A Personal Opinion Survey on Process Compliance Checking in the Safety Context

Julieth Patricia Castellanos Ardila and Barbara Gallina

IDT, Mälardalen University, Västerås, Sweden
{julieth.castellanos, barbara.gallina}@mdh.se

Abstract. Manually checking the compliance of process plans against the requirements of applicable standards is a common practice in the safety-critical context. We hypothesize that automating this task could be of interest. To test our hypothesis, we conducted a personal opinion survey among practitioners who participate in safety-related process compliance checking. In this paper, we present the results of this survey. Practitioners indicated the methods used and their challenges, as well as their interest in a novel method that could permit them to move from manual to automated practices via compliance checking.

Keywords: (Automated) Compliance Checking · Process Plan · Safety-critical · Current Practices · Challenges · Personal Opinion Survey.

1 Introduction

Safety standards usually include requirements that prescribe the planning of tasks, and the resources required and produced, e.g., personnel, work products, and tools. Nair et al. [13], reports 9 essential process plans required in safety assessment, i.e., Safety Management, Communication, Risk Management, Configuration Management, Development, Verification and Validation, Modification Procedures, Operation Procedures, and Staff Competence. Manually checking the compliance of such plans against the requirements of applicable standards is a common practice. The checklists used can be obtained by listing the requirements of the standard, or listing personal or organizational practices [15]. A process compliance checklist, which has been accurately filled-in, requires a proper evaluation of the satisfaction of the requirements. Thus, missed requirements are highlighted, providing hints to improve the process.

Process compliance checking could be overwhelming due to the sheer volume and complexity of the knowledge included in the standards. Thus, we hypothesize that automating this task could be of interest. To test our hypothesis, we conducted a personal opinion survey [12] among practitioners who participate in safety-related process compliance checking. In this paper, we present the results of this survey. In particular, practitioners indicated the methods used and their challenges, as well as their interest in a novel method that could permit them to move from manual to automated process compliance checking. These results

contribute to systematizing the knowledge about process compliance checking and finding methods and tools for facilitating this practice.

The rest of the paper is organized as follows. In Section 2, we present essential background. In Section 3, we present the research method used to conduct the survey. In Section 4, we present the survey results. In Section 5, we discuss our findings. In Section 6, we examine related work. Finally, in Section 7, we conclude our work and present future work.

2 Background

This section presents essential background.

2.1 Facilitating Automated Process Compliance Checking

In the context of the European project AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems)[1], we proposed a process-centered planning-time method for safety-related process compliance checking [4, 5]. The method requires users to create artifacts in a SPEM 2.0 (Systems & Software Process Engineering Metamodel)[2] reference implementation supported with Eclipse Process Framework (EPF) Composer[3] (see Fig. 1), as follows. (1) Method content, which are elements that are part of a process, i.e., roles, tasks, work products, and guidance. (2) A knowledge base of compliance information based on the formalization of standard requirements in Formal Contract Logic (FCL) [10]. FCL is a defeasible deontic logic, i.e., it supports the modeling of norms representing obligations and permissions in a normative context that can be defeated by evolving knowledge. In FCL, a rule has the form: r: $a_1, ..., a_n \Rightarrow c$, where r is the rule identifier, $a_1, ..., a_n$ are the propositions that represent the conditions of the applicability of the norm, and c is the concluding proposition that contains normative effects. For this, SPEM 2.0 guidance elements are customized as requirements, FCL rules, and compliance effects (which correspond to the propositions of the rules). (3) Compliance effects are annotated in the process tasks. As compliance effects describe the concrete actions prescribed by the standard requirements, users need to evaluate each task action and define its effects in the overall process compliance to make the annotation. For example, the task *Start software Unit Design Process* indicates that the process is performed and has two inputs. Thus, the annotated compliance effects are *addressSwUnitDesignProcess*, *ProvideSwArchitecturalDesign* and *ProvideSwSafetyRequirements*. (4-a) A sequential representation of the process plan, as well as its dynamic representation (4-b), are created by using the compliance annotated tasks. The dynamic representation is used to automatically generate a compliance state representation of the process, which permits automatic

[1] https://www.amass-ecsel.eu/
[2] https://www.omg.org/spec/SPEM/About-SPEM/
[3] https://www.eclipse.org/epf/

compliance analysis with the compliance checker Regorous[4]. Regorous provides (5) compliance checking results, i.e., description of compliance issues, rules and elements involved, and possible resolutions. For facilitating FCL formalization, the concept of Safety Compliance Pattern (SCP) [3, 6] has been defined. An SCP describes commonly occurring normative safety requirements on the permissible state sequence of a finite state model of a process. These patterns can be instantiated from predetermined templates. EPF-C has been recently updated to Eclipse Neon 4.6.3 in the context of the AMASS project [11].

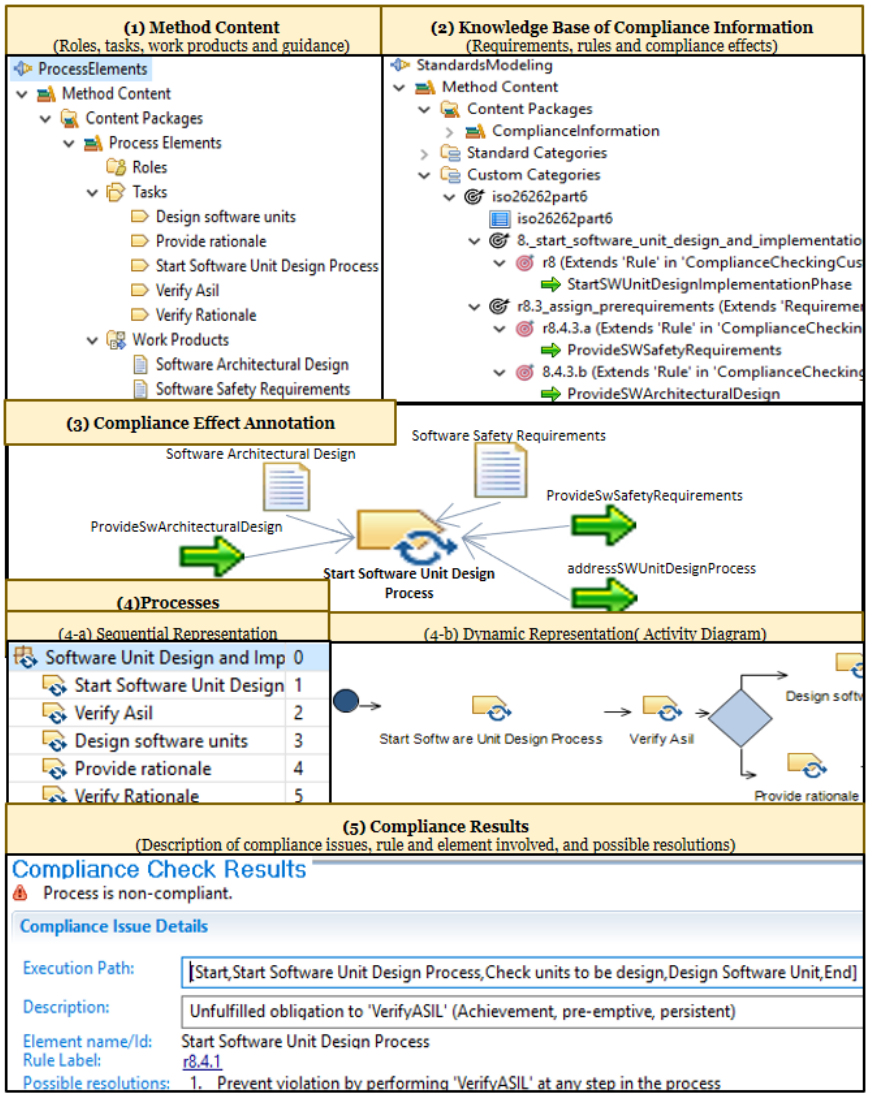


Fig. 1: Method for Facilitating Automated Process Compliance Checking.

[4] https://research.csiro.au/data61/regorous/

2.2 Personal Opinion Surveys

A personal opinion survey [12] is a comprehensive research method for collecting information using a questionnaire completed by subjects. When creating a survey, the first step is to define the expected outcomes. Then, the survey should be designed, e.g., cross-sectional (participants are asked for information at one fixed point in time). It is also essential to define options related to how the survey would be administered. Once designed, the survey instrument should be developed, evaluated, and applied to a sample population, from which obtained data is analyzed.

Four types of validity need to be addressed to make sure that the survey instrument is measuring what it supposes to measure [12]. 1) *Face validity* is a cursory review of items by untrained judges. 2) *Content validity* is a subjective assessment of how appropriate the instrument seems to a group of reviewers with knowledge of the subject matter. 3) *Criterion validity* is the ability of a measurement instrument to distinguish respondents belonging to different groups. 4) *Construct validity* concerns how well an instrument measures the construct it is designed to measure.

In the creation of surveys, Likert Scales [1] are widely used. Likert Scales are psychometric response scales, e.g., a five-point scale ranging from "Strongly Disagree" to "Strongly Agree," used to ask respondents to indicate their level of agreement with a given statement. On a Likert scale, each specific question can have its response analyzed separately, or have it summed with other related items to create a score for a group of statements. Individual responses are generally treated as ordinal data because although the response levels do have a relative position, we cannot presume that participants perceive the difference between adjacent levels to be equal.

2.3 Technology Acceptance Model

The Technology Acceptance Model (TAM) [7] provides general determinants of computer acceptance. TAM is capable of explaining user behavior across a broad range of end-user computing technologies and user populations, while at the same time being theoretically justified. TAM focuses on three main facets of user acceptance. The first is the degree to which a person believes that using a particular method will be free of effort (Perceived Usability). The second is related to a person's subjective probability that using a particular system would enhance his/her job (Perceived Usefulness). The third is the extent to which a person intends to use a particular system (Intention to Use).

3 Research Method

In this section, we present the details regarding the creation of a personal opinion survey. We followed the guidelines recalled in Sections 2.2 and 2.3.

3.1 Research Questions

In this survey, we aim at gathering information about current industrial practices and challenges in process compliance checking, as well as the acceptance level of the method for automated compliance checking (recalled in Section 2.1). Within this scope, we formulate the research questions presented below.

- RQ1: How do practitioners currently perform process compliance checking?
- RQ2: What are the challenges that practitioners face when performing process compliance checking?
- RQ3: What is the level of acceptance of practitioners regarding a novel method for facilitating automated compliance checking?

3.2 Survey Design

We designed a cross-sectional web-based personal opinion survey, whose goal is to collect data relevant to answer the research questions presented in Section 3.1. The target population is practitioners involved in process compliance checking in the safety-related context. The final survey[5], which starts with a short introduction to the purpose of the study, is composed of 21 questions, which are organized into four parts.

1. **Demographics.** Questions 1-7 aim at gathering the background characteristics of the practitioners.
2. **Current practices.** Questions 8-14 aim at gathering information about practitioners' experiences in compliance checking.
3. **Challenges.** Questions 15 and 16 aim at inquiring about the challenges appearing in process compliance checking. In question 15, practitioners rate the importance of 7 possible challenges by using a five-point Likert scale ranging from Unimportant to Very Important. Question 16 is an open question in which practitioners can write further challenges.
4. **Automated process compliance checking.** First, practitioners read information about the method for facilitating automated compliance checking recalled in Section 2.1. Then, we present the questions 17-21 as a series of claims from which we seek practitioners' degree of acceptance regarding the user acceptance aspects described in the TAM model (see Section 2.3), i.e., the method usefulness, usability, and user's intention to use it. To collect the answers, we use a five-point Likert Scale ranging from Strongly Agree to Strongly Disagree.

We were interested in the practitioners' overall experience. Thus, where possible, the practitioners were allowed to select more than one option to indicate their experience regarding several practices. Practitioners were also given the possibility to mention additional options or answer "Don't know" if this was the case. We consider that completing the survey would take between 20-25 minutes.

[5] https://www.dropbox.com/s/efcab84me7kxpj8/FinalSurvey.pdf?dl=0

3.3 Instrument Evaluation and Data Collection

The first author created a set of initial questions. The second author helped to structure and design the survey by providing comments for cleaning ambiguity and a more in-depth analysis that led to the formulation of further questions. Then, we distributed the survey to a selected group of safety experts during the Scandinavian Conference on System & Software Safety[6]. One expert provided valuable comments that were used to improve the survey. The final evaluation was performed by both authors, improving textual explanations and questions.

The data was collected from January 22th to February 28th of 2020. The survey was distributed via personal e-mail invitations. The selection of the practitioners included industrial experts (on purpose, we discarded research institutions) that participate in European projects related to certification and self-assessment. We also extracted industrial-related practitioners from conferences, symposiums, and workshops related to safety assurance. In total, we obtained 15 valid responses from which 8 were received after the initial invitation letter, and 7 were received after a reminder e-mail.

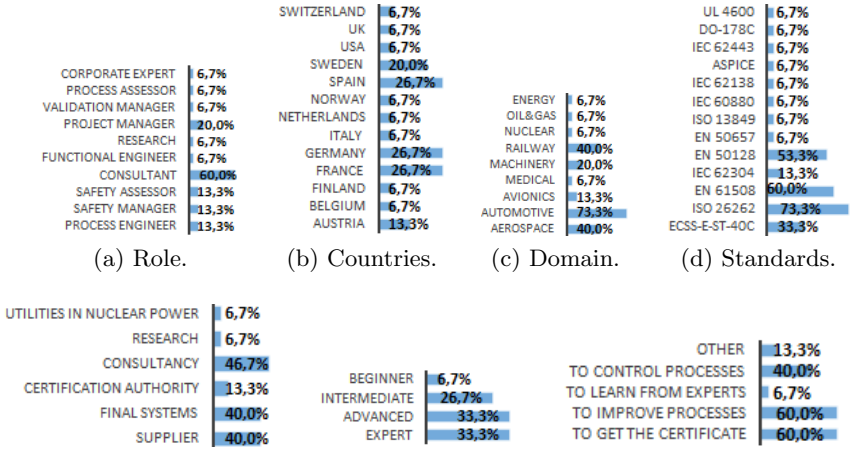
3.4 Subject Characteristics and Data Analysis

The valid answers were obtained from practitioners mostly working in the consultatory branch (see Fig. 2a and Fig. 2g) which have experience demonstrating process compliance checking in 13 countries (see Fig. 2b), predominantly Europe. The practitioners have experience in 9 safety-related domains (see Fig. 2c) and 13 standards (see Fig. 2d), where automotive is the most represented. The major interest of the practitioners, which shows higher levels of expertise (see Fig. 2f) in process compliance checking, is to get the compliance certification and improve processes (see Fig. 2g). The analysis of our survey was adjusted with the information provided in the "Others" option.

3.5 Survey Validity

The four types of validity of the survey instrument (recalled in Section 2.2) were addressed as follows. To avoid *face validity*, we perform a careful review of our survey instrument in several stages and with experts in the field of safety certification. *Content validity* was assured by doing a careful literature review on the topic and validating as well with experts. Regarding *criterion validity*, we assure that the practitioners' background was related to the type of expertise we were looking by making a careful selection process. For reducing the *construct validity*, we allow the practitioners to include the "Others" option. Thus, the threat of providing an incomplete list of options is minimized. Additionally, to avoid evaluation apprehension, we guaranteed confidentiality and anonymity of the responses.

[6] http://safety.addalot.se/2019



(a) Role. (b) Countries. (c) Domain. (d) Standards.

(e) Company Type. (f) Expertise. (g) Checking Reasons.

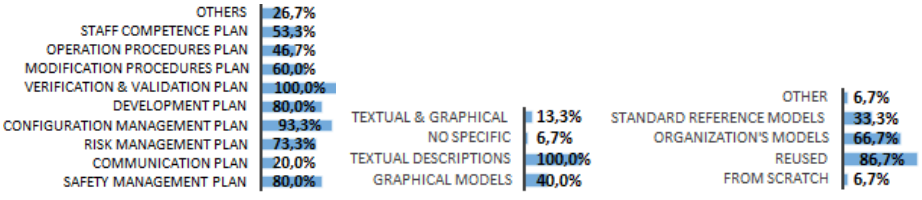
Fig. 2: Demographic Results.

4 Survey Results

In this section, we present the results of the survey by answering the research questions presented in Section 3.1.

4.1 Current Practices (RQ1)

Fig. 3a shows the 9 process plans (recalled in the introductory part) provided as alternatives in the questionnaire in the vertical axis, and the percentage of respondents, who selected each type in the horizontal axis. Fig. 3a shows that practitioners have performed compliance checking mostly on the Verification and Validation, Configuration Management, Safety Management, Development, Risk Management, and Modification Procedure Plans. The remaining plans listed were less considered as part of the practitioners' compliance checking duties. In the "Others" option, practitioners mentioned the Software Quality Assurance, Safety Assessment, Documentation, and Cybersecurity Plans.

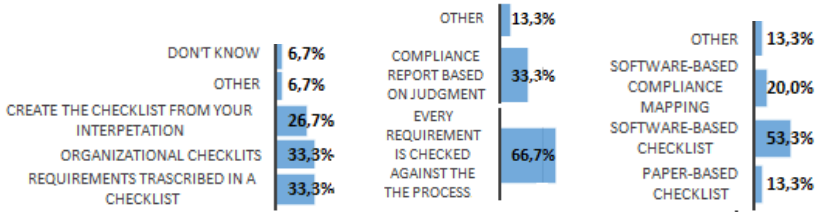


(a) Plan Types. (b) Representation. (c) Creation.

Fig. 3: Information Regarding Processes.

Current practices indicate that processes are mostly represented with only text, but graphical representations are also relevant (see Fig. 3b). Moreover, process plan reuse is a common practice (see Fig. 3c).

Regarding checklist preparation, we found that the three alternatives given in the questionnaire are almost equally used (see Fig. 4a). The practice of compliance checking is done in different ways. Most commonly, practitioners take every requirement and check it against the information provided by the process specification (see Fig. 4b). Practitioners also base the compliance assessment on other practices, such as the use of points of compliance, and the assessment of strengths and weaknesses of the findings. It is common that practitioners use software tools for performing compliance management tasks (see Fig.4c). Rational doors, Microsoft suite (e.g., Word, Excel, and MS project), opencert, verification studio, engineering studio, stages (for modeling processes) were the tools mentioned by practitioners in the survey.



(a) Preparation. (b) Checking. (c) Mechanism.

Fig. 4: Information Regarding Compliance Checking.

4.2 Challenges (RQ2)

Fig. 5 presents a set of challenges that could appear during process compliance checking to which we ask respondents to rate them from very important to unimportant. The results shows that one of the challenges that was considered very important by the practitioners is that *"it is common to miss requirements"*. Important challenges are: *"Check process-based compliance requires that many people are involved"*, *"Check the compliance of a process requires many interactions"*, *"Check process-based compliance requires many hours of work"* , and *"It isn't easy to determine the kind of information that should be provided as evidence from the process perspective."* The practitioners considered the other challenges moderately important. The practitioners also have the option to list their challenges to which they answer that *"Sometimes there is no access to the evidence"*, *"Sometimes the safety assessor could have different interpretations"*, and *"It is difficult to check the user acceptance of the defined processes."*

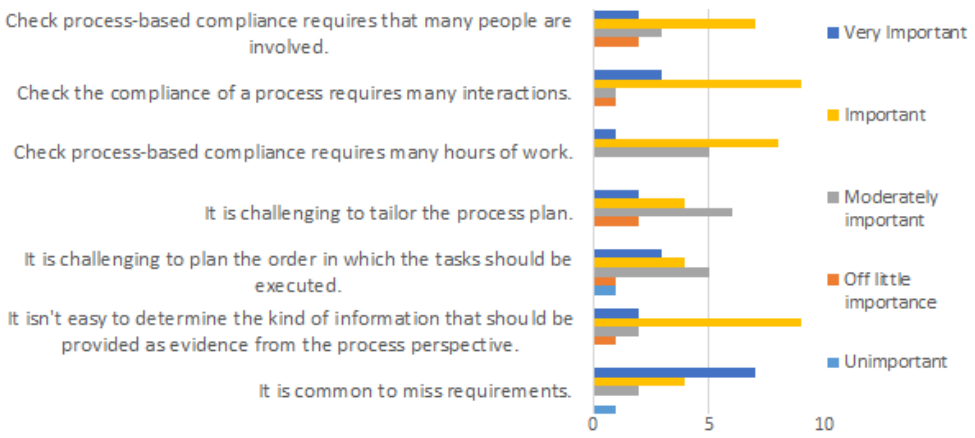


Fig. 5: Challenges in Process Compliance Checking.

4.3 Automatic Process Compliance Checking (RQ3)

This part of the survey gathered data regarding the user acceptance level of the method for facilitating automated process compliance checking (recalled in Section 2.1). Initial evaluation is performed on FCL, which is the logic used to formalize the requirements prescribed by the standards. Practitioners somewhat agree that the formalization of standard requirements could be facilitated with FCL since it provides the compliance concepts and there are safety compliance patterns to instantiate (see Fig. 6). Practitioners also somewhat agree that FCL can be used to support the creation of the tailoring rules. However, most of the practitioners are neutral whether the analysis required to formalize process requirements could help them to understand their intention.

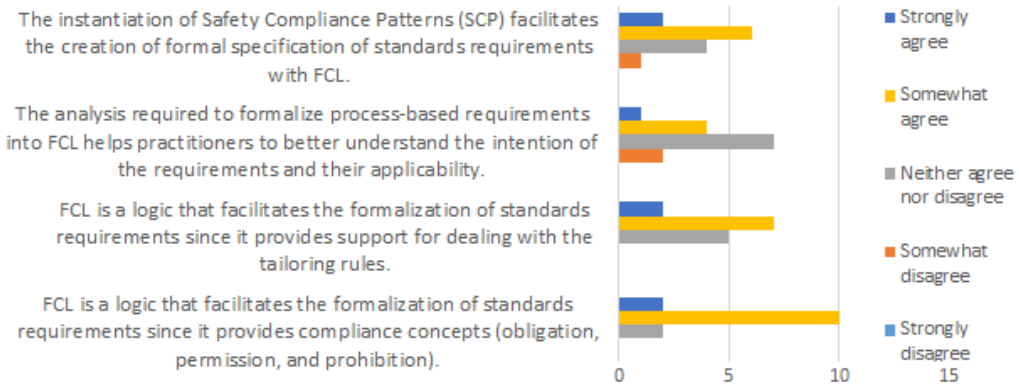


Fig. 6: The Ability to Formalize Requirements with FCL.

Regarding the ability of the method to represent processes and compliance information (see Fig 7) we found that the majority of the practitioners somewhat agree with the statements regarding the provision of graphical representations.

In particular, graphical representation of the compliance information, as well as process plans, facilitate their understanding and documentation. Similarly, the majority of the practitioners somewhat agree that this aspect also would facilitate compliance management.

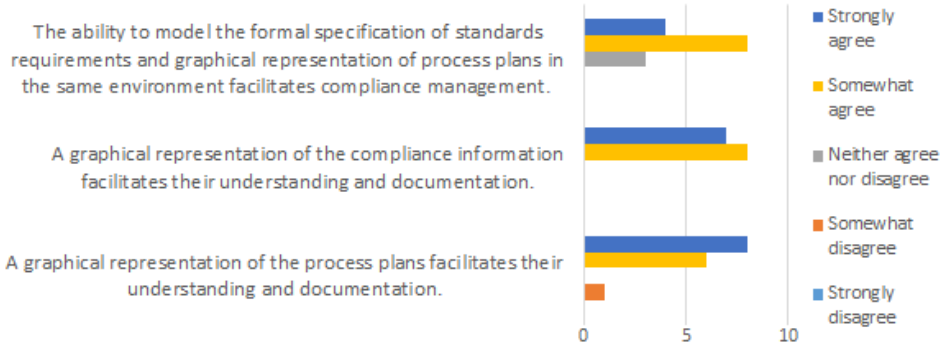


Fig. 7: The Ability to Represent Processes and Compliance Information.

Then, we focused on the ability of the method to perform automated compliance checking (see Fig. 8). As the figure depicts, the ability to perform automated compliance checking is seen by the majority of the practitioners as favorable. In particular, practitioners somewhat agree that the iterative application of automated compliance checking can help them to reach process plans with compliant states. Moreover, the majority of the practitioners strongly agree that modifying a compliant process plan to define a new process reduces the work that needs to be done. Finally, traceability could be facilitated with a hierarchically organized knowledge-based of compliance artifacts. Such an organization helps to understand the source of compliance problems.

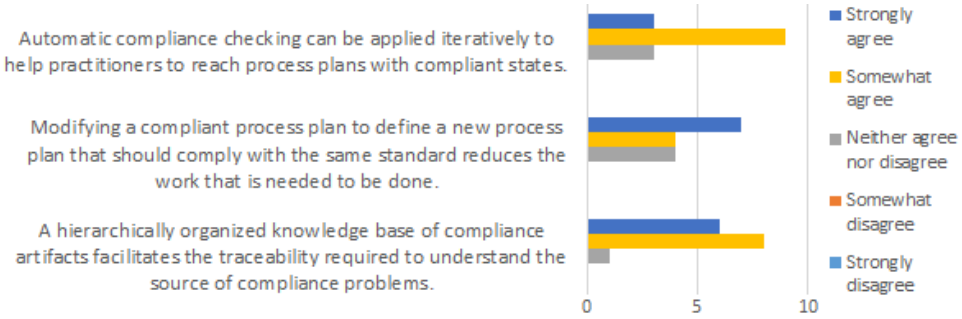


Fig. 8: The Ability to Perform Automated Compliance Checking.

Fig. 9 shows the results regarding the perceived usability aspect of the method. Practitioners do not strongly agree or strongly disagree with any of the questionnaire's options. However, there are two statements that practitioners somewhat agree: it is easy to 1) trace uncompliant situations and 1) graphically model process elements.

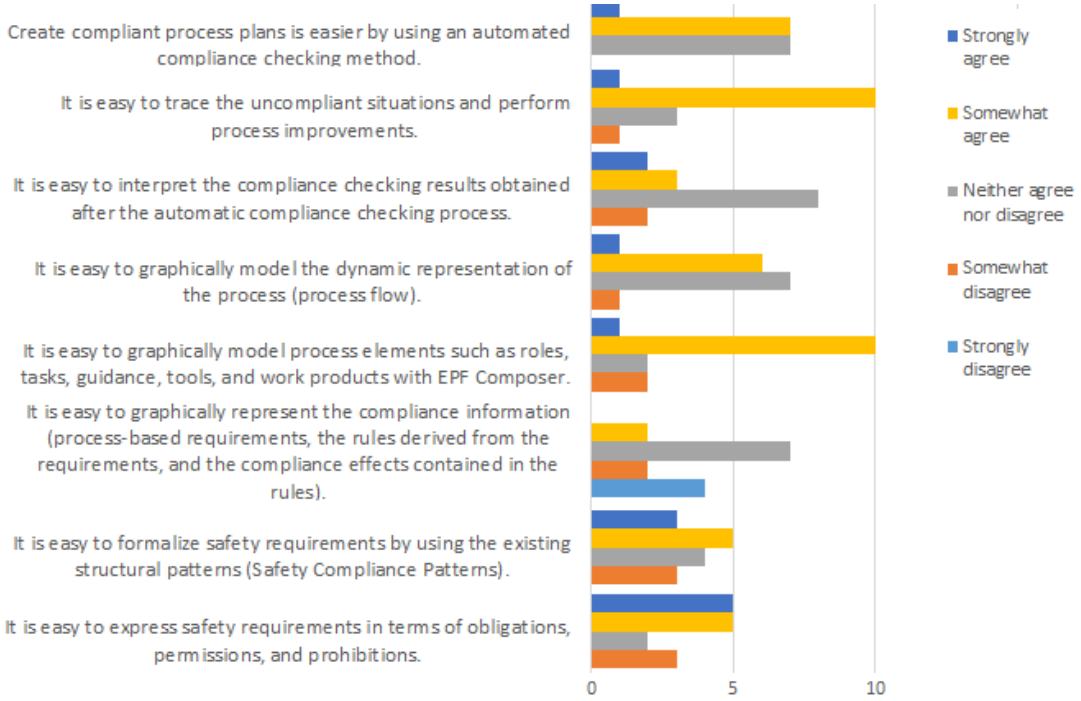


Fig. 9: Perceived Usability Aspect of the Method.

Finally, one question was asked to the practitioners about their intention to use the method. As Fig. 10 depicts 67% of the practitioners indicated that they would use the method for facilitating automated compliance checking if it were made available. In contrast, 13% of the practitioners do not know, and 20% would not do it.

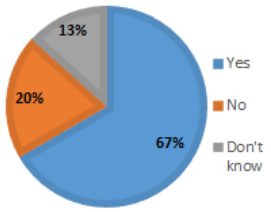


Fig. 10: Intention to Use.

5 Discussion

In this section, based upon the result of the survey, we discuss our findings.

Current Practices: Given the characteristics of the subjects, presented in Section 3.4, we consider our sample to be representative of the European safety-critical context. For this kind of population, process compliance checking is not only the way towards a safety certificate but also a mechanism for process improvement (see Fig. 2g). Their current practices include the checking of a variety of process plans (see Fig. 3a). Additional plan types respect to the ones described in the introductory part were considered necessary in the safety-critical context, i.e., Software Quality Assurance Plan, Safety Assessment Plan, Documentation Plan, and Cybersecurity Plan (see Section 4.1). Thus, it seems that compliance management from the process perspective is a growing area. Practitioners also

create process plans mostly by reusing previous processes or their elements (see Fig. 3c). This aspect indicates that support for reusability is significant in process compliance management. We also could see that there are different ways to create checklists (see Fig. 4a). It is interesting to see that most of the time, the practitioners receive the checklist from the organization (which is based on the organization's experience in the domain) or transcribe the actual requirements provided by the standard direct into a checklist. In those cases, there is not additional intellectual work included in the preparation of the checklist, and the provision of a general, widely accepted checklist could be useful for minimizing such initial work. Finally, most of the practitioners use software tools to perform compliance checking to support their activities (see Fig. 4c). Thus, it is not expected that the introduction of more sophisticated software tools would generate extreme distortions in their daily job. However, it would be good to revise the ways to introduce them smoothly.

Challenges: Practitioners are faced with several challenges when performing compliance checking, as presented in Section 4.2. In general, practitioners consider that compliance checking is prone-to-error. For them, it is possible to miss requirements. Moreover, they consider that it is not easy to determine the kind of information that should be provided as evidence (or there is no access to evidence), and that there are different possible interpretations provided by the assessors. In addition, practitioners consider that compliance checking is time-consuming since it requires many hours of work and several iterations. Finally, many people in the organization are needed making it also resource-consuming. Thus, there is a need for solutions that provide more confidence and efficiency in process compliance checking.

Automated compliance checking: User acceptance is a major for any technological endeavor. In general, as we presented in Section 4.3, there are advantages regarding automated process compliance checking. In particular, as depicted in Fig. 6, there is a good degree of acceptance for the characteristics provided by FCL, which is the formal approach used for requirements representation. However, there is some hesitation regarding its usage, as expected with formal methods. In particular, practitioners do not see how the analysis required to formalize process requirements would help them to understand their intention. For this reason, it is necessary to explain further the formalization part of the method by providing more guidance and examples. As presented in Fig. 7 and Fig. 8, the ability to represent processes and compliance information graphically and the ability to automatically check compliance also have a good degree of acceptance. Thus, the method has high acceptability potential, and its graphical representations are considered the strongest advantage. Finally, as presented in Fig. 9, two aspects regarding the method are considered easy to use, i.e., graphically represent process models and trace uncompliant situations. However, we need to provide mechanisms for improving the tool usability in terms of compliance information representation, which appears to be not easy to use by practitioners. In addition, we need to improve the representation of checking results. For facilitating these aspects, we can provide more specific graphical

representations of the compliance artifacts and, after backpropagating the results of Regorous into EPF Composer, present them in a suitable user interface that provides detailed explanations. Finally, practitioners show a willingness to use the method, which could be helpful for evolving from the current manual practices to automated practices via compliance checking.

6 Related Work

Nair et al. [15] performed in-depth interviews with 7 safety-related practitioners, which show the importance of checklists in safety assessment. In [14], a personal opinion survey was applied to 53 experts to study safety evidence management practices. Our survey also analyzed the use of the process plans analyzed in [14], and found that additional process-related plans are required in safety assessment. In [2], the authors present the results of interviews with practitioners regarding change impact analysis, which is essential during safety assessment. De la Vara et al. [8] surveyed safety evidence, particularly the circumstances under which it is created, the tool support used, and the challenges faced. In contrast to the works previously mentioned [15, 14, 2, 8] our focus is to investigate the currently used methods and its challenging aspects in process compliance checking, as well as the practitioner's interest in novel methods for facilitating the automation of this task. The work conducted by Diebold and Scherr [9] reports industrial practices regarding the use of software process descriptions. In particular, the survey shows that companies use different process representations, i.e., graphical, table-based, or structured text notations. It also shows that the use of formal models and their advantages are highly desirable by practitioners. Our study differs from [9] in that we also include aspects regarding the use of formal descriptions of processes for compliance checking.

7 Conclusions and Future Work

In this paper, we presented the results of a personal opinion survey conducted among practitioners who participate in process compliance checking in the safety-critical context. The practitioners indicated that they mostly represent process plans and standard requirements by using software-based tools. Thus, software-based compliance checking aids are not new for them. However, practitioners consider that process compliance checking is prone-to-error; e.g., missing requirements is a common problem. Process compliance checking also requires many hours of work and several people. Finally, the practitioners show a favorable position regarding automated process compliance checking based on SPEM 2.0-like artifacts. They also indicated usability aspects regarding the formalization of requirements that we need to revisit and improve.

Future work will include more empirical research with the use of interviews and observations to see, for instance, how practitioners carry out their compliance checking in real settings. In addition, the usability aspects will be revisited, in order to provide more guidance and improve the representation of compliance

artifacts and checking results. Finally, the tool support will be concretized to facilitate evaluations in terms of efficiency through industrial case studies.

References

1. Bertram, D.: Likert Scales Are the Meaning of Life. CPSC 681-Topic Report (2006), http://poincare.matf.bg.ac.rs/ kristina/topic-dane-likert.pdf
2. Borg, M., de la Vara, J., Wnuk, K.: Practitioners' perspectives on change impact analysis for safety-critical software – A preliminary analysis. In: International Conference on Computer Safety, Reliability, and Security. pp. 346–358 (2016)
3. Castellanos Ardila, J.P., Gallina, B.: Formal Contract Logic Based Patterns for Facilitating Compliance Checking against ISO 26262. In: 1st Workshop on Technologies for Regulatory Compliance. pp. 65–72 (2017)
4. Castellanos Ardila, J.P., Gallina, B., Ul Muram, F.: Enabling Compliance Checking against Safety Standards from SPEM 2.0 Process Models. In: Euromicro Conference on Software Engineering and Advanced Applications. pp. 45 – 49 (2018)
5. Castellanos Ardila, J.P., Gallina, B., UL Muram, F.: Transforming SPEM 2.0-compatible Process Models into Models Checkable for Compliance. In: 18th International SPICE Conference (2018)
6. Castellanos Ardila, J., Gallina, B., Governatori, G.: Lessons Learned while formalizing ISO 26262 for Compliance Checking. In: 2nd Workshop on Technologies for Regulatory Compliance. pp. 1–12 (2018)
7. Davis, F.: A technology acceptance model for empirically testing new end-user information systems: Theory and results. Massachusetts Institute of Technology (1985)
8. De La Vara, J., Borg, M., Wnuk, K., Moonen, L.: An Industrial Survey of Safety Evidence Change Impact Analysis Practice. IEEE Transactions on Software Engineering **42**(12), 1095–1117 (2016)
9. Diebold, P., Scherr, S.: Software process models vs descriptions: What do practitioners use and need? Journal of Software: Evolution and Process **29**(11), 1–13 (2017)
10. Governatori, G.: Representing business contracts in RuleML. International Journal of Cooperative Information Systems **14**(02n03), 181–216 (2005)
11. Javed, M., Gallina, B.: Get EPF Composer back to the future: a trip from Galileo to Photon after 11 years. In: EclipseCon (2018)
12. Kitchenham, B., Pfleeger, S.: Personal Opinion Surveys. In: Guide to Advanced Empirical Software Engineering, chap. 3, pp. 63–92. Springer Science & Business Media (2008)
13. Nair, S., De La Vara, J., Sabetzadeh, M., Briand, L.: An extended systematic literature review on provision of evidence for safety certification. Information and Software Technology **56**(7), 689–717 (2014)
14. Nair, S., De La Vara, J., Sabetzadeh, M., Falessi, D.: Evidence management for compliance of critical systems with safety standards: A survey on the state of practice. Information and Software Technology **60**, 1–15 (2015)
15. Nair, S., Kelly, T., Jørgensen, M.: A Report on the State-of-the-Practice of Safety Evidence Assessment. Tech. rep. (2014)