BENEFITS OF MODEL-BASED SYSTEM ENGINEERING FOR FDIR

Régis de Ferluc[(1)], Olivier Rigaud[(2)] Délia Cellarier[(3)], Valentin Beauplet[(4)], Gérald Garcia[(5)]
[(1)]*Thales Alenia Space, regis.deferluc@thalesaleniaspace.com*
[(2)] *Thales Alenia Space, olivier.rigaud@thalesaleniaspace.com*
[(3)] *Thales Alenia Space, delia.cellarier@thalesaleniaspace.com*
[(4)] *Thales Alenia Space, valentin.beauplet@thalesaleniaspace.com*
[(5)] *Thales Alenia Space, gerald.garcia@thalesaleniaspace.com*

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, from the high level functional aspects down to low level physical aspects. Model Based techniques applied to FDIR Design bring great benefits and open new opportunities. This paper provides a return of experience of Thales Alenia Space in this area, and describes the journey of applying MBSE to the FDIR discipline in an industrial context.

KEYWORDS – MBSE, Capella, FDIR

1. Introduction

In the past, FDIR design was mainly a time-consuming and error prone paper-based workflow, not appropriate to cope with the growing complexity of the space systems. In addition, adequacy of the FDIR design was often assessed very late in the process (integration and test phase), sometimes even after the launch of the spacecraft (FDIR parameter tuning). Projects after projects, FDIR engineers are facing every day challenges like ensuring the alignment of the FDIR Design with regard to the system design, to the reliability requirements, or to the suppliers information, or like optimizing the FDIR concepts (Detection, Isolation, Recovery of failures) with regard to mission objectives and operational concepts.

Fault Detection, Isolation, and Recovery is not necessary a complicated discipline, in the sense that concepts are quite simple, everything is based on logical mechanisms or rules, and the FDIR design generally relies on a lot of heritage and background experience from past successful projects. However, FDIR is complex in the sense that it considers a very large number of data, and an even larger number of possible combinations of situations that needs to be analysed and properly handled in order to meet the reliability and availability requirements of the mission. The challenge thus resides in the right management of this data without spending too much effort and time but still achieving the specified goals.

2. Starting point of the story – the Excel Table

FDIR design basically consists in selecting in the system design the observable parameters or signals impacted by the occurrence of considered failures, and to define suitable monitoring and reconfiguration mechanisms to detect and recover the failures, depending on the mission phase and the operational modes, taking advantages of the redundancy of the system, and using the appropriate commandable actions. These aspects can easily be captured in an Excel Table. In Thales Alenia Space, in the previous decade, the FDIR engineers job consisted in copying and pasting parameter names from documentation or from the spacecraft database into the Excel Tables, and to keep the data up-to-date manually. Because of this manual process, each FDIR engineer was trying to optimize the Excel table he was using on his project, leading to a large variety of practices across the company, and preventing efficient re-used from project to project.

3. Introducing a FDIR Domain Specific Language

When MBSE started to be introduced in Thales Alenia Space in the early 2010s, a small budget was invested to automate the configuration of the PUS mechanisms dedicated to the FDIR within the on-board software (OBSW). The proposed approach relied on the use of an FDIR Domain Specific Language - DSL (implemented with the Eclipse Modelling Framework - EMF) coupled with a code generator tool (implemented with the Acceleo technology) producing the Ada files configuring the PUS library embedded in the OBSW. To make this approach feasible, two major improvements were introduced :

First, an harmonisation of the existing FDIR Excel templates was required. Indeed, the objective was to minimize the change for the FDIR engineer (i.e. keep the Excel interface to design the FDIR), but to map the Excel data to a formal DSL, a consolidation of the template was required. It took quite a long time for all experts working on different projects to converge towards a common Excel template. This was facilitated as the use of the PUS library became the baseline of most of the projects.

The second improvement was to check the consistency of the FDIR data prior to the code generation. When the data is imported from the Excel tables into the intermediate FDIR model required by the code generator, the importer tool checks if the observable parameters and commandable actions used by the FDIR are well defined in the Spacecraft Data Base. Early consistency checks permit to save time and avoid to discover issues when the on-board software is running.

Although different prototypes of HMI where developed to get rid of Excel and to directly edit the model (Tree based editor, Table interface in Eclipse, Diagrams, …), FDIR engineers have always preferred keeping the Excel table as their privileged user-interface. The reason invoked was that it was simple to deliver the complete FDIR design to the customer in this format.

This first generation of the tool was named the FDIR Editor (Figure 3-1), and was used operationally on Sentinel 3, Exomars TGO, and Iridium Next projects.

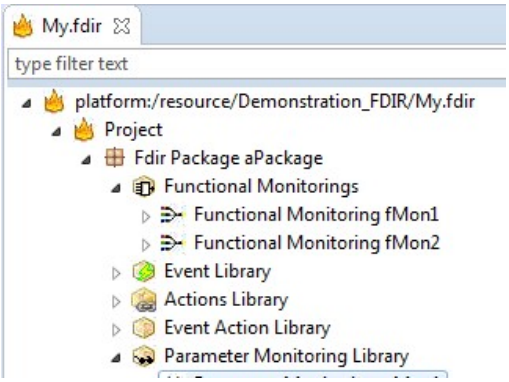

Figure 3-1 - screenshot of a simple FDIR model

4. Leveraging on model to produce documentation

Instead of delivering to the customer the complete FDIR Excel Table, or to copy/past parts of this table into documents (e.g. the FDIR Implementation Report), a small budget was invested to develop a documentation generator, producing a PDF document containing all the FDIR design data organized in very nice sections and paragraphs. Despite several workshops aiming at optimizing the outline of the generated report, and despite the extensive use of cross-links to ease the navigation within the information, the generated document was always considered as hard to read (hundreds of pages with few engineering information) and useless for both the customer or the operator. At least, it saves the time of FDIR Engineers that can produce an updated FDIR Implementation Report in one-click, as requested by the applicable ECSS process.

A return on investment on this aspect is that a model suitable for a given objective (code generation) may not be suitable for another objective (doc generation). Since then, the FDIR meta-model has been extended with additional information that brings more added value to the generated report (e.g. references with other documents to add justification or traceability of the FDIR design).

5. Extending the FDIR Editor with capability to capture the FMECAs

The successful adoption of MBSE techniques for the FDIR design was replicated on the perimeter of the FMECAs (Failure Mode Effects and Criticality Analysis). Indeed, FDIR is designed to handle all the possible failures identified in the equipment datasheets provided by the suppliers, and identified as critical for the system or the mission. It is thus very convenient to have a model of the FMECAs, so as to link the FDIR monitoring to the failure modes they address. FMECA is an independent model so it can be reused across projects, and FDIR model can reference one or more FMECA models. The same approach than for the FDIR design was adopted to match the users' expectations in terms of User Interface : an Excel template was defined, and an importer tool was developed to build the FMECA model from the Excel spreadsheet. This allows to beneficiate from Model Based Engineering features (traceability, code and doc generation, configuration management, …) while preserving the habits of FDIR engineers.

The FMECA Editor was operationally used for the first time on the MTG FCI project.

6. Merging the FDIR Editor with SCOPE – the Thales Alenia Space Preparation Environment

The first versions of the FDIR editor and FMECA editor were standalone tools requiring, as input, the content of the data-base exported in an XML format (list of Telemetry and Telecommands). The natural improvement was to integrate the features directly into the SCOPE Preparation Environment *[1] ADCSS 2015 - FDIR - state of the art and evolutions - TAS [2]* , aside other editors such as the Flight Control Procedure Editor, the Action Sequence Editor, or the On-board Control Procedure editor (see Figure 6-1).
This integration was the opportunity for different teams of Thales Alenia Space to harmonize their practices, to share common building blocks, and to align the delivery and support activities. The use of Eclipse EMF as a standard set of Modelling techniques helped to face these challenges.

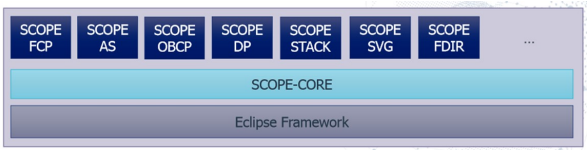

Figure 6-1 - SCOPE Editors

7. Using FDIR models to perform FDIR simulation

Having modelled both FDIR design and Action Sequences, end-to-end FDIR mechanisms can be simulated all the way from FDIR detection (PMON trigger), Failure Notification (Event) to the execution of consequent actions. Closing the loop defining TC behavior and equipment hardware configuration with a model-based approach is then the key to create a native FDIR Simulator prototype. Its goal is to check, early in the process, that the FDIR design achieves the FDIR objectives, in order to reduce the number of expensive non-compliance that could be discovered at test-on-bench level. Definition of the FDIR Simulator scenarios and test campaigns relies on other MSBSE products included in SCOPE.

Although emulation of the FDIR dynamic behavior with a native FDIR Simulator will remain limited by unexpected physical phenomena or hardware failures, new features are being developed to enhance its representativeness and action range. Indeed, studies are on the way to couple it with a native AOCS simulation on Matlab/Simulink, while others focus on the integration of Reconfiguration Modules models.

8. Improving the customer experience when using models

Models are not always the good format to organize the information for a review with a customer, who, up-to-now, seems to prefer Excel tables as he can re-arrange the data according to its own needs, that may depend on the reviewer's profile, and of the kind of the review (PDR, CDR, TRR,…). It is thus very important to capture those user needs, and to display the information in a user-friendly interface, using the most recent web-based technology, and using the concepts and terminology of the reviewer (as opposed to the organisation's internal accronyms). Sometimes the reviewer is not interested by the data itself, but by precise Key Performance Indicators (KPI) that reveals the complexity of the FDIR, its completeness, its maturity, or its correctness. The FDIR model is a strong asset in this situation, as the structured data can be translated into appropriate formats.

9. Consolidation of the process : the SAVOIR FDIR handbook

Model Based techniques requires to consider a clear and coherent process to implement engineering activities within a tool, less flexible than textual documentation. The consolidation of the FDIR process was considered as a pre-requisite to the extension of the FDIR MBSE practices in Thales Alenia Space, as highlighted in *[1]* . The work performed by the SAVOIR FDIR working group, and the elaboration of a Handbook, was a cornerstone to continue deploying MBSE for the FDIR process.

10. Embracing the complete FDIR process with models

The next target is to deploy an end-to-end model-based approach covering all the FDIR engineering activities as defined in the SAVOIR FDIR Handbook, with the support of an appropriate toolchain. This will allow to perform early verification and validation analyses which are key to optimise the FDIR design, manage the complexity, and de-risk the test activities.

Thales Alenia Space is currently putting a significant effort in a GSTP de-risk activity which aims at de-risking the use of a Model-Based FDIR Design approach based on Capella. This approach will open the door to early verification and validation thanks to Model Checking and Simulation in the near future, for example with the COMPASS toolset. The tooled methodology defined in the frame of this GSTP activity is assessed through a use-case based on the PLATO project.

11. Further opportunities

Thales Alenia Space considers the use of models as a very strong foundation to introduce new capabilities in the field of Fault detection or prognostics thanks to AI techniques in addition to classical FDIR mechanisms. Models are also very useful to formalise the information and feed Chatbot or virtual agents that can support operators or engineers in their day to day task. Finally, models support not only early validation and verification activities, but also can be optimised or even produced by smart algorithms trained over the data of numerous past projects, taking into account not only the design phase, but also the operational phase.

Conclusion

FDIR is a specific discipline which can beneficiate a lot from MBSE techniques. However, MBSE deployment in an industrial context takes time, and requires to progress step by step in order to build an efficient and user-friendly environment. The human factor is one of the main aspects impacting the success or the failure of the MBSE deployment, and the definition of a clear vision covering both the R&D exploration phase and the operational needs is required to federate all the initiatives, and disseminate the appropriate culture. Thales Alenia Space has been progressing a lot in this field during the last 10 years, and expect to continue this journey in the coming years, together with the European Space community and with the Agencies.

[1] ADCSS 2015 - FDIR - state of the art and evolutions - TAS
[2] ESAW 2017 "SCOPE : the Thales Alenia Space Preparation Environment"