Development of Failure Modes and Effects Analysis methodology using Model-Based Safety Assessment approach

A S Savelev, O D Bersutskaya, N D Silin and E S Neretin
Moscow Aviation Institute (National Research University), 4, Volokolamskoe shosse, Moscow, 125993, Russia
E-mail: arssavelev@mai.education

Abstract. During the development of aircraft systems, the safety assessment process activities are carried out in parallel. Traditionally, safety professionals perform Functional Hazard Assessment, Preliminary System Safety Assessment, and System Safety Assessment. Despite the availability of many modern and advanced tools for performing calculations during the implementation of the System Safety Assessment, a great responsibility (and, accordingly, the risk of error) remains with the person. Model-Based Safety Assessment is a new and rapidly developing approach to evaluate the safety of airborne equipment worldwide, which improves existing methodologies for performing various analyzes, such as Failure Modes and Effects Analysis (FMEA). Implementation of FMEA using this approach requires the development of special software tools that allow both to create a model of the analyzed onboard equipment and systems, and to provide an opportunity to use this model when performing FMEA. One such tool is ANSYS Medini Analyze. Model-oriented method for performing FMEA is proposed within this article. This method fully complies with the requirements of ARP-4761 and provides possibility to minimize the likelihood of human error. Model-oriented method for performing FMEA has been probated on the example of flight control system at various levels of abstraction (system, item, functional block and hardware/software level).

1. Introduction
A Failure Modes and Effects Analysis (FMEA) is a systematic method of identifying the failure modes of a system, item, function, or piece-part and determining the effects on the next higher level of the design. The detection method (if any) for each failure mode may also be determined. An FMEA may be a quantitative or qualitative analysis and may be performed on all types of systems (e.g., electrical, electronic or mechanical systems). If a quantitative FMEA is being performed, a failure rate is determined for each failure mode.

An FMEA is performed at a given level (system, item, etc.), by postulating the ways the chosen level’s specific implementation may fail. The effect of each failure mode is determined at the given level and usually the next higher level for each operating mode of the equipment. The FMEA must account for all safety related effects and any other effects identified by the requirements. In cases where it is not possible to identify the specific nature of a failure mode, the worst case effect must be assumed [1].

At the same time, despite all the theoretical simplicity of FMEA and considerable experience in its application (FMEA has been used since the 1940s), the problem of the human factor is still relevant. The analyst cannot always adequately assess the failure and determine its effects.
Especially this problem increases with an increase in the number of components and their failure conditions that must be analyzed [2]. This problem is especially relevant for modern complex items of onboard equipment, made based on electronic hardware.

In the scientific world, there has been a long history of research devoted to improving the entire safety assessment process (although until now a number of such improvements have not been accepted as recommendations for achieving certification goals). Currently, among the approaches to improvement, the use of the Model-Based Approach to Safety Assessment (MBSA) plays a significant role. It is often understood only as a means of the fault trees development automating by using the state transitions logic for the components of the analyzed system. For this, new programming languages are being developed [4] and different options of using the widely applicable tools are proposed [5]. MBSA for FMEA is mainly proposed to be used for the failure propagation model investigation [6].

The proposed methods of MBSA implementation can help to solve a significant set of problems arising during the implementation of safety assessment activities. However, these methods are based, among other things, on the fact that the architecture of the analyzed system is correct, and the failure states are correctly identified, which contradicts the research results [2]. This work is devoted to the development of a method for performing FMEA using modern software tools for supporting safety assessment—ANSYS Medini Analyze, which allow minimizing, as much as possible, errors in FMEA caused by human factors. The results of the work can be applied from the lowest hardware/software level to the highest—for aircraft system. The best result this methodology can show when systematically used at all levels of the hierarchy, regardless of the distribution of responsibilities between the organizations involved into development and safety assessment at different levels.

2. Methodology

2.1. Overview of the MBSA application for FMEA

Currently Failure Modes and Effects Analysis is mostly performed manually by safety assessment engineers, that, along with the obvious advantage, such as the use of extensive experience of engineers, also has disadvantages, namely, there is a high risk of making an error in manual calculations, missing any functions during analysis or components, or, most often, do not adequately incorporate design changes in the FMEA.

The application of the Model-Based approach to Safety Assessment (MBSA) will significantly reduce the likelihood of such errors by using the automation when determine the configuration of the analyzed component and formalizing the description of the possible effects of failures.

Automation of configuration determination means that it is possible to make changes to the architecture by adding new components, changing the composition and relationships of functional blocks with simultaneous binding to the FMEA implementation, which can be treated and monitored by modern software tools for model-based development and safety assessment. Such tools allow to track changes in an automatic mode, which helps to avoid missing a critical component or functional block when performing FMEA.

The formalization of failure effects determination is that the completely transferred logic of functioning, control and propagation of failures (considering their probability) into a model form will allow to get away from an expert decision on the failure effects and move on to their formal justification. The most convenient way to simulate such processes is the state machine method. Modern tools using the MBSA principles allow modeling the failure effects using the state machine method within the tool itself or by receiving results from third-party tools automatically.

2.2. FMEA methodology approaches

There are two main approaches to FMEA—functional (typically used for complex electronic equipment such as FPGAs and microprocessors) and component (usually used for simple
mechanical and electrical components). For both functional and component FMEA, quantitative approach could be applied, when the failure fate is determined for each type of failure either based on data from the service experience, or from reference books with data on failure rates, for example, such as MIL-HDBK-217 [7], MIL-HDBK-338 [8], RAC “Nonelectronic Parts Reliability Data” [9], MIL-HDBK-978 [10] and Rome Laboratory “Reliability Engineer’s Toolkit” [11].

![Diagram](https://via.placeholder.com/150)

**Figure 1.** Hierarchy levels general overview.

When performing FMEA, it should be taken into account that the item under analysis has a multi-level structure—the item itself, its functional blocks and hardware elements included in the functional block, as shown in figure 1.

2.3. Proposed FMEA methodology

The proposed methodology for FMEA implementation is to bottom up sequentially analyze and summarize failures (i.e., from the hardware level to the item level and above) by executing step-by-step instructions. It is assumed that during the development at the Preliminary Safety Assessment stage, functions and their failure states were determined for all items and functional blocks.

2.3.1. Step 1—Hardware/software level FMEA

Hardware/software FMEA is the most fundamental analysis compared to the rest of the abstraction levels. This is explained by the fact that at this level the structure of the product is considered in detail, without generalizations. If, according to the results of this analysis, it is revealed that there are no failure modes leading to catastrophic or hazardous situation, then the FMEA goals of the overall system will be achieved (however, this does not exclude the need for generalization and presentation at higher levels of the hierarchy to simplify the adjacent Fault Tree Analysis (FTA) and in the interests of certification). On the other hand, if a failure mode is detected as leading to a catastrophic or hazardous situation, then the architecture should be redesigned to mitigate the effect of this failure mode, regardless of the readiness of the considered and interfacing equipment.
Input data for hardware/software FMEA are:

- list of hardware elements and functions;
- list of software components and functions;
- hardware reliability rates from appropriate reference books;
- list of failure conditions for functional blocks where hardware under consideration is located (for definition of failure effects).

For software—functional FMEA is applicable (software components’ functions are analyzed to define functional failure conditions that are considered as failure modes).

For hardware—piece-part FMEA is applicable (failures of similar hardware elements are analyzed based on service experience and information on reliability in reference books and considered as failure modes).

| Hardware X FMEA          | Failure Mode | Failure Rate | Failure Effect |
|--------------------------|--------------|--------------|----------------|
| R5 Open                  | A            | Loss of +5V  |                |
| R5 Short                 | B            | 5V tied of GND|                |
| ...                      | ...          | ...          |                |

| Hardware Y FMEA          | Failure Mode | Failure Rate | Failure Effect |
|--------------------------|--------------|--------------|----------------|
| C5 Short                 | C            | 5V tied of GND|                |
| C5 Open                  | D            | No Safety Effect|                |
| ...                      | ...          | ...          |                |

Results are documented in a table, where the following information should be presented:

- function and its ID (only for functional FMEA);
- hardware element and its ID (only for piece-part FMEA);
- failure mode;
- failure rate (only for piece-part FMEA);
- failure effect at functional block level (that is functional block failure condition, identified within PSSA).

To reduce volume of reports at the higher hierarchy level, hardware/software FMEA results are summarized within FMES (Failure Modes and Effects Summary) based on similar failure effects; failure rates add up. This process is reflected at figure 2.

**2.3.2. Step 2—Functional blocks level FMEA**

FMEA for functional blocks is the most convenient analysis for safety engineers compared to other levels of abstraction. The reason is that at this level obvious failure states are considered that do not require a detailed understanding of the hardware failure physics, but the failures are...
not abstract and are tied directly to the equipment functions. Failure effects at a higher level and failure causes at a lower level are amenable to analysis and identification of relationships in the behavior of items in case of failures.

The inputs for functional blocks level FMEA are:

- FMES (see step 1) for the hardware elements within functional blocks under analysis;
- list of failure conditions for item where functional block is located (for failure effects definition).

Results are documented in a table where the following information should be presented:

- function of the functional block, that could be violated by failure mode under consideration, and function ID;
- failure mode (from FMES table from step 1);
- failure rate (from FMES table from step 1);
- failure effects at item level (that is item failure condition, identified within PSSA);
- monitoring means;
- possible failure causes.

---

### Functional block X FMEA

| Failure Mode | Failure Rate | Failure Effect | Detection Method | Potential Failure Cause |
|--------------|--------------|----------------|------------------|------------------------|
| 5V tied of GND | B+C | No Command Signals | Built-In-Test | Hardware X – R5 Open; Hardware Y – C5 Short |
| Loss of +5V | A | No Command Signals | Built-In-Test | Hardware X – R5 Short; Hardware Y – C5 Open |
| No Safety Effect | D | No Safety Effect | Hide | Hardware Y – C5 Open |

### Functional block Y FMEA

| Failure Mode | Failure Rate | Failure Effect | Detection Method | Potential Failure Cause |
|--------------|--------------|----------------|------------------|------------------------|
| No Safety Effect | E | No Safety Effect | Hide | … |

---

### FMES

| Failure Mode | Failure Rate | Failure Effect | Detection Method | Potential Failure Cause |
|--------------|--------------|----------------|------------------|------------------------|
| No Command Signals | A+B+C | Loss of one channel | Built-In-Test | Functional block X – 5V tied of GND; Functional block X – Loss of +5V |
| No Safety Effect | D+E | No Safety Effect | Hide | Functional block X – No Safety Effect; Functional block Y – No Safety Effect |

---

**Figure 3.** Example of transition from FMEA for functional blocks to FMES.

To reduce volume of reports at the higher hierarchy level, step 2 results are summarized within FMES (Failure Modes and Effects Summary) based on similar failure effects; failure rates add up. This process is reflected at figure 3.

2.3.3. Step 3—Item FMEA

Items FMEA is the most acceptable analysis for top-level safety engineer (aircraft or aircraft system level) compared to other levels of abstraction. The reason is that at this level specific failure states are considered that do not require detailed knowledge of the item structure, while the failures are tied directly to those functions that are performed by this item, and the effect
on the failure conditions, identified during the Functional Hazard Assessment (FHA), can be investigated. Consequences at a higher level and causes at a lower level are amenable to analysis and identification of relationships in the behavior of the system in case of failures.

The inputs for item level FMEA are:

- FMES (see step 2) for functional blocks within item under consideration;
- list of failure conditions for overall aircraft system, where item is located (for failure effects definition).

Results are documented in a table where the following information should be presented:

- item function, that could be violated by failure mode under consideration, and item ID;
- failure mode (from FMES from step 2);
- failure rate (from FMES from step 2);
- failure effects at aircraft system level (that is system failure condition, identified within FHA);
- monitoring means;
- possible failure causes.

![Figure 4. Example of transition from item FMEA to FMES.](image)

To reduce volume of reports, step 3 results are summarized within FMES (Failure Modes and Effects Summary) based on similar failure effects; failure rates add up. This FMES is further used as FTA input and during certification authority liaison. This process is reflected at figure 4.

### 2.4. Ansys Medini Analyze toolset description

Ansys Medini™ Analyze is a model-based and integrated toolset supporting the safety analysis and design for safety critical functions. All safety analysis methods in Medini Analyze are based on design models. Here “based on” means that models define structure and behavior of the system to be developed and all safety methods augment these with an analysis of potential failures. Supported modeling languages are SysML for expressing various aspects of the functional architecture, system design with physical structure and behavior, and MATLAB/Simulink.
The point of interest for safety assessment is mostly possible failures of system under consideration and its components. In the Ansys Medini™ Analyze failures are in most cases directly linked to model elements, i.e. they are contained inside the model elements and then shown in different analyses such as FTA or FMEA. Therefore, all analyses provide a consistent view on the failure models. For example, a failure mode “short circuit” of a physical model might appear in an FMEA as well as an event in a fault tree. If the failure rate of the element/failure mode changes, both analyses will automatically be synchronized, since the data is stored in the underlying model. If models are imported from development tools (e.g. SCADE Architect, IBM Rhapsody), failures are annotated to imported model elements and preserved during update of the models [12].

The identified advantages of the Medini Analyze make it possible to define this tool as modern and convenient for implementation of safety assessment activity for aircraft systems.

3. Results and Discussion
Within the framework of this work, the object of the research was the part of Flight Control System (FCS), which is responsible for the control of the main and secondary aerodynamic surfaces.

Figure 5. Hierarchy levels of Flight Control System part responsible for main and secondary aerodynamic surfaces control.

The following hierarchy levels have been implemented in Ansys Medini™ Analyze (depicted at figure 5):
- flight control system (FCS) with number of items—controls, computing units, actuators;
- main control unit (one of the FCS items);
- actuators control unit (one of the FCS items);
- functional block “Control” (one of the functional blocks of Actuators control unit);
- hardware elements within “Control” functional block.
4. Summary
In the course of the work, the main errors that arise when safety engineers perform FMEA were studied. It was found that currently the issue of mitigating the human factor when performing FMEA is poorly investigated. So, for example, an aircraft and system-level safety engineers often cannot monitor the state of software/hardware-level safety data. Accordingly, if changes are made to the product architecture (i.e. components are added or excluded) or failure rates are calculated (operating conditions change or new reliability data are received), this change could be missed. Also, safety engineers have difficulties in determining the failure effects, since often the effects are attempted to be described subjectively, without reference to available data from earlier stages of development (for example, failure conditions identified during the FHA or PSSA).

An integrated approach was used to address these problems.

First, a methodology was proposed for performing FMEA from the lowest hardware/software level to the highest aircraft system level, which can be also used in the FTA of the aircraft level, as well as for certification authority’s liaison. Thus, the problem of determining the failure effects was solved.

Secondly, this technique has been implemented in the modern Ansys Medini Analyze tool for MBSA. The model structure of the system design in Ansys Medini Analyze at various levels of abstraction, which includes a list of failure modes as an attribute, allows automated tracking of possible mistakes in the FMEA part. This mitigates the risk of error when making architectural changes or reliability calculations at any level of abstraction.

Acknowledgments
This work was supported by the Russian Foundation for Basic Research (Grant No. 20-31-90028).

References
[1] 1996 Aerospace Recommended Practice SAE ARP 4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment (USA: SAE International) p 331 URL https://www.sae.org/standards/content/arp4761/
[2] Banghart M, Babski-Reeves K and Bian L 2016 Human induced variability during failure mode effects analysis 2016 Annual Reliability and Maintainability Symposium (RAMS) Tucson, AZ pp 1–7 DOI: 10.1109/RAMS.2016.7448000
[3] Joshi A, Miller S P, Whalen M and Heimdahl M P E 2005 A proposal for model-based safety analysis 24th Digital Avionics Systems Conference (Washington, DC) vol 2 pp 13 DOI: 10.1109/DASC.2005.1563409
[4] Batteux M, Prosvirnova T, Rauzy A and Kloul L 2013 The AltaRica 3.0 project for model-based safety assessment 11th IEEE International Conference on Industrial Informatics (INDIN), Bochum, 2013 pp 741–746 DOI: 10.1109/INDIN.2013.6622976
[5] Joshi A and Heimdahl M P E 2005 Model-Based Safety Analysis of Simulink Models Using SCADE Design Verifier Computer Safety, Reliability, and Security. SAFECOMP 2005. Lecture Notes in Computer Science vol 3688, ed R Winther, B A Gran and G Dahl (Berlin, Heidelberg: Springer) DOI: 10.1007/11563228_10
[6] Struss P, Fraracci A 2012 Automated Model-based FMEA of a Braking System IFAC Proceedings Volumes vol 45(20) pp 373–378 DOI: 10.3182/20120829-3-MX-2028.00230
[7] MILITARY HANDBOOK RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT MIL-HDBK-217F NOTICE 1995 (USA: Department of Defense) p 80 URL http://everyspec.com/MIL-HDBK/MIL-HDBK-217F NOTICE 1995
[8] MILITARY HANDBOOK: ELECTRONIC RELIABILITY DESIGN HANDBOOK MIL-HDBK-338B 1998 (USA: Department of Defense) p 1046 URL http://everyspec.com/MIL-HDBK/MIL-HDBK-338B 1998
[9] Nonelectronic Parts Reliability Data Publication NPRD 2016 URL https://www.quanterion.com/publications/nonelectronic-parts-reliability-data-publication-nprd-2016/
[10] NASA PARTS APPLICATION HANDBOOK 1989 URL https://global.ihs.com/doc_detail.cfm?item_s_key=00058925
[11] RELIABILITY ENGINEER’S TOOLKIT 1993 URL http://everyspec.com/USAF/USAF-RADC/RADC_RELIABILITY_ENGINEERS_TOOLKIT_1993_38123/
[12] Ansys Medini™ Analyze User Guide Copyright © 2020 ANSYS Germany GmbH