SAVOIR
space avionics open interface architecture

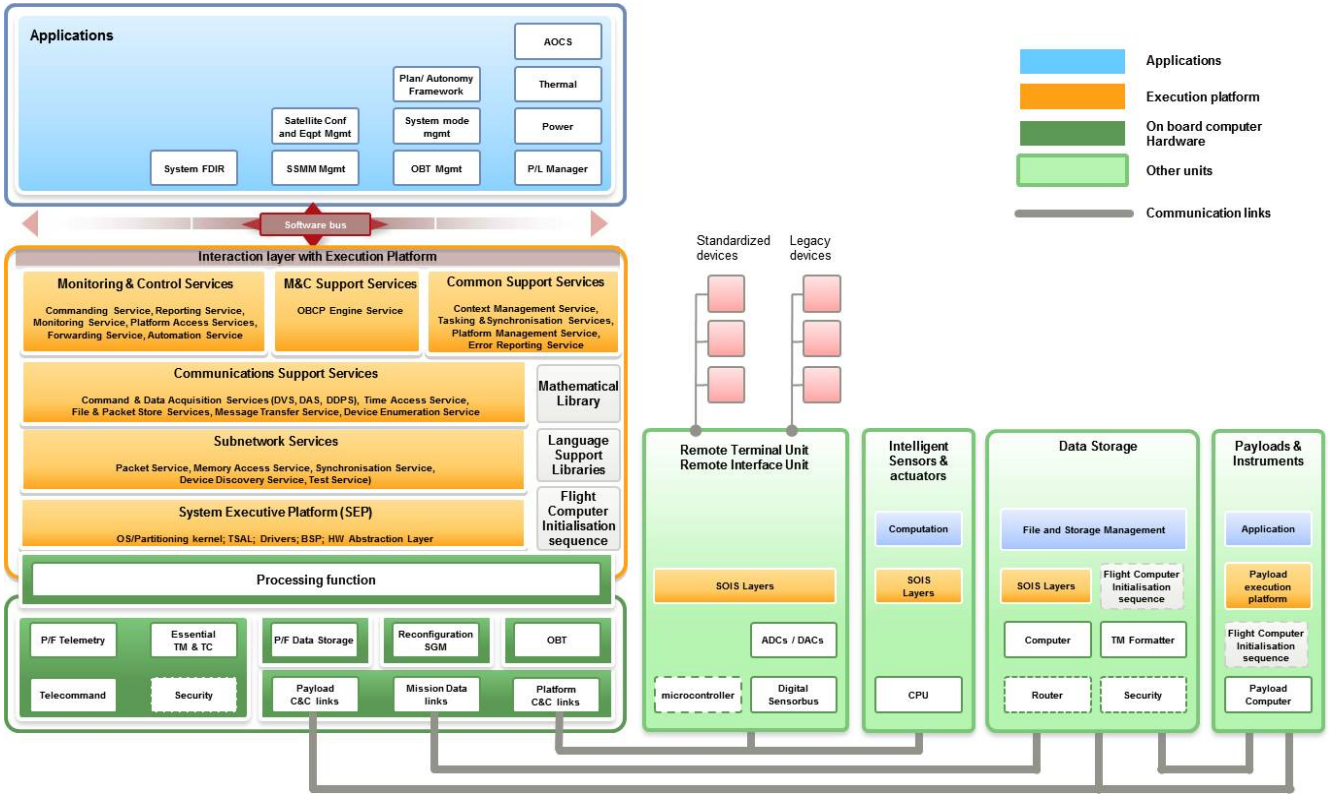
Proposed changes to the ECSS-E-ST-50-15C standard

Torbjörn Hult

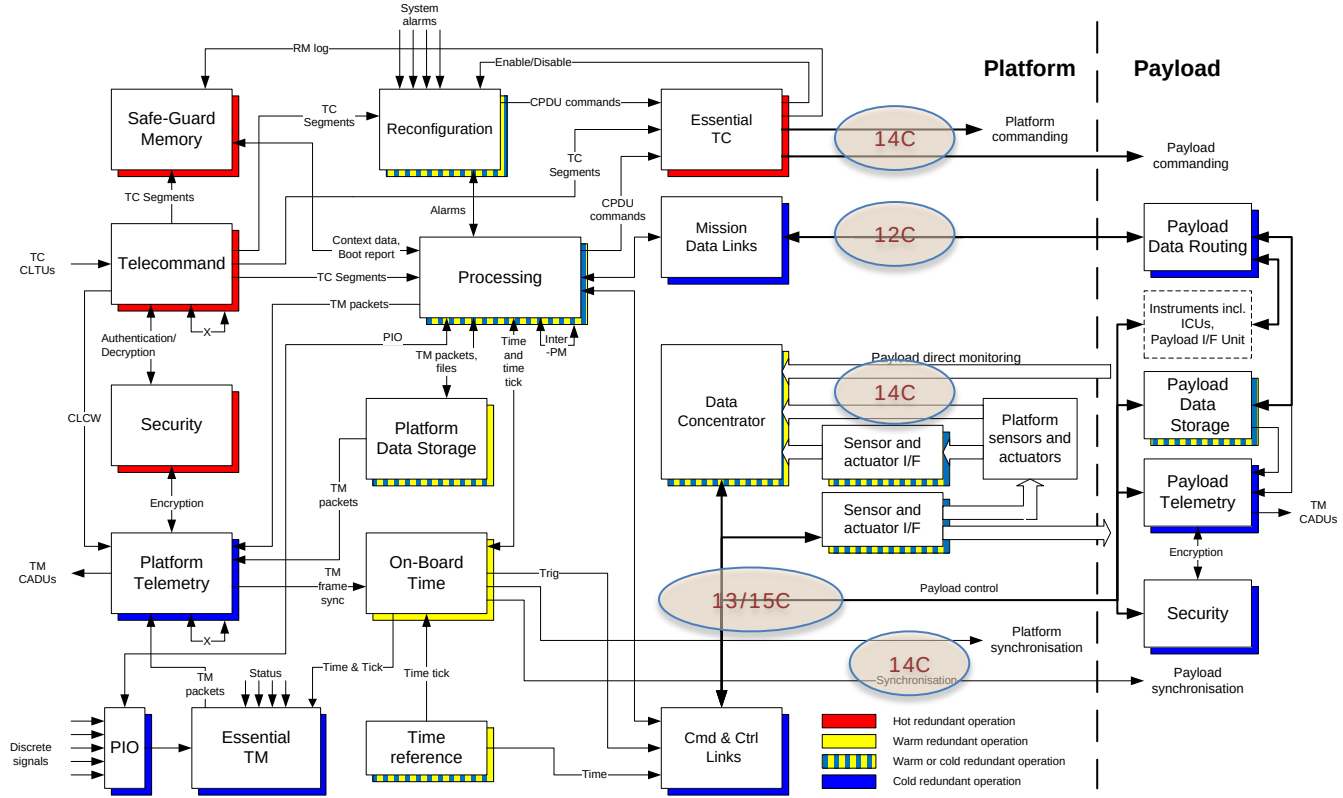
Background

- The SAVOIR initiative is aimed at standardising the functionality and interfaces of avionics for some types of spacecraft, typically satellites and deep space probes.
- Baseline interfaces are selected but the detailed requirements of the interfaces are found in other documents, typically ECSS standards.
  - 1553, SpaceWire, SpaceFibre and CAN are ECSS standards
  - UART is a SAVOIR document
- → There is a need to influence the ECSS standards in order to keep them in line with the SAVOIR needs.
- → Proposals to change ECSS-E-ST-50-15C has been generated for all layers except the CANopen application layer

The SAVOIR consolidated avionics architecture



The SAVOIR avionics functional diagram and interface standards



Proposed change: Bus redundancy

- Figures 5-1 and 5-2 in clause 5.1.1.1 defines a redundant bus as optional.
- In space applications buses are almost always redundant to avoid single-point failures.
- The proposal is to have a redundant bus being the baseline, as is done e.g. in 1553 (ECSS-E-ST-50-13C)
- This implies rewording clause 5.2.1.2 as a "may" clause to allow non-redundant bus topology as an exception. Today it starts with “If implemented, “

Proposed change:
Bus redundancy management

- The redundancy management sections (clause 8 and annex 4) mixes definitions of selective and parallel architecture
- Clause 8.2.2 (Parallel bus access architecture) refers to annex 4.2 where it is correctly stated:
  - “The detailed mechanisms for communication on the two busses are application specific and out of scope for this standard.”
- Clause 8.2.2 incorrectly refers to clause 8.3.3 for the selection mechanism
- Clause 8.2.3 (Selective bus access architecture) also states that:
  - “The details of this selection mechanism is implementation specific and out of scope for this standard.”
- The proposal is to correct these two clauses such that only clause 8.2.3 refers to Clause 8.3.3, which defines the bus monitoring and selection mechanism

Proposed change:
Simplify bus failure detection

- Quite complex bus failure detection requirements (clause 5.3.3)
  - It seems that an FMECA has turned into requirements
  - No other ECSS standard has this level of detail
  - Has any quantitative analysis of the probability of all defined failures been made?
- 11898-2:2003 clause 7.6 "Bus failure management“ specifies how to handle a non-redundant bus. As mentioned in a previous slide, buses are almost always redundant to avoid single-point failures .
- The proposal is to make clause 5.3.3.2 and its sub-clauses optional and only applicable if a non-redundant bus is selected.

Proposed change: Electrical interface

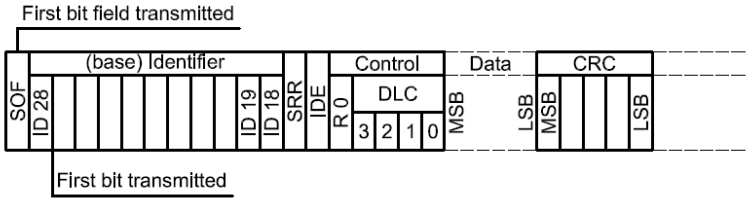
- Clause 5.3.3.1 specifies that “Transceivers shall withstand a voltage in the range between -10V and +15V on their bus pins w.r.t to chassis ground.”
- The heritage from ISO 11898-2 is that the bus can be shorted to a 12V battery voltage. No other ECSS standard requires such tolerance.
- The rationale is that “those numbers envelope possible performances from present and future ISO and RS-485 transceivers”
- The proposal is to reduce the levels to something that is in line with other ECSS standards, like -3V to +8V. This is and allows for using for instance other transceivers in the future.
    - Fault voltage tolerances are normally tightly coupled to the ground potential difference between the units connected to a link/bus

Proposed change: Clarifications

- CANopen requires little endian byte order while almost all other protocols for space (TM, TC, 1553,…) use big endian byte order
- ISO 11898-1 defines:

10.6 Order of bit transmission

A frame shall be transferred bit field by bit field, starting with its SOF field. Within a field the MSB shall be transmitted first (see Figures 10 and 11).



- The proposal is to clearly state somewhere, e.g. when it first appears in Figure 7-1. that the byte order according to CiA 301 is LS byte being sent first.

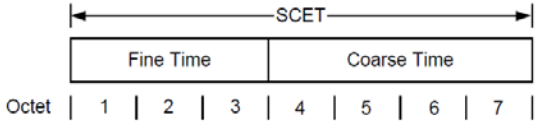


Figure 7-1: Format for objects containing the SCET

octet number	1.	2.	k.
	b_7 .. b_0	b_{15} .. b_8	b_{8k-1} .. b_{8k-8}

Figure 12: Transfer syntax for bit sequences

Proposed change:
Erroneous design requirements/suggestions

- Clause 5.3.6 contains erroneous detailed design requirements:
  - “Data Input (DI) …. shall be driven by the inverted CAN Transmit bit of the controller (TXD).”
    - In the figures in the annex DI is correctly grounded
  - “An example of a fail-safe mechanism is an input filter.”
    - An input filter does not prevent the bus from being in a permanent dominant level
  - “Receive Output (RO) shall be taken as the true value of the CAN signal”
    - “True” is not defined anywhere. RO = High → Recessive state, RO = Low→ Dominant state

Other proposed changes

- The most used combination today is to have ISO 11898-2 electrical interface and a 9-pin connector with dual buses. The latter is for some reason only allowed when the RS-485 electrical interface is used.
  - The proposal is to add a clause 10.6 with ISO 11898-2 electrical interface and a 9-pin connector with dual buses.
  - Note ECSS-E-ST-20c clause 4.2.1:

> b. Redundant functions shall be routed separately.
>
> c. Provision 4.2.1b should be met via redundant harness and physically separated connectors.

- Clause 5.3.4 can be interpreted such that an isolated transceiver is necessary everywhere.
  - The proposal is to clearly state that isolation is an option for EGSE only, i.e. delete requirement 5.3.4a, or for limited applications

An additional personal reflection

- Is CANopen really the solution we need for space?
  - Several projects seem to prefer simple master/slave type protocols.
  - Limited number of PDOs: 512. This is just the number of thermistors in a large satellite
  - Fast reaction times to some messages puts stringent requirements on software response time

Contact

Feedback: savoir@esa.int

savoir.estec.esa.int