An Example of Generic Spec (OBC initialisation)

F. Torelli, TEC-SWS
ACDSS 2010 - GeSOR Session
03/11/2010

Outline

1. Definition of OBC Initialisation Sequence
2. Why do we need a Generic Specification for OBC Initialisation Sequence
3. Definition process of the Generic Specification
4. Context and main requirements
5. Conclusions and way forward

Definition of OBC Initialisation Sequence

Definition of OBC Initialisation Sequence

In the specification and in the current presentation, the term “OBC Initialisation Sequence” is referred to:

All the operations executed by SW starting from the reset of the CPU up to the start of execution of the Application SW.

This includes:

- CPU and processor module initialisation and self-tests.
- integrity checks on ASW images and execution.
- SW maintenance functions.

In different projects this SW item (or part of it) is referred as:
Start-Up SW, Boot SW, Bootstrap SW, Init Mode.

Why do we need a Generic Specification for OBC Initialisation Sequence

Motivation for the Generic Specification 1 / 2

1. Initialisation Sequence is required in any onboard computer.
2. The functionality should be independent from the mission requirements.
3. Mission requirements covering the Initialisation Sequence are often incomplete or overlap with Application SW functionalities.
   For example:

   "**At power ON, the boot-up sequence shall autonomously start and bring the spacecraft to a safe configuration (power, thermal, pointing and communication). The boot-up sequence shall be mission dependent (pre-launch, separation, LEOP and nominal operation mode).**"

   Is this a requirement for the Initialisation Sequence or for the Application SW safe mode?

Motivation for the Generic Specification 2 / 2

4. Initialization Sequence allows to execute the Application SW and gives a unique opportunity to investigate malfunctions when the Application SW fails to start.
   For this reason, the scenario described below should be avoided:

   The Boot Report is only stored in local RAM memory and it is downloaded to Ground by the Application SW.
   - It is made available when the sequence is successful (not interesting)
   - It is <u>not</u> available in case of error in the Application SW (very interesting).

   These kind of "inconsistencies" can be avoided by specifying the minimal set of requirements of the Initialisation Sequence to be applicable to every mission, eventually this will also lead to a reusable SW component.

Definition process of the Generic Specification

Definition Process of the Generic Specification

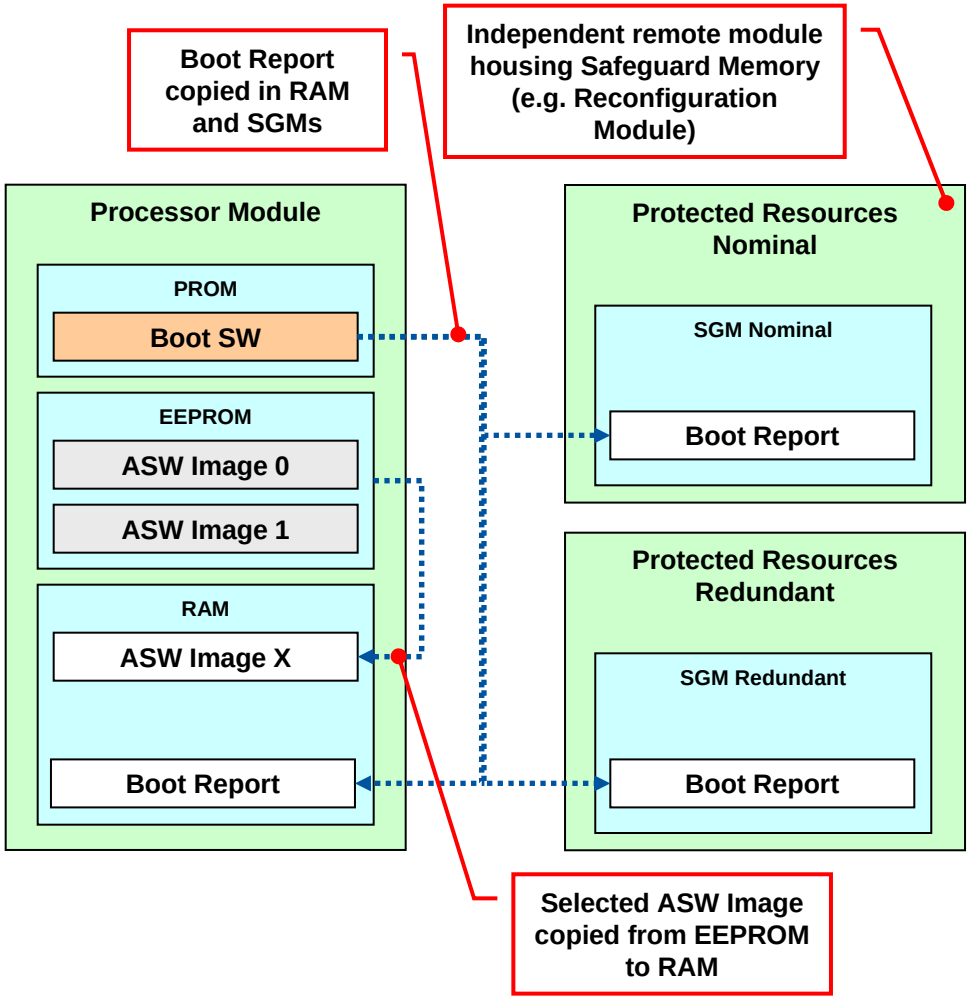
1. The initial draft requirements document has been prepared taking into account (or inspiration) the functionality of existing Initialisation Sequence SW of different projects/OBC suppliers products.
2. The document has been reviewed and refined within the Onboard SW & Operations Working Group (TEC-SWS) taking into account the return of experience from other projects/missions.

Then…

3. The document will now be submitted to review to a wider number of ESA experts, for example:
    - TEC-EDD (Data Handling);
    - Earth Observation;
    - Science and Robotics.
4. Finally industry can be involved in the review.

Context and main requirements

OBC Initialisation Nominal Sequence

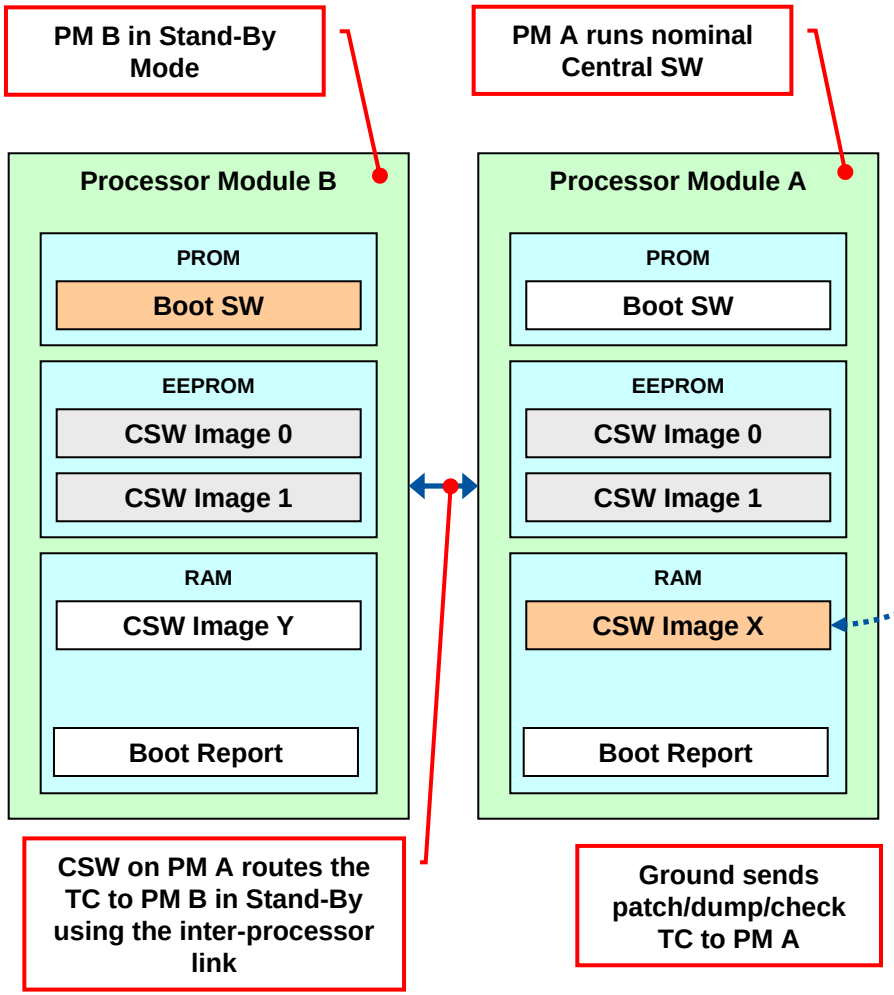


##RQ-OIS-BEF-FN-20

The Boot SW **Nominal Sequence** shall execute as minimum the following steps:

1. Perform processor module initializations;
2. Perform processor module self-tests;
3. Check for ASW Image selection;
   a. If ASW Image 0 is selected;
      – Test ASW image 0 in EEPROM;
      – Copy ASW Image 0 from EEPROM to processor RAM;
      – Test ASW image in processor RAM;
      – Execute ASW in processor RAM.
   b. If ASW Image 1 is selected;
      – Test ASW image 1 in EEPROM;
      – Copy ASW Image 1 from EEPROM to processor RAM;
      – Test ASW image in processor RAM;
      – Execute ASW in processor RAM.

OBC Initialisation Stand-By function



##RQ-OIS-BEF-FN-70

The Boot SW shall support the capability to **load, dump and check processor memories in flight** by means of separate equipment supporting the space-ground communication (Stand-By).

##RQ-OIS-BEF-FN-80

The Boot SW Stand-By function shall be triggered by the **logical AND of two independent conditions**.

OBC Initialisation Criticality

Once again the Initialisation Sequence is essential for the nominal execution of the Application SW and allows the in-flight SW maintenance of the On-Board SW.

For this reason this SW package shall have criticality B and shall be **strictly** developed according to ECSS SW standards.

The simple design and the sequential nature of the operations do not justify to use **Operating Systems** or **external unqualified libraries.**

##RQ-OIS-STD-QT-480

The Boot SW (**including any SW libraries**) shall be compliant to the ECSS-E-ST-40C.

##RQ-OIS-STD-QT-490

The Boot SW (**including any SW libraries**) shall be compliant to the ECSS-Q-ST-80C.

##RQ-OIS-STD-QT-500

The Boot SW shall be developed in compliance with the applicable coding standards.

##RQ-OIS-STD-QT-510

The Boot SW **criticality shall be at least category B.**

Note: ref. ECSS-Q-ST-80C section D.1

Conclusions and way forward

Conclusions

Summary:

- Initialisation Sequence has been defined.
- Motivations for the Generic Specification have been presented.
- The definition process leading to the Generic Specification document have been outlined.
- Some main requirements have been discussed.

Way Forward:

- The draft document is already informally used as a guideline in some reviews.
- Once finalised, the document will be made available to projects, to be incorporated in the ESA mission requirements baseline.
- Some requirements rely on assumptions on the OBC HW capabilities, these will be used as input in the definition of the OBC Generic Specification.
- The definition process for this specification can be refined and used in the definition of other Generic Specifications.