

# ATESST

## ATESST2 newsletter #4 2010



[Click here to download the UML Modeling tool Papyrus and the EAST-ADL2 profile](#)



[Click here to download a presentation with an overview of EAST-ADL2 Dependability Modelling](#)

### Dear Colleague,

in this ATESST2 newsletter, we will present how EAST-ADL2 supports the development of safety critical systems, in compliance with new standard ISO 26262 and we will give a short overview of its connection to AUTOSAR.

Further information about the ATESST2 project and the EAST-ADL2 language can be found at <http://www.atesst.org/>.

### In This Issue

- [Final Open Workshop of the ATESST2 Project, 21 June 2010, Frankfurt](#)
- [ISO26262: short overview](#)
- [Concepts for Functional Safety approach in EAST-ADL2](#)
- [AUTOSAR and Functional Safety](#)

### EAST-ADL2 Spotlight

*ATESST2 defines EAST-ADL2 as a domain-specific language using meta-modeling constructs such as classes, attributes, and relationships.*

*The project also implements a UML2 profile which is used in UML2 tools for user modeling.*

*The EAST-ADL2 definition also serves as the specification for implementation in domain-specific tools.*

**EAST-ADL2**

### Final Open Workshop of the ATESST2 Project, 21 June 2010, Frankfurt

As announced previously we would like to welcome you to the Final Open Workshop of the ATESST2 project.

#### **21 June 2010 in Frankfurt.**

We will present the major results of the project and have a tools and demonstrator session. Participation to the workshop is free of charge and open to everyone interested.

Please confirm your participation by email [atesst-coordinator@vtec.volvo.se](mailto:atesst-coordinator@vtec.volvo.se) by June 11<sup>th</sup>.

*The Workshop starts with a keynote by Stefan Bunzel, Continental. He is currently the spokesperson of the AUTOSAR consortium.*

#### **Agenda**

08:30 Welcome coffee

09:00 Seminar session

12:00 Lunch

13:00 Break-out sessions: Small presentations and demonstrations on selected topics

17:00 End of Day

**ISO/DIS 26262 Spotlight**

The standard consists of 10 Parts:

**Part 1-**

Vocabulary.

**Part 2-**  
Management of functional safety: comprehensive of functional safety assessment.

**Part 3-** Concept phase: risk assessment and functional safety concept.

**Part 4-** Product development-system level: technical safety requirements and verification&validation.

**Part 5-** Product development-hardware level: HW safety requirements and testing&validation.

**Part 6-** Product development-software level: HW safety requirements and testing&validation.

**Part 7-** Production and operation: requirements on production, operation, service and decommissioning.

**Part 8-** Supporting processes: qualification of software tools, qualification of hardware and software components and proven in use argument.

**Part 9-** ASIL-oriented and safety-oriented analyses: ASIL-oriented, and the ASIL

decomposition approach **Part 10-** Guideline on ISO 26262: informative part

**Venue**

Mercure, FRANKFURT ESCHBORN OST

Helfmann-Park 6

D - 65760 Eschborn

Tel +49(0)6196-901-0

Fax +49(0)6196-901-900

h0491@accor.com

[www.mercure-frankfurteschborn-ost.com](http://www.mercure-frankfurteschborn-ost.com)

Topics in the seminar session include EAST-ADL2 Overview, relation to AUTOSAR, methodology, tooling, modelling concepts for variability, safety, requirements and V&V, cooperative systems and environment.

Modelling example and in-depth presentations will concern requirements modelling, cooperative systems modelling, safety and variability.

Tooling examples will include Simulink exchange, fault-tree analysis, feature modelling and variability resolution, AUTOSAR synthesis, timing analysis and cost-dependability-timing optimization.

**ISO 26262: short 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.

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.

The ISO 26262 applies to all activities during the safety lifecycle of safety-critical electrical / electronic systems, the safety workflow 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)

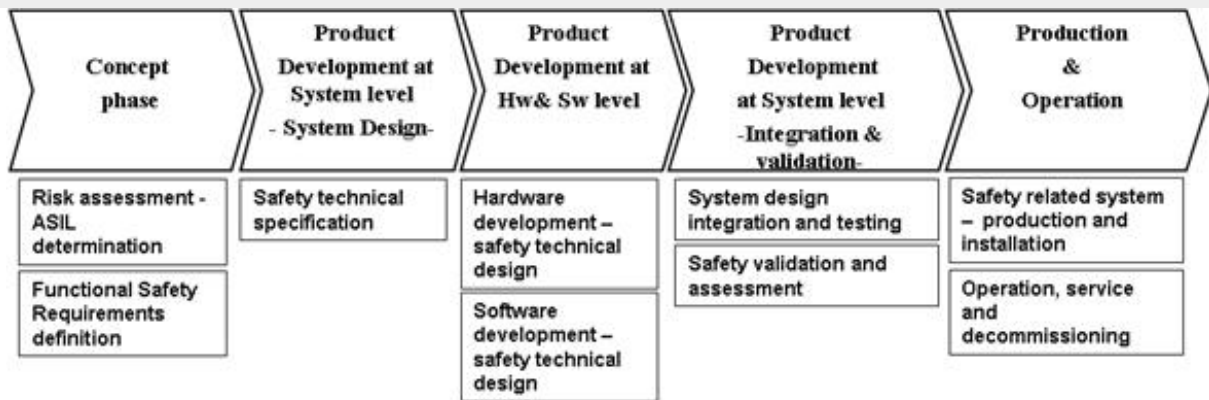


Figure 1. ISO 26262 Safety workflow

### Concepts for Functional Safety approach in 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. Following a top-down approach, the safety analysis starts 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.

Item definition and Hazard & Risk analysis are all modeled on the VehicleLevel 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.

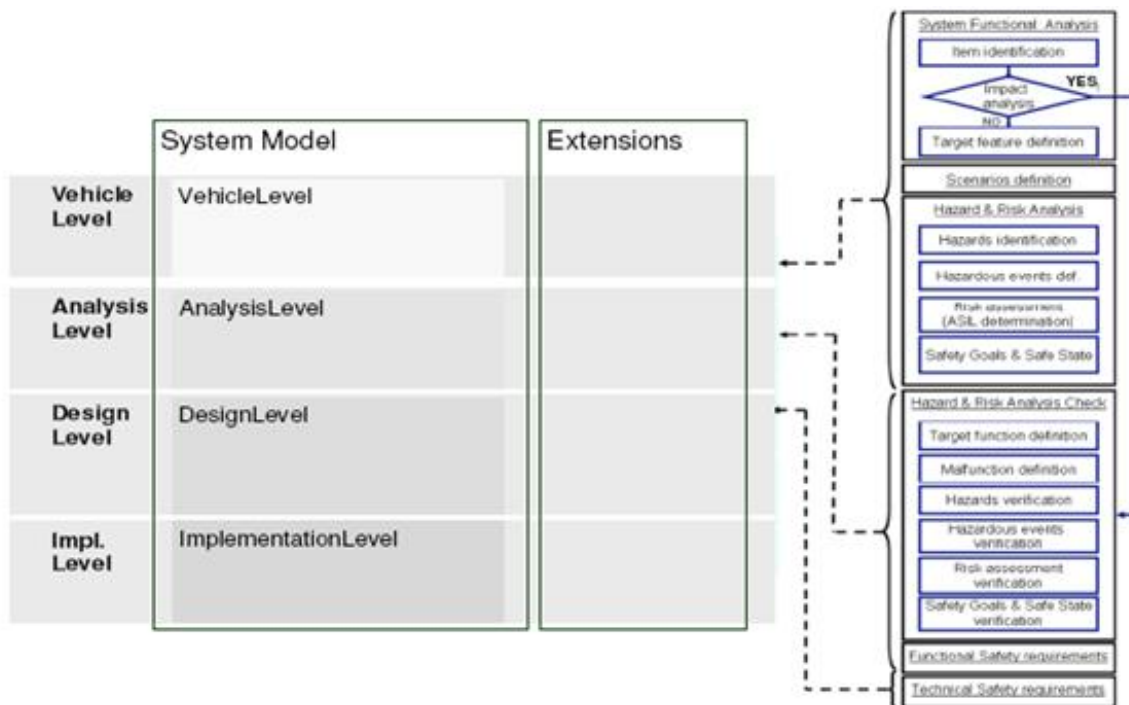


Figure 2. Safety Design Flow linked with the corresponding EAST-ADL2 abstraction level

The safety analysis starts, at EAST-ADL2 VehicleLevel, from the item's "target feature" definition (the

feature description in terms of the vehicle's output(s) behaviour). Therefore, on VehicleLevel, 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), results in the so called "hazardous events" (HE).

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 "VehicleLevel" 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.

## AUTOSAR Spotlight

*AUTOSAR defines a software architecture platform by standardization of its infrastructure and a communication layer suitable for distributed systems.*

*The standard also defines description means for the execution platform including control units, network topology, I/O, and middleware and application software components.*

*The platform and the description means make it possible to integrate software from different suppliers on the same hardware. Reuse is favored and dependencies between application software and hardware are avoided.*

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. 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.

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 DesignLevel. 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.

## AUTOSAR and modeling of Safety Information

One main principle in EAST-ADL is that AUTOSAR should fit in on the implementation level of the system model. In the scope of Safety, this implies that there should preferably be a common pattern for expressing safety requirements in EAST-ADL and in AUTOSAR. This follows the same idea as for expressing timing, which is another non-functional aspect of a system where the general principles are the same for both EAST-ADL and AUTOSAR. Expressing timing was a part of AUTOSAR release 4.0, and for safety this is currently under definition. Recently, there was a workshop called CARS (Critical Automotive applications: Robustness & Safety) where people from the AUTOSAR and EAST-ADL communities jointly showed a possible common pattern to follow. See further "[A Road-Map for Enabling System Analysis of AUTOSAR-Based Systems](#)", CARS'2010, April 27. The current version of EAST-ADL is compliant to this road-map.



If you choose to receive/not to receive future ATESS2 newsletters, please inform [owner-sig-adl@vtec.volvo.se](mailto:owner-sig-adl@vtec.volvo.se).

The ATESS2 consortium

