

# Application of ISO DIS 26262 in Practice

Marc Born  
ikv++ technologies ag  
Dessauer Str. 28/29  
D-10963 Berlin, Germany  
+49 30 3480 770  
born@ikv.de

John Favaro  
Intecs S.p.A.  
via E. Giannessi, 5y  
I-56121 Pisa, Italy  
+39 050 9657 511  
John.Favaro@intecs.it

Olaf Kath  
ikv++ technologies ag  
Dessauer Str. 28/29  
D-10963 Berlin, Germany  
+49 30 3480 770  
kath@ikv.de

## ABSTRACT

Automotive manufacturers and suppliers need to follow the requirements stated in ISO DIS 26262 since it is now published state-of-the-art. In this paper we report on experience gained with the application of ISO 26262 in a pilot project at a German car manufacturer as well as experience from various consultancy projects, and recommend a transition from a document-centric approach to safety analysis and associated documentation to a model-based approach.

## Categories and Subject Descriptors

D.2.0 [Software Engineering]: Standards.

## General Terms

Management, Documentation, Design, Standardization, Legal Aspects, Verification.

## Keywords

Safety, process, model, traceability.

## 1. INTRODUCTION

In 2009 the ISO 26262 standard for functional safety of road vehicles became a Draft International Standard (DIS) [1]. Through our activities in safety process consulting and support tool construction we have had the opportunity to work with and observe the ways in which different participants in the automotive industry have approached the incorporation of this standard into their own working environments.

We have observed different attitudes toward the Draft Standard depending on the type of automotive industry participant. In Europe, the United States, and Japan, the *Original Equipment Manufacturers* (OEMs) – that is, the automakers themselves – are currently defining and adapting their safety processes in terms of the ISO DIS 26262 standard.

With Tier 1 and 2 participants, however – those who constitute the major suppliers to the OEMs – the story is more differentiated.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

CARS '2010, April 27, 2010, Valencia, Spain.

Copyright 2010 ACM 1-58113-000-0/00/0010...\$10.00.

While a number of very large Tier 1 suppliers, which are responsible for whole item development and sometimes even for whole vehicle development, are active in the standard definition and production, the majority of suppliers is still hesitant and waiting to see the degree of acceptance of the Draft International Standard by the OEMs and large Tier 1s before committing to it.

## 2. ISSUES FOR INDUSTRY ACCEPTANCE

There are a number of issues influencing the eventual acceptance of the DIS in the automotive industry. Some of these are commercial: for example, some Japanese companies appear to consider ISO 26262 as a barrier introduced to give European and U.S. manufacturers a trade advantage (similar sentiments have been expressed concerning the AUTOSAR initiative [2]). Other concerns, however, reflect uncertainty about the legal impact of the DIS and the availability of the standard as such. Some companies do still not believe that it will be finally adopted (at least not in the near future) due to the large number of comments and issues raised. However, we still expect the voting process will be further processed without major complications. The last vote of the task force at the ISO was held in December 2009 and all parts were voted “YES”. If DIS 26262 is approved in the official vote it becomes FDIS (Final Draft International Standard).

The legal implications of the introduction of ISO DIS 26262 were already a significant point of discussion at the EUROFORUM DIS 26262 Conference in Stuttgart in September 2009. Attorneys Thomas Klindt and Andreas Reuter recalled that the German law on product liability (§ 823 Abs. 1 BGB, § 1 ProdHaftG), which has analogues in other Member States, states that car manufacturers are generally liable for any damage to the health or death of a person caused by a malfunction of the product, and that liability may be excluded only if the potential malfunction could not have been detected according to the so-called *technical state of the art* at the time of placing the product on the market. Since ISO 26262 has now been published – even in draft form – they noted that it may now be viewed as current state of the art, and strongly recommend that it be followed by auto industry participants in order to exclude possible future liability claims.

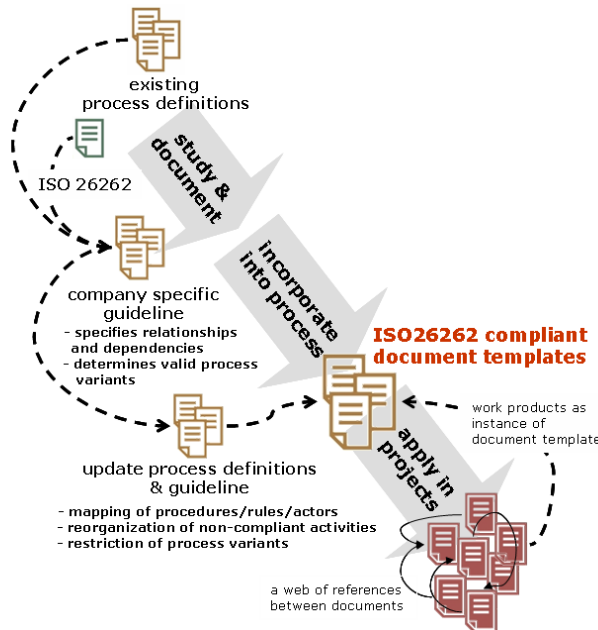
## 3. ISSUES IN 26262 MIGRATION

### 3.1 Investment in Existing Processes

We have found that organizations already had their own safety processes in place, and are unwilling or unable to migrate quickly to an *a priori*, “standardized” ISO 26262 process that is imposed from the outside. Instead, they require that the safety related activities be integrated with their existing requirements and

engineering processes and existing tool landscape. These organizations tend to want to keep their existing processes, as they constitute a significant part of their know-how, and an established and assessed process is considered an important corporate asset. Therefore, they are developing strategies for gradual migration whereby priorities are set on some aspects of their processes.

Specifically, the provision of the *documentation* required by the DIS (and, in case of suppliers, by their customers) in the context of safety analysis is currently seen as a key issue, and a typical strategy of an organisation is to migrate first the documentation activities, and the actual development processes in a subsequent phase. This generally involves the following steps (Figure 1):



**Figure 1 - Document-centric approach to ISO DIS 26262 safety analysis and documentation**

- First, an intensive study of ISO 26262 with regard to work products and requirements;
- Second, a definition/tailoring of process phases in conjunction with company development process and methods;
- Third, the definition of document templates;
- And finally, the company-specific application of the standard.

### 3.2 Document-Centric Approaches

The approach described above is *document-centric*. That is, the effort is concentrated on managing the various documents themselves rather than their relevant content. In this context we have seen many Excel® and Word® templates developed. For example, one customer provided as many as 21 different templates, and another customer is currently adapting his Excel templates from company-specific safety formats towards ISO 26262-compliant formats. (In this context, “ISO compliance” means, for example, adopting the ISO terminology like “Item”, “Safety Goal”, “ASIL” and enforcing the ISO rules concerning e.g. ASIL determination or ASIL decomposition and to reflect that in the respective documents.)

This document-centric approach is not unique to the automotive industry. In nearly all the domains in which we are active in consulting, including railway, defence, and space, we have observed a similar reliance on templates and forms for documentation production and change management. We believe that this approach is fundamentally flawed.

In general, organizations are having trouble keeping up with the documentation requirements of the safety process. The different reports required for different purposes and audiences often contain redundant information, which may lead to consistency problems, if they are managed and updated individually.

In a document-centric approach, sources of dependent, related information are distributed over multiple documents. Information is reused through copy-and-paste techniques. It becomes difficult to manage consistency, since changes in individual artefacts lead to multiple updates in different documents – whereby it is difficult to understand which documents are affected.

The problem is exacerbated under iterative development and versioning: changes in some documents may lead to other use of the information becoming invalid. In iterations and other change scenarios, it is not easy to determine effects.

Finally, document-based approaches offer limited possibilities to offer guidance to safety engineers. Modern techniques such as “context sensitive help” are not applicable with documents. Furthermore, it is difficult to identify the current state of a project solely by analyzing the contents of documents.

### 3.3 Problems with Traceability

A further problem with document-centric approaches is traceability, a key requirement in ISO 26262. Traceability is necessary to show the relations between artefacts, and is a pre-condition for constraint checks, such as the Automotive Safety Integrity Level (ASIL) “inheritance” rules, whereby elements across levels of system decomposition inherit ASIL from higher-level elements.

In document-oriented approaches, traceability is in most cases established through cross-referencing: artefacts are given IDs (reqID, testID, objectID, hazardID, etc.). Then, in various kinds of templates such as Word or Excel tables, cross-references to other artefacts are made via IDs. All traces are created manually, with the attendant risks of errors. Trace management is done manually, or at most semi-automatically. All IDs must be continuously updated and changes must be incorporated into separate, distinct documents – another potential source of error.

Some tools like IBM DOORS already support traceability between some artefacts (e.g. requirements) and help to improve the above situation. There are also some tool-to-tool integrations (e.g. from IBM DOORS to MathWorks MATLAB/Simulink) that allow tracing between elements. However, these solutions are only a first step, since complete traceability among *all* artefacts involved in safety analysis is required.

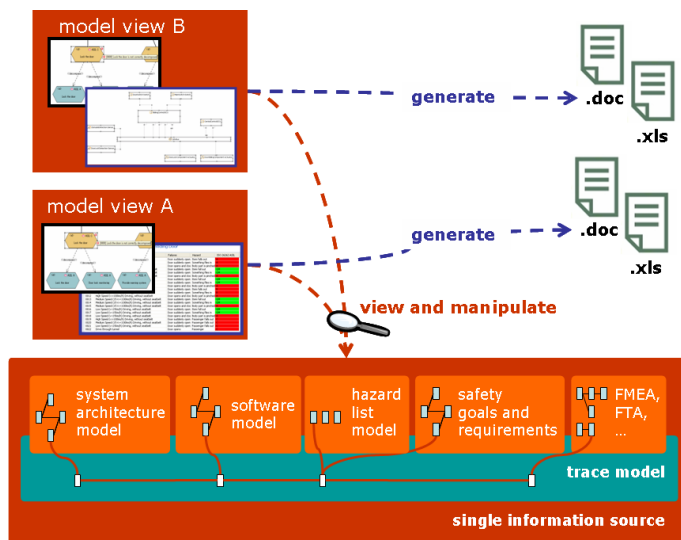
## 4. A MODEL BASED APPROACH

A model based approach to ISO 26262 safety analysis and the provision and management of its associated documentation offers the possibility to solve the problems highlighted in the previous sections. Note that ISO DIS 26262 contains many explicit

provisions for accommodating the model based approach (in contrast to IEC 61508 [3], which contains no mention) because of a growing acceptance of model-based development in the automotive industry [4].

The cornerstones of the model based approach to safety analysis are the following (Figure 2):

- Every piece of information is a model (“even if it is represented as Excel”). Rigorous application of the model/view paradigm separates artefacts from their external representation(s).
- Introduce the principle of a single source of information. No information is stored redundantly.
- Establish fine-grained traces between model elements (rather than between parts of documents).
- Generate and import documents based upon the defined templates.



**Figure 2 Model based approach to ISO DIS 26262 safety analysis and documentation**

Tool and methodological support for this approach have been implemented and are undergoing evaluation in pilot projects.

Obviously, a model based approach may take a longer time for its introduction, depending on the existing development process of the adopter (i.e. to what degree model based methods are already used). A similar stepwise introduction as described in Figure 1 would be intended also for the introduction of model based safety analysis. The difference is that the definition of document templates is not the focus, but rather the definition of the necessary models and their interrelations. Furthermore, considerable effort must be expended for establishing the tool chain, including personal training, that supports the model based development style.

## 5. EVALUATION OF THE APPROACH

We have evaluated the relative merits of a document-centric versus model-centric approach to safety analysis and documentation in a pilot project with a major German OEM, in

which we provided methodological and tool support for the integration of DIS 26262 into their safety processes. In this section we report on the principal advantages cited by the users of this OEM upon conclusion of the pilot.

**Traceability maintenance support.** This was cited in particular between related requirements across system decomposition levels.

**Redundancy elimination.** Consistency is ensured through establishing links in the model instead of repeating content (copy and paste) in documents.

**Standardized choices.** This is another technique enabled by tool-supported, model-based approaches for ensuring consistency. Document-centric approaches are subject to the risk of “semantic drift” in unstructured prose text, whereby different words or expressions are gradually introduced to describe the same concept. A tool can offer standardized choices that ensure that the same concepts are always denoted in the same way.

**Conservation of organisational know-how.** Typical starting points for the ISO 26262 safety process are the driving situations and conditions of use for the new system to be developed and a high level description of the system architecture. The driving situations and conditions are mostly known by car makers and can be re-used. Such possibilities for reuse are not limited only to operational scenarios, but occur also in the context of other safety related artefacts such as safety measures, component failure rates, and the like. Tool-supported, model-based approaches make it possible to store and reutilize these artefacts that constitute a valuable organizational patrimony.

**Consistency checking across safety analyses.** ISO 26262 supports a number of different types of safety analyses. For example, Fault Tree Analysis (FTA) is a top-down technique, whereas Failure Modes and Effects Analysis (FMEA) is a complementary bottom-up technique. Although they are different, however, they must remain consistent with each other. A model-based approach supports semi-automatic consistency checking. Related information can be accessed very quickly and precisely from each individual artefact and ease the work of safety analysis (e.g. FMEA tables can be pre-generated if the system architecture elements are known and known failure modes can be accessed).

**Consistency checking across description and analysis.** A model based approach also supports semi-automated consistency checking between system descriptions and system safety analysis artefacts. For example, in case of a design model change, a tool could automatically check the relations to the safety analysis models like FMEA or FTA.

**Consistency checking between analysis and corporate policies.** Semi-automated consistency checking between system safety analyses and corporate policies is supported. This may include corporate specific guidelines on the re-use of existing components in the system design, the set of existing safety analysis for those components. Another example concerns company specific probability values for tolerable risks, which may exceed the ISO requirements.

**Support for impact analysis.** A model based approach encourages a highly iterative form of development and safety analysis. Impact analysis can be performed in case of iterations or other kind of changes (e.g. in case of a changed system

architecture, which related safety goals must be re-considered). Visualization support is provided for identification of dependencies and the highlighting of areas in which change will have an impact.

**Condition-dependent process guidance.** Model-based approaches make it relatively simple to provide workflow support for safety engineers, guiding them through the various steps required by the standard and/or organisation.

**Context-sensitive help.** As indicated earlier, document-based approaches preclude the provision of context-sensitive help. However, model-driven approaches enable context sensitive help, which may include a wide range of assistance, such as process help, best practice documents, templates or reference documents.

In addition to these observations, another client has expressed a strong interest in the potential of a model-based approach in safety analysis to support the determination and justification of the ASIL of automotive system components. The ASIL is an important factor in determining the cost of developing a component, and can be a source of disagreements between customers and suppliers. For example, a customer might request a supplier to develop a component according to an ASIL that the supplier considers to be unreasonably high (and thus unreasonably costly for the supplier to produce). With the full traceability afforded by model-based tool support, the supplier is supported much more strongly in the exploitation of all kinds of analyses to document and justify a particular ASIL allocation. For example, the availability of component failure rates directly in the model environment, combined with fully traced FMEA analyses, could potentially be fed back into Exposure calculations that justify and document a particular Exposure allocation. Similarly, severity (S) factor estimation is also supported by well-documented techniques such as the Abbreviated Injury Scale [5], which can be incorporated into tool support. Even the traditionally more problematic Controllability (C) factor has been the subject of studies resulting in guidelines that could be candidates for incorporation into methodological guidance in the tool support system [6].

Besides the already mentioned improvements of the safety analysis process by a model based approach, other benefits may arise in the future. For example, model based development combined with model based safety analysis would offer possibilities like fault injection into software models. The potential faults to be injected and simulated could be obtained from the safety analyses like FMEA and FTA. By doing this, the results of the FMEA and FTA could be verified at an early development stage. Doing the safety analyses in a model based manner is a pre-condition for the efficient establishment of a tool chain that supports fault injection [7][8].

## 6. CONCLUSIONS

Much of the work that we expect to see in the near future within organisations will be to reconcile 26262 activities with already-

existing processes, migrating only slowly and only when necessary to different configurations of the process. A flexible, componentized and highly adaptable approach for any supporting tools is the consequence. In the past, safety activities were executed in an isolated manner by individual tools, which is no longer possible when implementing ISO 26262. Some organizations have constructed their own *ad hoc* tools to manage traceability, but we have seen nearly no coherent or consistent approach to safety process traceability emerge from these fragmented efforts.

Our main conclusion gained from first practical experience is that safety analysis must move from a document centric working style with isolated tools for single analysis tasks to a model centric workflow with full fine-grained traceability and supporting automatic generation of role-based reports. Certainly, this implies a strong need for further tool support, a trend which has been already observed in development as well as in quality assurance over the past years.

As stated earlier, however, all the tools need to be adapted to the development and safety processes and need to be customizable to fulfil the requirements of individual users.

## 7. REFERENCES

- [1] ISO/DIS 26262 Road vehicles -- Functional safety.
- [2] AUTOSAR AUTomotive Open System ARchitecture. <http://www.autosar.org/>.
- [3] IEC 61508 Functional safety of electrical / electronic / programmable electronic safety-related systems.
- [4] Törngren, M., Chen, D., Malvius, D., and Axelsson, J. 2009. Model-Based Development of Automotive Embedded Systems. In Automotive Embedded Systems Handbook, N. Navet and F. Simonot-Lion Ed., Industrial Information Technology Series, CRC Press, Boca Raton.
- [5] Copes, W, Sacco, W, Champion, H, Bain, L. Progress in Characterising Anatomic Injury. In Proceedings of the 33rd Annual Meeting of the Association for the Advancement of Automotive Medicine, Baltimore, MA, USA, pp. 205-218.
- [6] Schwarz, J., Code of Practice for development, validation and market introduction of ADAS. 5th European Congress on ITS, Hannover, Germany. 3 June 2005.
- [7] Schlingloff, Vulinovic. Zuverlässigkeitsprüfung eingebetteter Steuergeräte mit modellgetriebener Fehlerinjektion. Proceedings der Jahrestagung der ASIM/GI-Fachgruppe 4.5.5 'Simulation technischer Systeme', 2005.
- [8] Olah, J. Majzik, I. A Model Based Framework for Specifying and Executing Fault Injection Experiments. DepCos-RELCOMEX '09. Fourth International Conference on Dependability of Computer Systems, 2009.