A model based approach to design for reliability and safety of critical aeronautic systems

Eugenio Brusa
Politecnico di Torino, Dept. Mech. and Aer. Eng.
Torino, Italy
eugenio.brusa@polito.it

Candida Stigliani
Politecnico di Torino, Dept. Mech. and Aer. Eng.
Torino, Italy

Davide Ferretto
Politecnico di Torino, Dept. Mech. and Aer. Eng.
Torino, Italy
davide.ferretto@polito.it

Claudio Pessa
Leonardo Company, Finmeccanica Aircraft Division
Torino, Italy
claudio.pessa@leonardocompany.com

Copyright © held by the authors.

***Abstract*—This paper explores how the safety engineering practices applied to the aircraft design can be effectively associated to the MBSE. Requirements and procedures of the ARP4754/ED-79 and ARP4761 were considered. As an example the fuel system of a civil aircraft was used. Some key issues were found relevant, whilst modeling the system through the MBSE tools. The management of both the functional and dysfunctional analysis, leading to the Functional Hazard Analysis (FHA) of the whole aircraft, within the same modeling environment was tested. The elicitation of safety requirements with a direct link to the FTA and FMEA used to quantify the risk of failure was performed. The software tools which can be interoperated for those tasks were tested. As a result, the integration between the two above mentioned analyses looks fairly easy. In fact, further efforts are required to make fully interoperable the tools currently available to perform this activity and to include the human interaction with the analyzed system.**

Keywords—Model Based Systems Engineering, Machine Design, Numerical methods, Functional Analysis, Risk analysis, System reliability and safety.

I. INTRODUCTION

A main goal of the Model Based Systems Engineering (MBSE) is the safety assurance in critical systems. To be assumed as a main reference for the design, the MBSE needs to be fully integrated with the tools of the Safety engineering. Aeronautics is a typical application of safety critical systems with an increasing complexity, associated to the number of subsystems connected, of functions exploited and of interfaces [1]. A bright integration among subsystems and components is strictly required to assure a suitable level of safety and to comply with the homologation of the aircraft product [2]. It is known that the high level of complexity generally might increase the risk of failure, without a suitable prevention and a careful reliability assessment. Those motivations led to the requirements expressed by the Recommended Practices ARP4754/ED-79 [3] and ARP4761 [4]. They define a process to provide all the relevant information to certify the safety of complex and highly integrated aeronautic systems. Nevertheless, daily practice demonstrated that processes and definitions of those standards led to several interpretations and slightly different implementations, depending on the manufacturer [5] or even upon the technical domain [6]. Clear statements about functions, interfaces, hierarchy of control functions and safety based trade–off of the proposed layouts are needed. As it looks evident the Systems Engineering can greatly support that activity as it is discussed in this paper. In particular, the aim is that of assessing a procedure to perform the safety analysis of the system, through the tools of the MBSE [7,8], suitable for homologation according to the standards of civil aircrafts [2]. The development of this analysis basically deals with an integration between the usual functional analysis performed in SE and the dysfunctional analysis used in safety engineering to quantify and prevent the risk of failure [10]. As an example the fuel system of a civil aircraft with two engines for 90 passengers equipped with an Auxiliary Power Unit (APU) will be described. As it is known the fuel system is required to be highly reliable, to suitably perform in all of operating conditions foreseen by the aircraft design [11,12,13]. In addition its configuration must fit some requirements about the weight, cost and performance in service, as well as those of maintainability and availability.

II. SAFETY ANALYSIS AND DESIGN

The aim of safety analysis in design is that of defining suitable requirements to be fitted to comply with the needs of conformity to the manufacturer's practice, technical standards and directives, homologation items and tests. The whole process to perform the safety analysis is described by the ARP4761. In practice, the aircraft functions and those of its systems should assure a risk degree compatible with the norms. The main activities are described in Fig.1. The safety analysis can be integrated within the MBSE approach, for instance by associating the above mentioned activities to the steps defined by the V–model, as the ARP4754A states (Fig.2).

A key issue of this analysis is the so–called FHA (Functional Hazard Analysis), which was performed in the test case first at the aircraft level, then applied to the fuel system. According to the FHA, for each system function, failure modes, severity and risk associated are explored [14]. Obviously the safety targets are defined by fixing the degree

of severity and risk compatible with a safe operation as in other similar safety critical systems [15,16]. Once that all the requirements could be allocated to the system functions, and these are associated to subsystems and components, the FHA has to be performed for all of those. If the MBSE is applied this activity looks fairly easy. A preliminary functional analysis is performed thus identifying use cases, stakeholders, functions and architecture of the designed system. Then a dysfunctional analysis can be run, thus allowing a critical review of all the eventual failure modes. It might be noticed that this approach provides a clear outline to proceed straightforward, particularly during the concept design activity. Safety analysis is performed fairly fast through the FHA and is easily documented.

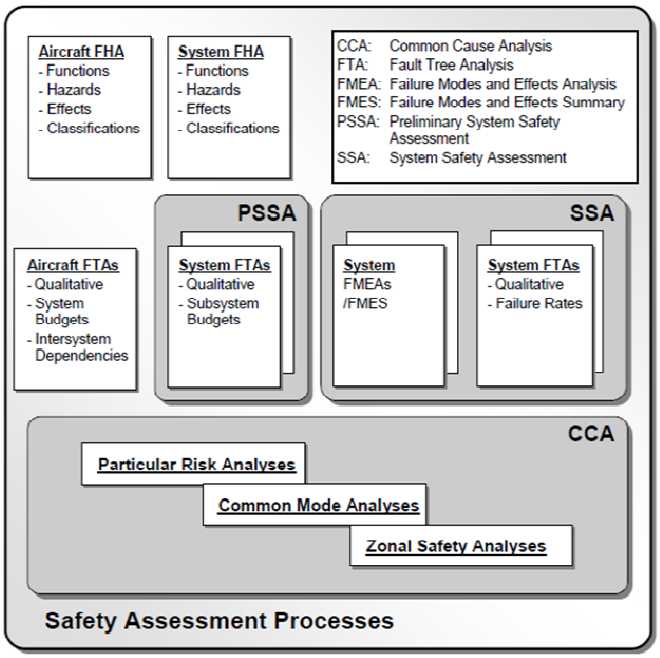

Fig. 1. Main contents and tools of the safety analysis performed in aeronautical engineering (from ARP 4761)[4].

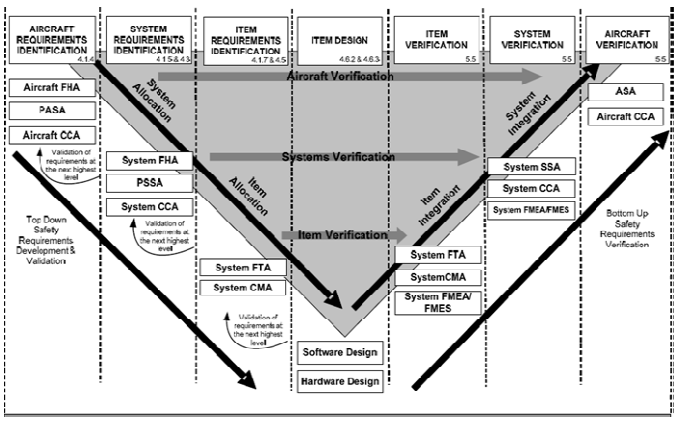

Fig. 2. Integration of the tasks of safety analysis within the V-diagram of the Systems Engineering (from ARP 4754A) [3].

III. Functional Hazard Analysis

As the FHA is performed, all the failure modes of the system functions are identified. Failure conditions are evaluated for both single and multiple events, in normal and degraded environment. Effects of failures are then defined and classified. Some requirements to be associated to the failure conditions are then defined and their coverage in allocation is finally checked. In the test case, the FHA at the aircraft level was provided as an input of the modeling of the fuel system. Functions included were mainly referenced to the ARP 4754. Many of those may affect the behavior of the fuel system. Among all, for instance, the thrust, self-piloting, data monitoring and recording, electric power, internal and external connections and energy conversion were analyzed. For each function, four states were considered in failure condition. A severe failure occurs in case of total or partial loss of the function, while less dangerous is considered an error signal. Moreover, a function might be performed too early or too late. In addition, failure might be either detected or not.

Once that the failure modes are defined, a relevant task is investigating the severity of effects. This activity might be very difficult, since associating a too severe consequence to a dysfunction might turn out into a stringent requirement, as well as under evaluating the severity of a failure might affect the overall safety of the system. This difficulty could be overcome through the System Engineering. It provides the functional analysis, puts in evidence the stakeholders and the use cases and allows tracing the effect of a failure through the product development from the constructed part to the corresponding function and requirement.

The FHA was formalized in the test case to be integrated with the MBSE approach. Some degrees of severity of the failure modes were set up. They were evaluated by considering in sequence the absolute safety of system, its operational capability, effects on the crew, effects on passengers. Catastrophic is the dysfunction preventing continued safe flight and landing, thus leading to the death of humans, inhibiting some important operational capability or causing even injuries to crew to be urgently treated. Hazardous is each event decreasing significantly the safety margins, increasing the amount of work produced by the system or affecting a number of other functions, or even strongly tiring the crew or causing injuries not requiring an immediate treatment for the occupants. A major dysfunction for the aircraft allows it cruising and landing safely and significantly increases the work of crew. Less relevant dysfunctions might be classified either as minor or irrelevant, depending on the appreciable reduction of safety margins.

TABLE I. Safety Targets and Requirements

Degree	*Probability per flight hour*
Catastrophic	$< 10^{-9}$
Hazardous	$10^{-9} < x < 10^{-7}$
Major	$10^{-7} < x < 10^{-5}$
Minor	$10^{-5} < x < 10^{-3}$
Irrelevant (no effect)	$10^{-3} <$

To complete the FHA the probability of occurrence was associated to each degree of severity of failure (Tab.1). This action immediately allowed writing the corresponding safety requirements.

IV. Requirement Analysis

The elicitation of requirements for the fuel system in the test case was driven by two parallel set of needs. Safety requirements were directly derived from the results of the FHA applied to the aircraft first, then on the system. Functional requirements were found by means of the functional analysis performed in IBM Rhapsody®. It is worthy noticing that some goals were assumed as needs: redundancy of critical functions, automatic monitoring with warning capabilities, location of commands preventing any accidental activation, double signal transmission. The requirement analysis was performed by following the standard IEEE 1220 [17]. Therefore, their attributes are specific, measurable, suitable, feasible and traceable, as is required by that standard. Additional requirements were written to fit the standard ASD S 1000 D (former ATA 100) [18]. To digitalize those requirements the IBM Rational DOORS® tool was used.

V. Functional Analysis

Typical diagrams of the System Modeling Language (SysML) were drawn to perform the functional and operational analysis of the system [19]. As a matter of fact, in the test case which includes several material components to be either assembled or connected to constitute the system, some questionable issues were found in the MBSE as is known in the literature. For instance, the sequence of diagrams and their topology might have an impact on a straight implementation of the approach. According to the Harmony© approach proposed by IBM [20] and widely used to run the Rhapsody® tool, functional analysis can be performed by following some alternate paths.

Provided that a preliminary definition of requirement diagrams is performed and behavioral diagrams (use cases, activity, sequence, state machine) are drawn before the architectural diagrams, including block (BBD) and internal black diagrams (IBD), respectively, to perform the functional analysis, after the use cases, sequences, activities and IBD together with the state machine diagrams can be used. Alternatively, activities can be drawn before the sequences or even the state machine diagram can be used to derive the other ones. This choice is up to the user, but effectiveness of the software implementation changes as it might change the impact of the proposed MBSE approach on the existing practices of the technical domain.

In the test case, the fuel system was easily described by resorting to the use cases and the sequences of actions performed in operation, thus allowing a natural derivation of activities and states. Some use cases were dedicated to a dysfunctional behavior, according to the FHA, by implementing the approach described in Fig.2. It was remarked that many requirements could be assessed and refined and others added by completing this task. Moreover, the path followed in drawing the diagrams looked the most suitable to be compatible with the tradition of the aeronautical domain and to describe the dysfunctions, since it was sufficient negating the operations defined in the sequence diagrams to create several dysfunctional behaviors.

Some critical issues in the proposed architecture were detected thanks to the dysfunctional analysis, which helped in updating the Functional Breakdown Analysis of the fuel system.

A. *Use cases*

When a safety analysis is integrated with the functional analysis of the system, a more general interpretation of the use case is applied. Instead of only a goal to be achieved by the system, which usually involves as a stakeholder more the users than other subsystems, a use case might be even considered an action performed by the stakeholder, without a specific request. As an example, the engines feeding (Fig. 3) might be seen a logic action operated simply by changing some parameters in the FCU (Fuel Control Unit) [21]. However, this interpretation makes the engine a sort of a shadow stakeholder, poorly considered in the dysfunctional analysis. If the engine is considered as a regular stakeholder, all of functions, connections, errors are activated and dysfunctional paths can be easily defined. In the test case, for instance, the fuel storage performed by the tank, according to the SE literature, cannot be assumed as function since the tank does not require to the system to be filled nor the system requires to store the fuel. Therefore, the tank is a sort of service, poorly compatible with the role of stakeholder. However, if it is assumed to be a component of the fuel system, whose use case is store the fuel, in case of permeability of the tank structure dysfunction of fuel loss can be foreseen and analyzed.

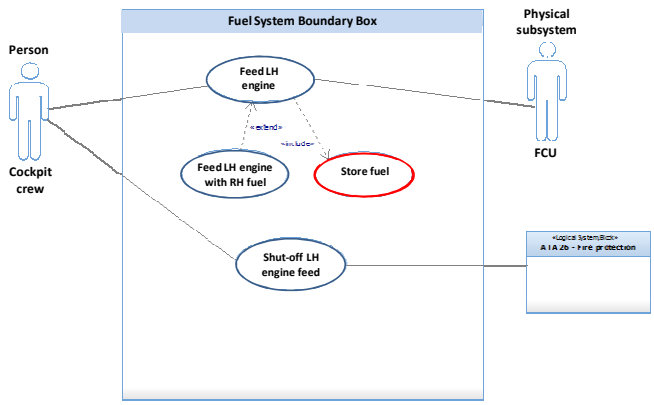

Fig. 3. Use case diagram, with special operational use case highlighted.

As it could be remarked in the test case, safety analysis affects the definition of the use cases. This happened for the heating control. It was found after a preliminary elicitation of requirements that a control of the temperature of the stored fuel is required and temperature cannot be below a define threshold in operation, to assure a prompt use. The hydraulic system plays the role of stakeholder in the heat exchange, since it provides the required amount of heat to the fuel tank. This refinement was added after identifying a critical issue in

the dysfunctional analysis of the fuel system. As usual, the functional analysis was performed in IBM Rhapsody® by resorting to the connection between IBM DOORS® and Rhapsody® through the existing gateway, which assures a synchronization of contents.

B. Use cases realization

The realization of use cases is aimed at investigating the system behavior case by case and at identifying the functions exploited. This task is usually based on the sequence diagrams, which highlight the functions performed and the stakeholders involved in each one. It is worthy noticing that they can be used for both the functional and dysfunctional analyses. An example of negation of a function is shown in Fig.4. Moreover, in the test case it was demonstrated that a preliminary set-up of functional sequence diagrams allows identifying all the critical issues for an eventual dysfunction, thus driving the dysfunctional analysis. A difference between a functional and dysfunctional sequence diagram is that to describe a dysfunction often it is required to resort to several additional details or links and some more functions. They increase the nodes of possible failure in the related architecture of the system, which have to be enclosed inside the FHA.

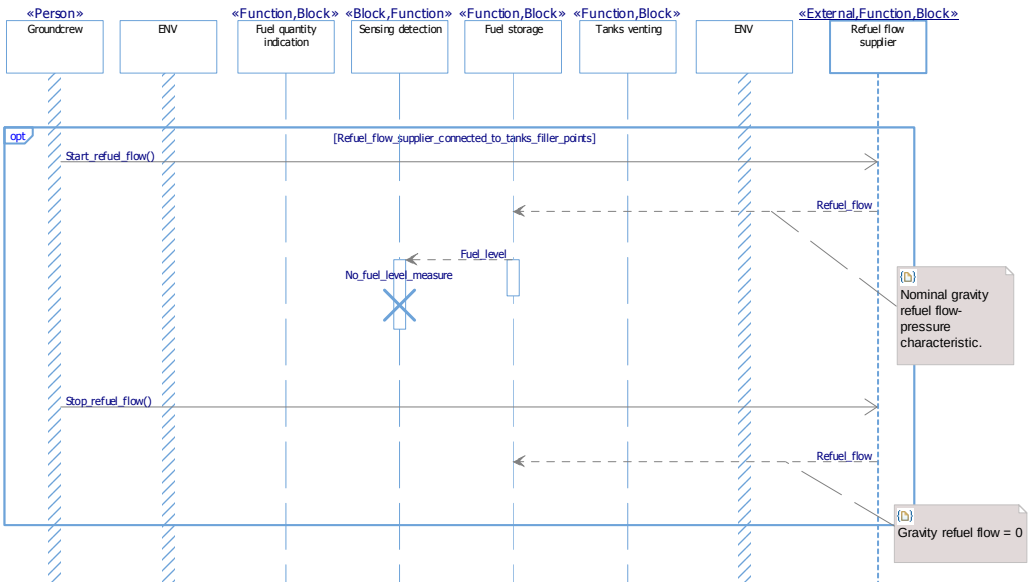

Fig. 4. Dysfunctional scenario related to a lack of measurement of the fuel level during a feed by gravity

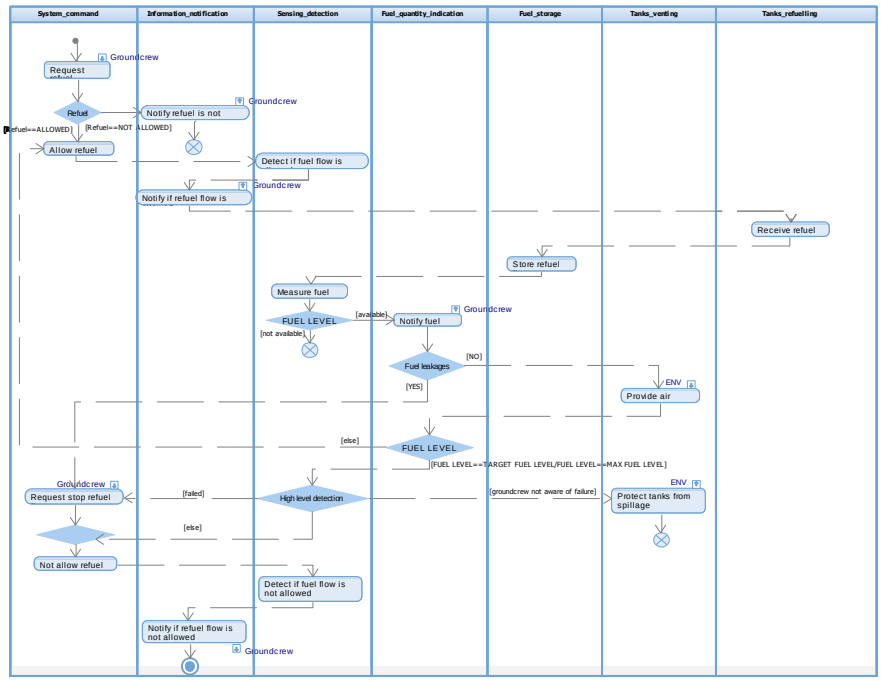

Fig. 5. Activity diagram used for the dysfunctional analysis of the system.

C. *Activities and swimlanes*

Activity diagrams were then drawn to complete the description of the system behavior. Action flows are there shown, thus allowing immediately to identify a dysfunction wherever the flow is stopped (Fig.5). The role of each function or capability can be easily highlighted and further analyzed in this diagram by resorting to the columns, thus describing the so–called “swimlanes”. The connection with stakeholders can be represented as well.

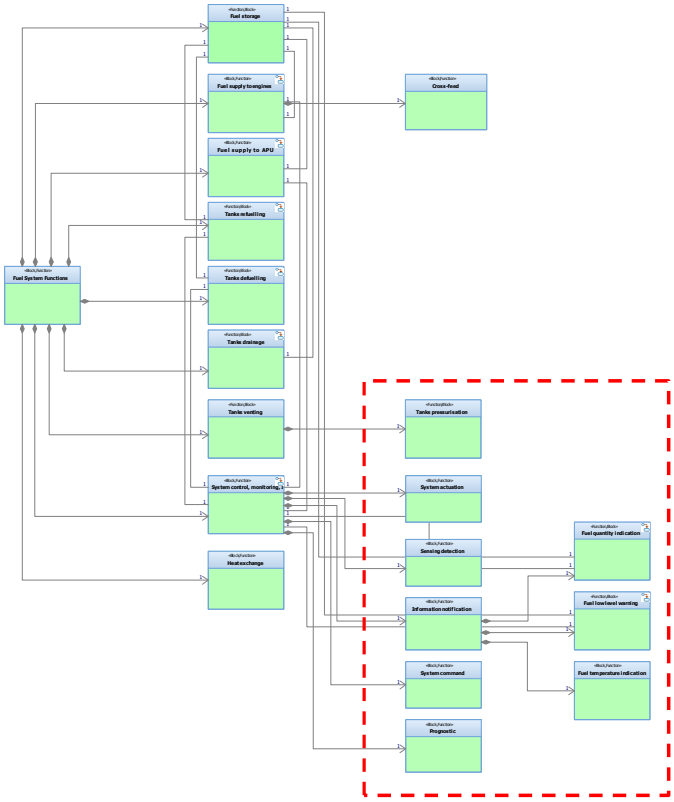

Fig. 6. Functional breakdown structure of the system.

VI. PRODUCT DESIGN

A. *Functional breakdown structure*

According to the MBSE to avoid a pure repetition of the layouts already applied in a previous version of the product, a good practice consists of dividing the architecture definition into three steps. Functions to be required to the system can be suitably defined by a breakdown structure and then instantiated into a logical architecture, being different from the real architecture since for each function only a generic device or subsystem capable to perform it is included instead of the real and material component, which will contribute to compose the system assembly. In the test case it was realized that the Functional Breakdown Structure (FBS) might be enriched if the functional analysis is performed in parallel with the dysfunctional one. In particular, control functions were detailed, as is shown in Fig.6.

B. *Logical architecture*

The system operation can be preliminarily described by the logical architecture of the system. It allows the transition between the functional and the physical modeling of the system. Usually physical blocks are there not yet represented, while the allocation of system functions to logical blocks, which will be then allocated to subsystems, components and parts in a next step (Fig.7), is described. A logical block is used to identify the relation between a certain operational task and the components of the system involved. Each logical block is already an active entity like a device, no more a pure function, not yet a real component. In practice a preliminary layout of the system architecture is drawn, without forcing the designer to select the corresponding components. The logical architecture can be also helpful to provide a preliminary system breakdown suitable for the first allocation of the reliability of the system, whilst the real prediction will be performed thanks to the Product Breakdown Structure (PBS), as described in Section VI.C.

Name	From	To
APU_Fuel_Supply_System	Fuel_supply_to_APU	APU_Fuel_Supply_System
ATA_Indicating_System	Fuel_low_level_warning	ATA_Indicating_System
ATA_Indicating_System	Fuel_quantity_indication	ATA_Indicating_System
ATA28_Fuel_System	Fuel_System_Functions	ATA28_Fuel_System
Centralised_Point_Defuelling_System	Tanks_defuelling	Centralised_Point_Defuelling_System
Centralised_Point_Refuelling_System	Tanks_refuelling	Centralised_Point_Refuelling_System
Cross_Feed_Fuel_Supply_System	Fuel_supply_to_engines	Cross_Feed_Fuel_Supply_System
Distribution_System_Valves	System_control_monitoring_actuation	Distribution_System_Valves
Distribution_System_Valves	System_actuation	Distribution_System_Valves
Drainage_Subsystem	Tanks_drainage	Drainage_Subsystem
Engine_Shut_Off_System	Fuel_supply_to_engines	Engine_Shut_Off_System
Engine_Supply_System	Fuel_supply_to_engines	Engine_Supply_System
Fuel_and_refueling_panels	System_command	Fuel_and_refueling_panels
Fuel_heater	Heat_exchange	Fuel_heater
Fuel_Pressure_Monitoring_System	Sensing_detection	Fuel_Pressure_Monitoring_System
Fuel_Pressure_Monitoring_System	System_control_monitoring_actuation	Fuel_Pressure_Monitoring_System
Fuel_Quantity_Indicating_System	Fuel_quantity_indication	Fuel_Quantity_Indicating_System
Fuel_Quantity_Indicating_System	Fuel_low_level_warning	Fuel_Quantity_Indicating_System
Fuel_Tanks_Subsystem	Fuel_storage	Fuel_Tanks_Subsystem
Fuel_Temperature_Monitoring_System	Heat_exchange	Fuel_Temperature_Monitoring_System
Fuel_Temperature_Monitoring_System	System_control_monitoring_actuation	Fuel_Temperature_Monitoring_System
Fuel_Temperature_Monitoring_System	Fuel_temperature_indication	Fuel_Temperature_Monitoring_System
Gravity_Refuelling_System	Tanks_refuelling	Gravity_Refuelling_System
Indicating_System_Control_Logic	System_control_monitoring_actuation	Indicating_System_Control_Logic
Indicating_System_Control_Logic	Information_notification	Indicating_System_Control_Logic
Pressurization_Venting_Subsystem	Tanks_venting	Pressurization_Venting_Subsystem
Pressurization_Venting_Subsystem	Tanks_pressurisation	Pressurization_Venting_Subsystem
Prognostic_subsystem	Prognostic	Prognostic_subsystem

Fig. 7. Logical blocks of the system.

C. *Product breakdown structure*

Once that the FBS and the logical blocks could be enriched according to results of the dysfunctional analysis, a preliminary Product Breakdown Structure (PBS) can be drawn as in Fig.8. It includes some new components introduced into the FBS and fits the requirements of allocation of the logical blocks description. Each physical block might allocate several logical blocks, while a logical block must be allocated uniquely on a physical one. This criterion allows reducing the number of components used, the failure modes and the system complexity. It is worthy noticing that this approach fails in case of required redundancy of the system. From this point of view if the safety analysis drives towards the application of a redundancy, the allocation between function, logical block and physical blocks might be affected. In the test case it was found that, according to the standards ATA some components were necessarily added (Fig.8). Moreover,

some safety requirements might suggest to introduce additional components, like in test case it was the heat exchanger for the heat transfer between the hydraulic and the fuel system.

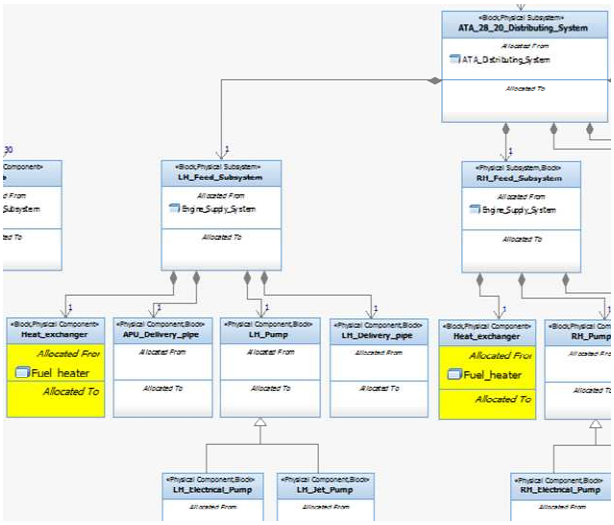

Fig. 8. Portion of the Product breakdown structure of the system with additional blocks.

D. System architecture

The above mentioned rationale led in the test case to define the overall architecture of the fuel system. According to the ATA standards three subsystems were introduced. A fuel storage, a fuel feeding, a fuel monitoring and management.

A preliminary system layout was proposed, including two tanks, located inside the wings, each one capable of storing 3185 l (approximately 2500 kg) and accessible from the upper surface of each wing through two gates. In regular service each engine shall receive the fuel from the nearest tank. To prevent any problem in case lack of gravity, each tank is equipped with a small fuel reservoir of about 200 l (feeder compartment), always full and connected to an electric pump and to a jet pump. The first one is used during the engine start-up operation, then the jet pumps are automatically activated. The electric pumps automatically are switched on when pressure of fuel goes below 350 mbar, thus assuring the fuel feeding. A cross-feed valve, being controlled by an electromechanical actuator, allows feeding the fuel to both the engines, through the same pump, in case of emergency, or to connect the right engine to the left pump and vice versa. A second valve is applied to each tank, to stop the fuel feeding and to prevent the risk of fire. If the minimum amount of fuel of 160 kg is detected in one tank, the related electric pump automatically starts. Some heat exchangers allow keeping the temperature of fuel under control and transferring the heat to the hydraulic system.

Re-fueling on ground is operated through a main connector, located just close to a landing gear. A piping system distributes the fuel through the aircraft, until that the maximum level in each tank is reached, then the refueling valve automatically is closed. A backup system was added, in case the main control of fuel level does not suitably work. It consists of a sensor, being applied to the roof of each tank. It assures that a warning is sent to the operators and the pilot when the tank is full and that refueling is stopped. It might be remarked that a panel is applied close to the refueling connector to allow the ground operator monitoring the state of each valve, even in case of feeding by gravity. If an emergency landing is decided, refueling system is used to control to open the valves through a dedicated depressurizing device operating at 0,77 bar.

A venting circuit assures that pressure be always positive during the whole mission profile. Each tank is pressurized through a venting valve connected to another one located at the end of the corresponding wing. This one is connected to the external environment through an air intake NACA, designed against the risk of ice accretion. The venting circuit is used even to prevent any risk associated to an accidental spill-out of fuel during the refueling operation. The upper part of the fuselage includes an empty and pressurized room, connected to the cross-feeding circuit of the fuel system which allows controlling the steam present inside the system.

A control system manages the fuel stored on the aircraft. A set of six sensors in each tank allows monitoring the fuel level in each tank. Their measurements are elaborated and displayed to the pilots. Additional magnetic sensors assure monitoring the fuel level even on ground. Temperature of the fuel system is always monitored and shown to the crew. A typical warning is activated when pressure in jet pumps is lower than 300 mbar, to indicate the lack of fuel or a failure occurring to the pumps.

VII. Functional Hazard Analysis (FHA)

Previous definition of the fuel system layout was performed through a functional analysis based on the MBSE approach. However, as is clearly remarked by the number of redundant devices foreseen in the proposed architecture, especially sensors, this system looks highly safety critical. It means that functional analysis might be incomplete and somehow unsuitable to detect all the risks associated to its operation and to refine both the list of requirements and the system layout. As it was previously described a dysfunctional analysis is associated to the functional one to perform a deeper investigation and to complete the trade-off of the system layout.

The so-called Functional Hazard Analysis already performed at aircraft level (as in section 2.1) was developed for the fuel system. This action needs some preliminary activities:

- system functions should be clearly defined as in the Functional Breakdown Structure (FBS);
- interfaces with the operational environment should be known, as in the Use Case diagram;

- functions of the super-system should be evenly known, i.e. in this case those of the whole aircraft;
- related failure modes and conditions of the super-system should be already explored and detected through the FHA of the whole system, i.e. the aircraft;
- system requirements should be defined and listed as in requirements list and diagrams, respectively.

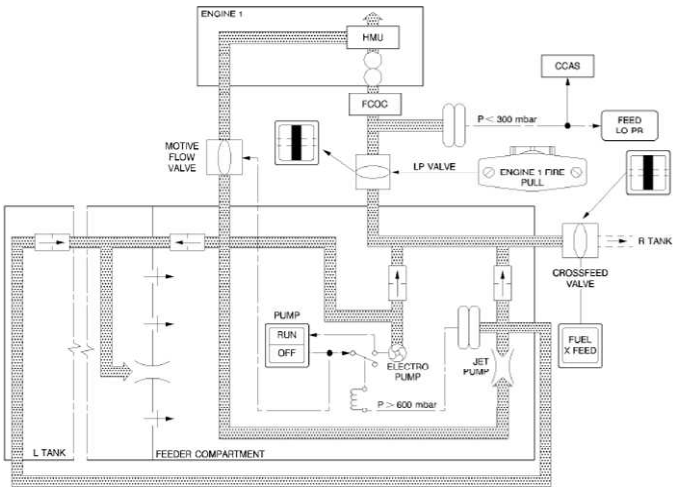

Fig. 9. Sketch of a typical layout of a fuel system similar to that forseen in the test case for a civil aircraft for regional connections.

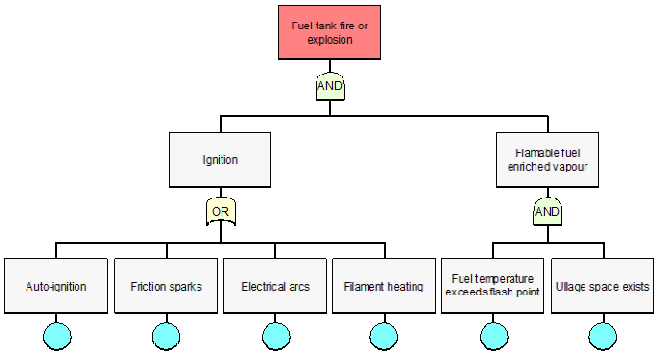

Fig. 10. Example of FTA for a failure event of tank esplosion.

A main benefit of the MBSE applied to the test case was that FHA naturally flows if one looks at the FBS as well as at the other SysML diagrams previously drawn, especially to identify the system functions and interfaces. Practically, it was sufficient negating the actions foreseen in sequence and activity diagrams. Moreover, safety engineering procedures can be easily performed by all of involved operators since the models are shared through a platform among all. From the point of view of scenarios and missions starting from the use cases, linking each failure condition to a specific and known flight phase helps a lot. Designer should avoid detailing too much in this activity the contents of the FHA, as it could be easily the case, because of the availability of those functional diagrams.

The FHA allows deriving the safety requirements for the system. Failure modes simultaneously are the high level failure condition to start the derivation of the Fault Tree Analysis (FTA) [10,22], as in Fig. 10.

VIII. System Safety Assessment (SSA)

Once that the dysfunctional analysis is ready, as it happens in case of the heterogeneous simulation for the prediction of the dynamic behavior of system after the functional, for instance, an interoperation with the System Safety Assessment (SSA) is performed, to enable a verification of the safety requirements.

The SSA consists of a systematic analysis of the architecture to link all the dysfunctions previously identified by the FHA to safety requirements. This activity needs a preliminary verification plan, based on the severity of each failure as the ARP4761 describes. In particular, in this work it was done by following some criteria as: the function type, its severity, the flight step in which the failure occurs and the complexity of the subsystem or component analyzed. According to that approach, it is relevant resorting to the classification of degrees described in Table 1. Dangerous and catastrophic events are usually more deeply analyzed.

A. FTA

Each failure condition detected by the FHA leads to verify the corresponding safety requirements. To perform this activity, the FTA is used. Starting from a main failure event, all the related failures are detected through the connections present inside the system and the interfaces according to a sort of "top-down" screening as in Fig.10. This analysis resorts to the hierarchic structure of the system. Therefore, the functional and dysfunctional analyses performed through the BBD and IBD immediately support this action. In case of the explosion of a tank, for instance, it could be possible detecting the tree of faults easily by considering the use cases and the proposed system architecture.

B. FMECA

A quantitative evaluation of risk is possible when the cause and effects analysis is performed, by creating the homonymous FMEA (Failure Mode and Effect Analysis) [10]. To introduce some metrics inside the FTA, failure rates have to be identified, component by component, as well as their reliability. If one assumes that those values are constant over time, at least in this step of the analysis, a FMEA report can be linked to the functional model and then used to fit requirements of the ARP4761. Relevant inputs are the component identification number and name, the failure modes foreseen, a description of effects, tools to detect the failure, to measure their severity and to repair, when possible.

Once that the FMEA is completed, failure rates can be easily derived by looking at the FTA. Moreover, there is a time of exposure to the detected risk. In the test case, for many components it simply corresponds to the time of flight, since this subsystem is highly critical, the failures

severe and the consequences mainly dangerous or even catastrophic. In some cases other values were set up, according to the literature herein indicated. The interoperability in this case is played with the software used to define the above mentioned values, i.e. the RAM-COMMANDER®. Each FTA allows computing the probability of failure associated to the main event at the top, through the Boolean algebraic function described by the tree.

It might be considered that those approaches can benefit of other currently developed within the frame of computer science and information technology. Even in this field a full interoperability of tools is looked for. Some examples of reliability analysis linked to a system dynamic behavior was already proposed by resorting to Modelica® as a tool for a full safety analysis [24]. Moreover, structured reliability analysis and safety assurance processes are currently developed and tested to be used in connection with the MBSE and related tools. They could be integrated with the process above described, to enrich and complete the tool chain and create a suitable platform to support the overall system development [25].

IX. CONCLUSION AND FUTURE WORK

A challenging issue to demonstrate the effectiveness of the Model Based Systems Engineering in developing and integrating mechanical and aeronautical systems is using its tools to enhance the elicitation and the verification of safety requirements. Actually the analyzed test case of the fuel system for a civil aircraft demonstrated that coverage and traceability of requirements can be greatly improved by using the MBSE. Safety engineering basically needs a clear definition of functions, interfaces and hierarchies in the system layout to proceed with a straight evaluation of failure modes and their propagation in terms of effects upon the whole system. Functional modeling allows developing a dysfunctional analysis, which helps in detecting the failure modes and defining the corresponding safety requirements. A key activity is the Functional Hazard Analysis, which might easily be performed by following the information described by the behavioral and architectural diagrams of the MBSE. Moreover, safety analysis requires a quantitative prediction of risk and of the related probability of occurrence. In this second step of the activity it might be noticed that FTA and FMEA are supported by the MBSE, never substituted, although functional modeling allows deriving fairly easily the contents of those analyses. A better correlation between the FHA of the whole aircraft and of the fuel system was even found. Critical issues at the interface between those two systems could be even detected. As a matter of facts, the designed fuel system demonstrated to be capable of feeding the required amount of fuel along a complete flight mission, for given pressure, temperature, altitude and scenario. Fuel level is continuously monitored [23] and fuel heating suitably controlled by heat exchangers. Interoperation between functional models, FMEA and FTA looks possible and effective, although a corresponding interoperation of related software has to be further tested. A future work could be focused on the effect of human mistakes in operation, i.e., upon including humans in the model, or even of multiple failures simultaneously occurring.

Acknowledgment

This work was funded by the ARTEMIS Joint Undertaking under Grant Agreement N° 332830.

References

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

[2] Federal Aviation Admnistration (FAA), Advisory Circular, System Safety Analysis and Assessment for Part 23 Airplanes, AC 23.1309-1E (11/17/2011), ACE-100

[3] 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

[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] A. Mitschke, E. Brusa, A. Calà, D. Ferretto, C. Pessa, G. Bachelor, “Heterogeneous simulation based on standards: deepening interoperability in trade-off analysis approach for aeronautical application”, Proc. 23rd Conf. Italian Ass. of Aeronautics and Astronautics, AIDAA 2015, 17-19 November 2015, Torino.

[6] 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.

[7] D. Walden, G.J. Roedler, K. Forsberg, R. D. Hamelin, T. Shortell, INCOSE Systems Engineering Handbook v.4, INCOSE-TP-2003-002-04, 2015.

[8] NASA, NASA System Safety Handbook, 2 vv., Washington D.C., National Aeronautics and Space Administration, 2014

[9] E. Brusa, A. Calà, D. Ferretto, “Integration of heterogeneous functional-vs-physical simulation within the industrial system design activity”, IEEE Int. Symposium on Systems Engineering, Rome, September 29–30, 2015, ISBN: 978-1-4799-1919-2, pp.303-310.

[10] S. Chiesa, Affidabilità, sicurezza e manutenzione nel progetto dei sistemi, Torino: CLUT Editrice, 2008.

[11] S. Chiesa, Impianti di bordo per aeromobili: impianto combustibile, Torino: CLUT Editrice, 1994.

[12] I.G.Medvešek, T. Perić, J. Šoda, Fault Tree Analysis in the Reliability of Heavy Fuel Oil Supply, 2014.

[13] S. Quilty, Overview of Airport Fueling Operations, Washington, D. C., Transportation Reserach Board, 2015.

[14] T.P. Kelly, P.J. Wilkinson, “Functional Hazard Analysis for highly integrated aerospace sytems”, in Certification of ground/air Systems seminars, IEE, 255, 1998.

[15] K.J. Hayhurst, J.M. Maddalon, P.S. Miner, G.N. Szatkowski, M.L. Ulrey, M.P. DeWalt, C.R. Spitzer, Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems, Hampton, Virginia, NASA TM-2007-214539, L-19299, 2007.

[16] TEC-DOC, IAEA, Component reliability data for use in probabilistic safety assessment, Vienna: International Atomic Energy Agency, October 1988.

[17] T. Doran, “IEEE 1220 for practical Systems Engineering”, Computer, 39:5,2006.

[18] ASD – AIA – ATA, International specification for technical publications using a common source database, S1000D, 2007.

[19] J. Holt, S. Perry, SysML for Systems Engineering, London: The Institution of Engineering and Technology, 2008.

[20] H. Hoffmann, Systems Engineering Best Practices with the Rational Solution for Systems and Software Engineering Deskbook, Release 4.1, U.S.A, IBM Corporation, 2011

[21] Wang XiaoYang, "Aircraft Fuel System Prognostics and Health Management", Master thesis, University of Cranfield, 2012.

[22] U.S. Nuclear Regulatory Commission, Fault Tree Handbook, Washington, D.C., 1981.

[23] C. Pessa, M. Cifaldi, E. Brusa, D. Ferretto, K. Malgieri, N. Viola, "Integration of different MBSE approaches within the design of a control maintenance system applied to the aircraft fuel system", in Proc. IEEE Int. Symposium on Systems Engineering, Edinburgh, October 4–5, 2016.

[24] L. Rogovchenko-Buffoni, A. Tundis, M.Z. Hossain, M. Nyberg, P. Fritzson, "An integrated toolchain for model based functional safety analysis", J. Computational Science, Vol. 5, Issue 3, May 2014, pp.408–414.

[25] A. Garro and A. Tundis, "On the Reliability Analysis of Systems and SoS: The RAMSAS Method and Related Extensions", IEEE Systems Journal, Vol. 9, issue 1, pp.232-241, March 2015; doi: 10.1109/JSYST.2014.2321617.