Time-Triggered (Gigabit) Ethernet

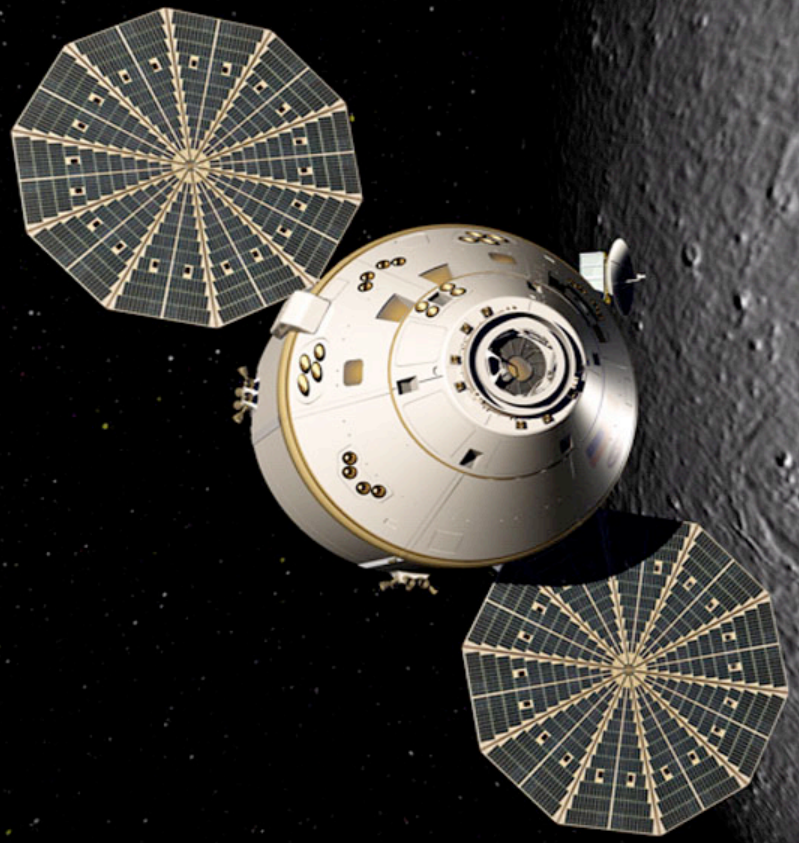
Dr. Michael Paulitsch

Important

- Work carried out while at Honeywell
- Information based on publicly available knowledge
- Design credit goes to Honeywell and TTTech (partners in design)

Orion

- Human-rated spacecraft
- Entry into service: 2015
- Challenges:
  - Weight: integrated architecture for weight reduction
  - Extremely long mission times in harsh environment without repair



Crew+Launch Vehicles

Why TT-GbE / TTEthernet?

- Ethernet is everywhere
  - Knowledge, tools, test equipment existing
- TTEthernet provides up to dual fault tolerance with only F+1 components (switch or end systems) at a minimum
  - Critical components are dual (COM/MON)
  - Leveraging COM/MON design to optimize system size, weight, and power
  - Inline integrity can be weak for components (e.g. CRC coverage; timing faults)
- Network Time and Space Partitioning
  - No interference between data flows from different end systems
  - No masquerading
  - Guaranteed bandwidth / time slots
- Relation of TT-GbE and TTEthernet
  - TT-GbE = special implementation of TTEthernet
  - Special physical layer designed for space (financed by U.S. government)
  - Radiation hardened silicon – HX5000 Honeywell 150nm process
- Advantage over ARINC664 (AFDX) in this architecture
  - Decreased need for expensive memory
  - Support of distributed time base for application purposes

TTEthernet Research Challenges

- Support of high-integrity design (self-checking)
- Synchronization algorithm
  - System “converges” from any possible state under fault hypothesis → robustness
  - Failure mode example: Despite high-integrity design, any combination of synchronization frames could be lost
  - Algorithm works despite not needing one round of consistency (current similar approaches like ROBUS need round of consistent RX of frames)
- Integration of time-triggered, rate-constraint, and “COTS”:Ethernet frames

TT-GbE Ethernet Features - I

- TT-GbE is a scaleable highly deterministic fault-tolerant Ethernet
- TT-GbE extends Ethernet, supporting 3 classes of traffic
  - Best-effort (BE) (standard COTS traffic)
    - No fault tolerance, delivery not guaranteed
  - Fault-Tolerant Rate-Constrained (RC) – AFDX compatible
    - Asynchronous, rate-limited messages
    - Controlled through bandwidth allocation and flow management
    - Statistical upper bound on latency (no lower bound enforcement)
  - Fault-Tolerant Slot-Based (SB) (TT traffic)
    - Control messages and time-triggered data messages
    - Managed via schedule enforcement
    - Near zero jitter
- TT-GbE incorporates services and enforcement strategies to enable all three traffic classes to coexist and interoperate on shared network infrastructure
- Aspects of security for embedded systems addressed

TT-GbE Ethernet Features - II

- TT-GbE provides additional services and mechanisms to support fault-tolerant systems deployment including:
  - A Clock Synchronization Service
    - Supporting multiple synchronization domains
  - A Startup and Integration Service
    - Ensuring rapid clique detection and recovery
  - Configurable Traffic Redundancy Management Service
    - For SB and RC traffic
  - Traffic Protection and Enforcement
    - Via integrated “Guardian” functionality in switches
- A TT system allows a large reduction in the system resources (bandwidth, memory, CPU time, etc) usually needed in asynchronous systems to handle peak demands!
- TT-GbE is intended to be a modular IP Library enabling the easy selection and instantiation of the different traffic classes and support services

Conclusions and Status

- New approach for integrating time-triggered, rate-constraint and COTS traffic classes created
- High-integrity mechanisms verified
- Extensive use of formal methods increased in-depth understanding of algorithms (combinatorial explosion)
- High performance components designed
- Established integration laboratory with high controllability and observability
- Standardization under SAE started