

SAVOIR: Reusing specifications to favour product lines

Jean-Loup Terraillon

▶ **To cite this version:**

Jean-Loup Terraillon. SAVOIR: Reusing specifications to favour product lines. 8th European Congress on Embedded Real Time Software and Systems (ERTS 2016), Jan 2016, TOULOUSE, France. hal-01261720

HAL Id: hal-01261720
https://hal.science/hal-01261720

Submitted on 24 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SAVOIR: Reusing specifications to favour product lines



SAVOIR Advisory Group
represented by
Jean-Loup Terraillon
European Space Agency
Savoir@esa.int

Keywords
SAVOIR, space avionics, product line, reference specifications

Abstract
SAVOIR has taken inspiration from AUTOSAR, although the underlying industrial business model is different. The space community is smaller, the production is based on a few spacecraft per year, and there are industrial policy constraints. Still, there is a need to streamline the production of avionics and improve competitiveness of European industry. Reference architectures, reference specifications and standard interfaces are an efficient mean to achieve the goal. Space agencies and space industry are actively working at developing such reference specifications. Reusing specification is expected to allow reusing products.

1. Description of SAVOIR

A. What is SAVOIR

SAVOIR (***S****pace* ***A****vionics* ***O****pen* ***I****nterface a****R****chitecture)* (http://savoir.estec.esa.int) is an initiative to federate the space avionics community and to work together in order to improve the way that the European Space community builds avionics subsystems.

The objectives are:

- to reduce the schedule and risk and thus cost of the avionics procurement and development, while preparing for the future,
- to improve competitiveness of avionics suppliers,
- to identify the main avionics functions and to standardise the interfaces between them such that building blocks may be developed and reused across projects

- to influence standardisation processes by standardising at the right level in order to obtain equipment interchangeability (the topology remains specific to a project).
- to define the governance model to be used for the products, generic specifications, interface definition of the elements being produced under the SAVOIR initiative.

The process is intended to be applied as part of the Agencies ITTs, and throughout the subsequent procurements and development process. A particular goal is to have SAVOIR outputs exploited in future projects and relevant products as part of European supplier's portfolios.

SAVOIR is coordinated by the SAVOIR Advisory Group (SAG) including representative of ESA, CNES, DLR, AirbusDS, TAS, OHB, RUAG, Selex Galileo, and Terma.

SAVOIR has been presented in ERTSS2012 [ERTSS2012]. The purpose of this paper is to give an update on the status of the initiative, the new technical areas that have been investigated, the documents that are available, the review process aiming at achieving consensus on the documents, and the application in space projects.

It is interesting to note how SAVOIR intentions have evolved. The initial ambition was to propose not only reference architecture and specification, but also building block products allowing the construction of the avionic systems. The discussions with industry have shown that it was more efficient to leave the development of the products to industry and let them manage their product lines. However, it was clear that the role of the Agencies was to prepare generic specifications at system level, as well as the basic technology that industry will then use to build products.

In addition, SAVOIR started with three pillars (data handling, control systems and software). It appeared soon that the operability was another important pillar which has a substantial impact on the variability of on-board avionics. This addresses space ground interface, operability concepts, and can also lead to harmonizing the software architecture on board and on ground.

B. State of the Art

The closest example of state of the art is AutoSar [AUTOSAR], triggered in the automotive industry. The business model is different (producing high number of cars and equipment), and therefore the resulting cooperation consensus is different. But the principle of "cooperating on standards and competing on implementation" remains. This was the motivation to start SAVOIR, but some differences where quickly noted:

- Managing complexity is the driver for AutoSar, but not for SAVOIR. Instead, SAVOIR aims at product lines within a domain of reuse which is relatively well known. The concern was more the variability of the requirements than their complexity. Beside, complexity is intended to be addressed with the model based approach, both system and software.
- The hardware architecture includes nearly a hundred of ECUs in a car, whereas the spacecraft platform computers can be counted with two hands' fingers.
- The business model is different, while millions of the same car are sold, space industry delivers some one-off spacecrafts a year. Instead, the European space cooperation rules enforce sub-contracting through "geographical return" (ESA must finance the industry of a Member State proportionally to the Member

State's contribution to ESA), creating the need for interoperability and clean-cut architecture.

The American initiative SUMO (Space Universal MOdular Architecture) [SUMO] has been started by the American office of the director of national intelligence, with inspiration of SAVOIR. According to the SUMO published data (credit Bernie Collins ODNI/AT&F), this innovative satellite acquisition has for objective to reduce the overall cost of space assets to government clients, and to enhance the global responsiveness of the space industrial base.
The policy drivers are based on the US National Space Policy 2010: "To promote a robust domestic commercial space industry, foster fair and open global trade and commerce through the promotion of suitable standards and regulations that have been developed with input from U.S. industry."

Other worldwide initiatives include (credit SUMO):

- SPA: AFRL's Space PnP Architecture – focused on reducing satellite development to months instead of years. A draft standard has been created through AIAA. It evolved to MONArch.
- cFE: NASA Goddard's core Flight Executive software framework enables basic software functions to be reused across programs, while allowing for tailoring of mission-specific software application functionality.
- Common Avionics Architecture (SpaceAGE Bus): NASA Goddard combines cFE/CFS with modular hardware (intra-box electrical & mechanical) definition for board level building-block functional elements; may be combined to form box level functionality
- FDK: DARPA's F6 Developer's Kit, which is a set of open source interface standards, protocols, behaviours, and reference implementations thereof, necessary to develop a new module that can fully participate in a fractionated cluster.
- Joint Architecture Standard (JAS): DOE Sandia National Labs – satellite PL processing & data com architecture, focuses on increasing mission flexibility, accommodating enhanced sensor performance, optimizing payload size, weight & power (SWaP) consumption.

2. Scope of the project

A. Initial working groups

At the time of ERTSS2012, the SAVOIR Advisory Group was supported by three sub working groups:

SAVOIR-SAIF (Sensor/Actuator InterFace)

This working group addresses the electrical interface of the sensor and actuators used for the attitude control and the guidance of the spacecraft.

The group achievement has been to detect the excessive costs due to the systematic redevelopment of an RS422 protocol, and therefore to propose its standardization in the scope of ECSS. A preliminary study defined physical and data link layer

requirements as input to an update of the ECSS-E-ST-50-14C standard. This update is on-going.

SAVOIR-SAFI (Sensor/Actuator Functional Interface)

This working group is in charge of the standardization of the functional interface with sensors and actuators.

The group's achievement has been to define a standardized functional interface for the Star Trackers, which was proposed to be included in the ECSS-E-ST-60-20C (Star Sensor Terminology And Performance Specification).

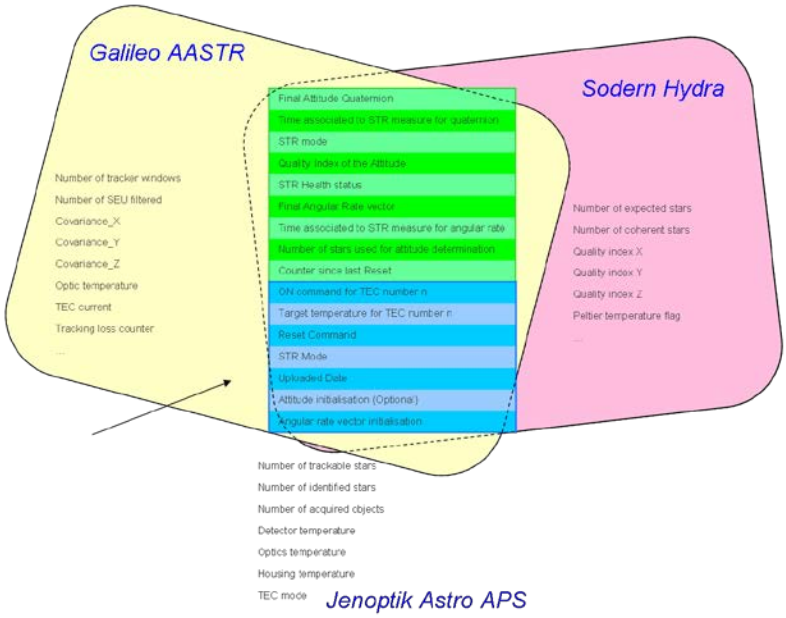


Figure 1 Star Tracker functional interface

The group investigated then the possibility to expand the same activity to gyroscopes. The results of the discussion in SAFI are that there are coarse and FOG gyro which are so different that it is not possible to harmonize between the two families. So there could be two standardizations. However, the FOG gyros have been harmonized already by the primes who are procuring them. The coarse gyros are too few for harmonization. Therefore this investigation was stopped. For the other sensors-actuators, which are simpler, the standardization is not necessary. Therefore the work of SAFI was stopped.
Further activity on sensor-actuator interface will happen around the technology of Electronic Data Sheet (EDS) that intends to support the automatic configuration of the access to the devices within the software architecture.

SAVOIR-FAIRE (Fair Architecture and Interface Reference Elaboration)

This working group is in charge of the on-board software reference architecture.

The group achievement has been to come with a complete definition of the on-board software reference architecture [OSRA], including:

- Users' needs and high level requirements for such an architecture
- the definition of two layers (application and execution platform)

- a Space Component Model description to support the description of application with components
- a functional specification of the execution platform, and of the interface between the components and the execution platform.
- a demonstrator of feasibility in ESA laboratory.

B. Recent working groups

Since ERTSS 2012, two new working groups have been created:

SAVOIR-IMA (Integrated Modular Avionics)



The working group addresses the spin in of the aeronautical Integrated Modular Avionics (IMA) concept into space.

The group's achievement has been to produce high level requirements for a concept of Time and Space Partitioning in the software architecture, use cases and their prioritization, the definition of industrial roles in the production of IMA for Space systems, and an architecture of a TSP based execution platform.
Several R&D activities supported this achievement. The last one intended to harmonize the "classical" architecture produced by SAVOIR-FAIRE with the IMA architecture. Its results are now being integrated in the final SAVOIR-FAIRE documents.
The motivation was to segregate the integration, verification and validation of some software functions that could be independent, such as the various payload software or sensor software, while running them on a single computer and thus saving electronics costs.

SAVOIR-MASAIS (MAss Storage Access Interfaces and Services)



The working group addresses the data storage (for platform and payload) and the related use of files in spacecraft's operation.

The group achievement for the moment is to produce system level requirements for a data storage system. Later results will be to produce requirements of a File Management System, supported by a specific R&D activity. Spacecraft operation has traditionally be based on packet transfer, and only recently files are used on-board (e.g. Euclid). This requires harmonization between the spacecraft operators and the on-board implementation of data storage.

A new working group is under creation:

SAVOIR-UNION (User Needs In On-board Network)



The working group will investigate the definition of the functional, performance, operational and interface requirements of the functional links and their management. The scope is limited in the identification and characterisation of the needs of users in term of communication and does not address the definition of communication standards and protocols.

The group will come with system level requirements of an avionics network. The difficulties encountered in some project to integrate and validate some avionics link within the system composed of the main computer, the data storage and the payloads, has shown that the avionics system approach had not been enough investigated.

3. Major results

A. Reference Architecture

The SAVOIR Advisory Group, supported by R&D activities, came up with a reference avionics architecture:

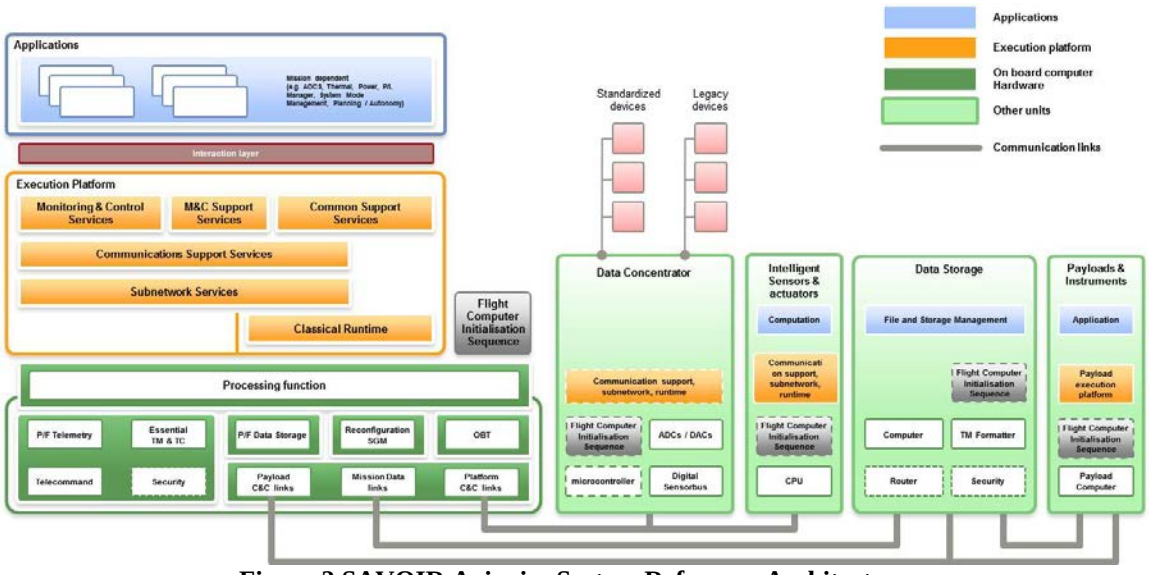


Figure 2 SAVOIR Avionics System Reference Architecture

On the hardware side, avionics was organized in functional blocks with interfaces:

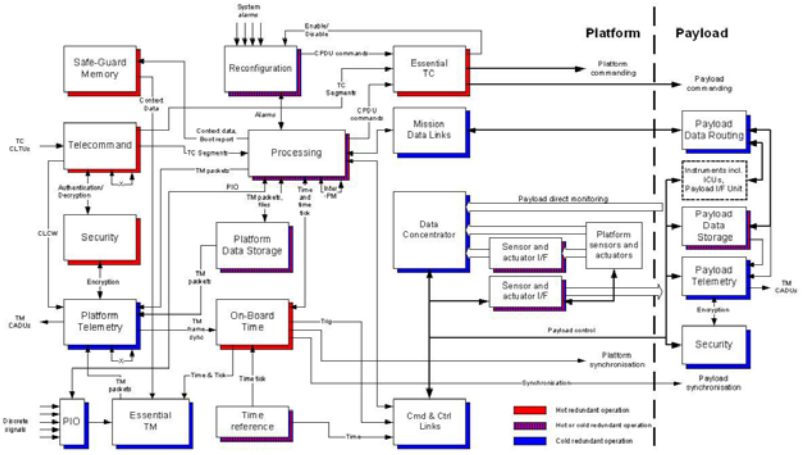


Figure 3 The avionics functions

The mapping of these functions on actual physical boxes is let to industry to decide, in the scope of their definition of product lines. Some examples are given in the document SAVOIR-TN-001.

On the software side, the notion of execution platform was further described in the following diagram:

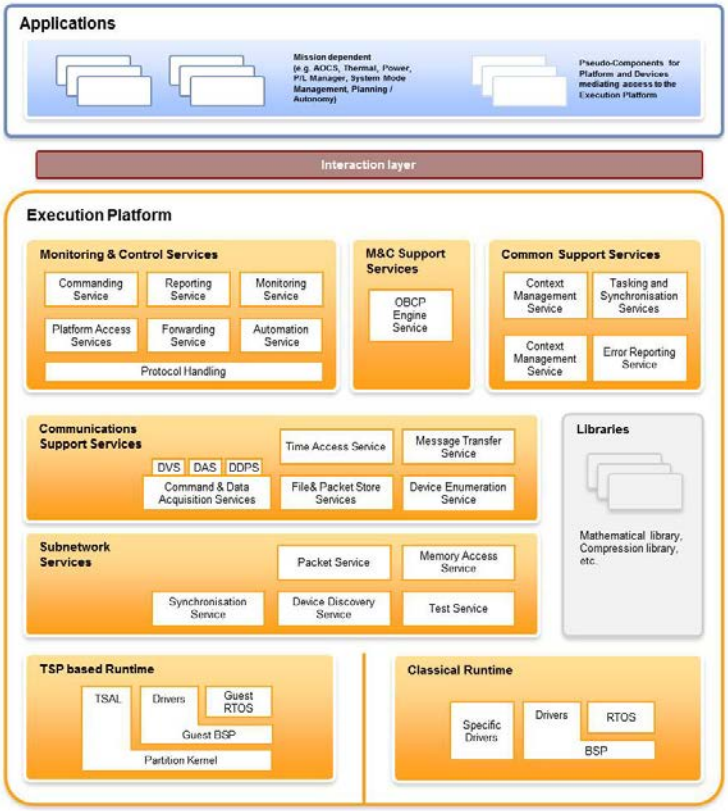


Figure 4 Details of the Execution Platform

B. Documents

The SAVOIR documents are organized in a similar way as projects documents, such that they can be easily used at the appropriate place.

Figure 2 introduces the typical documentation tree of a project:
ESA includes in its Invitation To Tender in particular the Statement Of Work, the project SRD/OIRD, and other documents such that the ECSS and CCSDS applicable standards.

The project prime produces out of them its own documents, to be used for the procurement of the spacecraft elements, in particular system, sub-systems and units requirements specification.

The SAVOIR documents follow the same logic.

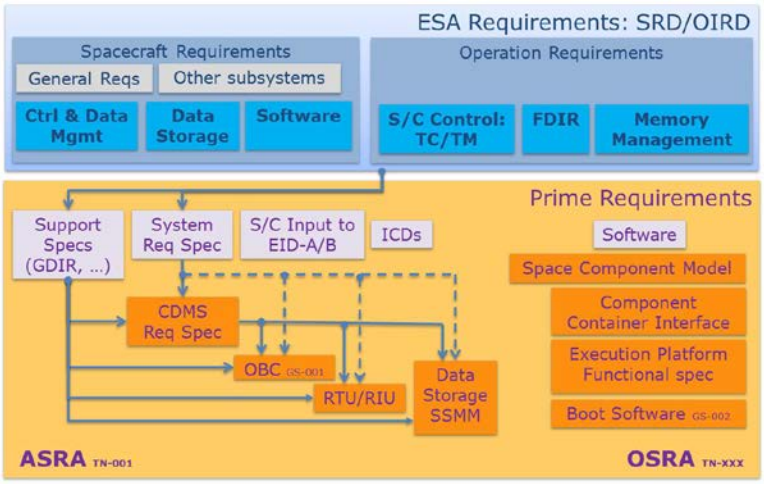


Figure 5 SAVOIR documentation tree

In Figure 2, the top documents are the ESA System Requirement Documents (SRD) and Operation Interface Requirement Documents (OIRD). The bottom documents are the product specifications intended to be used by the Large System Integrators. They address hardware (ASRA side: Avionics System Reference Architecture) and software (OSRA side: On-board Software Reference Architecture).

SAVOIR ASRA SAVOIR OSRA

Figure 3 shows the process that produces product specification from SAVOIR documents. The Prime contractor prepares his own documents such as the System Requirement Specification, the ICDs, some high level software Requirement Baseline, etc.

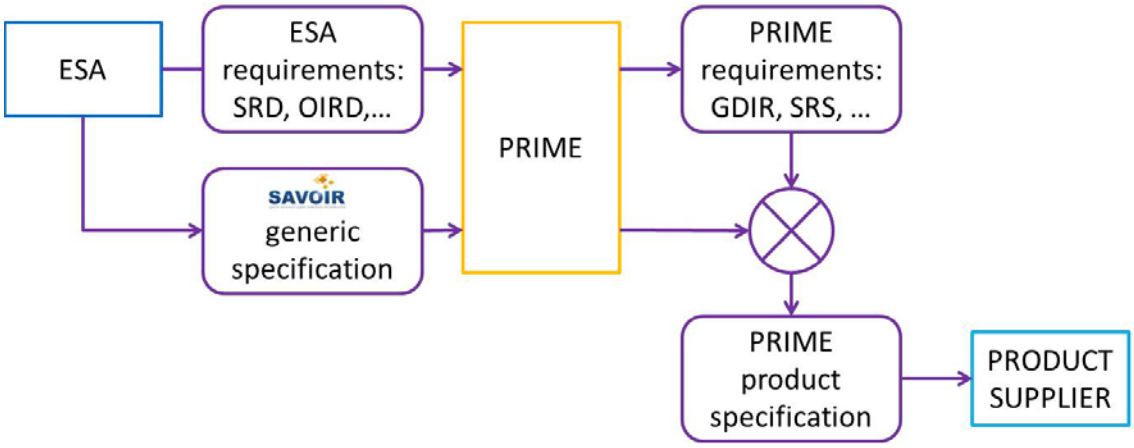


Figure 6 Use of SAVOIR documents

Then the Prime prepares the Product Specifications for the procurement, for the hardware (CDMS specs, unit specs) and for the software (Application specification, execution platform specification). The SAVOIR documents are intended to support this activity, by allowing the Prime to reuse product specifications for his own procurement. This is when the Prime's avionics architect envisages a physical architecture and maps the Savoir functional architecture on the physical units that he

intends to procure, tuning the configuration parameters of the generic specification to actual project's values.

The envisaged SAVOIR product tree at the time of edition of this document is based on General Specifications (normative), and Technical Notes, Handbooks and Technical Reports (informative):

Technical Notes: context			
[ASRA]	SAVOIR Functional Reference Architecture	SAVOIR-TN-001	(under SAG endorsement)
[OSRA]	SAVOIR On-Board Software Reference Architecture	SAVOIR-TN-xxx	(under conversion from a R&D document into a Savoir document)
[PLIF]	SAVOIR general recommendations for Platform Payload interface	TEC-SW/12-538/JLT	(drafting)
[SCMON]	SAVOIR General Recommendations for Spacecraft Monitoring and Control,	TEC-SW/12-539/JLT	(drafting)
Generic Specification: product specification			
[OBC]	SAVOIR generic OBC Specification	SAVOIR-GS-001	(under SAG endorsement)
[BootSW]	SAVOIR Flight Computer Initialisation Sequence Generic Specification	SAVOIR-GS-002	(under SAG endorsement)
[RTU]	SAVOIR generic RTU specification	SAVOIR/12-003/GM	(drafting)
[RTUop]	SAVOIR RTU – Operability Requirements	TEC-EDD/2013.11/GM	(drafting)
	Data Storage SSMM	-	From Savoir-Masais + R&D
	Space Component Model	-	(under conversion from a R&D document into a Savoir document)
	Component Container Interface	-	(under conversion from a R&D document into a Savoir document)
	Execution Platform Functional spec	-	(under conversion from a R&D document into a Savoir document)

Handbook: how to			
	SAVOIR On-board Software Reference Architecture Training Material	SAVOIR-HB-001	Released
	SAVOIR Avionics System reference Architecture Handbook	SAVOIR-HB-xxx	(drafting)
Technical Reports: working group results			
	SAVOIR-SAFI - Standardisation of AOCS Sensors and Actuators Functional Interface	TEC-SWE/11-481/AJ	Released
[AOCS]	SAVOIR SAIF - AOCS Sensor and Actuator Interfaces Working Group report	SAVOIR/12-005/PA	Released
[SAFRA]	SAVOIR-FAIRE - On-board Software Reference Architecture	TEC-SWE/09-289/AJ Issue 1 Rev 0 2010-06-10	Released
	SAVOIR-IMA -	-	(available, not yet released)
	SAVOIR-MASAIS -	-	(drafting)
	SAVOIR-UNION	-	(drafting)

For reference, Figure 4 shows the relation between the documents and the architecture.

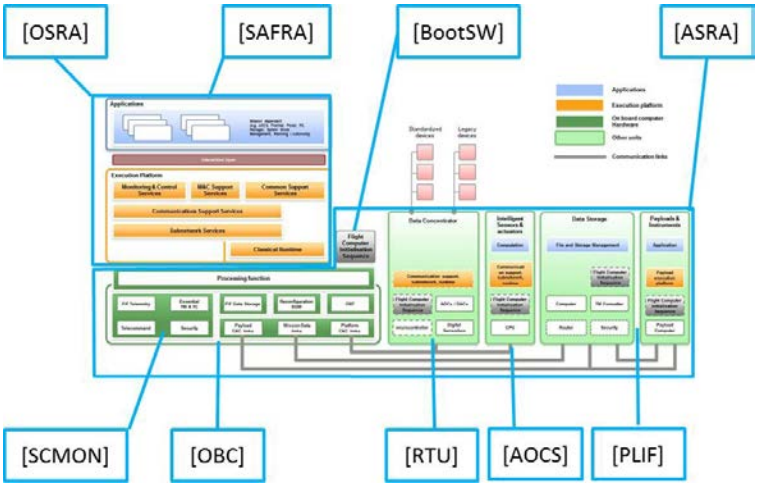


Figure 7 The documents and the architecture

Note: the list of documents is intended to be up to date on http://savoir.estec.esa.int .

In addition to the reports of some of the working groups (SAVOIR-FAIRE, SAVOIR-IMA, SAVOIR-SAIF and SAVOIR-SAFI), 4 documents are available at the time of ERTSS2016:

- SAVOIR documentation tree (SAVOIR-TN-000 technical note)
- Avionics System Reference Architecture (SAVOIR-TN-001 technical note). This document introduces the reference architecture with a functional approach. A list of the functions usually implemented in hardware on a spacecraft platform (and partially on payload) is provided, together with their description.
- On-Board Computer generic specification (SAVOIR-GS-001 applicable document). This document list the requirements applicable to the group of functions commonly implemented in an on-board computer.
- Initialisation Sequence Software (boot software) (SAVOIR-GS-002 applicable document). This document lists the minimum set of requirements that are applicable to any boot software of a spacecraft processor.

The two –GS- documents (Generic Specification) associate requirements with a formal reference, their justification, and some notes on their applicability. They can be optional or mandatory. They are associated with parameters to be defined when the document is actually used in a project. They are intended to be later administered in an IBM Rational DOORS requirement database.

The documents are distributed using the European Space Software Repository (ESSR) http://essr.esa.int, a repository intended for the diffusion of ESA software assets. This repository allows for a controlled distribution, in particular allowing the dissemination within member states only. The ESSR has been opened to the public in September 2015.

SAVOIR status is also disseminated every year in the Avionics Data Control Software Systems in October at Estec (http://adcss.esa.int).

Out of SAVOIR, ESA is working on generic System Requirements Document and Operation Interface Requirement Document that will harmonize further spacecrafts procurements.
However, within SAVOIR, some sections of the avionics part of the SRD have been internally drafted. A draft generic OIRD has been produced in ESA and is under SAG review.

In the future, the software documents are being refined in order to be ready to enter into a public review:

- Space Component Model (including pseudo-component definition and component-container interface) (applicable)
- Execution Platform functional specification (applicable)
- Interaction layer – execution platform interface (technical note)
- Execution Platform internal interface (technical note)

C. Public review

The process of public review is similar to the ECSS process. Through ECSS, Eurospace, the entity that represents the space industry, has nominated reviewers from selected companies. An organisation note of this industrial consultation has been agreed.
The public review started in January 2015. About 500 comments (159 majors and the rest minors) from 20 companies were received on the 3 documents. The spirit of the review was very constructive. The penetration of the SAVOIR knowledge within industry was considerably improved. About 300 modifications on the 3 documents were implemented intending to improve the understanding of the documents (scope, applicability, and glossary), the applicability of the document (refinement of the domain of reuse, applicability matrix, additional industrial relevance) and some technical aspects of the document. The review used the web-interface tool that ESA actually deploy in the spacecraft's project reviews, which allows for a full visibility of the comments by the community and a full traceability of the evolutions.

D. Progress

Key indicator of progress are the assiduity to the SAG meetings and the constant high audience of the dissemination events ADCSS, as well as the increasing maturity of the SAVOIR documents, through substantial R&D work, prototyping, industry exchanges and reviews.

The main difficulty encountered is to initiate this change process. SAVOIR is a not only a technical adaptation, but it is a "life style" involving view point change from all the stakeholders. Agencies have to specify always the same way, Large System Integrators have to procure with the same specification, and Suppliers have to arrange for product lines. Harmonizing the way that ITTs are done at Agencies level is a substantial task, as well as it is to influence product line management in large companies who have also commercial markets out of the institutional Agencies market.

The applicability of SAVOIR documents must also be defined. Indeed, if they are labelled in ITTs as Reference Document, there is no incentive for industry to take them on-board projects, and there is no way for the SAVOIR coordination to measure their suitability and to adapt the documents to the needs. On the other hand, if they are labelled as Applicable Documents, they are binding, traceability of non-compliance is feasible and can be fed back to the SAVOIR organization. But at the same time, non-compliance is seen at contractual level as a competitive disadvantage decreasing the chances to win the contract, whereas the nature of non-compliance to SAVOIR is not going to change the mission performance, but maybe to achieve the mission objectives with a different set of functional specification. Still, it will break the product lines industrial objective.
An intermediate level, called "Normative document" will be used, it is less constraining than Applicable Document, but still allow to trace the non-compliances and to allow review by ESA.

The measure of SAVOIR success is somehow difficult to quantify, as long as the documents are not formally made applicable. However, they find their way in some projects, and several proposals have clearly been derived from the SAVOIR documents. They should be formally made applicable in an ESA payload project in 2016.

4. Conclusion

The fulfilment of the objectives listed in section 1-A is assessed in the following way.

The two first objectives are very long term and cannot be directly measured:

- *to reduce the schedule and risk and thus cost of the avionics procurement and development, while preparing for the future,*
- *to improve competitiveness of avionics suppliers,*

The other objective starts to be reached:

- *to identify the main avionics functions and to standardise the interfaces between them such that building blocks may be developed and reused across projects*

This has been done and examples of building blocks are existing (OBC, RTU, software operating system, execution platform)

- *to influence standardisation processes by standardising at the right level in order to obtain equipment interchangeability (the topology remains specific to a project).*

A number of standards have been created or modified, in particular in ECSS. The SAVOIR technical activities have also been useful to review external standards, in particular the [CCSDS]. The [SOIS] standards have been reviewed by industry, and consequently their use in OSRA has been better targeted. The [MOS] standard have been analysed and a technical roadmap has been produced for a long term consideration in on-board architecture.

- *to define the governance model to be used for the products, generic specifications, interface definition of the elements being produced under the SAVOIR initiative.*

We are at the beginning of the governance of products, but software experience exists with the management at ESA level of the qualification of the operating system [RTEMS]. In the same line, discussions are on-going to define the governance of the separation kernel [Xtratum]. Cooperation ESA-CNES is discussed around the product [LVCUGEN].

Some lessons learned may be derived from the exercise:

- it takes a lot of time to federate a community around objectives that are globally beneficial,
- however, this background continuous harmonization between customers and suppliers is extremely efficient to keep heads aligned in the same direction.
- customers should not try to rule it all, instead each stakeholder can act at his level in the scope of its own constraints
- avionics is not only software, hardware and control, but also operability has a substantial impact on it.

SAVOIR should not be seen as direct product standardization, where on-the shelves products are imposed by the agencies in spacecrafts. This would not work. Instead, SAVOIR is a continuous Harmonization process within the avionics community where each stakeholder adjusts his behaviour at his level for the benefit of all industry.
This change process is challenging, but the progressive penetration of the concept within the many layers of the avionics community is successfully on-going.

5. Literature

[AUTOSAR] (http://www.autosar.org)

[CCSDS] The Consultative Committee for Space Data Systems (http://public.ccsds.org/default.aspx)

[ERTSS2012] What You Must KNOW About SAVOIR… SAVOIR Advisory Group represented by J.L. Terraillon, February 2012

[ESSR] https://essr.esa.int/

[MOS] Mission Operations Services (http://public.ccsds.org/publications/archive/520x0g3.pdf) standard.

[OSRA] Documentation : SAVOIR-HB-001 i1 r0 - SAVOIR On-board Software Reference Architecture Training Material
(https://essr.esa.int/ ; registration needed; access to ESA member states representatives only)

[RTEMS] Real-Time Executive for Multiprocessor Systems (https://www.rtems.org/). [Xtratum] (http://www.xtratum.org/).

[SOIS] The Spacecraft Onboard Interface Services Area (http://public.ccsds.org/publications/SOIS.aspx)

[SUMO] Space Universal MOdular Architecture (SUMO): CCSDS Spring Plenary Bordeaux, France
http://www.google.nl/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CCIQFjABahUKEwjkicLXo7LIAhWFVhoKHaOPCXg&url=http%3A%2F%2Fcwe.ccsds.org%2Fsois%2Fdocs%2FSOIS-APP%2FMeeting%2520Materials%2F2013%2FSpring%2FSUMO%2520CCSDS%2520Spring%2520Plenary.pdf&usg=AFQjCNEnk7inVj4QS-onNXkMhUmbgIKQUQ&sig2=wH9enbnuDDiwYp79UBKWkA

[LVCUGEN] Logiciel de Vol Charge Utile GENérique (https://indico.esa.int/indico/event/53/session/10/contribution/53/material/1/0.pdf).