Early validation of satellite COTS-on-board computing systems

Philippe CUENOT

FRENCH INSTITUTES OF TECHNOLOGY

Agenda

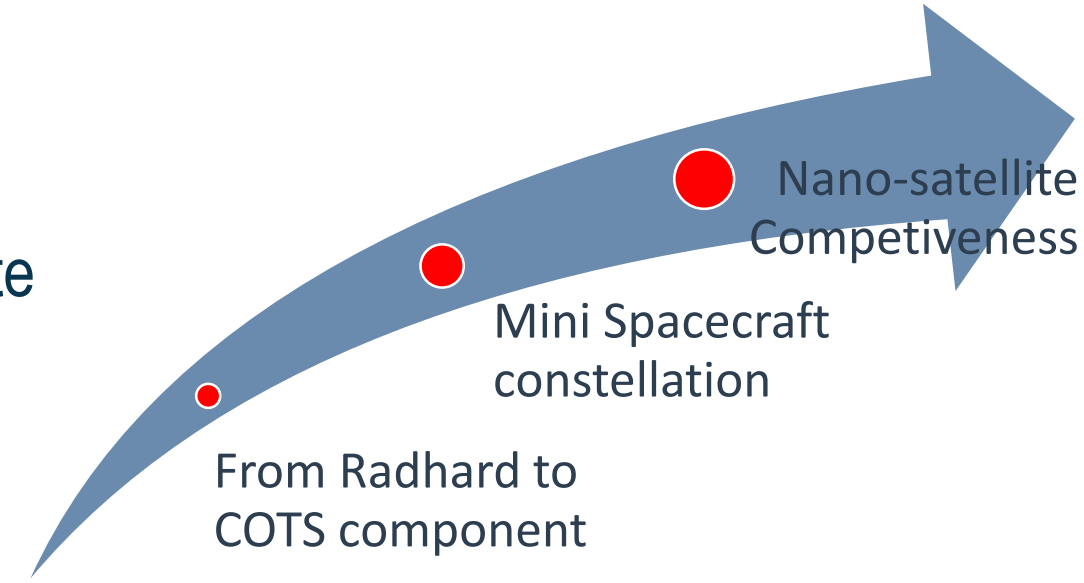
- Project Context
- Assessment Methods
- Availability assessment method
- Experimentation Results
- Conclusion

Agenda

- Project Context
- Assessment Methods
- Availability assessment method
- Experimentation Results
- Conclusion

Context

- Space industry evolution:



- Competitive market for Micro and Nano Satellite
- Perspective for introduction **COTS**
  - Multi-core, large memory, FPGA…
- Modular and integrated design for On-Board-Computer
- Still demanding requirements for **Quality of Service and Fault Tolerance**

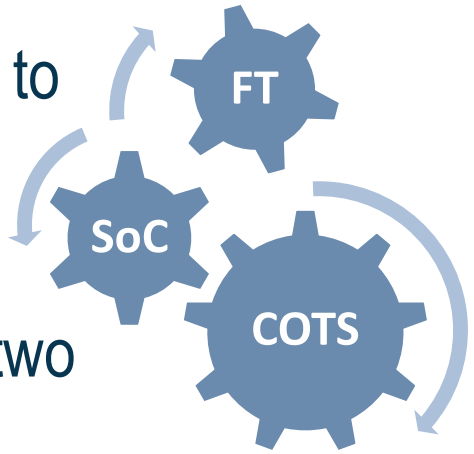
COTS : Commercial Off-The-Shelf

Context

- ATIPPIC IRT Saint Exupéry Project:

- De-risking of disruptive and low cost spacecraft avionic

- Identification and demonstration of Fault Tolerance mechanisms to balance weakness of COTS in space environment



- Work-package on early system using Model Based technics on two critical aspects:
  - **Conflict** in data communications inboard and interconnects
  - **Availability** of functions in case of resource failure (from solar radiation)

ATIPPIC : French acronym for “Highly *integrated avionics for small platforms including COTS*

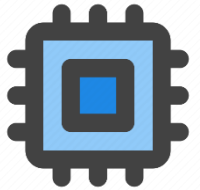
Agenda

- Project Context
- **Assessment Methods**
- Availability assessment method
- Experimentation Results
- Conclusion

Assessment Methods

- Assessment Methods
  - Synchronized with system Physical Architecture (with abstraction)
  - Quantitative measures on architecture and on changes (element allocation / introduction)

- Data Communication Conflict – **Congestion assessment**
  - Identify congestion in SoC interconnects and effect on function
  - Estimate **bus load and maximum interference rate** for each bus of the SoC
  - Estimate **latency effect on each function execution**



- Availability of functions – **Availability assessment**
  - Support for understanding FDIR, detection and mitigation mechanism
  - Evaluate radiation impact (SEU/MBU) on physical component, failure mitigation and propagation
  - Estimate **mission un-availability of critical function chain**

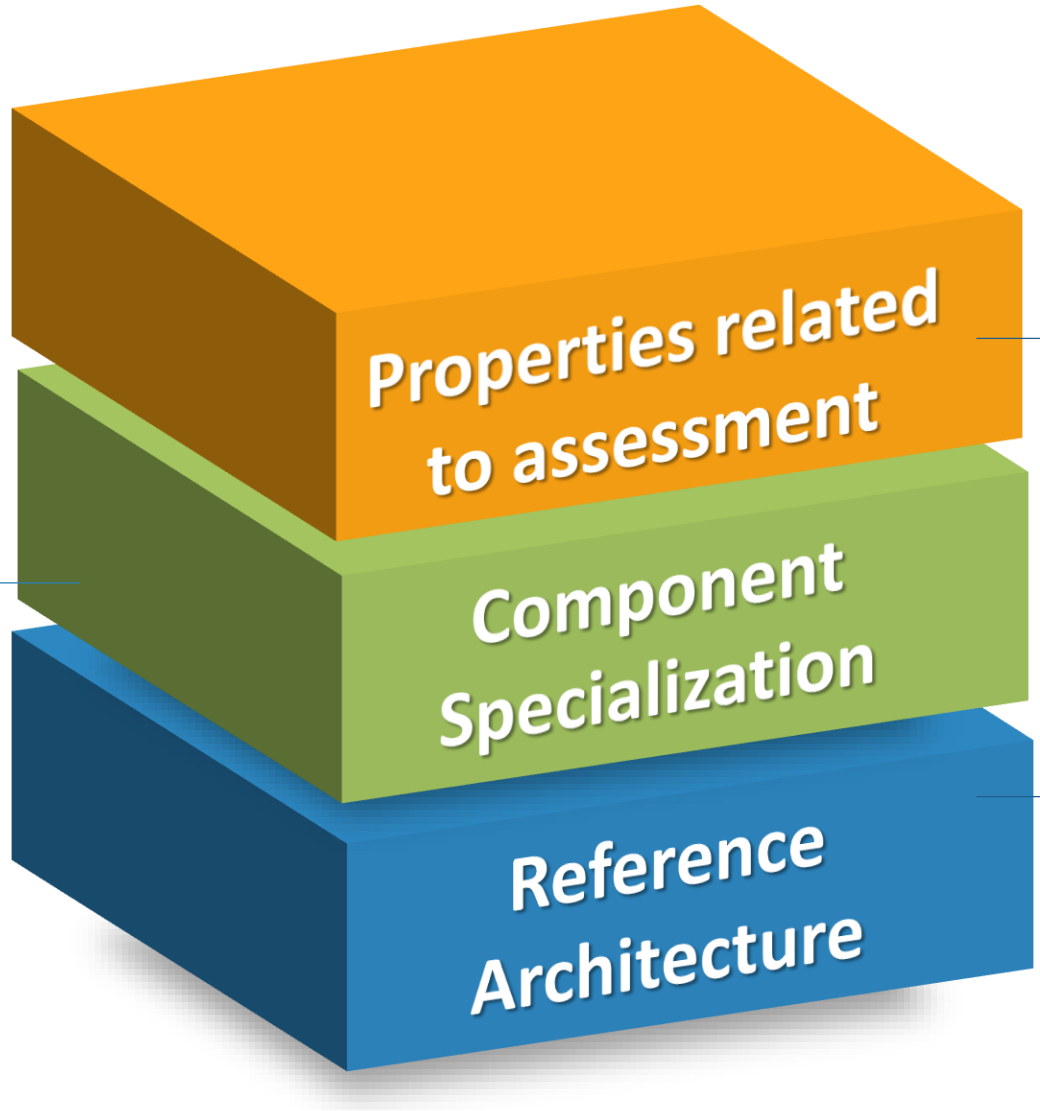
FDIR : Failure Detection Isolation and Recovery

Analytic Method

Static Analysis* (worst case)

SPECIALIZATION

Capella view with general properties for component specialization
General properties used for the analysis (e.g. size for RAM, bus size, …)



ASSESMENT

Capella view point dedicated to assement.
Plug-in to access parameters and manage assessment.

Capella Studio

CAPELLA MODEL

Architecture model in Capella.
Used for all analysis

*For congestion and availability

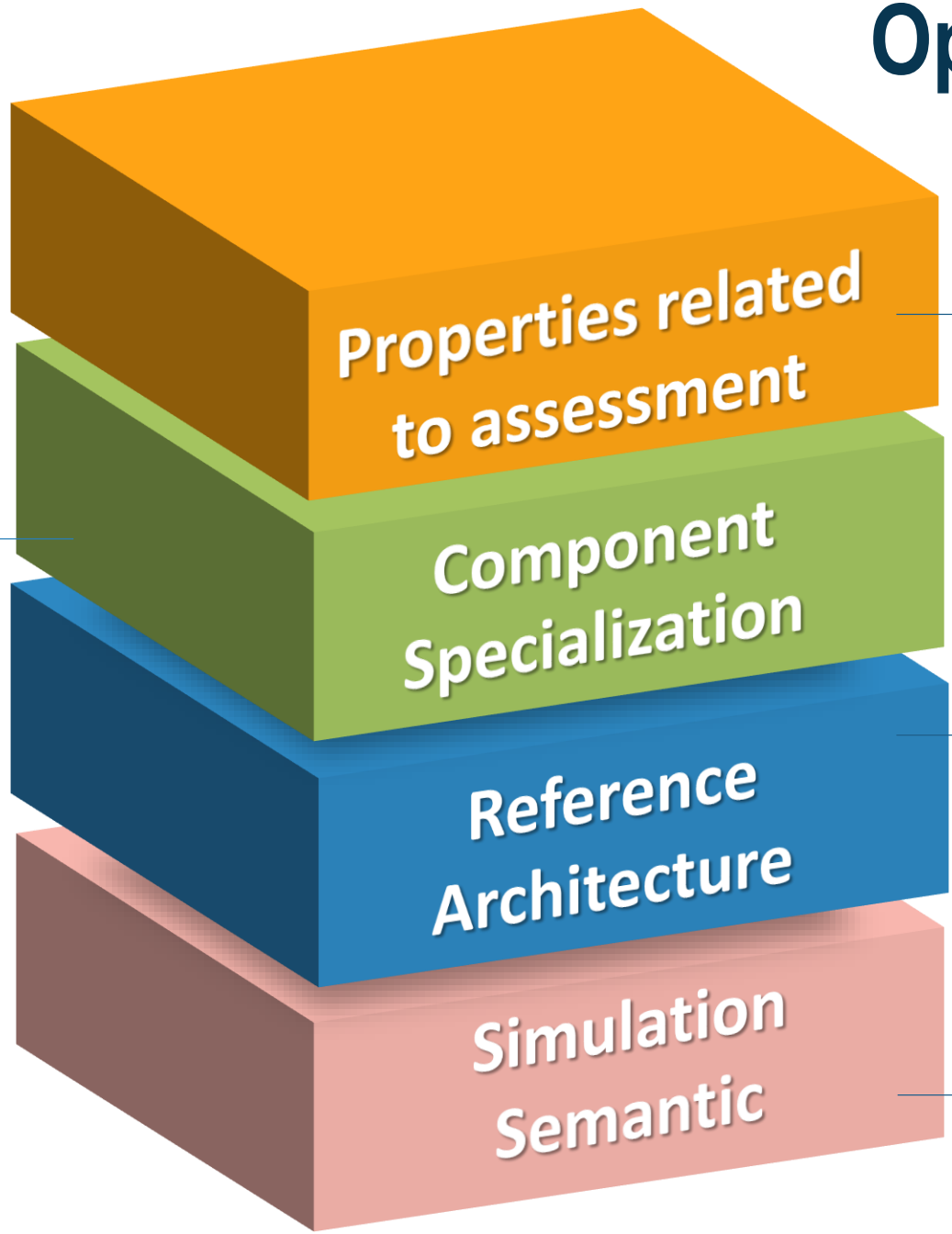
Operational Method

Scenario based simulation*
- Exhautive
- More accurate

SPECIALIZATION

Capella view with general properties for component specialization
General properties used for the analysis (e.g. size for RAM, bus size, …)

*Only for congestion today



ASSESMENT

Capella view point dedicated to assement.
Plug-in to access parameters and manage assessment.

Capella Studio

CAPELLA MODEL

Architecture model in Capella.
Used for all analysis

Gemoc Studio

GEMOC MODEL

Operational semantic of the model (Action and event associated to model, control flow of the execution)

Agenda

- Project Context
- Assessment Methods
- **Availability assessment method**
- Experimentation Results
- Conclusion

Availability Assessment

Radiation Type
Single Event Upset (SEU)
Multiple Bit Upset (MBU)

Failure Type
Erroneous Data In Range (EIR)
Erroneous Data Out Of Range (EOR)
No Data (ND)

Mitigation
For Radiation Detection
For Failure Detection

Un-availability

$$u_F = \sum \rho_{\%res} * \max(T_{mit}) * T_{mission}$$
$$u = \sum u_F$$

Component Specialization
Communication – bandwidth
Execution – N/A
Storage - size

Sensitivity
Radiation Type (SEU or MBU)
Sensitivity value (SBU per device per day)

Internal Protection
Radiation Type

Hardware dependencies
Relation Table on Radiation-Failure
Usage Rate of component

Function Failure Propagation
Logical Equation

Failure/Radiation Detection
Function / Physical Comp Monitored
Failure / Radiation Type Monitored
Detection Time Duration

Mitigation Mechanism
Relation to Detection
Number of detection (threshold)
Mitigation Time Duration
Impacted Component

Functional Chain
Functional Chain Definition

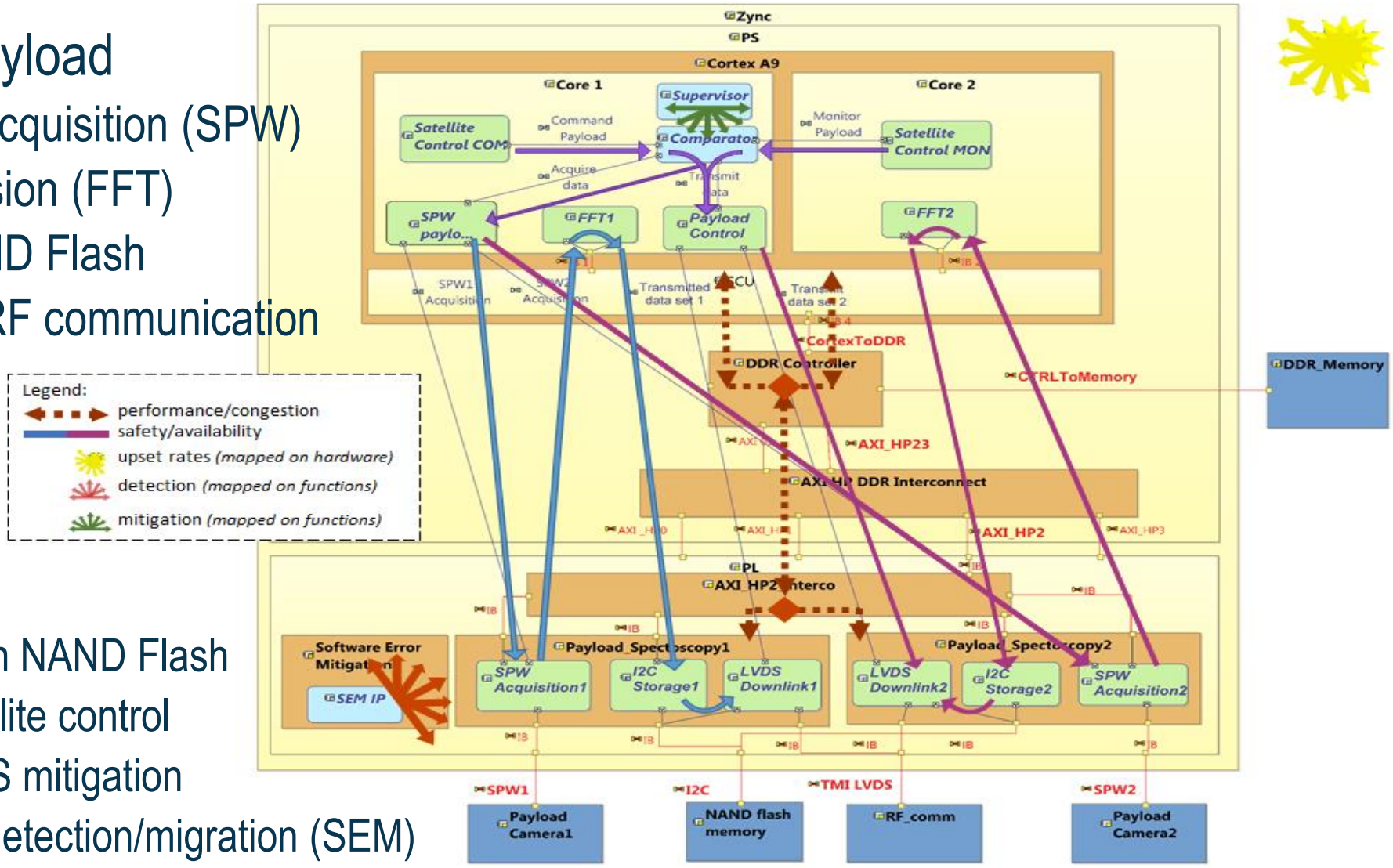
Assumption : No interaction between SEU

Agenda

- Project Context
- Assessment Methods
- Availability assessment method
- **Experimentation Results**
- Conclusion

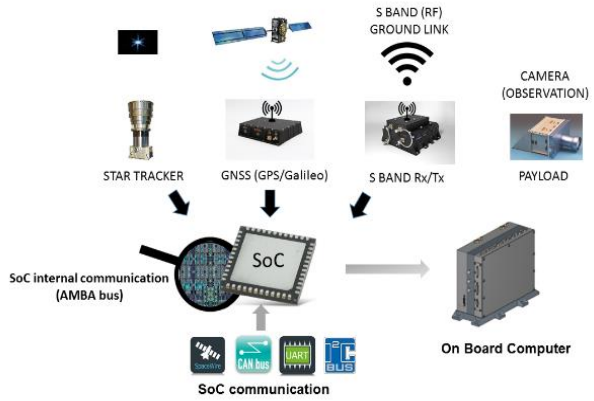
Experimentation Results

- Spectrometry Payload
  - Dual Camera Acquisition (SPW)
  - Data Compression (FFT)
  - Storage in NAND Flash
  - Download via RF communication
- FDIR Architecture
  - SBU protection in NAND Flash
  - COM/MON Satellite control
  - Supervisor for PS mitigation
  - PL CRAM SEU detection/migration (SEM)



Experimentation Results

- **Congestion :** Interference on buses to access DDR Controller
  - R/W - Image size 150 Mb acquired and compressed at 1 Hz
  - R - I2C storage in NAND flash of 3 Mb at 1 Hz
  - R/W - Satellite control 300Kb managed at 10 Hz
  - 4 Kb burst size configured for memory transaction
  - DDR Controller configured with LGR policy
  - Then Priority Control with high priority on Supervisor and COM/MON safety function



  - Zynq SoC processor
    - Bus : 64 bits width and 1.2 Gb maximum bandwidth
    - CortexA9 SW function execution (offset parameter on 1 Hz and 10 Hz function)
  - Capability of offset exploration with small DSL

LGR : Least Grant Recent

Experimentation Results

- **Congestion :** Interference on buses to access DDR Controller

	CortexToDDR	AXI_HP23	AXI_HP2
Dual spectrometry payload (Analytic)			
MaxInterenceRate	25.6%	25.25%	25.25%
Load	28.8%	25.5%	25.5%
Dual spectrometry payload with safety function (analytic)			
MaxInterenceRate	26.16%	25.25%	25.25%
Load	33.8%	25.5%	25.5%
To be compared to dual spectrometry payload (Operational and Fair)			

Capella View point annotation

CortexToDDR
maxInterferenceTime = 2616.4001us
maxInterferenceRate =261.64%
load = 33.8%

SPW_Acquisition1
transfer time = 125.0us
maxDelayedTime = 130.0us

FFT1
transfer time = 127.5us
maxDelayedTime = 135.8us

I2C_Storage1
transfer time = 2.5us
maxDelayedTime = 252.5us

Satellite Control MON
transfer time = 1.66us
maxDelayedTime = 261.64us

Analytic assessment

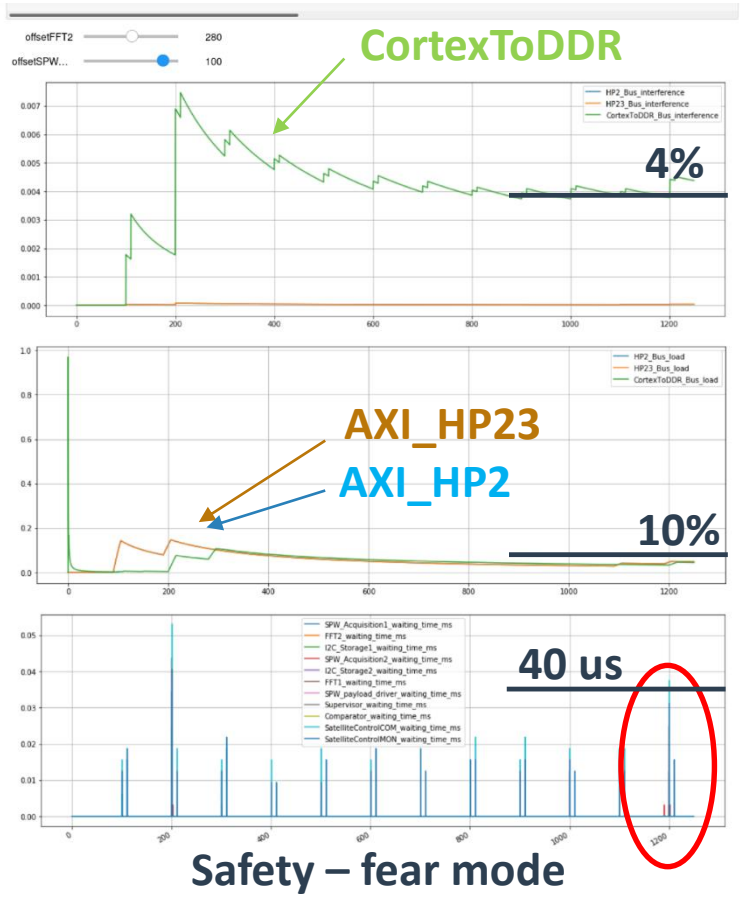
Experimentation Results

- **Congestion :** Interference on buses to access DDR Controller

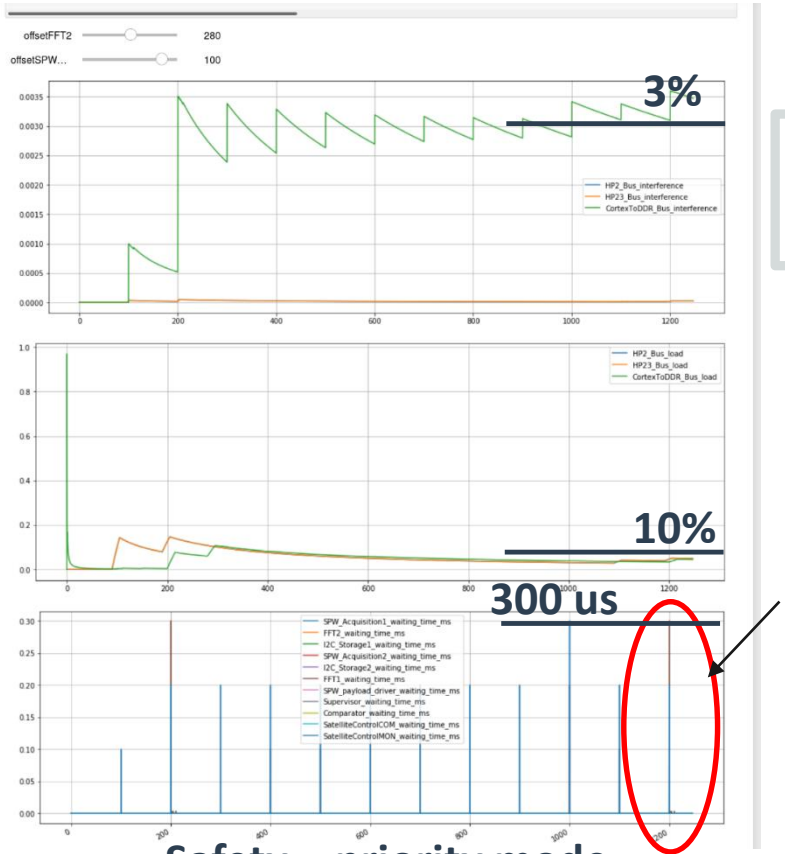
Bus interference

Bus load

Function waiting time



Safety – fear mode



Safety – priority mode

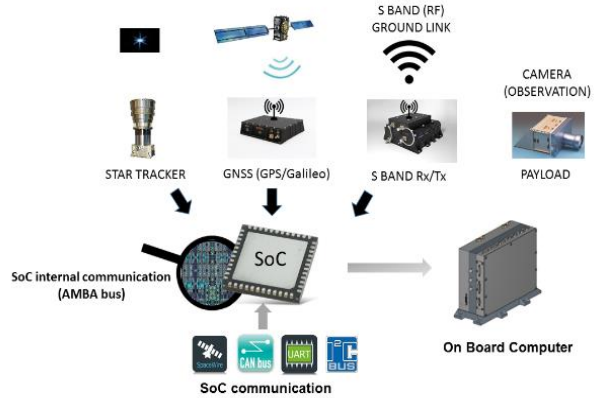
Jypyter Lab view

No dispersion
Non safety (FFTx) function shift to high delay

Operational assessment

Experimentation Results

- **Availability :** SoC (Zynq) un-availability for 1 year mission
  - SBU hardware sensitivity value from literature or arbitrary fixed
  - PS function: hardware dependency to Core1/2 and DDR
  - PL function: hardware dependency CRAM (and NAND Flash)
  - All function: hardware SEU/MBU allocation (%) to Failure Mode
  - All function: encoding of Failure Mode propagation
  - Safety mechanism detection/mitigation and associated delay
    - NAND Flash protection (triplication)
    - COM/MON comparator for detection and mitigation by supervisor
    - Supervisor self detection and self mitigation
    - CRAM MBU failure detection by SEM IP and mitigation by supervisor, SEU internal
  - Ground station detection duration 48h (survey of downlink) with 30s for rebooting satellite



Experimentation Results

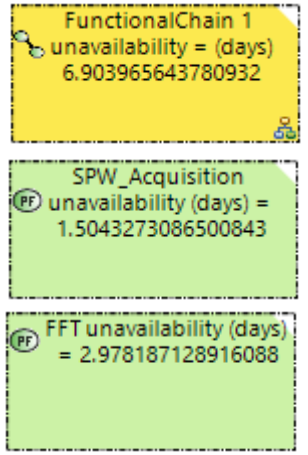
- **Congestion :** SoC (Zynq) un-availability for one year mission

Functional Chain or Function	Un-availability (days) without Ground Station	Un-availability (days) without Ground Station
Functional Chain	285.5	6.9
SPW Acquisition1	$7.23\ 10^{-2}$	1.5
FFT1	244.2	2.98
I2C Storage 1	$4.55\ 10^{-3}$	0.75
LVDS Downlink	$2.44\ 10^{-3}$	0.75
Supervisor	0	0
Satellite Control COM	$3.74\ 10^{-5}$	0.4
Satellite Control MON	$2.78\ 10^{-5}$	$2.78\ 10^{-5}$
Comparator	3.5	0.13

Due to lack of mitigation mechanism

Arbitrary choice to compute radiation (/day) for each day of the mission

Capella View point annotation



Due to worst case mitigation duration (Ground value)

Analytic assessment

Agenda

- Project Context
- Assessment Methods
- Availability assessment method
- Experimentation Results
- Conclusion

Conclusion

- Early MBSE quantitative balancing of system design choice for COTS in space environment
  - Congestion : Help to predict SoC real time guarantee on function execution
  - Availability : Help to improve SoC Fault Tolerance for COTS radiation weakness
- Two steps approach analysis
  - Analytic : rapid results and bounded value as worst case scenario
  - Operational: more accurate results from operational scenario but longer to get
- Unified Capella environment for design and analysis

- But not replace implementation/micro-architectural analysis
- Operational improvement shall be bounded (abstraction criteria)

Thank you

© IRT AESE "Saint Exupéry" - All rights reserved Confidential and proprietary document. This document and all information contained herein is the sole property of IRT AESE "Saint Exupéry". No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of IRT AESE "Saint Exupéry" . This document and its content shall not be used for any purpose other than that for which it is supplied. IRT AESE "Saint Exupéry" and its logo are registered trademarks.