Boot Software Document

F. Torelli, TEC-SWS
SAVOIR Status / Reference Architecture
ADCSS 2014, 27/10/2014

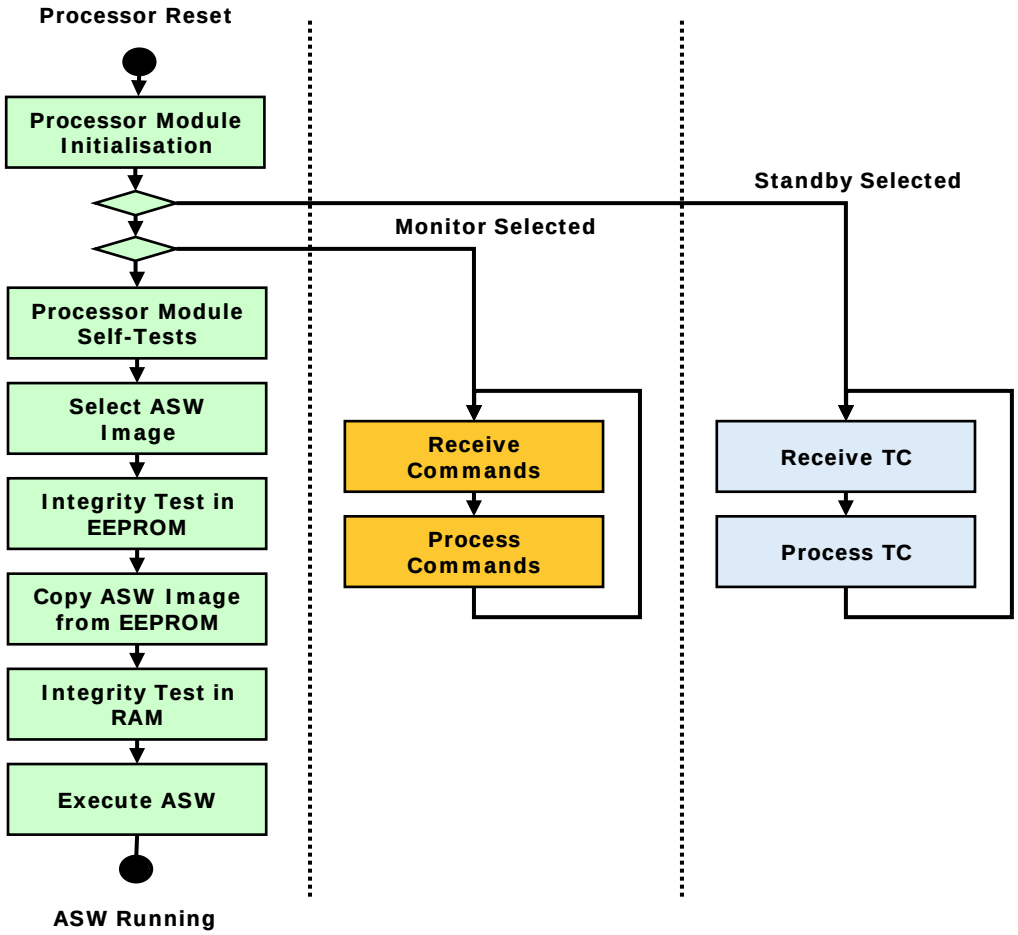
Outline

1. The story so far…
2. Intended use and what to avoid
3. …Where do we go from here

The story so far…

The Requirements Document

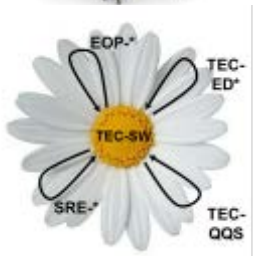
- Integrates the projects' lessons learned
- Is applicable to platform or payload computers
- Covers nominal sequence, software maintenance in-flight and on ground
- Lists a **minimum set** of requirements
- Includes justifications and explanatory notes



The Review Process

1. Prepared and reviewed within Flight Software Systems Section

2. Reviewed by a large number of ESA experts:
   - → EOP, SRE, TEC-QQS, TEC-ED
   - → 18 reviewers, 190 RIDs, ~100 action items



3. Reviewed by a large number of Industry experts:
   - → DLR, GMV, INTECS, OHB, RUAG, Scisys, SSF, Terma
   - → ~15 reviewers, 121 RIDs, 20 action items

4. Reference implementation on GR-CPCI-AT697E (ATB-RTB)
   - → Feedback on requirements consistency and usability
   - → 3 action items

Formal & Informal Users

Flight Computer Initialisation Sequence - ESA Requirements

TEC-SWS/10-373/FT, issue 1.0, November 2011

Adopted [formally or informally] by:

Bepi Colombo, MTG, Euclid, ESEO, Proba 3, JUICE, others…

Now available TEC-SWS/10-373/FT, issue 1.2 embedding all the action items from the previous reviews and activities

Intended use and what to avoid

Intended Use

The document is self-contained and self-consistent.

Similarly to ECSS standards, it is meant to be an applicable document:

- → Refer to it for Boot SW requirements
- → Define a tailoring matrix (with justifications) if not all the requirements are applicable to your mission
- → Complement the document with mission specific requirements (if needed)

What to Avoid

The requirements are **not meant** to be copied/pasted into another requirement document, then partially rewritten.

Example:

##Req-1:

At start-up, the bootstrap shall disable interrupts to test the interrupt mechanism before its use.

- **Objective of the requirement changed!**
- **Justification converted in a [piece of] requirement!**
- **Multiple requirements in one!**

##RQ-IS-BIN-FN-240

The Boot SW shall disable interrupts at start-up.

##END-REQ

Justification: before interrupts are to be handled, the processor needs to initialise a number of registers […], it is therefore important to start the SW execution with interrupts disabled and to enable (and unmask) them only when the system is capable to handle them (i.e. after Self-Test).

…Where do we go from here

Conclusions

Summary:

- Requirements document thoroughly reviewed
- Reference implementation
- Already adopted by many projects
- Issue 1.2 available including the inputs of the above activities

Way Forward:

- Requirements document to be formally published
- Subset of core requirements to be identified for
  Space Segment Requirements Document
  Instruments Interface Document

- Public review?
- Harmonisation with the other SAVOIR Generic Specifications?