Model Based FDIR process with Capella and COMPASS

Results of a CNES / TAS-F study and way forward

R. de Ferluc – A. Provost-Grellier – B. Dellandrea

MBSE ESA WORKSHOP – DEC 2016

Agenda

- Context
- Study objectives
- TAS-F background
- Model Based Process
- Prototyping and use-case
- Way forward

Context

Context

Previous R&T CNES study conclusions

- Evaluation of FDIR formal verification
  - Thanks to Model Simulation
  - Thanks to Model Checking techniques
- State of the art and experimentations conclusions :
  - Promising techniques to assist Spacecraft Safety, Dependability and FDIR engineers
  - Increasing efficiency and performance of existing tools
- However, rarely applied on programs
  - Not only in Space domain, but also in other domains.

Context

Why ?

- Need for detailed knowledge on the methodology and hands-on practice by prospective users.
- Big effort required to build a formal model of the system
- Insufficient means or methodology to ensure that the modelled system matches the real system
- Scarce understanding of properties to be proved
- Tools with shortcomings in ergonomic and interoperability with other engineering environments.

Context

How to ?

- Provide domain analysis (RAMS, FDIR, …) based on formal methods / languages integrated to tools the user knows (engineering environments).
- Share modelling effort between engineering and Safety/FDIR teams
- Ensure that the modelled system matches the real system
- Clearly specify which properties need to be proved

Study objectives

Study objectives

CNES has initiated a study with the following objectives

- Define a Safety/FDIR process for Space Domain starting from the state of the art of other domains (aeronautical domain, transportation, ...)
- Identify the most suitable tools
- Experiment on a small case-study
- Elaborate some recommendations

Timeline : 2013 - 2014

Purpose :

- Increase efficiency of safety analysis
- reduce the FDIR validation & verification costs

TAS-F background

TAS-F background – Melody Advance / Capella (1/)

Beginning of Model Driven Engineering:

- Slow & high-effort deployment of modeling techniques
- COTS are not well adapted to industrial needs
- Tool vendor dependencies are too constraining

ARCADIA

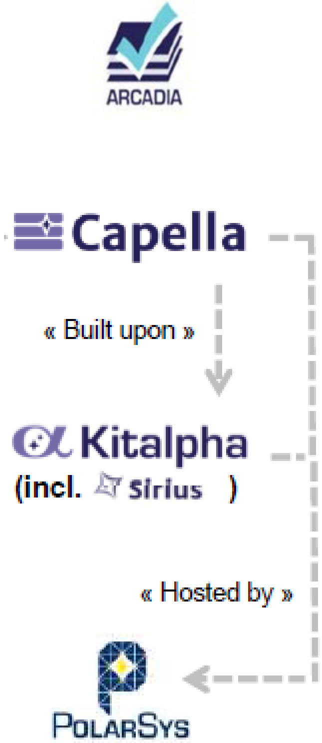
THALES strategy:

- Define a method: ARCADIA
- Develop dedicated tooling: Melody Advance
  - Specified, designed & developed from operational needs
  - With the necessary capabilities (allow for quality and productivity, user-friendly, permits early validation, performance & scalability, suitable for configuration management and collaborative engineering, ...).
  - Applicable to every domain (Aeronautical, transportation, communication, ...)

melody advance

TAS-F background – Melody Advance / Capella (1/)

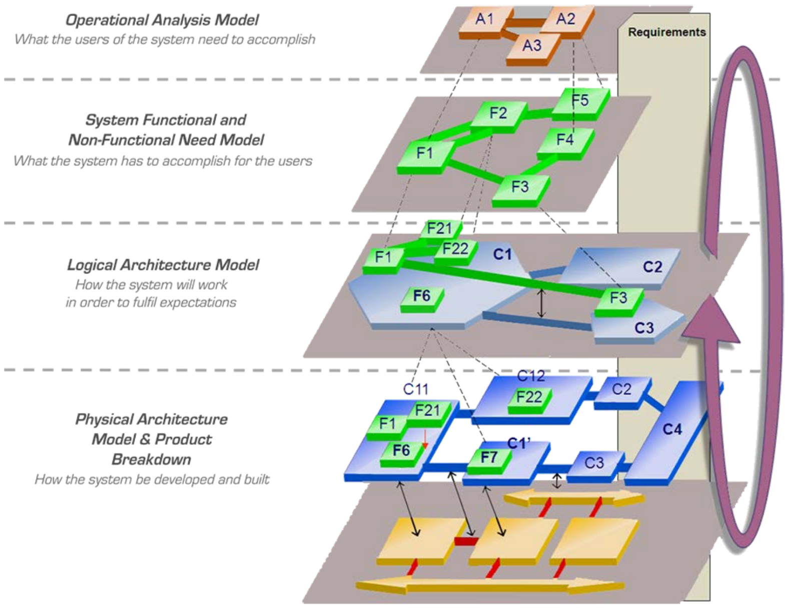
OSSing Melody Advance: public name is Capella



www.polarsys.org/capella

TAS-F background – Melody Advance / Capella

Melody Advance / Capella



Satellite model

Avionics models

OBSW / Eqts models

Different scopes and purposes for modeling activities.

TAS-F background - numerous ESA studies

ESA studies :

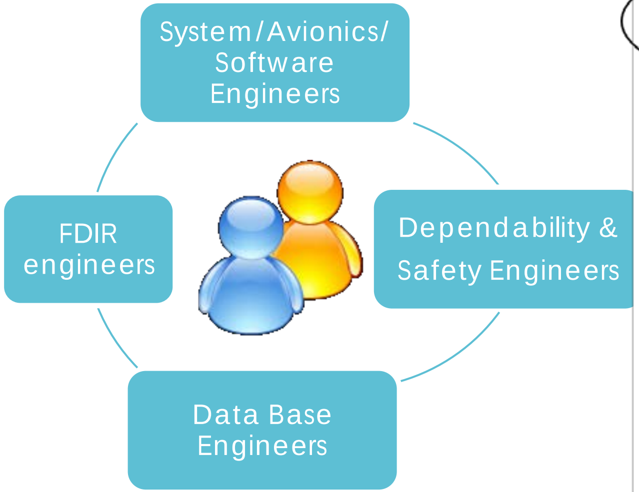
- **COMPASS**
  - develop a toolset for evaluation of system-level correctness, safety, dependability, and performance (performability) of the on-board computer-based systems.
- **COMPASS GRAPH**
  - Develop a graphical editor for SLIM models.
- **AUTOGEF**
  - Development of the Automated Model Generation Toolset for FDIR (AUTOGEF) as an add-on to the COMPASS Toolset, and definition of the associated methodology. (Synthesize FDIR diagnosis and controllers in SLIM model for an given system).
- **FAME (Failure and Anomaly Management Engineering)**
  - Definition of the FDIR development methodology and associated V&V process, and development of the Failure and Anomaly Management Engineering (FAME) Environment as an extension to COMPASS toolset.
- **FDI AOCS**
  - Improvement of AOCS, FDIR & Avionics for compliance with LEO de-orbitation new requirements

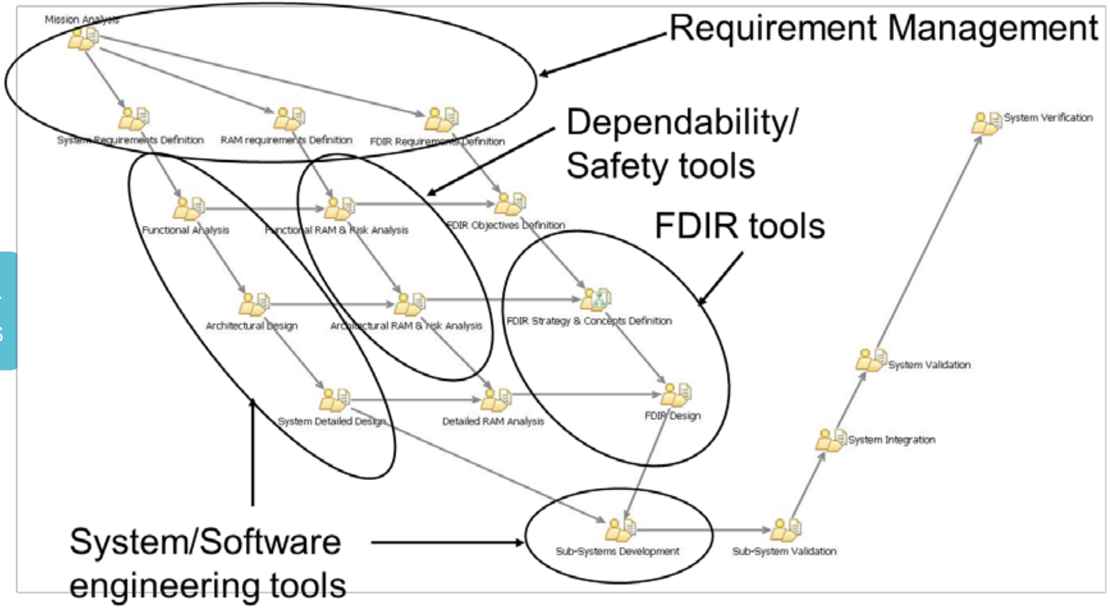
Model Based Process

Model Based Process

Proposed approach

- Identification of roles and activities => the process
- Identification of tools





THALES ALENIA SPACE France

Model Based Process

Proposed activities :

- Requirements analysis
- Functional /logical Analysis
  - System Functional Analysis
  - System Dependability / Safety analysis
  - Consolidation of the functional analysis
  - RAMS analysis at functional level
- System Physical Design
  - System design at physical level
  - System Dependability / Safety analysis at physical level
  - Consolidation of the System Physical Design
- FDIR development
  - FDIR requirement analysis
  - FDIR objectives definition
  - FDIR concepts and FDIR strategy specification
  - FDIR design
  - FDIR implementation
  - Final FDIR V&V

Aligned with ESA study results

Proposed tools :

- Requirements Management tool (e.g. DOORS)

Requirements

melody advance

Capella

- FunctionalAnalysis
- Logical / Physical Design
- Dependability / Safety analysis
- RAMS analysis

COMPASS

- FDIR specification
- FDIR design
- FDIR Verification

FDIR Editor

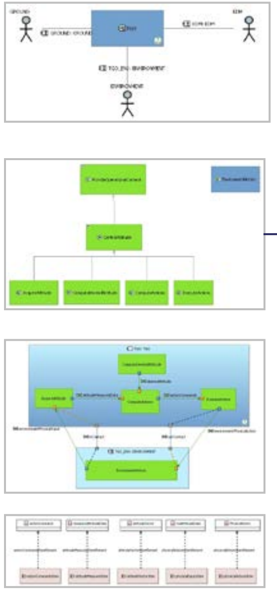
THALES ALENIA SPACE France

Prototyping and use-case

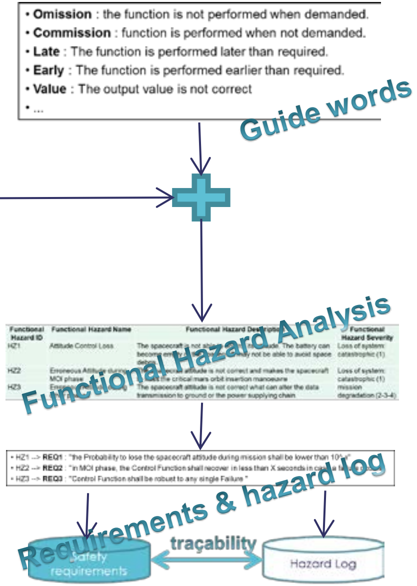
Prototyping and use-case

Exomars TGO case study

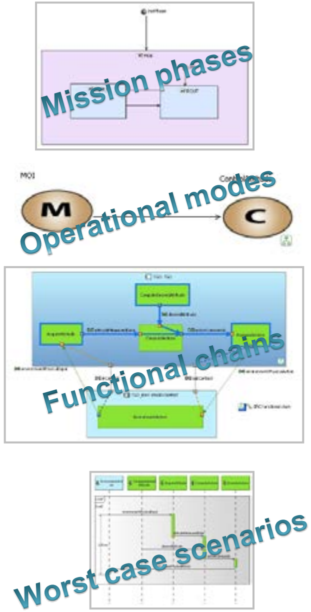
- Functional Analysis



- Functional Hazard Analysis



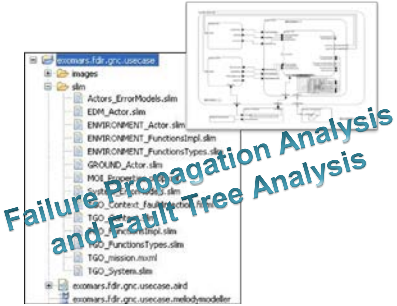
- Safety objectives allocation on FA



- RAMS analysis

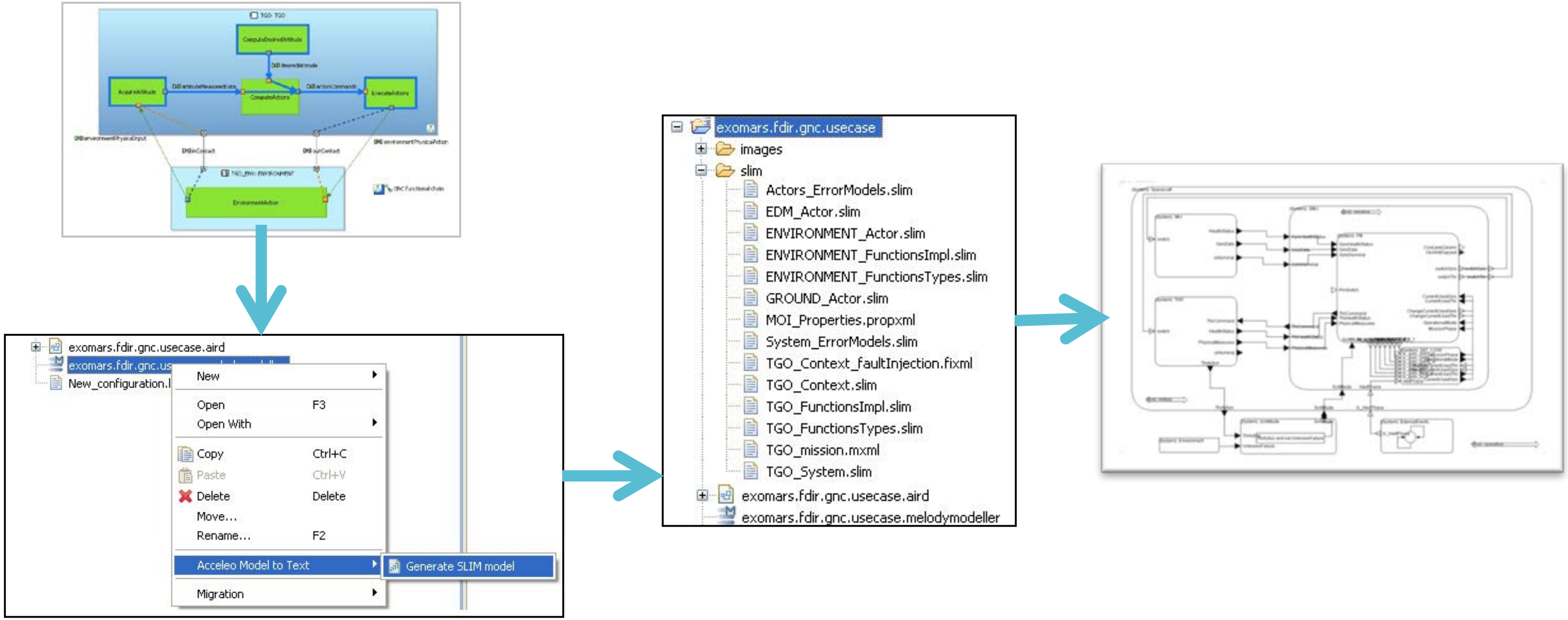
Functional FMEA

Involved Unit	Failure Mode	Effects on output functional exchanges
Compute desired spacecraft attitude function	Bad desired attitude	BAD_DESIRED_ATTITUDE
Measure spacecraft attitude function	No measures	NO_MEASURES
	Biased measures	BIASED_MEASURES
	Erroneous measures	ERRONEOUS
Compute Actions for desired Attitude function	No action is generated	NO_ACTIONS
	Biased actions are produced	BIASED_ACTIONS
	Erroneous actions are produced	ERRONEOUS
Execute Action Function	No action is executed	NO_ACTIONS
	bad action is executed	BAD_ACTIONS



Prototyping and use-case

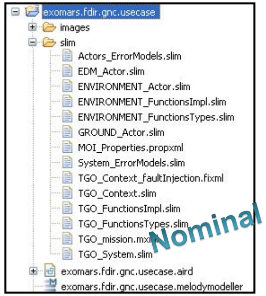
From Melody Advance/ Capella to SLIM models



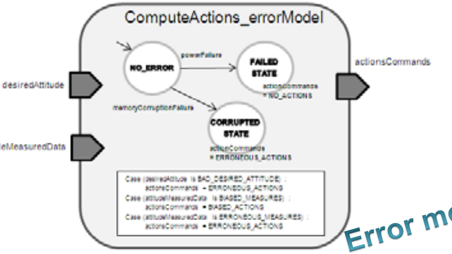
THALES ALENIA SPACE France

Prototyping and use-case

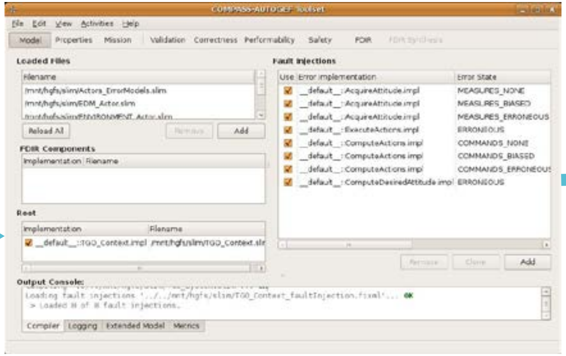
COMPASS analysis at functional level



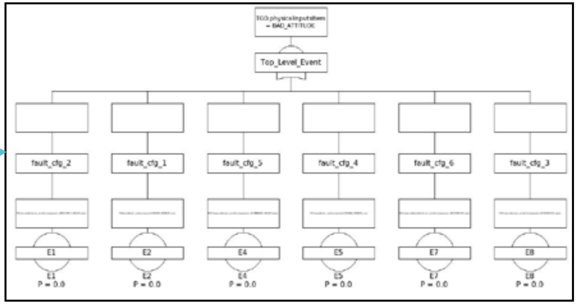
Nominal SLIM model



Error models



Fault injection within COMPASS



Fault Tree Analysis within COMPASS

THALES ALENIA SPACE France

Prototyping and use-case

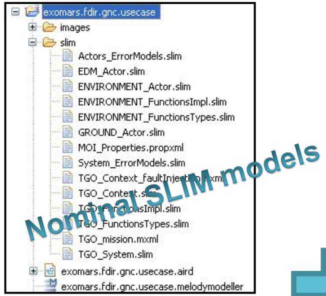
System design

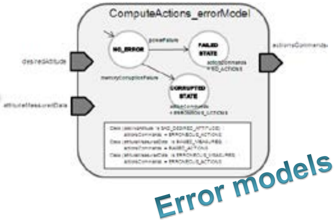
- Physical design

- FMEA based on Equipment Datasheet (EDS?)

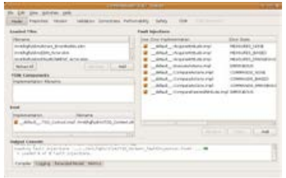
Failure Modes and Effects Analysis (FMEA)											
Product: Project/Phase: System/Subsystem/Equipment:					Prepared by: Approved by: Date:			Document ref.: Issue: Page of			
Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. End effects	Severity	Failure detection method/ observable symptoms	Compensation provisions	Correction actions	Remarks

- Modeling of Failure modes and fault propagation at physical level





- Fault Injection and COMPASS analysis : FMEA / FTA



- Criticity analysis

ID	Item	Function	Failure Mode	Failure Cause	Mission Phase	Failure Effects (local / end)	Severity	Failure detection	SN	PN	CN	Corrective Actions
FM1	IMU	measure inertial parameters	No measures	no more power, internal failure, ...	MOI	no measures is sent to OBSW	loss of attitude	absence of measures	3	2	6	switch to redundant
FM2	IMU	measure inertial parameters	Biased measures	un-calibrated sensor	MOI	measures are biased	biased attitude	biased measures detected by a filter	1	2	2	reset equipment
FM3	IMU	measure inertial parameters	Erroneous Measures	internal failure	MOI	measures are erroneous	erroneous attitude	No detection until attitude is detected erroneous	3	2	6	switch to redundant

THALES ALENIA SPACE France

Prototyping and use-case

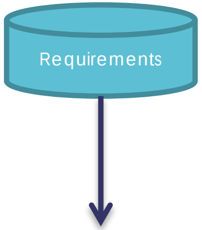
Remarks

- The process should be iterative
  - Add new safety related functions (filter, detection, ...)
  - Specify new observables / commandable data
  - Add FDIR related components / mitigation / redundancy
  - Add cross-strapping
  - ...

Prototyping and use-case

FDIR

- FDIR objectives definition



- **FDIR_OBJ1**: Surviving shall be ensured for any single failure
- **FDIR_OBJ2**: Achieve S/C manoeuvres for critical phase even in case of failure
- **FDIR_OBJ3**: Fuel consumption shall be optimized and reconfiguration and equipment loss shall be minimized

- FDIR strategy definition
  - Classify failures
    - Detection level
    - Isolation level
    - Reconfiguration level

Fault	Detection level	Reconfiguration level
FM1-1	Level 0	Level A
FM1-2	Level 1	Level B
FM2	Level 2	Level B
FM3	Level 2	Level B

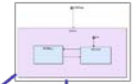
FMECA

Detection	IMU	CSW
HW only	FM1-1	
Processor unit with SW		FM1-2 FM2 FM3

Isolation	IMU	CSW
HW only	FM1-1	
Processor unit with SW		FM1-2 FM2 FM3

Recovery	IMU	CSW
HW only		
Processor unit with SW		FM1-1 FM1-2 FM2 FM3

  - Define reconfiguration strategies
    - Fail'Op
    - Fail'Safe
    - …



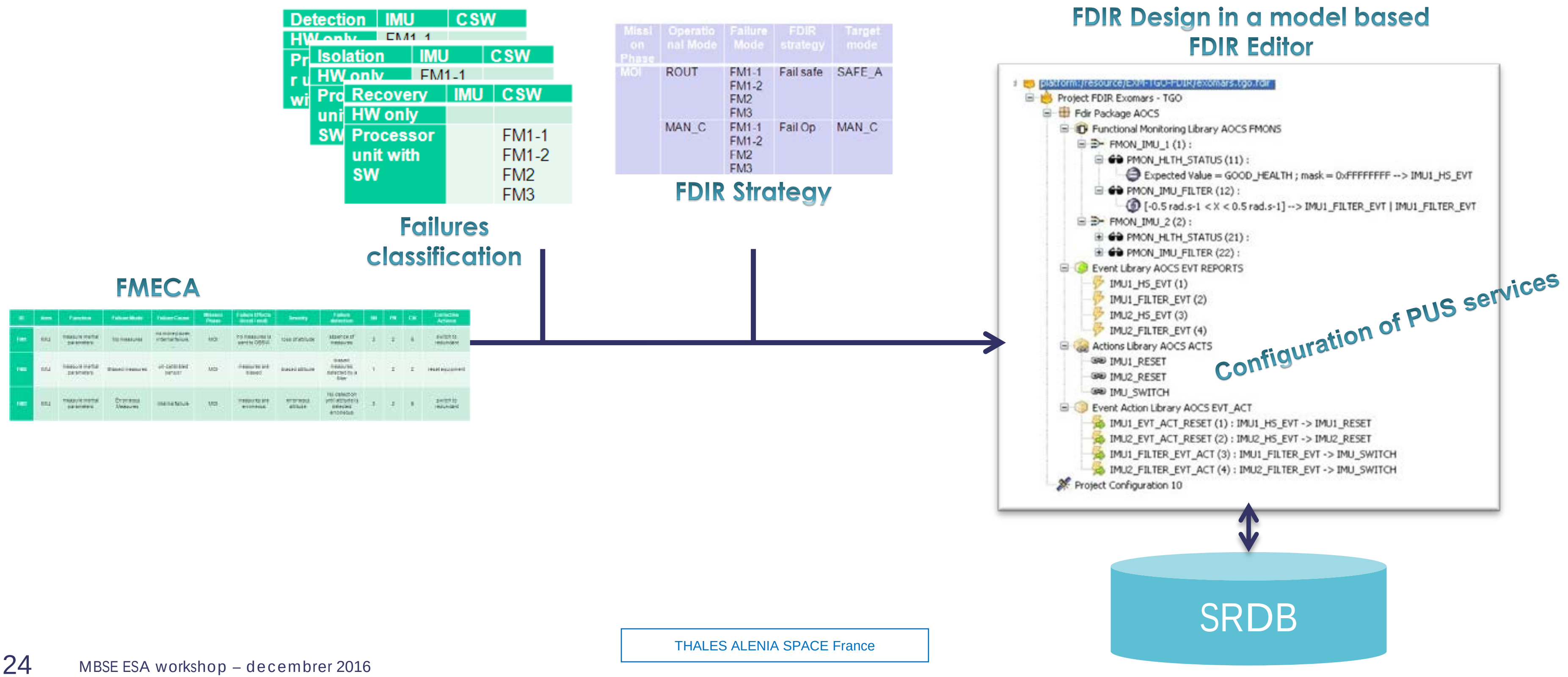
FDIR Objectives

FDIR Objectives
FDIR_OBJ1
FDIR_OBJ2
FDIR_OBJ3

Mission Phase	Operational Mode	Failure Mode	FDIR strategy	Target mode
MOI	ROUT	FM1-1 FM1-2 FM2 FM3	Fail safe	SAFE_A
	MAN_C	FM1-1 FM1-2 FM2 FM3	Fail Op	MAN_C

FDIR Implementation

Configuration of PUS monitoring and action services based on models



THALES ALENIA SPACE France

Way forward

Way forward

Step 1 : Deployment of Model Based practices in the Engineering process

- At architecture level
  - Requires a mature and already proven tool and methodology (like Capella and Arcadia)
  - Guidelines and validation rules should ensure semantics of the models
  - Models should be used to produce artefacts : specification / code / database / tests / ...
- At behaviour level:
  - Use of different formalisms to cope with different contexts (Matlab/Simulink, SDL, SLIM, TFPG, scenarios, ...)
  - Models should be used to produce artefacts : specification / code / tests / ...
  - Behavioural models should be coupled with architectural design models

Step 2 : Define a Safety / Dependability / FDIR reference architecture

- Extend the Avionics Reference Architecture (ASRA) and the On-Board Software Reference Architecture (OSRA) with dedicated concepts and methodology
- Provide dedicated « viewpoints » in the engineering tools (Matlab/Simulink, Capella, SCM, ...)
- Investigate use of Electronic Data Sheets to support Failure Mode definition (at equipment level) and coupling with engineering models.
- Focus on production of artefacts (specification, code, configuration, ...)

Step 3 : coupling Model Checking and Simulation tools

- Consolidate objectives : early validation of the system design (redundancy, cross-strapping, strategy, ...), generation of FMEA, FTA, Failure Propagation Analysis, ...
- Connect Model Checking & Simulation tools to Engineering tools : set-up model to model (M2M) transformations like Capella -> AADL/SLIM
- Map the system behavioural models to formal languages used for model checking and simulation (cope with synchronisation, timing aspects, ...)

Way forward

Classical approach :