Opportunities from Standardization in Automotive Safety Assessment

Raul Barbosa and Johan Karlsson
Department of Computer Science and Engineering
Chalmers University of Technology
SE-412 96 Gothenburg, Sweden
{raul.barbosa, johan}@chalmers.se

ABSTRACT

An important initiative in the automotive domain is the development of the ISO 26262 standard for functional safety of road vehicles. The standard introduces numerous techniques for analysis and verification throughout the lifecycle of automotive systems. There is therefore a need for the scientific community to contribute with new and existing knowledge on safety assessment. This position paper identifies challenges and opportunities for research in automotive safety assessment by connecting the research roadmap published in the AMBER project with the ISO 26262 standard.

1. INTRODUCTION

The automotive industry has experienced a rapid increase in the number and complexity of safety-related electronic and electrical (E/E) systems installed in road vehicles. This has motivated a great deal of effort to improve the existing processes and methods for achieving system safety. An important initiative in this domain is the development of the ISO 26262 standard for functional safety of road vehicles, currently a Draft International Standard [2] expected to be finalized during 2010.

The ISO 26262 standard covers the development of electrical and electronic systems (including the software running) that perform safety-related functions. It specifies processes and requirements for mitigating risks associated to random hardware faults and systematic faults in hardware and software. Given that the standard is on its way to being adopted by the automotive industry, there are many challenges and opportunities for research supporting the processes and methods that it recommends.

Safety assessment is a key topic addressed by the ISO 26262 standard. This topic was also covered in project AMBER (Assessing, Measuring and Benchmarking Resilience). The project – a research coordination action – aimed to study resilience assessment, measurement and benchmarking for computer systems. The consortium, consisting of seven members from academia and industry, published among other documents a *research roadmap* [1] identifying developments that the field should have in the future. The goal of this position paper is to connect the research roadmap with the ISO 26262 standard, and identify challenges and opportunities for research in automotive safety assessment.

CARS '2010, April 27, Valencia, Spain

2. THE AMBER RESEARCH ROADMAP

The AMBER research roadmap provides a research agenda in assessment, measurement and benchmarking of computer systems. The document has a broad scope that is reflected in the motivating scenarios that are described in its early pages: *future internet* (including green urban transport and network 2020: information on the move); *embedded subsystems in automobiles*; *information management in a financial enterprise*; *high-level education for IT administration*; and *safety certification and regulation.*

The main body of the roadmap (Chapter 4) is divided into four areas of research. The first area addresses the *scientific and technological foundations.* The second area deals with research efforts in *measurement and assessment.* The third area discusses issues related to *resilience benchmarking.* The fourth area targets activities in *education, training, standardization and take up* of technologies for assessment, measurement and benchmarking.

In each of the four areas, the roadmap specifies a comprehensive list of research needs, challenges, objectives and actions. This research agenda was constructed using the experience of the consortium in the field, taking into consideration the inputs from diverse stakeholders and experts in the area.

The list of needs, challenges, objectives and actions that compose the roadmap is quite extensive. This lead the consortium to select the items that are seen as deserving high priority, *i.e.*, the (deliberately short) list of items that are considered as priorities for a potential research programme.

Consensus on this kind of prioritization is naturally difficult to achieve, and reflects the viewpoint of the consortium partners. In order to provide also an objective analysis, the document includes six domain-specific perspectives on the priorities, that aim to tailor the roadmap to specific industrial segments. The six perspectives are: *embedded systems*, *transportation*, *certification authorities and assessors*, *future internet technological platforms*, *service architectures, platforms and infrastructures*, and *enterprise security.*

3. OVERVIEW OF ISO 26262

The ISO 26262 standard defines a *safety lifecycle* consisting of three main development phases: *concept phase*, *prod-*

uct development, and *after start of production*. The three phases are structured according to the well-known V-model for systems development, and the standard specifies the activities that should take place throughout the lifecycle.

During the concept phase, a key activity is to determine the safety integrity level of the item (i.e., system or function) under development. The ISO 26262 standard specifies four possible levels – A to D – known as Automotive Safety Integrity Levels or ASILs. Level A is the lowest integrity level and level D is the highest integrity level. The concept phase does not include safety assessment activities, but determines to a great extent the necessary methods to assess safety during product development.

The product development phase is divided into three parts, corresponding to parts 4, 5 and 6 of the standard. Part 4 specifies the activities that should be carried out during product development at the system level; part 5 describes the hardware-level development activities; and part 6 addresses the software-level development activities. These three parts are tightly interconnected and include the specification of safety assessment activities, which are the focus of this paper.

Product development at the system level includes three technical sub-phases addressing safety assessment:

Item integration and testing. This sub-phase aims at integrating the elements that compose an item and to test for compliance with safety requirements (according to the item's ASIL level). Here, the standard recommends diverse assessment methods for each specific goal. One of the goals is to assess the diagnostic coverage provided by hardware fault detection mechanisms, for which the standard recommends fault injection tests and error guessing tests. Another example of a goal is to assess the level of robustness, for which the standard recommends resource usage testing, stress testing and testing for interference resistance and robustness to environmental conditions.

Safety validation. The intent of this sub-phase is to gather evidence supporting that the system complies with the safety goals and that the safety goals are correct and achieved at the vehicle level. The validation methods recommended for safety validation are reproducible tests according to specified test procedures, analyses (such as FMEA, FTA, ETA or simulation), long term tests (e.g., vehicle driving), user tests under real-life conditions, and reviews.

Functional safety assessment. The goal of this sub-phase is to assess the functional safety of the item, which is documented in a functional safety assessment report.

Product development at the hardware level includes three technical sub-phases addressing safety assessment:

Hardware architectural metrics. This sub-phase aims at evaluating an item's hardware architecture in the light of two hardware architectural metrics. These metrics concern the item's ability to handle random hardware faults. Depending on the safety goals, there are target-values that should be met.

Evaluation of violation of safety goals. Addressing random hardware faults, the goal of this sub-phase is to show that the residual risk of safety violation is acceptable. A probabilistic method can be used to quantify and compare the result with the target value for safety violation; alternatively, one may perform an individual evaluation of each identified class of fault.

Hardware integration and testing. This sub-phase addresses hardware testing to determine if the item meets the hardware safety requirements. It includes recommendations on the usage of several hardware integration testing methods (functional testing under environmental conditions, expanded functionality testing, statistical testing, worst case testing, over limit testing, etc.).

Product development at the software level includes three technical sub-phases addressing safety assessment:

Software unit testing. As the name indicates, the goal of this sub-phase is to confirm that the software units fulfil their specification and are free from unintended functionality. Several unit testing methods are recommended (requirement-based testing, interface testing, fault injection testing, resource usage testing, and back-to-back testing). There are also recommendations on methods for deriving test cases (e.g., analysis of boundary values) and metrics of structural coverage at the software unit level.

Software integration and testing. In this sub-phase the software components are integrated and the correctness of the architectural design is verified. The methods recommended for this sub-phase are similar to those used for unit testing (with the exception of the structural coverage metrics).

Verification of software safety requirements. The goal of this sub-phase is to show that the software fulfils the safety requirements in the target environment. The standard recommends several distinct environments for carrying out the verification (hardware-in-the-loop, electronic control unit network environments, and vehicles).

The recommendations made by the standard depend on each ASIL level. Each method is assigned a high recommendation, a recommendation or no recommendation depending on the ASIL selected for a given item. Intuitively, the standard puts more demands on assessment activities related to items with higher safety integrity levels.

4. CHALLENGES AND OPPORTUNITIES

The fact that so many techniques for analysis and verification are being introduced in the lifecycle of automotive systems creates challenges and opportunities for research in safety assessment. This section highlights some of the points that were prioritized in the AMBER research roadmap and that are relevant for the automotive domain.

In the automotive domain it is an important concern to be able to predict, as early as possible, the robustness of any new design. This requires methods for extrapolating measurements from previous designs to new ones, possibly by using the field data accumulated by mature companies. Any such methods should be easy to integrate with existing

development methodologies, such as model-based development, in order to facilitate adoption. Thus, there is a need for:

- methods allowing extrapolation of measurements to predictions of system behaviour, in spite of differences between the system/environment where measurements were taken and the system/environment in operation; and
- improving the cost-effectiveness of methods for safety assessment by developing techniques and tools that can be easily integrated into existing development methods and tool chains.

The ISO 26262 standard places high requirements on the documentation of the entire development process. The goal is to document the necessary arguments sustaining that a given product is safe. This documentation (called a "safety case") allows all stakeholders to access and examine the available evidence. Therefore, an important issue is:

- argumentation processes allowing the formulation of complex arguments, combining evidence from measurements with human judgement, including the ability to treat uncertainty and confidence levels.

Finally, the ISO 26262 standard recommends the usage of techniques such as fault injection, to verify the safety of a system and that the safety mechanisms cover the identified faults. Some guidance is given on the types of faults that should be examined, but there is room for improvement with regards to:

- reference faultloads (sets of faults) that are validated and representative of faults arising in the automotive domain, and practical injection tools to perform the evaluation.

5. CONCLUSION

The upcoming ISO 26262 standard for functional safety of road vehicles is on its way to adoption by the automotive industry. This creates many challenges and also many opportunities to conduct research supporting the processes and methods that it recommends for safety assessment.

Among other topics, safety assessment was covered in the AMBER research coordination action. Aiming to study resilience assessment, measurement and benchmarking, the consortium published a research roadmap, highlighting key areas of scientific and technological development in this field for the future.

This position paper identifies challenges and opportunities for research in automotive safety assessment by connecting the AMBER research roadmap with the ISO 26262 standard. The main needs identified are: extrapolation of measurements, reducing the cost of safety assessment methods, improved argumentation processes, and reference faultloads.

6. REFERENCES

[1] A. Bondavalli, P. Lollini, R. Barbosa, A. Ceccarelli, L. Falai, J. Karlsson, I. Kocsis, A. Kovi, H. Madeira, I. Majzik, L. Montecchi, A. van Moorsel, L. Strigini, M. Vadursi, and M. Vieira. Final research roadmap. AMBER Project Deliverable D3.2 (http://www.amber-project.eu/roadmap.php, accessed 27-01-2010), Dec. 2009.

[2] International Organization for Standardization (ISO). ISO/DIS 26262: Road vehicles – Functional safety – Parts 1 to 10, 2009.