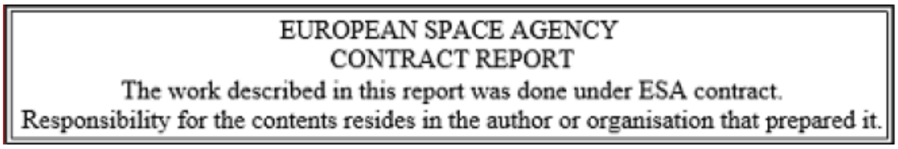
GSTP model-based FDIR Design

-

ESR. Executive Summary Report



EUROPEAN SPACE AGENCY
CONTRACT REPORT
The work described in this report was done under ESA contract.
Responsibility for the contents resides in the author or organisation that prepared it.

Written by	***Responsibility*** + handwritten signature if no electronic workflow tool
Regis De ferluc	SW R&D Project Manager
Délia Cellarier	On-board Software and Modelling R&D Engineer
Verified by	
Olivier Rigaud	Data Handling and FDIR Engineer
Approved by	

Approval evidence is kept within the document management system.

1. INTRODUCTION

This document is the executive summary report of the GSTP Model Based FDIR Design de-risk activity.

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 every day challenges like ensuring the alignment of the FDIR Design with regard to the system design, the reliability requirements, or the suppliers 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, supported by the open-source and widely deployed Capella toolset.

In the frame of this activity, the Modelling objectives are to later support early validation and verification of the FDIR, thanks to simulation and model-checking. It is clear that to achieve those objectives, modelling guidelines will be very precise in order to ensure a certain level of formalism in the models.

Although FDIR analysis are defined in ECSS standard, the Design process has only been discussed recently in the scope of a working group, resulting with a non-normative handbook, reflecting the commonalities and variabilities of today industrial practices. The Model-Based FDIR Design Process takes into account the process breakdown as proposed by this handbook, and tries to adopt the same definition of terms and concepts for sake of clarity.

This report provides a summary of the activities conducted during this project.

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 (the current activity) focuses 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. Once this result is achieved, 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, so-as to prepare operational deployment. This Proposed approach is represented in the following figure:

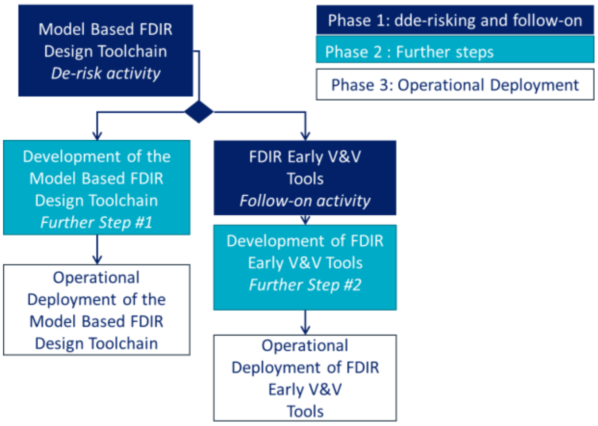

Model Based FDIR Design Toolchain *De-risk activity*
Phase 1: dde-risking and follow-on
Phase 2 : Further steps
Phase 3: Operational Deployment
Development of the Model Based FDIR Design Toolchain *Further Step #1*
FDIR Early V&V Tools *Follow-on activity*
Development of FDIR Early V&V Tools *Further Step #2*
Operational Deployment of the Model Based FDIR Design Toolchain
Operational Deployment of FDIR Early V&V Tools

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 in Thales Alenia Space programs.

The first objective is to establish a FDIR process leveraging on Model Based Techniques. Even though the de-risk activity only implements the early definition of the system FDIR the full life cycle will be defined as part of this objective.

The second objective is to develop the Model Based FDIR tool as a set of Capella viewpoints, potentially taking benefits of the Electronic Data Sheet. Specific focus will be given to the features allowing to map functional engineering level on logical engineering level, and to map logical engineering level on physical level.

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

If the de-risk activity of Phase 1 is successful, a further step (Further step #1) will consist of the industrialisation of the prototype, including the production of the data pack at the expected level (design documents, test suite, test reports, and user manual, maintenance plan and exploitation plan).

At the end of de-risk and Further Step #1, it will be possible to use the Model Based FDIR Design tool on operational projects.

The proposed approach is to start with the process definition (step 1), to build a prototype in an incremental manner (step 2), to demonstrate the connection to the Data Hub (step 3), and to evaluate each aspect of the prototype by applying the methodology and the tool to a representative use-case (step 4). The following figure illustrates the architecture of the prototype, and highlights the perimeter considered by each technical step:

[1] Further Step #1 is not part of this activity. This activity only consists of the de-risk part.

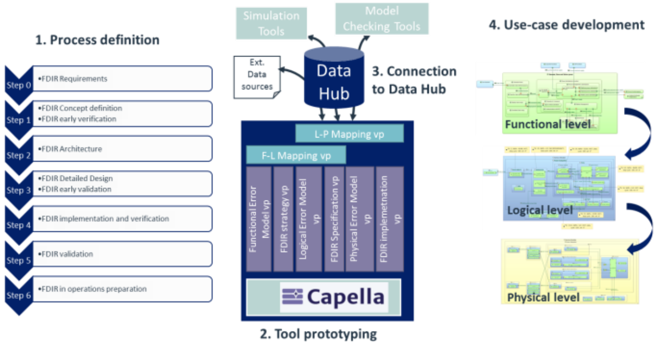


Figure 2-2: overview of the Tool-chain architecture, process and use-case

3. MODEL-BASED FDIR PROCESS

The model based FDIR process has to consider all the system models from the early phases to the development phases. FDIR activities and analysis are thus spread over the system design process described in [D0]. The following figure depicts where the FDIR related activities take place in the big picture:

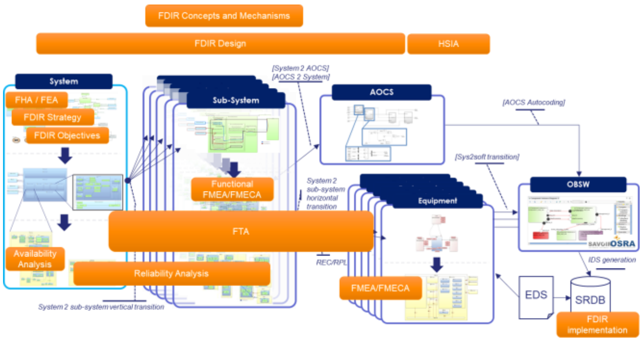


Figure 3-1: Overview of the Model-Based FDIR Process

For each applicable step of the FDIR process described in the Handbook ([**Erreur ! Source du renvoi introuvable.**]), the study has analyzed in details 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 have 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 the study, a compatibility with current practices and other studies outcomes has been targeted.

EDS was also taken into account : [D0] provides an overview of where and when in the System Engineering process Electronic Data Sheets should be used. For what concerns FDIR, EDS is an interesting base, and 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, it is clear that FDIR was not in the scope of this activity.

4. SPECIFICATION OF CAPELLA FDIR VIEWPOINT

[D2.1] provides the specification of the Capella FDIR design viewpoint allowing to implement and support the Model Based FDIR Design process elaborated in the frame of the GSTP Model Based FDIR Design activity.

The Capella FDIR Design viewpoint will be implemented 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 FDIR process described in [D1].

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 [D0], 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.

In [D3], the Model Based FDIR Design Process mapping with SAVOIR FDIR Handbook and COMPASS has been established. Regarding the traceability with [**Erreur ! Source du renvoi introuvable.**], 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 [D2.1]. 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:

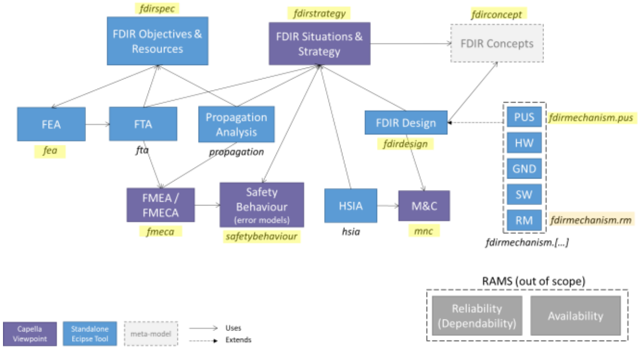


Figure 5-1: FDIR Design Toolset Architecture

This architecture contains different kinds of elements:

- in purple, Capella Viewpoints, which allow to extend Capella models;
- in blue, plugins allowing to create models which are not 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 can be found in the [D2.2] document, which consists in a coverage and traceability matrix of the requirements specified in [D2.1].

There is also a Software User Manual [SUM01] detailing how to install and use each tool.

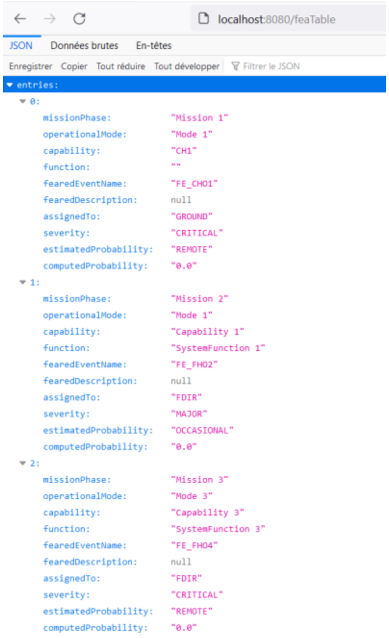
6. CONNECTION TO THE DATA HUB

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).



```
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

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, ..).

7. USE-CASE

The mission taken as reference for the use-case modelling is PLATO (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 characterisation of terrestrial exoplanets.

The use-case goal was to assess model-based FDIR Design process defined in [D4] and the prototyped FDIR Design toolset. It is described in the [D4] document. This document gives an overview of the mission and spacecraft architecture of PLATO, as well as an overview of the FDIR concept defined for PLATO. It also details the scope of the FDIR which has been modelled and the implemented models.

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.

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 FEA, FDIR Specification and FDIR Design models. The architecture of the use-case is depicted on the figure below:

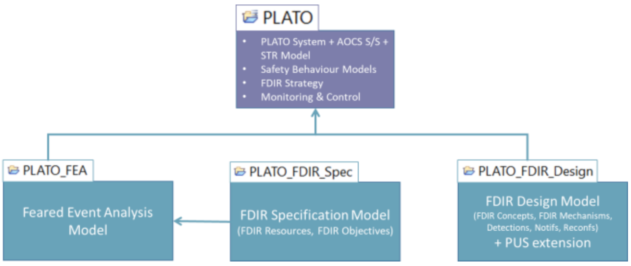


Figure 7-1: Use-Case Architecture

8. CONCLUSION

The Model Based FDIR design activity has allowed to de-risk and develop a toolset allowing to implement most of the design activities of the FDIR process, assuming a model of the system exists at the right level (system, sub-system, and equipment level).

The Toolset has been experimented taking into account a real on-going project (PLATO), and fruitful discussions have allow to consolidate the features of this tool. Although it is not yet ready for industrial adoption, the study has reached 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.