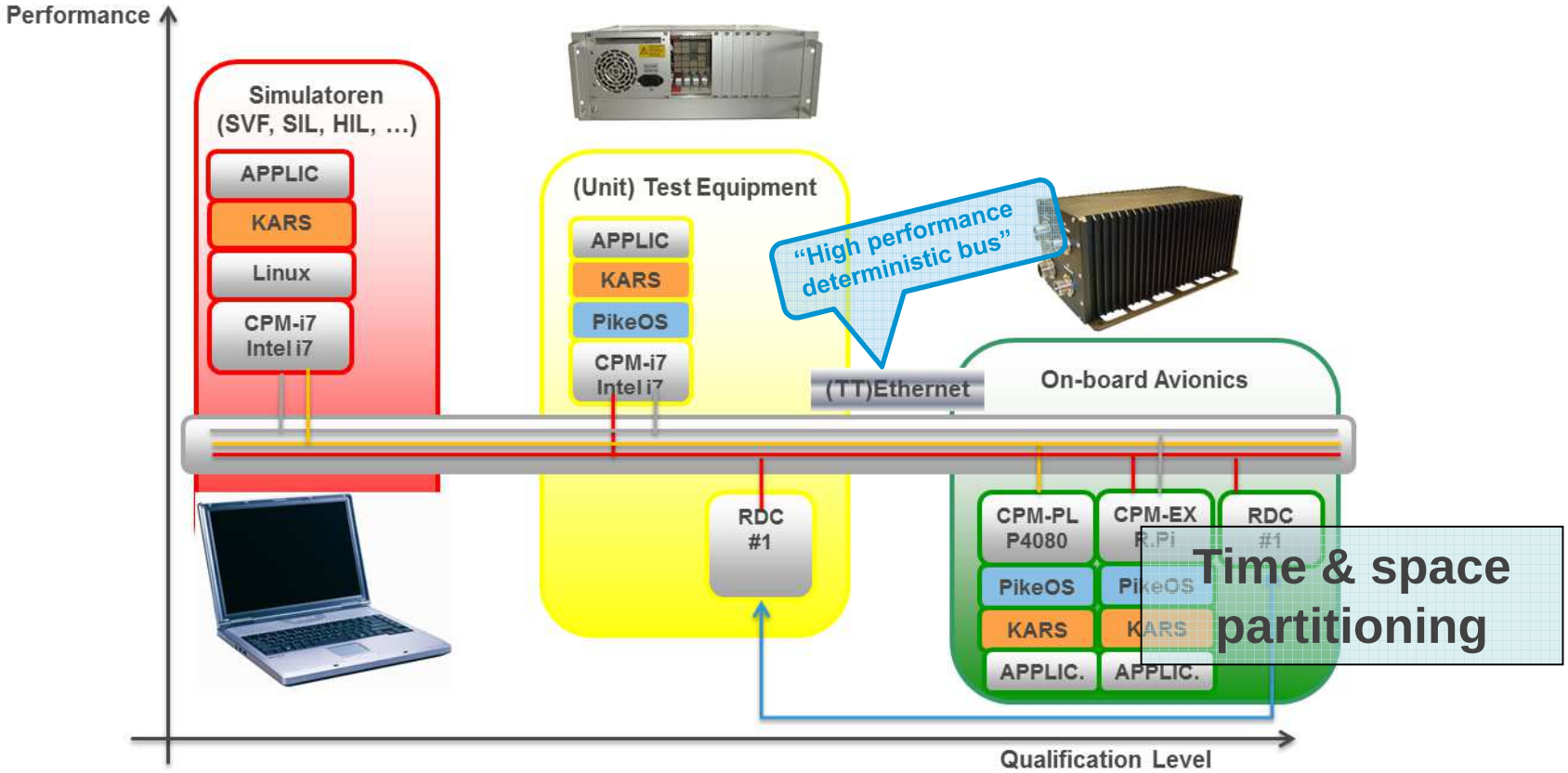
Ensuring Reliable Networks TTTech

- Space industry needs to focus on space specifics = environmental challenges
- Due to market size and development risks:
  Space cannot afford any longer own CPU cores and data handling protocols
- Need for “spin-in”
- Works successfully – example CAN
- A very large user base ensures that a technology is well tested and supported with software as well as tools
- Now: Ethernet
- Flavors of **deterministic Ethernet**:
  EtherCAT, TTEthernet, TSN…

Federated Architectures / DIMA

Ensuring Reliable Networks TTTech

OMAC4S - One Concept – Different Applications



OMAC4S Open Modular Architecture for Space · DLR · ASTRIUM AN EADS COMPANY · Fraunhofer FOKUS · SYSGO EMBEDDING INNOVATIONS · TTTech Ensuring Reliable Networks

Scalable, Modular Platforms

- Scalable hardware designs (performance / qualification)
- Robust network – bandwidth as needed, separation of traffic classes, timing guarantees (latency/jitter), FDIR
- Standardized interfaces (legacy interfaces to be included)
- Re-use of software (building) blocks through middleware
- But: Development budgets outside programs limited (Autosar-like funding can only be dreamed of)

Resulting savings:

- Over life-time greatly reduced software efforts
- Faster integration and testing

Current European R&D

- ESA TRP on building blocks for reliable high-speed communication bus/network
- DLR OBC-SA (“OMAC4S” initiative)
- Austrian ASAP 10 - “Safesat” project
- Several CNES/Onera studies
- ESA Avionique-XE (completed in 10/2015)
- ESA FLPP-3 and Ariane 6
- ESTEC “iSAFT PVS with Time-Triggered Ethernet capabilities”
- ESA TRP on Ethernet PHY transceiver characterization
- European space-graded Ethernet transceiver development – SEPHY, funded by EU Horizon 2020 (www.sephy.eu)
- Starting soon: ESA GSTP “validation testbed”

Airbus DS and TTTech in FLPP-3

Ensuring Reliable Networks TTTech

- Continuation from earlier FLPP activities
- Airbus DS Bremen with TTTech in sub-project “TTEthernet Switch Maturation”
- Development of FPGA-based breadboard and TTEthernet switch ASIC up to tape-out
- Duration: August 2014 – September 2016
- Regarded as preparation for Ariane 6
- PDR successfully passed
  - CDR end of November 2015

Time-Trigged Ethernet for Space: TTE-Switch Controller Design

Ensuring Reliable Networks TTTech

❶ Switch Controller COM

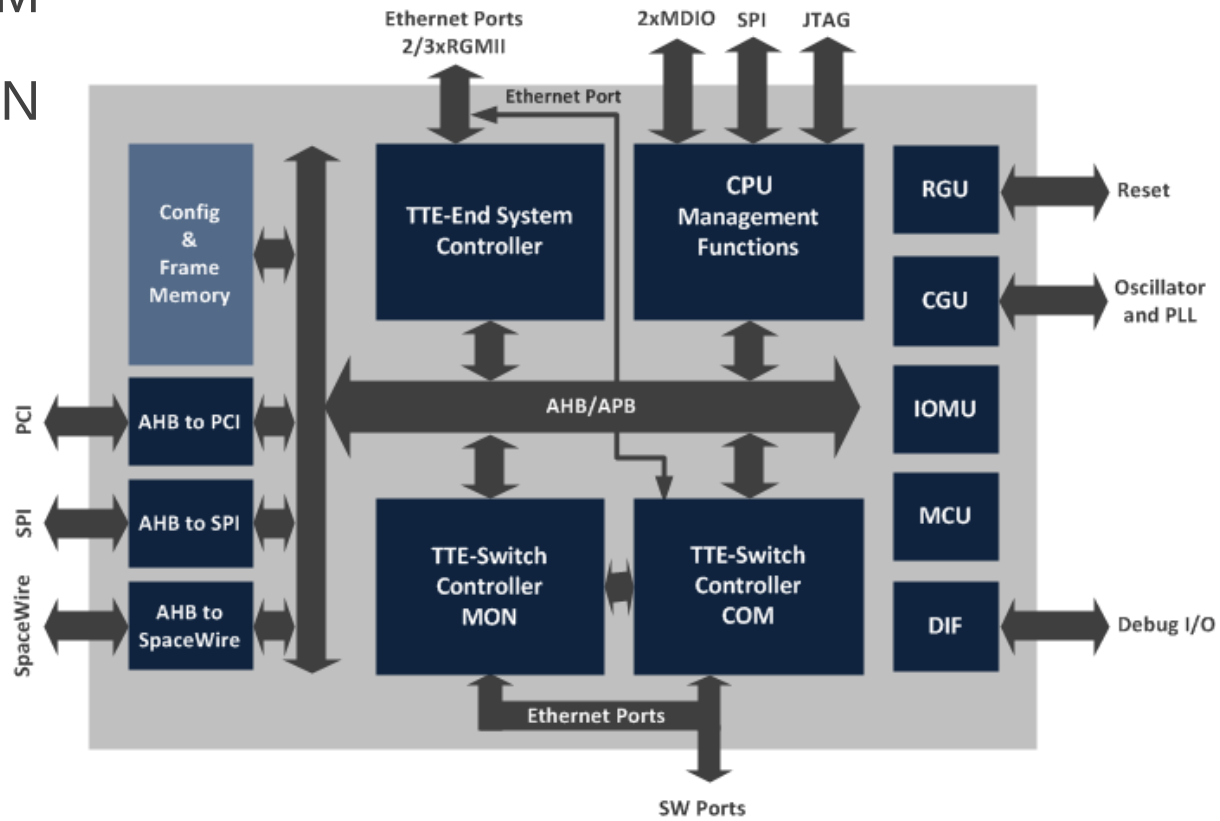
❷ Switch Controller MON

❸ End System

- For the connection of the host to the switch controller

❹ CPU (Leon2FT)

- Management
- Diagnostics



TTEthernet's Coverage

CIF: Harness Reduction Workshop

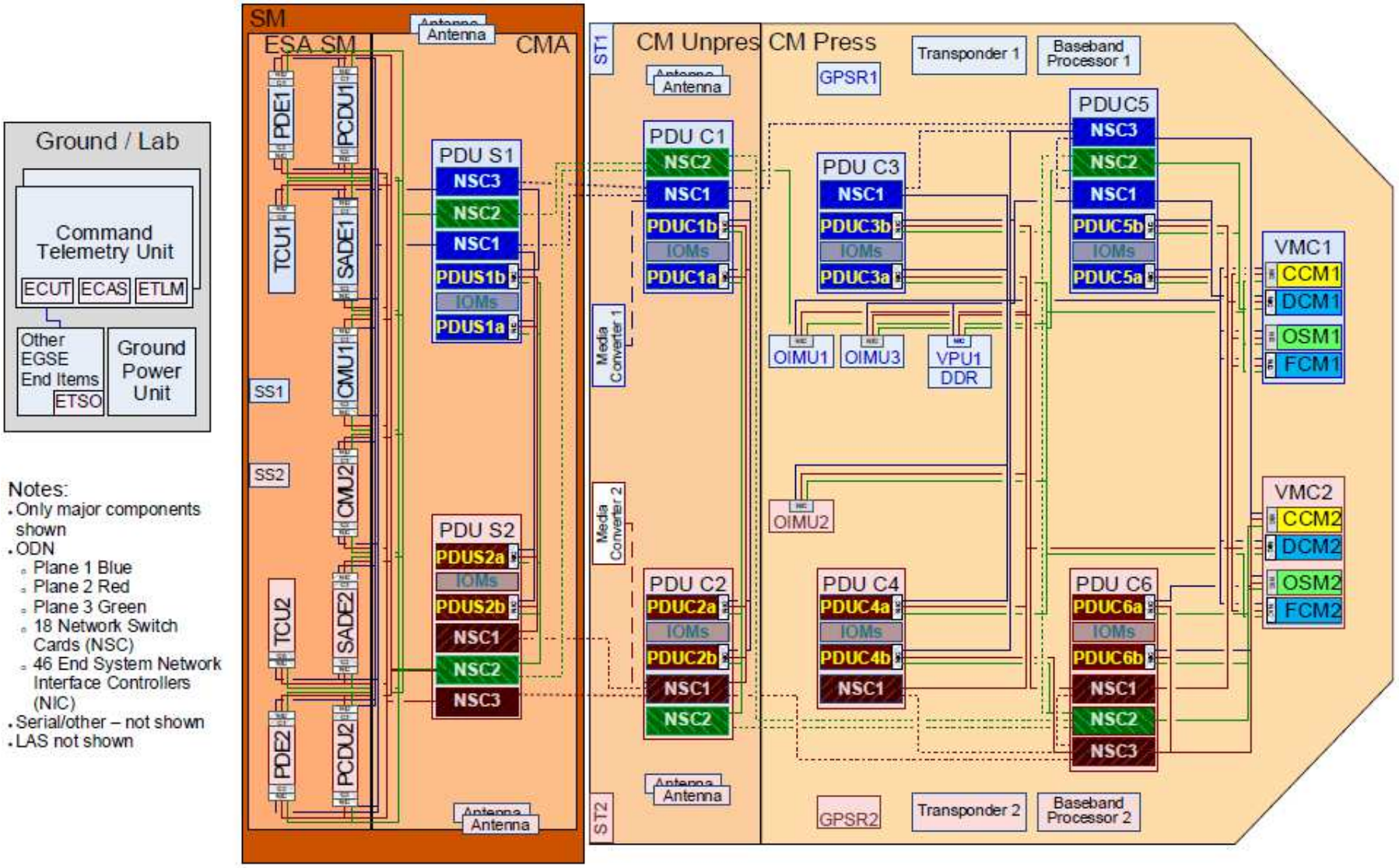
Jet Propulsion Laboratory Div. 34

- Real World Interconnect "Care-abouts" — Priority
  - **Must be serial** — **(0)**
  - Must have commercial COTS test equipment — (1)
  - Redundancy considerations built in — (2)
  - Must have programmatic legs — (3)
    - User base outside of JPL
  - Must have technical legs — (4)
    - Higher data rates possible
    - Fiber optic implementation possible
  - Must be dc isolated — (5)
  - Must be self-clocking protocol — (6)
  - **Must be 100 mbps or better** — **(7) → 100 times faster**
  - 20 meter length — (8)
  - Must support separation interfaces — (9)
  - Time Distribution Support — (10)
- Buses that failed these top criteria were deemed "Not Worthy"

August 11th, 2013
JAD - 13
Europa System Bus Trade

TTEthernet Usage Example 1
MPCV

Ensuring Reliable Networks TTTech



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

TTEthernet Usage Example 2
Launcher

Ensuring Reliable Networks TTTech

Main considerations:

- Simplification: Single network for control and telemetry
- Determinism: Scheduling guarantees and resource reservation for flight communication
- Scalability: Dramatic bandwidth increase, potential for future additions (e.g. cameras)
- Modularity: Allows for different states and configurations
- Connectivity: To ground segment via standard Ethernet

Current focus:

- Standardization of interfaces
  (TTE-controller, PHY, connectors, download tool)

Conclusions

Ensuring Reliable Networks TTTech

- TTEthernet as scalable and modular network
  - Simple to high reliable/available architectures
  - Low speed (10 Mbps) to high speed (10 Gbps in near future)
  - Based on open standards
- Offers single and dual fault-tolerance
- Built-in fault-tolerant network synchronization
- Robustly partitioned network ideal for future DIMA, already running with VxWorks, PikeOS, Xtratum
- Favored by the world's largest space agencies and industrial players
- Now working on Time-Triggered Ethernet sensor bus to further reduce network complexity and simplify wire harness
- European chip development ongoing (TRL 6 in 2016)

Meet us in room Einstein for further discussions!

TTTech

Ensuring Reliable Networks

www.tttech.com