Model-Based FDIR Design

Délia Cellarier[1], Régis De Ferluc[1], Carl Todd[2], David Perillo[2]

(1) *Thales Alenia Space France (Thales Alenia Space-F), France,*
Email: delia.cellarier@thalesaleniaspace.com, regis.deferluc@thalesaleniaspace.com
(2) *European Space Agency (ESA), ESTEC Noordwijk, The Netherlands,*
Email: Carl.Todd@esa.int, David.Perillo@esa.int

ABSTRACT – *Designing Fault Detection, Isolation and Recovery (FDIR) of space systems is a tight task spanning all along the development lifecycle and covering all the elements of the system. This paper presents the work performed by Thales Alenia Space in the de-risk activity of the GSTP Model-Based FDIR Design, which allowed to define and prototype an end-to-end MBSE solution based on Capella for the design of the FDIR of a spacecraft.*

KEYWORDS – FDIR, MBSE, Capella

1 INTRODUCTION

Today, satellite or spacecraft FDIR design is a time-consuming and error prone paper-based workflow, which does not help mastering the growing complexity of the space systems, and which mostly prevents early validation and verification of the design. Adequacy of the FDIR design is often assessed very late in the process (integration and test phase), sometimes even after the launch of the spacecraft (FDIR parameter tuning). FDIR engineers face everyday challenges like ensuring the alignment of the FDIR Design with regard to the system design, the reliability requirements and the supplier's information, or like optimizing the FDIR concepts (Detection, Isolation, Recovery of failures) with regard to mission objectives and operational concepts.

This activity aims at de-risking the extensive use of models to support the design of an FDIR system. Expected benefits includes the emergence of the so-called “digital continuity” which promises to significantly reduce the Non-Quality Costs, the reduction of development costs (zero-doc, no duplication of information) and planning (reduced time-to-market, agility, load-balancing of the effort all along the lifecycle) and the capability to cope with more and more complex systems (increased autonomy, reduced impact of failures on the mission, …).

The Model-Based FDIR Design process is defined as an extension of an assumed Model Based System Design Process. In the frame of this study the Arcadia methodology is considered and supported by the open-source and widely deployed Capella toolset.

In the frame of this activity the Modelling objectives are intended to later support early validation and verification of the FDIR, thanks to simulation and model-checking. It is clear that to achieve those objectives, early verification and validation, the modelling guidelines will need to be very precise in order to ensure a certain level of formalism in the models, as they will be used for generating automatically other artefacts in a correct by construction approach.

Although FDIR analysis is defined in the ECSS standards, the Design process has only been discussed recently in the scope of a working group, resulting with a non-normative handbook [1], reflecting the commonalities and variabilities of today industrial practices. The developed Model-Based FDIR Design Process is mapped to the process described in the SAVOIR FDIR Handbook and tries to adopt the same definitions and concepts for the sake of clarity.

2 TECHNICAL OBJECTIVES

The technical objectives of the full activity are i) to develop a model-based FDIR design tool allowing to support the FDIR design workflow, and ii) to build specific assets for performing FDIR early validation and verification analysis through ad-hoc simulation or model checking.

The de-risk activity (described in this paper) focused on the end-to-end Model Based solution to assist FDIR engineers in the various steps of the design of the FDIR of a spacecraft, applying co-engineering practices with System/Avionics engineers. A follow-on activity will allow to work on the validation and verification assets, leveraging on the results of the de-risk activity. In parallel, further steps will consist in the complete development of the toolset, in order to prepare operational deployment. This proposed approach is represented in Figure 2-1.

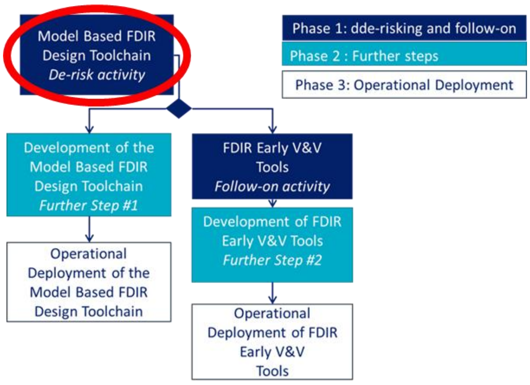


Figure 2-1: Proposed approach to reach the operational deployment of i) the Model Based FDIR Design tool chain and ii) the FDIR Early Validation Tools

The first objective of the de-risk activity was to establish a FDIR process leveraging on Model Based Techniques and covering from Step 0 (Requirements) to Step 3 (FDIR Detailed Design) as described in the SAVOIR FDIR Handbook [1]. Steps 4 (FDIR Implementation and Verification) to 6 (FDIR in Operations Preparation) in the handbook were not considered as these are very dependent of the industrial means such as the Spacecraft Data Base, etc.

The second objective was to prototype the Model Based FDIR tool as a set of Capella viewpoints. Specific focus was given to the traceability between models and between functional, logical and physical levels.

The third objective was to use the concept of Data Hub (or Model Based Data Hub) to exchange (import or export) data (exchange items) between the different actors of the process. Although design and development of such a Data Hub solution is out of scope of the activity, it remains an essential concept to achieve tool harmonisation around a common (semantic) data model. This is a strong pre-requisite for deploying co-engineering practices.

The fourth objective was to prepare a representative use-case to assess the tooled methodology during the de-risk phase and during the follow-on phase.

The following figure illustrates the approach followed during the de-risk activity, giving an overview of the architecture of the prototype, and highlighting the perimeter considered by each technical step:

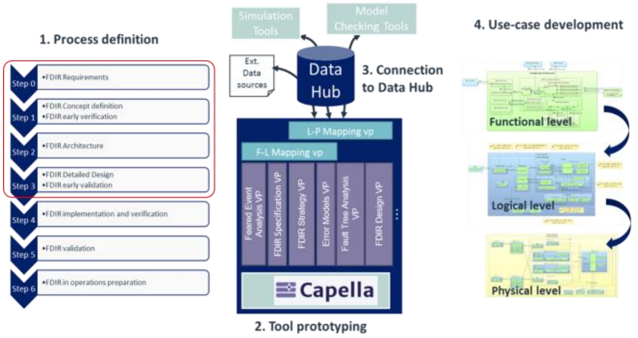


Figure 2-2: Overview of the process, tool-chain architecture and use-case

3 MODEL-BASED FDIR DESIGN PROCESS

The Model-Based FDIR Design process assumes a model-based process relying on Capella for the design of space systems, which was described in [2]. The FDIR process must consider all the system models from the early phases to the development phases. FDIR activities and analysis are thus spread over the design process. The following figure depicts where the FDIR related activities take place in the big picture:

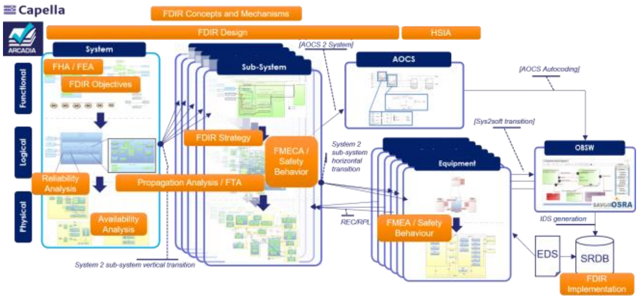


Figure 3-1: Overview of the Model-Based FDIR Design Process

For each applicable step of the FDIR process described in the SAVOIR FDIR Handbook [1], the study has analyzed in detail the process objectives, and has derived the modelling objectives. This was the starting point of the definition of the modelling activities that the Model-Based FDIR Design Toolset needs to support.

A specific analysis has been done for the AOCS/GNC perimeter. This discipline has to be considered specifically as it mainly relies on the Matlab/Simulink modelling tool. Although this aspect is out of scope of this study, a compatibility with current practices and other studies outcomes has been targeted.

EDS was also taken into account : [2] provides an overview of where and when in the System Engineering process Electronic Data Sheets should be used. For what concerns FDIR, extension of EDS can be envisaged to help modelling FMEA.

In particular, the work performed in SAVOIR EDS has started to specify Domain models to address physical level aspects. However, FDIR was not considered in the scope of the SAVOIR EDS activity.

4 SPECIFICATION OF CAPELLA FDIR VIEWPOINT

The second step of this activity consisted in the specification of the Capella FDIR Design Viewpoint allowing to implement and support the Model-Based FDIR Design process elaborated in the frame of this GSTP.

The Capella FDIR Design viewpoint was thought as a set of Eclipse plugins that can be installed on a specific version of the Capella platform and used to perform the different steps composing the Model-Based FDIR Design process.

The Capella FDIR viewpoint is specified as an extension of the Capella toolset and is composed of :

- A data model, which is defined as an extension of the Capella data model itself. This data model defines the language concepts that are needed to build a model representing the FDIR Design. This Data Model is not specified in this document, as it is implementation dependent.

- A set of validation rules that are implemented to ensure that the model defined by the user is coherent and complete. This section is empty as it depends on the Ontology. It is considered out of scope of the de-risking activity.

- A set of Graphical User Interfaces that are either Tables or diagrams. Diagrams can be standalone diagrams or additional layers on existing Capella diagrams.

Considering the Modelling Guidelines defined in the study [2], the FDIR Design viewpoint data model shall be able to take into account several Capella models.

A traceability between Viewpoint specification requirements and activity high level requirements has been elaborated.

The Model Based FDIR Design Process mapping with SAVOIR FDIR Handbook [1] and COMPASS [3] has been established in a dedicated document. Regarding the traceability with [1], an analysis has been provided for each relevant step of the process. Some recommendations have been made to update parts of the SAVOIR FDIR Handbook.

5 CAPELLA VIEWPOINT DEVELOPMENT

A FDIR Design toolset has been derived from the FDIR Capella Viewpoint Specification described in the previous section. This toolset is actually composed of a set of Capella Viewpoints and other standalone EMF-based tools. The architecture overview of the toolset is shown on the following figure:

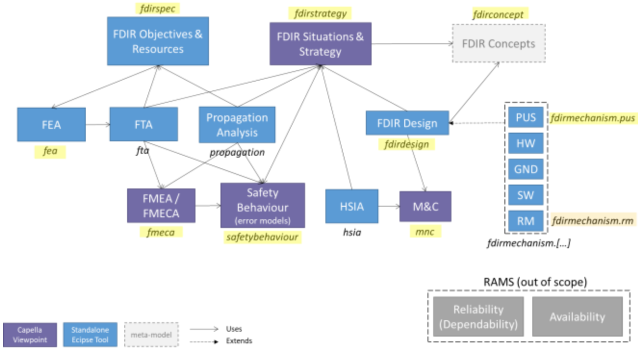


Figure 5-1: FDIR Design Toolset Architecture

This architecture contains different kinds of elements:

- in blue, Viewpoints allowing to create models which are not Capella models;
- in purple, Capella Viewpoints, which allow to extend Capella models;
- in light grey, plugins which do not define a specific model, but which are only used by other plugins. It is also the case for a “Common Kernel” plugin which is not represented here.
- In grey, the RAMS viewpoints, which are out of the scope of this activity.

The names of the plugins are highlighted in yellow if they have been implemented in the prototyped FDIR Design toolset. The detail of what has been implemented is documented in a coverage and traceability matrix of the requirements specified in the Capella FDIR Viewpoint specification.

The Viewpoints include specific graphical representation means (i.e. diagrams or tables) which support the modelling activities of the FDIR process. The following figure gives an example of Functional Error Model diagram that can be performed thanks to the Safety Behaviour Viewpoint:

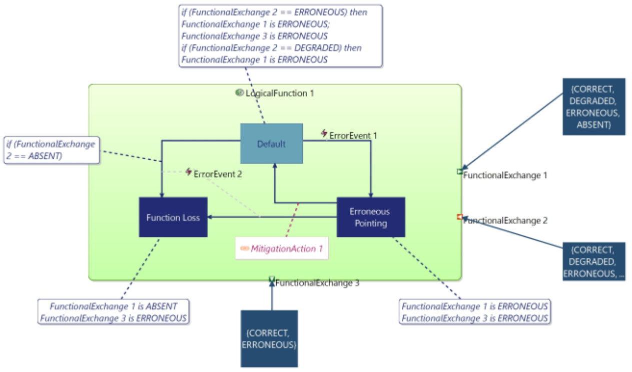

if (FunctionalExchange 2 == ERRONEOUS) then
FunctionalExchange 1 is ERRONEOUS;
FunctionalExchange 3 is ERRONEOUS
if (FunctionalExchange 2 == DEGRADED) then
FunctionalExchange 1 is ERRONEOUS
LogicalFunction 1
{CORRECT, DEGRADED, ERRONEOUS, ABSENT}
if (FunctionalExchange 2 == ABSENT)
Default
ErrorEvent 1
ErrorEvent 2
FunctionalExchange 1
Function Loss
Erroneous Pointing
FunctionalExchange 2
MitigationAction 1
{CORRECT, DEGRADED, ERRONEOUS, ...
FunctionalExchange 3
FunctionalExchange 1 is ABSENT
FunctionalExchange 3 is ERRONEOUS
FunctionalExchange 1 is ERRONEOUS
FunctionalExchange 3 is ERRONEOUS
{CORRECT, ERRONEOUS}

Figure 5-2: Example of Functional Error Model diagram (Safety Behaviour Viewpoint)

6 CONNECTION TO THE DATA HUB

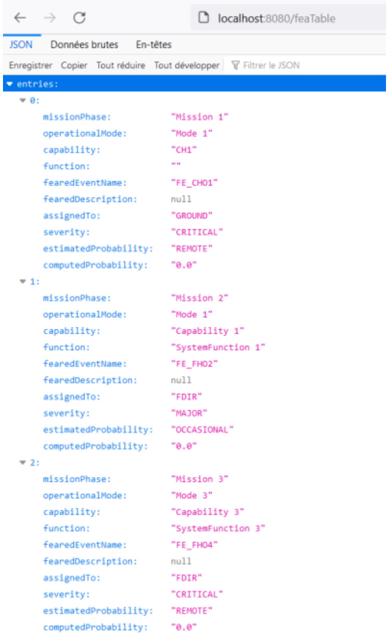
One of the major roadblock of model based practices in industry relies on the fact that existing tools are not always inter-operable. The Data Hub initiative has the objective of ensuring the possibility to exchange data across various actors, independently of the tools they use.

By implementing the Model Based FDIR design toolset as an extension of the Capella open-source software, it is of main importance to provide a mechanism allowing external stakeholders to access the FDIR data captured in the model independently of the Capella toolset.

As this aspect is going to be tackled in a dedicated study, only a proof of concept has been developed in the frame of this activity.

The demonstration covers the export of some FDIR relevant information from the Capella models, and the retrieval of this information in a Capella agnostic environment (typically, a web browser).

This demonstrates that, thanks to the Data Hub concept, the FDIR related data authored thanks to the Model Based FDIR design toolset can be accessed and used by any actor within the project (System and RAMS engineers, customer, operation engineers, ..).



```
▾ entries:
  ▾ 0:
      missionPhase:           "Mission 1"
      operationalMode:        "Mode 1"
      capability:             "CH1"
      function:               ""
      fearedEventName:        "FE_CH01"
      fearedDescription:      null
      assignedTo:             "GROUND"
      severity:               "CRITICAL"
      estimatedProbability:   "REMOTE"
      computedProbability:    "0.0"
  ▾ 1:
      missionPhase:           "Mission 2"
      operationalMode:        "Mode 1"
      capability:             "Capability 1"
      function:               "SystemFunction 1"
      fearedEventName:        "FE_FH02"
      fearedDescription:      null
      assignedTo:             "FDIR"
      severity:               "MAJOR"
      estimatedProbability:   "OCCASIONAL"
      computedProbability:    "0.0"
  ▾ 2:
      missionPhase:           "Mission 3"
      operationalMode:        "Mode 3"
      capability:             "Capability 3"
      function:               "SystemFunction 3"
      fearedEventName:        "FE_FH04"
      fearedDescription:      null
      assignedTo:             "FDIR"
      severity:               "CRITICAL"
      estimatedProbability:   "REMOTE"
      computedProbability:    "0.0"
```

Figure 6-1: FDIR Feared Event Analysis data retrieved from a web-browser in JSON format, independently of Capella or Model Based FDIR Design Toolset

7 USE-CASE

The reference for the use-case modelling is the PLATO spacecraft (PLAnetary Transits and Oscillations of stars). It is a medium-class astronomical science mission belonging to ESAs Cosmic Vision Programme, which is dedicated to the detection and characterization of terrestrial exoplanets.

The goal of the use-case was to assess the specified model-based FDIR Design process and the prototyped FDIR Design toolset. Documents from the PLATO project were used to analyze the mission and spacecraft architecture, as well as the PLATO FDIR Concept and Implementation. Some relevant failures covered by the PLATO FDIR (one for each detection level) were selected for the modelling activities.

Indeed, the use-case does not cover the whole spacecraft and its complete FDIR, but only a subset which is relevant to demonstrate the model-based FDIR process. Moreover, as the FDIR of PLATO was still being consolidated during the use-case implementation, the use-case may not reflect the final PLATO FDIR design.

To simplify the use-case, different models for the system, sub-systems and equipment (as envisaged by the modelling guidelines defined in this activity) were not produced. Instead, all the PLATO modelling was merged in a single model.

This PLATO model, contained in a Capella Project, also includes information coming from different Capella Viewpoints: Safety Behaviour, M&C and FDIR Strategy. In addition to this model, the use-case is composed of three other projects for Feared Event Analysis, FDIR Specification and FDIR Design models. The architecture of the use-case and the references between the models are depicted on the figure below:

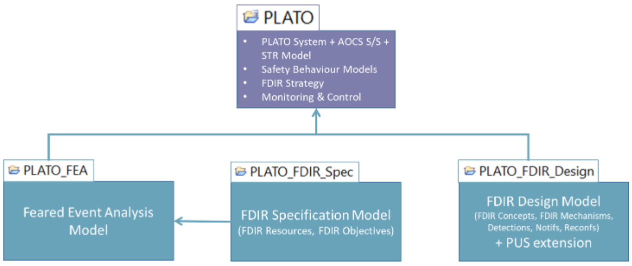


Figure 7-1: Use-Case Architecture

8 CONCLUSION

The Model Based FDIR design activity has allowed to de-risk and show the feasibility of developing a toolset which allows to implement the FDIR design of space systems, assuming a system models exist at the right level (system, sub-system, and equipment level).

A prototype toolset has been demonstrated taking into account a real on-going project, PLATO, and the activity has allowed the consolidation of the necessary features of this tool. Although it is not yet ready for industrial adoption, the study has more than exceeded the de-risking objectives.

This opens the door to follow-on activities : FDIR data formalised in well-structured models extending system models is a very interesting input for simulation and analysis activities. This can be done independently of the Capella environment thanks to the Data Hub concept which allows to retrieve the required information in agnostically of the Model Based FDIR Design Toolset.

9 REFERENCES

[1] SAVOIR, "HB-003: FDIR Handbook," Issue 2.0, 11-2019.

[2] GSTP Model-Based FDIR Design, "D0. Capella Modelling Guidelines for Space Domain," Issue 1.2.

[3] "COMPASS," [Online]. Available: http://www.compass-toolset.org/.