Illustration of the information model for complex system modeling: from requirement to V&V

Romaric Guillerm, Hamid Demmou, Nabil Sadou

Illustration of the information model for complex system modeling: from requirement to V&V

Romaric Guillerm[1, 2], Hamid Demmou[1, 2], Nabil Sadou[3]
[1] CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France
[2] Université de Toulouse, UPS, INSA, LAAS, F-31400, Toulouse, France
[3] SUPELEC / IETR, avenue de la Boulais, F-35511, Cesson-Sevigne, France
guillerm@laas.fr, demmou@laas.fr, nabil.sadou@supelec.fr

Abstract. This paper presents an illustration of the utilization of an information model through a complex system. The information model is in support of a model driven methodology of complex system design. It allows addressing requirements definition and their traceability towards the solution and the Verification and Validation (V&V) elements. The work considers especially an important system propriety which is safety. SysML language is used to establish the information model thanks to the different available diagrams which make SysML as the language for systems engineering. The system considered is the braking system of an aircraft.

Keywords: system engineering, safety, requirements, SysML, braking system.

1 Introduction

Modern systems are inherently complex [1]. Complexity implies that different parts of the system are interdependent so that changes in one part may have effects on other parts of the system. In this case system engineering processes are critical and addressing safety proprieties (considered as emergent) needs a global approach. In [2] we proposed an approach that integrates safety [3] evaluation of complex systems in the system engineering process. This approach allows considering safety not in small but in large. The proposed approach is based on system engineering standard *EIA-632*.

The requirement engineering process is generally considered as the most critical process within the development of complex systems [4]. In the support of the integration approach, we have defined an information model [2] based on SysML language to address requirements definition and their traceability [5] towards the solution elements and the V&V (Verification and Validation) elements. In this paper we illustrate the utility of the information model through a complex system which is the brake system of an aircraft.

2 Integration approach

2.1 System engineering approach

System engineering is an interdisciplinary approach which develops concepts that allow building new applications. It is a collaborative process for problem resolution, supporting knowledge, methods and techniques resulting from the sciences and experiment in order to define a system which satisfies identified needs and is acceptable for the environment, while seeking has to balance total economy of the solution, on all the aspects of the problem in all the phases of the development and the life of the system. In SE it is a good practice to describe processes adopting the EIA standard. There are thirteen processes covering the management issues, the supply/acquisition, design and requirement and verification validation processes [6].

2.2 Integration approach

Managing requirements, and specially safety requirements, at the early stages of system development becomes more and more important as system complexity is continuously growing. Safety of complex systems relies heavily on the emergent properties that result from the complex interdependencies that exist among the involved systems or sub-systems and their environments. System Engineering (SE) is the ideal framework for the design of complex system. The need for systems engineering arose with the increase in complexity of systems and projects. A system engineering approach to safety starts with the basic assumption that safety properties can only be treated adequately in their entirety when taking into account all the involved variables and the relations between the social and the technical aspects. This basis for system engineering has been stated as the principle that a system is more than the sum of its parts. The Safety management must follow all the steps of SE from the requirements definition to the verification and the validation of the system. The integration of safety must concern all system engineering processes. In our approach [2] we have identified all sub-processes concerned by the safety evaluation and we have indicated how they must be considered. In other words, the sub-processes of EIA-632 standard [7] are translated or refined in terms of safety and included in system design process.

3 Information model

3.1 Requirements management

Requirements management is a crucial activity for the success of a project [4]. It is necessary to ensure that each requirement is properly declined, allocated, monitored, satisfied, verifiable, verified and justified. Figure 1 presents an overview of the requirements management of the EIA-632 standard. The proposed information model

is inspired from this pattern. We see that *other stakeholder requirements*, when added to the *acquirer requirements*, make up a set of *stakeholder requirements* that are transformed into *system technical requirements*.

The *logical and physical solution representations* are derived from *technical requirements*. *Design solution* and *specified requirements* are defined by completing the *solution definition* Process.

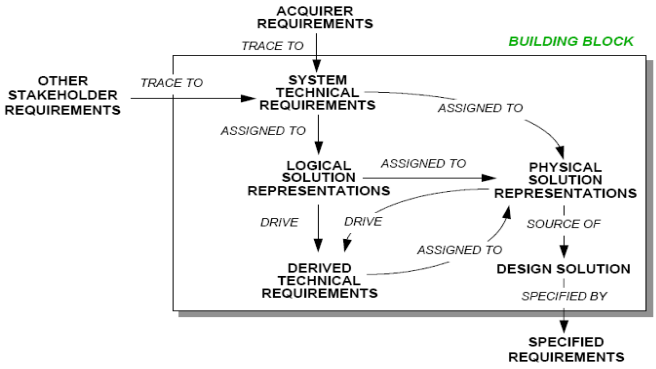

Fig.1. Requirements management of the EIA-632

An information model can be used to guide the design, to manage requirements changes, or to evaluate project progress. Indeed, modeling is important for the following reasons: it is a support for system analysis and design, it can be used for sharing knowledge and it is used to capitalize knowledge. Our information model is compatible with the requirements of the EIA-632 standard, while adding aspects of safety and risk management. We use SysML [9] language to establish this information model thanks to the different available diagrams which make SysML as the language for systems engineering.

3.2 Requirements modeling and management for safety

In this part, we propose a system approach to improve requirements management for safe system design. This approach is based on a SysML information model, following the SE process of the EIA-632 standard. This information model is the "system" knowledge basis of the design project, allowing data sharing between all expertise trades (mechanical, hydraulic, thermal, electrical...). Therefore, the model is intended to model the "system" level, showing the interactions with the environment and the connections between the various subsystems.

The information model must be seen as a means of knowledge sharing, including the 3 components: requirements, design solution and V&V. It is considered as the interconnection level between all the different trades.

The requirements, the design solution and the V&V parts are developed independently. We distinguish clearly these different concepts.

SysML allows mixing all the concepts in a single diagram. We proposed an extension of SysML and information meta-model that allows structuring the elements

of the design project with respect of the separation concepts. In other words, our approach allows a rigorous organization of the project design. Indeed, different diagrams manage different concepts.

3.3 The information model

The information model (Figure 2) that we propose is adapted to the EIA-632 standard and makes a clear distinction between different requirements classes (acquirer, other stakeholders, technical or specified).

To achieve this meta-model in SysML, we have extended the language. Firstly, we define new stereotypes to requirements, while adding new attributes to our requirements. Then we define a new link type (*specify*) linking the specified requirements to model elements.

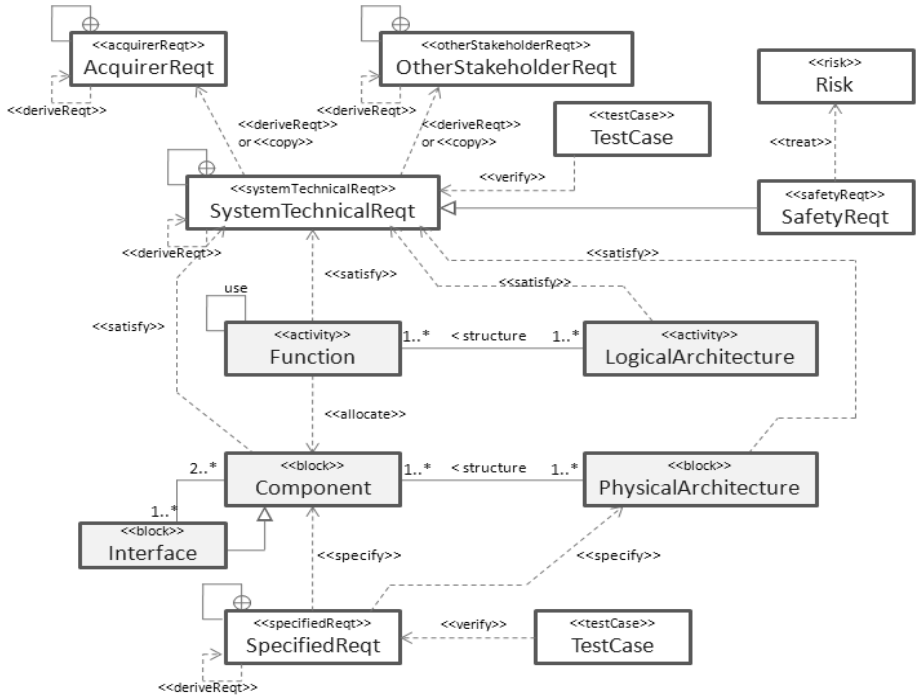

Fig.2. Information model

In this model, we have simplified the number of requirements classes. Indeed, we consider that the "*systemTechnicalReqt*" represents the system technical requirements, but also the system technical requirements non-allocated to the logical solution and the derived technical requirements coming from the logical and the physical solutions.

The acquirer and other stakeholders' requirements are represented, knowing that the field 'requirement source' must be consistent with the stereotype and indicates better the concerned stakeholders in the case of "*OtherStakeholderReqt*".

***Note**: We invite readers who are not necessarily friendly with all the above concepts (system technical requirements, logical solution, physical solution ...) to refer themselves to the EIA-632 standard [7] or the overview article [8].*

All traceability links requested by the EIA-632 are considered in this model, and the distinction between logical solution (functional part) and physical solution (component part) appears.

In this model, we highlight the definition of interfaces, which are components themselves and which links several components together. The concept of interface is essential for a proper system design. Indeed, it is one source of problems encountered during development.

The last important element that is included in this model, neither a requirement nor a design solution element, is the "*TestCase*". These elements of V&V are included in the model to be directly connected to the requirements they satisfy.

Concerning safety requirements and the consideration of safety in design, which can be derived from risk analysis, a block risk is defined and is linked to safety requirements. In fact, identification of risks is the starting point for many studies about security, but also reliability. Thus, defining a block "risk" in the information model and its link with the safety requirements, allows on one way to improve the system understanding and justifying the requirement, and on the other way to show that all the identified risks are taken into account.

Impact analyses also derive benefit from the presence of risks in the information model, because the risks, which could be challenged by model element (requirement, function, component…) changing, can be viewed directly.

4 Application: the "S18 aircraft" system

In this part we present a case study to illustrate the interest of the SysML information model on a complex example. It consists on an S18 aircraft that the specifications are provided by the standard ARP-4761 [10]. We will consider a hierarchical decomposition using the notion of the building block defined by the standard EIA-632 and on which is based our approach of safety integration in system engineering processes. However, due to limited space in the paper, we will present only one building block (one level).

4.1 Presentation

The S18 aircraft is a four engine airliner used to transport passengers. It can carry out 300 to 500 passengers on 5,000 nautical miles at Mach 0.86. The average flight time is 5 hours.

4.1.1 Functions

Various functions are performed by this system: "*control thrust*", "*control flight path*", "*determine orientation*", "*determine position and heading*", "*control aircraft on the ground*", "*control cabin environment*"…

These functions can be decomposed into sub-functions, like "*control aircraft on the ground*" whose sub-functions are: "*determine air/ground transition*", "*decelerate the aircraft on the ground*", "*control aircraft direction on the ground*"…

In this paper, we focus on only one the sub-function "*decelerate the aircraft on the ground*".

4.1.2 Sub-systems

The aircraft system consists of several sub-systems, like: structure, thrust system, control surface system, spoiler system, thrust reverse system, wheel brake system… Thanks to the interaction between these sub-systems, the above listed functions can be performed.

Sub-systems involved in the "*decelerate the aircraft on the ground*" function are: the "*thrust reversers*", the "*spoilers*" and the "*wheel brakes*".

Thrust reversers are associated with reactors and can reverse the direction of thrust. They can be used only above a certain speed (otherwise hot gases are injected again in the reactors which can cause damage).

Spoilers are movable surfaces on the wings which are used to reduce lift and increase drag. Consequently, they slow down the speed of the aircraft, preventing to take-off again by transferring more weight on the wheels. They are efficient only above a certain speed.

Finally, the wheel brakes are used at all speeds and are located on the main landing gear (not on the front). They can be used asymmetrically, to counteract against a crosswind or to make tight turns.

4.2 SysML Modeling

The following section presents the SysML modeling of the building block corresponding to the level presented previously: the aircraft system.

This modeling will respect the information model defined in paragraph 3.3 and its goal is to share engineering data through a common basis. This information will be shared between the various participants in the design, particularly between system engineers and safety engineers. In fact, most of the modeling presented here focuses on the definition of requirements and traceability links.

A structure in three packages organizes the modeling following the separation of concepts (requirements, solution design and verification and validation). Thus, the three packages are: "*Design Solution"*, "*Requirements*", and "*V&V*". The tool TauG2 of IBM is used to generate the different diagrams.

4.2.1 "Design solution" package

The first package presents the design solution. It contains two diagrams:

1. **A use case diagram**, showing the system functions,
2. **A block diagram** for the system structure.

4.2.1.1 System functions

Figure 3 shows the system functions through a use case diagram. Showing also the system's actors, the use cases represent the functions. A hierarchical structure between these functions is performed using "*include*" links. For example, the "*decelerate aircraft on the ground*" function is a sub-function of the "*control aircraft on the ground*" function, which is a sub-function of the "*pilot the aircraft*" function.

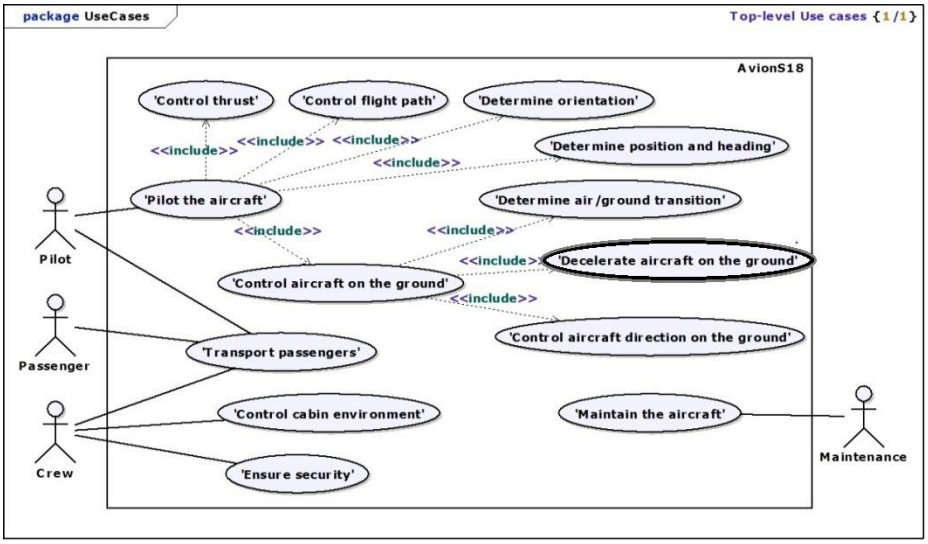

Fig.3. S18 aircraft – System functions

4.2.1.2 System structure

Parts of the "S18 aircraft" system structure are represented in a blocks diagram in Figure 4. It shows that the "S18 aircraft" is composed of a structure, a thrust system, a surface control system, a spoiler system, a thrust inverser system, and a wheel brake system.

4.2.2 "Requirements" Package

The second presented package is the "*Requirements*" package. There are four requirement diagrams for:

1. **Top-level requirements**, to present the requirements at the system level, "S18 Aircraft" for this first building block, and to link those requirements to the risks they deal with the "*treat*" link
2. **Requirement declinations**, to show the declination of the system requirements into subsystem requirements through the *composition* link,
3. **Requirement satisfaction**, to indicate the system elements (system or subsystems) that meet the requirements by the "*satisfy*" link,
4. **Requirement verification**, to denote elements of V&V which satisfy the requirements by the "*verify*" link.

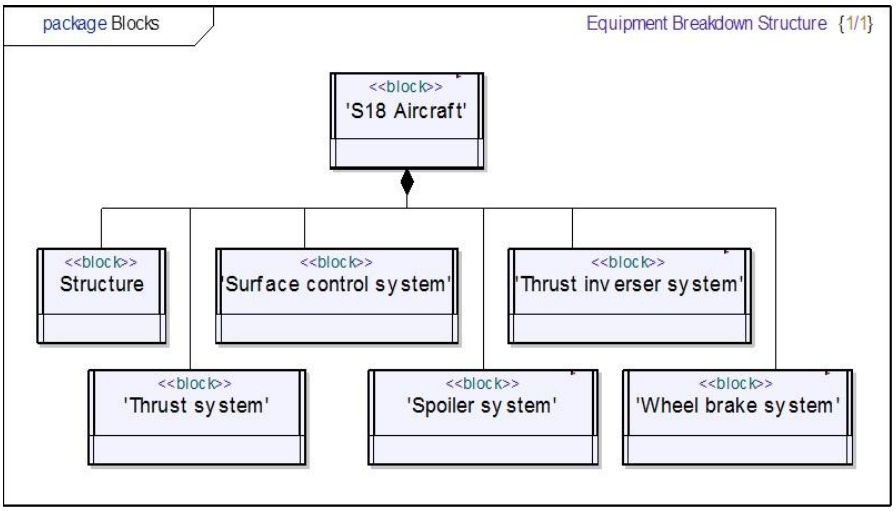

Fig.4. S18 aircraft – System structure

4.2.2.1 "Top-level requirements" diagram

Figure 5 shows the top-level requirements of the S18 aircraft. Only two risks appear "*high speed overrun*" and "*offside excursion from the runway*". Their severities are between two values; this is due to a modeling simplification to not multiply the number of risks according to the landing, taxi, or aborted takeoff phases.

In this diagram, we find for example the system safety requirement "*unannounciated loss of deceleration capacity must have a frequency <5.10-9/flt*" identified during the FMEA of the S18 aircraft system [11]. This requirement, whose identifier is "*R2*", can treat the risk "*Risk_1*": "*the aircraft do a high speed overrun and can hit obstacles*" identified during the preliminary risk analysis.

4.2.2.2 Requirement declinations diagram

Figure 6 shows the declination of top-level requirements (S18 aircraft system) in sub-systems requirements. We find here two declinations concerning the system requirements "*unannounciated loss of deceleration*" and "*inadvertent deceleration after V1*", which are declined on the sub-systems: thrust inversers, wheel brakes and spoilers.

4.1.1.1 Requirement satisfaction diagram

Figure 7 shows the allocations of requirements to the elements of the design solution, through the "*satisfy*" link of SysML. These elements can be any elements other than the SysML requirements, but in our model they correspond to blocks (representing systems) or use cases (representing functions).

Regarding the two above requirement declinations, system requirements are related to system elements, which correspond to "S18 aircraft" system functions (modeled with use cases). For the subsystem requirements, they are associated to blocks representing sub-systems (wheel brakes, thrust inversers, spoilers).

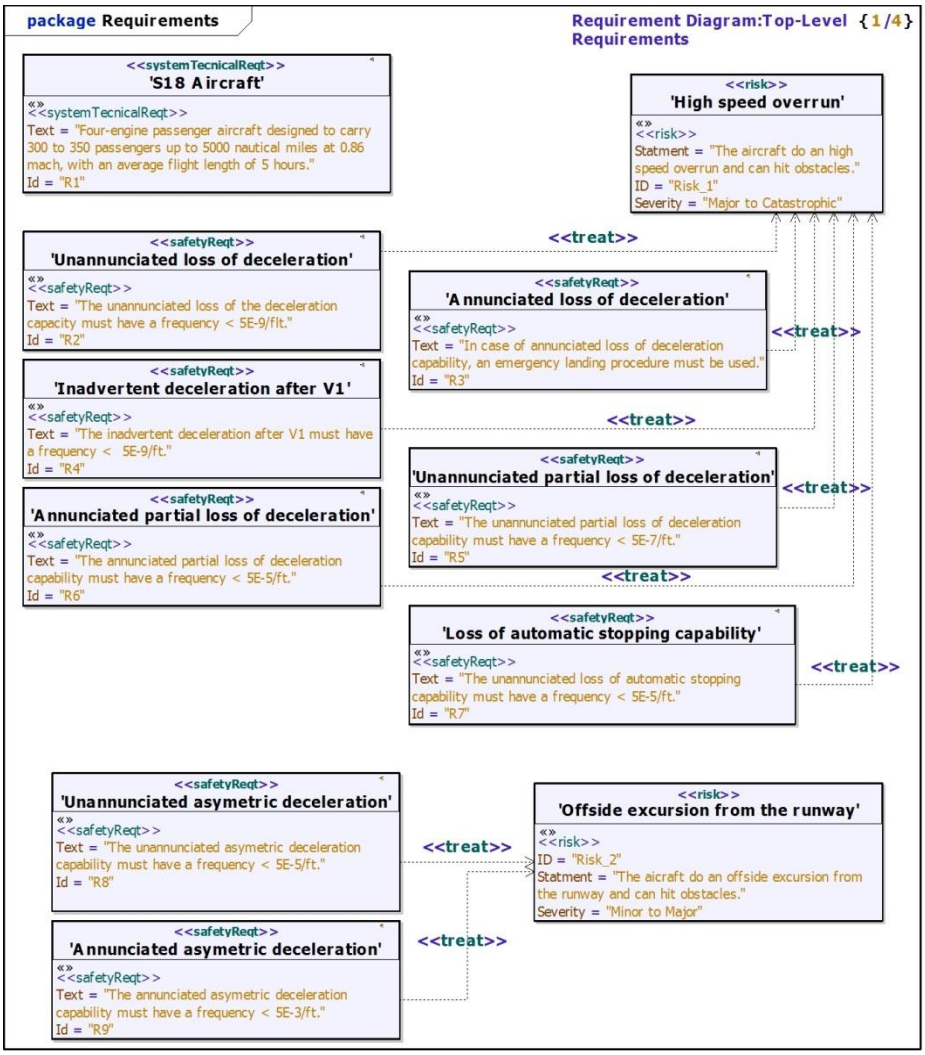

Fig.5. S18 aircraft – "Top-level Requirements" diagram

On the bottom of the diagram (figure 7), a set of requirements was simply linked to the "S18 aircraft" block representing the system. For a complete modeling, these requirements should also be declined. But to limit the size of the example, we do not study in depth these requirements.

4.1.1.2 Requirement verification diagram

Figure 8 shows the verification links between operations of V&V (which are stereotyped by "*TestCase"*) and system requirements. In this paper, only two basic system requirements, roots of the declinations, are considered in this diagram. Then, operations of V&V correspond to safety analysis. They are defined in the "*V&V*" package presented below.

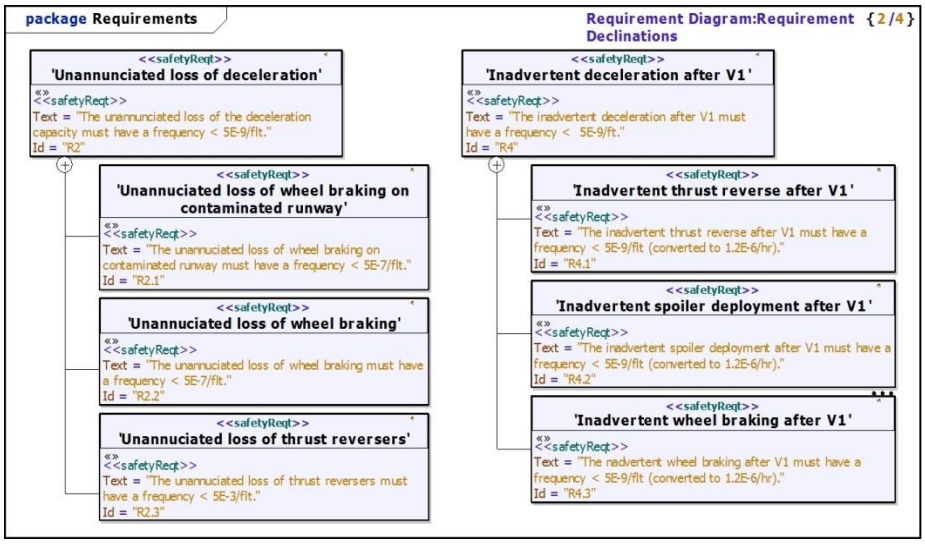

Fig.6. S18 aircraft – Requirement declinations diagram

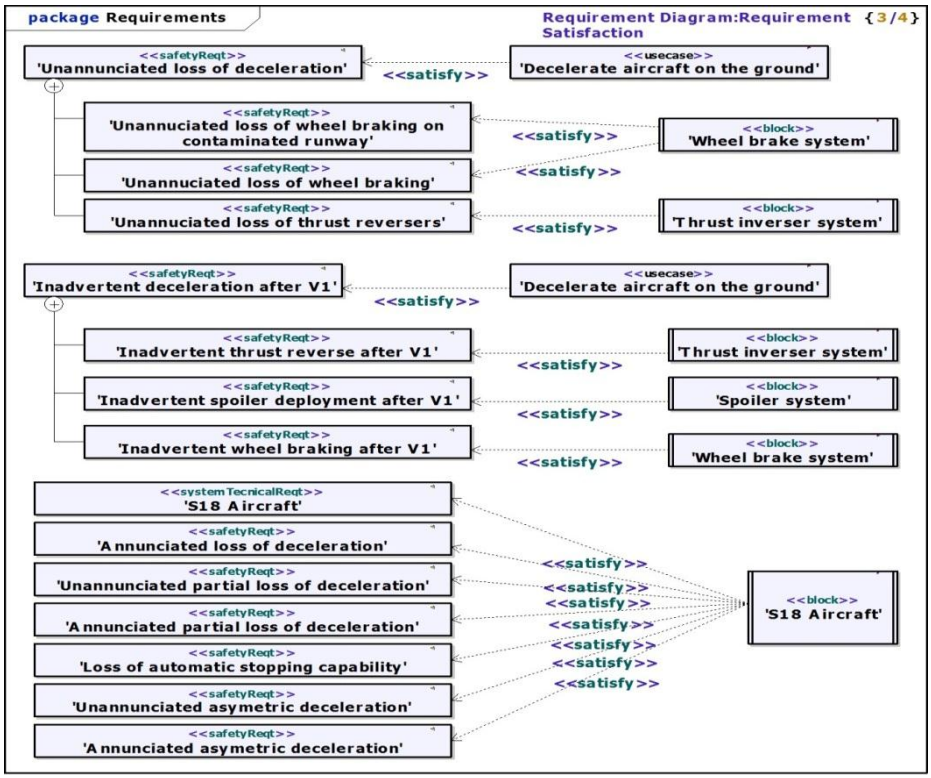

Fig.7. S18 aircraft – Requirement satisfaction diagram

Thus, the requirement named "*unannounciated loss of deceleration*" will be verified, according to the diagram, by the operation called "*loss of deceleration safety analysis*".

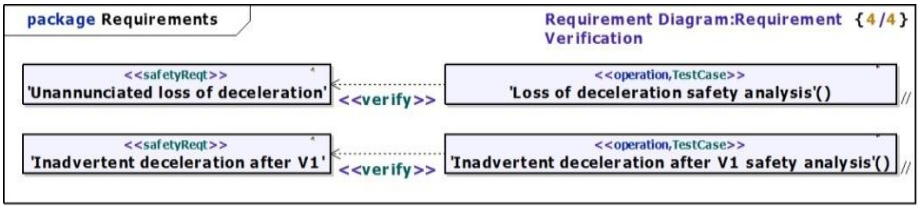

Fig.8. S18 aircraft – Requirement verification diagram

4.1.2 V&V package: test cases

The last package presented is the "*V&V*" package, which contains the test cases. It contains the diagram of Figure 9, which defines the two operations of V&V presented in the previous paragraph. For these operations, we associate comments in the diagram to specify them:

- For the operation "*loss of deceleration safety analysis*": analyze with the fault tree of the root event "*unannunciated loss of deceleration*".
- For the operation "*inadvertent deceleration after V1 safety analysis*": analyze with the fault tree of the root event "*inadvertent deceleration after V1*".

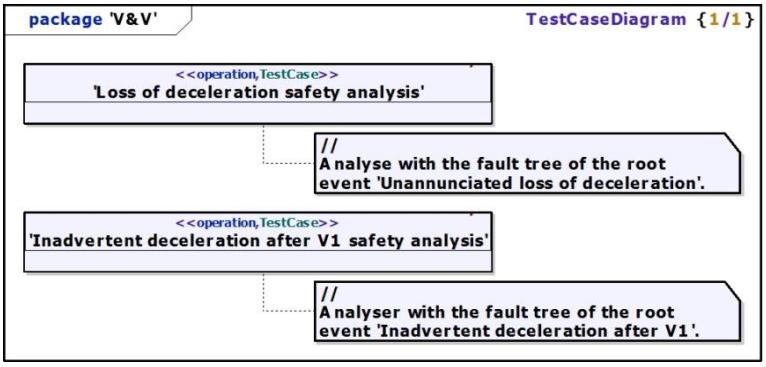

Fig.9. S18 aircraft – Test case diagram

In this paper, the two lower levels: the "wheel brake system" and the "BSCU calculator" are not presented. The same organization as the first level is considered.

5 Conclusion

Different concepts are handled in complex system design: requirements, design solution and V&V. An information model aims to help engineers in the expression of

these concepts, and the creation of traceability links between them in order to facilitate the comprehension and/or the impacts analysis. It also helps to formalize the practice of systems engineering through the use of models. The objective is to improve quality/productivity and to reduce risk by introducing rigor, precision, and communications among system/project stakeholders and managing complexity.

The present paper show how the information model can be used through a complex system which consists on braking system of an aircraft. The objectives are to demonstrate the contribution and the added value of the information model and the scalability of the approach. Some additional work is needed for the validation of this information model and will be considered in future work. It is, for example, interesting to define automatism to ensure consistency with the meta-model.

References

(1) Bar-Yam Y., *About engineering complex systems: Multiscale analysis and evolutionary engineering*, Engineering self-organizing systems: methodologies and applications 2005, vol. 3464, pp. 16-3. ISBN 3-540-26180-X.

(2) Guillerm R., Sadou N., and Demmou H., *Information model for model driven design of complex system based on system engineering approach*, International Conference on Complex Systems Design and Management (CSDM 2010), Paris (France), 27-29 October 2010, pp.99-111.

(3) Avizienis A., Laprie J.-C., Randell B., and Landwehr C., *Basic Concepts and Taxonomy of Dependable and Secure Computing*, IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 11-33, 2004.

(4) Juristo N., Moreno A. M., and Silva A., *Is the European Industry Moving Toward Solving Requirements Engineering Problems?* IEEE Software, vol. 19, no. 6, pp. 70–77, 2002.

(5) Sahraoui A.-E.-K., *Requirements Traceability Issues: Generic Model, Methodology and Formal Basis*, International Journal of Information Technology and Decision Making, vol. 4, no. 1, pp. 59–80, 2005.

(6) Sahraoui A.-E.-K., Buede D., and Sage A., *Issues in systems engineering research*, INCOSE congress, Toulouse, 2004.

(7) *EIA-632: Processes for engineering systems*, Electronic Industries Alliance standard, 7 January 1999.

(8) Martin J. N., *Overview of the EIA-632 Standard: Processes for Engineering a System*, Digital Avionics Systems Conference, 31 Oct-7 Nov 1998.

(9) Friedenthal S., Moore A., and Steiner R., *A Practical Guide to SysML: The Systems Modeling Language*, 576 The MK/OMG Press Series 2009.

(10) ARP-4761: *Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment*, Society of Automotive Engineers (SAE) standard, December 1996.

(11) Guillerm R., Sadou N., Demmou H., *Combining FMECA and Fault Trees for declining safety requirements of complex systems*, European Safety & Reliability Conference (ESREL 2011), Troyes (France), 18-22 Septembre 2011, 8p.