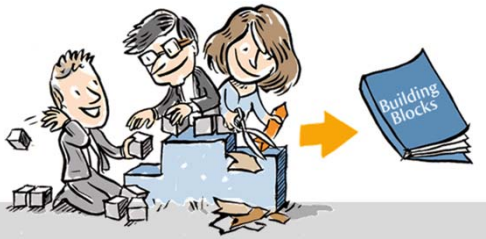
SAVOIR

space avionics open interface architecture

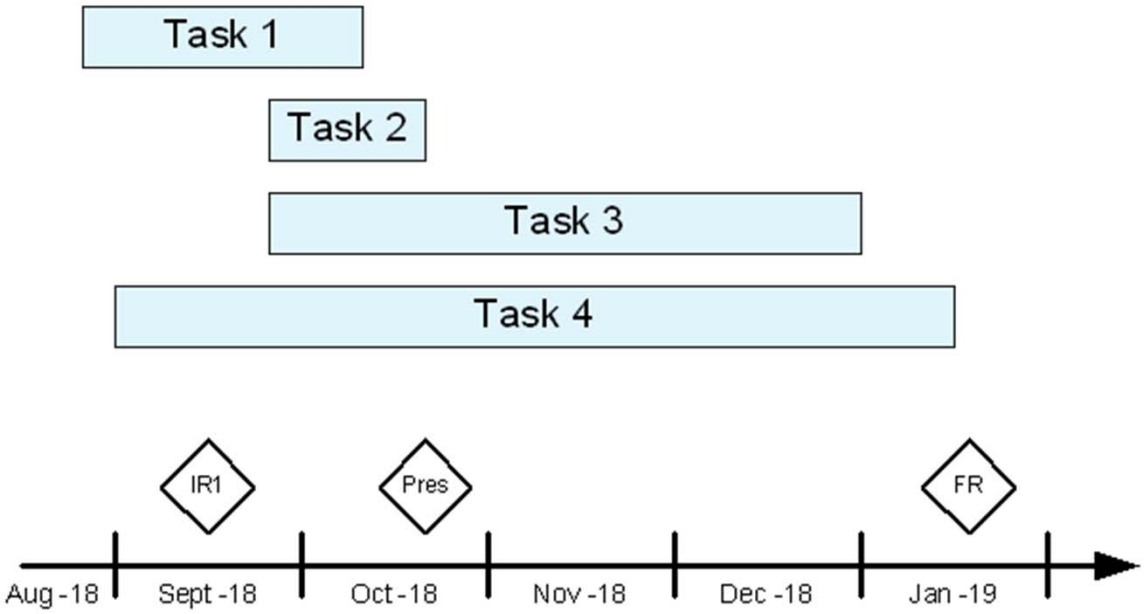
SAVOIR documentation update

Torbjörn Hult



Schedule

- Kick-off with team by telecon 4th September
- Current planning:



Task 1:
Update of TN-000 and TN-001

Task 2:
Update of OBC spec GS-001

Task 3:
Update of SAVOIR Handbook

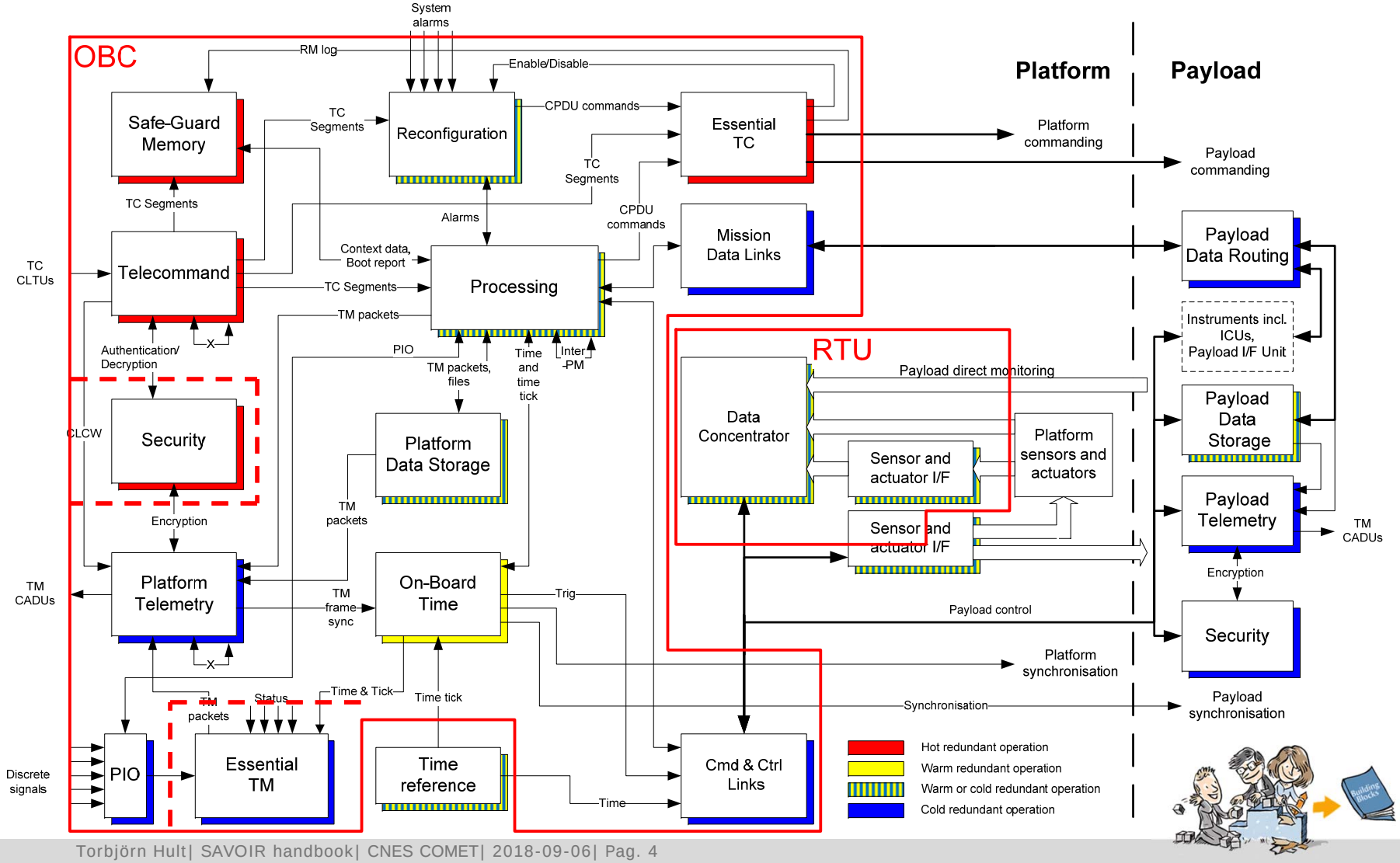
Task4:
Draft Generic SRD

Update of the reference architecture

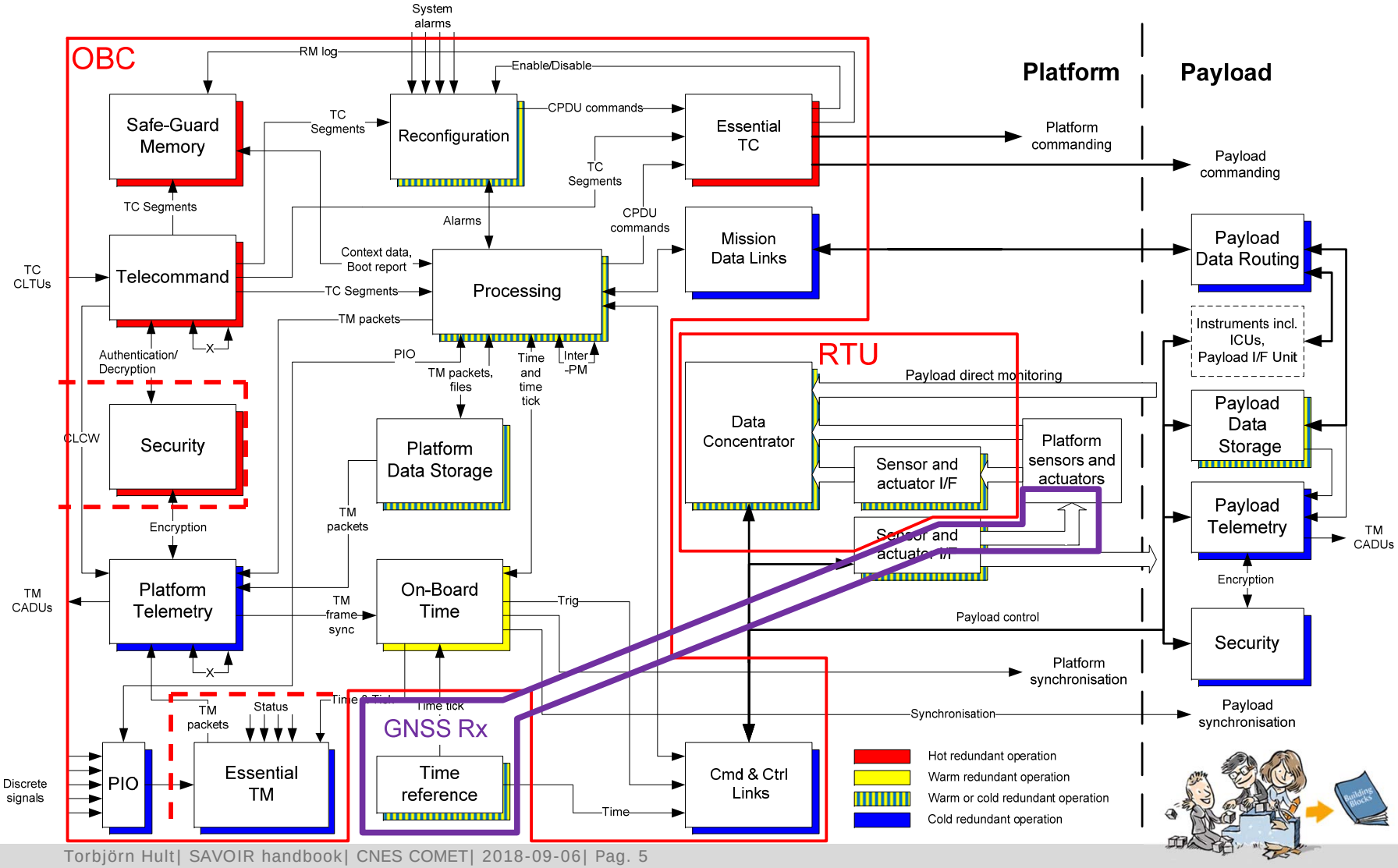
- The GNSS receiver has this far been considered as a standalone unit having two main functions:
  - Position and velocity sensor
  - Time reference
- Now it will be included as an option in the OBC

- The SAVOIR MASAIS activity has resulted in a need to update the reference architecture with more details on the Payload Data Storage and Payload Telemetry functions. There are also some discrepancies in the descriptions of the Payload Data Storage and Payload Telemetry functions that need to be corrected, including a clear definition of the links to the downlink Modulator.

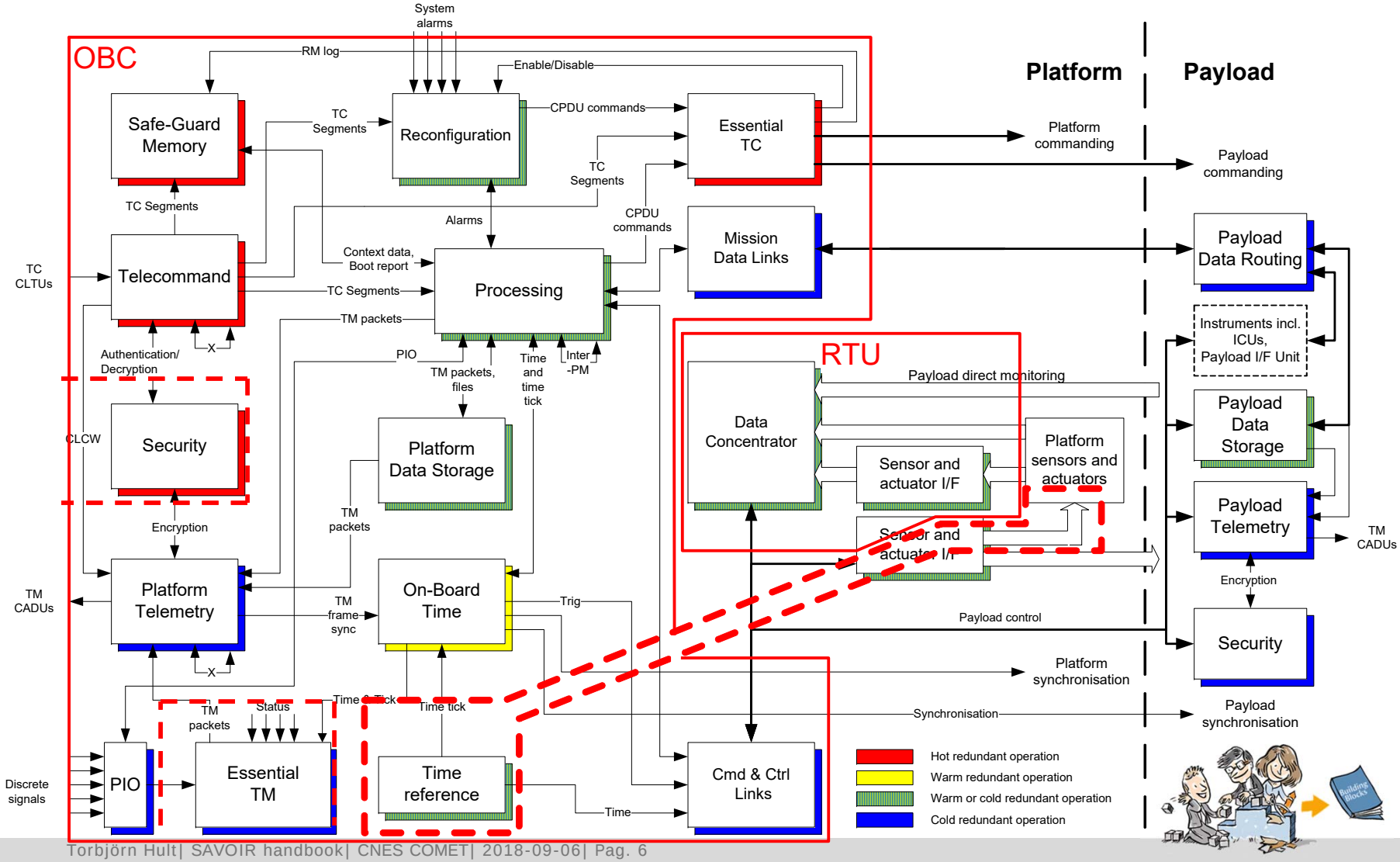
The OBC and the RTU in the SAVOIR architecture



The GNSS receiver functionality

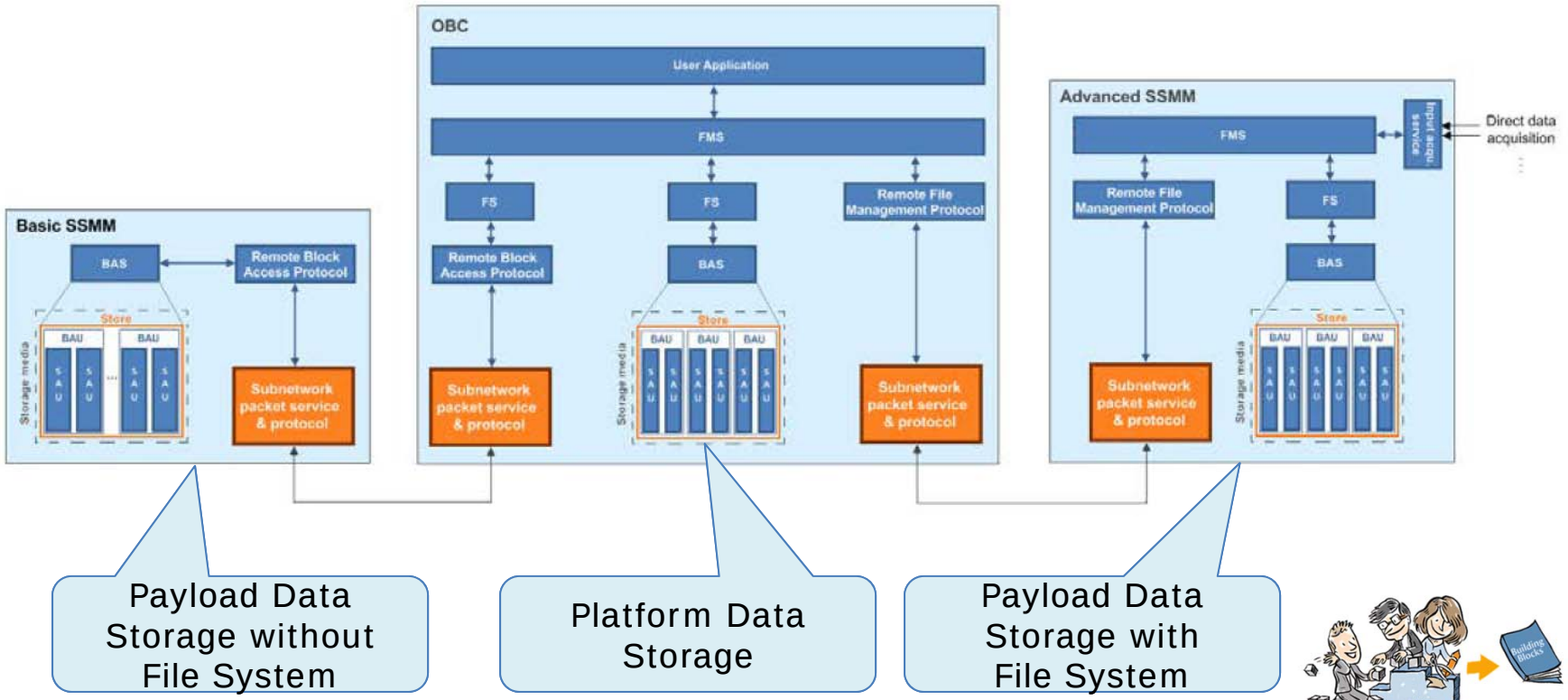


OBC with embedded GNSS receiver



Update of Data Storage functionality

- Updated with different views of where a file system can be located
  - Within the Payload Data Storage
  - Within the Central Software executing on the OBC processing function



Updated to include CFDP

- CCSDS File Delivery Protocol, CFDP, is now standard on science missions where Euclid is the first mission to adopt.
- CPDP controls the transfers and chops files using into Protocol Data Units, PDUs, that are embedded into CCSDS Space Packets
  - File Directive PDUs (Metadata, ACK, NAK, EOF, Finished, ...)
  - File Data PDUs

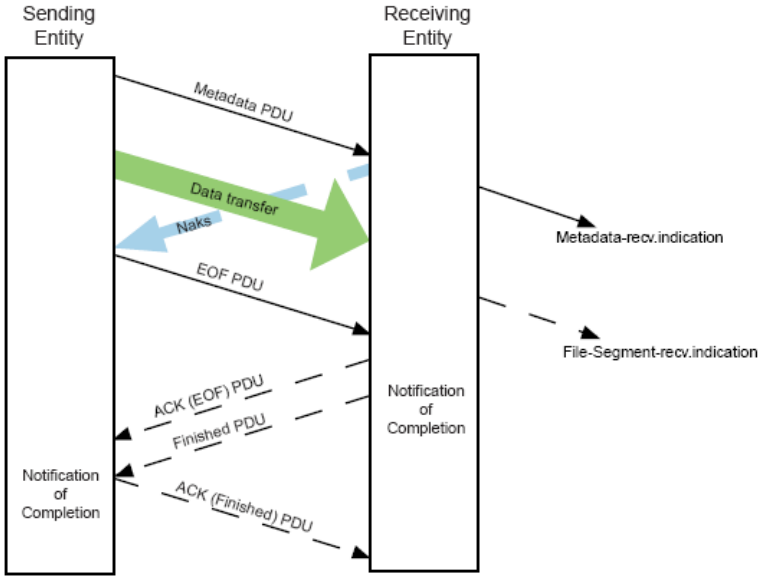


Figure 2-3: Copy Operations, Sequence of Events

- Downlink of Fila Data PDUs is typically done on a dedicated high rate Payload TM link at K or Ka band.
- Metadata (containing the file name), EOF and ACK(Finished) are typically downlinked on the Platform TM link VC0 to ensure Ground visibility of the file downlink operations in progress.

Generic SRD

- SRD variability and requirement wording is a main cost driver in many programmes as it often prevents reusing solutions and products accepted in earlier missions without time consuming negotiations.
- Typically this is due to design requirements in addition to functional requirements
- Different definitions of satellite basic operational modes and phases also plays a major role

- In Task 4 we will analyse existing ESA SRDs and propose generic avionics requirements that can be applicable on most missions

How we tackle the SRD problem

- The analysed missions should cover the widest scope of requirements e.g. there are missions (e.g. LEO) with and without security, or mission (e.g. Exploration) with and without FO behaviour
  - MTG, Euclid, PLATO, JUICE MetOp SG, Galileo,
- We focus on running projects (latest “trends” in SRD’s) where the product lines are clearly proposed and used
- First step: Capture lessons learnt by projects when reusing product lines to implement avionics related SRD requirements.
- ADCSS presentation
- Then capture the best SRD requirements from selected SRD’s
- Split the avionics in functionality and divide the functionalities among the primes to compile a proposed SRD text for the avionics.
  - Problem: SRD ToCs have no easily identified avionics boundaries

Preliminary findings when analysing SRD's

- A recurring requirement across SRD's deal with separation of resources (HW and SW) between Safe mode and Nominal modes.
  - This may lead to discussion as state-of-the-art avionics architectures are integrated and share certain critical resources between Safe and Nominal modes.
- Examples and variations
  - "The Satellite Safe Mode shall guarantee … provided by hardware or software functions not involved in the other modes of operations" => the later part has been eventually removed.
  - "Hardware and software redundancy scheme: The AOCS design of the spacecraft Safe Mode shall avoid common failure with the modes used for the nominal mission."
  - "Safe mode shall be implemented such that, as far as possible, the units and SW modes/branches that are used in Safe mode are different than those that were being used at entrance to the Safe mode."

Preliminary findings when analysing SRD's

- A non-recurring example of a required function, non mission-specific, that may be considered unusual
  - "An end-to-end DHS self-test capability shall be implemented to allow verifying the correct functioning of the DHS."
- Although not an issue by themselves, general design requirements might be questioned as they lead to extra requirements engineering effort
  - "The DHS shall be designed hierarchically." could have been skipped (no added value)
  - "Digital communication links shall be protected by transmission error protection mechanisms" goes beyond the ECSS requirement (BER) and already contained within link standards
  - "The DHS TC decoding chain shall be hot redundant." derives from higher-level requirement

Other common problems

- Quality of requirements:
  - Key qualifier as necessity, verifiability, attainability, and clarity needs sometimes to be improved
  - Subjective attributes as “easy”, “simple”, “best”, or “maximum” needs to be avoided
- Ambiguity:
  - Various terms for the same subsystems and components are used in existing SRDs
  - The term “Avionics” has been found ambiguous in several cases
- Projects specific standards made applicable since new and never used before

Contact

Feedback: savoir@esa.int

savoir.estec.esa.int