# Mixed criticality and partition systems

10th Workshop on Avionics, Data, Control and Software Systems
ESTEC, Noordwijk, The Netherlands

**A. Rossignol , HJ. Herpel, T. Planche Airbus Defence and Space**
**October, 19th, 2016**



AIRBUS
DEFENCE & SPACE

# Agenda

- Global context and some definitions
- Next Generation Execution Platform
  - IMA architecture
  - Hardware : Multicore, smart I/O Controller, Satellite Data Communication Network
  - IMA process
  - Secure partitioning architecture
- Synthesis for next step discussion





AIRBUS DEFENCE & SPACE

# Global context and some definitions

- Mixed criticality is first a System and Avionics need and not only computer / OBSW concern.

- Behind the term Mixed Criticality Systems we can find:
  - ECSS Levels A/B/C/D
  - Safety Critical vs Mission Critical
  - Failed-OPS vs Failed-SAFE
  - Applications and associated OBSW of different V&V maturity
  - Platform and Payalod Systems
  - Security requirements included in RAMS

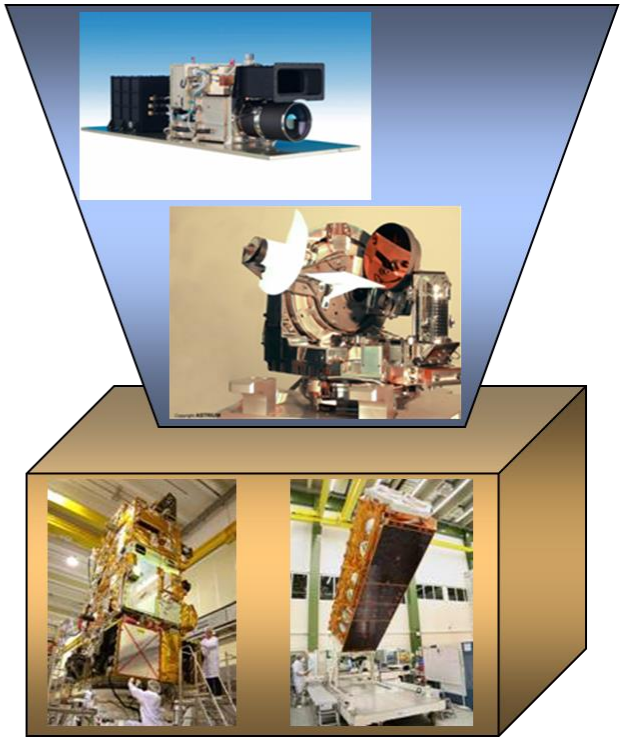
  ….

- Depending on type of mission and on the objectives above, several different gaps & solutions have to be identified and developed

- Payload Data Processing
  - Mission specific (instruments…)
  - Huge data volumes
  - Non-real time Data
  - High speed data links

**Performance For Payload**

**Reliability For Platform**



METOP Platform TERRASAR Platform

- Platform Command and control
  - Mostly generic
  - Low data volumes
  - Real-time constraints
  - Low speed data bus





AIRBUS DEFENCE & SPACE

# ECSS-E-30 Software Criticality levels

## *Defined by impact on the system*

| Criticality level | Definition |
|---|---|
| ***Level A*** | *Software whose anomalous behaviour would cause or contribute to a failure of the space system resulting in a **catastrophic** event: loss of life, of complete system,* |
| ***Level B*** | *Software whose anomalous behaviour would cause or contribute to a failure of the space system resulting in a **critical** event: major damage to flight systems,* |
| ***Level C*** | *Software whose anomalous behaviour would cause or contribute to a failure of the space system resulting in a **major** event: Temporary loss of satellite or ground facility not leading to a catastrophic or critical consequence;* |
| ***Level D*** | *Software whose anomalous behaviour would cause or contribute to a failure of the space system resulting in a **significant** event: Degradation of mission performances not leading to catastrophic / critical / major consequence* |
| ***Level E*** | *Software whose anomalous behaviour would cause or contribute to a failure of the space system resulting in a **negligible** event: all others* |

- ➔ ***Todays more or less all our applications and OBSW are Mission Critical B or C***
- ➔ ***Few differences at the end in the process/product development between B & C***
- ➔ ***A challenge could be to integrate some SW level D in the same computer !***





AIRBUS DEFENCE & SPACE

# Next Generation Execution Platform

## *Modular Avionics with Higher Integration*

**Object**: Onboard execution platform based on modular avionics.

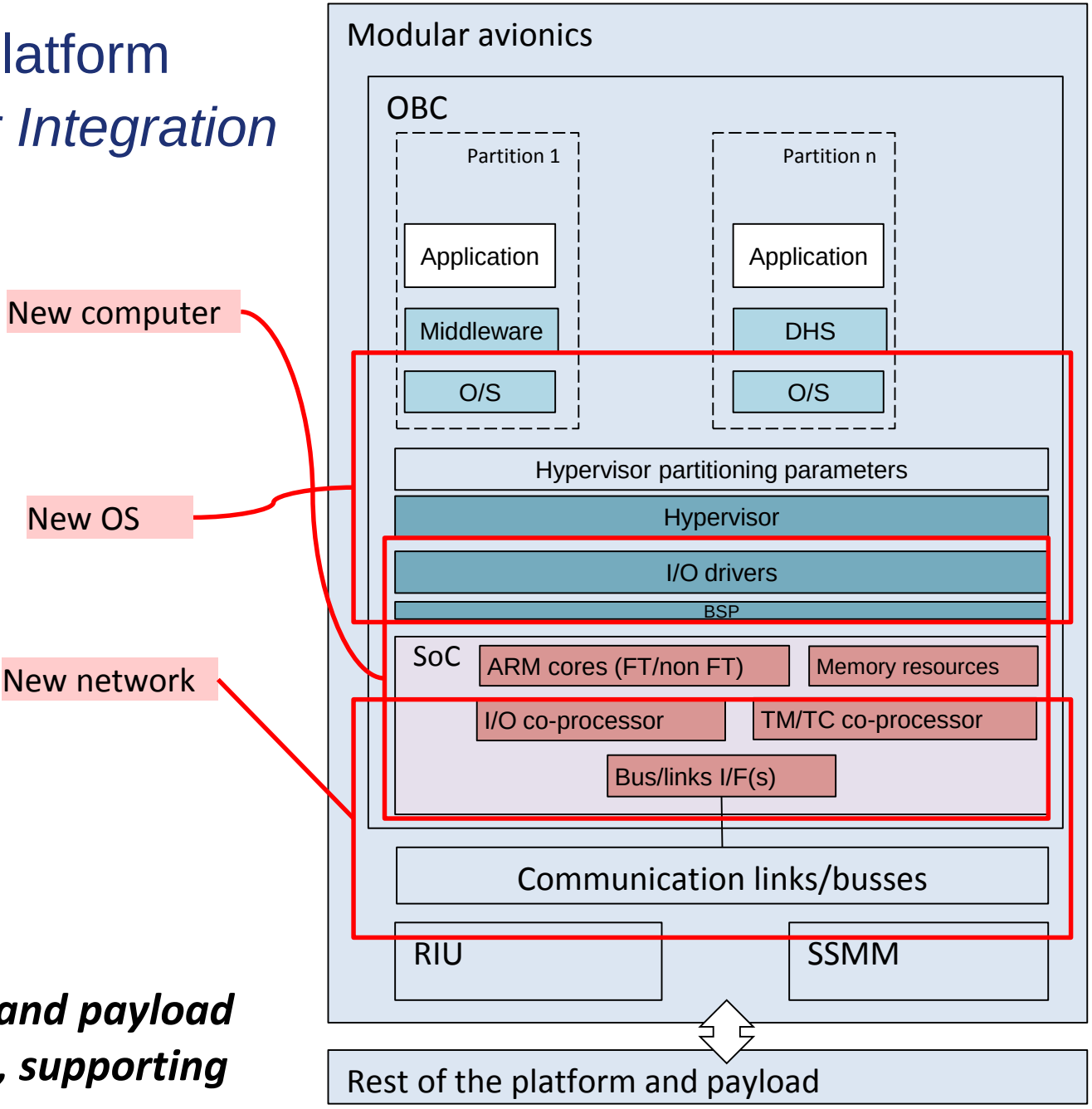
**Changes for computer**: SoC embeds multicore, ARM core, integrates an I/O processor and I/O interfaces (Spacewire, Ethernet…), ready for partitioning. New WCET methodology (pWCET).

**Changes for OS**: IMA concept. Provides shared resources to several hosted applications. Guaranties the partitioning of these applications.

**Changes to network**: new communication means for all platform. SpaceWire and Ethernet based media can be used.

**Changes to process and tools**: support IMA concept: parallel development, performance contract.

***For: higher integration of avionics and payload functions, cost and mass reduction, supporting new satellite missions and operations.***







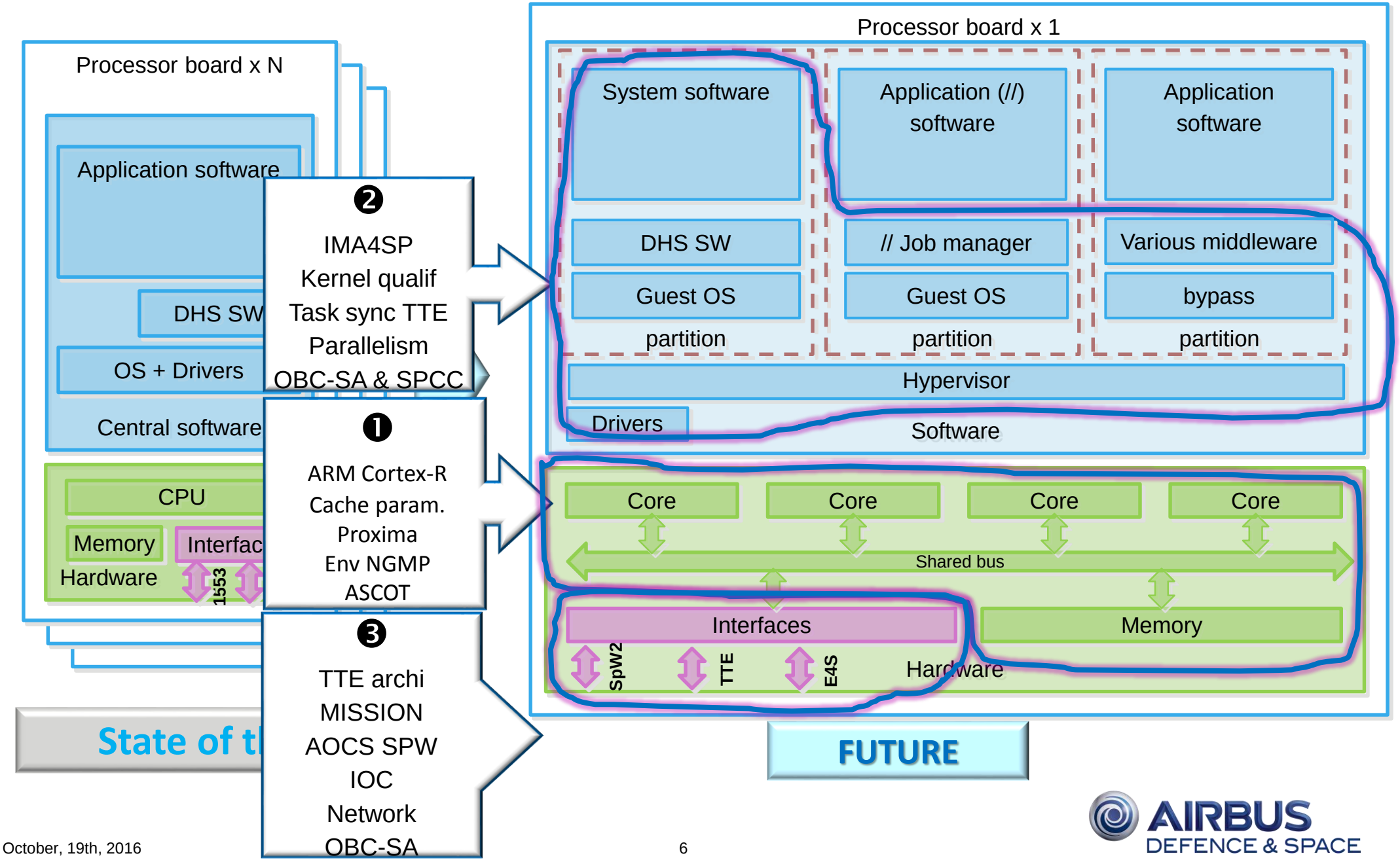

AIRBUS DEFENCE & SPACE

# Next Generation Execution Platform

## *Many recent and on-going studies are preparing*









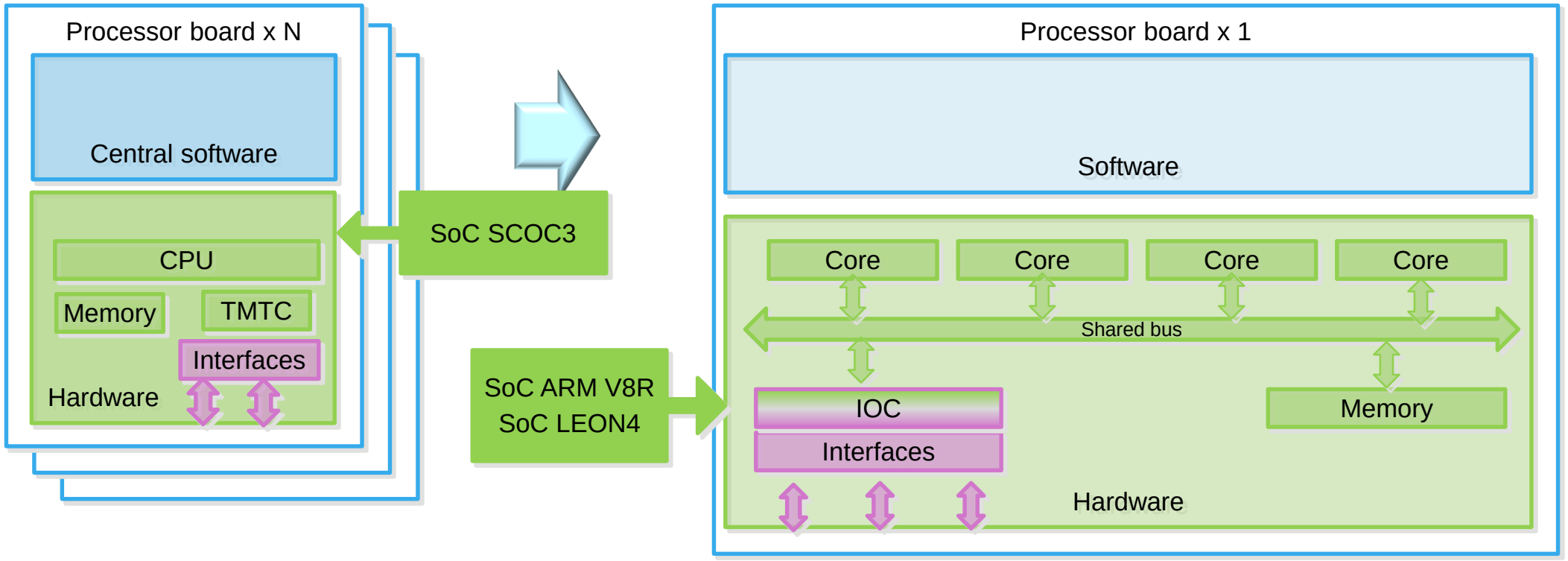

AIRBUS DEFENCE & SPACE

# Next Generation Execution Platform

## *Multicore processing concerns*








SCOC3: Rad-Hard, single core, SPARC architecture. TM/TC, SpW, 1553 interfaces.

2 alternatives:

GR740: Rad-Hard, quad-core LEON 4 SoC with Gaisler IPs

ARM: rad-tolerant and lockstep for SEUs, efficient, synthesizable, single or multicore, mature ecosystem (probes, GCC…)

Supported by:

**pWCET**: new approach for determinism demonstration

**Cache**: optimum cache parameter for spacecraft platform use case.



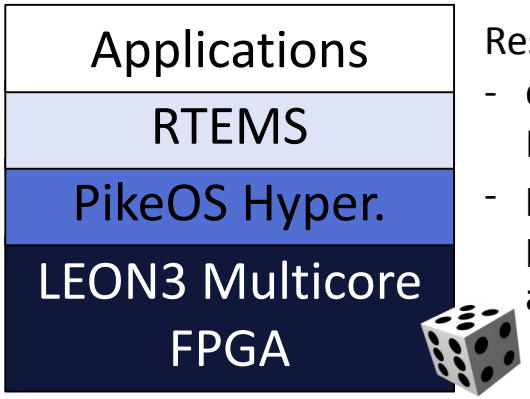
AIRBUS DEFENCE & SPACE

# Next Generation Execution Platform
## *Multicore processing concerns*
## *Probabilistic WCET and Proxima Project*

**Conclusion established at analysis time shall remain valid at deployment time !**

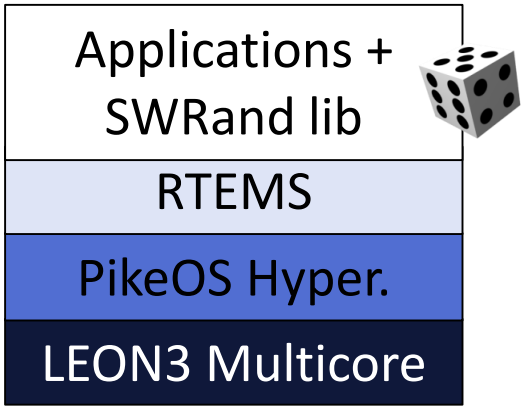
- **Impacts on execution platform** to control source of execution time variation
- **New tools** developed to support MBPTA analysis based on Rapita RVS industrial tool

***Hardware solution***




Response time is either made
- deterministic (**constant time** FPU operations)
- probabilistic (**random** cache policies, **random** bus arbitration)

***Software solution***




SW randomization consists in **randomly relocating functions** (instructions) and **padding stack frame** (data)

**On going activities, roadmap**:

- Roadmap for integration of MBPTA HW features
- Industrialization of SW randomization tools
- Need for a multicore interference model for ARM
- Discussion with agencies (ESA, CNES)

**Looking for ESA funding for follow-up on SW randomization**







AIRBUS DEFENCE & SPACE

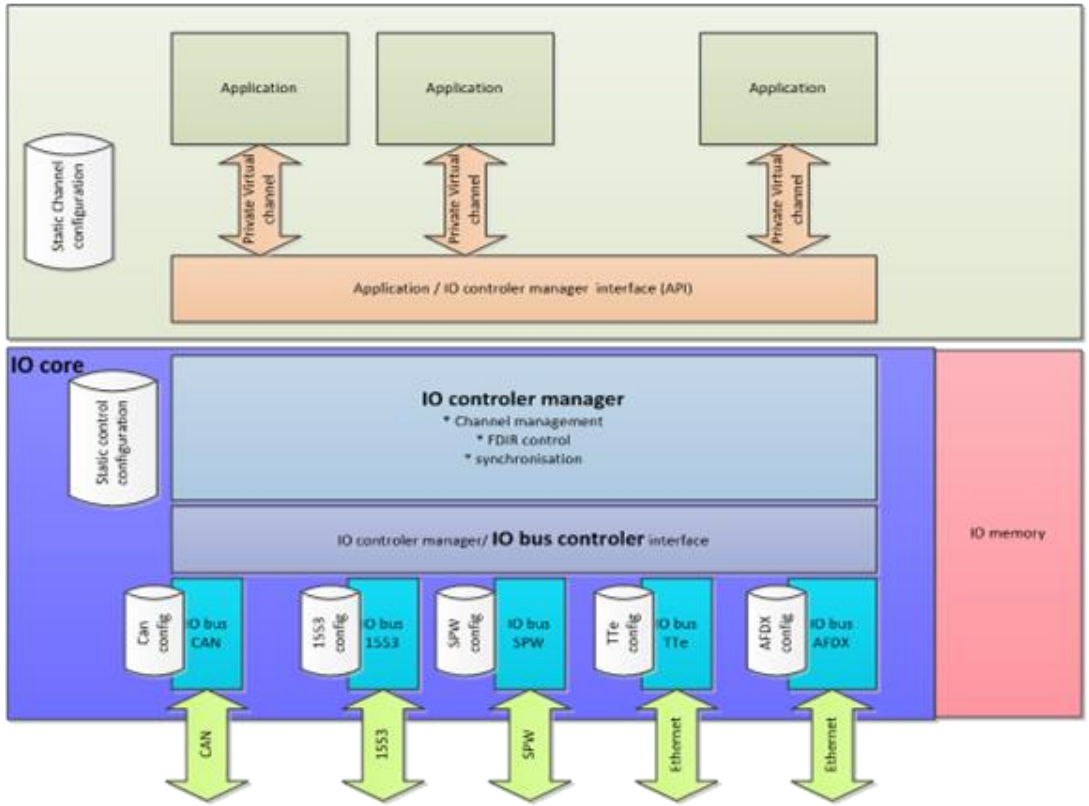
# Smart I/O Controller (study with CNES)

## *Use dedicated HW for IO management*

- *Management of the data flow*
- *Simplify application communications and interfaces levels (isolation, efficiency)*

## Concept: physical abstraction interface

- Time Partitioning: The application has no overhead to manage the physical communication interface. IOC acts as a coprocessor without intense support from applications.
- Space Partitioning: The IO controller enables the sharing of communication links by providing private channels (VC) dedicated to each partitions




**Virtual Channel** concept (I/O partitioning):

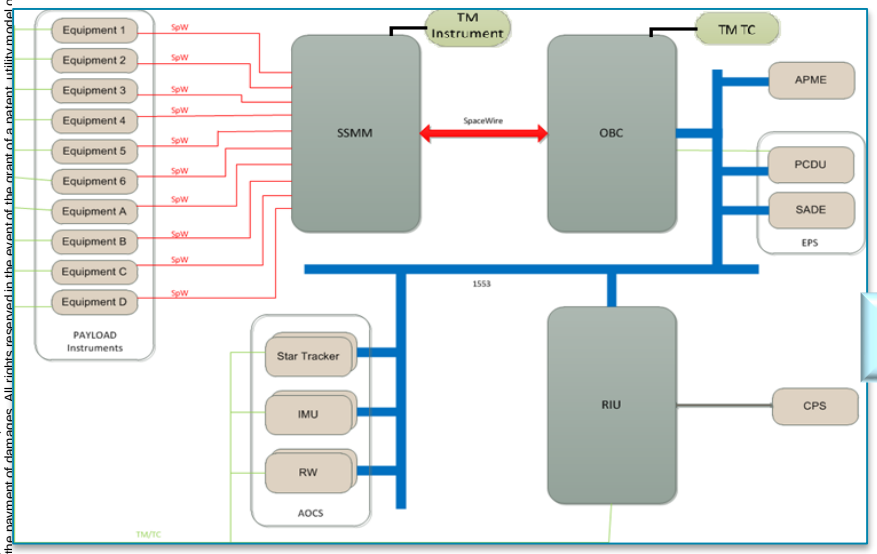
- ***Mixed criticality: Private VCs guaranteeing isolated routes from/to API to/from Physical layers***
- ***Mixed traffic support with high bandwidth and real time low latency (mixed QoS)***
- Sampling and Queuing buffer policies
- Allow shared multiplexed communication buses



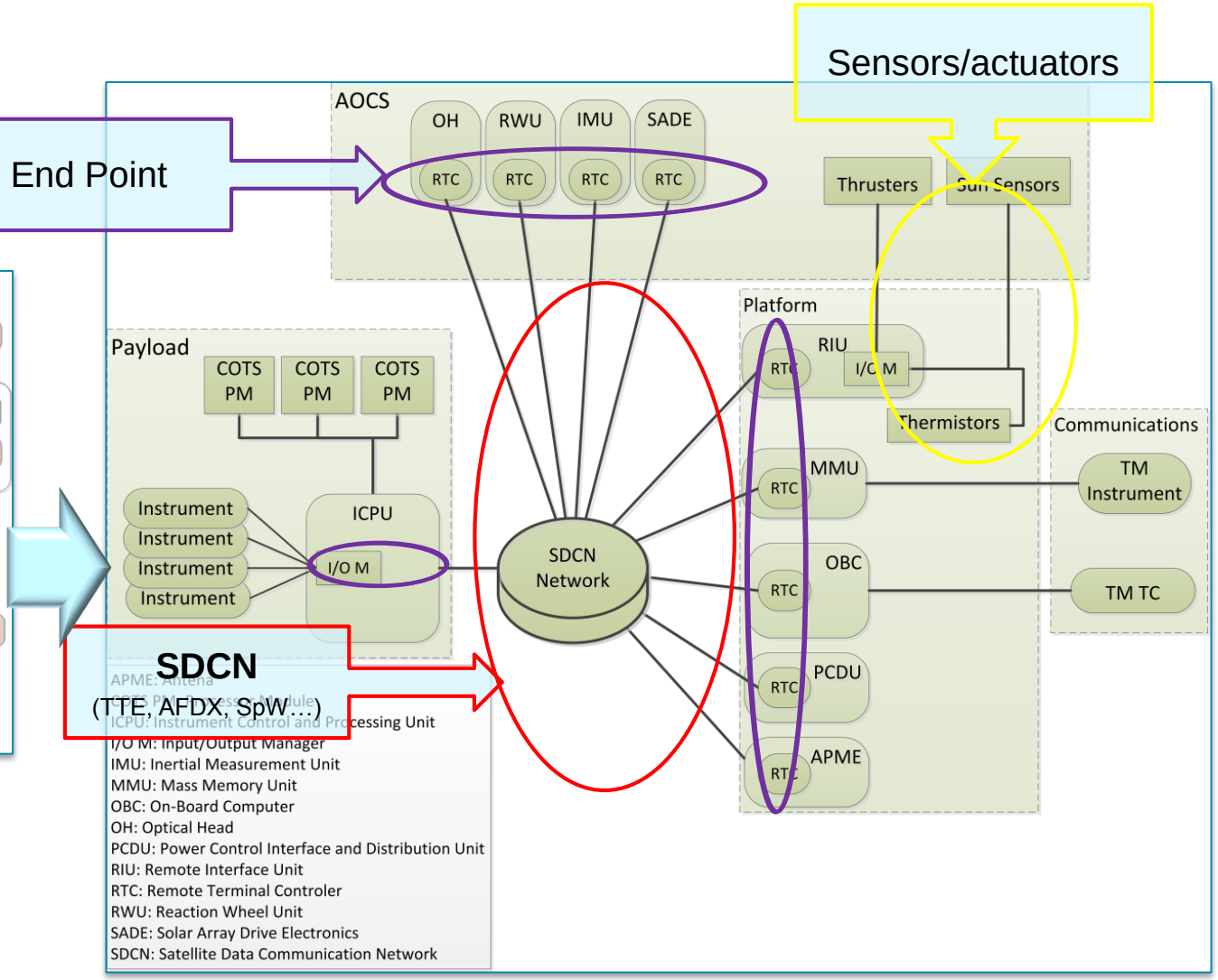


AIRBUS DEFENCE & SPACE

# Satellite Data Communication Network




State of the art








AIRBUS DEFENCE & SPACE

# Process: IMA process overview

## IMA process objectives:

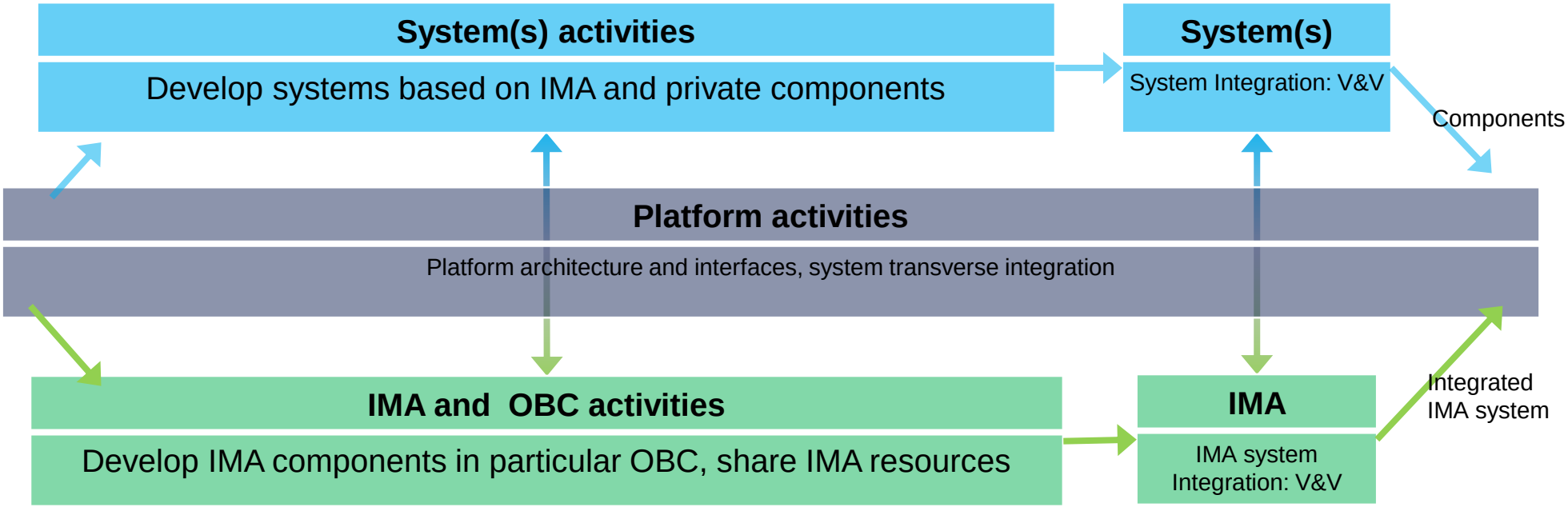
Support **independent system development**, qualification, update,

Support **independent computer platform** life cycle,

**New platform activities** to manage application and platform independent development: support spacecraft platform architecture, interfaces and systems transverse integration.

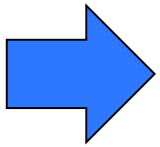
## IMA process properties:

Definition of tasks, roles, stakeholders, life cycle documents, supporting toolset



# Security Concerns

- SW Trends in Space
  - Security requirements (e.g. in commercial applications)
  - SW developed by third party / use of COTS
  - Operation of Space platform shared by various entities
  - Use of low-cost service
  - Downgrading of data quality
- Reference scenarios
  - Multi-use missions
  - Payloads from different stakeholders
  - Integrated Modular Avionics



- Security objectives
  - Safe boot (no corruption of boot sequence or detection)
  - Data confidentiality/integrity/authentication
  - Observability
  - Compatibility with operational phases (e.g. FDIR, maintenance)
  - Control of resources (including CPU time, RAM, I/O, devices)
  - Prevent from error propagation, data leaks, covert/side channels
- Security Threats
  - Tampering with software (malware injection)
  - Equipment/Software malfunction
  - Saturation of the information system
  - Unauthorized use of equipment
  - Corruption or interception of data (i.e. encryption keys)
  - Illegal processing + abuse/forcing of rights
  - Error injection + denial of service

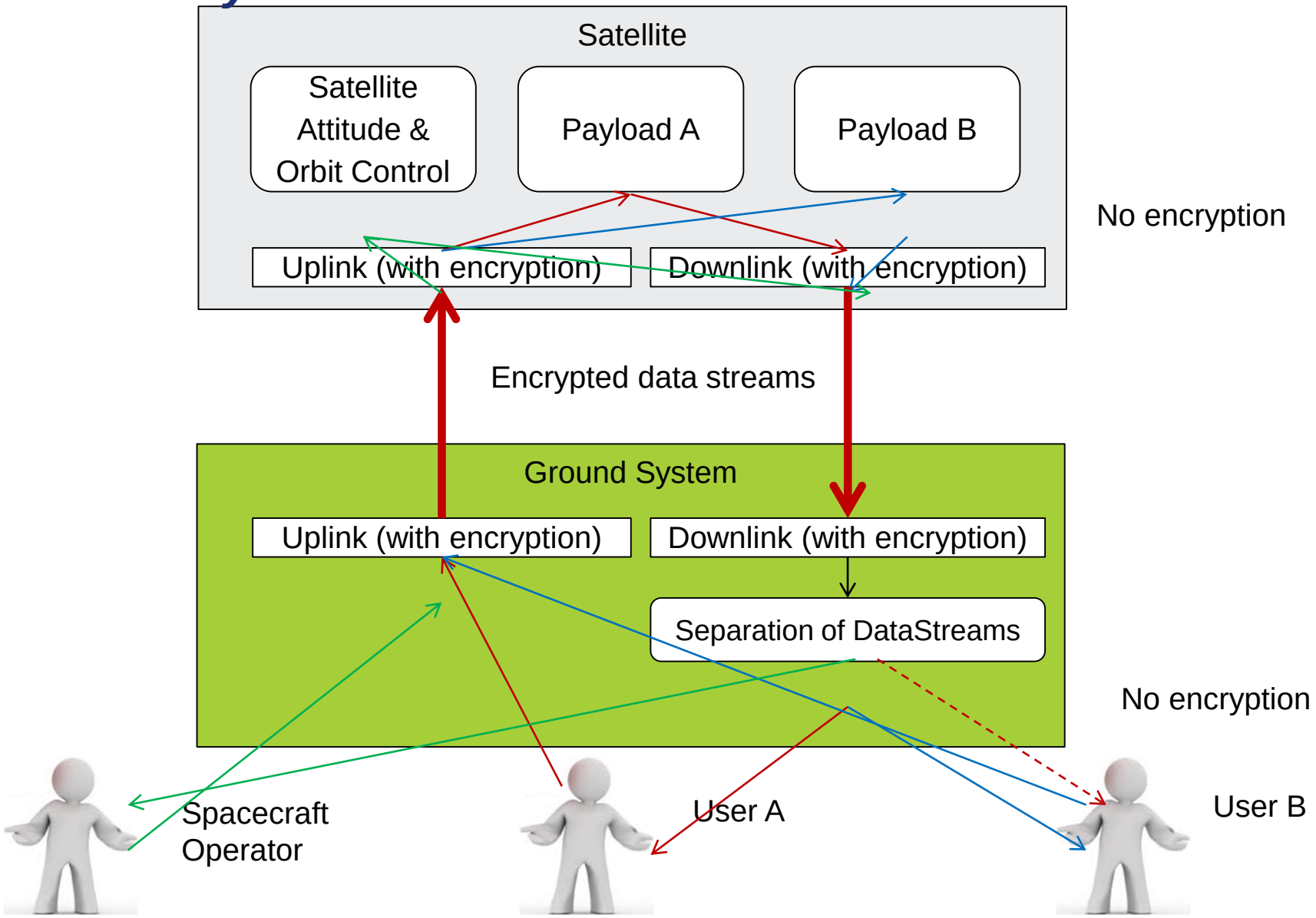




AIRBUS DEFENCE & SPACE

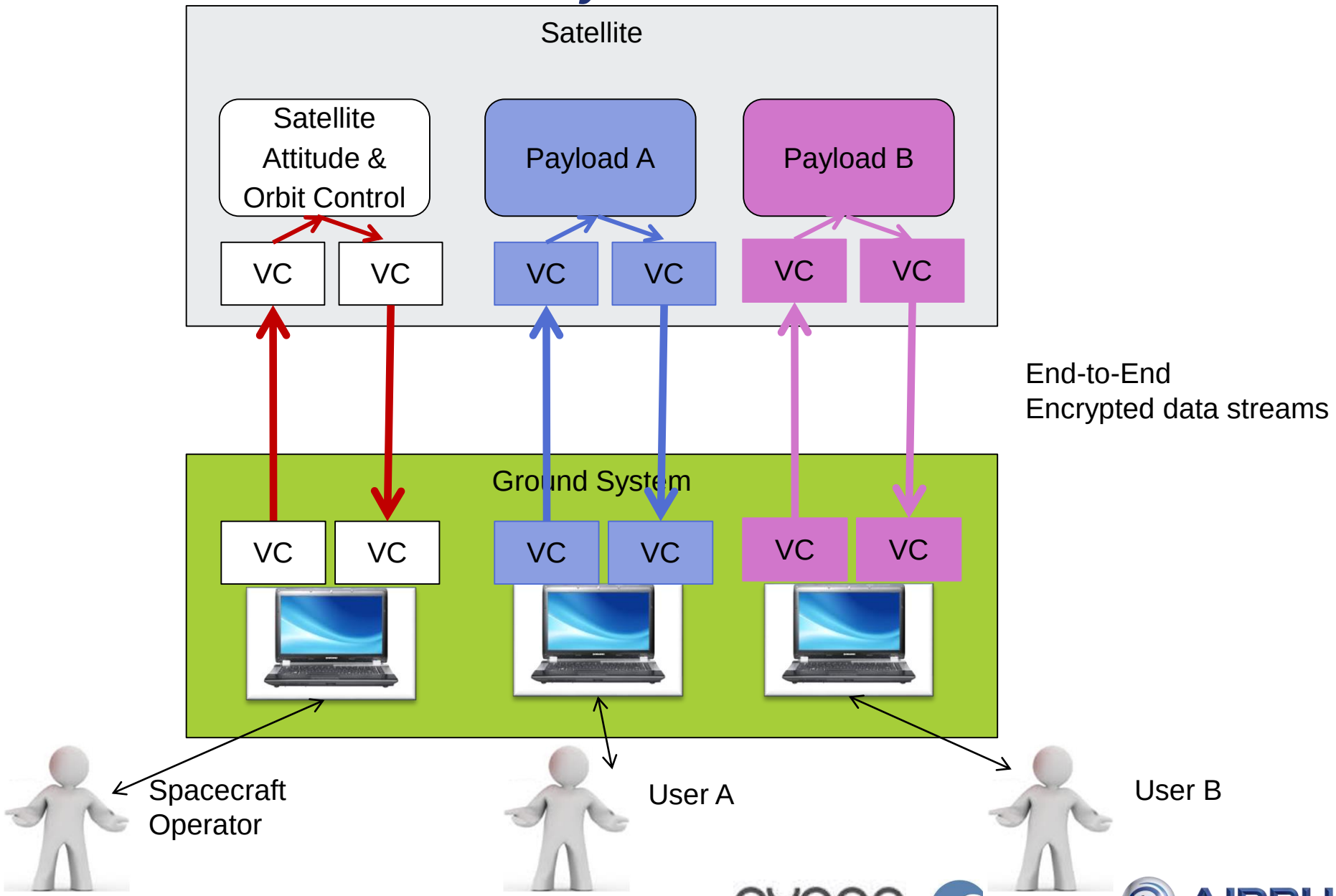
# SPCC : Secure Partitioning Communication Controller (ESA Study)

## *Today Secure System Architecture*



# SPCC : Secure Partitioning Communication Controller (ESA Study)

## *Tomorrow Secure Oriented System Architecture*

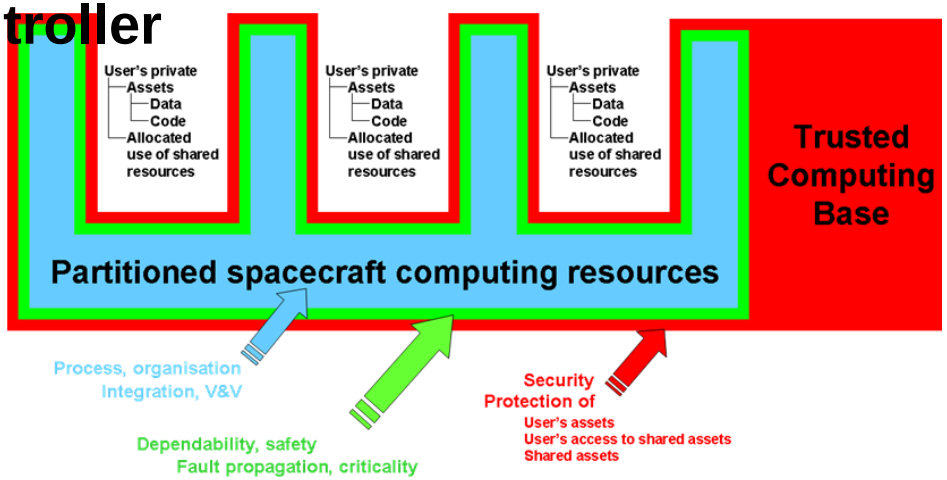


# SPCC : Secure Partitioning Communication Controller (ESA Study)

## *Software Elements for Security*

- **Security**
  - Encryption on TM/TC link (hardware)
  - Access control implemented on ground
- **IMA-SP Study**
  - Supports the principle of „separation of concerns“ through Time & Space Partitioning (TSP)
  - Focus on development flow and scheduling („safety aspects“)
- **Combining IMA/TSP approach with security features**
  - TSP guarantees non-interference, resilience against malicious actions (safety aspect)
  - TSP ensures integrity, availability, confidentiality of data within each partition (security aspect)
  - Additional components are needed to ensure secure communication between partitions

**➔ Software Elements for Security – Partition Communication Controller**








SYSGO EMBEDDING INNOVATIONS · esa · AIRBUS DEFENCE & SPACE

# Applying mixed criticality partitioning on board
# … a system-wide problem

- In the context of Space systems, logical partitioning is candidate to support to the key elements identified
  - adapted validation effort
  - independent life-cycles
  - runtime isolation
  - security barriers on board
  - allocation/separation of responsibilities

- Validating this option requires a system-wide analysis
  - encompassing the operational, functional, design and performance aspects as well as the life-cycle and organisation issues
  - redefining processes, methods & tools , and the industrial organisation for new V&V objectives to take befits from mixed Criticality applications in same computer

# Mixed Critical systems issues in relation to spacecraft avionics
## *Synthesis for next step discussion*



- After R&D studies on Integrated Modular Avionics (IMA) architecture and process, after definition and development of Time & Space Partitioning solutions with Hypervisors & Separation Kernels, the first space operational use cases are starting:
  - with the need to maximize the integration of different functions & sensors software inside the same computer (STR, GNSS, Payload in OBC)
  - With more powerful computing boards based on new available multicore processors (NGMP, ARM)

- Depending on the mission and the industrial organization, the different application software running in the different partitions could come from different companies or teams with different levels of maturity. As for aeronautical first IMA generation, in order to simplify the first partitioning deployments, only a unique criticality approach is applied on all software components and partitions in the same computer.

- In future projects we are targeting to enlarge the solution with mixed criticality application software in the different partitions, taking also benefits from multicore processors solutions and also to consider, in some specific use cases, a set of data security needs and requirements.



AIRBUS DEFENCE & SPACE

# Thank you for your attention !

Questions ?





AIRBUS DEFENCE & SPACE