An Integrated Process for FDIR Design in Aerospace

Fondazione Bruno Kessler, Trento, Italy
Benjamin Bittner, **Marco Bozzano**, Alessandro Cimatti, Marco Gario

Thales Alenia Space,France
Regis de Ferluc
Thales Alenia Space,Italy
Andrea Guiotto

European Space Agency, ESA-ESTEC,
Noordwijk - The Netherlands
Yuri Yushtein

ADCSS 2015; October 21, 2015; ESA-ESTEC, Noordwijk

Outline

Outline

The FAME Project

FAME

- FDIR Development and Verification and Validation Process

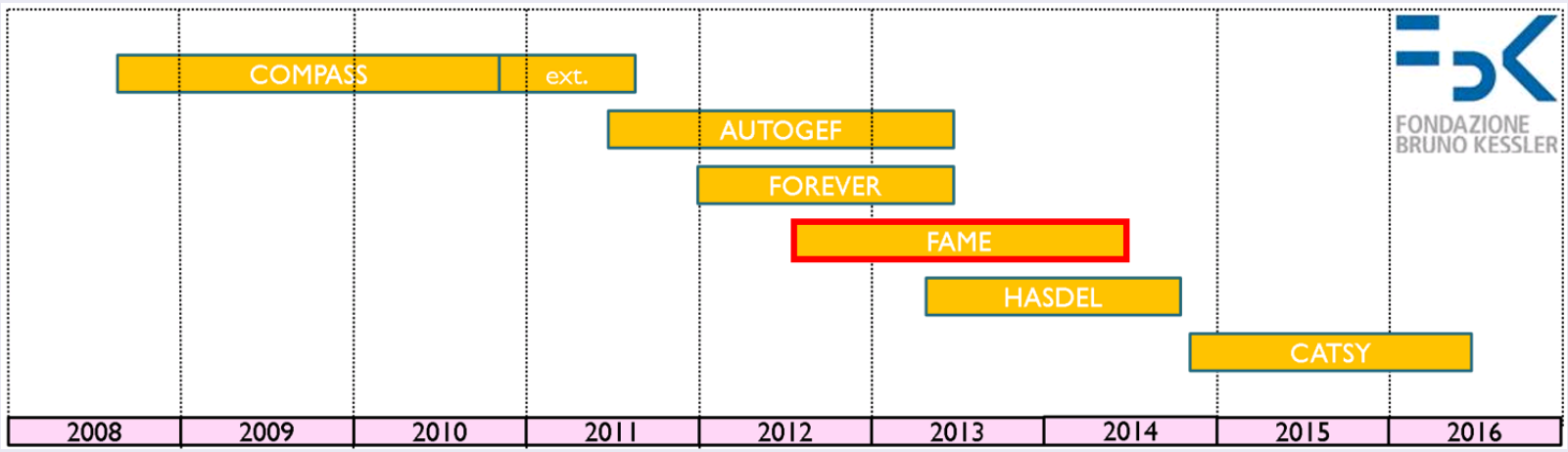
Funding & Supervision

- European Space Agency

Consortium

- Thales Alenia Space Italy, Thales Alenia Space France, FBK

Timeline: FBK participation in ESA Projects



Based on COMPASS (2008-2011)

COMPASS Consortium

- Funded by the European Space Agency
- Consortium: RWTH Aachen Univ., FBK, Thales Alenia Space France

COMPASS in a Nutshell

- A model-based approach to system-software co-engineering
- A coherent set of modeling and analysis techniques
- Correctness, safety, dependability, and performance of on-board computer-based aerospace systems

COMPASS Contributions

- Modeling in a variant of AADL called SLIM
- Verification methodology and toolset based on state-of-the-art formal methods

FDIR: Challenges

Motivation

- Complex safety-critical systems
- Safety, availability and autonomy are at stake
- Need to to detect and recover from faults, reliably and timely
- Effective coverage must be ensured

FDIR: Challenges

Motivation

- Complex safety-critical systems
- Safety, availability and autonomy are at stake
- Need to to detect and recover from faults, reliably and timely
- Effective coverage must be ensured

Challenges of FDIR Design

- Complexity of the underlying system
- Number of possible faults, complex dynamics and interaction

FDIR: Challenges

Motivation

- Complex safety-critical systems
- Safety, availability and autonomy are at stake
- Need to to detect and recover from faults, reliably and timely
- Effective coverage must be ensured

Challenges of FDIR Design

- Complexity of the underlying system
- Number of possible faults, complex dynamics and interaction

Limitations of Existing FDIR Designs

- Ad-hoc solutions, based on experience and past projects
- Developed late in the design process, when systems RAMS analyses (e.g. FTA and FMEA) become available
- Poorly phased: they do not cover full FDIR lifecycle

The FAME Goal in a Nutshell

Develop a comprehensive and coherent FDIR design methodology and process, able to deal with limitations and shortcomings of existing practices

FAME

The FAME Goal in a Nutshell

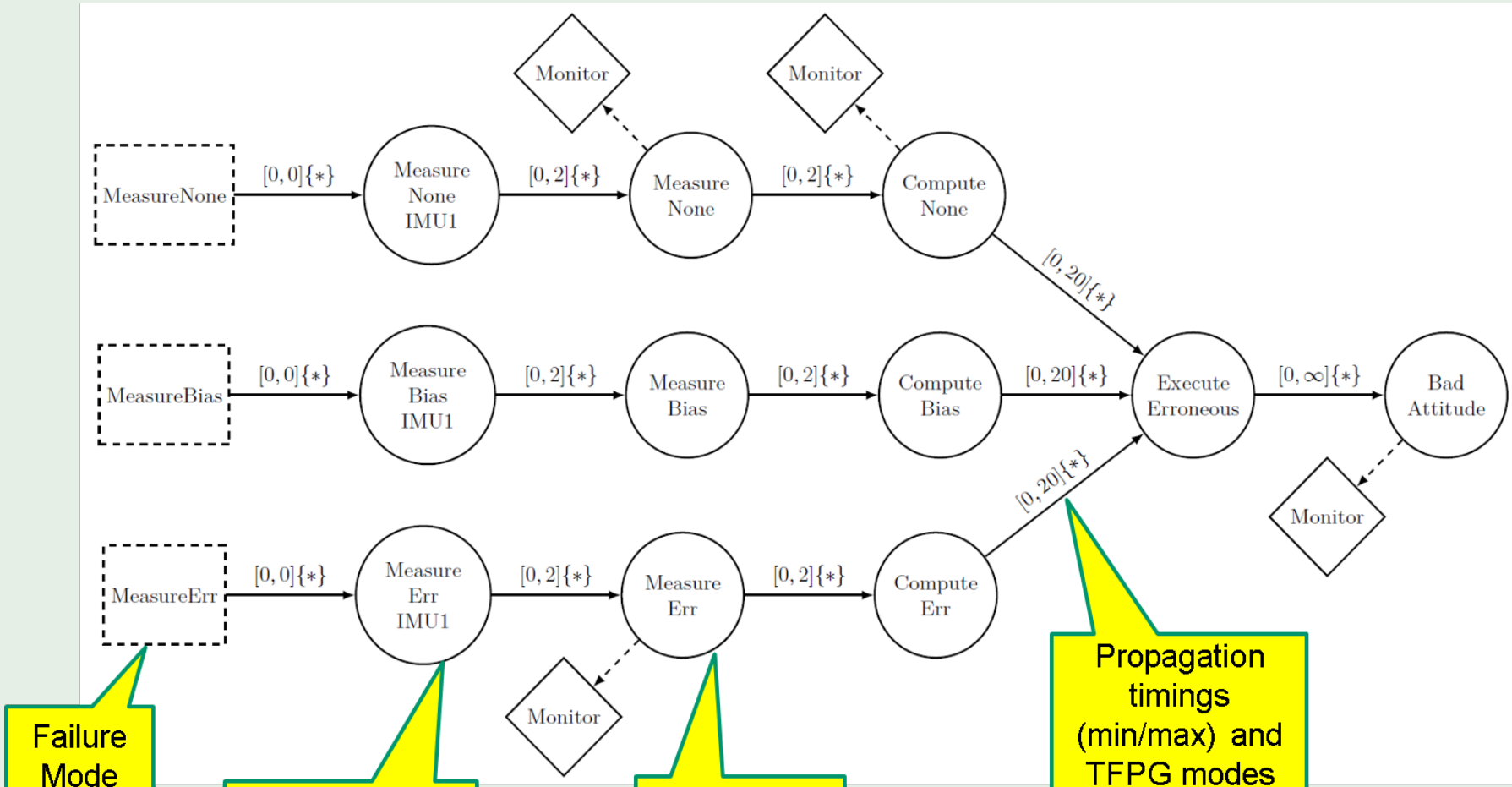
Develop a comprehensive and coherent FDIR design methodology and process, able to deal with limitations and shortcomings of existing practices

FAME Contributions

- Dedicated and coherent FDIR development methodology
- FDIR Development and V&V Process encompassing the full FDIR lifecycle, and enabling a consistent and timely FDIR conception, development, V&V
- Dedicated formalisms for modeling failure propagation: Timed Failure Propagation Graphs (TFPGs)
- FAME Environment: a tool – based on COMPASS – implementing the methodology and process
- Demonstration and evaluation of the approach on case studies

Timed Failure Propagation Graphs

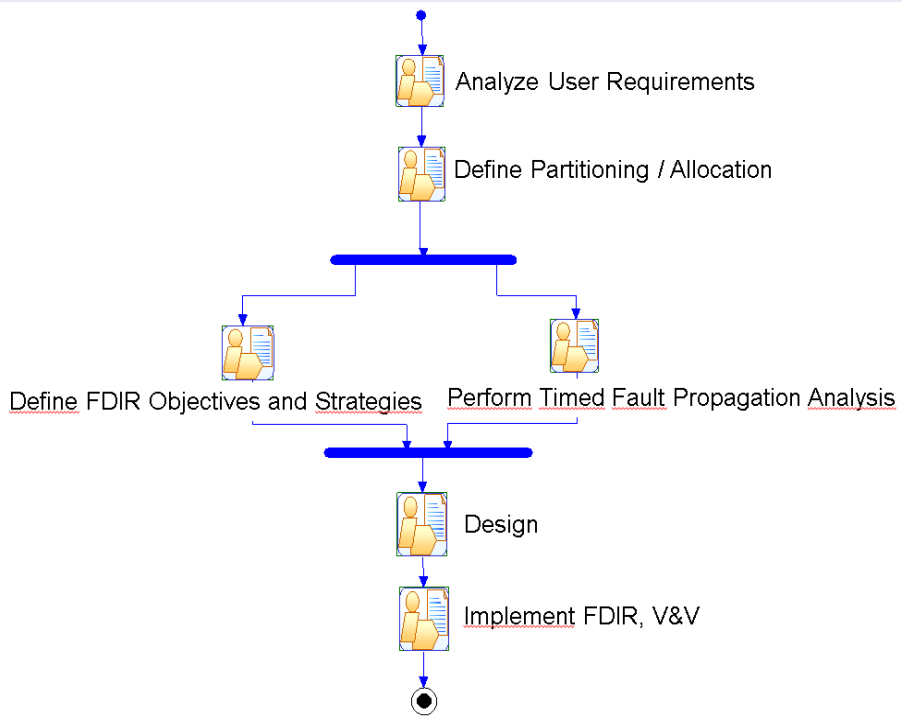
An Example TFPG



Outline

The FAME Process

FAME Process – Flow View

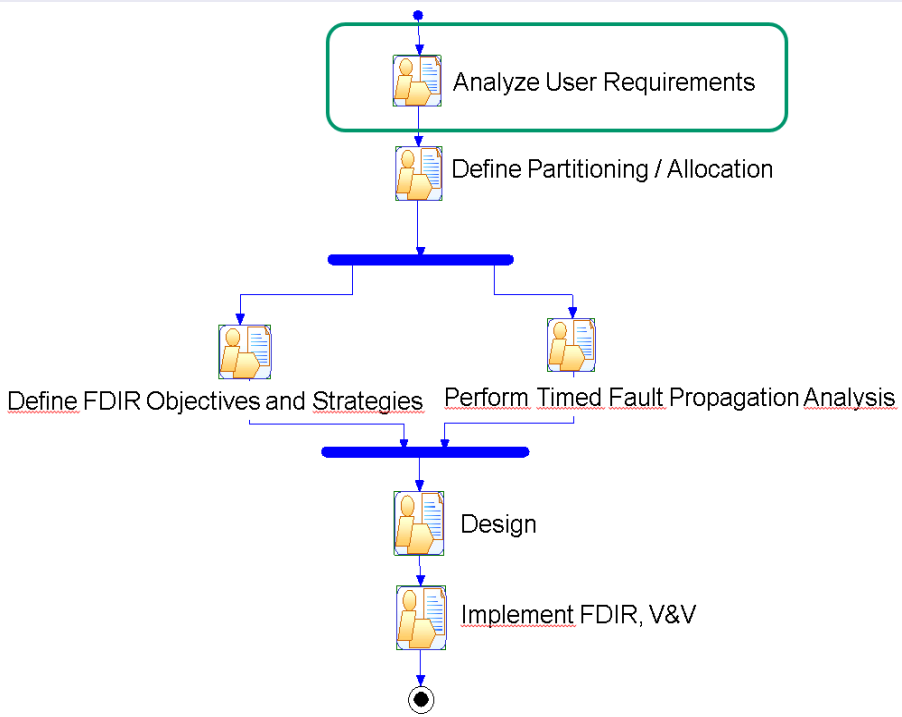


Process Steps

- Analyze User Requirements
- Define Partitioning / Allocation
- Define FDIR Objectives and Strategies
- Perform Timed Fault Propagation Analysis
- Design
- Implement FDIR, V&V

The FAME Process

FAME Process – Flow View

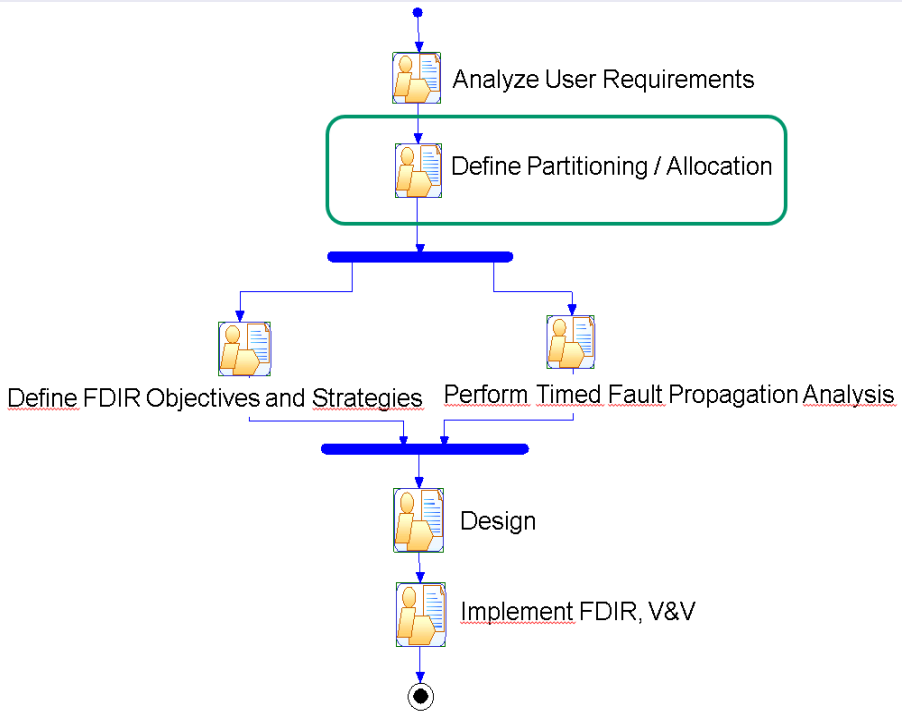


Analyze User Requirements

- Collection and analysis of user requirements
- Classification of failures, identification of FDIR levels, components to be re-used
- Derivation of FDIR objectives and FDIR strategies
- Building of Mission Phase / Spacecraft Operational Mode matrix

The FAME Process

FAME Process – Flow View

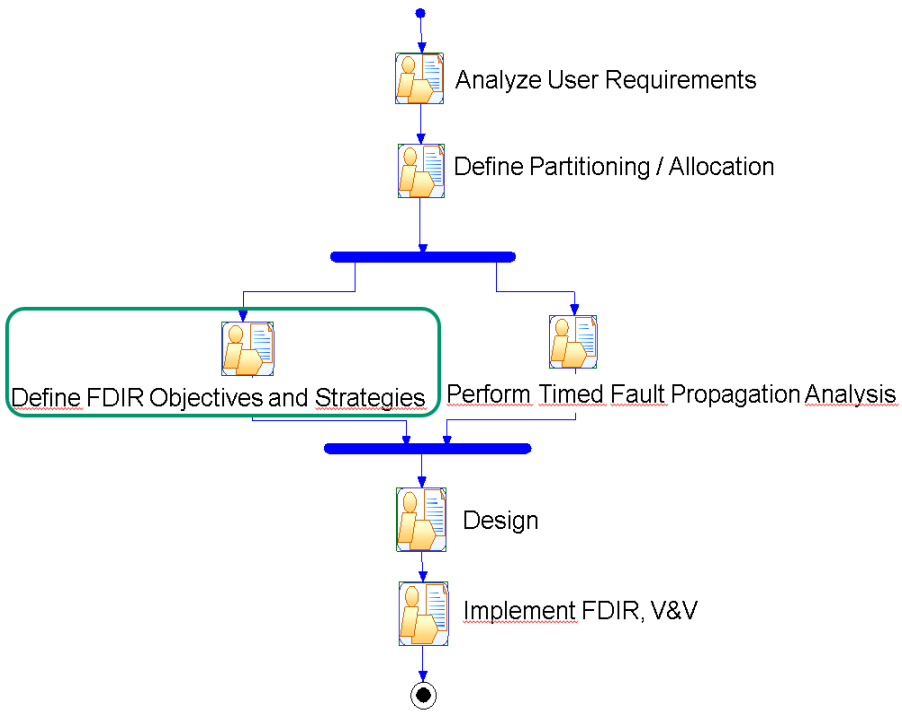


Define Partitioning / Allocation

- Allocation of requirements per Mission Phase / Spacecraft Operational Mode
- Modeling of the FDIR architecture
- Definition of functional decomposition, HW/SW partitioning, redundancy, integration of existing components

The FAME Process

FAME Process – Flow View

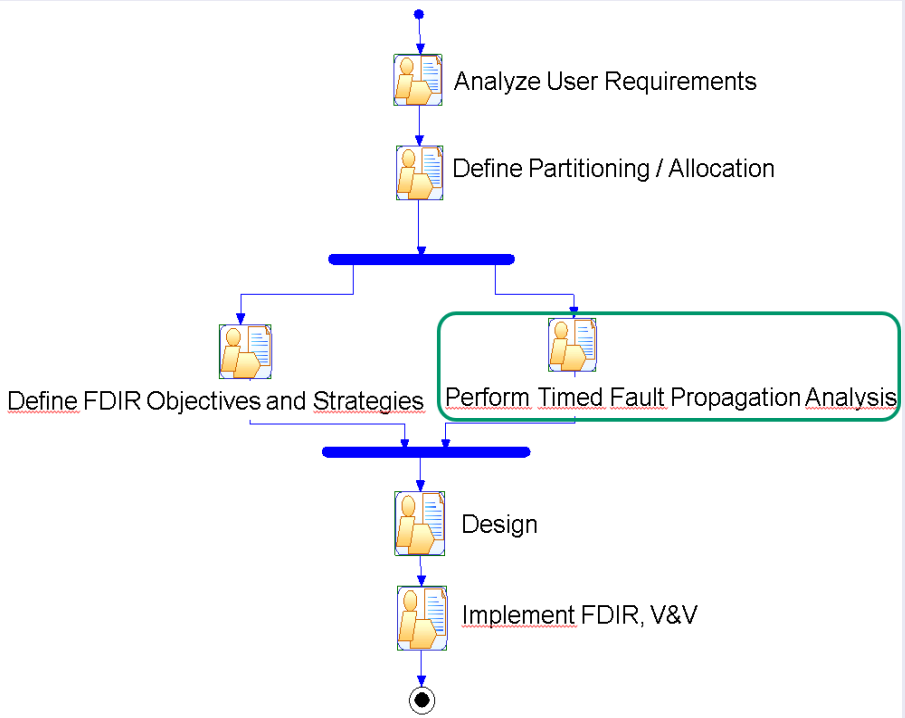


Define FDIR Objectives and Strategies

- Specification of FDIR objectives (required behavior in presence of failures)
- Specification of FDIR strategies (functional steps to be performed)

The FAME Process

FAME Process – Flow View

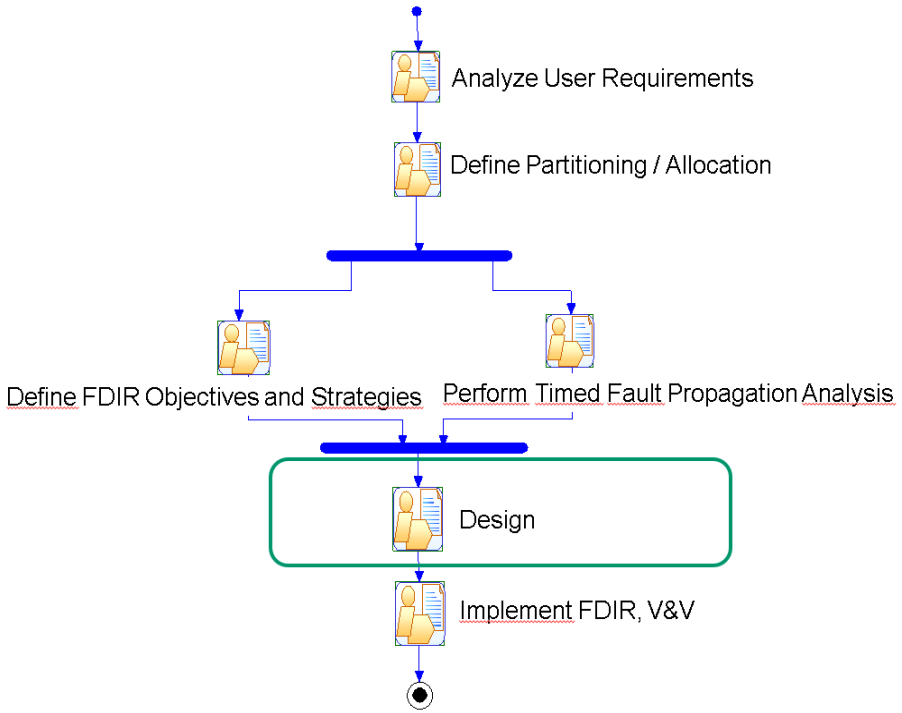


Perform Timed Fault Propagation Analysis

- TFPG modeling / synthesis
- Analyze completeness of the TFPG wrt the system model (behavioral validation)
- Analyze suitability of TFPG as a model for diagnosis (effectiveness validation)

The FAME Process

FAME Process – Flow View

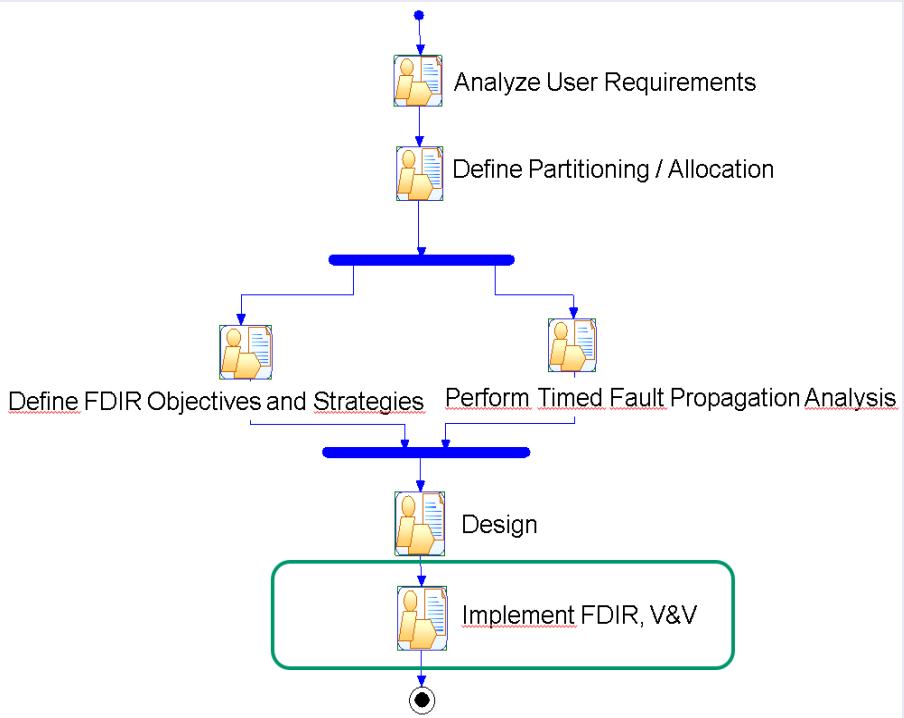


Design

- Definition of the detailed FDIR implementation: FDIR parameters, ranges, reconfiguration actions
- Define detailed SW specification

The FAME Process

FAME Process – Flow View



Implement FDIR, V&V

- Implementation of FDIR in HW/SW
- V&V via testing campaign

Outline

The FAME Environment

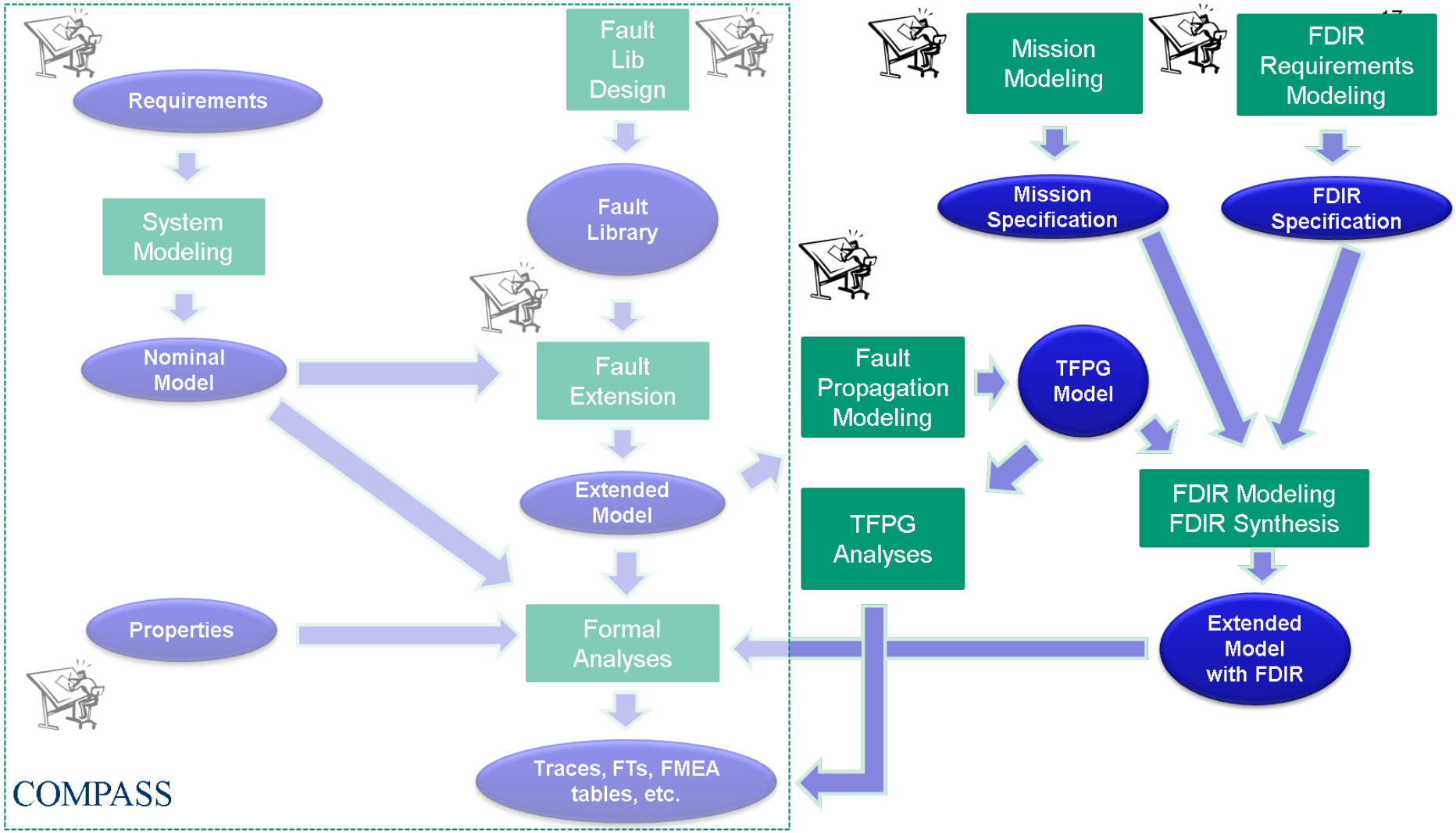
The FAME Environment

- Built on top of the COMPASS toolset
- Implemented in FBK model checking tools

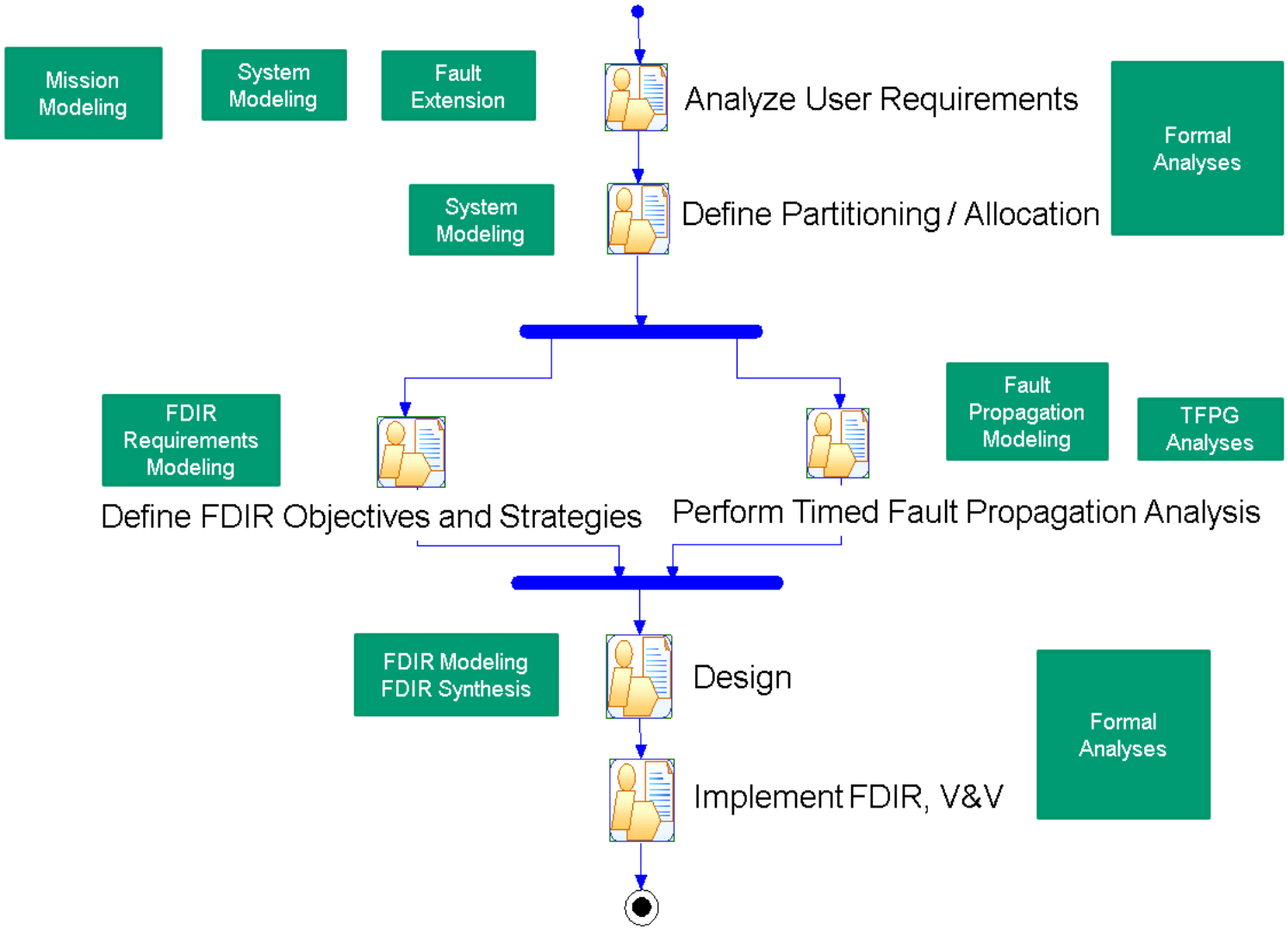
Main functionality

- Definition of mission phases, operational modes, FDIR requirements
- Fault Propagation Analysis: validation and synthesis of TFPGs
- Synthesis of FD and FR

The FAME Environment: Flow



The FAME Environment supports the FAME Process



Licensing

Licensing

FAME tool

- Freely available for ESA member states
- Released under variant of GPL (GNU Public License) – restriction to ESA member states + some backends released under FBK's Additional Components License
- Needs ESA approval for export outside ESA member states

Tool Download

- http://es.fbk.eu/projects/fame

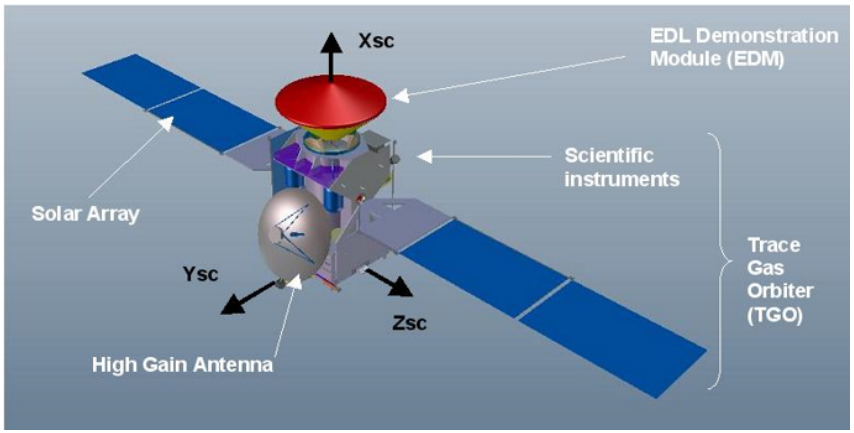
Outline

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
  - Science and data acquisition
  - 2018 : new Rover support

Complex mission = Complex FDIR

- Autonomy
- Mission phase dependent
  - Fail Operational / Fail Safe strategies
  - Hot / Cold redundancies



Case Study: Analyses

Summary of analyses

- Specification of nominal model
- Feared events analysis and FMECA (to identify faliures)
- Specification of error model and fault injections
- Automatic generation of Fault Trees
- TFPG modeling/synthesis
- Mapping of TFPG to system model
- TFPG validation wrt system model
- Specification of mission requirements
- Specification of FDIR requirements (objectives and strategies)
- Synthesis of FD and FR

Case Study: Evaluation Results

Process

- Suitable for industrial usage, coherent with standards and lifecycle, beneficial in early phases
- Formal models prevent misinterpretations
- FDIR specification similar to the one developed in the ExoMars project – FAME produced richer results in terms of fault propagation

Technology

- Good characterization of the system in SLIM
- TFPG formalism adequate to model fault propagation
- Timing information in TFPGs well understood

Environment

- FAME environment adequately supports the FAME process
- Structure of synthesized TFPG identical to the manually designed one

Outline

Conclusions

Summary

- A model-based, dedicated process for FDIR development and V&V
- It enables a consistent and timely FDIR conception and development
- Successful evaluation in an industrial context

Future Work

- Traceability of requirements
- Specification and synthesis of FDIR for decentralized or distributed architectures – requires coordination between different FDIR sub-components
- Hierarchical decomposition of TFPGs into multiple models
- Use contract-based design to address state-space explosion

References

- COMPASS (Bozzano et. al, Computer Journal 2011)
- Industrial evaluation (Bozzano et. al, RESS 2014 - to appear)
- AADL model checker (Bozzano et. al, CAV 2010)
- Our variant of AADL (Bozzano et. al, MEMOCODE 2009)
- FAME tool (Tutorial) (Bittner et. al, IMBSA 2014)
- TFPGs (Karsai, Abdelwahed, Biswas, AIAA-GNC 2003)
- TFPGs Validation (Bozzano et. al, AAAI 2015)
- Formal Framework for FDI (Bozzano et. al, TACAS 2014)