Simula Research Laboratory, Technical Report 2014-18, November 2014

Survey on Safety Evidence Change Impact Analysis in Practice: Detailed Description and Analysis

Jose Luis de la Vara[1], Markus Borg[2], Krzysztof Wnuk[3], and Leon Moonen[1]
[1]Certus Centre for Software V&V, Simula Research Laboratory, P.O. Box 134, 1325 Lysaker, Norway
[2]Department of Computer Science, Lund University, P.O. Box 118, SE-22100 Lund, Sweden
[3]Software Engineering Research Lab, Blekinge Institute of Technology, SE-37179 Karlskrona, Sweden
{jdelavara, leon}@simula.no, markus.borg@cs.lth.se, krzysztof.wnuk@bth.se

Abstract. In many application domains, critical systems must comply with safety standards. This involves gathering safety evidence in the form of artefacts such as safety analyses, system specifications, and testing results. These artefacts can evolve during a system's lifecycle, creating a need for impact analysis to guarantee that system safety and compliance are not jeopardised. Although extensive research has been conducted on change impact analysis and on safety evidence management, the knowledge about how safety evidence change impact analysis is addressed in practice is limited. This paper reports on a survey targeted at filling this gap by analysing the circumstances under which safety evidence change impact analysis is addressed, the tool support used, and the challenges faced. We obtained 97 valid responses representing 16 application domains, 28 countries, and 47 safety standards. The results suggest that most practitioners deal with safety evidence change impact analysis during system development and mainly from system specifications. Furthermore, the level of automation in the process is low and insufficient tool support is the most frequent challenge. Other notable findings include that the different artefact types used as safety evidence seem to co-evolve, the evolution of safety case should probably be better managed, and no commercial impact analysis tool has been reported as used for all artefact types. Finally, we identified over 20 areas where the state of the practice in safety evidence change impact analysis can be improved.

Keywords. Safety-critical system, safety evidence, impact analysis, change management, safety assurance, safety certification.

1 Introduction

Most critical computer-based and software-intensive systems in domains such as aerospace, railway, and automotive are subject to some form of safety assessment by a third party (e.g., a certification authority) as a way to ensure that these systems do not pose undue risks to people, property, or the environment. The most common type of assessment is compliance with safety (or safety-related) standards, usually referred to as safety certification. Examples of safety standards used in industry [53] include IEC 61508 for electrical, electronic, and programmable electronic systems in a wide range of industries, and more specific standards such as DO-178 for avionics, the CENELEC standards for railway (e.g., EN 50128), and ISO 26262 for the automotive sector.

Demonstration of compliance with a specific standard involves gathering and providing convincing safety evidence, defined as artefacts that contribute to developing confidence in the safe operation of a system and that are used to show the fulfilment of the criteria of a safety standard [55]. Examples of artefact types that can be used as safety evidence include safety analysis results, system specifications, testing results, reviews, and source code. Such artefacts can evolve during a system's lifecycle. The corresponding changes must be managed and impact analysis might be necessary in order to guarantee that the changes do not jeopardise system safety or compliance with a standard. By safety evidence change impact analysis (SECIA), we refer to the activity that attempts to identify, in the body of safety evidence, the potential consequences of a change. Possible consequences can be the need for adding, modifying, or revoking some artefact.

Impact analysis can be regarded as a crucial activity in the lifecycle of any safety-critical system. Indeed, it is prescribed in most of the safety standards used in industry. However, the standards do not explain in detail how to perform an impact analysis, but just provide general guidance [15, 31]. In some cases, the standards do not even clearly state when an impact analysis should be performed. This can lead to inadequate impact analysis in practice. Examples of critical systems that have had some accident or near-accident because of inadequate impact analysis can be found in the literature [31, 32, 43, 74, 77].

Although safety evidence management and impact analysis are two research areas that have received significant attention in the last decades, prior research barely reflects on the state of the practice. The percentage of publications reporting insights into how practitioners deal with these activities is very low [41, 55], and we are not aware of any publication that has studied yet in depth how SECIA is addressed in industry. Therefore, a global picture of current SECIA practices does not exist. The scope of previous empirical studies is also limited, as they have focused on specific practices related to a reduced set of companies, standards, application domains, or artefact types. Without the corresponding knowledge, it is very difficult to effectively determine general industry practices and needs, and to shape future research towards these needs.

As a way to mitigate the above weaknesses, we conducted a survey aimed at gaining insights into how industry deals with SECIA. We designed a web-based questionnaire targeted at practitioners that are or have been involved in SECIA. This includes people who provide, check, and/or request safety evidence. We asked about the circumstances under which SECIA is addressed, the tool support used, and the challenges faced. We obtained 97 valid responses from 16 application domains, 28 countries, 47 safety standards, nine types of organizations, and five overall roles.

Modification of a new system during its development was reported as the situation in which the respondents had performed SECIA more frequently. Manual verification and validation (V&V) results was the artefact type that most frequently indicated as affected by changes in the body of safety evidence, despite the fact that other artefact types had triggered SECIA more often. Strong and very string SECIA-related correlations have also been found between the artefact types analysed in the survey. Requirements specifications and traceability specifications are the artefact types for which a highest ratio of respondents was aware of SECIA tools. More advanced tool support is the area on which the respondents expected and seem to need the greatest progress.

To our knowledge, the survey is the largest empirical study concerning the state of the practice on safety evidence management and on impact analysis for safety-critical systems. Therefore, it is the study that provides the strongest empirical evidence on SECIA practices in industry. As further discussed below, the results can help academia to identify areas in which further research is necessary. Practitioners can benefit by gaining new insights into how they can or should deal with SECIA, and also use the survey results as a benchmark for their own practices.

The rest of the technical report is organized as follows. Section 2 presents the background of the report. Section 3 describes the research method followed. Section 4 presents the results and how we interpret them. Section 5 summarises our conclusions. Finally, Appendix A shows the survey instrument, whereas Appendix B, C, and D contain information about the standards and tools mentioned by the respondents.

2 Background

This section presents the background of the technical report, focusing on related work on impact analysis in practice. The section is divided into general literature on impact analysis, whose insights can apply to safety evidence, and specific literature on impact analysis for safety-critical systems. Related work is also used in Section 4 for discussing the results of the survey.

The main differences between our survey and related work are that: (1) we are not aware of any SECIA-related study whose results are based on a higher number of responses, application domains, countries, and safety standards; (2) prior research has acknowledged the existence of many phenomena (e.g., artefact types involved in impact analysis or challenges faced by practitioners), but has not provided insights into how often the phenomena occur in SECIA; (3) most related work has only studied a reduced number of artefact types (e.g., requirements or source code), and; (4) very little information exists about the tools used for SECIA in industry, and this information is practically non-existence for some artefact types (e.g., assumptions and operation conditions specifications).

2.1 General Literature on Impact Analysis

Impact analysis has been the subject of extensive research for the last four decades, especially in the context of software evolution and software maintenance [6]. It is also a recommended or prescribed practice in systems and software engineering standards (e.g., [27]).

Most research has focused on impact analysis for software source code change [41], studying both effects between source code artefacts and on other artefact types (e.g., test cases to re-execute after a change). Another area that has received great attention is requirements change impact analysis, especially during requirements management or traceability [33]. Publications on impact analysis that deal with artefact types such as architecture specifications [29], design specifications [11], software components [78], or test cases [19] can also be easily found.

Regarding tool support, requirements management tools and their support for requirements change management have been analysed [13, 28]. Tools for impact analysis of software source code change have also been reported [42, 44], and the authors indicated that most of them are just academic prototypes and that only JRipples seems to be stable and mature. According to Jamshidi et al. [29], most of the research on architecture-centric software evolution provided tool support, and full automation in some cases. The literature also reports on the extension and adaptation of commercial tools for impact analysis purposes [73]. Although automatic traceability has been acknowledged as suitable for facilitating and improving impact analysis, the validation of the current approaches presents weaknesses in order to assess their real potential in industry. The weaknesses include validation with a too low number of artefact instances [8] and of artefact types [54]. Some authors suggest that some manual work is always necessary for impact analysis [12].

There are works that have provided insights into the state of the practice. In the case study reported by Goeritzer [23], most software engineers performed impact analysis on source code manually and indicated that they would like to have more tool assistance. Babar et al. [1] conducted a survey on the usefulness of design rationales for software maintenance and conclude that documenting the rationale can facilitate the identification of the elements impacted by a change. Impact analysis issues related to aspects such as the lack of resources, the need for experience and expertise, inadequate traceability, insufficient tool support, and the need for more structured information have been indicated in an interview study [63]. The authors also propose improvement areas, including arranging meetings to discuss impact analysis and the introduction of tool and method support. Tao et al. [69] analysed how software engineers understand software source code changes. This study reports the need for more tool support and the difficulty in determining (1) the completeness and consistency of a change and (2) the effect on other software components.

Requirements changes have recurring nature according to the majority of survey respondents of the study by Ferreira et al. [20]. According to the same study, evaluating the consequences of the changes could be complex and time-consuming. This is in line with the case study reported by Wnuk et al. [75], where the authors report on the difficulty in impact analysis for large requirements specifications, and more concretely for changes that affect several product releases. Other reported challenges related to requirements change impact include the need for having several development roles involved to properly understand the impact [79], managing the dependencies between and thus the co-evolution of requirements and architecture specifications [39], and difficulties in accurately predicting the cost of requirements change management [45, 46]. In a study on embedded software engineering [24], the lack of documented relationships between requirements was reported as a major issue for impact analysis, as well as the lack of requirements management tools for adequately managing the relationships of requirements with other development artefacts. Challenges of tracing requirements and test cases and of maintaining alignment between requirements and test cases as requirements change have also been reported [4], as well as lack of satisfaction in industry with the processes and practices for impact analysis regarding regression testing [19].

Other challenges and areas for improvement that have been indicated include the possibility of ripple effects [3], the need for more cost-effective traceability approaches [22], and the need for integrating data from different sources and for ensuring quality in software evolution [50].

2.2 Literature on Impact Analysis for Safety-Critical Systems

Publications on impact analysis can also be found in the literature on safety-critical systems. Changes during system development, system modification and re-certification, and component reuse are examples of situations in which SECIA is necessary for a critical system [14]. The evolutionary nature of a safety case, defined as a documented argument aimed at providing a compelling, comprehensive, and valid case that a system is acceptably safe for a given application in a given operating environment, has been discussed in works such as [36, 51]. Previous work has also studied the evolution of safety analyses and assessments [47], the possible impact of architectural changes in a safety case [5], and safety case-based impact analysis [57]. Ge and Bai [21] have proposed an approach for safety-related requirements impact analysis that also deals with safety analysis artefacts such as fault tree analyses. Regarding software aspects of safety-critical systems, the literature on software evolution for industrial automation systems [66], change management in families of safety-critical embedded systems [67], and software evolution of medical devices [72] have been analysed. Finally, recently published metamodels for safety assurance and certification explicitly address evidence change-related aspects (e.g., [15]).

Among the tools for supporting impact analysis of safety-critical systems, Born et al. [10] have outlined a model-based tool for impact analysis in the automotive domain, and Jo et al. [30] have presented a tailored tool for software source code in railway. According to Lloyd and Reeve [48], widely available tools can facilitate impact analysis of safety-critical systems, and change management can be tracked with workflow tools or wikis. Nonetheless, the authors also indicated the suitability and use of mainly manual procedures. ASCE (Assurance and Safety Case Environment) and Reqtify are commercial tools that have been referred to in the literature [40, 51]. All these publications have provided evidence of use in industry only for Reqtify, in an avionics hardware development project. An important aspect to consider regarding tool support is tool qualification [40], a formal assurance of output suitability. In many domains, the output artefacts of a tool used in a critical system's lifecycle, including SECIA tools, need to be formally reviewed unless the tool is qualified. In this sense, tools can be regarded as safety-critical systems themselves, as their malfunction can lead to safety risks. As an example, Reqtify is qualified for avionics and railway.

Regarding previous empirical studies related to the state of the practice on impact analysis for safety-critical systems, a survey on safety evidence management [53], in which 52 practitioners participated, suggests that evidence change management is mainly performed manually. Surveys among the partners of industry-academia research projects [58, 64] have reported tools for the development and assurance of safety-critical systems that can be used for impact analysis and change management purposes (e.g., Reqtify and VectorCAST). Although their results are valuable, these surveys provide few insights into SECIA. The surveys studied safety evidence management in general, and not, for instance, the artefact types that more frequently trigger SECIA, the tool support for specific artefact types, and SECIA challenges. An interview study with engineers from four companies in four different application domains [60] reports component reuse as a common practice in system change. The study also reports the execution of safety analysis activities after requirements changes, and the need for allocating sufficient resources to handle change and for awareness of change impact on system safety.

Other authors have analysed information from past projects as a way to study impact analysis for safety-critical systems. Borg et al. [9] analysed over 10,000 impact analysis reports from a company in the power and automation domain. The authors identified the artefacts involved in source code impact analysis in the past, which include both pieces of source code and other artefact types (e.g., requirements, design, and test cases specifications). Case studies in automotive domain have indicated the advantages of adequate architecture structures for guiding impact analysis [18], challenges for change management in relation to tool support and to systematic procedures in testing practices [35], and the use of safety cases as an impact analysis tool in system changes and with respect to system safety [70]. In the medical domain, problems related to traceability (e.g., trace granularity not clearly defined and missing traces) have been reported [49], and past system failures and issues such as incomplete impact analysis and insufficient V&V after changes [74]. The importance of processes, methods, and tools for change management has been highlighted for the aerospace and nuclear domains [68].

Prior research has indicated the existence of other specific challenges and needs, such as the impact of component reuse and evolution on safety [16], determining if a component can be reused [26], safety re-assessments after a change [47], the vast amount of artefacts to trace and the need for safety assessors' confidence [56], the need for planning and documenting impact analysis [61], and the difficulty in ensuring system safety after a change [71].

3 Research Method

We used the survey approach and a web-based questionnaire because of the following main reasons: (1) it allows us to understand the views of many individuals that work in different companies or industries in an unified way; (2) it brings the potential of collecting a larger number of responses than for example in an interview study; (3) it supports data collection for many variables in a short time; (4) the data collection is unified and framed by survey questions which enables better focus, and; (5) a wide and heterogeneous sample can be reached, wider and more heterogeneous than if we only conducted interviews with known practitioners in our industry network.

The survey reported corresponds to qualitative (aka flexible) research [62]. This type of research is mainly targeted at investigating and understanding phenomena within their real context and at seeking new insights, ideas, and possible hypotheses for future research. The following subsections present the research questions, the survey design, instrument evaluation, data collection, data analysis, and threats to validity.

3.1 Research Questions

The goal of the survey was to gain insights into how industry deals with SECIA. This goal was decomposed into the following Research Questions (RQs).

RQ1: Under what circumstances is safety evidence change impact analysis addressed?

RQ1.1: How often do the circumstances occur?

The purpose of this RQ was to determine the situations during a system's lifecycle when SECIA is actually conducted, and their frequency. For example, system re-certification has been acknowledged as a situation in which evidence evolves and thus SECIA might be necessary [14]. However, the paper does not provide information about the frequency of this situation in industry. For better answering RQ1, the artefact types that trigger the analyses and the artefact types affected by changes were also studied. To our knowledge, no publication has studied a large range of the artefact types that can be involved in SECIA, or if some artefact types trigger it more often than others.

RQ2: What is the tool support for safety evidence change impact analysis?

The purpose of this RQ was to collect information about the current level of automation for SECIA and the tools currently used. Such tools also include those used for storing evidence of safety evidence change management. There is almost no knowledge about, for instance, tools for SECIA in relation to safety cases. We have found only ASCE in the literature [51], but without evidence of use for SECIA in practice.

RQ3: What challenges are faced when dealing with safety evidence change impact analysis?

RQ3.1: How often are the challenges faced?

The purpose of this RQ was to explore the current issues in industry regarding SECIA. Many different SECIA challenges have been acknowledged in the literature, but there has been no in-depth study yet on how often practitioners face them and how practitioners consider that state-of-practice SECIA could be improved.

3.2 Survey Design

We designed a structured cross-sectional web-based survey [38], aimed at obtaining information from the participants at a fixed point in time based on their past experience in dealing with SECIA. The questionnaire is presented in Appendix A.

The survey was targeted at practitioners that were or had been involved in SECIA. This included people who provided safety evidence (e.g., safety engineers or testers of a company that supplies components), people who checked safety evidence (e.g., an independent safety assessor), and people who requested safety evidence (e.g., a person that represents a certification authority).

The questionnaire was created with close reference to prior work:

- Questions 2-8 were an adaptation of background information [53]
- The situations presented in Question 9 were adopted from [14]
- Questions 9, 11, 13, and 20 adapted an existing Likert scale [65]. Such a scale is on frequency: Never, Few projects (i.e., rarely), Some projects (i.e., sometimes), Most of the projects (i.e., very often), Every project (i.e., always).
- The levels of automation in Question 15 were adapted from [59] (see Section 4.2.1)
- The artefact types presented in Questions 11, 13, 15, and 17, and their definitions, corresponded to a synthesis of a safety evidence taxonomy presented validated with practitioners [53, 55].
- All the challenges listed in Question 20 had been acknowledged in previous publications:
  - Difficulty in assessing system-level impact of component reuse [16]
  - Lack of a systematic process for performing impact analysis [19]
  - Long time for evaluating the consequences of a change [20]
  - Difficulty in deciding if a component can be reused [26]
  - Excessive detail of the traceability between artefacts, making traceability management more complex than necessary for impact analysis purposes [49]
  - Insufficient traceability between artefacts to accurately know the consequences of a change [49]
  - Too coarse granularity of the traceability between artefacts to accurately know the consequences of a change [49]
  - Difficulty in estimating the effort required to manage a change [54]
  - Unclear meaning of the traceability between artefacts in order to know how to manage a change [54]
  - Insufficient confidence by assessor or certifiers in having managed a change properly [56]
  - Vast number of artefacts to trace [56]
  - Insufficient tool support [63]
  - Difficulty in determining the effect of a change on system safety [71]

The final version of the questionnaire consisted of 23 questions and we expected that less than 20 minutes would be required to provide the answers. The pages and the options of the questions were presented in a randomized order when possible in order to mitigate threats to validity of the outcome, particularly errors and omissions due to respondents' fatigue. Definitions and clarifications were provided for those parts of the questionnaire in which misinterpretation was possible. For example, we provided examples of the artefact types used as safety evidence the first time they appear in one questionnaire page. Respondents were also given the possibility to mention other options in the questions.

3.3 Instrument Evaluation

A two-stage process was adopted to evaluate the survey instrument. First, we asked three domain experts (two senior software engineering researchers and one safety-critical system developer) to read the questionnaire and provide feedback on its readability, understandability, potential ambiguities, and length. The feedback led to the removal of four questions and to rewriting several. Second, we asked three practitioners (one safety assessor, one safety assurance manager, and one developer) to complete the revised version of the questionnaire and to provide feedback on the same points. This resulted in the removal of two questions and in minor clarifications of some questions.

3.4 Data Collection

Data collection started on November 21st of 2013 and finished on January 11th of 2014. We used the following sampling strategy:

- The survey was advertised on several LinkedIn groups related to safety-critical systems. Some groups were on specific application domains (e.g., aerospace, automotive, avionics, defence, medical, nuclear, oil and gas, and railway), some on specific safety standards (e.g., ARP4754, DO-178, DO-254, EN 50126, IEC 61508, IEC 62304, ISO 13849, and ISO 26262), and others on more general subjects (e.g., functional safety and safety engineering). The complete list of groups is as follows:
    - Ada Programming Language
    - AEROSPACE - Reliability & system Safety
    - American Society of Safety Engineers (ASSE)
    - ARP4754
    - Assurance Case
    - Automotive Electronics and Embedded Software
    - Automotive SPICE and Functional Safety
    - Automotive SPICE to Automotive Systems Engineering
    - Avionics Design
    - Board of Certified Safety Professionals
    - Defense & Aerospace
    - DO-254
    - DO-178B (and C too!)
    - DO-178B - Guidelines for Safety-Critical Software
    - DO-178B and DO-254 Programming Group
    - DO-178C - New Standard for Safety Critical Software
    - DO-178C For Avionics Engineers & Managers, from DO-178B
    - DO-254 Avionics Engineers & Managers Group
    - ERTMS group
    - exida
    - Functional Safety
    - IEC 61508 on Functional Safety
    - IEC 62061 and ISO 13849 machinery functional safety
    - IEC 62304
    - IEC The Electrotechnical Standards Group
    - IEEE Product Safety Engineering Society (PSES)
    - Indian Safety Critical Professional
    - Industrial Robotics
    - Inside Functional Safety
    - ISO 26262 Functional Safety
    - Medical Device Engineers Network
    - Medical Device Risk Management
    - Medical device software
    - Medical Device Software Life Cycle - Safety Critical - IEC 62304
    - Nuclear Safety
    - Oil and Gas HSE Practitioners
    - Open-DO

  - OPENCOSS
  - Public Safety Professionals
  - RAIL PROFESSIONALS
  - RailTech
  - Safety Case Workers
  - Safety Critical Developers Forum
  - Safety Integrity Levels (SIL)
  - Safety-Critical Systems Club
  - SIL3
  - Systems Safety Engineers
  - The New EN50126 Standard for Rail RAMS
  - The Safety and Risk Engineer
  - UK Nuclear Matters

  This step was intended to reach a large number of practitioners worldwide, and with different backgrounds. Two reminders were posted on each group. The benefits of using LinkedIn or other social networks have been discussed in the literature [2, 17, 34], and include the increase in subjects' heterogeneity, the increase in the level of confidence in the representativeness of a sample, and the possibility of reaching a population for which no centralized bodies of professionals exist.
- The survey was advertised on two mailing lists on safety-critical systems:
  - systemsafety@lists.techfak.uni-bielefeld.de
  - general-opencoss@listserver.tue.nl

  This was aimed at complementing the social network advertisement, since we could not predict how many practitioners would regularly check the updates on LinkedIn groups. One reminder was posted on each mailing list.
- Finally, we contacted practitioners that we personally knew and participants in a previous survey [53] that agreed upon being contacted for follow-up studies. In both cases, we also asked the practitioners to please forward the invitation to additional colleagues. We sent one reminder to the practitioners that we personally knew.

3.5 Data Analysis

We obtained 129 responses, and rejected 28 because the respondents only filled in the background information. The remaining 101 responses were examined to detect careless responses that should be rejected. Responses were considered careless if they fulfilled one of the following criteria:

a) The response did not provide relevant information (e.g., the respondent only indicated "I don't know" to all the questions answered);
b) The response contained clear and significant inconsistencies (e.g., between Questions 9 and 11; Appendix A), or;
c) The response displayed patterns for which we could not find a justification (e.g., selection of "always" for all the options of the questions about the frequency of some phenomenon).

Identification of careless responses was performed incrementally: the first author conducted an initial filtering; then, he discussed it with the last author, resulting in a reduced set of potentially careless responses; finally, the second and the third authors checked this set. The final number of valid responses was 97 (75.2% of all responses), including incomplete but non-careless responses, as long as they provided answers to some RQs.

After the sanity check and outliers removal, we unified the answers to Questions 1-5, 17, and 19 so that they had the same, homogeneous format. For example, DO-178 was referred to in different ways in Question 3 (e.g., DO178, DO 178, DO-178B, and DO-178C). We also coded the answers to Question 6, which indicated the respondents' overall roles, in a two-step process:

- First, all the answers were harmonized and interpreted, resulting in these roles:
  1. Certifier (e.g., for 'review and approval of safety evidence' at a certification authority)
  2. Hardware engineer (e.g., for 'hardware consultant')
  3. Reliability, availability, maintainability, and safety engineer, which is a typical role in railway, among other application domains.
  4. Safety engineer (e.g., for 'system safety engineer')
  5. Software developer
  6. Software engineer (e.g., for 'software designer and architect')
  7. Systems engineer (e.g., for 'design')
  8. System developer (e.g., for 'developer')
  9. V&V engineer (e.g., for 'testing of systems')

10. Certification manager (e.g., for 'software certification and airworthiness expert')
11. Change manager
12. Project leader (e.g., for 'team lead')
13. Product manager (e.g., for 'section manager for hardware development')
14. Quality assurance manager (e.g., for 'project quality assurance')
15. Safety manager (e.g., for 'define new methods for efficient safety analysis')
16. Safety assessor (e.g., for 'safety consultant')
17. Researcher (e.g., for 'scientist')

In this step, we also checked the type of organization of the respondents as a way to better understand and thus code their role.

- Second, we synthesised the roles above into five overall roles:
  - Certifier (role 1 in the first step)
  - Engineer (roles 2-9 in the first step)
  - Manager (roles 10-15 in the first step)
  - Safety assessor (role 16 in the first step)
  - Researcher (role 17 in the first step)

We assigned two overall roles to five respondents, and none to one. This respondent did not clearly indicate the role. Finally, we coded the answers to Question 22 for classifying the improvement areas indicated. Details about the codes are provided in Section 4.3.

The first author, as the most knowledgeable in safety assurance and certification, conducted the initial unification and coding. The third author validated the outcome from unifying the answers to Questions 1-5, 17, and 19, and from coding the answers to Question 6. Regarding the coding to the answers to Question 22, the second author also coded the answers, with the codes defined by the first author. They then discussed the answers to which different codes had been assigned and the possibility of adjusting the codes and their definitions. The codes and their definitions were refined, and then the first author revised the answer coding. The second author reviewed the outcome, both authors discussed the revision, and they finally agreed upon the final coding.

In the last step of data analysis, we calculated Spearman rank-order correlation coefficients [25] for the questions whose answers were provided according to an ordinal scale (Q7, 8, 9, 11, 13, 15, and 20).

3.6 Threats to Validity

We discuss general threats to validity according to the four perspectives presented by Wohlin et al. [76]. Threats related to specific answers and interpretations are discussed in Section 4, which also presents the respondents' demographics.

Construct validity: This type of validity is concerned with the relationship between a theory behind an investigation and its observation. We guaranteed confidentiality and anonymity of the responses and allowed the respondents to complete the survey without identifying themselves in order to mitigate potential threats on evaluation apprehension. The threat of providing incomplete option lists was mitigated by allowing the respondents to specify additional information. Obtaining data from a set of respondents with different backgrounds mitigated mono-operation bias.

Internal validity: This type of validity deals with the relationship between a treatment and its results. We provided an introduction to the survey in order to make the respondent familiar with the context of the study and its purpose. We also provided the respondents with information about the intent of the questions and definitions of the terminology used when ambiguity could exist. Instrument evaluation also allowed us to mitigate ambiguity and misinterpretation. The order of presentation for the different parts of the questionnaire and for the options to individual questions was randomized when applicable. This design decision mitigated the threats to omission of questions due to fatigue. The adoption and adaptation of well-established Likert scales minimized threats related to the elicitation of expert opinions. Designing the survey instrument so that it could be completed in approximately 20 minutes helped to mitigate maturation and mortality.

Conclusion validity: This type of validity is concerned with the causal relationship between a treatment and its outcome. Overall, the large and heterogeneous sample of the survey, in which most respondents can be regarded as senior practitioners, contributes to conclusion validity. As suggested by Kitchenham et al. [37], we focused on the analysis of strong (corr. > 0.59) and very strong (corr. > 0.74) correlations for confirming the importance for practice of the relationships between phenomena. The p-values of these correlations are also below 1e-08. We use the lack of strong or very strong correlations and the existence of weak or very weak ones (corr. < 0.3) for indicating that the relevance in practice of some relationships cannot be guaranteed. Finally, more than one author participated in answer unification and coding, which also contributes to conclusion validity.

External validity: This validity is concerned with the generalization of the conclusions of an investigation. The study was aimed at characterizing and understanding the state of practice on SECIA. It also corresponds to qualitative research, thus it is not strictly meant to generalize its conclusion beyond its context. Nonetheless, we are confident that the results are a good representation of the state of the practice. First, it is not common that a survey on a narrow topic in systems and software engineering has so many responses. Second, the population of the area addressed (SECIA) is for sure not very large due to the specific types of systems (safety-critical systems) and activity (impact analysis) targeted. The sample is also very heterogeneous, more than in other related surveys (e.g., [58]) regarding the number of countries, domains, and safety standards represented. Although the number of respondents from Sweden (17) can be considered high, we think that this has a minor impact on our conclusions. Overall, the rest of the background information is similar to [53], and we think that it reflects industry characteristics. For example, respondents' demographics are in line the characteristics of LinkedIn groups. The domain-specific group in which the survey was advertised with the highest number of members was on aerospace, and the standard-specific group was on DO-178. We assume that there exists a correlation between the number of members of LinkedIn groups on a specific area and the number of practitioners in that area.

4 Results and Interpretation

This section reports on the results of the survey by presenting the answers to each RQ (Sections 4.1 to 4.3). In each table below, the cells with bold text indicate the mode of each option, whereas the shaded cells highlight the option most frequently indicated for each possible answer. In both the tables and the figures, we show the frequency of the phenomena by means of percentages (ratio of respondents indicating a phenomenon) and data points (in brackets). We also explain how we interpret the results, discussing their possible implications in research and practice, and compare the results with related work. Section 4.4 presents a summary of the results.

Figure 1 shows the respondents' demographics in relation to their background in SECIA. Most of the respondents did not find the survey via a personal invitation. Among the 16 application domains represented in the survey, the domain with the highest number of responses was aerospace, followed by automotive, railway, and avionics. The respondents mentioned 47 individual safety standards, with DO-178, IEC61508, and ISO26262 as the standards mentioned by the highest number of respondents. Out of the 97 respondents, 34 reported more than one individual safety standard. More information about the standards is provided in Appendix B. The respondents had worked upon SECIA in 28 individual countries in total, and 26 respondents specified more than one individual country. USA was the country indicated in the highest number of respondents, followed by UK, Sweden, Germany, and France. Most of the companies for which the respondents worked corresponded to developer/manufacturer of final systems, and most of the respondents were engineers, had 5 or more years of experience in SECIA, or had been involved in 5 or more projects.

4.1 RQ1. Under what circumstances is safety evidence change impact analysis addressed?

Out of the 97 respondents, 84 provided information for answering RQ1 (Questions 9-14 in Appendix A). The next subsections present the aspects studied for this RQ. An overall conclusion is that SECIA usually affects several artefact types.

4.1.1 Situations frequency

Table 1 shows how often the respondents had been involved in SECIA in various situations. *Modification of a new system during its development* has the highest median, followed by *Modification of a new system as a result of its V&V*, *Reuse of existing components in a new system*, and *Re-certification of an existing system after some modification*. *Modification of a new system during its development* is also the situation most frequently indicated as happening in every project, and the least frequently indicated as never happening. Table 1 shows that SECIA is an activity that most respondents had dealt with frequently in a wide variety of situations.

The only strong correlation found between the situations is for *Modification of a new system during its development* and *Modification of a new system as a result of its V&V* (corr. = 0.6). This strong correlation makes sense to us, and suggests that the more often changes and SECIA happen during safety-critical system development, the more likely are changes and SECIA during V&V. No strong correlation has been found between the situations and other questions. Therefore, we cannot claim that the frequency of SECIA from certain artefact types greatly depends on the situation in which a SECIA is performed, or that certain challenges happen more often in some situations.

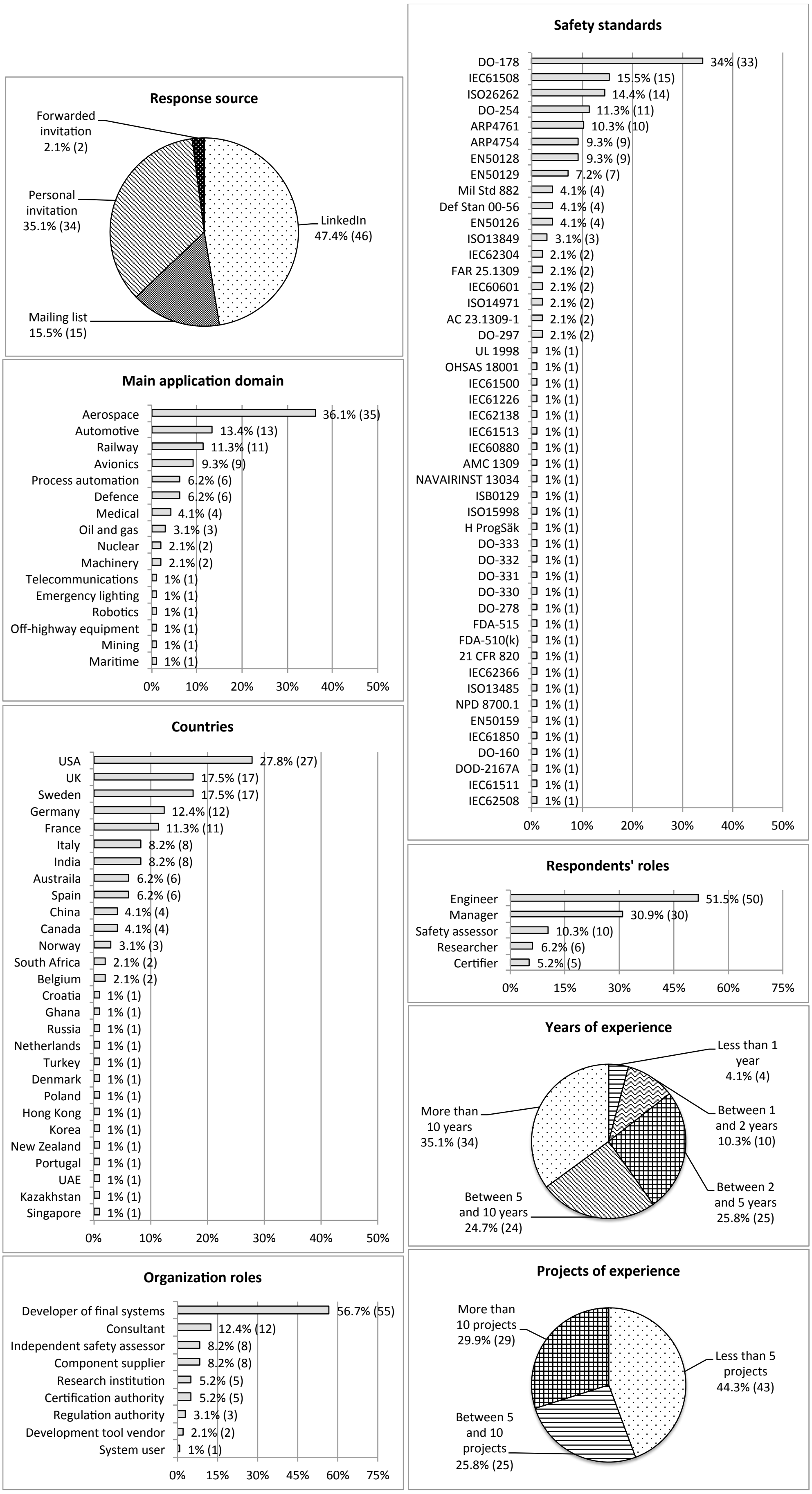


Figure 1. Respondents' demographics

Although they are the two situations with the lowest medians, we find the ratio of respondents that reported to have been involved in SECIA for *Re-certification of an existing system for a different standard* (50%) and *Re-certification of an existing system for a different application domain* (40.5%) particularly interesting (see Table 1). We regard the ratios as higher than expected, and consider that the results show that re-certification in these situations happen more often than most people think. Our pre-understanding is based on discussions among different practitioners and researchers. Given the difficulty in effectively and efficiently managing re-certification in these situations, research efforts targeted at them are necessary. They can have an important impact, and the amount of publications dealing with safety assurance and certification for different standards and domains is very small [55]. The need for re-certification (and thus for SECIA) and the associated effort and cost are also among the main demotivating factors for system modifications [14].

When asked about further situations in which they had been involved in SECIA, individual respondents reported:

a) Changes in system criticality
b) Independent assessment of the risk management process
c) Hazards identified after the fact
d) Re-certification for temporary works
e) Accidents
f) System of system reuse

Most of this additional information only provides further details about the situations listed in the questionnaire. For example, (d) is a concrete example of re-certification for a different operational context. Nonetheless, some answers represent situations whose SECIA practices might need further investigation. We think that it would be particularly interesting to study SECIA practices for (e) and (f). Our hypothesis is that SECIA after an accident might be performed more thoroughly than in other situations, as no one wants to be blamed for a second accident. SECIA for systems of systems also seems like a situation in which general, past practices might not be effective and efficient. The size and complexity of these systems very likely give raise to new challenges for SECIA, or make other challenges more difficult to address.

4.1.2 Frequency of impact analysis from artefact types

Table 2 shows how often the respondents had performed a SECIA as a consequence of changes in different artefact types. The 'N' column indicates the number of respondents that provided an answer different to 'I don't know'. The median of six out of the 14 artefact types (*Design Specifications, Requirements Specifications*, *Safety Analysis Results*, *Source Code*, *Test Case Specifications*, and *Traceability Specifications*) is 'most projects', and the mode for all these artefact types is 'every project'. *Requirements Specifications* is also the artefact type most commonly reported as triggering a SECIA in every project. In contrast, *Personnel Competence Specifications* has the lowest median. The artefact types for which the highest ratio of respondents had performed SECIA because of changes to them (i.e., artefact with the highest ratio of answers different to 'never') are *Requirements Specifications* (96.2%) and *Safety Analysis Results* (96.1%).

The results are in line with related work. For example, requirements changes and thus impact analysis from them are commonly acknowledged as happening very often [20] and have been studied in many publications. However, we consider that the results indicate an important gap in prior research: *Safety Analysis Results* seem to trigger SECIA in most projects, but their evolutionary nature and means for impact analysis from them have been barely studied.

Table 3 shows 17 strong correlations and four very strong correlations (in bold) between the artefact types triggering SECIA. Only *Personnel Competence Specifications* does not have any strong or very strong correlation with another artefact type. The way we interpret these correlations is that if SECIA is performed from one of the artefact types (e.g., *Requirements Specifications*), then it is very likely that SECIA has to be performed from the other artefact type (e.g., *Design Specifications*). These correlations provide evidence that efforts on aligning and studying the relationships between these artefact types are worthwhile for safety-critical system development. Some relationships have barely been studied so far (e.g., between *Test Case Specifications* and *Safety Cases*). Approaches for analysing past impact analysis reports (e.g., [9]) can facilitate the analysis of these relationships and provide further insights into them.

Interestingly, there is a very strong correlation between *Requirements Specifications* and *Source Code*, which in our opinion shows that requirements change once source code has already been implemented. This could happen at late system development stages of a project or when a new version of a system is developed, among other scenarios. The very strong correlation between *Assumptions and Operation*

Conditions Specifications and *Safety Analysis Results* shows the importance of the former artefact type for creating the latter. The same applies to the very strong correlation between *Requirements Specifications* and *Design Specifications*. It is also very interesting that no strong correlations have been found for some pairs of artefact types commonly studied together in the literature, such as *Requirements Specifications* and *Architecture Specifications*. Our interpretation is that most architecture changes resulting from requirements changes do not trigger SECIA.

When asked if there were further artefact types from which SECIA was performed, the respondents provided the following additional information:

a) COTS (Commercial Off-The-Self) components information regarding their impact on safety
b) Critical component maintenance information for security assurance
c) Project methodology and regulation authority documentation
d) Trace evaluation of safety impacts
e) Compliance plans
f) Means for verification
g) System capabilities specifications

We think that this additional information shows two characteristics of the current state of practice. Firstly, there is a growing interest in the relation and dependence between safety and security (b). Secondly, changes in safety standards and how to address SECIA from them is an important concern (c), including changes in the way to comply with the standards (e and f) and in the evaluations and assessments (a and d).

4.1.3 Frequency of change impact on artefact types

Table 4 shows how often the artefact types had been affected by changes to the body of safety evidence. Column 'N' indicates the number of respondents that provided an answer different to 'I don't know'. *Manual V&V results* obtained the highest median, whereas *Requirements Specifications* were reported as being affected in every project by the highest ratio of respondents. *Personnel Competence Specifications*, *Reused Components Information*, *System Lifecycle Plans*, and *Tool-Supported V&V Results* are the artefact types with the lowest medians, with *Personnel Competence Specifications* again as the artefact type with the highest ratio of respondents answering 'never'. The two artefact types for which the highest ratio of respondents indicated that they had been affected by changes are *Design Specifications* (98.7%) and *Source Code* (97.3%). More than 90% of respondents indicated change impact also in *Test Case Specifications*, *Manual V&V Results*, *Safety Analysis Results*, *Requirements Specifications*, and *Safety Cases*.

These results, in combination with those in Table 2, indicate that *Requirements Specifications* probably have the most important role in SECIA, whereas *Personnel Competence Specifications* probably have the least important one. A possible explanation for the latter can be that personnel's competence rarely changes during a system's lifecycle because of the stringent requirements and constraints from safety standards on the involved people's experience and education. Another reason could be that *Personnel Competence Specifications* barely depend on other artefact types, and vice-versa. Nonetheless, we show below that some strong correlations with *Personnel Competence Specifications* have been found.

Table 5 shows the 25 strong correlations and the very strong correlation (in bold) that we have found between artefacts types as affected by changes and artefact types triggering SECIA. These correlations show the existence of many, important relationships between the artefacts used as safety evidence for change-impact analysis sequences. Each artefact type has at least one strong correlation with another. We have found a strong or very strong correlation between the pieces of nine out of 14 artefact types. We interpret the very strong correlation in Table 5 between pieces of *Source Code* as a clear indicator of ripple effects on safety-critical source code. Regarding correlations between artefact types that were reported as affected by changes, Table 6 shows 27 strong correlations and one very strong correlation (in bold). Only *Personnel Competence Specifications* and *Tool-Supported V&V Results* do not have any correlation in Table 6. The very strong correlation between *Requirements Specifications* and *Design Specifications* in Table 6 suggests that these artefact types jointly evolve usually.

When asked to indicate further artefact types affected by changes to the body of safety evidence, individual respondents provided the following additional information:

a) Communications and security information
b) Hardware specifications
c) Simulation results
d) Compliance plans

As for the artefact types that trigger SECIAs, this additional information explicitly shows the importance of the relation and dependence between safety and security (a).

Table 1. Frequency of situations for SECIA

	N	Never	Few projects	Some projects	Most projects	Every project	*Median*
Modification of a new system during its development	84	7.1% (6)	13.1% (11)	28.6% (24)	**31% (26)**	20.2% (17)	*Most projects*
Modification of a new system as a result of its V&V	84	13.1% (11)	21.4% (18)	**25% (21)**	**25% (21)**	15.5% (13)	*Some projects*
Re-certification of an existing system after some modification	84	23.8% (20)	15.5% (13)	17.9% (15)	**34.5% (29)**	8.3% (7)	*Some projects*
Reuse of existing components in a new system	84	13.1% (11)	19% (16)	**33.3% (28)**	28.6% (24)	6% (5)	*Some projects*
Modification of a system during its maintenance	84	23.8% (20)	**29.8% (25)**	23.8% (20)	17.9 (15)	4.7% (4)	*Few projects*
New safety-related request from an assessor or a certification authority	84	26.2% (22)	**35.7% (30)**	25% (21)	10.7% (9)	2.4% (2)	*Few projects*
Re-certification of an existing system for a different operational context	84	**40.5% (34)**	23.8% (20)	21.4% (18)	11.9% (10)	2.4% (2)	*Few projects*
Re-certification of an existing system for a different standard	84	**50% (42)**	20.2% (17)	17.9% (15)	10.7% (9)	1.2% (1)	*Never - Few projects*
Re-certification of an existing system for a different application domain	84	**59.5% (50)**	13.1% (11)	15.5% (13)	10.7% (9)	1.2% (1)	*Never*

Table 2. SECIA frequency as a consequence of changes in artefact types

	N	Never	Few projects	Some projects	Most projects	Every project	*Median*
Requirements Specifications	78	3.8% (3)	9% (7)	25.6% (20)	23.1% (18)	**38.5% (30)**	*Most projects*
Source Code	74	13.5% (10)	16.2% (12)	16.2% (12)	20.3% (15)	**33.8% (25)**	*Most projects*
Test Case Specifications	77	9.1% (7)	16.9% (13)	22.1% (17)	20.8% (16)	**31.1% (24)**	*Most projects*
Traceability Specifications	78	10.3% (8)	21.8% (17)	12.8% (10)	24.3% (19)	**30.8% (24)**	*Most projects*
Design Specifications	76	7.9% (6)	13.1% (10)	25% (19)	23.7% (18)	**30.3% (23)**	*Most projects*
Safety Analysis Results	76	3.9% (3)	22.4% (17)	19.7% (15)	26.3% (20)	**27.7% (21)**	*Most projects*
Manual V&V Results	76	9.2% (7)	23.7% (18)	**26.3% (20)**	14.5% (11)	**26.3% (20)**	*Some projects*
Safety Cases	77	10.4% (8)	22.1% (17)	**27.2% (21)**	14.3% (11)	26% (20)	*Some projects*
Assumptions and Operation Conditions Specs.	73	11% (8)	20.5% (15)	**32.9% (24)**	16.4% (12)	19.2% (14)	*Some projects*
Tool-Supported V&V Results	76	18.4% (14)	22.4% (17)	**25% (19)**	13.2% (10)	21% (16)	*Some projects*
Architecture Specifications	71	**22.6% (16)**	21.1% (15)	18.3% (13)	19.7% (14)	18.3% (13)	*Some projects*
System Lifecycle Plans	76	23.7% (18)	**25% (19)**	18.4% (14)	15.8% (12)	17.1% (13)	*Some projects*
Reused Components Information	72	20.8% (15)	**29.5% (21)**	16.7% (12)	18% (13)	15.3% (11)	*Few projects - Some projects*
Personnel Competence Specifications	70	**40% (28)**	24.3% (17)	14.3% (10)	8.6% (6)	12.8% (9)	*Few projects*

Table 3. Strong and very strong correlations between artefact types as SECIA triggers

	Safety Cases	**Source Code**	**Manual V&V Res.**	**Tool V&V Results**	**Test Case Specs.**	**Traceability Specs.**	**Design Specs.**	**Arch. Specs.**	**Reqs. Specs.**	**Assu&Oper Con. Specs**	**Safety A. Results**	**Personnel C. Specs.**	**Reused C. Info.**
System LC. Plans				0.64									0.65
Reused C. Info.	0.6							0.61					
Personnel C. Specs.													
Safety A. Results	0.6									**0.75**			
Assu&Oper Con. Specs	0.61								0.6				
Reqs. Specs.		**0.82**			0.71	0.7	**0.78**						
Arch. Specs.							0.64						
Design Specs.		0.71			0.61	0.72							
Traceability Specs		0.68			0.7								
Test Case Specs.	0.6	**0.75**	0.63										
Tool V&V Results													
Manual V&V Res.													
Source Code													

Table 4. Change impact frequency on artefact types

	N	Never	Few projects	Some projects	Most projects	Every project	*Median*
Manual V&V Results	74	4.1% (3)	18.9% (14)	25.7% (19)	24.3% (18)	**27% (20)**	*Most projects*
Test Case Specifications	77	3.9% (3)	15.6% (12)	**31.1% (24)**	27.3% (21)	22.1% (17)	*Some projects*
Source Code	74	2.7% (2)	14.9% (11)	**33.8% (25)**	21.6% (16)	27% (20)	*Some projects*
Safety Cases	73	6.9% (5)	21.9% (16)	23.3% (17)	21.9% (16)	**26% (19)**	*Some projects*
Requirements Specifications	76	5.3% (4)	18.4% (14)	**31.6% (24)**	15.8% (12)	28.9% (22)	*Some projects*
Safety Analysis Results	73	4.1% (3)	23.3% (17)	**30.1% (22)**	17.8% (13)	24.7% (18)	*Some projects*
Design Specifications	76	1.3% (1)	25% (19)	**32.9% (25)**	17.1% (13)	23.7% (18)	*Some projects*
Traceability Specifications	74	10.8% (8)	24.3% (18)	**25.7% (19)**	14.9% (11)	24.3% (18)	*Some projects*
Architecture Specifications	75	10.7% (8)	25.3% (19)	**37.3% (28)**	10.7% (8)	16% (12)	*Some projects*
Assumptions and Operation Conditions Specs.	71	14.1% (10)	**29.6% (21)**	26.7% (19)	12.7% (9)	16.9% (12)	*Some projects*
Tool-Supported V&V Results	73	13.7% (10)	**37% (27)**	17.8% (13)	13.7% (10)	17.8% (13)	*Few projects*
System Lifecycle Plans	75	22.7% (17)	**29.3% (22)**	22.7% (17)	10.7% (8)	14.6% (11)	*Few projects*
Reused Components Information	70	21.4% (15)	**31.4% (22)**	25.7% (18)	11.5% (8)	10% (7)	*Few projects*
Personnel Competence Specifications	68	**39.7% (27)**	30.9% (21)	16.2% (11)	7.3% (5)	5.9% (4)	*Few projects*

Table 5. Strong and very strong correlations between artefact types as impacted by changes (left column) and artefact types as SECIA triggers (top row)

	System LC. Plans	**Reused C. Info.**	**Personnel C. Specs.**	**Safety A. Results**	**Assu&Oper Con. Specs**	**Reqs. Specs.**	**Arch. Specs.**	**Design Specs.**	**Traceability Specs.**	**Test Case Specs.**	**Tool V&V Results**	**Manual V&V Res.**	**Source Code**	**Safety Cases**
System LC. Plans	0.64		0.67											
Reused C. Info.		0.63	0.7											
Personnel C. Specs.			0.67											0.61
Safety A. Results				0.61	0.62	0.6								
Assu&Oper Con. Specs					0.68									
Reqs. Specs.						0.66							0.67	
Arch. Specs.				0.62										
Design Specs.						0.63							0.67	
Traceability Specs.									0.67				0.64	
Test Case Specs.						0.66		0.6					0.66	
Tool V&V Results											0.64			
Manual V&V Res.									0.63	0.65			0.72	
Source Code						0.64							**0.76**	
Safety Cases														

Table 6. Strong and very strong correlations between artefact types as impacted by changes

	Safety Cases	**Source Code**	**Manual V&V Res.**	**Tool V&V Results**	**Test Case Specs.**	**Traceability Specs.**	**Design Specs.**	**Arch. Specs.**	**Reqs. Specs.**	**Assu&Oper Con. Specs**	**Safety A. Results**	**Personnel C. Specs.**	**Reused C. Info.**
System LC. Plans							0.67			0.6			
Reused C. Info.								0.66		0.69			
Personnel C. Specs.													
Safety A. Results	0.74								0.62	0.62			
Assu&Oper Con. Specs	0.61						0.62	0.64	0.68				
Reqs. Specs.	0.61	0.69			0.71	0.68	**0.78**	0.68					
Arch. Specs.							0.72						
Design Specs.		0.74	0.64		0.67	0.71							
Traceability Specs		0.69	0.73		0.65								
Test Case Specs.		0.7	0.68										
Tool V&V Results													
Manual V&V Res.		0.69											
Source Code													

4.1.4 Synthesis of correlations between artefact types

We interpret the strong and very strong correlations between artefact types as the evidence of their joint involvement in SECIA. More importantly, the correlations indicate relationships whose documentation and maintenance is arguably of utmost importance. The relationships show the artefact types that will very likely be involved in SECIA when other types are involved, thus the former artefact types must be analysed to ensure that SECIA has been properly addressed. This kind of information can help practitioners know the artefact types to consider for SECIA, and it is not provided in detail in safety standards. Standards typically only state that impact analysis might be necessary as a result of system or software changes and maintenance, and that re-assessment needs after a change must be determined.

When comparing the correlations shown in Tables 3, 5, and 6, the tables have nine pairs of correlated artefact types in common:

1. *Requirements Specifications* and *Source Code*
2. *Requirements Specifications* and *Design Specifications*
3. *Requirements Specifications* and *Test Case Specifications*
4. *Test Case Specifications* and *Source Code*
5. *Design Specifications* and *Source Code*
6. *Traceability Specifications* and *Source Code*
7. *Test Case Specifications* and *Manual V&V Results*
8. *Design Specifications* and *Test Case Specifications*
9. *Safety Analysis Results* and *Assumptions and Operation Conditions Specifications*

These pairs can be regarded as the most relevant ones for SECIA in practice. It is important to note that prior research has studied most of them. Nonetheless, publications on SECIA and traceability related to *Manual V&V Results* are scarce [55], and some pairs (5-9) have been considerably less studied than others (1-4). Figure 2 summarises and synthesises all the correlations found by means of a graph.

One result subject to interpretation is change impact on *Safety Cases*. A safety case corresponds to a collection of references to other artefacts to justify system safety and compliance. Therefore, changes in the artefacts referred to affect safety and compliance justification. Using the medians as basis, *Safety Cases* seem to be less often affected by changes ('some projects', Table 4) than the frequency with which SECIA is performed as a consequence of changes in other six artefact types ('most projects'; Table 2). In addition, *Safety Cases* have no strong or very strong correlation as artefact type affected by changes when SECIA is performed from other artefact types (Table 5). These results suggest that not all the possible change impacts on *Safety Cases* lead to actual changes in this artefact type. We find three possible explanations. First, changes in other artefact types might be usually made before they are referred to in a safety case. Second, although some artefacts are referred to in a safety case, their changes might not impact the safety case. Third, industry might not be adequately addressing how changes in the body of safety evidence impact a safety case. Indeed, the results raise some concerns on how safety case evolution is managed.

It is acknowledged as a good practice to create safety cases incrementally and iteratively [36], as instances of other artefact types are created and maintained. In fact, this is explicitly recommended in some safety standards (e.g., Defence Standard 00-56). Consequently, it could be expected that the median for *Safety Cases* in Table 4 was higher than 'some projects', and that *Safety Cases* had strong or very strong correlations with more artefact types (e.g., *Architecture Specifications*, in line with [5]). More surprisingly, and despite the fact that 'every project' was the mode for *Safety Cases*, the ratio of respondents that indicated that *Safety Cases* had been never affected by changes in the body of evidence or in few projects account for 28.8%. Given the importance of safety cases, we consider that how they are affected by changes in other artefact types, and how their evolution is managed, are two areas that require further research. Safety case creation at late system development phases can lead to deficiencies such as confirmation bias and thus decrease their credibility. Many experts have discussed the adequacy of and need for safety case regimes for critical systems, arguing according to their own insights or single case studies (e.g., [43]). Our study is the first that empirically shows that many practitioners might not be adequately managing safety cases, at least from a SECIA perspective.

As an overall conclusion, we think that new research efforts on impact analysis for safety-critical systems are necessary. Different artefact types can be used as evidence, and some of those that most frequently trigger SECIA have received little attention in relation to how their changes should be handled. More specifically, we believe that further research on impact analysis regarding safety-targeted artefact types is essential, especially for those with over half a dozen of strong or very strong correlations. These artefact types are *Safety Analysis Results*, *Assumptions and Operation Conditions Specifications*, *Manual V&V Results*, and *Safety Cases*, whose adequate change management and impact analysis involving them are essential for ensuring safety. This can be especially important for software-intensive systems, as it has been acknowledged that many practitioners fail to understand and identify software safety risks (e.g., [43]), including software change impact on system safety.

Finally, an open question is why only one strong correlation has been found for *Tool-Supported V&V Results*, and with *System Lifecycle Plans*. Someone could expect not so fewer strong or very strong correlations than *Manual V&V Results*, and a higher correlation with *Test Cases Specifications* or *Source Code*. Changes in these artefacts might impact, for instance, existing testing results. The results suggest that *Test Cases Specifications* and *Source Code* most commonly change before *Tool-Supported V&V Results* are available.

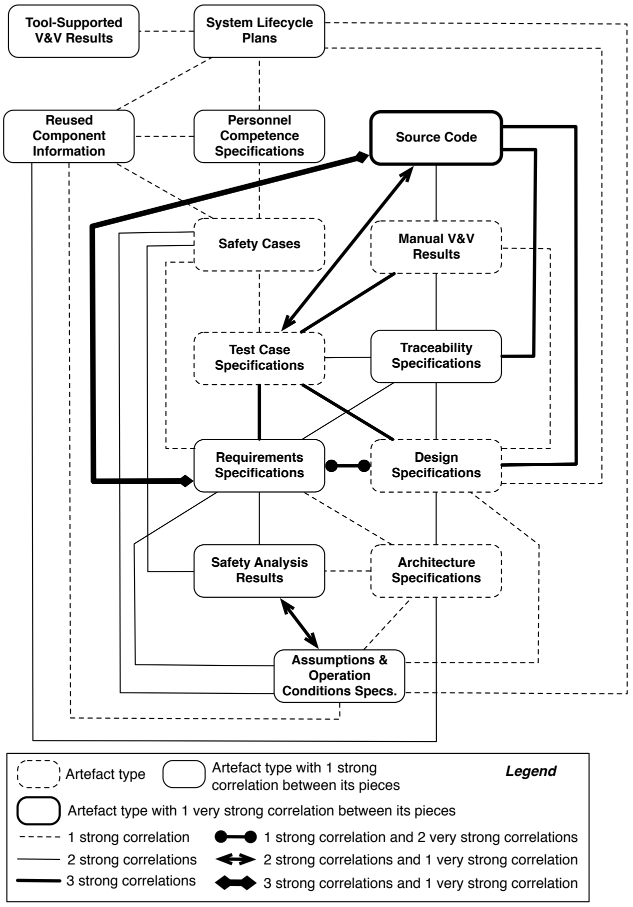

Tool-Supported V&V Results
System Lifecycle Plans
Reused Component Information
Personnel Competence Specifications
Source Code
Safety Cases
Manual V&V Results
Test Case Specifications
Traceability Specifications
Requirements Specifications
Design Specifications
Safety Analysis Results
Architecture Specifications
Assumptions & Operation Conditions Specs.
Artefact type
Artefact type with 1 strong correlation between its pieces
Legend
Artefact type with 1 very strong correlation between its pieces
1 strong correlation
2 strong correlations
3 strong correlations
1 strong correlation and 2 very strong correlations
2 strong correlations and 1 very strong correlation
3 strong correlations and 1 very strong correlation

Figure 2. Artefact types correlations graph

4.2 RQ2. What is the tool support for safety evidence change impact analysis?

Out of the 97 respondents, 84 provided information for answering RQ2 (Questions 15-19 in Appendix A). The next subsections present the aspects studied for this RQ. An overall conclusion is that tool support is used in industry for all artefact types, but there seem to be many improvement opportunities.

4.2.1 Level of automation in safety evidence change impact analysis

Table 7 shows the level of automation offered by the tool support used for SECIA when the artefact types change, according to the respondents. The 'N' column indicates the number of respondents that provided an answer different to 'I don't know'. The levels of SECIA automation were defined, based on a previous study on human interaction with automation [59], as follows:

- Fully manual: no automation in the process; e.g., impact determined by reading documentation and asking colleagues.
- Decision support available: limited support for narrowing down a selection of possible impact; e.g., search tool used to seek impact, repositories easy to browse thanks to information structure.
- Semi-automated recommendations: tools suggest artefacts that might be impacted but humans must confirm.
- Highly automated recommendations: tools report impact and humans have the authority to veto the suggestions.
- Automatic impact analysis: tools determine the impact without human involvement.

The level of automation was reported as 'automatic impact analysis' by at least one respondent for 10 out of the 14 artefact types, with *Traceability Specifications* as the artefact type whose level of automation was most frequently reported as automatic. Nonetheless, we think that the overall, average level of SECIA automation is low. Except for *Source Code*, the median for all artefact types is 'decision support available' or 'fully manual'. In addition, the mode of only *Architecture Specifications*, *Traceability Specifications*, and *Source Code* is different from 'fully manual'. In other words, SECIA from the rest of artefact types seems to be most often performed manually. This can lead to mistakes and issues with detecting safety and compliance risks.

SECIA from *Requirements Specifications* was reported as 'fully manual' by 40% of the respondents, despite the existence of many requirements management tools that provide some automated support [13, 28]. One could also have expected a higher median and lower ratio of 'fully manual' answers for *Tool-Supported V&V Results*. It could be argued that *Source Code* is the artefact type with the highest median because it is usually created in development environments. An alternative is code automatically generated. But even in this case, it remains surprising that 31.5% of the respondents indicated that the level of automation for *Source Code* was 'fully manual'.

We think that the level of automation for *Assumptions and Operation Conditions Specifications* can raise some concerns. It is not only the artefact type whose level of automation has been most frequently reported as 'fully manual', but also an artefact type whose inadequate change management led to, for instance, the well-known accident of Ariane 5 in 1996 [43]. In addition, most of the respondents had dealt with SECIA from *Assumptions and Operation Conditions Specifications* (Table 2) and with *Re-certification of an existing system for a different operational context* (Table 1). To some extent, this result suggests that prevention measures for avoiding past accidents can be improved. Furthermore, *Assumptions and Operation Conditions Specifications* are essential for any critical system, as they can only be deemed safe for a given operational context.

We have found strong correlations between the levels of automation for *Design Specifications* and *Traceability Specifications* (corr. = 0.62), *Traceability Specifications* and *Tool-Supported V&V Results* (corr. = 0.61), and *Source Code* and *Safety Cases* (corr. = 0.67). These correlations make us think of the use of tool support that can automate SECIA actions from both artefact types of these pairs, probably DOORS or some internal tool according to the results in Section 4.2.2. This hypothesis should be further investigated. Regarding the answers to the questions related to RQ1, we have not found any strong or very strong correlation with the level of SECIA automation. We consider that this implies that the level does not vary much between the circumstances studied.

When asked to add any further artefact types and the level of automation for performing SECIA when they changed, individual respondents indicated:

- Test cases to be executed on the release build at the end of project (automatic impact analysis)
- Component impact indication (automatic impact analysis)

Respondents further emphasised that:

a) The level of automation is increasing;
b) SECIA qualified tools are important and necessary;
c) Although tools are used, change impact is always assessed manually;
d) Some compare tools can be used to check differences between two versions of documents or models, but they are seldom used for models, and;
e) More advanced tools, whose results can directly be used as safety evidence, are necessary for evidence (document) review.

This additional information indicates that some practitioners regard the level of automation as increasing, but they still expect improvements. The information in (b), (c), and (e) relate to SECIA qualified tools. The use of these tools would imply that manual assessment would not be necessary in (c), and that certification authorities would accept (e).

The results outlined in Table 7 are consistent with related work. Research very often focuses on impact analysis for *Source Code*. In our opinion, this leads to a higher number of automated impact analysis proposals and thus more possible automated solutions for practice. Previous work (e.g., [23, 53, 63, 69]) has also suggested that the level of SECIA automation is low. We have further refined this general insight by providing evidence of the level of automation for each artefact type used as safety evidence and from a larger sample. Finally, there seems to be a research gap in impact analysis automation for *Assumptions and Operation Conditions Specifications*, *Manual V&V Results*, *Personnel Competence Specifications*, *Reused Components Information*, *Safety Cases*, and *System Lifecycle Plans*.

Table 7. Level of automation offered by tools for SECIA from each artefact type

	N	Fully Manual	Decision Support Available	Semi-Automated Recommendations	Highly-Automated Recommendations	Automatic Impact Analysis	***Median***
Source Code	73	**31.5% (23)**	16.4% (12)	**31.5% (23)**	17.8% (13)	2.8% (2)	*Semi-Automated Recommendations*
Traceability Specifications	79	25.3% (20)	26.6% (21)	**27.8% (22)**	15.2% (12)	5.1% (4)	*Decision Support Available*
Architecture Specifications	72	34.7% (25)	**41.7% (30)**	19.4% (14)	1.4% (1)	2.8% (2)	*Decision Support Available*
Tool-Supported V&V Results	79	**32.9% (26)**	21.5% (17)	24.1% (19)	17.7% (14)	3.8% (3)	*Decision Support Available*
Test Case Specifications	79	**39.2% (31)**	29.1% (23)	20.3% (16)	8.9% (7)	2.5% (2)	*Decision Support Available*
Requirements Specifications	80	**40% (32)**	33.8% (27)	16.2% (13)	8.7% (7)	1.3% (1)	*Decision Support Available*
Safety Analysis Results	76	**40.8% (31)**	23.7% (18)	23.7% (18)	10.5% (8)	1.3% (1)	*Decision Support Available*
Design Specifications	76	**42.1% (32)**	35.5% (27)	17.1% (13)	4% (3)	1.3% (1)	*Decision Support Available*
Safety Cases	73	**56.1% (41)**	27.4% (20)	13.7% (10)	1.4% (1)	1.4% (1)	*Fully Manual*
Manual V&V Results	78	**56.4% (44)**	23.1% (18)	16.7% (13)	3.8% (3)	0% (0)	*Fully Manual*
Reused Components Information	71	**59.2% (42)**	31% (22)	7% (5)	1.4% (1)	1.4% (1)	*Fully Manual*
Personnel Competence Specifications	66	**63.6% (42)**	28.8% (19)	7.6% (5)	0% (0)	0% (0)	*Fully Manual*
System Lifecycle Plans	75	**65.4% (49)**	21.3% (16)	9.3% (7)	4% (3)	0% (0)	*Fully Manual*
Assumptions and Operation Conditions Specifications	72	**68.1% (49)**	20.8% (15)	9.7% (7)	1.4% (1)	0% (0)	*Fully Manual*

4.2.2 Tools for safety evidence change impact analysis

In total, the respondents reported the use of 98 different tools for SECIA purposes. The artefact types for which a highest ratio of respondents indicated some tool are *Traceability Specifications*, *Requirements Specifications*, and *Test Case Specifications* (Figure 3), whereas the highest variation of tools has been found for *Source Code*, *Test Case Specifications*, and *Design Specifications* (Figure 4). Interestingly, no impact analysis commercial tool has been reported as used for SECIA from all the artefact types (Figure 5), and tailored extensions of commercial tools have been reported for most artefact types. Only two commercial tools (VeroTrace and DOORS) are among those indicated for more than half of the artefact types. Nonetheless, a single respondent reported the use of VeroTrace. Some model-based tool was reported for 10 out of the 14 artefact types (71.4%).

Internal tools are used for all the artefact types, and basic, non-SECIA-targeted tools such as Excel and Word are commonly used. The specific tools and their frequencies for each artefact type are specified in Figures 7 and 8, which show that internal tools are the most frequently used ones for nine out of the 14 artefact types (64.3%) and that only DOORS is more frequently used for some types. DOORS is also the tool that has reached the highest number of respondents reporting it use for a given artefact type (*Requirements Specifications* and *Traceability Specifications*). Regarding tools for storing SECIA evidence (Figure 6; 37 different tools), internal tools, Excel, DOORS, and Word were the ones indicated by a highest number of respondents. The ratios of Figures 3, 6, 7, and 8 have been calculated according to the number of respondents that provided information for answering RQ2 (N=84). Details about all these tools are provided in Appendices C and D.

When asked about further artefact types and the tools that were used for performing an impact analysis when they change, individual respondents provided the following additional information:

a) Relex for reliability block diagrams and fault trees;
b) Bugzilla project control for requested change/impact, and;
c) Catia and Mathworks tools features for comparing two products and determining differences.

Related work has acknowledged the existence of several impact analysis tools for different artefact types. The comparison with the results of the survey show that: (1) many more tools than those reported in the literature have been found; (2) previous publications have barely paid attention to the use of basic tools (e.g., Excel and Word) for impact analysis purposes; (3) some tools usually mentioned in the literature (e.g., JRipples) do not seem to have been adopted for safety-critical system development. Phenomena acknowledged in prior work for which the results provide evidence of the extent to which they happen include the use of internal tools for SECIA, the extension of commercial tools for impact analysis purposes, the adoption of basic, widely available tools for impact analysis, and the use of models for safety evidence management. We also are not aware of any publication that has indicated the use of NOR-STA and OpenFTA for SECIA from *Safety Cases*, and ASCE from *Test Case Specifications*.

These results greatly contribute to extending the knowledge about the tools used in industry for SECIA. The results should help in bridging the gap between the insights and assumptions presented in the literature and the state of the practice. We think that researchers should be careful when making statements regarding the need for new impact analysis tools. Although more tool support is probably necessary, we wonder if, for instance, research on new source code impact analysis tools should be prioritized, given the high number of available tools. The remaining question is what new SECIA tool support is necessary, especially taking into account the challenges perceived by the respondents (Section 4.3), and thus what specific tool aspects should be studied. Tools that integrate safety evidence meta-information from different sources for SECIA purposes seem to be highly desirable [55].

4.3 RQ3. What challenges are faced when dealing with safety evidence change impact analysis?

Out of the 97 respondents, 90 provided information for answering RQ3 (Questions 20-22 in Appendix A). The next subsections present the aspects studied for this RQ. An overall conclusion is that although *Insufficient tool support* seems to be the most frequent challenge, SECIA would probably further benefit from improvements on *Information aspects* than on *Tools aspects*.

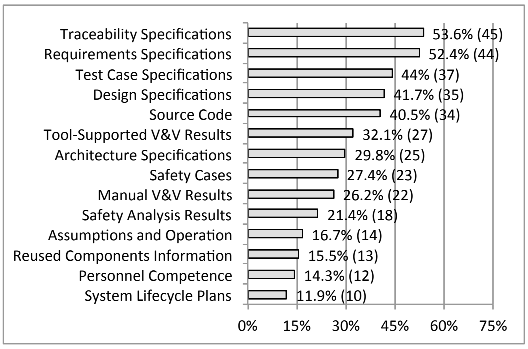


Figure 3. Respondents that indicated some tool for each artefact type

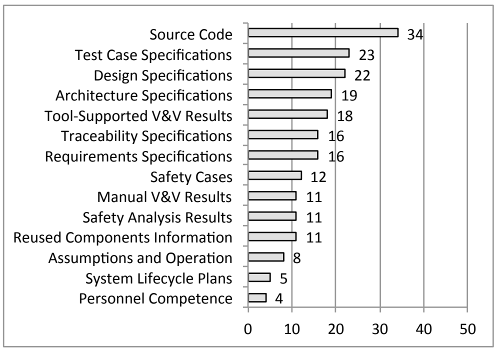


Figure 4. Number of tools indicated for each artefact type

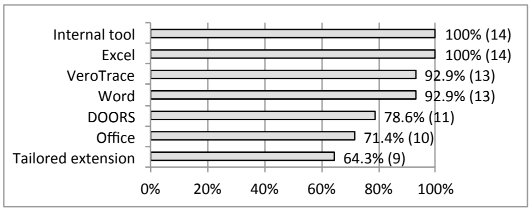


Figure 5. Tools for SECIA reported for more than half of the artefact types

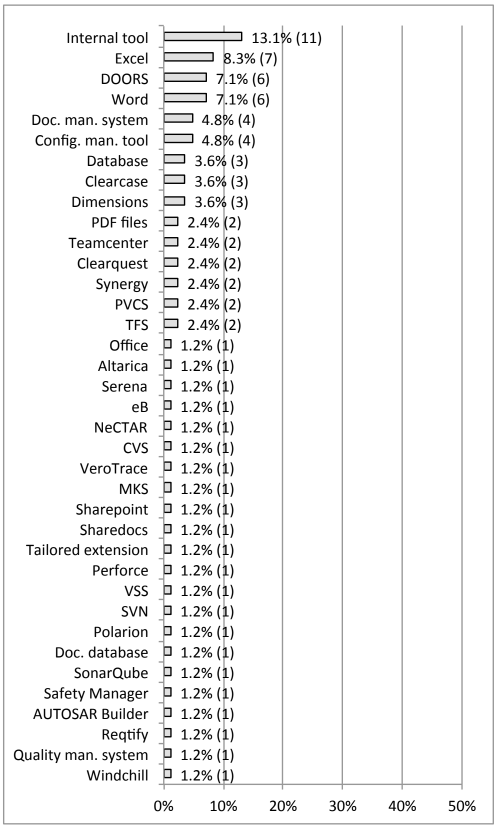


Figure 6. Tools for storing SECIA evidence

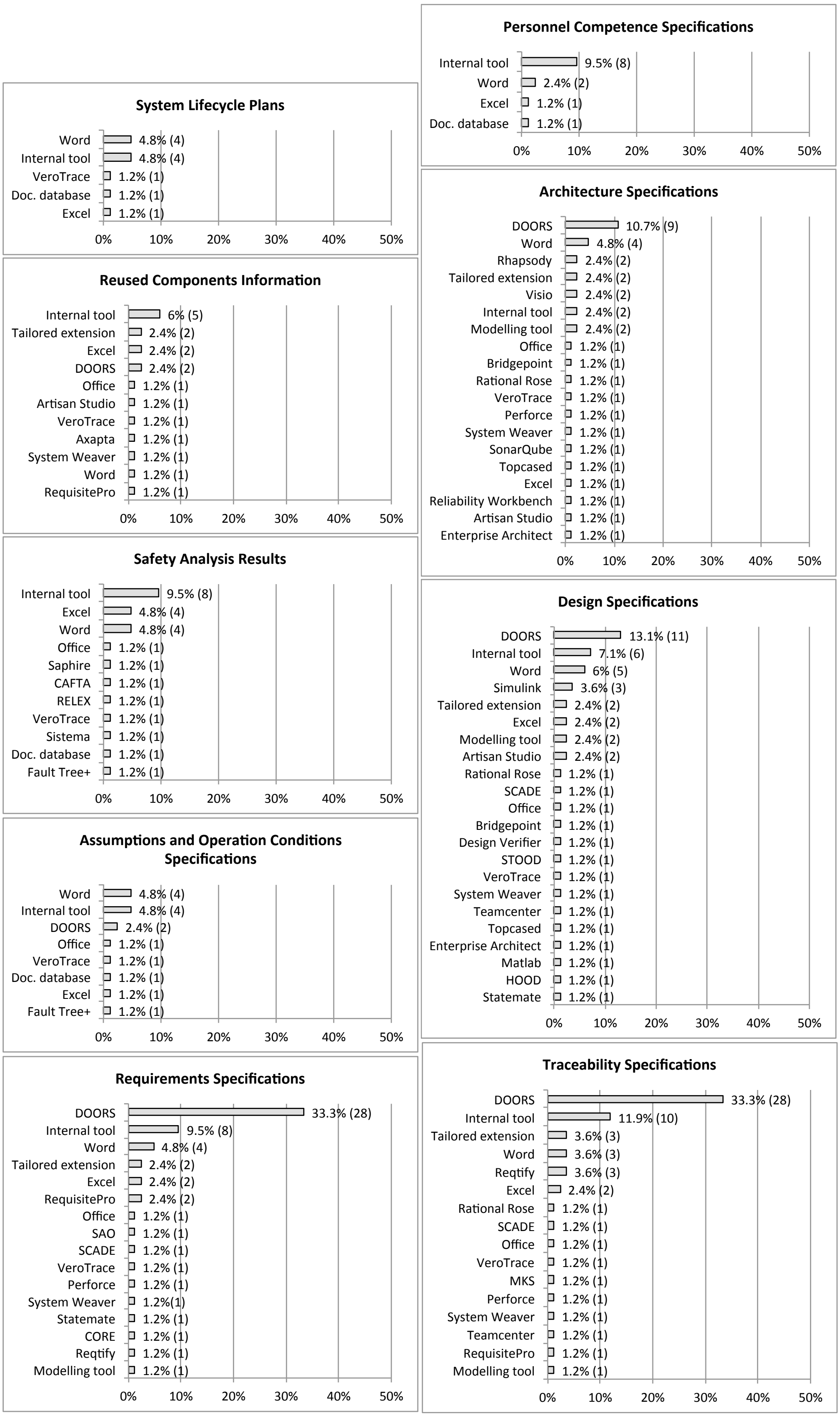
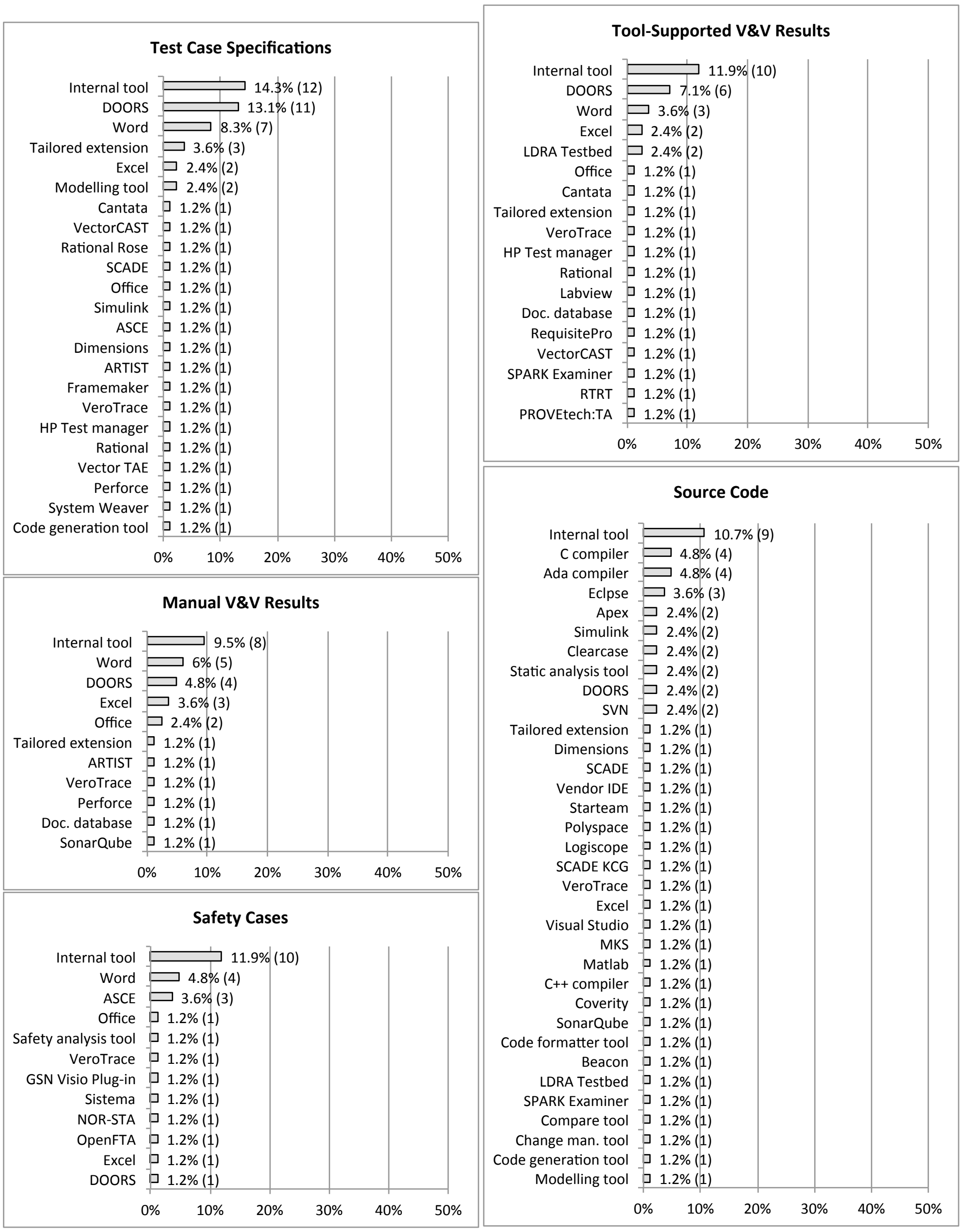


Figure 7. Tools for SECIA (I)


Test Case Specifications

Tool-Supported V&V Results

Manual V&V Results

Source Code

Safety Cases

Figure 8. Tools for SECIA (II)

4.3.1 Challenges frequency

Table 7 shows the frequency with which the respondents had experienced different SECIA challenges. The challenge with the highest median is *Insufficient tool support*, whereas *Difficulty in deciding if a component can be reused* and *Excessive detail of the traceability between artefacts, making traceability management more complex than necessary for impact analysis purposes* have the lowest medians. *Insufficient tool support* and *Vast amount of artefacts to trace* are the challenges most frequently reported as happening in every project. In contrast, *Excessive detail of the traceability between artefacts, making traceability management more complex than necessary for impact analysis purposes* is the challenge most frequently reported as never happening or happening in few projects. From a more global perspective, each challenge has been experienced by between 95.6% and 74.4% of the respondents. The challenges that have been faced by a highest ratio of respondents are *Difficulty in determining the effect of a change on system safety* (95.6%), *Difficulty in estimating the effort required to manage a change* (95.6%), *Insufficient traceability between artefacts to accurately know the consequences of a change* (94.4%), and *Long time for evaluating the consequences of a change* (94.4%). No challenge has 'never' or 'every project' as mode.

We identified a strong correlation between the challenges *Difficulty in assessing system-level impact of component reuse* and *Difficulty in deciding if a component can be reused* (corr. = 0.61). We find particularly interesting that the correlation between the respondents' experience (in years and number of projects; see Figure 1) and the frequency of the challenges is very weak, weak, or very close to weak (-0.32 <= corr. <= -0.1; average corr. = -0.19). This suggests that experience does not greatly make practitioners avoid or mitigate the challenges. In other words, it cannot be claimed that experienced practitioners face the challenges less often than novices. Another interpretation is that the challenges are clearly visible as soon as someone gets involved in SECIA, thus less experienced practitioners also recognise them. We think that this finding is important for experiments on SECIA in which students participate as subjects, and more concretely on SECIA challenges discovery. It cannot be claimed that their results would differ if experienced practitioners participated instead.

We also cannot claim that a higher level of SECIA automation will strongly contribute to decreasing the frequency of the challenges, because we have not found any strong or very strong correlation. This can be regarded as strange for *Insufficient tool support*, which has weak or very weak correlations (-0.27 <= corr. <= 0.02) with the level of SECIA automation for each artefact type. In this sense, we understand that better tool support is beyond simply automation. For example, tools can guide users.

Individual respondents provided the following further challenges:

a) Traceability between all the different environments and tools used in system lifecycle
b) SECIA for derived requirements
c) Feature creep (scope creep), lack of support or documentation for programming language, undocumented source code, and ageing legacy systems
d) Lack of automated support for SECIA effort estimation
e) Difficulty in assessing safety impact using the available trace data
f) Difficulty in understanding and following safety standards' indications
g) Involvement of many different people and organisations (sub-suppliers, customers, system engineers, safety engineers, lawyers...), with different interests
h) Finding the right balance between fine and coarse traceability
i) Change assessors' lack of knowledge to adequately assess an impact or subsequent impact(s)
j) Pressure to meet project time scale, and insufficient staff with the right level of competence
k) Lack of a detailed process and use of inadequate tools
l) Difficulty in tracing the origin and real date of a change cause
m) Lack of an efficient regression verification strategy
n) Insufficient attention to traceability
o) Inefficient SECIA and variability in how to address it depending on the artefacts involved
p) Management's lack of knowledge about risks
q) Lack of detail in existing data justification (e.g., trace link but no explanation), making it difficult to know if change compromises the justification.

Although most of these challenges reported have already been acknowledged in the literature, the respondents provided additional valuable information (e.g., in (b), (i), (o), (p), and (q)). In our opinion, the large final set of challenges (those included in the questionnaire and those mentioned by the respondents) shows that SECIA can be very complex in practice.

Table 7. SECIA challenges frequency

	N	Never	Few projects	Some projects	Most projects	Every project	*Median*
Insufficient tool support	90	11.1% (10)	21.1% (19)	17.8% (16)	**34.4% (31)**	15.6% (14)	*Most projects - Some projects*
Difficulty in estimating the effort required to manage a change	90	4.4% (4)	17.8% (16)	31.1% (28)	**36.7% (33)**	10% (9)	*Some projects*
Vast number of artefacts to trace	90	7.8% (7)	15.6% (14)	**35.6% (32)**	25.6% (23)	15.6% (14)	*Some projects*
Too coarse granularity of the traceability between artefacts to accurately know the consequences of a change	90	10% (9)	25.5% (23)	26.7% (24)	**28.9% (26)**	8.9% (8)	*Some projects*
Insufficient traceability between artefacts to accurately know the consequences of a change	90	5.6% (5)	25.6% (23)	**32.2% (29)**	28.9% (26)	7.8% (7)	*Some projects*
Difficulty in determining the effect of a change on system safety	90	4.4% (4)	23.3% (21)	**38.9% (35)**	24.4% (22)	8.9% (8)	*Some projects*
Long time for evaluating the consequences of a change	90	5.6% (5)	27.8% (25)	**34.4% (31)**	25.6% (23)	6.7% (6)	*Some projects*
Difficulty in assessing system-level impact of component reuse	90	10% (9)	28.9% (26)	**38.9% (35)**	18.9% (17)	3.3% (3)	*Some projects*
Unclear meaning of the traceability between artefacts in order to know how to manage a change	90	15.6% (14)	26.7% (24)	**35.6% (32)**	17.8% (16)	4.4% (4)	*Some projects*
Insufficient confidence by assessor or certifiers in having managed a change properly	90	20% (18)	27.8% (25)	**32.2% (29)**	16.7% (15)	3.3% (3)	*Some projects*
Lack of a systematic process for performing impact analysis	90	12.2% (11)	**28.9% (26)**	27.8% (25)	20% (18)	11.1% (10)	*Some projects*
Difficulty in deciding if a component can be reused	90	21.1% (19)	30% (27)	**31.1% (28)**	14.4% (13)	3.3% (3)	*Few projects*
Excessive detail of the traceability between artefacts, making traceability management more complex than necessary for impact analysis purposes	90	25.6% (23)	**32.2% (29)**	26.7% (24)	11.1% (10)	4.4% (4)	*Few projects*

4.3.2 How to improve safety evidence change impact analysis

A total of 76 respondents provided information about how SECIA could be improved. We found three main improvement categories: information aspects, process aspects, and tool aspects. Their definition was based on the following codes for the answers:

- Information aspects, referring to the need for more information related to or for SECIA execution
  - Communication: information exchange among those involved in SECIA activities
  - Data used for analysis: pieces of data that are consulted when deciding upon how to perform SECIA activities
  - Guidance: information available and that can be followed for SECIA
  - Knowledge: existing information about how to deal with SECIA
  - Safety cases: documented system safety justification
  - SECIA process transparency: degree of knowledge about SECIA activities for those not directly involved in the activities
  - Standards: industrially-accepted best practices followed for ensuring system safety
  - System specifications: artefacts describing system structure, behaviour, or constraints
  - Traceability: relationship between two artefacts
  - Training: knowledge acquisition for those involved in SECIA
- Process aspects, referring to the need for better SECIA execution processes
  - Analysis of impact on safety: the effect that the changes in the body of safety evidence can have on system safety
  - Analysis process: the process followed for SECIA
  - Coordination: degree to which those involved in SECIA activities work cooperatively
  - Credibility: degree to which someone would agree that SECIA activities have been adequately performed
  - Independence: degree of difference between those involved in SECIA activities
  - SECIA verification: activities targeted at guaranteeing that impact analysis and change management have been adequately addressed
  - System development: activities targeted at specifying and creating a system
  - System V&V: activities targeted at providing an assurance of certain system properties
  - Time aspects: time resources necessary for and time constraints on SECIA
- Tool aspects, referring to the need for new or better SECIA tools
  - Level of automation: degree of automatic support offered by tool support
  - Tool integration: degree of information exchange between the tools used in a system's lifecycle, including SECIA-related tools
  - Tool support: available tools for performing SECIA

Based on the results, we have created the taxonomy of areas for improvement shown in Figure 9. The improvement categories and codes are not completely independent, but relationships and dependencies among them can be established. For example, information is used or necessary for process execution, which can use tools as means. On the other hand, new tool support can enable improvements in information and process aspects.

Figure 10 shows the percentage and the number (in brackets) of respondents that indicated each improvement area, among the 76 that provided information. Over two thirds of the respondents mentioned *Information aspects*. The most frequent specific area was *Tool support*, followed by *Traceability*, *Analysis process*, and *Guidance*. Specific topics mentioned by individual respondents that we consider especially relevant are:

a) Impact analysis activities need to be more systematic
b) Existing tools are either (1) too expensive and complex or (2) not very suitable and useful
c) Use of modular safety cases
d) Better understandings of change effect semantics
e) Better safety engineering principles and methods
f) Standards' requirements clarification
g) Wider knowledge about safety goals in development teams
h) Impact simulation, including simulation of system behaviour after a change
i) Higher quality of safety evidence, in particular better documentation of the scope, assumptions, and estimated impact of potential future changes

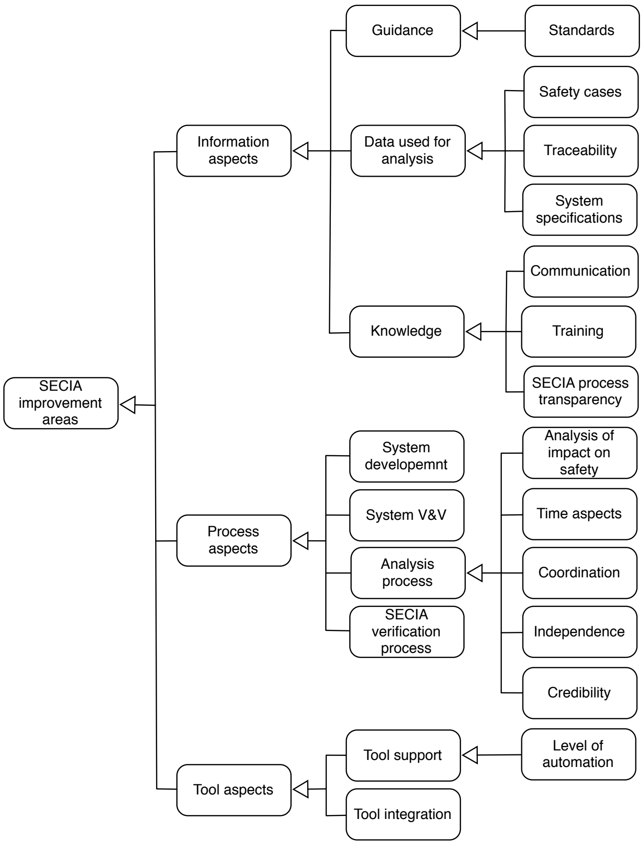


Figure 9. Taxonomy of SECIA improvement areas

Although text in safety standards and publications referring to the improvement areas can be found, there are several aspects on which further research seems to be necessary. In our opinion, and also based on the insights provided in the publications reviewed in Section 2 and on the answers to RQ1 and RQ2, some of the main areas that require further study are:

1. Development of traceability guidelines, including heuristics for deciding upon granularity suitability and trace semantics for SECIA
2. Identification of the artefact types with which traceability-related SECIA challenges are most often faced
3. Establishment of the degree to which SECIA can or should really be automated as a way to tackle tool support-related challenges, according to certification authorities' expectations and tool qualification requirements
4. Safety cases in SECIA, for analysing change impact both from and on safety cases

4.4 Summary of results

The main results of the survey can be summarised as follows:

- SECIA seems to be most frequently addressed (RQ1) as a result of the *Modification of a new system during its development*, and triggered by changes in *Design Specifications, Requirements Specifications*, *Safety Analysis Results*, *Source Code*, *Test case Specifications*, and *Traceability Specifications*. The artefact type most frequently reported as affected by changes is *Manual V&V results*, and *Requirements specifications* can be regarded as the most central artefact type for SECIA from a general perspective. Nonetheless, some less frequent phenomena require more research efforts on how to address them, since they correspond to practices for which very few systematic means for SECIA exist (e.g., re-certification for a different application domain) or they are critical for ensuring system safety and showing compliance with safety standards (e.g., safety case evolution).
- A total of 69 strong SECIA-related correlations exist between the artefact types, and all the artefact types have some strong correlation. This shows that SECIA usually affect several artefact types. Six very strong correlations have been found between pieces of *Source Code*, and between *Requirements Specifications* and *Design Specifications* (2), *Requirements Specifications* and *Source Code*, *Test Case Specifications* and *Source Code*, and *Safety Analysis Results* and *Assumptions and Operation Conditions Specifications*.

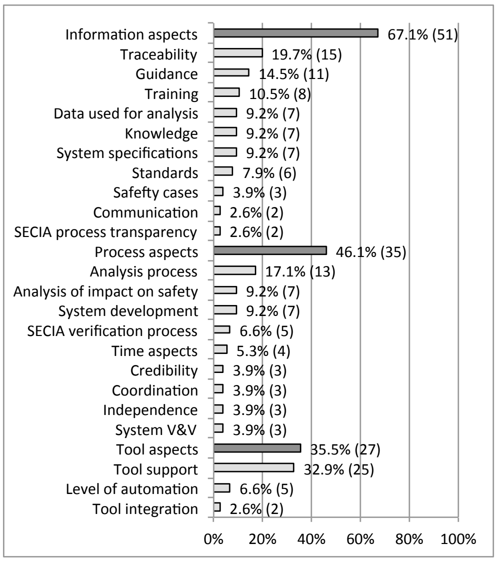


Figure 10. Frequency of SECIA improvement areas

- Regarding tool support (RQ2), the overall level of SECIA automation is low and practitioners perform a significant amount of manual work. Practitioners also commonly use basic tools such as Excel and Word, which have clear limitations (e.g., no tool qualification), and internal tools. No commercial tool is widely used in industry for SECIA or used for all the artefact types, and the tools seem to vary among organizations. An open question is if future research on tool support should focus on the development of new tools for specific artefact types or in the provision of means for integrating information from different tools.
- Practitioners face a wide variety of challenges for SECIA (RQ3), with *Insufficient tool support* having the highest median. Indeed, *Tool support* is the specific area with the highest ratio of respondents indicating that it could contribute to improving SECIA. Nonetheless, over two thirds of the respondents mentioned *Information aspects* in their SECIA improvement suggestions, and almost half of them referred to *Process aspects*. Experience and the level of SECIA automation do not seem to greatly help practitioners in reducing the frequency of the challenges.

5 Conclusion

We have presented the results of an industrial survey on safety evidence change impact analysis (SECIA). SECIA is an essential activity for any safety-critical system, as it can easily lead to safety assurance and certification risks if not adequately managed. The results provide a rather comprehensive picture of the circumstances under which SECIA is addressed, the tool support used, and the challenges faced. The results also indicate aspects that practitioners should carefully analyse when performing SECIA and that are not mentioned in the text of safety standards, such as that certain artefact types usually evolve jointly (see Figure 2), and tools that can be used for SECIA (see Section 4.2).

Many results are in line with the insights provided in prior research. For example, requirements specifications seem to play a major role in SECIA, and practitioners expect improvements on tool support. However, the survey is the first study that provides strong empirical evidence of how often the phenomena occur. More importantly, the results report on phenomena for which no evidence existed (e.g., use of internal tools for SECIA from all the artefact types studied), and suggest frequencies of phenomena in industry that very likely were unexpected (e.g., re-certification for different application domains) or that can raise some concerns about current industrial practices (e.g., safety case evolution management seems to be inadequate often).

Several areas for future research can be identified from the results. Some examples are the study of SECIA needs for safety-specific artefact types, the analysis of how tools with basic functionality are used for SECIA, and the definition of effective and efficient guidelines for tackling traceability-related SECIA challenges. Furthermore, the results highlight several aspects on which we think that industry clearly needs improvements, such as SECIA tools for all artefact types and an increase in their level of automation.

The survey represents a major milestone for other research efforts in which we are currently involved, including cross-domain and evolutionary safety assurance and certification [15], component-based impact analysis (e.g., [52]), and recommendation-driven impact analysis (e.g., [7]) for critical systems.

The results of the survey help us to identify several areas on which our future work should focus. We plan to further investigate the relationships that can exist between different artefact types and their implications for impact analysis, as well as how to improve safety case evolution management.

Acknowledgement. The research leading to this report has received funding from the FP7 programme under the grant agreement n° 289011 (OPENCOSS), from the Research Council of Norway under the projects Certus-SFI and EvolveIT, and from the Industrial Excellence Center EASE - Embedded Applications Software Engineering. The authors would like to thank the people that participated in the pilot studies and the respondents of the survey, especially David Callele for his suggestions towards improving the readability of the survey instrument.

References

1. Babar, M.A., Tang, A., Gorton, I., Han, J.: Industrial Perspective on the Usefulness of Design Rationale for Software Maintenance: A Survey. In: Sixth International Conference on Quality Software (QSIC 2006), pp. 201-208
2. Barzilay, O., Hazzan, O., Yehudai, A.: Using social media to study the diversity of example usage among professional developers. In: 19th ACM SIGSOFT symposium and the 13th European conference on Foundations of software engineering (SIGSOFT FSE 2011), pp. 472-475
3. Bennet, K.: Software evolution: past, present and future. Information and Software Technology 38(11): 673-680 (1996)
4. Bjarnason, R., Runeson, P., Borg, M., Unterkalmsteiner, M., Engström, E., Regnell, B., Sabaliauskaite, G., Loconsole, A., Gorschek, T., Feldt, R.: Challenges and practices in aligning requirements with verification and validation; a case study of six companies. Empirical Software Engineering 19(6): 1809-1855 (2014)
5. Björnander, S., Land, R., Graydon, P., Lundqvist, K., Conmy, P.: A Method to Formally Evaluate Safety Case Evidences against a System Architecture Model. In: 23rd IEEE International Symposium on Software Reliability Engineering Workshops (ISSRE Workshops 2012), pp. 337-342
6. Bohner, S.A., Arnold, R.S.: Software Change Impact Analysis. IEEE Press, 1996
7. Borg, M., Runeson, R.: Changes, Evolution and Bugs - Recommendation Systems for Issue Management. In: Robillard, M.P., Maalej, W., Walker, R.J., Zimmermann, T. (eds.) Recommendation Systems in Software Engineering. Springer, 2014, pp. 477-509
8. Borg, M., Runeson, P., Ardö, A.: Recovering from a decade: a systematic mapping of information retrieval approaches to software traceability. Empirical Software Engineering 19(6): 1565-1616 (2014)
9. Borg, M., Gotel, O., Wnuk, K.: Enabling traceability reuse for impact analyses: A feasibility study in a safety context. In: 7th International Workshop on Traceability in Emerging Forms of Software Engineering (TEFSE 2013), pp. 72-78
10. Born, K., Favaro, J., Kath. O.: Application of ISO DIS 26262 in Practice. In: 1st Workshop on Critical Automotive Applications: Robustness & Safety (CARS 2010), pp. 3-6
11. Bratthall, L., Johansson, E., Regnell, B.: Is a Design Rationale Vital when Predicting Change Impact? A Controlled Experiment on Software Architecture Evolution. In: Second International Conference on Product Focused Software Process Improvement (PROFES 2000), pp. 126-139
12. Buckley, J., Mens, T., Zenger, M., Rashid, A., Kniesel, G.: Towards a taxonomy of software change. Journal of Software Maintenance 17(5): 309-332 (2005)
13. Carrillo-de-Gea, J.M., Nicolás, J., Fernández-Alemán, J.L, Toval, A., Ebert, C., Vizcaíno, A.: Requirements engineering tools: Capabilities, survey and assessment. Information and Software Technology 54(10): 1142-1157 (2012)
14. de la Vara, J.L., Nair, S., Verhulst, E., Studzizba, J., Pepek, P., Lambourg, J., Sabetzadeh, M.: Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards. In: Next Generation of System Assurance Approaches for Safety-Critical Systems Workshop (SASSUR 2012), pp. 64-78
15. de la Vara, J.L., Panesar-Walawege, R.K.: SafetyMet: A Metamodel for Safety Standards. In: 16th International Conference on Model-Driven Engineering Languages and Systems (MODELS 2013), pp. 69-86
16. de Lemos, R.: Safety Analysis of an Evolving Software Architecture. In: 5th IEEE International Symposium on High-Assurance Systems Engineering (HASE 2000), pp. 159-168
17. de Mello, R.M., Travassos, G.H.: Would Sociable Software Engineers Observe Better? In: 2013 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM 2013), pp. 279-282

18. Durisic, D., Nilsson, M., Staron, M., Hansson, J.: Measuring the impact of changes to the complexity and coupling properties of automotive software systems. Journal of Systems and Software 86(5): 1275-1293 (2013)
19. Engström, E., Runeson, P.: A Qualitative Survey of Regression Testing Practices. In: 11th International Conference on Product-Focused Software Process Improvement (PROFES 2010), pp. 3-16
20. Ferreira, S., Shunk, D.L., Collofello, J.S., Mackulak, G.T., Dueck, A.: Reducing the risk of requirements volatility: findings from an empirical survey. Journal of Software Maintenance 23(5): 375-393 (2011)
21. Ge, Y., Bai, L.: Probability-based Safety Related Requirements Change Impact Analysis. In: 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010), pp. 719-722
22. Ghazarian, A.: A Research Agenda for Software Reliability. In: IEEE Reliability Society 2009 Annual Technology Report
23. Goeritzer, R.: Using impact analysis in industry. In: 33rd International Conference on Software Engineering (ICSE 2011), pp. 1155-1157
24. Graaf, B., Lormans, M., Toetenel, H.: Embedded Software Engineering: The State of the Practice. IEEE Software 20(6): 61-69 (2003)
25. Gray, D.E.: Doing Research in the Real World, 3rd ed. Sage, 2014
26. Hinchey, M., Coyle, L.: Evolving Critical Systems: a Research Agenda for Computer-Based Systems. In: 17th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS 2010), pp. 430-435
27. IEEE: Systems and software engineering - System life cycle processes, Std. 15288-2008
28. INCOSE: Requirements Management Tools Survey, http://www.incose.org/productspubs/products/rmsurvey.aspx (Accessed Sept. 26, 2014)
29. Jamshidi, P., Ghafari, M., Ahmad, A., Pahl, C.: A Framework for Classifying and Comparing Architecture-Centric Software Evolution Research. In: 17th European Conference on Software Maintenance and Reengineering (CSMR 2013), pp. 305-314
30. Jo, H.J., Hwang, J.G., Kim, Y.K.: S/W Change Impact Analysis Tool in Railway Systems. In: 2009 Asia and Pacific Transmission & Distribution Conference & Exposition, pp. 1-4
31. Johnson, C.W., Bowell, M.: Using Software Development Standards to Analyse Accidents Involving Eletrical, Electronic or Programmable, Electronic Systems: The Blade Mill PLC Case Study. In: Second Workshop on the Investigation and Reporting of Incidents and Accidents, 2003
32. Johnson, C.W., de Almeida, I.M.: An investigation into the loss of the Brazilian space programmes launch vehicle VLS-1 V03. Safety Science 46(1): 38-53 (2008)
33. Jönsson, P., Lindvall, M.: Impact Analysis. In: Aurum, A., Wohlin, C. (eds) Engineering and Managing Software Requirements. Springer, 2005, pp. 117-142
34. T. Kanij, R. Merkel, J. Grundy, Lessons learned from conducting industry surveys in software testing, in: Conducting Empirical Studies in Industry (CESI), 2013 1st International Workshop on, IEEE, 2013, pp. 63-66.
35. Kasoju, A., Petersen, K., Mäntylä, M.: Analyzing an automotive testing process with evidence-based software engineering. Information and Software Technology 55(7): 1237-1259 (2013)
36. Kelly, T.: A Systematic Approach to Safety Case Management. In: SAE 2004 World Congress
37. Kitchenham, B., Pfleeger, S.L., Pickard, L., Jones, P., Hoaglin, D.C., El Emam, K., Rosenberg, J.: Preliminary Guidelines for Empirical Research in Software Engineering. IEEE Transactions on Software Engineering 28(8): 721-734 (2002)
38. Kitchenham, B., Pfleeger, S.L.: Personal opinion surveys. In: Shull, F., Singer, J., Sjoberg, D.I.K., (eds.) Guide to Advanced Empirical Software Engineering. Springer, 2008, pp. 63-92
39. Khan, S.S., Greenwood, P., Garcia, A., Rashid, A.: On the Impact of Evolving Requirements-Architecture Dependencies: An Exploratory Study. In: 20th International Conference on Advanced Information Systems Engineering (CAiSE 2008), pp. 243-257
40. Kornecki, A.J., Zalewski, J.: Certification of software for real-time safety-critical systems: state of the art. Innovations in Systems and Software Engineering 5(2): 149-161 (2009)
41. Lehnert, S.: A Review of Software Change Impact Analysis. Ilmenau University of Technology, Technical Report, 2011
42. Lehnert, S.: A Taxonomy for Software Change Impact Analysis. In: 12th International Workshop on Principles of Software Evolution and 7th annual ERCIM Workshop on Software Evolution, (EVOL/IWPSE 2011), pp. 41-50
43. Leveson, N.: Engineering a Safer World: Systems Thinking Applied to Safety. The MIT Press, 2011

44. Li, B., Sun, X., Leung, H., Zhang, S.: A survey of code-based change impact analysis techniques. Software Testing, Verification & Reliability 23(8): 613-646 (2013)
45. Lindvall, M.: Evaluating Impact Analysis - A Case Study. Empirical Software Engineering 2(2): 152-158 (1997)
46. Lindvall, M., Sandahl, K.: How well do experienced software developers predict software change? Journal of Systems and Software 43(1): 19-27 (1998)
47. Lisagor, O., Kelly, T.: Incremental Safety Assessment: Theory and Practice. In: 26th International System Safety Conference (ISSC 2008)
48. Lloyd, M.H., Reeve, P.J.: IEC 61508 and IEC 61511 Assessments - some Lessons Learned. In: 4th IET International Conference on System Safety, 2009
49. Mäder, P., Jones, P.L., Zhang, Y., Cleland-Huang, J.: Strategic Traceability for Safety-Critical Projects. IEEE Software 30(3): 58-66 (2013)
50. Mens, T., Wermelinger, M., Ducasse, S., Demeyer, S., Hirschfeld, R., Jazayeri, M.: Challenges in Software Evolution. In: 8th International Workshop on Principles of Software Evolution (IWPSE 2005), pp. 13-22
51. Mistry, M., Felici, M.: Implementation of Change Management in Safety Cases. In: Formal Aspects of Safety-Critical Systems, 2008
52. Moonen, L.: Towards evidence-based recommendations to guide the evolution of component-based product families. Science of Computer Programming (accepted paper, 2013)
53. Nair, S., de la Vara, J.L., Sabetzadeh, M., Falessi, D.: Management of Evidence for Compliance with Safety Standards: A Survey on the State of Practice, Simula Research Laboratory, Technical Report, 2013
54. Nair, S., de la Vara, J.L., Sen, S.: A Review of Traceability Research at the Requirements Engineering Conference. In: 21st IEEE International Requirements Engineering Conference (RE 2013), pp. 222-229
55. Nair, S., de la Vara, J.L., 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)
56. Nair, S., de la Vara, J.L., Melzi, A., Tagliaferri, G., de-la-Beaujardiere, L., Belmonte, F.: Safety Evidence Traceability: Problem Analysis and Model. In: 20th International Working Conference Requirements Engineering: Foundation for Software Quality (REFSQ 2014), pp. 309-324
57. Nicholson, M., Conmy, P., Bate, I., McDermid, J.: Generating and Maintaining a Safety Argument for Integrated Modular Systems. In: 5th Australian Workshop on Safety Critical Systems and Software (SCS 2000), pp. 31-41
58. OPENCOSS project: Deliverable D6.1 - Baseline for the evidence management needs of the OPENCOSS platform, http://www.opencoss-project.eu/node/7, 2012 (Accessed Sep 26, 2014)
59. Parasuraman, R., Sheridan, T.B., Wickens, C.D.: A model for types and levels of human interaction with automation. IEEE Transactions on Systems, Man, and Cybernetics, Part A 30(3): 286-297 (2000)
60. Pedersen-Notander, J., Höst, M., Runeson, P.: Challenges in Flexible Safety-Critical Software Development - An Industrial Qualitative Survey. In: 14th International Conference on Product-Focused Software Process Improvement (PROFES 2013), pp. 283-297
61. Rierson, L.: Developing Safety-Critical Software: A Practical Guide for Aviation Software and DO-178C Compliance. CRC Press, 2013
62. Robson, C.: Real World Research, 2nd ed. Blackwell, 2002.
63. Rovegard, P., Angelis, L., Wohlin, C.: An Empirical Study on Views of Importance of Change Impact Analysis Issues. IEEE Transactions on Software Engineering 34(4): 516-530 (2008)
64. SafeCer project: Deliverable D1.0.1 ‑ State-of-practice and state-of-the-art agreed over workgroup, http://www.safecer.eu/text/view/50/, 2011 (Accessed Sep 26, 2014)
65. Siegle, D.: Likert Scale, http://www.gifted.uconn.edu/siegle/research/instrument%20reliability%20and%20validity/likert.html, 2010 (Accessed Sep 26, 2014)
66. Stammel, J., Durdik, Z., Krogmann, K., Weiss, R., Koziolek, H.: Software Evolution for Industrial Automation Systems; Literature Overview. Karlsruhe Institute of Technology, Technical Report, 2011
67. Stephenson, Z.R.: Change Management in Families of Safety-Critical Embedded Systems. PhD Thesis, University of York, 2002
68. Sudgen, R.C., Strens, M.R.: Strategies, Tactics and Methods for Handling Change. In: IEEE Symposium and Workshop on Engineering of Computer Based Systems (ECBS 1996), pp. 457-463

69. Tao, Y., Dang, Y., Xie, T., Zhang, D., Kim, S.: How do software engineers understand code changes? - An exploratory study in industry. In: 20th ACM SIGSOFT Symposium on the Foundations of Software Engineering (SIGSOFT FSE 2012)
70. Törner, F., Öhman, P.: Automotive Safety Case: A Qualitative Case Study of Drivers, Usages, and Issues. In: 11th IEEE High Assurance Systems Engineering Symposium (HASE 2008), pp. 313-322
71. Tracey, N., Stephenson, A., Clark, J., McDermid, J.: A Safe Change Oriented Process for Safety-Critical Systems. In: International Workshop on Software Change and Evolution, 1999
72. van der Spek, P.: Managing software evolution in embedded systems. PhD Thesis, Vrije Universiteit Amsterdam, 2010
73. von Knethen, A., Grund, M.: QuaTrace: A Tool Environment for (Semi-) Automatic Impact Analysis Based on Traces. In: 19th International Conference on Software Maintenance (ICSM 2003), pp. 246-255
74. Wallace, D.R., Kuhn, D.R.: Failure modes in medical device software: an analysis of 15 years of recall data. International Journal of Reliability, Quality and Safety Engineering 8(4): 351-371 (2001)
75. Wnuk, K., Regnell, B., Schrewelius, C.: Architecting and Coordinating Thousands of Requirements - An Industrial Case Study. In: 15th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2009), pp. 118-123
76. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B.: Experimentation in Software Engineering. Springer 2012
77. Wong, W.E., Debroy, V., Surampudi, A., Kim, H., Siok, M.F.: Recent Catastrophic Accidents: Investigating How Software was Responsible. In: Fourth International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2010), pp. 14-22
78. Yazdanshenas, A.R., Moonen, L.: Fine-grained change impact analysis for component-based product families. In: 28th IEEE International Conference on Software Maintenance (ICSM 2012), pp. 119-128
79. Zhang, H., Li, J., Zhu, L., Jeffery, D.R., Liu, Y., Wang, Q., Li, M.: Investigating dependencies in software requirements for change propagation analysis. Information and Software Technology 56(1): 40-53 (2014)

Appendix A. Survey Instrument

This appendix presents the questionnaire used as survey instrument. The questions with an asterisk indicate that they required an answer, the ‘PR’ superscript indicates that the order of the corresponding page was randomized, and the ‘OR’ superscript in the questions indicates that the order of the options to answer about was randomized.

SURVEY ON SAFETY EVIDENCE CHANGE IMPACT ANALYSIS FOR CRITICAL SYSTEMS

Introduction

Most critical computer-based and software-intensive systems in domains such as avionics, railway, and automotive are subject to some form of safety assessment by a third party (e.g., a certification authority) as a way to ensure that these systems do not pose undue risks to people, property, or the environment. The most common type of assessment is compliance with safety (or safety-related) standards, usually referred to as safety certification. Examples of safety standards include the general IEC61508 standard for electrical/electronic/programmable electronic devices in a wide range of industries, and more specific standards such as DO-178C for avionics, the CENELEC standards for railway, and ISO26262 for the automotive sector.

Demonstration of compliance with a specific standard involves gathering and providing convincing safety evidence. **By safety evidence, we refer to the artefacts that contribute to developing confidence in the safe operation of a system and that are used to show the fulfilment of the criteria of a safety standard**. Examples of artefact types that can be used as evidence include safety analysis results, testing results, reviews, and source code.

Such artefacts can evolve during the system lifecycle. The corresponding changes must be managed and change impact analysis might be necessary in order to guarantee that the changes do not jeopardise system safety or compliance with a standard. **By safety evidence change impact analysis, we refer to the activity that attempts to identify, in the body of safety evidence, the potential consequences of a change.** Possible consequences can be the need for adding, modifying, or revoking some artefact.

The purpose of this survey is to gain **insights into how industry deals with safety evidence change impact analysis**. The survey is part of the work in OPENCOSS (http://www.opencoss-project.eu/), a European research project that is developing an open-source infrastructure for safety assurance and certification of critical systems. Your answers will help us to develop solutions that fit the current practices and needs regarding safety evidence change.

The survey is targeted at **practitioners that are or have been involved in safety evidence change impact analysis**. This includes people who provide safety evidence (e.g., safety engineers or testers of a company that supplies components), people who check safety evidence (e.g., an independent safety assessor), and people who request safety evidence (e.g., a person that represents a certification authority).

Completing the survey is expected to take less than 20 minutes. Please answer the questions in the context of the projects targeted at developing a safety-critical system in which you have participated. All the responses will be held confidential and anonymous.

Finally, if you are interested in the results of the survey, please contact Jose Luis de la Vara (jdelavara@simula.no) or Markus Borg (markus.borg@cs.lth.se).

Thank you very much for your participation in the survey.

Background information

1. How did you find this survey? *

- Post on LinkedIn
- Post on a mailing list
- Personal invitation
- Other - please specify:

2. What is the main application domain in which you have worked on safety evidence change impact analysis? *

- Aerospace
- Automotive
- Avionics
- Defence
- Machinery
- Maritime
- Medical
- Mining
- Nuclear
- Off-highway equipment
- Oil and gas
- Process automation
- Railway
- Robotics
- Trucks
- Other - please specify:

3. In relation to what safety standards have you been involved in safety evidence change impact analysis? *

4. In what country or countries have you principally worked upon safety evidence change impact analysis? *

5. What is the main role of the organization for which you have worked regarding the development of safety-critical systems? *
- Certification authority
- Component supplier
- Consultant
- Developer/manufacturer of final systems
- Development tool vendor
- Independent safety assessor
- Regulation authority
- System user
- Research institution
- Other - please specify:

6. What is your main role in the organization? *

7. How long have you been involved in activities related to safety evidence change impact analysis? *
- Less than 1 year
- Between 1 and 2 years
- Between 2 and 5 years
- Between 5 and 10 years
- More than 10 years

8. How many projects dealing with safety evidence change impact analysis have you participated in? *
- Less than 5 projects
- Between 5 and 10 projects
- More than 10 projects

Circumstances under which safety evidence change impact analysis is addressed ^{PR}

Safety evidence change impact analysis might be performed in different scenarios and for different artefact types used as safety evidence. You will be asked about these aspects in this section.

9. How often have you been involved in safety evidence change impact analysis in these general situations? *^{OR}

Frequency:
- Never
- Few projects (i.e., rarely)
- Some projects (i.e., sometimes)
- Most of the projects (i.e., very often)
- Every project (i.e., always)

Situations:
- Reuse of existing components in a new system
- Modification of a new system during its development
- Modification of a new system as a result of its verification and validation
- Modification of a system during its maintenance
- New safety-related request from an assessor or a certification authority
- Re-certification of an existing system after some modification
- Re-certification of an existing system for a different operational context
- Re-certification of an existing system for a different standard
- Re-certification of an existing system for a different application domain

10. If you would like to add any further general situations in which you have been involved in safety evidence change impact analysis, please do so in the box below, and also indicate their frequency (for example, Situation X: some projects; Situation Y: few projects, etc.)

11. For the artefacts used as safety evidence, how often is safety evidence change impact analysis performed as a consequence of changes in the following artefact types? *^{OR}

Frequency:
- Never
- Few projects
- Some projects
- Most of the projects
- Every project
- I don't know

Artefact types:
- System Lifecycle Plans (e.g., development plans, validation and verification plans, modification procedures, and operation procedures)
- Reused Components Information (e.g., historical service data and reliability specifications)
- Personnel Competence Specifications (e.g., personnel training and experience assessment)
- Safety Analysis Results (e.g., the results from Fault Tree Analysis and Failure Mode and Effects Analysis)
- Assumptions and Operation Conditions Specifications (e.g., the constraints on the working environment of a system)
- Requirements Specifications (e.g., safety requirements or performance requirements)
- Architecture Specifications (e.g., system components and AADL diagrams)
- Design Specifications (e.g., the internal characteristics of system components and SysML diagrams)
- Traceability Specifications (e.g., the relationships between requirements and test cases and between requirements and design)
- Test Case Specifications (e.g., the inputs, execution conditions, and predicted results using a system)
- Tool Supported Validation and Verification Results (e.g., testing results, simulation results, and formal verification results)
- Manual Validation and Verification Results (e.g., inspection results and review results)
- Source Code (e.g., Ada code or C code)
- Safety Cases (documented argument aimed at providing a compelling, comprehensive, and valid case that a system is safe for a given application in a given operating environment)

12. If you would like to add any further artefact types from which safety evidence change impact analysis is performed, please do so in the box below, and also indicate their frequency (for example, Artefact type X: some projects; Artefact type Y: few projects, etc.)

13. For the artefacts used as safety evidence, how often are the following artefact types affected by changes to the body of safety evidence? *^{OR}

Frequency:
- Never
- Few projects
- Some projects
- Most of the projects
- Every project
- I don't know

Artefact types:
- System Lifecycle Plans
- Reused Components Information
- Personnel Competence Specifications
- Safety Analysis Results
- Assumptions and Operation Conditions Specifications
- Requirements Specifications
- Architecture Specifications
- Design Specifications
- Traceability Specifications

- Test Case Specifications
- Tool Supported Validation and Verification Results
- Manual Validation and Verification Results
- Source Code
- Safety Cases

14. If you would like to add any further artefact types affected by changes to the body of safety evidence, please do so in the box below, and also indicate their frequency (for example, Artefact type X: some projects; Artefact type Y: few projects, etc.)

Tool support ^{PR}

Tools can support and facilitate safety evidence change impact analysis. Such tools can vary depending on the artefact types from which the analysis originates. For example, an organization can use some change impact analysis tool for requirements or for source code. It is also usually necessary to show how the change, its consequences, and the actions to address the consequences have been managed. We refer to this information as evidence of safety evidence change management. Such information might be stored in some tool. You will be asked about these aspects in this section.

15. For the artefacts used as safety evidence, please rank the level of automation offered by the tool support used for performing an impact analysis when the following artefact types change. *^{OR}

Levels of automation:
- Fully manual *(no automation in the process; e.g., impact determined by reading documentation and asking colleagues)*
- Decision support available *(limited support for narrowing down a selection of possible impact; e.g., search tool used to seek impact, repositories easy to browse thanks to information structure)*
- Semi-automated recommendations *(tools suggest artefacts that might be impacted but humans must confirm)*
- Highly automated recommendations *(tools report impact and humans have the authority to veto the suggestions)*
- Automatic impact analysis *(tools determine the impact without human involvement)*
- I don't know

Artefact types:
- System Lifecycle Plans (e.g., development plans, validation and verification plans, modification procedures, and operation procedures)
- Reused Components Information (e.g., historical service data and reliability specifications)
- Personnel Competence Specifications (e.g., personnel training and experience assessment)
- Safety Analysis Results (e.g., the results from Fault Tree Analysis and Failure Mode and Effects Analysis)
- Assumptions and Operation Conditions Specifications (e.g., the constraints on the working environment of a system)
- Requirements Specifications (e.g., safety requirements or performance requirements)
- Architecture Specifications (e.g., system components and AADL diagrams)
- Design Specifications (e.g., the internal characteristics of system components and SysML diagrams)
- Traceability Specifications (e.g., the relationships between requirements and test cases and between requirements and design)
- Test Case Specifications (e.g., the inputs, execution conditions, and predicted results using a system)
- Tool Supported Validation and Verification Results (e.g., testing results, simulation results, and formal verification results)
- Manual Validation and Verification Results (e.g., inspection results and review results)
- Source Code (e.g., Ada code or C code)
- Safety Cases (documented argument aimed at providing a compelling, comprehensive, and valid case that a system is safe for a given application in a given operating environment)

16. If you would like to add any further artefact types and the level of automation for performing an impact analysis when they change, please do so in the box below (for example, Artefact type X: fully manual; Artefact type Y: semi-automated recommendations, etc.)

17. For the artefacts used as safety evidence, please indicate the name of the tools that are used for performing an impact analysis when the following artefact types change. If it is a tool developed internally in some organization, please indicate “Internal tool”. If you do not know the tools, please leave the corresponding boxes empty. ^{OR}

System Lifecycle Plans	
Reused Components Information	
Personnel Competence Specifications	
Safety Analysis Results	
Assumptions and Operation Conditions Specifications	
Requirements Specifications	
Architecture Specifications	
Design Specifications	
Traceability Specifications	
Test Case Specifications	
Tool Supported Validation and Verification Results	
Manual Validation and Verification Results	
Source Code	
Safety Cases	

18. If you would like to add any further artefact types and the tools that are used for performing an impact analysis when they change, please do so in the box below (for example, Artefact type X: tool W; Artefact type Y: tool Z, etc.)

19. What tools are used to store the evidence of safety evidence change management? If you do not know the tools, please indicate "I don't know". *

Challenges ^{PR}

When dealing with safety evidence change impact analysis, different challenges can arise and thus hinder this activity. Implicitly, this means that some improvement opportunities exist. You will be asked about these aspects in this section.

20. How often have you faced or observed the following challenges regarding safety evidence change impact analysis? *^{OR}

Frequency:
- Never
- Few projects (i.e., rarely)
- Some projects (i.e., sometimes)
- Most of the projects (i.e., very often)
- Every project (i.e., always)

Challenges:
- Difficulty in estimating the effort required to manage a change
- Too coarse granularity of the traceability between artefacts to accurately know the consequences of a change
- Excessive detail of the traceability between artefacts, making traceability management more complex than necessary for impact analysis purposes
- Unclear meaning of the traceability between artefacts in order to know how to manage a change
- Insufficient traceability between artefacts to accurately know the consequences of a change
- Long time for evaluating the consequences of a change
- Insufficient confidence by assessor or certifiers in having managed a change properly
- Vast number of artefacts to trace
- Insufficient tool support
- Lack of a systematic process for performing impact analysis
- Difficulty in determining the effect of a change on system safety

- Difficulty in deciding if a component can be reused
- Difficulty in assessing system-level impact of component reuse

21. If you would like to add any further challenges, please do so in the box below, and also indicate their frequency (for example Challenge X: every project, very important; Challenge Y: few projects, moderately important, etc.)

22. How do you think that safety evidence change impact analysis could be improved? *

Follow-up studies

23. Please provide the following information if you are interested in participating in follow-up studies.

Name

Organization

Email

Appendix B. Safety Standards

This appendix presents the scope of each individual safety standard mentioned by the respondents of the survey.

Standard	Scope
21 CFR 820	Quality system regulation for medical devices in US
AC 23.1309-1	Advisory circular on system safety analysis and assessment for airplanes
AMC 1309	Acceptable means of compliance for system safety objectives and assessment criteria in aviation
ARP4754	Aerospace recommended practice on guidelines for development of civil aircraft and systems
ARP4761	Aerospace recommended practice on guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment
Def Stan 00-56	Safety management of defence systems in UK
DO-160	Environmental conditions and test procedures for airborne equipment
DO-178	Software considerations in airborne systems and equipment certification
DO-254	Design assurance of airborne electronic hardware
DO-278	Guidelines for communications, navigation, surveillance, and air traffic management systems software integrity assurance
DO-297	Integrated modular avionics development guidance and certification considerations
DO-330	Software tool qualification considerations for airborne software assurance
DO-331	Model-based development and verification supplement to DO-178C and DO-278A
DO-332	Object-oriented technology and related techniques supplement to DO-178C and DO-278A
DO-333	Formal methods supplement to DO-178C and DO-278A
DOD-2167A	Standard for defence systems software development in US
EN 50126	Railway applications - The specification and demonstration of reliability, availability, maintainability and safety
EN 50128	Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems
EN 50129	Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling
EN 50159	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
FAR 25.1309	Federal aviation regulation for equipment, systems, and installations
FDA-510(k)	Regulation on premarket notification for medical devices in US
FDA-515	Regulation on premarket approval for medical devices in US
H ProgSäk	Handbook for software in safety-critical applications by the Swedish Armed Forces
IEC 60601	Standard for medical electrical equipment
IEC 60880	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions
IEC 61226	Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions
IEC 61500	Nuclear power plants - Instrumentation and control important to safety - Data communication

	in systems performing category A functions
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511	Functional safety - safety instrumented systems for the process industry sector
IEC 61513	Functional safety - safety instrumented systems for the nuclear industries
IEC 61850	Measurement of return loss on waveguide and waveguide assemblies
IEC 62138	Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
IEC 62304	Medical device software - Software life cycle processes
IEC 62366	Medical devices - Application of usability engineering to medical devices
IEC 62508	Guidance on human aspects of dependability
ISB 0129	Clinical risk management: its application in the manufacture of health IT systems
ISO 13485	Medical devices - Quality management systems - Requirements for regulatory purposes
ISO 13849	Safety of machinery - Safety-related parts of control systems
ISO 14971	Medical devices - Application of risk management to medical devices
ISO 15998	Earth-moving machinery - Machine-control systems (MCS) using electronic components - Performance criteria and tests for functional safety
ISO 26262	Road vehicles - Functional safety
Mil Std 882	US Department of Defense standard practice for system safety
NAVAIRINST 13034	US Navy flight clearance policies
NPD 8700.1	NASA policy for safety and mission success
OHSAS 18001	Occupational health and safety management systems
UL 1998	Software in programmable components

Appendix C. Information about Tools for Safety Evidence Change Impact Analysis

This appendix presents the main purpose of each commercial tool reported by the respondents of the survey as used for SECIA. The websites have been accessed on Sep 27, 2014.

Tool	Description
Apex	https://apex.oracle.com/i/index.html Web-based software development environment
Artisan Studio	http://www.atego.com/products/atego-modeler/ System modelling tool
ARTIST	http://www.zirconsoftware.co.uk/client-solutions/test-solutions/artist Testing and simulation tool
ASCE	http://www.adelard.com/asce/choosing-asce/index.html Tool for the development and management of assurance cases and safety cases
Axapta	http://www.microsoft.com/en-us/dynamics/erp-ax-overview.aspx ERP solution
Beacon	http://adi.com/pdfs/product/BEACON_DS3.pdf Tool suite for the design, implementation, test, and maintenance of high-integrity embedded systems
Bridgepoint	http://www.mentor.com/products/sm/model_development/bridgepoint/ System modelling tool
CAFTA	http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001024831 Safety analysis tool
Cantata	http://www.qa-systems.com/cantata.html Unit testing tool
Clearcase	http://www-03.ibm.com/software/products/en/clearcase Software configuration management tool
CORE	http://www.vitechcorp.com/products/core.shtml Product design and development tool
Coverity	http://www.coverity.com/products/code-advisor/ Static analysis tool
Design Verifier	http://www.mathworks.se/products/sldesignverifier/ Model analysis tool
Dimensions	http://www.serena.com/index.php/en/products/featured-products/dimensions-cm/overview/ Configuration management tool
DOORS	http://www-03.ibm.com/software/products/en/ratidoor Requirements management tool
Eclipse	http://www.eclipse.org Integrated development environment
Enterprise	http://www.sparxsystems.com.au/products/ea/index.html

Architect	System modelling tool
Excel	http://office.microsoft.com/en-us/excel/ Spreadsheet application
Fault Tree+	http://www.isograph.com/software/reliability-workbench/fault-tree-analysis/ Safety analysis tool
Framemaker	http://www.adobe.com/products/framemaker.html Content management system
GSN Visio Plug-in	http://www.goalstructuringnotation.info/archives/41 Plug-in for GSN modelling with Visio
HP Test manager	http://h71000.www7.hp.com/commercial/decset/brochure.html Software testing tool
Labview	http://www.ni.com/labview/ System design tool
LDRA Testbed	http://www.ldra.com/en/testbed-tbvision Static and dynamic analysis tool
Logiscope	http://publib.boulder.ibm.com/infocenter/rsdp/v1r0m0/index.jsp?topic=/com.ibm.help.download.logiscope.doc/topics/logiscope_version66.html Static analysis tool
Matlab	http://www.mathworks.se/products/matlab/ Interactive environment for numerical computation, visualization, and programming
MKS	http://www.mkssoftware.com Windows/Unix interoperability tool support
NOR-STA	https://www.argevide.com/en/products Assurance case development and management tool
Office	http://office.microsoft.com/en-us/ Office suite
OpenFTA	http://www.openfta.com Fault tree analysis tool
Perforce	http://www.perforce.com Version control software
Polyspace	http://www.mathworks.se/products/polyspace/?s_cid=wiki_polyspace_2 Static analysis tool
PROVEtech:TA	https://www.mbtech-group.com/eu-en/electronics_solutions/tools_equipment/provetechta_test_automation.html Test automation tool
Rational	http://www-01.ibm.com/software/rational/ Software and system lifecycle tool suite
Rational Rose	http://www-03.ibm.com/software/products/en/ratirosefami UML-based development environment
RELEX	http://www.ptc.com/product/windchill/quality/tryout Reliability analysis tool
Reliability Workbench	http://www.isograph.com/software/reliability-workbench/ Reliability, safety, and maintainability analysis tool
Reqtify	http://www.3ds.com/products-services/catia/capabilities/systems-engineering/requirements-engineering/reqtify/ Requirements and system engineering tool
RequisitePro	http://www.ibm.com/developerworks/downloads/r/rrp/ Requirements management tool
Rhapsody	http://www-03.ibm.com/software/products/en/ratirhapfami Software and system collaborative development tool
RTRT	http://www-03.ibm.com/software/products/en/realtime Component testing and runtime analysis tool
SAO	http://www.hiqube.com/(S(0ruk5lskagjinwbv34rhx1ur))/navigation.aspx?top_nav=Discover_Solutions&sec_nav=Product_Showcase&item_name=Software_Asset_Optimization Project management tool
Saphire	https://saphire.inl.gov Probabilistic risk and reliability assessment
SCADE	http://www.esterel-technologies.com/products/scade-suite/ Model-based development environment
SCADE KCG	http://www.esterel-technologies.com/products/scade-suite/generate/qualified-code-generation/ Code generator
Simulink	http://www.mathworks.se/products/simulink/ Tool for multi-domain simulation and model-based design
Sistema	http://www.dguv.de/ifa/Praxishilfen/Software/SISTEMA/index-2.jsp

	Safety integrity software tool for the evaluation of machine applications
SonarQube	http://www.sonarqube.org Code quality management tool
SPARK Examiner	http://didawiki.cli.di.unipi.it/lib/exe/fetch.php/magistralesicurezza/sss/examiner_um_win.pdf Static analysis tool for Ada
Starteam	http://www.borland.com/products/starteam/ Change and configuration management tool
Statemate	http://www-03.ibm.com/software/products/no/ratistat/ Design, simulation, and prototyping tool
STOOD	http://www.ellidiss.com/products/stood/ System modelling tool
SVN	https://subversion.apache.org Software versioning and revision control system
System Weaver	http://systemite.se/content/products-services/systemweaver-platform Software and system lifecycle tool suite
Teamcenter	http://www.plm.automation.siemens.com/en_us/products/teamcenter/ Product lifecycle management tool
Topcased	http://www.topcased.org Software modelling tool
Vector TAE	https://vector.com/vi_test_automation_editor_en.html Test automation tool
VectorCAST	http://www.vectorcast.com/software-testing-products Testing suite
VeroTrace	http://www.verocel.com/products/requirements-traceability/ Requirements management and lifecycle traceability tool
Visio	http://office.microsoft.com/en-us/visio/ Diagram creation tool
Visual Studio	http://msdn.microsoft.com/en-us/vstudio/aa718325.aspx Integrated development environment
Word	http://office.microsoft.com/en-us/word/ Word processor

Appendix D. Information about the Tools for Storing Evidence of Safety Evidence Change Management

This appendix presents the main purpose of each commercial tool reported by the respondents of the survey as sued for storing SECIA evidence. The tools also used for SECIA and thus presented in Appendix C are: Clearcase, Dimensions, DOORS, Excel, MKS, Office, Perforce, Reqtify, SonarQube, SVN, Teamcenter, VeroTrace, and Word. The websites have been accessed on Sep 27, 2014.

Tool	Description
Altarica	http://altarica.fr Formal verification tool
AUTOSAR Builder	http://www.3ds.com/products-services/catia/capabilities/systems-engineering/embedded-systems/autosar-builder/ Tool for modelling, definition, simulation and deployment of embedded systems to automotive electronic control units
Clearquest	http://www-03.ibm.com/software/products/en/clearquest Change management tool
CVS	http://savannah.nongnu.org/projects/cvs Revision control system for software development
eB	http://www.bentley.com/en-US/Products/eB+Insight+Services/ Change management tool
NeCTAR	https://nectar.org.au/home Collaboration and information sharing environment
Polarion	https://www.polarion.com/products/alm/index.php Application lifecycle management tool
PVCS	http://www.serena.com/index.php/en/products/other-products/pvcs-pro/ Version management tool
Safety Manager	https://www.safetyinfo.com/sm-pages/safetymanager.htm Safety assurance management tool
Sharedocs	http://www.elad.co.il/en/Solutions/Pages/DocumentKnowledgeManagement.aspx Document management system
Sharepoint	http://office.microsoft.com/en-us/sharepoint/ Collaboration and content management tool

Synergy	http://www-03.ibm.com/software/products/en/ratisyne Configuration management tool
TFS	http://www.visualstudio.com/products/tfs-overview-vs Source code management tool
VSS	http://msdn.microsoft.com/en-us/vstudio/aa700907.aspx Version control system
Windchill	http://www.ptc.com/product/windchill Product lifecycle management tool