TSN Time Synchronization NASA’s Use Cases and Needs

Presented by Rob Donnelly
<robert.donnelly@jpl.nasa.gov>

For IEEE P802.1DP / SAE AS6675 Ad Hoc

May 24-26, 2022

Jet Propulsion Laboratory
California Institute of Technology

Introduction

Overview

- Robotic Exploration
  - Orbiters and flybys
  - Landers
  - Rovers and helicopters
- Human Exploration and Operations
  - International Space Station
  - Orion
  - Gateway

Challenges

- SWaP-C (Size, Weight, Power, Cost)
- Temperature
- Radiation (SEU, TID)
- Fault tolerance

Today

Satellite On-board Network Use Case

By Franck Wartel (Airbus)

https://www.ieee802.org/1/files/public/docs2021/dp-wartel-satellite-onboard-network-use-case-0526-v01.pdf

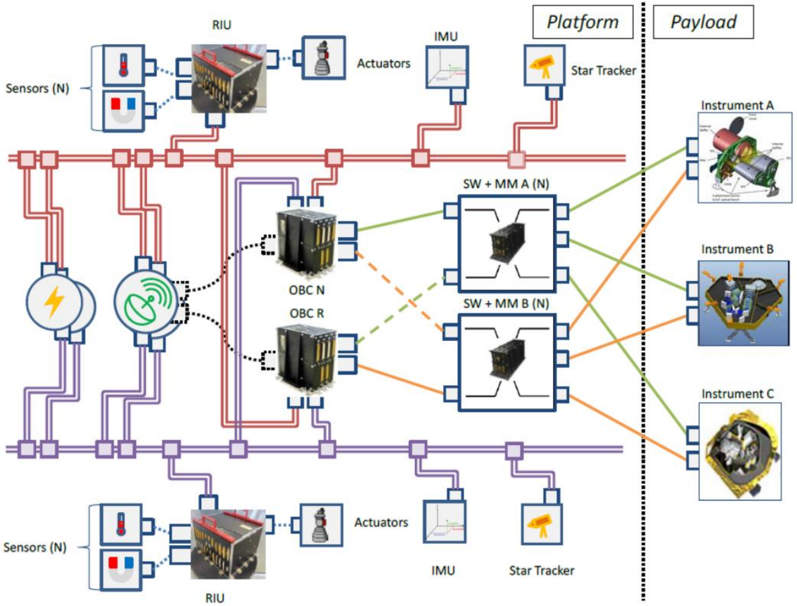
- A prior contribution to IEEE P802.1DP / SAE AS6675
- Legacy Networks slide is representative of NASA's robotic (non-human) use cases

DEFENCE AND SPACE

Legacy Networks

This is representative of NASA's robotic (non-human) use cases

	Platform	Payload
MIL-STD-1553 1 Mbps	Command and Control Time synchronisation	Command and Control Time synchronisation
Spacewire 100 Mbps	Data transfer	Data transfer
Dedicated high bw datalink > 1 Gbps	N/A	Data transfer
dedicate discrete wire 1Hz, 8Hz	synchronization	synchronization



From: https://www.ieee802.org/1/files/public/docs2021/dp-wartel-satellite-onboard-network-use-case-0526-v01.pdf

5 May 26th, 2021 Satellite On-board Network Use Case AIRBUS

Tomorrow

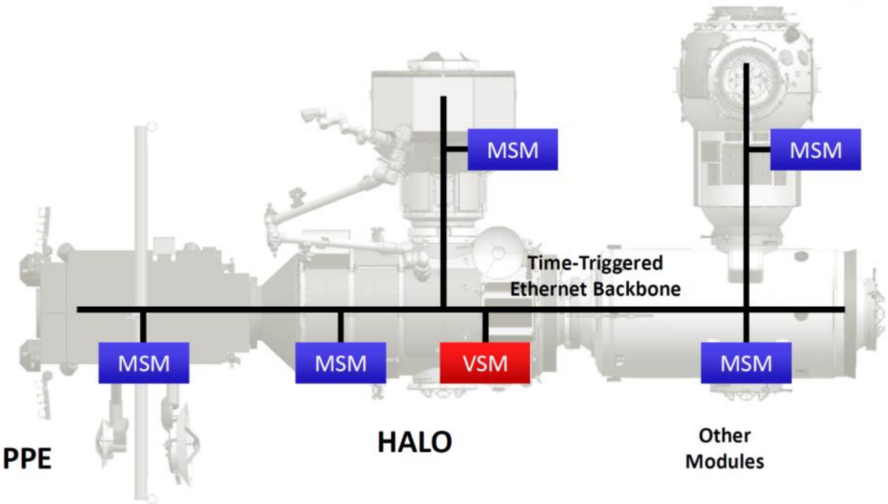
On Time-Triggered Ethernet in NASA's Lunar Gateway

By Andrew Loveless (NASA-JSC)

https://ntrs.nasa.gov/citations/20205005104

Tomorrow

Lunar Gateway



- Multiple modules
- Modules operate separately then come together and join network seamlessly
- Visiting vehicles can join and leave the network seamlessly

MSM = Module System Manager; VSM = Vehicle System Manager
PPE = Power and Propulsion Element; HALO = Habitation and Logistics Outpost

Beyond Tomorrow

TSN

Open Standards

Growing Ecosystem

Time Synchronization Needs

Time Synchronization

Preface

- Relative time synchronization
  - Used for network communications
- Verses synchronization to a reference
  - Used for e.g. guidance, navigation, and control
- The following slides are concerned with relative time sync for network comms

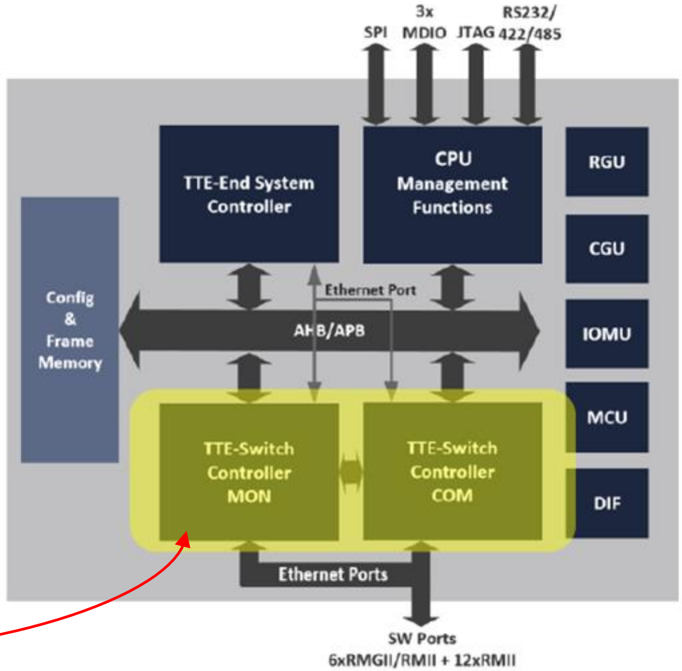
Fault Tolerance

- Bit flips can and will happen
- Level of tolerance must be sufficient for worst-case time and safety critical uses cases (e.g. human landing systems)

Fault Tolerance

Tolerate non-benign failure modes of network components

- End systems => arbitrary failures
  - Note: Includes timing failures. Drives the need for fault-tolerant averaging rather than a single trusted high-priority master
- Switches => asymmetric omissive failures
  - Note: This is normally justified through use of a high-integrity switch design (e.g., COM/MON self-checking processors).



Fault Tolerance

Tolerate multiple device failures

At least one simultaneous worst-case failure of an end system and switch.

Fault Tolerance

Transparent and bounded-time failure recovery

- Ideally the network should tolerate the failure of any network component, per the fault hypothesis on previous slides, without any non-faulty devices transitioning out of a stable synchronized state.
- If not possible, then there must be an a priori known bounded time between each worst case failure, and the time at which all non-faulty devices are known to be in a stable synchronized state (< 5-10 ms).

Formal Correctness Guarantees

- Should have formal proofs of correctness for key properties (e.g., self-stabilization) and subprotocols, such as
  - Coldstart
  - Integration
  - Clique detection
- Or have a clear path by which formal verification is possible

Multiple Synchronization Domains

- Two independent synchronized networks must be able to operate independently
  - Then seamlessly join to operate together (one timebase)
  - And seamlessly separate

Software Participants

- There is a desire for low-cost non-critical devices to be able to synchronize to the time base without using specialized hardware (i.e. non-TSN NIC)
- The protocol must be straightforward and lightweight enough to enable a possible software implementation for devices with relatively loose timing requirements

Bounded Traversal Time

- Must be possible to use network calculus or other means to calculate worst case traversal times for sync messages
- This is used to enable verification of time sync requirements (e.g., must reach a sync state in XX ms) by analysis instead of by test

Compatible with Heterogenous Networks

- The sync protocol needs to work in a network with different link speeds (e.g., 100M, 1G, 10G, 40G)
- And potentially different physical layers (e.g., copper, fiber).

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov