SAVOIR
space avionics open interface architecture

Integrated Modular Avionics: SAVOIR-IMA status and progress

M. Hiller / M. Hernek
European Space Agency ESTEC

ADCSS 2013 – 22/10/2013

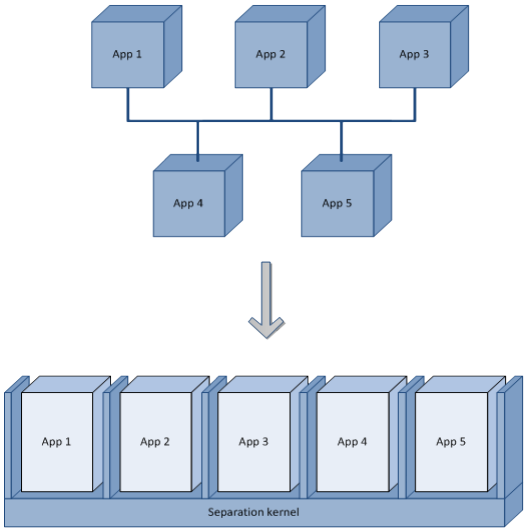
SAVOIR IMA
space avionics open interface architecture

Outline

- IMA
- SAVOIR-IMA Working Group
- Scope and members
- How do we link to other working groups?
- IMA Roadmap
- Activities and Status
- Outlook

Integrated Modular Avionics

- The aviation domain has been working since the early 1990's on integration of different software applications onto the same hardware
  → **Integrated Modular Avionics (IMA)**
- A key enabler for this is guaranteed separation and non-interference
  - **Partitioning** provided by partitioning kernel
- Benefits
  - Savings on mass, volume and power
  - Parallel development
  - Incremental V&V
  - Fault containment
  - Improved SW maintenance
- Supported by ARINC standards (A651, A653, DO-297)
- Used by Boeing (777 & 787) and Airbus (A380)



Time and Space Partitioning (TSP)

- At the core of IMA, partitioning ensures proper separation and non-interference across software functions
  - Partitioning kernel
- Time
  - Each partition is assigned a time slot in which the software is allowed to execute
- Space
  - Each partition is assigned a special area in memory where it may access contents

- Violations during executions will be detected and the failing partition is stopped, ensuring that other partitions remain unaffected

SAVOIR IMA WGs Scope and its member

- Use cases and System Requirements
- *Terminology*
- *Reference Architecture and Interface Description*
- Qualification package for Separation kernel
- Execution Platform
- *Process, Roles and Responsibilities*
- RoadMap for IMA aspects

Name	Company
Marie del Carmen Lomba	GMV
Alain Rossignol	Astrium
Aldo Sala	Intecs
Christian Spinelli Gerald Garcia Jacques Busseuil	ThalesAleniaSpace
Massimo Ferraguto	SSF
Massimo Molteni	Intecs
Massimo Tipaldi	OHB
Patrik Sandin	RUAG Space
Paul Arberet	CNES
Poul Hougaard	Terma
Stuart Fowell	SciSys
James Windsor	ESA/ESTEC
Maria Hernek	ESA/ESTEC
Martin Hiller	ESA/ESTEC
Andreas Jung	*ESA/ESTEC -- FAIRE*
Fabio van Hattem	*ESA/ESTEC -- SAFI*
Giorgio Magistrati	*ESA/ESTEC – HW std*

Liaisons and interfaces

SAVOIR
space avionics open interface architecture

SAVOIRFAIRE
space avionics open interface architecture

Andreas Jung

CCSDS
The Consultative Committee for Space Data Systems

Maria Hernek

Stuart Fowell

SAVOIRIMA
space avionics open interface architecture

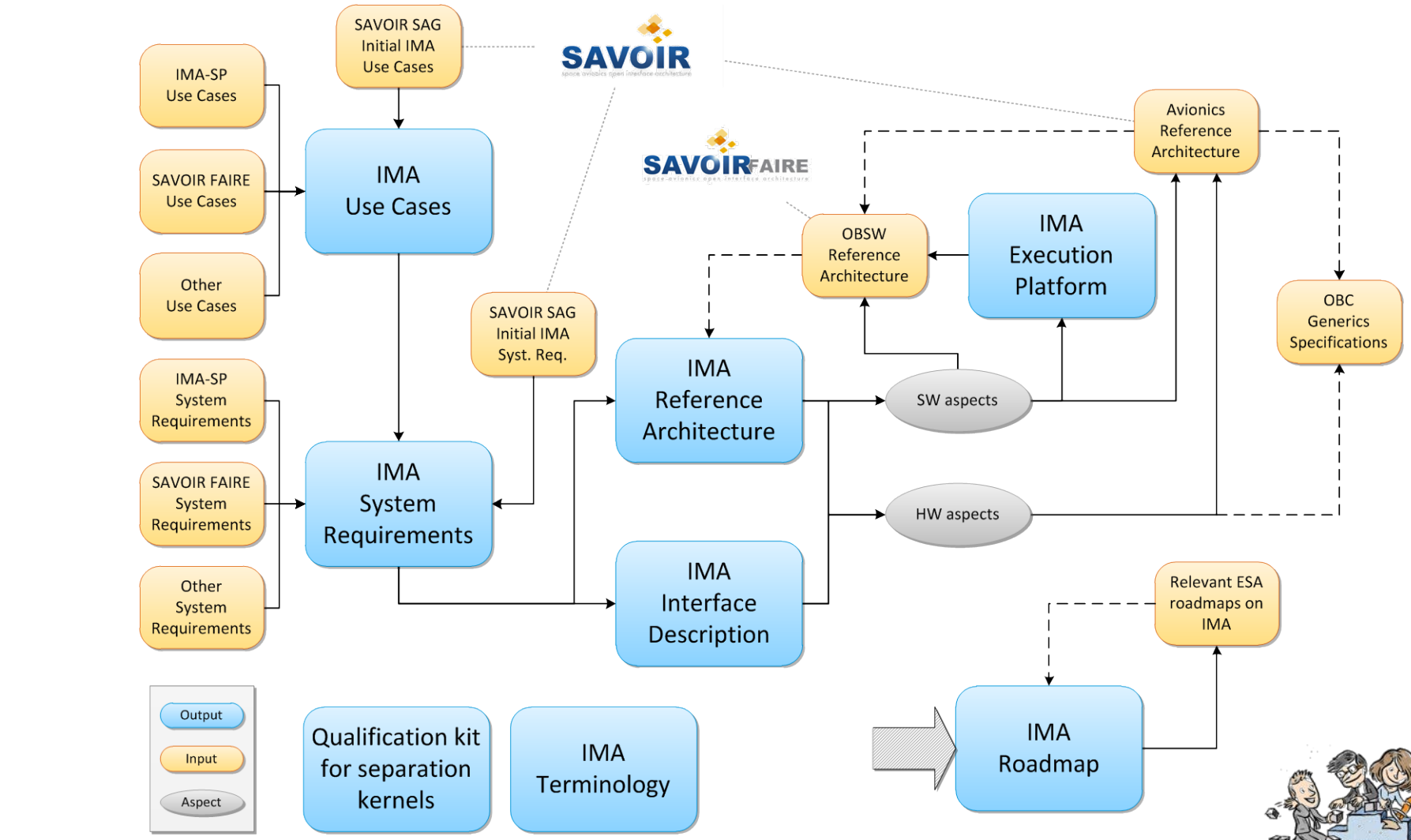
Fabio van Hattem

Giorgio Magistrati

SAVOIRSAFI
space avionics open interface architecture

Hardware reference and standardisation

WGs Inputs and outputs



Use cases and System Requirements

- Objective
  - Revisit TSP WG results from 2007 and update with any new insights and experiences gained from IMA related activities completed since then. Primarily, IMA-SP results are considered as new input.
  - Set priorities to use cases, features and requirements.
- Purpose
  - Ensure that the needs and requirements that initiated the work on introducing IMA to spacecraft avionics are still valid.
  - Ensure that new findings and experiences are taken into account when moving forward with IMA for spacecraft avionics.
  - Ensure that SAVOIR IMA members all agree on the use cases and requirements.

Terminology

- Compilation terminology across SAVOIR, SAVOIR FAIRE, COrDeT, IMA-SP
- Two-fold purpose
  - Get each camp to understand what they talk about in the other camp
  - Move towards common set of terms and definitions
- The terminology will/must evolve along with efforts on alignment between OBSWRA and IMA-SP

  → This will be covered along side the SAVOIR FAIRE/IMA support activity

Reference Architecture and Interface Description

COrDeT-3, SIFSUP

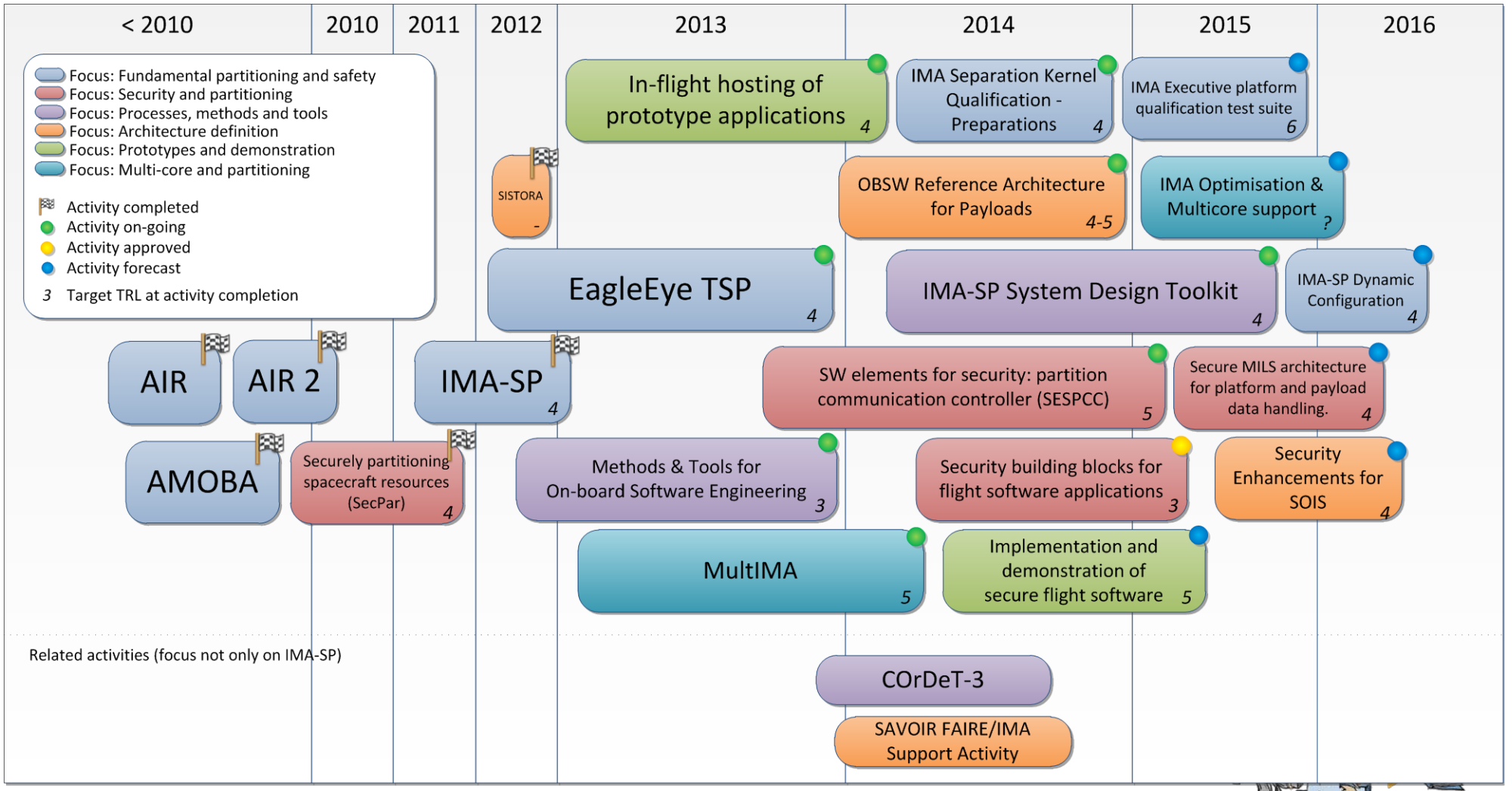
Harmonised Onboard Software architecture

Non IMA as well as IMA system

- Architecture description
- Interfaces
- Component model specification
- Terminology

Activities followed by both FAIRE and IMA WGs

IMA Roadmap



On-going IMA activities

- EagleEye TSP – SSF
  - Use case of TSP with Xtratum on Avionics lab platform
  - To be completed shortly.
- Methods and Tools for On-board Software Engineering – LERO
  - IMA-related part: Definition of general requirements for separation kernel and use of those requirements in formal verification of a kernel.
  - To completed by end of year.
  - Final presentation scheduled for December.

On-going IMA activities, cont

- MultIMA – GMV
  - Adding multi core support to AIR.
  - CDR scheduled for November 19.
  - To be completed by end of January 2013
- IHPA – SpaceBel
  - Partitioning PROBA 2 SW and exploring SW maintenance and SW boot approaches
  - CDR scheduled January 10 2014.
  - To be completed by end of February 2014
- SW Elements for Security: Partition Communication Controller - Astrium
  - Implementation of Partition Communication Controller (router partition for secure inter-partition communication) and IO Manager (offloading IO to external HW unit).
  - Activity recently kicked off. Completion expected in first half of 2015

Upcoming IMA activities

- OSRA-P (On-board Software Reference Architecture for Payloads)
  - Definition of a reference architecture for payloads based on OBSWRA and IMA-SP
  - ITT closed Oct 15. Aim to kick off before end of the year.
- IMA System Design Toolkit
  - SoW definition in progress
  - ITT targeted for end of 2013
- Preparation for SEP Kernel Qualification package
  - SoW definition in progress
  - Objective: baseline Kernel Qualification Requirement, identify and assess V&V methods for partition kernel, define Verification and Validation strategy and plan, assess Candidate kernels conformance, perform Use case

Conclusions and future steps

- SAVOIR IMA mainly active in first half 2013
- WGs support contract now in place – resume WGs activites
- Multicore and/or multiprocessor to be considered in IMA architecture

Contact

Feedback: savoir@esa.int

Contact SAVOIR-IMA

Maria.Hernek@esa.int

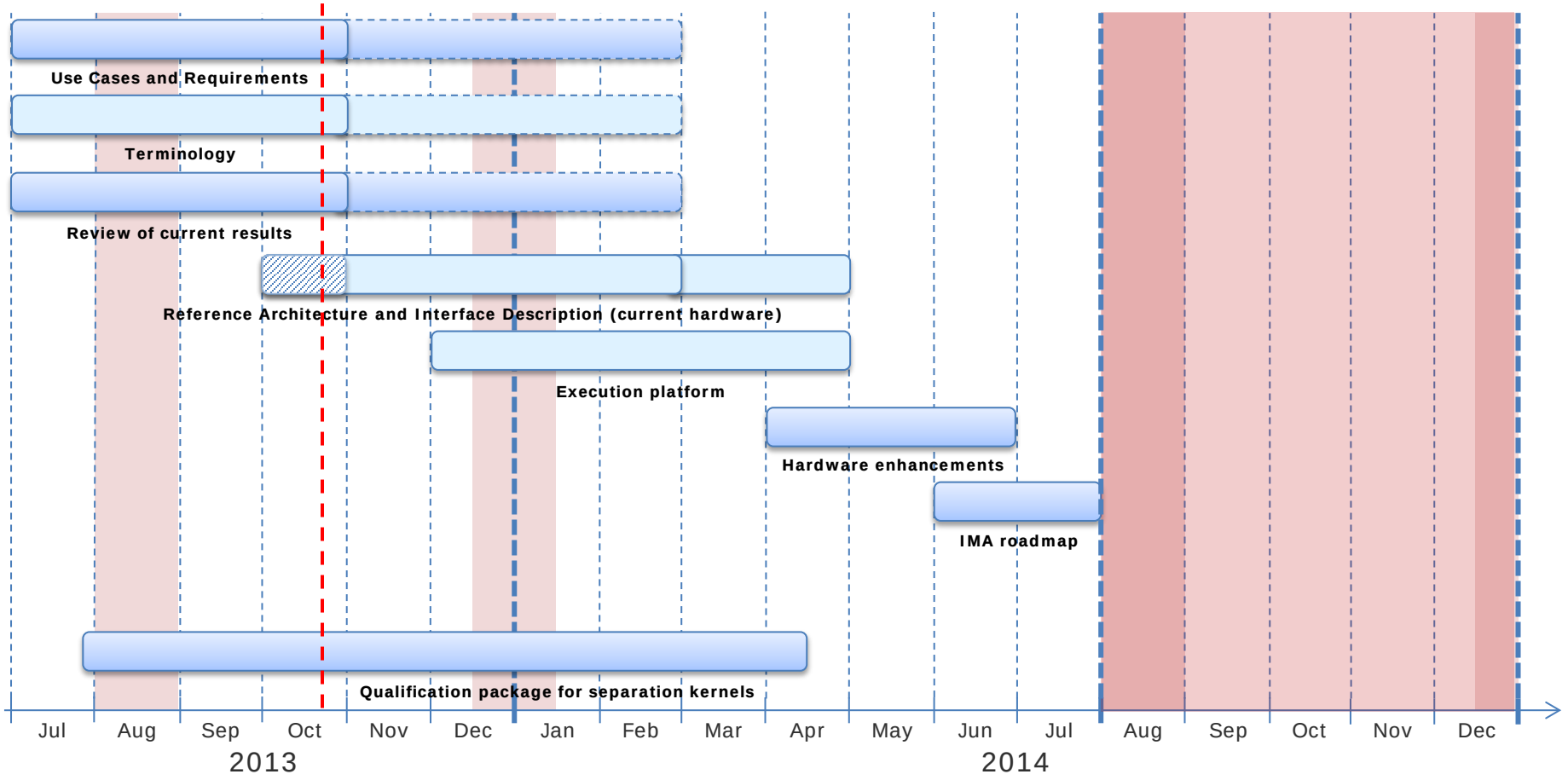
Martin.Hiller@esa.int

SAVOIR IMA

space avionics open interface architecture

BackupSlides

Activities and overall schedule



Status of IMA related activities (4/4)

Preparation for SEP Kernel Qualification package

- SoW in preparation,
- Objective: baseline Kernel Qualification Requirement, identify and assess V&V methods for partition kernel, define Verification and Validation strategy and plan, assess Candidate kernels conformance, perform Use case

SISTORA

Study on IMA Space – TSP in the OBSW Reference Architecture Context

- Initial study on how the OBSWRA and IMA-SP approaches could come together
  - Identifies a set of areas/topics for deeper analysis
  - Analyses overlap and potential conflicts
  - Proposes ways in which alignment can be achieved
- SAVOIR IMA WG has had the opportunity to review the results and provide feedback to the consortium
  - And was invited to the Mid-Term Review on September 11 and to the Final Review on October 9
- Final presentation in just a few minutes…
- Results are valuable input to definition of upcoming harmonization activities

Baseline HW perimeter

THIS SLIDE IS FROM THE SAVOIR IMA MEETING IN AUGUST AND NEEDS TO BE CHECKED AND/OR UPDATED!

- OBC
  - Processor: LEON3-FT
    - SCOC3
    - UT699
  - Plus the following OBC spec functions:

OBC functions	
Safe Guard Memory	Essential TC
Reconfiguration	Mission Data Links
Telecommand	Cmd & Ctrl Links
Platform TM	On Board Time
Platform Data Storage	PIO

- SpW network: SMCS332SpW and SpW-10X router
- 1553 bus
- UART (for debugging)

User Needs review

- Phase 1: Revisit the Benefits, Use Cases, Impact, and Features
  - Are they still valid?
  - Are they properly described?
  - How should they be prioritised?
  - Should anything be added?
- Phase 2: Revisit the high-level requirements and consolidate with IMA-SP results (where applicable).
- Phase 3: Review remaining TSP WG results
  - Differences between aeronautical and space domain
  - Implementation considerations
  - Ideas for evolving TSP

Avionics Time And Space Partitioning User Needs

Benefits

Impact

Use Cases

Features

Requirements

1. Integrating DMS, AOCS and other CFS functions on one OBC
2. Software development using multiple teams
3. OBCP development and management
4. Payload software development and integration in OBSW
5. Mission specific flight software
6. Guaranteeing on-board security in dual-use missions

1. Shared libraries
2. Publishing of on-board data through the on-board parameter database functionality
3. Access to CPU margin for sporadic and intensive computations
4. Guaranteed/assured access to I/O bandwidth
5. Execution of the same application code
6. Maintainability
7. Evolution
8. Flexibility of the design w.r.t. various functional modes

- 17 high-level user requirements

Qualification package for Separation kernel

Workshop organized spring 2013

- $\sim 30\ persons\ attended$

Topics addressed:

- What requirements to use for Qualification?
- What Qualification process to be used?
- Candidate Kernels status, AIR, PikeOS, XtratuM

R&D activity to address Qualification package preparation

- Requirements
- V&V methods for partition kernel
- Verification and Validation strategy and plan
- Candidate kernels conformance
- Use case