The Agile Safety Plan

Thor Myklebust[1], Tor Stålhane[2] and Narve Lyngby[1]

[1]*SINTEF ICT, S.4, 7465 Trondheim, Norway. Email: firstname.last name@Sintef.no*

[2]*IDI NTNU, 7465 Trondheim, Norway. Email:stalhane@idi.ntnu.no*

Objectives: During the last years, there has been an increased use of agile development methods for safety-critical software in order to shorten the time to market, to reduce costs and to improve quality. The Agile Safety Plan forces the Applicant to be specific about the safety process, enabling the Certification Body to be proactive and to plan the work according to the Applicant's schedule.
Moving from a Waterfall/V-model to an agile model affects several parts of the development process. The European Committee for Electrotechnical Standardisation (CENELEC) and the International Organisation for Standardisation (ISO) have issued a series of standards with requirements and guidelines for the establishment of quality plans (ISO 10005), and project plans (see ISO 10006) but no standards for safety plans. The railway safety standard, however, does include a list of topics that shall be included in a safety plan (CENELEC's EN 50126-1).

Methods: In this paper we have analysed the standards mentioned above plus the safety standards IEC 61508 (offshore/process domain) and EN 50128 (railway domain). The acquired information is used to suggest an Agile Safety Plan that satisfies the requirements in these standards and at the same time enables an agile development process.

Results: The purpose of the Agile Safety Plan is to aid Manufacturers in achieving the certification of their products by satisfying the planning requirements using the Agile Safety Plan together with high-level plans and the Sprint planning approach.
The paper starts by presenting and clarifying relevant terms and definitions, as these may differ from standard to standard and especially between the safety domain and the agile domain. The main part of the paper structures and describes the crucial elements of the Agile Safety Plan.

Conclusions: An Agile Safety Plan ensures a good start of the development project, minimized costs and reduced time to market. It also ensures that the safety process is complete and produces sufficient information for the Manufacturer and the Certification Body.

I.Introduction

I.1 On safety and agility

During the last years, there has been an increasing use of agile methods and practices when developing safety-critical software in order to reduce time to market, reduce costs and to improve quality.

Companies introducing agile methods like SafeScrum should also have an Agile Safety Plan (ASP) to get the full benefit of an agile approach and at the same time satisfying relevant safety standards. The ASP may include the Certification plan as presented in [1, 2].

The Agile Safety Plan forces the ISA (Independent Safety Assessor) or CB (Certification Body) to be specific about the safety process, enabling the Certification Body to be proactive and to plan the work according to the Applicant's schedule. The Applicant is normally the Manufacturer in the Oil & Gas domain. In the Railway domain the Manufacturer or the sometimes the Railway authority (Infrastructure Manager) is the Applicant.

All too often, developing companies have started creating a safety plan too late in the project. The reason is often that they believe that a complete knowledge of the project is needed before starting to write the safety plan. This has turned out to be a costly solution. It is much more efficient to build the safety plan by inserting information as it becomes available during project development – an agile approach. This would also strengthen the communication with the ISA and/or the CB. The Agile Safety Plan forces the applicant to be specific about the safety process, enabling the CB to be proactive and to plan its work according to the applicant's schedule.

We have thus started the work to include the safety plan construction into the SafeScrum process. This is part of our general work towards including all or most of the IEC 61508 phases into SafeScrum.

This Agile safety plan satisfies all the requirements mentioned in EN 50126-1:1999 chapter 6.2.3.4 and IEEE std. 1228:1994, which has been used as a basis for EN 50126-1ch. 6.2.3.4.

This paper starts with defining relevant safety terms and agile terms. For further information regarding terms used by assessors, see [3]. We then explain the high-level plans and how we should plan for using the tools. To ensure an effective project we have included the reuse and template approach and finally we present the Agile safety plan topics with the related activities.

Acknowledgements: This work was partially funded by the Norwegian Research Council under grant #228431 (the SUSS project) and SINTEF SEP project Safe Software.

I.2 Definitions

There are some terms that we will use later and thus need to be defined before we go on – Safety Plan, Safety Manual, Sprint and Backlog Refinement Meeting.

Safety Plan: Neither the term nor the concept of a safety plan is used in IEC 61508. We have thus looked to two other standards to find useful definitions.

ISO 26262-1:2011 Safety plan: "*1.112 safety plan: plan to manage and guide the execution of the safety activities (1.104) of a project including dates, milestones, tasks, deliverables, responsibilities and resources*"

EN 50126-1:1999. 3.39 safety plan: "*A documented set of time scheduled activities, resources and events serving to implement the organisational structure, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project*".

Safety manual: This is so far not a concept used in EN 5012x series. However, it will be included in the next edition of this standard series. The concept of a safety manual was introduced in edition 2 of the IEC 61508 series. In IEC 61508-4:2010, section 3.8.17, the term is defined as

"*Safety manual for compliant items document that provides all the information relating to the functional safety of an element, in respect of specified element safety functions, that is required to ensure that the system meets the requirements of IEC 61508 series*".

Sprint: This is a Scrum term used to describe an iteration in the Scrum process. The term is also used in SafeScrum [4]. The sprint is a time-boxed effort and it is restricted to a specific duration. The duration is fixed in advance for each sprint and is normally one to four weeks.

Backlog Refinement Meeting: This is a new concept in Scrum, added due to a perceived need. It is defined by its purpose as follows: The purpose of the backlog refinement meeting is to decompose the highest priority items in the product backlog into user stories, or similar, which are suitable for inclusion in the next sprint. The backlog refinement meeting usually takes place towards the end of the current sprint.

II.High level safety plans

A high-level safety plan helps a project manager (PM), the RAMS or safety manager and the ISA/CB to track project tasks to a budget over time and it allows the PM to keep management informed of progress. A high-level version of a plan is management-oriented and includes an overview over how to satisfy the relevant safety regulations [5] and standards, including concrete safety plan requirements, e.g. the requirements as given in EN 50126-1:1999 ch. 6.2.3.4. Together the Agile Safety Plan, the High Level Safety Plan and the Sprint planning constitutes the main Agile plans.

While the Safety plan should be established in phase two according to EN 50126, the detailed planning is performed as part of the phases 6-8 of IEC 61508, or in Agile planning, as part of the Sprint planning.

Managers generally are concerned with approving a project before its initiation and then tracking it at the executive or program management level e.g. gate approach or similar [6, 7], while the ISA is concerned with how the plan fits to the assessment plan and concrete requirements for a safety plan.

An important topic in the high-level project plan is the expected outcome. A project manager will explain in writing the purpose of a project and highlight the expected benefits. The ISA expects information related to e.g. audits, deliverables like V&V reports and safety cases or similar documents.

The Scrum master role should be mentioned as part of the EN 50126-1:1999 ch. 6.2.3.4: "d) details of roles, responsibilities, competencies and relationships of bodies undertaking tasks within the lifecycle" requirement.

A high-level plan will include future reviews by management. Management will expect to see interim deliverables or accomplishments, e.g. milestones. Gate reviews are designed to allow management to terminate a project or allow it to continue, and they will be scheduled into the high-level plan.

The plan might include a time estimate. Assuming that the PM will deliver something of value, people will be awaiting its delivery. Having a good idea of the delivery date allows the recipients of the project's deliverable to plan ahead for putting the deliverable to use.

The figure below shows the link between the High level safety plan and the Sprint planning.

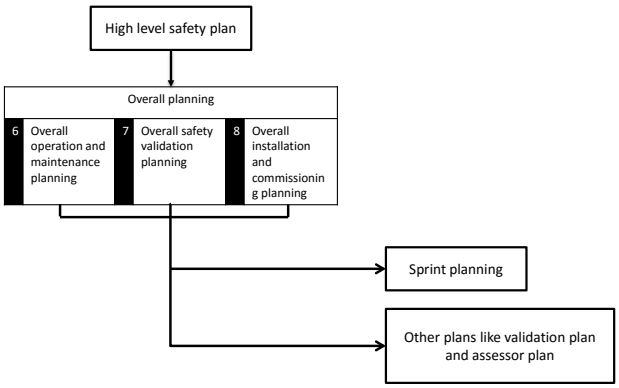

Figure 1: From HLSP to the Sprint planning as part of the "Overall safety lifecycle"

III.Reuse Opportunities and Templates

III.1 Reuse Opportunities

Reuse is important in order to make the work manageable and cost-effective. Reuse should be planned for as an upfront task, i.e. before the first sprint. Reuse of documents and the use of templates have several benefits, e.g.:

- Increased productivity of information and documents
- Reuse of documents and information available as part of the tools
- Reduce duplication effort
- Move information and documents more easily among projects
- Quick and effective process when developing new documents

In the subchapters below, we have first looked at reuse of information and documents while the last chapter look at the use of templates together with the use of other relevant topics.

If a safety product, for which both a safety plan, safety manual and a safety case already exists, is modified, the new documents can be based on the already existing ones. We mainly needs to argue for the changes and their effects. This is considerably less work than producing these three documents every time.

Reusable documents have low extra costs. This is documents where parts are reused as is, while the remaining parts need to be adapted for each project and even for each sprint for some documents. If reuse is the goal right from the start, the changes between projects or iterations will be smaller.

In some cases up to 50% of all project resources has been spent on activities related to the development, maintenance and administration of documents [8]. A customer-case shows potential for a 40% reduction in engineering hours on subsea paperwork [9]. As part of a study of relevant proof of compliance documentation when certifying products according to IEC 61508, we found that more than 50% of the documents can be reusable [10] and that there are significant more documentation work when developing systems with higher SIL [11]. It is important that the manufacturer make these documents generic. For documents that has to be updated over several sprints, reusable documents is important. These documents could e.g. include tables or point lists that are easily updated. Reusability of tests and analysis should also be included in these evaluations – see IEEE 1517:2010. This is also an important part to perform regression in an automatic and effective manner.

III.2 The use of Templates

When doing modification of an already certified product, only a few documents are new [9] e.g. when using new tools. Normally the companies do not change tools often but when moving from Waterfall to e.g. SafeScrum we might expect several changes in the first project. The new documents can be based on templates or reuse or be automatically generated to further reduce documentation costs.
Creating new documents are costly. These documents have to be written more or less from scratch for each new project. We should therefore include the use of already available templates that have been published as industry papers, e.g. [12], or published by organizations developing guidelines like e.g. Misra (www.misra.org.uk) and AAMI (www.aami.org). Some standards, such as ISO/IEC/IEEE 29119-3:2013 includes procedures and templates for reports such as Test status report, Test data readiness report, Test environment readiness report, Test incident report, Test status report and Test completion report. Exida has issued a book [13] that includes a template for the safety manual as required by IEC 61508. The topics for a safety manual are presented in IEC 61508-2 (Annex D) and IEC 61508-3 (Annex D).

As part of the SafeScrum mind set it is important to reduce the amount of documentation and it is assumed that the assessor should be involved early in the project. What could be the minimum of documentation should therefore be discussed with the ISA/CB before starting to develop any new document. Templates could be discussed with the assessor early in the project.

IV.Tools and agile safety planning

Satisfying the safety plan means to satisfy regulators – follow the rules – and the customer – realize the requirements. Two tools are of paramount importance – one needed to satisfy the traceability requirements and one needed to test fulfilment of the functional requirements. Neither activity is doable without tool support. This is true both for agile projects and for any other development organization model.

Testing is important in all software development and even more so in agile development due to the frequent changes in the code. Tests function as a safety net that support code changes – test, change and then test again.

Without a large set of test cases, the probability of introducing new errors during changes would be too high. However, the test – change – test approach requires the developers to run a large set of tests quite often, which would be next to impossible without a testing tool allowing a large degree of test automation. The tool should allow automatic executions and correctness check of the tests.

The safety plan needs to contain tool identifications – which tools are we going to use – and how are we going to use them. The latter include such things as scripts and templates. In addition, we need to categorize and in some cases certify, the tools we use, depending on what they are used for. IEC 61508, part 4, section 3.2.11 use three categories for tools used in software development:

- ***T1****: generates no outputs which directly or indirectly can contribute to the executable code (including data) of the safety related system, e.g. text editor or configuration control tool.*
- ***T2****: supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software, e.g. test harness generator or static analysis tool.*
- ***T3****: generates output, which directly or indirectly can contribute to the executable code of the safety related system, e.g. optimizing compiler where the relationship between the source code program and the generated object code is not obvious or a compiler that incorporates an executable run-time package into the executable code.*

Tools of category T2 and T3 will need a certificate or some kind of assurance that they will not create safety-problems. If we cannot assure the assessors and ourselves that tools of category T2 and T3 are safe, we might need to reconsider our tool use and thus the safety plan for the whole project.

It is also important to be aware of the reduced number of requirements when using limited variable language/programs (LVL), see e.g. IEC 61508-3 chapter G.4 and IEC 61511. LVL can be used as part of the SafeScrum process [14].

V.The Agile Safety Plan

In the table below, we have adapted the requirements given in EN 50126 clause 6.2.3.4 and E.1 in EN 50129 to an Agile approach.

Table 1: Requirements for a safety plan

No.	Requirements (copied from EN 50126 clause 6.2.3.4 and E.1 in EN 50129)	General comments	Agile adaptations
	Requirements for a safety plan from EN 50126 clause 6.2.3.4		
a	The policy and strategy for achieving safety.	Policy: a set of ideas or a plan of what to do in particular situations that has been agreed to officially by a business organization. Strategy: a detailed plan for achieving success in situations such as business.	Policy example: In this project we plan to apply the SafeScrum process. Strategy example: This product shall be developed with only sufficient documentation, still obtaining relevant approvals.
b	The scope of the plan.	In the "waterfall" methodology, you control scope creep through "Change Control". A reference to the contract is therefor often given.	The agile community "embrace change" so one may expect updates of the scope several times during an Agile project. Often the safety requirements are far more stable than the other requirements.

No.	Requirements (copied from EN 50126 clause 6.2.3.4 and E.1 in EN 50129)	General comments	Agile adaptations
c	A description of the system.	It is sufficient and common to refer to a document describing the system.	An incremental development of the design is foreseen while the architecture of the system is defined before the first Sprint.
d	Details of roles, responsibilities, competencies and relationships of bodies undertaking tasks within the lifecycle.	Normally this part includes defining roles like: • Project manager • RAMS manager • Testers • Verificators • Validators • QA roles • Auditors • Assessors	Sprint team and relevant engineers outside the Sprint team should be defined. See also [15] for details regarding QA role as part of the Sprint team.
e	A description of the system lifecycle and safety tasks to be undertaken within the lifecycle along with any dependencies.	Mention the waterfall and e.g. the V-model.	One may e.g. mention parts of waterfall that are applied and the SafeScrum process. See also [16] regarding important considerations when applying other models than the waterfall/V-model.
f	The safety analysis, engineering and assessment processes to be applied during the lifecycle, including processes for:	-	-
f.1	ensuring an appropriate degree of personnel independence in tasks, commensurate with the risk of the system;	See d above. The required degree of personal independence differs among the different domains.	See d above. Parts of the risk evaluations can be agile [18] but much of the risk work is performed before the first Sprint.
f.2	hazard identification and analysis;	Often based on already existing hazard logs from both the manufacturer and the purchasing company together with new hazard identification analysis. The core hazard for the ETCS (European Train Control System) for the reference architecture is defined as (Subset 091): *Exceedance of the safe speed / distance as advised to ETCS.*	Agile CIA (Change Impact Analysis) is described in [19] and they may result in new hazards. See also [21] regarding safety stories.

No.	Requirements (copied from EN 50126 clause 6.2.3.4 and E.1 in EN 50129)	General comments	Agile adaptations
f.3	risk assessment and on-going risk management;	This is project and product dependent. Project risk and predictive analysis to identify risks and opportunities are assumed to be taken care of as part of the Project plan.	Using existing generic and domain specific information it is possible to get an early start on safety analysis. This is important since architectural decisions made early in a project – agile or not – are expensive to change later. E.g. FMEA (Failure Mode and Effect Analysis) and its variants IF-FMEA works well in an agile setting [19] and [18].
f.4	risk tolerability criteria;	This is domain and cultural dependent. The tolerability is decided by regulations in the railway domain.	-
f.5	the establishment and on-going review of the adequacy of the safety requirements;	This is also dependent on the contract between the manufacturer and the purchasing company.	This may be performed as part of e.g. the "Backlog Refinement Meeting" also named "Backlog grooming".
f.6	system design;	See CLC/TR 50506-2:2010 for informative information.	Incremental design development. This also require a thorough configuration management plan [16]
f.7	verification and validation;	A reference to V&V plans are normally included.	Specify which parts of the verifications that are performed as part of the Sprints.
f.8	safety assessment, to achieve compliance between system requirements and realisation;	The assessor has a duty to answer questions related to clarification of safety standards and regulations.	Communication with the assessor is important.
f.9	safety audit, to achieve compliance of the management process with the safety plan;	ISO 19011:2011 "Guidelines for auditing management systems" is also of help when planning and performing safety audits.	See comments to p below.
f.10	safety assessment to achieve compliance between sub-system and system safety analysis.	See CLC/TR 50506-2 for informative information.	-
g	Details of all safety related deliverables from the lifecycle, including:	-	-

No.	Requirements (copied from EN 50126 clause 6.2.3.4 and E.1 in EN 50129)	General comments	Agile adaptations
g.1	documentation	The latest edition of ISO 9001:2015 is more goal-based when it comes to documentation. E.g. one of the most important objectives in the revision 2015 is the amount and detail of documentation required to be more relevant to the desired results of the organization's process activities. ISO 9000:2015 clause 3.8.5 gives the following examples: paper, magnetic, electronic or optical computer disc, photograph and master sample	Discuss with the assessor which documents that are relevant and what e.g. can only be information as part of databases and tools [9].
g.2	hardware	See CLC/TR 50506-2 for informative information. Hardware components can be split in two major parts: Components with Inherent Physical Properties (see EN 50129, C.7), and Programmable Components or Devices.	Hardware can be developed using an Agile approach, for further information see www.infoq.com/articles/hardware-can-be-agile.
g.3	software	See CLC/TR 50506-2 for informative information. Two of the author's have experienced in several projects that within the railway domain, often the required "software assessment report" is not mentioned.	Regarding development of safety-critical software, see http://safescrum.no/
h	A process to prepare system Safety Cases	In the railway domain normally a short information is presented together with e.g. a figure showing the different documents resulting in a SASC (Specific Application Safety Case).	The safety case should preferably be developed incrementally. For further information see [20].
i	A process for the safety approval of the system	Description of the approval process. This varies between the different domains.	- Communication with all relevant stakeholder is important.
j	A process for the safety approval of system modifications.	Ensure that evidence must be provided that the modifications have not adversely affected the safety properties of the unmodified rest of the system.	Agile CIA is described in [19].

No.	Requirements (copied from EN 50126 clause 6.2.3.4 and E.1 in EN 50129)	General comments	Agile adaptations
k	A process for analysing operation and maintenance performance to ensure realised safety is compliant with requirements.	See e.g. information related to "safety qualification tests" in CLC/TR 50506-2.	We may foresee that having an Agile approach it should be more convenient to update the software if necessary.
l	A process for the maintenance of safety-related documentation, including a Hazard Log.	See CLC/TR 50506-2 for informative information.	For further information see [10] and [20]. UIC (the worldwide railway organization) has published a template for the Hazard Log at www.uic.org/cdrom/2007/02.../docs/.../generic_hazard_log_template_v7.0.pdf
m	Interfaces with other related programmes and plans.	No further comments needed.	Communication is an important part of an Agile approach.
n	Constraints and assumptions made in the plan.	Be aware of the fact that sometimes different constraints and assumptions are mentioned several places in the SC.	-
o	Subcontractor management arrangements.	See CLC/TR 50506-2 for informative information.	The Norwegian Agency for Public Management and eGovernment has issued guidelines for agile contracts. For further information, see www.anskaffelser.no/verktoy/smidigavtalen-ssa-s
p	Requirements for periodic safety audit, safety assessment and safety review, throughout the lifecycle and appropriate to the safety relevance of the system under consideration, including any personnel independence requirements.	See CLC/TR 50506-2 for informative information.	It is important to establish a strategy for the safety reviews [10]. Safety audits performed by the assessor should be part of the communication plan between the assessor and the supplier.
	Techniques and measures to be covered by a safety plan according to the informative table E.1 of EN 50129. An application Guide for this table is presented in CLC/TR 50506-2 (Table 9).		
E.1.1	Checklists. A checklist of activities and items to be produced. Recommended for all SIL classes	No further comments needed.	-
E.1.2	Audit of tasks. Recommended for SIL 1 and 2; Highly Recommended for SIL 3 and 4	No further comments needed.	-

No.	Requirements (copied from EN 50126 clause 6.2.3.4 and E.1 in EN 50129)	General comments	Agile adaptations
E.1.3	Inspection of issues of documentation. For SIL 1 and 2: documents agreed between railway/safety authority and industry. For SIL 3 and 4: *all documents*	Whether communication with the safety authority is necessary is strongly domain dependent.	Communication with the relevant decision-makers regarding the documentation is of crucial importance and one of the corner stones of an Agile approach. See also [10].
E.1.4	Review after change in the safety plan. Highly Recommended for all SIL classes	No further comments needed.	It is important to establish a strategy for the safety reviews [10].
E.1.5	Review of the safety plan after each safety life-cycle phase. Highly Recommended for all SIL classes	Regular updates are normal but even in "Waterfall" projects, different parts of the development team may work in different lifecycle phases.	Whether an update in necessary can be discussed as part of the sprint planning. See also [10].
	Topics not mentioned in current editions of EN 50126 or EN 50129		
	A process to prepare the Safety Manual(s)	This work can preferably be coordinated together with the preparation of the Safety case.	We are in the process of developing an Agile Safety Manual.

VI.Conclusions

VI.1 General conclusions:

An Agile Safety Plan ensures a good start of the development project, minimizing costs and reduced time to market. It also ensures that the safety process is complete and produces sufficient information to be developed by the Manufacturer and reviewed by the Certification Body.

The requirements for a safety plan using EN 50126 clause 6.2.3.4 as a basis is possible. Only requirements for a safety manual is added in addition to the requirements in EN 50126.

VI.2 Suggestions for improvements of current safety standards are:

- IEC 61508 should include requirements for a safety plan and safety case. The safety plan requirements could be similar to EN 50126-1:1999 ch.6.2.3.4 requirements and the SC requirements could be similar to the requirements for a SC in ISO 26262-2.
- EN 50128 should include requirements for a safety manual. The safety manual requirements could be similar to the IEC 61508 requirements for a safety manual.

REFERENCES

1. T. Myklebust. Certification plan for development of safety products. PSAM11/ESREL2012. Helsinki June 2012.
2. T. Myklebust. Certification of safety products in compliance with directives using the CoVeR and the CER methods. ISSC, Boston MA august 2013.

3. T. Myklebust. Terminology for safety assessors related to Findings. SINTEF Memo 90513021-NOT-2010-01. Edition 2.0, 2013-02-27
4. T. Stålhane, T. Myklebust and G. Hanssen. The application of Safe Scrum to IEC 61508 certifiable software. PSAM11/ESREL 2012. Helsinki June 2012.
5. T. Myklebust. SINTEF Memo: Use of the CER(tify) method and CER templates for the IEC 61508:2010 requirements. 2013-04-10
6. D. Karlstrom and P. Runeson. Combining Agile Methods with Stage-Gate Project Management. IEEE Software 2005.
7. C. Wallin, F. Ekdahl and S. Larsson. Integrating Business and Software Development Models. IEEE Software 2002.
8. T. e. a. Wien, "Reducing Lifecycle Costs of Industrial Safety Products with CESAR" presented at the Emerging Technologies and Factory Automation (ETFA), Bilbao, Spain, 2010.
9. T. Myklebust, T. Stålhane, G. K. Hanssen, T. Wien and B. Haugset. Scrum, documentation and the IEC 61508-3:2010 software standard. PSAM 12 Hawaii 2014
10. DNVGL-RP-0101 Recommended Practice. Technical documentation for subsea projects. Ed. June 2016
11. T. Myklebust, T. Stålhane and B. Haugset. Software development cost related to different SILs in an agile development environment. ISSC 2015 San Diego.
12. T. Myklebust, T. Stålhane, G. K. Hanssen and B. Haugset. Change Impact Analysis as required by safety standards, what to do? PSAM 12 Hawaii 2014
13. Exida book. Functional safety – An IEC 61508 SIL 3 compliant development process, 3rd edition, 2014.
14. T. Myklebust, T. Stålhane and N. Lyngby. An Agile Development Process for Petrochemical Safety Conformant Software. RAMS Symposium, Tucson USA 2016
15. G. K. Hanssen, B. Haugset, T. Stålhane, T. Myklebust and I. Kulbrandstad. Quality Assurance in Scrum Applied to Safety Critical Software. XP 2016 Edinburgh
16. T. Stålhane and T. Myklebust. The role of CM in Agile development of safety-critical software. SafeComp/SASSUR 2015. Delft, Netherlands.
17. Myklebust, T. Stålhane and G. K. Hanssen. Important considerations when applying other models than the Waterfall/V-model when developing software according to IEC 61508 or EN 50128. ISSC 2015 San Diego.
18. T. Stålhane and T. Myklebust. Agile Safety Analysis. XP 2016 Edinburgh
19. T. Stålhane, G. K. Hanssen, T. Myklebust and B. Haugset. Agile change impact analysis of safety critical software. SafeComp_Sassur, 2014
20. T. Stålhane and T. Myklebust. The Agile Safety Case. ASSURE SafeComp Trondheim 2016
21. T. Myklebust and T. Stålhane. Safety stories – A New Concept in Agile Development. SafeComp, Trondheim 2016.