ISO 26262 Verifiering av programvara i säkerhetskritiska EE-system, dnr: 2011-04438

Project within Traffic safety

Miroslaw Staron

2017-01-31

Content

FFI in short

FFI is a partnership between the Swedish government and automotive industry for joint funding of research, innovation and development concentrating on Climate & Environment and Safety. FFI has R&D activities worth approx. €100 million per year, of which half is governmental funding. The background to the investment is that development within road transportation and Swedish automotive industry has big impact for growth. FFI will contribute to the following main goals: Reducing the environmental impact of transport, reducing the number killed and injured in traffic and Strengthening international competitiveness. Currently there are five collaboration programs: **Vehicle Development, Transport Efficiency, Vehicle and Traffic Safety, Energy & Environment and Sustainable Production Technology.**

For more information: www.vinnova.se/ffi

1. Executive summary

Ska bland annat innehålla kort projektbeskrivning, mål samt resultat.
(Denna sammanfattning kan lyftas in i slutredovisningen i VINNOVAs Intressentportal punkt 1. Sammanfattning av projektet och dess resultat, max 5000 tecken. Från Intressentportalen kommer den automatiskt att publiceras på webben).

The safety of road vehicles in general is improved by active safety systems through advanced embedded systems where software plays the key role. At the same time the increasing complexity of the corresponding systems and software requires new methods and tools in order to drastically increase performance of safety systems without compromising the cost of developing them. The new ISO 26262 provides requirements and high-level guidelines for functional safety, but these are not detailed enough to ensure cost-effective industrial adoption and argumentation towards fulfilment of safety goals at the level of the complete electric system (today done only at the level of groups of functions). Therefore, the project had the goal to:

- Establish ISO26262 requirements validation by providing statistical evidence for assessment of safety goals of the complete electrical system.
- Improve efficiency of development and verification of active safety systems by guidelines and methodology for verification complementing the ISO 26262 by describing how to efficiently combine simulation and testing.

An iterative approach was adopted in the project combining theoretical investigations, development and industrial case studies (evaluation using real-life projects at industrial partners, aka in-kind projects). The collaboration was organized in a set of sprints which guarantee knowledge transfer to regular car projects and regular workshops will be organized to disseminate project results outside of collaboration partners.

The project has primarily contributed to the safe vehicles program target by addressing the challenges of effective implementation of the safety standard ISO 26262 and secondary to increasing competitiveness of the Swedish industry by making the validation of the safety requirements more efficient. The main results of the project were methods and tools assuring efficient ISO 26262 verification and validation in car development projects. The proposed VISEE project involveed the following partners: Chalmers, University of Gothenburg and Volvo Cars with Chalmers as applicant and project leader.

2. Background

Driven by needs to improve vehicle safety and reduce environment impact, vehicles are becoming autonomous, being equipped with active safety systems, advanced power trains and energy management, and with an increasing connectivity to the traffic environment. Unless new, drastically more efficient, methods for software development, safety argumentation and modeling are adopted, the growing connectivity of systems in modern cars and growing complexity have potential to greatly reduce the possibility of delivering customer value (in terms of safety) and thus limiting the growth opportunities for the automotive industry. To successfully develop such methods, it is necessary to go beyond pure software in order to properly capture the characteristics of the software in the context of its embedded system and automotive environment.

A number of initiatives address the challenge of efficient development and integration of Electical/Electronic systems (EE-systems). For example, AUTOSAR provides open and extensible architecture which in the long run can provide easier adaptations and reuse of components across different car platforms. However, the AUTOSAR initiative is focused on software engineering aspects such as configuration of software components and does not address analysis of safety of vehicles at the OEM level, something that is required according to ISO 26262 (Road vehicles – Functional Safety).

ISO 26262 provides best practices for developing safety related systems in terms of activities and means that are required to ensure that risks are as low as reasonably practicable. However, these requirements and guidelines are mostly process oriented and are not detailed enough to ensure cost-effective industrial adoption and argumentation towards fulfillment of safety goals.

As a result of the growing complexity and interaction between different software/mechatronic systems in the car, verification and validation increasingly become growing challenges; challenges which can potentially jeopardize the argumentation of fulfillment of safety goals at the level of the complete electrical systems. The state space and number of potential defects (aka bugs) imply that testing and simulation alone are not sufficient to meet safety requirements.
This proposed project addresses the following topics:

- How to simulate and test software in order to be able to build statistical evidence for the assessment of safety goals at the level of complete electric system?

  We intend to expand simulation models by introducing modelling elements for dependability mechanisms, augmenting models with diagnostic mechanisms to inject defects and collect data about defects in simulations and, finally, we intend to find the trade-off between in-development function-/system- testing and run-time dependability assurance (e.g. partitioning, sandboxing).

- How can and should different types of defect analysis techniques best be combined with verification and validation methods in order to provide argumentation of ISO 26262 goal fulfillment?

  We intend to investigate the different types of defects analysis techniques (e.g. RCA[1] [1] or FMEA[2] [2]) and to classify them using safety goals and their corresponding ASIL[3] as defined in ISO 26262. Related to the first topic, we also intend to correlate this classification with information about defect profiles. The purpose is to provide a taxonomy that is useful for selecting combinations of effective verification methods across the development stages.
- How can tools for safety defects analysis and prediction (e.g. fault-tree analysis, defect inflow prediction models) and verification (e.g. testing) be better integrated with model-based simulation tools such as Simulink?

  Research results are industrialized by demonstrating that tools for collecting statistical evidence used for argumentation of safety goals can be integrated with the tools used in the automotive industry today and in the nearest future, as demonstrated partially in [3]. We also plan to investigate the impact of the level of formality of models on the argumentation [4-6].
- What challenges exist in the development workflow constraining cost-efficient validation of ISO 26262 requirements?

  The proposed VISEE project plans to assess the selected parts of the industrial development processes of the partners in order to identify bottlenecks. This will be useful as a further input for guiding the work in the project and will clearly be beneficial for the industrial partners themselves.

ISO 26262 safety goal analysis

The introduction of the ISO 26262 standard poses hard safety requirements (safety goals) on software in modern cars in terms of, among others, fault tolerance, hazard analysis and software validation processes. Fulfilling these requirements in an efficient way through reusable functional and technical concepts is vital for retaining the competitive edge of automotive OEMs such as Volvo Cars. As for the current day, these requirements are being fulfilled by dependability mechanisms in car software and by verification/validation/simulation of software in development. However, these dependability mechanisms are often realized at the level of single functions (e.g. Adaptive Cruise Control, Airbag, Line Assistance [7]) and when they are integrated in the complete electrical systems, this analysis might not be complete. The realization of the

[1] Root Cause Analysis
[2] Failure Mode and Effect Analysis
[3] Automotive Safety Integrity Level

ISO 26262 Verification and Validation (V&V) that would address this problem of fragmentation of evidence for safety goals is addressed by this proposal.

Active safety systems, like the Volvo Cars’ City Safety system, and future functionalities such as vehicle platooning are of particular focus of this validation, and thus this proposal, since they increasingly constitute an important part of cars’ safety mechanisms (former case) and are highly safety-critical.

Adoption of the ISO 26262 moreover implies that it needs to be integrated with existing processes, practices and tools, such as configuration management, model-based development, top-down function and bottom-up platform development [8]. Given the profit margins in the automotive industry, the constant competition and the growing amount of software in cars, the car manufacturers cannot continue securing the ISO 26262 requirements in the traditional way. New, efficient and cost-effective active software safety systems need to be developed where fulfilling the requirements of ISO 26262 can be assured at the maximum level with low verification/development costs.

Defect classification and injection

Systematic detailed logging of defects when developing active safety software creates a unique opportunity to use the knowledge of commonly discovered types of problems in the safety analysis and to build statistical safety models for the electrical systems.

As in the current state-of-practice and according to requirements from ISO 26262 the main focus of verification and validation of safety goals is on functions or groups of functions there is a considerable challenge of defects that are discovered when functions are integrated. This situation can be observed clearly in the defect inflow diagram in Figure 1.

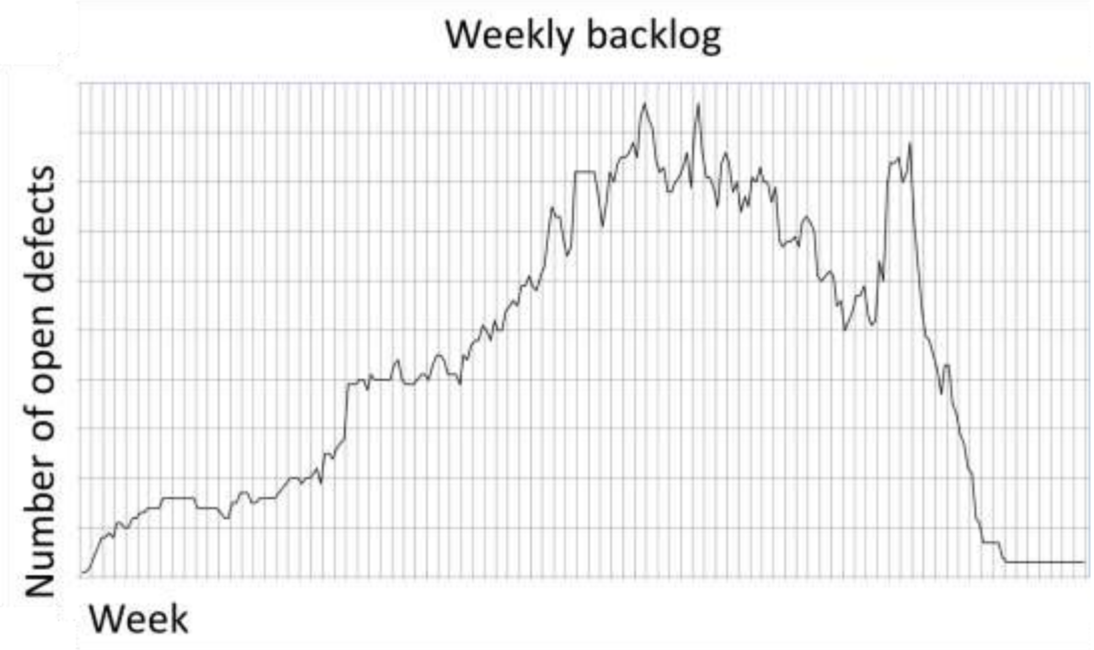

Figure 1. Defect inflow profile in active safety system development over time[4]

The diagram shows that there is a late “peak” with an inflow of defects in the integration phase. These defects should have been found earlier if they were sought for. Established techniques for defect classification (e.g. Orthogonal Defect Classification [9]) might be attempted to identify which kind of defect should be searched for in the modelling/design phase to avoid this late peaks. These general techniques, however, require adaptations for the specific context the automotive domain constitutes (see [10, 11] for a similar adaptation in the telecom domain and its resulting significant improvements of defect discovery effectiveness).

Both the ISO 26262 standard and the mainstream of research in active safety systems considers individual functions or systems (e.g. City Safety) as the main items for which the safety goals are set and the argumentation is provided. However, as the diagram shows the defects related to the complete electrical system of the car can constitute threats to the safety of the complete car (i.e. when systems like City Safety are integrated with systems like cruise control).

3. Objective

The objective of this project was to develop cost-effective ISO 26262 requirements validation through the use of statistical models and optimal defect injection during simulations combined with testing.

4. Project realization

In order to achieve the objective motivated by section 1, we structured the project in the following work packages (WP):

- WP1: Challenges of the effective implementation of ISO 26262.
- WP2: Defect prediction/prevention.
- WP3: Product verification methods.
- WP4: Case and pilot studies.

[4] The time scale and the number of defects cannot be provided due to confidentiality reasons. The diagram was taken from an ongoing Vinnova project ASIS (Algorithms and Systems for Improved Safety) at VCC and Chalmers.

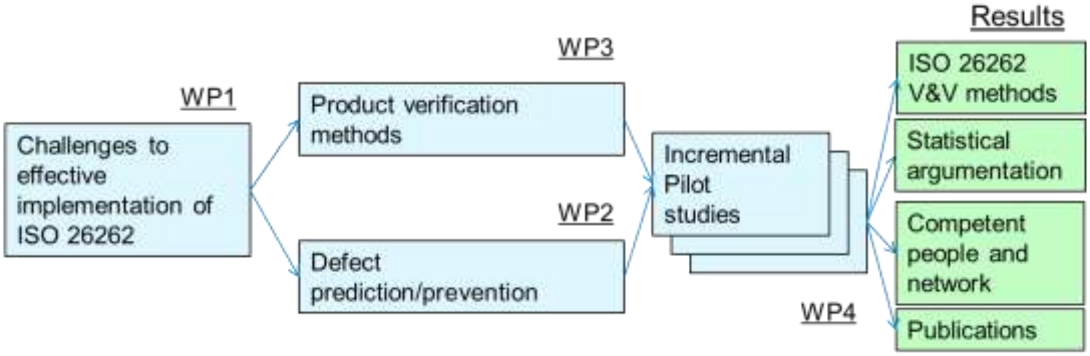
Results
WP3
WP1
Product verification methods
Challenges to effective implementation of ISO 26262
Incremental Pilot studies
ISO 26262 V&V methods
Statistical argumentation
WP2
Defect prediction/prevention
Competent people and network
WP4
Publications

Figure 1: Project work-packages, their relations and project results

The lower level (WP2) contributed to the development of industrial processes and methods (ways-of-working), and was also highly influenced by the ISO 26262 standard - thus more generic to other companies in the automotive sector. The upper level (WP3) was related mainly to ISO 26262 and the product verification methods, which was reused by other companies in the automotive sector. The two levels together, however, formed a complete package with both theoretical research and its practical applications evaluated in WP4.

Work packages

Work package 1: Challenges to effective implementation of ISO 26262

This work package (WP) created a map of challenges to effective implementation of ISO 26262 including quantifiable goals. The goal of this work package was to establish a set of quantifiable goals for the project and to identify which dependability mechanisms, modelling methods and tools that have been proven in other contexts to support these quantifiable goals. A basis for the work was provided by a study of current development processes for safety related systems at the industrial partners and an assessment of state of the art.

The main result of this work package was planned to be a better understanding of the improvement potential in safety critical systems development by integrating the mechatronics and software engineering perspectives and of means to get there. The results were published in publications #6, #16 and #22 listed in Section 6.2.

Work package 2: Defect prediction/prevention

This WP investigated the current trends in defect discovery and develop methods to prevent these defects by adjusting tools and verification methods based on the predictions. This work package addressed the problem of providing statistical evidence in argumentation for the fulfilment of safety goals for the complete electrical system based on model simulation and defect injection.

The main result of this work package was a set of methods for verification and validation of ISO 26262 safety goals with the particular focus on providing statistical evidence in the argumentation of attainment or violation of safety goals. In particular, in this work package we focused on the ability to predict defects on a complete E/E system level. Our results showed the accuracy of over 90% of the predictions, in particular when combining historical data from the same projects. The results were published in publications #3, #4, #5, #8, #12, #13, #14, #17, #18, #21.

Work package 3: Product verification methods

This WP developed guidelines for combining traditional simulation and testing-based methods for verification and validation of ISO 26262. In particular, during the project we found that there are two types of improvements which should be introduced.

The first kind of improvement was to assure that the environment models (aka plant models) should include an extra component to prevent infinite control loops in the presence of certain types of bugs in the ECU models – the method was called FBM (Fault Bypass Modelling).

The second kind of improvement was to address the problem of design defects (aka bugs) in ECU models by improving their testing. This improvement was based on the techniques combining fault injection and mutation testing of Simulink models.

The results of this work package are included in the following publications listed in Section 6.2: #1, #2, #7, #11, #13, #19, #20.

Work package 4: Incremental case studies

The main goal of this work package was to provide a set of case studies evaluating the results of the project. In this project we worked on the cases provided by our industrial partner Volvo Cars and validated the results on the open data set provided by Audi. We also used the collaboration with Software Center to validate the prediction models at Ericsson, and Saab Electronic Defense Systems. As almost all out publications contain an element of validation, the results of the work package are present in almost all papers. However, the following publications, listed in Section 6.2, are focused mainly on reporting of the case study results: #9, #10 and #15.

5. Results and deliverables

5.1 Delivery to FFI-goals

To describe the delivery to the FFI goals we re-use the table provided in the application for funding linking the results of the project to the FFI program targets and the short motivation.

Target	**Short motivation**	**Results of the project**
Program specific target statements (source: "Program beskrivning Fordonsutveckling, februari 2011")		
Inbyggda system och mjukvara: *Höja den tekniska mognadsgraden för att*	This research project focuses on safety of embedded software systems in vehicles at the level of the	Thanks to the validated mathematical models of defect inflows, the companies can now

snabbare kunna industrialisera resultaten och öka kundvärdet.	complete EE system. This will lead to increased technical maturity of the electrical system of the car. Mature and dependable software in the car will increase the customer value	predict whether their product is ready for release. This leads to better test planning, lower costs and faster releases of high-quality functionality to the customers.
Metoder och verktyg för fordonsutveckling*:* *Säkerställa att den svenska fordonsindustrin bidrar och får tillgång till metoder, verktyg och kompetens i världsklass för att möjliggöra snabb och effektiv utveckling.*	This research project will provide methods that complement existing development process and new tool chains for cost-effective verification of safety critical EE-systems and software with the goal to increase competitiveness of Volvo Cars and to increase development speed of dependable EE systems.	The project developed new methods of Fault Bypass Modelling (FBM) and the combination of mutation testing with fault injection. The FBM method can reduce the cost of testing by more robust test environments. The second method increases the certainty that no unknown defects are left in the product after the Verification and Validation activities.
Contribution to targets stated in the template "Vägledning FFI ansökan engelsk februari 2011"		
how well the project satisfies the targets defined within transport, energy and environmental policy	Indirectly by providing enabling technology for developing dependable active safety systems.	Verification of systems using FBM increases dependability.
the ability of industry to operate knowledge-based production in Sweden in a competitive way	Not applicable for this project; this is a knowledge –based project focused on the development of safety-critical systems.	N/A
contribute towards a vehicle industry in Sweden that continues to be competitive	This research project focuses on methods and tools to efficiently and with high quality develop and validate distributed safety-critical embedded systems, such as active safety systems. Safety is one of the most important areas in the evolution of the vehicles, efficiency and quality is the key enablers for Sweden to be competitive.	In the project we validated the results based on the open data set from Audi as well as the data from Ericsson and Saab Electronic Defence Systems. The results of the validation contributed to increased portability and thus quality of the software development methodologies at our industrial partner.
undertake development initiatives of relevance to industry	Fulfilment of ISO 26262 and effective argumentation supporting that fulfilment is a key in developing safety systems in the future. This project will provide methods to do that in quantitative ways, which will support the industrial partners in being drastically more efficient in ISO 26262 implementation.	In this project we evaluated defect prediction models in a number of scenarios and established the parameters under which they are valid. This allows to predict such project parameters as product release readiness or the number of residual faults in the system.
lead to industrial technology	This is a research project with a focus	The developed new architecture

and competence development	to strengthen the conformance of automotive electrical systems to ISO 26262	view (Safety view) provides the ability to link safety argumentation with the construction elements of the vehicle's software (e.g. classes, blocks and components). This enables explicit traceability and therefore the ability to develop safer software.
contribute towards secure employment, growth and stronger R&D operations	This research project aims to strengthen the competencies to efficiently validate ISO 26262 requirements. This is one of the enablers to efficiently develop safer vehicles and stay competitive in the automotive industry. If the vehicle industry can stay competitive, it will contribute to secure employment and growths. As this is proposed to be an industrial Ph.D. project, it will contribute to stronger R&D operations with a much needed competence combining mechatronics and software engineering.	The project resulted in the education of one PhD (Rakesh Rana), one professor promotion, three invited presentations and 22 publications. All of the above contribute to the stronger R&D environment in the project consortium.
contribute towards actual improvements being made to production at participating companies	Not applicable, the focus on this project is on the development and validation of safety-critical systems.	N/A
strengthen research environments in selected, prioritised research areas in the field of production technology	Not applicable as the focus of the project is on R&D of automotive vehicles.	N/A
support environments for innovation and collaboration	This is a research project done in close collaboration with *Software Center* at Chalmers which is a collaborative research environment with a number of partners from industry and academia. The results of this project will be of high interest for other members of the Software Center.	The results of the project were introduced to Ericsson and Saab Electronic Defence Systems (Software Center Partners). The project has presented the results at a number of dedicated events organized for the Center's partners, each of ca. 100 participants.
strive to ensure that new knowledge is developed and implemented, and that existing knowledge is implemented in industrial applications	This is a project where the results are validated in in-kind projects at the development organization at Volvo Cars (electrical systems), where the doctoral students are planned to work on-site at Volvo Cars aligned with in-kind projects. Through case studies we maximize the benefit from the results in industrial applications at	As mentioned above, the results were validated at other companies and introduced to Volvo Cars in form of measurement systems and visualization systems.

	Volvo Cars, later generalized to other industrial contexts.	
rationalise the application of R&D results so that actual production improvements are implemented in participating companies	Not applicable as this project is only focused on the development and validation of software systems.	N/A
improve the quality of technical production training	Not applicable as this project is only focused on the development and validation of software systems.	N/A
reinforce collaboration between the vehicle industry on the one hand and the Swedish Road Administration, universities, colleges and research institutes on the other	Indirectly as we do not plan to explicitly involve the Swedish Road Administration since they are not part of product development at Volvo Cars.	N/A
strive to secure national supplies of competence and to establish R&D with competitive strength on an international level	ISO 26262 is an international standard and its implementation has an influence on the international level. Those companies which have efficient ISO 26262 realization at the complete electric system levels will need the competence provided by this project	The results of this project were disseminated in a number of workshops with our partners, many of the workshops were focused on teaching the methods used in the project.

6. Dissemination and publications

6.1 Knowledge and results dissemination

So far the dissemination of the results has been done internally in the project and externally. Internally, the project conducted a number of workshops at our industrial partner and made a number of presentations. Externally, the project has disseminated the results through conference presentations, journal and book publications.

As stated in the application for funding, the project has collaborated closely with Software Center (a collaborative center at Chalmers / University of Gothenburg with ten companies and five universities). Thanks to numerous presentations at Software Center we could validate the results at other companies – Ericsson and Saab Electronic Defense Systems (paper #3 and paper #4 in Section 6.2). We have also conducted presentations at large forums like *Elektronik i fordon* in 2015 where over 100 automotive engineers participated.

Finally, we organized three workshops on automotive software engineering, where we disseminated the results to the international forum. As a result of that dissemination we could conduct a study with data from Audi to cross-validate the mathematical prediction models used in our project.

6.2 Publications

During the course of the project we focused on the direct dissemination of the results at different levels – from a book about automotive software architectures (in press) through journal papers and conference presentations, to organization of international workshops on automotive software architectures. Below we provide the full list of publications of the project results

1. Book: M.Staron, *“Automotive Software Architectures – An Introduction”*, under publication, to be launched in connection with ICSE (International Conference on Software Engineering), 2017. Publisher: Springer
2. Book Chapter: R. Rana, M. Staron, C. Berger, J. Hansson, M. Nilsson and F. Törner, *“Early Verification and Validation According to ISO 26262 by Combining Fault Injection and Mutation Testing”*, chapter in Communications in Computer and Information Science" (CCIS) Series, Springer-Verlag, 2015
3. Journal: R. Rana, M.Staron, C.Berger, J. Hansson, M. Nilsson, W. Meding, *“Analyzing Defect Inflow Distribution and Applying Bayesian Inference Method for Software Defect Prediction in Large Software Projects”*, Journal of Systems and Software, 2017.
4. Journal: Rakesh Rana, Miroslaw Staron, Christian Berger, Jörgen Hansson, Martin Nilsson, Fredrik Törner, Wilhelm Meding, Christoffer Höglund, “*Selecting software reliability growth models and improving their predictive accuracy using historical projects data”*, Journal of Systems and Software, 2015.
5. Conference: Miroslaw Staron, Darko Durisic, Rakesh Rana, *“Improving Measurement Certainty by Using Calibration to Find Systematic Measurement Error - A Case of Lines-of-Code Measure”*, KKIO Software Engineering Conference, 2016.
6. Conference: Staron, Miroslaw. *"Automotive Software Architecture Views and Why we need a new one–Safety view"* In Workshop CARS 2016-Critical Automotive Applications: Robustness & Safety. 2016.
7. Conference: M. Staron, R. Scandariato, *“Data veracity in intelligent transportation systems: the slippery road warning scenario”*, Intelligent Vehicles (IV’16), 2016.
8. Conference: R. Rana, M. Staron, *“Machine Learning Approach for Quality Assessment and Prediction in Large Software Organizations”*, 6th IEEE International Conference on Software Engineering and Service Science, 2015
9. Conference: R. Rana, M. Staron, C. Berger, *“On the role of cross-disciplinary research and SSE in addressing the challenges of the digitalization of society”*, 6th IEEE International Conference on Software Engineering and Service Science, 2015.
10. Conference: R Rana, and M Staron, *“When Do Software Issues and Bugs Get Reported in Large Open Source Software Project?”*, in International Conference on Software Measurement (Mensura), 2015.

11. Conference: R Rana, M Staron, and C Berger, *“Improving Dependability of Embedded Software Systems Using Fault Bypass Modeling (FBM)”*, in KKIO Software Engineering Conference, 2015.
12. Conference: Rakesh Rana, Miroslaw Staron, Jörgen Hansson, Martin Nilsson: “*Defect Prediction over Software Life Cycle in Automotive Domain - State of the Art and Road Map for Future”*. International Joint Conference on Software Technologies ICSOFT-EA Conference, 2014.
13. Conference: Rakesh Rana, Miroslaw Staron, Jörgen Hansson, Martin Nilsson, Wilhelm Meding: “*A Framework for Adoption of Machine Learning in Industry for Software Defect Prediction”*, International Joint Conference on Software Technologies ICSOFT-EA Conference, 2014.
14. Conference: Rakesh Rana, Miroslaw Staron, Christian Berger, Jörgen Hansson, Martin Nilsson: “*Analysing defect inflow distribution of automotive software projects”,* PROMISE 2014: 22-31
15. Conference: Rana, Rakesh, Miroslaw Staron, Christian Berger, Jörgen Hansson, Martin Nilsson, and Wilhelm Meding. "*The Adoption of Machine Learning Techniques for Software Defect Prediction: An Initial Industrial Validation*." In Knowledge-Based Software Engineering Conference, 2014.
16. Conference: M. Staron, R. Rana, W. Meding, M. Nilsson, *"Consequences of Mispredictions of Software Reliability: A Model and its Industrial Evaluation"*, International Conference on Software Process and Product Measurement (Mensura), 2014.
17. Conference: Rana, Rakesh; Staron, Miroslaw; Berger, Christian; Hansson, Jörgen; Nilsson, Martin; Törner, Fredrik: “*Evaluating long-term predictive power of standard reliability growth models on automotive systems”*, 24th IEEE International Symposium on Software Reliability Engineering, 2013.
18. Conference: Rana, Rakesh; Staron, Miroslaw; Berger, Christian; Hansson, Jörgen; Nilsson, Martin; Törner, Fredrik: “*Comparing between Maximum Likelihood Estimator and Non-Linear Regression estimation procedures for Software Reliability Growth Modelling”*, International Conference on Software Measurement (Mensura), 2013.
19. Conference: Rana, Rakesh; Staron, Miroslaw; Berger, Christian; Hansson, Jörgen; Nilsson, Martin; Törner, Fredrik: “*Improving Fault Injection in Automotive Model Based Development using Fault Bypass Modeling”*, 2nd Workshop on Software-Based Methods for Robust Embedded Systems (SOBRES), 2013.
20. Conference: Rana, Rakesh; Staron, Miroslaw; Berger, Christian; Hansson, Jörgen; Nilsson, Martin; Törner, Fredrik: “*Increasing Efficiency of ISO 26262 Verification and Validation by Combining Fault Injection and Mutation Testing with Model Based Development”*, International Joint Conference on Software Technologies-ICSOFT-EA, 2013.
21. Conference: Rana, Rakesh; Staron, Miroslaw; Mellegård, Niklas; Berger, Christian; Hansson, Jörgen; Nilsson, Martin; Törner, Fredrik: “*Evaluation of Standard Reliability Growth Models in the Context of Automotive Software System*s”, International Conference on Product-Focused Software Process Improvement, 2013.

22. Conference: Rana, Rakesh; Staron, Miroslaw; Hansson, Jörgen; Berger, Christian; Nilsson, Martin; Törner, Fredrik: "*Verification of ISO 26262 Software requirements in safety critical EE-systems*", ICRES Double workshop" Benchmarking Functional Safety and Efficient Systems, 2012.

During the project we organized two international workshops about automotive software architectures. The workshops are co-located with the largest conference on software architectures with over 200 participants. The link to these workshops are:

- 2015: http://www.win.tue.nl/wasa2015/
- 2016: http://www.win.tue.nl/wasa2016/

The third workshop is going to be organized in 2017 in Gothenburg co-located with the same conference, to make sure that the results of the projects are disseminated after the project is finished. The link to the workshop is: http://www.win.tue.nl/wasa2017/.

Finally, we have also organized a workshop co-located with XP 2016 conference (eXtreme Programming) to disseminate the results in communities that can bring in new experience to automotive software development - http://xp2016.org/cfp/devops.html.

7. Conclusions and future research

The objective of the VISEE project was to develop cost-effective ISO 26262 requirements validation through the use of statistical models and optimal defect injection during simulations combined with testing. We achieved this objective by developing two new testing methods (FBM and a combination of model fault injection with mutation testing) and identification of the best defect-inflow prediction models for the entire EE system development.

The results from the project enables the automotive companies to predict when the products are ready to release with respect to the quality of the embedded software in the car. This kind of predictions, when done on the ECU level, can be used in safety argumentation and linked to the architectural models as shown in the project.

The continuation of the work of this project is to develop tooling for automated generation of software quality assurance plans based on the ISO 26262 ASIL classification of the components. These tools could utilize the defect inflow profiles to optimize the test process wrt test effectiveness.

8. Participating parties and contact person

Chalmers Tekniska Högskola

Göteborgs Universitet

Volvo Personvagnar

Instructions for report

- The report should be written in both Swedish and English (separate reports).
- Maximum length 15 pages
- Use pictures and illustrations if possible.