Abstract. The ISO/DIS 26262 standard on functional safety for road vehicles has a wide implication on the need for information exchange among partners in the automotive domain. As most development today is distributed among several companies and departments, it is important that all information exchange is precise enough to enable the OEM to take full responsibility of the entire functional safety. Still, there is also a need to protect Intellectual Property, because giving away detailed design information may jeopardize the commercial advantage for a company. The solution to this dilemma is a dedicated language for exchanging exactly the needed information in an unambiguous way. In ISO/DIS 26262 there is a standardized reference life cycle in which information should be generated and communicated in each phase. In this paper we show how dedicated language support can facilitate this in the distributed automotive industry structure of today. All phases are covered, but this paper has a special focus on the needs for the concept phase. The dedicated language support is a part of the EAST-ADL2 language. EAST-ADL2 is an AUTOSAR compliant architectural language covering the more abstract views of an automotive E/E system. It is an extendable modular language giving the possibility to add dedicated packages for special purposes. This paper describes the module of EAST-ADL2 dedicated for ISO/DIS 26262 support

Keywords: ASIL, EAST-ADL2, Functional Safety, Functional Safety Concept, ISO/DIS 26262, Safety goal, Safety Life-cycle.
1 Introduction

The automotive industry shares the view that in the next 10 years 90% of its expected innovations will be based on Electrical Electronic (E/E) systems with a huge emphasis on the Safety Systems. This also because the European Commission has the target to reduce by 50% (vs. 2001) the dead rate due to road accidents before 2010 and by 75% before 2020. This important goal will be supported by new passive, preventive and active safety systems to decrease the probability that an accident occurs and to mitigate the consequences on vehicle occupants and other road users. New functionalities for active safety are starting to be available on the market to assist the driver in the task of controlling the vehicle to guarantee the Maximum Vehicle Stability and the Automatic Recovery in Emergency Manoeuvres. Driving assistance functions are based on E/E systems and are built by integrating electronic units (and even software components) from different suppliers. These functionalities are potentially safety-critical, because in case of malfunctioning, they could have an impact on the system behaviour and, consequently, on the vehicle controllability. These hazardous situations could cause severe injury to the involved people. The increasing number of safety critical systems installed in vehicles, coupling among different sub-systems and the increased complexity of the architecture make it necessary to define an appropriate methodology for addressing all aspects concerning the effects of potential faults. In other words it is necessary to define a set of methods to allow the application and management of the functional safety. The methodology has to be unified, internationally recognized and peculiar for the automotive field. The solution adopted by the international community has been to develop and to apply the new standard ISO/DIS 26262 “Road vehicles – Functional safety”. ISO/DIS 26262 represents the state of the art regarding the safety processes with the related methods and the safety requirements for the development, production, maintenance and decommissioning of E/E systems installed in series production passenger cars (currently with a max gross weight up to 3,5 t). This standard has a wide implication on the information exchange among OEMs and suppliers in the automotive domain. As most development today is distributed among several companies and departments, it is important that all information exchange is precise enough to enable the OEM to take full responsibility of the entire functional safety process. The solution we propose is to use a semi-formal approach for exchanging the information specified by the standard in an unambiguous way. An architecture description language for model-based development of automotive embedded systems associated to a “safety analysis based” methodology can cover these needs. In this field EAST-ADL2 (www.atesst.org) provides a well-defined information structure for specifying and managing various engineering concerns and system aspects across development stages. One specific objective of EAST-ADL2 is to provide a native, language-level support for the ISO 26262 safety process and safety concepts, as well as their integration with other aspects of system development.

In this paper we will provide an overview of the ISO 26262 standard and then explain how the EAST-ADL can support development according to the standard in each safety life cycle phase.
2 ISO DIS 26262 Overview

The ISO 26262 is an International Standard for functional safety, intended to be applied for passenger cars. It is the adaptation of IEC 61508 to comply with the automotive specific application related to Electric / Electronic systems within passenger cars. The current status is Draft International Standard (DIS), and the forecasted release is March 2011.

In a later stage (2013), it is planned to evaluate the standard extension to the heavy road vehicles (e.g. trucks, busses).

The ISO/DIS 26262 “Road vehicles – Functional safety” includes guidance to avoid risks, caused by “systematic failures” and “E/E random hardware failures”, by providing feasible requirements and processes.[1]

Central in this International Standard are the concepts of risk and safety goals. The risk is a function of frequency (or likelihood) of the hazardous event and the related degree of injury (severity). Since the approach of the new standard to the risk consists in considering that the zero risk can never be reached, the objective is to reduce the risk to an ALARP level (As Low As Reasonably Practicable level). Afterward, the risk is reduced to a tolerable level by applying safety concepts to reach the safety goals and the safety constraints depending on the risk.

The ISO/DIS 26262 requires to apply the “functional safety approach”, starting from the preliminary vehicle development phases and continuing along the whole product life-cycle. This approach will allow to design a safe automotive system. Furthermore it provides an automotive specific risk-based approach for determining risk classes named ASILs (Automotive Safety Integrity Levels). The new standard uses the ASILs for specifying the item’s necessary safety requirements for achieving an acceptable residual risk, and provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved [1].

ISO 26262 consists of the following parts:

- Part 1- Vocabulary: specifies the terms, definitions and abbreviated terms for application in all parts of ISO 26262.
- Part 2- Management of functional safety: specifies the requirements on functional safety management for automotive applications.
- Part 3- Concept phase: specifies the risk assessment procedure and the requirements to be applied during the concept phase to define a safe E/E architecture archetype.
- Part 4- Product development- system level: specifies the requirements to be applied during the product development at the system level.
- Part 5- Product development- hardware level: specifies the requirements to be applied during the product development at the hardware level.
- Part 6- Product development- software level: specifies the requirements to be applied during the product development at the software level.
- Part 7- Production and operation: specifies the requirements on production, operation, service and decommissioning.
The ISO 26262 safety life-cycle includes the following phases:

- Concept phase, (Part 3)
- System level development – specification, (Part 4)
- Hardware level development, (Part 5)
- Software level development, (Part 6)
- System level development – integration and validation (Part 4)

This paper describes how to perform a safety analysis compliant with the ISO/DIS 26262, by focusing on concept phase, and how the related information can be represented.

### 3 Functional Safety in the ISO 26262 Concept Phase

The EAST-ADL2 supports several of the safety life-cycle phases defined in ISO 26262. Below, we will explain the modeling concepts relevant for the concept phase.

The first step of the safety design flow consists of identifying and describing the “item” under development. It represents the functions, components, or (sub)systems of particular concern in regards to functional safety.

To perform the item safety analysis, it is essential to properly understand the item itself in terms of input(s)/output(s), functionality, interfaces, environmental conditions and, to define the item target function, which is the function description in terms of...
outputs behavior. At the beginning of the safety analysis activities, the boundary of the item and the item’s interfaces with other elements are determined.

To evaluate the risk associated with the item under safety analysis, a risk assessment is carried out. A risk assessment considers the functionality of the item and a relevant set of scenarios (operating conditions & environmental conditions). To identify hazards, the potential sources of harm, it is helpful to define the malfunction(s) related to the item. If the item target function(s) has been correctly identified and described, the malfunction can be always defined in terms of anomalies of function activation. To assess the risk level, hazardous events, the hazard in concomitance with a particular scenario, is considered.

As required by the ISO 26262, for each identified hazardous event, the severity, controllability and exposure values should be ranked, to determine the associated Automotive Safety Integrity Level (level of risk). It is important to remark that the controllability levels assigned to the various situations should be assessed through specific testing on the road, fault injection, etc.

The ASIL specifies the item’s necessary safety requirements for achieving an acceptable residual risk. A risk (R) can basically be described as a function F of the frequency (f) of occurrence of a hazardous event, the ability of to avoid the specific harm through opportune reactions of the involved persons (C = Controllability) and the potential severity of the resulting harm or damage (S = severity); the frequency of occurrence f depends only on the probability of the driving scenario taking place in which the hazardous event can occur (E = exposure) [1].

During the concept phase a safety goal shall be defined for each hazardous event. This is a fundamental task, since the safety goal is the top level safety requirement, and it will be the base on which the functional and technical safety requirements are defined. The safety goal leads to item characteristics needed to avert the hazard or to reduce risk associated with the hazard to an acceptable level. Each safety goal is assigned an ASIL value to indicate the required integrity level according to which the goal shall be fulfilled. For every Safety goal a Safe state, if applicable, shall be identified in order to declare a system state to be maintained or to be reached when the failure is detected, so to allow a failure mitigation action without any violation of the associated safety goal. For each safety goal and safe state (if applicable) that are the results of the risk assessment, at least one safety requirement shall be specified.

4 EAST-ADL2 Support for ISO 26262

EAST-ADL2 provides an ontology and a concrete language for system definition and information management. The purpose of the EAST-ADL2 language is to capture automotive Electrical and Electronic (E/E) Systems with enough detail to allow modeling for documentation, design, analysis, and synthesis.

The language contains multiple levels of abstraction: the VehicleLevel, the AnalysisLevel, the DesignLevel, and the ImplementationLevel. Each abstraction level corresponds to one specific view of the system architecture at a particular development stage. The models at the VehicleLevel provide a top-level view of the E/E system of a vehicle where the intended electronic features are described and
elaborated with respect to its required functionality and its product-line organization. The realizations of such electronic features in terms of logical functions and principal interfaces is given at the AnalysisLevel [3]. A further refined view is provided at the DesignLevel where more implementation-oriented aspects are taken into consideration as well as the hardware architecture. System models at the ImplementationLevel specify the actual software and hardware architectures according to AUTOSAR [4].

The structural aspect of EAST-ADL2 is annotated with additional information in its extensions for requirements, V&V, dependability and timing. A plant model is also defined.

**Fig. 2** An overview of modeling scope and levels-of abstraction by EAST-ADL2.

EAST-ADL2 provides support for the safety design flow and related safety design concepts like item, hazard, and safety concept according to ISO 26262 as shown in Figure 3. This information corresponds to the Dependability extension in the previous picture. Following a top-down approach, the safety analysis can start at the VehicleLevel, beginning with the identification and description of the item. Item is defined in terms of Features. Since the item is a system or array of systems or functions, the Item definition spans all EAST-ADL2 abstraction levels.

As is shown in the figure, Item definition and Hazard & Risk analysis are all modeled on the vehicle level of abstraction in the EAST-ADL2 language. What is inside the scope of one Item could still be identified on any abstraction level, based on the “Realize” and “Satisfy” relations of EAST-ADL2 that identifies what parts of an architecture that has the same scope as the features confining a certain Item.
4.1 EAST-ADL2 Support for ISO 26262

Following a top-down approach, the safety analysis can start from the Vehicle level, beginning from the item’s “target feature” definition (the feature description in terms of the vehicle’s output(s) behaviour). Therefore, on Vehicle level, it is already possible to perform a Hazard analysis and Risk assessment to preliminarily evaluate the “safety relevance” of the Item under safety analysis. For this purpose, the hazards should be evaluated in different scenarios for assessing Severity, Controllability and Exposure. The hazard under analysis, when applied to the various operational situations (operative & environmental conditions), result in the so called “hazardous events” (HE), as you can see in the diagram in Fig. 4.

Each Hazardous Event has to be classified in terms of associated risk defined as its Automotive Safety Integrity Level (ASIL). Since the identified hazardous events are related to a target feature, it makes sense to define (for each hazardous event that appears safety relevant) the Safety Goals on Vehicle level too. In EAST-ADL2, the Safety Goal artifact is modeled as a specialization of Requirement. The ASIL determined for the hazardous event should be assigned to the corresponding safety goal. ASIL and safe state are attributes of the Safety Goal metaclass.
To verify the correctness and completeness of the preliminary Hazard analysis and risk assessment performed on VehicleLevel, a deeper analysis has to be performed, by looking at the architectural level. Therefore the target function on AnalysisLevel should be defined by deriving it from the target feature introduced at the upper abstraction level, see Figure 5. At this point it is possible to define the malfunction as anomalies of the item’s outputs. This serves as a more concrete basis for hazard identification and risk assessment, and therefore offers an opportunity for validation. Note that this process may be iterative and parallel: hazards and risks may be identified and assessed at any abstraction level, but the information is solution independent and Hazards, the Safety Goals and the Safe States are managed as Vehicle level information.
The top-down approach above described is intended to be applicable whether or not the item/function is a new development. In the case of a modification of an already existing item, then an impact analysis is required and a tailored safety lifecycle is advisable. Therefore, with the hypothesis that the safety analysis on VehicleLevel is already available (inherited from original item), the most convenient approach is the bottom-up one, i.e. by entering directly on the AnalysisLevel and by verifying the impact in terms of differences in hazard list and risk assessment outcomes. The vehicle level compared to the analysis level abstracts away all implementation details of a function. This means that even if you have a rough architecture on analysis level to start with, it is easy to present this on vehicle level where you express the Item etc in the language.

For each safety goal and safe state (if applicable), which are the results of the risk assessment, at least one functional safety requirement must be specified. The definition of functional safety requirements only makes sense in EAST-ADL2 at the AnalysisLevel. Note that what is expressed in the ISO26262 standard as “preliminary architectural assumptions” is exactly the purpose of analysis architecture in the EAST-ADL2 language. At this level, the goal is to verify that the functional safety concept realises all safety goals defined at VehicleLevel. More than one safety requirement could be associated with the same Function.

Once the functional safety concept is specified, the item can be developed at the system perspective, starting from the technical safety requirements specification. In EAST-ADL2, this is done at the the Design level. The safety requirements should be allocated to architectural elements, of “system design specification” according to ISO 26262 i.e. elements in the Functional Design Architecture and Hardware Design Architecture. Hence, these activities can be performed only at DesignLevel, when the item is realised with concrete functional elements.
4.2 Example Case

As a case study we illustrate how to apply functional safety according to ISO 26262 to an Electric Parking Brake (EPB) feature, and how the information can be represented in EAST-ADL2.

Electric Parking Brake usually allows enhanced functionality compared to a conventional parking brake and may support e.g. automatic take-off, hill-hold as well as improved user interface. In the example, we only consider conventional parking brake functionality, but assume its realization is an architecture where parking brake and service brake share actuators.

The complete and correct definition of a feature includes the system output(s) identification. For each identified output the corresponding target feature shall be defined. For EPB this means:

- Parking brake [EPB] operates on driver's demand or in auto modes, in coherence with defined proper scenarios.

In particular, we considered the hazard (H) “Sudden loss of braking”, triggered by the Feature flaw “Unwanted Parking Brake deactivation”. To assess the level of risk of the hazard H, we analyzed it in several environmental and operating conditions and thus obtained several hazardous events, e.g. (HE) “Sudden loss of braking when vehicle is parked on a slope road, and driver is out of vehicle”.

In the Table 1 the Risk assessment results are shown.

Table 1 Risk assessment results

<table>
<thead>
<tr>
<th>Hazardous Event</th>
<th>Persons at Risk</th>
<th>Controllability Level</th>
<th>Severity Level</th>
<th>Exposure Time</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sudden loss of braking when vehicle is parked on a slope road, and driver is out of vehicle</td>
<td>(driver), passengers, other drivers [vehicles, motor/bicycles], pedestrians</td>
<td>Expected Task of Persons for Averting Danger</td>
<td>none, the driver is out the vehicle</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C Value</td>
<td>C3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accidental Scenario if Controllability Task will fail</td>
<td>The vehicle moves away without any driver's control: possible accidents with vehicles/ tram/ cycles/pedestrians or out of road</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S Value</td>
<td>S3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E Value</td>
<td>E4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The safety goal defined for the hazardous event is: “do not release the PB force when the driver's presence is not detected on board the vehicle [service brake pedal released]”. The Safe state, that is the system state to be maintained or to be reached when the failure is detected is: “Maintain EPB applied”.

The described risk assessment example is modelled on EAST-ADL2 vehicle level as shown in Figure 6.

To meet the SafetyGoal, a Functional Safety Concept is defined on analysis level. The Functional Safety Concept consists of a functional architecture with functional safety requirements allocated to it. Fig. 7 shows the functional safety requirement being a derived from the safety goal. The requirement is allocated to the architecture with a satisfy relation.
The Functional Safety Concept of the parking brake

Fig. 7. Functional Safety Concept of the parking brake

The Functional Safety Requirements of the Functional Safety Concept can be formalized using safety constraints. These represent the meaning of the requirement in terms of an error model defined for the function. The failure addressed by the safety constraint corresponds to the identified Hazard.

Fig. 8 shows how faults propagate through the error models of the brake function, and that this error model is associated with the nominal model. A safety constraint on a failure on the EPBOutErrorModel formalizes the requirement to avoid parking brake release without driver detected.

Two features, parking brake and service brake, share the same actuators in the presented solution. The same actuator failure therefore represents more than one system failure, which is illustrated by the two failures EPB_OmissionNoDriver and Service_Brake_Omission. To formalize this, the nominal signals HMI_DriverPresent
and HMI_BrakeRequest are included in the error model. They do not represent faults or failures, but are included to formalize the meaning of the system level failures.

Fig. 8 Safety Constraint formalizing the Functional Safety Requirement

5 Conclusion

Functional Safety and means to maintain an adequate safety level are currently highly relevant. This is a consequence of the upcoming international standard ISO/DIS 26262, but also the general trend to add more software and electronics to vehicle functions while maintaining high safety and quality.

This paper has shown an approach to supporting the safety related information related to the ISO26262 life cycle. Being able to unambiguously define the safety related information and have means to trace it, is a huge advantage in contemporary development scenarios. Cost, complexity, correctness and safety are examples of aspects that should be controlled in a distributed development scenario where different roles are responsible for different things. To do this efficiently, systematic and model-based approaches are necessary.

5 Acknowledgements

This work is supported by the EU FP7 Project ATESST2 (Grant 224442).
14 Fulvio Tagliabò¹, Sandra Torchiaro¹, Rolf Johansson ², Henrik Lönn ³, Martin Walker ⁴, Yiannis Papadopoulos ⁴, Anders Sandberg ⁵, DeJiu Chen ⁶

References

2. ATESTST², www.atesst.org