Uni-REPM Safety Module: evaluating the maturity of safety processes in requirements engineering

Student: Jéssyka Flavyanne Ferreira Vilela, Universidade Federal de Pernambuco (UFPE) (jffv@cin.ufpe.br)
Advisor: Jaelson Castro, Universidade Federal de Pernambuco (UFPE) (jbc@cin.ufpe.br)
Co-Advisor: Luiz Eduardo Galvão Martins, Universidade Federal de São Paulo (UNIFESP) (legmartins@unifesp.br)
Level: Doctoral
Graduate program: Centro de Informática (CIn) of Universidade Federal de Pernambuco (UFPE)
Year of Entry: March/2015 **Conclusion Expectation:** February/2019
Qualification: August/2017
Related Event: SBES

Abstract. Context: *Safety-Critical Systems (SCS) require more sophisticated requirements engineering (RE) approaches as inadequate, incomplete or misunderstood requirements have been recognized as a major cause in many accidents and safety-related catastrophes.* ***Objective****: In order to cope with the complexity of integrating the safety processes in RE, the objective of this thesis is to develop a module for evaluating the maturity of the safety issues in the RE phase.* ***Method****: we followed the design science methodology and to solve this practical problem, we propose a Safety Module, which consists of an enhancement of the Unified Requirements Engineering Process Maturity model (Uni-REPM) maturity model.* ***Results****: The safety module has seven main processes, 14 sub-processes and 149 safety actions describing principles and practices that form the basis of safety processes maturity.* ***Conclusions****: As an evaluation instrument, we expect the safety module to be a simple solution for professionals to identify the status of safety processes in their RE process. As a guiding tool, we hope the module can help organizations in evaluating their current safety practices in the RE process as well as offer a step-wise improvement strategy to reach higher maturity.*

Keywords: Requirements Engineering, Safety Engineering, Maturity Models, Safety-Critical Systems.

1. Problem Characterization

Safety-critical systems (SCS) are those composed of a set of hardware, software, processes, data and people whose failure can result in accidents that cause environmental damage, financial loss, injury to people and even loss of lives [2][4].

There are many cases in the literature as, for example, (i) the computer-controlled radiation therapy machine called Therac-25 that massively overdosed six people [6]; (ii) the crash of a Turkish Airline DC-10 resulting in 346 deaths [6]; (iii) the Milstar satellite that was placed in an incorrect and unusable low elliptical final orbit, as opposed to the intended geosynchronous orbit [4]; (iv) Bacterial Contamination of a Public Water Supply that resulted in half of the people in the town of 4,800 that became ill and seven died [4]; (v) the loss of the Mars Climate Orbiter spacecraft [14]; and many others where inadequate or misunderstood requirements have been recognized as the major cause (not coding or implementation [14]) of a significant proportion of accidents [7] and safety-related catastrophes [8].

Therefore, SCS must be carefully specified, demanding more sophisticated RE approaches [4][8]. However, requirements engineers, traditionally, are not familiar with system safety analysis processes which are performed by safety engineers. One reason is the gap that exists among the traditional development processes, methodologies, notations and tools used in safety engineering [11].

This gap makes the safety analysis process by the requirements engineers a difficult and challenging task [11]. Among the consequences of the insufficient guidance we can cite: (1) safety activities are isolated from RE and developers responsible for developing the system [4]; (2) engineers are confronted with important safety concerns only after it is too late or too expensive to make significant changes [4]; (3) engineers mostly decide how to specify the system based on personal intuition and experience [1]; (4) difficulties in the certification of safety-critical systems.

The problems related to safety in RE tend to be reduced in higher maturity RE process [5] [9]. Therefore, the organizations should improve their RE process in order to overcome the challenges of developing SCS. We argue that a maturity model can be capable of guiding organizations in the implementation of safety processes, reduce the development cost as it will allow evaluate the level of safety in the development process, but also it will identify what is missing or it is necessary in order to achieve the safety level they desire.

The industry challenges about the RE process of safety-critical systems above mentioned motivated the investigation about how the quality of this process with respect to the safety of such systems can be improved. In this thesis, we propose a Safety Module, for the Uni-REPM which is a maturity model for RE process and currently does not support processes related to safety. The module has seven main processes, 14 sub-processes and 149 safety actions describing principles and practices that form the basis of safety processes maturity.

2. Theoretical Background

2.1. Safety-critical systems

Safety-critical systems are those systems whose failure could result in harm (generally meaning injury or death) [2]. Loss may involve human death and injury, but it may also involve other major losses, including mission, equipment, financial, and information losses [4]. The safety engineering comprehends many concepts such as safety [3], hazard [4], accident [4], safety requirement [3], functional safety requirement and safety engineers.

During the development of SCS, safety engineers typically review the requirements documents in early development stages in order to perform safety analyses. Such reviews are periodically repeated throughout the entire development process in order to align the safety analyses with requirements changes. As a major result of the safety analyses, requirements and safety engineers define safety requirements.

Safety requirements describe the constraints or actions to support and improve system's safety. These requirements can be defined as any quality requirement that specifies a minimum, mandatory amount of safety in terms of a system-specific quality criterion and a minimum level of an associated metric [3]. A functional safety requirement prevents or mitigates the effects of failures identified in safety analysis [3].

2.2. Maturity Models

According to [12], in general, maturity can be defined as the state of being complete, perfect or ready. Maturity implies an evolutionary progress from an initial to a desired target or naturally existing end stage. In the software engineering area, maturity is regarded as a measure to evaluate the capabilities of an organization.

Maturity models facilitate this evaluation by outlining anticipated, typical, logical, and desired evolution paths [12]. A maturity model is a structured collection of elements that describe the characteristics of effective processes at different stages of development [13]. It also suggests points of demarcation between stages and methods of transitioning from one stage to another. Models in different areas such as software engineering, education, project management, construction processes and information management for example are available in the literature.

2.3. Uni-REPM

The Unified Requirements Engineering Process Maturity model (Uni-REPM™) [5][15] is constructed based on studies of good practices and it is intended as an instrument for assessing RE process maturity as well as to offer a concrete, complete, and contemporary view of state of the art in requirements engineering, so that researchers and practitioners alike may get an overview of which requirements engineering practices that have been proposed and empirically validated.

The model hierarchy has three levels, namely Main process area (MPA), Sub-process area (SPA) and Action. On the top level of the model, there are seven MPAs (Organizational Support, Requirements Process Management, Elicitation, Requirements

Analysis, Release Planning, Documentation and Requirements Specification, and Requirements Validation) corresponding to RE main activities (see Figure 1).

Each MPA is further broken down into several SPAs, which contributes to better understanding. On the bottom level, an Action denotes a certain activity that should be performed or a certain item that should be present. The model establishes a certain level to each action (from 1 to 3, corresponding to “Basic", “Intermediate", and “Advanced" level) depending on the difficulty to implement the action, how essential it is for the RE process, and dependencies between actions.

The Uni-REPM has an assessment instrument in which the appraiser can mark one of three options: “Incomplete" (vital action performed partially or not at all in the RE process), “Complete" (action was completed in the RE process), and “Inapplicable" (action was not necessary or possible to be performed in the process).

3. Proposed Solution

The objective of this work is to provide an easier, understandable and secure way to organizations evaluate the maturity in key safety-RE process areas but also guide them to discover what they miss or need to achieve the maturity level they desire.

Accordingly, we proposed a safety module for the Uni-REPM maturity model. The module follows its dual-view-approach: Process Area view and a Maturity Level view. Since we want to integrate safety in the RE process, we maintained the seven MPAs of Uni-REPM (Figure 1) that were defined considering well-adopted RE processes.

We propose fourteen SPAs to be connected to the seven MPAs of Uni-REPM: Safety Knowledge Management (SKM), Safety Tool support (STO), General Safety Management (GSM), Safety Planning (SP), Safety Configuration Management (SCM), Safety Communication (SCO), Safety Traceability (ST), Supplier Management (SM), Preliminary Safety Analysis (PSA), Failure Handling (FH), Safety Certification (SC), Human Factors (HF), Safety Documentation (SDO), and Safety Validation and Verification (SVV).

Finally, we proposed 149 actions that are connected to these SPAs. Actions represent a specific good practice (see an example of an action in Figure 2). By performing the action, the organization can improve their process and gain certain benefits [5].

4. Current Status of Work

The student started this PhD in March 2015 and the expected date for thesis defense is February 2019. In these 28 months, we achieved the following goals:

- **Literature reviews:** comprehensive analysis of important authors in the field.
- **Systematic literature review**: a systematic literature review about requirements communication in safety-critical systems and integration between RE and safety analysis was already conducted. This activity resulted in two papers: one published in Journal of Systems and Software [24], and another one that is under submission.

- **Application of a hazard analysis method in a real case study**: traditional hazard analysis techniques usually were not proposed to be used in the RE process. Hence, we applied the STAMP (Systems-Theoretic Accident Model and Processes) [4] and STPA (System Theoretic Process Analysis) [4]

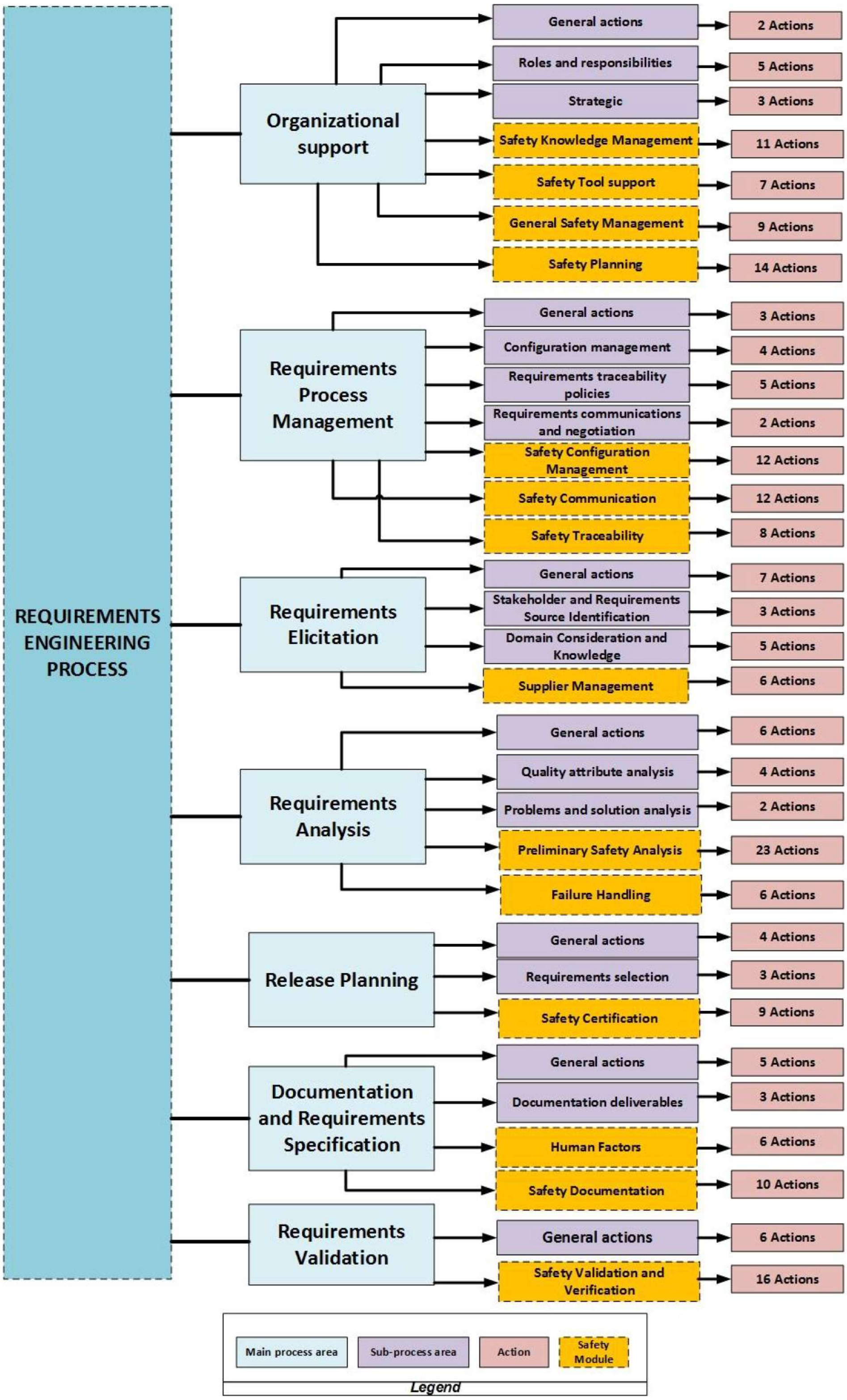

Figure 1. Safety Module and its relationships with Uni-REPM.

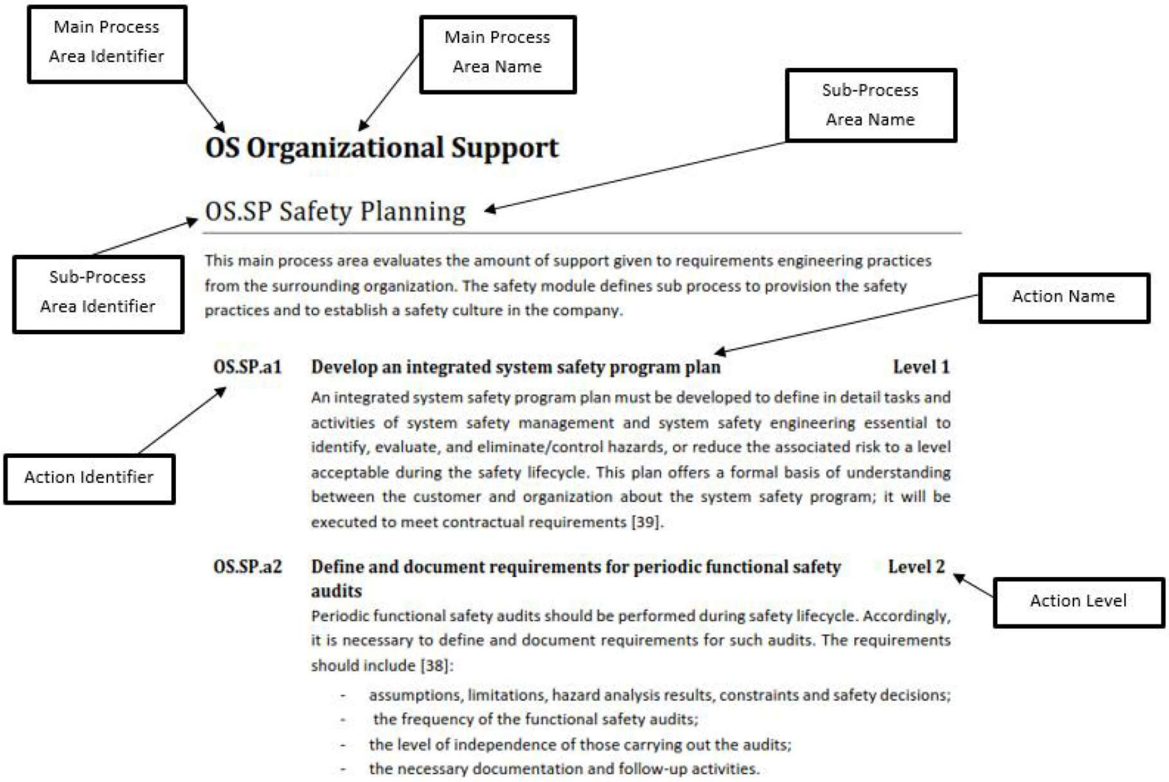

Figure 2. Example of an action in the safety module.

techniques, developed to be used in a safety-guided design, in a low-cost insulin infusion pump which is a real industry project being developed in Brazil. We aimed to understand the difficulties faced in the safety analysis and to evaluate the complexity of using such techniques in the RE process. As a result, we proposed a Safety Requirements Specification Method based on STAMP/STPA and i* (SaRSSI*) which is being prepared to submit.

- **Analysis of Safety standards**: since SCS should be submitted to certification processes prior to their commercialization, we analyzed which activities and information are required by the most adopted safety standards in different domains to incorporate them as actions in the safety maturity module.
- **Construction of Safety Maturity Module**: development of a safety maturity module for RE process to evaluate safety processes maturity during RE.
- **Integration of the safety maturity module with Uni-REPM™**: definition of relationships between the proposed module and the Uni-REPM™ [5].

As future works, we highlight the following goals:

- **Development of a tool**: development of a tool to support the application of the safety maturity module;
- **Evaluation and Validation of the module**: to evaluate the module, we intend to conduct interviews with experts, a survey, and case studies.
- **Refinements**: perform refinements and adjustments in the module based on the results obtained during evaluation and validation.

5. Evaluation of the proposed solution

The evaluation of the module will occur in academia as well as in industry in order to prepare it for widespread industry use. We will conduct at least four validations following the steps and nomenclature of the technology transfer framework [10]: a static validation based on interviews with academic and industry experts; a dynamic validation where the module will be applied in industrial organizations; the conduction of a survey with academics and professionals; and the usability evaluation of the tool.

We aim to conduct a web questionnaire-based survey with academics and professionals to increase the reliability of the module and its coverage of safety practices through larger sample sizes. The survey will be available online and disseminated in forums/groups of SCS and RE. Besides, we will send an email to the authors of the papers resulted in the SLRs performed [3][24] and the ones derived from the literature review. We aim for the participants who have experience in RE and safety fields.

The static validation will be conducted through interviews with academic experts in order to ensure that the module is understandable and it has a sufficiently complete coverage of the safety RE needs. A set of industry projects of different domains will be the basis for dynamic validation in order to ensure the applicability of the module. Moreover, we also want to obtain their feedback about the coverage of the safety requirements engineering needs.

After the static and dynamic validation, we expect to perform a survey aiming to increase the reliability of the result through larger sample sizes. Moreover, we will conduct the usability evaluation of the tool to support the use of the module.

6. Comparison with Related Work

Generic software process improvement frameworks such as CMMI, SPICE ISO9000 have been proposed and adopted by companies. However, they do not provide details about how company should proceed since their scope is to cover all phases of development process having a much bigger scope than just RE [15].

These generic models emphasize bespoke RE which is related to the development of a customized software system for a specific customer [16]. Nevertheless, they have not been updated with RE actions/practices in industry [15]. According to Svahnberg et al. [15], there are practices not handled at all by these models, and other actions are classified as being very advanced whereas in current state of practice they are the common norm.

SLRs about maturity models [17][18] show that there is a clear trend to propose models customized to specific domains such as small and medium enterprises, testing and quality assurance, security engineering, extreme programming, e-government, medical systems, space, telecommunications, software development.

There are some RE assessment frameworks, for example, the Requirements Engineering Good Practice Guide (REGPG) [19], Requirement Engineering Process Maturity Model (REPM) [20], Market-Driven Requirements Engineering Process Maturity Model (MDREPM) [16], and others that allow organizations to evaluate the strengths and weaknesses regarding the RE process. However, REGPG, REPM, and MDREPM do not cover both market-driven and bespoke RE as required by industry

[15]. To fill this gap, the Uni-REPM [15] was proposed but it does not consider safety issues required for the development of a safety-critical system. Therefore, in this work, we propose a safety module for the Uni-REPM model.

Safety culture maturity models are available in literature [21] [22]. Fleming [21] developed a model with the objective of helping organizations to identify the level of maturity of their safety culture. Gonçalves et al. [22] proposed a framework to measure safety culture maturity in the Brazilian oil and gas companies. However, safety culture is a characteristic of groups and organizations that handle organizational collective practices to avoid accidents during the work in factories [22] and not about developing SCS.

Some safety maturity models have been developed, for example, +SAFE-CMMI-DEV, ISO 15504-10, SW-CMM, and SE-CMM. However, these models are too general [23], usually adopted by safety engineers, and do not consider the integration between safety and RE as well as the particularities of these two areas as in our work.

7. Conclusions

The application of maturity models creates useful benefits [13]. First of all, maturity models generate an awareness of the analyzed aspects: their state, importance, potentials, requirements, complexity, and so on. Furthermore, they may serve as reference frame to implement a systematic and well-directed approach for improvements, ensure a certain quality, avoid errors, and assess one's own capabilities on a comparable basis [13].

We designed the module to be a self-assessment and improvement tool. It can be used by professionals themselves acting as evaluators – making small improvements based on recent lessons learned. This has been used as traditional assessment tools, but also as a part of agile organizations and a part of retrospective work on RE maturity models (SVAHNBERG et al., 2013).

8. References

[1] Sikora, E.; Tenbergen, B.; Pohl, K. Industry needs and research directions in requirements engineering for embedded systems. In: Requirements Engineering, v. 17, n. 1, 2012, pp. 57-78.

[2] Hatcliff, J. et al. Certifiably safe software-dependent systems: challenges and directions. In: Proceedings of the on Future of Software Engineering. ACM, 2014. pp. 182-200.

[3] Martins, Luiz Eduardo G.; GORSCHEK, Tony. Requirements engineering for safety-critical systems: A systematic literature review, Information and Software Technology 75 (2016) 71–89.

[4] Leveson, N. Engineering a safer world: Systems thinking applied to safety. Mit Press, 2011.

[5] Svahnberg, M. et al. Uni-REPM: a framework for requirements engineering process assessment. Requirements Engineering, v. 20, n. 1, p. 91-118, 2015.

[6] Leveson, N. Safeware: system safety and computers. ACM, 1995.

[7] Simpson, A.; Stoker, J. Will it be safe? An approach to engineering safety requirements. In: Components of System Safety. Springer, 2002, pp. 140–164.

[8] Leveson, N. An approach to designing safe embedded software. In: Embedded Software. Springer, 2002, pp. 15–29.

[9] Hall T., Beecham S., Rainer A. Requirements Problems in Twelve Companies: An Empirical Analysis. In: IEE Proceedings for Software, vol.149, no.5, pp.153-160, 2002.

[10] Gorschek T., Garre P., Larsson S., Wohlin C. A model for technology transfer in practice. In: IEEE Software 23(6), 2006, pp. 88–95.

[11] Scholz, S.; Thramboulidis, K. Integration of model-based engineering with system safety analysis. International Journal of Industrial and Systems Engineering, v. 15, n. 2, pp. 193-215, 2013.

[12] Marx, F.; Wortmann, F.; Mayer, J. A maturity model for management control systems. Business & information systems engineering, v. 4, n. 4, p. 193-207, 2012.

[13] Wendler, R. The maturity of maturity model research: A systematic mapping study. Information and software technology, v. 54, n. 12, p. 1317-1339, 2012.

[14] Lutz, R. Software engineering for safety: a roadmap. In: Proceedings of the Conference on The Future of Software Engineering. ACM, 2000, pp. 213–226.

[15] SVAHNBERG, M. et al. Uni-REPM: validated and improved. Requirements Engineering, v.18, n.1, pp.85–103, 2013.

[16] GORSCHEK, T. et al. Introduction of a process maturity model for market-driven product management and requirements engineering. Journal of software: Evolution and Process, v.24, n.1, pp.83–113, 2012.

[17] REIS, T. L.; MATHIAS, M. A. S.; OLIVEIRA, O. J. de. Maturity models: identifying the state-of-the-art and the scientific gaps from a bibliometric study. Scientometrics, pp.1–30, 2016.

[18]WENDLER, R. The maturity of maturity model research: a systematic mapping study. Information and software technology, v.54, n.12, p.1317–1339, 2012.

[19] SAWYER, P.; SOMMERVILLE, I.; VILLER, S. Requirements process improvement through the phased introduction of good practice. Software Process: Improvement and Practice, v.3, n.1, pp. 19–34, 1997.

[20] GORSCHEK, T.; SVAHNBERG, M.; TEJLE, K. Introduction and application of a lightweight requirements engineering process. In: International workshop on requirements engineering: foundation for software quality, 2003.

[21] FLEMING, M. Safety culture maturity model. Offshore Technology Report-Health and Safety Executive OTH, 2000.

[22] GONCALVES FILHO, A. P.; ANDRADE, J. C. S.; OLIVEIRA MARINHO, M. M. de. A safety culture maturity model for petrochemical companies in Brazil. Safety science, v.48, n.5, p.615–624, 2010.

[23] PEREIRA, R.; SILVA, M. M. da. A maturity model for implementing ITIL V3 in practice. In: International enterprise distributed object computing conference workshops (EDOCW), 2011, pp. 259–268.

[24]VILELA, J.; CASTRO, J. MARTINS, L.; GORSCHEK, T. Integration between requirements engineering and safety analysis: a systematic literature review. In: Journal of Systems and Software, v.125, pp.68–92, 2017.