MILS Compliant Software Architecture for Satellites

ESA Contract No. 4000108471/13/NL/LvH

MILS Workshop, Praque, 19.01.2016

H.J. Herpel, K. Eckstein, M. Schön, M. Kerep, G. Montano, A.Krutak

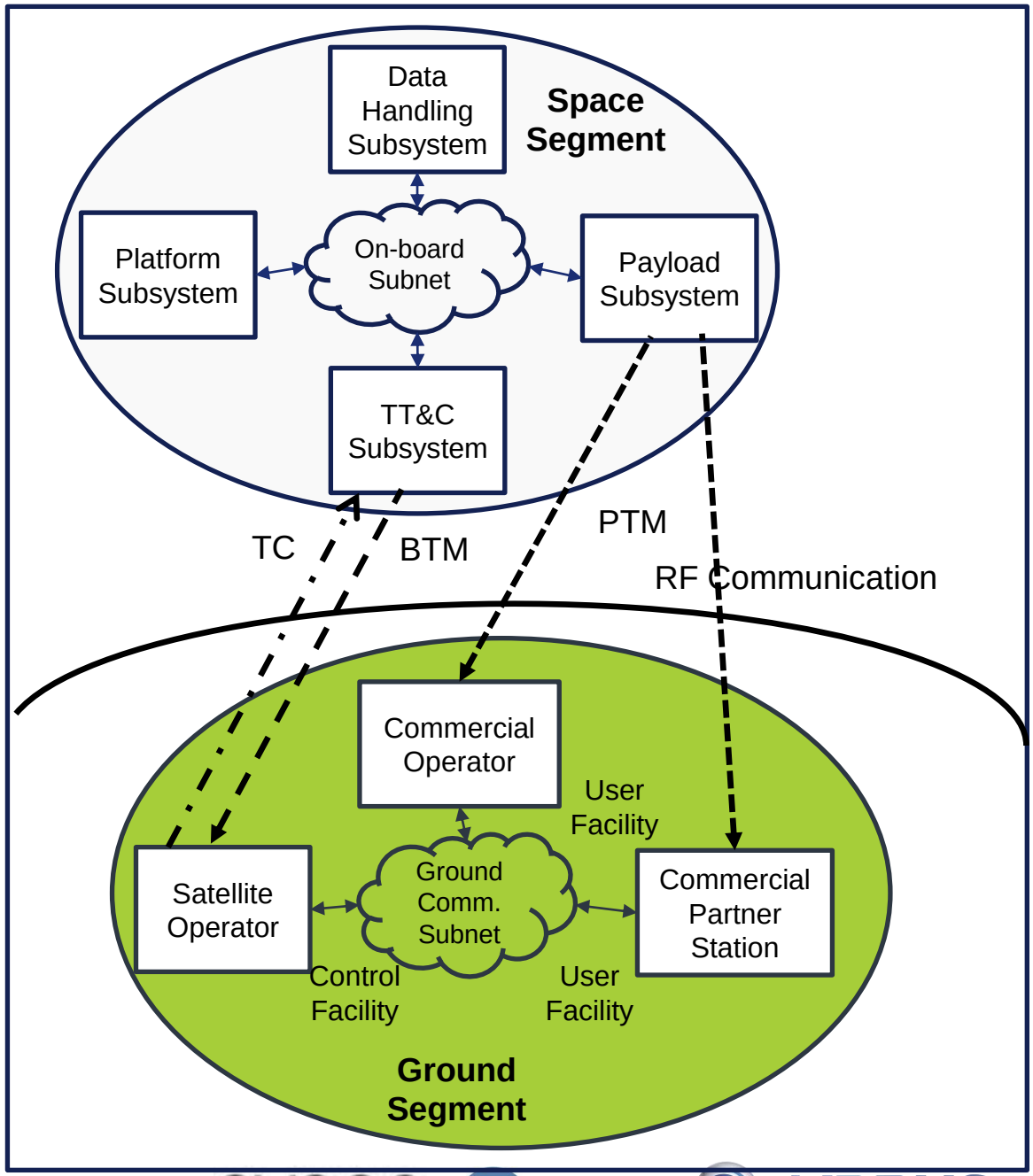
AIRBUS DEFENCE & SPACE

esa

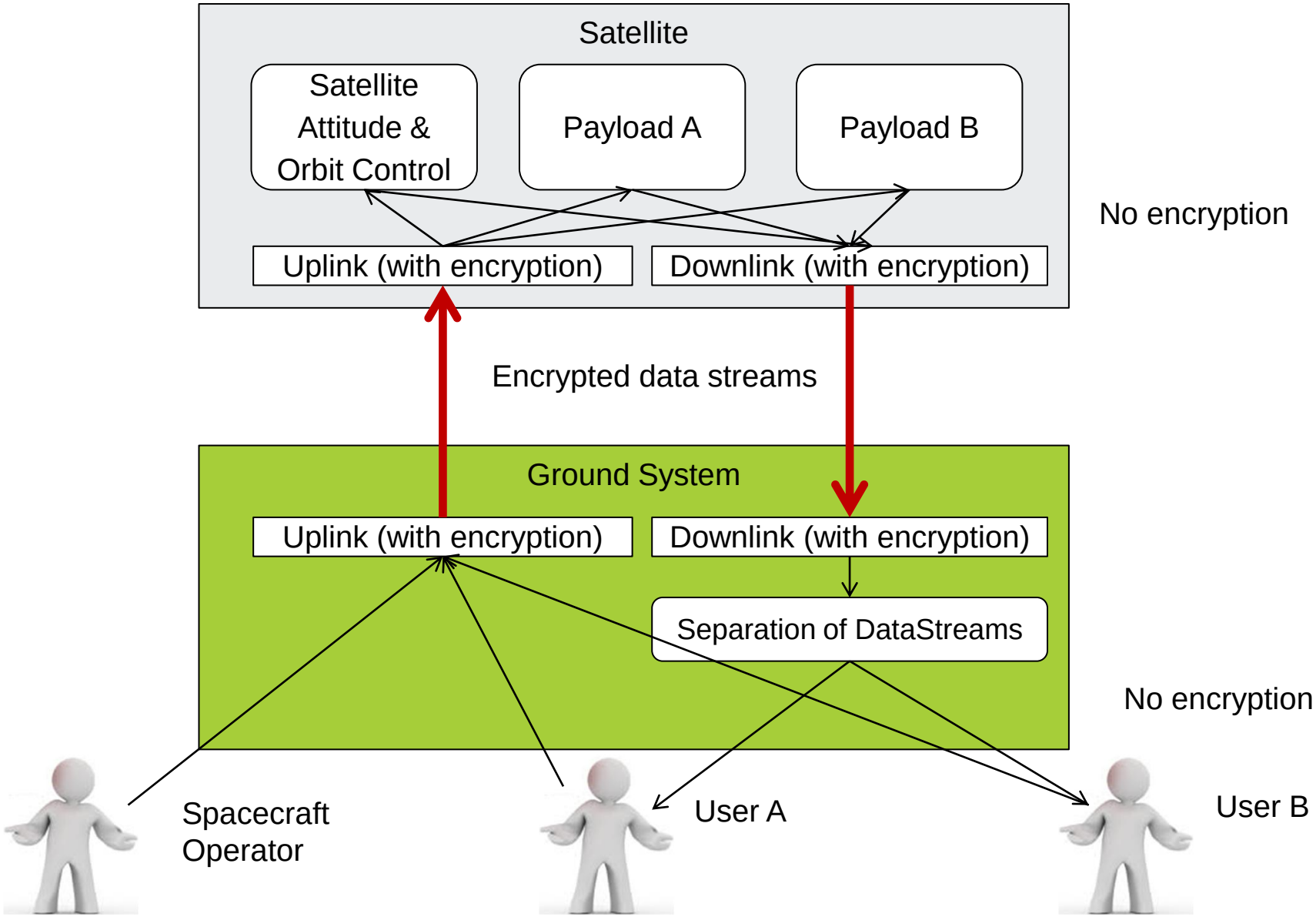
SYSGO EMBEDDING INNOVATIONS

Is there a security issue in space applications?

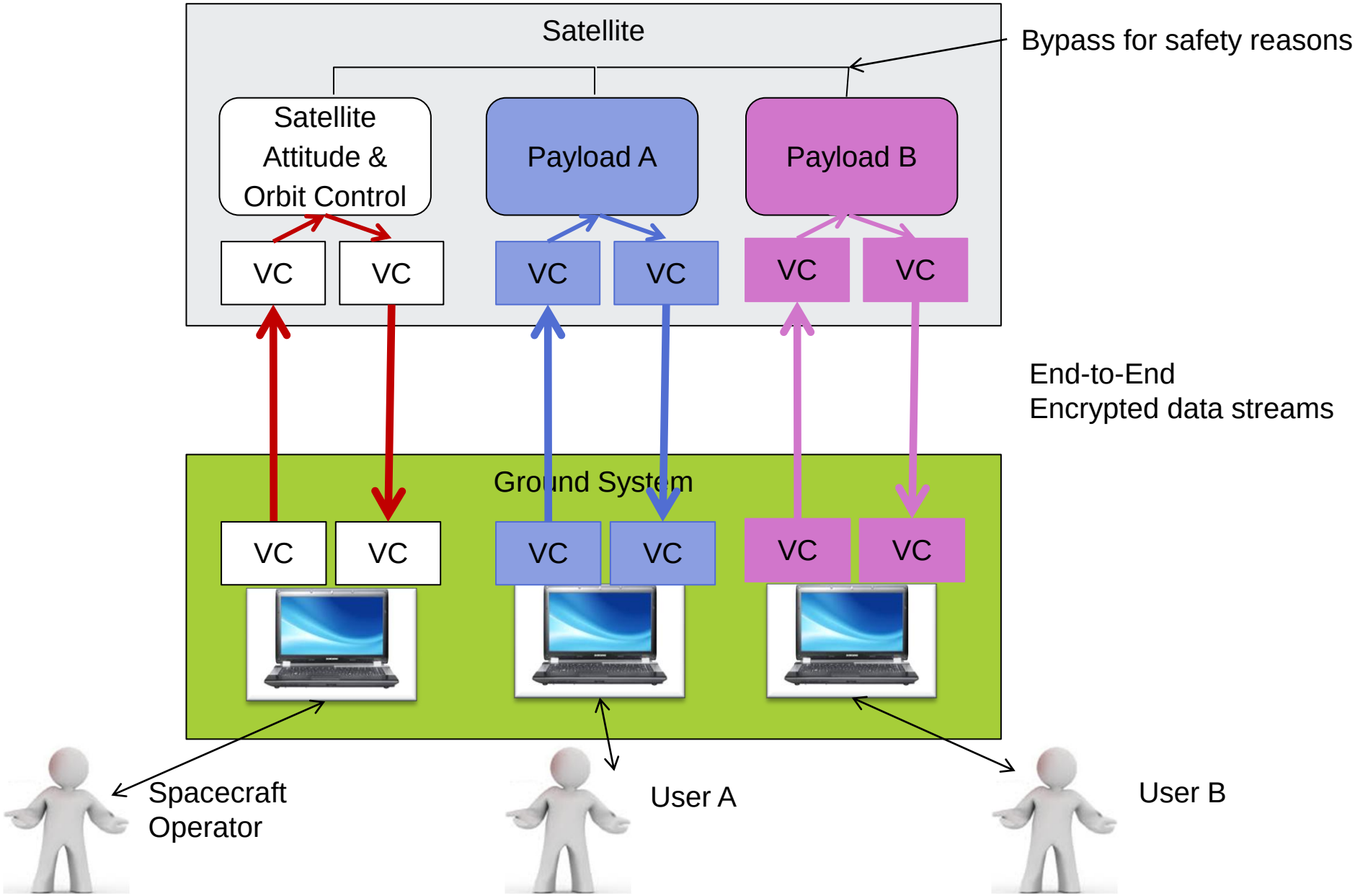
- **Yes, demonstrated in several James Bond movies (Golden Eye, …)**



Solutions today



Security oriented architecture

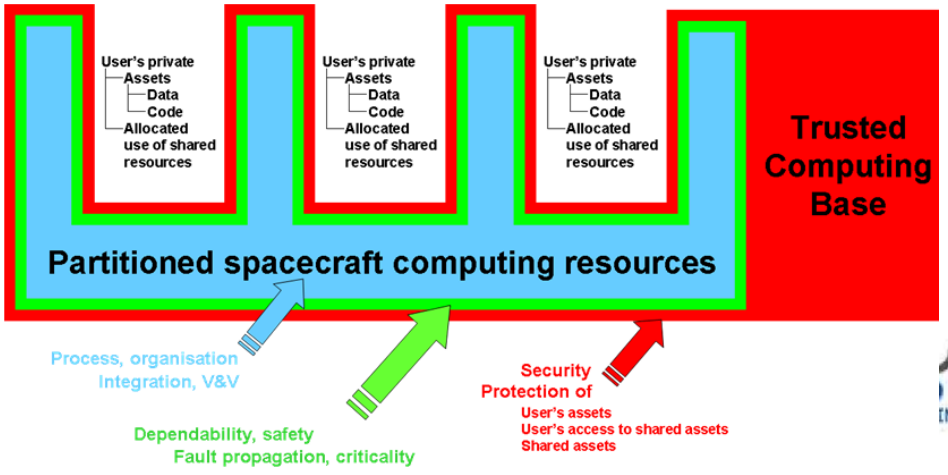


The Starting Point

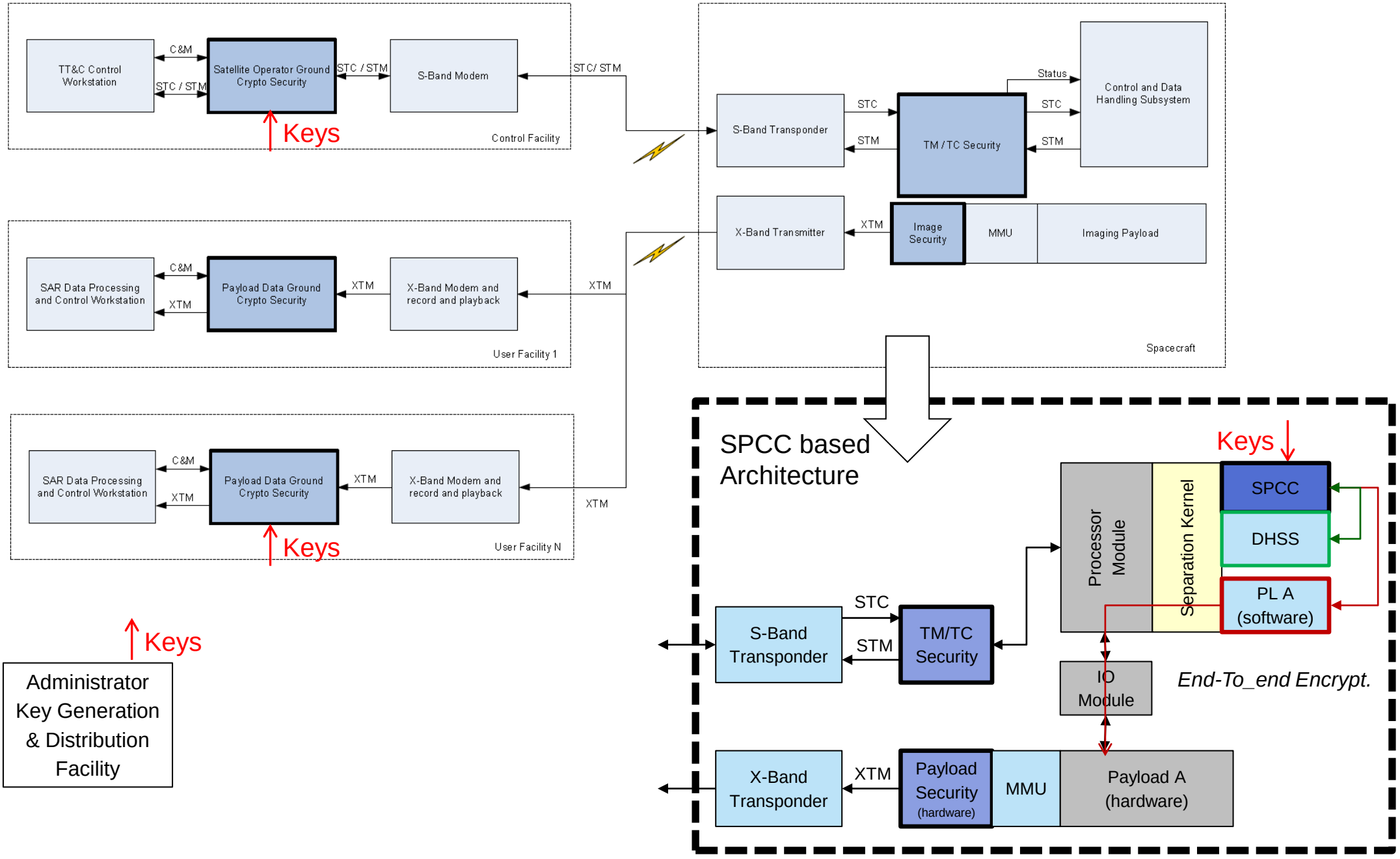
- **Security**
  - Encryption on TM/TC link (hardware)
  - Access control implemented on ground
- **IMA-SP Study**
  - Supports the prinicple of „separation of concerns“ through Time & Space Partitioning (TSP)
  - Focus on development flow and scheduling („safety aspects“)

- **Combining IMA/TSP approach with security features**
  - TSP guarantees non-interference, resilience against malicious actions (safety aspect)
  - TSP ensures integrity, availability and confidentiality of data within each partition (security aspect)
  - Additional components are needed to ensure secure communication between partitions

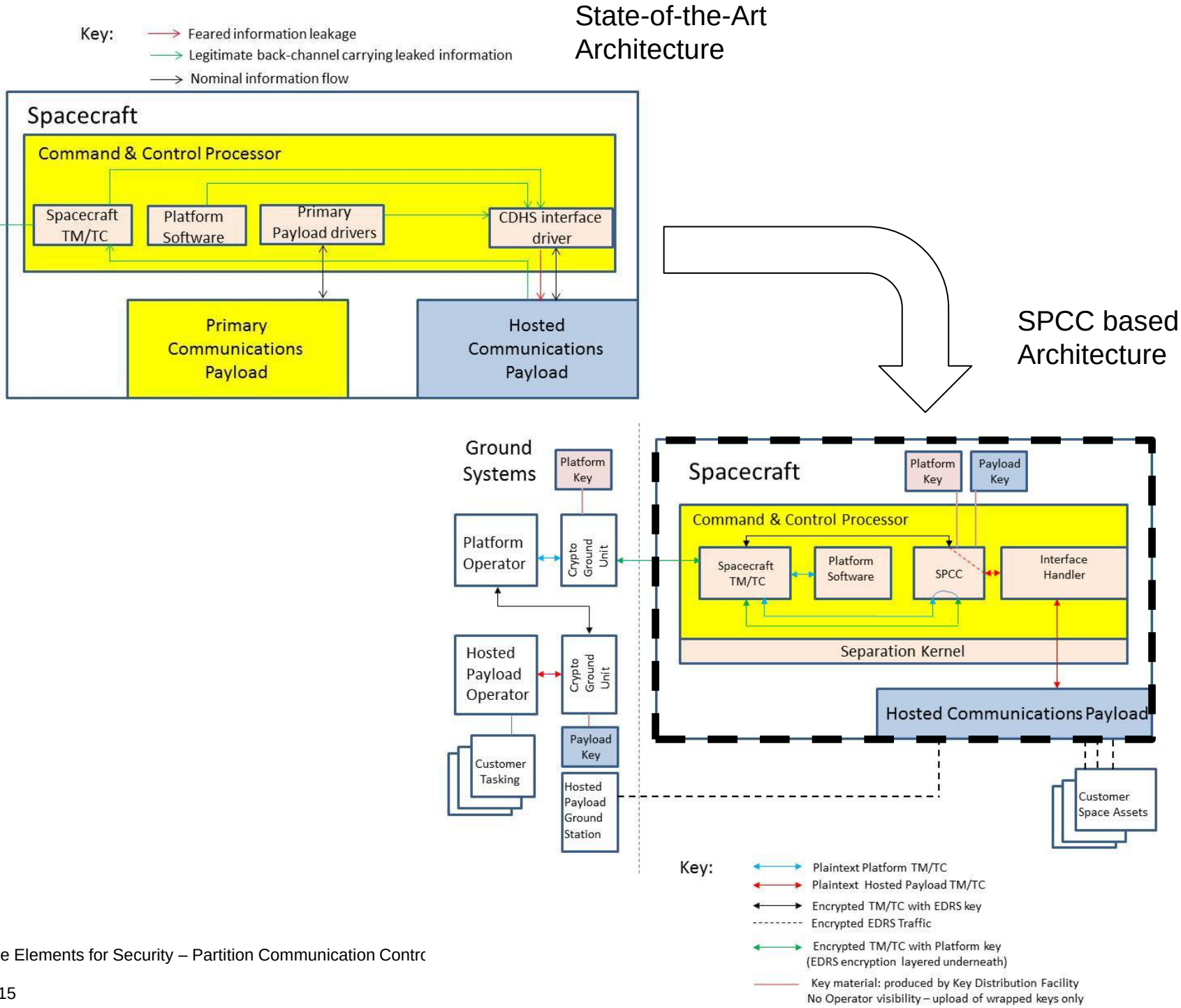
➔ **Software Elements for Security – Partition Communication Controller**



Use Case „Earth Observation“



Use Case „Telecom“



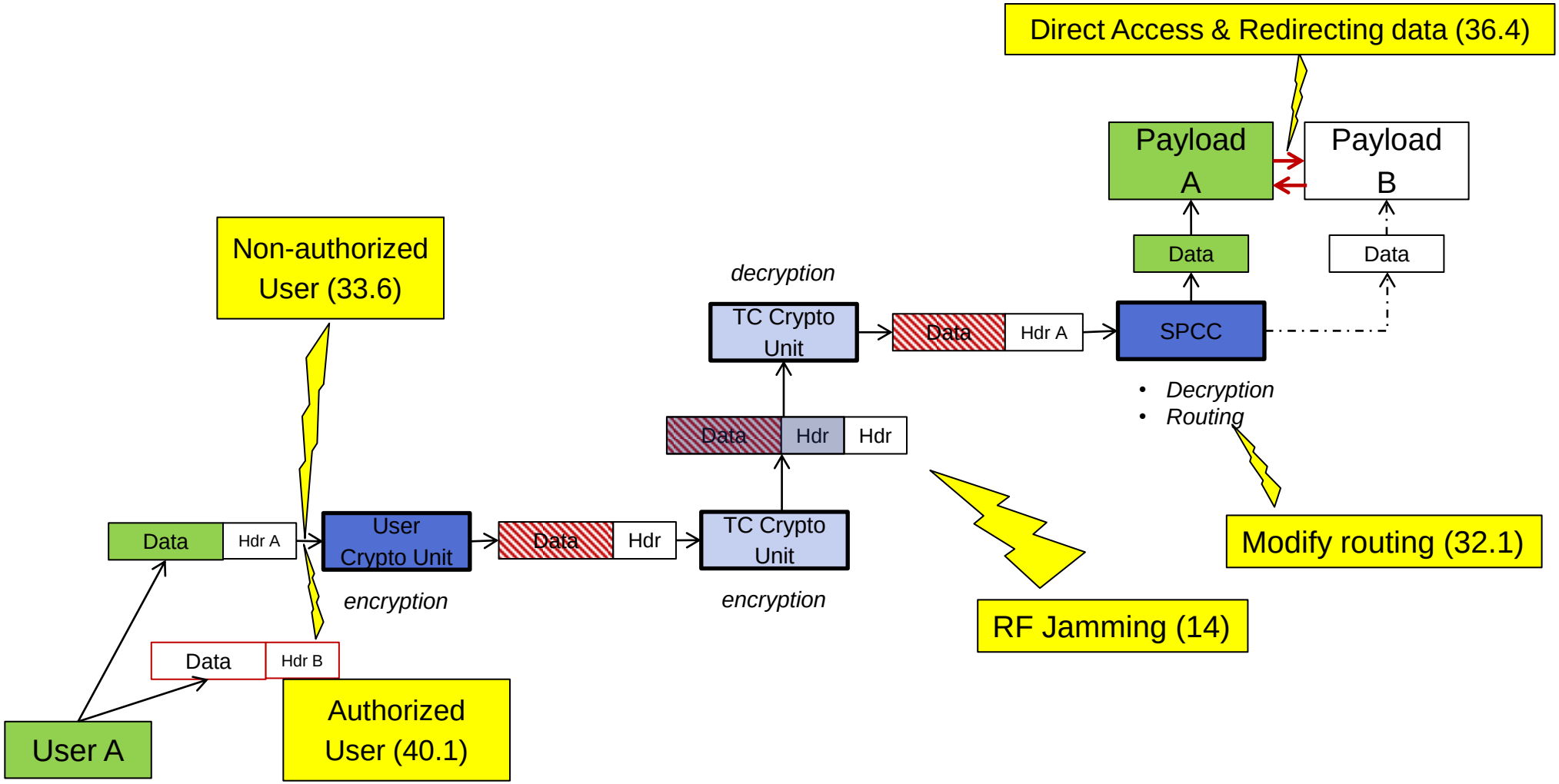
Threat Assessment - Methodology

1. **Identify relevant threats** based on generic list provided by EBIOS v2 Section 4, Tools for Assessing ISS Risks FIPS PUB 197, Nov 26 2001.

EBIOS Ref	Generic Threats	Selected Threat	Ref	Specific Threat	Assumptions	Additional Comments
17	Interception of compromising interference signals	No	17.1	Electrical signal interception during integration and test	Appropriate facilities are provided during test and integration, to limit the potential for sensitive electrical signal interception	This is only relevant to flight equipment before launch, for commercial missions, but the threat is countered by the environment, and not specific technical means, so is not considered here.
18	Remote spying	No			Physical protection of ground equipment eliminates potential for unauthorised personnel to observe critical data or operations	
19	Eavesdropping	Yes	19.1 19.2 19.3	BTM interception between a Platform Operator and Platform subsystems. TC interception between a Platform Operator and Platform subsystems. PTM interception between a Payload and a Mission Data user		This is one of the primary security considerations for the TT&C system
20	Theft of media or documents	No			N/A +	
21	Theft of equipment	No			N/A +	
22	Retrieval of recycled or discarded media	No			Organisational policies provide for appropriate protection and destruction of media and documents	
23	Disclosure	Yes	23.1 23.2 23.3	PTM external disclosure BTM external disclosure TC external disclosure	Organisational policies and access controls provide for the appropriate protection of sensitive data to prevent unwanted internal disclosure.	Information disclosed to an **external** party i.e. through the RF link
24	Data from untrustworthy sources	Yes	24.4 24.5	Information is used without guarantee of origin by the Platform Information is used without guarantee of origin by the Payload		This considers the potential for modification or inserting of TC on the RF link, including replay of authorised commands. The potential for modification of BTM, PTM on the RF link is not included as this is considered practically infeasible. Because of the directivity of the ground receive antenna, and hence its selectivity for spacecraft location.
25	Tampering with Hardware	No			N/A +	

EBIOS=Etude des Besoins et Identification des Objectifs de Sécurité

Relevant Threats



Threat Assessment - Methodology

2. Identify **Target of Evaluation (TOE)**: indicate the boundary and the contents of the security equipment analysed and evaluated

TOE identification: SPCC + Cryptographic Component + Separation Kernel
Assurance Level: EAL4.

TOE Boundary: The TOE lies within the Spacecraft computer, and specifically comprises:

- The SPCC (software) which performs the security functions
- The separation kernel (software) which prevents the SPCC being bypassed
- Any hardware support in the onboard computer processor (memory management unit), required to ensure that only the SPCC can access particular I/O.

Threat Assessment - Methodology

3. Map identified **specific threats** to a set of **Security Objectives** which will prevent the threat from occuring

O.ADMIN The TOE must provide functionality which enables an authorised user to effectively manage the TOE and its security functions, and must ensure that only authorised users are able to access such functionality, while also maintaining confidentiality of sensitive management data.
O.AUDIT The TOE must provide a means of recording any security relevant events, so as to assist an authorised user in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions that they perform that are relevant to security.
O.ENCRYPT The TOE must provide the means of protecting the confidentiality of information transmitted across the communications link.
O.ROLES The TOE must prevent users from gaining access to, and performing operations on its resources for which their roles is not explicitly authorised.
O.INITIALKEYS The TOE must provide a means to manually load a full set of Red keys before launch, ensuring both the integrity and confidentiality of those keys**.**
O.OTAR The TOE must provide means for receiving new keys throughout the operation of the TOE, whilst maintaining the confidentiality and integrity of those keys.
O.INTEGRITY The TOE must provide a means of detecting loss of integrity affecting information received by the TOE.
O.REPLAY The TOE must provide a means to prevent undetected replay of previous information sent to the TOE.
O.PROTECT The TOE must protect itself against external interference or tampering by untrusted subjects, or attempts to bypass the TOE security functions.
O.FAILSAFE In the event of an error occurring, the TOE must preserve a secure state.
O.SIDECHANNEL Authorised user(s) of the TOE, e.g. Operator and Platform Software developer, are not cleared to view Key Material within the TOE (defined in O.ROLES). Therefore, the TOE prevent any key information from leaking from the TOE via a side-channel to another software partition. Examples of side-channels are – cache-timing, cache-contents, power-analysis, differential fault analysis. This is addressed in document [TN02] Internal Security Threat Assessment

Threat Assessment - Methodology

2. Map a set of **Security Requirements** for implementation on the **Target of Evaluation** which will meet those **Security Objectives**

Objective	Objective Description	Security Functional Requirements	Requirement Name
O.ENCRYPT	Provide the means of protecting the confidentiality of information transmitted across the communications link from TOE to Hosted Payload Operator Provide the decryption service for availability of information transmitted across the communications link from Hosted Payload Operator to TOE, transmitted confidentially	FCS_CKM.3.1.1 FCS_CKM.3.1.2 FPT_ITC.1.1	KEY Cryptographic key access KEY Cryptographic key access Inter-TSF confidentiality during transmission
O.PARTITION	Ensure that software partitions co-located on the same processor shall have no visibility of the data of another, except via inter-partition communication	FDP_ACF.1.1.1	Partition Security Based Access Control
O.HWPARTITION	The Hardware interfaces to the I/O must be consistent with O.PARTITION, and ensure that the physical partitioning of the data between interfaces / domains / end-users, is maintained, and that no data is passed between interfaces / domains / end-users (that function remains the sole responsibility of the SPCC).	FPT_FLS.1 FPT_PHP.1 FPT_RVM.1 FPT_SEP.1	Failure with preservation of secure state Passive detection of physical attack Non-bypassability of the TSP TSF domain separation
O.SIDECHANNEL	Prevent any information from leaking from the security domain of one software partition, to another security domain that may be a software partition or to a physical interface. Specifically, information concerning application timing from the source application, and impact of confidential	FPT_ITC.1.1.1	Inter-TSF confidentiality during transmission

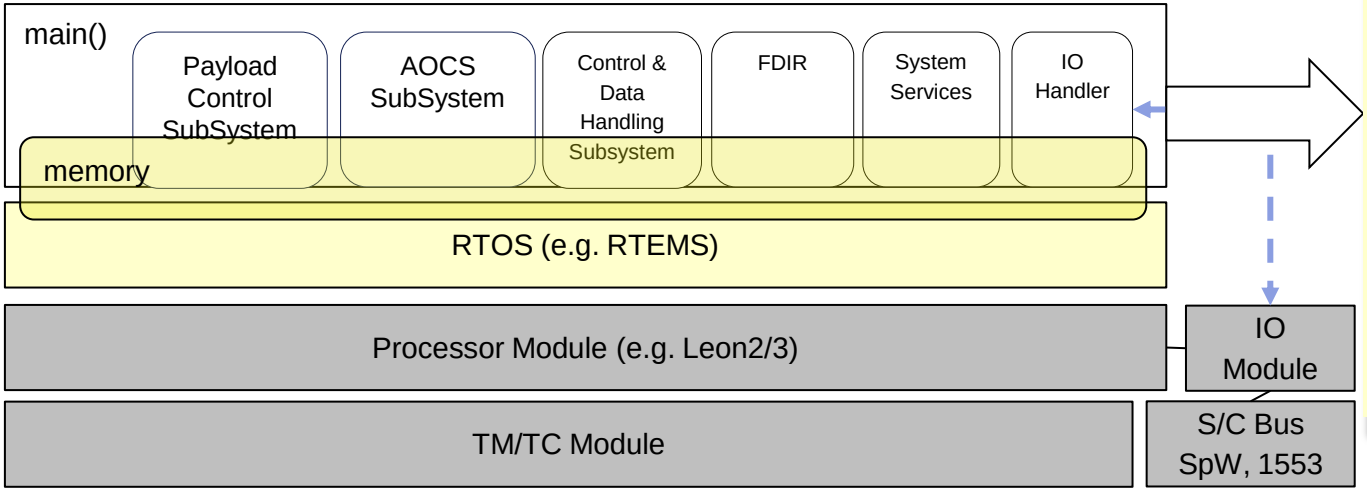
TASK 2: Requirements and Architecture

Initial Set of Functional Requirements

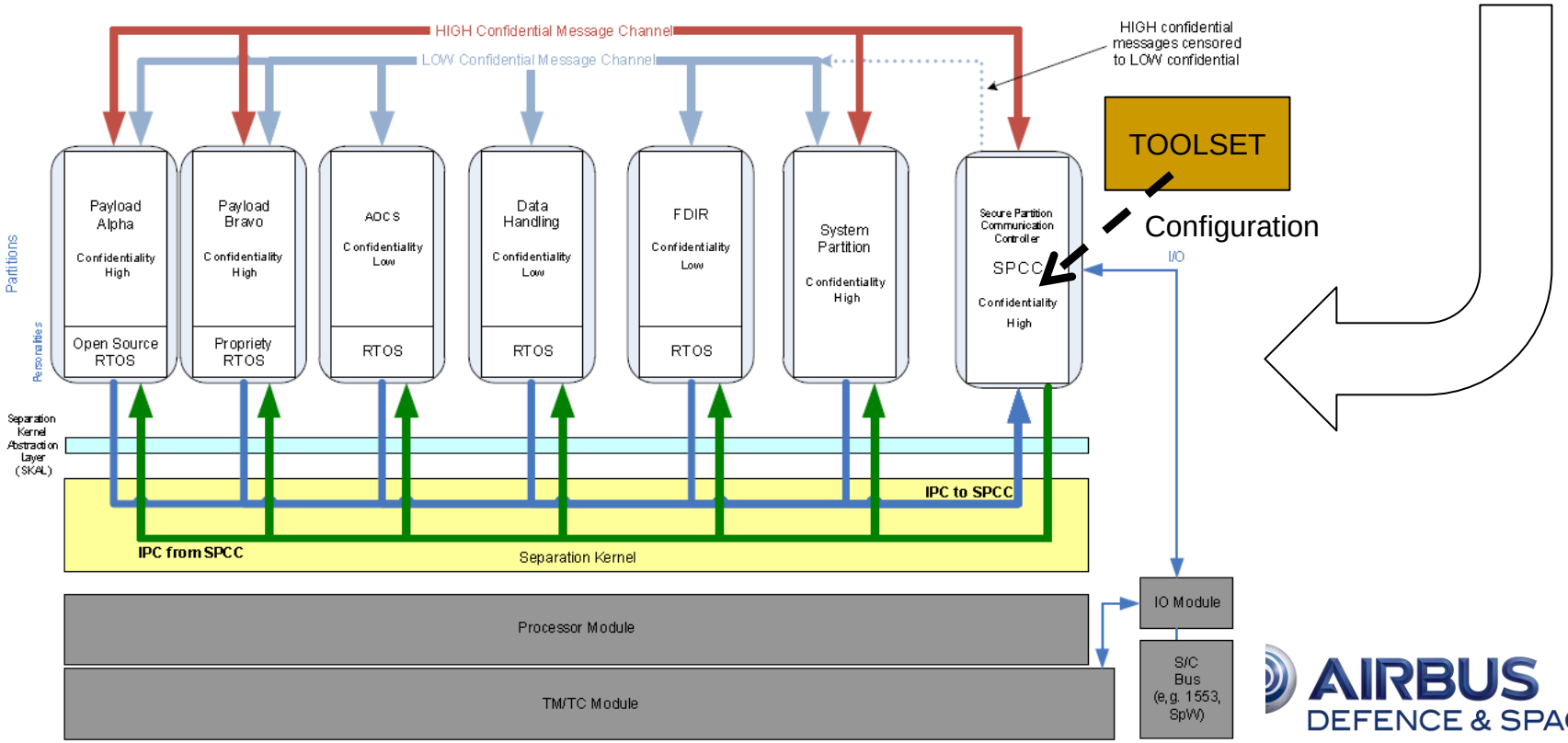
- SPCC 6.2 The SPCC shall support the telecommand to upload a new Key
- SPCC 6.3 The SPCC shall unwrap a new uploaded Key, using the appropriate Key Encryption Key stored locally and AES cryptographic algorithm – CFB mode, 128-bit key (FIPS 197,FIPS 140-2)
- SPCC 6.4 The SPCC shall authenticate the uploaded Keys before use, using the wrapping integrity-checks. If the unwrapped Key fails wrapping integrity-check, the unwrapped Key shall be discarded
- SPCC 6.5 At boot, the SPCC shall use the root key key loaded to EEPROM as its Key Encryption Key
- SPCC 6.6 The SPCC shall report key labels of all Keys currently loaded, in telemetry, but not any key material
- SPCC 6.7 The SPCC shall report any status of the SPCC in telemetry, including;
  - Key unwrapping and validity status
  - Number of authentic / inauthentic telecommand packets received
  - Number of replayed / non-replayed telecommand packets received
  - Current value of Local Authentication Count reply counter
- SPCC 6.8 All SPCC telemetry shall be encrypted and transmitted to S-band transponder interface handler in an identical manner to spacecraft platform telemetry
- …

- SEP.1 The Separation Kernel shall control the access of each software partition to defined areas of memory. A software partition shall not be allowed to access an area of memory (read or write) unless permitted by the Separation Kernel
- SEP.2 The Separation Kernel shall control the execution timing of each software partition, such that it executes at a time completely independent of the activities of any other software partition
- SEP.3 The Separation Kernel shall control the access of each software partition to I/O's, both read and write. Specifically, from a security perspective:
- SEP 3.1 The I/O corresponding to S-band transponder Rx and Tx shall be accessible only to the S-band Rx and Tx interface handlers. These two interface handlers may or may not share a partition
- SEP 3.2 The I/O corresponding to X-band transponder Tx shall be accessible only to the X-band Tx interface handler
- SEP 3.3 The I/O corresponding to Mass Memory shall be accessible only to the Mass Memory interface handler
- SEP 3.4 The I/O corresponding to Data Handling Bus shall be accessible only to the Data Handling Bus interface handler
- …

From State-Of-The-Art to MILS Compliant on-board Architecture Software Architecture



Multiple Independent Levels of Safety and Security (MILS) compliant architecture: is a high-assurance security architecture based on the concepts of separation and controlled information flow; implemented by separation mechanisms that support both untrusted and trustworthy components; ensuring that the total security solution is non-bypassable, evaluatable, always invoked and tamperproof.



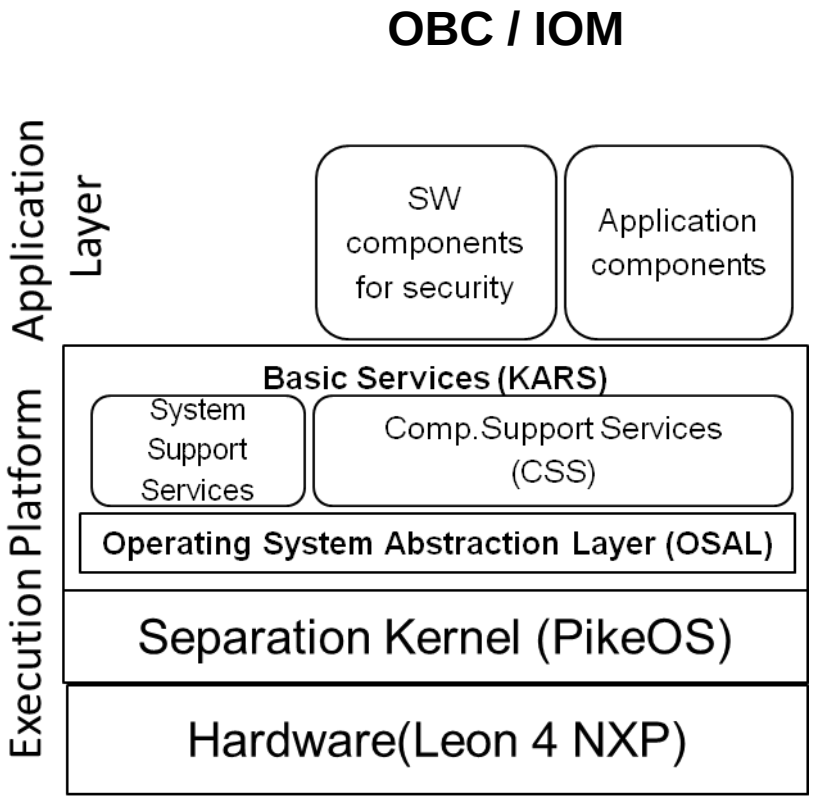
AIRBUS DEFENCE & SPACE

Basic Execution Platform – Design Decisions

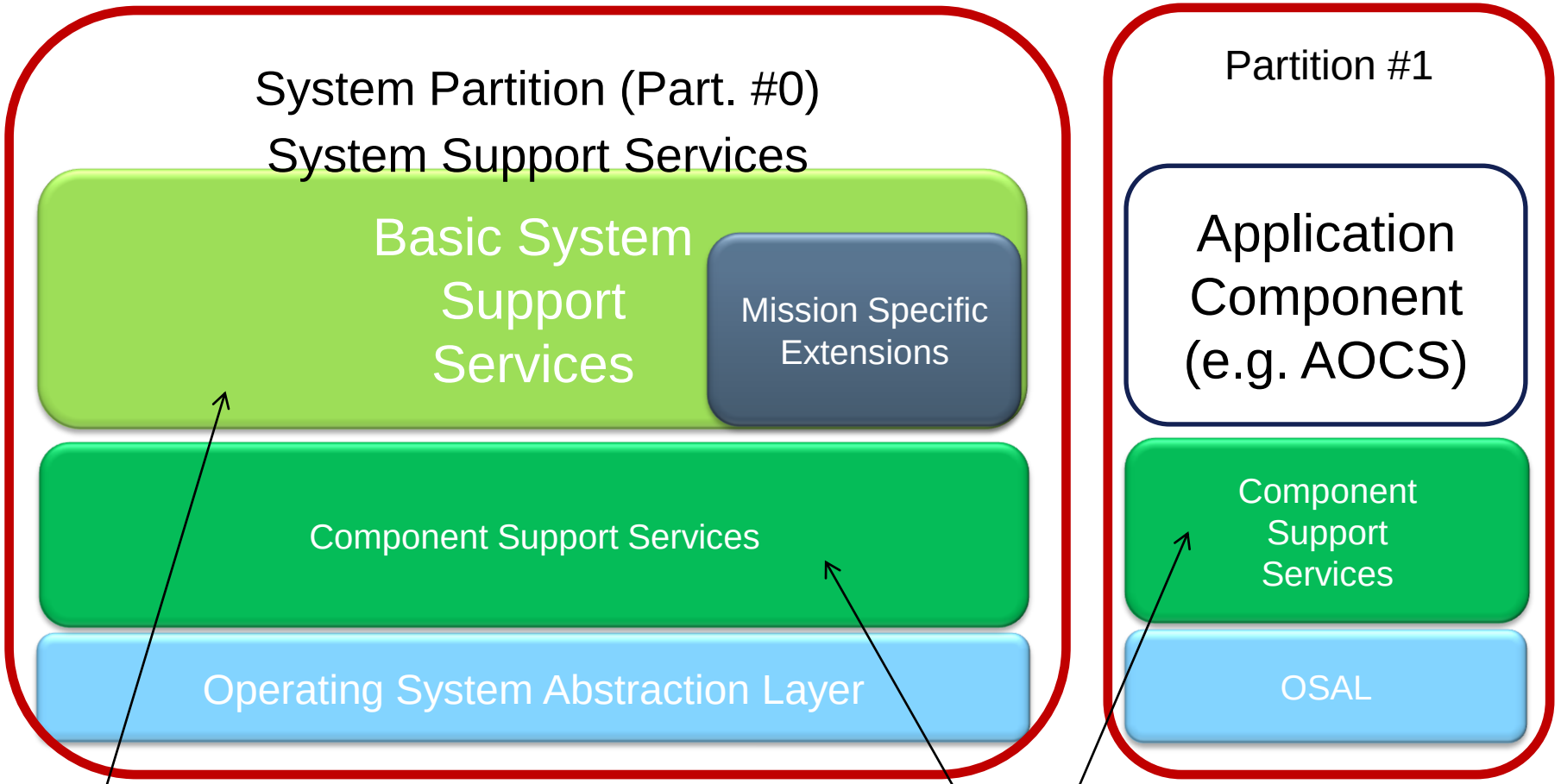
- **Processor Module / IO Module:**
  OBC: Leon2/3 (MDPA, SCOC3) vs. ***Leon4***
  IOM: Leon2 (MDPA) vs. ***same as for OBC***

- **Separation Kernel:**
  OBC: xTratum vs. ***PikeOS***
  IOM: RTEMS vs. ***same as for OBC***

- **Basic Software**
  OBC: CDHS vs. ***KARS***
  IOM: CDHS stripped down vs. ***same as for OBC***



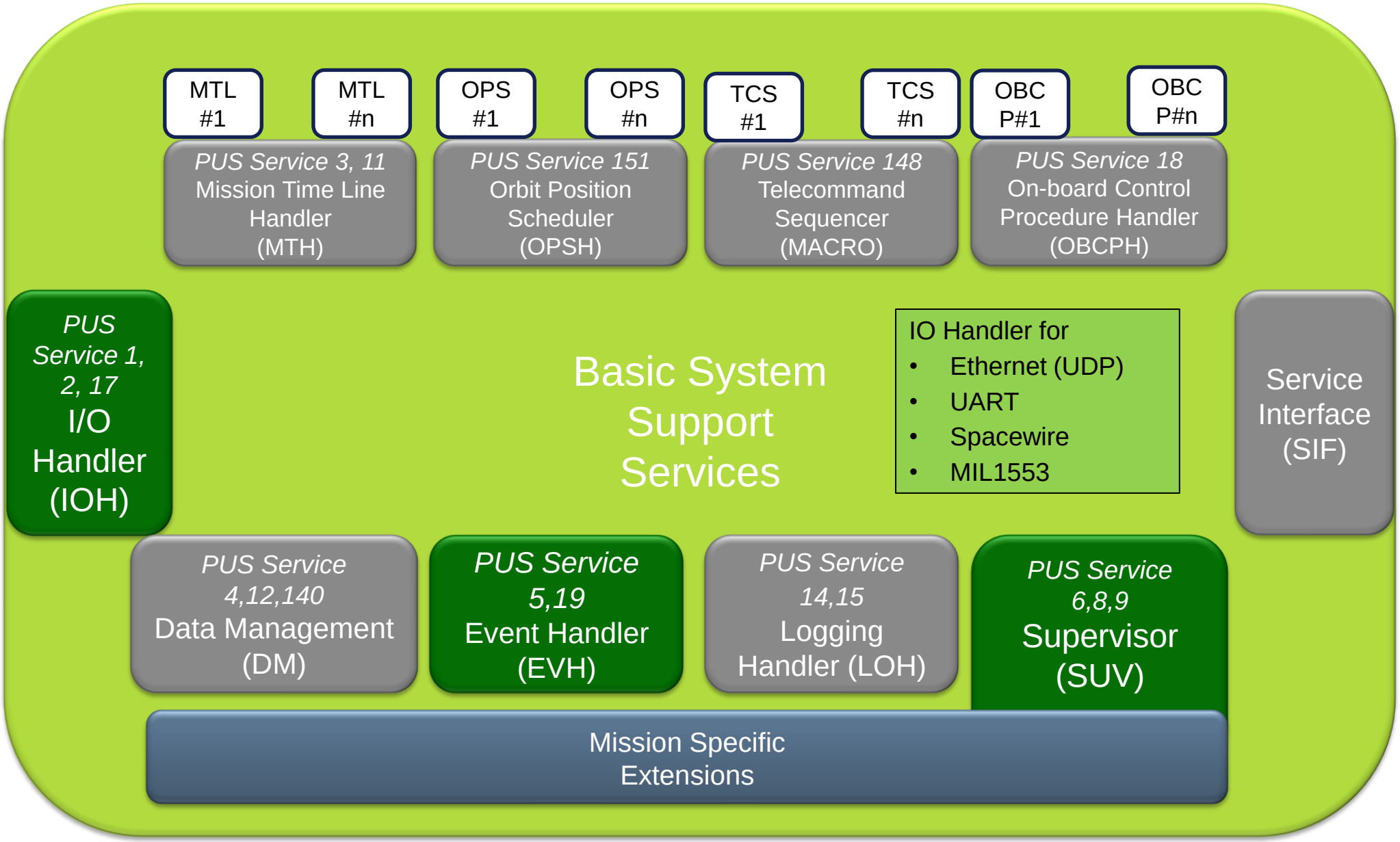
KARS – Controller for Autonomous Spacecraft (developed under DLR contract)



Implements PUS services (1..19, 140, …)

Provides an API (mainly ARINC 653 compliant):
Tasking, communication, …

KARS System Support Services



Selected for SPCC

SYSGO EMBEDDING INNOVATIONS

esa

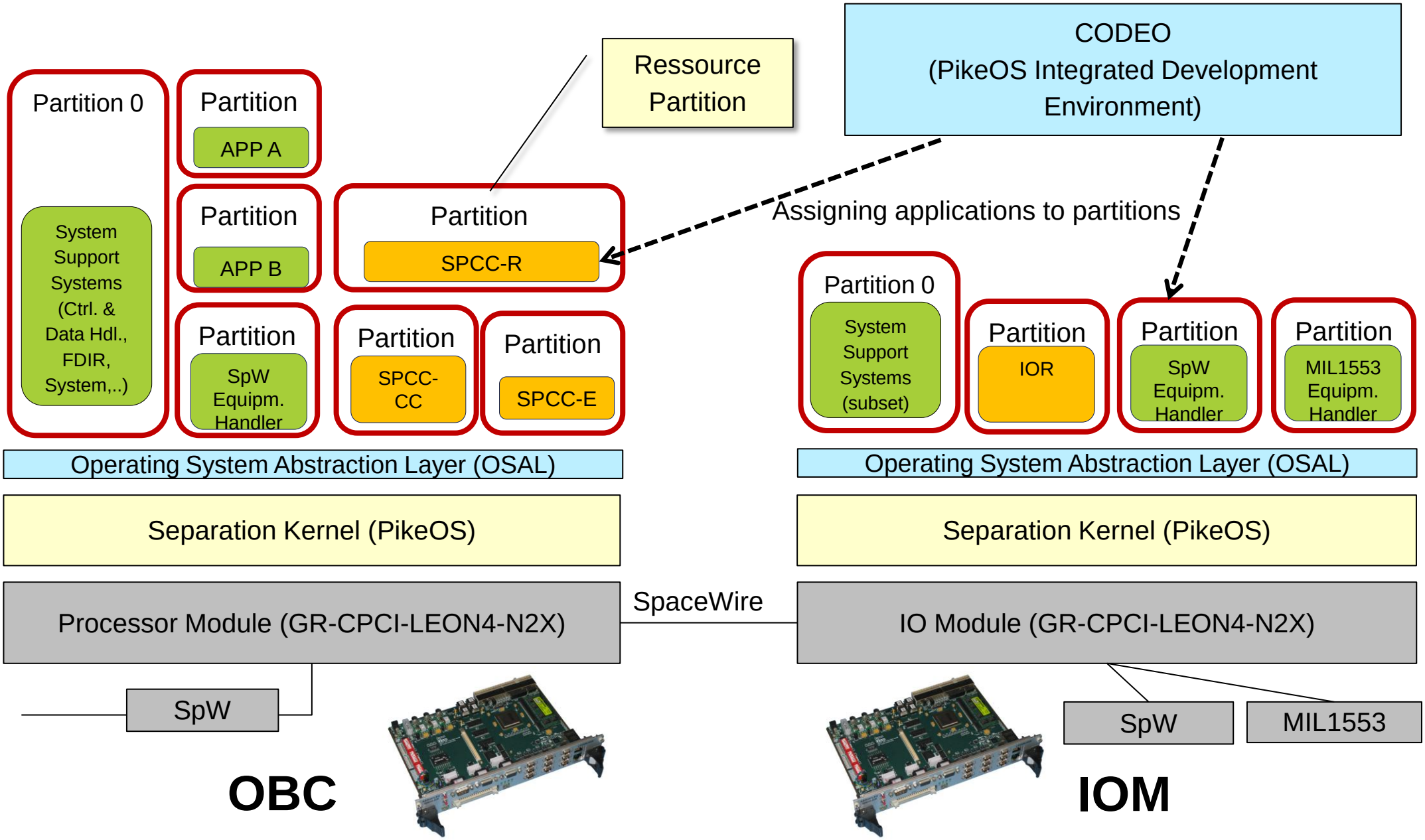
AIRBUS DEFENCE & SPACE

TASK 3: Design and Implementation
Sofware Components

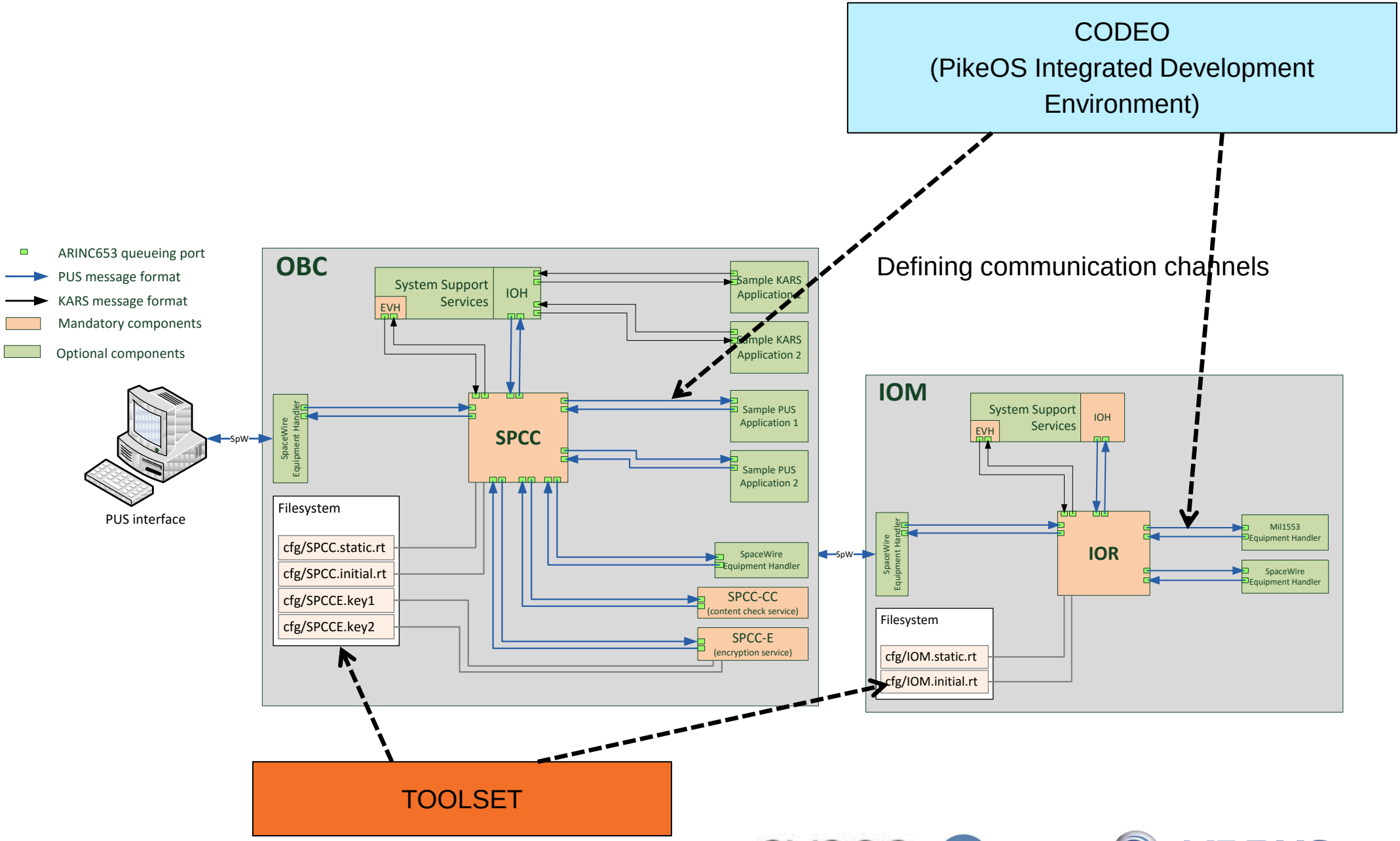
- **Toolset** ➔ *Phython (SYSGO)*
  - Routing table compiler (spcc-rtc)
  - Routing table validation (spcc-validate)
- **SPCC Components** ➔ *C using the KARS API*
  - Secure Partitioning Communication Controller (SPCC-R)
  - En-/Decryption Component (SPCC-E)
  - Content Checking Component (SPCC-CC)
  - Equipment Handler (SpW, MIL1553)
  - Sample Applications
- **IOM Components**
  - Input/Output Router (IOR)

➔ *Instance of the SPCC*

Overall System Architecture

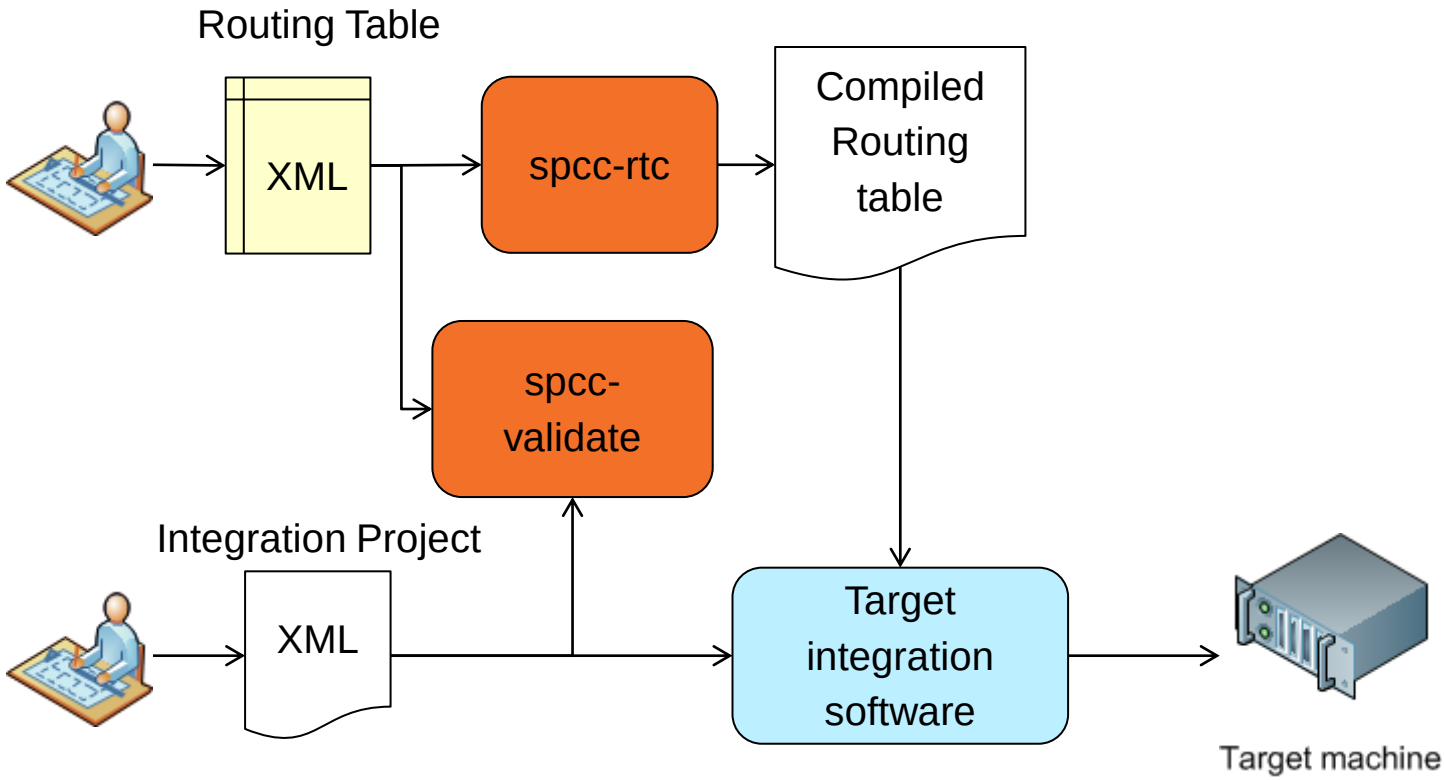


Overall Communication Channels

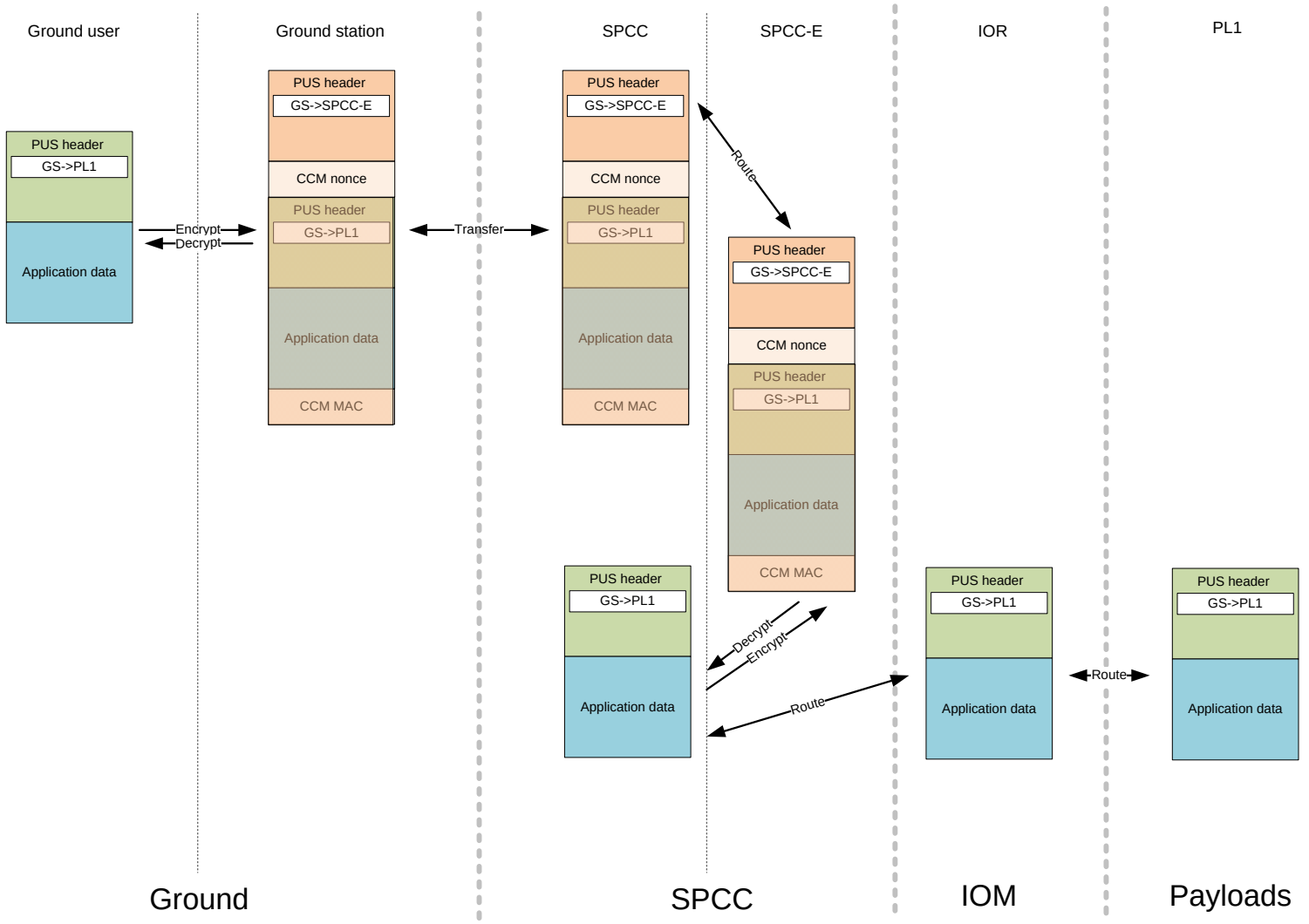


Packet Routing - Definition

Source PRID	Target PRID	PUS Service	Source Port	Target Port
GS	MP2	(140,*)	GS	SPCC-E
GS	MP2	(140,1)	SPCC-E	SPW_IOM
SP1	GS	(*,*)	SPCC-E	GS
SP1	GS	(140,1)	SPW_IOM	SPCC-E
GS	MP2	(140,*)	SPW_SPCC	MIL1553_BC
SP1	GS	(*,*)	SPW_PL	SPW_SPCC



Packet Routing – Encrypted Packet



Implementation results

- SLOC: ~ 6000
- Unit test cases: 148 (VectorCAST)
- Statement coverage:
  - ✓ SPCC-R: 93%
  - ✓ SPCC-CC: 100%
  - ✓ SPCC-E: 100%
- Decision coverage:
  - ✓ SPCC-R: 94%
  - ✓ SPCC-E: 97%
  - ✓ SPCC-CC: 100%

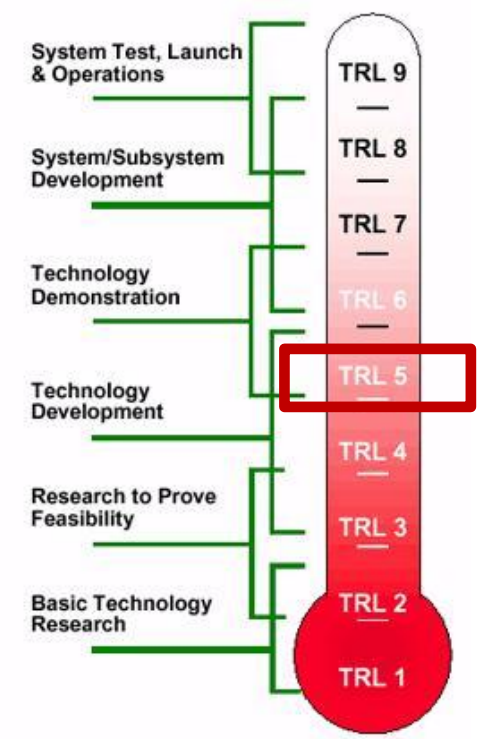
TASK 4/5 Validation and Demonstration

Which TRL and EAL has been achieved?

Table 11 - Assurance Requirements Summary

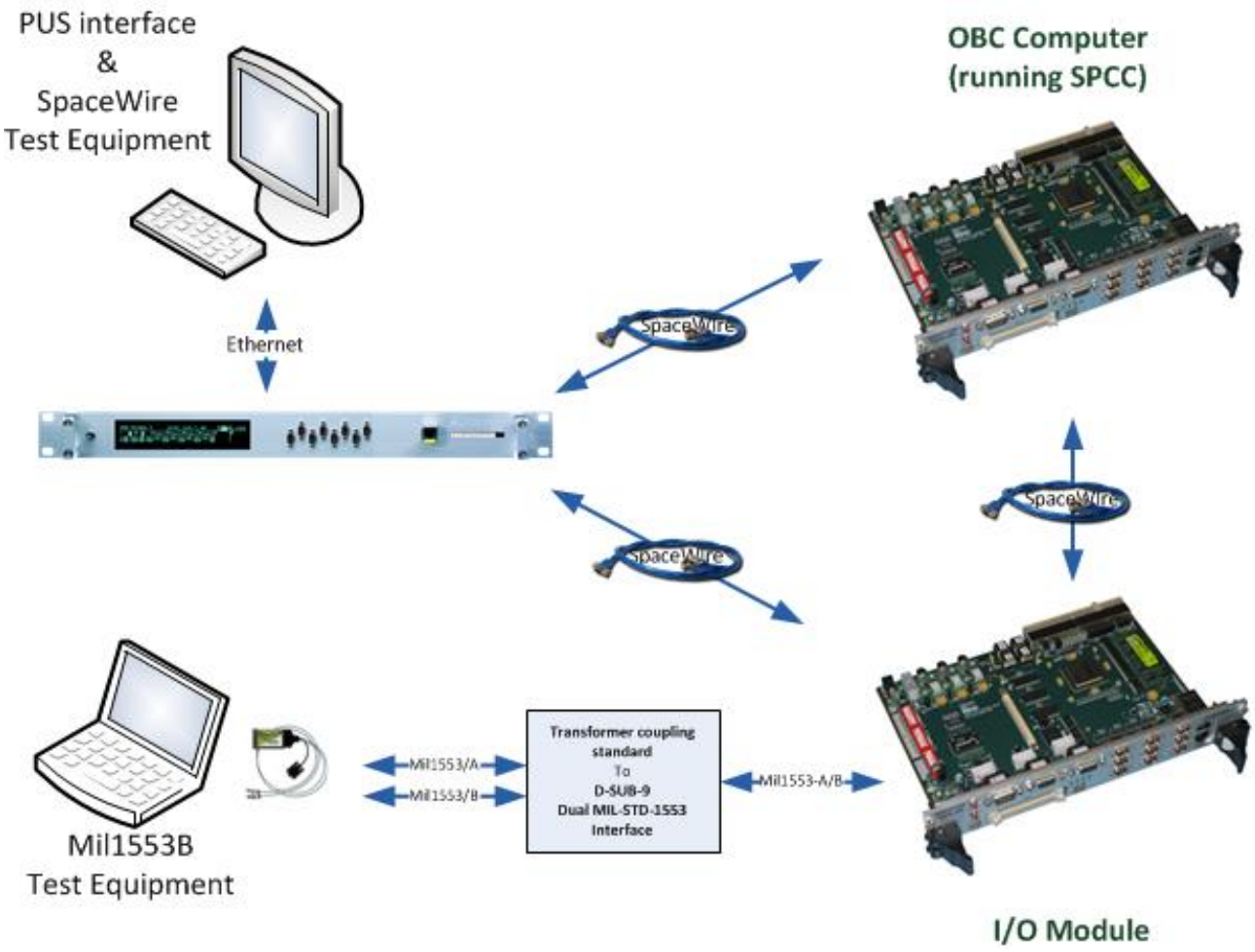
Family	Identifier	Name
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedure
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Standardised life-cycle model
	ALC_TAT.1	Compliance with implementation standards
TESTS	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

EAL1: Functionally Tested
EAL2: Structurally Tested
EAL3: Methodically Tested and Checked
EAL4: Methodically Designed, Tested, and Reviewed
EAL5: Semi-formally Designed and Tested
EAL6: Semi-formally Verified Design and Tested
EAL7: Formally Verified Design and Tested

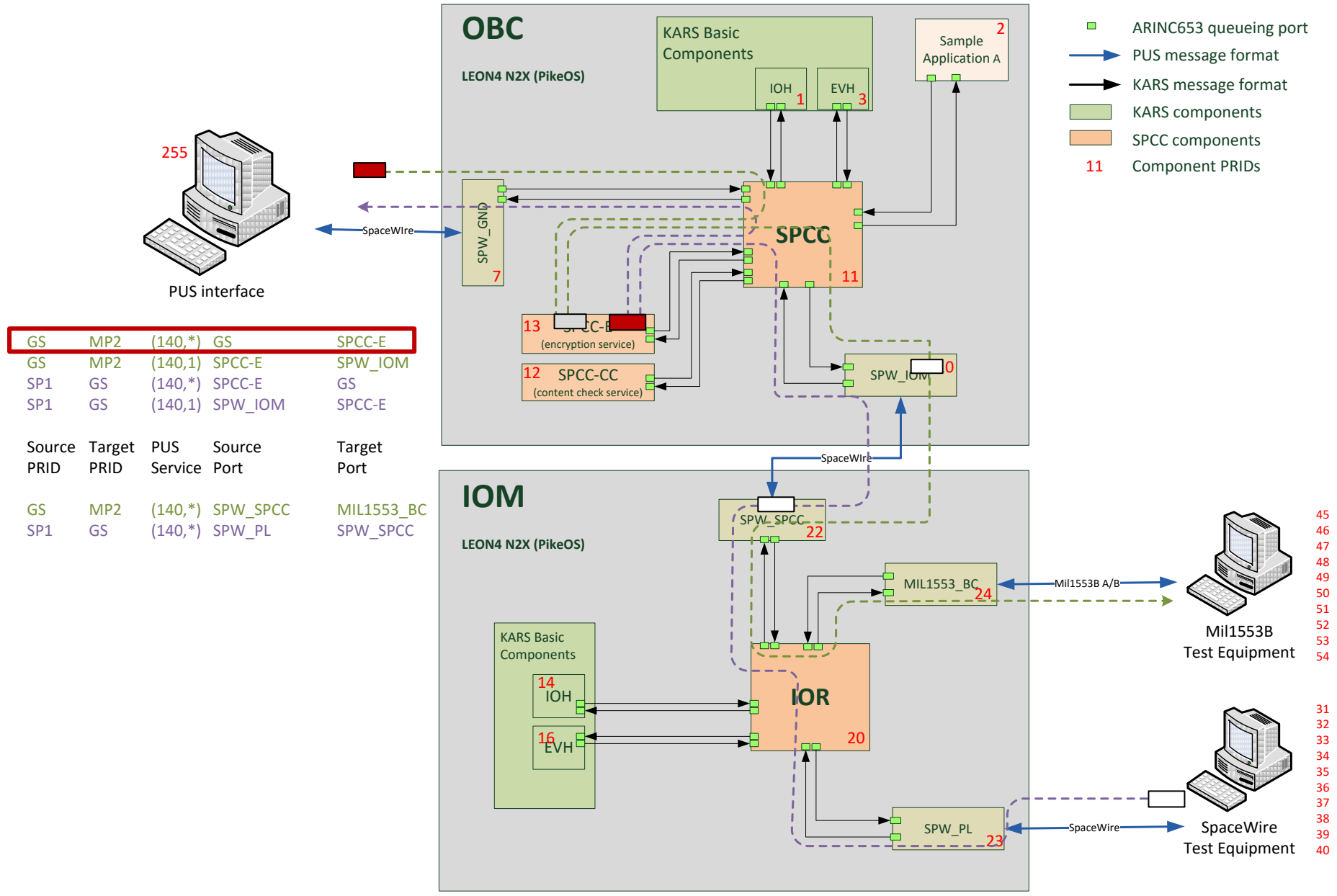


Validation Results

- Validation platform:
  - Leon4 with simulated equipments connected via
    - SpaceWire and
    - MIL1553.



Message Routing Example



Source PRID	Target PRID	PUS Service	Source Port	Target Port
GS	MP2	(140,*)	GS	SPCC-E
GS	MP2	(140,1)	SPCC-E	SPW_IOM
SP1	GS	(140,*)	SPCC-E	GS
SP1	GS	(140,1)	SPW_IOM	SPCC-E
GS	MP2	(140,*)	SPW_SPCC	MIL1553_BC
SP1	GS	(140,*)	SPW_PL	SPW_SPCC

Time measurements and data rate

- **Required:**

  1 OBC, 4 Payloads, 10 TC/s and 20TM/s per element,

  max. packet size:1024 = 30*5*1024Byte/s = **1229kiB/s**
- **Achieved:**
  - IO overhead: *0.12ms* (time of execution of void IO call),
  - Message transfer time between applic. via SPCC: *1.5ms*
  - Data transfer between two SpW ports via the PikeOS SpW driver: *0.4ms … 0.43ms* (depending on packet size)
  - maximum data transfer rate: ***2340kiB/s***.

Validation Results

- Aim at

EAL1: Functionally Tested
EAL2: Structurally Tested
EAL3: Methodically Tested and Checked
EAL4: Methodically Designed, Tested, and Reviewed
EAL5: Semi-formally Designed and Tested
EAL6: Semi-formally Verified Design and Tested
EAL7: Formally Verified Design and Tested

- System test cases: 46
- Acceptance test cases: 16
- approx. 80% of the requirements are verified by testing, 20% by review and inspection.
- Requirements coverage:
  - ✓ 100% for 114 software requirements and 98 user requirements.
  - – *Independent testing has not been performed ➔ EAL 4*

Technology Readiness Level (TRL)

Models	TRL
Actual system „flight proven“	TRL 9
Actual System „flight qualified“	TRL 8
FM (Flight Model) PFM (Protoflight Model)	TRL 7
QM (Qualification Model) EQM (Engineering Qual. Model)	TRL 6
EM (Engineering Model)	**TRL 5**
EBB (Elegant Breadboard)	TRL 4
BB (Breadboard Model)	TRL 3
Technology concept	TRL 2
Basic principles	TRL 1

goal

Definition TRL 5:

(1) *System/subsystem/component validation in relevant environment:*
(2) *Thorough testing of prototyping in representative environment.*
(3) *Basic technology elements integrated with reasonably realistic supporting elements.*
(4) *Prototyping implementations conform to target environment and interfaces.*

SPCC Implementation:

(1) YES: *see demonstrator setup*
(2) YES*: 148 UT, 46 ST, 16 AT*
(3) YES*: Software components embedded in TSP environment on next generation platform computer.*
(4) YES*: LEON 4 with MIL1553 and SpW Interfaces.*

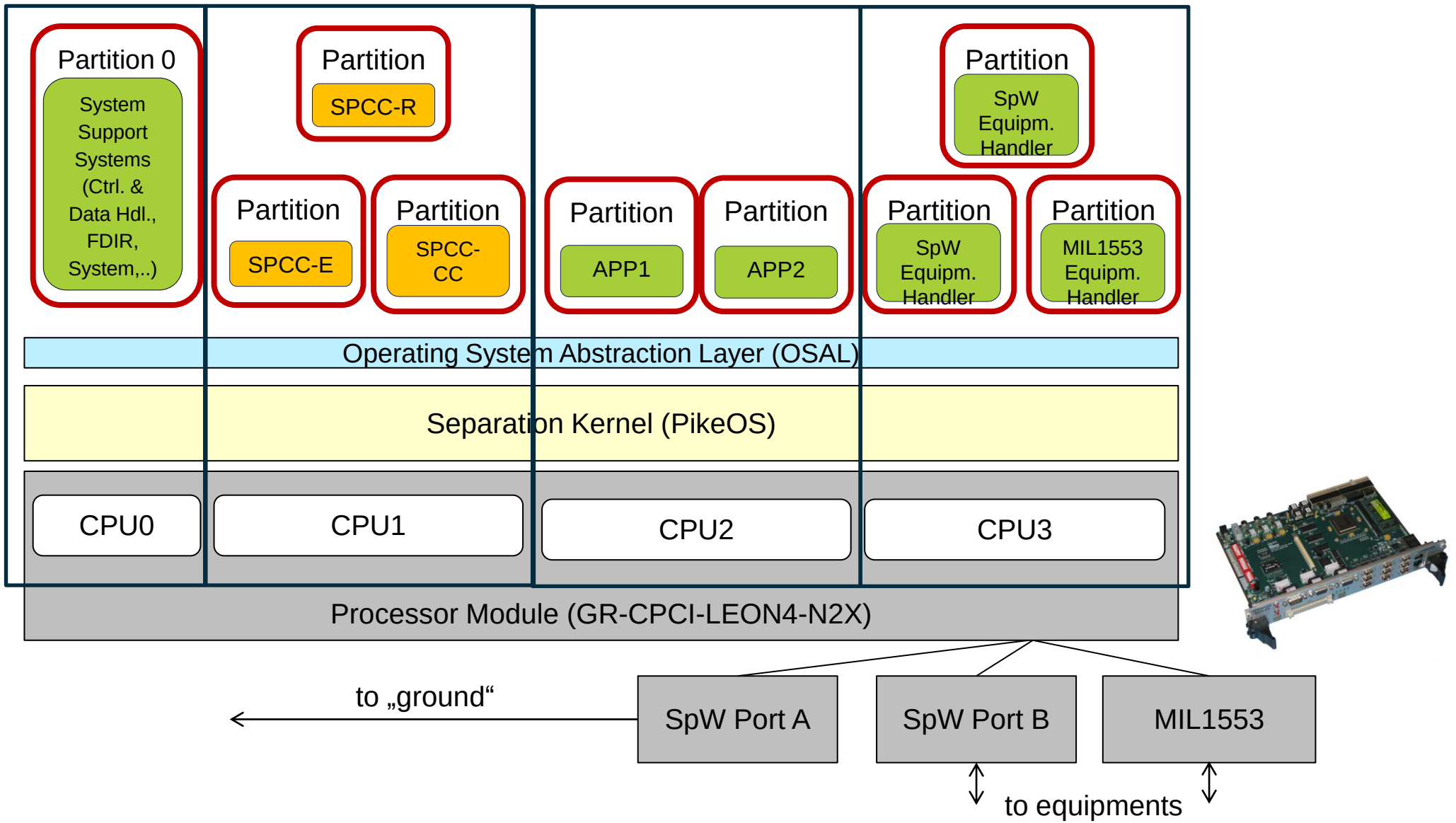
Conclusion (1)

- The implemented architecture allows to combine **safety** and **security** features on **one platform**.
  - ✓ the additional costs when introducing security on-board a satellite in terms of processing resources, mass, power consumption and development effort is limited.

Conclusion (2)

- **SPCC implements a MILS compliant architecture**
  - ✓ a CPU board that provides privilege modes, MMU and a memory bus,
  - ✓ a separation kernel guaranteeing separation by allocation of CPU time and memory to partitions
  - ✓ controlled information flow by configuring communication rights of partitions,
  - ✓ software components providing crypto functionality implementing the information flow policy.
- The TRL achieved is five
- The EAL achieved is four

Utilizing Multicore - Example



Questions ?

OR

Darts ?