

GS-005: SAVOIR OSRA - Execution Platform Functional Specification

Andreas Jung, European Space Agency

Marco Panunzio, Thales Alenia Space





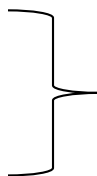
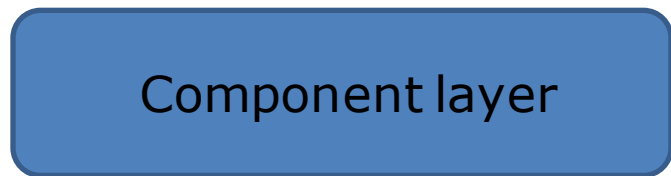
- Introduction
 - Overview of the OSRA architecture
 - Overview of the OSRA execution platform
- GS-005: SAVOIR OSRA - Execution Platform Functional Specification
 - Relationship to other SAVOIR OSRA specifications
 - Goal of GS-005
 - Document evolution
 - Document overview
- Open points and future work



The OSRA architecture



- Overview of the SAVOIR On-board Software Reference Architecture



Application software is designed by specifying “software components”.
Non-functional aspects are only “declaratively specified”.
Their implementation is left to the automation capabilities of the design environment



Automatically generated layer that implements the non-functional concerns declared by components (e.g., tasking, synchronization)



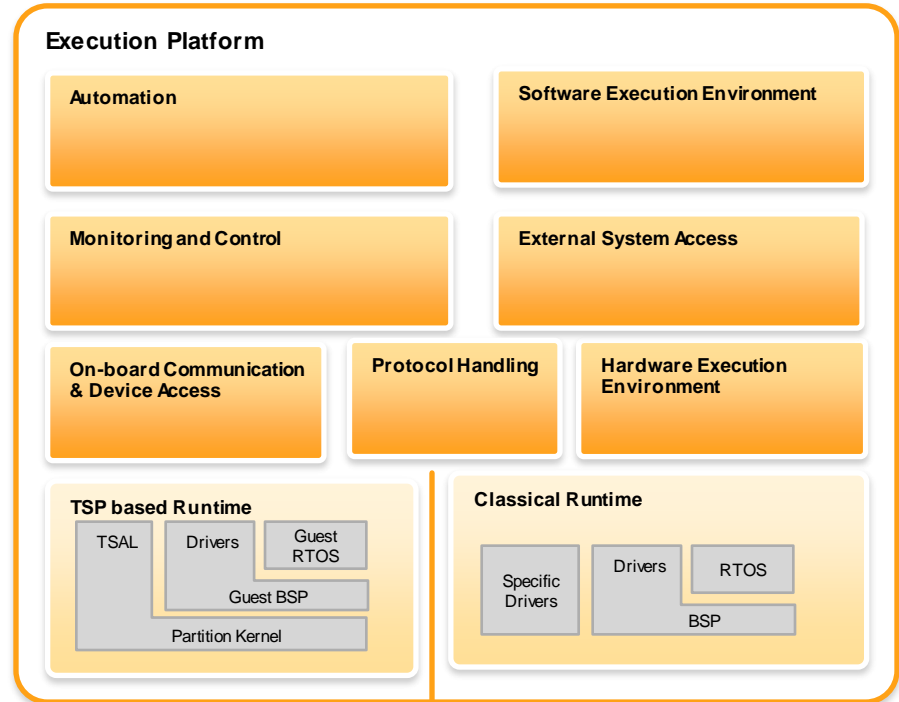
Provides services to the component layer (e.g., context saving) and interaction layer (e.g., tasking primitives, access to devices, message transfer)



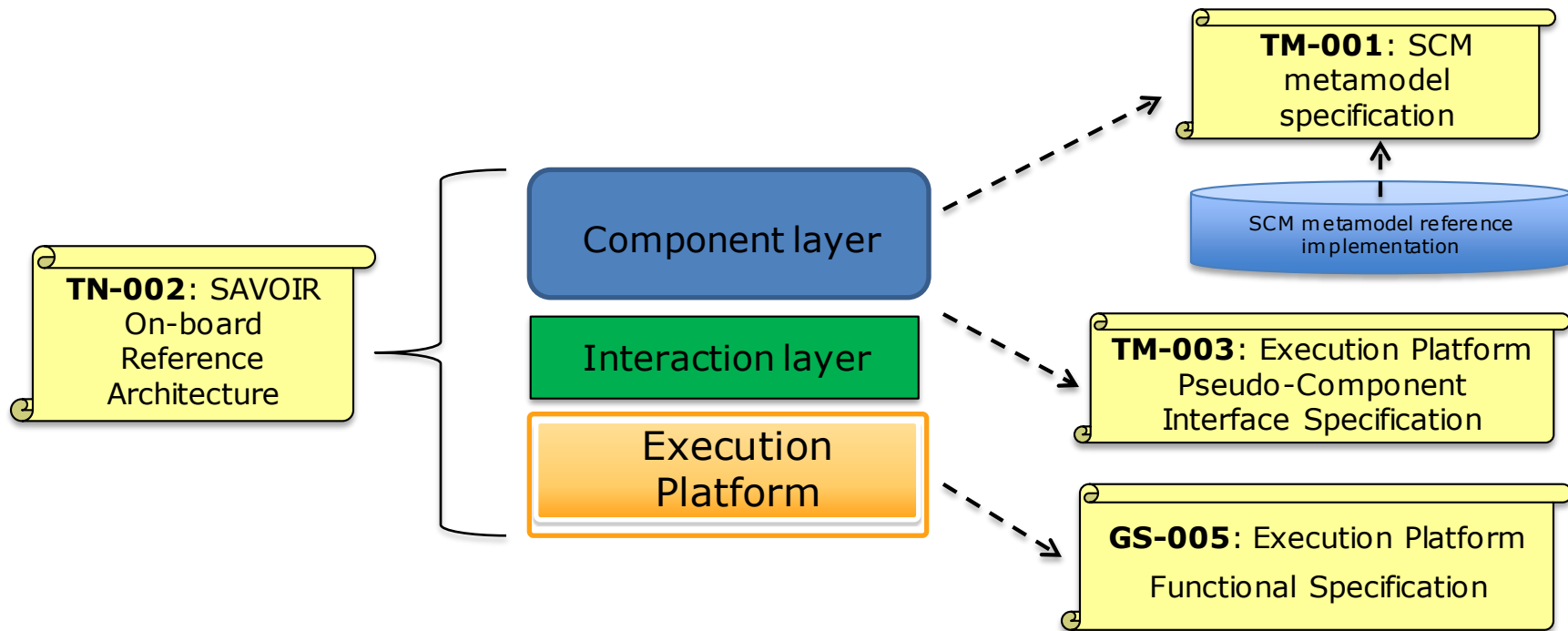
Execution Platform overview



- Provide for
 - Communication to / from ground
 - Automation
 - Monitoring & Control
 - Access to avionics devices (sensors, actuators, mass memory, etc...) and on-board communication media
 - I/O and HW abstraction
 - Platform Management
 - Tasking and real-time mechanisms
 - Execution and segregation mechanisms
 - (Partitions for Time and Space partitioning)
 - Support libraries



SAVOIR-FAIRE documents



Goal of GS-005



- GS-005 was written, as per other SAVOIR documents, as a generic specification
- GS-005 aims at consolidating the shared view around the concept of Software Execution Platform, and to promote harmonisation
 - Oriented to capabilities, functions, alignment of terminology across the domain
- The intent is to provide it as normative document for projects
 - Projects bidders provide a Statement of Compliance in their proposals
 - Requirements can be tailored out if not relevant
 - No VCD tracing / closeout is required



GS-005 Document Evolution



- GS-005 i1r0 issued in December 2018
- Undertook SAVOIR-FAIRE review
 - In the period 04/12/2018 – 18/01/2019, although some late RIDs have been accepted until 03/2019

 - 254 RIDs
 - 49 Major
 - 117 Minor
 - 88 Editorial



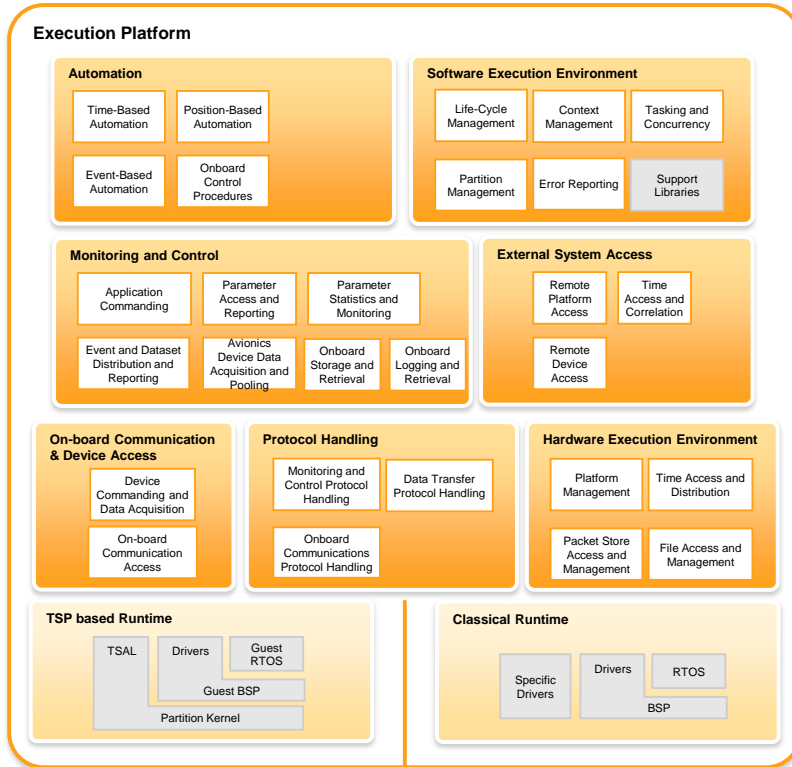
GS-005 Document Evolution



- A subsequent interim version was released in November 2019 (i1r1)
- Current version released in October 2020 (i1r2) and approved by SAG
 - Contains the implementation of dispositions to all major and minor RIDs
 - Only the implementation of a few dispositions has been kept open for the next version
 - More details in the presentation
- Companies of ESA member states can download the specification from ESSR
 - <https://essr.esa.int/project/osra-onboard-software-reference-architecture>



GS-005 Document Structure



- Terms, Definitions
- General Description
- Execution Platform Requirements
 - General Requirements
 - Capabilities Requirements
 - System Interface Requirements
- Appendix (Preliminary mappings)
 - PUS-C and CCSDS MOS



GS-005 Document Contents



- Defines requirements for capabilities and functions which must be present in the OSRA Execution Platform
 - No requirements on how functions shall be *implemented*
 - No requirements for service interfaces / function prototypes
- Provides a clear definition for what is expected of an OSRA Execution Platform and how the Execution Platform relates to other layers of the OSRA
 - However, there is no firm assumption or obligation that the layers above the execution platform are OSRA-compliant
 - The Execution Platform could be used also with an architecture that does not implement components or MBSE code generation



GS-005 Document Contents



- GS-005 was written specifically to abstract from a given Monitoring and Control (M&C) protocol
 - M&C capability leverage on the “Protocol Handling” capability to adapt to a specific protocol such as PUS or CCSDS MOS
- GS-005 built up to facilitate compliance statement declaration and tailoring out requirements
 - E.g., because not relevant to a given mission profile
- GS-005 recommends a given architectural decomposition
 - However implementations may easily tailor out the required decomposition, if infeasible to implement in their context



Open points and future work



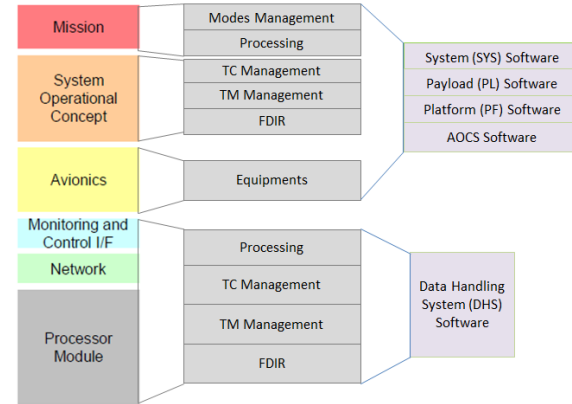
- Minimum capability set
 - Opportune to highlight a normative minimum set of capabilities and functions that shall be implemented in the execution platform
 - Also to highlight services that are considered essential w.r.t. those that could be more plausibly tailored out
 - Shall consider classical and TSP runtime
 - For the latter, user partitions and supervisor partitions will likely require different sets of minimum capabilities
- Detailed mapping to ECSS PUS-C
 - Current mapping is only high-level (per service)
 - Ideally mapping per service and sub-service would provide additional value added



Open points and future work



- Review of concept of variability and “variability levels” in the OSRA, and in particular in the Execution Platform
- Deferred non-critical applications initialisation and start in partitioned environments



Contact



Feedback: savoir@esa.int

