ISO 26262 conformant Verification Plan

Ralf Nörenberg, Ralf Reissing, Jörg Weber*

Specification and Test (GR/PST), Functional Safety (GR/PSP)*
Daimler AG, Group Research and Advanced Engineering
Hanns-Klemm-Str. 45, 71034 Boeblingen
ralf.noerenberg@daimler.com

Abstract: This contribution highlights the challenges of implementing ISO 26262 to an industrial E/E verification and testing environment. A methodology to obtain a verification plan and an adequate test strategy in order to meet ISO 26262 requirements is presented and evaluated in an in-house project.

1 Introduction to ISO 26262

Almost all functionality of a vehicle is realized by embedded systems consisting of networked hardware components with implemented software, and today, a total fraction of 70% to 90% of future automotive innovations is predicted to be based on such systems [Do07]. This increase of software-based functionality however results in higher numbers of possible software faults which may cause system failure [We10]. A 50% ratio of vehicle breakdowns caused by such failures was already estimated by [Be03].

The ISO 26262 [ISO], an automotive domain specific derivation of the generic IEC 61508 standard for functional safety of E/E-systems, addresses this subject [IEC]. Its goal is to further improve the high safety standards of the automotive industry by recommending appropriate methods and tools to contain product safety inherent in specification, design and verification. Central to the specification and design part of the standard are the concepts of risk identification, risk classification and derivation of safety requirements with a corresponding ASIL (Automotive Safety Integrity Level) to avoid or mitigate a particular risk.

2 Challenges to ISO 26262 conformant Verification and Testing

Several OEMs have started pilot projects to integrate ISO 26262 requirements into their industrial environments [Sc09], however, with a strong focus on specification and design processes. This contribution, in contrary, highlights the challenges of integrating ISO 26262 verification by discussing the development of a methodology to 1) to create a project specific “verification plan” according to ISO 26262, part 8, requirement 9.5.1 (short: 8-9.5.1) and 2) derive a sufficient test strategy (8-9.4.2).

The general concept of the ISO 26262 verification approach is the definition of several test objectives to be met on each test level. Further, to accomplish the required objectives, the standard recommends methods for deriving test cases, test methods and coverage criteria to be applied. Foremost, these recommendations are to be understood as a guideline to choose appropriate methods for verification, intentionally demanding a tailoring towards specific work environments. Each OEM thus may elaborate a specific approach, which is unambiguous in interpretation and application and provides a good feasibility within its environment. The three degrees of freedom available by ISO 26262 are: interpretation, selection and combination.

The freedom of interpretation is applicable as ISO 26262 does basically refer to test methods without defining them in detail, e.g. stress testing (4-8.4.2.3.5). Thus, the OEM is free to define the method's exact meaning to its specific environment, or even provide argumentation why an available substitute method applied is sufficient as well (4-4.2).

The freedom of selection is valid as ISO 26262 methods are goal oriented. A right set of "feasible" methods thus is adequate to reach a test objective (4-8.4.1.5; 4-8.4.2.3(.1)). This enables the user to limit methods recommended for a safety requirement to those which are applicable in terms of practicability and usefulness. For example, the method "long term test" may not be reasonable to all safety requirements.

The freedom of combination is given as the standard only recommends an appropriate combination of methods to derive test cases in consideration of the level of integration (recommended test methods), which includes both, selection and combination. Certain combinations of recommended test methods (e.g. 4-8.4.2.3.1) and methods to derive test cases (e.g. 4-8.4.1.5) therefore may be chosen, as some combinations might not even be suitable ("analysis of Boundary values" in dependency with "performance test").

These freedoms enable a variety of verification approaches to be developed. However, the OEM is still in charge to provide (sufficient) argumentation and documentation of its specific approach of functional safety according to ISO 26262: The rationale of the developed test strategy shall be reasonable, the traceability of chosen verification methods to corresponding ISO 26262 requirements and the proof of completeness shall be given. This information is to be documented in the ISO 26262 required verification plan. As ISO 26262 gives only a rough idea on how the document has to be structured, the OEM is strongly advised to define a process to achieve a harmonized and universal verification plan (8-9.5.1). The approach taken at Daimler is shown in Fig 1.

3 Integrated Verification Plan

The integrated verification plan developed at Daimler considers two aspects: First, the work product "verification plan" is achieved by a document template prescribing a standardized, clear and complete framework for documentation. Second, a methodology efficiently guides the developer through filling in the template and to derive an integrated test strategy for a specific project correctly.

The following discussion is focused on ISO 26262 subjects only. However, the great benefit of the presented methodology / verification plan is to be considered the first-time merge of ISO 26262 verification requirements with existing in-house standards and methodologies for systematic derivation of test specifications. Therewith, the methodology also allows the derivation of a tailored test strategy for non ASIL rated systems. Thus, the verification plan is obligatory for all future verification and test activities.

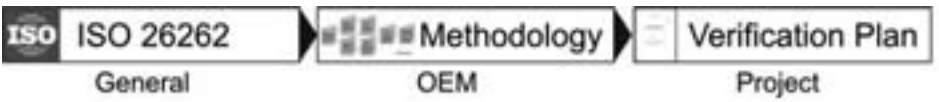

Figure 1: Approach to implement ISO 26262 to a specific project

The supplement of the word integrated to the verification plan describes the generality of the document as all test levels are considered in one document. The integrated view on all test levels provides the most efficient and effective test implementation and execution as it grants identification of test gaps and unnecessary test redundancies over the whole verification process. Moreover, the unified approach allows test objectives to be moved or split up to other possible test levels while ISO 26262 conformance is still met. In case verification activities are distributed over various parties (e.g. OEM and its suppliers), the integrated verification plan also describes the responsibilities of each party and the interfaces between these parties.

3.1 Integrated Verification Plan Template

The integrated verification plan document template is based on the ISTQB interpretation of IEEE 829-1998 test plan [Sp05] [IEEE] and prescribes the structure and relevant content of the template. The 90-page template allows to define test objects, document objects and elements verified elsewhere, define test levels, assign test platforms, to acquire test objectives, select methods to derive test cases and finally, to combine everything into an ISO 26262 conformant test strategy.

The high generality of the document features the ability to be adjusted to specific projects by offering predefined tailoring measures and argumentation choices to be made (for example, consideration of available test platforms) by systematically guiding the developer through ISO 26262 requirements. Of course, in order to assure the sufficiency of ISO 26262 consideration (for argumentation), a separately documented traceability matrix traces the requirements to the proper location in the template. The template is currently provided to in-house pilot projects being subject to ISO 26262 analyses.

3.2 Methodology

The methodology – currently available as a handbook – has been developed to assist filling in the integrated test concept template. In order to guide the user through the most efficient way to fill in the template, a workflow has been defined, whose upper-most level is depicted in Fig 2. As each workflow step is to be completed by determined employees, each step is assigned to certain roles (test manager, test designer, tester).

This masks out all steps not being relevant to the role and thus increases work efficiency. Independent of the role, each available workflow step is split into six subsections: 1) objectives, a description of the main goals 2) required inputs, a specification the required information and documents; 3) procedure, a specification of the individual tasks to performed 4) tools, a list of tools that may assist the tasks 5) work products, a description of intended results and pointers to the locations where to document the results in the template and 6) checklist, to check items to validate the results of this step.

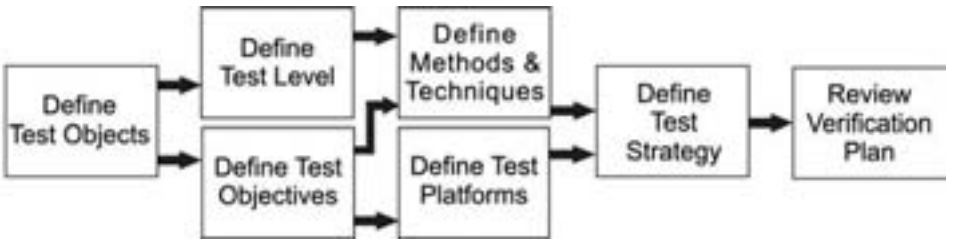

Figure 2: Workflow of the methodology handbook to maintain an integrated verification plan

For a more advanced guidance throughout the topics of the subsections a 3rd level of information has been attached to the individual tasks. This layer consists of 1) background information for general knowledge about the topic, basic ideas and definitions, 2) tutorial on the how to perform the task in detail and how to fill in the template, and 3) an example for a completed section of the verification plan template.

3.3 Towards a Daimler tailored Verification Methodology

The main goal of a Daimler tailored verification methodology is firstly, to provide a highly standardized implementation of the ISO 26262 requirements and simultaneously being unambiguous in interpretation and application, thus being feasible to be put into practice. Secondly, to manage the complex challenge of selecting a right set of methods for verification by using the three degrees of freedom outlined in section 2.

Therefore a twofold approach is chosen: The total quantity of recommended ISO 26262 methods for verification has been evaluated and interpreted to have a standardized and reasonable understanding of the terms and their common sense. Potential substitute methods were also identified. Within the evaluation, the number of methods could be reduced to a smaller number by introducing “test types” – a classification of methods which are similar for all test levels. Defined test types are: function test, interface test, robustness test, performance test, back-to-back test, experience-based test, long term test, and diagnosis test. For example, ISO 26262 defines many interface test methods, which here are summarized by one test type. This approach reduces the number of methods and thus complexity without endangering ISO 26262 conformance.

In order to maintain the link between a test type and ISO 26262 methods it originated from a separate document contains all traceability and background information of the transformation. Of course, knowledge of the original test objective and the method the test type represents at a particular test level is retrievable. In order to document coverage of test methods by a set of test cases (a test specification), test types (multiple choice) are assigned to every test case. Thus, test types offer not only an easy understandable application of the ISO 26262 methods but also an efficient way to meet documentation and organizational requirements.

However, the integration of the freedoms of selection and combination has not been completely resolved yet and is subject to our current focus of research. The approach is to assign safety requirements to a selection of test objectives – an ISO 26262 tailoring similar to the test types is to be considered – which then rule the application of certain verification methods (test types). For example, a safety requirement with a given ASIL is set to meet test objectives "A: validation of robustness" and "B: examination of interfaces" by the safety manager. This now requires the test designer to create test cases with the test types "robustness test" and "function test" (for A) and "interface test (for B). The freedom of selection and combination would thus be reduced by the choice of valid test objectives. The test designer would still have to decide whether all test types ruled by the test objective are necessary or not.

Additionally, this methodology enables an automated evaluation to rate running test activities against defined criteria. Thus if achieved, allowing the conclusion of having obtained – in terms of an entry criterion - an adequate ISO 26262 conformance in the test specification. A manual review therefore may be postponed to the time the entry criterion is achieved, greatly improving personnel capacity and work efforts.

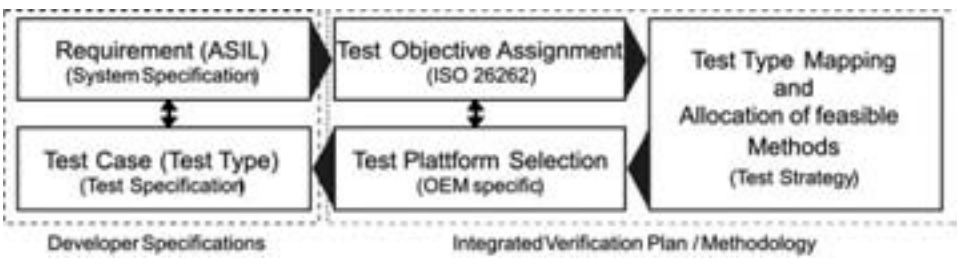

Figure 3: Workflow on how to verify and test ASIL rated requirements with the methodology.

Figure 3 shows the workflow on how an ASIL rated requirement is to be verified and tested. The requirement is assigned to an ISO 26262 test objective which is to be achieved by certain pre-set methods (e.g. test types). The identification of feasible methods is subject to the tailoring guideline of the methodology documented in the verification plan. The assignment to test platforms (on available test levels) is defined by a matrix, however, does allow shifting tests to different test levels in regard to the ISO 26262 test objective to be achieved. The final test cases derived are obtained by the developer/tester and are marked by with the additional attribution "test type" only. The bi-directional traceability to the ISO 26262 methods applied and test objectives covered is provided by the integrated verification plan.

4 Qualitative evaluation of the integrated Verification Plan

Analyses of completed integrated verification plan during a pilot project showed that all strategic and technical information for verification is contained and ISO 26262 compliance is met by using described tailoring mechanisms. The template still needs some improvement on usability at few areas. In order to have the testers complete their own verification plan more efficiently further guidance and automation of the tasks are required. This is subject to current work.

In comparison with ISO WD 26262 (baseline 12), which required an application of all recommended methods to an ASIL rated requirement (and therefore was difficult to be applied in a real life environment due to test and argumentation efforts), the evaluation of the test strategy derived from ISO DIS 26262 shows good conformance for most of the reviewed parts. An attained result of the pilot project therefore is that 1) a general approach on deriving a integrated verification plan containing a 2) project-specific tailoring of the ISO 26262 recommendations becomes necessary in order to achieve ISO 26262 implementation and 3) the ISO DIS 26262 therefore made good progress towards being applicable in practice.

5 Conclusion

The evaluation of the pilot project shows that the challenge of integrating processes and methods required by the ISO DIS 26262 into an existent OEM verification and test environment can be met. A few remaining challenges exist, but are expected to be resolved soon. The introduction of a work-flow oriented methodology to derive an integrated verification plan as well as an ISO 26262 conformant test strategy are on a good development level to face future ISO 26262 requirements. Current research is focused on perfection of the presented test methodology and on an intranet portal solution to present the methodology and its tools in a way that increases usability.

References

[Be03] Behlmer, A.: Discordant notes in the ensemble. Automobil Industrie 48, 16-18 (2003)

[Do07] Dold A., Trapp M.: Herausforderungen und Erfahrungen eines OEM bei der Gestaltung sicherheitsgerechter Prozesse, Lecture Notes in Informatics, (GI), 2007

[IEC] International Electrotechnical Commission: IEC 61508: Generic Standard Functional Safety “Electrical/electronic/programmable electronic safety-related systems”, 2001

[IEEE] Institute of Electrical and Electronic Engineers, Standard for Software Test Documentation (IEEE 829), 1998

[ISO] International Organisation for Standardization: ISO DIS 26262 baseline 15, 2010

[Sc09] Schwarz, J. and Buechl, J.: Preparing the future for functional safety of automotive E/E systems, 21st Int. Tech. Conference on the Enhanced Safety of Vehicles, 2009

[Sp05] Spillner A.: Basiswissen Softwaretest, Page 173, dpunkt.verlag GmbH, 2005

[We10] Weber, J.: An Aspect Driven Approach for the Analysis, Evaluation and Optimization of Safety within the Automotive Industry. SAE 2010 World Congress & Exhibition, 2010