# On-board Software Reference Architecture for Payloads

Prime: Space Systems Finland (FIN)

Subco: Evolving Systems Consulting (CZ)

Duration: Feb 2014 – Nov 2015

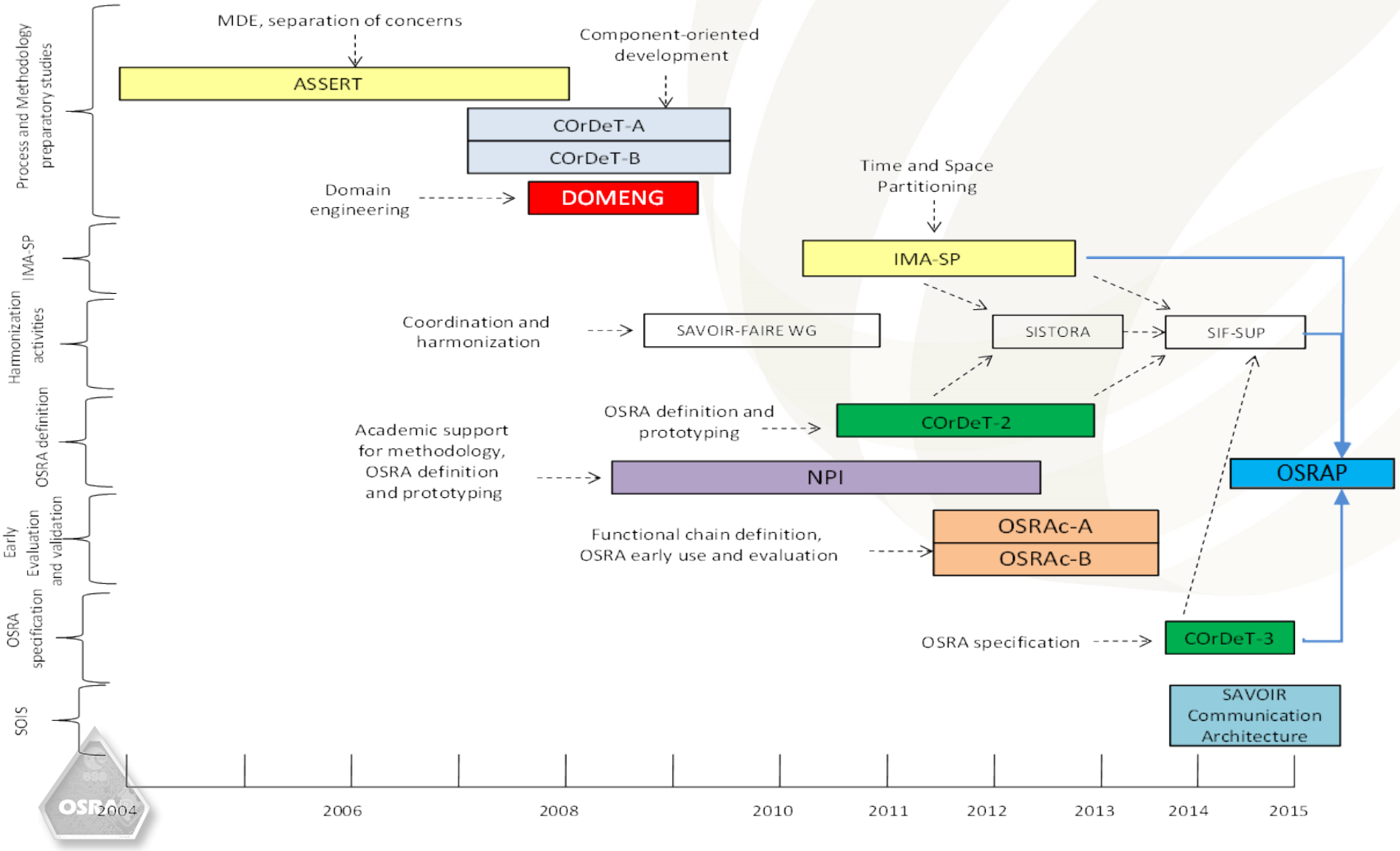
Contract No: 4000110034/13/NL/LvH

Technical officer: A. Rugina

# Overview

1. Introduction
2. Timeline and project logic
3. Payload Domain
4. OSRA-P Definition
5. OSRA-P Workshop
6. Case studies
7. Conclusions

# Timeline


Process and Methodology preparatory studies
IMA-SP
Harmonization activities
OSRA definition
Early Evaluation and validation
OSRA specification
SOIS
MDE, separation of concerns
ASSERT
Component-oriented development
COrDeT-A
COrDeT-B
Domain engineering
DOMENG
Time and Space Partitioning
IMA-SP
Coordination and harmonization
SAVOIR-FAIRE WG
SISTORA
SIF-SUP
OSRA definition and prototyping
COrDeT-2
Academic support for methodology, OSRA definition and prototyping
NPI
OSRAP
Functional chain definition, OSRA early use and evaluation
OSRAc-A
OSRAc-B
OSRA specification
COrDeT-3
SAVOIR Communication Architecture
2004
2006
2008
2010
2011
2012
2013
2014
2015

# Capabilities Matrix

| Payload HW | | | | | | | |
|---|---|---|---|---|---|---|---|
| Processor module | RAM available [MB] | Memory Storage Needs of Flight SW [MB] | On-board Mass Memory available [MB] | Computational Power requirements of IDPU [MIPS or MHz] | Internal Network Interface to Payload HW | External Payload Interfaces to S/C | EDAC |

| Payload SW | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Payload specific FDIR | RTOS | Mode Management | Duration of control loops, if any | SCC (DAL) | Memory scrubbing | Programming languages | Average Load on processor of FSW [idle, and worst case, in CPU %] | LOC |

| Communication services | | | | |
|---|---|---|---|---|
| Downlink bandwidth available to instrument [rate, bits/s] | TM Services2 | Number of TM packets | TC Services | Number of TC packets |

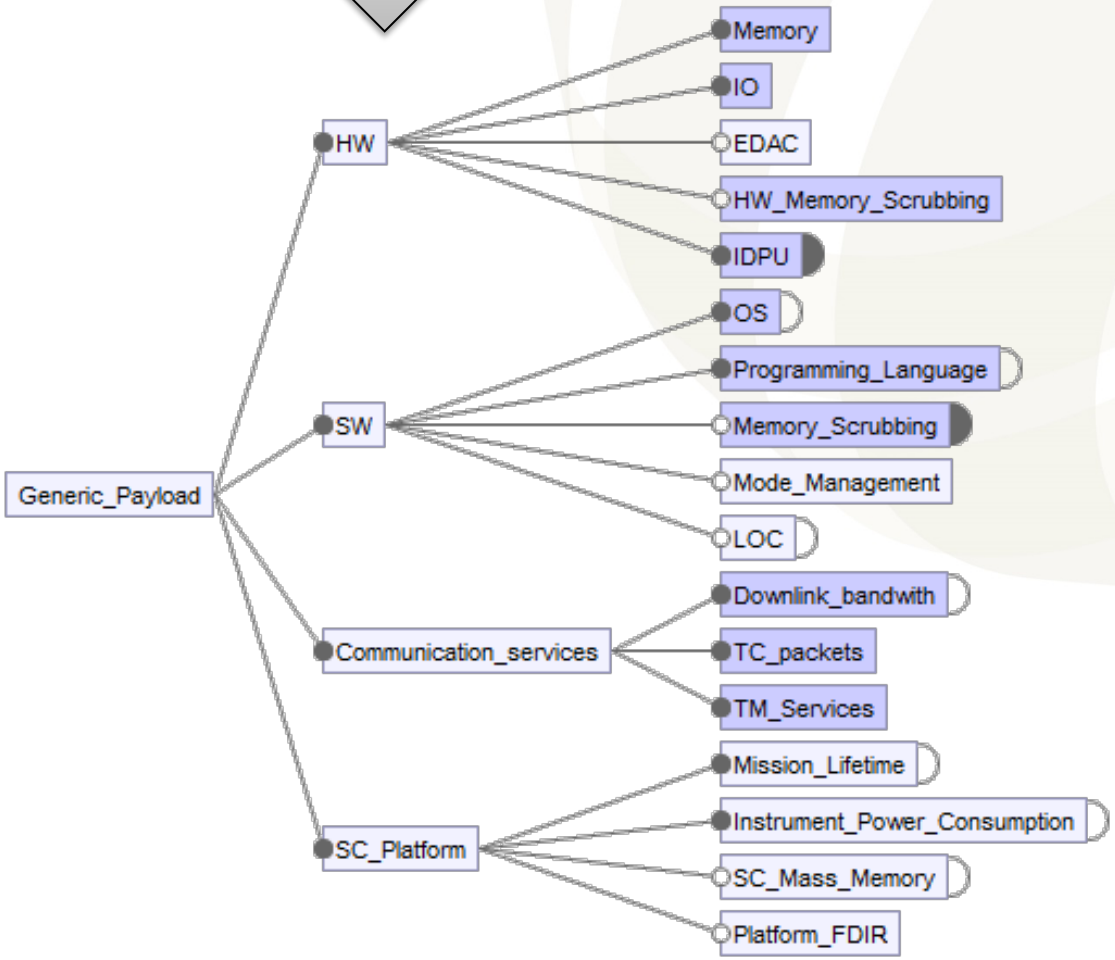
| Spacecraft Platform | | | |
|---|---|---|---|
| Planned mission lifetime [months] | Instrument Power Consumption (max/avg) [W] | S/C Mass Memory available [MB] | Platform FDIR |

# Capabilities Matrix (numerical Results)

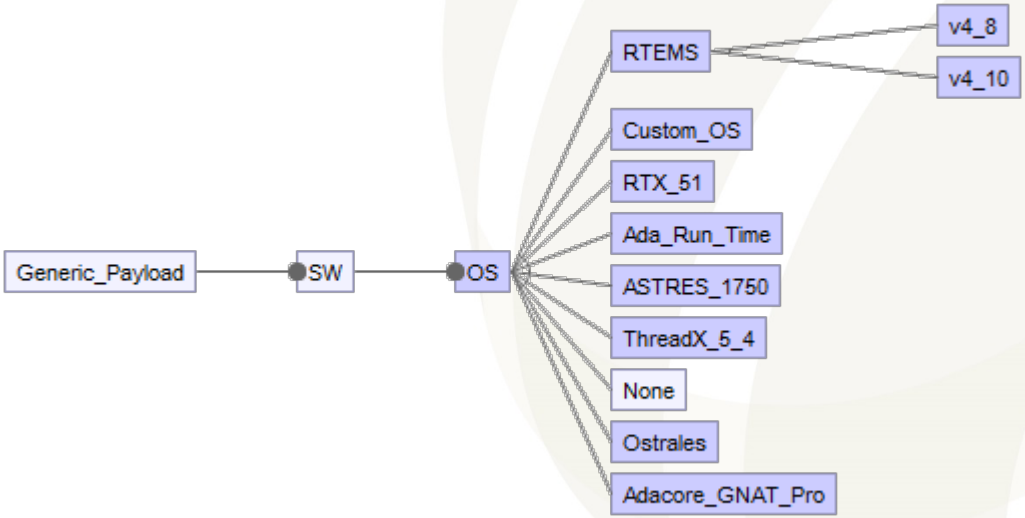
| Mission | | Payload HW | | | | Payload SW | | Communication services | Spacecraft Platform | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Payload instrument reference name | Platform/ Spacecraft Name | RAM available [MB] | Memory Storage Needs of Flight SW [MB] | On-board Mass Memory available [MB] | Computational Power requirements of IDPU [MHz] | Mode Management | Average Load on processor of FSW [idle, and worst case, in CPU %] | Downlink bandwidth available to instrument [rate, bits/s] | Planned mission lifetime [months] | Instrument Power Consumption (max/avg) [W] | S/C Mass Memory available [MB] |
| **SIXS/MIXS** | BepiColombo | 4 | 1 | 0 | 25.00 | 13 | 86.00% | 401,604.00 | 12 | 46 | |
| **FCI** | MTG-I | 8 | | 0 | 20.00 | - | 0.00% | | 240 | N-A | |
| **IRS** | MTG-S | 8 | | 0 | 20.00 | - | 0.00% | | 240 | N-A | |
| **S4 UVN** | MTG-S | 50 | 2 | 0 | 64.00 | 6 | 0.00% | 4,000.00 | | | |
| **SAR** | Sentinel 1 | 8 | 2 | 0 | 80.00 | 9 | 57.00% | | 84 | (3650w/?) | 176,250.00 |
| **EUI** | Solar Orbiter | 4 | 2 | 7000 | 40.00 | 5 | 60.00% | 20,500.00 | 120 | 30 | 6,650.00 |
| **RPW** | Solar Orbiter | 64 | 64 | 4 | 25.00 | 9 | 60.00% | 5,500.00 | 84 | 23 | 3,648.00 |
| **EPD** | Solar Orbiter | 128 | 1 | 0 | 20.00 | 5 | 47.00% | 3,500.00 | 84 | 28 | 2,393.60 |
| **STIX** | Solar Orbiter | 128 | 10 | 8162 | 20.00 | 5 | 75.00% | 700.00 | 84 | 8.6 | 230.00 |
| **PHI** | Solar Orbiter | 256 | 4 | 64 | 0.00 | 9 | 20.00% | 20,500.00 | 120 | 16 | 6,809.60 |
| **ACC3** | SWARM | 0 | 0.064 | 0 | 12.00 | 7 | 0.00% | 1,310.00 | 36 | 8.2 | - |
| **AVERAGE** | | 60 | 9.56 | 1,384.55 | 29.64 | 7.56 | 36.82% | 57,201.75 | 110.40 | 22.83 | 27,997.31 |
| **SUMS** | | 658 | 86.06 | 15,230.00 | 326.00 | 68 | | 457,614.00 | 1,104.00 | 159.80 | 195,981.20 |

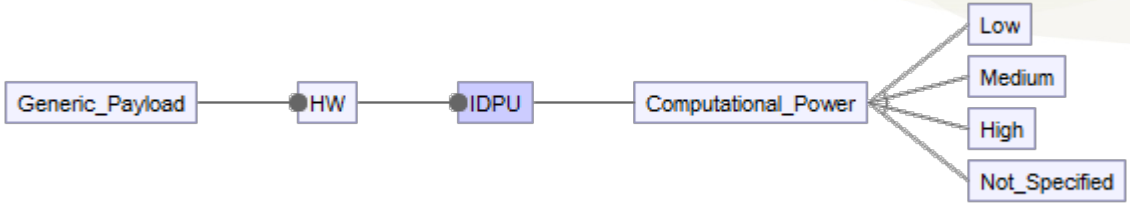
# Feature Diagrams

| Mission | | Payload HW | | | | Payload SW | | Communication services | Spacecraft Platform | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Payload instrument reference name | Platform/ Spacecraft Name | RAM available [MB] | Memory Storage Needs of Flight SW [MB] | On-board Mass Memory available [MB] | Computational req ents of ID MHz] | Mode Management | Average Load on processor of FSW [idle, and worst case, in CPU %] | Downlink bandwidth available to instrument [rate, bits/s] | Planned mission lifetime [months] | Instrument Power Consumption (max/avg) [W] | S/C Mass Memory available [MB] |

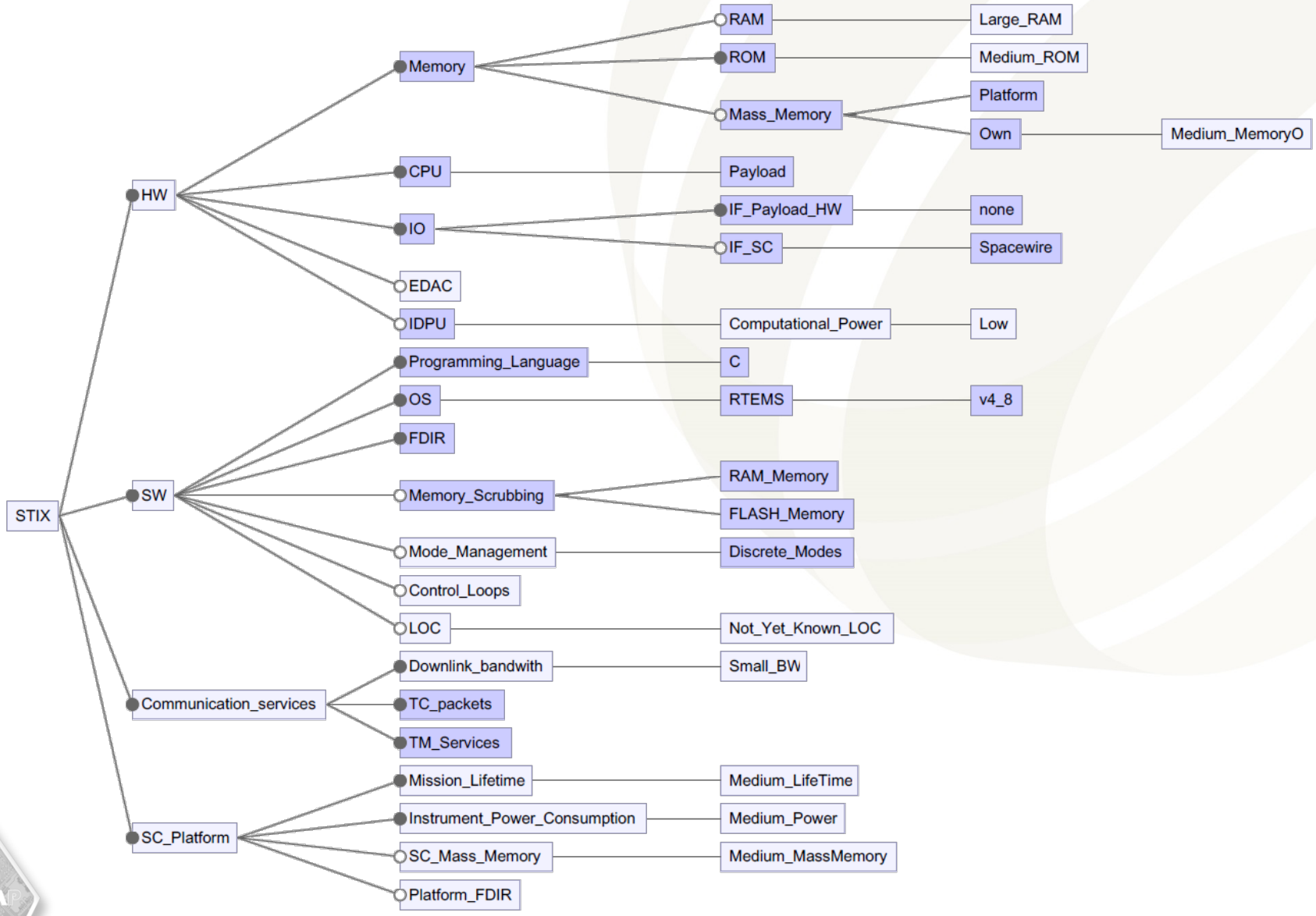


# Feature Diagrams

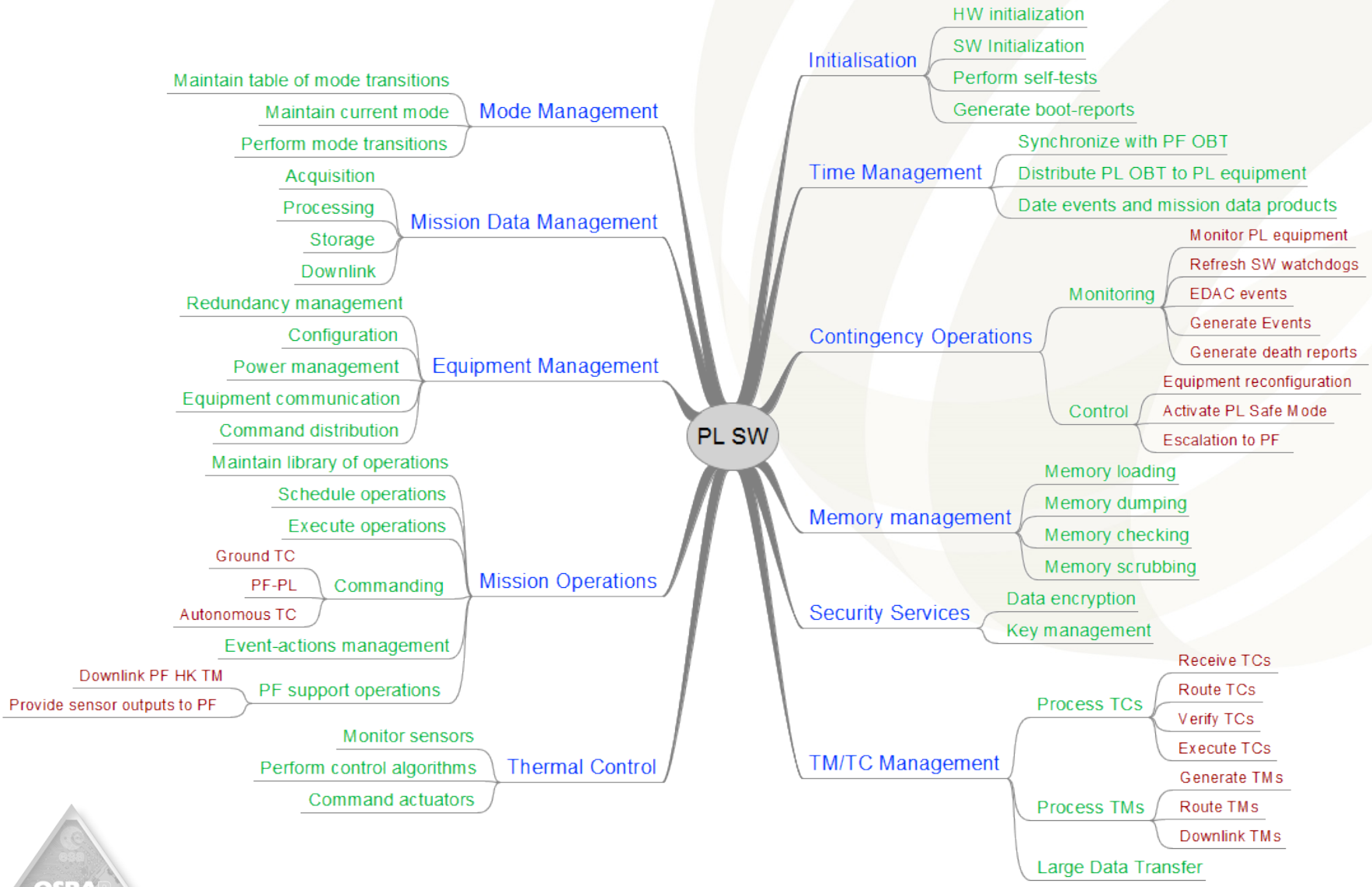


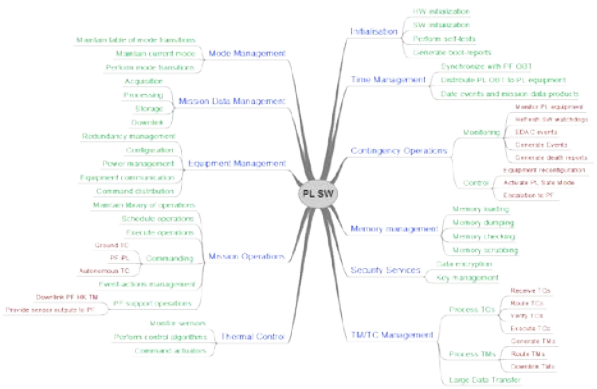
# Feature Diagram - STIX



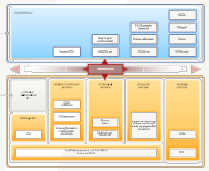
# Functional Decomposition

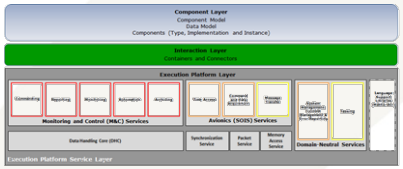


# Towards OSRA-P




SAVOIR



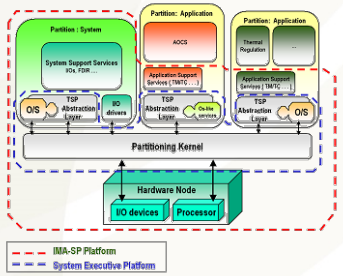


COrDeT

Harmonized SAVOIR software reference architecture (Component based + IMA)

SIFSUP

IMA-SP




Payload domain

**OSRA-P Architecture**

# Payload Deployment Options

**Monolithic**

without TSP, generally on dedicated HW node

**Partitioned**

with TSP, on non-dedicated HW node

# Payload Deployment Options

## @ RUNTIME

**Monolithic**

**Classical**

- RTOS
- Common drivers
- Specific Drivers
- BSP

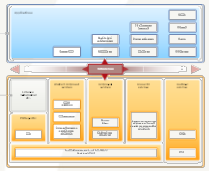
**Partitioned**

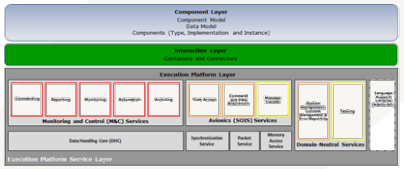
**TSP based**

- Guest RTOS
- Guest BSP
- Common drivers
- Specific drivers
- TSAL

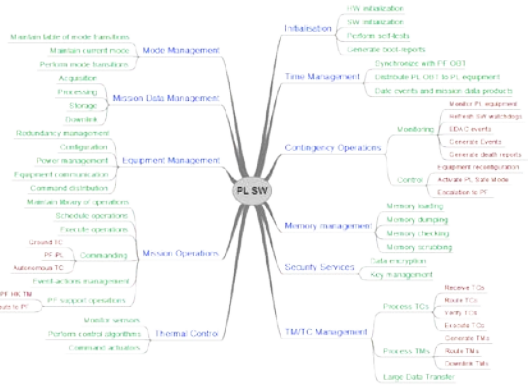
# Towards OSRA-P

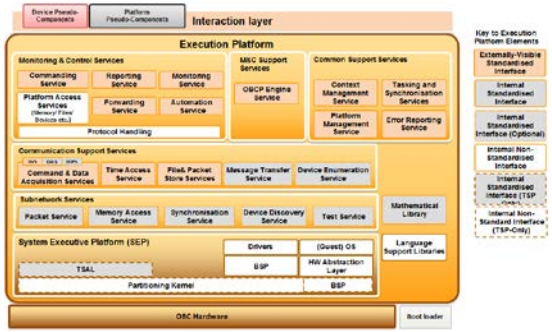
SAVOIR



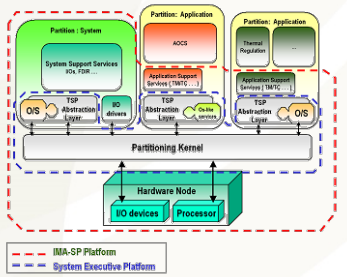


COrDeT



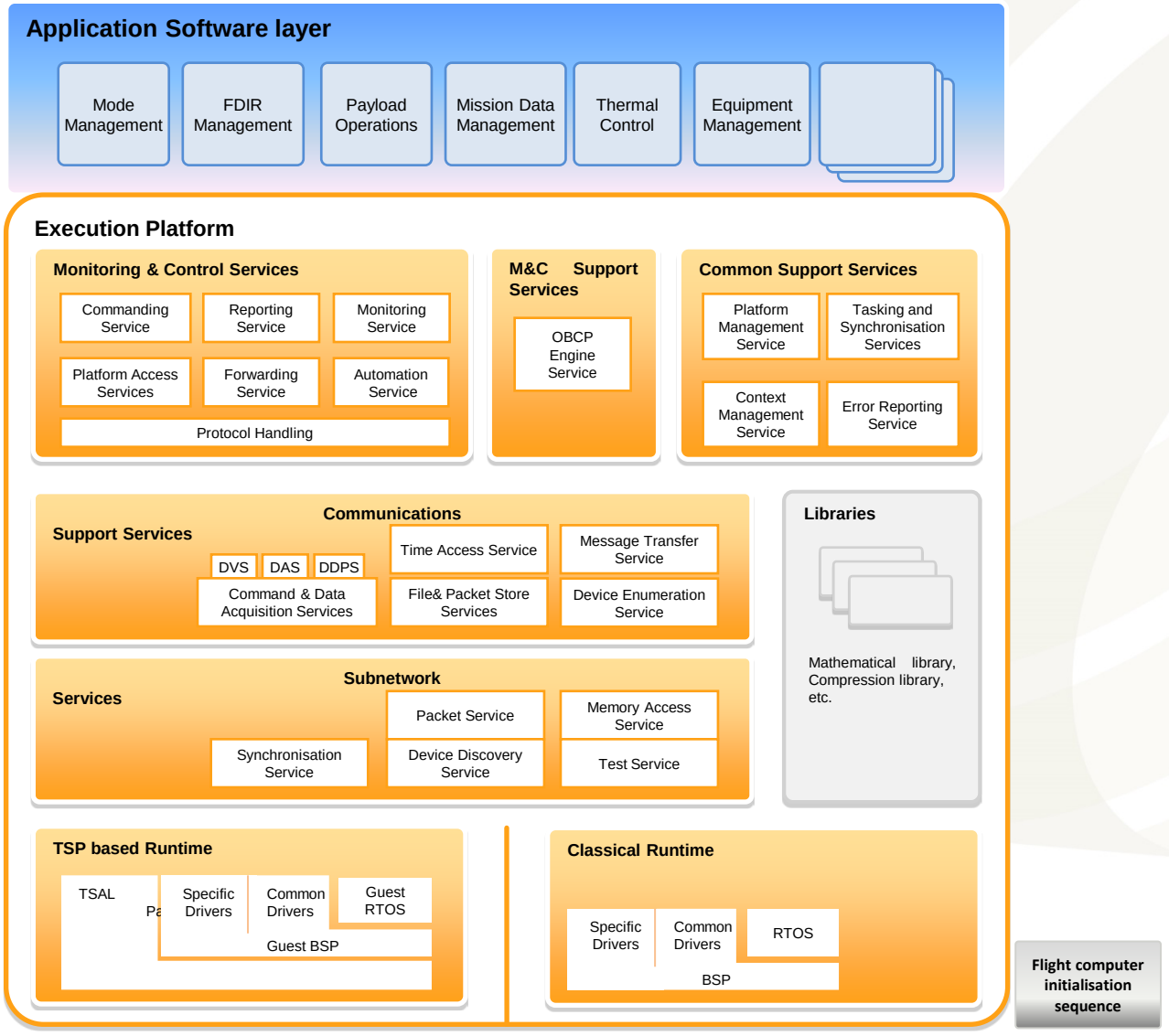

IMA-SP




Payload domain

**OSRA-P Architecture**

# OSRA-P Architecture



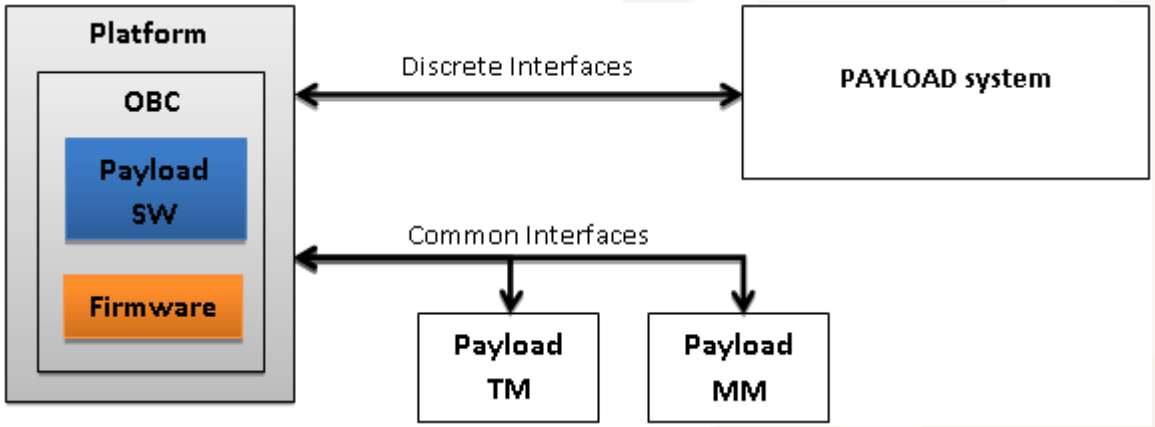
# Payload-Platform interface

Three main types (SAVOIR - ASRA):

1. Direct PL interface
2. PL interface unit (PLIU)
3. PL management unit (PLMU)

OSRA-P is PL application software: what do these PL-PF interface approaches mean for PL application software?

# 1. Direct Payload-Platform Interface




PL SW integrated with PF SW

- PF and PL share same OBC (onboard computer)
- **PF ASW and PL ASW share OSRA-P execution platform**

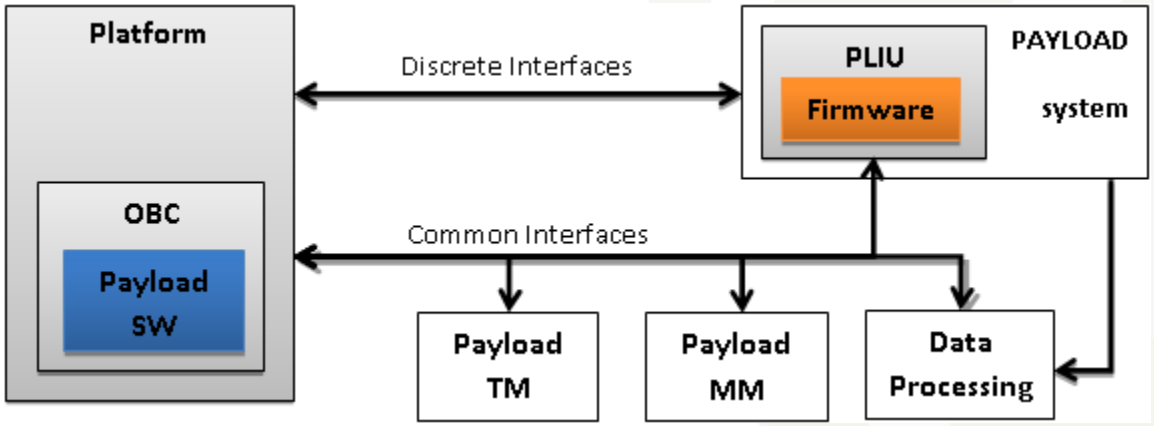
TSP-based runtime:

- PL and PF development processes are more independent
- Different criticality of PL and PF SW
- I/O partitioning

Classical runtime:

- PL and PF development processes depend on each other
- Same criticality of PL and PF SW

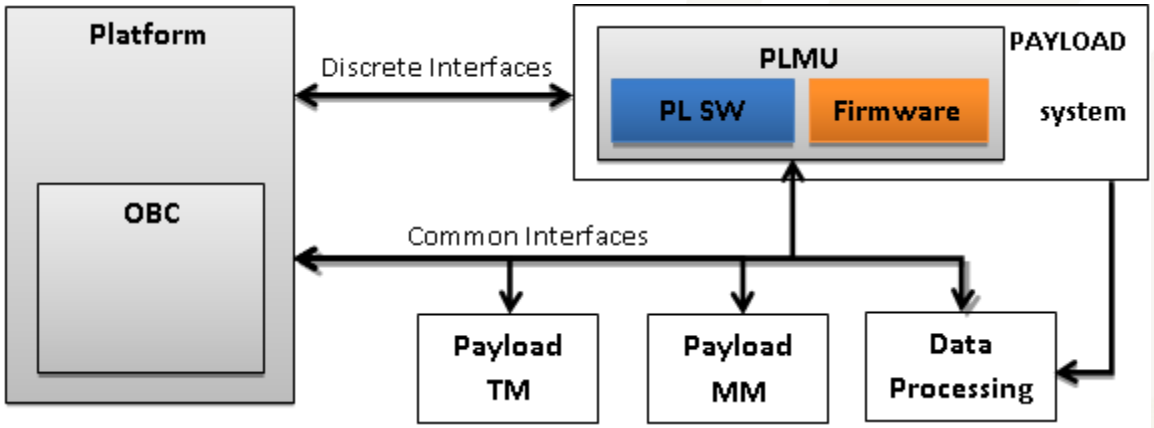
# 2. Payload Interface-Unit Interface




PL interface-Unit: (programmable HW, FPGA/ASICs)

- Similar SW characteristics as Direct PL-PF interface
- Some SW functions (possibly EP functions) are delegated to the PLIU

# 3. Payload Management-Unit Interface




PL Management-Unit:

- PL processor running PL SW
- (Programmable) HW running PL functions

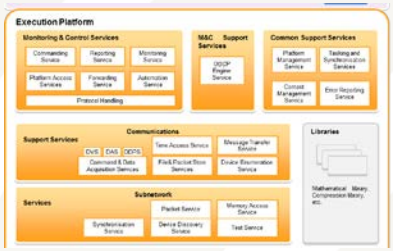
Independence between PF and PL SW

- PF and PL on different OBCs
- **PF ASW and PL ASW have their own execution platform**
- Independent development processes
- Possibly different criticalities for PL and PF SW

## OSRA-P execution Platform Configuration

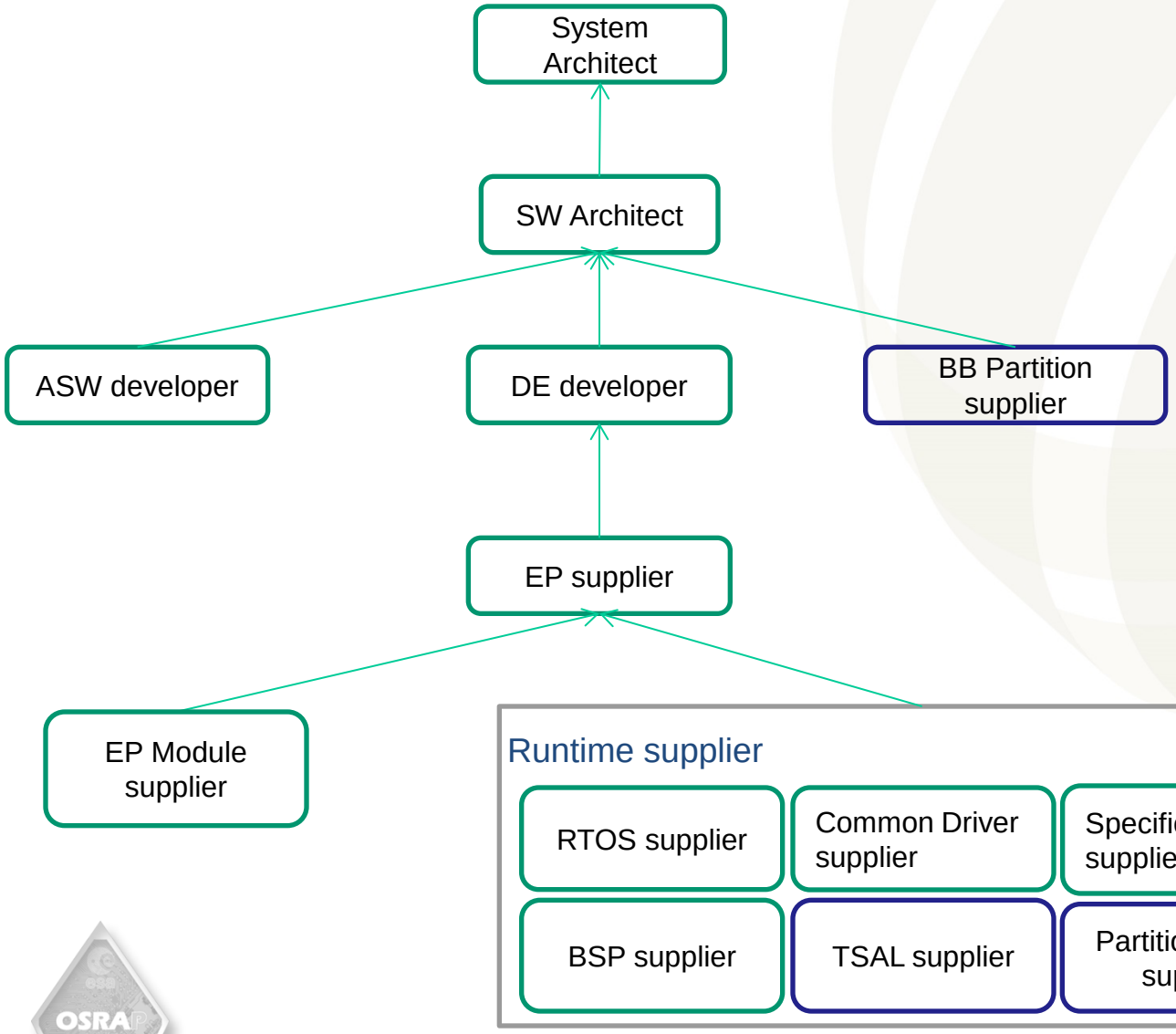
1. Module selection (e.g., OBCP engine, Memory Access Service)
2. Source code adaption (e.g., Common drivers)
3. New module integration (e.g., Specific drivers, libraries)
4. Executable image generation (e.g., tayloring based on mission SDB)

# Relation to PUS




| Service | Service name | EP Module | Applicability M: mandatory O: optional |
|---|---|---|---|
| 1 | Telecommand verification service | Protocol Handling | M |
| 2 | Device command distribution service | Platform Access Service | M |
| 3 | Housekeeping & diagnostic data reporting service | Reporting Service | M |
| 4 | Parameter statistics reporting service | Reporting Service | O |
| 5 | Event reporting service | Reporting service | M |
| 6 | Memory management service | Platform Access Service | M |
| 7 | Not used | | |
| 8 | Function management service | Commanding Service | O |
| 9 | Time management service | Platform Access Service | M |
| 10 | Not used | | |
| 11 | On-board operations scheduling service | Automation Service | O |
| 12 | On-board monitoring service | Monitoring Service | M |
| 13 | Large data transfer service | FPSS, Platform Access Service | O |
| 14 | Packet forwarding control service | Forwarding Service | O |
| 15 | On-board storage and retrieval service | FPSS, Platform Access Service | O |
| 16 | Not used | | |
| 17 | Test service | Platform Access Service | M |
| 18 | On-board operations procedure service | OBCP Engine | O |
| 19 | Event Action | Automation service | M |

# OSRA-P Roles




Each role includes responsibilities for

- Specification
- Design
- Integration
- Validation
- Qualification

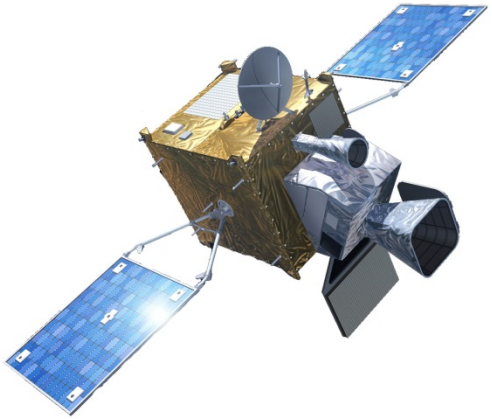
# OSRAP Workshop Discussion & Feedback

| Discussion topics / feedback | |
|---|---|
| • Data pool: where / how? | Distributed over EP modules |
| • Reporting service is responsible for Parameter setting | Currently, as in COrDeT OSRA |
| • Mandatory and optional EP modules | EP modules are selectable |
| • Support for time-and-space partitioning | 2 EP runtimes |
| • Common and specific HW drivers | Configuration vs new modules |
| • Actors, roles, contractual aspects | OSRA-P roles applied to case study |

43 Attendees (16 from ESA, 27 from industry)
From 27 industry attendees, 6 (22%) provided feedback

# Case study 1: MTG FCI/IRS ICU SW

## Focus: Development Process



Two instruments (imager & sounder)

Similar SW architecture based on an *MTG Execution Platform*

MTG execution platform contains shared FCI/IRS functionality

FCI and IRS specific functionality implemented on top of MTG execution platform

# Case study: MTG FCI/IRS ICU SW

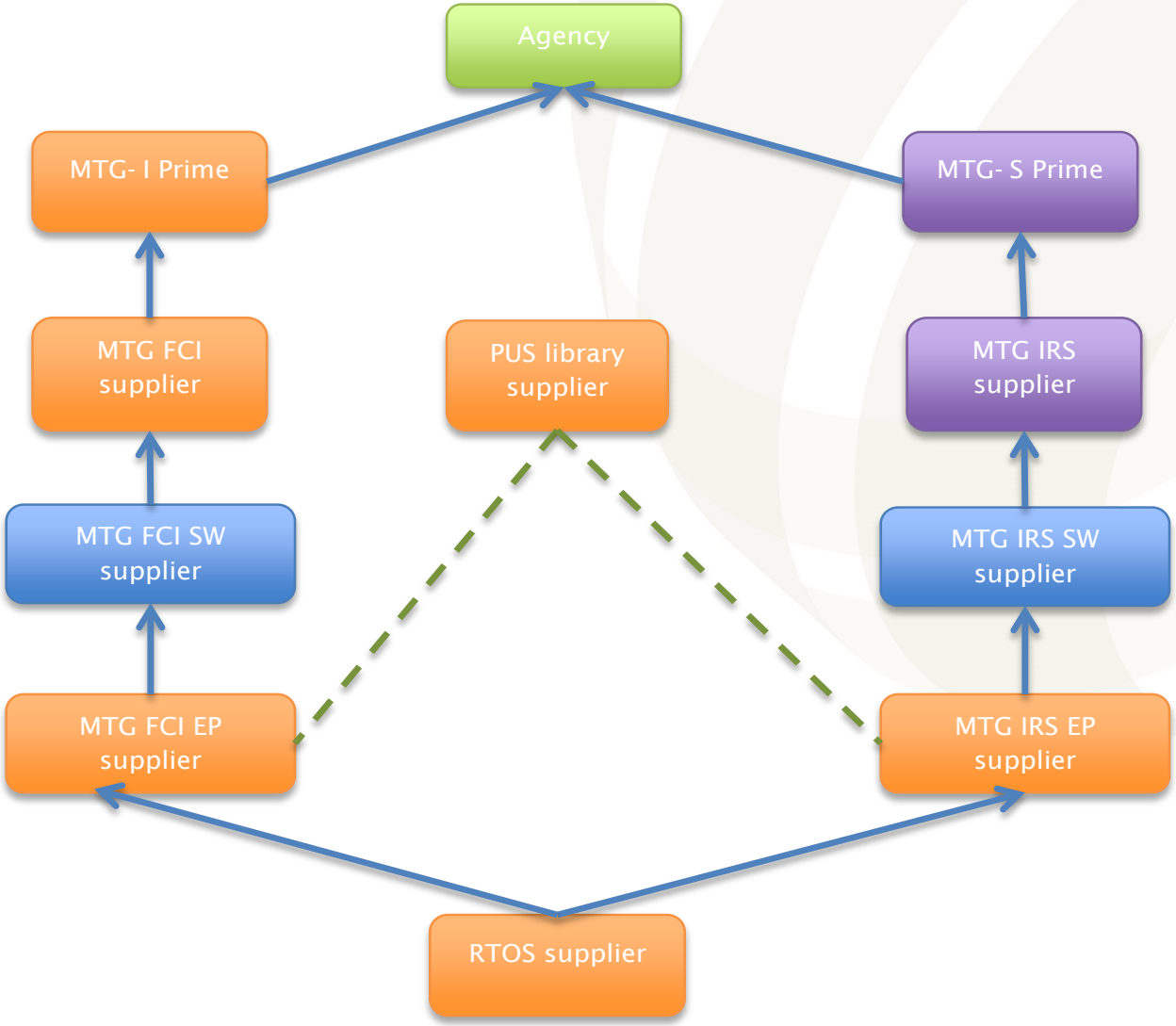
FCI/IRS instantiation of OSRA-P:

Use generic OSRA-P functionality as much as possible

Remaining, FCI/IRS specific, functionality:

1. Workplan management (mission operations)
2. Thermal control
3. PUS 128+ (application specific services)
4. Specific HW management

# MTG FCI/IRS ICU ASW Actors

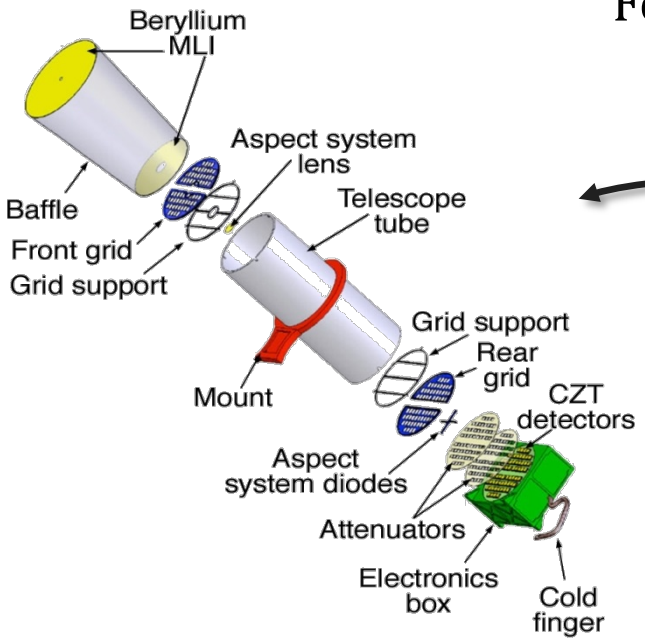


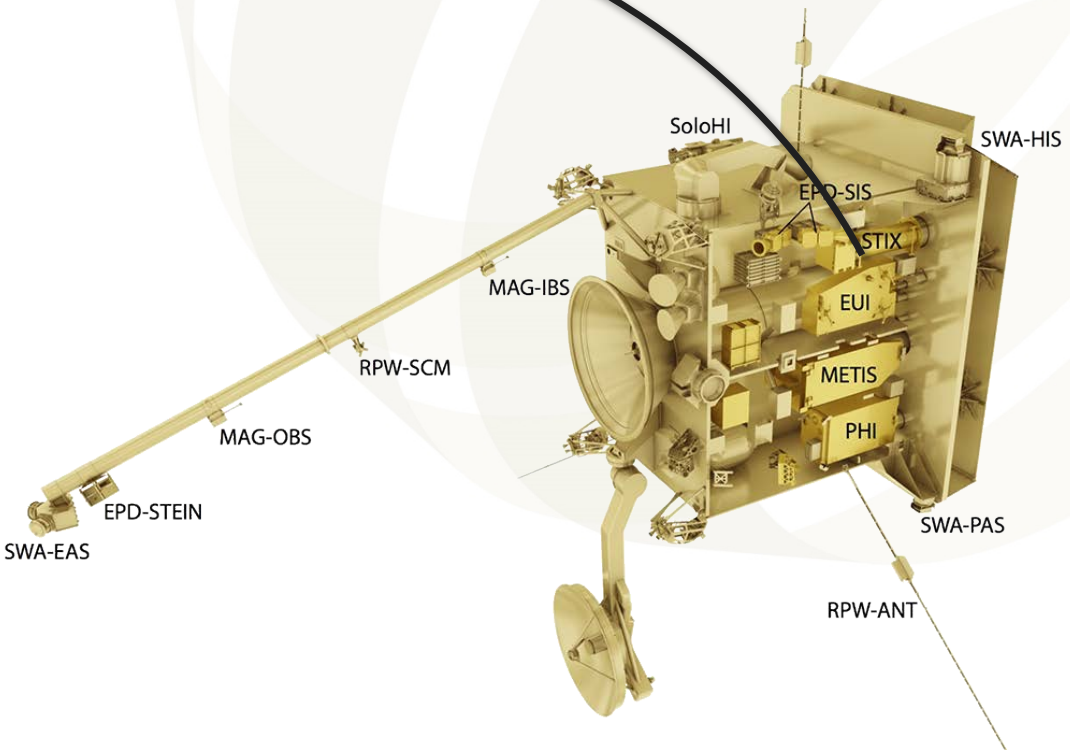
# Mapping roles and (FCI) actors

| Role | Actor |
|---|---|
| System Architect | MTG FCI prime |
| SW Architect | MTG FCI SW supplier |
| ASW supplier | MTG FCI SW supplier |
| Design Environment Engineer | MTG FCI Execution Platform supplier |
| Black-Box Partition Supplier | N.A. |
| Execution Platform Supplier | MTG FCI Execution Platform supplier |
| Execution Platform Module Supplier | MTG FCI Execution Platform supplier |
| Common driver supplier | MTG FCI OBC supplier |
| Specific driver supplier | MTG FCI Execution Platform supplier |
| BSP | *MTG FCI OBC supplier* |
| Guest RTOS Supplier | MTG FCI Execution Platform supplier |
| Partitioning Kernel Supplier | N.A. |

# Case study 2: STIX

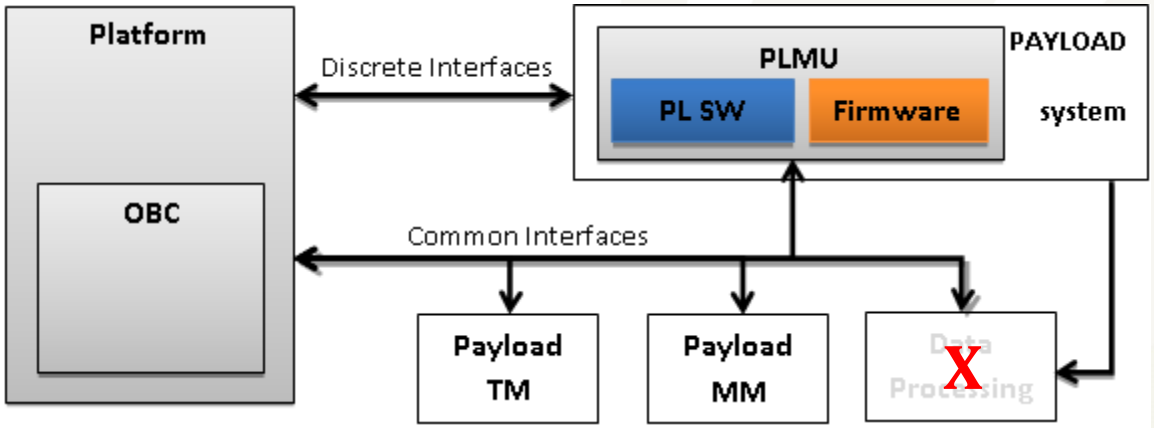
## Focus: Technical Depth



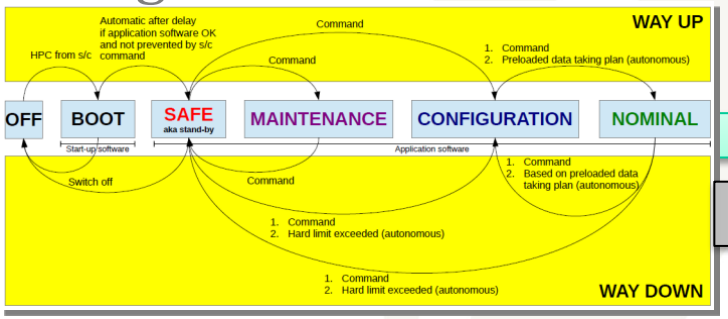

The rebuilding of a FSW's static architecture based on its TMTC structure/ICD using the EP

# PF – PL Type: Payload Management-Unit Interface



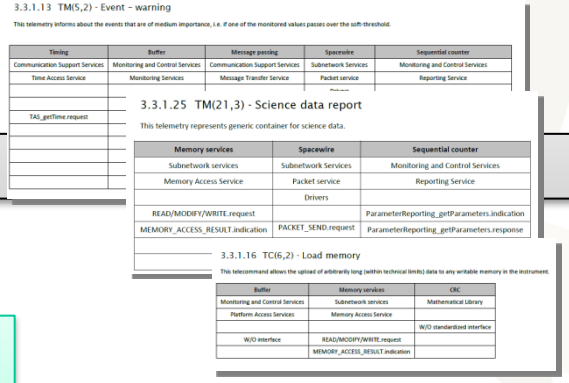

- PL Management-Unit:
  - PL processor (ICU) running PL ASW
  - (Programmable) HW running PL functions
  - Local (private) MM also available
- PF-PL communication via standardized link (SpW)
- Independence between PF and PL SW
  - Typical ECSS waterfall development processes
  - B criticality level (mission critical)

# Re-design of STIX FSW in OSRAP




Current Development

OSRAP use case



3.3.1.13 TM(5,2) - Event – warning

This telemetry informs about the events that are of medium importance, i.e. if one of the monitored values passes over the soft-threshold.

| Timing | Buffer | Message passing | Spacewire | Sequential counter |
|---|---|---|---|---|
| Communication Support Services | Monitoring and Control Services | Communication Support Services | Subnetwork Services | Monitoring and Control Services |
| Time Access Service | Monitoring Services | Message Transfer Service | Packet service | Reporting Service |

TAS_getTime.request

3.3.1.25 TM(21,3) - Science data report

This telemetry represents generic container for science data.

| Memory services | Spacewire | Sequential counter |
|---|---|---|
| Subnetwork services | Subnetwork Services | Monitoring and Control Services |
| Memory Access Service | Packet service | Reporting Service |
| | Drivers | |
| READ/MODIFY/WRITE.request | | ParameterReporting_getParameters.indication |
| MEMORY_ACCESS_RESULT.indication | PACKET_SEND.request | ParameterReporting_getParameters.response |

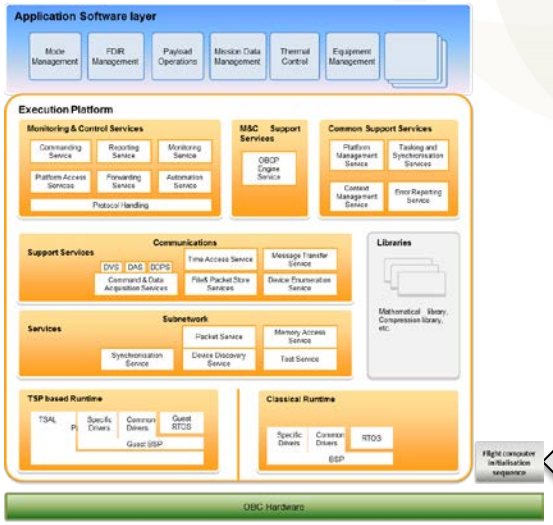
3.3.1.16 TC(6,2) - Load memory

This telecommand allows the upload of arbitrarily long (within technical limits) data to any writable memory in the instrument.

| Buffer | Memory services | CRC |
|---|---|---|
| Monitoring and Control Services | Subnetwork services | Mathematical Library |
| Platform Access Services | Memory Access Service | |
| | | W/O standardized interface |
| W/O interface | READ/MODIFY/WRITE.request | |
| | MEMORY_ACCESS_RESULT.indication | |

| TC/TM | | Start-up SW | Application SW operational modes | | | |
|---|---|---|---|---|---|---|
| Service/ subservice | Short Description | BOOT | SAFE | MAINTENANCE | CONFIGURATION | NOMINAL |
| TM(1,1) | TC rec ACK | X | X | X | X | X |
| TM(1,2) | TC rec NACK | X | X | X | X | X |
| TM(1,7) | TC exec ACK | X | X | X | X | X |
| TM(1,8) | TC exec NACK | X | X | X | X | X |
| TC(3,5) | HK report enable | X | X | X | X | X |
| TC(3,6) | HK report disable | X | X | X | X | X |
| TM(3,25) PC = 4 SID = 1 | Regular HK mini report | X | | | | |
| TM(3,25) PC = 4 SID = 2 | Regular HK maxi report | | X | X | X | X |
| TM(3,25) PC = 5 SID = 4 | Heartbeat | X | X | X | X | X |
| TM(3,25) PC = 8 SID = variable | On-request Parameter report | X | X | X | X | X |
| TC(3,129) | HK set period | | X | X | X | X |
| TM(5,1) | Event – info/progress | X* | X* | X* | X* | X* |
| TM(5,2) | Event – warning | X* | X* | X* | X* | X* |
| TM(5,3) | Event – error (Ground action) | X* | X* | X* | X* | X* |
| TM(5,4) | Event – error (On-board action) | X* | X* | X* | X* | X* |
| TC(6,2) | Load memory | X | | X | | |
| TC(6,5) | Dump memory | X | | X | | |
| TM(6,6) | Memory dump report | X | | X | | |
| TC(6,9) | Check memory | X | | X | | |
| TM(6,10) | Memory check report | X | | X | | |
| TC(9,129) | Accept time update | X | X | X | X | X |
| TC(17,1) | Connection test (ping) | X | X | X | X | X |
| TM(17,2) | Connection test report (ping) | X | X | X | X | X |
| TC(20,128) | Information Distribution to User (STIX) | X | X | X | X | X |
| TC(21,1) | Enable science data transfer | | | X | X | X |
| TC(21,2) | Disable science data transfer | | | X | X | X |
| TM(21,3) | Science data report | | | X | | X |

Background definitions or specs (SOIS, CCSDS)



# Re-design of STIX FSW in OSRAP

Current Development

| Parameter | Value | Remark |
|---|---|---|
| APID – PID | 90 | STIX Command & Control Application |
| APID – Packet Category | 7 | Event |
| Packet data field length - 1 | Variable | - |
| Service Type | 5 | Event reporting |
| Service Subtype | variable | 1, 2, 3, 4 |
| EID (2 octets) | variable | Defined below |
| Parameters (variable length) | variable | Defined below in Table 52, Table 53, Table 54 and Table 55 |

*Table 50: TM(5,X) – Event reporting*

### 6.7.2 TM(5,2) – Error/Anomaly Report – Low Severity (warning)

Implementation according to Solar Orbiter Generic frame and packet structure [AD-09].

| EID | Meaning/parameters/applicability | | |
|---|---|---|---|
| 0x5420 | **Too many IRQs warning report** | | |
| | Too many IRQs detected or spurious IRQs detected | | |
| | Parameters | 1 octet – 8bits | Timer TBC IRQ counter |
| | | 1 octet – 8bits | Space Wire TBC IRQ counter |
| | | 1 octet – 8bits | ADC Read TBC IRQ counter |
| | | 1 octet – 8bits | TBD IRQ counter |
| | | 1 octet – 8bits | TBD IRQ counter |
| | | 1 octet – 8bits | TBD IRQ counter |
| | | 1 octet – 8bits | TBD IRQ counter |
| | | 1 octet – 8bits | TBD IRQ counter |
| | | 1 octet – 8bits | TBD IRQ counter |
| | | 1 octet – 8bits | TBD IRQ counter |
| | Applicability | Any mode (both Start-up and Application SW) | |
| 0x5421 | **Stack pointer problem warning report** | | |

OSRAP use case

### 3.3.1.13 TM(5,2) - Event – warning

This telemetry informs about the events that are of medium importance, i.e. if one of the monitored values passes over the soft-threshold.

| Timing | Buffer | Message passing | Spacewire | Sequential counter |
|---|---|---|---|---|
| Communication Support Services | Monitoring and Control Services | Communication Support Services | Subnetwork Services | Monitoring and Control Services |
| Time Access Service | Monitoring Services | Message Transfer Service | Packet service | Reporting Service |
| | | | Drivers | |
| | | | | |
| TAS_getTime.request | *various* | Send.request | | ParameterReporting_getParameters.indication |
| | | Query.request | PACKET_SEND.request | ParameterReporting_getParameters.response |
| | | Reply.request | | ParameterReporting_setParameters.indication |
| | | Message.indication | | ParameterReporting_setParameters.response |
| | | Reply.indication | | |
| | | Fault.indication | | |

# Case study conclusions / lessons learned

1. No analyzed instrument needs all EP modules - EP modules are selectable and configurable
2. Original EP definitions,- some appeared applicable, but their detailed definitions were found either ambiguous or incomplete (i.e. how to define/set groups)
3. In certain circumstances, the EP gave room for design options. In STIX, this was in FDIR – we could have used Automation Service or OBCP for implementing low severity or simple response FDIR
4. Actual roles were used to define generic OSRA-P roles. OSRA-P roles can help defining contractual relations

# Conclusions

## High level Aims Of common SW Arch.

1. Faster and more efficient development and integration of payload systems.
2. Improve reuse
3. Reduced effort for quality assurance and qualification
4. Streamline cooperation between PL experts and PL SW developers
5. Facilitating multi-team suppliers
6. de-risk/improve the interfacing between SW elements

## Objectives of OSRAP

1. Review Payload Domain
2. Define an OSRA for Payloads ((leverage results of OSRA on platform side)
3. Demonstrate OSRA-P

## Results

1. Domain analyzed based on 12 Payloads
2. OSRA-P Built on top of existing platform OSRA
3. OSRA-P encapsulates generic functionality of Payload systems, based on real instruments
4. Replication of development process of a real instrument
5. Technical Design of instrument SW feasible

# Open issues / future work

- Component-based PL SW Engineering?
- OSRA-P based Boot SW?
- How best to divide actor responsibilities?
- OSRA-P Requirement specification
- Specification of reusable components
- Prototype implementations
- Tool-support
- Qualification