Change Impact Analysis as required by safety standards, what to do?

Authors: Thor Myklebust[1,a], Tor Stålhane[b], Geir Kjetil Hanssen[a] and Børge Haugset[a]
[a] SINTEF ICT,
[b] IDI NTNU

Abstract: Change Impact Analysis related to safety of products and systems is used by companies in many industries and is required by several standards. The International Electrotechnical Commission (IEC) has issued several standards with requirements and guidelines for the establishment of analysis like FMECA (IEC 60812), FTA (IEC 61025), Design review (IEC 61160), HAZOP (IEC 61882), Markov (IEC 61165) and RBD (IEC 61078) but no standard for Change Impact Analysis. Based on the aforementioned standards, a literature study and experience from several projects, this paper proposes a Change Impact Analysis Report adapted to the specific characteristics of the Railway and Process industry domains. The purpose of this paper is to serve as a tool to aid manufacturers in performing a Change Impact Analysis at the appropriate level which will be approved by assessors and certification bodies. This is important since the Change Impact Analysis report is one of the main inputs to the assessor/certification body.
The paper starts by presenting and clarifying relevant terms and definitions, as these differ from standard to standard. The main part of the paper structures and describes the relevant topics for a Change Impact analysis report.
Using the described approach will save time and cost and reduce the risk of having to re-issue the Change Impact analysis, thus ending up with a product having hidden defects. Using the mindset from SafeScrum - a method that introduces elements from agile into safety-related software development, will result in further savings.
This work is part of a series of Railway and IEC 61508 certification projects and the SUSS[2] Research projects.

Keywords: Change Impact Analysis, EN 5012X, IEC 61508, Certification

1 Introduction

Change Impact Analysis (CIA) related to safety of products and systems is used by companies in many industries and is required by several standards. The CIA report (CIAR) is one of the main inputs to the assessor. A standardized CIAR will simplify the work both for the manufacturer and the assessor and will also improve the certification process.

The International Electrotechnical Commission (IEC) has issued several standards with requirements and guidelines for the establishment of analysis like FMECA (Failure mode effect and criticality analysis) [1], FTA (Fault Tree Analysis) [2], Design review [3], HAZOP (Hazard and operability studies) [4], Markov[3]

[1] Thor.myklebust@sintef.no
[2] Norwegian: Smidig utvikling av Sikkerhetskritisk Software. English: Agile Development of safety Critical Software
[3] Copy from IEC 61165: The Markov techniques make use of a state transition diagram which is a representation of the reliability, availability, maintainability or safety behaviours of a system, from which system performance measures can be calculated. It models the system's behaviour with respect to time.

[5] and RBD[4] (Reliability Block Diagram) [6] but no standard for CIA. Based on the above mentioned standards, a literature study, experience from several projects and study of agile methods like Scrum, this paper proposes a CIAR adapted to the characteristics of the Railway and Process industry domains. The purpose of this paper is to serve as a tool to aid manufacturers in achieving a CIA at the appropriate level that will be approved by assessors and certification bodies. We also provide guidelines on how to perform a CIA.

The guidance for an impact analysis plan and report provided in the present paper is intended to be complementary to the standards and plans. The guidance for an impact analysis report will ensure that the manufacturers document the CIAR in such a way that an assessor will accept the report. It will also ensure that the modifications performed are sufficiently thought-through. Several examples exists where this has not been the case, and an inadequate CIAR has resulted in products that either have not been approved or the time before the product was on the market has been delayed with months and even years.

Furthermore, we relate our guidelines for CIA to ongoing work (see www.sintef.no/SafeScrum that is updated on a regular basis) on improving both the development and assessment efficiency for safety critical software by applying principles and techniques from agile software development methods. In particular, we look at Scrum, which has had a large uptake in industry over the past decade. We have proposed the SafeScrum approach which combines the benefits of agile development with the requirements of the IEC61508 standard. In this paper we show how a process like SafeScrum can be used to make CIA more efficient and coupled to the development process, making it more practical and with reduced costs.

The rest of the paper explains our research approach and the research questions we address (section 2). We present an overview of the key concept of the SafeScrum process as a background for our guidelines for CIA (section 3) and then go on to provide an overview of identified requirements for CIA (section 4), followed by requirements in the analysis and review techniques in relevant IEC standards (section 5) and an insight on CIA plans (section 6) and CIA reports (section 7). Finally we summarize and conclude our work (section 8).

Assumptions: It is assumed that a modification/change request report exists.

Terms and definitions: So far there is not an international consensus on terminology related to CIA, and only a few relevant terms are defined in the standards that we have studied. These terms are presented in Table 1 below. The regulations for the European process industry do not have a directive or regulation related to change, while the railway industry has the CSM (Common Safety Method) regulations [7] and [8]. The risk management and risk assessment processes in the CSM Regulation relate to the processes that are put in place for assessing the safety levels and compliance with the safety requirements of any significant change. The CSM on risk assessment shall be applied by the person in charge of implementing the change under assessment. The EN 5012X series [9] and Railway CSM regulations [7] and [8], do not include any of the definitions mentioned in the Table below.

[4] Copy from IEC 61078: A reliability block diagram (RBD) is a pictorial representation of a system's reliability performance. It shows the logical connection of (functioning) components needed for successful operation of the system (hereafter referred to as "system success").

Table 1: List of definitions in different standards and regulations

Term	IEC 61508-4 [10]	ISO 26262-1 [11]	ISO/IEC/IEEE 24765 [12]
Change	Not defined	Not defined	**3.379 Change.** The modification of an existing application comprising additions, changes and deletions.
Modification	Not defined	**1.75 Modification.** Authorized alteration of an item. NOTE 1 Modification is used in ISO 26262 with respect to re-use for lifecycle tailoring. NOTE 2: A change is applied during the lifecycle of an item, while a modification is applied to create a new item from an existing item.	Not defined
Impact analysis	**3.7.5 Impact analysis.** Activity of determining the effect that a change to a function or component in a system will have to other functions or components in that system as well as to other systems.	Not defined	**3.1360 Impact analysis *1.*** Identification of all system and software products that a change request affects and development of an estimate of the resources needed to accomplish the change NOTE This includes determining the scope of the changes to plan and implement work, accurately estimating the resources needed to perform the work, and analyzing the requested changes' cost and benefits.

Limitations: This paper is limited to products and systems such as e.g. a railway signalling system and E/E/E/PES (electrical/electronic/programmable electronic safety-related systems) including railway signalling systems and process industry domains with emphasis on the EN 5012X standards and the IEC 61508 series. Only modification of products delivered by the manufacturer is considered, not modifications of existing products on site.

2 Research method and research questions

We have performed a literature search including a survey of mainly European directives and International and European standards. Relevant directives and information about these directives can be found at www.newapproach.org. The main standardization organizations we searched were ISO, IEEE, IEC and CENELEC. We identified the following regulations, directives and standards: [2-8, 13-19].

The work we have done is related to an ongoing industrially oriented research project (Agile development of safety critical software) were we are developing a new software engineering method for more efficient development and certification of safety critical systems up to safety integrity level 3. This new approach, named SafeScrum [20], is based on the agile software development method Scrum [21] which is extensively used in the software industry. As part of this research effort we have defined the following research questions which are being addressed in this paper:

RQ1: How can we develop a CIAR that ensures that the product is approved by the assessor/certification body?

RQ2: How can agile development improve CIA and the process towards recertification?

3 Agile development of safety critical software

Agile software development is a way of organizing the development process, emphasizing direct and frequent communication, frequent deliveries of working software increments, short iterations, active customer engagement throughout the whole development life cycle and change responsiveness rather than change avoidance. This can be seen as a contrast to waterfall-like models such as the V-model, which emphasize thorough and detailed planning, an upfront design, and consecutive plan conformance. Several agile methods are in use, whereof Scrum [21] is one of the most commonly used. Figure 1 explains the basic concepts of an agile development model.

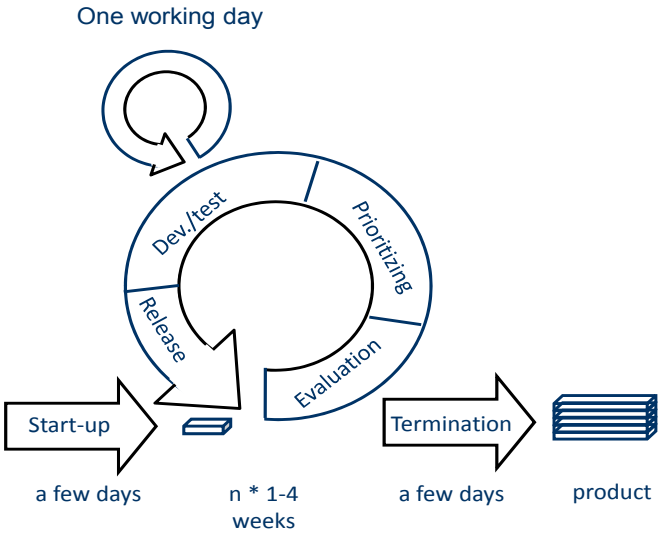

Figure 1: Scrum model

The main constructs of this model are (based on Scrum):

- Initial planning phase is short and results in a prioritized list of requirements for the system called *the product backlog*. Developers also provide *estimates* per item, in essence how much effort it takes to fulfil the requirement.
- Development is organized as a series of *sprints* (iterations) that lasts a few weeks.

- Each sprint starts with a *sprint planning meeting* where the items with the highest priority from the product backlog are moved over to the *sprint backlog* – adding up to the amount of resources available for the period. These requirements will be implemented in the following sprint.
- Each working day starts with a *scrum***,** which is a short meeting where each member of the development team (1) explains what she/he did the previous work day, (2) any impediments or problems that need to be solved and (3) planned work for the work day.
- Each sprint *releases* an *increment,* which is a running or demonstrable part of the final system.
- The increment is *demonstrated* for the customer(s), which will decide which backlog items that have been resolved and which that need further work. Based on the results from the demonstration the next sprint is planned. The product backlog is revised by the customer and is potentially changed / reprioritized. This initiates the sprint-planning meeting for the next sprint.
- When all product backlog items are resolved, all available resources are spent and / or time does not permit further development, the final product is released. Final tests can be run to ensure completeness.

In order to realize some of the proven benefits of agile development, such as better quality, more efficient development and closer involvement of customers, we have proposed a method called SafeScrum [20]. This variant of Scrum is motivated by the need to make it possible to use methods that are flexible with respect to planning, documentation and specification while still being acceptable to IEC 61508 and e.g. EN 50128 (Railway), as well as making Scrum a useful approach for developing safety critical systems. The rest of this section explains the components and concepts of this combined approach.

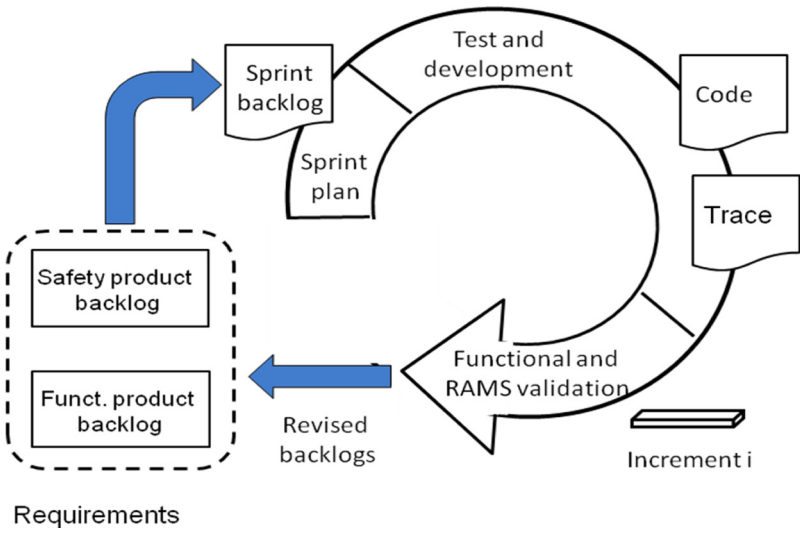

Figure 2: SafeScrum model

Our model has three main parts. The first part consists of the IEC 61508 steps needed for developing the environment description and the SSRS phases 1-4 (concept, overall scope definitions, hazard and risk analysis and overall safety requirements). These initial steps result in the initial requirements of the system that is to be developed and is the key input to the second part of the model, which is the Scrum process. The requirements are documented as *product backlogs.* A product backlog is a list of all of the functional and safety related system requirements, prioritized by the customer or a similar role having the users and/or owners view and interests in mind. It might be practical to also include the developers in the prioritization process. We have observed that the safety requirements are quite stable, while the functional

requirements can change considerably over time. Development with a high probability of changes to requirements will favour an agile approach.

Test-driven development (TDD) is a development practice that embraces the principle of never adding or changing code without first having added or changed the runable test case that verifies its success criteria. The method is popular within the agile community and perceived benefits include having to think about design prior to coding, a safety harness for making changes, and less time spent debugging. In essence TDD has, through studies, been shown to increase quality at the possible expense of productivity [22, 23]. We believe this focus on quality could present a benefit in using TDD for safety-critical software development, and that the increased trust in the code could also benefit the assessment.

4 Agile Change Impact Analysis

We propose a CIA-approach that integrates with the SafeScrum process in two phases. Phase 1 analysis is done upfront of the change implementation process, like the present practice but with more detailed guidelines as described in chapters 7-8. In phase 2, analysis is performed as an integrated part of the SafeScrum process and is thus done iteratively throughout the change process itself. For each item that is selected from the product backlog to enter the sprint backlog (to be implemented in the upcoming sprint) the change impact is evaluated per item by checking whether the change will impact the safety level of the system. This happens at the same time as the requirements (often described as a User Story, i.e. "As a *<role>*, I want *<goal/desire>* so that *<benefit>*") are broken down into a set of smaller tasks that are easier to develop. All these evaluations are logged to keep track of the process and will eventually be added to the CIAR. In cases where a change is found to affect the safety integrity level of the system, a strategy needs to be developed on how to tackle it. This strategy may lead to new items to be added to the backlog to change one or more items in order to avoid a conflict. In the figure below, the different CIA are presented in the SafeScrum model. In this paper only the first CIA is described. Phase 2 will be described in a later paper.

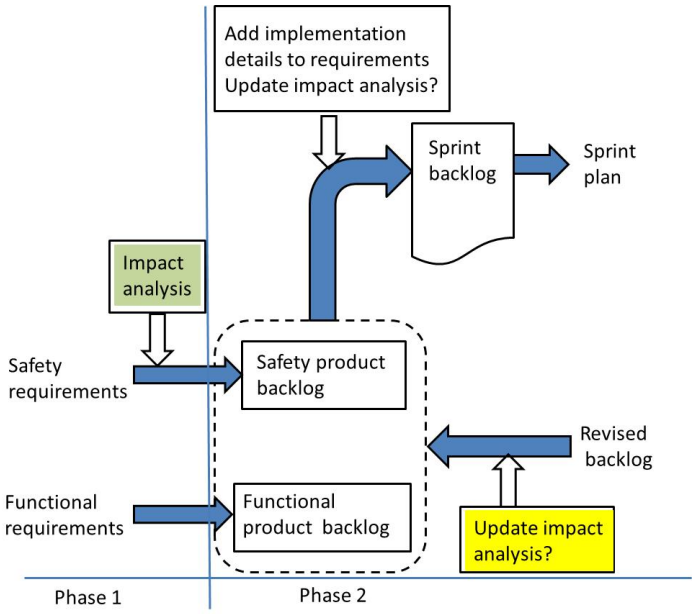

Figure 3: SafeScrum and Change Impact Analysis

5 Important requirements for the analysis and review techniques in relevant IEC standards

The requirements for impact analysis during change are the same in most standards on the development of safety critical systems. The impact analyses requirements in IEC 61508 and in several other standards does, however, not provide any guidance on how this analysis shall be carried out and documented. In one way, this is good, since it is now up to the developers and the assessor to agree on what is needed on a case by case basis, hence opening for methods like SafeScrum to be used. On the other hand, it leaves companies that are new to the trade totally in the dark.

The standards for FTA [2] and FMEA [13] are normally used by the companies developing E/E/E/PES and SIL4 signalling systems. When evaluating relevant chapters for a CIA Report, the following four topics where studied in these six standards [2-6, 13] Experts/teams, Plan, Process and Documentation. Experts/teams and Planning are important for all projects, and our SafeScrum approach emphasize an effective Process and an optimal amount of documentation.

Table 2: Overview of comments to different analysis standards

Topics	Experts/team	Plan	Process	Documentation
HazOp	Selection of a relevant team is an important part of the standard, see e.g. ch. 6.3 in the standard	This is an important part of the standard. What the plan should include is also listed.	A process for the HAZOP is well written and figures are included.	Documentation is presented in ch.6.6 and states that this is one of the strengths by using HAZOP.
FTA	Not emphasized.	Some information is included.	Some information is included.	Requirements for the FTA report are presented in ch. 9.
FMEA	Selection of relevant experts is important part of the standard.	This is an important part of the standard. What the plan should include is also listed.	Some information is included	Requirements for the FMEA report are presented in ch. 5.4.
Design review	Selections of relevant experts (specialists) are an important part of the standard. Top management shall be included.	This is an important part of the standard.	A process for the Design review is well written and a figure is included.	Documentation is mentioned.
RBD	Not emphasized.	Not emphasized.	Not emphasized.	Not emphasized.
Markov	Not emphasized.	Not emphasized.	Not emphasized.	Requirements for the Markov analysis report are presented in ch. 10.

Experts/team: From the table above we see that the HazOp, FMEA and Design review supports our view and experience that selection of a relevant team is important.

Plan: See ch.6 below.

Process: Two of the standards, HazOp and Design review, present a description of the process.

Documentation: No relevant information is presented regarding the right amount of documentation.

6 Change Impact Analysis plan

6.1 The need for a plan for change impact analysis

The European Committee for Electrotechnical Standardization (CENELEC), the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE) have issued a series of standards with requirements and guidelines for the establishment of safety plans (EN 50126-1, Railway), quality plans (ISO 10005) and project plans (ISO 10006). IEEE has also issued a standard for software safety plans (IEEE Std 1228-1994). As mentioned earlier, none of these organisations have issued guidelines or requirements for a CIA plan. The closest we get to this is the work done by OLF[5] with their planning matrix in OLF 070 [24]. This section is an attempt to fill this need.

6.2 On change and risk

During a project's lifetime we often need to change either part of existing code or part of an existing requirement. In many cases, we have to do this irrespective of cost and risk. In other cases there are two questions: (1) what are the costs and risks and (2) what are the benefits and regrets. There are several ways to identify cost, risk, benefits and regrets. We will not discuss these methods here but instead assume that the company in question has appropriate methods for assessment of these four values and the ability to make informed decisions.

The most important item that must be in place for a CIA are traceability information and relevant documentation. Without these CIA will be extremely difficult and costly.

6.3 Needed activities

Changes may relate to behaviour (what the system does), quality (how the system does it) and safety (the risk incurred by putting the system into operation). The CIA process needs to go through the following steps:

1. Use the traceability information to identify artefacts that need to be changed. This will include – but is not necessarily limited to
    a. Code and code documentation
    b. User documentation
    c. Tests and test plans
    d. Earlier relevant analysis – e.g. HazOp, FMEA and CIA for related requirements and system parts.
2. We need to assess the risks related to the planned changes. The risk assessment should also include mitigations for all important risks. In addition, it is important to take into consideration that doing nothing will also carry risks.

[5] OLF: Norwegian OljeIndustriens Landsforening, English: Norwegian Oil and Gas Association (www.norskoljeoggass.no/en)

3. Who shall participate? It is important that we have covered all relevant aspects – e.g. code, testing, user needs and domain knowledge.
4. Decide and plan necessary V&V-activities, e.g. document inspections, unit tests, system tests, user tests. The necessary tests will depend on the artefacts changed and the related risks.
5. Run a retrospective when all the activities have been performed. Important issues to consider:
    a. What worked well
    b. What needs improvement

In addition it might be practical to check whether relevant standards have been changed since the last CIA.

6.4 Special considerations for Scrum development

The diagram in section 4 shows how impact analysis can be used for the backlog content in an organization using Scrum. Note that we might need a new CIA when a requirement is detailed for implementation after it has been taken out of the backlog, or when a requirement is returned to the backlog after it has been rejected by the customer or we have found errors in the implementation.

We recommend that all requirements in the functional product backlog – may be also in the safety product backlog – are formulated as user stories. This will help to make sure that we have information on (1) who: user role, (2) what: goal – what we want to achieve and (3) why: rational for user story requirement. The why-part is important when we want to assess the change's effect on customer satisfaction or on system's safety.

The results from the change CIA can lead to updates of the SRS and we may thus need to change both safety requirements and functional requirements in addition to already written backlog elements.

7 Change Impact Analysis report

Below is a suggestion for a report including chapters and corresponding information presented.

Table 3: Table including an overview of relevant chapters

Chapter	CIA report chapter information
Distribution list	This chapter should be in line with ISO 9001:21008 [11] "*4.2.3 Control of documents…f) to ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the quality management system are identified and their distribution controlled*". This also applies for the safety management.
Names of authors and signatories	No further explanation needed
Revision history including version number	Summarize the change in a few sentences. Version number and date has to be included. This is also a practical information for assessors and employees
Table of content	No further explanation needed
Introduction	Purpose, scope, relevant standards and definitions.

Chapter	CIA report chapter information
Name of participants including information related to competence and experience	Selection of relevant and sufficient number of experts is an important part of an Impact analysis. Even SW may e.g. have influence on EMC performance [25]. This information is often included as part of other chapters in the CIA, e.g. the chapter containing the names of the participants, analysis dates, meeting days, etc.
Any deviations from normal operations and conditions that occur as a result of this change	Failure behaviour related to the change has to be checked. This can be performed as part of e.g. a HazOp. The condition list or e.g. SRAC (safety related application condition) list should be checked.
Re-entry point of lifecycle	It is required by both IEC 61508 and EN 50128 that all changes shall initiate a return to an appropriate phase of the lifecycle. This is normally not a problem for the SafeScrum approach, as the sprints are part of Phase 10 in IEC 61508 and phase 6 in EN 50126 (Railway).
Required verification and validation	Describe the verifications and validation steps required. This can normally be based on the former verification and validation plan. *When applying SafeScrum and the sprints are completed, a final RAMS validation will be done. Since most of the system has been incrementally validated during the sprints, we expect the final RAMS validation to be less extensive than when using other development paradigms. This will also help us to reduce the time and cost needed for certification. A further decrease in assessment cost is expected if test-driven development is used. An extended decrease in assessment cost is expected when test-driven development is used.*
Assessor, certification and authorization aspects	New certification body or assessor? More countries involved that may affect the authorization? Special interpretations of the standards in the new design that should be discussed with the assessor in the beginning of the project?

Chapter	CIA report chapter information
Required document changes	All affected documents shall be updated. The documents that have to be updated should be mentioned in the CIA report. The relevant documents that normally have to be updated are normally listed in the "Document plan", "Safety Case" and/or the "CER[6] ". The CER Method: This method is based on the IEC TRF (Test Report Format) method, as described in Worldwide System for Conformity Testing and Certification of Electrotechnical Equipment and Components (IECEE) guide [26]. The IEC TRF system is intended to facilitate certification or approval according to IEC standards. The TRF and CER method seeks to help industry avoid unnecessary obstacles to trade and to encourage different countries to harmonise their national standards and certification activities
Conclusion/summary	The conclusion of a CIAR has to summarize the content and purpose of the analysis. The conclusions should be precise and straight to the point. The conclusion should also briefly state the implications of these analyses. Why should the assessor believe your result? Show evidence that your result is valid or why it will be valid—that it actually helps to solve the problem you shall solve.
Document references	No further explanation needed

8 Summary

We have studied all relevant standards and identified the need for help in planning, performing and reporting on CIA. Even though this is a common problem, especially for those who are new to a standards regime, the problem is of special interest for companies who want to use Scrum in the development of safety-critical software.

Based on the observations above, we have written a guideline for planning a CIA and reporting of the analyses results. We have also considered and given guidelines for dealing with problems that are relevant when using Scrum for development of safety-critical software. These guidelines are of special importance since they help the developers to incorporate the change impact planning and analysis into the backlog administration. They can thus be included in the Scrum process in a simple, seamless way.

The answer to RQ1 is presented in chapter 7 above.

The RQ2 is answered by dividing the CIA process into phase 1 and phase 2 as described in chapter 4. In addition further information are presented in chapter 6.4 and also as part of V&V and required document changes.

[6] CER: Conformity Evidence Report

9 References

[1] "IEC 60812: Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA), Edition 1," ed, 2006.
[2] "IEC 61025 Fault tree analysis (FTA), ed. 2," ed, 2006.
[3] "IEC 61160 Design review. Ed. 2," ed, 2005.
[4] "IEC 61882 Hazard and operability studies (HAZOP studies) – Application guide. Ed 1," ed, 2001.
[5] "IEC 61165 Application of Markov techniques. Ed. 2," ed, 2006.
[6] "IEC 61078 Analysis techniques for dependability – Reliability block diagram and Boolean methods (RBD). Ed. 2," ed, 2006.
[7] "CSM 352/2009. Commission Regulation 352/2009 on the adoption of ac common safety method on risk evaluation and assessment as referred to in Article 6(3) of Directive 2004/49/EC of the European Parliament and of the Council," ed.
[8] "CSM 402/2013. Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009," ed.
[9] "EN 5012X series. Railway applications," ed.
[10] "IEC 61508: Part 4. Functional safety of electrical/electronic/programmable electronic safety-related systems – Definitions and abbreviations. Ed 2," ed, 2010.
[11] "ISO 26262-1. Road vehicles – Functional safety – Part 1: Vocabulary. Ed. 1," ed, 2011.
[12] "ISO/IEC/IEEE 24765. Systems and software engineering – Vocabulary. First edition ", ed, 2010.
[13] "IEC 60812:2006, Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA), Edition 1," ed, 2006.
[14] "Directive 89/336/EEC Electromagnetic compatibility (EMC)," ed.
[15] "Directive 2004/108/EC Electromagnetic compatibility (EMC)," ed.
[16] "Directive 2006/42/EC Machine directive (MD)," ed.
[17] "Directive 1999/5/EC radio and telecommunications terminal equipment (RTTE)."
[18] "Directive 2006/95/EC Low voltage directive (LVD)," ed.
[19] "Directive 89/106/EC Construction products (CPD)."
[20] T. Stålhane, T. Myklebust, and G. K. Hanssen, "The application of Scrum IEC 61508 certifiable software," presented at the ESREL, Helsinki, Finland, 2012.
[21] K. Schwaber, Beedle, M., *Agile Software Development with Scrum*. New Jersey: Prentice Hall, 2001.
[22] A. Causevic, D. Sundmark, and S. Punnekkat, "Factors Limiting Industrial Adoption of Test Driven Development: A Systematic Review," presented at the IEEE Fourth International Conference on Software Testing, Verification and Validation (ICST), Berlin, Germany, 2011.
[23] H. Munir, M. Moayyed, and K. Petersen, "Considering rigor and relevance when evaluating test driven development: A systematic review," *Information and Software Technology,* vol. ONLINE, 2014.
[24] "Olf 070. APPLICATION OF IEC 61508 AND IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY. Ed.2," ed, 2004.
[25] T. Williams, *EMC for Product Designers*, 4 ed.: Newness, 2007.
[26] "IECEE CB-SCHEME OD- CB2020-Ed.1.7. TRF – Development, maintenance and use," ed, 2010.