BENEFITS OF MODEL-BASED SYSTEM ENGINEERING FOR FDIR

MBSE 2021

Régis de Ferluc, *Olivier Rigaud, Délia Cellarier, Valentin Beauplet, Gérald Garcia*

Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

Introduction

Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

1/ FDIR IN A NUTSHELL

FDIR = Fault Detection, Isolation, and Recovery

```
While True
        wait(monitoring period)
        if (condition)
                if (parameter != expected value)
                        N++
                        if N > repetitionNumber
                                raise_event(event ID)
```

…hundreds of SW monitorings

```
eventID => TC XXX
```

… a lot of events

… plenty of recovery actions

```
Simple TC
```

```
Action Sequence:
        wait (tempo1)
        sendTc (tc1)
        wait (tempo2)
        sendTC (tc2)
        …
```

```
OnBoard Control Procedure :
        If (…)
                …
        then ()
                …
        else ()
                …
        for (i=0, i<N, i++)
                …
```

/// Standardized mechanisms, implemented in the OBSW as PUS services

- FDIR engineers have to provide the PUS configuration parameters for the mission
  >> incremental and iterative process
- FDIR mechanisms are validated independently of the configuration
- Need also to validate the FDIR design

Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

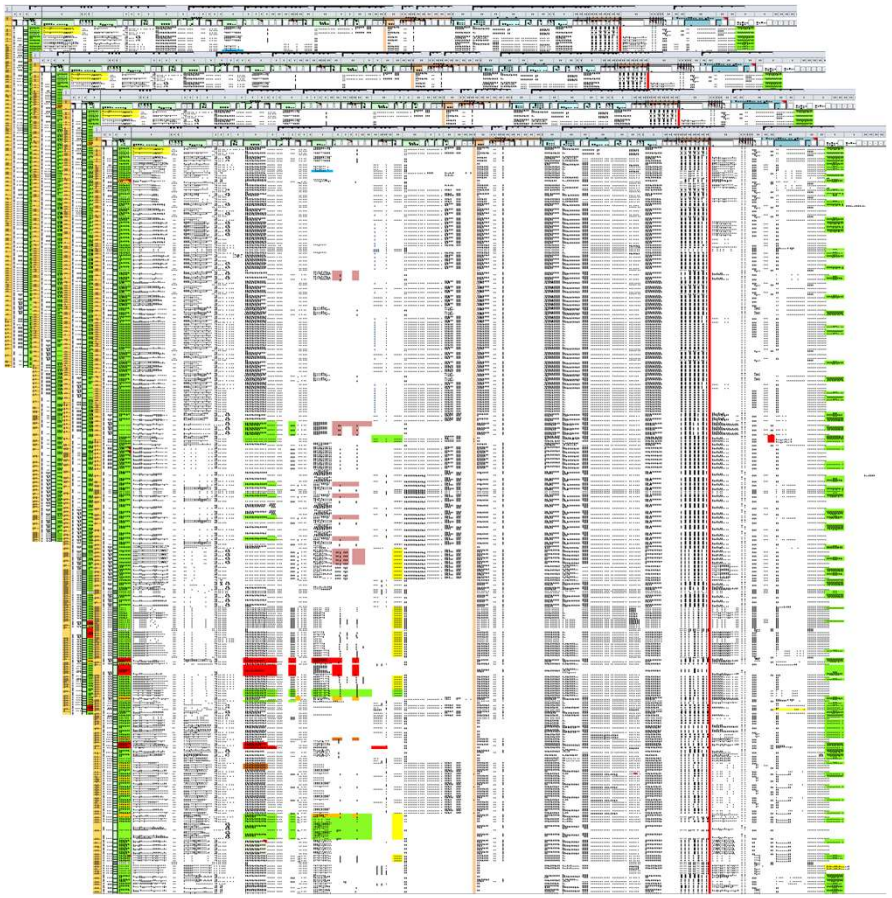
2/ EXCEL AS THE STARTING POINT

/// Before 2010:

- PUS was not used in all programs
- FDIR specification was done in Excel tables
- Manual fastidious error prone process
- Version configuration based on file name
- Each FDIR engineer was using a different Excel Template

/// Before introducing models, need to harmonize Excel formats

- Internal working group to analyse state of the practice
- Definition of a reference Excel Table
- Based on the PUS semantics



Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

3/ INTRODUCING A FDIR DOMAIN SPECIFIC LANGUAGE

/// Early 2010's : MBSE deployment in TAS

- Eclipse based Modelling tools (Melody CCM, Melody Advance, …)
  - Eclipse Modeling Framework (EMF)
  - Accelo (code generation)
- Objective for FDIR
  - Reduce the effort required to configure the on-board software

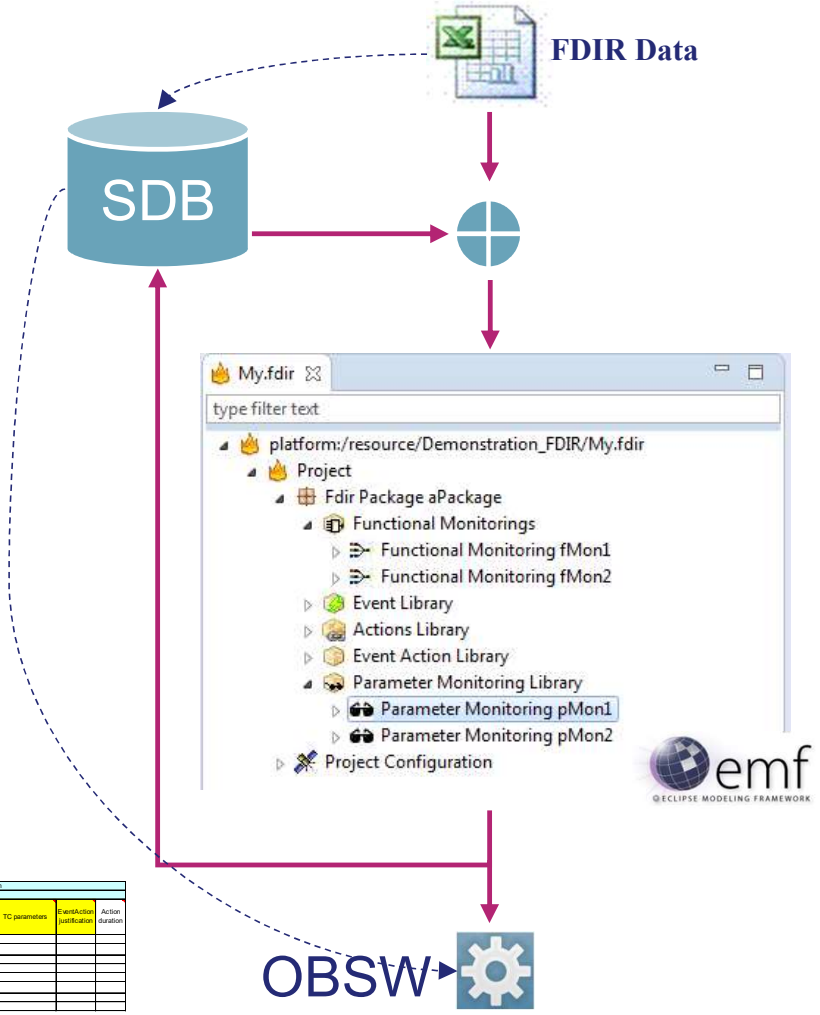
    => Rely on autogeneration of configuration files
  - Ensure the consistency of the FDIR Design with the content of the Satellite Data Base
    - However the database is not on the critical path between FDIR engineers and OBSW team

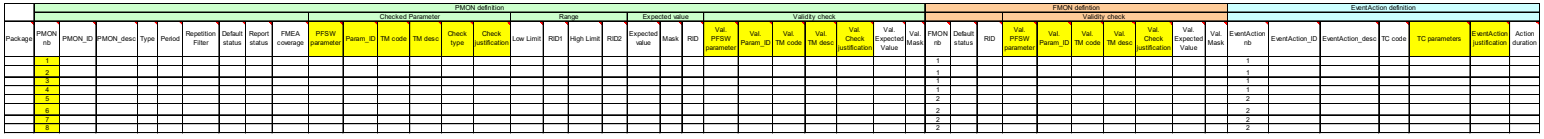
/// Benefits

- Significant reductions of planning observed at each iteration of the FDIR design

/// Lessons learnt (Sentinel 3, Exomars TGO, Iridium Next projects)

- FDIR engineers prefer Excel user interface than Eclipse HMI





Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

4/ USING MODELS TO GENERATE DOCUMENTATION

/// documentation process

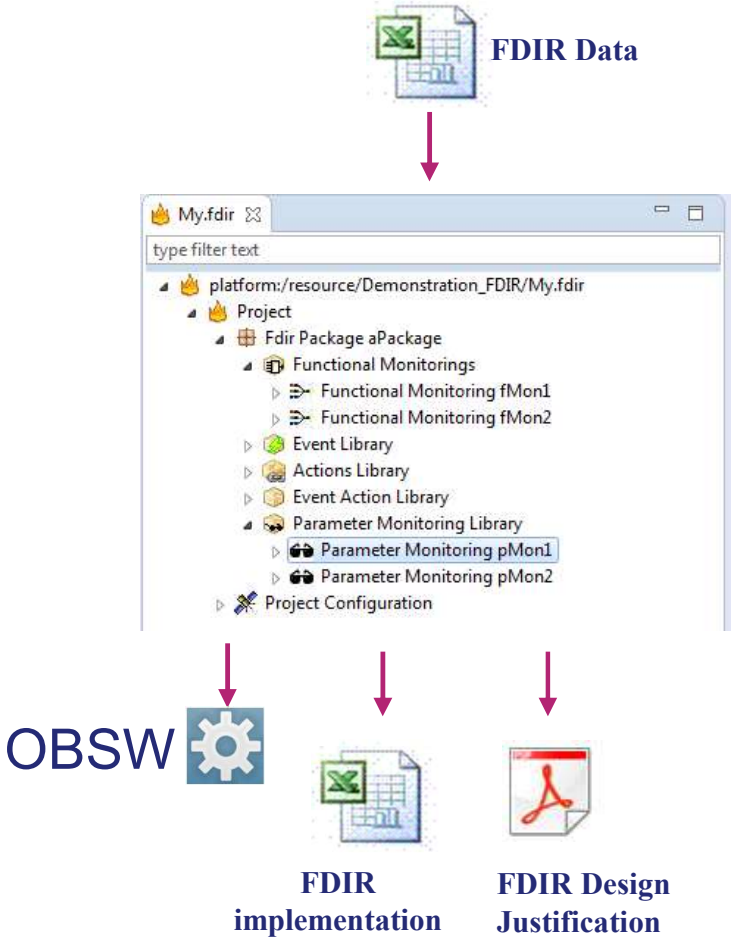
- At each iteration, delivery of
  - All the FDIR data in an Excel table
  - The FDIR implementation and justification report (PDF)
- Pains :
  - Keep data coherent between the Excel table and the manually written documents
  - Perform update of the documents at each iteration of the FDIR Design

/// Benefits of the documentation generation from models

- Save efforts and planning
- Avoid inconsistencies

/// Lessons learnt

- ++ Doc Generation allows to easily insert hyperlinks to facilitate navigation within the document
- + Doc generation techniques allow to mix manually written sections and generated sections.
- - Customers expectations are not always the same regarding deliverables
  - May impact the structure of the document to be generated
- - - Generated documents can be very long (>200 pages) if we insert all the information
  - Need to find the appropriate level of information



Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

5/ ADDITION OF FMECA INFORMATION

/// FDIR aims at covering all the Failure modes identified in the FMECA

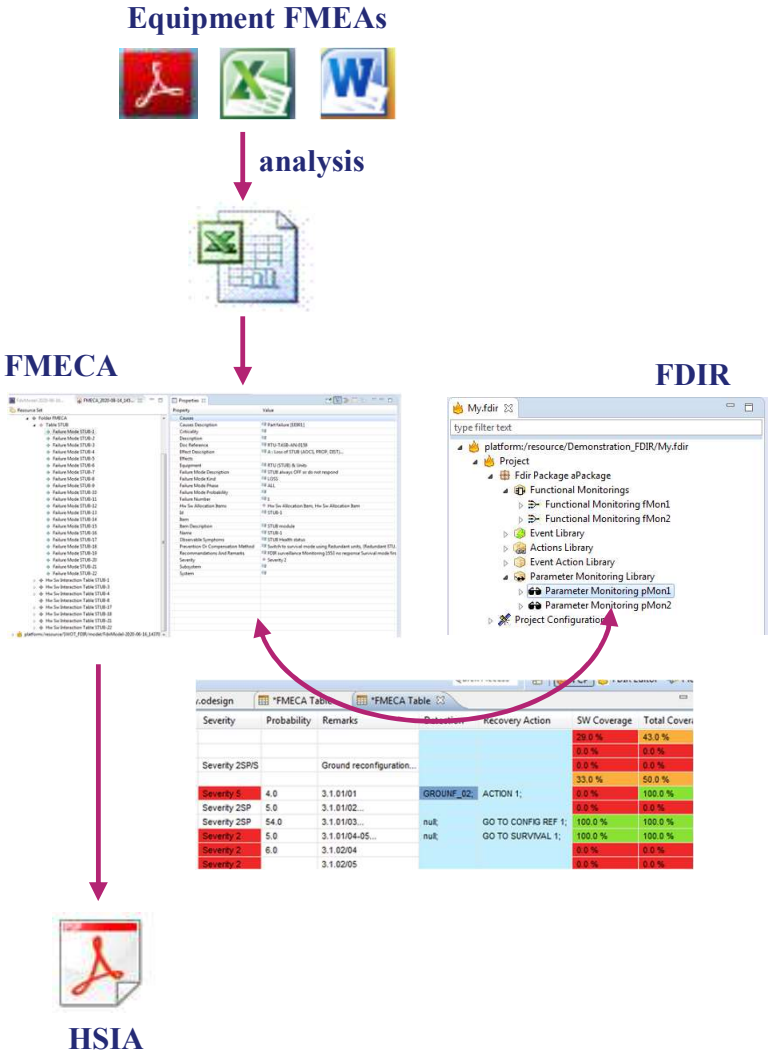
- Each FDIR monitoring is linked to a Failure mode
- Each FDIR recovery refers to the mitigations recommanded for the Failure Mode considering the impact in the system
- Pains :
  - Keep data coherent between FMECA and FDIR
  - Ensure the FDIR covers all the Failure Modes in an appropriate way

/// Benefits of using models

- Consistency checks and coverity analysis between FDIR and FMECA
- Easier impact analysis
- HSIA documentation generation

/// Lessons learnt

- Split the data into different models to reflect each team's perimeter
  - Preserves the capability to work in parallel
- Adopt co-engineering practices to identify data dependencies and set-up efficient workflows

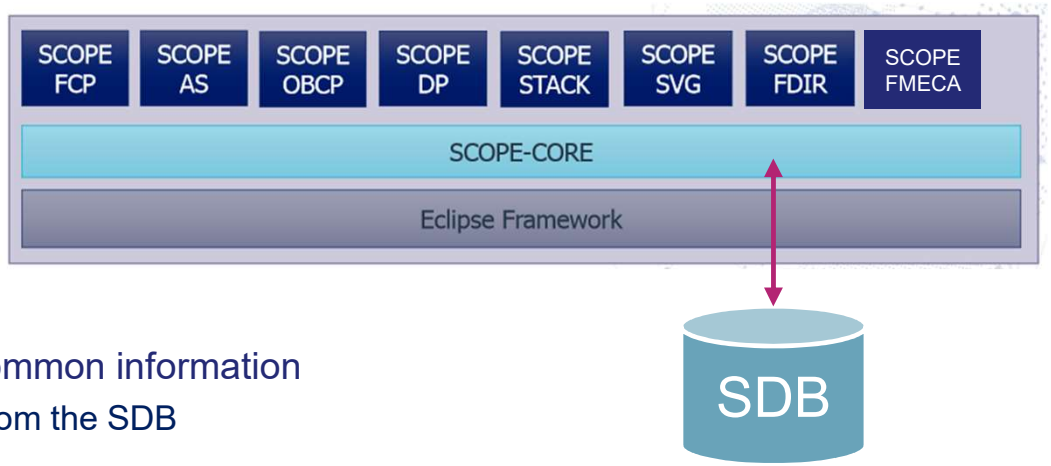


Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

6/ MERGE WITH SCOPE

/// SCOPE is the Preparation Environment in TAS

- FCP, Action Sequences, OBCPs, … Editors
- Based on Eclipse / EMF



/// Benefits of using models

- Each domain has its own specific language
  - Independent evolution of each editor is preserved
- Dependences between models can be created to share common information
  - Typical example is the list of telecommands and telemetries from the SDB
- Code / Doc generation tools are harmonized

/// Lessons learnt

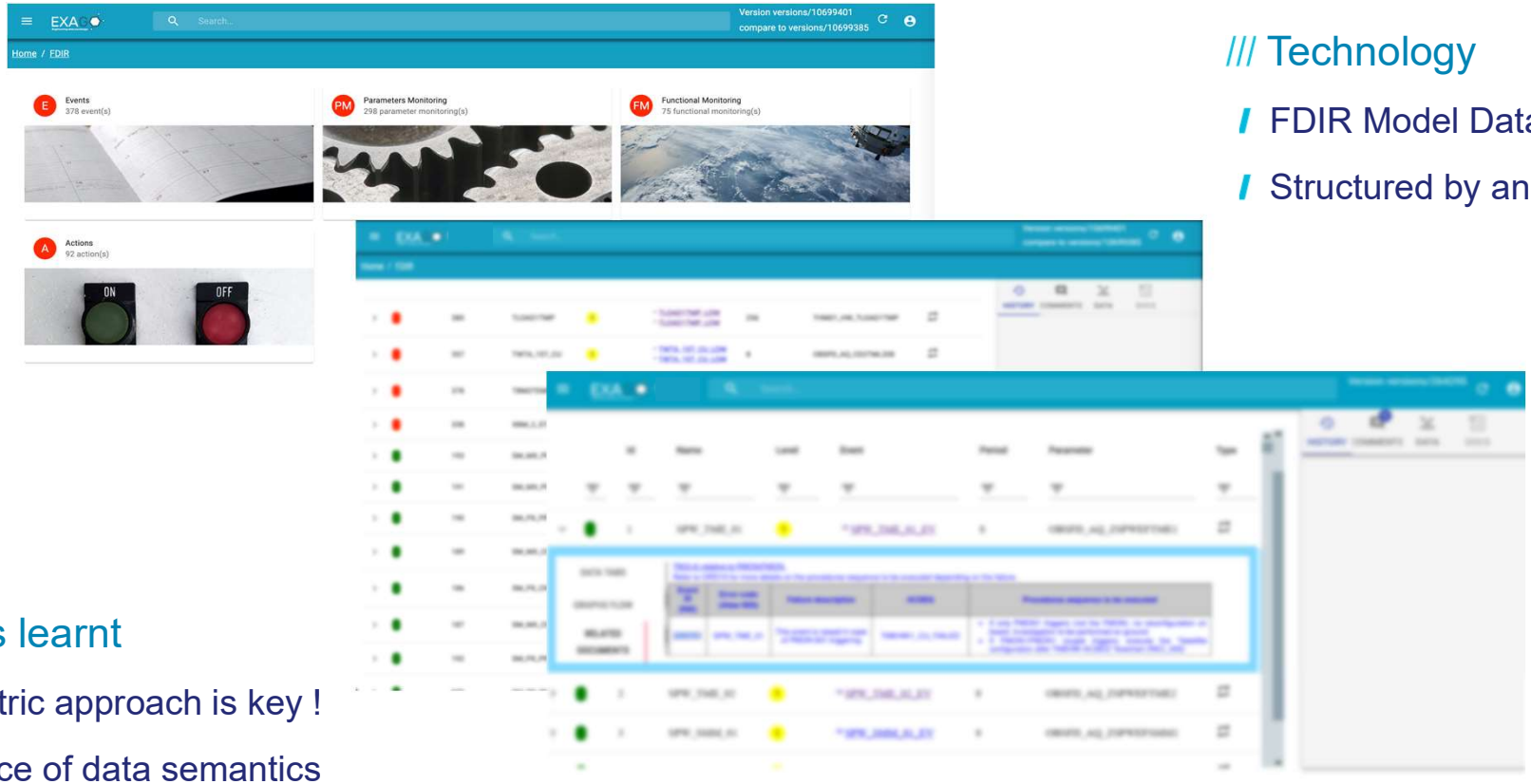
- Better to use a compositional approach rather than a global approach
- Adoption of continuous integration / continuous delivery practices required to shorten the evolution and maintenance iterations.

Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

7/ FOCUSING ON CUSTOMER'S EXPERIENCE

EXAGO* Engineering data exchange

/// FDIR specific UI in EXAGO to allow reviewing FDIR data during projects reviews.



/// Technology

- FDIR Model Data organised as a graph
- Structured by an ontology

/// Lessons learnt

- User centric approach is key !
- Importance of data semantics

*Dedicated presentation : "APPLICATION OF DIGITAL EXCHANGES BETWEEN PROJECT PARTNERS IN THE FRAME OF ENVISION PROJECT"

Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

8/ LEVERAGING MODELS TO PERFORM FDIR SIMULATION

/// Objective is to perform early verification of the design

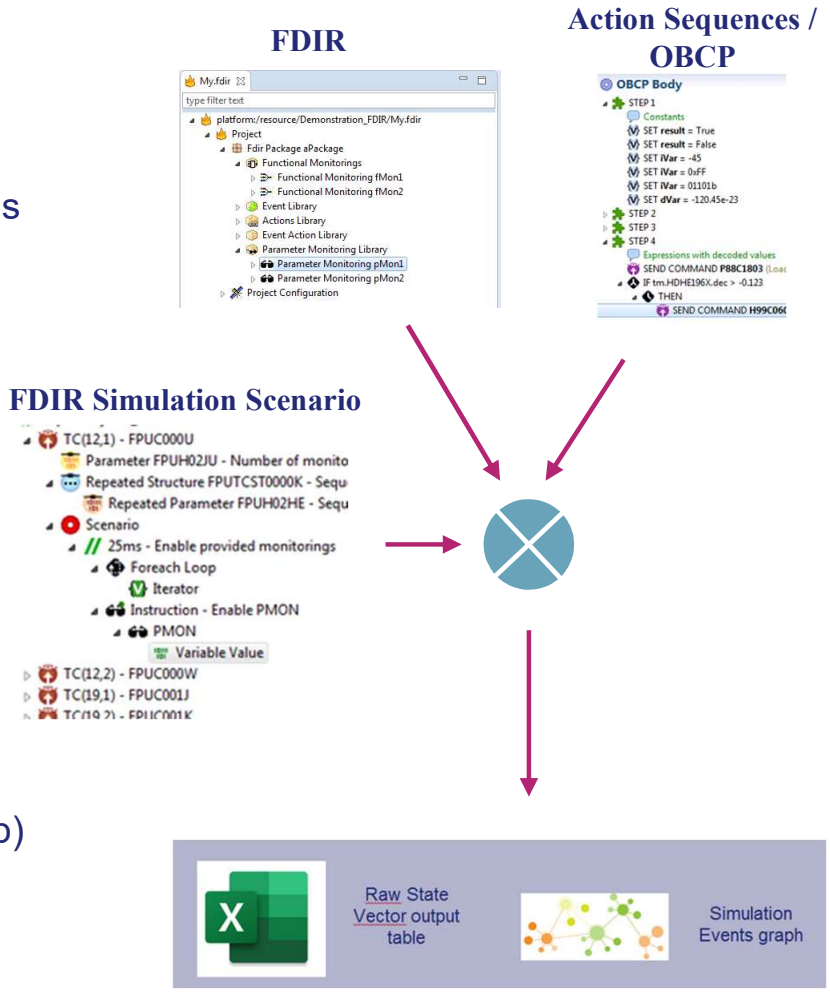
- Study FDIR design dynamic behavior through particular scenarios
- Check that the configuration of FDIR mechanisms satisfies the expectations
- Prepare scenarios that will be tested at FCV level.

/// Benefits of using models

- Models are used to capture the configuration of the Spacecraft
  - Applications/ instruments/equipment/Reconfiguration Module, …
- Models are used to capture scenario in a formal way
  - Change a parameter value, modify a state, trigger an event, send a TC, ….

/// Lessons learnt

- FDIR engineers are « dreaming » of « executing » the FDIR Design
- Simulation is limited until you add behavioural information (to close the loop)
- Real added value to perform early verification



Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

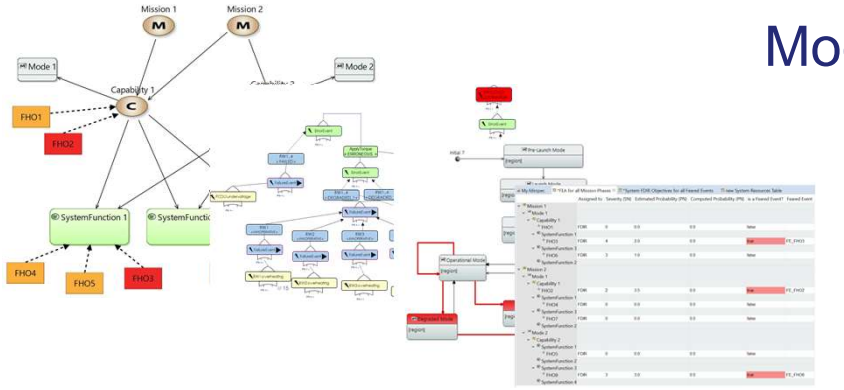
9/ ADDRESSING THE COMPLETE DESIGN PROCESS USING MODELS

Model Based FDIR Process (derived from HB)

- Step 0 •FDIR Requirements
- Step 1 •FDIR Concept definition •FDIR early verification
- Step 2 •FDIR Architecture
- Step 3 •FDIR Detailed Design •FDIR early validation
- Step 4 •FDIR implementation and verification
- Step 5 •FDIR validation
- Step 6 •FDIR in operations preparation

SCOPE FDIR

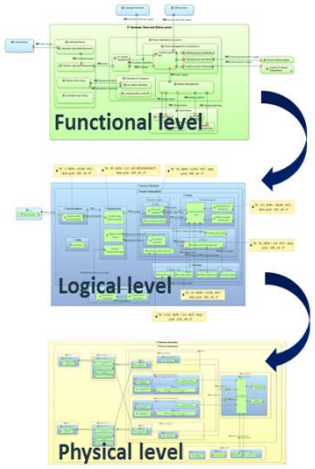
Model Based FDIR Design Tool



Capella

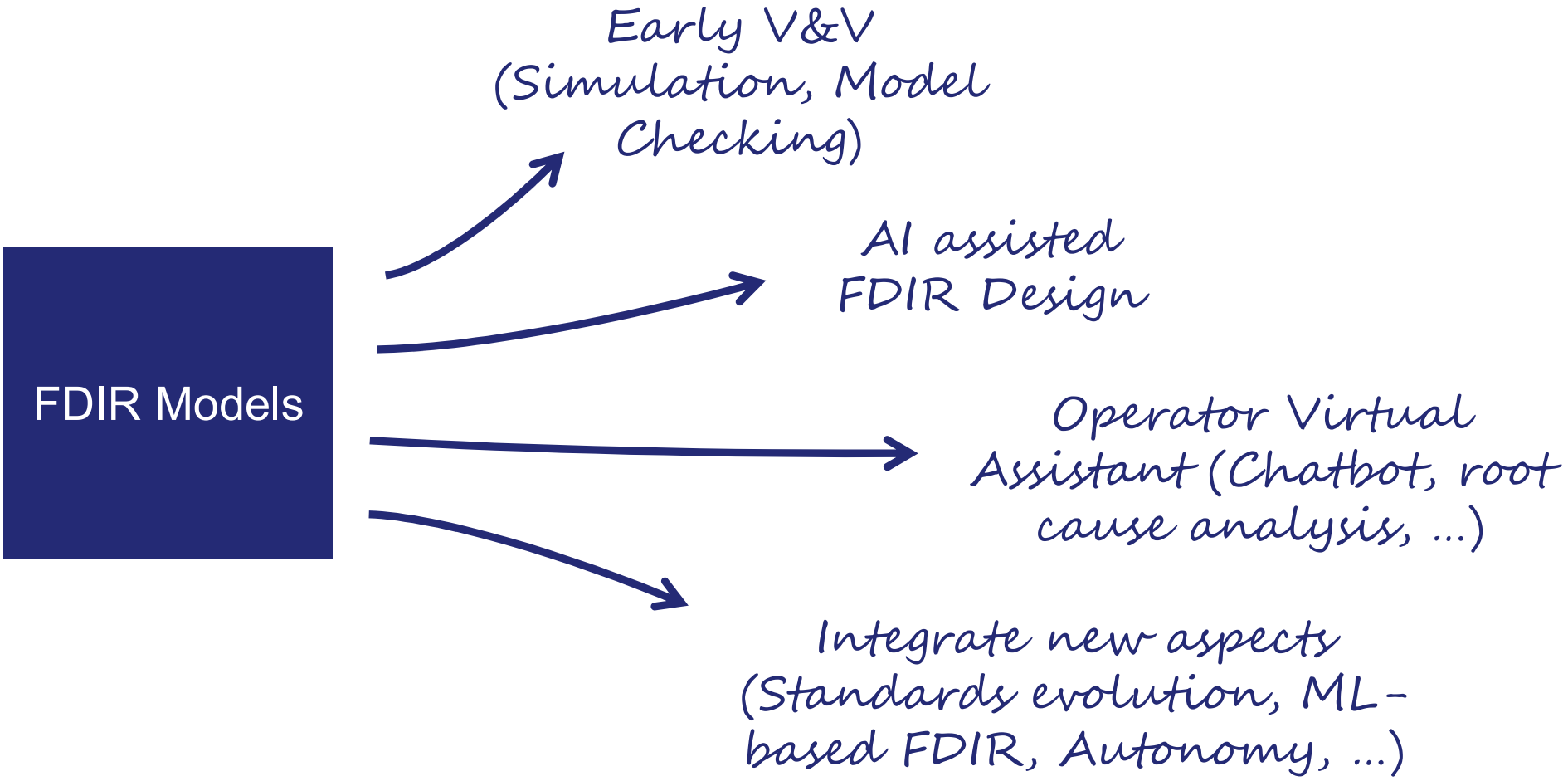
FEA VP
FDIR Strategy VP
Error Model VP
FMEA/FMECA VP
FTA VP
FDIR Design VP

Capella



Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

10/ FUTURE WORK



Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009

11/ CONCLUSION

/// Introducing MBSE for FDIR design has been a long story in TAS

- Step-by-step approach, with short term and realistic objectives
- Co-engineering approach to understand domain specific needs and implement user-friendly tools

/// Return on Investment is demonstrated

- Tool development activity internally funded after ROI analysis
- Tool evolutions requested by users based on their field experience

/// Models are not solving all problems

- Underlying process is even more important => MBSE forces to consolidate the process first !
- Data semantics is key => MBSE forces you to work on data semantics
- MBSE is a real cultural change, requires time and efforts (training, support, …)

/// See you in 10 years to see where we are !

Date : 15/09/2021
Ref : Non référencé
Ref Modele : 83230347-DOC-TAS-FR-009