About using of ontology for the formalization of safety requirements based on the concept of working situation

Yasmine SAADI[1], *Alain ETIENNE*[1], *Ali SIADAT*[1], *Bruno DAILLE-LEFEVRE*[2]
1: LCFC. École Nationale Supérieure d'Arts & Métiers, 4 rue Augustin Fresnel, 57000 Metz, France
2: INRS. Institut National de Recherche et de Sécurité, Rue du Morvan, 54500 Vandoeuvre les Nancy
saadi_yasmine@hotmail.com, {alain.etienne, ali.siadat}@ensam.eu, bruno.daille-lefevre@inrs.fr

Summary—*Designers struggle to formalize the transition of safety needs with safety requirements during the design of a production system. It presents through this article a methodological approach which, from a working situation on the production system, designers highlights the usual criteria that influence the health and safety of users in the form safety requirements. The methodology is based mainly on the use of ontology known to be rich sources of knowledge. The goal is to make available to designers a methodological tool to help elicitation and formalization of safety requirements.*

Keywords — Safe design, requirements engineering, work situation, formalization, ontology.

INTRODUCTION

The statement usually done by examining requirements specification documents is that the safety requirements, when they appear, are in a separate section and copied from a generic list of security features, which makes the security measures taken by designers mainly corrective, thus penalizing the costs and deadlines for any changes retrospectively [1].

They thus become an important obligation to include in the early stages of needs analysis based on the future use of the equipment to ensure the inclusion of preventive safety aspects and not corrective.

The concept of working situations defined in [2] to take into account the usual criteria that influence the health and safety of users in the form of future activity operators.

Also, though the textual expression is essential, it is only part of all performances needed for rigorous and efficient approach for specifying security requirements. As a basis on a well-defined process, accurate and adaptable for the expression of requirements, equipped simple modeling methods, and reliable is one of the secrets to design a good product.

Requirements engineering (RE), aims to provide such rigorous framework for describing systems to be developed, and even argues for the integration of aspects of prevention earlier by modeling the context of design equipment (work situation) usage by using formal models which NIAM, a translation method of textual requirements by a formal language offering a more attractive pedagogy by identifying knowledge (need) via implicit knowledge modeling (need) explicit.

And the purpose of a more precise specification, ontologies will be mobilized, a modeling language often used in information systems and rarely in the field of design of industrial equipment, known to be a rich sources of knowledge and, being structured and equipped with reasoning mechanisms, they form a powerful tool to guide the analysis of the safety requirements.

Thus, the purpose of the study is to just test four main assumptions

- The discovery of the security requirements may be performed in several steps by analogy to requirements engineering.
- The contexts of use and the future performance of the system and the user do they allow the identification of safety problems.
- The use of engineering method of knowledge does it allows the structure of safety requirements expressed in natural language.
- Use the representation field of knowledge is it an initial response to the formal specification of safety requirements.

METHODOLOGY

The proposed approach is based on the interoperability of methods from the field of Requirements Engineering and Knowledge Engineering (Fig 1).

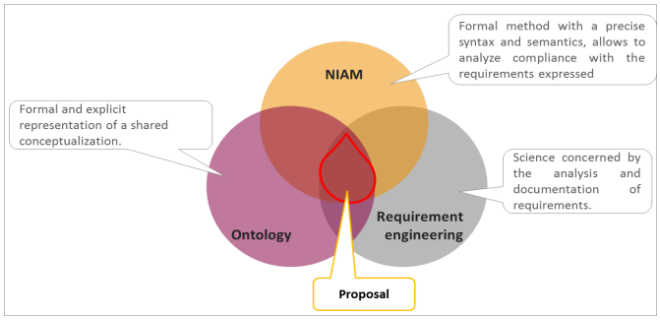

Fig. 1. *Proposed méthodology*

Xème Conférence Internationale : Conception et Production Intégrées, CPI 2015, 2-4 Décembre 2015, Tanger - Maroc.

Xth International Conference on Integrated Design and Production, CPI 2015, December 2-4, 2015, Tangier - Morocco.

The principle is to rely on the framework of the process of requirements engineering (RE) (first hypothesis) (clarify, analyze, specify, verify) [3] which will join -to phases- different, different methods to ensure the discovery of safety needs as follows :

1. Elucidation

The RE provides a wide range of techniques, methods and tools for the identification, collection and transcription requirements. [4] Presents four categories elicitation techniques: conversational techniques, observational techniques, analytical techniques, synthetic techniques.

The 2nd hypothesis of this work is the identification of safety problems from the contexts of use the performance of the equipment and the work team: Concept of Work Situations.

The elucidation is based on using observational techniques [5] that allow recording the behavior of people, view, capturing scenes and generating narrative descriptions of situations when they occur and thus identify threats, dangerous phenomena, hazardous areas and actors exposed to danger and anticipate certain countermeasures.

The result is a set of textual security needs to be analyzed and to be modeled in the following steps.

A generic definition of a work situation after the census of different definitions [2] gives

«A work situation is surrounded by a set of physical, chemical, biological, organizational, social and cultural elements in which it operates; there are one or more systems on which work teams perform one or more tasks, which may also require tools (tools and consumables).

A hazardous event is likely to occur by chance in a work situation that may contain many hazards phenomena and thus generate hazardous areas.

The possibility of interaction between the user and the hazardous area allows the identification of risks ».

2. Analysis

Only a part of the initial knowledge on safety -formulated in step-1 is specifically used as a requirement need [6].

This second step is to purify, reorganize and complete the security requirements collected during the previous step by identifying domain elements and the interactions between them through the development of basic sentence about types subject-verb-complement -principle of NIAM method [7] - support the required knowledge without any loss of information.

In order to have a clear understanding of all the knowledge contained in the descriptive text above (Step elucidation) the work situation described in text form are analyzed by constructing basic sentences and definition of interactions between elements of the domain according to 'NIAM approach. Below an introduction to the first central concept "work situation" to facilitate understanding of the methodology:

- A work situation identifies none, one or more risks.
- A work situation has one or more tasks of implementation.
- A work situation involves one or more work teams.
- A work situation contains none, one or more dangerous areas.
- A work situation is influenced by one or more environmental factors.
- In a work situation is used none, one or more auxiliary.
- In a work situation evolves none, one or more hazards.
- A work situation concerns one or more systems.
- In a work situation occurs zero, one or more hazardous events.

(The rest of the system elements, Principle of solution, Task, dangerous phenomenon, Risk, Auxiliary Safety measure, Hazardous area, Environment, Work team Task Force, Dangerous event are present in [8].)

3. Specification

The process of formalization and specification is in first time to transform basic sentences from the analysis phase to a representation in the formalism proposed by NIAM. Then in a second time to introduce ontologies relating to aspects of prevention and safety in the field of equipment safety.

A. Step 1:

Each of these ideas in basic sentences is represented by concepts and by relations between concepts that contribute to limit the possibilities of text interpretation.

Figure 2 presents an overview of the proposed formalization conducted by NIAM method to highlight the borders of the work situation notion and the different aspects relating to identifiable safety from this work situation.

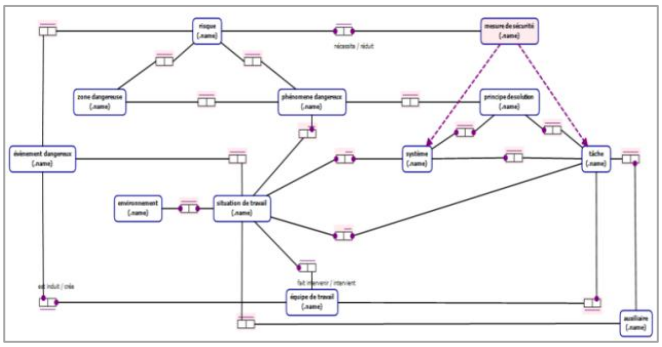

Fig. 2. *Global view of generic model work situation - NIAM.*

B. Step 2:

The aim is to learn about the construction of an ontology part covering safety aspects involved in work situations that

provides the necessary structure for a capitalization of knowledge for the purpose of preservation and transmission.

1) Specification

Development begins with the specification phase of establishing a document of requirements specification where to build the ontology is derived through five aspects:

- Knowledge area: the ontology is part of operator safety when using a machine. It takes its concepts in machine safety, and work situation field.
- Objective: the major objective of the incorporation of ontology within a process of specifying safety requirements is to formalize and standardize expert knowledge to improve consistency and usability of these requirements.
- Users: shows all the users who can exploit the ontology. In this case, they represent designers and customers who need to use ontology to achieve the objective which is the specification of safety requirements.
- Sources of information: on which is based the construction of ontology applications; they can be the technical documents of machine safety, standards, regulations and safety standards.
- Scope of ontology: determine the list of terms that make up ontology of the domain to specify, concepts of work situations described in section 2.2 constitute a key terms to appear in the center of ontology : hazardous event, solution of principle...

2) Conceptualization

Once the majority of acquired knowledge, it should be organized and structured by using formal representations and easy to understand. The representation formalized with NIAM shown in Fig 2 constitutes the conceptual model on which is based the ontology proposed.

a) Organization

The ontology must cover (eventually) all regulatory standards and elements of the field of machine use (work situation), Figure 3 proposes a reorganization of the elements of work situation representing the central concepts that must appear in the ontology.

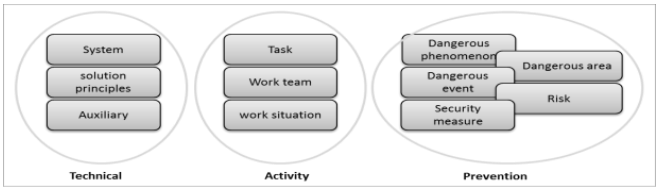

Fig. 3. *Organization concepts "work situation" -NIAM model- in classes.*

- The class "Technical" identifies elements relevant to the analysis of a system consisting of a combination of solution principles, creating and / or subjected to potentially dangerous events engaged in activity.
- The class "Activity" includes actors who manage the progress of work to get a result set by the work situation.
- The class "Prevention" allows for each work situation to clarify any dangerous phenomenon, real or potential operating in a dangerous area and may cause risk to the health of the operator following the occurrence of a dangerous event.

b) Structure

In the first stage of experimental introduction to the mobilization of ontology, only subclasses "dangerous phenomenon", "Danger" and "Security measure" of class "Prevention" have been specified and instantiated. The bibliography [9] [10] [11] [12] [13] [14] indicates that there is no current approach is designed to exploit ontology in the requirements development process of machine Security.

- Subclasse : dangerous phenomenon

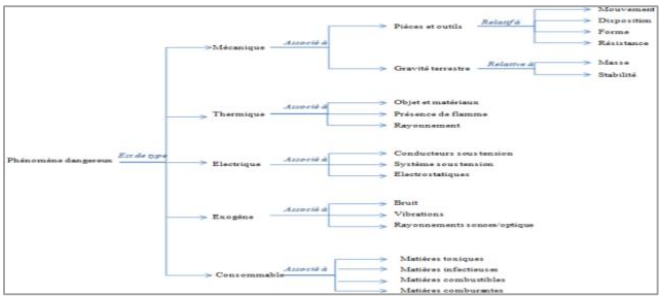

Fig. 4. *Subclasse dangerous phenomenon structure.*

- Subclasse : Risk

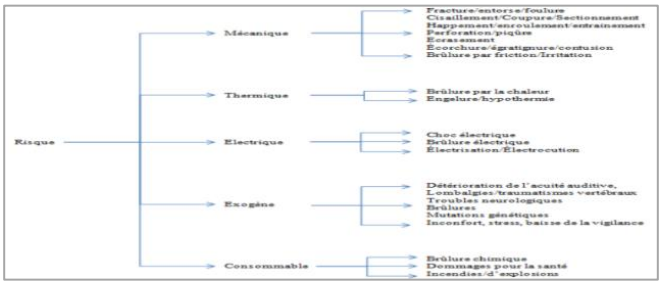

Fig. 5. *Subclasse Risk structure.*

- Subclasse : Security measure

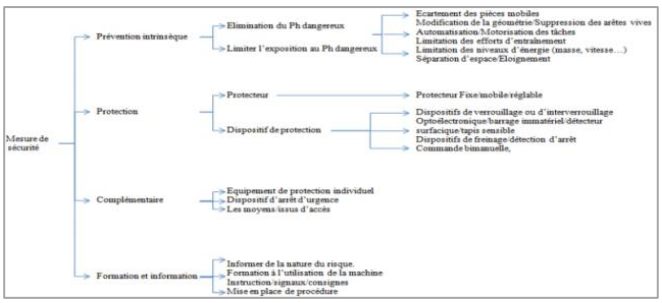

Fig. 6. *Subclasse security measure.*

c) Relations

Once the field concepts explained, they must be instantiated to reproduce a story on a situation. To do this you must define the relationships that express the semantics of the field. The table below gives an overview of the most important relationships between these concepts.

TABLE 1. THE RELATIONS BETWEEN THE CONCEPTS OF ONTOLOGY.

Type of relationship	**Definition**	**Exemple**
Sémantique	Provides more informations to the relationship. Assists designers in understanding the field. Eliminates ambiguity and ensures consistency.	“Sort of" Relation generalization specialization expresses a concept is a particular case of another concept.
Specific	Form a more specific conceptual model of the domain.	Relationship "requires" indicates that an element is exposed to the action of another element..
Logic	Consisting of one or more conditions connected to one or more conclusions	"If ... Then" Prediction Relation defined as any rule whose antecedent known a priori and result unknown.

4. Verification :

The aim is to ensure the proper application of the rules imposed by the methods used.

For formalism NIAM control regarding the rule of uniqueness, consistency and syntactic representation and consistency constraints. The result of this control produces a list of errors that is, non-compliance. This verification process is mostly automated on NIAM support software tools.

To increase the effectiveness of this approach, a second process associated more oriented towards validation, which is a transposition of this scheme in a more vulgarized view for natural language to compare the result of the formalization and modeling be unique with sensible initial knowledge. The estimate of the difference between the two forms of representation falls within the subjectivity of the domain expert who believes that the formal representation or not sufficiently comply with the initial knowledge.

And for the verification and validation of the conceptual and semantic structure of the proposed ontology, a domain expert must intervene. The validation can be based on the terminology of the domain or a lexicographical dictionary. However the built ontology helps some accuracy since its structure is based on the formalized model NIAM the results of which meet the criteria of verification and validation

RESULTS

This project demonstrated a new axis of research possible on the interoperability of methods from different areas of engineering (system and knowledge) to support the specification of safety requirements in the machine equipment field, taking the problems related to the using equipment earlier in the design process through the understructure of requirements engineering.

The main innovation is the use of the knowledge extracted from safety ontology. The approach will guide the analyst designer by providing ontology, a tool and mechanisms to extract relevant facts of knowledge to apply in its analysis of the safety requirements. The intended result is a better definition of the safety requirements.

DEBATE

New features requested by users to engineering safety requirements require the development of new tools and methods for the elicitation of requirements; the research project articulate around the formalization of the key concepts of work situation in order to translate them as requirements.

Nevertheless if the application of good practice can help to achieve this objective, it does not guarantee to do this without fail. Based on best practices, the research project is even seen that primarily, no research on a method of passing the requirements of needs-based on ontology was identified in the field of design industrial equipment.

Indeed to improve the work and better fulfill its objectives, future research should focus on the following points:

- Enrichment of the ontology by the use of experts and documents from the field and databases.
- Implementation of association rules for automatic identification of situations inducing the context of accidents.
- Programming a reasoner to find similar work situations and adapt the solutions to the current work situation.
- Strengthening the verification and validation process.

CONCLUSION

This research project concerns the conceptual tools available to participants to specify and formalize the transition of safety needs with safety requirements during the design of a production system. A production system characterized by its human, physical and informational attributes. Exposing its users to threats which exploit vulnerabilities in the system. Around which proposed a methodological approach (Fig 7), which acquired part of requirements engineering by taking over its four steps, and argues for the integration of aspects of prevention through formal models which NIAM and mobilizes ontology: the originality of this project.

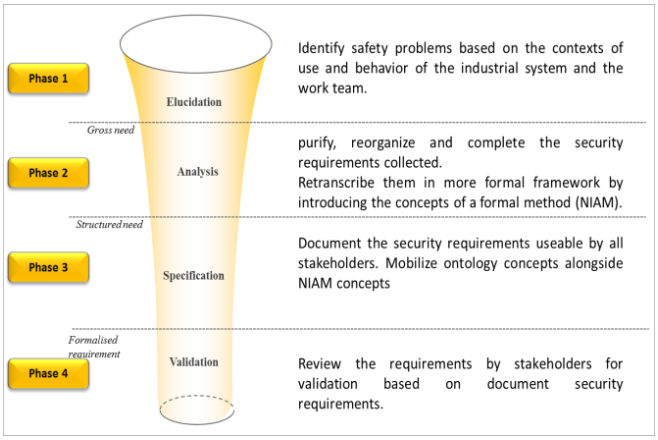

Fig. 7. *The approach of the proposed methodology and the tools useds.*

REFERENCES

[1] Fabian et al.,2010. A comparison of security requirements engineering methods. Requirements Engineering.

[2] HASAN R., 2002. Contribution to improving the performance of complex systems by taking into account socio-economic aspects from conception.Thesis of Henry Poincaré Nancy 1 University.

[3] Wiegers K. E.,2003. Software Requirements, Microsoft Press.

[4] Zheying Z.,2007. Effective Requirements Development - A Comparison of Requirements Elicitation Techniques, Software Quality Management journal, pp. 225-240.

[5] Coulin C. R., 2007.A situational approach and intelligent tool for collaborative requirements elicitation [Report] :Doctoral Thesis / Computing Sciences ; University of Technology and Université Paul Sabatier. - Sydney and Toulouse, 33 .

[6] Eljamal M. H.,2007. Contribution to evolution of requirements and its impact on security [Report]: Doctoral Thesis / Industrial Systems; Paul Sabatier University. - Toulouse: [s.n.] 161.

[7] Habrias H., 1988. Binary Relational model: Method IA NIAM.book.

[8] Saadi Y., 2013. Contribution à l'amélioration de l'outillage conceptuel pour la formalisation des exigences de sécurité : Rapport d'études bibliographiques. Master Recherche Conception Industrialisation et Innovation. Ensam.ParisTech Metz

[9] Lodderstedt T., 2002. SecureUML: A UML-Based Modeling Language for Model-Driven Securit, Proceedings of the 5th International Conference on The Unified Modeling Language.

[10] Jürjens H., 2002. UMLsec: Extending UML for Secure Systems Development", Proceedings of the 5th International Conference on The Unified Modeling Language.

[11] McDermott J., 1999. Using Abuse Case Models for Security Requirements Analysis. In Proc. of ACSAC'99. IEEE Press, 55–66.

[12] Firesmith, Donald G., et Firesmith Consulting. 2003.Engineering Security Requirements . Journal of Object Technology 2, 53–68.

[13] Liu L.,J., 2003. Security and Privacy Requirements Analysis within a Social Setting, RE, Proceedings. 11th IEEE International, 2003.