FAME
Final Presentation Days
Noordwjik, 22-05-14

WE LOOK AFTER THE EARTH BEAT

A. Guiotto (TAS-I)
M. Bozzano (FBK)
R. De Ferluc (TAS-F)

23/05/2014

Ref.:

FONDAZIONE BRUNO KESSLER

ThalesAlenia Space
A Thales / Finmeccanica Company

83230352-DOC-TAS-EN-001

Agenda

- Study framework
- FAME Process
- FAME Proposed solution
- Demo of FAME Environment
- Evaluation on a case study
- Characterization of the approach
- Conclusions

Study Framework

FAME: FDIR Development and Verification & Validation Process

Thales Alenia Space Italia
Prime Contractor
System Specification
Validation and Characterization of FAME

FBK
Subcontractor
Design and Implementation of FAME

Thales Alenia Space France
Subcontractor
Selection of case study and performance evaluation

Based on COMPASS study

Duration: 20 months

Motivations

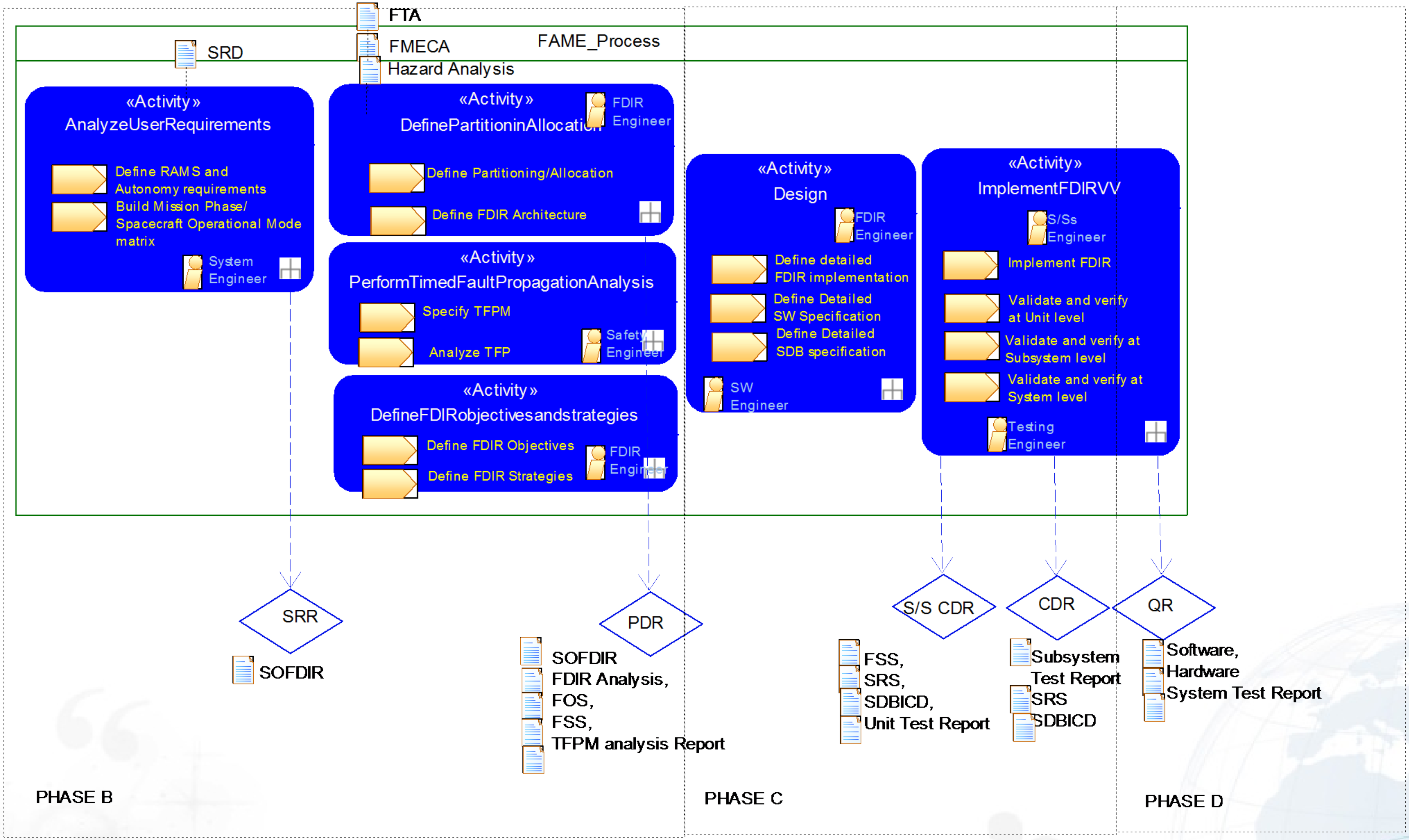
- FMECA and FTA becomes available late in the process, leading to late initiation of the FDIR development, which has a detrimental effect on the eventual FDIR maturity
- All possible fault and failure combinations are inherently complex to analyse and to define an adequate FDIR strategy for
- As various sub-systems and equipment tend to incorporate some local FDIR functionalities, the global FDIR concept shall account for coordination of the local FDIR elements to achieve the FDIR coherency
- Safety-critical systems being double failure tolerant need adequate FDIR operation in all double failure configurations and their propagation
- Currently employed approaches to FDIR development are poorly phased**.**
- No dedicated approach to FDIR development exists

Study Objectives

- Definition of the FDIR development methodology be based on the formal specification and analysis techniques
- Definition of the FDIR Development and V&V Process based on the aforementioned Methodology, encompassing the full FDIR lifecycle
- Development of the *Failure and Anomaly Management Engineering* (FAME) Environment implementing the Process and allowing for the System-level coherent definition, specification, development, and V&V of the FDIR functionalities
- Demonstration of the approach on case studies
- Evaluation of the adequacy of the approach and developed environment for use in the context of critical on-board space systems and software development

FAME Process

Overview of FAME Process

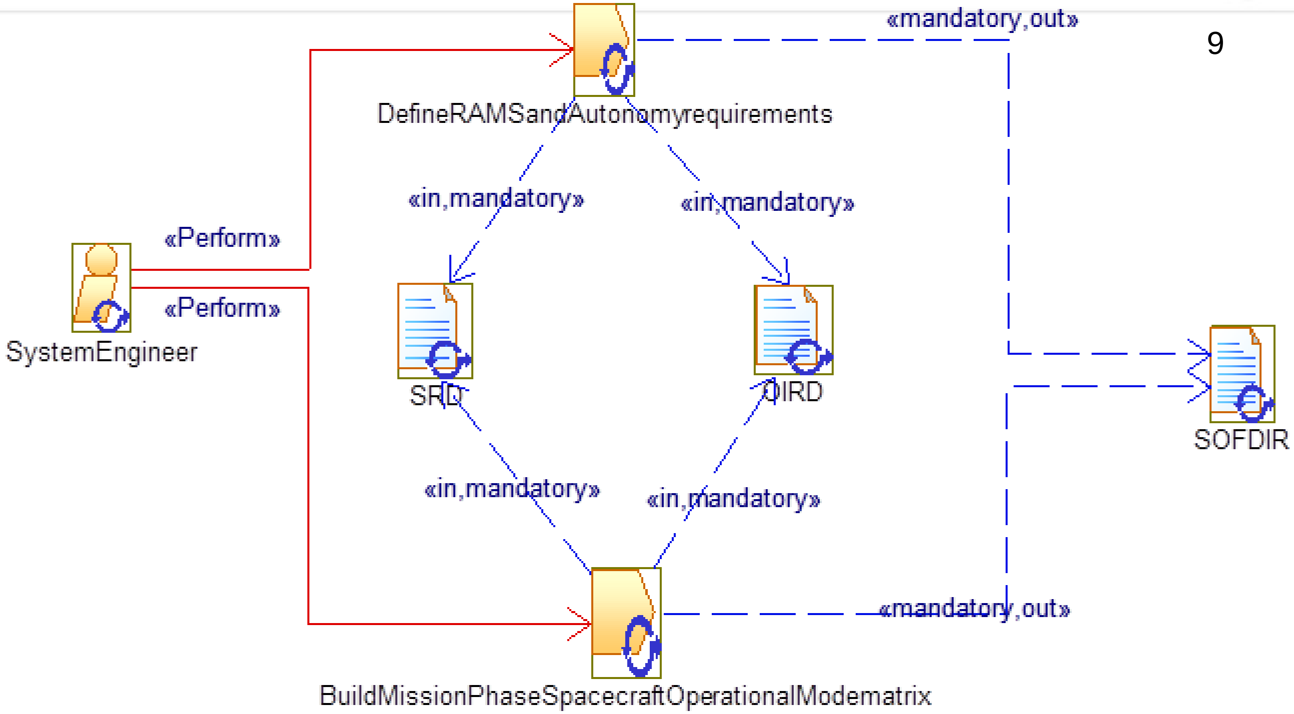


FONDAZIONE BRUNO KESSLER

ThalesAlenia Space — A Thales / Finmeccanica Company

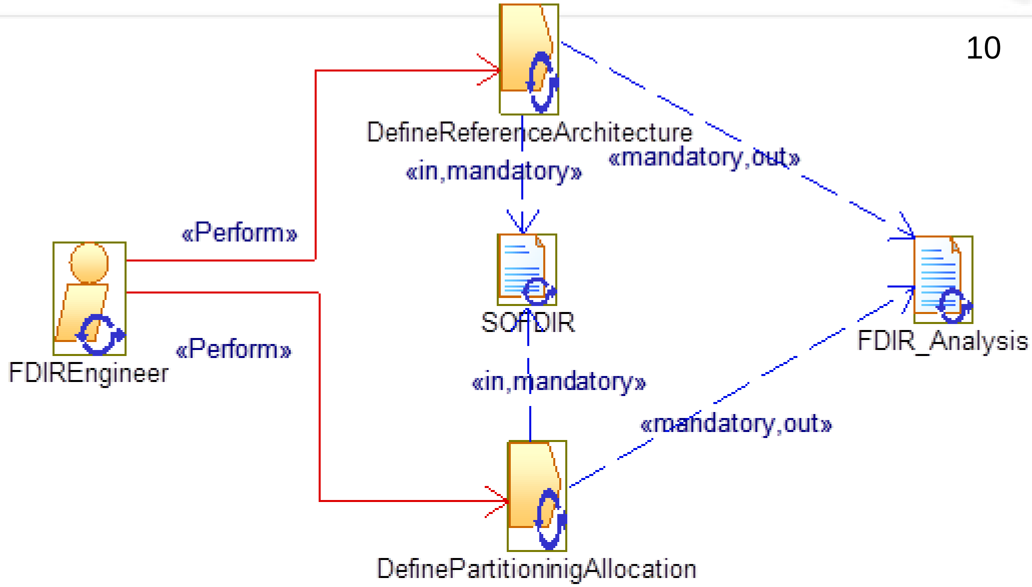
Analyze User Requirements

- System engineers:
  - collect and analyze all the user requirements contained in SRD and OIRD that impact the FDIR to derive the objectives of the FDIR and define the impacts they will have on the S/C design from system level down to unit level.
  - Highligth possible limitations
- Start: ***begin of System Phase B***
- End: ***before System SRR***



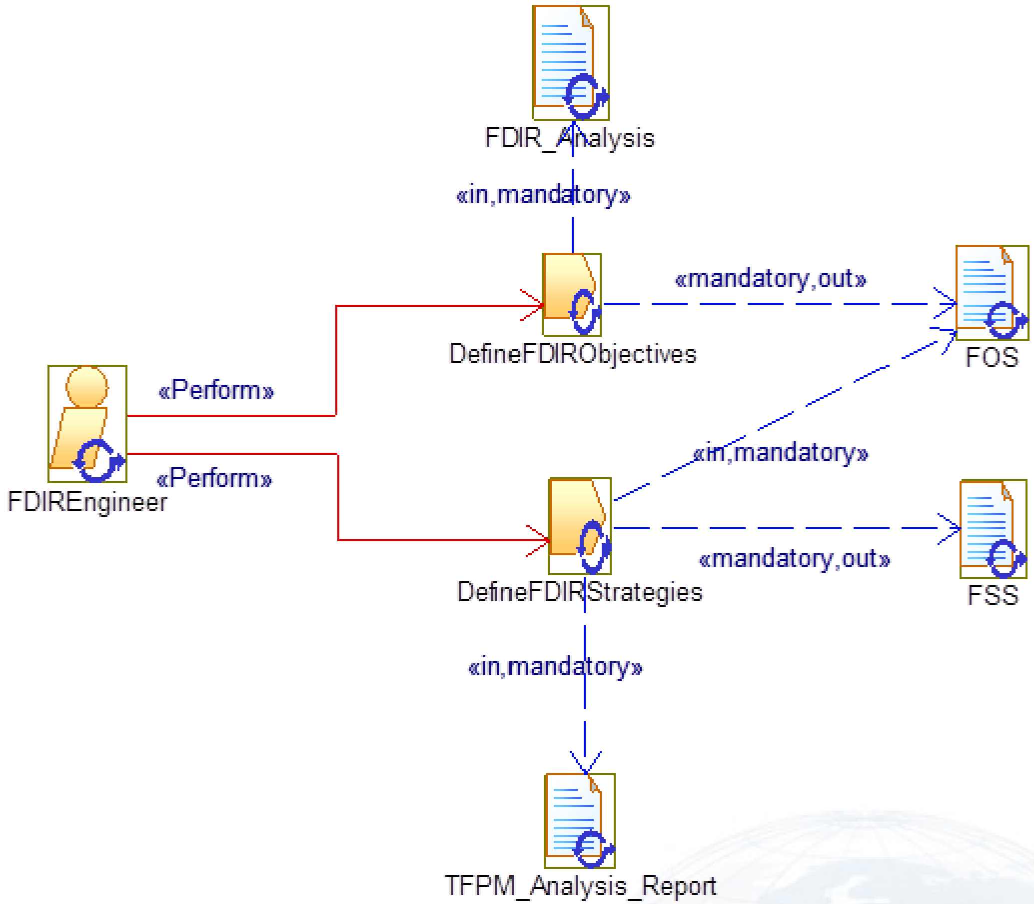
Define Partitioning/allocation

- FDIR engineers:
  - Allocate RAMS and Autonomy Requirements contained in SOFDIR per Mission Phase/Spacecraft Operational Mode in order to define FDIR approach and Autonomy Concept during different mission phases/Spacecraft Operational Mode.
  - Model spacecraft FDIR architecture including all the involved subsystems (avionics, payload…)
- Start: ***after System SRR***
- End: ***System PDR***



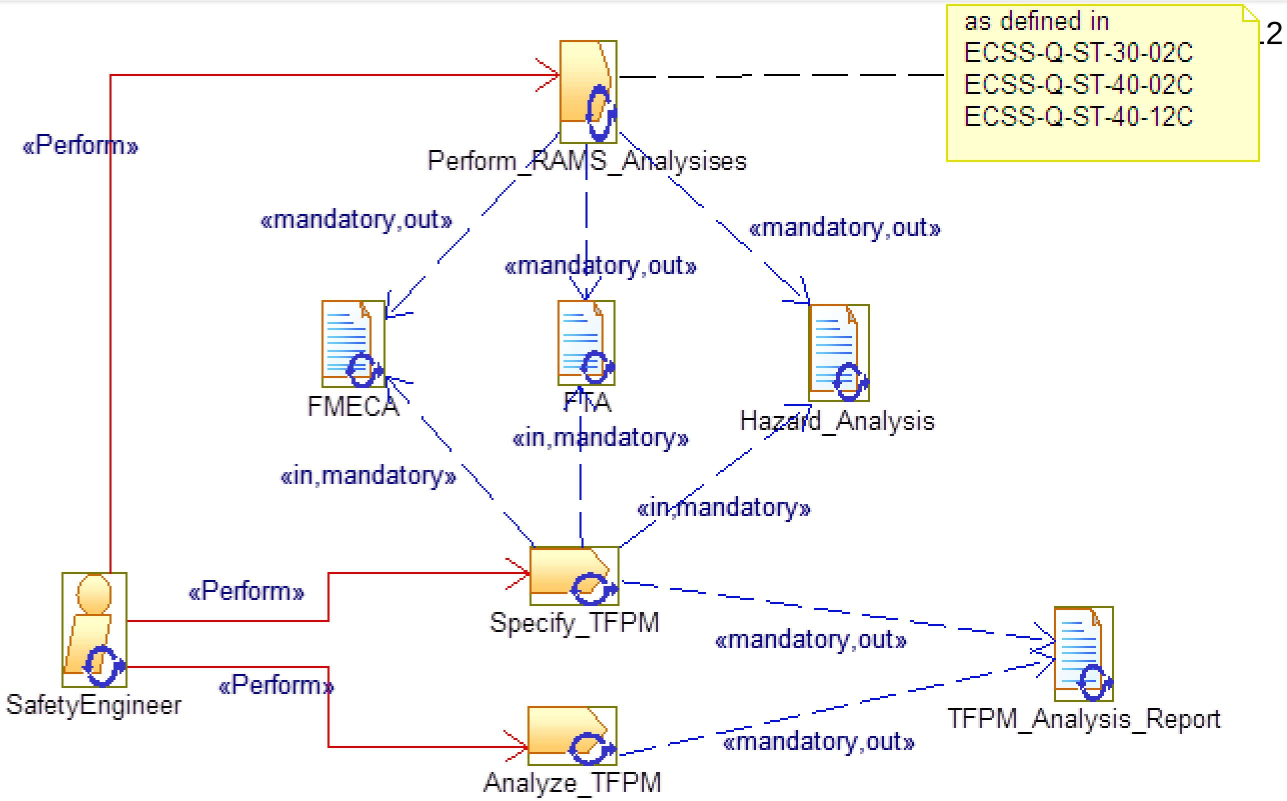
FDIR objectives and strategies

- FDIR engineers:
  - specify FDIR Objectives at system-level specification in FOS and FDIR Strategies at subsystem level in FSS by using FDIR Analysis and TFPG Analysis Report.
- Start: ***after System SRR***
- End: ***System PDR***



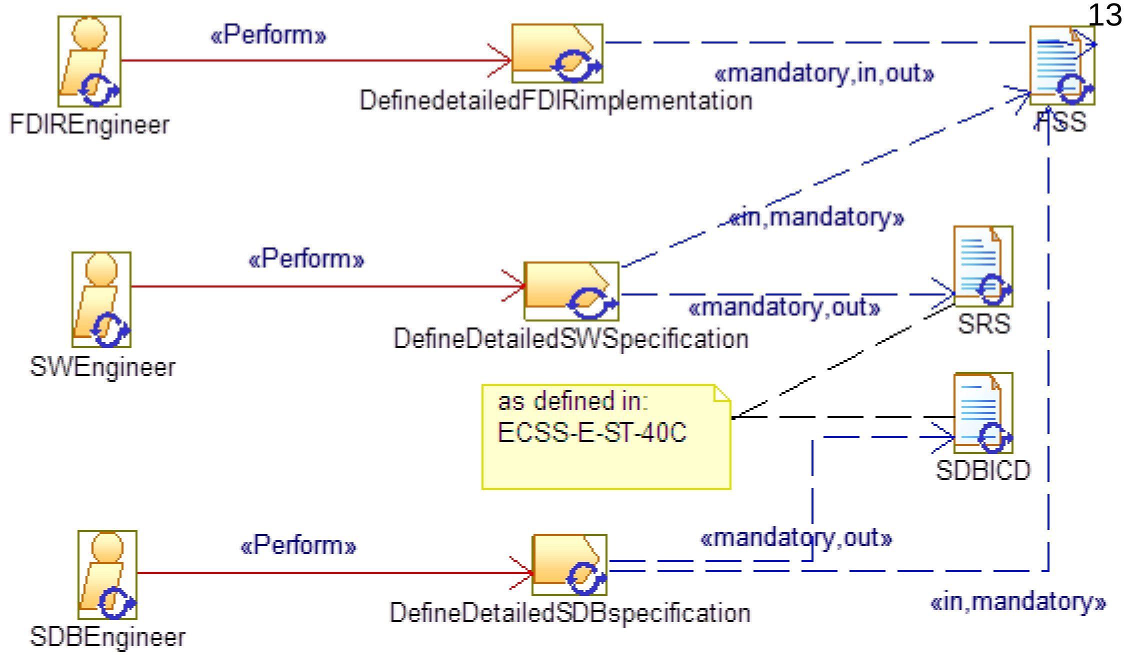
Perform Timed Fault Propagation Analysis

- Safety engineers:
  - specifies a TFPM for the design starting from fault trees, FMEA tables and Hazard Analysis
- Start: ***System SRR***
- End: ***System PDR***
- ***Outputs:*** TFPM analysis Report
- ***Tasks:***
  - Specify TFPM
  - Analyse TFPM



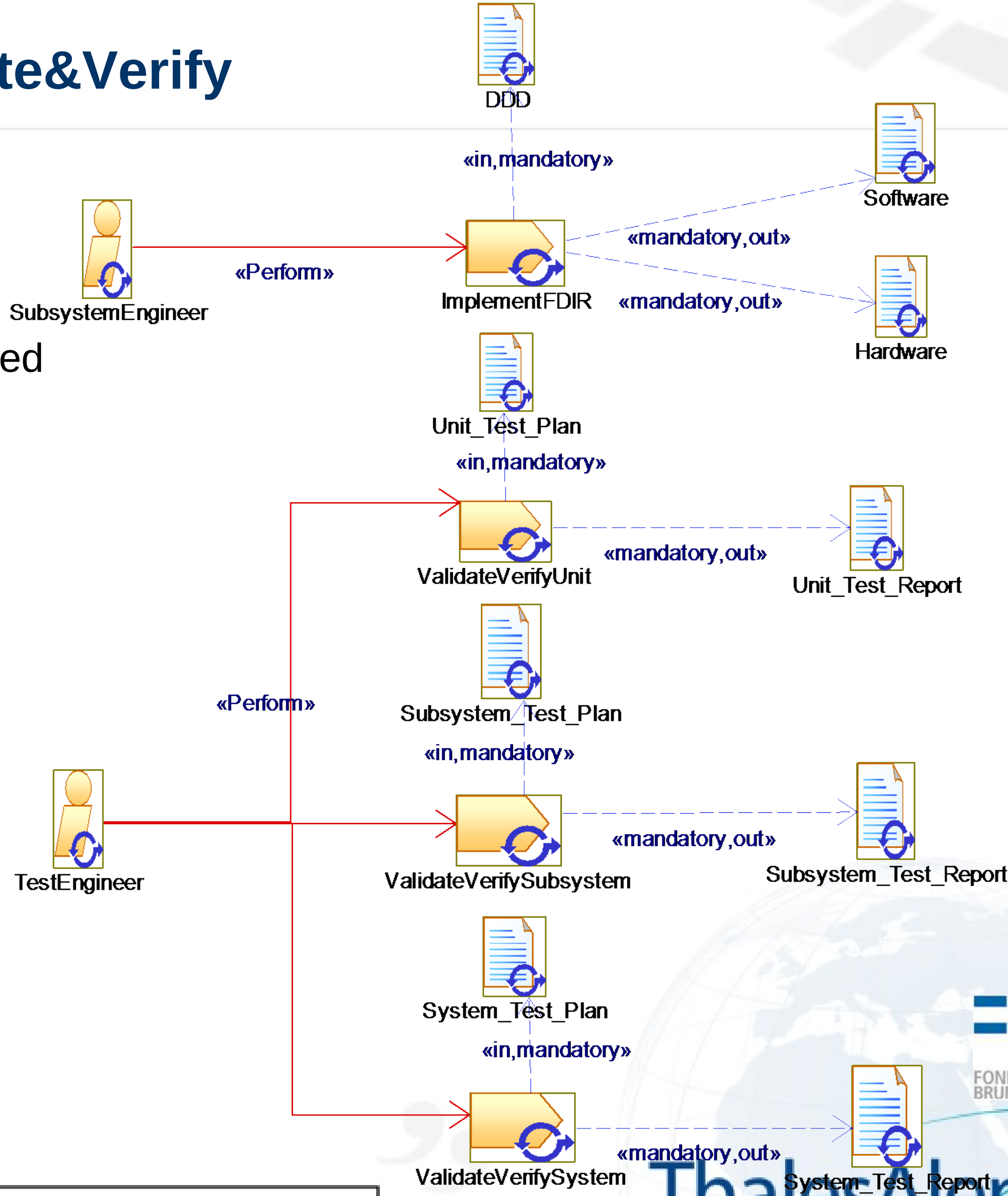
Design

- FDIR engineers, SW engineers, SDB engineers:
  - design FDIR in the various subsystems, software and database on the base of FDIR Reference Architecture.
- Start: ***System PDR***
- End: ***S/S CDR***



Implement FDIR, Validate&Verify

- S/S engineers, Testing engineers:
  - Implement FDIR in hardware or software and validated and verified respect to specifications
- Start: ***S/S PDR***
- End: ***System QR***

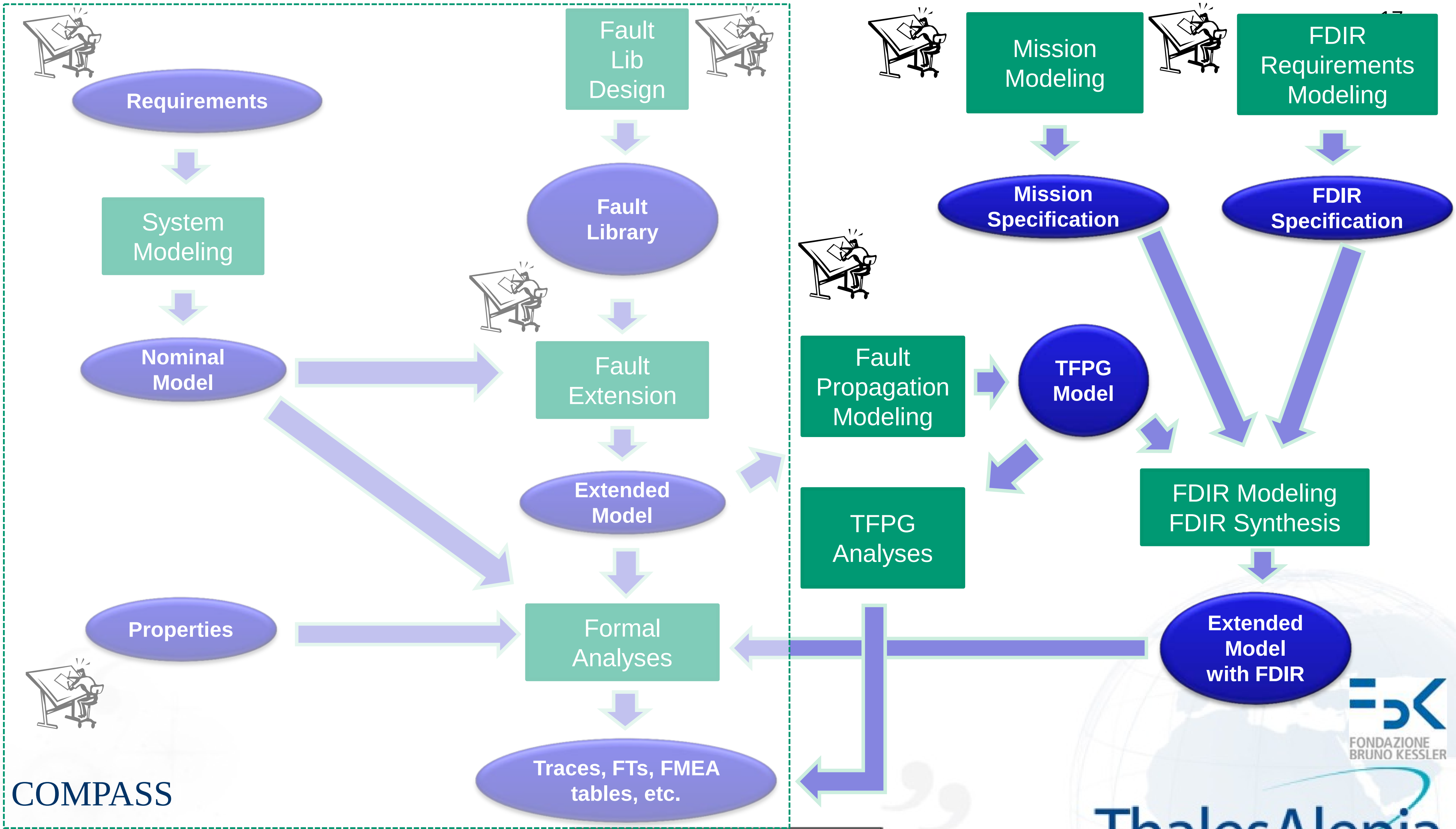


FAME Proposed Solution

Proposed Solution: the FAME environment

- FAME environment
  - Built on top of the COMPASS environment
    - Modeling in SLIM, a variant/extension of AADL language
    - Formal verification based on model checking engines
  - See demo
- Technical solutions
  - Routines for synthesis of FD from a TFPG
    - Synthesis of *alarms* - raised whenever faults can be diagnosed
  - Routines for synthesis of FR
    - Based on techniques for model-based planning
    - A *plan* is a recovery strategy that is guaranteed to bring the system into the specified target configuration, whenever an alarm is activated

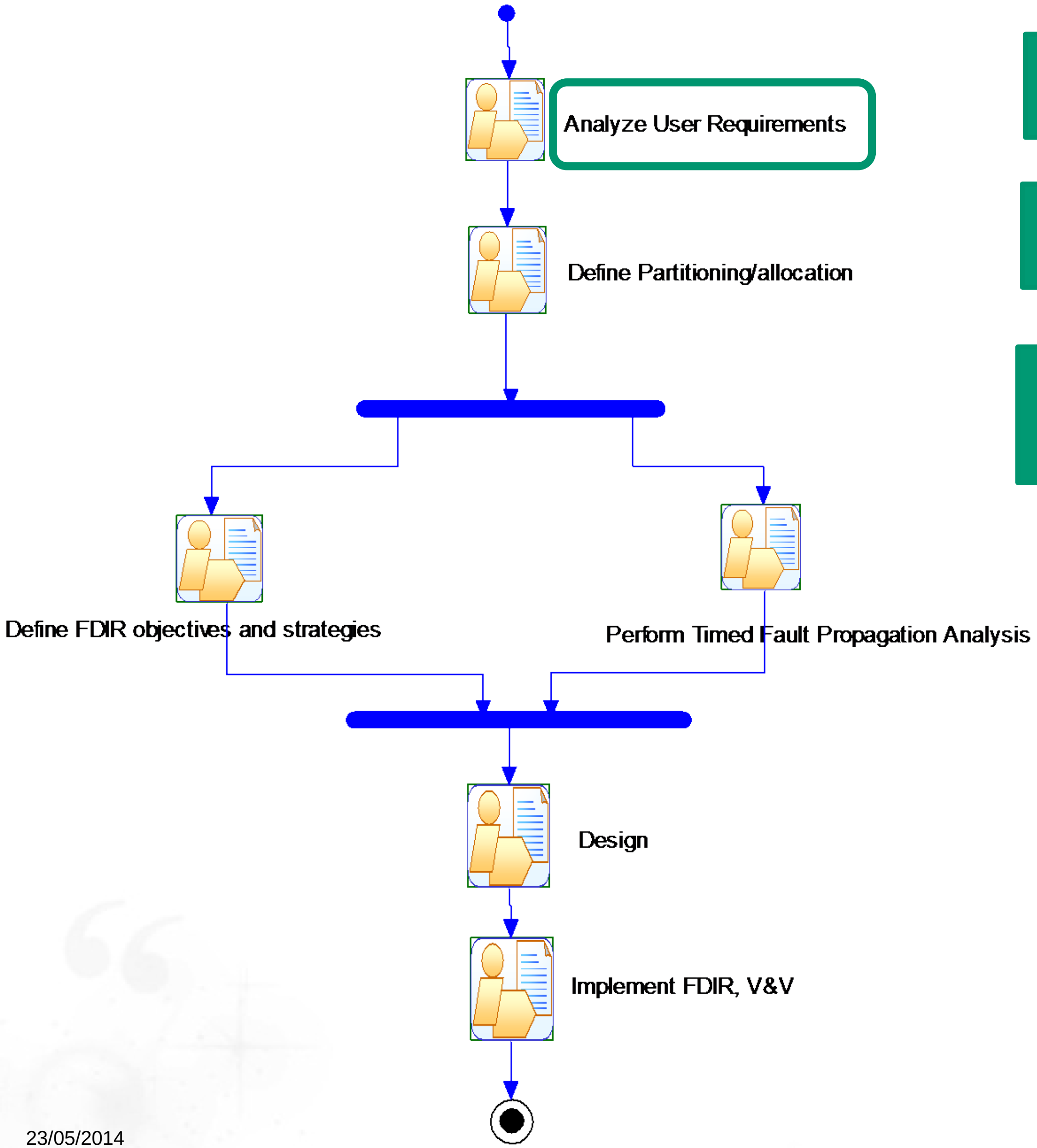
Proposed Solution: flow of the FAME environment



FONDAZIONE BRUNO KESSLER

ThalesAlenia Space
A Thales / Finmeccanica Company

FAME Environment and FAME Process

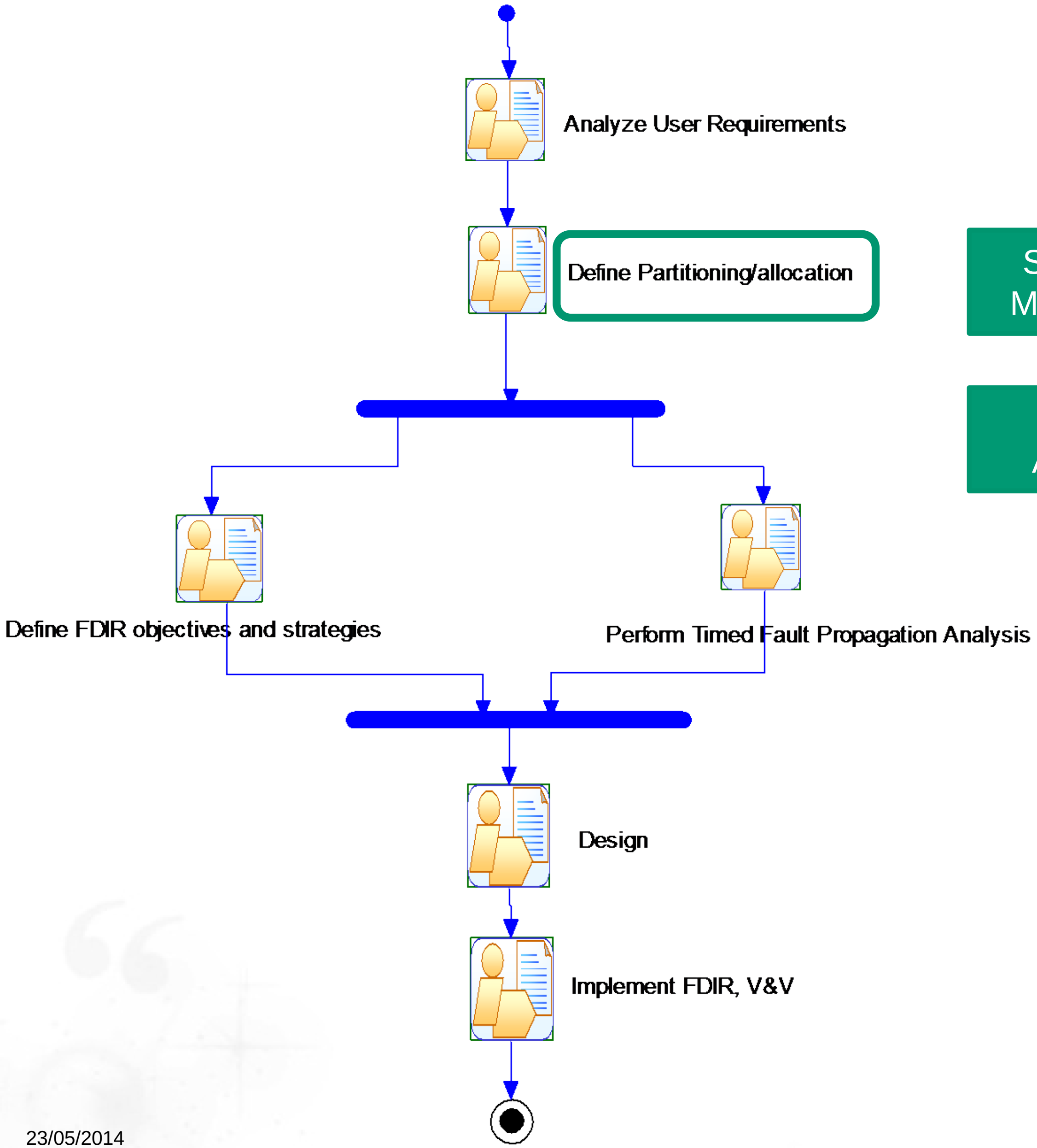


System Modeling + Fault Extension — Modeling nominal and faulty behavior

Formal Analyses — Derive requirements on the design of FDIR

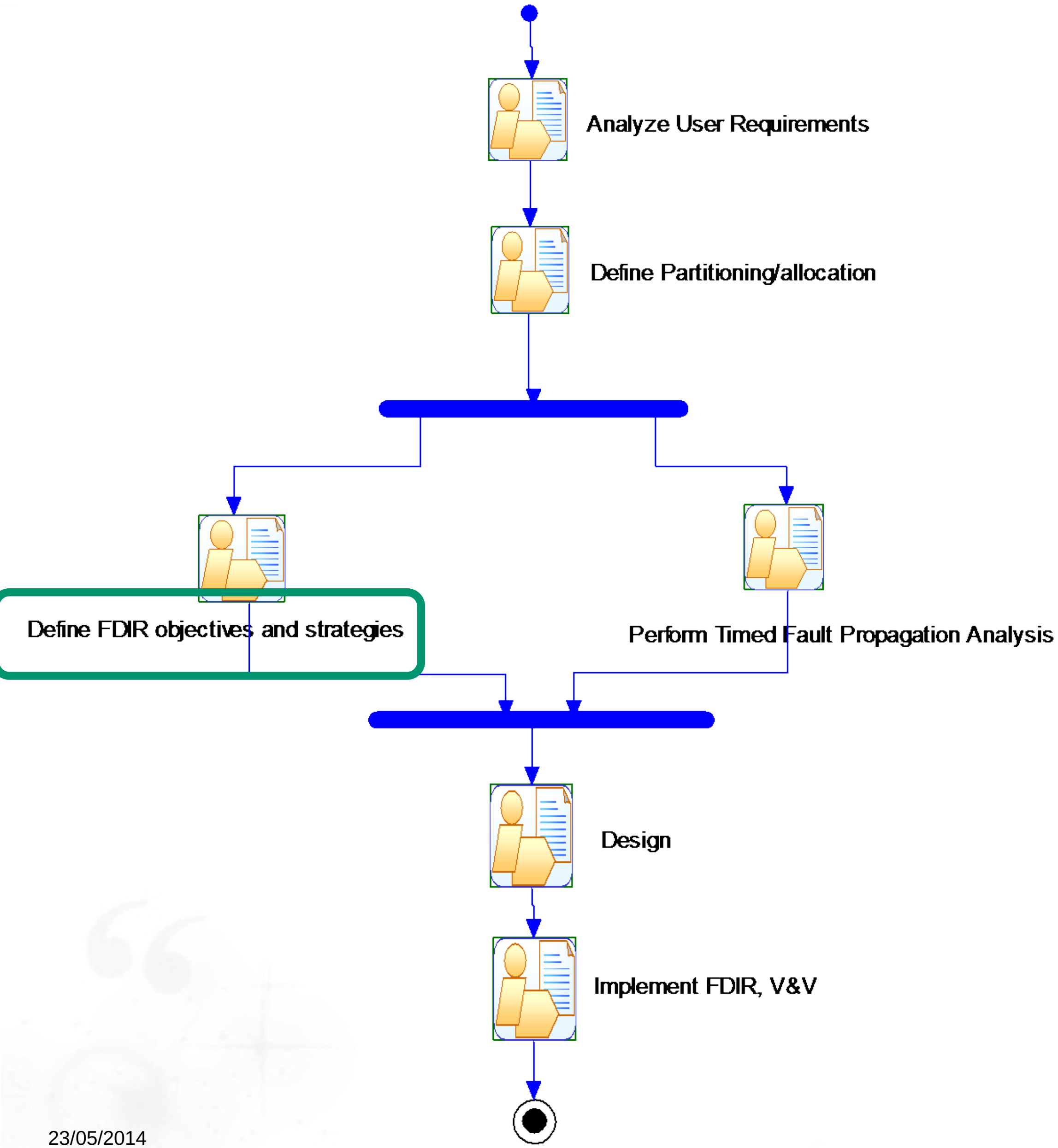
Mission Modeling — Definitions of phases, modes, and S/C configurations

FAME Environment and FAME Process



System Modeling	Modeling of FDIR, context, scope, architecture
Formal Analyses	Derive and collect FDIR requirements

FAME Environment and FAME Process



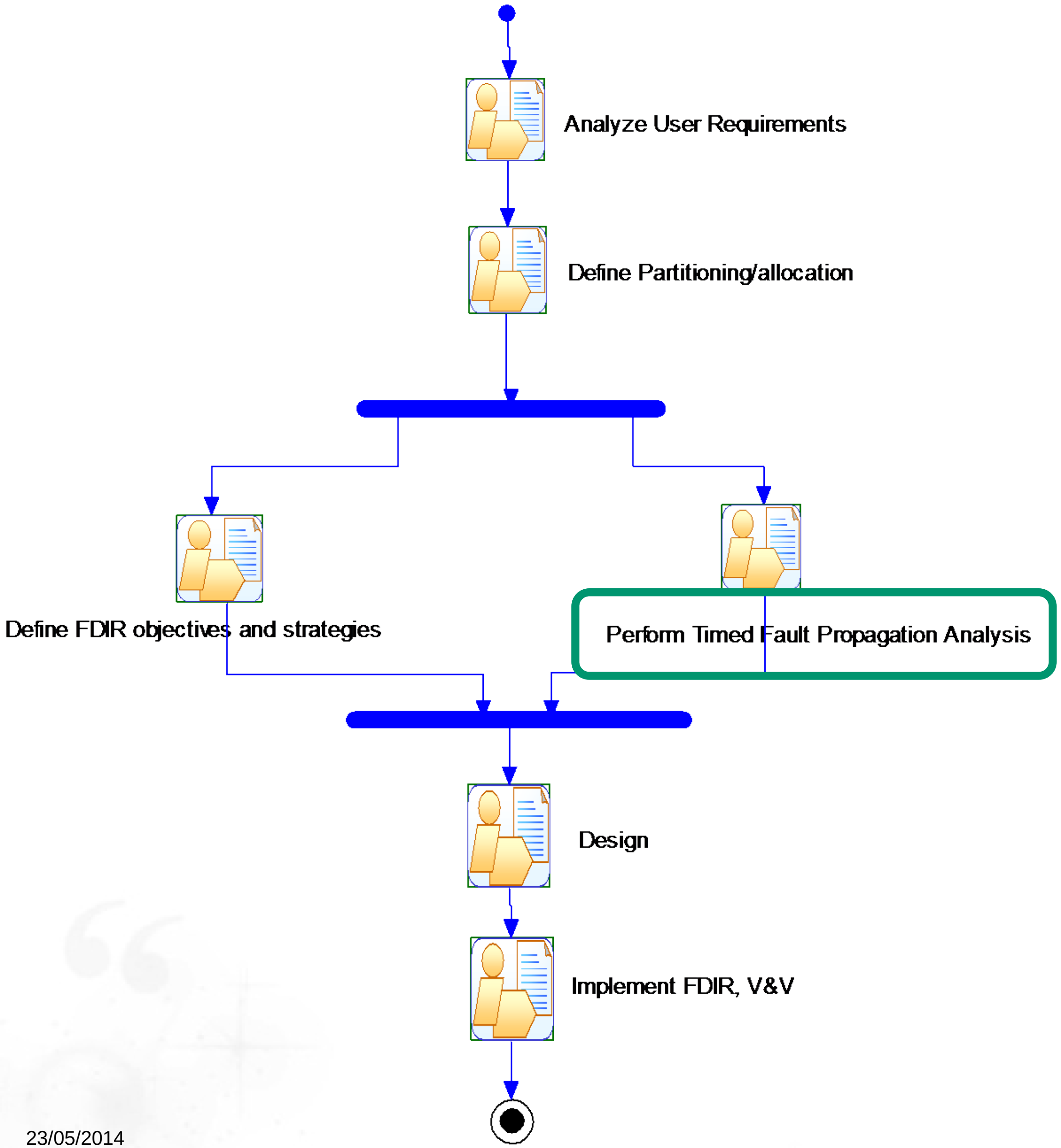
FDIR Requirements Modeling

FDIR objectives, strategies, pre-existing components, hierarchy, …

FONDAZIONE BRUNO KESSLER

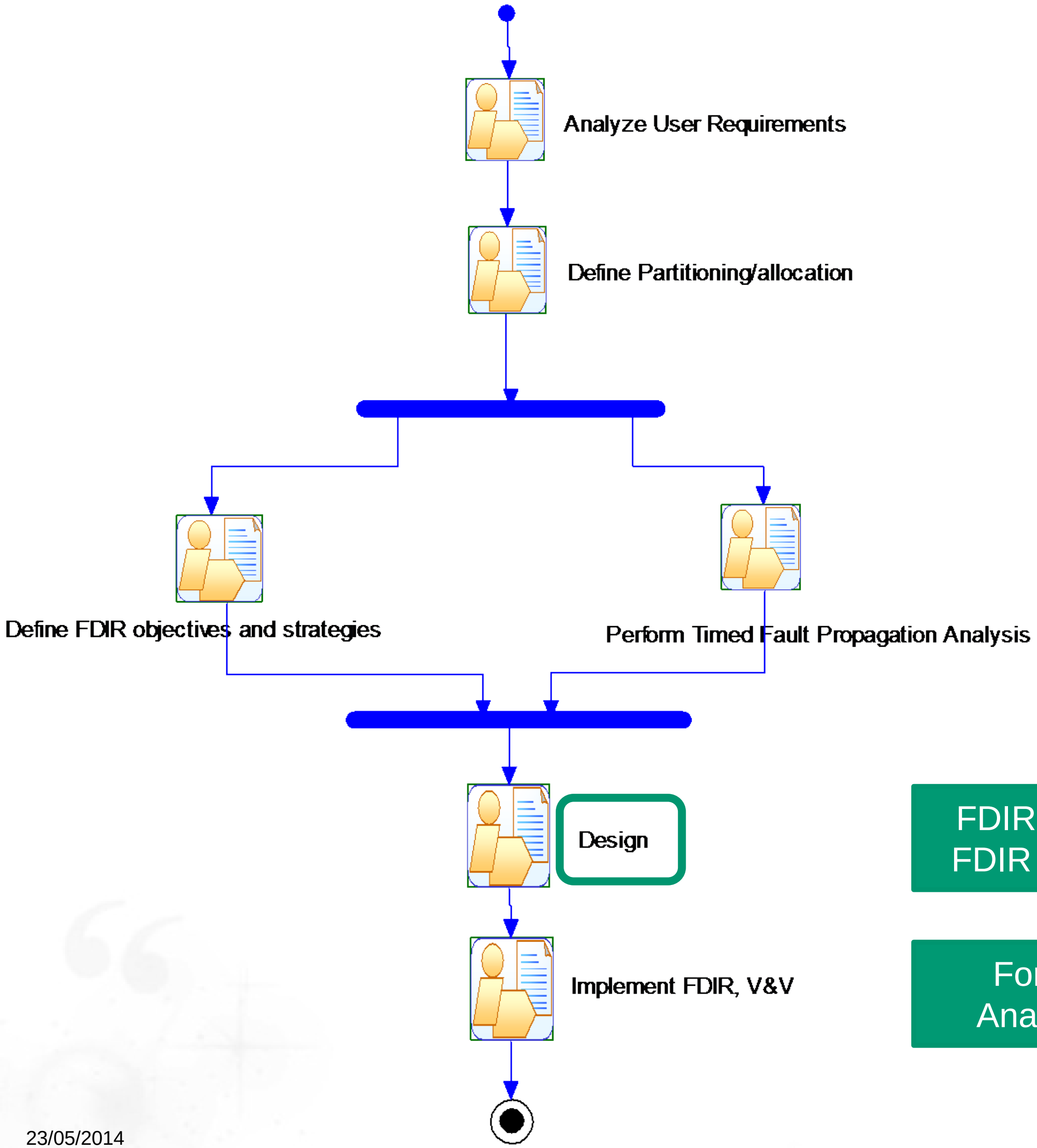
ThalesAlenia Space
A Thales / Finmeccanica Company

FAME Environment and FAME Process



Formal Analyses	Derive information on causality and fault propagation
TFPG (Fault Propagation) Modeling	TFPG modeling, editing, viewing
TFPG Analyses	TFPG behavioral validation, effectiveness validation, synthesis

FAME Environment and FAME Process



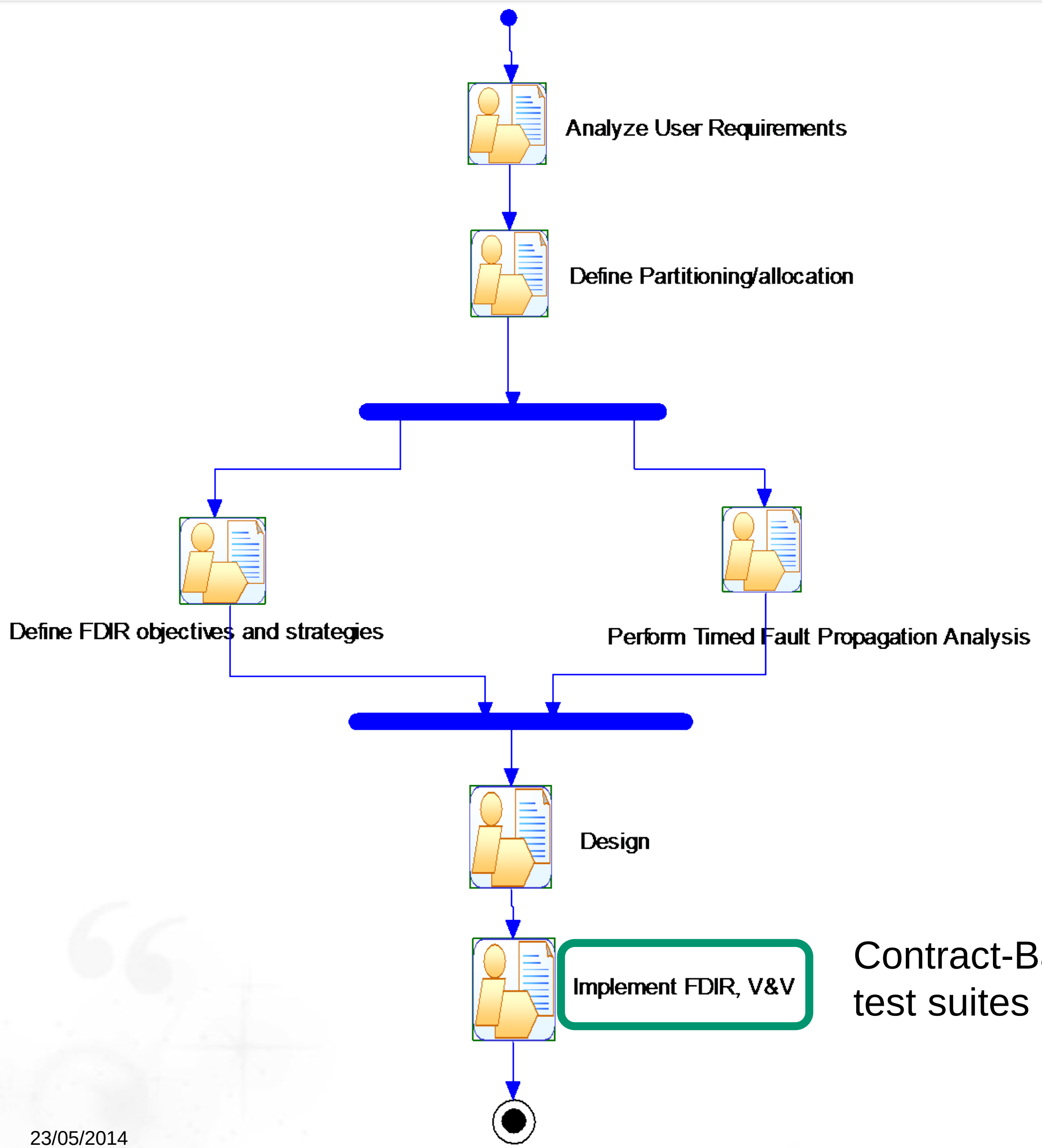
FDIR Modeling
FDIR Synthesis

Modeling / synthesis of FDIR

Formal Analyses

FDIR effectiveness verification

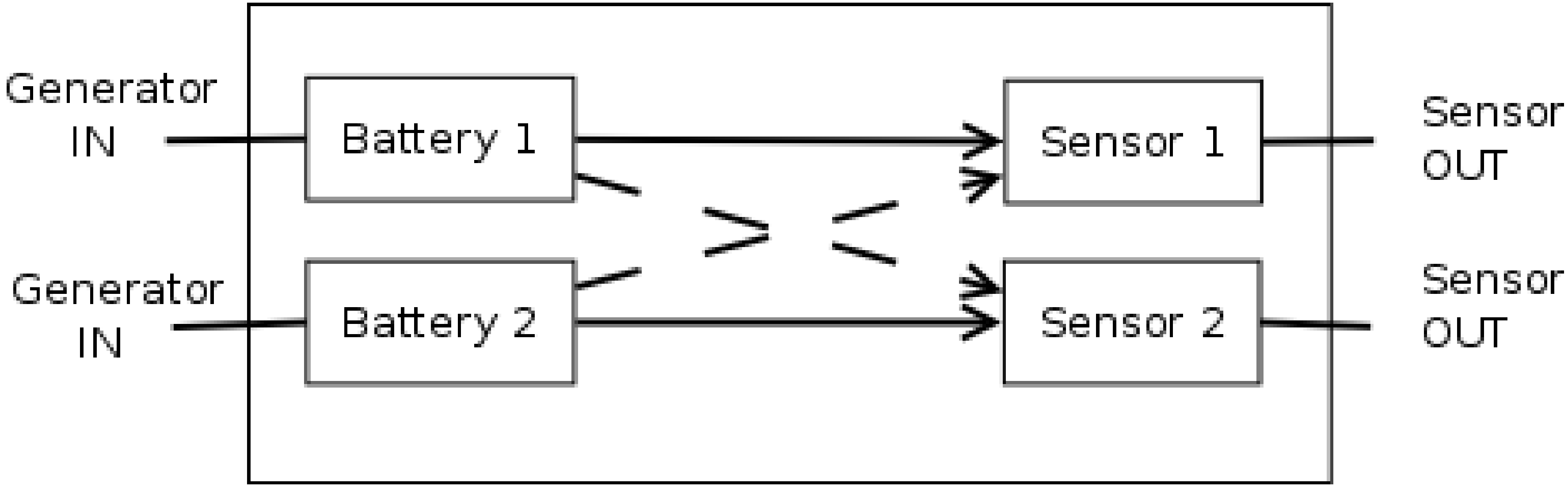
FAME Environment and FAME Process



Contract-Based Generation of test suites (future work)

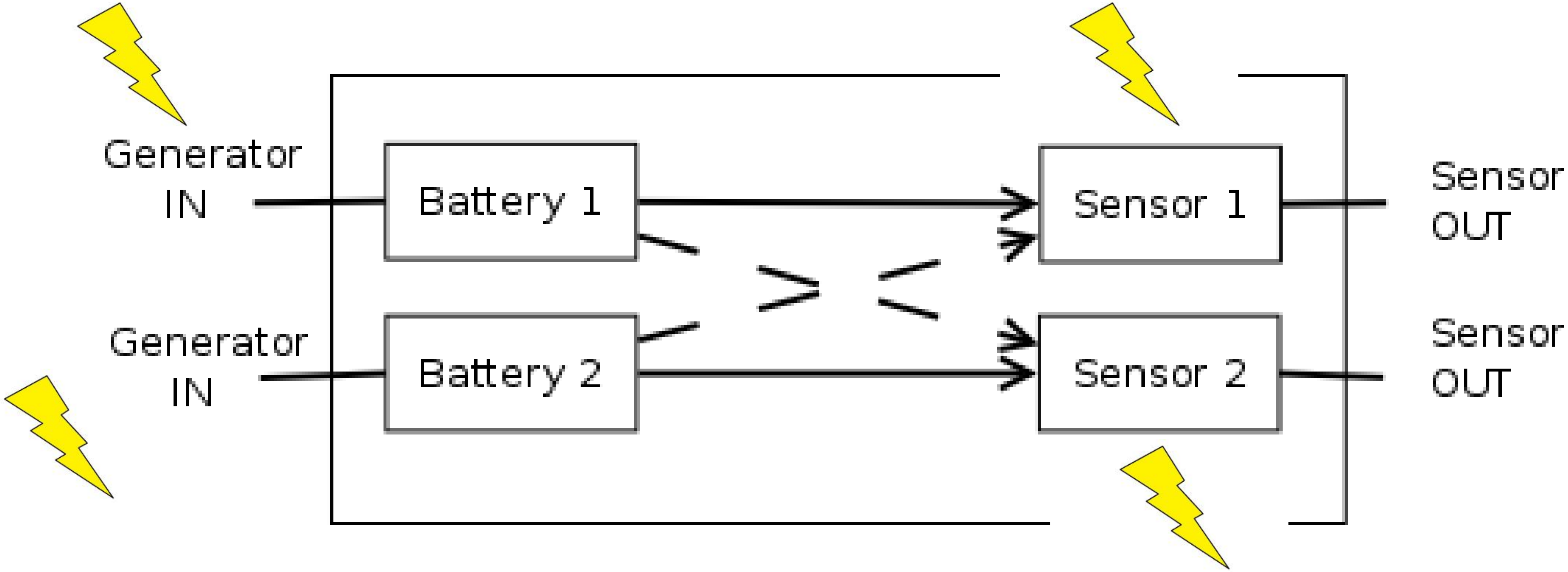
Demo of FAME Environment

The Battery Sensor Example: nominal system



- Battery Sensor
  - Generators powering batteries, in turn powering sensors
  - Redundant system: 2 Generators, 2 Batteries, 2 Sensors
  - At least one sensor must be working, for the system to be alive

The Battery Sensor Example: fault injections

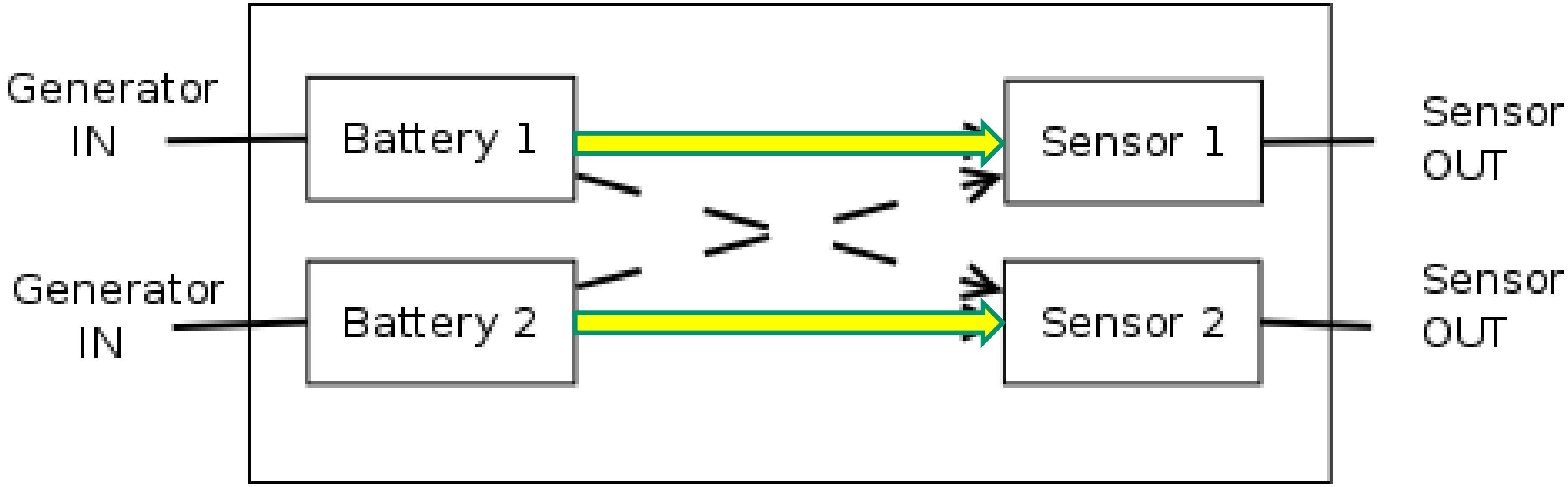


- Faults
  - Generators: off
  - Sensors: wrong output

THALES ALENIA SPACE INTERNAL

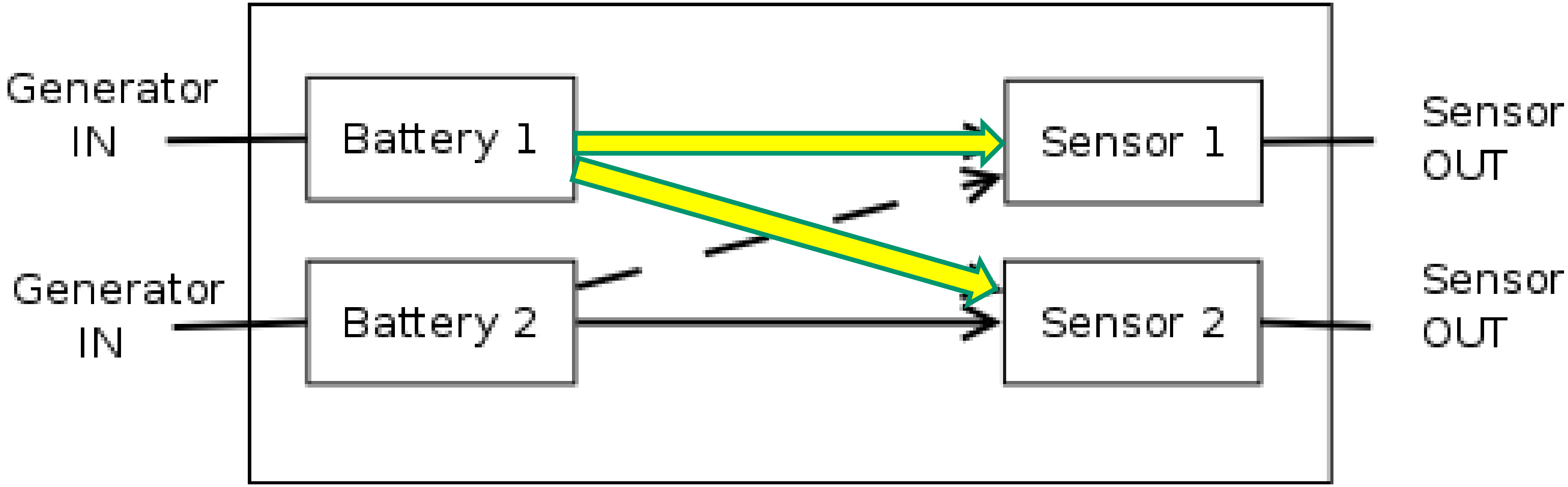
Ref.:

The Battery Sensor Example: system re-configuration



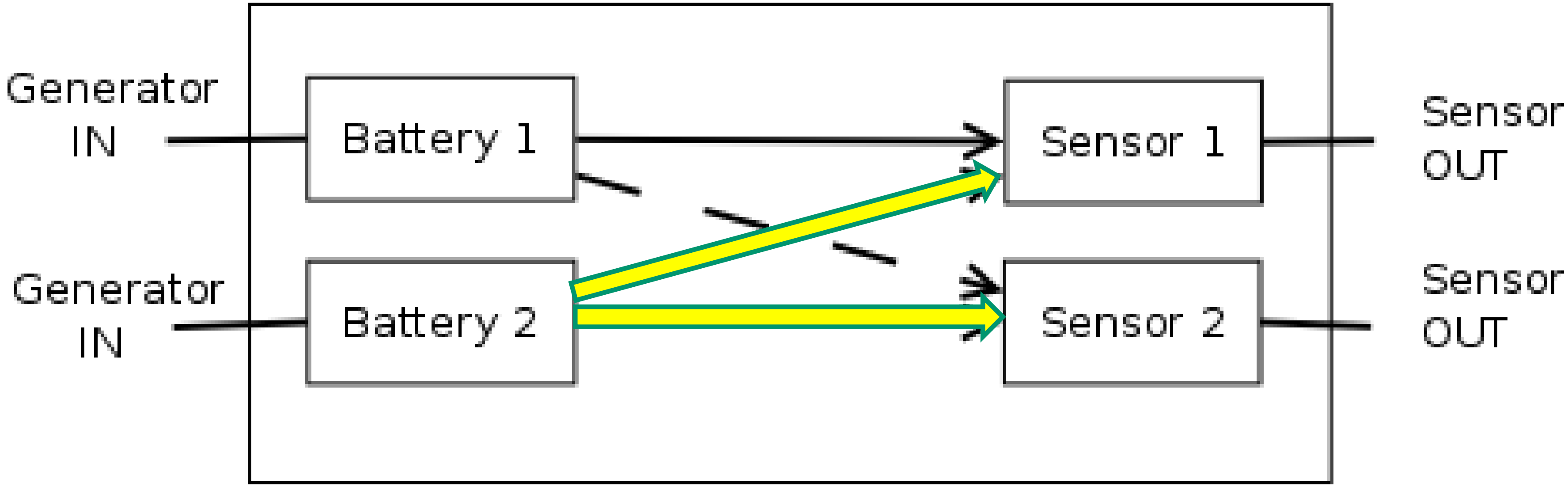
- Primary configuration
  - Battery 1 feeding sensor 1
  - Battery 2 feeding sensor 2

The Battery Sensor Example: system re-configuration



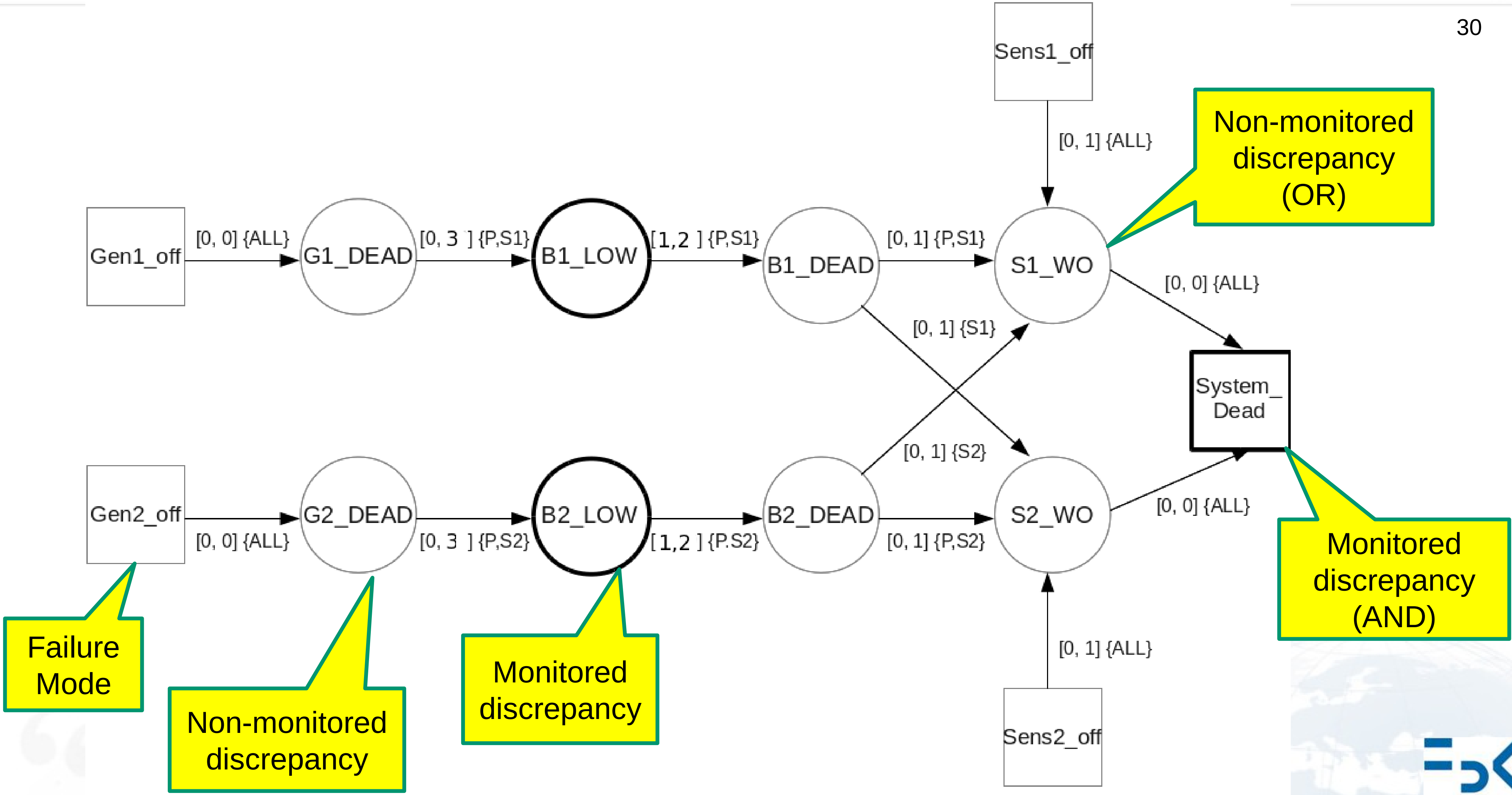
- Secondary 1 configuration
  - Battery 1 feeding both sensors

The Battery Sensor Example: system re-configuration



- Secondary 2 configuration
  - Battery 2 feeding both sensors

The Battery Sensor Example: TFPG



Demo of the FAME Toolset

- Structure of the demo
  - Loading of
    - Models
    - Fault injections
    - Mission Specification
    - TFPG and associations
    - FDIR specification
  - TFPG analyses
    - Behavioral validation
    - Effectiveness validation
  - Synthesis of FDIR
    - Synthesis of FD
    - Synthesis of FR
  - TFPG Synthesis

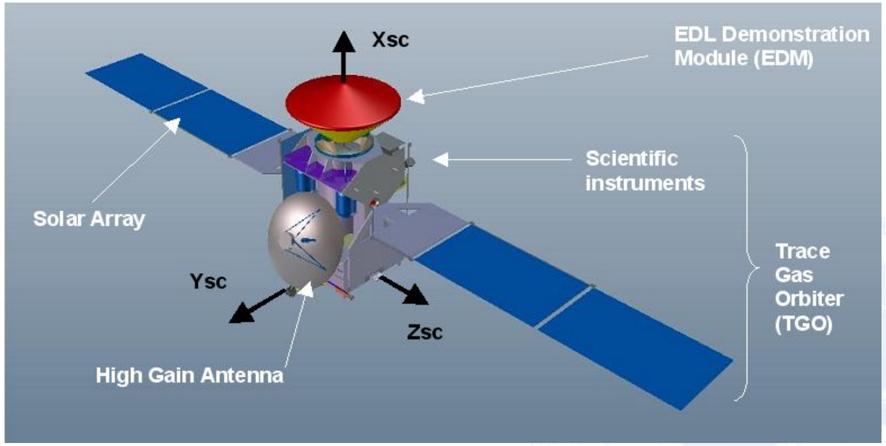
- DEMO follows …

Evaluation on a Case Study

Evaluation on a case-study

- Case-study : EXOMARS Trace Gas Orbiter (TGO)
  - Will be launched in 2016 and will arrive at Mars 9 month later.
  - Rich mission:
    - During transit to Mars : provide services to the Entry Descent Module
    - Atmosphere entry / Orbit Insertion after EDM ejection
    - Aerobreaking to reach the science orbit after EDM operations completion
    - Science and data acquisition
    - 2018 : new Rover support

- Complex mission = complex FDIR:
  - autonomy
  - Mission phase dependent:
    - Fail Op / Fail Safe strategies
    - Hot / Cold redundancies



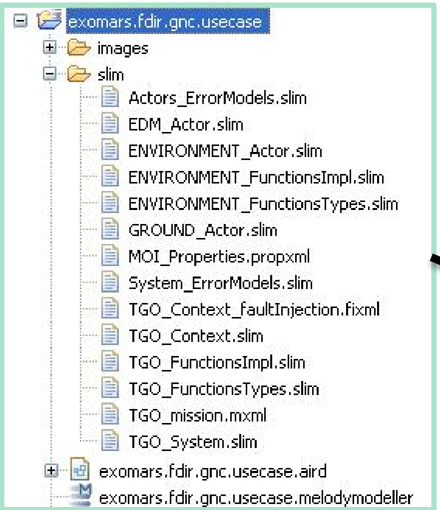
FONDAZIONE BRUNO KESSLER

ThalesAlenia Space
A Thales / Finmeccanica Company

Evaluation on a case-study

Safety analysis :

1. Nominal behaviour of the system is defined in SLIM language



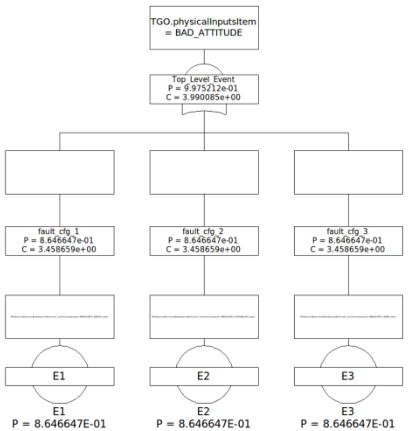
2. Feared event analysis and FMECA allows to identify failures

Item No.	Function Desc.	Part Name & Ref. Des.	Failure Mode or Fault	Failure Detect Method	Local Effect	System Effect	Cat. of Crit.	Remarks
FAME_IMU_001	GYRO	SENS_01	Sensor Signal is too low	EXT	Continuous self-reset of IMU	No measure is sent	2R	External equipment should be able to detect absence of measures
FAME_IMU_002	GYRO	SENS_01	Sensor output is biased	EXT	none	Biased Δθ output from sensor channel.	2R	External equipment should perform inertial data reasonable checks. Failure mode can be detected only if failure effect exceeds pre-determined acceptable operating Limits (see FAME_IMU_003)
FAME_IMU_003	GYRO	SENS_01	Sensor output is erroneous	INT	Loss of RLG dither control;. Dither stripper gains outside of expected limits. Dither amplitude shows fault.	Erroneous Δθ output from sensor channel. Degraded gyro performance including ... instability.	2R	IMU Health status indicate the error to external world.

3. Error models and fault injection are defined

Fault Injections

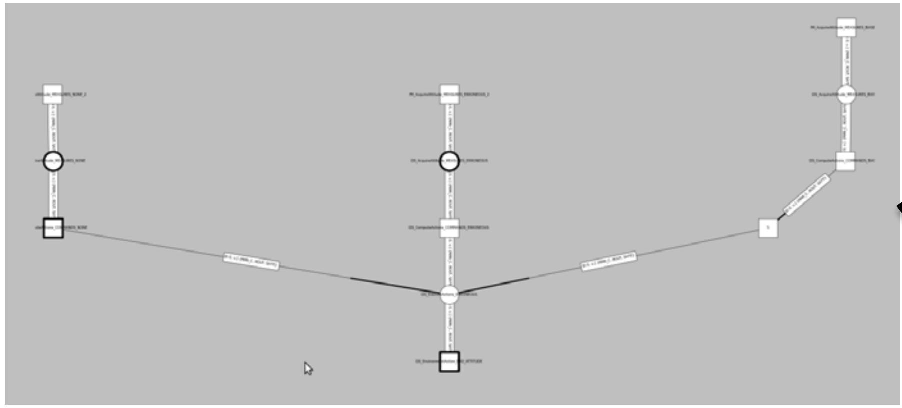
Use	Error Implementation	Error State	Effect
☑	_default_::AcquireAttitude.impl	MEASURES_NONE	TGO.AcquireAttitude_Block.AcquireAttitude1.attitudeMeasuresItem := MEASURES_NONE
☑	_default_::AcquireAttitude.impl	MEASURES_ERRONEOUS	TGO.AcquireAttitude_Block.AcquireAttitude1.attitudeMeasuresItem := MEASURES_ERRONEOUS
☑	_default_::AcquireAttitude.impl	MEASURES_BIASED	TGO.AcquireAttitude_Block.AcquireAttitude1.attitudeMeasuresItem := MEASURES_BIASED



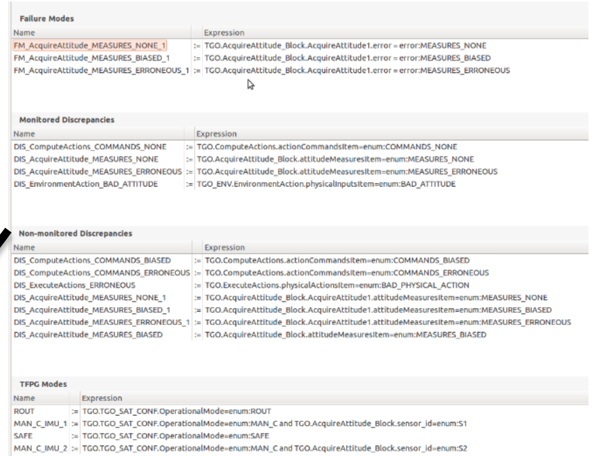
4. Fault trees are generated by COMPASS

FONDAZIONE BRUNO KESSLER

TFPG modeling and validation



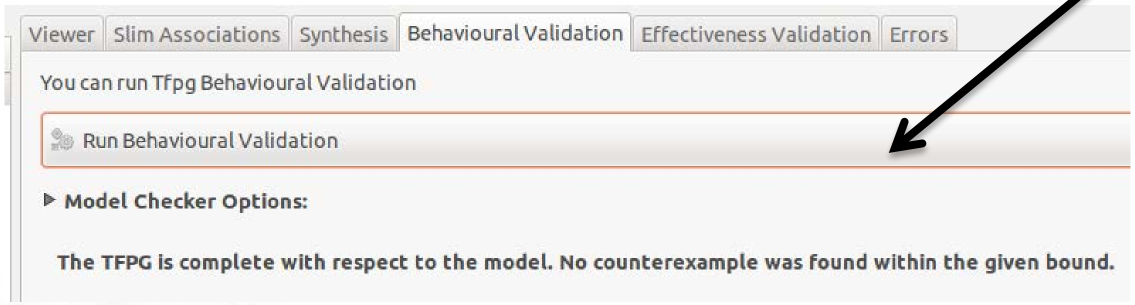
1. TFPG modeling or synthesis



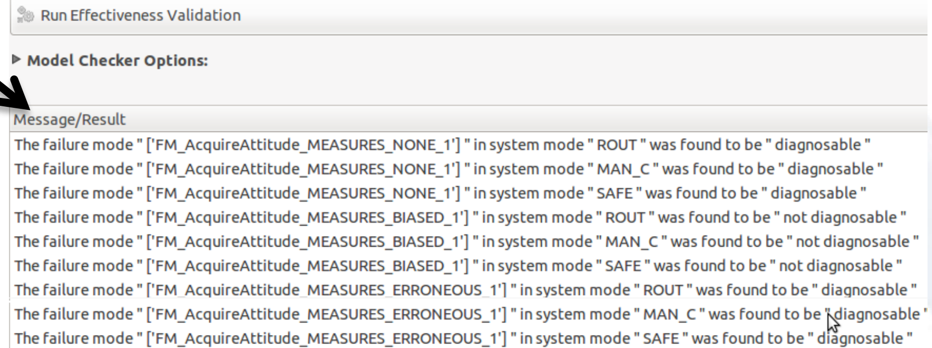
2. TFPG associations definition

FAME

3. TFPG behavioural validation



4. TFPG effectiveness validation



FDIR requirement analysis

1. FDIR requirement analysis

[FAME-SUB-CASE-STUDY-FDIR-REQ-010]
Mission shall be ensured for any single failure

[FAME-SUB-CASE-STUDY-FDIR-REQ-020]
TGO shall be able to achieve its manoeuvres of Mars Orbit Insertion even in case of single failure.

2. FDIR objectives definition

[FAME-SUB-CASE-STUDY-FDIR-OBJ-010]
If IMU failure item “FAME_IMU_001” occures during phase “MOI” and mode “MAN_C”, TGO shall be able to carry on the manoeuvre.

[FAME-SUB-CASE-STUDY-FDIR-OBJ-020]
If IMU failure item “FAME_IMU_001” occures during phase “MOI” and mode “ROUT”, TGO shall not start the manoeuvre and go to SAFE mode.

3. FDIR strategy definition

[FAME-SUB-CASE-STUDY-FDIR-STR-010]
If a failure occures on the nominal IMU during phase “MOI” and mode “MAN_C”, the TGO system shall autonomously switch to redundant unit.

[FAME-SUB-CASE-STUDY-FDIR-STR-011]
If a failure occures on the redundant IMU during phase “MOI” and mode “MAN_C”, the TGO system shall reset this redundant unit and try to carry on the manoeuvre.

Evaluation on a case-study

FDIR Specification :

FAME

1. Modes

Phases

Name
MOI

Op-modes

Name
ROUT
MAN_C
SAFE

2. Space-craft configurations

S/C Configurations

Configuration ID	Allowed spacecraft configuration	Associated Op-modes
IMU_1	TGO.AcquireAttitude_Block.sensor_id = enum:S1	MAN_C ROUT
IMU_2	TGO.AcquireAttitude_Block.sensor_id = enum:S2	MAN_C SAFE

3. Phases/modes combination

Phase / Op-mode combination

Phases	Associated Op-modes	Definition via Observable
MOI		
	MAN_C	TGO.TGO_SAT_CONF.MissionPhase=enum:MOI and TGO.TGO_SAT_CONF.OperationalMode=enum:MAN_C
	ROUT	TGO.TGO_SAT_CONF.MissionPhase=enum:MOI and TGO.TGO_SAT_CONF.OperationalMode=enum:ROUT
	SAFE	TGO.TGO_SAT_CONF.MissionPhase=enum:MOI and TGO.TGO_SAT_CONF.OperationalMode=enum:SAFE

4. Fault Detection

Component	Error State	Failure Mode	Generated alarm	Predefined alarm	Enabled
TGO.AcquireAttitude_Block.AcquireAttitude1					
	MEASURES_NONE	FM_AcquireAttitude_MEASURES_NONE_1	NO_MEAS_1		☑
	MEASURES_ERRONEOUS	FM_AcquireAttitude_MEASURES_ERRONEOUS_1	ERR_MEAS_1		☑
	MEASURES_BIASED	FM_AcquireAttitude_MEASURES_BIASED_1	BIASED_MEAS_1		☑

4. Fault Recovery

FR Table

Alarm	Phase	Op-mode	Severity	Target mode	Target conf	Target constraints	Allowed Recovery Actions	Predefined recovery
NO_MEAS_1								
	MOI							
		MAN_C	2 (Critical)	MAN_C	IMU_2		all	
		ROUT	1 (Catastrophic)	SAFE	IMU_2		all	
		SAFE	1 (Catastrophic)	SAFE	IMU_2		all	
ERR_MEAS_1								
	MOI							
		MAN_C	2 (Critical)	MAN_C	IMU_2		all	
		ROUT	1 (Catastrophic)	SAFE	IMU_2		all	
		SAFE	1 (Catastrophic)	SAFE	IMU_2		all	
BIASED_MEAS_1								
	MOI							
		MAN_C	2 (Critical)	MAN_C	IMU_2		all	
		ROUT	1 (Catastrophic)	SAFE	IMU_2		all	
		SAFE	1 (Catastrophic)	SAFE	IMU_2		all	

- Fault Detection and Recovery Synthesis :

FAME

Alarms Generated: 3 out of 3
Size of the FD (number of states): 2413

Plans Generated: 6 out of 9
Size of the FR (number of states): 64

Evaluation on a case-study

- Process and technology evaluation
  - Process compatible with industrial process
  - Benefits : formalism (SLIM and TFPG), well defined and guided process, timing analysis of failure propagation
  - Limitations : state space explosion on big models, decentralized FDIR not yet supported, still some problems in FR synthesis

- Conclusion :
  - Experiments on TFPG is promising
  - Still some technical challenges to solve
  - Requires a strong cooperation between industrials and academics

Characterization of the Approach

Characterization of the approach

	FAME Process	FAME Methodology	FAME Environment
Adequacy	• Compliance with current project life-cycle • Compliance with applicable standard	Complexity of TFPG respect to number of failure mode and discrepancy	• Number and type of outputs provided by tools • Computing and elaboration time
Effectiveness	• Which part of project life cycle are improved • Time reducing	Complexity of TFPG versus SLIM model complexity	• Scalability of the tool-suite • Estimation of time spent for design
Usability	• Technical skills required to the industrial team. • Number of modifications to insert in the current industrial process	How SLIM model generated support the design of FDIR?	• Format of outputs • Graphical aspects. • Level of automation

Metrics

Characterization of the approach: Process

Adequacy	• **FAME process is compliant with the current project life cycle in terms of respect of phases (B,C,D)and reviews** • **It is independent from any tools** • **Starting point of FAME process is Mission Requirements Document that is available at the beginning of life-cycle** • **FAME process is compliant with applicable standards**
Effectiveness	• The project can benefit of FAME process in the initial phases where FDIR is not yet defined • A clear definition of inputs and outputs of each activity with criteria for ach check point guarantees an optimization of time spent for each activity by avoiding to waste time and effort to accomplish premature tasks
Usability	• FAME process can be inserted easily in the current industrial process • FAME process can be inserted inside the ECSS standards • The use of TFPG requires a training of users in order to learn the methodology

Characterization of the approach: Methodoloy

Adequacy	• **TFPG is based on the identification of failure mode and discrepancies, and transitions between discrepancies** • **TFPG complexity depends on number of nodes and edges and by temporal constants in use** • **Slim generated by synthesis can be analyzed by using COMPASS features as correctness.**
Effectiveness	• The application of the FAME methodology to the space domain may be limited by the state-space explosion when introducing time on complex models. • SLIM models used in the FAME process shall not be created from scratch, but shall be derived from existing models of the system
Usability	• The failure management is designed in an incremental way, considering small subset of failures, and taking into account the assumptions related to these failures • At the end, all the results should be combined in order to generate FD and a FR modules that covers the entire set of FDIR specification for the entire set of failures in the system, and therefore taking into consideration all the TFPGs

Characterization of the approach: FAME Environment

Adequacy	• **There is a need to set up a strong configuration management process for input and outputs files** • **Computing and elaboration time depends on complexity of TFPG for what concerns the synthesis of detection**
Effectiveness	• Scalability of the tool-suite depends on several factors (Dimension of slim model, number of observables and time constants
Usability	• TFGP respects the structure of TFPGs but not easily readable when the graph is big. TFPG format should also include the possibility to model system, subsystems and units • Level of automation is good: changes on TFPG textual file are reflected in graphical view (roundtrip is good)

Output	xml	slim	tfpg	FAME Window
TFPG	x		x	x
FD Synthesis		x		x
FR Synthesis		x		x
Effectiveness Validation				x
Behavoir validation				x
Fault Injections	x			x
Mission specification	x			x
Associations	x			x
FDIR Specification	x			x

Tmin to tmax	Computing time [sec]
1 to 2	40
1 to 3	50
1 to 4	65
1 to 5	75
1 to 6	90
1 to 7	115
1 to 8	992

Number of monitored Node	Time[sec]
1	20
2	40
3	60
4	94
5	874

Conclusions

Conclusion (1/3)

Challenge	FAME Process	FAME environment
Conflict between bottom-up approach and top-down approach for fault identification methods	Use of functional analysis in FDIR analysis Performing diagnosability analysis	TFPG effectiveness analysis for diagnosability
Show quantitative benefits to support engineering trades	identification of redundancy in Define FDIR Architecture task	-
It is necessary to better define products and processes, and process metrics	- List of checkpoints - List of roles - List of artifacts - Rules to checking consistency of FAME process	future extension of FAME foresees process verification using NuSMV.
Perform adequate V&V	contract based validation	Future extension
Write relevant, decomposable requirements	use FDIR analysis as input to Define FDIR Objectives tasks to derive FOS	-
Improve the generation of FDIR artifacts	Perform analysis for each failure step in Define FDIR Architecture	TFPG synthesis, TFPG Effectiveness Validation and TFPG Behavioural Validation
Difficulty to determine the propagation of failure in terms of time	Perform Timed Fault Propagation Analysis activity.	TFPG Management

Challenges for current industrial approach

Conclusions (1/2)

- Functional Analysis can be used early in the process with a positive effect on the eventual FDIR maturity
- Failure propagation can be analyzed with TFPG
- FAME process is phased
- FAME process can be employed starting form the early system development phases, and which is able to take into account the design and RAMS data from both, Software and System perspective
- FAME process includes the corresponding V&V perspective, and puts the FDIR in the system operation and mission execution context

Conclusion (1/3)

- Future Extensions
  - FDIR architecture
    - Modeling of scope/context/level of authority of FDIR
    - Modeling of FDIR levels - hierarchy
    - Hierarchical TFPGs
    - Synthesis of hierarchical/decentralized FDIR
  - Hazard Analysis
  - TFPG synthesis
    - Synthesis of timings and modes
  - Contract-based Design and Verification of FDIR

Questions?

- Marco Bozzano bozzano@fbk.eu
- Regis De Ferluc regis.deferluc@thalesaleniaspace.com
- Andrea Guiotto andrea.guiotto@thalesaleniaspace.com

Thank you!