Functional Safety Extensions to Automotive SPICE According to ISO 26262

Per Johannessen[1], Öjvind Halonen[2], and Ola Örsmark[1]

[1] Volvo Car Corporation
pjohann1@volvocars.com, oorsmar1@volvocars.com
[2] EIS by Semcon
ojvind.halonen@eis.semcon.com

Abstract. The automotive industry is currently focused on feature development to deliver green, safe and connected vehicles. Implementations of these features increase both complexity and function integration in software as well as in electronic hardware. In order to maintain safety in vehicles due to this more complex and integrated environment, the upcoming ISO 26262 functional safety standard will give support. The automotive manufacturers who develop safety related functionality could benefit from using this new ISO standard to address functional safety. One requirement of ISO 26262 is to assess the capability of the development process used to comply with the standard. This paper describes an approach to extend ISO/IEC 15504 and Automotive SPICE to fulfill this ISO 26262 requirement for both software and hardware development. The functional safety extensions can be used together with Automotive SPICE for process assessments of functional safety in the automotive industry.

Keywords: Automotive SPICE, DFEA2020, Functional Safety, ISO/IEC 15504, ISO 26262, Safety Assessment.

1 Introduction

Today, the automotive industry is undergoing significant changes due to many different external factors, such as increased focus on environmental care, awareness of safety, and integration of consumer electronics in vehicles. At Volvo Cars, this is visible in feature development in the three key areas; green, safe and connected. This leads to an exponential growth of electronics and software in our vehicles. Together with an increasing focus on functional safety and dependability, there is a need to further develop both electrical architectures and development methods. To address these challenges in the automotive industry, the DFEA2020 national research project is conducted at Volvo Cars in collaboration with several partners. DFEA2020 is funded by VINNOVA, a Swedish government agency for innovation, and the DFEA2020 project partners.

Due to a new functional safety standard, ISO 26262 [1], one part of DFEA2020 is dedicated to functional safety and this standard. ISO 26262 is in its final stage before publication in 2011. Even if the standard has been used in its draft versions, the impact

R.V. O'Connor et al. (Eds.): SPICE 2011, CCIS 155, pp. 52–63, 2011.

on the automotive industry for passenger cars will be significant. ISO 26262 is applicable for safety related functions, systems, and components that are implemented in electronics or software. ISO 26262 will address both safety related implementations and the development process used. For the development process, there is a need and also an ISO 26262 requirement to determine whether it is compliant with the process prescribed by ISO 26262.

A specific goal for DFEA2020 is to develop a framework for process assessment meeting the ISO 26262 standard. An interim result is described in this paper.

The paper starts with a brief overview of standards related to the proposed functional safety extensions and a summary of current state of functional safety assessments in the automotive industry. This is followed by a presentation of the selection of assessment framework and the proposed extensions. Further, two examples of the extensions as proposed to Automotive SPICE and ISO 15504 are included to give the reader a better understanding. Next, a guide to implementation is presented. Finally, the paper provides some conclusions and discusses ideas for further work.

2 Related Work

There are several standards and efforts to address functional safety in product development. Some of these are related to the proposed functional safety extensions to Automotive SPICE. The related standards are briefly introduced here.

2.1 ISO 26262

ISO 26262 [1] is the upcoming automotive standard for functional safety applicable for safety related Items that are implemented in electronics or software. An Item in [1] is defined as "system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied".

In the version to be released, the standard is limited to passenger cars up to 3.5 metric tonnes. Possibly, the standard could become applicable for heavy vehicles in its first revision.

The standard is currently available as Final Draft International Standard (FDIS), which is the last step before being a public international standard. ISO 26262 has been in development within ISO since 2005. From this time, it has increasingly been introduced for product development in the automotive industry.

The standard includes ten different parts and its lifecycle spans from concept development, through product development, to service, operation and decommissioning. With that scope, the impact from this standard on the automotive industry will be significant.

One key concept of ISO 26262 is the Automotive Safety Integrity Level (ASIL) which is determined during the concept phase of product development. ASIL is both a measure of risk for hazards and a measure of necessary risk reduction that should be addressed during product development. There are four levels, attributed ASIL A, ASIL B, ASIL C, and ASIL D where ASIL D implies the highest level of rigor during development. In case the Item has no hazard with an associated ASIL, a QM attribute is used. QM denotes Quality Management for which ISO 26262 has no requirements.

Many driveline and chassis systems need to manage ASIL C or ASIL D safety requirements while body systems often only have to manage ASIL A, ASIL B, or QM. In general, ASIL A and ASIL B systems do not typically require redundancy in electronic hardware which ASIL C and ASIL D typically do. Further, ISO 26262 has different rigor in requirements on the development process depending on the ASIL.

A Functional Safety Assessment shall ensure that Item under development has an appropriate level of functional safety according to ISO 26262, i.e. a functional safety product assessment. For an Item under development, this is done by checking that the Item has both the required documentation and the required safety measures implemented according to ISO 26262. Examples of required documentation are Hazard Analysis and Risk Assessment reports and Safety Cases. Typical safety measures are safety monitors and redundant sensors. The Functional Safety Assessment shall also consider the results of a Functional Safety Audit.

A Functional Safety Audit is required by ISO 262626 to ensure that the development process used for the Item is compliant with ISO 26262, i.e. a functional safety process assessment.

Both the Functional Safety Audit and the Functional Safety Assessment are depending on the ASIL of the Item under development. The higher the ASIL, the more processes are needed and the assessor should be more independent.

Even if ISO 26262 has requirements for Functional Safety Audits, there is no guidance in the standard on how to carry it out. However, the standard provides notes that the Safety Audit is related to SPICE assessments.

2.2 Automotive SPICE

The automotive industry in general has during the last decade focused on implementation of Automotive SPICE [2, 3], which is an adopted subset of ISO/IEC 15504 [4]. The vehicle manufacturers have strived to achieve process fulfillment at maturity level 3 for a subset of the processes required for their suppliers. During the last two years, the focus on Automotive SPICE has decreased and instead the focus has moved from quality to safety. Even if Automotive SPICE assessments are valuable for development of safety related software, there are several gaps to ISO 26262 that need to be addressed, e.g. system and hardware development.

2.3 +SAFE

+SAFE [5] is an extension to Capability Maturity Model Integration (CMMI) for Development (CMMI-DEV) that covers safety management and safety engineering. It was developed by the Defence Materiel Organisation within the Australian Department of Defence and the latest version, version 1.2, was released in 2007. The +SAFE extension supplements CMMI-DEV with two additional process areas that provide a basis for appraising or improving an organization's processes for providing safety-critical products.

+SAFE was developed for standalone use. It is not intended to be embedded in a CMMI model, but can be modified to support different safety standards.

This extension is a good starting point for ISO 26262 process capability determination. However, +SAFE is not sufficient by itself to be used in the automotive industry due to gaps to ISO 26262, e.g. electronic hardware processes are missing in +SAFE.

2.4 ISO/IEC 15504-10 - Safety Extension

This part 10 of ISO/IEC 15504 [6] defines processes and guidance to support the development of safety related systems. It is currently under development and is expected to be released during 2011. The process assessment model for this part 10 complements the process assessment model for system and software as defined in ISO/IEC 15504 Parts 5 and 6.

ISO/IEC 15504-10 defines three processes to support safety. The processes are:

- Safety Management process
- Safety Engineering process
- Safety Qualification process

ISO/IEC 15504-10 claims that the defined processes are consistent with the five different safety standards:

- IEC 61508
- +SAFE, A Safety Extension to CMMI-DEV, V.1.2.
- IEC 60880
- UK MoD Def Stan 00-56
- ISO 26262

These five standards use different safety lifecycles with different processes and it is challenging to write a standard such as ISO/IEC 15504-10 to cover all of these processes. In the case of ISO 26262, there are gaps between the three additional processes defined in ISO/IEC 15504-10 and the processes needed to be assessed according to ISO 26262, e.g. electronic hardware processes are missing in ISO/IEC 15504-10. In this paper, we suggest additional processes to close this gap.

2.5 Functional Safety Assessments in the Automotive Industry

Currently in the automotive industry, there is no commonly used functional safety assessment framework. To a large degree, functional safety assessments are done by expert judgment. Some companies, offering functional safety assessment, use company internal instructions and checklist when doing these assessments for customers. However, from our perspective, there is currently a large degree of ad-hoc functional safety assessments performed in the automotive industry. This is particular true when it comes to functional safety processes assessments, for processes not covered by Automotive SPICE. Further, most functional safety assessments seem to focus more on technology rather than development processes used. As ISO 26262 soon will be released as an international standard, there is a need in the industry to standardize functional safety process assessments.

2.6 Swedish Standardization for Functional Safety Process Extensions

In the Swedish working group for ISO 26262, a task has been initiated to develop a Swedish standard based on the functional safety process extensions described in this paper. Sweden has four major automotive manufacturers with a strong tradition on safety, all participating in this standardization effort.

The goal is to have an international standard instead of a Swedish national standard. The main reasons for developing a Swedish standard is that it will be a good basis to propose as an international standard and it could be developed in less than six months. With the current plan for this standard, it would be available approximately at the same time as ISO 26262 is released as an international standard. Hence, this Swedish standard could be used by any early adopter and be a proposal for a new international standard.

3 Functional Safety Process Assessment Strategy

In order to ensure that the development of safety related systems will result in safe systems, an assessment strategy is needed. Two parts have been identified as necessary for functional safety process assessment:

- Performing a functional safety process assessment on a reference project before development, i.e. a process capability determination.
- Performing a tailored functional safety process assessment during development as a part of the functional safety product assessment.

The strategy, as can be seen in Fig 1, implies a wider context than ISO 26262 suggests where functional safety process assessment is only required to be performed on projects during development. The possibility to assess a reference project adds significant value, e.g. at procurement, and supports long term relations with suppliers. During development the effort will be reduced accordingly.

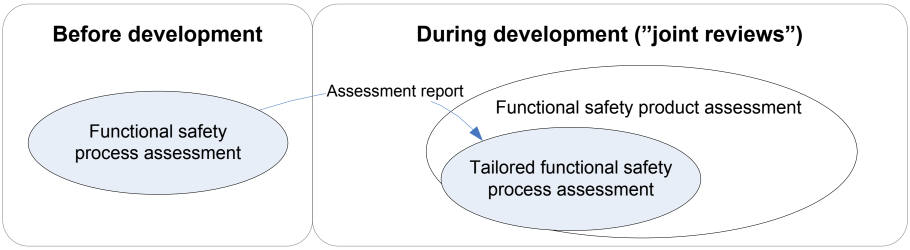
Before development
During development (”joint reviews”)
Assessment report
Functional safety process assessment
Functional safety product assessment
Tailored functional safety process assessment

Fig. 1. Overall strategy for functional safety process assessment

The ability to tailor the assessments for different ASIL becomes essential since the ISO 26262 requirements depend on the ASIL. The selected approach is to base the assessment framework on ASIL D requirements and allow for further tailoring by the assessors. Adapting this assessment framework to each ASIL would be impracticable.

4 Assessment Framework

Implementation of the functional safety process assessment strategy will benefit from a supporting assessment framework. An assessment framework requires a process reference model to scope the ISO 26262 objectives, requirements, and work products, as well as a process assessment model.

4.1 Selection of Assessment Framework

Three different approaches for developing the assessment framework were considered:

- Use the Automotive SPICE framework
- Develop custom framework based on ISO 26262
- Use framework from other domains

The first approach, reusing the Automotive SPICE framework, was found to be quite attractive due to the organizational knowledge, established methods for SPICE assessment, and global knowledge of SPICE assessment in the industry. However, an extended framework for functional safety assessment would need to be developed.

The second approach, to develop a custom framework based upon ISO 26262, was attractive due to the lightweight approach, to just use what was required, and easy to tailor for its needs. However, this approach would be informal and hard to establish especially for suppliers since it would not relate to established assessment practices. To compare the results from different assessments would also be hard with a custom framework. This approach is similar to the ad-hoc approach taken by assessment companies today as discussed earlier in this paper.

To use a framework from other domains would give the benefit of an established framework and certification scheme. One such framework is CASS (Conformity Assessment of Safety-related Systems) [7] which is based on the standard IEC 61508 [8]. However, major adoption to automotive industry and ISO 26262 would be required.

The decision was to reuse the Automotive SPICE assessment framework, extended by ISO 26262 compatible processes for functional safety process assessment. This gave most organizational and domain benefits.

4.2 Assessment Model

Four categories of processes have been identified with respect to Automotive SPICE, as shown in Fig. 2, in order to incorporate the ISO 26262 requirements:

- Additions for functional safety to Automotive SPICE
- Additions for functional safety to ISO/IEC 15504
- New processes, also called extensions according to SPICE, to Automotive SPICE and ISO/IEC 15504 for unique functional safety processes
- Reused processes, which are processes in Automotive SPICE that need to be assessed to show full compliance with ISO 26262

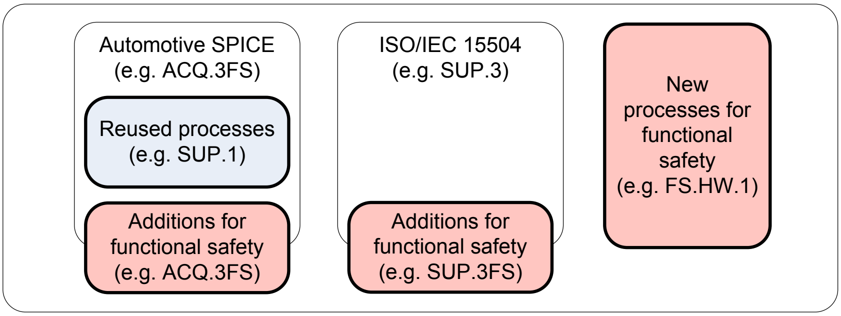

Fig. 2. Process extensions for functional safety process assessment

The functional safety process assessment framework extends the Automotive SPICE model by adding new processes or making additions to existing processes. Existing process outcomes were not altered and none were removed.

4.3 Identification of Extensions

A process ID is used for identification of the functional safety extensions, but in order to separate those from the Automotive SPICE processes, the processes and practices have been uniquely defined by adding FS, representing Functional Safety.

Additions are identified through a postfix, ".FS" to the process ID. As an example, the functional safety addition to the Automotive SPICE process ACQ.3, Contract Agreement, is identified as ACQ.3FS. As a second example, Software Validation which is only defined according to ISO/IEC 15504 has to be extended with safety validation, which is identified as the addition SUP.3FS.

The new processes, i.e. extensions, are identified through a prefix, "FS" to the process ID. As an example, Automotive SPICE does not cover hardware development and a new process needs to be developed. The new process is identified as FS.HW.1.

Note that reused processes have been included but without the FS prefix/postfix. The process definitions for these processes are not modified, but are essential to meet the assessment scope of ISO 26262.

In order to get a complete process assessment model, each safety related process has been extended with so-called safety practices (SP) to cover the wider scope of ISO 26262. The safety practices correspond to base practices in Automotive SPICE.

Safety practices are identified through the process extensions ID and by adding a postfix ".SP#", e.g. SUP.3FS.SP1

4.4 Functional Safety Extensions to Automotive SPICE and ISO/IEC 15504

The required functional safety extensions, and their associated work products, have been established and traced to ISO 26262. The four tables below show the resulting functional safety extensions, including the reused processes, needed to cover ISO 26262 requirements.

Table 1. Overview of functional safety additions to existing Automotive SPICE processes

Automotive SPICE additions	Process name	ISO/DIS 26262 references
MAN.3FS	Project Management	2-5, 8-5, 4-5
SPL.2FS	Product release	4-11
SUP.10FS	Change request management	3-6, 8-8
ENG.2FS	System requirements analysis	3-5, 4-6, 8-6
ENG.3FS	System architectural design	4-7
ENG.4FS	Software requirements analysis	6-6
ENG.5FS	Software design	6-7
ENG.6FS	Software construction	6-8, 6-9
ENG.7FS	Software integration test	6-10
ENG.8FS	Software testing	6-10, 8-9
ENG.9FS	System integration test	4-8
ENG.10FS	System testing	4-8, 6-11, 8-9
ACQ.3FS	Contract Agreement	8-5

Table 2. Overview of functional safety additions to existing ISO/IEC 15504 processes

ISO/IEC 15504 additions	Process name	ISO/DIS 26262 references
SUP.3FS	Validation	4-5, 4-6, 4-9

Table 3. Overview of new functional safety processes, i.e. extensions, to Automotive SPICE and ISO/IEC 15504

Extension	Process name	ISO/DIS 26262 references
FS.MAN.1	Safety Culture Management	2-5
FS.MAN.2	Safety Life Cycle Management	2-5, 2-6, 2-7, 3-6
FS.AN.1	Hazard Analysis	3-7
FS.AN.2	Safety Analysis on System Level	4-7, 9-7, 9-8
FS.AN.3	Hardware Safety Analysis	5-7, 5-8, 5-9, 9-7, 9-8
FS.AN.4	Software Safety Analysis	6-7, 9-7, 9-8
FS.SUP.1	Safety Case Development	2-6, 8-10
FS.SUP.2	SW Component Qualification	8-12
FS.SUP.3	HW Component Qualification	8-13
FS.SUP.4	Calibration and Configuration Data Management	6-Annex C
FS.HW.1	Hardware Safety Engineering	5
FS.TOOL.1	Qualification of Tools	8-11
FS.PROD.1	Production, Operation, Service and Decommissioning	7

Table 4. Overview of reused processes from existing Automotive SPICE processes

Automotive SPICE	Process name	ISO/DIS 26262 references
MAN.5	Risk management	-
SUP.1	Quality assurance	2-5
SUP.2	Verification	4-5, 4-8, 4-9, 5-10, 6-9, 6-10, 6-11, 8-9
SUP.4	Joint review	8-5
SUP.8	Configuration management	8-7
SUP.9	Problem resolution management	2-4
REU.2	Reuse program management	-
ACQ.4	Supplier monitoring	8-5

4.5 Examples of Extensions and Safety Practices

As described there are different types of extensions needed. For these, it was decided to use the same structure as in Automotive SPICE.

In Table 5, there is an example of an extension to an Automotive SPICE process. This extension is an addition that is needed for change management since the SUP.10 process does not include safety analysis, safety lifecycle, and safety manager approval. Therefore, these three aspects have to be added to SUP.10 as shown in Table 5.

Table 5. The Change Request Management addition to SUP.10 in Automotive SPICE

<table>
<tr><td><b>Process ID</b></td><td>SUP.10FS</td><td><b>Applicable ASIL</b></td><td>A-D</td></tr>
<tr><td><b>Process Name</b></td><td colspan="3">Change request management</td></tr>
<tr><td><b>Process Purpose</b></td><td colspan="3">The purpose of the FS addition to the change request management process is to ensure that safety related work products are analyzed and managed during the entire safety lifecycle.</td></tr>
<tr><td><b>Process Outcomes</b></td><td colspan="3">As a result of successful implementation of this process:
1) the change request is analyzed for impact on functional safety of the product;
2) the change request is analyzed for impact of the safety lifecycle and what safety activities that needs to be carried out again;
3) if there are changes related to safety, the decision to accept, reject or delay the change is agreed with the safety manager.</td></tr>
<tr><td><b>Safety Practices</b></td><td colspan="3">SUP.10FS.SP1: Perform an impact analysis with respect to safety of the product. This analysis should also include new or changed hazards.
SUP.10FS.SP2: Perform an impact analysis with respect to the functional safety activities that need to be conducted. If the ASIL level is increased because of the change, a gap analysis shall be performed to find out what needs to be done to achieve the higher ASIL.
SUP.10FS.SP3: The safety manager is included in the decision process.</td></tr>
</table>

There are five different work products in ISO 26262 impacted by SUP10.FS, these are shown in Table 6 together with their reference to ISO 26262.

Table 6. The work products from the Change Request Management extension SUP.10FS with the corresponding ISO 26262 references

Output Safety Work Products	ISO/DIS 26262 reference
Change management plan	8-8.5.1
Change request	8-8.5.2
Impact analysis	8-8.5.3
Change request plan	8-8.5.3
Change report	8-8.5.4

Another type of extensions to Automotive SPICE and ISO/IEC 15504 is for new processes. An example of this extension is shown in Table 7, which is for hazard analysis. The hazard analysis process is one key process needed for functional safety as the whole safety lifecycle is impacted by the outcome of this process.

Table 7. The Hazard Analysis extension as proposed

Process ID	FS.AN.1	**Applicable ASIL**	QM, A-D
Process Name	Hazard Analysis		
Process Purpose	The purpose of the hazard analysis is to identify and classify hazards related to the item.		
Process Outcomes	As a result of successful implementation of this process: 1) the target for the analysis is clearly defined; 2) the failure modes of actuators and functions (use cases) are identified; 3) the relevant situations are identified; 4) the hazards are clearly expressed; 5) the hazards are classified according to an international standard; 6) the top level safety requirements (safety goals) are clearly defined; 7) the analysis is revised during the development to seek for new or changed hazards.		
Safety Practices	FS.AN.1.SP1: Define the item. This includes external interfaces, functional requirements, non-functional requirements, assumptions and foreseeable misuse. FS.AN.1.SP2: Define the failure modes of 1) actuators and 2) functions (e.g. based on use cases). Define the system effect (technical) and the effect on the vehicle level as a result of the failure modes. *NOTE: Omission (no effect) and commission (full effect when not wanted) shall always be considered. Other failure modes (late, early, more, less and stuck effect) may be considered depending on the function.* FS.AN.1.SP3: Define the relevant situations for the failure modes. This includes all common operating situations (e.g. driving on straight road, city driving, and situation when function is used) and may also include production, service and other special situations. The situation coverage should be determined. FS.AN.1.SP4: Define the hazards based on the failure modes and situations. FS.AN.1.SP5: Perform classification according to an international standard relevant for the automotive industry. Justify the classifications with descriptions of the assumptions made. Involve a group of people in the hazard analysis effort. FS.AN.1.SP6: Define the top level safety requirements (safety goals) together with their safety integrity levels and safe states. FS.AN.1.SP7: Revise the analysis during development.		

There are three different work products in ISO 26262 impacted by FS.AN.1, these are shown in Table 8 together with their reference to ISO 26262.

Table 8. The work products from the Hazard Analysis extension FS.AN.1 with the corresponding ISO 26262 references

Output Safety Work Products	ISO/DIS 26262 reference
Hazard analysis and risk assessment	3-7.5.1
Safety goals	3-7.5.2
Verification review of hazard analysis and risk assessment and safety goals	3-7.5.3

5 Implementation

When doing functional safety assessments on Items according to ISO 26262 and the proposed work in this paper, there are four steps recommended:

- Request an Automotive SPICE Assessment from the supplier
- Carry out a functional safety process assessment on a reference project, decided jointly with the supplier, based on the assessment framework presented in this paper
- Perform a functional safety product assessment on the Item during the product development, from project start to start of series production
- Follow up the action plan from the functional safety process assessment and the functional safety product assessment during the project.

For functional safety process assessment, maturity level 0-3 should be assessed where level 3 is required. Level 3 should be sufficient since ISO 26262 does not require organizational process implementation and level 3 is commonly accepted as a minimum level for Automotive SPICE compliance. Level 3 has the advantage that the outcome should have minimum dependency on specific development projects. Further, it is also possible to tailor the process assessment depending on the ASIL. The ASIL to be used could for instance depend on the types of systems developed by the assessed organization.

For functional safety product assessment, maturity level 0-1 is assessed for work products, where level 1 is required. The reason for choosing level 1 is that this type of assessment is focused on the achievement of the process purpose, i.e. safety practices, and the characteristics of the work products. To ensure that the development process used for the Item is compliant with ISO 26262, it is sufficient to check that the development process has satisfactorily been assessed and, by simple checks, confirm that the previously assessed process is being used in the development. Inspection of the work products refers to the same processes as used for the tailored functional safety process assessment.

6 Conclusion and Further Work

The work to implement safety extensions to ISO/IEC 15504 and Automotive SPICE was quite straight forward once the methodology for the extensions was set. Further, since the ISO 26262 requirements on safety organizations are similar to Automotive

SPICE requirements, the smoothest approach was to reuse the software quality organization setup and the software process assessment methods for the ISO 26262 safety organization and functional safety assessments.

The challenge has been to verify the extensions through product and process assessments. This work is ongoing within the DFEA2020 project and also in vehicle programs within Volvo Cars.

Since quality and safety go hand in hand, the people working with safety assessment and those working with quality assessment may well be in the same organization. If similar work methods can be used, higher efficiency will be achieved at an organizational level. Tools already in use for SPICE assessment can be expanded to also support the extensions required for functional safety assessment.

For organizations which base their processes on ISO/IEC 15504 and not Automotive SPICE, the safety extensions presented in this paper should be easy to adopt.

Once the Swedish working group for ISO 26262 has developed a Swedish standard for the process extensions described in this paper, the next step, apart from its use in product development, will be to target international standardization.

Acknowledgments

This work has been funded by the Swedish FFI program (Strategic Vehicle Research and Innovation) through the project DFEA 2020.

The authors would like to thank Joacim Bergman who participated in the work developing the Safety Extensions presented in this paper.

References

1. ISO/DIS 26262, Road vehicles - Functional safety, International Organization for Standardization, Geneva, Switzerland (2009)
2. Automotive SPICE Process Reference Model, v4.5, Automotive SIG (2010)
3. Automotive SPICE Process Assessment Model, v2.5, Automotive SIG (2010)
4. ISO/IEC 15504:2006 Information Technology - Process Assessment – Part 5: An exemplar Process Assessment Model. International Organization for Standardization, Geneva, Switzerland (2006)
5. +SAFE, A Safety Extension to CMMI-DEV, V1.2, Defence Materiel Organisation. Australian Department of Defence, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA (2007)
6. ISO/IEC DTR 15504-10, Information technology – Software process assessment – Part 10: Safety Extensions. International Organization for Standardization, Geneva, Switzerland (2010)
7. The CASS Guide to Functional Safety Management Assessment, Issue 2.a. The CASS Scheme Ltd., United Kingdom (2000)
8. IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneva, Switzerland (1998, 2000)