Contribution to Nuclear Safety Demonstration Through System Modelling and Artificial Intelligence

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

Contribution to Nuclear Safety Demonstration through System Modelling and Artificial Intelligence.

Emir Roumili, eroumili@assystem.com; Jean-François Bossu, jfbossu@assystem.com; Vincent Chapurlat, vincent.chapurlat@mines-ales.fr, Nicolas Daclin, nicolas.daclin@mines-ales.fr; Jérôme Tixier, jerome.tixier@mines-ales.fr, Robert Plana, rplana@assystem.com

Abstract

Nuclear Power Plant (NPP) engineering projects become increasingly complex. For instance, a nuclear reactor includes more than 50 buildings, 500 km of piping, 500,000 components and 100 million units of data (requirements, reports, schemes…). However, nuclear safety demonstration of any nuclear facility is at the heart of the nuclear industry, being the most important and limiting factors for all requested engineering activities. Ensuring all these activities are performed considering safety demonstration is mandatory to get permission to license, build, operate, dismantle, etc. This article synthetizes an innovative methodology that mix and take advantages of Artificial Intelligence techniques and System Engineering principles, processes, and is based on Model-Based System Engineering principles and usages. This methodology aims to guide and support engineers to improve their vision, their knowledge and vocabulary, and their capacities in terms of, first, safety requirements elicitation, and second of safety requirements demonstration.

Keywords: Nuclear Safety, Systems Engineering, Model Based System Engineering, Requirements Engineering, Machine Learning, NLP, Licensing

Introduction

Nuclear Power Plant (NPP) engineering projects are becoming increasingly complex. For instance, a nuclear reactor includes more than 50 buildings, 500 km of piping, 500,000 components and 100 million units of data (requirements, reports, schemes…). Safety demonstration of such NPP becomes then more difficult. The safety demonstration is defined as the "*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.*" [1]. It is mandatory and a priority in projects having different constraints of scope, schedule, budget, quality, resources… [2]. Indeed, the research, analysis, organization, and links that need to be established between reference documents and the installation or activities being demonstrated, can quickly become time-consuming and costly. The reduction of time and costs facing a competitive industrial world may lead to incomplete analysis, which will not be accepted by the safety authority and lead to cost drifts. For this, among other expectations, engineers and architects must face safety requirements engineering and analysis activities all along the project.

System engineering (SE) [3] [4] has proven advantages in various industrial fields for carrying out complex systems engineering projects. It promotes concepts, principles, and processes, but also the use of models as early as possible in the project. It is the purpose of Model Based System Engineering (MBSE) [5] that considers modelling and use of models all along engineering projects. The research question is then: How to integrate the use and manipulation of the expected safety concepts and safety demonstration approaches in line with MBSE approach allowing to manage cost, quality, and duration considering that safety demonstration must be mastered from a lean engineering perspective?

This article introduces a method aiming to guide and support engineers and architects deploying and conducting safety demonstration. By assumption, this method assumes crossing both model (MBSE context) and data-centric approach (AI tools and techniques), instead of the document-centric approach currently used. The goal is to describe method part that concerns and focuses on safety requirements engineering activities [6]

Contribution

Error! Reference source not found. illustrates approach to safety demonstration as practiced in the nuclear industry by using element presented lower. It is in points 4,5 and 6 that we find our addition of AI and MBSE approaches in relation to 3 pillars detailed in the next part. A more detailed explanation of this contribution can

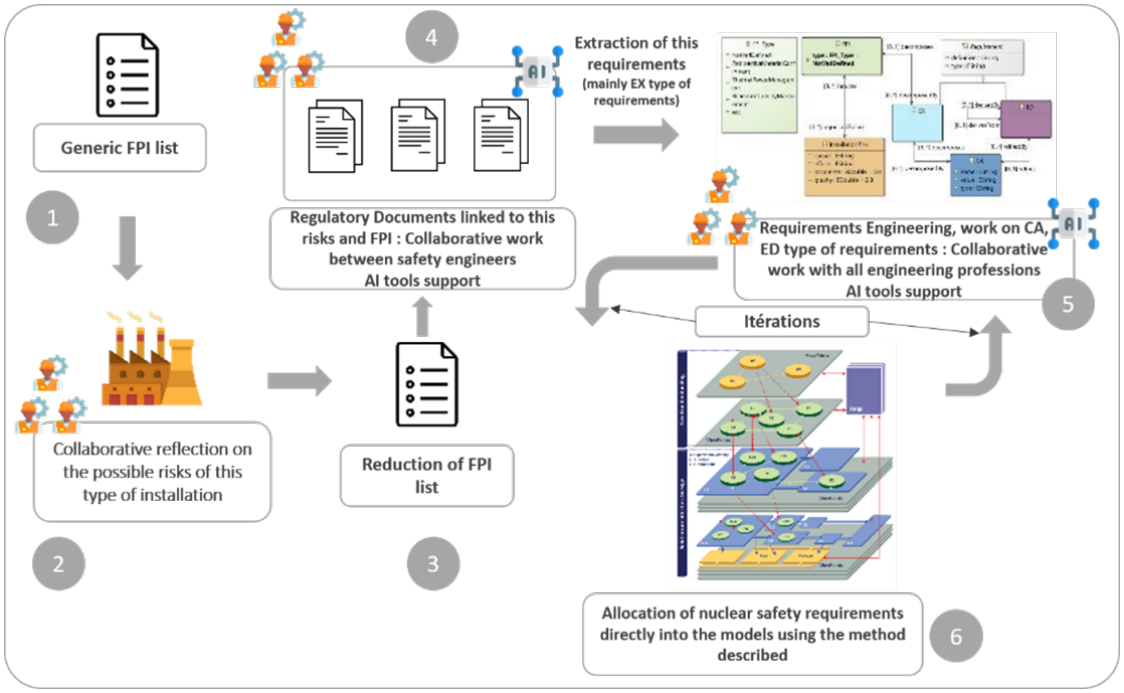

Figure 1 Big picture of proposed method

be found in [7] [11].

The proposed method relies on the following three pillars:

- **Pillar 1**: **Set of nuclear safety requirements.** Demonstration of nuclear safety is a long, iterative process requiring a thorough analysis of regulatory texts (International Atomic Energy Agency (IAEA), French Nuclear Safety Authority (ASN), feedback…). This analysis will lead to a use of these texts with an industrial objective: **"Demonstrate that a particular activity or installation is safe in our country's nuclear safety authority's regulation",** considering regulatory requirements and contractual aspects to move towards demonstrating the safety of nuclear critical installations and infrastructures. Statistical models from connectionist AI (inductive approach) require training on specific tasks and identified with quality datasets and validated by domain experts. It is worth considering this:
  - A corpus of qualitative requirements has been created; based on the aggregation of various documents of the International Atomic Energy Agency (1141 requirements).
  - Training of the BERT model (Natural Language Processing algorithm from Google AI teams [6]) is done on the recognition of safety requirements. The dataset used for the training was the IAEA requirements corpus (the choice of BERT is argued in [7]). This makes various concepts and relations between these concepts emerge that are requested to address the Pillar 2. Indeed, this analysis allows us to set up parts of the safety demonstration that lend themselves to the use of a connectionist (inductive) approach of the AI. A second set of data of interest will allows us to train our algorithms on a Corpus of qualitative requirements based on the 'Codes of rules for design and construction" (RCC's) [9]. The deployment of trained algorithms on current datasets requires webapps, and APIs allowing engineers to use them.
- **Pillar 2: MBSE for nuclear safety.** The immersion in MBSE context [5] [8] deals with:
  - Engineering and management of safety requirements: This integrates work on the rewording of requirements and mass processing of textual data to identify the requirements applicable to installation systems (semantic search, clustering…) by applying supervised and unsupervised algorithms adapted to nuclear safety processes.

- Architectural design: multi-views and multi-paradigms modelling of installations, linking requirements and traceability of the latter by means of these models to ensure analysis and move towards the desired safety demonstration.

As a first approach, analysing how nuclear safety demonstration is conducted in the industrial world leads us to consider the following elements:

- **Interests Protection Functions** ("FPI" in French literature): functions that, if compromised, could result in radioactive releases or damage to the environment, the public or employees ("interests" in French regulation [9]). Considering the initial design of the power plant, the types of risks that may affect the facility, which could compromise a FPI are analysed. From that, a list of generic FPIs that must be preserved on the facility of interest is established.
- **Safety Requirements** ("EX" in French literature): for each type of risk, definition of the safety requirements for conducting the risks analysis and design: these are general design principles, "primary" safety requirements (e.g., "absence of radioactive material dissemination in the event of an earthquake"), which serve as input data for the safety analyses.
- **Expected Characteristics** ("CA" in French literature): performance of design-based risk analysis (iterative process with the technical design engineers) and the safety requirements. CA are secondary requirements. They are the result of the risk analysis. They are broken down by technical batch and are directly applicable by the technical design engineers. A "primary" safety requirement generally generates several CAs.
- **Defined Requirement** ("ED" in French literature): 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.

A 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 is made with the corresponding concepts in system engineering in working groups comparing to the semantics/concepts of nuclear safety engineering and system engineering. It is considered more interesting to link the FPI to the concept of "function" in SE and all other elements introduced to the notion of requirements.

The contribution to this Pillar 2 is formalized as a metamodel integrating more than 40 concepts, their inter-relationships as well as their attributes. This will allow the integration of the safety demonstration into general MBSE methodologies, thus facilitating collaboration between safety teams and project teams on shared models.

- **Pillar 3: Digital modelling tools.** This methodology will rely on an ecosystem of tools. Usually, safety guided engineering and analysis activities are mainly done manually with a written approach. This impedes a global vision of the safety demonstration and takes more time than the proposed approach. These tools will enable working faster, in agreement with time and completeness expectations from the regulations, and to have a better vision of the requirements demonstrated and their traceability throughout the project, i.e., over several years (the construction of a reactor takes about 6-10 years). The modelling tool will require an alignment of our metamodel with that of the software in which the integration will take place. It is necessary to identify equivalent and missing concepts and to propose an extension of the metamodel that will include the elements that will allow safety engineers work.

Application

An application of the tools and concepts to a real case is being developed on a project with a high "nuclear safety" stake for the company in charge of the EPCm (Engineering, Procurement, Construction management) and for its nuclear operator. The objective is to measure the contribution of AI and MBSE to an operation that is complex enough to raise frequent questions and to feed the dialogue with the safety authorities, while being sufficiently comprehensive for all the issues to be integrated into the developed approach.

Validation

The question of the validation of the method naturally arises. In this context, it will be the use in the context of nuclear projects including safety demonstrations that will allow us to verify the interest of such a method based on the digitalisation of processes permitted by the field of MBSE and AI. It will be necessary to increase the competence of the teams in this type of modelling.

However, our methodology would benefit from partial validation if it could be applied to a concrete case because:

- The elements on which it is based, and our metamodel, are those recommended by the safety authorities for demonstration purposes. The contribution of the digital approaches does not contravene the typical safety's demonstration.
- Also, this work is based on elements that exist in the state of the art and have been proven (e.g. metamodels approach), so we gather valid elements between them to result in a new methodology applied to a new field but based on a solid approach.
- The supervision of this work is therefore carried out in the context of a company with expertise in the subject and, by people with expertise in the field of nuclear safety. The feedback on our work from these people is of interest in the context of this partial early validation.

Finally, in the nuclear industry, there are high risks that the license for projects construction and commissioning might be delayed or never obtained due to lack of traceability or of reproducibility. To reduce these risks, the use of digital techniques is essential due to the number of costly non-conformities in most complex projects. In this context, we propose the combination of SE and AI and its application through the demonstration of nuclear safety, a highly complex discipline only addressed in a document-oriented way.

This convergence between data centric approach and MBSE will ensure the digital continuity throughout the project and minimize errors, bottlenecks propagating from licensing to design, construction, commissioning, and operations translating into major time and costs overrun observed for the majority of NPP projects.

References

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

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

[3] ISO/IEC JTC 1/SC 7 Software and systems engineering, ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes, 2015.

[4] S. E. B. 2020, The Guide to the Systems Engineering Body of Knowledge (SEBoK), v.2.2, R.J. Cloutier (Editor in Chief). Hoboken, NJ: The Trustees of the Stevens Institute of Technology..

[5] B. Schindel, «INCOSE Model-Based SE Transformation, Aerospace Corporation System Engineering Forum,» 2018.

[6] D. Jacob, M.-W. Chang, K. Lee et T. Kristina, «BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding,» *2019 Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL),* 2018.

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

[8] J.-L. Voirin, Model-based System and Architecture Engineering with the Arcadia Method, ISTE Press - Elsevier, 2017.

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

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

[11] E. Roumili et e. al, «Collaborative safety requirements engineering: an approach for modelling and assessment of nuclear safety requirements in MBSE context,» *PRO'VE,* 2021.