A model-based rams estimation methodology for innovative aircraft on-board systems supporting mdo applications

AIAA AVIATION Forum
June 15-19, 2020, VIRTUAL EVENT
AIAA AVIATION 2020 FORUM

10.2514/6.2020-3151

A Model-Based RAMS Estimation Methodology for Innovative Aircraft on-board Systems supporting MDO Applications

Francesco Bruno*
German Aerospace Center (DLR), Politecnico di Torino

Marco Fioriti†
Politecnico di Torino, Turin, Italy, 10129

Giuseppa Donelli‡, Luca Boggero§, Pier Davide Ciampa**, Björn Nagel††
German Aerospace Center (DLR), Hamburg, Germany, 21129

The reduction of aircraft operating costs is one of the most important objectives addressed by aeronautical manufactures and research centers in the last decades. In order to reach this objective, one of the current ways is to develop innovative on-board system architectures, which can bring to lower fuel and maintenance costs. The development and optimization of these new aircraft on-board systems can be addressed through a Multidisciplinary Design Optimization (MDO) approach, which involves different disciplines. One relevant discipline in this MDO problem is Reliability, Availability, Maintainability and Safety (RAMS), which allows the assessment of the reliability and safety of aircraft systems. Indeed the development of innovative systems cannot comply with only performance requirements, but also with reliability and safety constraints. Therefore, the RAMS discipline plays an important role in the development of innovative on-board systems. In the last years, different RAMS models and methods have been defined, considering both conventional and innovative architectures. However, most of them rely on a document-based approach, which makes difficult and time consuming the use of information gained through their analysis to improve system architectures. On the contrary, a model-based approach would make easier and more accessible the study of systems reliability and safety, as explained in several studies. Model Based Systems Engineering (MBSE) is an emerging approach that is mainly used for the design of complex systems. However, only a few studies propose this approach for the evaluation of system safety and reliability. The aim of this paper is therefore to propose a MBSE approach for model-based RAMS evaluations. The paper demonstrates that RAMS models can be developed to quickly and more effectively assess the reliability and safety of conventional and innovative on-board system architectures. In addition, further activities for the integration of the model-based RAMS methodology within MDO processes are described in the paper.

* Master Student, Mechanical and Aerospace Engineering Department, Turin.
† Assistant Professor, Mechanical and Aerospace Engineering Department, Turin, marco.fioriti@polito.it.
‡ Research Scientist, Institute of System Architectures in Aeronautics, Aircraft Design & System Integration, Hamburg, Giuseppa.Donelli@dlr.de.
§ Research Scientist, Institute of System Architectures in Aeronautics, Aircraft Design & System Integration, Hamburg, Luca.Boggero@dlr.de.
** Head of MDO Group, Institute of System Architectures in Aeronautics, Aircraft Design & System Integration, Hamburg, Pier.Ciampa@dlr.de, AIAA MDO TC member.
†† Founding director, Institute of System Architectures in Aeronautics, Hamburg, Bjoern.Nagel@dlr.de.

Nomenclature

ECS = Environmental Control System
EHA = Electro-Hydrostatic Actuator
ELAC = Elevator Aileron Computer
FCS = Flight Control System
FHA = Functional Hazard Analysis
FMEA = Failure Modes and Effects Analysis
FTA = Fault Tree Analysis
MBSA = Model Based Safety Analysis
MBSE = Model Based Systems Engineering
MDO = Multidisciplinary Design and Optimization
RAMS = Reliability, Availability, Maintainability and Safety
RBD = Reliability Block Diagram
SysML = System Modeling Language

I. Introduction

THE reduction of aircraft fuel consumption is one of the most important objectives addressed by aeronautical manufacturers and research centers in the last decades. A fuel reduction would bring to significant benefits in terms of lower environmental impact and lower fuel costs. Therefore, different new technologies and solutions are being developed, e.g. more efficient engines, alternatives to kerosene-based fuels and hybrid electric aircraft. In addition, more reliable and safer solutions are being investigated, since they entail reductions of maintenance costs.

A significant improvement in operating costs can be reached by aircraft on-board systems. Nowadays, especially in conventional civil transportation aircraft, the on-board systems are driven by a combination of four types of secondary power source: pneumatic, mechanical, hydraulic and electrical [1]. They are all derived from the gas turbine engines and their energy consumption is approximately 5% of the total fuel burnt [2]. The pneumatic power is obtained from the engines high-pressure compressors and delivered to the Environmental Control System (ECS), Wing Ice Protection System (WIPS) and Cowl Ice Protection System (CIPS). The mechanical power is instead transferred to hydraulic pumps, some fuel pumps, and to the main electrical generators, by means of gearboxes. Afterwards, hydraulic and electrical power is distributed throughout the aircraft to drive subsystems such as flight control actuators, landing gear, avionics, aircraft lighting and galley loads [3], [4]. Supplying all these kinds of secondary power sources requires many complex systems and a failure in one of them may lead to unavailability of important subsystems, resulting in a grounded aircraft and flight delay. Having more than one power source to be distributed throughout the aircraft, the number of redundancies to obtain the necessary safety level is higher. Moreover, power off-takes, especially bleed air off-takes cause a reduction of engine efficiency, resulting in an increase of fuel consumption and hence operating costs.

Therefore, the short term goal is to develop innovative on-board system architectures, using the electrical power in place of hydraulic and pneumatic power [5]. Ultimately, the goal for future aircraft is to replace every kind of power source with the electrical one. The first concept characterizes the More Electric Aircraft (MEA), whereas the second defines the All Electric Aircraft (AEA). In the last decade the MEA concept has already been adopted by Boeing with the B787 Dreamliner, in which the no-bleed systems architecture allows to eliminate the traditional pneumatic system. Therefore, the power source of most functions (such as the air-conditioning and the anti/de-icing) is converted to electric power. This new architecture offers a number of benefits, including improved fuel consumption (with a predicted fuel saving of about 3%), reduced maintenance costs and improved reliability due to the use of modern power electronics and fewer components in the engine installation [6]. The same can be observed on the Airbus A380 Flight Control System (FCS), in which one of the hydraulic systems has been replaced with a set of electrically powered actuators. The type of actuators that has been selected is the Electro-Hydrostatic Actuator (EHA). The reduction of the total number of hydraulic components in the FCS architecture has involved different benefits, including weight savings, improvements of reliability and increased safety [7].

The development of different new on-board system architectures, which may influence many disciplines and parameters (e.g. aerodynamic performance, fuel consumption, aircraft geometry, engine efficiency and costs), should be done through a Multidisciplinary Design Optimization (MDO) approach. MDO is a field of engineering that focuses on numerical optimization for the design of systems [8], i.e. it uses optimization methods to solve design problems, allowing to incorporate of all the relevant disciplines simultaneously. Among these, the Reliability,

Availability, Maintainability, and Safety (RAMS) is one of the most important disciplines for the development of any on-board systems architecture. Nevertheless, even though RAMS is a very relevant discipline, currently it is still difficult to define the reliability and safety of aircraft on-board systems implementing innovative architectures. Moreover, improving those configurations during the design process to avoid their possible faults is still a challenge.

In the last years, different techniques and methods have been developed to assess systems reliability and safety. Examples or techniques for the estimation of system reliability and safety are Reliability Block Diagram (RBD), Functional Hazard Analysis (FHA), Fault Tree Analysis (FTA), Physics of Failure (PoF) analysis, Failure Modes and Effects Analysis (FMEA), Failure Modes, Effects and Critical Analysis (FMECA), Markov Analysis (MA), and Common-Cause Analysis (CCA). All these techniques are used during the reliability assessment process of the aircraft, and are adopted by aircraft manufacturers, such as Boeing and Airbus [9]. In addition there are handbook-based methods, which rely on documents as MIL-HDBK-217 [10] to estimate reliability properties of on-board equipment, especially of the electronic one. Even if they have been strongly criticized by the U.S. National Academy of Sciences due to their inaccuracies and deficiencies, they are still used in different commercial and military avionic applications [11]. A complete RAMS estimation method has been developed at Polytechnic of Turin, by Prof. Sergio Chiesa and described in [12]. Such a method defines the reliability of conventional aircraft subsystems (such as structure, engines and on-board systems) using a top-down approach. In particular, it uses statistical data of conventional aircraft to evaluate their failure rate. Afterwards, by means of subsystems weights, it defines the failure rate for each one of them, allowing the estimation of their reliability. Based on this work, a novel RAMS estimation method has been developed [13], which has updated the one proposed by Chiesa by including a selection of new technologies, e.g. composite structures and Laminar Flow Wings (LFW). This novel RAMS estimation method addresses also one innovative technology for the on-board system, the EHA, but the approach used to estimate the systems reliability and safety is still based on statistical data of conventional solutions. However, this work represents a relevant attempt towards the evaluation of reliability and safety of innovative on-board systems.

All the techniques and methods just mentioned rely on a document-based approach, which makes difficult and arduous to use the information gained through their analysis to improve system architectures. Furthermore, this kind of approach strongly increases the possibility of human errors. On the contrary, a model-based approach would make development activities easier, enhancing design quality, system specification and communications within the development team [14].

Due to all the benefits of a model-based approach, Joshi *et al.* propose in [15] and [16] the employment of modeling and simulation tools (e.g. Simulink [17] and SCADE [18]) to support activities of system safety analysis as prescribed by the standard ARP 4761 [19]. This approach is called *Model Based Safety Analysis* (MBSA): after FHA and FTA safety analyses are performed, safety requirements are derived and the system is designed. System models and fault models are then developed to support verification activities. However, models can be built not only to support design and verification tasks, but to support also the activities that are traditionally performed by means of a document-based approach: development of system requirements, identification of functions that should be performed by the systems and determination of one ore multiple system architectures. These activities are part of a Systems Engineering process [20] and they can be enhanced whether a model-based approach is adopted. This is the reason why it is expected that Model-Based Systems Engineering (MBSE) will play an increasing role in the practice of Systems Engineering in the next decades [21]. Therefore, many studies have been conducted in the past to integrate RAMS activities in a MBSE approach. Some studies (e.g. [22], [23] and [24]) employ Unified Modeling Language (UML) [25] as standard modeling language. Other kinds of modeling language are also proposed in literature, for instance the Architecture Analysis and Design Language (AADL) [26]. However, the standard modeling language to be used in MBSE activities promoted by the International Council On Systems Engineering (INCOSE) is the System Modeling Language (SysML) [27]. SysML [28] is a general-purpose graphical modelling language, which consists of nine types of diagram to represent the functional behavior and the structure of systems.

SysML is generally employed in the design of conventional and innovative systems, but several works propose the use of this modeling language in safety evaluation activities. The majority of these studies (e.g. [29], [30] and [31]) deals with the generation of FMEA from SysML models. Other works instead focus on the generation of FHA (e.g. [32]) and FTA (e.g. [33], [34] and [35]). Moreover, some papers deal with techniques for reliability assessment, therefore including RBDs (e.g. [36]). It is worth noting that two different approaches are followed by the different studies. All these mentioned studies propose the generation of RAMS techniques from a system model. The functional behavior and the structure of the system are described by SysML models, from which FHA, FTA, FMEA and RBD are generated. Both Brusa *et al.* [32] and Izygon *et al.* [37] instead suggest the development of functional and dysfunctional SysML models, hence entailing a more complete model, and with the advantage of quickly updating the RAMS analyses in case of modifications of the design. Instead of performing the RAMS analyses only

once the design solution is baselined, with this approach these analyses can be performed in the design phase, during which multiple alternative solutions are identified. Results of RAMS evaluations can therefore drive the tradeoff among all the possibilities, together with all the other results of the design process, for instance masses and performance characteristics.

All the studies previously mentioned propose methods for the generation, sometimes automated, of RAMS analyses from SysML models. However, the results of these model-based RAMS methods are in the form of documents, as tables. The aim of the present paper is therefore to propose a different use of SysML diagrams within the RAMS context. Although the focus in this paper is on FHA, FTA, FMEA and RBD, several RAMS analyses can be represented by models, instead of documents, hence entailing advantages as improved communications between system designers and safety experts, re-use of models, less prone to error solutions. Most importantly, the RAMS models can be quickly updated in case some changes of the system architecture are made, for instance when new components are introduced. In this way, a high number of alternative system architectures can be evaluated, as it might happen during the development of a novel solution. Indeed in traditional document-based RAMS, only a limited set of architectures can be assessed. Furthermore, the shift to a model-based solution will facilitate the integration of RAMS within collaborative MDO applications, reducing the communication challenges faced by collaborative development teams [38]. Guidelines about the use of SysML models for reliability and safety analyses are provided in Section II. An application example based on the aileron command of conventional and innovative FCS is described in Section III. The paper demonstrates that this approach allows the fast generation of the four RAMS analyses mentioned before for multiple system architectures. As explained in Section IV, the work here presented forms the basis to perform trade-off evaluations accounting for reliability and safety aspects, and additional performance characteristics (e.g. on-board system masses and efficiencies). The integration of the RAMS discipline in MDO processes is introduced. Section V collects conclusions and outlines further improvements.

II. Model-based representation of RAMS analyses

The present Section poses the guidelines for the development of models for the investigation of four RAMS analyses, namely FHA, FTA, FMEA and RBD. The explanation of all the SysML elements used in the proposed approach is out of the scope of the present paper. However, the Appendix provides an overview on all the SysML elements used in the four analyses. More details on SysML are available in references [14] and [39].

A. Model-based Functional Hazard Analysis

One of the first analyses of the safety assessment process is the FHA. This technique aims at identifying failure modes, severity and risk associated to each system function [40]. This technique is generally adopted during the initial phase of design process when the focus is mainly on the functions that should be performed by the system instead on the components of the system architecture. However, in this initial phase an allocation of functions to system components might be already done, and this information can be utilized in the application of the FHA.

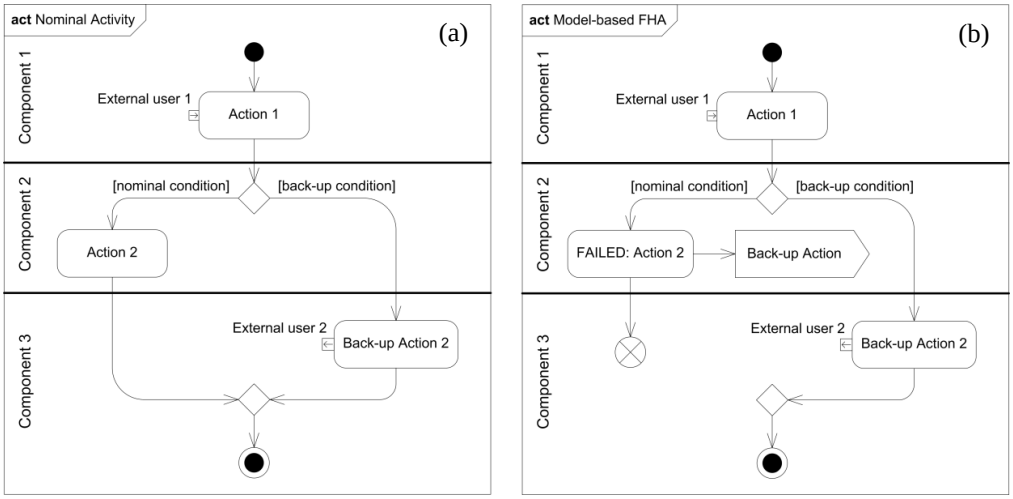


Figure 1 Model-based FHA represented through SysML Activity Diagram, showing functional failures and failure effects. More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

A process based on *SysML Activity* and *Sequence Diagrams* is proposed in [32]. This process is here rearranged and the following steps are proposed to build a model-based FHA. The proposed process employs a *SysML Activity Diagram* showing the functions that should be performed by the system. The diagram is divided in *partitions*, in order to allocate functions to system components. In addition, the functions can represent both the nominal and the off-nominal behavior of the system, as some back-up functions might be included and allocated to redundant components. The safety process continues with the assessment of each function. Functional failure modes are identified for each function, and consequences are investigated. This step is supported by the *Activity Diagram*: each function represented in the diagram might bring to a failure mode, causing and interruption to the sequent part of the functional branch, bringing in some cases to a stop of the entire activity. The *Activity Diagram* represented in Figure 1 (a) represents the functional behavior of a system, i.e. all the actions that the system should perform. The model-based FHA is instead represented by the *Activity Diagram* of Figure 1 (b), where a functional failure entails an interruption to part of the functional flow. The *send signal action* can be used to represent the effect of the functional failure mode.

B. Model-based Fault Tree Analysis

A deductive top-down method for the analysis of system faults is represented by the FTA [41]. All the possible causes (e.g. component failures) that originate a top event as a system-level fault are traditionally assessed through Boolean logic gates in a Fault Tree like the one depicted in Figure 2 (a). Different SysML diagrams are used in literature to generate FTAs, as *Internal Block Diagrams* in [34] and *State Machine Diagrams* in [37].

The model-based version of the traditional Fault Tree peculiar of this analysis and proposed in this work is represented by a *SysML Sequence Diagram*. The top event investigated with the FTA is written in the diagram header. The *Sequence Diagram* includes the *blocks* representing the system components. The SysML *actor* element is employed to represent users and other systems interacting with the system under design. Other SysML elements of the *Sequence Diagram* are used to represent all the information collected in the FTA, although this paper is limited to only two types of Boolean logic gate: *and – or*. Figure 2 shows both a traditional Fault Tree and a model-based FTA embodied by a *Sequence Diagram*. The interaction operator *alt* is used to represent the logic gate *or*, while the logic gate *and* is represented by the interaction operator *par*. The *guard* that is generally used to specify the condition of the operands is used now to define all the events of the Fault Tree. Since the interaction operator *par* is not characterized by guards, a third type of interaction operator (*opt*) can be introduced to specify the events linked to the Boolean logic gate *and*. It is worth noting that the proposed approach based on the *Sequence Diagram* contains more information than the traditional Fault Tree. In particular, the interactions among the system components and users can be represented inside the three types of interaction operator. Hence, it is clear which interactions cannot happen during the different failure events. This additional information can be helpful for the engineers during the safety assessment.

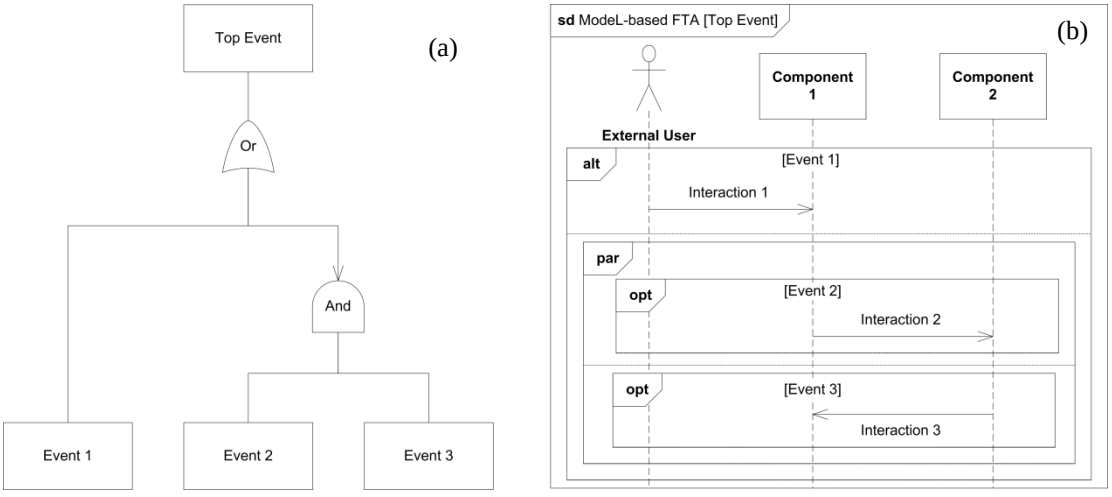


Figure 2 Traditional FTA (a) model-based FTA (b). The SysML Sequence Diagram (b) represents events and Boolean logic gates as shown in the Fault Tree (a). More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

C. Model-based Failure Modes and Effects Analysis

Another analysis of the safety assessment process is the FMEA [42]. The aim of this technique is the identification of potential failure modes of all the components of a system and the assessment of their causes and effects. Traditionally, this analysis is document-based since it results in a table. The most interesting proposal about the generation of a FMEA from a model is suggested by David *et al.* [29]. This proposal is based on a Dysfunctional Behavior Database (DBD) represented through a *SysML Block Definition Diagram* that shows all the failure modes of several system components. This database model is built on the basis of the experience of the safety expert. The authors then suggest the use of *Internal Block Diagrams* to highlight the connections between all the system components. These connections are employed to assess the effects in case of failure modes propagation. This information together with failure modes collected in the DBD are sufficient to set up a FMEA, although other diagrams can be used, e.g. *Sequence* and *Parametric Diagrams*. This approach is very convenient in case the user wishes to automatically generate FMEA from a system model. However, the automatic generation of RAMS analysis is out of the scope of the present paper.

Therefore, a different approach based on a model represented by only *SysML State Machine Diagrams* is suggested in this work. These kinds of diagram represent different *states* of the system or its components. *States* can be nominal but also off-nominal conditions. Therefore, failure modes that are collected in a FMEA are represented by means of *states*. In this case, *terminate pseudostate nodes* are connected to failure states to terminate the behavior of the state machine. The causes that entail the transition from one state to another one are represented by *Triggers*. In case of change from a nominal condition to a failure mode, *triggers* represent failure causes. Eventually, *send signal nodes* are linked to the failure state to identify its effects. It is worth noting that the presence of a *terminate pseudostate node* and *send signal nodes* distinguishes nominal states from failure states. Figure 3 collects all the elements of the *State Machine Diagram* that represent the most relevant information generally included in a FMEA table. However, the proposed model doesn't represent other details that can be part of a FMEA, for example the severity of the failure.

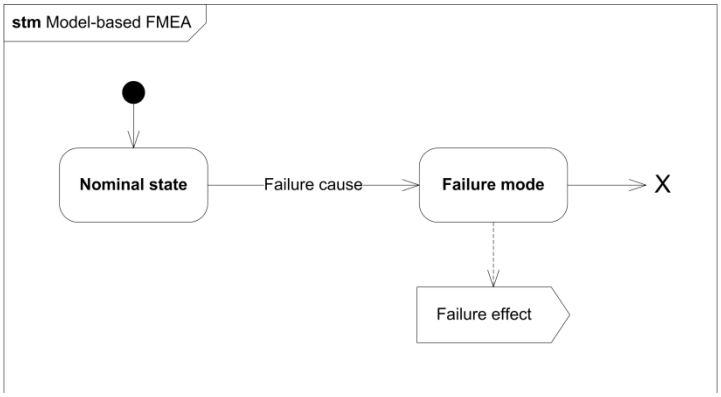


Figure 3 Model-based FMEA represented through SysML State Machine Diagram, showing failure modes, causes and effects. More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

D. Model-based Reliability Block Diagram

The fourth technique investigated in the present paper is the RBD, which is used to evaluate the reliability of a system [43]. Liu *et al.* [36] suggest the use of *Internal Block Diagrams* for the generation of RBDs. Since this SysML diagram is the most appropriate for the evaluation of system components, the approach proposed in this paper is based on this kind of representation. However, the aim here is not to extract an RBD from an *Internal Block Diagram*, but to model the system reliability by means the SysML diagram. Figure 4 (a) shows a traditional RBD of a generic system made of six components. Each block contains the reliability value of each component. The *Internal Block Diagram* depicted in Figure 4 (b) is generated from the RBD by representing all the components as *parts*, and for each of them specifying the *value* "reliability". The *Internal Block Diagram* shows also the connections among all the *parts*, defining groups of components in parallel and in series. It can be noted that *Component 5* represents a component which is outside the system under design. However, the system reliability might be affected by it, and thus it must be included in the diagram. *Component 5* is therefore represented in the *Internal Block Diagram* as a *Reference element* (see the dashed boundary).

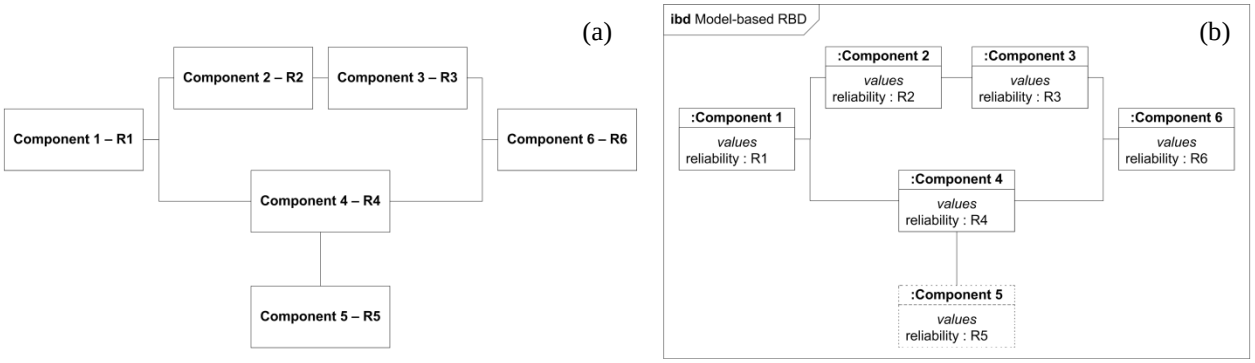


Figure 4 Traditional RBD (a) and model-based RBD (b). The SysML blocks in (b) report the reliability values of the system components. More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

III. Example of application of the proposed guidelines

The guidelines proposed in Section II are applied for the safety and reliability assessment of two architectures of a FCS. Due to the extent and complexity of a RAMS evaluation of an entire on-board system, the application case described in this Section is simplified with the introduction of some assumptions. The main assumption is relative to the scope of the application case: only the aileron command is evaluated and not the entire system. Other minor assumptions will be provided below.

The aircraft selected as reference for the application is an Airbus A320, since some data is available in literature (e.g. [44]). The first system architecture evaluated in this Section is the conventional one. Figure 5 (a) shows the schema of the whole conventional FCS. All the control surfaces are moved by hydraulic actuators, which are supplied by three hydraulic circuits: "Blue" (B), "Green" (G), and "Yellow" (Y). In particular, each one of the two ailerons is moved by two hydraulic linear actuators. One actuator is always active, while the other one is in stand-by mode and used only in case of failure of the main actuator. The second architecture considered in this study is a "more-electric" one, and it is schematized in Figure 5 (b). The proposed solution is similar to the one installed on the Airbus A380, as described in Section I. In this innovative architecture, the "Blue" hydraulic circuit is removed and replaced by an electric line. As assumption, only a single electric line is installed in place of the hydraulic circuit, although the solution adopted on the Airbus A380 is characterized by two electric lines. In the case of the ailerons, each of them is again moved by two actuators, one active and the other one in stand-by mode. The active one is a linear hydraulic actuator, while an EHA is selected as redundancy.

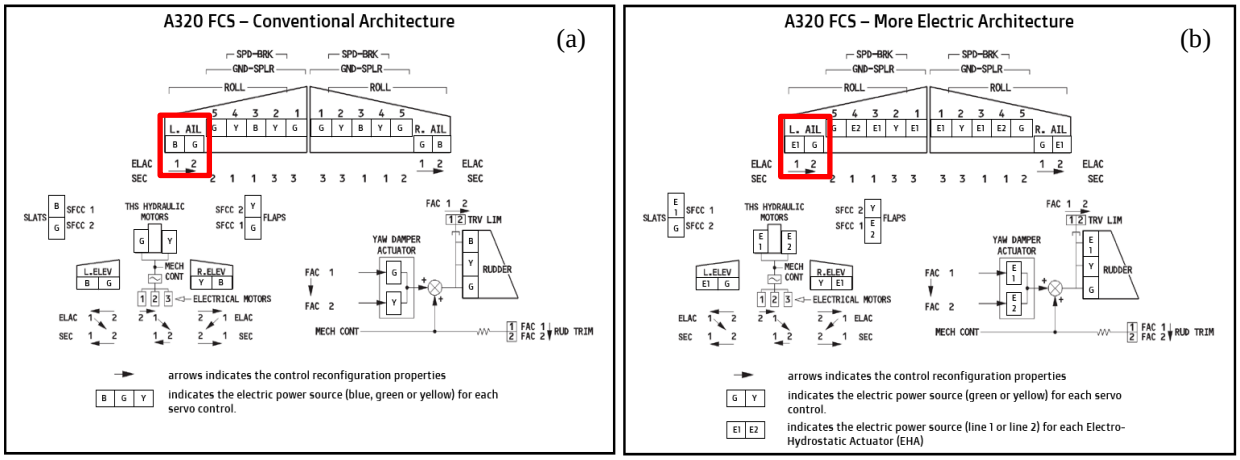


Figure 5 Schema of A320 FCS: conventional architecture [44] (a) and more-electric architecture (b). The present application focuses on the left aileron (highlighted in red).

Since this Section aims at presenting an example of application of the proposed RAMS model, the reference system is here simplified. The reason of this choice is to limit the size and complexity of the RAMS model, since otherwise it might affect the clarity of the proposed example. The following assumptions are identified:

- The roll command is given only by the pilot. Co-pilot or auto-pilot commands are not considered in the application case.
- Only a single ELAC is considered in the system. Actually, two ELACs are installed for safety purposes. In addition, the ELAC should be connected with the Avionic System, since it receives information about the aircraft and flight needed to command the actuators. However, this connection is not considered in the present use case.
- Actuators and aileron position feedback is not considered.

By adopting all these assumptions, a simplified version of the conventional architecture is represented by the *Internal Block Diagram* of Figure 6 (b). A similar diagram is derived to represent the more-electric system architecture, as shown in Figure 6 (c). In this case, the back-up hydraulic actuator is replaced with an innovative EHA, which is supplied by the electric system.

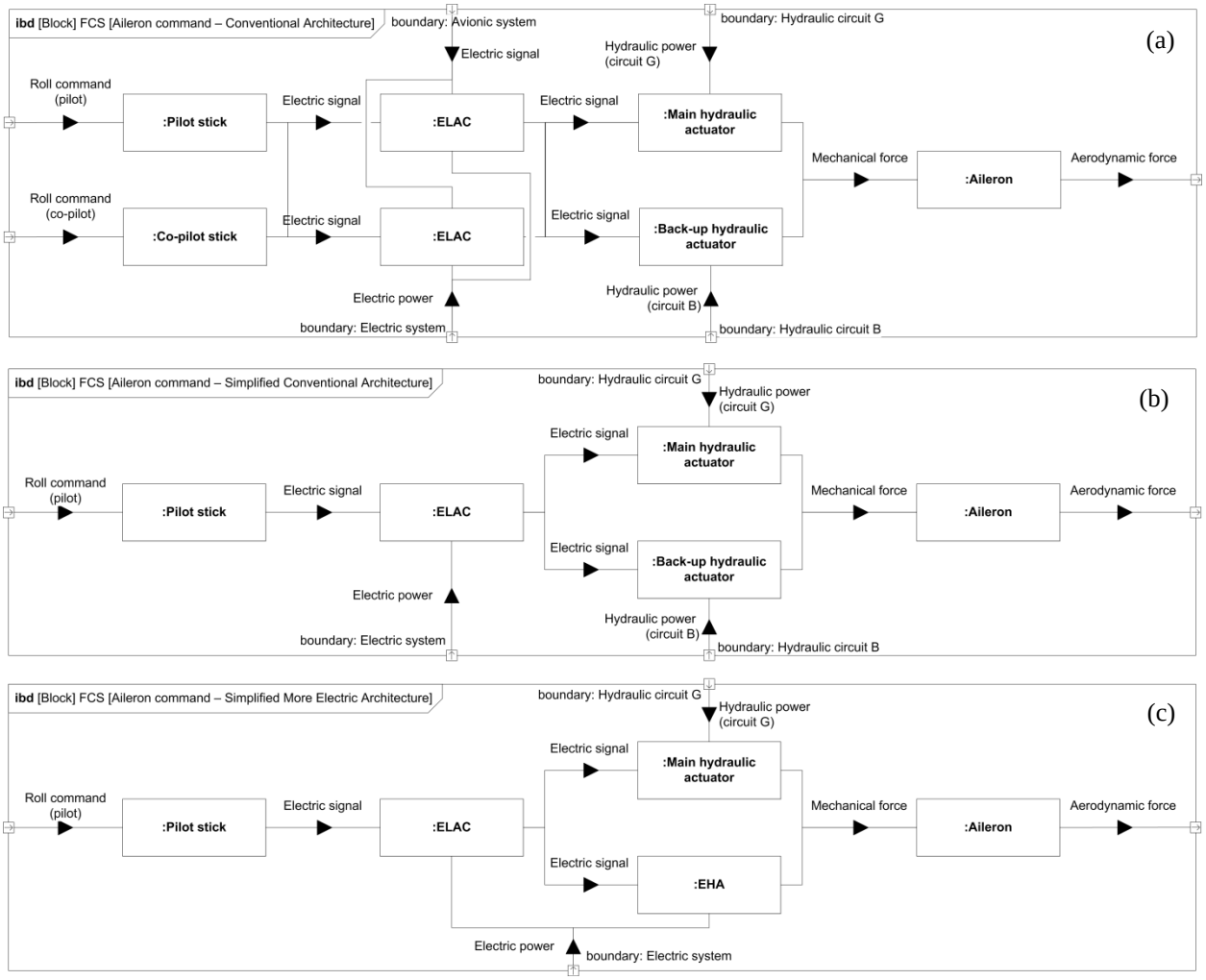


Figure 6 SysML Internal Block Diagrams representing aileron command: conventional (a), simplified conventional (b) and simplified more-electric (c) system architectures. More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

The description about the functioning of the system can be also provided through a model. The *Sequence Diagram* of Figure 7 shows the interactions between components and users of the conventional system. It is worth

noting that the diagram shows *nominal behavior* – i.e. the main actuator moves the aileron – and *off-nominal behavior*, i.e. in case the redundant actuator is utilized.

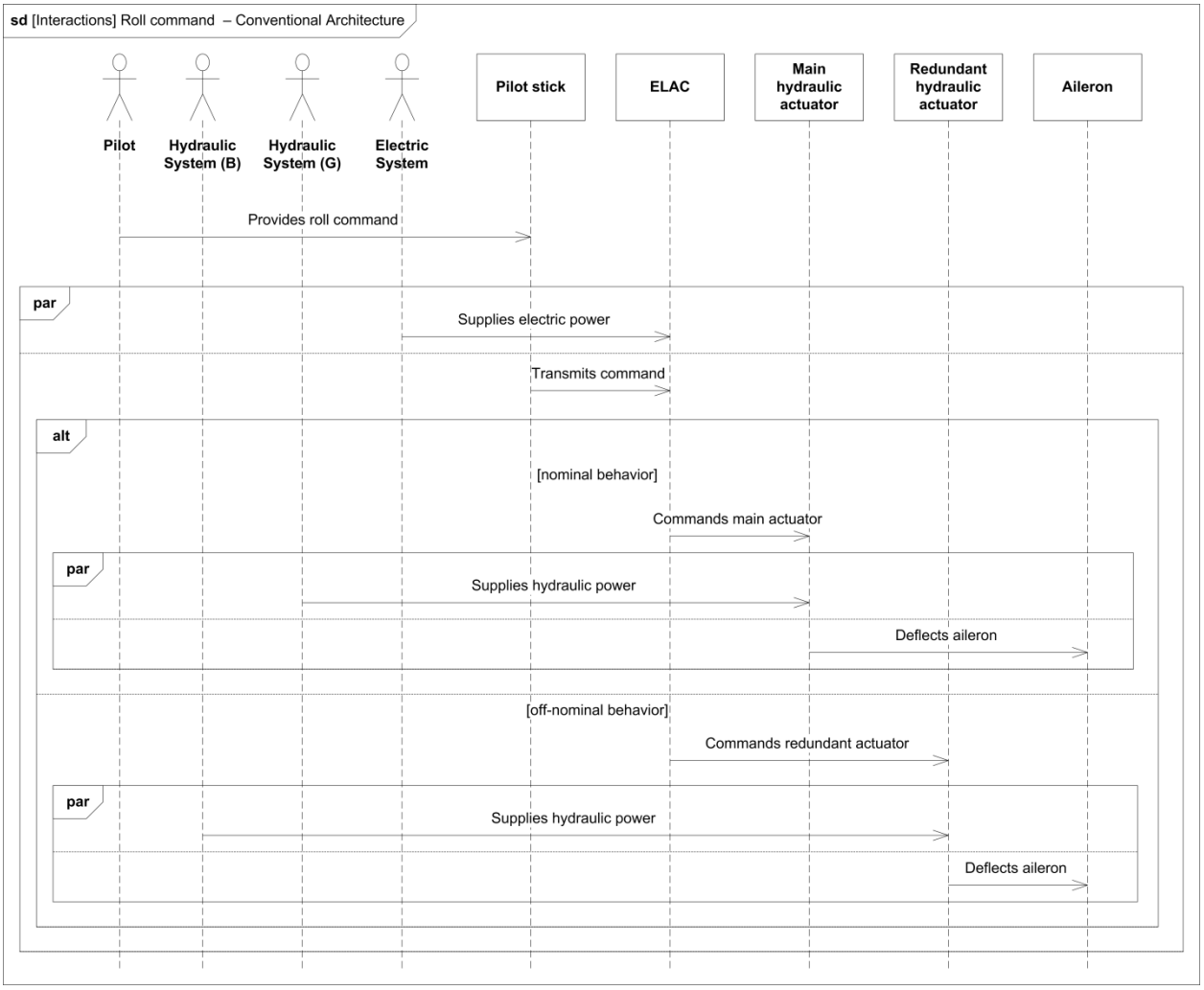


Figure 7 SysML Sequence Diagram representing the interactions among users and system components of the simplified conventional architecture. More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

The system model represents the starting point for the RAMS evaluation by means of the proposed model-based approach. The four analyses explained in Section II are applied and described in the following subsections.

A. Model-based Functional Hazard Analysis – Aileron command

Figure 8 shows three *Activity Diagrams* representing the model-based FHA. Figure 8 (a) collects the functions performed by the conventional system. All the system main functions are allocated to the different components. The reader can note the presence of a conditional element, which directs the flow of functions from the main actuator to its redundancy, in case of failure. The same *Activity Diagram* can be re-used to show what happens in case of a functional failure. Figure 8 (b) depicts the event of functional failure involving the function associated to the main actuator. The corresponding branch of the *Activity Diagram* is interrupted and as a consequence the alternative function is performed by the system. The same happens in case of innovative architecture (Figure 8 (c)), where instead the same back-up function is allocated to a different component.

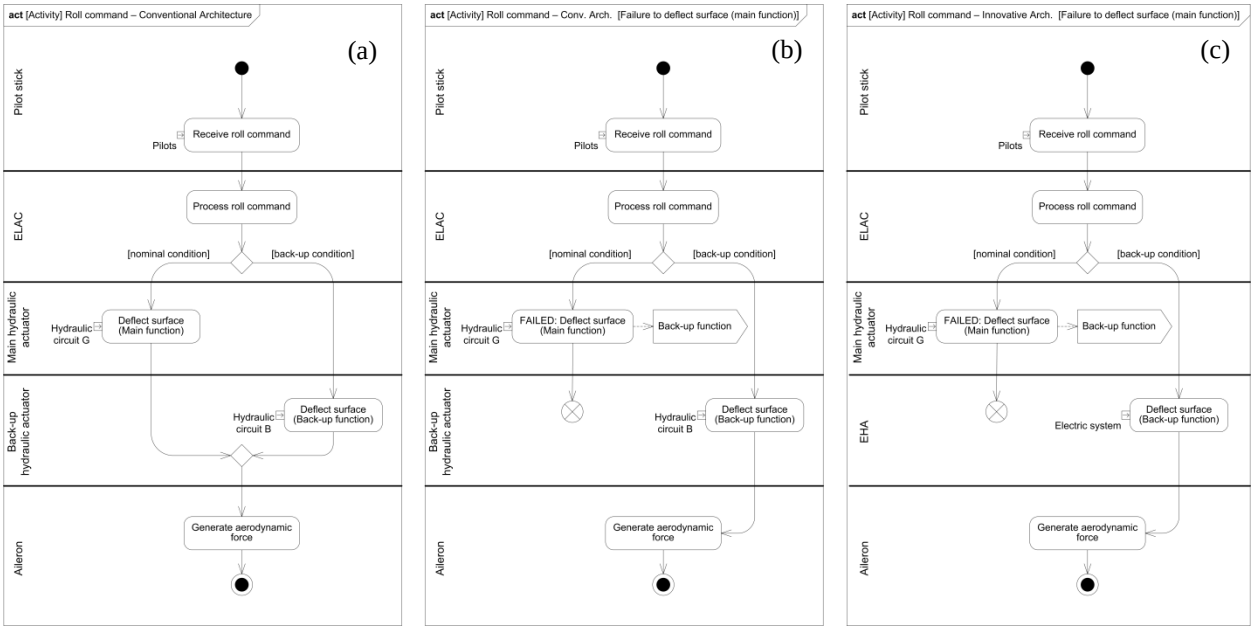


Figure 8 SysML Activity Diagrams representing system nominal functions (a), model-based FHA applied to a simplified conventional (b) and more-electric system architecture (c). More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

B. Model-based Fault Tree Analysis – Aileron command

The RAMS assessment of the aileron command proceeds with the FTA. Figure 9 depicts the Fault Tree of the conventional system. The identified top event is the not deflection of the aileron. This failure happens if at least one of following conditions occurs:

- The pilot stick cannot transmit the electric signal.
- Issues affect the ELAC, i.e. it doesn't receive power from the electric system or it results in failure mode.
- Both the actuators have a failure, which can be a generic issue (in this case *the actuator is broken*) or a more specific low pressure problem affecting the hydraulic circuit.

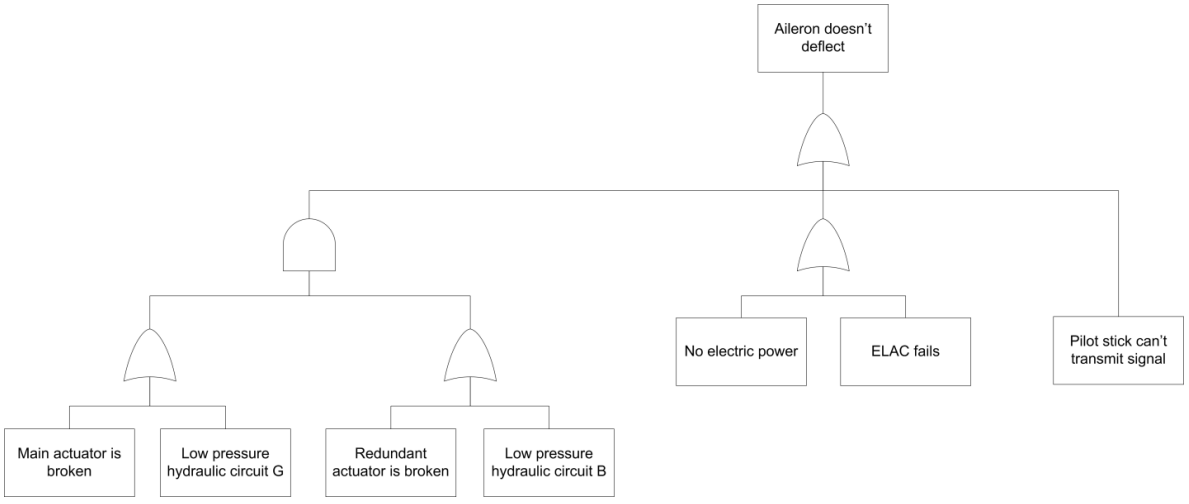


Figure 9 Traditional FTA applied to a simplified conventional system architecture.

The same Fault Tree of Figure 9 can be modeled and represented through a *Sequence Diagram*, where the Boolean logic gate *or* is represented by the interaction operator *alt* and the Boolean logic gate *and* is represented by

the interaction operator *par*. This *Sequence Diagram* is shown in Figure 10 (a). The same diagram shows the interactions of Figure 9, but in this diagram they are all considered as failed interactions. The *Sequence Diagram* can be re-used to realize the model-based FTA of the more-electric architecture, as shown in Figure 10 (b). The actor *Hydraulics System (B)* is removed and the block *Redundant hydraulic actuator* is replaced by *EHA*. The final part of the diagram is slightly modified, since a change in failure event is introduced: in the case of innovative architecture, the events *EHA is broken* and *No electric power to EHA* are considered. The modifications of the FTA of the more-electric architecture are highlighted in red.

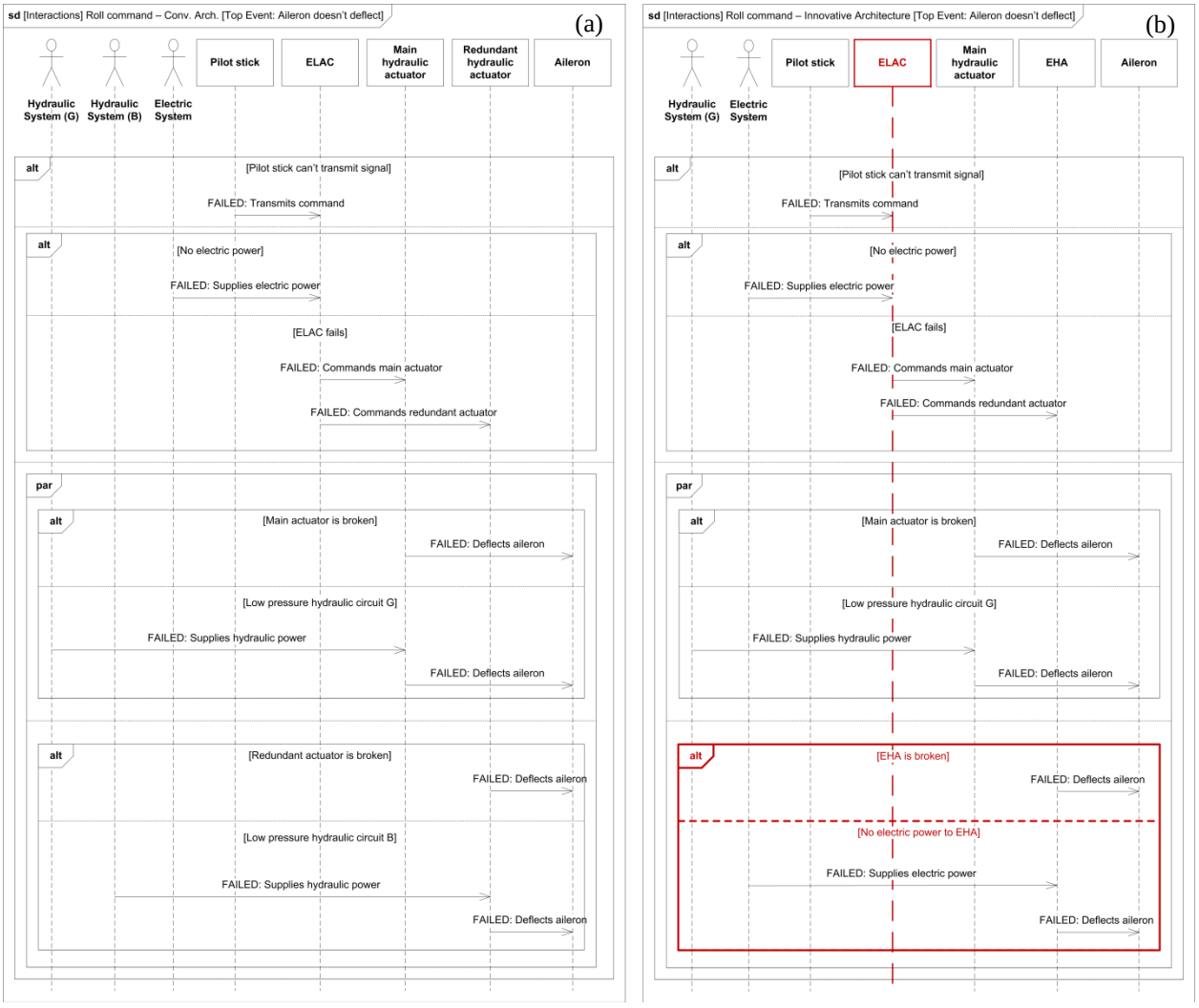


Figure 10 SysML Sequence Diagram representing the model-based FTA applied to simplified conventional (a) and more-electric (b) system architectures. More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

C. Model-based Failure Modes and Effects Analysis – Aileron command

The following RAMS assessment is the FMEA. In this application case, two components are evaluated. The former is the hydraulic actuator, which is installed in both the conventional and more-electric architectures. The latter is the EHA, which is peculiar of only the innovative solution. The two *State Machine Diagrams* of Figure 11 show the failure modes, their causes and their effects. Both the actuators can fail and change their status to *damping mode*. As a consequence, they wouldn't be able to actuate the ailerons. However, two different causes can bring to this failure condition. In the case of hydraulic actuator, a low pressure in the hydraulic circuit might cause the failure, while in case of the EHA, a shortage of electric power would entail the fail state.

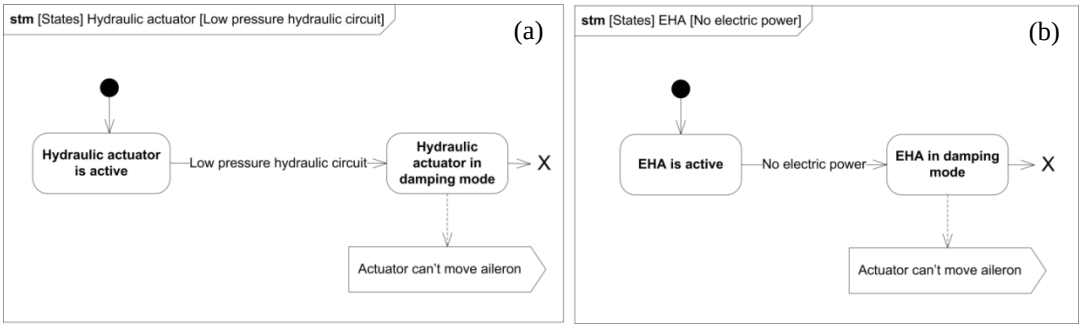


Figure 11 SysML State Machine Diagram representing the model-based FMEA applied to a simplified conventional (a) and more-electric system architecture (b). More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

D. Model-based Reliability Block Diagram – Aileron command

The RAMS analysis of the proposed use case ends with the reliability evaluation. The guidelines proposed in Section II are applied for the study of the present application case. Figure 12 shows the model-based RBD of the conventional and more-electric system architectures. The two diagrams are similar to the ones of Figure 6 (b) and (c), with the addition of the value *reliability*. Moreover, the components belonging to interface systems – namely the hydraulic and electric systems – are represented as *Reference elements*, since characterized by a reliability value.

The main difference between the two diagrams is represented by the redundant actuator. The hydraulic actuator installed in the conventional solution and the EHA of the more electric architecture are characterized by a different value of reliability. Furthermore, the removal of the hydraulic line B changes the system reliability of the innovative alternative.

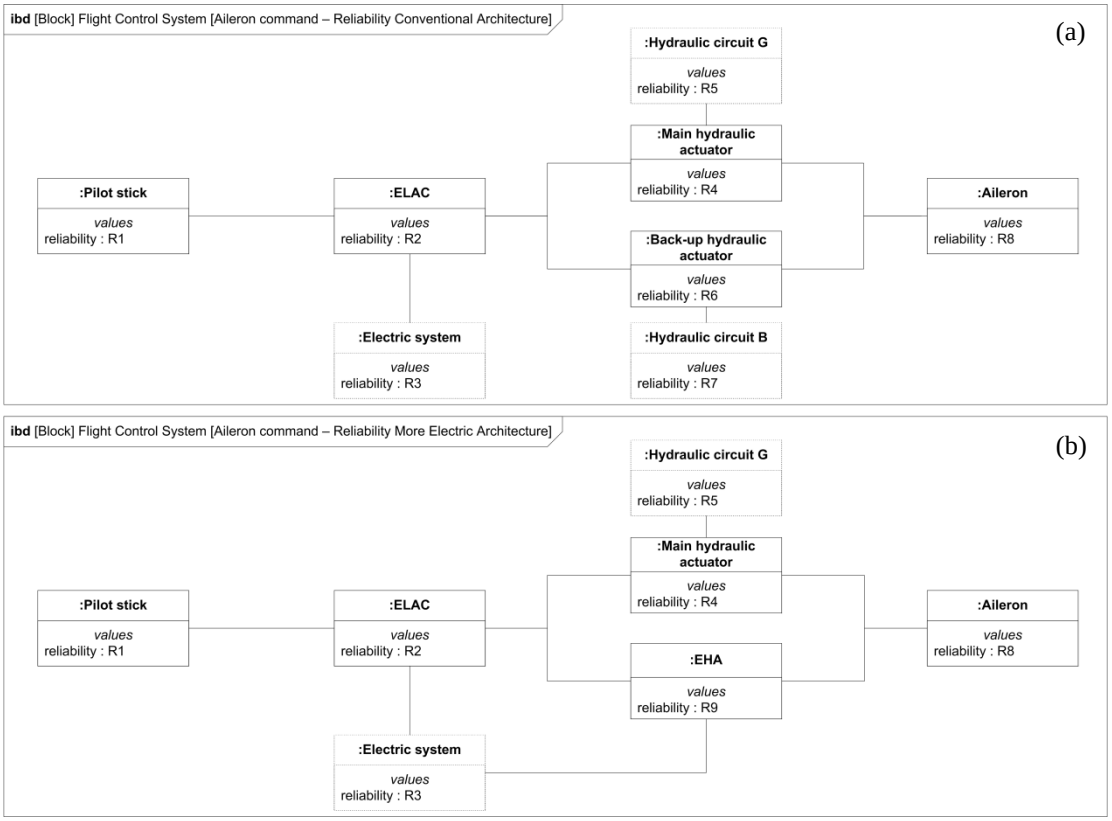


Figure 12 SysML Block Definition Diagrams representing the model-based RBD applied to a simplified conventional (a) and more-electric system architecture (b). More information about the employed SysML elements are reported in the Appendix and in references [15] and [40].

E. Advantages of the model-based RAMS

The application described in the present Section proves that the model-based version of the RAMS analysis has the following advantages over the document-based approach:

- The safety and reliability models can be re-used to quickly model and evaluate alternative architectures. In this specific case, only two architectures are considered, but many more alternative solutions can be identified and assessed. This advantage gains importance and relevance for the selection of the system architecture, since the RAMS analyses are used in a trade-off study together with other system performance, e.g. masses and efficiencies.
- The communication and understanding between the teams involved in the development is improved and facilitated.
- Reliability and safety models can be queried, to check completeness, consistencies and to verify the system solution against the RAMS requirements and constraints.
- In the case of the FHA, since the *Activity Diagram* represents the functional model of the system, all the functional failures can be considered, without neglecting anyone. Moreover, the diagram supports the identification of effects in case of functional failure.
- The *Sequence Diagram* of the model-based FTA contains more information of the traditional Fault Tree. In particular, all the actions that can't be performed in case of failure events are included in the model.
- The *State Machine Diagram* used to represent the model of the FMEA can be simulated to predict the system behavior in case of malfunctioning.
- The model used to represent the RBD is more intuitive of the traditional technique, since it can be extracted from the *Internal Block Diagram* representing all the system components and their connections.

IV. Towards Integration of the RAMS discipline in a MDO processes: EU-H2020 AGILE 4.0 project

Section III has demonstrated the advantages of adopting a model-based approach for the evaluation of the reliability and safety of multiple on-board system architectures. However, RAMS is only one of the multiple disciplines involved during the development of an aircraft. Several disciplinary results other than reliability and safety should be evaluated in a trade-off study. For instance a trade-off for the design and optimization of aircraft systems has to account for subsystem masses, bleed air and shaft power off-takes, fuel weight, equipment volumes and relative installation constrains. Therefore, a multidisciplinary approach for the simultaneous assessment of all these disciplinary results is needed. Such a trade-off study is among the ones envisioned within the EU funded project H2020 AGILE 4.0 [45]. AGILE4.0 project is a follow up of the EU funded project AGILE [46], which has proved to accelerate the deployment of large-scale collaborative MDO processes, as shown in [47], [48] and [49].

AGILE 4.0 project (September 2019 – August 2022) targets the digital transformation of the main pillars of the aeronautical supply-chain: design, production, certification and manufacturing [50]. The project leverages a MBSE approach to MDO for development of complex products, described in [51], and extends it to model, assess, and optimize complex systems addressing the entire life cycle. The technologies developed will enable stakeholders and actors of the aeronautical supply chain to perform trade-off studies which have never been possible to model before. The impact of AGILE 4.0 is to bring significant reductions in aircraft development costs and time-to-market through the implementation of an integrated cyber-physical aeronautical supply chain, thereby leading to innovative and more sustainable aircraft products.

One of the use cases tackled during the project specifically investigates on different conventional and innovative on-board system architectures. The models representing all these system architectures are built. The models proposed in the paper are included to evaluate RAMS characteristics, and MDO workflows are generated and executed to eventually identify the optimal on-board systems solution. The main goal of this use case is to include RAMS analyses in MDO processes. In this way, the optimal solution wouldn't be determined only by aircraft and on-board systems performance, but also by reliability and safety characteristics. This aspect is important since it means taking into account certification requirements and constraints from the beginning of the aircraft development process. Anticipating the certification process during the design phases when the main design decisions are taken would entail future changes to the baseline, which would entail high modification costs, delays and the determination of a not-optimal solution.

V. Conclusions

The transition from a document to a model-based approach is one of the most relevant enablers to develop the next generation of aerospace systems. Several studies and research projects focus on the creation and usage of system models due to all the advantages of this approach over a traditional document-based approach. Due to all the claimed advantages, several studies are proposing the adoption of a model-based approach in the context of reliability and safety evaluations. The majority of these studies aims at generating RAMS techniques from system models, but the results are still collected in documents, e.g. tables. This paper instead exploits the MBSA approach for the development of RAMS models. The models and their application proposed in this paper demonstrate several advantages, e.g. better communication and understanding between development teams, more consistent and complete results. Moreover, the reliability and safety models here proposed can be always up-to-date in case of variations of the system architecture, facilitating trade-off studies that include RAMS results.

The proposed approach is still affected by some limitations, as highlighted in the previous Sections. Therefore, other studies should be conducted to improve and expand this work. In particular, two main research topics are identified to exploit the proposed approach. First, additional reliability and safety techniques can be modeled, since the proposed model-based approach addresses only four RAMS analyses. Second, the integration of the RAMS models within MDO processes can be addressed to simultaneously and automatically trade-off reliability and safety characteristics with other system performance. Future works of the authors will proceed towards this second direction within the context of AGILE 4.0.

Appendix

The most important SysML elements used in the proposed model-based RAMS analyses are collected in the following tables. The OMG's SysML version 1.4 [39] has been used as reference standard. The description of each element is adapted from [14].

A. Activity Diagram

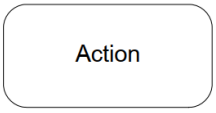
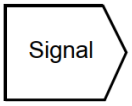
Diagram Element	Notation	Description
Action		It represents and action performed by the system during the activity. It is characterized by inputs and outputs. A sequence of actions defines a functional flow.
Partition		A set of activity nodes can be grouped into an activity partition (also known as a swim-lane) that is used to indicate responsibility for execution of those nodes.
Send signal Action		An activity can send signals using a send signal action.

Table 1 Main elements of the SysML Activity Diagram [14] used for the model-based RAMS analyses.

B. Internal Block Diagram

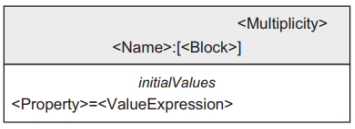
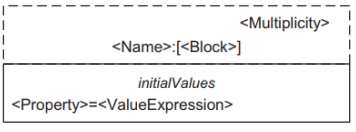
Diagram Element	Notation	Description
Part Node		A part is a property of an owning block that is defined (typed) by another block. The part represents a usage of the defined block in the context of the owning block.
Reference Node		A reference property of a block is a reference to another block.

Table 2 Main elements of the SysML Internal Block Diagram [14] used for the model-based RAMS analyses.

C. Sequence Diagram

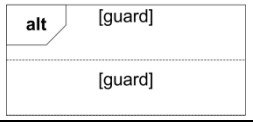
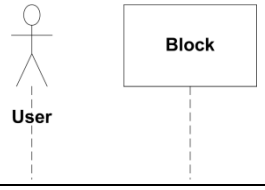
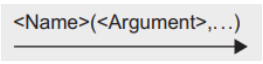
Diagram Element	Notation	Description
Combined fragment		A combined fragment can be used to model complex sequences of messages. This logic of sequence is determined by interaction operator (e.g. *alt*, *par* and *opt*)
Lifeline		A lifeline represents the relevant lifetime of an instance that is part of the interaction's owning block, which will either be represented by a part property or a reference property (e.g. an actor or the component of another system).
Synchronous Message		A synchronous message corresponds to the synchronous invocation of an operation, and is generally accompanied by a reply message.

Table 3 Main elements of the SysML Sequence Diagram [14] used for the model-based RAMS analyses.

D. State Machine Diagram

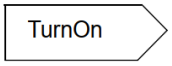
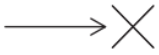
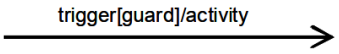
Diagram Element	Notation	Description
Send signal node		This node represents a send signal action. The signal's name, together with any arguments that are being sent, are shown within the symbol.
State		A state represents some significant condition in the life of a block. Each state may have entry and exit behaviors, and a do behavior.
Terminate pseudostate node		If a terminate pseudostate is reached, then the behavior of the statemachine terminates.
Transition		Change events indicate that some condition has been satisfied. The transition can also include a guard and behavior/effect.

Table 4 Main elements of the SysML State Machine Diagram [14] used for the model-based RAMS analyses.

Acknowledgments

The research presented in this paper has been performed in the framework of the AGILE 4.0 project (Towards cyber-physical collaborative aircraft development) and has received funding from the European Union Horizon 2020 Programme under grant agreement n◦ 815122.

References

[1] P. W. Wheeler, J. C. Clare, A. Trentin and S. Bozhko, "An overview of the more electrical aircraft," *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, vol. 227, no. 4, pp. 578-585, 2013.

[2] V. Madonna, P. Giangrande and M. Galea, "Electrical Power Generation in Aircraft: Review, Challenges, and Opportunities," *IEEE Transactions on Transportation Electrification*, vol. 4, no. 3, pp. 646-659, 2018.

[3] J. A. Weimer, "Electrical Power Technology for the More Electric Aircraft," *AIAA/IEEE Digital Avionics Systems Conference*, pp. 445-450, 1993.

[4] J. A. Rosero, J. A. Ortega, E. Aldabas and L. A. Romeral, "Moving Towards a More Electric Aircraft," *IEEE Aerospace and Electronic Systems Magazine*, vol. 22, no. 3, pp. 3-9, 2007.

[5] B. Sarlioglu and C. T. Morris, "More Electric Aircraft: review, Challenges, and Opportunities for Commercial Transport Aircraft," *IEEE transactions on Transportation Electrification*, vol. 1, no. 1, pp. 54-64, 2015.

[6] M. Sinnett, "787 No-Bleed Systems: Saving Fuel and Enhancing Operational Efficiencies," in *Aero Quarterly*, 2007, pp. 6-11.

[7] D. van den Bossche, "The A380 Flight Control Electro-Hydrostatic Actuators, Achievements and Lesson Learnt," in *25th International Congress of the Aeronautical Sciences (ICAS)*, Hamburg (DE), 2006.

[8] J. R. Martins and A. B. Lambe, "Multidisciplinary Design Optimization: A Survey of Architectures," *AIAA journal*, vol. 51, no. 9, pp. 2049-2075, 2013.

[9] E. Zio, F. A. Mengfei, Z. E. Zhiguo and K. A. Rui, "Application of reliability technologies in civil aviation: Lessons learnt and perspectives," *Chinese Journal of Aeronautics*, vol. 32, no. 1, pp. 143-158, 2019.

[10] U.S. Department of Defense, "MIL-HDBK-217F," Washington (DC), 1991.

[11] G. P. Pandian, D. A. Diganta, L. I. Chuan, E. Zio and M. Pecht, "A critique to reliability prediction techniques for avionics applications," *Chinese Journal of Aeronautics*, vol. 31, no. 1, pp. 10-20, 2018.

[12] S. Chiesa, Affidabilità, sicurezza e manutenzione nel progetto di sistemi, Turin (IT): CLUT, 2008.

[13] D. A. Giovingo, "RAMS and Maintenance cost assessment in a Multidisciplinary Design Optimization environment," M.Sc. Thesis, Politecnico di Torino, 2019.

[14] S. Friedenthal, A. Moore and R. Steiner, A Practical Guide to SysML - The Systems Modeling Language, Waltham (US-MA): Elsevier, 2012.

[15] A. Joshi and M. Heimdahl, "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, 2005.

[16] A. Joshi, M. Whalen and M. Heimdahl, "Model-based safety analysis final report," NASA Techreport, 2005.

[17] J. B. Dabney and T. L. Harman, Mastering simulink, Pearson, 2004.

[18] "Scade suite product description," Esterel Technologies, [Online]. Available: https://www.ansys.com/products/embedded-software/ansys-scade-suite. [Accessed 3rd May 2020].

[19] Society of Automotive Engineers (SAE), "ARP-4761–Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," 1996.

[20] International Organization for Standardization, "ISO/IEC 15288 - Systems and Software Engineering - Software Life Cycle Processes," 2002.

[21] A. L. Ramos, J. V. Ferreira and J. Barceló, "Model-Based Systems Engineering: An Emerging Approach for Modern Systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 1, pp. 101-111, 2011.

[22] C. Leangsuksun, H. Song and L. Shen, "Reliability Modeling Using UML," *Software Engineering Research and Practice*, pp. 259-262, 2003.

[23] Z. Pap, I. Majzik, A. Pataricza and A. Szegi, "Methods of checking general safety criteria in UML statechart specifications," *Reliability Engineering & System Safety*, vol. 87, no. 1, pp. 89-107, 2005.

[24] F. Iwu, A. Galloway, J. McDermid and I. Toyn, "Integrating safety and formal analyses using UML and PFS," *Reliability Engineering & System Safety*, vol. 92, no. 2, pp. 156-170, 2007.

[25] Object Management Group (OMG), "Unified Modeling Language (UML)," [Online]. Available: https://www.omg.org/spec/UML/About-UML/.

[26] A. Joshi, S. Vestal and P. Binns, "Automatic generation of static fault trees from AADL models," in *DSN Workshop on Architecting Dependable Systems*, vol. 10, Berlin (DE), Springer, 2007.

[27] INCOSE, Systems Engineering Handbook v.3, 2006.

[28] Object Management Group (OMG), "System Modeling Language (SysML)," [Online]. Available: https://www.omg.org/spec/SysML/About-SysML/.

[29] P. David, V. Idasiak and F. Kratz, "Reliability study of complex physical systems using SysML," *Reliability Engineering & System Safety*, vol. 95, no. 4, pp. 431-450, 2010.

[30] F. Mhenni, J. Y. Choley and N. Nguyen, "Extended mechatronic systems architecture modeling with SysML for enhanced safety analysis," in *IEEE International Systems Conference Proceedings*, 2014.

[31] M. Hecht and D. Baum, "Use of SysML for the creation of FMEAs for Reliability, Safety, and Cybersecurity for Critical Infrastructure," *INCOSE International Symposium*, vol. 29, no. 1, pp. 145-158, 2019.

[32] E. Brusa, D. Ferretto, C. Stigliani and C. Pessa, "A model based approach to design for reliability and safety of critical aeronautic systems," in *Proceedings of INCOSE Conference on System Engineering*, Turin (IT), 2016.

[33] A. H. de Andrade Melani and G. F. de Souza, "Obtaining Fault Trees Through SysML Diagrams: A MBSE Approach for Reliability Analysis," 2002.

[34] F. Mhenni, N. Nguyen and J. Choley, "Automatic Fault Tree Generation From SysML System Models," in *IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM)*, Besançon (FR), 2014.

[35] J. Xiang, K. Yanoo, Y. Maeno and K. Tadano, "Automatic synthesis of static fault trees from system models," *Fifth International Conference on Secure Software Integration and Reliability Improvement. IEEE*, pp. 127-136, 2011.

[36] X. Liu, Z. Wang, Y. Ren and L. Liu, "Modeling method of SysML-based reliability block diagram," *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC) - IEEE*, pp. 206-209, 2013.

[37] M. Izygon, H. Wagner, S. Okon, L. Wang, M. Sargusingh and J. Evans, "Facilitating R&M in spaceflight systems with MBSE," *Annual Reliability and Maintainability Symposium (RAMS)* , pp. 1-6, 2016.

[38] P. D. Ciampa and B. Nagel, "AGILE Paradigm: the next generation of collaborative development in aeronautical systems," *Progress in Aerospace Sciences, (Accepted for publication)*, 2020.

[39] Object Management Group (OMG), "OMG Systems Modeling Language (OMG SysML™) - Version 1.4," 2015.

[40] P. J. Wilkinson and T. P. Kelly, "Functional hazard analysis for highly integrated aerospace systems," 1998.

[41] C. A. Ericson, Hazard analysis techniques for system safety, John Wiley & Sons, 2015.

[42] U.S. Department of Defense, "MIL-STD-1629A," Washigton (DC), 1980.

[43] M. Rausand and A. Høyland, System reliability theory: models, statistical methods, and applications (Vol. 396), John Wiley & Sons, 2003.

[44] "Airbus A319-320-321 [Flight Controls]," [Online]. Available: http://www.smartcockpit.com/aircraft-ressources/A319-320-321-Flight_Controls.html. [Accessed 1st April 2020].

[45] AGILE 4.0 Project Consortium, "AGILE 4.0 - Towards cyber-physical collaborative aircraft development," [Online]. Available: https://www.agile4.eu/. [Accessed 1st April 2020].

[46] "AGILE Aircraft 3rd Generation MDO for Innovative Collaboration of Heterogeneous Teams of Experts," [Online]. Available: http://www.agile-project.eu. [Accessed 2019 March 12].

[47] P. D. Ciampa and B. Nagel, "AGILE the Next Generation of Collaborative MDO: Achievements and Open Challenges," in *AIAA Aviation Forum*, Atlanta (GA), 2018.

[48] P. D. Ciampa and et al., "Streamlining Cross-Organizational Aircraft Development: Results from the AGILE Project," in *AIAA Aviation Forum*, Dallas (TX), 2019.

[49] M. Fioriti, L. Boggero, P. S. Prakasha, A. Mirzoyan, B. Aigner and K. Anisimov, "Multidisciplinary Aircraft integration within a collaborative and distributed Design framework using the AGILE paradigm," *Progress in Aerospace Sciences, (Accepted for publication)*, 2020.

[50] EC INEA Agency, AGILE 4.0 Project Consortium, "Grant Agreement Number 815122 - AGILE 4.0," 2019.

[51] P. D. Ciampa, G. La Rocca and B. Nagel, "A MBSE Approach to MDAO Systems for the Development of Complex Products," in *AIAA Aviation Forum*, Reno (NV), 2020.

[52] J. E. Penner, D. Lister, D. Griggs and D. D. MacFarland, "Aviation and the Global Atmosphere, Intergovernmental Panel on Climate Change Special Report," 1999.