BeSafe –
BEnchmarking of Functional SAFEty

Project within FFI Fordonsutveckling

Mats Olsson, Volvo Technology AB

2014-05-20

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

Executive summary

Functional safety is becoming increasingly important in the automotive industry to deal with the growing reliance on the electrical and/or electronic (E/E) systems and the associated complexities. The introduction of ISO 26262, a new standard for functional safety in road vehicles, has made it even more important to adopt a systematic approach of evaluating functional safety. However, standard assessment methods of benchmarking functional safety of automotive systems are not available as of today. This is where the BeSafe (Benchmarking of Functional Safety) project comes into the picture. BeSafe project aims to lay the foundation for benchmarking functional safety of automotive E/E systems.

In this document, we present a brief overview of the project along with the benchmark targets that we have identified as relevant for the automotive industry, assuming three abstraction layers (model, software, hardware). We then define and discuss a set of benchmark measures. Next, we propose a benchmark framework encompassing fault/error models, methods and the required tool support to perform benchmarking of functional safety. Finally, we present some preliminary results and highlight potential future works.

The BeSafe consortium consists of Chalmers University, Qrtech, Scania, SP, Volvo Cars and Volvo Technology, with Volvo Technology being the project coordinator and main applicant. The project duration was three years, with project started in January 2011 and ended in March 2014. Project budget was 17 550 500 SEK, of which 8 775 200 SEK was publicly funded.

1. Background

Safety has always been an important property in the automotive industry. The safety provided can loosely be divided into *passive safety*, aiming at mitigating the effects of a crash, and *active safety*, aiming at preventing a crash altogether. An aspect, which is gaining in importance increasingly in the automotive industry, is that of *functional safety*. This is due to the fact that electronics have invaded virtually all vehicle functions and about 90% of all vehicle innovations are centered around software and hardware [1]. As opposed to passive and active safety provided by dedicated systems and functions, functional safety is an inherent attribute in systems indicating their ability to remain safe under various conditions, with and without faults. ISO 26262 [2], a new standard for functional safety in road vehicles, defines functional safety as absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems.

The bases of functional safety are the avoidance of faults (e.g. systematic software faults) or else the detection and handling of faults (e.g. random hardware faults) in order to mitigate their effects and thus prevent the violation of a safety goal by the embedded system [3]. To this end, ISO 26262 [2] provides requirements on an automotive safety lifecycle of electrical and/or electronic (E/E) systems within road vehicles. Furthermore, AUTOSAR (AUTomotive Open System ARchitecture) is a key enabling technology to manage the growing E/E complexity and provides mechanisms as well as systematic design approach to facilitate achieving functional safety of software-based systems [3]. However, standard assessment methods of evaluating functional safety of automotive systems are not available as of today.

2. Objective

BeSafe project aims to lay the foundation for benchmarking functional safety of automotive E/E systems. A common way of evaluating functional safety will improve the industry's ability to provide safer vehicles. Benchmarking is also a way of evaluating to what extent the expected requirements of a system have been fulfilled. Consequently, benchmarking functional safety will be a valuable help in evaluating the fulfillment of safety goals and safety requirements, and will thus be a stepping stone in fulfilling the requirements stemming from the standards such as ISO 26262 [2] and IEC 61508 [4].

We define a number of Benchmark Targets (BTs). A BT can in principle be any system or sub-system which has clear boundaries, and is equivalent to the word element used in ISO 26262 [2]. For each BT, we define a set of measures relevant for providing a useful

benchmark along with methods for assessing those measures, and then evaluate those measures on the selected BTs.

Alongside the work on measures for the selected benchmark targets, the BeSafe project defined a general benchmarking framework in which the benchmarks will operate. This framework will include methodology and process, and tool support – both in terms of tools for performing the actual benchmarks and in terms of supporting the benchmark measures in development tools. The contents of the benchmark result will be made up of multiple measures as defined by the project. Both quantitative and qualitative measures will be included, and the generation of the measurements considers analytical measurements, the process by which the element is developed, and empirical measurements, based on the realizations of the element (e.g., fault injection or robustness testing).

Each included measure will have a clear relation to the functional safety properties of the benchmark target. However, a single measure is typically not sufficient for the benchmark results to be useful. Instead the whole vector of measures will be considered for any particular use of a benchmark result. We focus on four generic uses which are of particular interest to benchmarking of functional safety: (a) *comparison*. Compare suitability of an element with respect to functional safety, during system development/integration; (b) *profiling*. Profile an element for identifying and highlighting strengths and weaknesses with respect to safety; (c) *requirements*. Safety-related requirements on the system, or its elements, can be communicated using benchmark details for a common understanding; and (d) *properties*. In a compositional way, safety benchmarks can aid in assessing system safety properties given safety profiles of its elements.

We consider a generic “V” process model as our reference process to enable straight-forward mapping from BeSafe to ISO 26262. Moreover, we define a use case space in order to identify the realm in which the use cases for the BeSafe project reside. This use case space is a generic description of roles/actors (e.g., functional safety assessor, software developer, software supplier, E/E architect), activities (e.g., specification, evaluation, verification, assessment), process steps (e.g., concept phase, product development, production and operation), artifacts (e.g., E/E architecture, Function, ECU design, Software element) and so on.

3. Project realization

The project is divided into three iterations in time and a number of work packages, structured as illustrated in Figure 1.

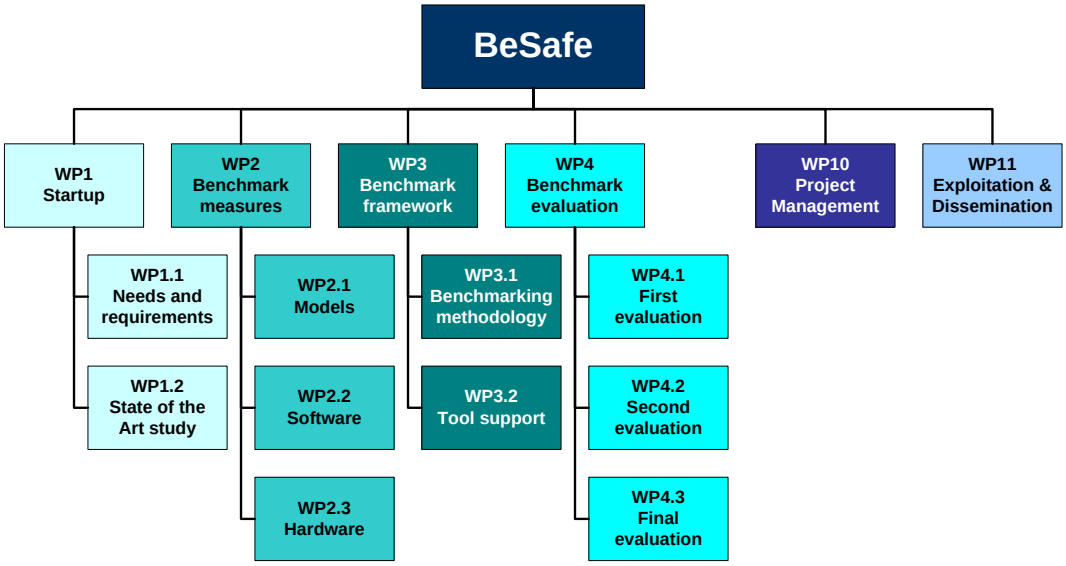

Figure 1. Project work packages.

Table 1 provides more details about the work packages and their contents. The partners, indicated within parentheses, are the designated work package and sub-work package leaders.

Table 1. Work package details.

WP1 Startup – Leader: VTEC	
WP1 will define the requirements for the subsequent work packages, including overall goals, state of the art analysis, investigation of needs and requirements, use cases for benchmarking and benchmark targets.	
WP1.1	Needs and requirements (VTEC). WP1 investigates how benchmarking of functional safety is and could be used by different stake holders in the product creation process. The needs of the identified stake holders are mapped to the uses of safety benchmarks. We will also define the details of the project plan, the goals and vision of the project in order to ensure that all partners work in the same direction, as well as the detailed forms of cooperation among the project partners. A set of benchmark targets will be selected for the project.
WP1.2	State of the Art Study (Chalmers). Many challenges emerging from increasingly digitalized systems are general, and other disciplines, e.g., consumer electronics and telecom, have a relatively long tradition of such issues. The objective of this work package is to identify different methods and mechanisms to assess and benchmark all dimensions of functional safety and to establish state-of-the art within this area.
WP2 Benchmark measures – Leader: Scania	
Based on the requirements from WP1 the measures to be collected for the chosen elements/benchmark targets are defined. Here, we also have the definition of assessment techniques for providing values of the defined measures (e.g. FI techniques, as well as analysis principles), definition of faultload and workload. There	

will be parallel sub-work packages with one area or type of benchmark target per such track.	
WP2.1	Models (SP). This area deals with benchmarking of application models. On implementation level these are designed in Simulink and on more abstract levels they define what the Simulink model structure should be. Architecture solutions in the models (safety patterns and deployment) and control software generated from models, which are benchmarked in WP2.1, will be used as BT's in WP2.2 to enable comparison across software and model-level benchmarking.
WP2.2	Software (VTEC). This area deals with benchmarking of individual components and sub-systems which are integrated in in-vehicle software. Some examples of such components could be either individual modules in or the entire AUTOSAR BSW/RTE. Approaches for assessment of application SW-Cs is also of interest, and especially to be able to correlate results from benchmarks performed on application models with results from benchmarks performed on generated software implementations based on those models.
WP2.3	Hardware (QRTECH). This target area focuses on hardware elements, such as ECUs and power electronics. The following areas are to be examined: Control electronics – evaluation of HW metrics defined in ISO 26262 and similar standards; Power electronics – evaluation of what metrics and targets that are applicable to power electronics in HEVs and EVs. Fault models related to packaging and mounting needs to be examined in order to benchmark safety in this type of systems. Relationship to EV standards such as ECE-R100 is to be considered; and Sensor electronics – evaluation of the safety properties of sensors and sensor models.
WP3 Benchmark framework – Leader: Chalmers	
WP3 defines the overall methodology for how to use benchmark results, and defines how the benchmark should be used in the context of ISO 26262 and other relevant standards and processes. Included is also an account of the necessary tool landscape and tool support for implementing the framework.	
WP3.1	Benchmarking methodology (Chalmers). This part of defines the methodology to follow for performing benchmarking activities, how to use the results and so on.
WP3.2	Tool support (SP). This work package defines the necessary tools needed to implement the defined framework and their interactions. The use of a common data warehouse for storing and accessing benchmark results is evaluated.
WP4 Benchmark evaluation – Leader: QRTECH	
After each iteration the results from WP2 and WP3 is evaluated on case studies and examples. For example, here it is ensured that the results do not conflict with internal methodologies and techniques used by the project partners. Also, we make sure that the measures are useful for the activities we have defined. The efforts entail verification and validation of the requirements from WP1.	
WP4.1	First evaluation. The results from Iteration 1 are evaluated and the results provide input from Iteration 1 to Iteration 2 on any necessary modifications

	or possible refinements.
WP4.2	Second evaluation. The results from Iteration 2 are evaluated and the results provide input from Iteration 2 to Iteration 3 on any necessary modifications or possible refinements.
WP4.3	Final evaluation. Here a final evaluation of the results in this project is performed, with a focus on the new additions and modifications from the second iteration.
WP10 Project Management – Leader: VTEC	
Overall project management is performed here. This work packages also performs wrap-up activities at the end of the project duration and shuts down the project.	
WP11 Exploitation & Dissemination – Leader: VTEC	
This work package deals with disseminating results and exploiting relevant and applicable results at the various project partner organisations, as well as in academia. In particular we plan to have project workshops, seminars, and teaching units.	

4. Results and deliverables

The project results provided a framework for benchmarking of functional safety for a range of areas relevant for the development of automotive electronic systems. Results and findings from relevant work package (see chapter 4) are documented in the deliverables, briefly described in the following chapters.

D1.1 Needs and requirements

This document describes roles and artefacts associated with benchmarking of functional safety. Moreover, D1.1 presents a number of automotive use cases to realize the needs and requirements of benchmarking of functional safety.

Describes how benchmarking of functional safety is and could be used by different stake holders in the product creation process. The needs of the identified stake holders are mapped to the uses of safety benchmarks (comparison, profiling, requirements, and properties). This document also lists and describes the benchmark targets selected for the project.

D1.2 State of the Art

Presents a state of the art study relating the BeSafe results to work done in other domains and other application areas, as well as scientific results in academia. Gives an overview of automotive functional safety standards and describes research in the area of dependability benchmarking. Techniques for fault injection, robustness testing and model-based assessment of functional safety are also discussed.

D2 Benchmark measures

Describes the concepts related to safety elements out of context (SEooC) and in a context with respect to ISO 26262 and a reference model for experimental and analytical benchmarking. For each benchmark target defined in D1.1 Needs and Requirements, a set of benchmark measures are given along with assessment methods for those measures.

D3 Benchmark framework

Provides a framework for benchmarking of functional safety in automotive embedded systems. The framework describes processes as well as methods and tools for performing benchmark activities linked to process standards such as ISO 26262 and ISO 15998.

D4 Evaluation

An evaluation of the proposed measures, assessment methods and framework demonstrating the suitability of the results to development of automotive embedded systems. The evaluation was made on several demonstration and validation systems suitable for the selected benchmark targets.

Delivery to FFI-goals

Here follows our estimation of how BeSafe contributes to the targets set forth in the programme FFI Fordonsutveckling, version 2011-02-01 (Table 2).

Table 2. Summary of visions from the FFI Program description, version 2011-02-01.

Vision Svensk text har tagits från programbeskrivningen, version 2011-02-01. Engelsk översättning av Volvo Technology. *Swedish text is taken from the programme description, version 2011-02-01. English translation by Volvo Technology*	**Level** (Low, Medium, High)
Specific for FFI Vehicle Development	
Svensk fordonsindustri ligger i framkant med fordon, fordons-komponenter och utvecklingstjänster som är säkra, miljöanpassade och energieffektiva. *The Swedish automotive industry is at the forefront with vehicles, vehicle components and development services that are safe, environmentally friendly and energy efficient.*	High
E/E Systems/Embedded Systems and Software	

Vision Svensk text har tagits från programbeskrivningen, version 2011-02-01. Engelsk översättning av Volvo Technology. *Swedish text is taken from the programme description, version 2011-02-01. English translation by Volvo Technology*	**Level** (Low, Medium, High)
Etablera nationell kompetens som förmår att utveckla komplexa inbyggda mjukvarusystem Gröna, Säkra och Anslutna fordon kräver hög nationell kompetens vilken är kapabel att utveckla komplexa elektriska system som nyttjar både ett nationellt och ett globalt utbud av forskning och teknik. *Establish national competence that is able to develop complex embedded software systems. Green, Safe and Connected vehicles require high national skills which are capable of developing complex electrical systems that use both a national and a global range of research and technology.*	High
Materials technology for more efficient vehicles	
Fordonsindustrin har fått användbara och innovativa material samt tillgång till nydanande materialanvändning. 1. Substantiell (mätbar) viktreduktion 2. Substantiell kostnadsreduktion 3. Väsentligt bättre materialegenskaper *The automotive industry has got useful and innovative materials and access to innovative use of materials.* *1. Substantial (measurable) weight reduction* *2. Substantial cost reduction* *3. Significantly better material properties*	Low Medium Low
Methods and tools for vehicle design	
Etablera världsledande metoder och verktyg för fordonsutveckling. *Establish world-leading methodologies and tools for vehicle development.*	High

The Swedish automotive industry is at the forefront with vehicles, vehicle components and development services that are safe, environmentally friendly and energy efficient

Safety is one of the most important areas in the evolution of vehicles. In addition to new vehicle safety systems, we have increasing requirements and focus on functional safety, i.e., a systems ability to stay safe during operation, also in the event of faults.
In the EuroNCAP, vehicle safety is benchmarked, assessing the ability of new cars to protect drivers, passengers, and pedestrians in accidents. Besides that these tests have led to safer cars they have also led to an increased awareness around safety among the public.

Today there is no corresponding standardized evaluation methodology for functional safety. BeSafe has therefore contributed to further development of the Functional safety field by identifying benchmark targets, benchmark measures, and develop a methodology to efficiently and reliably perform such measures. A standardized and reliable way for benchmarking functional safety will improve the industry's ability to rapidly provide safer, more environmentally friendly and more energy efficient vehicles.

Establish national competence that is able to develop complex embedded software systems. Green, Safe and Connected vehicles require high national skills which are capable of developing complex electrical systems that use both a national and a global range of research and technology

The major Swedish OEMs (Volvo AB, Volvo Cars, Scania) along with leading SMEs and research institutes have formed the BeSafe consortium.

In order to maintain Sweden’s leadership in safety and quality the development of new concepts and methods, to quantify the reliability and safety of complex electrical and electronic (E/E) automotive systems, is of utmost importance. BeSafe's results and findings have high potential to contribute to this.

Activities carried out within the BeSafe project strengthens Volvo's and other project partner’s position within research on functional safety for complex E/E automotive systems. The project has also attracted a lot of attention and interest both within Volvo and within the other participating companies and the field of functional safety has been raised on a number of agendas for highlighting the need of increased activity in this area. Furthermore, some of the project results will be used for fulfilling the requirements in ISO 26262. In the short term competitiveness and jobs will be secured by starting up new research projects that are based on the results from BeSafe.

BeSafe is a so-called horizontal FFI project meaning that a number of companies are participating. This enables the building of research and innovation environments that extend beyond Volvo. Here it should be noted that the dissemination of information from projects to academia and research institutes (Chalmers and SP), in the field of functional safety, has created strong links between Volvo, Chalmers and SP and discussions are

ongoing around new ideas for future project proposals. In addition, results from BeSafe are used in an ARTEMIS project called VeTeSS. Its composition offers an internationally competitive research environment in which academia, institutes and industry work together.

Results and findings from BeSafe have directly been reused in other research projects (both national and international). In addition to the projects already mentioned, Volvo has been involved in the preparation of the project proposal Safe ADAPT, which is a proposal under EU's seventh framework programme. Here Volvo has contributed with ideas and proposals based on experience gained from BeSafe and from the internal project (completed in July, 2012), called DEDICATE.

The automotive industry has got useful and innovative materials and access to innovative use of materials: With targets such as substantial (measurable) weight reduction, substantial cost reduction and significantly better material properties

Substantial (measurable) weight reduction and significantly better material properties have not been addressed in this project. Therefore we don't contribute to the achievement of these goals.

Even though initiatives like AUTOSAR there are still problems with misbehavior of E/E systems in cars. It is reported in March 2014 that nearly 60-70% of all vehicle recalls in North America and Europe are due to software errors [5]. In 2009 Toyota had problems with unintended acceleration of cars which could be caused by defects in the software [6]. Recently General Motors was forced to a large recall due to a malfunctioning ignition switch in several car models that could be linked to multiple deaths [7].

Malfunctions similar to those described above causes enormous costs for the vehicle manufacturers. We believe that by standardizing the implementation and interpretation of functional safety analyses performed during the development phase, signification cost savings can eventually be made.

Standardization also reduces development costs since the competition among third-party manufacturers will increase. Using a standard it becomes possible to easily compare functionally identical products, communicate requirements and measuring system characteristics. This in turn leads to a greater variety of safer, more reliable and cheaper products.

The requirement of substantial cost reduction can thus be said to be satisfied.

Establish world-leading methodologies and tools for vehicle development

BeSafe has initiated the development of a general standardized method for benchmarking functional safety in complex vehicle E/E systems. Such a structured method can easily be

integrated into existing development processes and thereby contribute to more efficient and reliable development processes. Among the innovative concepts are:

- Identification of target systems - models, software and hardware
- Techniques to develop metrics for these systems
- Development of tools and a methodology for the measurement and interpretation of the results linked to established development processes and to ISO 26262
- Evaluation of benchmarks, measurement techniques and methodologies

Efficient methods and tools lead to more players with a focus on functional safety, which in turn leads to a greater variety of safer and cheaper products.

5. Dissemination and publications

6.1 Knowledge and results dissemination

Information, i.e. deliverables and other reports, that describes results and findings in the BeSafe project is available for all employees within the Volvo Group, for project partners and for certain selected third parties. A number of activities for the dissemination of project results have been arranged as external and/or internal seminars and workshops. In addition, parts of BeSafe's project results have been re-used in other research projects (e.g. VeTeSS) and in three master thesis works.

Dissemination activities performed within the project timeframe are as follows (Table 3).

Table 3. Performed dissemination activities in the Besafe project.

Date	Event	Main Topics
2011-11-01	First open workshop	• Introduction to BeSafe (Martin Hiller, Volvo) • Framework and tools for benchmarking of functional safety (Daniel Skarin, SP, Johan Karlsson, Chalmers) • Benchmarking functional safety using models (Jonny Vinter, SP, Mattias Nyberg, Scania) • Benchmarking the functional safety of software (Martin Hiller, Volvo) • Benchmarking the functional safety of hardware (Andreas Käck, QRTech, Sylvester Vertetics, Saab)
2012-02-09	Open seminar	• Some observations on the ISO 26262 Functional Safety standard (Olle Bridal, Volvo)
2012-03-08	Open seminar	• Evaluation-driven design of fault handling

		mechanisms (Prof. Johan Karlsson, Chalmers)
2012-04-12	Open seminar	• ISO 26262: Functional Safety Process Capability Determination –An Automotive SPICE approach (Ola Örsmark, Volvo Cars)
2012-05-29	Second Open Workshop	• Introduction to BeSafe (Patrik Isaksson, Volvo) • General Introduction to Benchmark Measures (Mafijul Islam, Volvo) • Analytical Benchmarking (Andreas Käck, QRTECH and Mattias Nyberg, Scania) • Fault Injection Benchmarks (Jonny Vinter, SP) • Tools (Behrooz Sangchoolie, Fatemeh Ayatolahi, Chalmers, Jonny Vinter SP, Johan Haraldsson, Sigurjon Thorvaldsson, Volvo)
2012-11-14	ICES Seminar	• Introduction to BeSafe (Patrik Isaksson, Volvo) • Fault injection-based benchmarking of software components (Johan Karlsson, Fatemeh Ayatolahi, Behrooz Sangchoolie, Chalmers) • Simulation of sensor failures using model-implemented fault injection (Jonny Vinter, SP)
2012-11-29	Open lunch seminar	• Safe cooperative autonomous vehicles in an uncertain environment (Rolf Johansson, SP)
2013-05-30	Third open workshop	• Benchmarking functional safety using Continuous Time Markov Chains (Andreas Käck, QRTECH) • Functional Safety Benchmarking Using Bayesian Networks Derived from Safety Requirements (Mattias Nyberg, Scania) • Do We Need to Inject Double Bit-flip Errors When Benchmarking the Hardware Error Sensitivity of Software Components? (Behrooz Sangchoolie, Chalmers) • Testing Robustness of Software Components in AUTOSAR (Johan Haraldsson, Volvo) • Model-based fault injection in the context of ISO 26262 (Jonny Vinter, Daniel Skarin, SP) • Demo section –fault injection tools
2013-06-27	Master thesis presentation	• Binary-level fault injection for AUTOSAR-based systems (NITHILAN MEENAKSHI KARUNAKARAN) • Robustness testing of AUTOSAR software components (VICTOR JANSSON, JERRY

		LINDAHL)
2014-03-13	Fourth open workshop	• Welcome and BeSafe Project Summary (Mats Olsson, Volvo • Overview of Activities and Results (Johan Karlsson, Chalmers) • Automatic Hardware FMEA:s Using SPICE (Andreas Käck, Qrtech) • Towards Benchmarking Hardware Error Sensitivity (Fatemeh Ayatolahi and Behrooz Sangchoolie, Chalmers) • Functional Safety Benchmarking Using Bayesian Network (Mattias Nyberg, Scania) • Mapping Model-Implemented Fault Injection to ISO 26262 (Daniel Skarin, SP) • Software Metrics in the Context of ISO 26262 (Mafijul Islam, Volvo)

6.2 Publications

An Investigation of the Fault Sensitivity of Four Benchmark Workloads (Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Karlsson, Johan).
SOBRES workshop in Braunschweig, Sep 16-21, 2012.

On the Impact of Hardware Faults – An Investigation of the Relationship between Workload Inputs and Failure Mode Distributions (Leo, Domenico Di; Ayatolahi, Fatemeh; Sangchoolie, Behrooz; Karlsson, Johan; Johansson, Roger).
SAFECOMP conference in Magdeburg, Sep 25-28, 2012.

Benchmarking the Hardware Error Sensitivity of Machine Instructions (Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Barbosa, Raul; Johansson, Roger; Karlsson, Johan).
SELSE workshop in Stanford, Mar 26-27, 2013.

Towards Benchmarking of Functional Safety in the Automotive Industry (Islam, Mafijul; Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Skarin, Daniel; Vinter, Jonny; Törner, Fredrik; Käck, Andreas; Nyberg, Mattias; Villani, Emilia; Haraldsson, Johan; Isaksson, Patrik; Karlsson, Johan).
EWDC workshop in Coimbra, May 15-16, 2013.

A Study of the Impact of Single Bit-Flip and Double Bit- Flip Errors on Program Execution (Ayatolahi, Fatemeh; Sangchoolie, Behrooz; Johansson, Roger; Karlsson, Johan).
SAFECOMP conference in Toulouse, Sep24-27, 2013.

Failure Propagation Modelling for Safety Analysis Using Causal Bayesian Networks (Mattias Nyberg).

2nd International Conference on Control and Fault-Tolerant Systems in Nice, Oct 9-11, 2013.

A Study of The Impact of Bit-flip Errors on Programs Compiled with Different Optimization Levels (Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Johansson, Roger; Karlsson, Johan).
EDCC conference in Newcastle, May 13-16, 2014.

Binary-Level Fault Injection for AUTOSAR Systems (Mafijul Md. Islam, Nithilan Meenakshi Karunakaran, Johan Haraldsson, Fredrik Bernin and Johan Karlsson).
EDCC conference in Newcastle, May 13-16, 2014.

6.3 Master Thesis Works

Robustness Testing of AUTOSAR Software Components (Victor Jansson and Jerry Lindahl).
An automatic prototype tool for robustness testing of AUTOSAR software components (SW-C) is presented.

Binary-Level Fault Injection (BLFI) for AUTOSAR-based Systems (Nithilan Meenakshi Karunakaran).
Proposes a binary-level fault injection technique called BLFI, which performs robustness testing on AUTOSAR-based systems.

Evaluation of Error Handling Mechanisms for Automotive Embedded Systems (Andreas Åkesson and Anton Hemlin).
On-going ..Will be finalized in Jun, 2014.

6. Conclusions and future research

We have presented a framework for benchmarking of functional safety in automotive embedded systems. Three different ways of addressing the benchmark framework have been discussed, namely experimental benchmarking of functional safety, analytical benchmarking of functional safety, and using software metrics for benchmarking functional safety. We presented different tools that can be used along with how to map benchmark measures and methods to functional safety, ISO 26262 standard, and to the defined needs and requirements.

In the experimental benchmarking of functional safety, fault injection experiments were the main mean of the benchmarking. However, only a small subset of available tools and methods has been used in this study. We presented MODIFI, BLFI, and GOOFI-2 as the main tools used to perform fault injection experiments, where they target Simulink model of programs, binary code of programs, and assembly code of programs, respectively. In the analytical benchmarking of functional safety, fault distribution and fault intensities of

a system are the main inputs to the analysis. Analytical methods can be used on both software and hardware systems. Two analytical tools have been used in this study. The first one uses Markov chain models that enable the automatic calculation of the functional safety benchmarking measure with respect to hardware faults and the second one uses Bayesian networks. Finally, we addressed a framework around using software metrics for benchmarking functional safety. An example of a software metrics discussed in this report is Static code analysis where, it is recommended for ASIL A and strongly recommended for ASIL B – ASIL D in ISO 26262-6:2011, Clause 8.4.5 as a method for the verification of software unit design and implementation.

It is worth mentioning that this report is just a starting point for benchmarking functional safety and more future research is required in order to turn it into a generic roadmap towards benchmarking of functional safety. For example more research is needed to be able to properly map benchmark measures defined in the Besafe project to different ASIL levels. This is especially due to the lack of information regarding the frequency and severity of all possible errors. As part of the future research, we would like to compare results achieved by analytical measures and experimental measures. This should be done both at the component level and item level. Moreover, enhancing software components with software handling mechanisms suggested by AUTOSAR is a part of our future work. In addition, in the Besafe project, we mostly targeted software components rather than the basic software in the AUTOSAR software platform. In other words, we mainly focused on out-of-context benchmarking of functional safety. Therefore, in-context benchmarking of functional safety along with targeting AUTOSAR basic software are parts of the future work.

7. Participating parties and contact persons

Volvo Technology AB
Mats Olsson
mats.olsson.2@volvo.com
+46 31 323 59 11

Volvo Technology AB
Johan Haraldsson
Johan.Haraldsson@volvo.com
+46 31 3223915

Volvo Technology AB
Mafijul Islam
mafijul.islam@volvo.com
+46 31 3228296

Chalmers Tekniska Högskola
Johan Karlsson
johan@chalmers.se
+46 31 772 16 70

Qrtech AB
Andreas Käck
Andreas.Kack@qrtech.se

Scania CV AB
Mattias Nyberg
mattias.nyberg@scania.com
+46 8 553 899 57

SP Technical Research Institute of Sweden
Jonny Vinter
jonny.vinter@sp.se
+46 10-516 53 59

Volvo Car Corporation
Fredrik Törner
fredrik.torner@volvocars.com
+46 31 3259271

8. References

[1] K. Lemke, C. Paar and M. Wolf, Embedded Security in Cars, Berlin: Springer-Verlag, 2006.

[2] ISO Standard, [Online] http://www.iso.org/iso/catalogue_detail?csnumber=43464. [Accessed 2013].

[3] Technical Safety Concept Status Report, [Online] http://www.autosar.org/download/R4.0/AUTOSAR_TR_SafetyConceptStatusReport.pdf [Accessed 2013]

[4] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, [Online] http://www.iec.ch/zone/fsafety . [Accessed 2013].

[5] B. Fleming, An overview of advances in automotive electronics, Vehicular Technology Magazine, IEEE 9 (1) (2014) 4{9.

[6] EmbeddedGurus: An Update on Toyota and Unintended Acceleration, http://embeddedgurus.com/barr-code/2013/10/an-update-on-toyota- and-unintended-acceleration, Accessed: 2014-04-08.

[7] Reuters: GM expands ignition switch recall to 2.6 million cars, http://www.reuters.com/article/2014/03/28/us-gm-recall-expanded-idUSBREA2R1Y920140328, Accessed: 2014-04-08.

FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

Adress: FFI/VINNOVA, 101 58 STOCKHOLM
Besöksadress: VINNOVA, Mäster Samuelsgatan 56, 101 58 STOCKHOLM
Telefon: 08 - 473 30 00