Purchasers and integrators of safety components and products, which information should they ask for?

Thor Myklebust[a] and Tor Stålhane[b]
[a] SINTEF Digital, Trondheim, Norway, thor.myklebust@sintef.no
[b] NTNU IDI, Trondheim, Norway, stalhane@ntnu.no

Abstract: Several manufacturers of safety products and safety systems have to purchase and integrate components and products produced elsewhere and sometimes for another environment or use. Examples of components and products that manufacturers integrate are semiconductors, libraries, openSafety protocols, COTS (Commercial Off-The-Shelf) software and hardware, sensors, and valves.

One could divide this integration into three categories: components and products having a (1) SIL (Safety Integrity Level) compatibility certificate, (2) integrator and supplier have DIA (Development Interface Agreement) or similar, and (3) COTS and EooC (Element out of Context) or similar.

This paper focuses on suppliers delivering components or products, including a SIL compatibility certificate and six other relevant documents (safety manual, safety case including safety-related application conditions (SRAC) and hazard log, safety assessment report, certificate report, and user manual). We starts with an explanation of the relevant documents and which safety standards including such documents.

This paper aims to aid purchasers and integrators with the purchasing process. Speed to market is the key to success. Having the knowledge and experience related to these documents implies less work for the manufacturer and earlier approval by certification bodies (CB).

We have found that not having experience using these documents has resulted in inferior contracts, delays, design challenges, and not having the relevant information available at the right time.

Using the described approach will save time and cost and reduce the risk of not having all the relevant information available for the engineers. An example is, e.g., an SRAC solved by the manufacturer by describing a solution in the user manual instead of having a sufficiently good design. Due to the SRAC, the design is acceptable from a safety point of view. The design is acceptable for the CB but may not be acceptable for the purchaser. We have also included some advice related to projects including an agile and DevOps approach.

1. INTRODUCTION

This paper aims to aid purchasers and integrators with the purchasing process. Time to market is the key to success. Having the knowledge and experience related to these documents implies less work for the manufacturer and earlier approval by certification bodies.

The paper focuses on suppliers of components or products, including a SIL/ASIL (Automotive SIL) compatibility certificate and six other relevant documents (safety manual, safety case including safety-related application conditions (SRAC) and hazard log, safety assessment report, certificate report, and user manual). We start with an explanation of the relevant documents and which safety standards include requirements for such documents.

Without a complete understanding of these documents, the integrators may experience project delays, design challenges, and not having the relevant information available at the right time. Using the described approach will save schedule time and cost and reduce the risk of not having all the relevant information available for the engineers.

2. BACKGROUND

2.1. Relevant safety standards

We have based this paper mainly on the safety standard series IEC 61508 (generic), ISO 26262 (automotive) and EN 5012X (railway). Safety standards do not include any information related to certification. As a result, they do not include requirements for certificates and certificate reports. Some domains have requirements and guidelines for such documents.

SIL/ASIL compatibility certificate and the corresponding certificate report are intentionally not part of safety standards.

Table 1: Overview of three safety standards and relevant documents

Documents/Standards	IEC 61508	ISO 26262	EN 5012X
Safety manual	Required and described in Part 2 and Part 3.	Not mentioned	Not mentioned
Safety case	Not mentioned. Planned to be mentioned in the next edition of the standard	Required	Required
Safety-related application conditions (SRAC)	Not mentioned	Not mentioned	SRAC is an important part of the safety case
Hazard log	Not mentioned	Not mentioned	HL is an important part of the safety case
Safety assessment report	Not mentioned	Required	Required
User manual	Required but not used the term "user manual"	Required but not used the term "user manual"	Required but not used the term "user manual"

2.2. Relevant components and products

In the description below we have only included comments related to libraries and semiconductors.

2.2.1 Libraries

Challenges with software libraries – three views and a recommendation: First and foremost – what is a software library? We will use the definition supplied by Technopedia, which runs as follows:

“A software library is a suite of data and programming code that is used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software.”

Libraries are important. They let the developers reuse solutions to a lot of problems within a wide range of applications areas – from mathematics to text analysis. There are, however, two problem areas, both related to updates. We will discuss them both below.

The developers’ point of view is as follows:
Somebody uses the library in a wrong or unanticipated way – mostly using some unintended functionality – to circumnavigate a problem. Then somebody fixes the error / problem in the library and

after this fix everything goes wrong. Another, related problem is that the developers and the customer use different version of the same library.

Another, related problem is that the same library may exist in different versions, depending on operating system and computer hardware. As a result, we do not just know the library's version but also the operating system it will work with and the hardware it will run correctly on. If this information is not available, you might get from the library provider. Otherwise, you might head "full throttle" into trouble.

However, as we see from the graph below, which is the result of a survey of 13 Norwegian software companies; libraries are not a major concern for the developers when it comes to software errors.

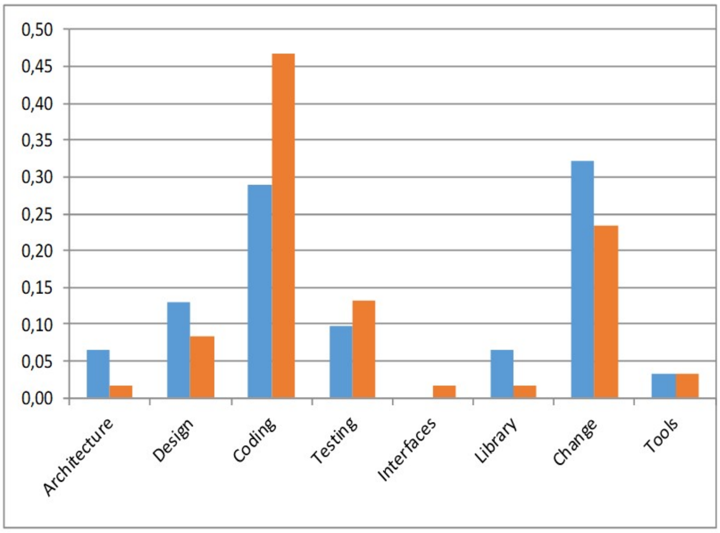

Figure 1: Knowledge based problem areas identified by software developers (blue: safety and security, orange: other)

Another problem is that some libraries are no longer maintained. This is a serious problem, especially since you will not know whether it is updated or not. If we no longer trust the library or those who maintain it, we need to change to another library, which might be a costly affair. In addition, new and better libraries will sometimes be released.

Developers also use libraries for another purpose – to test the applications that they develop. There are e.g., libraries that can be used to build and administer test cases, such as PractiTest [9] and "The Industrial Self-test library" for IEC 61508 [10]. Even though these libraries are not included in any delivery, they my still need to be controlled since they – like all other libraries – will undergo periodic changes.

The release mangers' point of view is different. They have observed that many libraries change all too often – mostly due to new security fixes. The company that releases the software needs to decide whether the new fixes are needed. However, it may give you a bad image in the marketplace if there are known security holes that are not fixed, even if they do not influence your product. This will, however, depend on how critical the security problem is. The increasing focus on security has, all in all, increased the cost of using and maintaining libraries.
In the general case - when using libraries in a system you have two choices:

- Include the libraries in the system at delivery
- Assume that the customer already has these libraries

The first one is the safer choice, but it may get you into trouble if you miss the newest version.

When you buy a software system, you need to check the following

- Which libraries are used – i.e., code not part of the delivered source code? Note that this includes not only the libraries that are explicitly included but also all libraries that are included by the libraries used. The list of indirectly included libraries may be long
- When were they updated and by whom?
- Which updates were included – source and purpose?

If the system shall be certified, all the libraries also need to be part of the certification. This might be a challenge since some of the libraries that are in use are not developed and maintained by companies but by enthusiastic individuals on a voluntary basis.

2.2.2 Semiconductors

Semiconductors are crucial components of electronic devices. The complexity and sophistication of especially the automotive technology keep presenting new challenges for all chipmakers, including MCU (Micro Controller Unit) companies. Safety is an important requirement of the increased use of semiconductors, and ensuring safe vehicles is a massive undertaking. Semiconductors are included in safety parts such as automatic driving assistant systems, e.g., automatic lane-keeping system. Safety standards include different names for semiconductors, microcontrollers, and "similar" components. See table below.

Table 2: Overview of three safety standards and semiconductors

Standards	Copied from the standard
IEC 61508-2:2010 generic functional safety	Copy from the standard: NOTE This standard does not contain specific requirements relating to the avoidance of systematic faults during the design of mass-produced electronic integrated circuits such as standard microprocessors. This is because the likelihood of faults in such devices is minimised by stringent development procedures, rigorous testing and extensive experience of use with significant feedback from users. For electronic integrated circuits that cannot be justified on such a basis (for example, new devices or ASICs (Application Specific Integrated Circuits)), the requirements for ASICs (see 7.4.6.7 and informative Annex F) will apply if they are to be used in an E/E/PE safety-related system. Annex E (normative) Special architecture requirements for integrated circuits (ICs) with on-chip redundancy. Annex F (informative) Techniques and measures for ASICs – avoidance of systematic failures Several improvements will be included in the next edition of IEC 61508. There will be different classes of semiconductors and "ASIC" will be replaced by "semiconductor" in some cases and ICs (Integrated Circuits) in other cases.
ISO 26262-11:2018 Automotive [13]	Par 11 includes: Guidelines on application of ISO 26262 to semiconductors. Copy from the standard: *The semiconductor component can be developed as a SEooC, as described in ISO 26262-10 [12]. In this case, the development is done based on assumptions on the conditions of the semiconductor component usage, and then the assumptions are verified at the next higher level of integration considering the semiconductor component requirements derived from the safety goals of the item in which the semiconductor component is to be used.*
EN 50129:2018 Railway	This safety standard includes an annex F named: Guidance on User Programmable Integrated Circuits (UPIC). UPICs are commonly defined by the following acronyms: • FPGA (field-programmable gate array) • PLO (programmable logic device) • EPLD (erasable programmable logic device) • CPLD (complex programmable logic device) • PAL (programmable array logic) • PLA (programmable logic array) • LCA (logic cell array).

When purchasing safety critical processors or similar, the purchaser should require that a safety manual, a safety case and a safety assessment report are included. Sometimes the FMEDA (Failure Modes Effects and Diagnostic Analysis) report is also of importance. If a safety report and a safety assessment report are not available, one should ask for a copy of the certificate and the corresponding certificate report issued by a certification body.

3. WHICH SAFETY INFORMATION SHOULD BE ASKED FOR?

In this chapter we describe SIL/ASIL compatibility certificate and six other relevant documents (safety manual, safety case including safety-related application conditions (SRAC) and hazard log, safety assessment report, certificate report, and user manual). Other relevant documents are mentioned in the Annex A of the book "Functional safety and proof of compliance" [3]. In addition, the offshore industry in Norway have listed relevant supplier documents in their Annex E.3 [4].

3.1. Safety manual

The safety manual shall describe the guaranteed safety properties and the limitations of the product and guide the users in product installation, commissioning, operation and maintenance. The 2010 edition of IEC 61508 introduced the Safety manual approach. The safety manual 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".

Requirements for the content of the safety manuals are presented both in IEC 61508-2:2010 - Hardware part of the requirements – and IEC 61508-3:2010 – Software part of the requirements.

Table 3: Content list for safety manuals

IEC 61508-2:2010 hardware safety manual content list	IEC 61508-3:2010 software safety manual content list
• a functional specification of the functions capable of being performed • identification of the hardware and/or software configuration • constraints • failure modes • failure rate • failure modes detected by diagnostics • failure modes of the diagnostics • diagnostic test interval • the outputs of the compliant item initiated by the internal diagnostics • periodic proof test and/or maintenance requirements • for those failure modes, in respect of a specified function, that are capable of being detected by external diagnostics, sufficient information shall be provided to facilitate the	• the element shall be identified and all necessary instructions for its use shall be available to the integrator. • the configuration of the software element, the software and hardware run-time environment the configuration of the compilation / link system • assumptions • the minimum degree of knowledge expected of the integrator of the element should be specified, • Degree of reliance placed on the element: Details of any certification of the element, independent assessment performed, integrity to which the integrator may place on the pre-existing element. This should include the integrity to which the element was designed, the standards that were followed during the design process, and any constraints passed to the integrator which shall be implemented in support of the systematic capability claimed. • Installation instructions • The reason for release of the element: Details of whether the pre-existing element has been subject to release to clear outstanding anomalies, or inclusion of additional functionality. • Details of all outstanding anomalies should be given,

IEC 61508-2:2010 hardware safety manual content list	IEC 61508-3:2010 software safety manual content list
development of an external diagnostics capability. • the hardware fault tolerance • type A or B • Systematic capability • any instructions or constraints relating to the application of the compliant item,	• Details of whether the element is compatible with previous releases of the sub-system, • Compatibility with other systems • Element configuration • Change control • Requirements not met • Design safe state • Interface constraints • Details of security measures • Configurable elements • All claims shall be justified • The supporting evidence that justifies the claims in the safety manual for compliant items is distinct from the element safety manual.

The purpose of a safety manual for a compliant item is to document all safety related information related to the item. This is required to enable the integration of the compliant item into a safety-related system, a subsystem or an element, to comply with the requirements of this standard. The safety manual is not mentioned in EN 5012x series or the ISO 26262 series. However, the safety manual is still important, especially at the GP (Generic Product) level since designers and integrators of products, equipment or systems need the information presented in the safety manual to ensure that the integration can be performed without compromising safety. Our experience is that the integrator often also needs a copy of one or more of the references in a safety manual. A mini survey of safety manuals shows that they consist of 100-200 pages.

3.2. Safety case

A safety case is a set of arguments to show that a system is safe. It is not a proof, just a set of arguments like what a lawyer would use in a criminal case.

The purpose of a Safety Case is to develop structured arguments supported by evidence, intended to justify that a product or system is acceptably safe for a specific application in a specific operating environment

A safety case has the following components:

- The purpose of the safety case – usually “The system is safe because…” What follows after “because” is the safety case.
- A description of the environments where the safety case is valid – the operational design domain (ODD). This is an important part for two reasons. It shows the requirements that the environment needs to fulfill, and it shows which changes to the environment that will make the safety case no longer sufficient.
- Intended use of the product or system
- Modern systems are increasing the use of detectors to detect potentially dangerous situations related to e.g., heat, movement, or vibrations. If the system has a set of sensors, it is important to document what the system’s sensors will be able to detect and how it will react to the detections. In the automotive domain this is called OEDR (Object and Event Detection and Response).
- A set of arguments that support the statement that the system is safe, such as “We have found all potential problems”
- A set of proofs that the arguments hold. Remember to include any assumptions made.
- Documentation that the necessary jobs have been done and that they have been done by competent people with the right tools.

- Hazards that should be transferred to the integrator or the operator
- SRAC – Safety Related Application Conditions – under which conditions is it safe to use the system.

A safety case that is useful to a buyer or operator must provide documentation that all the safety case components listed above are present and correct. In addition, it is important to check the assumptions, limitations and SRACs made to make sure that they do not have implications that you cannot accept.

There are several ways to present a safety case. It can be written as pure prose, as structured text or using a graphical notation. In order to be easy to maintain, the authors should use references to already existing documents whenever possible.

3.3. Safety assessment report

There is no internationally accepted common template for SARs even though this would have greatly helped when cross-accepting safety cases. The railway standard EN 50129 includes a list of relevant safety case chapters. Transportstyrelsen in Sweden has published a letter titled "Requirement on the content of an assessment report" which is simple, pragmatic and easy to follow when the SC has been developed according to EN 50129. The main principle is that the SAR shall have a one-to-one link to the SC, consequently having the same chapter headings as the SC.

The SAR should be checked for assumptions, constraints, intended use and limitations. In some cases, also the independence and competency of the assessor(s) should be evaluated, e.g. when they are not accredited. Also have in mind that there might be SRACs that are accepted by the assessor but may not be accepted by the integrator and/or the operator. This could e.g., be SRACs that limits the use of the product or make use of the product in a too detailed procedural manner.

3.4. Certificate

The certificate report presents the information from the certification that has been performed. A certification body normally issues a certificate. The certificate normally consists of only one page and states compliance with one or more standards.

Product certification is often required in sensitive industry and marketplace areas where a failure could have serious consequences, such as negatively affecting the health and welfare of the people or person using that product. This has also become more relevant due to security issues.

The certificate includes information about the manufacturer, the product or system, which standards the product or system comply with and the name of the certification body, including signature(s). In addition, the certificate includes a reference to the certification report and the logo of the certification body.

It is important to evaluate the certificate and the corresponding certificate report issued by the certification body. If an accredited certification body has performed the product or system assessment a logo from an accreditation body should appear on the certificate together with the logo from the certification body.

Figure 2: Example of a logo from an accreditation body (USA, Norway, France and China)

The railway domain issues three types of certification level documents [5], EC Certificates, QMS-Approvals and Intermediate Statements of Verification.

The certificates also include the edition of the certificate and for how long time the certificate is valid. If relevant, the certification body states the SILx or ASILx capability on the certificate.

3.5. Certificate report

The purchasers and integrators have to carefully read the certificate report, especially if the suppliers do not supply a safety case and a safety manual together with the certificate report.

A review of 15 certification reports issued by five certification bodies shows a more or less common set of chapters for certificate reports:

- Introduction including scope, assignment, and work method
- Definition of product or system
- References including relevant standards (and which edition of the standards), certification body procedures, and documents issued by the manufacturer
- Summary of activities performed
- Conclusions

The purchaser should study the certificate carefully regarding configurations, assumptions, user limitations, operational conditions, and SRACs. See also comments to the safety case above. Normally, the certificate reports include far less information than a safety case.

3.6. User manual

User manuals are important, even though many of them are seldom used. A sign on the wall of a room for a company's developers says it all: "In case of outmost despair – read the manual"

The most important issue when reading a system's use manual is to look for clues that the development company has discovered problem late in the process and instead of fixing them in the code they have "fixed" them in the manual. Watch out for sentences such as "Do not use function X after having used function Z if the status variable A is less than 6". There are two issues to consider here:

- Statements such as the one above is really an attempt to fix an error in the manual instead of fixing the software code.
- If this error remains in the system, what other errors are lurking in the dark corners of the program code?

Other important issues when assessing a manual as part of buying a system are:

- It is written in a plain, simple language. There are two reasons for this requirement – it makes it (1) easy to use and (2) difficult to hide the bad news, for instance that a function only works under another operating system that yours.
- It must be adapted to your operating system and to the level of expertise of the intended users. Both too noddy and too advanced manuals will get you into trouble.

Vermeulen [1], who write about the ISO 20607:2019 "Safety of machinery — Instruction handbook — General drafting principles", has formulated it as follows:
"ISO 20607 emphasises that the instruction handbook must be comprehensible and that the use of standardised terms, recognisable technical terms and explanations of terms that are necessary to use is the way to meet this requirement. Also, the handbook must be as simple and as brief as possible. This can for example be achieved by enhancing text with pictograms and drawings, the use of simple sentences and avoiding the use of synonyms"

How the manual is produced may also be of some interest. If it was written at the end of the development project, important information may be missing because it is no longer on the developers' agenda. If it was done the agile way – in parallel with the software development – the writing process will allow for the following important issues [2]:

- Customer involvement early in the development process
- Customers will be influencing the software design, particularly of the user interface
- There will be a close interaction between customers and developers, testers, usability, and other development roles

To sum up – when buying a software system – remember that a modern car has more than 100.000 lines of code [11] – check the following points for the user and installation manuals:

- Is it adapted to your hardware and operating system?
- Is it easy to read – plain simple language and terms that are unambiguous and well-known?
- Is it without error-fixing exception statements?
- When was it written? A manual that was written without user involvement and feedback tends to be of a lower quality than one that has been written with user involvement – the agile way.
- Includes errata

4. Important aspects when having an agile and DevOps approach

When using an agile and DevOps approach, living documents (information) are important. Living documents are also named dynamic documents. When developing living documents, it is important to have that in mind from day one. For safety documents it is important to have in mind complete understanding, monitoring, revision and review requirements. New documentation systems like Confluence should be adapted to ensure that the tool is adapted to safety requirements for editing, review and revisions.

The purchasers should gather information regarding the edition frequency of the product from the supplier. It is also possible to look at the release history, but be aware – the release frequency may become more frequent in the future.

4.1. SafeScrum and DevOps

The SafeScrum process was developed through collaboration between research and industry, involving leading Norwegian providers of safety-critical systems. All the main components of the Scrum process are kept and in addition the process includes all requirements presented in relevant safety standards.

SafeScrum extends the basic Scrum model in order to make the process applicable for development and certification of safety-critical software.

In order to add safety to the Scrum process, we have used the alongside engineering process– a set of supporting activities, including safety, running in parallel with the Scrum process. The alongside engineering concept fits quite well with development and purchasing of safety products. Outside stakeholders, as e.g., suppliers and certification bodies, normally communicates with the alongside engineering team, often also named the RAMS team (Reliability, Availability, Maintainability and Safety) or FuSa team (Functional Safety) [16]. It is also very important that the communication between the SafeScrum team and the alongside engineering team is good. SMEs (Small and Medium Enterprises) will not have the resources needed to have a dedicated safety and security team but should nevertheless have relevant advisors to assist the project team.

DevOps is all about communication and is not intended to be only a development process. The Gartner Glossary calls it a culture: “DevOps represents a change in the IT culture, focusing on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach. DevOps emphasizes people (and culture) and seeks to improve collaboration between operations and development teams.”

The hardware development normally stops when the product or system has been taken into operation while the DevOps approach then starts, and the improvement of the software can be continued on a regular basis.

DevOps is in many ways just what developers and operators always have done but in a more efficient and coordinated way. The operator experiences some problem or a need to change or extend the systems functionality, he writes a report and send it to the company that has developed the system. This can also be partly automated, both the monitoring of the system and the feedback. Sooner or later, the operator will receive a new version of the system where the reported needs have been covered. What is new with DevOps is that DevOps extend the development team by “including” site operations in the development process. In this sense, a system is under constant development where experience from the field and monitoring of the system is feed into the improvement of the system. This will benefit both developers and operators. Operators will be able to bring their problems to the attention of the developers quicker and thus get the problems solved earlier. Developers will get a better understanding of the operations problems and the consequences of delivering systems containing errors or not fully meeting the needs of its users.

4.2 Agile safety case

Purpose of "The Agile Safety Case" (TASC): As the SC above but also including: Adaptability, flexibility and effective solutions [7].

It is efficient to build the safety case by inserting information when it becomes available – an agile approach will also result in increased safety awareness and understanding

4.3 Software and PoC process to achieve evidence-based patching and upgrades

To satisfy the need for frequent updates and upgrades after the safety system (e.g., a vehicle) have been deployed, we have to combine the best from the safety and security domains, agile community and the DevOps approach.
There have to be a proactive reaction to unknown risks that will inevitably manifest during operation of autonomous vehicles. And there may be security issues. In addition, there will be planned improvements to move quickly to higher levels of autonomy. To satisfy both safety and security requirements when developing and operating autonomous vehicles, we have to implement the agile safety case approach [6].

It is important to have a DevOps process in place to ensure quick but safe patching (short-term response). The relevant safety and security standards have to be reissued more often than the traditional safety standards due to the rapid development of technology. As a result, the safety case has to be updated to adapt to these changes in the safety and security standards.

Many factors affect the type and amount of customer-supplier interactions. ISO 26262-8 [14] presents a template for a "development interface agreement" while The Norwegian Agency for Public and Financial Management has issued a template for an agile contract [15].

5. CONCLUSION

In this paper we have focused on relevant documents purchasers and integrators should ask for when buying products and systems. The most important documents have been described and what they should look for are presented: SIL compatibility certificate and six other relevant documents (safety manual, safety case including safety-related application conditions (SRAC) and hazard log, safety assessment report, certificate report, and user manual). We have also included some advice related to projects including an agile and DevOps approach.

Acknowledgements

This work has been supported by The Norwegian Research Council, Project name "TrustMe", project number: 309207-IPOFFENTLIG19, https://prosjektbanken.forskningsradet.no/#/project/NFR/309207, and the ISESAP project 309406.

References

[1] Vermeulen, F.: Guide to ISO 20607: Instruction Handbooks for Machinery, Sept. 10, 2019
[2] ISO/IEC/IEEE 26515:2018 Systems and software engineering. Developing user documentation in an agile environment.
[3] T. Myklebust and T. Stålhane. Functional safety and proof of compliance. ISBN 978-3-030-86151-3, ISBN 978-3-030-86152-0 (eBook) https://doi.org/10.1007/978-3-030-86152-0. Springer International Publishing. December 2021.
[4] Norwegian Oil and Gas Association. Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry. (Recommended SIL requirements). Revision no.: 04 Date revised: April 2020. The document can be downloaded at: www.norskoljeoggass.no/en/working-conditions/retningslinjer/health-working-environment-safety/technical-safety/070-guidelines/
[5] RFU-STR-001 EC certificates/QMS-approvals/ISVs 2022. The document can be downloaded at http://nb-rail.eu/co/co_docs_rfu_en.html
[6] T. Myklebust, T. Stålhane and Geir K. Hanssen. Agile Safety Case and DevOps for the automotive industry. ESREL2020/PSAM15 Venice, Italy 2020
[7] T. Myklebust and T. Stålhane. The Agile Safety Case. ISBN 9783319702643. Springer International Publishing. February 2018.
[8] G. K. Hanssen, T. Stålhane and T. Myklebust. SafeScrum – Agile Development of Safety-Critical Software. ISBN 9783319993348.Springer. December 2018.
[9] www.practitest.com/help/tests/test-library/
[10] www.microchip.com/en-us/products/microcontrollers-and-microprocessors/32-bit-mcus/32-bit-functional-safety/industrial-safety-self-test-library#
[11] https://spectrum.ieee.org/software-eating-car
[12] ISO 26262-10:2018 Road vehicles - Functional safety - Part 10: Guidelines on ISO 26262
[13] ISO 26262-11:2018 Road vehicles - Functional safety - Part 11: Guidelines on application of ISO 26262 to semiconductors

[14] ISO 26262-8:2018 Road vehicles - Functional safety - Part 8: Supporting processes

[15] Agile contract issued by The Norwegian Agency for Public and Financial Management (DFØ). Seen 2022-05-23 https://anskaffelser.prod.dfo-dev.no/nb/verktoy/maler-ogsa-kontrakt-og-avtalemaler/smidigavtalen-ssa-s

[16] T. Myklebust and P. Okoh. Functional safety, Sprints and Kanban approach in practice. ISSS 2022 Annual Conference, Cincinnati, USA