Moving Toward Product Line Engineering in a Nuclear Industry Consortium

Sana Ben Nasr, Nicolas Sannier, Mathieu Acher, Benoit Baudry

Moving Toward Product Line Engineering in a Nuclear Industry Consortium

Sana Ben Nasr, Nicolas Sannier, Mathieu Acher, and Benoit Baudry
Inria / IRISA, University of Rennes 1, France
{sana.ben-nasr, nicolas.sannier, mathieu.acher, benoitbaudry}@inria.fr

ABSTRACT

Nuclear power plants are some of the most sophisticated and complex energy systems ever designed. These systems perform safety critical functions and must conform to national safety institutions and international regulations. In many cases, regulatory documents provide very high level and ambiguous requirements that leave a large margin for interpretation. As the French nuclear industry is now seeking to spread its activities outside France, it is but necessary to master the ins and the outs of the variability between countries safety culture and regulations. This sets both an industrial and a scientific challenge to introduce and propose a product line engineering approach to an unaware industry whose safety culture is made of interpretations, specificities, and exceptions.

This paper presents our current work within the French R&D project CONNEXION, while introducing variability modeling to the French nuclear industry. In particular, we discuss the background, the quest for the best variability paradigm, the practical modeling of requirements variability as well as the mapping between variable requirements and variable architecture elements.

Categories and Subject Descriptors

J.7 [**Computer Applications**]: Computer in other Systems; D.2.1 [**Software Engineering**]: Requirements

General Terms

Legal Aspects, Experimentation

Keywords

requirements variability modeling, regulations, product line engineering, variability mining

1. INTRODUCTION

Nuclear power plants are some of the most sophisticated and complex energy systems ever designed. Nuclear safety covers the actions taken to prevent nuclear and radiation accidents or to limit their consequences. This covers nuclear power plants and, more particularly, their instrumentation and control systems (I&C), which have been using more and more digital devices since the middle of the 1980's. Countries utilizing nuclear power have special institutions overseeing and regulating nuclear safety. Nuclear industry projects must comply with regulatory safety requirements and recommendations that are expressed in large and heterogeneous documents: legal texts, international standards or even regulatory specific positions.

Due to the lack of international consensus on regulatory practices [17], the willingness to build such systems in different countries requires to face practices of several safety authorities and can challenge the initial system design [13]. Therefore, it is necessary for our industrial partners to find similarities in regulations in order to minimize the basic design efforts and its qualification. The French nuclear industry and academic partners have joined forces in the CONNEXION project to develop the major innovations in the design and implementation of the future nuclear power plants' I&C systems. One aspect of the project consists in the formalization, from a general and high level perspective, of both requirements and architecture elements variabilities.

Introducing a software product line engineering approach in this domain, which has a long history of exceptions and individualities, sets both scientific and industrial challenges. (Q1) How to introduce variability modeling to nuclear engineers? (Q2) What is the best variability modeling paradigm, accordingly to the domain practices? (Q3) How to deal with the search space in regulatory corpora and what is the right granularity level for modeling variability in requirements? (Q4) How to bind a requirements variability model and an architecture variability model in order to derive an architecture that conforms to a requirements configuration?

In this paper, we address in particular the retrieval of a variability model from regulatory requirements and its mapping to an architecture developed by a Nuclear consortium. The contribution of the papers are: 1. an approach to model variability in regulatory requirements, capture architectural variability and investigate the robustness of the architecture against requirements variability; 2. an illustration of the approach and tooling support on a realistic use case we have conducted with industrial partners; 3. lessons learned about the introduction of variability in this particular domain as well as upcoming challenges.

The remainder of the paper is organized as follows. In Section 2, we introduce a quick picture of the current nu-

clear regulatory requirements landscape and discuss the lack of variability awareness of the nuclear industry. Section 3 presents research background. Section 4 gives an overview of the proposed approach. Sections 5 and 6 describe the overall variability approach. Section 7 describes the different techniques used to implement our method and their applications in the context of the CONNEXION project. Section 8 presents related work while Section 9 concludes the paper and describes future work.

2. INDUSTRIAL BACKGROUND

In this section, we introduce the context of our research work (the CONNEXION project) as well as industrial and academic challenges.

2.1 The CONNEXION Project

Since 2011, the CONNEXION[1] project is a national work program to prepare the design and implementation of the next generation of I&C systems for nuclear power plants, with an international compliance dimension. The CONNEXION project is built around a set of academic partners (CEA, INRIA, CNRS / CRAN, ENS Cachan, LIG, Telecom ParisTech) and on collaborations between large integrators such as AREVA and ALSTOM, EDF and "technology providers" of embedded software (Atos Worldgrid, Rolls-Royce Civil Nuclear, Corys TESS, Esterel Technologies, All4Tec, Predict).

For the specific concern of having a high level and global perspective on requirements and architecture variability modeling, the working group started on November 2013 and was constituted of CEA, Inria, AREVA, EDF, Atos Worldgrid, Rolls-Royce Civil Nuclear, and All4Tec engineers and researchers. The group size varies from 3 to 14 persons depending of the individual or collective task to perform. In the group, Inria and All4Tec are considered as variability experts while the rest of the participants have neither academic nor industrial variability culture. Between November 2013 and April 2014, the group has organized a dozen of half-day to full day workshops as well as several regular or ad hoc telephone meetings, which ensures a high level of interactivity.

2.2 On the Regulation Heterogeneity and Variability

Safety critical systems must comply with their requirements, where regulatory requirements are first class citizens. These requirements are from various natures, from regulations expressed by national and international bodies, to national explicit or implicit guidance or national practices. They also come from national and international standards when they are imposed by a specific regulator [19].

In the specific context of nuclear energy, one applicant has to deal with very heterogeneous regulations and practices, varying from one country to another. This heterogeneity has a huge impact in the certification process as the regulators safety expectations, evidences and justification to provide can vary [18, 7].

At this level, the main concern comes from the difference between national practices and the set of documents (regulatory texts ans standards) to comply with. The nuclear industry has an unstable and growing set of safety standards. Worse, the set of safety standards is increasing within two main standards areas. On the one hand, there are the IEEE/ISO standards that are mainly applied in the US and eastern Asia. On the other hand, the IAEA/IEC standards and recommendations followed in Europe[2]. This heterogeneity and lack of harmonization of the different nuclear safety practices has been highlighted by the Western Europe Nuclear Regulators Association (WENRA)in 2006 [17].

Proposing one system, when having to perform a safety function, in different countries then leads to a huge problem of variability that concerns, not only the set of requirements to comply with and the certification process, but also the system's architecture itself.

2.3 Lack of Product Line Culture

Rise and Fall of the EPR reactor out of France. In France, EDF owns and operates 58 nuclear power units, following four different designs or series (same design but specific projects). Born from a European program, the *Evolutionary Pressurized Reactor (EPR)* design represents the new power plant generation and has been expected to be built on several countries: France, Finland, the United-Kingdom, China, and later, in the USA. The British safety authorities reference the same set of IEC standards as in France. However, their acceptable practices differ on some significant points. US authorities provide detailed written regulatory requirements and guidance but endorse but IEEE documents.

As a consequence, the concept of series that enabled to design and maintain the nuclear power plants in France can no longer be applied as such for export. Thus, since 2008, in the five most advanced EPR projects (construction in Finland, France and China, certification in progress in the USA and UK), EDF and Areva have been with four different I&C architectures and five different and ad hoc certification processes, specific to each country.

Conforming to different regulations. Comparing each IEC standard (and their interpretations) with its approximately relevant IEEE corresponding standard is difficult, time consuming and does not ensure to have the correct interpretation of the different standards. Though the domain owns a very precise and established vocabulary, ambiguities [16] and interpretations are legions. Legal documents and standards contain intended and unintended ambiguity [2, 12], causing interpretations, misunderstandings and negotiations between stakeholders. Scope of regulations may also differ as there is no direct mapping from one standard to another but many overlaps and differences.

Though the task is very difficult, formalizing the requirements variability and finding the common core that will enable the next I&C architecture generation is more than necessary from the industrial perspective. In the context of the CONNEXION Project, a product line approach consists to define a generic foundation that is refined for a given project by taking into account the specific requirements. This is an important challenge for building I&C systems on EPR units or other types of reactors in several countries in order to avoid the questioning of the initial design principles.

[1] http://www.cluster-connexion.fr/

[2] More details are provided in the following and in a previous work [18]

3. RESEARCH BACKGROUND

The Common Variability Language (CVL) [5] is a domain-independent language for specifying and resolving variability. We present here the three pillars of CVL and introduce some terminology that will be used in our approach.

Variability Abstraction Model (*VAM*) expresses the variability in terms of a tree-based structure. Inspired by feature and decision modeling approaches [6], the main concepts of the VAM are the variability specifications, called VSpecs. CVL distinguishes three types of VSpecs, essentially linked to their types: choice (Boolean), variable (other primitive types) and classifier (multiple instanciations).

Base Models (*BMs*) is a set of models, each conforming to a domain-specific modeling language (DSML). The conformance of a model to a modeling language depends both on well-formedness rules (syntactic rules) and business, domain-specific rules (semantic rules). The Object Constraint Language (OCL) is typically used for specifying the static semantics. In CVL, a base model plays the role of an asset in the classical sense of SPL engineering. These models are then customized to derive a complete product.

Variability Realization Model (*VRM*) contains a set of Variation Points (VP). They specify how VSpecs (i.e., Choices) are realized in the base model(s). An SPL designer defines in the VRM what elements of the base models are removed, added, substituted, modified (or a combination of these operations) given a selection or a deselection of a choice in the VAM.

4. OVERVIEW OF THE APPROACH

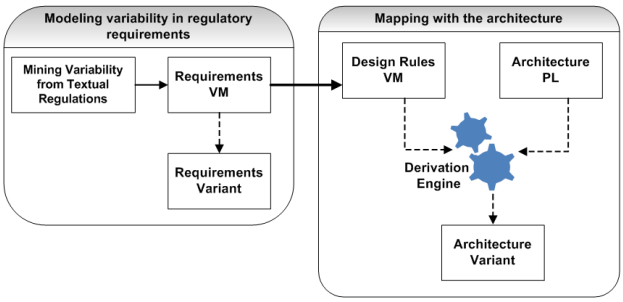


Figure 1: A two-stages approach (overview)

Fig. 1 depicts the approach we developed to tackle the variability issues. The long term goal is to configure a robust I&C architecture from features related to regulatory requirements. The gap between textual regulatory requirements and the architecture is obviously important and variability cross-cuts both parts. Therefore the key idea is to exploit architectural design rules as an intermediate between the regulatory requirements and the architecture.

Intensive interactions between all the involving partners and numerous workshops and meetings lead to the adoption of the approach (see also Section 7.3 for more details). Two separate areas of variabilities are part of the approach (1) variability among requirements (the main focus of the paper) led by Inria and (2) variability among the architecture led by another partner.

Regarding the requirements variability, it can take place at two levels: the variability of one particular requirement and the variability of a set of requirements within a product line. A first key task is to determine the variabilities within the set of requirements we want to satisfy. At the same time, the other key task is related to the adaptation of these variable elements by orchestrating the possible configurations from the architecture perspective.

The first stage aims at handling the multiple interpretations of ambiguous regulations using mining techniques. The second stage addresses the *impact* of requirements variability on the architecture and its certification through the variability in design rules. In Section 5, we address more precisely the mining and modeling of variability in nuclear standards. In Section 6, we describe how we model variability of design rules and the brige between variability in both requirements and architecture.

5. HANDLING VARIABILITY IN REGULATORY REQUIREMENTS

In this section, we present how we manage variability with nuclear regulatory requirements and its modeling with the OMG Common Variability Language (CVL) [5]. This domain is complex because of the variety of documents one has to handle; the number of requirements they contain; their high level of abstraction and ambiguity, etc. We proposed to analyze variability in regulatory documents with the smaller scope of topics (A topic is a concern within a corpus (e.g., "independence", "safety Classification", etc.)), on different corpora and on the same abstraction level: regulatory text, regulatory guidance or standards (see Section 5.3).

Our industrial partners proposed to model variability in IEC and IEEE standards for each of these two topics: independence (see Table 1) and safety classification (see Table 2).

I&C Architecture Concepts. In order to ease the understanding of the following sections, we briefly describe the main concepts of a classic I&C architecture. An I&C architecture can be decomposed into systems that perform functions. Systems and functions are classified with respect to their safety importance. These systems and functions are organized within lines of defense (LDs) and many constraints drive the organization of the architecture in order to prevent common cause failures. These constraints mainly deal with communication or independence (physical separation and/or electrical isolation) between lines of defense or systems with respect to their safety classification.

5.1 Requirements Similarity Identification

The first step of Fig. 1 is based on the intuition that features are made of clusters of related requirements. In order to form these clusters, requirements are considered related if they concern similar matters. Thus, the subject matter of the requirements has to be compared, and requirements with similar subject matter will be grouped. For example, in Table 1, the following safety requirements IEC 60709.1, IEC 60709.11, IEC 60709.12, IEEE 384.1 and IEEE 384.5 are similar because all of them are addressing the independence between systems. In particular, IEC 60709.1, IEC 60709.11 and IEC 60709.12 are dealing with preventing system degradation, while IEEE 384.1 and IEEE 384.5 specify how this must be achieved.

5.2 Feature clustering

The feature clustering step creates a feature tree based on the similarity measures from the previous stage. Requirements which are semantically similar, i.e., have the

most in common, are "clustered" to form a feature. These smaller features are then clustered with other features and requirements to form a parent feature. To return to our previous examples of Section 5.1, in standards, IEC 60709.1, IEC 60709.11, IEC 60709.12, IEEE 384.1 and IEEE 384.5 are clustered to form *Independence between Systems*. IEC 60709.1, IEC 60709.11 and IEC 60709.12 are clustered to create *Prevent System Degradation* feature, while IEEE 384.1 and IEEE 384.5 are clustered to give *Electrical Isolation* feature. Table 3 reports the global traceability between identified features and standards requirements.

5.3 Modeling Regulatory Requirements Variability with CVL

We propose to illustrate the complexity of safety requirements corpus through the manual search of similar requirements dealing with similar matter. As a reminder, this requirements analysis will be made on three different corpora, France, UK and US and on two standards: IEC and IEEE for each of these two topics: independence (see Table 1) and safety classification (see Table 2).

Fig. 2 shows an extract from the requirements model and its related variability model. Standards and regulatory texts concerns can be organized as variably concepts and properties like *ICFunction*, *Independence between Systems* (see Fig. 2), *Independence between Functions* and *Communication Separation* (see Fig. 3) which correspond to mandatory features.

In Fig. 2, *ICSystem* and *ICFunction* are two classifiers having an instance multiplicity [1..*] (i.e., at least one instance of *ICSystem* and *ICFunction* must be created). Each *ICSystem* is associated with a *Safety Class* (See IEC 60964.11 in Table 2) and each *ICFunction* is associated with a *Safety Category*. Each *ICFunction* is allocated to at least one *ICSystem* while *Safety Category* must be lower or equal to *Safety Class*. See the OCL constraint attached to *ICFunction* and IEC 61513.3 in Table 2.

There are two alternatives for *Safety Class*: *IEC Class* and *IEEE Class* form an *Xor-group* (i.e., at least and at most one feature must be selected). Similarly, *IEC Category* and *IEEE Category* form two alternatives of *Safety Category*. *Independence between Redundant Parts*, *Independence between Systems of Different Classes* and *Prevent System Degradation* are mandatory child features of *Independence.Sys*. On the other hand, in Fig. 3, *Independence between Functions of Different Categories* is a mandatory child feature of *Independence between Functions* (See IEC 61226.18 in Table 2).

In a previous work, Sannier and Baudry [19] proposed a formalization of nuclear regulatory requirements into a requirements model using Domain specific languages (DSLs). We rely on this DSL in our work. Yet, it is worth noticing that instead of representing only requirements within a linear organization, they represent a corpus of different kinds of documents, which contains different kinds of fragments with different semantics.

Fig. 2 depicts an excerpt of a standards BM that contains the minimal subset to formalize IEC 60709.1 requirement. From IEC 60709 standard, we present some transformation elements into text fragments and the traceability to requirements that are created and will be the analyzed elements. Moreover, this figure illustrates bindings between standards BM and the standards VAM. For instance, the "object existence" variation points against the IEC 60709.1 *Section* refer to the choice *Independence.Sys*, *IEC Class* and *IEC Category* meaning it will exist only when these choices are decided positively. The "object existence" variation point against the IEC 60709.1.b *Standard Requirement* is bound to the choice *Independence between Systems of Different Classes*.

6. MAPPING BETWEEN REQUIREMENTS AND ARCHITECTURE

6.1 Modeling Variability in Design Rules

Design Rules to Bridge Requirements and Architecture Elements.

Modeling requirements variability is useful, however there is no direct mapping from requirements to the architecture. To brige the gap between textual regulatory requirements and the architecture, we move towards variability in design rules. Design rules, edited by EDF and endorsed by the French safety authority, are intermediate elements to bridge the gap between an architecture and the regulatory or normative requirements. Our industrial partners rely on these rules to validate the architecture against regulations. A design rule can satisfy fully or partially one or more requirements: in Table 1 SA10 (resp. SA54) completely satisfies IEC 60709.1 and IEC 60709.11 (resp. IEEE 384.1 and IEEE 384.5).

Identifying and Modeling Variability in Design Rules.

Similarly to requirements, the identification of features in deign rules consists in comparing the subject matter of rules followed by a clustering step. For instance, SA10, SA12 and SA54 are similar because they are dealing with the separation of systems of different classes. In particular, SA10 and SA12 deal with communication without perturbation between systems of different classes whereas SA54 forbids the communication between them (see Table 1). Table 3 reports the traceability between identified features and design rules.

Comparing design rules interpretations in the three countries leads to the variability specification in Fig. 4. The concept of design rules are decomposed into the following mandatory features: *ICFunction*, *Communication Separation* in Fig. 3 and the two kinds of communication: *Functions Communication* (communication between functions) and *Systems Communication* (Communication between Systems). Similarly in standards VAM, each *ICFunction* is allocated to at least one *ICSystem* and only one *Line of Defense*.

France and UK allow the communication between systems of different classes only if it will not cause systems perturbation using isolation devices (see SA10 and SA12 in Table 1), however USA forbids it (see SA54 in Table 1). In Fig. 4, *Communication without Perturbation* and *No Communication between Systems of Different Classes* are two alternatives for *Separation between Systems of Different Classes*. Moreover, *decouplingType* is an optional classifier of *Systems Communication*. The latter has an OCL constraint written in its context comparing the *Sender Class* and the *Receiver Class*. If a *Sender Class* is lower than its *Receiver Class*, it requires isolation: the function non Empty() is used to state that there is at least one instance of the *decouplingType* classifier.

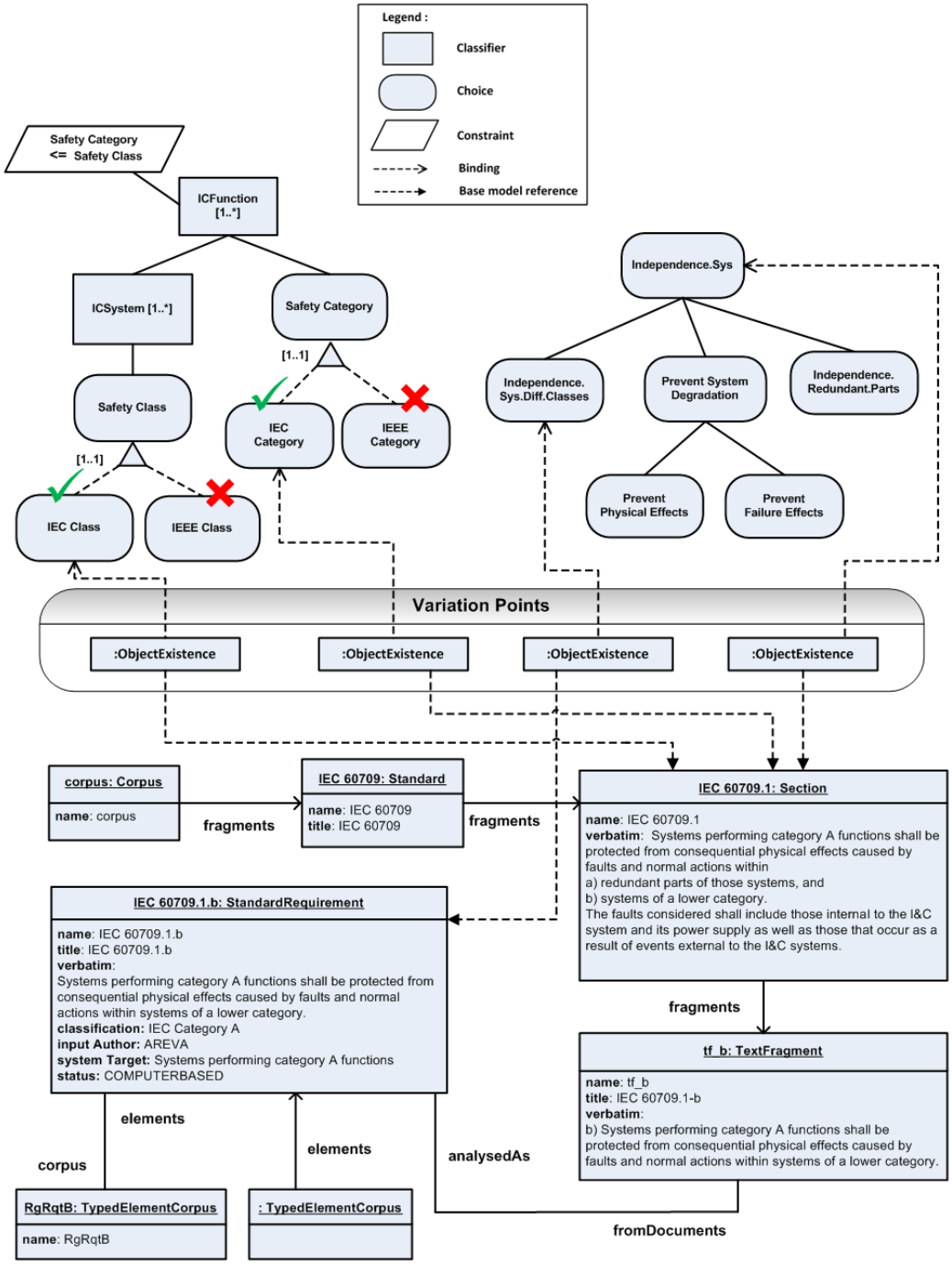


Figure 2: Mapping between standards BM and standards VAM

Table 1: Mining variability in *Independence* topic

Information sample from IEC and IEEE standard		Design Rules		Countries
Index	Verbatim	Index	Rule	
IEC 60709.1	Systems performing category A functions shall be protected from consequential physical effects caused by faults and normal actions within a) redundant parts of those systems, and b) systems of a lower category.	SA10	A lower classified system can not send information to a higher classified system or at least it should not disturb any of these features.	France and UK
IEC 60709.11	Failures and mal-operations in the non-category A systems shall cause no change in response, drift, accuracy, sensitivity to noise, or other characteristics of the category A system which might impair the ability of the system to perform its safety functions.			
IEC 60709.12	Where signals are extracted from category B or C systems for use in lower category systems, isolation devices may not be required; however, good engineering practices should be followed to prevent the propagation of faults.	SA12	A higher classified system can not directly send information to a lower classified system.	France and UK
IEEE 384.1	Physical separation and electrical isolation shall be provided to maintain the independence of Class 1E circuits and equipment so that the safety functions required during and following any design basis event can be accomplished.	SA54	No communication between systems with different classes.	US
IEEE 384.5	1) Non-Class 1E circuits shall be physically separated from Class 1E circuits and associated circuits by the minimum separation requirements specified in 6.1.3, 6.1.4, . . . 2) Non-Class 1E circuits shall be electrically isolated from Class 1E circuits and associated circuits by the use of isolation devices, shielding, and wiring techniques or separation distance.			

Table 2: Mining variability in *Safety Classification* topic

Information sample from IEC and IEEE standard		Design Rules		Countries
Index	Verbatim	Index	Rule	
IEC 60964.11	The design basis for information systems, including their measurement devices, shall take into account their importance to safety. The intended safety function of each system and its importance in enabling the operators to take proper pertinent actions . . .	SA5	Every system and sensor is associated with safety class.	US, France and UK
IEC 61513 .3	d) Each IC system shall be classified according to its suitability to implement IC functions up to a defined category.	SA8	Function with safety category n can be allocated only on systems of safety classes n or >n.	US, France and UK
IEC 61226.18	There shall be adequate separation between the functions of different categories.	FA11	A lower classified function can not send information to a higher classified function.	US, France and UK
IEC 61226.3a	An IC function shall be assigned to category C if it meets any of the following criteria and is not otherwise assigned to category A or category B: a) plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis not covered by 5.4.3 e).	SA57 SA58	The FA6 function associated category B. The FA5 function associated category A.	France

Table 3: Identification of features from IEC and IEEE standards and design rules

Features	IEC 60709.1	IEC 60709.11	IEC 60709.12	IEEE 384.1	IEEE 384.5	IEC 60964.11	IEC 61513.3	IEC 61226.18	IEC 61226.3a
ICSystem	✓	✓	✓	✓	✓	✓	✓		
ICFunction	✓	✓	✓			✓	✓	✓	✓
Safety Classes	✓	✓	✓	✓	✓	✓	✓		
IEC Classes	✓	✓	✓						
IEEE Classes				✓	✓				
Safety Categories	✓	✓	✓			✓	✓	✓	✓
IEC Categories	✓	✓	✓						✓
IEEE Categories									
Independence. Sys.	✓	✓	✓	✓	✓				
Independence. Sys.Diff.Classes	✓	✓	✓	✓	✓				
Independence. Redundant. Parts	✓								
Independence. Func. Diff.Categories								✓	
Prevent System Degradation	✓	✓	✓						
Prevent Physical Effects	✓								
Prevent Failure Effects		✓	✓						
Communication Separation	✓	✓	✓	✓	✓			✓	
Physical Separation				✓	✓				
Electrical Isolation				✓	✓				

Features	SA5	SA8	SA10	SA12	SA54	FA11	FA13
Safety Classes	✓	✓	✓	✓	✓		
Sender Class			✓	✓	✓		
Receiver Class			✓	✓	✓		
Safety Categories						✓	
Sender Category						✓	
Receiver Category						✓	
Sender LD							✓
Receiver LD							✓
Separation.Sys. Diff.Classes			✓	✓	✓		
Separation.Func. Diff.Categories						✓	
Separation .Func.Diff.LD							✓
Communication. Without. Perturbation			✓	✓			
No.Communication. Sys.Diff.Classes					✓		

The three countries forbid the communication from lower to higher classified functions (see FA11 in Table 2). An OCL constraint is attached to *Functions Communication*, requiring that the *Sender Category* must be higher or equal than *Receiver Category*. Furthermore, a function allocated to a line of defense shall not communicate with a function allocated to another line of defense. Consequently, a second OCL constraint, attached to *Functions Communication* is added.

6.2 Mapping Between the Standards VAM and the Design Rules VAM

Since design rules represent intermediate elements between the requirements and the architecture, the design rules VAM acts like a pivot between the standards VAM and the architecture variability model (VM). Fig. 3 depicts two extracts from both standards VAM and design rules VAM; and also the mapping between them. For instance, *Separation between Systems of Different Classes* in design rules VAM is related to *Independence between Systems of Different Classes* in standards VAM. This mapping is due to the fact that SA10 satisfies IEC 60709.1 and IEC 60709.11 and SA54 satifies IEEE 384.1 and IEEE 384.5, at the same time, SA10 and SA54 are related to *Separation between Systems of Different Classes* (see Table 3 right-hand side) while IEC 60709.1, IEC 60709.11, IEEE 384.1 and IEEE 384.5 refer to *Independence between Systems of Different Classes* (see Table 3 left-hand side).

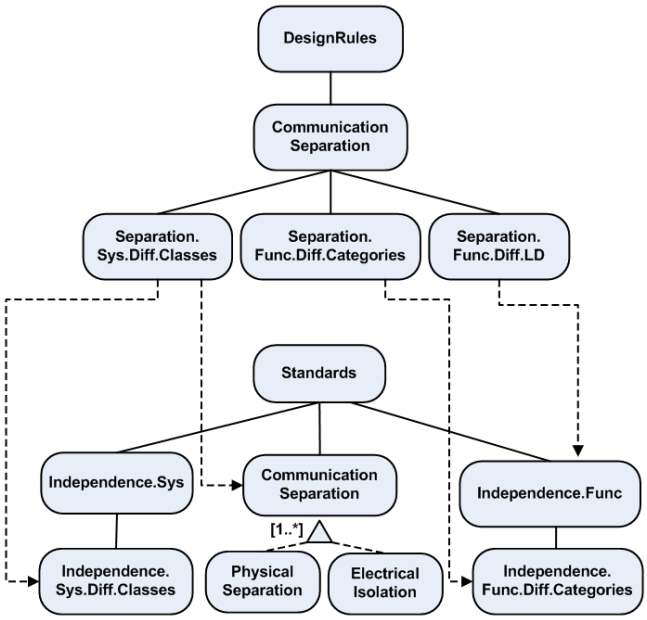


Figure 3: Mapping between the standards VAM and the design rules VAM

6.3 Mapping between the design rules VAM and the I&C architecture

An architecture metamodel is defined by one partner: the CEA, based on the different elements that characterize an I&C system of a nuclear power plant through a SysML profile. CEA uses the SysML modeler Papyrus with the Sequoia add-on for managing I&C architecture product line (see Fig. 4c). As mentioned earlier, industrial partners rely on design rules to validate the architecture against regulations. However, they do it for each derived architecture. Thus, we propose to consider both of the design rules VAM and the architecture VM during the derivation of a particular architecture.

Fig. 4 illustrates, first the binding between the architecture product line model and the corresponding feature model and then, the impact of the design rules VAM on the derived architecture. For instance, if we select *Communication Without Perturbation* in Fig. 4b, then we allow the communication between systems of different safety classes. Yet, the communication from a lower classified system to a higher classified system requires isolation: *decouplingType* (see OCL constraint). As shown in this figure, *System communication architecture* block in the derived architecture contains the following links: 1. from higher to lower classified system :from *SICS* (Class 1) to *DSS* (Class 2). 2. from lower to higher classified system: from *PICS* (Class 3) to *RCSL* (Class 2) by isolation means. 3. between equal classified systems: from *PS_A* (Class 1) to *SICS*.

Considering the two OCL constraints in Fig. 4a left-hand side, we forbid the communication between functions of different lines of defense or from lower to higher classified function. As a result, *Functional communication architecture* block in the derived architecture contains a link from *Monitoring LCO*(Category: C_NCAQ and Line of Defense: L1) to *Elaboration signal control C2*(Category: NC and Line of Defense: L1).

7. APPLICATION OF THE APPROACH

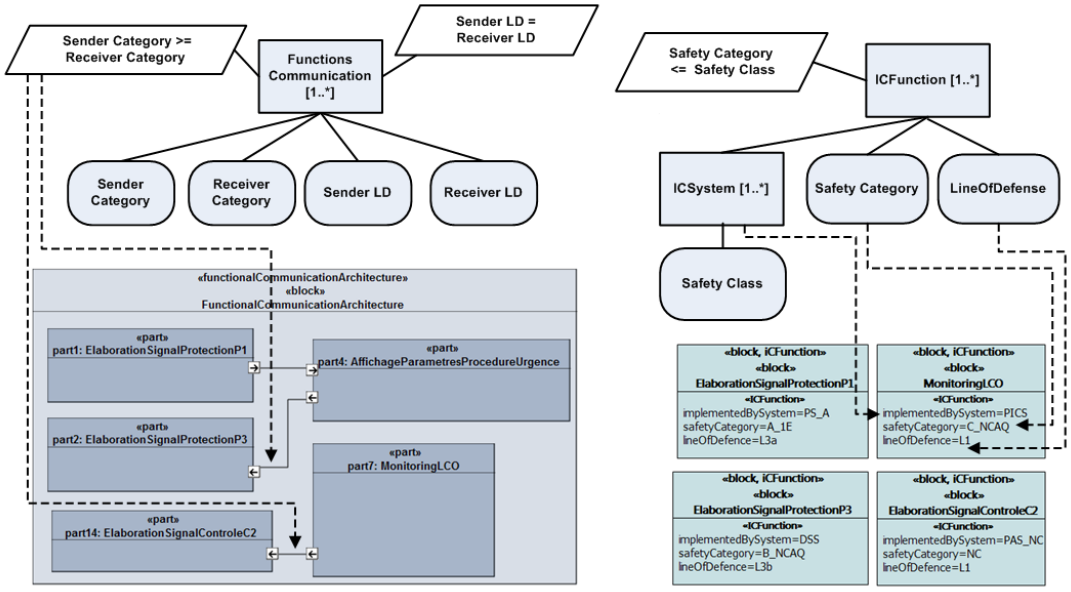
7.1 Implementation

As mentioned earlier, we use CVL language and tool support for modeling variability in requirements and design rules, while CEA address modeling variability in the architecture using Sequoia tool. The goal of the Sequoia approach [8], developed by the CEA LIST is to help designers to build product lines based on UML/SysML models. Variability in Sequoia is defined through a UML profile [21]. To specify an optional element, the designer simply adds the stereotype *VariableElement* to the item. The stereotype *ElementGroup* introduces additional information through its properties, such as constraints between variable elements. In Sequoia, the decision model is used as a guide enabling to analyze all available variants and paths leading to a completely defined product. Once the derivation activity is launched, the choices described by the decision model are proposed to the user as a series of questions. The output of this process is a completely defined product and the user is not able to make any kind of modification to the initial model until the derivation step is over.

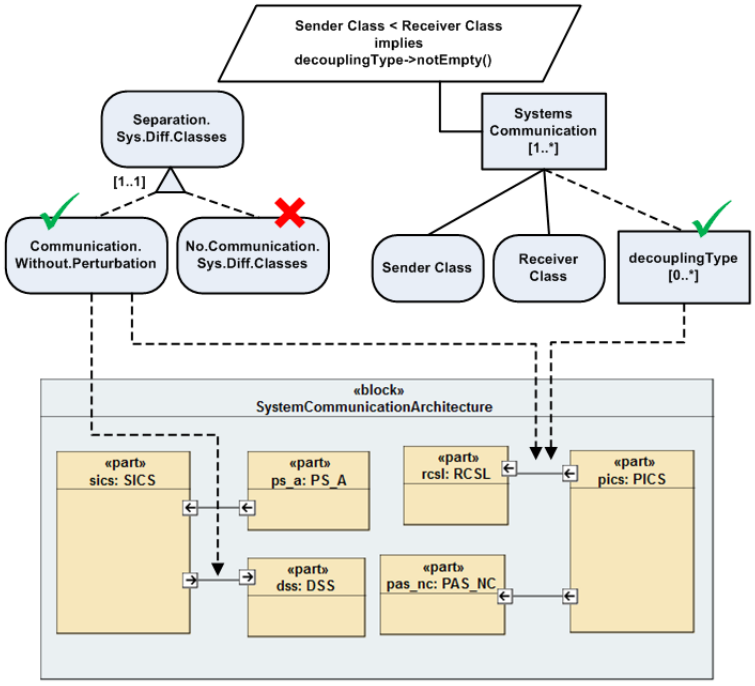
7.2 Use Cases

Data	Common Elements	Variable Elements		
		France	UK	US
# Requirements	21	13	15	9
# Design rules	3	4	4	4
# Functions	11	2	2	5
# Functions Communications	9	2	2	4
# Systems	19	0	0	1
# Systems Communications	33	15	15	27

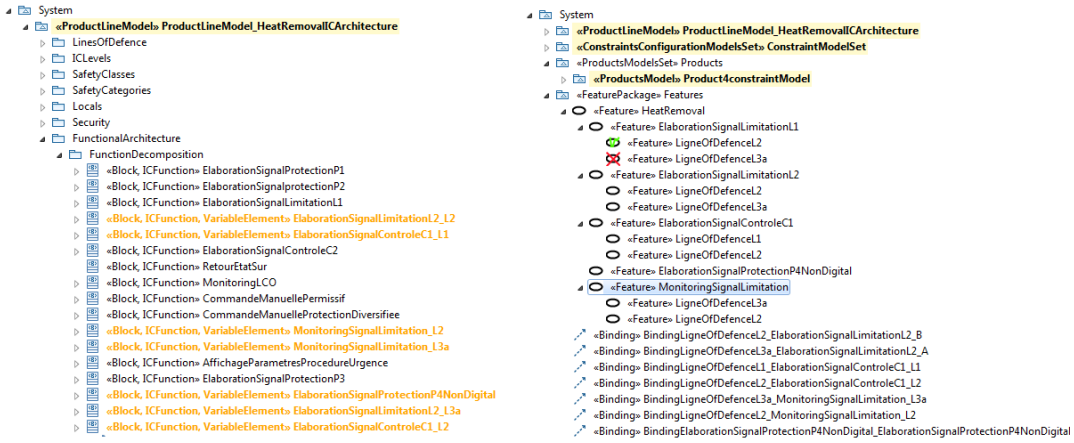
Table 4: Use Cases Data Description



(a) Mapping of Design Rules VAM with Functions Communication and Functions Decomposition



(b) Mapping Design Rules VAM with Systems Communication



(c) I&C Architecture PL (Sequoia)

Figure 4: Mapping between Design Rules VAM and I&C Architecture

Table 4 summarizes the input data in the illustrative example provided by the industrial partners to implement our proposed method. The use case contains one generic project which includes all common element in the product line and three other projects containing the variable elements, specific for these three countries (products): France, UK and USA. In particular, it describes the following information for each country: 1. Safety Requirements: excerpts from national regulations and international standards. 2. Design rules with their corresponding OCL constraints implemented in the architecture 3. I&C Functions with with their various properties (safety category, line of defense, number of redundancies, etc). 4. Functions communications: describes the different communications between functions (unidirectional and bidirectional) 5. I&C Systems and their different characteristics (safety class, I&C level, line of defense, number of redundancies) 6. Systems communications: a derivation of functional communications on the system architecture. To complete the use case, our industry partners provided us an association matrix that maps requirements and design rules.

Metric	Requirements VAM	Design Rules VAM
#Features	64	46
# OCL Constraints	5	5

Table 5: Variability Models Properties

Table 5 describes the main properties of the obtained variability models specific for our use case. Most of the features in both VAMs are mandatory. In fact, the challenge of our partners is not a customization of products, but, to maximize the common core to gain in terms of money and time during I&C systems certification.

7.3 Lessons Learned and Discussion

How to introduce variability modeling to nuclear engineers? In the group, Inria and All4Tec are considered as variability experts. Though the concepts of similarities and variabilities were roughly understood by our partners, we first had to introduce them to variability and, more specifically variability modeling. The aim of this introduction is to lay the foundation of the concepts but also identify the boundaries of the discipline. We set up several half to full-day workshops to allow our industry partners to localize where there will be valuable variability to model, and elicit what they expect from the variability modeling. From these inputs, we had been able to propose a dedicated variability training performed by one of the author, to build the bridge between initial industrial assumptions and current product line engineering practices.

What is the best variability modeling paradigm accordingly to the domain practices? We presented several different modeling paradigms, analysis capabilities, current limitations, etc. We discussed the choice of the modeling paradigm and the format of data that we will have to handle. Interestingly, CVL avoids the feature model (FM) terminology, while retaining FODA-like concrete syntax of FM. Since CVL is domain independent, it supports a broad range of types, including multiple instances, and a constraint language for expressing dependencies over these types. This terminology avoids the confusion caused by the ambiguous meaning of the term feature. Moreover, mapping to artifacts is a core objective of CVL and CVL stores the variability outside the base model, which allows the construction of an explicit common core for regulations.

How to deal with the search space in regulatory corpora and what is the right granularity level for modeling requirements variability? As mentioned earlier, nuclear domain is complex because of the variety of documents one has to handle, the number of requirements they contain, their high level of abstraction and ambiguity, etc. Following a naive method leads to variability models with fine granularity, verbose, and as a result, hard to understand and maintain by our industrial partners. To narrow this problem space, the first idea was to analyze variability in regulatory documents by topic on different corpora and on the same abstraction level. Thus, our industrial partners proposed to apply this approach on two standards and for different topics. Furthermore, using traceability matrix improves the understandability and the maintainability of variability models.

How to address the requirements variability on the architecture? Modeling requirements variability is useful, however there is no direct mapping from requirements to the architecture. Therefore, we propose heading toward modeling variability in design rules since they act as a pivot between requirements and the architecture. The industrial partners rely on these rules to validate the architecture against safety requirements because they claim to satisfy one or several requirements. This idea allowed us to investigate the robustness of the architecture against regulatory requirements variability not considered by the product line and identify its impact on the architecture. Therefore, our industrial partners proposed a use case to implement our CVL approach for modeling variability in requirements and design rules and mapping them to the architecture.

8. RELATED WORK

Requirements and Variability Modeling. Goal-oriented approaches like Tropos [3], i* [24], KAOS [22] or URN [10] have been used to address legal and regulatory requirements and their mapping to the system elements. However, though goal models explicitely describes influences on requirements, they lack of a concrete variability understanding. As stated by Siena *et al.* [20], goals applied to laws and regulations are useful when the complexity of the statements is little enough to be reduced to goal relations.

Mining Variability. Alves *et al.* [1], Niu *et al.* [15], Weston *et al.* [23] and Chen *et al.* [4] applied information retrieval techniques to abstract requirements from existing specifications, typically expressed in natural language. Ferrari *et al.* [9] applied natural language processing techniques to mine commonalities and variabilities from brochures. Our industrial context exhibits characteristics that makes the problem of mining variability difficult. Topic overlaps, absence of an ontology, intrinsic heterogeneity and ambiguity. Consequently, we have introduced lightweight manual techniques to gradually support participants. The question to determine whether automated techniques can provide a reliable support to the consortium is still open.

Analysing (Regulatory) Requirements Variabilities. Siena *et al.* proposed to address variability of law with Nómos 2 [20]. The proposed metamodel mainly aims to understand influences or margins within selected "norms" (text fragments from laws). Zhang *et al.* [25] propose "specialization, characterization, decomposition" links for their requirements refinements; "require, mutex, excludes" links for the constraints, as well as influence and interaction depen-

dencies. Maxwell *et al.* [14] propose a taxonomy of cross-references dedicated to the identification of conflicts between requirements. In both cases, the analysis remains manual and focused on selective and already defined sets of elements. One possible solution toward multiple jurisdictions can be to have the most constrained system possible. To this end, Gordon and Breaux [11] have developed a watermarking approach in order to determine the most constrained statement. Our goal is rather to capture all possible variations and keep flexibility.

9. CONCLUSION

With the renewal of the nuclear industry, the French nuclear energy industrials are aimed to sell and develop products outside France. A major challenge is the conformance of products to multiple different and heterogeneous regulations, which introduce a necessary product line perspective.

In this paper, we proposed an approach to model variability in safety requirements and I&C architectural design. Our approach provides a variability-aware bridging of these two levels of abstraction in order to derive a complying architecture. We instantiated our approach on a realistic use case. Participants of the nuclear consortium can now map the variability of regulatory requirements onto architecture elements. We provided some lessons learned about the introduction of variability into this particular domain.

We are currently improving the different variability modeling tools, based on the Common Variability Language, of both parts – requirements and architecture – of the project. As future work, we aim to investigate the use of automated techniques to mine variability in regulatory requirements. We also plan to further exploit traceability links in order to reason about the conformance between regulatory requirements and the architecture of the CONNEXION project.

Acknowledgements

This work is partially supported by the French BGLE Project CONNEXION.

10. REFERENCES

[1] V. Alves, C. Schwanninger, L. Barbosa, A. Rashid, P. Sawyer, P. Rayson, C. Pohl, and A. Rummler. An exploratory study of information retrieval techniques in domain analysis. In *SPLC'08*, pages 67–76. IEEE, 2008.

[2] T. D. Breaux and A. I. Anton. A systematic method for acquiring regulatory requirements: A frame-based approach. In *RHAS-6*, Pittsburgh, PA, USA, September 2007. Software Engineering Institute (SEI).

[3] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, and J. Mylopoulos. Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3):203–236, 2004.

[4] K. Chen, W. Zhang, H. Zhao, and H. Mei. An approach to constructing feature models based on requirements clustering. In *RE'05*, pages 31–40, 2005.

[5] Common Variability Language (CVL). http://www.omgwiki.org/variability/doku.php.

[6] K. Czarnecki, P. Grünbacher, R. Rabiser, K. Schmid, and A. Wasowski. Cool features and tough decisions: a comparison of variability modeling approaches. In *VaMoS'12*, pages 173–182, 2012.

[7] J. L. de la Vara and R. K. Panesar-Walawege. Safetymet: A metamodel for safety standards. In *MoDELS'2013*, pages 69–86, 2013.

[8] S. Deelstra, M. Sinnema, and J. Bosch. Product derivation in software product families: a case study. *Journal of Systems and Software*, 74(2):173–194, 2005.

[9] A. Ferrari, G. O. Spagnolo, and F. dell'Orletta. Mining commonalities and variabilities from natural language documents. In *SPLC'2013*, pages 116–120, 2013.

[10] S. Ghanavati, D. Amyot, and L. Peyton. Towards a Framework for Tracking Legal Compliance in Healthcare. In *CAiSE'2007*, pages 218–232, 2007.

[11] D. G. Gordon and T. D. Breaux. Reconciling multi-jurisdictional legal requirements: A case study in requirements water marking. In *RE'2012*, pages 91–100, 2012.

[12] E. Kamsties. Understanding ambiguity in requirements engineering. In *Engineering and Managing Software Requirements*, pages 245–266. Springer, 2005.

[13] J.-C. Laprie. Safety Demonstration and Software Development. In *SAFECOMP'2007*, pages 289–300, 2007.

[14] J. C. Maxwell, A. I. Antón, and P. Swire. A legal cross-references taxonomy for identifying conflicting software requirements. In *RE'2011*, pages 197–206. IEEE, 2011.

[15] N. Niu and S. M. Easterbrook. Concept analysis for product line requirements. In *AOSD'09*, pages 137–148, 2009.

[16] K. Pohl. *Requirements Engineering - Fundamentals, Principles, and Techniques*. Springer, 2010.

[17] W. R. H. W. G. RHWG. Harmonisation of Reactor Safety in WENRA Countries. Technical report, WENRA, 2006.

[18] N. Sannier and B. Baudry. Defining and retrieving themes in nuclear regulations. In *RELAW*, pages 33–41, 2012.

[19] N. Sannier and B. Baudry. Increment: A mixed mde-ir approach for regulatory requirements modeling and analysis. In *REFSQ'2014*, pages 135–151, 2014.

[20] A. Siena, I. Jureta, S. Ingolfo, A. Susi, A. Perini, and J. Mylopoulos. Capturing variability of law with nomos 2. *ER*, 7532:383–396, 2012.

[21] P. Tessier, S. Gérard, F. Terrier, and J.-M. Geib. Using variation propagation for model-driven management of a system family. In *Software Product Lines*, pages 222–233. Springer, 2005.

[22] A. van Lamsweerde. *Requirements Engineering - From System Goals to UML Models to Software Specifications*. Wiley, 2009.

[23] N. Weston, R. Chitchyan, and A. Rashid. A framework for constructing semantically composable feature models from natural language requirements. In *SPLC'09*, pages 211–220. ACM, 2009.

[24] E. S. Yu. Towards modelling and reasoning support for early-phase requirements engineering. In *RE'1997*, pages 226–235. IEEE, 1997.

[25] W. Zhang, H. Mei, and H. Zhao. A Feature-Oriented Approach to Modeling Requirements Dependencies. In *RE2005*, pages 273–284, 2005.