Integration of Development Interface Agreement, Supplier Safety Assessment and Safety Management for Driver Assistance Systems

Thomas Frese, Ford-Werke GmbH, Henry-Ford-Straße 1, 50735 Köln, tfrese@ford.com
Denis Hatebur, ITESYS Inst. f. tech. Sys. GmbH, Emil-Figge-Str. 78, 44227 Dortmund, d.hatebur@itesys.de, and Universität Duisburg-Essen denis.hatebur@uni-due.de
Isabelle Côté, ITESYS Inst. f. tech. Sys. GmbH, Emil-Figge-Str. 78, 44227 Dortmund, i.cote@itesys.de
Maritta Heisel, Universität Duisburg-Essen, Fakultät für Ing.-wissenschaften, Abteilung INKO, Fachgebiet Software Engineering, 47048 Duisburg, maritta.heisel@uni-due.de (korrespondierende Autorin)

Keywords:
Development Interface Agreement, Supplier Safety Assessment and Safety Management Advanced Driver Assistance Systems, Distributed Systems, Functional Safety, ISO 26262

Track: Automotive Engineering

Abstract

The development of electric / electronic (E/E) systems in the automotive domain requires close cooperation between suppliers and the Original Equipment Manufacturer (OEM, e.g. Ford). For most features, the realized software functions are spread over several Electronic Control Units (ECUs) provided by suppliers. The development interface between OEM and each supplier is a crucial aspect for a successful development of complex systems like Driver Assistance Systems. To cope with project management for distributed systems and the cooperation between OEM and suppliers, the international functional safety standard ISO 26262 was developed, and company-specific implementations of this standard were realized.

Our paper presents a successful safety management approach, based on an integration of Development Interface Agreement, Supplier Safety Assessment, and Safety Plan. We illustrate our process by using a Driver Assistant System as a case study.

1. Introduction

For most features in the automotive domain, the realized functionality is spread over several Electronic Control Units (ECUs) provided by a number of suppliers. To develop such a feature a close cooperation between suppliers and the Original Equipment Manufacturer (OEM, e.g. Ford) is necessary. During product development, the involved suppliers and the OEM have to create a large set of aligned artefacts, consisting of textual documents (e.g. specifications, test plans), requirements (e.g. in a requirement management tool), models, source code etc. To improve readability, we will use the term "documents" in this paper. Note that this includes all types of artefacts as mentioned above.

For considering Functional Safety in projects, the ISO 26262 standard is applied. Therefore, it acts as a base of our approach. In Section 1, we briefly introduce the ISO 26262.

Before developing a new approach, we investigated existing work in this field and document the results in Section 2.

Section 4 provides an overview on ISO 26262 requirements considering documenting distributed development. It is subdivided into three part for introducing the *Safety Plan* (Section 4.1), introducing the *Development Interface Agreement* (Section 4.2), and introducing the *Safety Supplier Assessment* (Section 4.3).

Section 5 provides an insight into the current situation in projects developing complex systems in a distributed environment and the challenges they pose. The interaction between OEM and each supplier is a crucial aspect for a successful development of complex systems like Driver Assistance Systems.

In Section 5, we present our approach tackling the challenges mentioned in Section 5 by establishing a defined workflow that ensures a systematic project documentation.

Finally, in Section 6, we provide a conclusion and an outlook on future work.

1. Background

In 2011, the functional safety standard, ISO 26262 [1], was published. It is derived from the generic functional safety standard IEC 61508 [2] and aligns with the automotive safety lifecycle including specification, design, implementation, integration, verification, validation, configuration, production, operation, service, decommissioning, and safety management.

ISO 26262 provides an automotive-specific risk-based approach for determining risk classes that describe the necessary risk reduction for achieving an acceptable residual risk, called automotive safety integrity level (ASIL). The possible ASILs are QM, ASIL A, ASIL B, ASIL C, and ASIL D. The ASIL requiring the highest risk reduction is called ASIL D. In case of a QM rating, the normal quality measures applied in the automotive industry are sufficient. The standard also addresses the OEM-supplier interface to some extent. ISO 26262 Part 8 requires an appropriate definition of the interface between OEM and supplier. This can be achieved e.g. by using a *Development Interface Agreement*). As the application of the standard should be possible in different project scenarios, the standard does not provide a predefined and dedicated method to split technical responsibilities among the different participating parties.

2. Related Work

We are not aware on any work integrating ISO 26262's *Safety Plan*, *Development Interface Agreement*, and *Supplier Safety Assessment*.

However, Dittel and Aryus [5] describe the application of *Safety Plan*, *Development Interface Agreement*, and *Supplier Safety Assessment* in an industrial project without integrating these documents explicitly. Armengaud et al. [6] provide details on the content of a *Development Interface Agreement*. Birch J. et al. [7] describe the role of Safety Cases in safety assessments. Hamann et al. [8] consider the distributed development in the automotive sector and therefore also the use of the *Development Interface Agreement.*

3. ISO 26262 requirements on distributed development

The ISO 26262 standard supports the interface alignment between the OEM and the suppliers by requiring the generation of some documents dedicated to this aspect: the *Development Interface Agreements*, the *Safety Plans*, and the *Supplier Safety Assessment Reports*. In the following sections, we describe the purpose and content of each of the aforementioned documents.

3.1. Safety Plan

The *Safety Plan* supports the overall planning of the safety project, including the definition of the required Functional Safety activities, the generated documents, the roles and responsibilities and the project schedule. Each party, i.e., OEM and each supplier, creates an individual *Safety Plan*. The Safety Manager of each party is responsible for the respective *Safety Plan*. It contains references to other documents and activities and defines the responsible person (being affiliated with the party) for performing, creating, supporting, reviewing, or approving documents and activities. The following documents and activities are considered:

- the hazard analysis and risk assessment,
- the development activities,
- the creation of the *Development Interface Agreement* for distributed development,
- the verification activities,

- the confirmation reviews,
- functional safety audit(s),
- usage of software tools,
- the supporting processes (e.g. document management, change management)
- functional safety assessment(s), and
- the safety analyses

The *Safety Plan* has to be referenced or included in the Project Plan to ensure that it is considered in the projects.

3.2. Development Interface Agreement

For distributed development, the OEM has to apply procedures specified in ISO 26262 jointly with the suppliers of all ECU’s involved in the safety-related feature. All involved parties have to agree on mutual responsibilities and on safety-related procedures concerning planning, execution and documentation. It is required to define safety responsibilities within distributed development and align the *Safety Plan* and all other Functional Safety documents between the OEM and the suppliers. OEM and supplier together have to define in the *Development Interface Agreement*

- who is responsible for which document,
- the type of document exchange (e.g., submit document, or document can only be checked on-site),
- the date of document exchange,
- the extent of document exchange (short document, full document), and
- the level of review (spot check, full technical review, approval).

3.3. Supplier Safety Assessment

The task is to assess the capabilities considering Functional Safety and the implementation of Functional Safety measures. The scope of the Functional Safety Assessment shall include

- the process documents,
- the development documents,
- the processes applied for Functional Safety, and
- the appropriateness and effectiveness of the implemented Functional Safety measures.

The OEM has to appoint person(s) forming an assessment team to carry out a Functional Safety Assessment. The supplier has to ensure the access of the assessment team to relevant information and tools. The assessment team creates a Functional Safety Assessment Report with recommendations for acceptance, conditional acceptance, or rejection of Functional Safety level achieved by the ECU, which is in the responsibility of the supplier.

4. Project Reality – an example of a Driver Assistance System

Modern systems, i.e. Driver Assistance Systems in a vehicle, consist of several sensors (Sensor 1 and Sensor 2, e.g. Camera and Radar), a processing ECU (that can be located in a Sensor), and Actuators (Actuator 1 and Actuator 2, e.g. Brake and Engine) as depicted in Figure 1. Several suppliers realize these ECU's and have interfaces to the OEM who is responsible for the overall system.

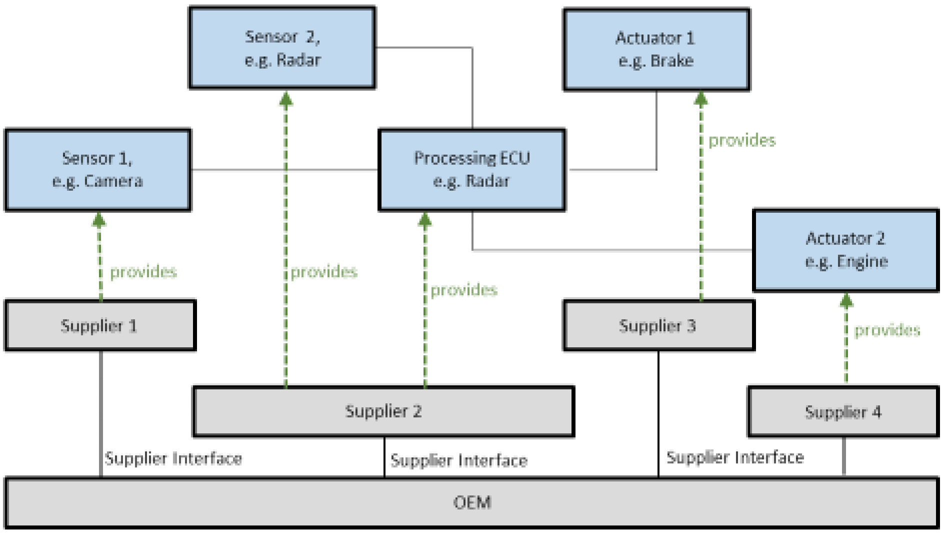

Figure 1: Driver Assistant System Introduction

Each supplier has to create a set of documents to demonstrate that their system is safe enough for its intended purpose and that the ISO 26262 requirements are fulfilled. Figure 2 shows a fragment of the documents to be created.

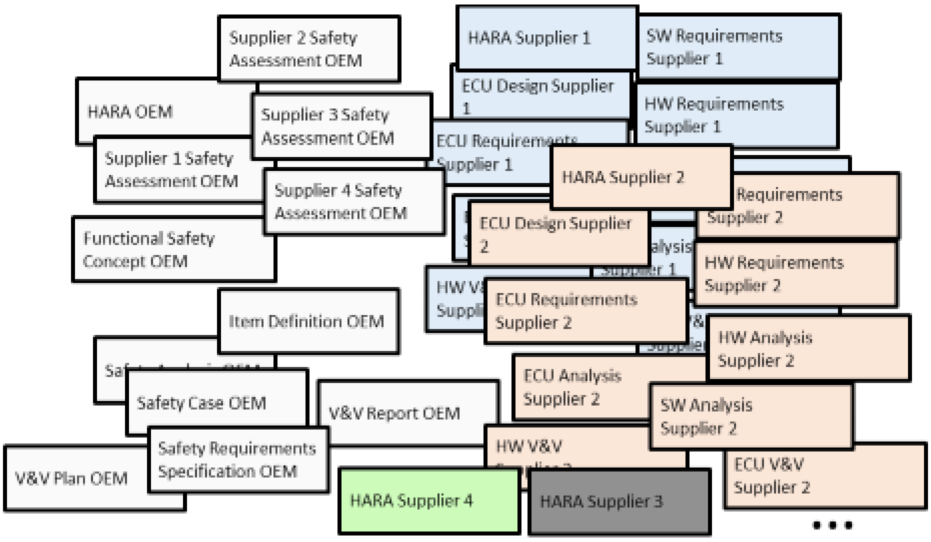
Supplier 2 Safety Assessment OEM
HARA Supplier 1
SW Requirements Supplier 1
ECU Design Supplier 1
HARA OEM
Supplier 3 Safety Assessment OEM
HW Requirements Supplier 1
ECU Requirements Supplier 1
Supplier 1 Safety Assessment OEM
HARA Supplier 2
Requirements Supplier 2
Supplier 4 Safety Assessment OEM
ECU Design Supplier 2
Functional Safety Concept OEM
HW Requirements Supplier 2
ECU Requirements Supplier 2
Item Definition OEM
HW Analysis Supplier 2
ECU Analysis Supplier 2
Safety Case OEM
V&V Report OEM
SW Analysis Supplier 2
Safety Requirements Specification OEM
HW V&V
V&V Plan OEM
ECU V&V Supplier 2
HARA Supplier 4
HARA Supplier 3
• • •

Figure 2: Driver Assistant System Documents

Another problem, increasing the complexity of the situation, is that the OEM and each supplier have a schedule with own milestones. Between these milestones, multiple dependencies exist (e.g., information in one document are necessary to create another document, i.e. Safety Goals are necessary to derive Functional Safety Requirements. Figure 3 depicts the milestones and relations for OEM and one supplier. Note, we do not show the relations to other suppliers explicitly.

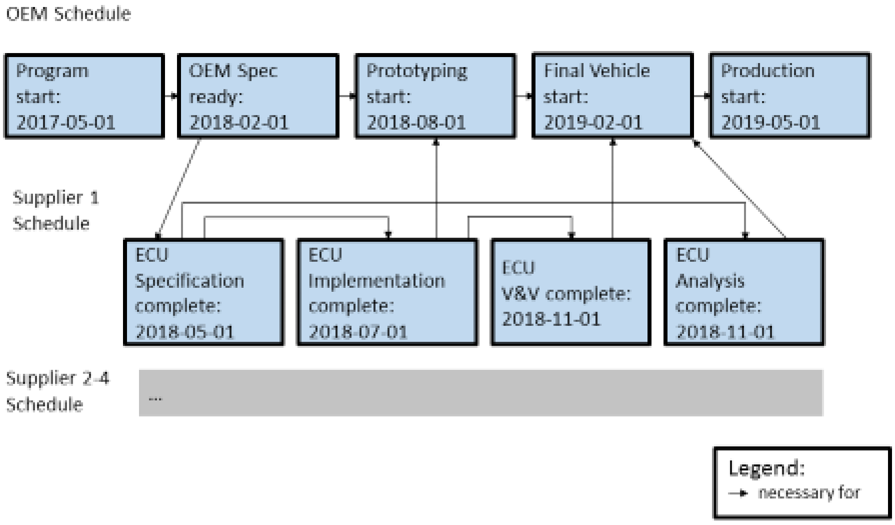
OEM Schedule
Program start: 2017-05-01
OEM Spec ready: 2018-02-01
Prototyping start: 2018-08-01
Final Vehicle start: 2019-02-01
Production start: 2019-05-01
Supplier 1 Schedule
ECU Specification complete: 2018-05-01
ECU Implementation complete: 2018-07-01
ECU V&V complete: 2018-11-01
ECU Analysis complete: 2018-11-01
Supplier 2-4 Schedule
...
Legend:
→ necessary for

Figure 3: Driver Assistant System Time Schedule

Challenges of distributed development are e.g.

- OEM and supplier planning need to be synchronized,

- the maturity of documents needs to be defined for certain milestones to fulfil dependencies,
- for all documents, it must be clear who creates them,
- documentation is spread,
- processes vary between the participating parties, and
- it is necessary to know the overall project status at each point in time.

5. Our Integrated Approach for Distributed Development

To allow an effective project planning and monitoring, we suggest that for each supplier all three documents described in Section 4 should include or reference elements of a separate *Document List* to ensure consistency. In addition to the documents needed to be exchanged between supplier and OEM, this *Document List* includes also internal documents of the supplier.

The internal dependencies of the milestones of each party and the dependencies between OEM and each supplier should be documented. The *OEM/Supplier Milestones Dependencies* make the dependencies of documents (that have to be finished at certain milestones) explicit to allow an appropriate project planning.

A *Project Monitoring Sheet* can be used to track the overall status of the project by monitoring the status of each supplier compared to the planning.

Figure 4 shows the relation of the documents, we describe in the following sections.

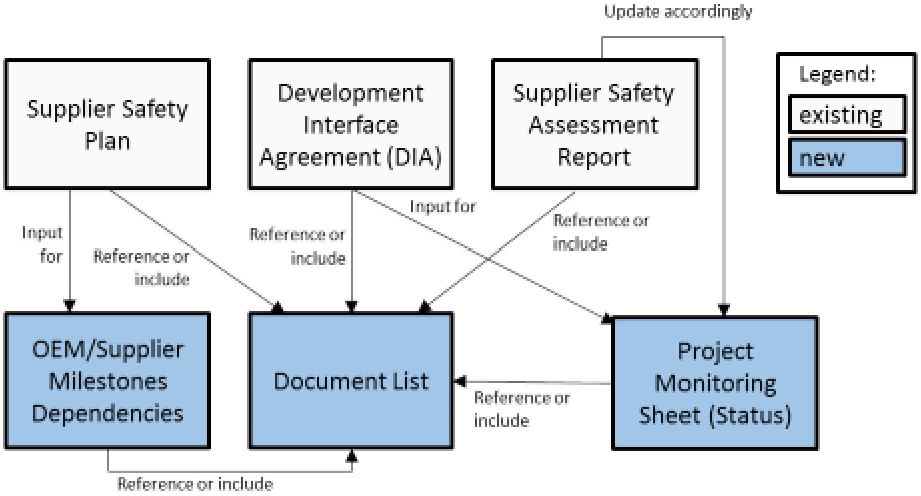

Figure 4: Documents for our integrated approach

5.1. Document List

The *Document List* – maintained by each supplier – contains all documents created by the party. It acts as a central repository for all documents of a supplier and the documents exchanged with the OEM. This list is referenced by all other management documents. For each document, the location where it is stored is documented to allow easy access, e.g. during the Safety Assessment. Additional useful information are target dates or milestones related to the document.

5.2. Safety Plan

All involved parties (i.e., all suppliers and the OEM) perform the safety management supported by a *Safety Plan*. It refers to documents named in the *Document List* (see Section 5.1). This ensures consistency between e.g. *Safety Plan* and *Development Interface Agreement*.

In addition, the milestone planning included in the *Safety Plan* is used as input for the *OEM/ Supplier Milestone Dependencies*.

5.3. OEM/Supplier Milestones Dependencies

The OEM usually has project milestones. For one milestone, a set of documents has to be finalized. To finalize a document, the document owner has to insert all its content and a different person has to complete the review. The supplier milestones should be set in a way that the OEM milestones can be achieved. The creation of one document may depend on the finalization of another document. There can be dependencies between documents of one party but also dependencies between documents of different parties. Usually, it is difficult to see all these dependencies. Therefore, we suggest to document the OEM/Supplier Milestones Mapping. Figure 3 shows an example of such a mapping.

5.4. Development Interface Agreement

The *Development Interface Agreement* defines which of the documents are exchanged and which documents can only be reviewed in an on-site-meeting. For each of the supplier documents it is also defined what kind of review is performed (approval, spot check, alignment with other document …) or if the document is provided for information purposes only. Additionally, all documents are assigned to work products and activities required by ISO 26262. The same is done for the OEM documents, and the direction of document exchange is documented.

We suggest that the *Development Interface Agreement* also

- names those documents that are not exchanged between OEM and supplier
- states who delivers a document at which point in time and the required maturity at fixed points in time.

By doing this, the *Development Interface Agreement* provides the input for the *Project Monitoring Sheet* (see Section 5.6) used for tracking the project progress.

5.5. Supplier Safety Assessment Report

According to our recommendation, the Supplier Safety Assessment focusses on technical engineering documents for the feature instead of process descriptions or presentations only. This helps to investigate how Functional Safety is applied in the project, to detect gaps or issues, and to react with appropriate countermeasures in a timely manner.

The OEM provides technical safety requirements to the supplier. For each technical safety requirement from the OEM, the corresponding safety requirement on the supplier side can be reviewed to ensure a correct understanding, interpretation and implementation. For the downstream activities, e.g. derivation of detailed software requirements or hardware requirements (as described in e.g. Beckers et.al. [3]), the reviews can be limited to spot check reviews of selected examples, to prove the supplier capability on these engineering levels. In the same way, the verification and validation capabilities can be checked. A huge amount of documents is investigated during the Supplier Safety Assessments.

Our proposal is to use the *Document List*, including the information of OEM/Supplier Milestones Dependencies, to plan and to perform the Safety Assessments.

We suggest that the technical details of the assessment are documented in the *Supplier Safety Assessment Report*, and the status of the assessment per document is summarized in the *Project Monitoring Sheet* (see Section 5.6).

5.6. Project Monitoring Sheet

The *Project Monitoring Sheet* documents the status of the project by giving the status of all supplier Documents at the supplier’s milestones.

It is a table with a row for each document to be created and columns for the supplier’s milestones. The fields are filled according to the project plan to show the desired state of all documents according to the milestones. After each assessment, the OEM creates a *Supplier Safety Assessment Report*. According to this report, the supplier inserts the information in the Project Monitoring Sheet. The information could be a “C” if the supplier has completed the reviews required by ISO 26262. It could be an “SR” if the OEM has done a spot-check. In case of a *Supplier Safety Assessment Report* entry that represents a finding in the review, a reference to the corresponding section in the report should be added.

5.7. Benefits of our process

The three newly introduced documents contain information that were previously only in mind (like the milestone dependencies) or spread over several documents (document list and project status). The other documents need only minor changes.

Our process ensures that, e.g.

- OEM and supplier planning is made more explicit,
- the maturity of documents is defined for certain milestones to fulfil dependencies,
- for all documents, it is clear who created them,
- the location of all documents and the authoritative source of each information is known,
- processes are defined and aligned, and
- the project status overview can easily be generated.

6. Conclusion and Future Work

The development of modern electronic features in the automotive domain requires a close cooperation between several parties, mainly the OEM and the involved suppliers. A huge amount of documents is created and needs to be managed. In all stages of the project, the OEM needs to have an overview of the project status, mainly measured by the maturity status of these documents.

For Functional Safety purposes, the international standard ISO 26262 supports distributed development by introducing the *Development Interface Agreement*, the *Safety Plan* (also for all suppliers), and the *Supplier Safety Assessment Report*.

We suggest to use a central *Document List* for tracking all Functional Safety documents created in the project. The internal *dependencies of the milestones* of each party and the dependencies between OEM and each supplier can be made visible in this document list, or in in a separate referenced document. A *Project Monitoring Sheet* ensures the correct tracking of the overall project status. This structure is a key enabler for

- effective synchronization of OEM and supplier planning,
- easy access to all documents during the product development,
- tracking the maturity of document according to the milestones,
- timely detection of gaps / deviations by performing *Supplier Safety Assessments*, and
- continuously monitoring the project status.

Up to now, the proposed process was successfully applied in pilot projects from the domains Chassis Electronics and Driver Assistance Systems. The next step is the company wide evaluation of the process and the introduction of this approach in an overall Functional Safety process. A further step can be to formalize the process by integrating it in the already available model based engineering approach described in Beckers et.al. [4].

7. Literature

[1] International Organization for Standardization (ISO), Road Vehicles – Functional Safety, ISO 26262, 2011.

[2] International Electro mechanical Commission (IEC), Functional safety of electrical/electronic/programmable electronic safety-relevant systems, IEC 61508, 2000.

[3] K. Beckers, I. Côté, T. Frese, D. Hatebur, M. Heisel, Systematic Derivation of Functional Safety Requirements for Automotive Systems, in: Proceedings of SAFECOMP, LNCS 8666, Springer, 65–80, 2014.

[4] K. Beckers, I. Côté, T. Frese, D. Hatebur, M. Heisel, A structured and systematic model-based development method for automotive systems, considering the OEM/supplier interface, in: Reliability Engineering & System Safety, vol 158, 172 – 184, 2017

[5] Dittel T., Aryus HJ. (2010) How to "Survive" a Safety Case According to ISO 26262. in: Schoitsch E. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2010. Lecture Notes in Computer Science, vol 6351. Springer, Berlin, Heidelberg

[6] E. Armengaud , Q. Bourrouilh , G. Griessnig , H. Martin2 , P. Reichenpfader, Using the CESAR Safety Framework for Functional Safety Management in the context of ISO 26262, *in:* ERTS² 2012 – EMBEDDED REAL TIME SOFTWARE AND SYSTEMS, 2012

[7] Birch J. et al. (2013) Safety Cases and Their Role in ISO 26262 Functional Safety Assessment, in: Bitsch F., Guiochet J., Kaâniche M. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2013. Lecture Notes in Computer Science, vol 8153. Springer, Berlin, Heidelberg

[8] R. Hamann, J. Sauler, S. Kriso, W. Grote, J. Mössinger, Application of ISO 26262 in Distributed Development ISO 26262 in Reality, SAE Technical Paper 2009-01-0758, 2009