Avionics Embedded Systems Roadmap

- Goal related to SAVOIR

Jean-Loup Terraillon

TEC-SWE

Software Systems Engineering

ADCSS2010 - 2 November 2010

Mission Needs

Two types of missions considered:

- Operational earth observation, navigation, telecom and earth or space science missions, which constitute the large majority of European missions
  - keep under control the development schedule and cost while at the same time having sufficient flexibility to accommodate the requirements of each specific application.
  - improve the industrialisation of the development process of the platform and its subsystems.
  - The goal is to reduce schedule and costs
- Large, complex, technologically challenging missions like planetary exploration missions, involving robotics devises, rovers, and longer term missions like Darwin or Mars Sample Return or human exploration missions or Space Transportation as Long range transportation, supply of space station (ISS), Transition ATV to ARV
  - These missions are driven by technology maturity, critical performance and high reliability/availability during certain phases of the mission
  - The development process is driven by the complexity of the payload technology and must ensure that the design is implemented efficiently and qualified at an affordable cost
  - The goal is to enable future missions

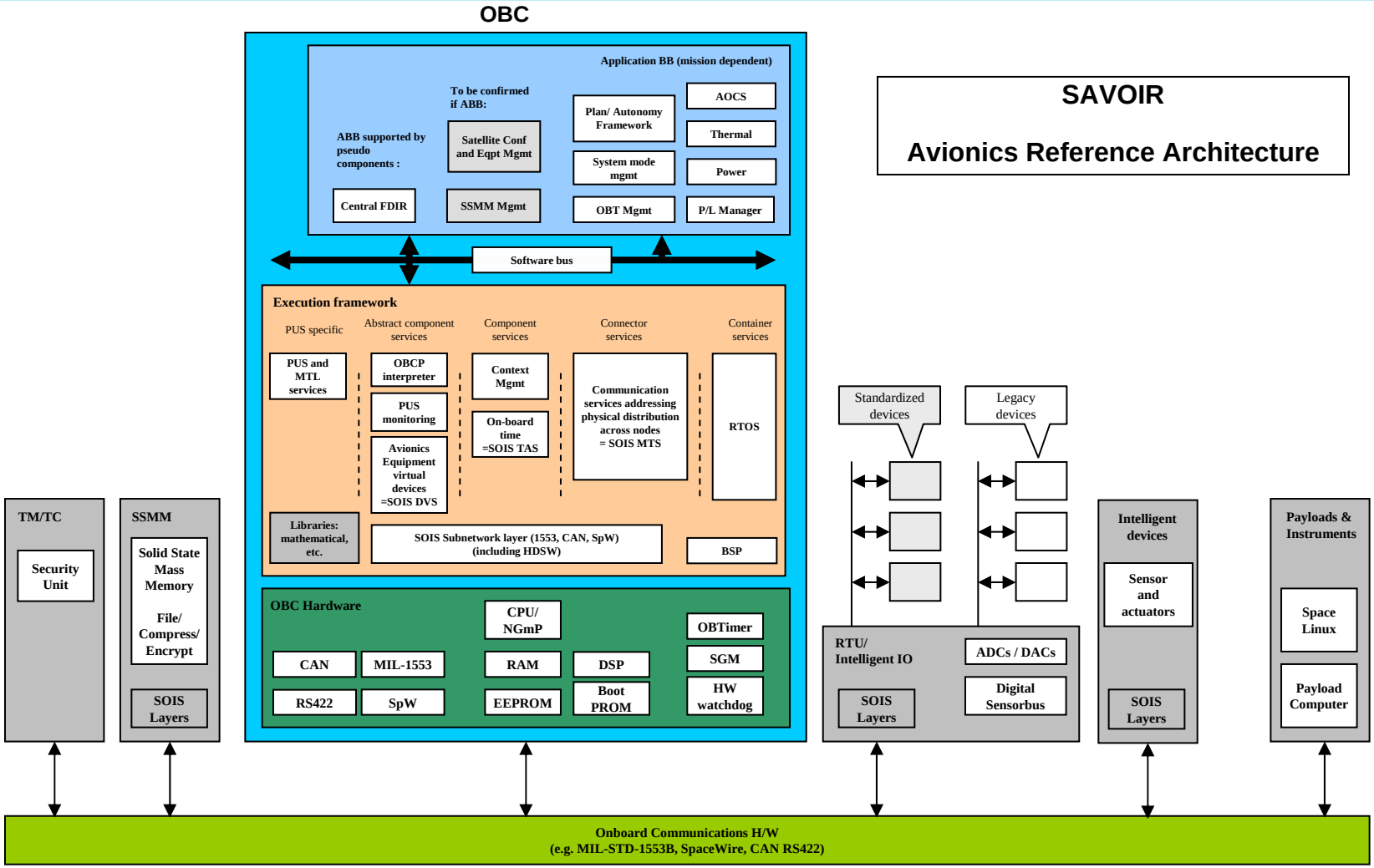
Proposed Development approach

1. **Goal 1 - Avionics Systems Architectures and Building Blocks**
   - **Aim A: Reference Architectures**
   - **Aim B: Building Blocks**
   - **Aim C: Interface Standardisation and Communication Protocols**
   - **Aim D: Integrated Modular Avionics**
   - **Aim E: COTS Embedded Systems**
   - **Aim F: Miniaturisation**

2. Goal 2 - Advanced Functions
   - Aim G: Autonomous Functions
   - Aim H: FDIR
   - Aim I: Distributed Command & Control
   - Aim J: Adaptive and Reconfigurable HW and systems
   - Aim K Security

3. Goal 3 - Avionics Development
   - Aim L: Model Based Systems Engineering
   - Aim M: System Software Co-engineering
   - Aim N: Hardware Software Co-Design
   - Aim O: Avionics Test Means
   - Aim P: Technology Demonstrators / Pilot Applications

Avionics Systems Architectures and Building Blocks



Proposed Development approach

Aim A: Reference Architectures

- A1 / A2 - Cordet prototype
- A3 - Avionics system reference architecture consolidation

  Refinement of SAG defined reference architecture: E2E requirements, Operations, FDIR, Security etc. Address interfaces to P/L, OBC, RTU, Security module, AOCS units etc
- A4 - AOCS Implementation on Avionics Reference Architecture

  AOCS implementation mapping on the avionics reference architecture definition: asynchronous execution of AOCS tasks, performance and robustness verification, centralised I/O unit for sensors data collection, AOCS application SW (buffer of time-stamped data). A first demonstration will be done on a simplified Real Time environment
- A5 - DHS Architecture Definition and Modelling

  As a concurrent complement to A3 at subsystem level, this activity is intended to define/refine a set of reference DHS architectures, model them and define suitable simulation tools for the longer term

Proposed Development approach

Aim A: Reference Architectures

- A6 - Payload Data Processing Architectures Definition and Modelling

  As a concurrent complement to A3 at subsystem level,this activity is intended to define/refine a set of reference Payload Data Processing Architectures, model them and define suitable simulation tools for the longer term.

- A7 - Avionics BB specification preparation

  Activity to support the work of the SAVOIR Advisory Group to produce high level specification of priority BBs and main interfaces

- A8 - Avionics Architecture Modelling Language

  Definition of a space profile on an existing commercial language a first phase should select the commercial tool and the space requirements demonstrate the validity of the tool by means of pilot application

- A9 - Innovative avionics for new generation launchers

  The purpose is to build an avionics demonstrator for future launchers, based on a precursor activity in the frame of FLPP;

Proposed Development approach

Aim B: Building Blocks

- B1 - SOIS Compliant Communication Library
- B2 - SOIS Compliant File and Packet Store Protocol Implementation
- B3 - Packet Utilisation Standard (PUS) library using SOIS services
- B4 - ECSS Compliant Modular RTU
- B5 - COTS Based general purpose Mass Memory

Proposed Development approach

Aim C: Interface Standardisation and Communication Protocols

- C1 - Software bus using PUS and SOIS
- C2 - RS-422 protocol standard definition and validation
- C3 - Interface Standardisation and Preparation

  Preparation of input to standardisation bodies from the harmonisation working groups and the reference architecture prototypes; Standardisation coordination, in particular providing the complete data model of the software, including the Assessment of SOIS/PUS for Databus at ESA, NSA and industry levels
- C4 - Standardisation of Digital Interfaces for Sensors (Temperature, Pressure, Position, Velocity, Acceleration)

Proposed Development approach

Aim D: Integrated Modular Avionics

- D1 - Integrated Modular Avionics for Space (IMA-SP)
- D2 - IMA-SP System design toolkit
- D3 - IMA-SP Consolidation of System Executive and I/O handling strategy
- D4 - IMA Executive platform qualification test suite
- D5 - IMA-SP Dynamic configuration

Proposed Development approach

Aim E: COTS Embedded Systems

- E1 - Qualification of COTS based modules/building blocks

  The development of On Board Computers for different types of applications (Fault Tolerant Computers, P/L processors, …) based on COTS CPUs is following a consolidated roadmap. The first step currently implemented is to derive Computer designs for three categories of applications; targeted to High-Availability, High-reliability and High Performance and validate them via a bread-boarding exercise. The second step which is the objective of this activity will be to raise the TRL of major BBs implemented in COTS based computers with special focus on the Processor module. Other aspects required for further qualification of these computers with be dealt with as well.

Proposed Development approach

Aim F: Miniaturisation

- F1 - Nano satellite AOCS bench top demonstrator
- F2 - Elements for miniaturised RTU implementation
- F3 - Miniaturised RTU Demonstrator
- F4 - Miniaturised re-entry black-box
- F5 - Adaptive system with 3D camera …

Schedule

	AIM A: Reference architectures	Priority Urg.	Crit.	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
A1	Cordet2 (existing)													
A2	Cordet prototype (planned)													
A3	Avionics system reference architecture consolidation	H	H											
A4	AOCS Implementation on Avionics Reference Architecture	M	H											
A5	DHS Architectures Definition and Modelling	H	H											
A6	Payload Data Processing Architectures Definition and Modelling	H	H											
A7	Avionics BB specification preparation	H	H											
A8	Avionics architecture modelling language	H	H											
A9	Innovative avionics for new generation launchers	M	H											
	AIM B: Building Blocks	**Priority Urg.**	**Crit.**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
B1	SOIS Compliant Communication Library	M	H											
B2	SOIS compliant File and packet store protocol implementation	M	H											
B3	Packet Utilisation Standard (PUS) library using SOIS services	M	H											
B4	ECSS compliant Modular RTU	H	H											
B5	COTS Based general purpose Mass Memory	M	M											
	AIM C: Interface Standardisation and Communication Protocols	**Priority Urg.**	**Crit.**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
C1	Software bus using PUS and SOIS	H	H											
C2	RS-422 protocol standard definition and validation	H	M											
C3	Interface standardisation preparation	H	M											
C4	Standardization of Digital Interfaces for Sensors (Temperature, Pressure, Position,Velocity, Acceleration)	H	M											
	AIM D: Integrated Modular Avionics	**Priority Urg.**	**Crit.**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
D1	Integrated Modular Avionics for Space	H	H											
D2	IMA-SP System design toolkit	M	H											
D3	IMA-SP Consolidation of System Excecutive and I/O handling stragety	M	H											
D4	IMA Executive platform qualification test suite	M	M											
D5	IMA-SP Dynamic configuration	L	L											
	AIM E: COTS Embedded Systems	**Priority Urg.**	**Crit.**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
E1	Qualification of COTS based modules/building blocks	H	M											

Costs

Activities A3 to A7 should be TRP/GSP since related to standardisation/harmonisation not product related

		Urg.	Crit.	Budget (kEuro) Approv.	Budget (kEuro) Add.	Approv. Prog.	Prop. Prog.	Proc. Policy Type	Proc. Policy Company	Remark	TRL level Curr.	TRL level Targ.	Date Start	Date End	ND	BB
	AIM A: Reference architectures															
A1	Cordet2 (existing)			490		TRP					3	4	2010	2011		
A2	Cordet prototype (planned)			350		GSTP					N/A	N/A	2010	2011		
A3	Avionics system reference architecture consolidation	H	H		300		GSTP	OC		Top level activity for SAVOIR Advisory Group	4	6	2012	2013		
A4	AOCS Implementation on Avionics Reference Architecture	M	H		300		GSTP	OC		to follow from A3 activity	4	6	2013	2014		
A5	DHS Architectures Definition and Modelling	H	H		250		GSTP	OC		to follow from A3 activity	4	6	2012	2013		
A6	Payload Data Processing Architectures Definition and Modelling	H	H		250		GSTP	OC		to follow from A3 activity	4	6	2012	2013		
A7	Avionics BB specification preparation	H	H		200		OTHER	RC		Support SAVOIR Advisory Group Activities	2	3	2011	2013		
A8	Avionics architecture modelling language	H	H		200		GSTP	OC			2	4	2011	2012		
A9	Innovative avionics for new generation launchers	M	H		800		OTHER	OC		FLPP	3	4	2011	2012		
	AIM B: Building Blocks															
B1	SOIS Compliant Communication Library	M	H		400		GSTP	OC			3	6	2012	2013		Y
B2	SOIS compliant File and packet store protocol implementation	M	H		300		GSTP	OC			3	5	2011	2013		Y
B3	Packet Utilisation Standard (PUS) library using SOIS services	M	H		300		GSTP	OC		Could start in TRP	2	5	2011	2012		Y
B4	ECSS compliant Modular RTU	H	H		600		GSTP	OC			4	6	2012	2013		Y
B5	COTS Based general purpose Mass Memory	M	M		250		GSTP	OC		Could start in TRP	2	5	1Q2011	1Q2012		Y

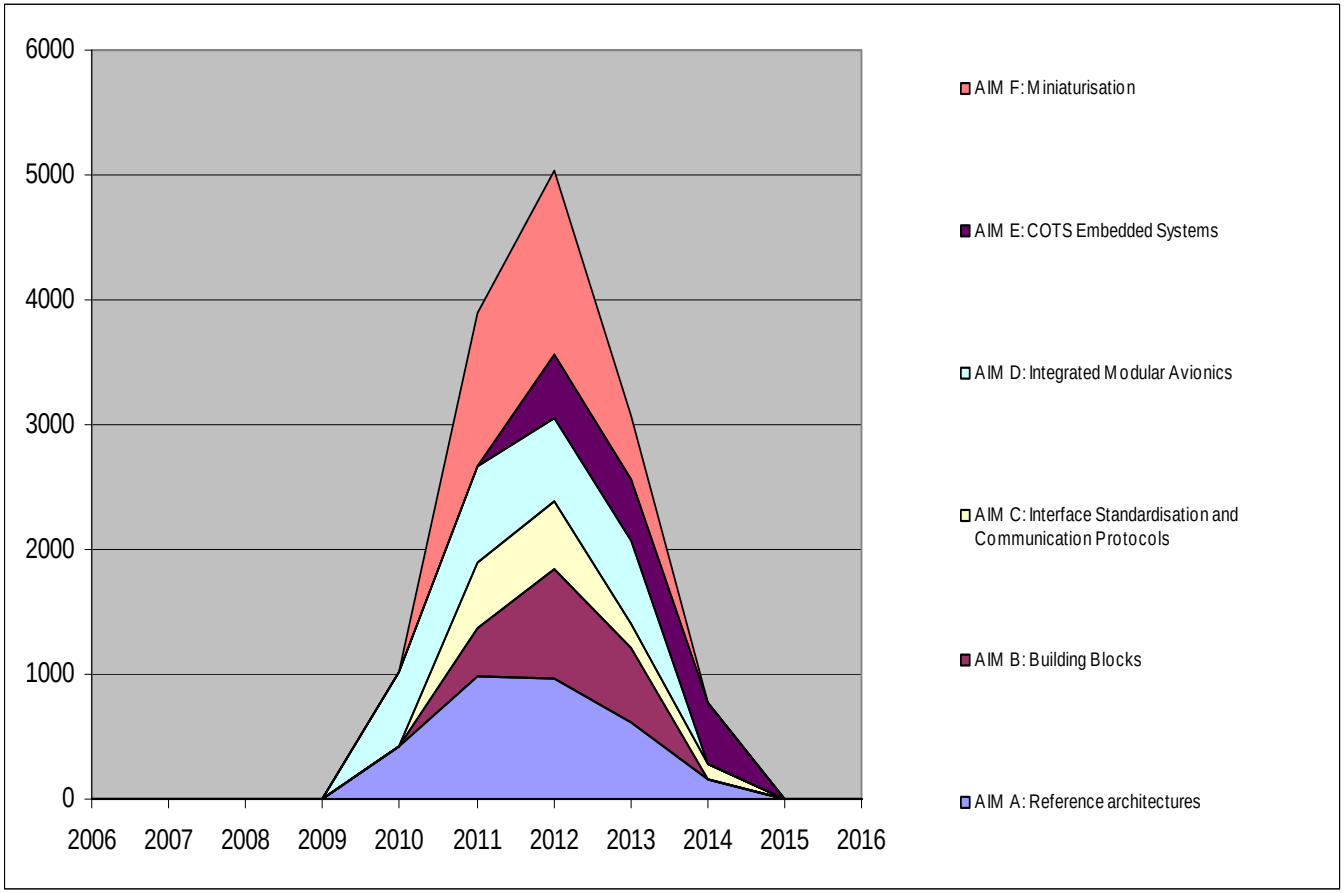
ESA should ensure (in the SOW) that all studies results on reference architectures can be used and are available to all stakeholders

Budgets for building blocks (AIM B) too low wrt target TRL

Costs

		Urg.	Crit.	Budget (kEuro) Approv.	Budget (kEuro) Add.	Approv. Prog.	Prop. Prog.	Proc. Policy Type	Proc. Policy Company	Remark	TRL level Curr.	TRL level Targ.	Date Start	Date End	ND	BB
	AIM C: Interface Standardisation and Communication Protocols															
C1	Software bus using PUS and SOIS	H	H		500		GSTP	OC			4	5	2011	2012		
C2	RS-422 protocol standard definition and validation	H	M		200		TRP	OC			N/A	N/A	2011	2012		
C3	Interface standardisation preparation	H	M		500		TRP	OC			N/A	N/A	2011	2014	N	
C4	Standardization of Digital Interfaces for Sensors (Temperature, Pressure, Position,Velocity, Acceleration)	H	M		200		TRP	OC			N/A	N/A	2011	2013	Y	
	AIM D: Integrated Modular Avionics															
D1	Integrated Modular Avionics for Space	H	H	1200		GSTP		OC			3	4	2010	2011		
D2	IMA-SP System design toolkit	M	H		400		TRP	OC			2	3	2012	2013		
D3	IMA-SP Consolidation of System Excecutive and I/O handling stragety	M	H		500		GSTP	OC			4	5	2011	2013		
D4	IMA Executive platform qualification test suite	M	M		350		GSTP	RC			4	6	2012	2013		
D5	IMA-SP Dynamic configuration	L	L		250		TRP	OC			1	3	2014	2015		
	AIM E: COTS Embedded Systems															
E1	Qualification of COTS based modules/building blocks	H	M		1500		GSTP	DN	AST-D, AST-F, TAS-I and potential other equipment suppliers		4	6	2012	2014	y	Y
	AIM F: Miniaturisation															
F1	Nano satellite AOCS bench top demonstrator	L	M		350		GSTP	OC			4	6	2011	2012		
F2	Elements for miniaturised RTU implementation	H	H		800		TRP	OC			3	5	2011	2012		
F3	Miniaturised RTU Demonstrator	M	M		400		TRP	OC			2	3	2012	2013		
F4	Miniaturised re-entry blac-box	H	H		700		GSTP	OC			3	7	2011	2012		
F5	Adaptive system with 3D camera ...	M	L		950		TRP	OC			2	3	2011	2013		

Costs


6000
5000
4000
3000
2000
1000
0
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
AIM F: Miniaturisation
AIM E: COTS Embedded Systems
AIM D: Integrated Modular Avionics
AIM C: Interface Standardisation and Communication Protocols
AIM B: Building Blocks
AIM A: Reference architectures

SAVOIR Advisory Group support activities

- A3
- ARAM

Proposed Development approach

Aim A: Reference Architectures

- A1 / A2 - Cordet prototype
- A3 - Avionics system reference architecture consolidation

  Refinement of SAG defined reference architecture: E2E requirements, Operations, FDIR, Security etc. Address interfaces to P/L, OBC, RTU, Security module, AOCS units etc
- A4 - AOCS Implementation on Avionics Reference Architecture

  AOCS implementation mapping on the avionics reference architecture definition: asynchronous execution of AOCS tasks, performance and robustness verification, centralised I/O unit for sensors data collection, AOCS application SW (buffer of time-stamped data). A first demonstration will be done on a simplified Real Time environment
- A5 - DHS Architecture Definition and Modelling

  As a concurrent complement to A3 at subsystem level, this activity is intended to define/refine a set of reference DHS architectures, model them and define suitable simulation tools for the longer term

A3:
Avionics system reference architecture consolidation

Refinement of SAG defined reference architecture: E2E requirements, Operations, FDIR, Security etc. Address interfaces to P/L, OBC, RTU, Security module, AOCS units etc

Scope and organisation

In his meeting of 17 June 2010, the SAG proposed the following activities to be performed as industrial activities:

- OBC functional requirements
- Payload interfacing (including data com, services).
- ECSS Tailoring, reference spec, tree of pointers on requirements
- Functional spec of the RTU
- Improve the way we represent the architecture (see modelling activity)
- Security interface
- FDIR
- Ground to Board interface
- Testing and validation building blocks

The work is organised as a Frame Contract with Call Off Orders.

1) Reference architecture consolidation coordination (RUAG)

- Management, consistency
- Meetings
- The SAG has produced a diagram of one reference architecture. This principle will remain the major assumption in the standardisation process. As such, the reference architecture will cover the maximum commonalities (at platform and payload interface level) of the considered missions (telecom, earth observation, science, etc).
- The result of the analysis will be a document describing the architecture, his domain of reuse, and its justification.

2) Functional architecture consolidation

- Define an intermediate level between the abstract reference architecture in PowerPoint and the physical architecture.
- Allows to define types of architecture which are independent from the physical decision of implementation
- Allows to use various building blocks in different physical architecture corresponding to the same functional architecture.

- Functional building blocks are:
  - OBC and RTU are the two fundamental building blocks that we start with.
  - The Mass Memory is the next important functional building blocks
  - TM/TC; security module; AOCS sensor/actuators;
- Use cases of the various configuration of physical topologies

3) Reference Ground/Board Interface specification

- The consortium will define, taking into account the ISIS initiative, the definition of ICDs in the ESA context, a reference ground/board interface specification (i.e. IRDs) (limited to the avionics).
- The consortium will analyze the impact of the interface definition on the reference architecture, the building blocks capabilities, the on-board communication (such as PUS and SOIS standards), and the software reference architecture.
- + ECSS context
- The activity will look at existing projects while foreseeing future needs.

4) Reference specification and OBC functional requirements

The long term objective will be

- to investigate which asset in the Avionics Compendium (to be found in [RD1]) can be subject to reference specification.
- to investigate in which way the specification can be “reference” or “generic”. This is linked to the domain of reuse in which the specification is valid.
- ECSS tailoring

Start with the case of the OBC functional requirements,

Define the domain of reuse of the OBC,

Establish list of functional requirements

Draft the external interface definition (electrical and hardware/software interface)

5) Payload interfacing

- This activity complements the CNES ISIS by extending the approach to the cover the data handling related interfaces between the platform and the payload.
- Prepare one or more architectures which cover the interfaces between platform and payload.
- the aspects of AIV should be addressed including the requirements for simulators,
- Derive a set of functional requirements “to the payload” and “for the platform”.
- For each functional interface identify the applicable ECSS standard to be applied.

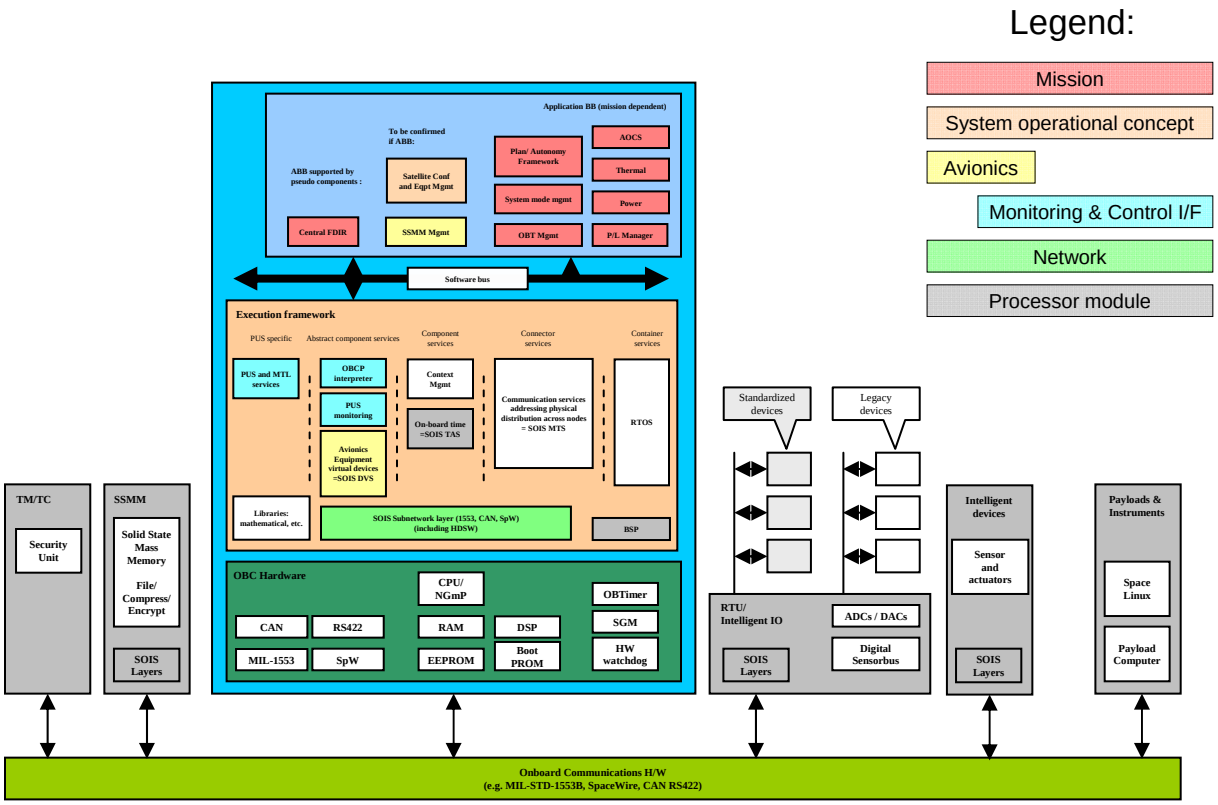
6) Mini RTU specification and interface definition

- The Contractor shall produce the specification and the interface definition of the mini RTU building block

ARAM

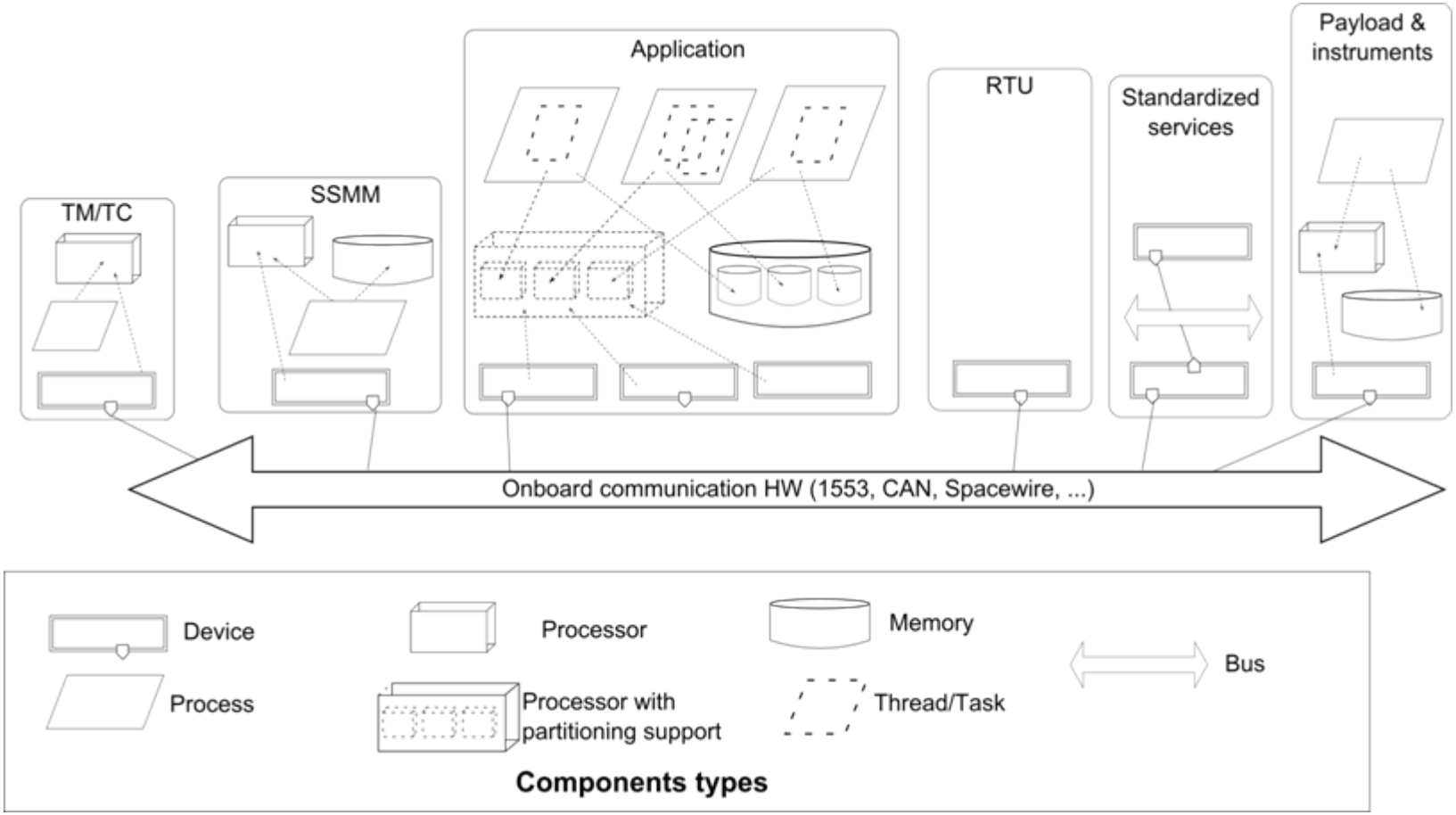
Avionics Reference Architecture Modelling

Avionics Architecture: Drawing

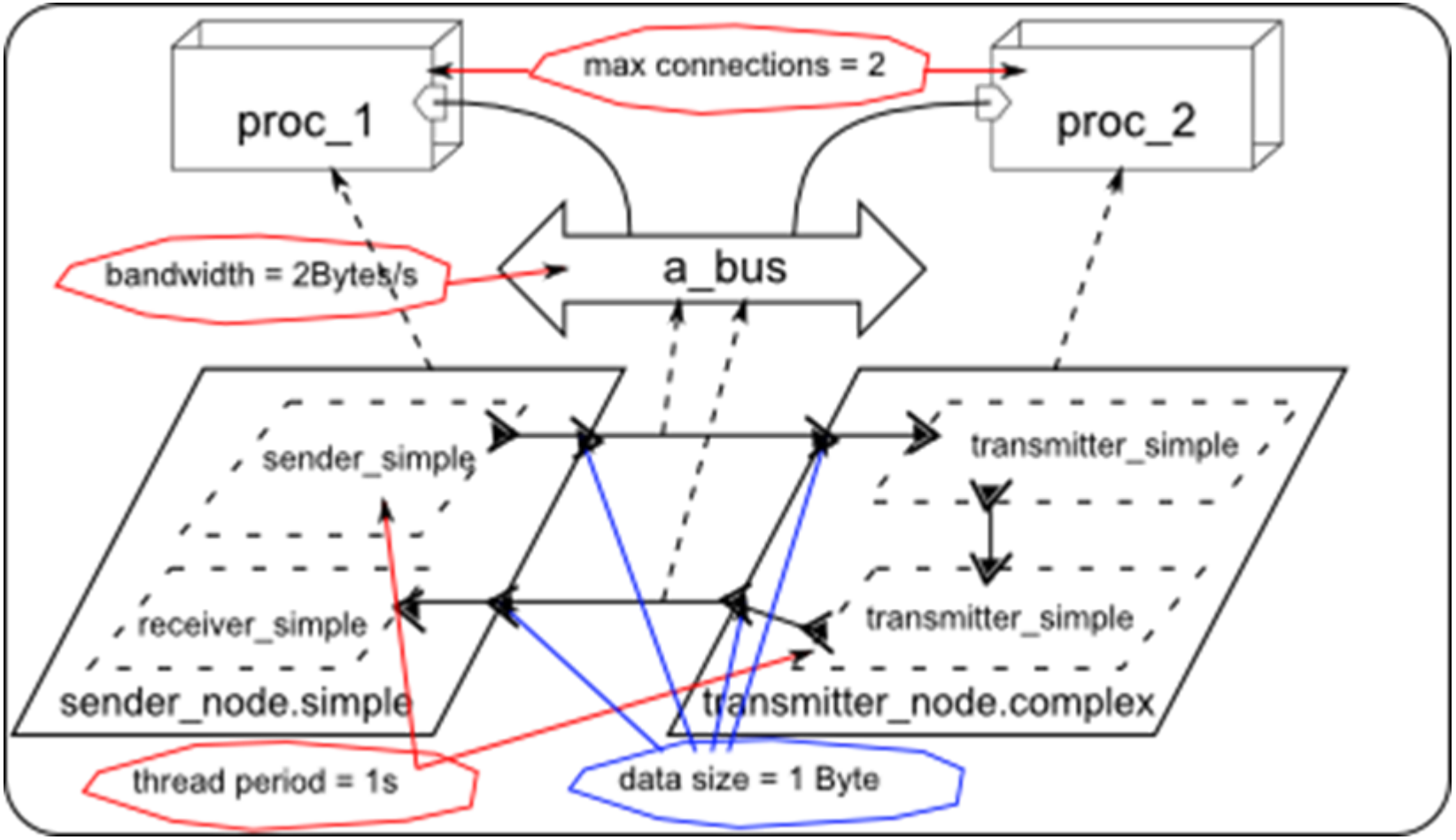


Avionics Architecture: Model

AADL: Architecture Analysis and Design Language



Example of parameters



Source code

```
data message
properties
  Data_Model::data_representation => integer;
  source_data_size => 1 Bytes;
  Deployment::Priority => 2;
end message;

subprogram transmit_message
features
  msg_in  : in parameter message;
  msg_out : out parameter message;
properties
  source_language => Ada95;
  source_name =>
"Repository.Transmit_Message";
  source_data_size => 1 Bytes;
  source_code_size => 1 KByte;
  source_stack_size => 3 KByte;
end transmit_message;

bus net
 properties
   Access_Bandwidth => 2 Bytesps;
end net;

bus implementation net.impl
end net.impl;
```

```
processor a_processor
properties
  RTOS_Properties::Max_Connections_Number =>
2;
end a_processor;

system shared
end shared;

system implementation shared.impl
subcomponents
  sn : process sender_node.simple;
  tr : process transmitter_node.complex;
  proc_1 : processor a_processor;
  proc_2 : processor a_processor;
  a_bus : bus net.impl;
connections
  cnx_1 : port sn.msg_out -> tr.msg_in;
  cnx_2 : port tr.msg_out -> sn.msg_in;
properties
  actual_processor_binding => (reference
(proc_1)) applies to sn;
  actual_processor_binding => (reference
(proc_2)) applies to tr;
  actual_connection_binding => (reference
(a_bus)) applies to cnx_1;
  actual_connection_binding => (reference
(a_bus)) applies to cnx_2;
end shared.impl;
```

Verification example: tool “Real”

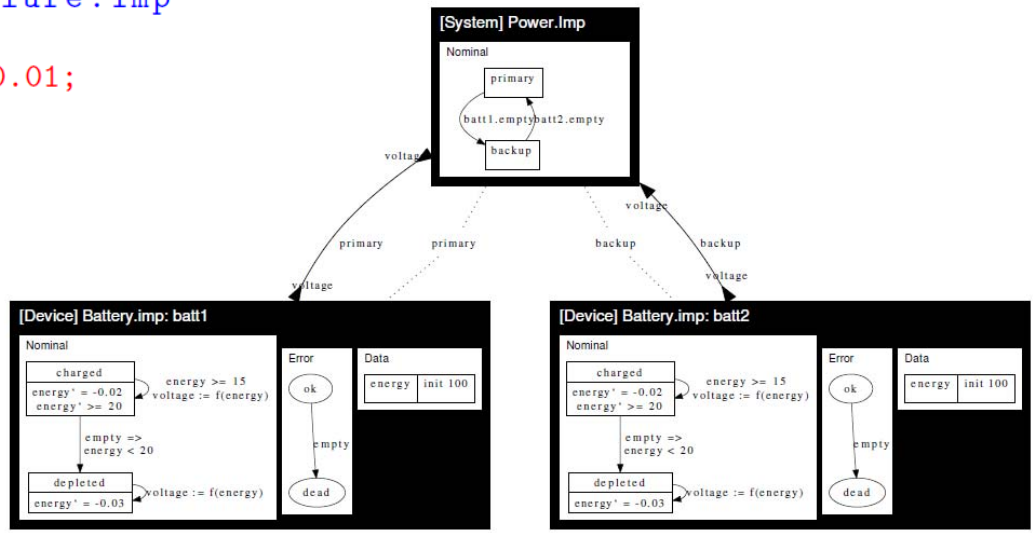
```
theorem Buses_Rate
foreach e in Bus_Set do

  Cnx_Set(e) := {x in Connection_Set | Is_Bound_To (x, e)};
  Connected_Data_Set :=
     {x in Data_Set | Is_Accessed_By (x, Cnx_Set)};

  check
   (Get_Property_Value (e, "Access_Bandwidth") >=
    Sum (Get_Property_Value (Connected_Data_Set, "source_data_size")));
end;
```

Verification example: tool “Compass”

```
error model implementation BatteryFailure.Imp
  events
    fault:  error event occurrence poisson 0.01;
  transitions
    ok -[fault]-> dead;
    dead -[batteryDied]-> dead;
end BatteryFailure.Imp;
```




```
system PowerSystem
  features
    voltage: out data port real;
    alarm: out data port bool initially false observable;
end PowerSystem;
```

```
transitions
  normal -[when voltage<4.5 then alarm:=true]-> critical;
  critical -[when voltage>5.5 then alarm:=false]-> normal;
```

AADL editors

- STOOD commercial from ElliDiss
- TOPCASED / ADELE open source from ElliDiss
- DIA/VISIO difficulty to generate anything out of the drawing
- OSATE open source (US) display, does not capture
- TASTE editor, ElliDiss, to be completed for Compass
- PAPYRUS editor