Collaborative Safety Requirements Engineering: An Approach for Modelling and Assessment of Nuclear Safety Requirementsin MBSE Context

Emir Roumili, Jean-François Bossu, Vincent Chapurlat, Nicolas Daclin, Robert Plana, Jérôme Tixier

Roumili E., Bossu JF., Chapurlat V., Daclin N., Plana R., Tixier J. (2021) Collaborative Safety Requirements Engineering: An Approach for Modelling and Assessment of Nuclear Safety Requirements in MBSE Context. In: Camarinha-Matos L.M., Boucher X., Afsarmanesh H. (eds) Smart and Sustainable Collaborative Networks 4.0. PRO-VE 2021. IFIP Advances in Information and Communication Technology, vol 629. Springer, Cham. https://doi.org/10.1007/978-3-030-85969-5_20

Collaborative Safety Requirements Engineering: An Approach for Modelling and Assessment of Nuclear Safety Requirements in MBSE Context

Emir Roumili[1 2], Jean-François Bossu[1], Vincent Chapurlat[2], Nicolas Daclin[2], Robert Plana[1], Jérôme Tixier[2]

[1] Assystem, {eroumili, jfbossu,rplana}@assystem.com

[2] Laboratoire des Sciences des Risques (LSR), IMT mines Alès, Alès, France
{emir.roumili, nicolas.daclin, jerome.tixier, vincent.chapurlat}@mines-ales.fr

Abstract. The nuclear safety demonstration aims to demonstrate that a Nuclear Facility respects all the requirements specified in standards from safety authorities, which is a key objective for the licensing of a nuclear installation. It requires, firstly, supporting the necessary collaborative work involving various stakeholders. Secondly, it should be able to use a common and shared requirements repository. However, it is still the so-called "classic" working methods that are put forward. Almost all the documents are in written form. Due to the complexity of the Nuclear Facility of interest, it is proposed to move from this document-oriented system engineering to a model-based system engineering approach which would improve the performance, delay, and qualities of the engineering processes. Models would allow a better cognition and sharing without ambiguities of information by the engineering teams. Subject of this paper is a hybrid MBSE/AI approach facilitating collaborative work on nuclear safety demonstration processes.

Keywords: System Engineering, Collaborative work, Nuclear Safety Demonstration, Requirements, Information Research, Information extraction, MBSE, Licensing, Machine Learning, NLP.

1 Introduction

It is understood that Nuclear Power Plant (NPP) projects are becoming increasingly complex. If we take the example of a nuclear reactor, there are more than 50 buildings, 500 km of piping, 500,000 components and more than 100 million units of data (requirements, reports, schemes, etc.). The nuclear safety demonstration is at the heart of the nuclear industry. It is the most important element and remains a limiting factor for all nuclear activities. Globally, nuclear safety represents the sine qua non condition for the licensing of installations. Indeed, even though nuclear energy is very low-carbon and represents 72% of the total electricity production in France in 2019, it remains an energy that worries the public opinion. [1] It is therefore important that all nuclear activities are fully controlled from a safety point of view. To ensure that all operations are carried out safely, a validation of the demonstration of safety is mandatory to obtain the license to build, operate, dismantle, etc.

The demonstration of safety is defined as follows: "*Assessment of all aspects of a practice that are relevant to protection and safety; for an authorized facility, this includes siting, design and operation of the facility.*" [2]

In this context, any demonstration of safety is part of an industrial project and is therefore a balance between different constraints of scope, schedule, budget, quality, resources, etc. [3]

The nuclear safety engineer calls upon the various disciplines present in the project to jointly carry out the safety demonstration of the installation.This safety demonstration is based on iterative and collaborative processes. Despite the difficulty in terms of collaboration, efficiency and productivity, a classic document-oriented approach is used to achieve this demonstration of safety. We propose a digital-based approach, which could be complementary to the work on documents. This approach draws its strengths from Artificial Intelligence (AI) and from the use of system engineering/MBSE. This paper illustrates the MBSE contribution in the whole safety demonstration methodology. Readers interested by AI contributions can have a look on [3] .

We will first present the problematic that underlies our work. The second section discusses our proposed contribution in the context of this problem. The last section proposes a concrete case to illustrate our approach.

2 Problematic and SoA

The nuclear safety demonstration is at the interface of several disciplines and constitutes the argument presented to the nuclear safety authorities justifying that the installation is, in its various phases of its life cycle (design, operation, decommissioning etc.), a safe facility. It represents a real challenge of collaboration between actors from different fields, with different levels of responsibilities and since the begin of the whole design and development project. Obviously, all of these actors must have a minimum level of understanding of the safety issues relating to the installation they are designing as part and all along their project. In the design phase of the project, they have to collaborate, define, trace rigorously and confidently all the requirements, architectural choices, intermediate results of evaluation and analysis, decisions, tests to be carried out for commissioning, etc. This work is carried out, as in many areas of engineering, through a document-oriented approach. These documents are not read then interpreted by all actors in the same way, some will read them completely, others partially, and still others will not read them at all. Indeed, this represents a time commitment, and time is often lacking in projects. Even for those with a full reading of the safety-related documents, the biases of their own experience and reflection will be mixed with the written information, the latter leave more or less room for subjective interpretation. This could have an impact on the cognition of these complex subjects in terms of information gathering and processing, as well as the possibility of using more often heuristics in their judgement on certain items. [4] In this way, system engineering (SE)

[5] allows these actors to take more attention and manage more efficiently the complexity of both the so-called system of interest to be designed and built, here considered a Nuclear facility, and the so-called system used to engineer, i.e. the project itself. So, SE based on systemic principles, proposes more suitable processes and promotes particularly modelling activities and models handling in opposition to documents management.In this sense, as stated during INCOSE Symposium in 2007 [6] Model Based System Engineering (MBSE) "*enhances the ability to capture, analyze, share, and manage the information*" This engineering approach that inherits from SE allows a better cognition and information sharing between engineering teams with less ambiguities by using models, highlighting the following benefits:

- Improved communications.
- Increased ability to manage system complexity.
- Improved product quality.
- Enhanced knowledge capture.
- Improved ability to teach and learn systems engineering fundamentals.

The MBSE approach is more and more used and well known in the nuclear world [7] [8]. However the elements related to the demonstration of nuclear safety remain poorly considered, and there is then a problem in the appropriation of the modelling way usages and analysis of models, by nuclear engineers.

As detailed in section 3, the classic approach to the demonstration of safety is described in IAEA (International Atomic Energy Agency) documents such as the GSR (general safety requirements). For Nuclear Power Plants, the SSR-2/1 describes this process and presents the main safety principles and concepts that must be fulfilled throughout the facility lifecycle. [9] The hazards to be addressed are then declined in lower level safety guides.

Driven by the Environmental law, the French regulation adds more general principles to those technical concepts. For instance, it is based on the responsibility of the owner of the plant and on the performance obligation rather than the obligation of means.

The French nuclear facility decree of 7 February 2012 is the one put forward in our work, allowing engineers to model more naturally, to use and to be confident with modelling activities and models. [10] We will see in the next section the operational approach and the concepts put forward by the safety authorities to move towards the safety demonstration.

3 Contribution

In our work, we consider the possibility of achieving this demonstration of safety being based on the principles of systems engineering: 1) by using systemic principles, 2) by following SE main processes that are collaborative and iterative throughout the project, and 3) by promoting the intensive use of models.

With regards to SE processes, two ways are used to establish and promote multi-actors collaboration during a project:

1. The classic approach of having milestones and reviews. When the milestones are reached, a review is carried out of the work and a decision is made whether as to validate the proposed design.
2. Refocus and share continuously an up to date requirements repository between all stakeholders of the project: engineers, business actors, customer, operator and authorities representatives at least.

Thus, to improve the level of demonstration, the proposed method does not oppose these two paths. However, it focuses on a requirements repository that would have the 'right' properties, i.e. composed of SMART requirements. This implies making available a formalized requirement modelling language as proposed in various works, allowing actors: to trace, assume the completeness and coherence of requirements, but also to refine, decompose, rewrite any requirement in a semantically equivalent way for the needs of certain domains by adapting to the domain vocabulary.

Thus, the elements quoted previously of the classical approach to safety demonstration have all been assimilated to requirements because they constitute a "contract" between the operator and the safety authority. [11] Indeed, a requirement is a *"statement that translates or expresses a need and its associated constraints and conditions"* [12]

Our analysis of the expected safety demonstration leads us to consider the following elements :

- **Interests Protection Functions** (formally denoted as "FPI" in french litterature): functions that, if compromised, could result in radioactive releases or damage to the environment, the public or employees (referred to as "interests" in french regulation [13])
    - Here we will have an identification, based on an initial design, of the types of risks that may affect the facility, which could compromise an FPI. We will then select from a list of generic FPIs the one that applies to the facility of interest, based on the risks identified.
- **Safety Requirements** (formally denoted as "EX" in french litterature): for each type of risk, definition of the safety requirements to be taken into account for conducting the risks analyses and design: these are general design principles, "primary" safety requirements (e.g., "absence of dissemination in the event of an earthquake"), which serve as input data for the safety analyses.
- **Expected Characteristics** (formally denoted as "CA" in french litterature): performance of design based risk analyses (iterative process with the technical design engineers) and the safety requirements. CA are "second level" requirements. They are the result of the risk analyses. They are broken down by technical batch and are thus directly applicable by the technical design engineers. A "primary" safety requirement generally generates several CAs.
- **Defined Requirement** (formally denoted as ED in french litterature): in an iterative way with the previous point, the design is carried out by the technical trades based on the CAs. These are the technical measures proposed by the technical design engineers to meet the CAs. An ED applies to a system or sub-system. Thus, several EDs may be required to meet a CA.

An FPI requirement will give rise to several EXs. An EX will give rise to several CAs and so on.

The terms used in our description of the safety demonstration are related to the regulatory semantics of nuclear power. [10] A parallel was made with the corresponding concepts in system engineering in working groups comparing the semantics/concepts of nuclear safety engineering and system engineering. It was considered more interesting to link all the elements introduced to the notion of requirements. The types of requirements, the relationships between requirements, the allocation relationships between requirements and functions or components allow great flexibility in the correct conceptualisation and specification of these ones considering the nuclear safety demonstration objectives.

As explained, considering these elements as "requirements" provides a great flexibility in the links that can be chosen to describe, for example, the transition from a CA to an ED. The literature on requirements engineering and recent work allow judicious choices to be made on these points in order to be as close as possible to the spirit intended by this division and this hierarchy intended by the nuclear safety domain.

Following this discussion, [14] proposes various relationships between requirements. Three of them are of particular interest to us:

- Decomposition: this consists of decomposing a requirement into several requirements in order to reduce its complexity, possibly making of different natures, both functional and non-functional, appear.
    - Relationship between : FPI to EX and EX to CA.
- Derivation: this relationship allows a new requirement set to be derived from a requirement set in order to specify the behaviour or state of a system when it is in a particular configuration. This relationship allows the abstraction level of the requirements to be changed.
    - Relation between a higher level ED and a lower level ED.
- Refinement: the purpose of requirement refinement is to add detail to a requirement, often in cases where the abstraction of a requirement is too strong. This requests then allows a set of requirement of the same nature as those that being refined to appear.
    - Relation between CA and ED.

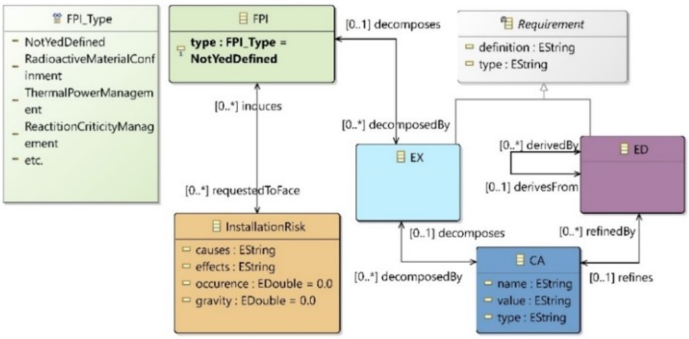

Figure 1: meta model of the method (partial view)

Figure 1 shows a simplified version of the main concepts and relationships between concepts that are presented in the text. This is a part of a global metamodel that allows us to formalise, structure and detail all the concepts, attributes and relationships that will be used in order to bridge the gap between MBSE domain and Safety demonstration domain.

4 Illustrative Case

In SE, a viewpoint model is a“*representation of a whole system from the perspective of a related set of concerns.*” [15] With this method we try to provide a safety view to the architecture models of new or ongoing projects.

This method is currently being implemented within an application project. We will present in this section the first elements of this method presented before. Prior on testing the approach, many exchanges with experts in the field of safety have been requested to understand the main processes that compose it.

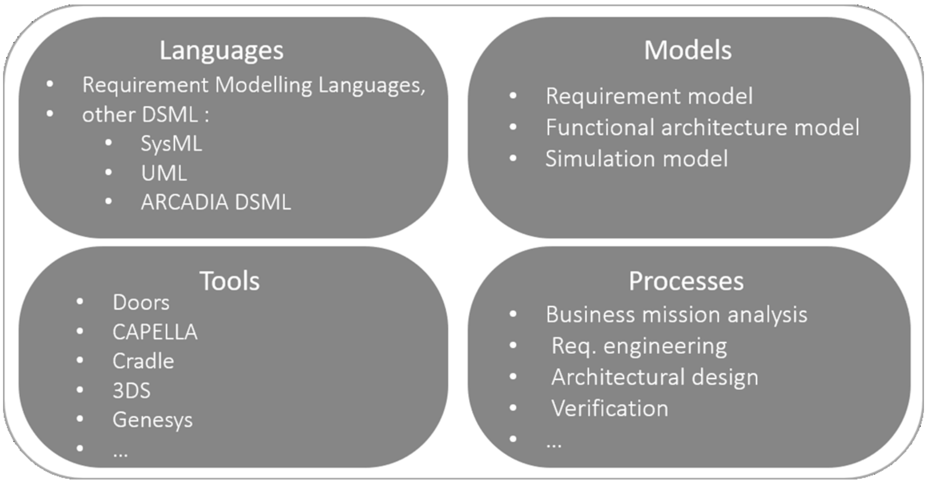

Figure 2: MBSE Pilars

Also, in order to have research work that will be valued and put into practice in our projects we make sure to have a coherent development around the four pillars of MBSE (see Figure 2) i.e. to have a research which covers these 4 pillars with a reflection on the models, on the processes which will allow their implementation, on the language used as well as the selected tool. These reflections must allow the proposal to be adapted to real application cases

It was therefore necessary to observe the current state of the MBSE approach within the compagny in order to develop a safety view, integrated with the multiple views offered by the MBSE approach, which could be adapted to the habits already present among our engineers. For several reasons, it is the Capella tool [15] from Thales that is the most used within the group. It is therefore around this software, the Arcadia method [16] and the Arcadia DSML language [15] [16] that we are integrating our current research to move towards the demonstration of safety.

Our work focuses in particular on processes, with a proposed methodology for integrating nuclear safety into the proposed installations models. Of course, the methodology may have software limitations that prevent the implementation of the new methodological elements provided. This could be overcome by modifications to the software, which is made possible by the open source nature of this software (i.e. Capella).

Figure 3 shows an example of a requirements decomposition structure diagram that allows us to trace the origin of a particular requirement in our model while respecting the requirements types (see meta model in Figure 1) specific to nuclear safety as presented above.

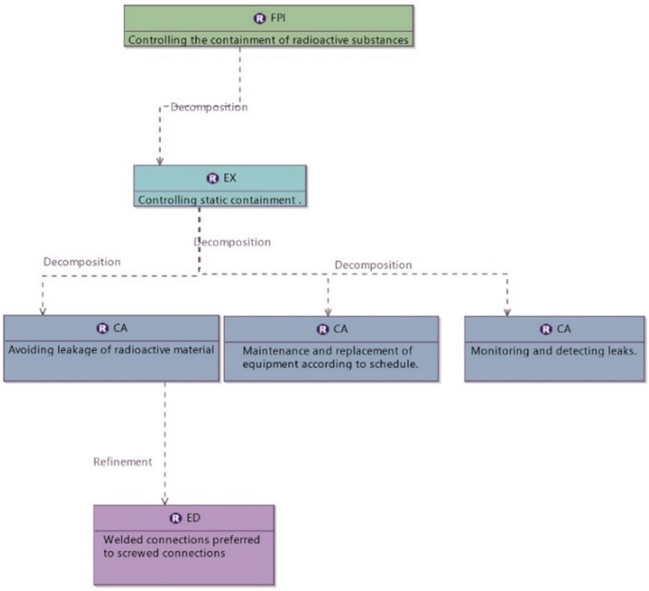
FPI
Controlling the containment of radioactive substances
Decomposition
EX
Controlling static containment .
Decomposition
Decomposition
Decomposition
CA
Avoiding leakage of radioactive material
CA
Maintenance and replacement of equipment according to schedule.
CA
Monitoring and detecting leaks.
Refinement
ED
Welded connections preferred to screwed connections

Figure 3: RBS

This method, illustrated in Figure 4, is a part of our proposed methodology in a MBSE context for nuclear safety demonstration. As shown in our big picture, the collaborative aspect is intrinsic to the work related to nuclear safety demonstration. This collaboration, if well conducted, allows each discipline to contribute its expertise in the best possible conditions in order to provide an optimal safety of the installation. The work of the nuclear safety engineer is not done alone but in interaction with all field of competencies. Moreover, projects in nuclear industry involve the nuclear safety engineer from start to end. In collaboration with the project manager and the technical manager, he must be able to check that each of the design proposals of the installation will ensure the protection of interests (security, public health and safety, protection of nature and the environment). [13]

Our proposal attempts to bring to the conduct of these projects the benefits of a Model-Oriented methodology rather than a Document-Oriented one. In order to achieve this, our work focuses on finding solutions to take into account nuclear safety in these models. These models constitute the common basis for collaboration between these different fields of expertise.

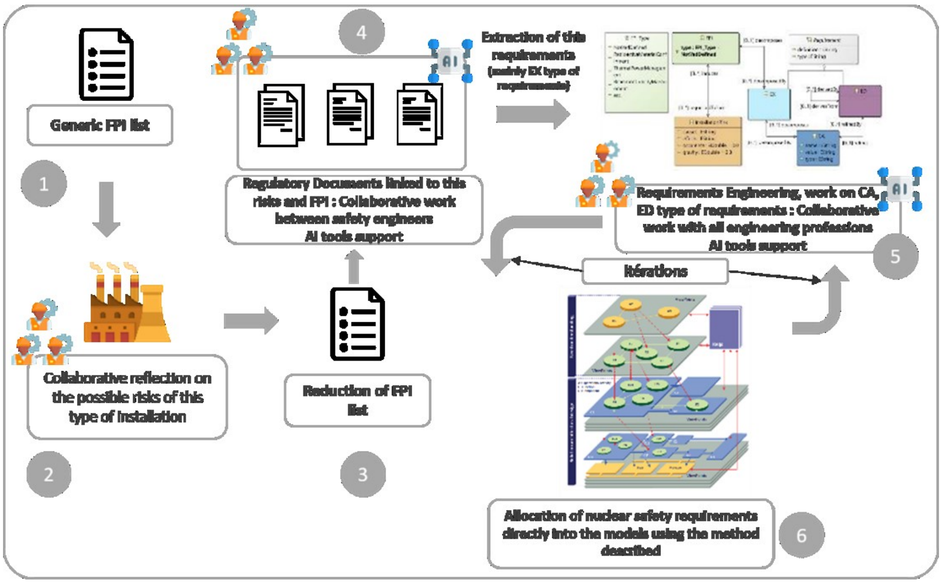
Generic FPI list
1
Collaborative reflection on the possible risks of this type of installation
2
Reduction of FPI list
3
4
AI
Regulatory Documents linked to this risks and FPI : Collaborative work between safety engineers
AI tools support
Extraction of this requirements
(mainly EX type of requirements)
Requirements Engineering, work on CA, ED type of requirements : Collaborative work with all engineering professions
AI tools support
5
Itérations
Allocation of nuclear safety requirements directly into the models using the method described
6

Figure 4: Big picture of proposed method

5 Conclusion and Perspectives: A Way to Safety Demonstration

We have presented here the first steps of the methodology we propose on the way to the demonstration of nuclear safety. A deep understanding of both engineering (nuclear safety and systems engineering) is necessary to propose the coherent concepts of the former for application to the latter.

The demonstration of safety, as the name implies, involves demonstrating to the safety authority that the installation is safe for the outside world, the environment, and the workers. To demonstrate this, it is necessary to rely on consistent evidence, which is contained in the safety requirements in relation to the systems and activities they specify. The next step is to propose the methodology for moving from this evidence to the demonstration itself. The elements we find of interest to exploit are the notions around evaluation criteria, technical indicators including measures of effectiveness (MOE) and performance indicators (MOP). [17] These elements could be coupled with our CA type requirements which includes expected characteristics from systems.

It is essential that the stakeholders grasp the issues and understand the elements of the demonstration, which makes it a collaborative work by excellence with a strong objective: to obtain the licence allowing the installation commissioning. There is no doubt that this highly collaborative work is facilitated using models.

Although we did not mention it in this paper as it was not the purpose, the model-based approach is complemented by the use of AI on safety demonstration tasks that can be learned from the data. It is applied in those tasks of the safety demonstration that lend themselves to the inductive approach to facilitate the work of engineers. (automatic extraction of requirements for example [3]).

In the end, it is a set of processes brought together in a tool-based methodology that will enable more productive collaboration of stakeholders in projects that include a nuclear safety demonstration.

References

[1] Statista, "L'énergie nucléaire en France - Faits et chiffres," 2017. [Online]. Available: {https://fr.statista.com/themes/2752/l-energie-nucleaire-en-france.

[2] IAEA, Safety Glossary STI/PUB/1290, International Atomic Energy Agency, 2007.

[3] PMI, Project Management Body of Knowledge (PMBOK GUIDE) 5th Edition, Project Management Institute, 2013.

[4] J. Baron, Thinking and Deciding, Cambridge, 2007.

[5] ISO, ISO/IEC 15288 Systems and software engineering — System life cycle processes, ISO, 2008.

[6] Sanford Friedenthal, Regina Griego and Mark Sampson, "INCOSE Model Based Systems Engineering (MBSE) Initiative," in *INCOSE 2007 symposium*, San Diego, 2007.

[7] Juan Navas, Philippe Tannery, Stephane Bonnet and Jean-Luc Voirin, "Bridging the gap between model-based systems engineering methodologies and their effective practice – a case study on nuclear power plants systems engineering," *INSIGHT,* vol. 21, no. 1, 2018.

[8] Miao Zhuang, Xu Zhao and Zhao Siqiao, "Study on the NPP general operation strategy design method based on MBSE," *Proceedings of the 27th international conference on nuclear engineering (ICONE-27),* 2019.

[9] IAEA, "Safety of Nuclear Power Plants : Design," Vienna, 2007.

[10] Légifrance, *Arrêté du 7 février 2012 fixant les règles générales relatives aux installations nucléaires de base,* France, 2012.

[11] INCOSE, « INCOSE SE Terms Glossary », 1998.

[12] ISO, ISO/IEC/IEEE 29148, 2011.

[13] Légifrance, *Article L. 593-1 du code de l'environnement,* 2012.

[14] L. Lori , "Conception d'un système avancé de réacteur PWR," 2018.

[15] ISO/IEC, "ISO/IEC 10746-1, Information technology — Open Distributed Processing — Reference model: Overview," ISO/IEC, 2009.

[16] P. Roques, "MBSE with the ARCADIA Method and the Capella Tool," in *8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)*, Toulouse, 2016.

[17] Thalès, "ARCADIA - Méthode pour l'ingénierie des systèmes soutenue par son langage de modélisation conceptuel - Description Générale," AFNOR, 2018.

[18] M. Lo, "Contribution à l'évaluation d'architectures en Ingénierie," 2013.

[19] AIEA, Licensing Process for Nuclear Installations (SSG-12), Vienne, 2010.

[20] E. Roumili and et al, "Requirements Engineering enabled by Natural Language Processing and Artificial Intelligence for Nuclear Safety Demonstration.," *11th Complex Systems Design & Management (CSD&M) conference,* 2020.