Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 49-3 (2016) 453–458

Flight Control System Modeling with SysML to Support Validation, Qualification and Certification

Faida Mhenni * **Jean-Yves Choley** * **Nga Nguyen** ** **Christophe Frazza** ***

* *Quartz (EA7393), SUPMECA, Saint-Ouen, France (e-mail: faida.mhenni, jean-yves.choley@supmeca.fr).*
** *Quartz (EA7393), EISTI, Cergy Pontoise, France (e-mail: nga.nguyen@eisti.fr)*
*** *DGA-TA SIE, Balma, France (e-mail: christophe.frazza@intradef.gouv.fr)*

Abstract: The introduction of new technologies to build 'More Electric Aircraft' induces new challenges for both the design and safety analysis of new aircraft. A model-based approach is needed for both design and validation processes in order to manage the complexity and validate the conformance to safety requirements. In this paper, a SysML-based approach merging MBSE and MBSA is presented. This approach is applied to a Flight Control System (FCS) both for the design and the validation processes. A parallel is made to compare the models used in each of these processes. This comparison led to suggestions of improvements both for the design and verification and validation approaches.

Keywords: Safety, Systems Engineering, Flight Control System (FCS), SysML, AltaRica.

1. INTRODUCTION

Most of the actuation systems in the aircraft are supplied by hydraulic power characterized with a poor global efficiency, and frequent maintenance operations. To cope with the drawbacks of the use of hydraulic technology, research works are focused on 'More Electric Aircraft' (see Derrien (2012), Reysset (2015)). In this scope, the Flight Control Systems (FCS) are progressively relying on electric energy to replace all or part of the hydraulic systems for the actuation of the flight control surfaces. The introduction of such new FCS implies the use of new technologies with new actuators and on-board control unit. This will result in new failure modes that are not mastered because of the lack of feedback from experience. New challenges are then faced in the design as well as in the verification, validation and qualification of these systems in compliance with aeronautics safety standards such as the ARP 4761 SAE-Aerospace (1996).

Model-Based Systems Engineering (MBSE) is becoming compulsory for the design of such complex systems to help in better understanding and mastering these new technologies. It also helps in making the design more efficient, easier and faster and as a consequence, reducing design time and cost. Integrating safety aspects as early as possible in the design process helps in reducing risks (see Berres et al. (2015)). The early integration of safety in the design process is made possible by extending the system models with safety aspects facilitating the generation of safety analysis artifacts and reducing the gap between the design and safety analyses. Such extended model is useful both for the design and for the verification, validation and qualification activities. Indeed, certification is currently based on huge set of documents provided by the aircraft manufacturers. Separate documents are used to describe the system and to detail the results of safety analyses (i.e. Functional Hazard Assessment and System Safety Assessment).

During the design stage, safety analyses aim at providing safety requirements that shall be met by the design team. As systems are getting more complex, it becomes almost impossible for a single safety expert to have a deep understanding of the whole system and all the technologies involved. Instead, a multi-disciplinary team is needed for safety and reliability analyses and this team shall collaborate with the designers to meet the safety requirements. A system model is then needed around which the multi-disciplinary team shall collaborate. This model should be built in a general system language understandable by all the team.

At the validation and qualification stage, a system model is also built, with different tools in order to validate that the safety requirements are well met and that the designed system complies with safety standards. In this paper, an integrated design approach including safety analysis using SysML language is presented. This approach is tested in a validation and qualification process. The different models used in each process are compared. A flight control system is used as an example to illustrate this work.

This paper is organized as follows. First, a state of the art about the integration of the MBSE-MBSA is given in section 2. Then, the FCS used as a case study example is described in section 3. Both the validation approach

10.1016/j.ifacol.2016.07.076

applied in the DGA-TA and SafeSysE are respectively presented in section 4 and section 5. A discussion with improvements suggestion for both approaches is given in section 7. The paper is finally concluded in section 8.

2. RELATED WORK

Model Based Safety Analysis (MBSA) aims to provide a model-based approach to perform safety analyses while seeking a tighter integration between safety artifacts and design models. In this approach, system and safety engineers share a common system model created using a model-based development process. Joshi et al. (2006) proposed to augment the nominal system behavior captured in Simulink model-based development with the fault behavior of the system. To illustrate the process, they studied the Wheel Brake System as described in ARP 4761 Appendix L (SAE-Aerospace, 1996). The fault model consists of different component failures, i.e. digital and mechanical failure modes. Fault tolerance verification is carried out by using additional variables and real-time temporal logic operators to investigate if the system can handle some fixed number of faults. Informal safety requirements are formalized by temporal logic, and the model checker NuSMV is used to validate these requirements. Nevertheless, research challenges must be addressed on the choice of languages and tools, as well as the scalability of the analysis tool to cope with realistic systems.

AltaRica (Point, 2000) is an event-based modeling language which is designed to specify the behavior of complex systems. Mathematically based on Guarded Transition Systems, an AltaRica model is composed of nodes that are characterized by their reachable states, *in* and *out* flows, events, transitions and assertions. Once a system model is specified in the AltaRica language, it can be compiled into a lower level formalism such as finite-state machines, fault trees, stochastic Petri Nets or Markov chains (Cherfi et al., 2014; Mortada et al., 2104). The language is widely used for safety assessment of automotive, avionic and transport applications. It is supported by industrial tools such as Simfia, Cecilia OCAS and open source tools like OpenAltaRica (OpenAltaRica, 2015) with a graphical interface to design models, to inject failures and to simulate models. In Morel (2014), a model-based safety approach for early validation of avionics architectures is proposed. The model building contains four different levels: the Functional Hazard Analysis (FHA) view, the functional view, the physical view and the allocation. However, there are still some issues concerning the validation and the completeness of the allocation of functions in the functional view to hardware modules in the physical view. Model-based systems engineering with SysML can facilitate this task by building an allocation matrix since the early design phases.

Algorithms and translation rules allowing transformation from SysML diagrams to AltaRica Data Flow language have been proposed in different research works (Cressent et al., 2011; Ruin et al., 2012; Yakymets et al., 2013). Cressent et al. (2011) proposed a mapping between SysML models and AltaRica Data Flow (ADF) language, based on the MéDISIS framework. The first step is the translation of the SysML model to obtain the ADF description of the functional view of the system. The second step is the modeling of the dysfunctional view using the Dysfunctional Behavior Database built and updated via different safety analyses such as Failure Mode and Effects Analysis (FMEA). Via AltaRica, existing tools to quantify reliability indicators such as the global failure rate, the mean time to failure, etc. can be used directly on the failure modes identified in different steps of MéDISIS. However, a complete automation of the translation between SysML and ADF language is not possible if some strict SysML construction rules such as expressive allocations between the modeling elements are not applied. As mentioned by the authors, some divergent declaration philosophies between the two languages (although sharing the object-oriented paradigm) impose complicated translation rules.

3. CASE STUDY DESCRIPTION

In this paper, we will study the flight control system (FCS) in civil aircraft. The flight controls of an aircraft typically include primary controls that govern the pitch, yaw and roll attitudes and the trajectory of the airplane as well as secondary controls dedicated to control the lift of the wings. The flight control surfaces of the civil aircraft Airbus A380 are illustrated in Fig. 1.

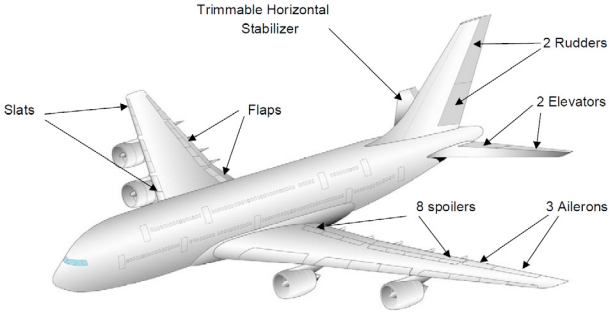

Fig. 1. A380 Flight Control System Architecture (Van den Bossche (2006))

The architecture of the flight control system is given by Fig. 2. The number of actuators per surface, as well as the number and distribution of power sources and flight control computers, are mainly imposed by safety considerations.

The FCS is made up of the actuators, sensors and on-board calculators. The flight control surfaces are actuated with different kinds of actuators powered by two different hydraulic circuits (Green circuit G and Yellow circuit Y) and two different electric circuits (E1 and E2). Each surface is actuated with one or two actuators powered by separate power sources. For instance, each side of the aircraft contains three ailerons O/B, M and I/B. The outer aileron (O/B) is actuated with two servocontrols powered by the Green and Yellow circuits respectively. The middle aileron (M) is actuated with a sevocontrol and an Electro-Hydrostatic Actuator (EHA) powered respectively with the Green hydraulic circuit and the E2 electric circuit. The inner aileron (I/B) is actuated by a servocontrol and an EHA powered respectively with the Yellow circuit and the E1 electric circuit.

The flight control surfaces are considered outside the system. The power sources i.e. hydraulic and electric power