2018 IEEE 26th International Requirements Engineering Conference

Assessment of Safety Processes in Requirements Engineering

Jéssyka Vilela[12], Jaelson Castro[2], Luiz Eduardo G. Martins[3], Tony Gorschek[4]
[1]Universidade Federal do Ceará (UFC), Brazil, e-mail: jessykavilela@ufc.br
[2]Universidade Federal de Pernambuco (UFPE), Brazil, e-mail: jbc@cin.ufpe.br
[3]Universidade Federal de São Paulo (UNIFESP), Brazil, email: legmartins@unifesp.br
[4]Blekinge Institute of Technology (BTH), Sweden, email: tony.gorschek@bth.se

***Abstract*— Context: Requirements issues tend to be mitigated in organizations with high process maturity levels since they do their business in a systematic, consistent and proactive approach. In a Safety-Critical System (SCS), requirements problems have been associated with accidents and safety incidents. Objective: This work investigates which safety practices/actions are suitable to be used in the Requirements Engineering (RE) process of SCS and how to design a safety maturity model for this area. Method: we adopted different empirical techniques to propose Uni-REPM SCS, which consists of a safety module to be included in the Unified Requirements Engineering Process Maturity Model (Uni-REPM). Results: The safety module has seven main processes, 14 sub-processes and 148 safety actions describing principles and practices that form the basis of safety processes maturity. Conclusions: Preliminary validation with two practitioners and nine academic experts indicates that the safety module can help organizations to evaluate their current safety practices with respect to their RE process. Moreover, it also offers a step-wise improvement strategy to raise their safety maturity level.**

***Index Terms*— Requirements Engineering, Safety Engineering, Maturity Models, Safety-Critical Systems, Process Assessment.**

I. Introduction

Safety-critical systems consist of a set of hardware, software, process, data and people whose failure could result in accidents that cause damage to the environment, financial losses, injury to people and loss of lives [2]. The need for handling software-related safety issues is increasing in the industry [19].

Indeed, safety requirements are a major source of safety incidents generally due to requirements problems [1][2][3][4]. The RE phase is critical because a substantial proportion (48%) of development problems [21] are derived from ill-defined requirements [6]. Fixing these requirements-related problems implies in costly rework in later states of the development.

In order to ensure well-ordered safety progress, engineers should handle several features (e.g., organizational, technical, strategic) which requires specialized processes, techniques, skills, and experience [20]. Improving the software process quality is a strategy adopted by many companies as a way to increase the confidence in the quality of the resulting software product [19]. In order to achieve such improvement, companies need methods to assess their processes strengths and weaknesses as well as strategies to mitigate the problems found. Additionally, organizations pursue well-structured and systematic processes to achieve their goals, with a set of resources or practices, resulting in a more mature organization.

Accordingly, there is a need for the development and evaluation of safety practices to support professionals working with planning and development of SCS [19][20]. Some safety maturity models are available such as +SAFE-CMMI-DEV [20], ISO 15504-10 [19]. RE assessment frameworks have also been proposed [9][10][11]. However, they do not cover market-driven and bespoke RE practices. The Unified Requirements Engineering Process Maturity Model (Uni-REPM) [6] was created to fill this gap. It is a universal lightweight model that has been well accepted in companies. However, Uni-REPM does not consider the safety aspects required for the development of a safety-critical system.

Previous Systematic Literature Reviews (SLR) about RE and SCS [7] [8] reported different types of contributions regarding the integration of these areas. A SLR about the research on maturity models [5] is also available in the literature. However, no maturity model for SCS was found in these SLRs. The SLR of Martins and Gorschek [7] returned 151 papers describing approaches to elicit, model, specify or validate safety requirements in the context of SCS. Considering the integration of RE and safety analysis [8], we obtained 57 studies that are contributions to improve the RE process of SCS. In [5], 237 studies about maturity models were found, but none is related to SCS.

The need of integrating safety and RE teams has been well discussed by some seminal papers in the SCS area [2][17][18]. There is a consensus in academia and industry that it is important to address safety concerns early in software development because it contributes to limit the propagation of safety problems through subsequent phases. Furthermore, the early consideration of safety concerns in RE should be a top priority in the development of SCS since RE is essential for software quality [6], and the effectiveness of the software development process. Besides, high safety levels are typically achieved by addressing safety issues early, avoiding to add protection components later in the development process [2]. Accordingly, such requirements issues tend to be mitigated in companies with high process maturity levels since they do their business in a systematic, consistent and proactive approach [21].

In this paper, we present an ongoing work about the assessment of safety processes in the RE phase. We have proposed a safety module for Uni-REPM to address safety practic-

RE 2018, Banff, Canada
RE@Next! Paper

2332-6441/18/$31.00 ©2018 IEEE
DOI 10.1109/RE.2018.00-25

es early in the development process. We describe its main features and results of a preliminary validation conducted with two practitioners and nine academic experts. We conclude the paper discussing the research status and long-term directions and prospects of this research.

Uni-REPM SCS differs from +SAFE-CMMI-DEV and ISO 15504-10 respectively in terms of scope; intended usage (RE phase against all system lifecycle); evaluated capabilities (14 against 2 and 3); Safety standards considered; Number of levels (3 against 5 in both); and number of practices (148 against 20 in which 13 actions have a correspondence with our model; and 26 actions being 16 present in Uni-REPM SCS). Therefore, our new maturity model is more descriptive and detailed because it was designed specifically for safety in RE. Moreover, it includes a comprehensive assessment instrument.

This paper is organized as follows. We provide a brief overview of safety analysis concepts and present related works in Section 2. An overview of the proposed solution is described in Section 3. In Section 4, we discuss the current status of work. Our conclusions, as well as further research, are presented in Section 5.

II. Background and Related Work

In safety analysis, accidents, hazards, and their causes are determined. An accident is an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss [2] (including loss of human life or injury, property damage, environmental pollution, and so on).

A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss) [2]. A cause of hazard is a reason that produces hazard as an effect. They occur due to an environmental hazard, procedural hazard, interface hazard, human factor or system cause [2].

Generic software process improvement frameworks such as CMMI, SPICE ISO9000 emphasize bespoke RE, which is related to the development of a customized software system for a specific customer [9]. Nevertheless, they have not been updated with RE actions/practices in the industry [6]. According to Svahnberg et al. [6], there are practices not handled at all by these models, while some actions despite being classified as very advanced are quite standard in the current state of practice.

There are some RE assessment frameworks, for example, the Requirements Engineering Good Practice Guide (REGPG) [10], Requirement Engineering Process Maturity Model (REPM) [11], Market-Driven Requirements Engineering Process Maturity Model (MDREPM) [9], 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 in the same model as required by industry [6]. In order to fill this gap, the Uni-REPM [6] was proposed. Unfortunately, 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, the new version will be called Uni-REPM SCS.

Some safety maturity models have also been developed, such as +SAFE-CMMI-DEV, ISO 15504-10, SW-CMM, and SE-CMM. However, these models are too general, usually adopted only by safety engineers. However, they do not consider the integration between safety and RE issues.

III. Proposed Solution

One of the challenges that the industry faces is to improve the quality of the safety-critical systems RE process [17][18].

The main goal of this work is to provide an easier and understandable way for organizations to assess their maturity in key safety-RE process areas. It is of paramount importance to guide them to discover what they miss in order to achieve the desired maturity level.

The following research questions motivated this work:

- RQ1: Which safety practices are suitable to be used in the requirements engineering process of safety-critical systems?
- RQ2: How to design a safety maturity module for the requirements engineering process of safety-critical systems?
- RQ3: How does the proposed safety maturity module compare with related solutions?
- RQ4: What is the effect of applying Uni-REPM safety module when it is instantiated in different safety-critical domains?
- RQ5: What is the perceived usefulness and ease of use of the Uni-REPM safety module?
- RQ6: How to evaluate whether the module has a sufficient coverage of safety practices?

Considering our goal and our research questions, we proposed the Uni-REPM SCS, which is a safety module for Uni-REPM maturity model.

Uni-REPM SCS is based on several sources such as SLRs, empirical studies, technical reports, existing maturity models, and comprehensive literature reviews. We also examined safety standards as a way to knowledge acquisition since regulatory entities should certify safety-critical systems. We also conducted interviews with practitioners that highlighted the need and importance of following an adequate safety standard.

Uni-REPM SCS consists of several *Main Process Area – MPs, Sub Process Areas – SPA*s and *Actions. MPs* are elements that correspond to the requirements engineering main activities. *SPA*s are elements that group actions related to a particular area that, when correctly implemented, contribute to the achievement of the goals considered important for improvement in this area. *Actions* are safety practices that are considered important for the achievement of the associated SPA.

The module also has *Supporting actions* that contain the list of actions related to the action in question, and reflects the high-level relationship between them; and *Examples* that give suggestions to practitioners on techniques or supporting tools when performing the action.

During the selection of safety actions/practices, we considered the highly cited definition of requirements practice of Davis and Zowghi [12]. They classify it as to be the use of a principle, tool, notation, and/or method to perform a RE activity. This definition was adopted since it matches with our understanding of a RE practice. When a practice reduces the cost of the development project or increases the quality of the resulting product, it is labeled as good requirements practice [12][13]. In this context, we selected safety practices capable of raising the likelihood of developing a SCS with better quality. An example of a practice of Uni-REPM SCS is presented in Fig. 1.

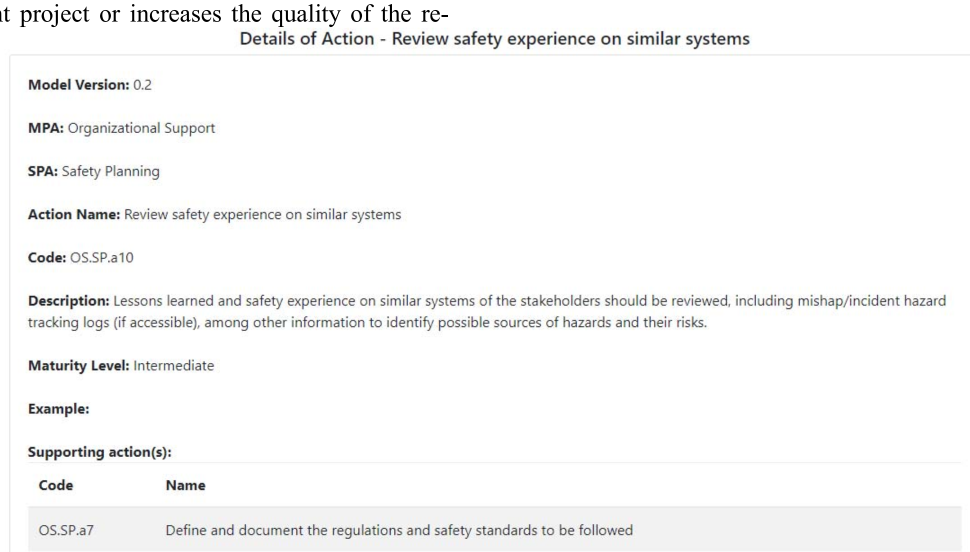

Fig. 1. Example of Uni-REPM safety practice.

The safety module follows the dual-view-approach of Uni-REPM: Process Area view and Maturity Level view. On hand the *process area* perspective allows visualization of the model process hierarchy and faster discovery of a group of actions/practices. On the other hand, the *maturity level* view, defines sets of consistent and coherent practices that belong to to the RE process. Notice that the practices in one level support each other as well as the more advanced practices on the next level.

In the safety module, we maintained the seven Main Process Areas of Uni-REPM [6] that were defined considering well-adopted processes, namely: *Organizational Support (OS), Requirements Process Management (PM), Requirements Elicitation (RE), Requirements Analysis (RA), Release Planning (RP), Documentation and Requirements Specification (DS), Requirements validation (RV).*

The 14 safety new sub-process areas are presented in TABLE I. We put forward these 14 new sub-processes aiming to group related safety practices in a category. We also considered the steps/phases described in safety standards, the frequency of their appearance in the different information sources as well as the ability to optimize the safety processes takin in consideration our experience and the results of literature reviews.

At the low-level of the module structure, we have "actions" that represent a specific good practice. By performing the action, the organization can improve its process and gain certain benefits. For example, an action "*Develop a safety information system to share knowledge in the organization"* once implemented will enable practitioners to share knowledge in the organization improving the communication between them.

The Maturity Level View is developed by assigning a level to each action in a Likert scale from 1 to 3, corresponding to "Basic," "Intermediate," and "Advanced" level, where 3 represents the highest level of maturity.

The safety module was designed to be used through an assessment instrument, as the one adopted by Uni-REPM [6]. The instrument follows the same structure as the module with questions grouped according to the MPA and SPA. The instrument has a query to evaluate each safety action in which the evaluator can select one of three options:

a) "Incomplete" (IC) - the action was deemed vital but was done partially or not at all in the RE process.

b) "Complete" (C) - the action was supported by the RE process.

c) "Inapplicable" (IA) - the action was not necessary or possible to be supported by the process.

The assessment instrument is implemented using an online software tool aiming to facilitate and automate the evaluation process. The tool supports three types of users: (1) external evaluator - this user can insert companies, projects and perform Safety/RE evaluations; (2) internal evaluator - this user can only insert projects to the company he/she belongs to and perform Safety/RE evaluations; (3) admin - besides the functionalities of external evaluators, this user can manage users and different versions of RE/Safety models.

After answering all questions of the assessment instrument, the tool determines and presents the evaluation results. In order to assign the maturity level, the tool takes in consideration: (1) for each SPA, all actions at a certain level must be Completed (or Inapplicable) in order to the MPA achieve such level; (2)

for the whole process, all actions at a certain level must be Completed (or Inapplicable) to the process achieve such level.

TABLE I. OVERVIEW OF NEW FUNCTIONAL SAFETY SUB-PROCESSES, I.E. EXTENSIONS, TO UNI-REPM.

UNI-REPM MPA	**UNI-REPM SCS SPA**	**Description**	**# practices**
Organizational Support	Safety Knowledge Management	It provides transparency in the development process by making sure that projects and the company have the required knowledge and skills to accomplish project and organizational objectives.	11
	Safety Tool support	It is responsible for facilitating the appropriate execution of the corresponding tasks and manage all safety-related information that should be created, recorded and properly visualized.	7
	General Safety Management	It covers project safety management activities related to planning, monitoring, and controlling the project.	9
	Safety Planning	It provides the safety practices and establishes a safety culture in the company.	14
Requirements Process Management	Safety Configuration Management	It addresses the control of content, versions, changes, distribution of safety data, proper management of system artifacts and information relevant to the organization at several levels of granularity.	12
	Safety Communication	It aims to improve the safety communication sub-process by establishing actions related to many safety terms, methods, process to support the safety analysis and assurance processes.	12
	Safety Traceability	It handles the traceability among artifacts helping to determine that the requirements affected by the changes have been thoroughly addressed.	8
Requirements Elicitation	Supplier Management	It is responsible for managing the acquisition of products and services from suppliers external to the project for which shall exist a formal agreement.	6
Requirements Analysis	Preliminary Safety Analysis	It addresses the realization of preliminary safety analysis to avoid wasting effort in next phases of system development.	23
	Failure Handling	It handles failures in system components that can lead to hazardous situations, the addition of redundancy as well as inclusion of protection mechanisms.	6
Release Planning	Safety Certification	It has actions related to system certification.	9
Documentation and Requirements Specification	Human Factors	It handles issues regarding system's users and operators that can lead to hazards and shall be considered during the RE stage of safety-critical system development.	6
Documentation and Requirements Specification	Safety Documentation	It has practices to record all information related to system's safety produced in RE phase.	10
Requirements Validation	Safety Validation and Verification	It contains actions related to requirements validation and the definition of strategies for the verification of requirements aiming to obtain requirements clearly understood and agreed by the relevant stakeholders.	16

An example of the Uni-REPM SCS assessment instrument is presented in Fig. 2. The Action ID in the checklist links the question(s) to the associated action in the model. These links help users in case they need to locate the item for further information or clarification.

If after careful analysis, an action is considered incomplete, must tick the appropriate option as well as record its rationale. The process improvement effort may consider such information.

The assessment results are presented in the tool in a tabular form or graphically, as in the example shown in Fig. 3. Such representation provides a better view, allowing the organization to benchmark their maturity and to monitor their development.

The blue dashed line presents actions which were considered Complete. In this case, 7 actions in the Basic Level were Complete, 6 actions in Intermediate level and 0 actions in the Advanced level. The purple dot line presents Complete actions together with Inapplicable ones.

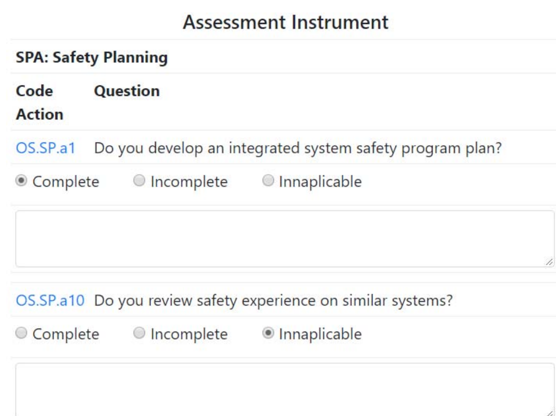

Fig. 2. Partial view of Uni-REPM SCS assessment instrument.

Fig. 3. Example of a graphical presentation of assessment results of SPA "Safety Planning."

Note that the green solid line depicts the total actions that should be completed in "Safety Planning" SPA. For example, at Advanced level, there is 1 action that should be finished.

The difference between the purple dot line and green solid line is significant because it denotes the improvement area of the process. It shows how many additional actions should be conducted to achieve a certain level of maturity.

For this example of SPA, Fig 3 denotes that the process has not considered all the actions at Advanced level. Hence, the result of the SPA indicates that the organization has reached an Intermediate Level of maturity. In order to reach the Advanced level, 1 more action has to be supported. The result for the whole process is reached when similar assessments all performed with the remaining SPAs

The complete description of Uni-REPM SCS, as well as its tool to evaluate the maturity, can be found at the project website[1].

IV. CURRENT STATUS OF WORK

Currently, we have answered RQ1-RQ3 by proposing Uni-REPM SCS. We will conduct the validation and evaluation of the safety module in academia as well as in industry to prepare it for widespread industrial use. In order to achieve this, we are following the technology transfer framework proposed by Gorschek et al. [14] that defines seven steps.

Steps 1-3 of the technology transfer model have already been completed in this work. They correspond to (1) Identify potential improvement areas based on industry needs, through process assessment and observation activities; (2) Formulate a research agenda using several assessments to find research topics, and formulate problem statements while studying the state of the art; (3) Formulate a candidate solution in cooperation with industry.

The next steps in this research are related to the validation and verification of the safety module. We have conducted a preliminary static validation (Step 4) with two practitioners and nine academic experts to evaluate the completeness, correctness, usefulness, and applicability of Uni-REPM SCS.

The majority of the suggestions were regarding the maturity levels of actions. We have addressed 98 of the 120 suggestions made and an improved version of the module was generated, which is currently available at the project website.

It is important to highlight that the model is fairly complete as there were no suggestions to add new actions. According to the experts' opinions, the actions in the model are applicable in real settings. Therefore, our research questions were answered and our goal to validate the module was successfully achieved. The module version presented in this paper has already been updated using the experts' feedback.

Furthermore, the purpose of this model is to present all the good practices that provide the company with a set of ideas to improve their safety processes in RE. However, it is the company responsibility to decide whether the recommended practices are indeed beneficial and suitable as well as when to implement them.

As future works, we intend to perform the usability evaluation of the tool; and a dynamic validation where the module will be applied in industrial organizations.

We are planning to use the PSSUQ (The Post-Study System Usability Questionnaire) [15] to evaluate the tool usability. This method provides a 19-item questionnaire, with administration and scoring instructions.

According to this method, we will assign some scenarios to the participants, and after they complete the tasks, they will rate the system according to the PSSUQ. This data will allow us to obtain feedback regarding the easiness of use of a tool that supports the module.

The PSSUQ analyzes the system's usability through four factors (overall satisfaction, system usefulness, information quality and interface quality) from the answers obtained from the evaluation questionnaire. We will conduct such evaluation with students in software engineering class as well as with experts during the case studies.

In the dynamic validation, the module will be applied in industrial organizations in real development projects, without the direct involvement of the researchers or industry champions. The conduction of case studies will allow the analysis of the applicability of the safety module, obtain feedback from practitioners about the coverage of the safety requirements engineering needs. After the conduction of such activities, we will be able to answer the following research questions: RQ4-RQ6.

V. CONCLUSIONS

Safety concerns and safety analysis should be addressed early in the system lifecycle. However, requirements engineers need systematic guidance to address these issues early in the development process of a safety-critical system.

This paper discusses ongoing research about the assessment of safety processes in RE phase. Accordingly, this work is crossing boundaries considering its goal of integrating the RE and safety areas increasing its impact in academia and industry.

The research is guided by six research questions, out of which three have been addressed so far. The main contribution is the proposal of a safety module, called Uni-REPM SCS, for the Uni-REPM maturity model. We aim to help companies that develop SCS to improve the maturity of their processes

[1] www.unirepm.com

regarding an evolutionary path from chaotic and eventual mature and disciplined software processes.

Uni-REPM SCS has 148 possible safety actions to be adopted in the RE process. These practices were obtained from a sound and convincing review of well-established prior work based on different sources of information. The module is focused on what to do instead of how to do. This approach provides flexibility for different companies to use established "in-house" procedures or processes.

We have conducted a pilot study with two practitioners and nine experts from academia to evaluate the completeness, correctness, usefulness, and applicability of our proposal. The results obtained from this static validation indicates that Uni-REPM SCS not only is novel and feasible, but that it is applicable, useful, and has appropriate coverage.

The novelty of this contribution consists of a set of sub processes and safety practices derived from many sources of information (SLR, interviews, technical reports, and safety standards) grouped in a safety module for a RE maturity model. For researchers, the safety module offers an inestimable summary of state of the art, by providing the identification and systematization of existing safety practices being a knowledge base. For industry practitioners, the module allows organizations to evaluate their current safety practices in RE process, improve their development processes contributing to improving software quality.

Therefore, the module contributes to providing clear guidance about which practices should be adopted in different maturity levels in SCS development addressing some critics that maturity models do not look deeply enough into all organizational practices [16].

ACKNOWLEDGMENT

This work was partially supported by FACEPE (grant APQ 0880-1.03/14), CNPq (grant 305634/2016-0) and the ORION project (reference number 20140218) from The Knowledge Foundation in Sweden. We also want to thanks the academia experts and practitioners for their availability to contribute to our research.

REFERENCES

[1] P. Panaroni, G. Sartori, F. Fabbrini, M. Fusani, and G. Lami, "Safety in automotive software: an overview of current practices," IEEE International Conference on Computer Software and Applications, pp. 1053-1058, July 2008.

[2] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety. Mit Press, 2011.

[3] R. Guillerm, H. Demmou, N. Sadou, "Information model for model driven safety requirements management of complex systems," Complex systems design & management, pp.99–111, 2010.

[4] A. Simpson, J. Stoker, "Will it be Safe?—An Approach to Engineering Safety Requirements," Components of System Safety pp.140–164, 2002.

[5] R. Wendler, "The maturity of maturity model research: a systematic mapping study," Information and software technology, v.54, n.12, pp.1317–1339, 2012.

[6] M. Svahnberg, T. Gorschek, TT Nguyen, M. Nguyen, "Uni-REPM: a framework for requirements engineering process assessment," Requirements Engineering Journal, v.20, n.1, pp.91–118, Mar 2015.

[7] L. Martins, T. Gorschek, "Requirements engineering for safety-critical systems: A systematic literature review," Information and Software Technology, v. 75, pp. 71-89, 2016.

[8] J. Vilela, J. Castro, L. Martins, T. Gorschek, "Integration between requirements engineering and safety analysis: A systematic literature review," Journal of Systems and Software, v. 125, pp. 68-92, 2017.

[9] T. Gorschek, A. Gomes, A. Pettersson, R. Torkar, "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.

[10] P. Sawyer, I. Sommerville, S. Viller, "Requirements process improvement through the phased introduction of good practice," Software Process: Improvement and Practice, v.3, n.1, pp. 19–34, 1997.

[11] T. Gorschek, M. Svahnberg, K.; Tejle, "Introduction and application of a lightweight requirements engineering process," International workshop on requirements engineering: foundation for software quality, 2003.

[12] A. Davis, D. Zowghi, "Good requirements practices are neither necessary nor sufficient," Requirements Engineering Journal, v.11, n.1, pp.1–3, 2006.

[13] B. Solemon, S. Sahibuddin, A. Ghani, "Requirements engineering problems and practices in software companies: an industrial survey," International conference on advanced software engineering and its applications, pp.70–77, 2009.

[14] T. Gorschek, P. Garre, S. Larsson, C. Wohlin, "A model for technology transfer in practice," IEEE software, v.23, n.6, p.88–95, 2006.

[15] J. Lewis, "IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use," International Journal of Human-Computer Interaction, v.7, n.1, pp.57–78, 1995.

[16] B. Solemon, S. Sahibuddin, and A Ghani, "Requirements engineering problems and practices in software companies: An industrial survey", International Conference on Advanced Software Engineering and Its Applications, pp. 70–77, 2009.

[17] E. Sikora, B. Tenbergen, K. Pohl, "Industry needs and research directions in requirements engineering for embedded systems,", Requirements Engineering Journal, 17(1), pp.57-78, 2012.

[18] Hatcliff, J., Wassyng, A., Kelly, T., Comar, C. and Jones, P. Certifiably safe software-dependent systems: challenges and directions. In: Proceedings of the on Future of Software Engineering, 2014, pp. 182-200.

[19] G. Lami, F. Fabbrini, and M. Fusani, "An extension of iso/iec 15504 to address safety processes," International Conference on System Safety, pp. 1–6, 2011.

[20] A. D. o. D. Defence Materiel Organisation. +SAFE: A safety extension to CMMI-DEV, version 1.2. Software Engineering Institute, Technical Note CMU, Tech. Rep., 2007.

[21] T. Hall, S. Beecham, and A. Rainer, "Requirements problems in twelve software companies: an empirical analysis," IEEE Proceedings-Software, vol. 149, no. 5, pp. 153–160, 2002.

[22] T. Reis, M. Mathias, O. Oliveira, "Maturity models: identifying the state-of-the-art and the scientific gaps from a bibliometric study," Scientometrics, pp.1–30, 2016.