Digital Twin: towards the integration between System Design and RAMS assessment through the Model–Based Systems Engineering

Digital Twin: towards the integration between System Design and RAMS assessment through the Model–Based Systems Engineering

Eugenio Brusa

***Abstract*—The design of a safety-critical system requires an effective prediction of its reliability, availability, maintainability and safety (RAMS). Anticipating the RAMS analysis at the concept design helps the designer in the trade-off of the system architecture and technologies, reduces cost of product development and the time to market. This action is rather difficult, because the RAMS analysis deals with the hazard assessment of system components, whose abstraction at concept level is never simple. Therefore, to integrate the system design and RAMS assessment, a clear path to follow is required. The paper investigates how the Model Based Systems Engineering (MBSE) supports this task and drives the system reliability allocation, through the functional and dysfunctional analyses. The implementation of the proposed approach needs to set up the tool chain. In the industrial context it must be compatible with practices, standards and tools currently used in product development. Defining a suitable process of integration of tools used for the System Design and the Safety Engineering is a need of industry. Therefore, this task is also discussed, in this paper, dealing with some examples of industrial test cases.**

***Index Terms*— Model-Based System Engineering (MBSE), RAMS analysis, Model-Based Safety Assessment (MBSA), Aircraft systems, Structural mechatronics.**

I. Introduction

THE development of a safety-critical system is based on an effective prediction of its reliability, availability, maintainability and safety, in operation (briefly RAMS) [1]. This is a crucial analysis within the whole Product Lifecycle Development, and it needs applying both some qualitative and quantitative approaches. Qualitative evaluations are performed in the concept design, when a preliminary layout of the system is defined [2]. Quantitative metrics are applied, to compute some numerical figures, as the design synthesis is drawn, and the technological issues are assessed [3]. Those analyses are usually performed only once that the product has been defined, in terms of architecture, components and materials. This leads to perform the Safety Assessment [4], which requires to evaluate the reliability of system, subsystems and components. This approach is practical, but it fully integrates the safety analysis, just after that the trade–off of technologies has been completed. Several authors claim that it might be late. The resulting design synthesis could be either poorly effective, because of a lack of information about the system failures, or at least more expensive, when failures are considered, and some refinements of RAMS requirements are needed [5].

In system design, a holistic approach is currently applied, since it is developed through the requirement, functional and physical analyses. It is based on the Systems Engineering [6]. The RAMS analysis resorts to some typical tools, as the Fault Tree Analysis (FTA) and the Failure Mode Effect and Cause Analysis (FMECA) [2]. They predict and classify the system failures, once that subsystems and components have been selected or designed. A challenging issue currently explored in the literature consists in anticipating the RAMS analysis at the concept design, as a part of the Model Based approach [7,8]. This solution allows exploiting the RAMS analysis in the trade-off of the system layout and technologies. How this action can be effectively performed is still matter of investigation. Allocating the safety and reliability requirements to system components needs a suitable action of abstraction, in the concept design, which is never simple, since some typical reliability figures are associated only to physical components. Nevertheless, a sort of analogy between the MBSE approach and the RAMS analysis allows to proceed gradually, and with an increasing level of details. It can help in anticipating those tasks to the early concept design and to the system trade-off, as is herein described.

II. Goals

In many applications, dealing with the industrial systems design and manufacturing, through material processing and component assembling, defining a suitable procedure to effectively integrate the design activity with the safety assessment is more difficult than in case of software engineering. This topic is here analyzed by investigating the beneficial role of the Systems Engineering. A key activity consists in performing a combined functional and dysfunctional analysis, to predict the system behavior in both regular operation, without evident failures, and in presence of faults. Some issues must be considered:

- how the dysfunctional analysis is performed and made compatible with the functional one? (method)
- which steps must be implemented and which tools are required to complete this task? (process)
- how practically this process can be set-up? Is it required to

Eugenio Brusa is with the *Department of Mechanical and Aerospace Engineering (DIMEAS) Politecnico di Torino,* Corso Duca degli Abruzzi 24, 10129, Turin, Italy eugenio.brusa@polito.it

add in the tool chain a specific link to the RAMS software tools, or the heterogeneous simulation proposed by the MBSE can include the RAMS tasks? (tool chain and implementation).

An effective concept design, in the early stage of the product lifecycle development, allows reducing the time to market and the intrinsic cost of a recursive assessment. It decreases the number of iterations required to optimize the product, often through an expensive prototyping and testing [9]. Exploiting a smart reuse of digital models of the product [6] surely helps, but even integrating the RAMS activities in early stage of design improves the performance of the whole process. Those issues are considered in this discussion.

Three industrial test cases are exploited, as practical examples to show the reader how concepts are implemented. A first one analyzes the central maintenance system (CMS) applied to the aircraft fuel system. It consists of a diagnostic electronic unit applied to the distribution of fuel to engines in the aircraft, and includes two main subsystems, consisting of the CMS avionics and the electromechanical system [10]. A second example belongs the structural mechatronics. It is a rotor on active magnetic suspension, used, for instance in steelmaking, to create the coils of steel wire rod. Despite the innovative technology, it exhibits a simple layout, composed by a horizontal and holed shaft, fed by an electric motor, and magnetically suspended by one thrust and two radial bearings, which shapes the incoming wire [11]. A third one is the aircraft de-icing system, which might be based either on pressurized boots distributed along the aerodynamic surfaces and fed by the air coming from the engines, or on some electric resistors, embedded in correspondence of those surfaces, and fed by current [12]. They are all safety critical systems, subjected to some specific technical standards, and enclosed in the heterogeneous simulation, aimed at coupling the functional to the numerical (in the MBSE 'physical') modeling [6].

III. The RAMS approaches

A. The RAMS assessment performed "a posteriori"

A typical approach proposed in the literature consists of defining the system architecture, by tentatively selecting the real components and subsystems to be used, according to a main list of requirements [2]. This activity refers either to a real selection of existing commercial components or to the design of new ones. Once that the activity has been performed, the system is assessed. To identify the failure modes and the real system RAMS, its structure is represented as a tree of elements, either connected in series or in parallel [3]. Some numerical indexes, as the failure probability, the failure rate, the mean time to failure (MTTF), and between failures (MTBF), and the mean time to repair (MTTR) are then associated to each element. This allows performing a number of analyses, aimed at defining the reliability and safety profile of the system. To design the maintenance operation, the FMECA is exploited to fill some tables. In those tables, the possible occurring faults are foreseen and written, for each element of the system. Particularly, the cause, effect and severity of fault are defined. The FTA and FMECA describe the real architecture of the analyzed system, and the failure mechanisms. This approach poorly helps the trade-off activity of system layout, components and technologies [2,4,6,7].

B. The RAMS assessment performed "a priori"

The literature and the technical standards highlighted the need of introducing a correlation between system functions and RAMS issues, since the early concept design [8]. This motivates the introduction of a dysfunctional analysis among the tasks of the V–diagram [4] (Fig.1).

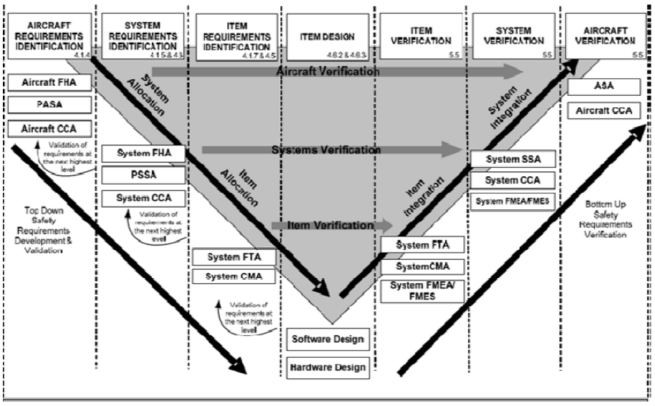

Fig. 1. Description of the Safety assessment within the V-diagram of the Systems Engineering according to the ARP 4754A [4].

According to the technical standard ARP 4754A [4] for aircraft systems, for instance, the safety assessment is based on some actions. The so-called Functional Hazard Analysis (FHA) identifies for each subsystem dysfunctions, failure modes, severity and risk associated [13]. It allows defining some safety targets, setting the level of severity and the risk compatible with a safe operation of the main system. The Preliminary (PSSA) and the System Safety Assessment (SSA) consist in the integrated RAMS analysis performed at different levels (system, subsystem, component), by means of the FTA and FMECA (or FMEA) tools. Those results converge into a final Safety Assessment, referred as Common Cause Analysis (CCA), including the risk analysis, the Common (Failure) Modes Analysis (CMA), and the Zonal Safety Analysis (ZSA), applied to selected sections of the whole system. The global safety assessment for the aircraft system is finally provided (ASA).

This standard clearly describes the goal of distributing along the Product Life Cycle Development the activities related to the RAMS assessment. The standards do not provide all the details for the implementation. Therefore, every company is prone to proceed with tailoring of the standards. Some examples are documented in the literature, as in case of the IBM Company, dealing with the Agile Systems Engineering [14], or specifically in case of aerospace systems, at Boeing [15], Airbus [16] and Bombardier [17].

IV. Model-Driven approaches to the integration between design and RAMS analysis

The 'a priori' approach looks more useful for the trade-off analysis, although the 'a posteriori' analysis is based on a defined system, whose reliability is better evaluable. To develop the first approach, a suitable implementation within a

real tool chain is required. Several contributions explored this topic in the literature, facing the problem of the integration between system design and safety engineering.

Exploiting the Digital Twin [18] is a current trend of industry, to access to both the functional and numerical models of systems and machines [19]. The MBSE is nowadays often applied. Among the other features, a full traceability, from requirements to the system numbered parts, allows identifying a weak requirement, as soon as a failure occurs.

A tight correlation between the customer needs and RAMS assessment is defined by the "Integrated, Customer Driven, Conceptual Design Method" [20], which resorts to the specific design tool called "Conceptual Failure Mode Analysis" (CFMA). It was conceived to modify the principles of FMEA to be applied to the conceptual design phase [21].

The model–driven approach applied to both the design and safety assessment greatly increases the powerfulness of those methodologies. Particularly, when the physical modelling of the system behaviour is performed, a comparison between the integer system, without faults, and the system operating in presence of some kind of fault, can be made. This leads to complete the dysfunctional analysis [22]. In this case, the analysis assumes that system design parameters are set at nominal values, first, and then introduces either some deterministic or random failures, affecting the values or the logic connections between elements [23]. This approach helps to face the complexity of aerospace systems, for instance, and makes easier the verification and validation process [24].

Considering the three pillars of MBSE, consisting of modelling language, tool and method [25], in the literature above mentioned they have been gradually introduced. The applied method resorts to requirement, functional and physical analyses to perform the product development. The functional modelling exploits several diagrams to describe the system behaviour, architecture and requirements. Those diagrams are represented through a language. The SysML language [25], for instance, allows describing the system architecture by means of the so-called Block Definition Diagram (BDD) and the Internal Block Diagram (IBD), to describe its details [6]. At basic level, those diagrams have been used to derive the FTA and FMEA, since the concept design stage [24]. A deeper use of the SysML language is even based on other diagrams. The Activity (AD), Sequence (SD) and State Charts or Diagrams (StD), are applied [26]. A procedure to connect the SysML diagrams, the FMEA and FTA has been defined by NASA [27]. Several of those contributions define a methodology, but details about the implementation are still poor.

It can be noticed that before the SysML, to integrate the RAMS and MBSE, even the UML has been considered [28]. It is more often applied to the software engineering. In case of mechanical, mechatronic and physical systems, which require the material processing and assembling, the SysML is currently more often used, although several limitations have been already identified, as the lack of a suitable library of reference diagrams and elements, dedicated to the industrial product design [29].

V. Implementation of the model-driven approach with integrated design and RAMS analysis

A roadmap to implement the joint action of predicting the system behavior and performance in terms of RAMS is described by Zhang et al. [30], by highlighting the mutual interaction between RAMS analysis and MBSE. Several tools used in the RAMS analysis are precisely located along the product lifecycle development, but the layout of the tool chain used was not yet disclosed. A clearer view is presented in [31], where a preliminary architecture of tool chain is defined. It consists of a SysML modeling activity applied to the analyzed system, which allows extracting an Internal Block Diagram (IBD), and then the StD and AD, useful to start a RAMS analysis in Altarica® [32]. A comprehensive approach was implemented by Cressant et al. [33], by introducing the MeDISIS process. It really improved the known approaches by reaching three targets. A first integration between the safety analysis and the MBSE is done, since the SysML modeler works together with the RAMS tools. The dysfunctional analysis is operated within the physical modeling, as a task of the Simulink® modeling. Some actions are performed, starting with a failure mode analysis, following with the reliability scenario, and leading to final simulation. The authors even tested the interoperability of selected tools [34]. Another example of tool chain is proposed in [35]. The dysfunctional analysis is there performed by modeling the system by means of AADL, Altarica®, eventB®, Safety Architect® and Safety Designer®. In all those valuable contributions, a deep analysis of the tools integration is performed, although generalizing a tool independent process looks still difficult.

In the recent literature, the concept of Model Based Safety Analysis (MBSA) has been successfully introduced [36] to perform a multi-level safety analysis, which recursively assesses the system design, by resorting to either the language UML or SysML. The tool suite is specifically exploited, and is integrated within the Papyrus UML/SysML modeler, to support the FTA, FMEA and hazard analysis. This is a key reference for the implementation even in other tool chains, as those considered in the industrial examples herein described.

A major issue in industrial product development is the integration of the Model Based Safety Analysis within an existing tool chain [37]. In this case, the sequence of functional, logical and physical analyses includes a preliminary non-functional analysis, aimed at defining some safety objectives and to perform the RAMS analysis. The ARCADIA approach is implemented within the Melody Advance/Capella system manager tool. Particularly, the architecture frameworks are used to describe the space system behavior and architecture, and then failures modes are foreseen and injected inside the system model. Similarly, that approach can be introduced even when a process model is exploited, as the V-diagram, more than the architecture frameworks, as in present study.

VI. The role of the Systems Engineering in the RAMS analysis

To clarify the role of the Systems Engineering, it is useful remarking that it is based on some pillars, as Delligatti defines [25]. It is a model-based approach in opposition to the document-based one. Modelling languages, methods and tools

are all relevant elements. In the context of industrial product development, this interpretation is more generalized [6]. The Systems Engineering supports the designer with a methodology including a process, to define what must be done along the product life cycle development, and a method, which introduces how the actions foreseen within the process can be performed [9]. A well-known example of process is the IBM Harmony© [38], which defines the structured sequence of steps and investigations, to define the system behaviour and architecture, once that requirements have been identified. The process resorts then to engineering methods, theoretical and software tools. A language supports their implementation. In industry, the infrastructure of tool chain and of data management system is even a critical issue. The data storage, exchange between tools and repositories, and the interoperability of tools need all to be designed, assured and tested. Therefore in following sections the contribution of the Model-Based approach, driven by the Systems Engineering is described.

VII. The Proposed Approach: Method

A. *Analogy between functional and dysfunctional analysis*

A first clear roadmap to effectively integrate the system design and the safety assessment is needed. To perform the functional and dysfunctional analyses, during the concept design, a useful analogy can be applied. It identifies steps and artifacts of the system development and of its safety assessment. This analogy is sketched in Fig.2. It might give answer to the first question of Section II, about the method.

The requirement analysis allocates customer needs to requirements, and a list of requirements is produced [6]. The functional analysis allocates requirements to functions, and their description populates the Functional Breakdown Structure of system (FBS). Those functions are then allocated by the logical analysis upon logical components and subsystems, i.e. on elements not yet corresponding to selected physical products, but characterized by some defined technological properties and functions, able to perform some required actions. The corresponding artifact is the Logic Breakdown Structure of system (LBS), describing the system logical architecture. The final step is allocating that layout to real products, identified through some specific properties and label data, by means of the physical analysis, and the corresponding artifact is the Product Breakdown Structure (PBS), leading to the design synthesis.

An analogy with the dysfunctional behavior can be defined. As the functional analysis identifies the system functions, the dysfunctional analysis describes just the system failures. In the example of aeronautic technical standards, this is the Functional Hazard Analysis (FHA) [19], and is just a part of the wider Functional Hazard Assessment [39]. The dysfunctional analysis is an element of the RAMS analysis [40]. Similarly, as the logical components allocate functions, the targets of reliability allocate dysfunctions, i.e. a selected value of reliability identifies the risk associated to each dysfunction. They allow performing the reliability allocation. The prediction of real reliability of the final product is performed as the real components are selected or designed, and their performance is known. Therefore, the digital artifacts in this branch of the sketch are dysfunctions, reliability targets and reliability performances. They correspond, to the sequence of the FBS, LBS and PBS in the opposite branch. Safety requirements are associated to each step of the above described process. As Fig.2 shows, the system picture becomes brighter, and the system reaches a better definition, at the end of this process. Moreover, the prediction of system cost is performed as the product is developed, since the concept design.

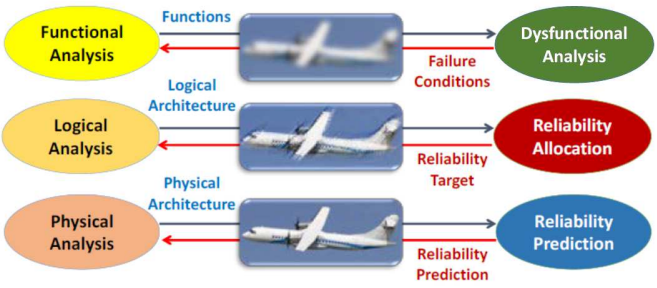

Fig. 2. Comparison between activities and outcomes of the functional and dysfunctional analyses.

B. *Role of logical analysis and reliability allocation*

It is worth noticing that it is still a matter of discussion within the industrial domain whether the LBS is a helpful artifact, or designer can easily pass from the FBS to the PBS [7,9]. The logical analysis is never pleonastic, if the innovation and reliability issues are considered. In terms of design activity, uncoupling the selection of a real product, either designed or available on market, from the technological item, which implements a set of functions, usually helps to identify more possible solutions, and really innovative products [15]. Similarly, defining first a reliability target should help the designer to select the subsystem or component, better than simply verifying whether the reliability associated to a selected device is compatible with the requirements. The difference is appreciated if one compares the software to the hardware design. In case of the software, LBS and PBS are naturally superposed, while in the hardware design they are sufficiently distinguished, to motivate the double step above described.

VIII. The Proposed Approach: Process

In Section II, the steps of process are even identified as an issue of the implementation of the proposed approach. For a practical implementation, the process needs to exploit some tools, and in particular a language. In the technical literature, some languages are used as the UML [28], the SysML [25, 41] or even some newer one as the LML, the AML, and the IML [6]. In the industrial environment, when material processing is performed to manufacture the product, the SysML is currently preferred, because of some useful and available features, as some diagrams, not yet included in the UML. This motivation suggests here resorting to the SysML, although the approach here described will be applicable even in case of use of some newer ones, like the IML. In this section, a preliminary theoretical description of typical activities performed by resorting to the MBSE tools is provided, and then in next

sections an industrial test case will clarify how the tool chain could be updated to implement the approach.

A. *Dysfunctions induced by either inner or outer agents*

To deploy the conceptual failure mode analysis, the dysfunctional analysis starts in parallel with the functional one (Fig.2). If one resorts to the SysML language, after the requirement analysis, summarized by the requirement diagrams, the system behavior is described by the Use Case (UCD), Activity (AD), Sequence (SD), and State Machine (or simply States) Diagrams (StD). Requirements are allocated to functions, use case by use case. The dysfunctional analysis must identify the failure modes, as a lack of system functionality [12]. Single and multiple events are considered. Nominal and degraded environments are compared. The effects of failures are then classified, from catastrophic, when the dysfunction prevents the safe operation of system, to minor or irrelevant. Faults become a reference for the elicitation of specific RAMS requirements. Another issue concerns the severity of faults, which needs to be properly defined, to avoid the introduction of either a poorly meaningful or too stringent requirement.

The UCD, for instance, not only defines the number of use cases to be considered, but even the stakeholders involved. Therefore, it allows screening any failures induced by external agents, or directly by the system itself. It helps in classifying faults either as internal or external. Eventually, new use cases can be defined to deal with the damaged system configuration, and to develop all the diagrams related to a specific failure mode, as is typical in the aircraft design [10].

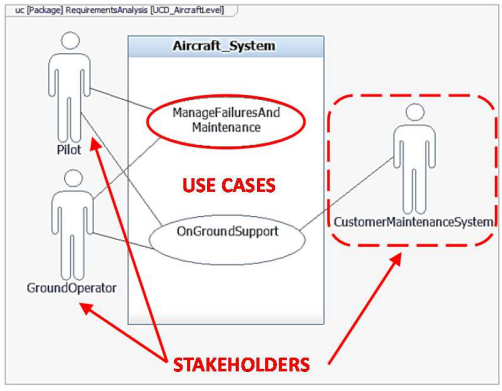

Fig. 3. Example of Use Case Diagram (UCD) related to the aircraft control maintenance applied to the fuel system exploited to define inner and outer fault sources.

In a first test case, for instance, related to the Central Maintenance System (CMS) applied to the aircraft fuel system [10], "managing failures and maintenance" is a specific task defining a new use case, which involves pilots and ground operators, in flight and at ground, and the customer maintenance support at least at ground (Fig.3). A long MTTR can be motivated, not only by an ineffective work of operators (ground and pilots), but even by a late delivery of new components, by the customer service, which does not belong strictly the airport system. That defect of dispatchability is assumed as an externally driven fault [3].

B. *Dysfunctional paths*

Performing the dysfunctional analysis is rather difficult, in complex systems, but this complexity can be decomposed by the MBSE. Particularly, the AD and SD diagrams help the designer in locating and identifying several dysfunctions, just by negating the functions, as is theoretically shown in Fig.4. In practice, the AD describes the system operation, as a tree of actions, performed according to a sequence, by the subsystem analyzed, while interacting with several other ones, being connected through some interfaces ('ports').

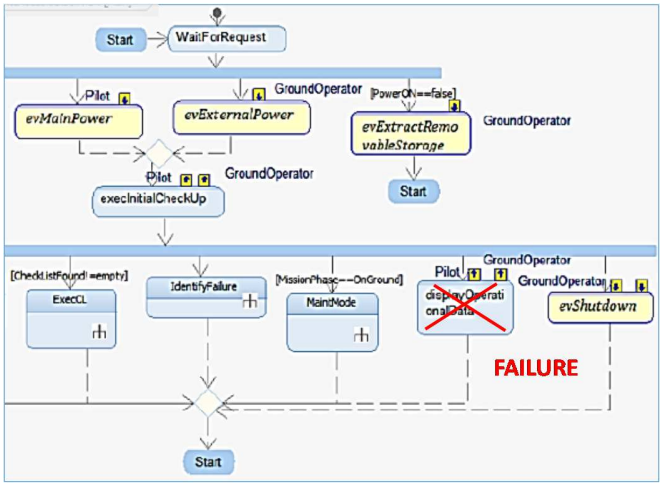

Fig. 4. Example of detail of the Activity Diagram (AD) of a Central Maintenance System of an aircraft with negated display function.

In the example, after the start up required either by the pilot or the ground operator, the CMS performs several checks, and acquires the data to be stored, displayed and communicated. A typical fault could be the absence of display, during the monitoring activity. The AD somehow plays the role of precursor of the Fault Tree, if each function is negated and related consequences are evaluated. Particularly, the designer in this approach:

- finds the whole list of functions to be considered as becoming potentially dysfunctions;
- evaluates the fault paths, through the tree of functions and identifies the related risks;
- realizes where a redundancy is required to assure safety;
- perceives the severity of fault associated to dysfunctions.

The above described analysis focuses on the subsystem monitored, but a clearer vision over the whole system operation is provided by the SD, including the interactions between actors (subsystems and stakeholders), as is theoretically shown in Fig.5. In this case, negating a function allows realizing:

- where and how the process stops;
- how this stop affects the behavior of a selected subsystem, and even of some other ones.

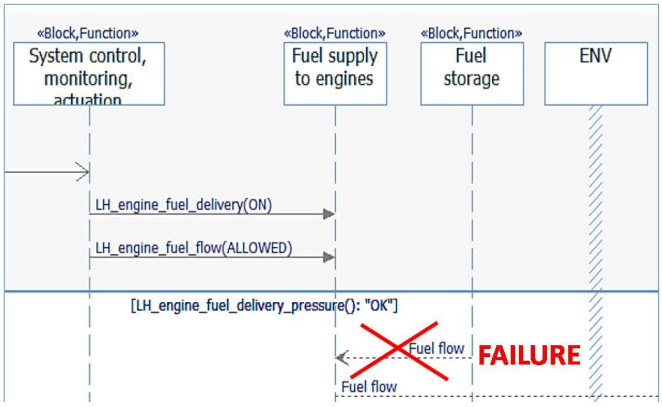

Fig. 5. Example of detail of the Sequence Diagram (SD) of a Fuel System of an aircraft with negated fuel flow function.

The above described analysis allows monitoring the intensity of a dysfunction. In Fig.5, for instance, a failure applied to fuel flow can be associated to a completely inhibited, partial or slow, continuous or never stopping flow. Those detailed cases can be analyzed separately and even more decomposed, when the logical elements performing the function "fuel flow" will be defined, during the logical analysis.

Finally, the StD completes the subsystem analysis. For given fault, the system may be either constrained to keep or to leave the state just reached. An example can be done, considering a second test case, i.e. the rotor supported by active magnetic suspension [10] depicted in Fig.6. If, for instance, the motor is unable to accelerate the shaft across the critical speed, it will remain in the subcritical regime of rotation. Therefore, the self-alignment will not occur, the unbalance response will be greater and more dangerous.

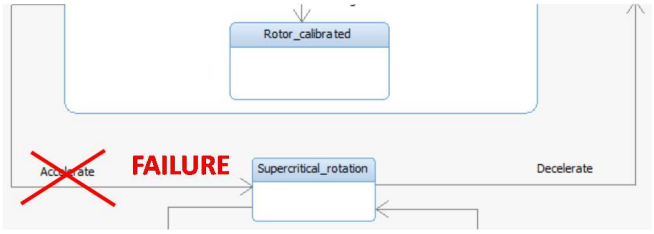

Fig. 6. Example of detail of a State Machine Diagram (StD) of a rotor system on active magnetic suspension.

C. *Reliability targets*

Once that functions and dysfunctions have been defined, to allocate requirements to functions, and then functions to system elements, the system architecture has to be drawn. If the SysML language is used, this is done by composing a preliminary Block Definition Diagram (BDD), with some Internal Block Diagrams (IBD). Those diagrams concur to compose the FBS, i.e. a BDD representing the system layout in terms of functions [6]. The logical analysis allocates the FBS elements to some selected devices, defined in terms of properties and technology, although they are not yet corresponding to some real product. Figure 7 shows an example of the LBS drawn. Despite the inner details of labels, it is evident that each component, identified by the bold label, represents a generic device, not yet a specific product. The LBS includes several details:

- it provides the list of components to which the reliability targets and the RAMS requirements are allocated;
- it defines the device and the technology of each element, but it does not indicate a real product yet.

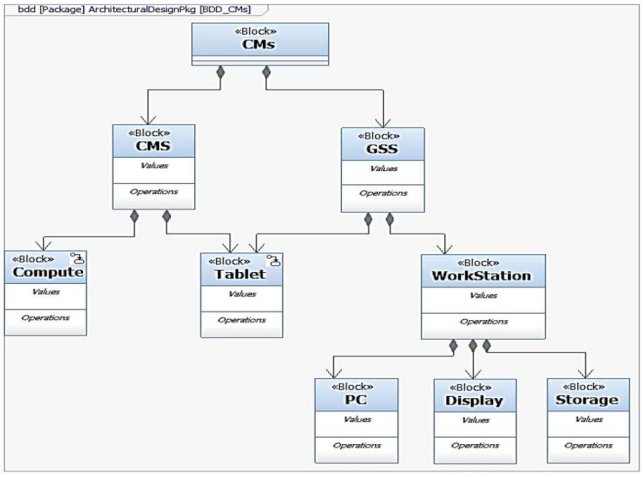

Fig. 7. Example of LBS of the aircraft Central Maintenance System.

The logical analysis allows defining each subsystem, and then a reliability target is tentatively associated. Its compatibility with the logical architecture is then checked. Once that the compatibility has been demonstrated, the designer proceeds with either the design of the selected subsystem, by inputting that reliability target as a requirement, or with the selection of a commercial system, compatible with the defined target.

D. *System reliability and safety assessment*

The last step, to converge towards the design synthesis, consists of the physical analysis. Nowadays, it exploits the heterogeneous simulation, as a tool to combine the functional and physical modeling, respectively [42]. The tool chain set up to perform the heterogeneous simulation includes some software tools, dealing with functional and numerical modelling. Digital models and data are exchanged between software tools, if a good interoperability is assured [12, 42]. As the logical components are allocated to real numbered parts, and the PBS is drawn, the numerical modeling allows evaluating quantitatively the system behavior, and predicting its performance.

The dynamic simulation can help the definition of the product reliability [43]. The LBS elements are allocated to the PBS. This is used to generate a digital model for the numerical analysis. The numerical artifact could be simply a geometric model, describing the real structure and volumes of the analyzed system [44], or a dynamic simulator, suitable to investigate its dynamic behavior [23], for given design parameters, or a structural model, to be used for a stress analysis to predict the material damage [43]. The RAMS assessment can be completed, by performing a first analysis based on a system set up, including all the nominal parameters and functions, corresponding to a regular operation, without fault, and then repeating the analysis, by introducing some dysfunctions, i.e. by modifying the set up suitably to simulate the occurrence of failure in operation [45].

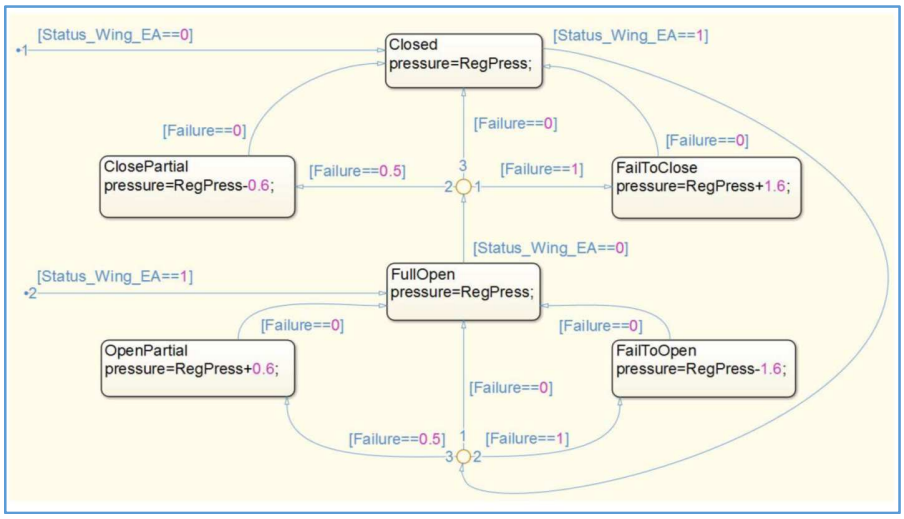

Fig. 8. Example of the Simulink© state flow of the functional and dysfunctional behavior of a dual distribution valve of the aircraft deicing system [45].

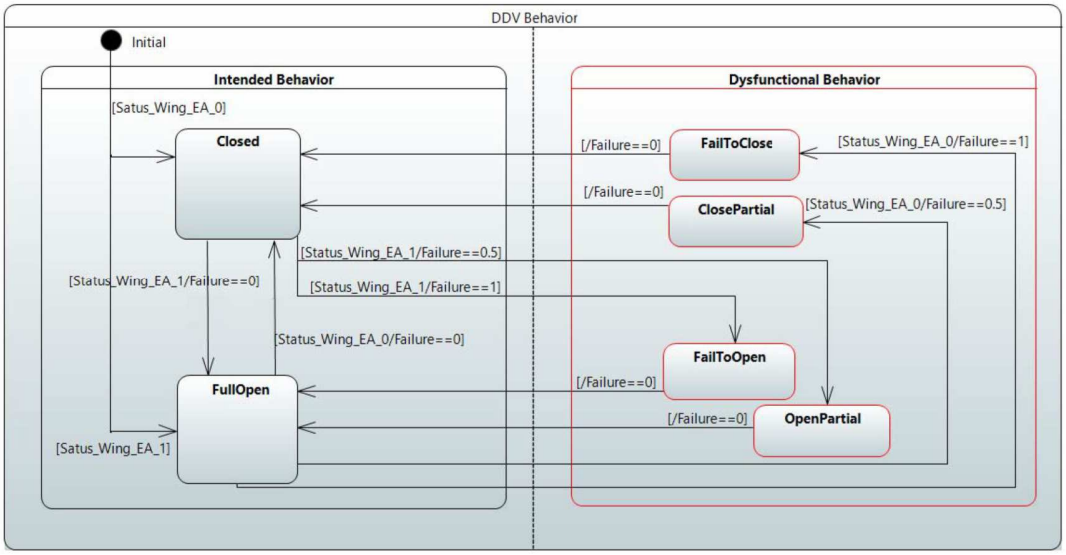

Fig. 9. Example of State Machine Diagram of the dual distribution valve of Fig.8.

The above described activity requires the failure modes analysis of each component of the system. The state flow can describe the coupled functional and dysfunctional behaviors and even provides a synthesis. Figure 8 describes, for instance, the state flow available in the Simulink®. In the test case of the aircraft deicing system, based on some pressurized boots applied to wings and to inlets of propellers, the crucial element is the dual distribution valve (DDV) [45]. It regulates the flow of pressurized air inside the boots, when the deicing action is required, and inhibits the flow, when it must be left in standby. This valve exhibits several failure modes. It might happen that it is unable to open, or to close, or it remains only partially open or close, while it should be either fully open or close. The state flow identifies those conditions and defines the transition between two states. The State Machine Diagram is helpful to draw the state flow (Fig.9).
Those representations are useful to:

- define the failure modes of a specific component of the system layout;
- create a filter for the implementation of dysfunctional analysis into a numerical model, like a dynamic simulator, as is performed, for instance, by the Matlab/Simulink® [45] and Modelica® software [19];
- start the FMEA, to be integrated in the final product description and safety assessment.

IX. The Proposed Approach: Numerical Simulation

The numerical simulation helps in investigating the effect of failures on the system behavior. This implies to set up the simulator to perform the dysfunctional analysis. In the test case of the deicing system with pressurized boots, for instance, after some simulations obtained by setting all the design parameters at nominal values, and assuming that every element works properly, a second set can be obtained, by injecting the failure.

This needs to introduce a dedicated set of blocks inside the model, to implement the options described in Fig.8.

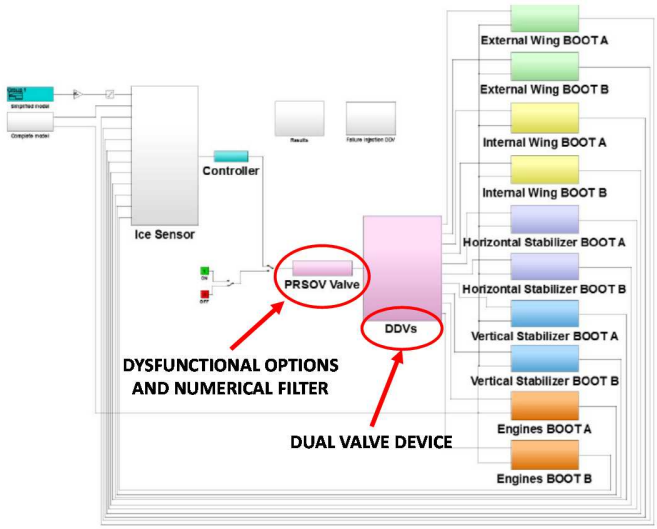

Fig. 10. Example of dynamic simulator of the dual distribution valve in the Simulink® environment.

As Fig.10 shows, it is a sort of numerical filter (PRSOV) applied before the numerical model of the valve, which is the subsystem investigated. The dysfunctional analysis consists in setting step by step all of options available inside the filter to check their effect on the monitored parameter of the digital model of de-icing system.

The options of the dysfunctional block can be activated either by the user, on line or offline, run by run, or automatically set up by programming the code. Numerical results are then used to check the RAMS requirements, refining the system design, in terms of components selection and of redundancy of the system layout.

X. The Proposed Approach: Implementation and Validation

The above described activities define some of the features of the integration between the MBSE and the MBSA. A practical implementation requires to define: context of application, process, tool chain, artifacts and outcomes. To clarify how the proposed approach is applied to an industrial test case, with a product based on material processing and components assembling, the design of the CMS of the aircraft applied to the fuel system will be here described [46].

A. *The industrial context*

The system analyzed is a subsystem of a commercial aircraft, is highly safety critical and its design must fulfill requirements of some technical standards, as the SAE ARP4754 [47] (system design), and the SAE ARP4761 (safety assessment) [48].

The technical domain already applies some consolidated procedures, needs to access to some libraries of products, including the relevant properties of systems, subsystems and components, requires to reuse the digital models of previous versions of the same or similar aircraft, already available, and to exploit the synergy of at least three departments, dealing with aircraft systems design, safety engineering and customer management, with an overall project management and the collaboration of the aircraft design group.

The typical process applied by the manufacturer consists in defining the customer needs and requirements, through the action of the customer management department, performing a preliminary concept design, according to the V-diagram, through the aircraft systems department to have a design synthesis, which is then analyzed by the safety engineering department for the final assessment.

The MBSE is applied and some typical procedures of RAMS analysis are implemented. However, the expressed need is that of performing now the conceptual failure modes analysis of systems since the concept design, and to integrate the tool chains used by the system designers and safety engineers, in accordance with the guidelines of the SAE ARP4754 and SAE ARP4761, and with the ASD S1000D for the aerospace systems [49].

B. *The method*

It has been observed that the system design performed in the test case is compatible with the typical approach of the MBSE, as is described by the left branch of sketch in Fig.2. Particularly, the manufacturer is prone to resort even to the logical analysis, although it was not yet defined in this way. The safety engineering department applies a process which is compatible with the right branch of sketch in Fig.2. Nevertheless, since the activity is usually performed on the designed system, the functional hazard analysis is just followed by the reliability analysis of selected components. A real reliability allocation is not introduced. Therefore, the analogy proposed has been found compatible with the current practices of the Company, and the quality assurance control of processes. Moreover, it allowed defining a clear correspondence of steps and of artifacts between the two parallel paths proposed in Fig.2, by introducing the reliability targets allocation, and helped in setting up the tool chain.

C. *The process*

The process selected by the manufacturer for the integration of system design and safety assessment replicates the standard depicted in Fig.1. The V-diagram is followed in designing the system from the level of the whole aircraft to the components of each subsystem. The safety assessment will be coherently performed. The model based approach will be exploited to anticipate the functional hazard analysis in the product development. To implement this approach, the process described in section VIII fits the exigencies expressed, but needs to be integrated into a tool chain.

D. *The tool chain*

Some constraints have been identified by the manufacturer in the implementation. Particularly, several practices have been already assessed in the past by resorting to some software tools. The proposed approach could be implemented, provided that a compatibility with those constraints could be demonstrated, as is herein described. Moreover, the interoperability among software tools has been defined as a crucial need. It will assure a seamless change configuration management of product [19].

The architecture of the tool chain has been first designed, as in Fig.11. It copes with the need of being compatible with the

current tool chain used by the manufacturer, but even to allow the integration of RAMS analysis, at the early step of system design. A main Product Lifecycle Manager (PLM) is the core of the tool chain. It controls the design activity and manages the connected requirement manager tool and the functional modeler as well as the simulators, exploited to perform a numerical analysis if the system behavior, through a numerical model of the system. It allows transferring data and requirements between levels. Particularly, it provides the allocation of the aircraft requirements and functions to each system, which is herein mainly considered. According to the proposed process the PLM even controls the interface with the RAMS software and the data exchanges with the functional modeler, which implements the MBSE. Finally, the elicitation of safety requirements is performed through the RAMS software and the requirements manager tool. In this case, the choice of interoperating the manager tool, the functional modeler and the RAMS tool was required by the manufacturer, to access easily to previous digital models and to the library of components, although in the literature it was demonstrated that the functional modeler can be directly exploited to perform the safety assessment [36].

In the definition of this architecture the proposed approach suggested the artifacts to be exchanged and elaborated by the different tools, as they are shown in Fig.11 and allowed focusing on the reliability targets and logical components as a key step of the mutual exchange of data between the two integrated analyses.

E. The interoperability of tools

In the test case, the interoperability of tools is crucial to compose the tool chain and to assure a fast data exchange between tools and among the users. It might be observed that tools are often supplied by different vendors. Therefore, in some cases the data exchange is based on proprietary connectors, since the tools are supplied by the same vendor, in other cases they need some additional element, for an effective connection.

In this example, the tasks defined by the standard ARP 4574 are performed by the requirements manager IBM Doors / DNG®, by the functional modeler IBM Rationale Rhapsody® and they are managed by the Product Lifecycle Manager IBM Design Manager®, which deals with the configuration management, and allows the design collaboration among units, through an extension to the IBM Jazz Platform®. All those tools are interfaced by proprietary connectors.

The RAMS analysis, implementing the tasks described by the standard ARP 4761, could be carried out by the Isograph Reliability Work Bench® (RWB). It needs to be connected through the Isograph Data Link Manager® (DLM) to the requirements manager. A possibility to connect this tool to the IBM Rationale Rhapsody® is given by the API connectors, while is more difficult the interoperation with the PLM manager. To overcome this limitation, the Open Services for Lifecycle Collaboration (OSLC) provides some standard connectors [50]. The OSLC initiative allows integrating tools in support of end-to-end lifecycle processes. The IBM Design Manager® is compliant to OSLC specifications. Therefore, a connector reads data from DM® via OLSC, provides them to the RWB® and assures the interface between the RAMS and PLM environments, as shown in Fig.11.

The dynamic simulation of system behavior could be performed in the Simulink®, but it requires to resort to the Functional Mock-up Interface (FMI) for Model Exchange®, by creating a mock-up unit (FMU) inside the numerical model [51]. Particularly, in Simulink® have been implemented the actions described in Fig.8 and Fig.9. By converse, the connection with the dynamic simulator is easier with Modelica®, since some proprietary connectors have been already provided.

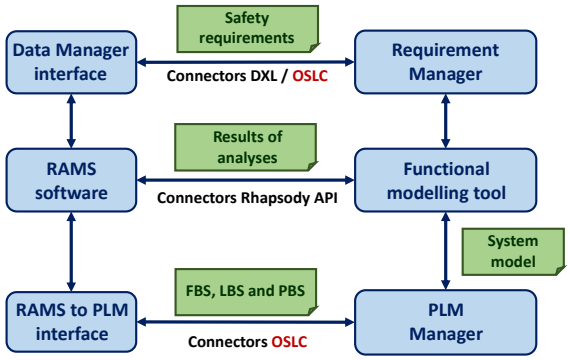

Fig. 11. Example of tool chain designed and tested to model the CMS applied to an aircraft fuel system.

Considering the issue of interoperability, it can be remarked that some solutions already presented in the literature as in [36, 37] are welcome to simplify the integration between the MBSE and the MBSA. It can be also remarked that, as in the test case, when constraints about the design of the tool chain are stringent, the approach here proposed allows identifying a suitable roadmap to set up the integrated tool chain, despite of the need of connections.

F. The procedure

A challenging issue for the validation of the proposed approach is the procedure to perform the MBSE and MBSA, at least for the tasks foreseen by the above mentioned standards applied by the manufacturer. The main data used to perform those analyses consist of the FBS, LBS and PBS, for the functional modeling, and the list of functions affected by failure, allocated failure rate, MTBF, MTTR, part number and logistic control number (LCN) for the dysfunctional modeling.

The process in Fig.2 has been implemented as follows and some benefits of the proposed approach are highlighted.

- Requirement analysis. A preliminary activity of identification of customer needs, and of elicitation of requirements is performed, as in the MBSE, and results are collected and classified in the Requirement Manager (Doors®).
- Functional analysis. The requirements are then allocated to functions, through the functional modeling (Rhapsody®). A first artifact is produced, i.e. the Functional Breakdown Structure is defined. It is transferred to the PLM tool (DM®), as a list of system functions.
- Dysfunctional analysis. The FBS is shared with the RAMS analyser, as a set of functional blocks and structures (RWB, Safety assessment module®), being the starting input for the

dysfunctional analysis. This action allows interfacing the aircraft system designer together with the safety engineer, and to share the system functions, since the concept design stage.
The Functional Hazard Analysis starts. Each function is analysed by the user, the failure condition is associated, the phase of aircraft operation is even described, the effect is foreseen, and the hazard is classified (Fig.12).

Function description	ID	Description	Phase descriptions	Effect description	Classification description
Fuel_Storage	1.1	Fuel Tank Explosion	GROUND TAKE OFF	Total loss of A/C	Catastrophic
Fuel_Storage	1.2	Fuel Leakage from tank	GROUND TAKE OFF	Risk of Fire	Hazardous
Fuel_Storage	1.3	Fuel unbalance (DQ>1000Kg)	FLIGHT LANDING	Loss of A/C control	Catastrophic
Fuel_supply_to_engines	2.1	Loss of fuel flow to both engines	TAKE OFF LANDING	Double engine Flame Out. Uncontrolle...	Catastrophic

Fig. 12. Example of functional hazard analysis performed in the RWB®.

The user associates to each item a safety requirement. Each function is updated, to allocate the safety requirement just defined, and then is transferred back to the functional model (IBM Rhapsody®). In this step, the user can navigate the model and resort to the behavioural diagrams to fill the proposed records of table in Fig.12, as is described in section VIII.
- Logical analysis. Starting from the updated functions and following the process, the Logic Breakdown Structure is defined (Rhapsody®). Logic elements are transferred to the PLM tool (DM®), and then to the RAMS analyser (RWB®), where logic blocks and structures are created.
- Reliability allocation. The RWB Allocation Module® supports the user in allocating the reliability targets to the logic blocks. This action is performed through a table similar to that of Fig.12, where failure rate and MTTF are defined. As it happens for functional blocks, the logic blocks are updated with those reliability targets, transferred to the PLM tool, and then back to the functional modeller (Rhapsody®).
- Physical analysis. The Product Breakdown Structure is defined in the functional modeller (Rhapsody®) by resorting even to numerical simulation and associated models. It is then transferred to the PLM (DM®), as a list of physical elements (logical elements with update and completed properties), and through it to the RAMs analyser (RWB®). The physic blocks and structures contain some numerical properties, and in case of commercial components, the label data.
- Reliability prediction. As physical blocks contain the required information, it is now possible associating a numerical reliability and some maintenance data. This is done by the RWB Prediction module®. The blocks are updated with the part numbers, the Logistic Control Number, Failure Rate (FR), MTTF, MTTR and MTBF, as in Fig.13.
- Design synthesis. The physical blocks, updated with the RAMS details are sent back to the PLM tool and to the functional modeller (Rhapsody®) to complete the architecture of the system, which allocates the requirements.

This test case allowed checking the feasibility of the proposed approach, within the frame of an industrial project for the development of MBSE methodologies [7]. If it is compared to some other solutions, in this case the study faced the problem of managing industrial products, with some crucial issues related to the nature of physical objects. Moreover, it was required to set up an approach which could overcome the limitations due to the specific needs of using some defined software tools and technical standards. This was done and the proposed approach allowed defining the roadmap implemented and described in this section. The main difficulty was found in interoperating several tools. Nevertheless, the FMI for Model Exchange and the OLSC compliant connectors allowed to complete the proposed tasks successfully.

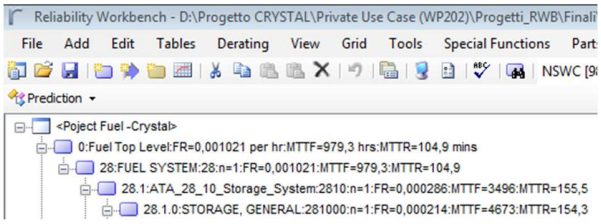

Fig. 13. Example of detail of physical blocks with RAMS parameters in the RWB®.

XI. Conclusion

The concept of Digital Twin is here developed and applied to the industrial product design. The industrial need of applying simultaneously the Model Based Systems Engineering (MBSE) for the system design and the Model Based Safety Assessment motivates this investigation. Anticipating the MBSA at concept level allows reducing the cost and the time of product development and increases the reuse of existing models and products.

A preliminary analysis of the state-of-arts is performed. A general approach is then proposed, to link the system design to the RAMS analysis, since the concept stage of product development. As much as possible the investigation focuses on the approach, more than on the specific features of software tools, currently used in the literature and in industrial practice. The methodology here introduced includes method, process and implementation, based on the heterogonous simulation, and exploits a tool chain of interoperable software. The validation performed on industrial test cases demonstrates the feasibility of the proposed approach. Particularly, in case of existing tool chain, the analogy between the MBSE applied to system design and the Safety Assessment, typical of the RAMS analysis allowed integrating the two environments, merging the functional and dysfunctional analyses, at concept design level. The interoperability of software can be the real obstacle to the effective integration. In the literature, this limitation has been overcome in some cases by resorting only to the MBSE tools to perform even the MBSA. Nevertheless, in the test case here described of a Central Maintenance System applied to the fuel system of a commercial aircraft, using some standard connectors as the FMI and the OLSC, the required interoperability has been reached.

Acknowledgement

This research activity was supported by the ARTEMIS JU project “Critical Systems Engineering Acceleration” under grant agreement 332830 and from the specific national program of funding of the Ministry of Education, University and

Research of the Italian Republic, Fondo Ricerca FIRST, 2012, DR n. 955, 27/12/2012.

REFERENCES

[1] P. O'Connor, *Practical reliability engineering*, Heyden & Son, London, 1981.

[2] C. Wasson, System analysis, design and development: Concepts, principles and practices, (2nd ed.), Wiley, 2015.

[3] S. Chiesa, Affidabilità, sicurezza e manutenzione nel progetto dei sistemi, Clut, Torino (Italy), 2008.

[4] SAE Aerospace, ARP4761: Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, U.S.A., SAE Committee S-18, Society of Automotive Engineers, Inc., 1996.

[5] D.J. Smith, A.H. Badd, Maintainability engineering, Pitman Publishing, 1973.

[6] E. Brusa, A. Calà, D. Ferretto, Systems Engineering and its application to industrial product development, Springer, Cham, Switzerland, 2018.

[7] ARTEMIS Joint Undertaking CRYSTAL Project, http://www.crystal-artemis.eu/ (as is on January 21st, 2020)

[8] SAE Aerospace , ARP4754: Certification Considerations for Highly-Integrated or Complex Aircraft Systems, SAE Systems Integration Requirements Task Group AS-1C, ASD., REV. A, Society of Automotive Engineers, Inc., 2010.

[9] J. Vollmar, "A New Approach to Master Complexity in Model Driven Systems Engineering", Proc. 2nd INCOSE-Italia Conf. on Syst. Eng., Turin, Italy, November 14-16, 2016, Invited talk, pp.121-122, CEUR Workshop Proc.Vol.1728.

[10] C. Pessa, M. Cifaldi, E. Brusa, D. Ferretto, K.M.N Malgieri, N. Viola, "Integration of different MBSE approaches within the design of a control maintenance system applied to the aircraft fuel system", Proc. 2016 IEEE Int. Symp. on Syst. Eng. (ISSE), Edinburgh, Scotland, 2016.

[11] E. Brusa, A. Calà, "Identifying the Smartness of a Mechatronic Coiler through the 'Systems Engineering'", Proc. INCOSE Conf. on Systems Engineering – CIISE 2014, Rome, Italy, November 24-25, 2014, pp.116–125, CEUR Workshop Proceedings, ISSN–1613–0073.

[12] E. Brusa, A. Calà, S. Chiesa, F. De Vita, D. Ferretto, "Towards an effective interoperability of models within the 'Systems Engineering' applied to aeronautics", Proc. INCOSE Conf. on Systems Engineering – CIISE 2014, Rome, Italy, November 24-25, 2014, pp.38–47, CEUR Workshop Proceedings, ISSN–1613–0073.

[13] T.P. Kelly, P.J. Wilkinson, "Functional hazard analysis for highly integrated aerospace systems", in Certification of ground/air Systems seminars, IEE, 255, 1998.

[14] B. Powel Douglass, Agile Systems Engineering, Kauffmann, 2015.

[15] E. Carrillo de Albornoz-Braojos, B. Figlar, R. Gomez, G. Kawiecki, "Developing Airplane Systems Faster and with Higher Quality through Model-Based Engineering", Boeing Research & Technology, Europe, available on line (May 20th 2020) at https://www.boeing.com/features/innovation-quarterly/may2017/feature-technical-model-based-engineering.page.

[16] R.A. Sharples, "Continuous Model Based System Engineering (MBSE) Improvement via Human System Integration and Customer Change" in W. Karwowski and T. Ahram (eds.), Intelligent Human Systems Integration, Springer, 2018. AIRBUS

[17] M. Chami, P. Oggier, O. Naas, M. Heinz, "MBSE at Bombardier Transportation", Proc. SWISSED 2015, September 2015, Zurich, Switzerland.

[18] E. Negri, L. Fumagalli, M. Macchi, "A review of the roles of Digital Twin in CPS-based production systems", Proc. 27th Int. Conf. on Flexible Automation and Intelligent Manufacturing (FAIM), 27-30 June 2017, Modena, Italy.

[19] G. Bachelor, E. Brusa, D. Ferretto, A. Mitschke, "Model Based Design of complex aeronautical systems through Digital Twin and Thread concepts", IEEE Systems Journal doi:10.1109/JSYST.2019.2925627, on line since 2019.

[20] A. Hari, M.P. Weiss, "Failure Mode Analysis in the concept stage eliminates failures before reaching the customers", Proc. ICED 99, 12th Int.Conf. on Eng. Design, Munich, Germany, August 1999

[21] M.P. Weiss, A. Hari, "Extension of the Pahl & Beitz systematic method for conceptual design of a new product", Procedia CIRP 36 (2015), 254–260.

[22] A. Garro, A. Tundis, "A Model-Based method for System Reliability Analysis", Proc. Symp. on Theory of Modeling and Simulation (TMS), SpringSim 2012, Orlando, FL, USA, 26-29 March 2012.

[23] A. Garro, J. Groß, M. Riestenpatt, G. Richter, A. Tundis, "Reliability Analysis of an Attitude Determination and Control System (ADCS) through the RAMSAS method", J. Comp. Sc., 5(3), 439-449, 2014.

[24] J.F. Castet, M. Bareh, J. Nunes, S. Okon, L. Garner, E. Chacko, M. Izygon, "Failure analysis and products in a Model-Based Environment", Proc. IEEE Aerospace Conf., 3-10 March 2018, Big Sky, MT, USA.

[25] L. Delligatti, SysML Distilled: A Brief Guide to the Systems Modeling Language, Pearson Education, 2014.

[26] Z. Huang, R. Hansen, Z. Huang, "Toward FMEA and MBSE Integration", Proc. IEEE Ann. Rel. and Maint. Symp. (RAMS), 22-25 Jan. 2018, Reno, NV, USA.

[27] J.M. Evans, F. Groen, L. Wang, R. Austin, A. Witulski, N. Mahadevan, S.L. Cornford, M.S. Feather, N. Lindsey, "Towards a framework for Reliability and Safety Analysis of complex space missions", Proc. AIAA Non deterministic approaches conf., 9-13 January 2017, Grapevine, Texas, USA; doi: https//doi.org/10.2514/6.2017-1099.

[28] C. Kaukewitsch, H. Papist, M. Zeller, M. Rothfelder, "Automatic Generation of RAMS Analyses from Model-based Functional Descriptions using UML State Machines", Software Engineering, arXiv:2005.01993

[29] A. Calà, A. Lüder, J. Vollmar and M. Foehr, "Evaluation of migration scenarios towards cyber-physical production systems using SysML," 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, 2017, pp. 1-5, doi: 10.1109/SysEng.2017.8088287

[30] J. Zhang, C. Haskins, Y. Liu, M.A. Lundteigen, "A systems engineering–based approach for framing

reliability, availability, and maintainability: A case study for subsea design", Systems Engineering, 21, 2018, 576–592; doi.org/10.1002/sys.21462

[31] M. Hecht, E. Nguyen, A. Chuidian, J. Pinchak, "Creation of Failure Modes and Effects Analyses from SysML", SAE Technical Paper 2015-01-2444, 2015, doi:10.4271/2015-01-2444.

[32] S.Li, X. Li, "Study on Generation of Fault Trees from Altarica Models", Procedia Engineering, 80, 2014, 140-152.

[33] R. Cressent, V. Idasiak, F. Kratz, P. David, "Mastering Safety and Reliability in a Model Based Process", Proc. Annual Reliability and Maintainability Symposium, Jan 2011, Lake Buena Vista, FL, United States. 6 p., 10.1109/RAMS.2011.5754506. hal-00630827

[34] R. Cressent, P. David, V. Idasiak, F. Kratz, "Increasing Reliability of Embedded Systems in a SysML Centered MBSE Process: Application to LEA Project. M-BED 2010, Mar 2010, Dresde, Germany. Increasing Reliability of Embedded Systems in a SysML Centered MBSE Process: Application to LEA Proj. hal-00630821

[35] R. López, A. Guillén, J. Sanmartí, C. Canart, J. Masfrand, "Direct integration of safety analysis in a model based system engineering process: Lessons learned from Ariane 6 control bench family RAMS studies", in Safety and Reliability – Safe Societies in a Changing World, Haugen et al. (Eds), 2018, Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

[36] N. Yakymets, M. Perin, A. Lanusse, "Model-Driven Multi-Level Safety Analysis of Critical Systems", Proc. SysCon 9th Ann. IEEE Int., 2015, Vancouver, Canada.

[37] R. de Ferluc, A. Provost-Grellier, B. Dellandrea "Model Based FDIR process with Capella and COMPASS. Results of a CNES/TAS-F study and way forward", Proc. MBSE ESA workshop, December 2016.

[38] H.P. Hoffmann, "Systems Engineering best practices with the Rational solution for systems and software engineering, Deskbook" (Model Based Systems Engineering with Rational Rhapsody and Rational Harmony for Systems Engineering), the IBM Software Group, © IBM Corporation, 2011.

[39] The FAA "System Safety Handbook, Chapter 8: Safety Analysis/Hazard Analysis Tasks", December, 2000.

[40] G. Biggs, T. Juknevicius, A. Armonas, K. Post, "Integrating Safety and Reliability Analysis into MBSE: overview of the new proposed OMG standard", INCOSE 2018

[41] J. Holt, S. Perry, "SysML for Systems Engineering", The Institution of Engineering and Technology, London, UK, 2008.

[42] E. Brusa, "Heterogeneous simulation and interoperability of tools applied to the design, integration and development of safety critical systems" Proc. AISE/INCOSE Conf. on Sys. Eng. – CIISE 2016, Turin, Italy, November 14-15, 2016, CEUR-WS.org/Vol.1728; urn:nbn:de:0074-1728-8, pp.132–134.

[43] E. Brusa, D. Ferretto, "Impact of the Model Based Systems Engineering on the design of a mechatronic flywheel–based energy storage system", Proc. II IEEE ISSE Int. Symp. Sys. Eng., Edinburgh, October 4–5, 2016 pp.171–178, IEEE Catalog Number: CFP16SYM-ART; ISBN: 978-1-5090-0793-6.

[44] E. Brusa, D. Ferretto, J.M.Cervasel, "Virtual engineering of a naval weapon system based on the heterogeneous simulation implemented through the MBSE", Proc. Conf. on Sys. Eng. – CIISE 2018, Rome, Italy, November 28-30, 2018, CEUR-WS.org/Vol-2248, pp.38–44, Best paper Award 2018.

[45] A. Tundis, D. Ferretto, A. Garro, E. Brusa, M. Mühlhäuser, "Dependability assessment of a deicing system through the RAMSAS method", Proc. IEEE III Int. Symp. on Syst. Eng., 11-13 October 2017, Vienna, Austria, 10.1109/SysEng.2017.8088257.

[46] I. Vagliano, D. Ferretto, E. Brusa, M. Morisio, L. Valacca, "Tool Integration in the Aerospace Domain: a case study", Proc 41st IEEE Annual Computer Software and Applications Conference (COMPSAC), 4-8 July 2017, Torino, Italy.

[47] SAE - ARP4754, "Certification Considerations for Highly-Integrated Or Complex Aircraft Systems", 1996, SAE Int., https://doi.org/10.4271/ARP4754.

[48] SAE - ARP4761, "Guidelines and methods for conducting the Safety Assessment process on civil airborne systems and equipment", 1996, SAE Int., https://doi.org/10.4271/ARP4761.

[49] ASD S-1000D, "International Specification for Technical Publications" – Aerospace and Defence Industries Association of Europe, current version.

[50] OSLC–OASIS Open Services for Lifecycle Collaboration, as it appears on http://www.oasis-oslc.org/ (as is in February 2020).

[51] MODELISAR Consortium. Functional Mock-up Interface for Model Exchange Version 1.0. http://www.fmi-standard.org

Eugenio Brusa received the M.Sc. degree in Aeronautical Engineering at the Politecnico di Torino, Italy, (1993), and the PhD in Machine Design (1997). Assistant professor in Machine Design, since 1998, he was appointed associate, in 2002, and then full professor, in 2013. He belongs the Dept. of Mechanical and Aerospace Eng. of the Politecnico di Torino. He has been Coordinator of the B.Sc. and M.Sc. courses in Mechanical Eng. (2015-2018), and currently he is Director of the Doctoral School of the Politecnico di Torino (2018-2021). He has been deputy Chair (2010-14), Chair (2014-15), and past Chair (2015-17), of the ASME (American Society of Mechanical Engineers), Italy Section. He is leader of the research group in Industrial Systems Design and Engineering, dealing with Machine and System Design, Structural Mechatronics and Systems Engineering. He has been key liaison officer at the Politecnico di Torino of the Artemis JU CRYSTAL project on the "Critical Systems Engineering Acceleration".