SAVOIR

space avionics open interface architecture

Software aspects of the reference architecture

J.L. Terraillon / A. Jung / J. Windsor
European Space Agency ESTEC

SAVOIRFAIRE

space avionics open interface architecture

Agenda

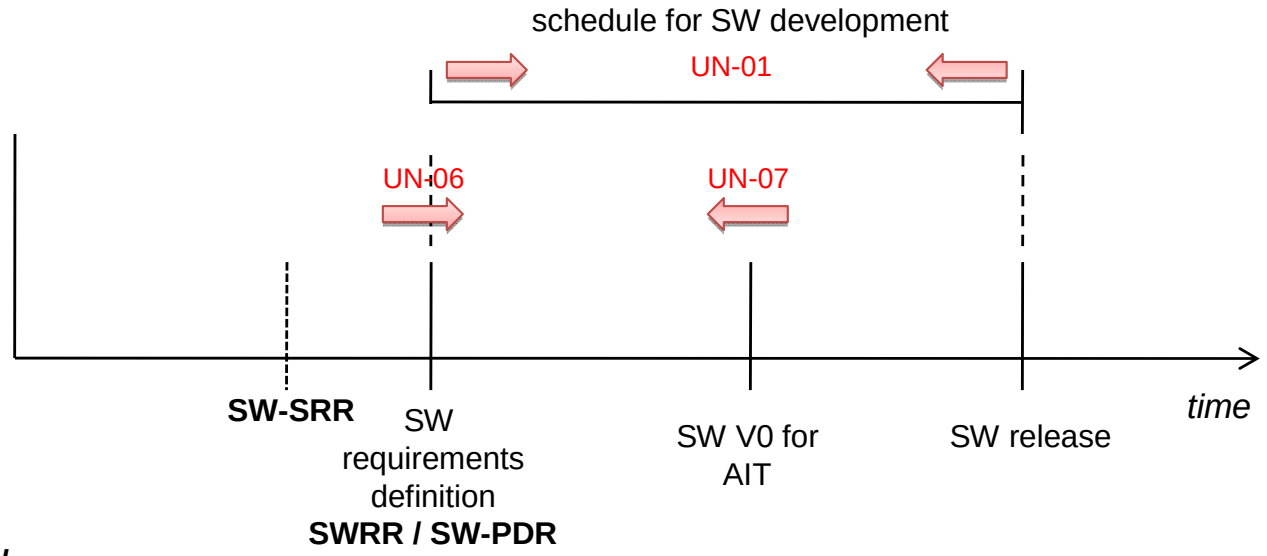
- [Recall] the software reference architecture: why and what?
- Supporting activities and status
- The IMA and Security dimension
- The configurable execution platform

Agenda

- **[Recall] the software reference architecture: why and what?**
- Supporting activities and status
- The IMA and Security dimension
- The configurable execution platform

On-board software schedule *issue*

The **schedule** for the software development is getting tighter:



Nevertheless:

Spacecraft platforms have **similar functionalities**. There are families of spacecrafts (for science, earth observation, …).

The **platform software is even more similar**… but currently, there are few opportunities to spend effort on advanced functions.

Software Engineering *needs:* Faster, Later, Softer

FASTER (increase productivity)

- Shorter software development time
- Reduce Verification and Validation effort
- Reduce recurring developments (don't redevelop recurring software: about 50% of platform sw)
- Increase cost-efficiency (more requirements same cost)
- Quality of the product (at least same quality)

LATER (increase reactivity)

- Mitigate the impact of late requirement definition or change
- Optimize flight maintenance
- Simplification and harmonization of FDIR

SOFTER (increase flexibility)

- Support for various system integration strategies (customer-supplier)
- Industrial policy support
- Role of software suppliers (multi-vendor policy)
- Dissemination activities (concept usable by system engineers)
- Future needs

Why a *reference architecture* reply to these needs?...

Faster? ➔ **automation of life cycle**, model driven engineering:

yes, but not enough…

Need also **predevelopment of software** for faster configuration, later configuration, softer developments (6 years, 6 months, …)

E.g. missionisation of launchers

Predevelopment of what? → Of **building blocks**

Are they Lego? → No, they are flexible (parameters)

Compose Building Blocks? → Therefore need **interface standard**

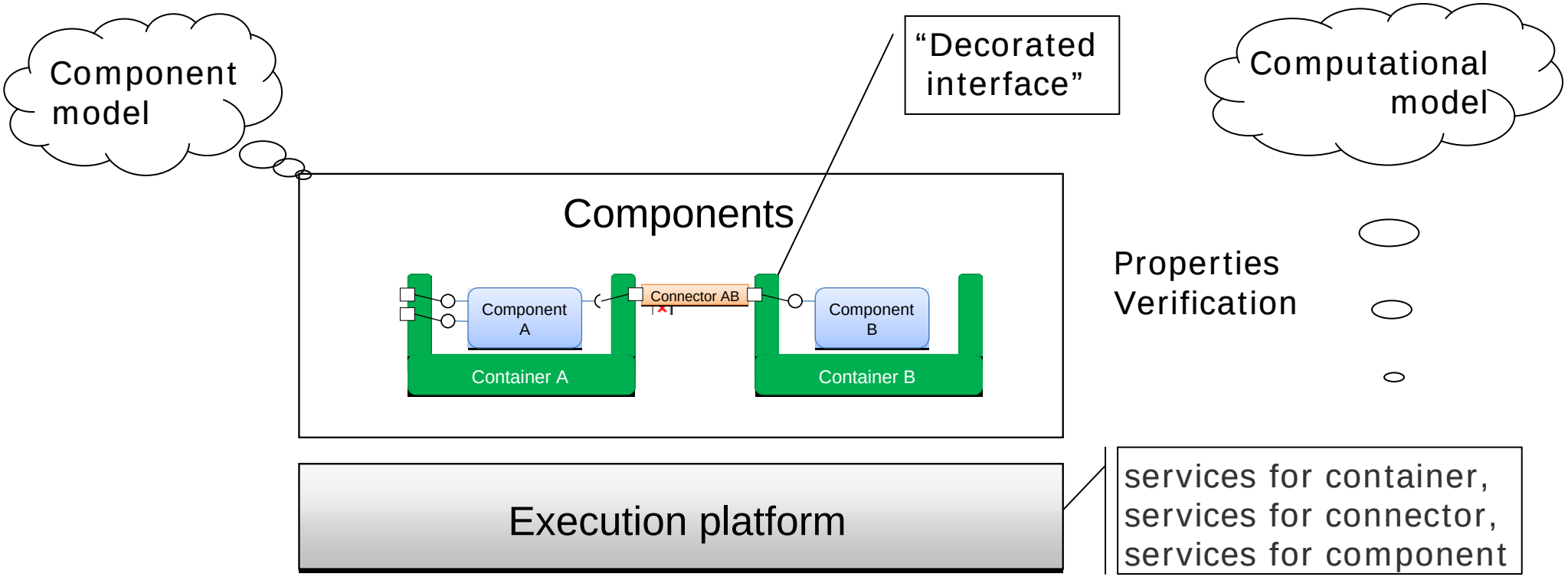
Where are the interface? → Therefore a **reference architecture**

Reduce validation? → Composability and compositionability,

Separation of concerns, correct by construction, component model

Reference architecture principles (1/2)

Architectural concepts: Component model (component + container + connector)

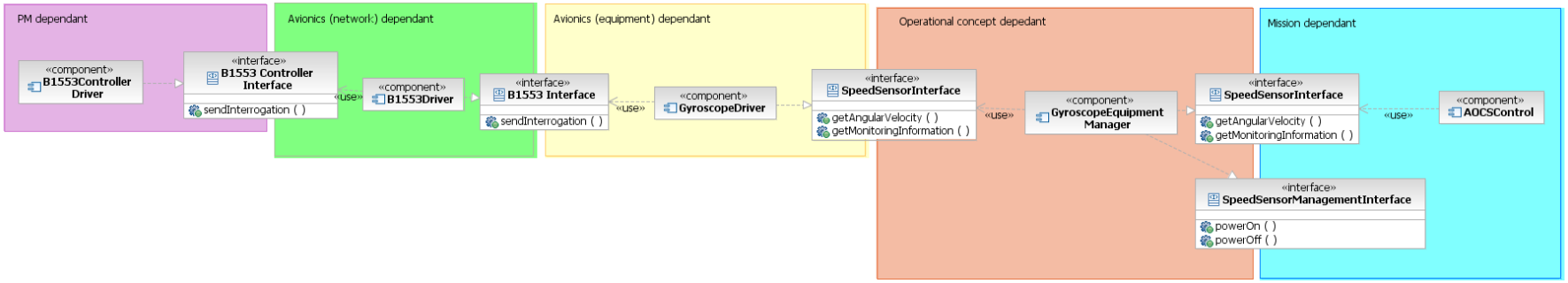


Reference architecture principles (2/2)

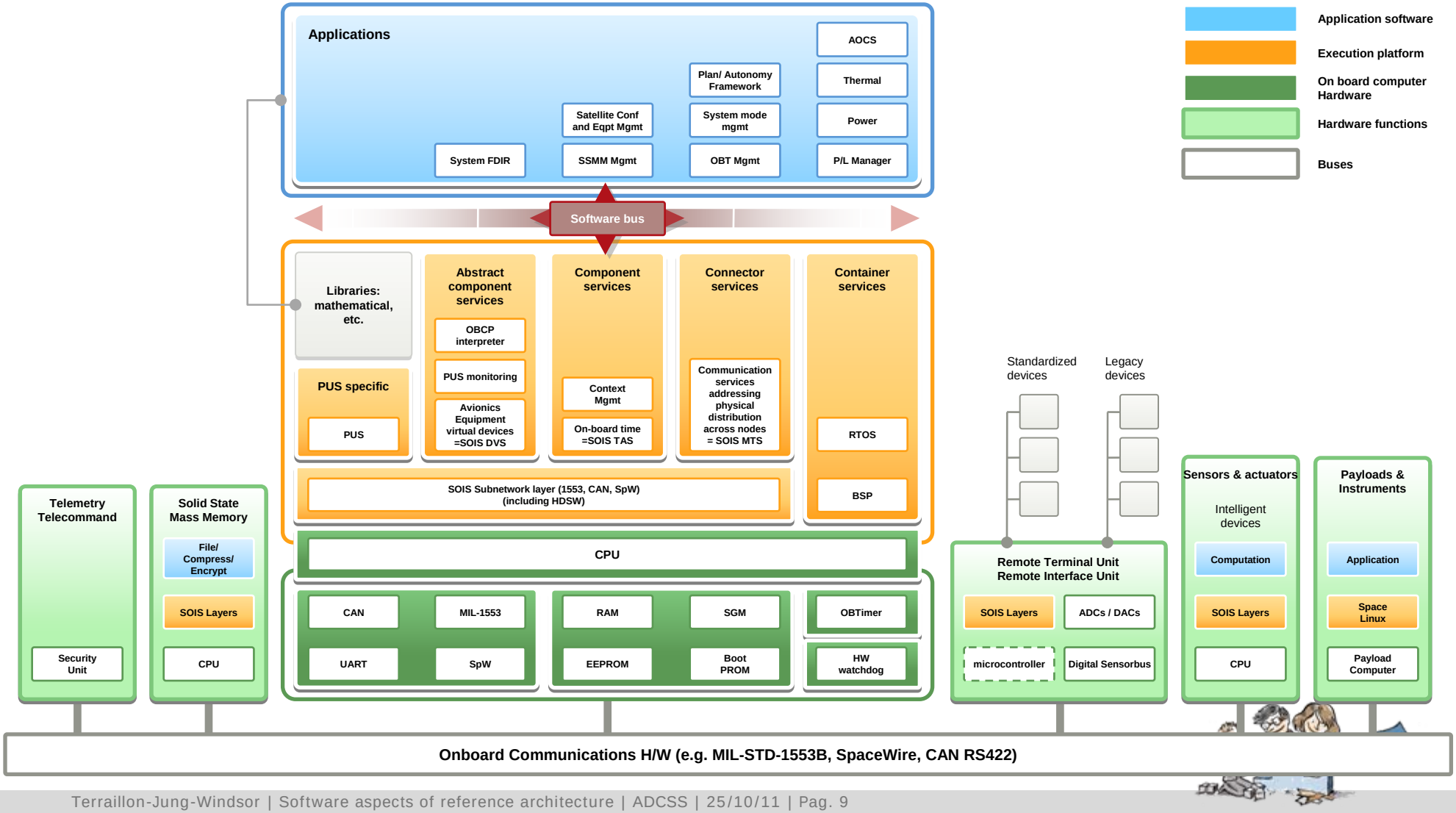
Mapping functional chains on the architectural concept

- Functional chain = AOCS, power management, thermal control
- **Domain engineering** to make functions **reusable** in a given domain
- **Variability factor** are used to describe the extend of flexibility of the domain.

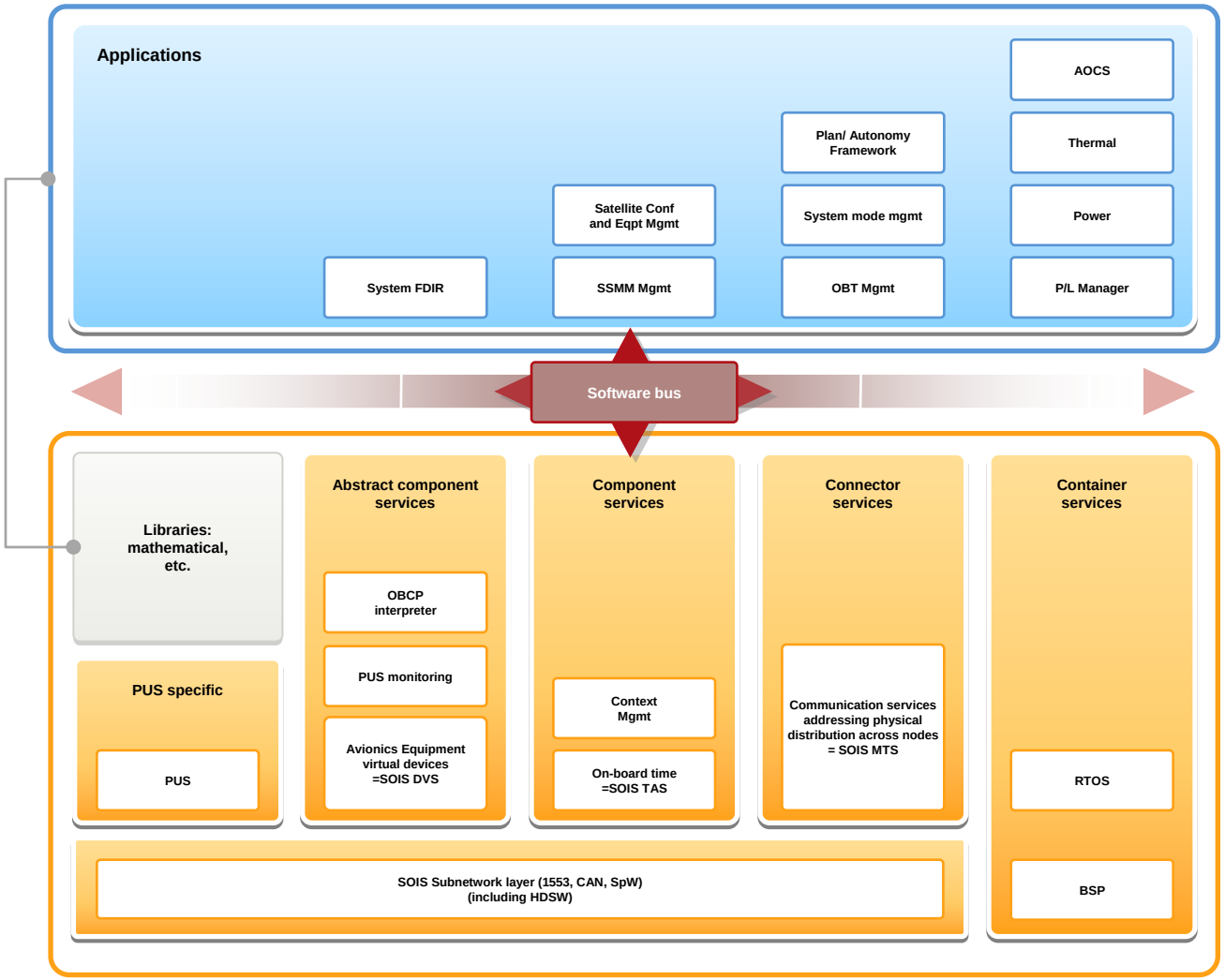
hardware | network | equipments | operation | mission



The avionics reference architecture (HW + SW)



The software reference architecture



Application level hosts the components of the functional chains

Software bus is a tool that generates the interaction layer between both

Execution platform hosts the services needed by the application (mediated through the interaction layer)

Agenda

- [Recall] the software reference architecture: why and what?
- **Supporting activities and status**
- The IMA and Security dimension
- The configurable execution platform

Supporting activities: Planning and Status

We are here!

SISTORA
Esa

IMA-SP
GSTP

SecPar
TRP

COrDeT-1A
completed – TRP

COrDeT-1A
completed – TRP

COrDeT-2
TRP

OSRA arch spec
(incl. Ex P/F IF)

OSRA
fct spec

DOMENG
completed – GSTP

Consolidation
Functional chains-A
GSTP

COrDeT
prototyping
TRP

AUTOSAR related
completed – TRP/GSTP

Consolidation
Functional chains-B
GSTP

SAVOIR
FAIRE

MBCODE
Danish return

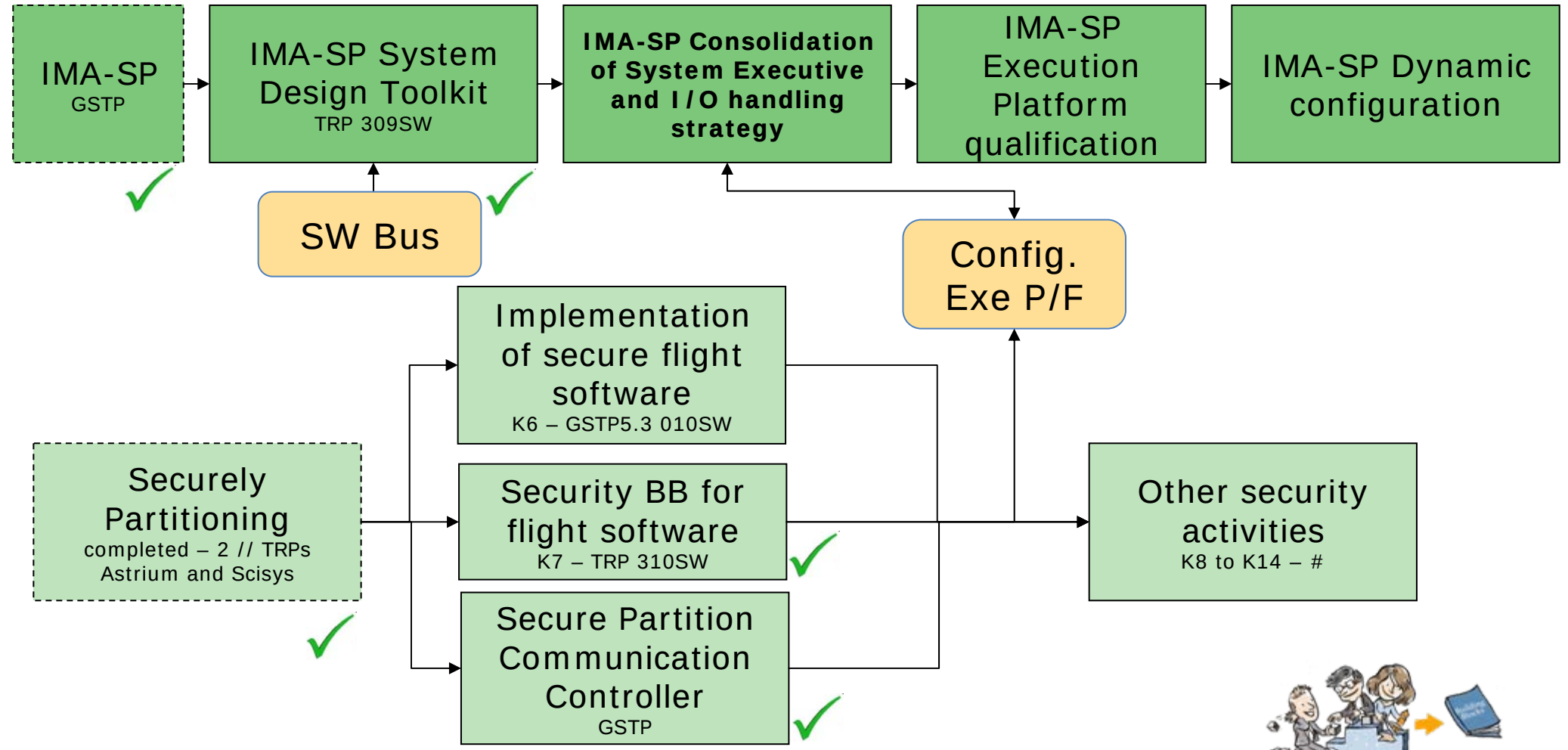
OBCP ref spec
GSTP

OBCP
ref spec

Agenda

- [Recall] the software reference architecture: why and what?
- Supporting activities and status
- **The IMA and Security dimension**
- The configurable execution platform

IMA and Security roadmap



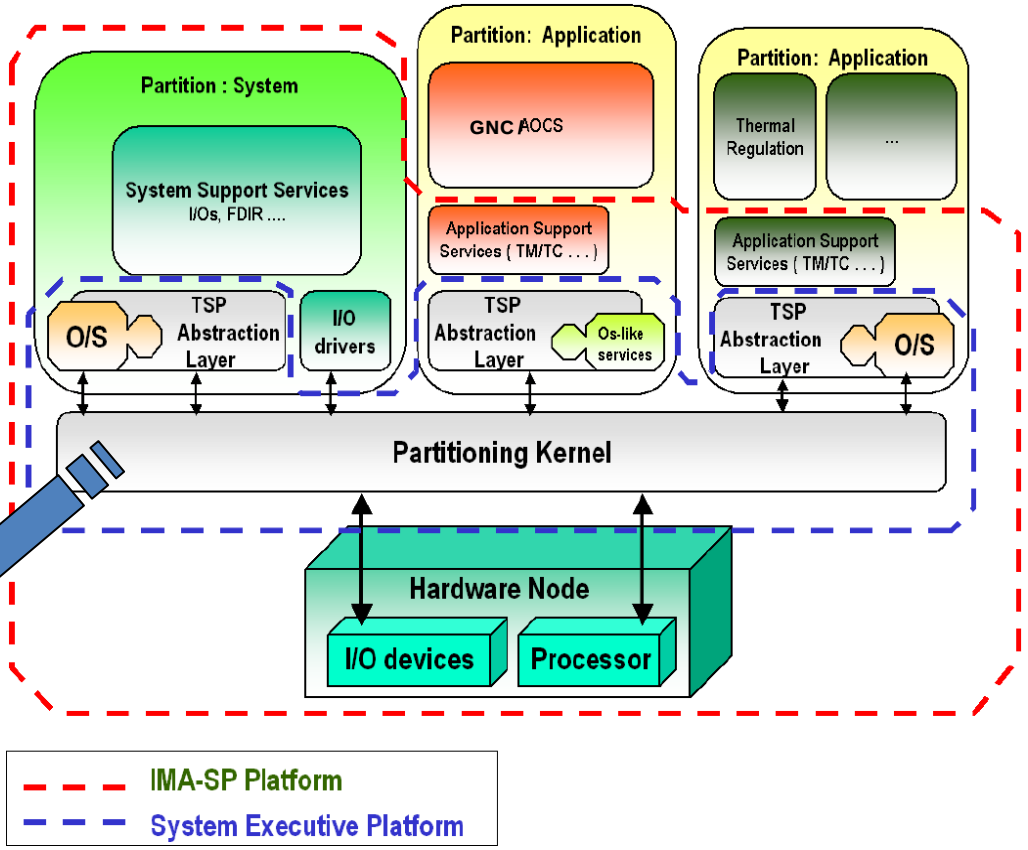
Status of IMA & Security

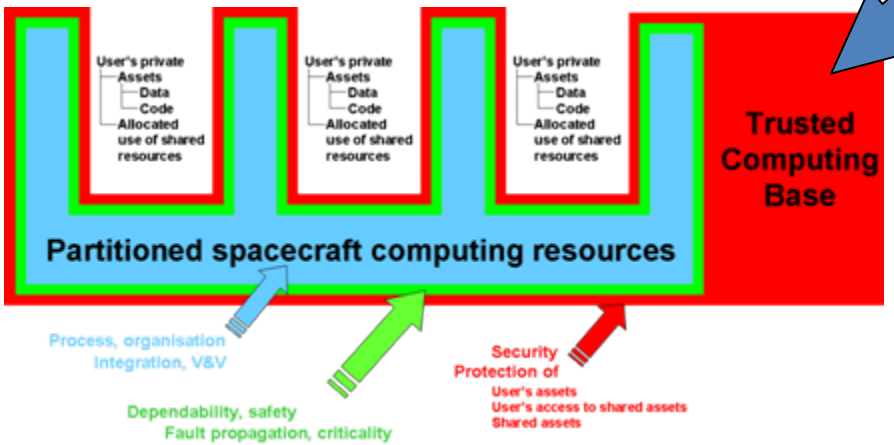
- IMA-SP and COrDeT compatibility shall be ensured via SISTORA
- Mapping of IMA-SP middleware to execution platform needs to be performed
  - Middleware services to be defined as part of IMA-SP use cases
- Security can be added via separation kernel into the Execution Platform
  - MILS and reduced trusted computing base concept
  - Security strategy needs to be defined (!)
- SAVOIR TSP Execution Platform **round table** on 26th January 2012 at ESTEC
  - Gather all TSP and Security stakeholders to coordinate ESA & non-ESA activities, report on roadmap progress, gain feedback from community and start the definition of future work
  - HW and SW focus

IMA-SP and Security architectures

The IMA-SP architecture consists of several layers

- System Executive Platform (SEP)
  - Partitioning kernel
  - TSP Abstraction Layer (~ ARINC 653)
  - Guest OS (optional)
- System support services
  - system middleware e.g. FDIR
- Application support services
  - application middleware e.g. TM/TC interface

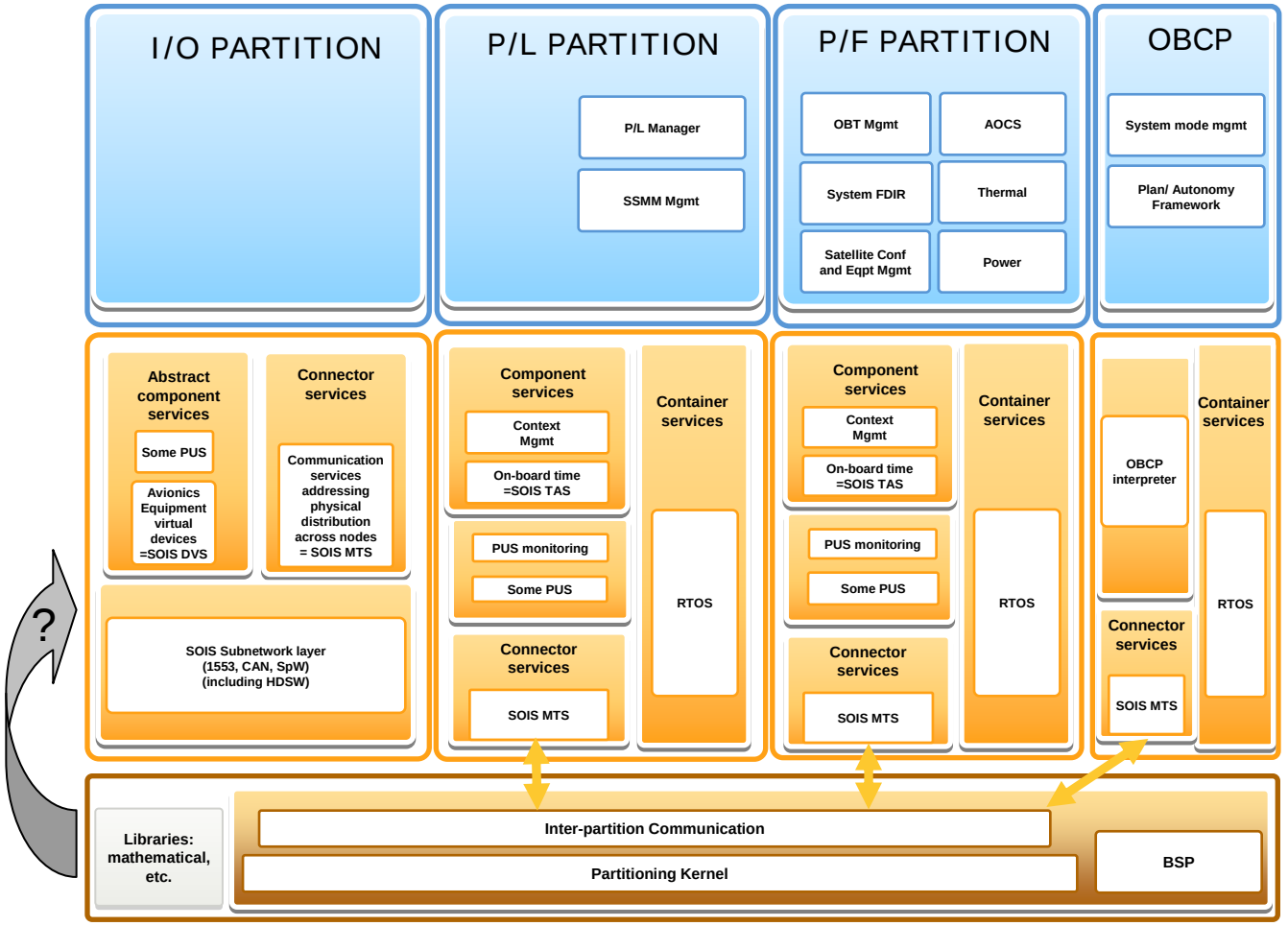




Agenda

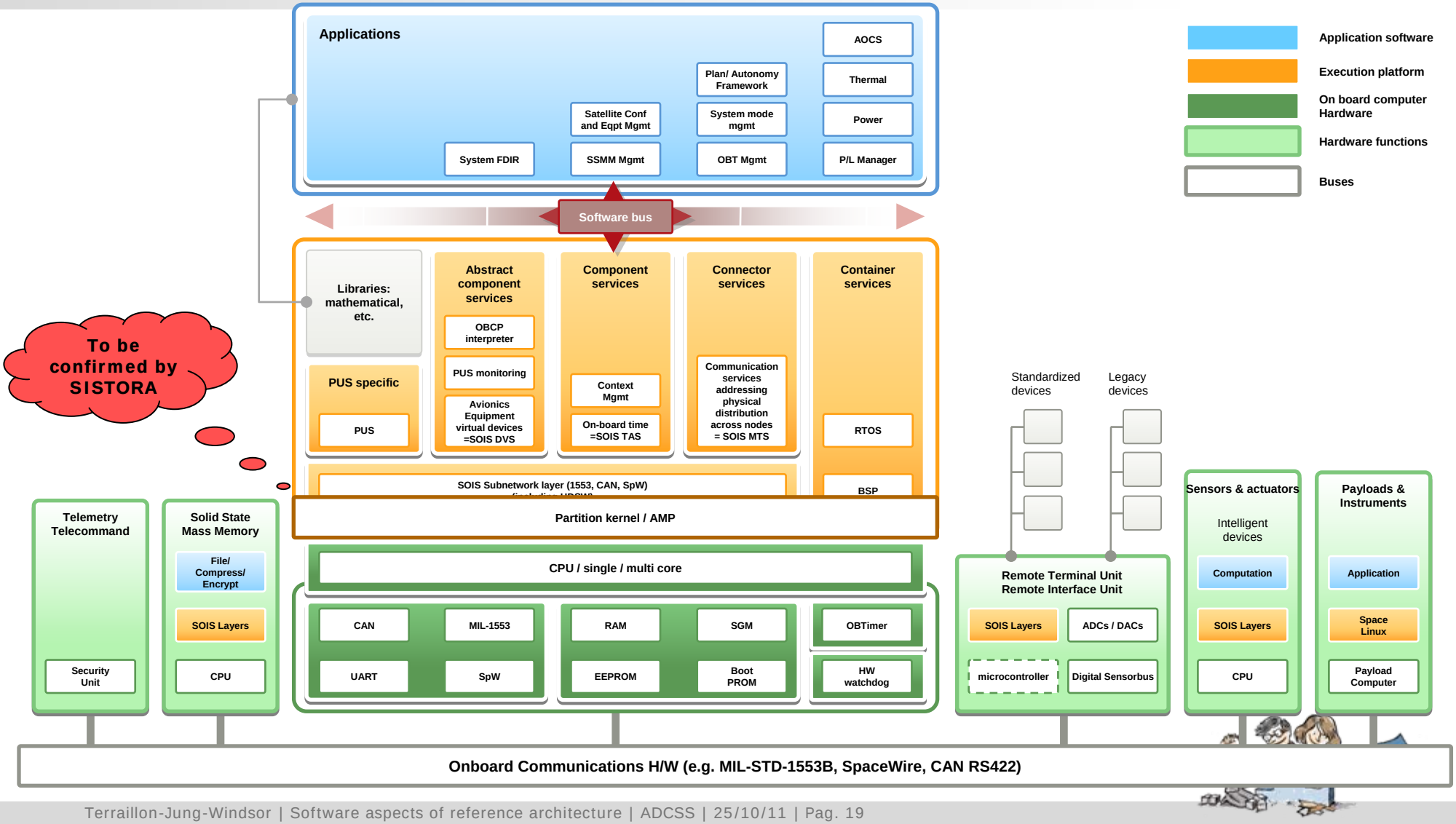
- [Recall] the software reference architecture: why and what?
- Supporting activities and status
- The IMA and Security dimension
- **The configurable execution platform**

The configurable execution platform



- A partitioning kernel schedules partitions
- Any OS (service for containers) can run in each partition
- Communication services (services for connectors) are in the I/O partition, only the API is in application partitions
- The SOIS MTS service must now include the inter partition communication mechanism of ARINC653
- Other services for components, and the application, are in other partitions
- Potential OBCP partition

The avionics reference architecture (HW + SW + TSP)



Contact

Feedback: savoir@esa.int