Satellite On-board Network Use Case

IEEE P802.1DP/SAE AS6675

DEFENCE AND SPACE

Presented by Franck Wartel (franck.wartel@airbus.com)
May 26th, 2021
Export control Information

This document contains EU or and Export Controlled technology (data):

☐ YES  ☑ NO

If YES:

1/ European / French regulation controlled content

☐ Technology contained in this document is controlled by the European Union in accordance with dual-use regulation 428/2009 under Export Control Classification Number [xExx]. (1)

☐ Technology contained in this document is controlled by Export Control regulations of French Munitions List under Export Control Classification Number [MLXX or AMAXX]. (1)

2/ US regulation controlled content

☐ Technology contained in this document is controlled under Export Control Classification Number [xExxx] by the U.S. Department of Commerce - Export Administration Regulations (EAR). (1)

☐ Technology contained in this document is controlled by the U.S. Department of State - Directorate of Defense Trade Controls - International Traffic in Arms Regulations (ITAR). (1)

(1) See applicable export control license/authorization/exception in Delivery Dispatch Note. Dissemination is only allowed to legal or natural persons with right to know who are covered by an appropriate export license/authorization/exception.
Before We Start

• **DISCLAIMER**: This presentation should be considered as the personal views of the presenter not as a formal position of AIRBUS DEFENCE AND SPACE

• **CREDITS**: The presentation is exploiting results from ADS internal and ESA/CNES co-funded activities and especially materials from EDEN project currently on-going @ IRT Saint-Exupéry

Spacecraft System

• **Payload - High Performance Domain**
  – Repeaters/Transponders for Telecom satellite
  – Instruments for Scientific Missions
  – Optical Payloads and image processing for Earth Observation

⇒ *high data rates / soft real time*

• **Platform - Time Critical Domain**
  – Attitude Control
  – Power Supply
  – Monitoring and Control of Payload
  – Telecommunication with ground

⇒ *low data rates / hard real time*
## Legacy Networks

<table>
<thead>
<tr>
<th>Platform</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL-STD-1553 1 Mbps</td>
<td>Command and Control</td>
</tr>
<tr>
<td></td>
<td>Time synchronisation</td>
</tr>
<tr>
<td>Spacewire 100 Mbps</td>
<td>Data transfer</td>
</tr>
<tr>
<td>Dedicated high bw datalink &gt; 1</td>
<td>Data transfer</td>
</tr>
<tr>
<td>Gbps</td>
<td>N/A</td>
</tr>
<tr>
<td>dedicate discrete wire 1Hz, 8Hz</td>
<td>Synchronization</td>
</tr>
</tbody>
</table>
Forecasted Representative Topology

RIU A, PCDU A, Power Conditioning and Distribution Unit

RIU B, PCDU B

OBC A, On Board Computer

OBC B

STR A, Star Tracker (attitude estimation)

STR B

PF A, PF: platform 100Mbps/1Gbps

PL A, PL: payload 1Gbps

PF B

INST 1, INSTR: Instrument. Camera, telescope...

INST 2

NAVCAM, Navigation Camera (Vision Based Navigation)

SSMM, Solid State Mass Memory (Payload data storage)
Topology Rationale

• OBC is central, it manages all the network nodes
  – non-intelligent end stations are triggered by incoming commands, including for messages generation (RIU) in a master/slave paradigm where OBC acts as the master
  – intelligent end stations have some autonomy with processing capabilities and are able to generate frames on their own (STR, NAVCAM, GNSS, INST, SSMM)

• Platform and Payload flows are duplicated and follow disjoint paths (excepted RIU, PCDU for use case simplification purpose) to make the system tolerant to
  – loss of a frame,
  – failure of a link,
  – failure of a switch,
  – failure of an end station network interface.

• All the PLAFTORM end stations are duplicated (A/B) to have redundancy for failure tolerance purpose. They are usually in cold redundancy

• PLATFORM OBCs are in cold redundancy

• Switches are in hot redundancy, nominally always ON
The GNC (Guidance, Navigation and Control) or AOCS (Attitude and Orbit Control System) is the part of the OBC software that is responsible for the satellite flight management. This software processing is executed cyclically with sensors acquisitions done at the start of the cycle, in order to produce actuator commands that must be received before the end of the cycle.
Ultra Low (1µs) & Low (500µs) Jitter definition

- **Network**
  - Sensors acquisition
  - AOCS algorithms
  - CPU
- **OBC**
- **RIU**

**AOCS inputs**

**Deadline acquisitions**

**Deadline OBC CPU**

**Deadline commanding**

8Hz

**31,25 ms**

**62,5 ms**

**31,25 ms**

**1µs**

reception date w.r.t start of cycle, with jitter <1µs
In addition to providing the PVT acquisition to the OBC, the GNSS offers a synchronization service to the network. Failure and reconfiguration to the redundant GNSS would lead to a synchronization loss. Indeed, GNSS takes one minute (order of magnitude) after switch-on to be able to provide the synchronization service.

To ensure the continuity of the network synchronization, the following solution is proposed: the OBC is the only slave of GNSS, the OBC is master for the rest of the network.
<table>
<thead>
<tr>
<th>Traffic Classes</th>
<th>Description</th>
<th>Period</th>
<th>Application Synchronized to Network</th>
<th>Data Delivery Guarantee Mode</th>
<th>Delivery Guarantee Value</th>
<th>Tolerable Jitter Value</th>
<th>Application payload size variability</th>
<th>Payload (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C&amp;C ultra low jitter</td>
<td>high frequency (8 Hz), time window, ultra low jitter</td>
<td>62.5 - 125ms</td>
<td>Yes</td>
<td>Deadline</td>
<td>Same period</td>
<td>1µs</td>
<td>Fixed</td>
<td>64</td>
</tr>
<tr>
<td>C&amp;C low jitter</td>
<td>high frequency (8 Hz), time window, low jitter</td>
<td>62.5 - 125ms</td>
<td>Yes</td>
<td>Deadline</td>
<td>Same period</td>
<td>500µs</td>
<td>Fixed</td>
<td>64</td>
</tr>
<tr>
<td>C&amp;C Time window</td>
<td>high frequency (8 Hz), time window</td>
<td>62.5 - 125ms</td>
<td>Yes</td>
<td>Deadline</td>
<td>Same period</td>
<td>N/A</td>
<td>Fixed</td>
<td>64</td>
</tr>
<tr>
<td>Acquisition list</td>
<td>time window, bounded delay between messages delivery</td>
<td>62.5 - 125ms</td>
<td>Yes</td>
<td>Deadline</td>
<td>Same period</td>
<td>N/A</td>
<td>Fixed</td>
<td>64-1100</td>
</tr>
<tr>
<td>Acquisition</td>
<td>deadline to the message delivery: end of cycle or before end of cycle</td>
<td>62.5ms-1s</td>
<td>Yes</td>
<td>Deadline</td>
<td>Same or different period</td>
<td>N/A</td>
<td>Fixed</td>
<td>64</td>
</tr>
<tr>
<td>MEO</td>
<td>min delay between messages delivery</td>
<td>62.5 - 125ms</td>
<td>Yes</td>
<td>Deadline</td>
<td>Same period</td>
<td>N/A</td>
<td>Fixed</td>
<td>64</td>
</tr>
<tr>
<td>VBN</td>
<td>high data rate, deadline to the message delivery</td>
<td>33.3ms</td>
<td>Yes</td>
<td>Deadline</td>
<td>Same period</td>
<td>N/A</td>
<td>Fixed</td>
<td>1048576</td>
</tr>
<tr>
<td>Instrument</td>
<td>high data rate</td>
<td>1ms - 3ms</td>
<td>No</td>
<td>Bandwidth</td>
<td>N/A</td>
<td>Fixed</td>
<td>4096</td>
<td></td>
</tr>
</tbody>
</table>
FDIR @ Network level

- To support management of cold/warm/hot redundancy at unit/interface level
- To prevent “babbling idiot” behavior from an instrument, causing an excessive packet rate to the Processor Module. Measures can be implemented at E/S and switch level.
- To provide to the Processor Module report of every error detected (and potentially recovered) locally at network E/S and switch level.
- To provide requirements on E/S failure groups, i.e. for terminals that are not cross-strapped to the switch, which combinations of those terminals may be reconfigured in case of a switch single-point failure affecting interface to those terminals.
- To provide failure recovery strategy at switch level.
- To provide protection against network communications against packet loss, at least for critical data.

- The detection mechanism must cover the local OBC scope up to the complete system involving remote equipments connected to this OBC. Each of these failures may be transient or permanent. It is in charge of the system to select the recovery actions.

- In case of failure the reporting mode can be either through:
  - an immediate failure status dispatch mechanism
  - a continuous monitoring based on confirmation, thresholds, and predefined metrics and statistics computation (MIBs)
FDIR Example

**In 1553**
- **Fault**
  - Babbling idiot transceiver

**In TSN**
- **Fault Detection**
  - More traffic than expected

- **Fault Isolation**
  - Switch to alternate bus and shut-down transceiver

- **Fault Recovery**
  - Reboot transceiver
  - Reboot transceiver on MIB analysis

**Expected ACK**

**More traffic than expected**

**Switch to alternate bus and shut-down transceiver**

**Drop the frames**
- Policing + Individual recovery

**Reboot transceiver**

**Reboot transceiver on MIB analysis**
Foreseen mandatory features (in line with current Synchronous Profile B)

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Name</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1AS</td>
<td>Timing and Synchronization</td>
<td>Time Distribution</td>
</tr>
<tr>
<td>IEEE 802.1Qci</td>
<td>Per-Stream Filtering and Policing</td>
<td>Policing (FDIR) + QoS management at Layer 2</td>
</tr>
<tr>
<td>IEEE 802.1CB</td>
<td>Frame Replication and Elimination (FRER)</td>
<td>Availability and FDIR</td>
</tr>
<tr>
<td>IEEE 802.1 Qbv</td>
<td>Scheduled Traffic</td>
<td>Ultra low jitter tenure</td>
</tr>
<tr>
<td>IEEE 802.1Qav</td>
<td>Credit Based Shaper</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>IEEE 802.1 Qcc</td>
<td>Time Sensitive Network Configuration</td>
<td>Static configuration part</td>
</tr>
<tr>
<td>IEEE 802.1Qbu &amp; IEEE 802.3br</td>
<td>Frame Pre-emption</td>
<td>Might be required for ultra low jitter tenure on 100 Mbps, TBC vs exclusive gating</td>
</tr>
</tbody>
</table>
Thank you!