

“Advancing Traffic Efficiency and Safety
through Software Technology, Phase 2 (ATESST2)”

Safety

ATESST2 Final Workshop

June 21 2010



Automotive E/E Challenges

Multiple domains

Multiple functions/functionalities

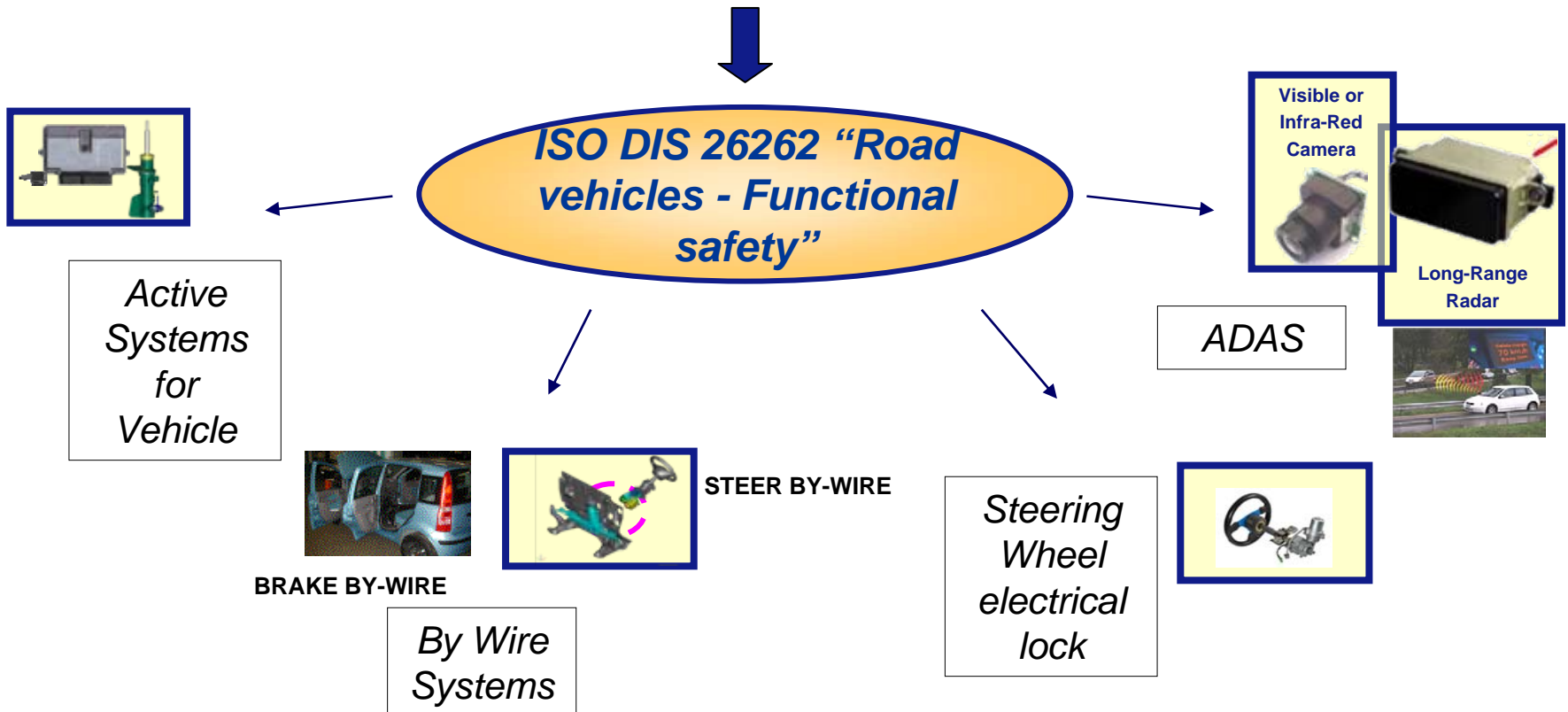
Multiple stakeholders in development

**Increasingly tight requirements in general on quality
and safety**

**Formal requirements from the ISO/DIS 26262 standard
on functional safety**

ISO 26262 “Road Vehicles - Functional Safety”

We need a sound **methodology** for addressing all aspects concerning **safety**.
The methodology has to be **unified, internationally recognized** and **specific for the automotive**

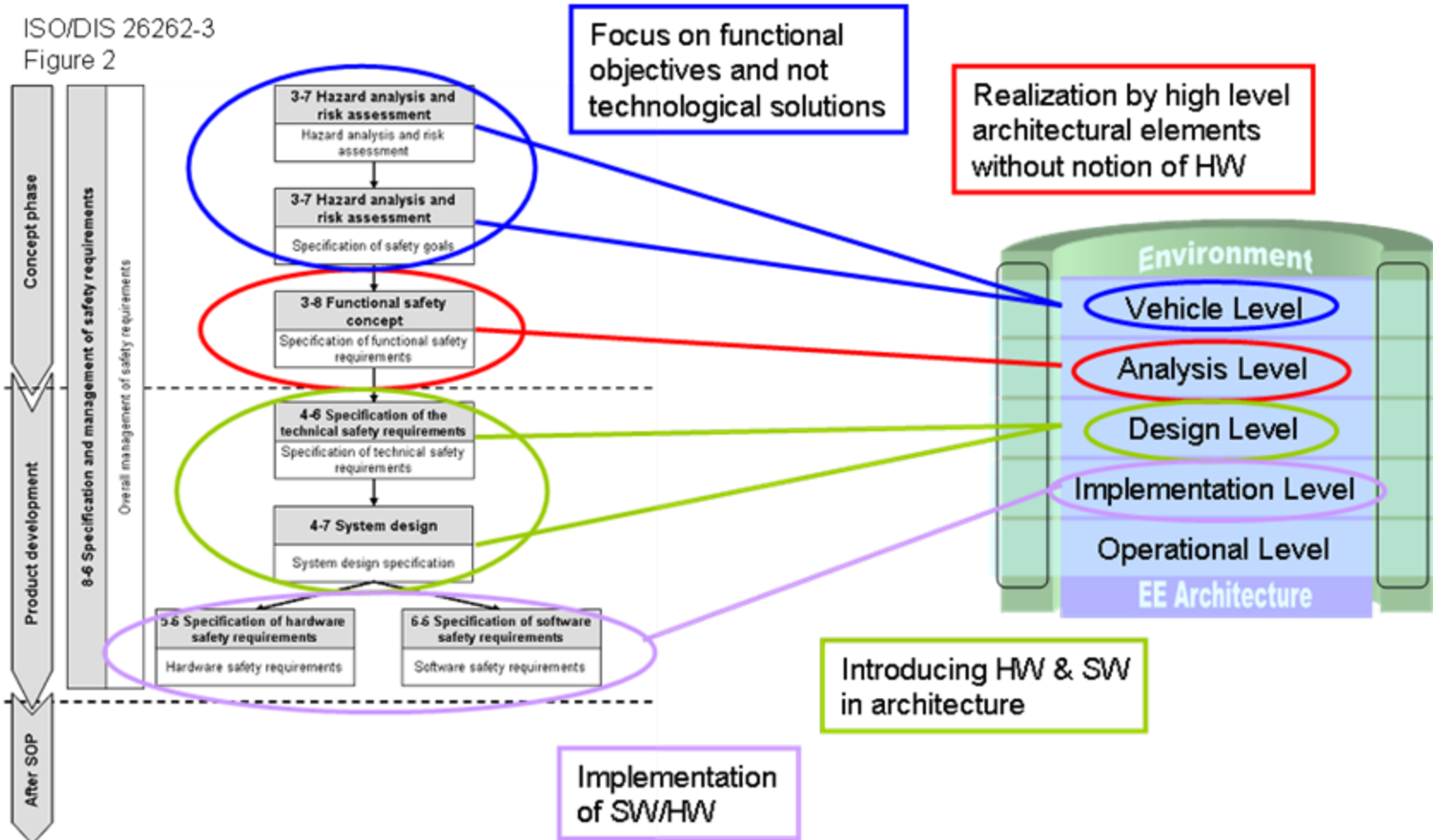


Safety Support

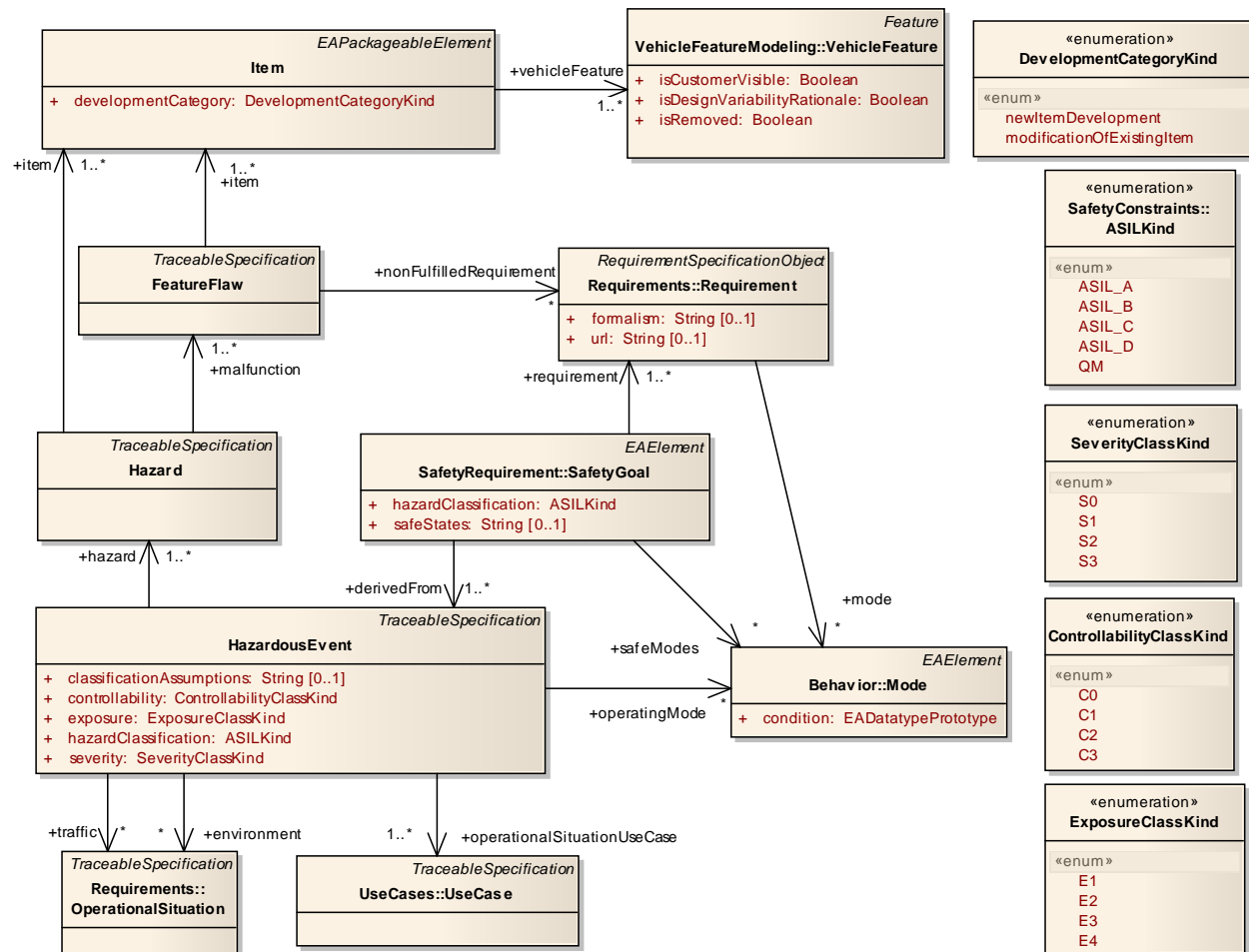
- EAST-ADL language modelling of ISO-26262 concepts
 - Covering artefacts of ISO-26262
- EAST-ADL methodology modelling of safety activities
 - Covering life-cycle of ISO-26262
- EAST-ADL language explicit modelling of safety constraints
 - Enabling well-defined modelling of
 - Semantics of each safety requirement
 - Allocation of each safety requirement
 - Built on Fault/Failure Model
 - Enabling automated tool support
 - ASIL decomposition
 - Architecture evaluation / optimization

ISO-26262 Support

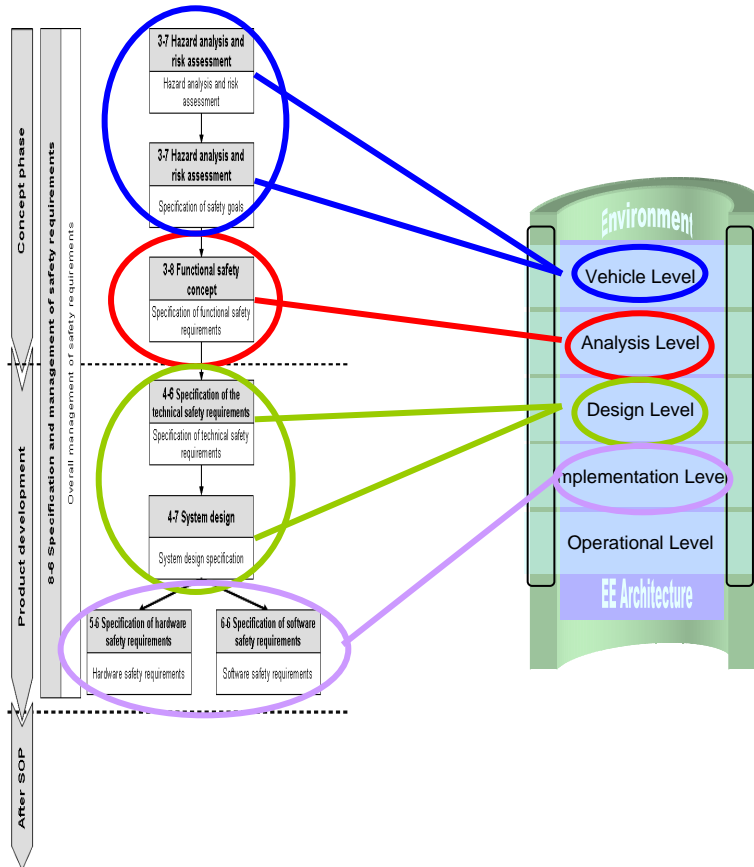
ISO/DIS 26262-3
Figure 2



EAST-ADL provides **language-level support for the concepts defined in ISO 26262**, including vehicle-level hazard analysis and risk assessment, the definition of safety goals and safety requirements, the ASIL (Automotive Safety Integrity Level) decomposition and the error propagation



Safety Info Integrated in Model



Semantically Well-Defined “Safety Constraints”

- * ASIL attributes
- * ...

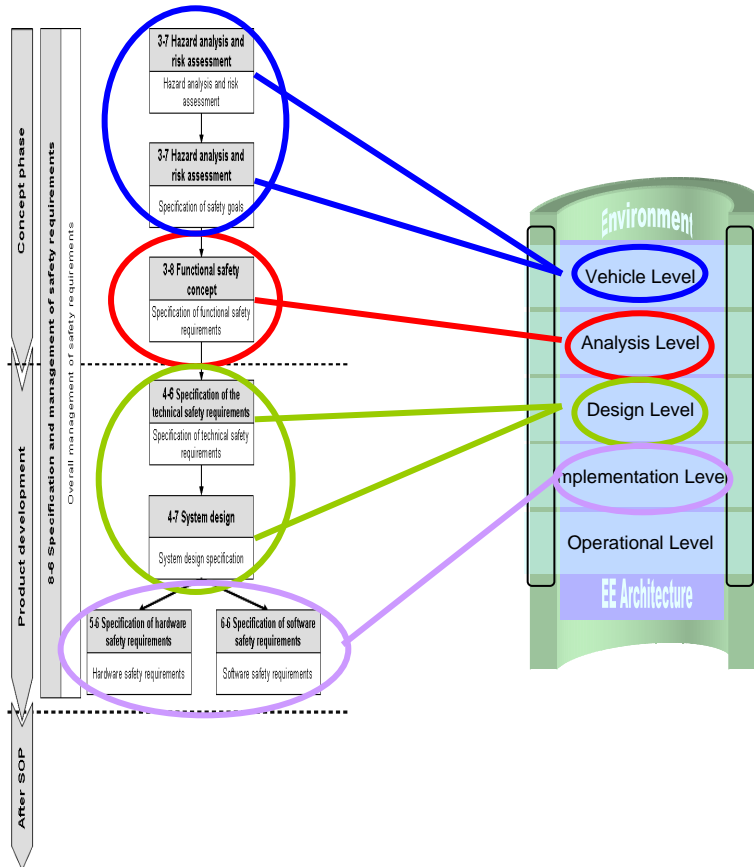
Not only as general Requirements
(without dedicated syntax and semantics)

(Compare Timing Constraints as defined by AR Timing and by TIMMO)

All Artefacts in ISO methodology
integrated in System Model

Different ISO-26262 Artefacts modelled
on different abstraction levels

Safety Concepts



Set of Safety Requirements
Allocated on Artefact
Elements

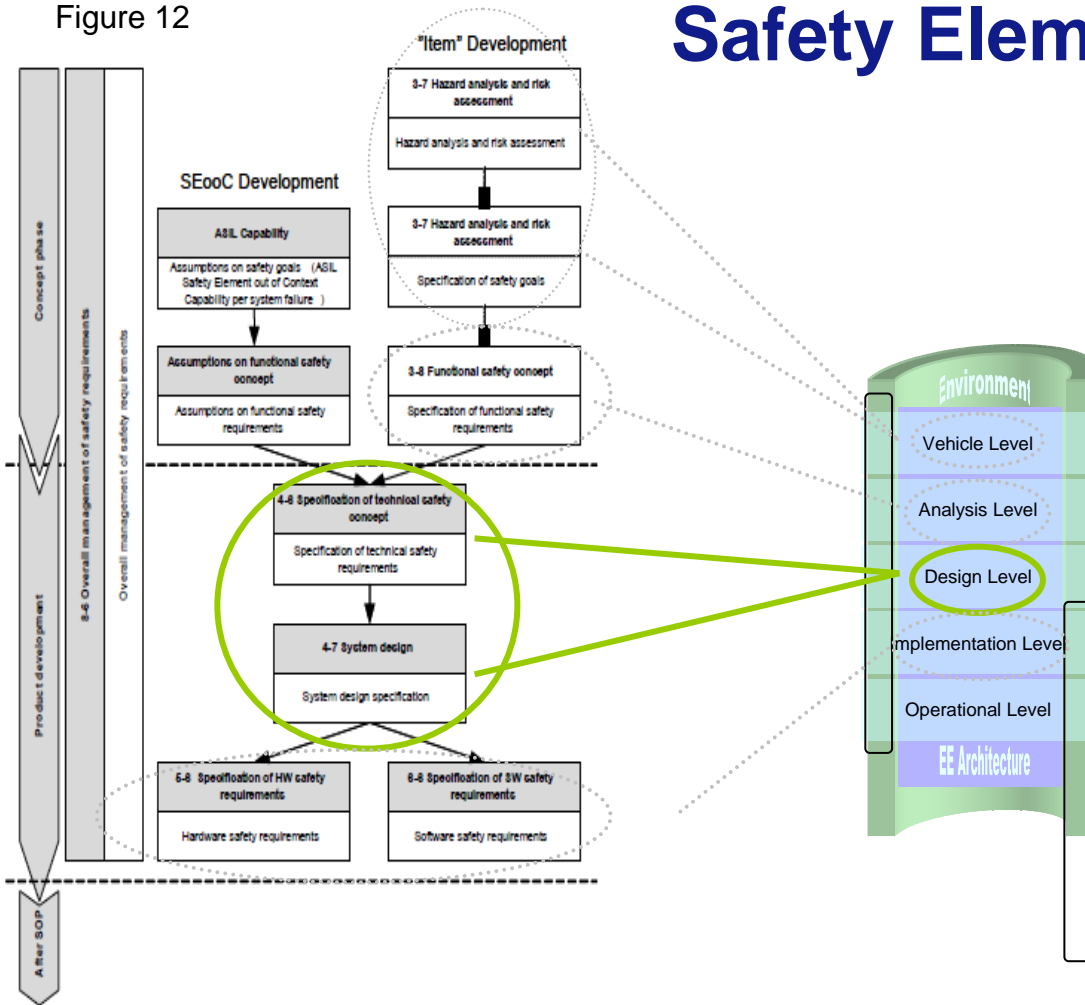
Allocation includes ASIL
Decomposition

Each Architecture implies
active decision of Safety
Requirement (Definition) and
Allocation

Safety Concept on less
Abstract Level Realizes
Safety Concept on more
Abstract Level

ISO/DIS 26262-10
Figure 12

Safety Element out of Context

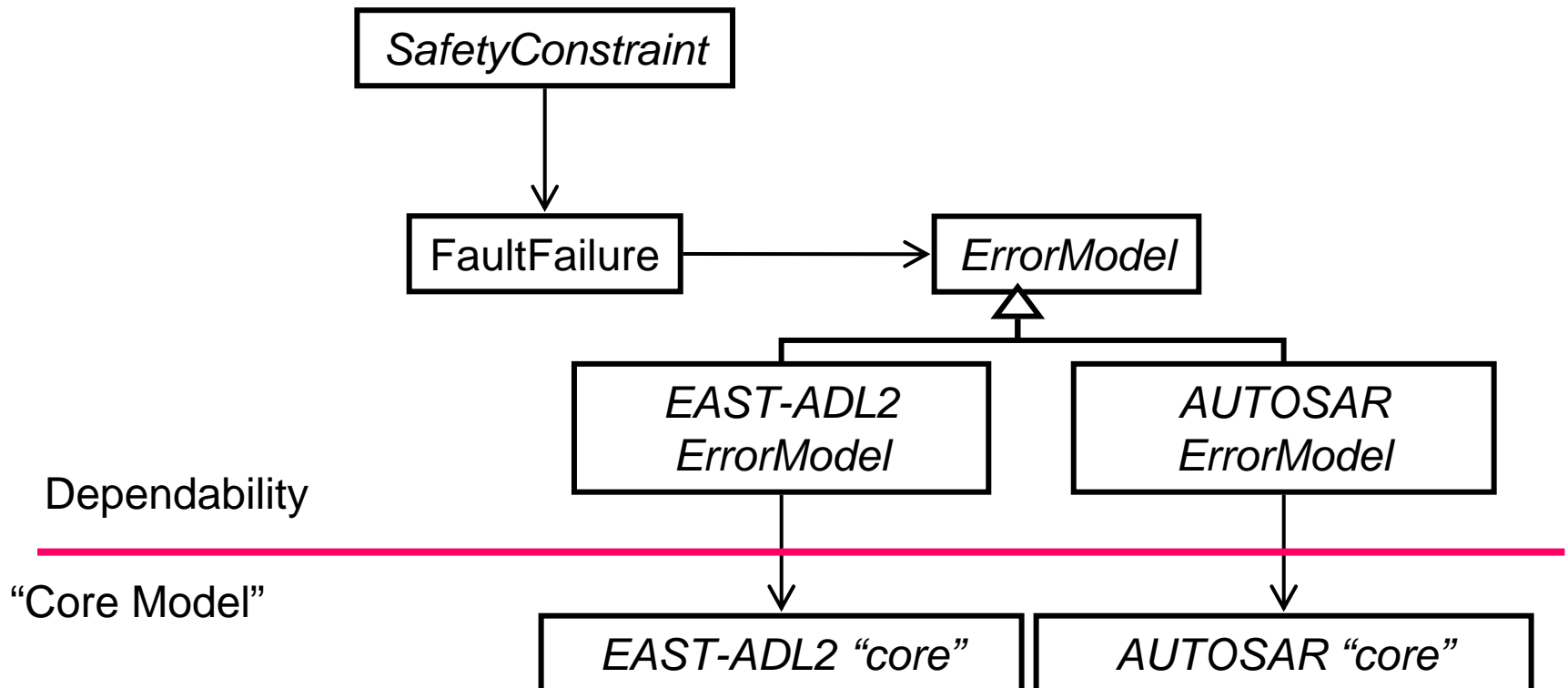


Example: Model “Technical Safety Concept” without Functional Safety Concept

Allocated “Safety Constraints” that can play the role of Technical Safety Requirements when Functional Safety Concept is available

Figure 12 — Safety Element out of Context Development lifecycle for a sub-system

Safety Constraints



Error Modelling in EAST-ADL

- EAST-ADL error model expanded to include concepts to support hazards & safety analysis
- Uses a parallel architecture to model failure behaviour
 - **ErrorModelTypes & Prototypes** describe individual architecture elements and allow hierarchical composition of error models
 - **ErrorBehaviors** describe the failure behaviour of a system or component
 - **InternalFaults** and **FaultFailures** describe individual component failures
 - **FaultFailurePorts** allow propagation of failures from one error model to another by means of **FaultFailurePropagationLinks**
 - **Hazards** and **HazardousEvents** link component errors to system failures
 - **SafetyConstraints** allow integrity constraints to be specified on errors

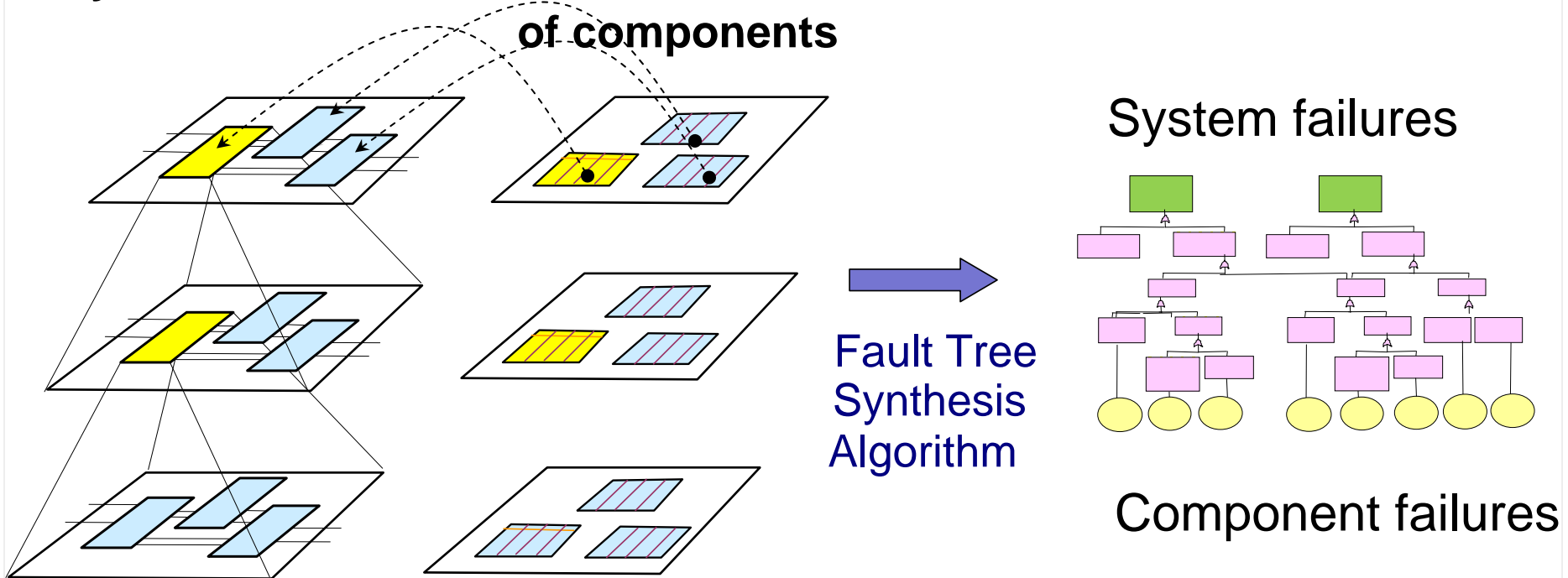
Safety Analysis

- Different analyses can be applied at different design stages
- Hazard analysis
 - Identification of hazards and failure scenarios in which hazards may occur
 - EAST-ADL provides support for hazard analysis on the vehicle feature level
 - Allows definition of safety requirements & safety goals
- Fault Tree Analysis (FTA)
 - Used to determine the root causes (component faults) of a system failure
 - Can also be used to estimate probability of failures
- Failure Modes & Effects Analysis (FMEA)
 - Shows effects of individual component failures on the system
- FTA and FMEA capabilities provided by HiP-HOPS tool

HiP-HOPS Safety Analysis Tool

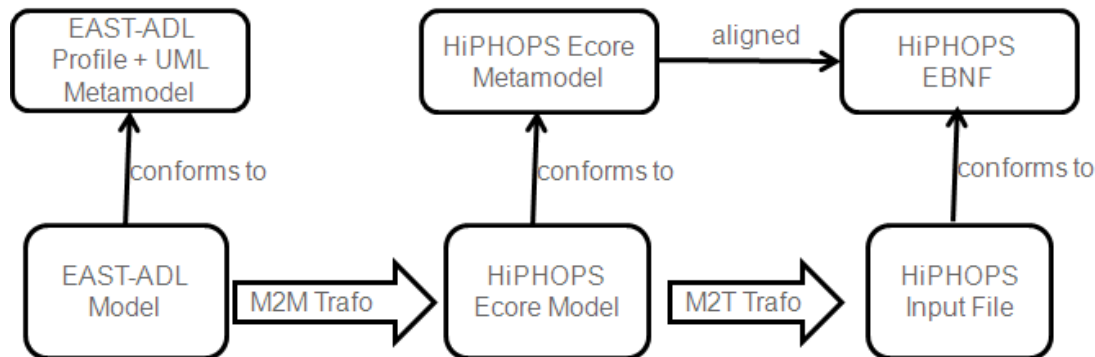
- **HiP-HOPS** is a method and tool that simplifies dependability analysis and architectural optimisation via partial automation

System Model + Failure annotations = Global view of failure:



Papyrus - HiP-HOPS Plugin

- Interface between EAST-ADL in Papyrus and HiP-HOPS
- Uses model transformation technology to convert EAST-ADL2 model into HiP-HOPS model in two phases
 - Semantic mapping of metamodel concepts in ATL
 - Representation transformation in Xpand



- Links new features in both EAST-ADL and HiP-HOPS

Automatic ASIL Decomposition

- Safety requirements specified with ASILs
- ASIL algebra is part of ISO 26262
 - If two components must both fail to cause a system failure, the ASIL for that component is shared between them, e.g. $ASIL\ D = C + A$ or $B + B$ etc
- HiP-HOPS can do this automatically using its fault trees
 - Causes of system failures are in cut sets (conjunctions of failure events)
 - ASILs for system failures can be shared amongst events of cut sets
 - Takes shared dependencies into account, e.g. if events are in >1 cut set
- Adds novel new capabilities to EAST-ADL2 & HiP-HOPS
 - ASILs can be allocated to failures, output errors, ports, or components
 - Can still produce many combinations however

Design Optimisation

- HiP-HOPS also provides design optimisation capabilities
 - Aim is to automatically evolve a system design to maximise some attributes (e.g. dependability) while minimising others (e.g. cost)
- ATESSST2 explored how this could be used by EAST-ADL
- Designer would provide system model in EAST-ADL
 - Design space is defined by EAST-ADL's variability mechanisms
 - Each variant provides enough information to be evaluated by external analysis tools, e.g. error models, cost information, timing characteristics
- HiP-HOPS performs multi-objective optimisation and produces set of Pareto optimal results
 - Each result is an optimal trade off between the various objectives
- Experimental results only so far - not part of current tool chain

Conclusion

- EAST-ADL language modelling of ISO-26262 concepts
 - Covering artefacts of ISO-26262
- EAST-ADL methodology modelling of safety activities
 - Covering life-cycle of ISO-26262
- EAST-ADL language explicit modelling of safety constraints
 - Enabling well-defined modelling of
 - Semantics of each safety requirement
 - Allocation of each safety requirement
 - Built on Fault/Failure Model
 - Enabling automated tool support
 - ASIL decomposition
 - Architecture evaluation / optimization

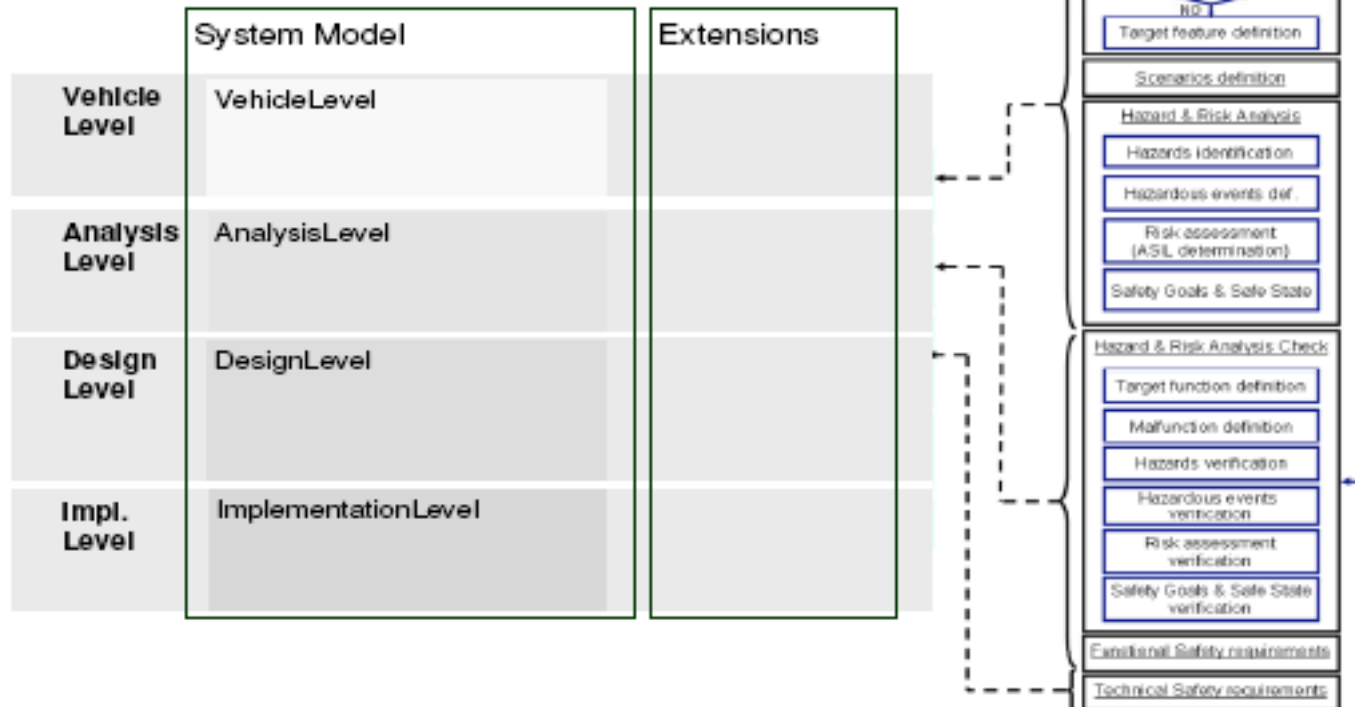
Back-up slides

ISO 26262 “Road Vehicles - Functional Safety”

- **Safety** turns out to be **one of the key issues of (future) vehicles development** as new functionalities as driver assistance, dynamics control will be introduced.
- The main **objective for the safety** will be **to reduce the risk**, *that is function of frequency (or likelihood) of the hazardous event and the event consequence severity*, **at a tolerable level**.
- Future development and integration of these functionalities will even strengthen the need of:
 - **New technologies** to enable such systems to function more effectively with increased design complexity and **managing the safety**;
 - **Safe system development processes** within the possibility to show evidence that all reasonable safety objectives are met (*acceptable risk reached*). This has thrown the spotlight on **the role of staff engaged in the design, development and maintenance** of these safety-related systems.

- The ISO°26262 requires conducting safety activities , beginning from the preliminary development phase of automotive systems and including the whole product life-cycle, in order to design a safer automotive system.
- It is necessary to integrate safety activities with the common development activities,

EAST-ADL supports this process by means of its Safety Design Flow methodology.



Supporting ISO 26262

- One major goal in ATESSST2 was to support ISO 26262
 - Requires analyses throughout design process to ensure system safety
- Current analysis capability provided by HiP-HOPS safety tool
- New concepts added to EAST-ADL and HiP-HOPS:
 - Enhanced error modelling and multi-perspective analysis capabilities
 - Support for safety constraints (including ASILs)
 - Hazards linking error models to hazard analysis of vehicle feature level
- ASIL decomposition algorithm implemented in HiP-HOPS
 - Allows automatic determination of possible ASIL allocation strategies
- ISO 26262 compatible safety methodology developed

