PhD thesis title: Executable Model-Based System Requirements Engineering (eMBRE) for early System requirements Validation and Design Verification (V&V)

This thesis work will be a contribution to an industrial chair. This chair involves Airbus, and two research laboratories, CRAN UMR CNRS and ERPI, from Université de Lorraine. Its main objective is to develop and experiment an Actionable Collaborative Trustworthy Executable (ACTE) Model-Based Systems Engineering (MBSE) framework, for early systems requirements validation and design verification and for the co-engineering of the main system and its manufacturing (or industrial) system.

Scientific issue

Designers need models and methods to perform early and collaborative Verification and Validation (V&V) respectively of system requirements and architectures (Chapurlat and Bonjour 2014), to detect specification and design errors and to avoid late and costly modifications, during the ground & flight test phase or even worse when the system is in operation. This approach ensures that system requirements at all layers and system design phases are trustworthy. The system requirement validation process aims to ensure the right system was built. The design verification process aims to ensure the system was built right. SE processes include requirements engineering based on the traceability of system requirements through the different system layers (Micaëlli et al. 2013). A text-based description is an ambiguous way for capturing and communicating system requirements, it leads system development teams to exchange incomplete, incoherent and incorrect descriptions of system requirements whereas executable model-based system requirements engineering (eMBRE) coupled with executable Concept of Operations open the opportunity to system requirements V&V: formally with proof-checking or factually with simulations reviewed with stakeholders. Executable" means that the model enables to support either proof-checking for formal system requirements validation or simulation for factual validation.

Systems Requirements Engineering (RE) is the result of iterative and recursive activities of definition, analysis and management (ISO/IEC/IEEE 15288: 2015). This process receives as input a list of needs and constraints from stakeholders, (i.e., customers, users, certification authorities), and transforms this list into technical (system) requirements that the system must satisfy in order to meet the needs. Requirements analysis is the activity that aims to verify the qualities of a requirement or a set of requirements, to negotiate changes, and to define the integration, verification and validation plans of the system. Requirements management is the activity of maintaining requirements along the life cycle of the system. In a complex system (system decomposed into subsystems and components at different layers), the requirements of subsystems are defined (or refined) through the system architecture. These transformations are potential sources of errors, therefore verification and validation activities (requirements analysis) should be led after each step. Today, most requirements are described in textual form, which does not allow for early detection of possible specification or design errors.

Moreover, there are different types of requirements (e.g., functional, performance, safety). ISO29148 or ARP 4754A standards define different qualities for a requirement or a set of requirements (e.g., consistency, completeness...). Different formal verification techniques exist but their application on complex systems seems difficult (scaling). In the field of Systems Engineering, different approaches

and tools have been developed in the last decade (Masmoudi et al. 2022), e.g., SysML Standard (omgsysml.org), Property Model Methodology (PMM) proposed by Micouin (Micouin 2008) (Micouin 2014), Stimulus software developed by Argosim and integrated in Dassault System's 3D Experience. The incoming version v2.0 of SysML will pay special attention on Property-Based Requirements (PBR). With PMM, Micouin proposed to model PBR using a set theory to describe the external relations of the system with its environment. These cause-effect assertions may be verified formally and factually. With Stimulus, the system engineer can model requirements with temporal logics expressions, being presented in a textual, natural language-like format. These properties can be completed with statecharts. The whole set can then be checked for consistency through simulated runs, or used as a basis for tests generation (Azzouzi et al, 2019).

In ISO 15288 and ARP 4754A standards, capturing complete, coherent and correct requirements is a key process. Our objective is to propose and experiment models and methods to support a collaborative and trustworthy eMBRE approach focused on the objectives of systems engineering (capture requirements with executable and therefore validable requirement models; design executable and therefore verifiable solution models), that shall be consistent with other SE processes, applicable for the development of key enabling systems (manufacturing, support & services), and able to prevent specification and design errors and foster collaborative approaches either on the overall SoI problem or on solution spaces. In this context, this PhD thesis aims to answer four main research questions:

- What are the needs for requirements modeling and V&V as well as their priorities.
- What are the appropriate formalisms according to the modeling and V&V needs?
- How to prove the qualities of requirements expressed by different languages and models?
- What are the requirements which is useful (in terms of benefit/cost/risk) to be further formalized?

Action plan

To provide contributions related to these questions, the following actions are possible:

- Elaborate a state of the art and a critical, comparative review of techniques and tools to verify and validate requirements.
- Define quality criteria to assess an eMBRE approach (particularly, based on current AIRBUS pain points for verifying requirements).
- Build a methodology to move from textual requirements to a verifiable model (formally or by simulation) allowing to verify the qualities of the requirements, at different stages of the multi-level system engineering process allowing to:
  - expressing the requirements without ambiguity and allowing them to be modeled,
  - represent multi-level modeling patterns (in particular, identification of inputs and outputs...)
  - model the system solicitations (formally or by scenarios)
  - verify that a set of requirements at system level respects a set of qualities
  - verify that requirements allocated and refined at the subsystem level respect a set of qualities (in particular, coherence and completeness with the system level requirements)
- Run use cases on the aircraft system to prove the interest of the proposed methodology
- Propose a framework for analyzing the usefulness (in terms of benefit/cost/risk) of formalizing and verifying requirement types or their quality

References

Azzouzi, Elmehdi, et al. "A survey on systems engineering methodologies for large multi-energy cyber-physical systems." 2019 IEEE International Systems Conference (SysCon). IEEE, 2019.

Chapurlat, Vincent, and Eric Bonjour. 2014. "From Model Based Systems Engineering to Model Based System Realization: Role and Relevance of IVTV Plan." Pp. 109–16 in *IFIP Advances in Information and Communication Technology*. Vol. 438. Springer New York LLC.

Masmoudi, Chedhli, Pascale Marange, Eric Bonjour, Eric Levrat, and Alain Kerbrat. 2022. "Adopting Formal Methods on Requirements Verification and Validation for Cyber-Physical Systems : A Systematic Literature Review." in *10th IFAC Conference on Manufacturing Modelling, Management and Control June 22-24, 2022, Nantes, France*.

Micaëlli, Jean Pierre, Samuel Deniaud, Éric Bonjour, and Dominique Loise. 2013. "How to Implement the Abstract Design Paradigm: The Case of Requirements Engineering." *International Journal of Product Development* 18(2):147. doi: 10.1504/IJPD.2013.053498.

Micouin, Patrice. 2008. "Toward a Property Based Requirements Theory: System Requirements Structured as a Semilattice." *Systems Engineering* 11(3):235–45. doi: 10.1002/sys.

Micouin, Patrice. 2014. *Model Based Systems Engineering: Fundamentals and Methods*. edited by Wiley-ISTE. Wiley-ISTE.

Keywords: Systems Engineering, Requirements Engineering, Modeling, Formal Verification, Validation
Partners: AIRBUS, Université de Lorraine (Laboratoire ERPI et Laboratoire CRAN UMR CNRS). The PhD student will be hired by the Université de Lorraine, for a 3-year period.
Beginning date: September/October 2022

Location: mainly at AIRBUS, Toulouse, France. Travel fees to Nancy will be in charge of the laboratory.
Applicant's profile. With a master degree or an engineer degree in computer science. Will be appreciated knowledge in the field of: formal verification, simulation (e.g., Matlab/Simulink), systems engineering, MBSE, requirements engineering.
Professional skills and motivation: autonomy, good writing in English, good interpersonal skills, motivation for action-research in aeronautics design offices.

Funding: Industrial Chair between Airbus and Université de Lorraine.
Net salary: about 1850€ per month.
Contact and applications. Co-supervisors :
Dr. Eric BONJOUR (eric.bonjour@univ-lorraine.fr), full professor, Université de Lorraine
Dr. Pascale MARANGE (pascale.marange@univ-lorraine.fr), associate professor, Université de Lorraine
Dr. Alain KERBRAT, MBSE expert, AIRBUS

Deadline for applications: June 24th, 2022

Date of answer to applicants: July 13th, 2022 (possibly after an interview and a recruitment exam)

Publication date: Nancy, May 25th 2022