VECTOR

PREEvision
Technical Article

Designing Advanced Systems – Safely!
Model-Based E/E Development Conforming to ISO 26262

Electrification, automation and vehicle networking demand maximum requirements for the functional safety of vehicles. The electronic systems for new vehicle functions are networked to a high degree, which makes a safety analysis on the level of the complete system necessary. In addition, technical trends such as automotive Ethernet and AUTOSAR Adaptive need to be considered. Model-based engineering environments support engineers in overcoming these challenges.

Functional safety must be analyzed on all levels during Electrical/Electronic development. The levels include the architecture design, requirements analysis, software and system design, communication design and the development of hardware components and the wiring harness (Figure 1). At the same time, consideration should be given to the reuse of Electrical/Electronics (E/E) in other product lines and equipment variants. On the one hand, consistent E/E models enable modeling of the numerous options for development which result from these degrees of freedom. On the other hand, such models make it possible to overcome the complexities involved in developing functionally safe E/E systems.

ISO 26262 – Standard with a Future

The ISO 26262 standard defines international requirements for the development of safety-relevant E/E of motor vehicles. It was established in the passenger car segment, and its upcoming second edition will be applicable to the motorcycle, truck, and bus industries as well as semiconductor manufacturers; further, manufacturers in the agricultural machine industry have adopted the standard as a 'best practice'. The standard sets comprehensive requirements – not only for the functional safety of end products, but also for methods and processes in product development and management. Proven methods of safety analysis and existing industrial standards were adopted in the standardization process. The revised version currently being prepared will take into account experience gained in applying the standard and also extend its scope of use. One tool that can be used to implement the requirements of ISO 26262 efficiently is PREEvision. Vector offers this tool as a model-based solution which can model – in a tool-supported and consistent way – all levels of the E/E architecture of a vehicle with a description language specially developed for this purpose. It facilitates the analysis and optimization of the functional safety of E/E systems by users (Figure 2).

Design of the logical system architecture begins with requirements that can be related to vehicle functions which will be experienced by users of the vehicle. Extending from this, the software and hardware architectures are created including the network topology. Along with the system view, the tool provides detailed views of the circuit and wiring diagrams and the wiring harness. In addition, it is also possible to capture the layouts of physical components and

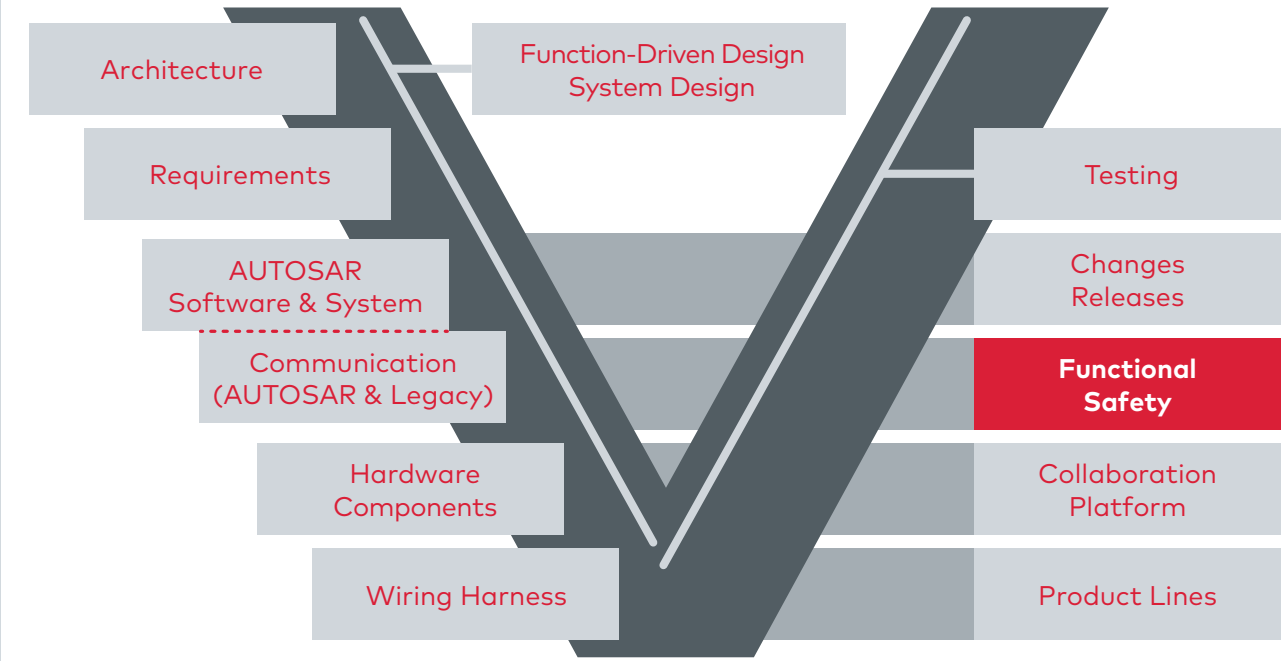

Figure 1: Functional safety is an integral component of E/E development.

connections as well as the geometry of the installation spaces in the vehicle. A version and change management system supports use of the engineering environment in production-level projects. Import and export interfaces which conform to relevant exchange formats are used to integrate PREEvision into the customer's existing tool landscape and environment.

Functional Safety Concept

The Hazard and Operability Study (HAZOP) – a qualitative analysis method – can be used as a starting point to systematically identify faulty operation of vehicle functions. It is applied to customer functions, requirements or logical functions which are abstracted from the technical implementation in software or hardware. The HAZOP results serve as a basis for the Hazard Analysis and Risk Assessment (HARA), in which safety goals are defined. To define the hazardous events, PREEvision applies a catalog-based method to functions and associated functional faults as well as operating modes of the vehicle systems and driving situations. Each hazardous event is assigned an Automotive Safety Integrity Level (ASIL) that results from classifying them according to severity, probability of occurrence and effectiveness of controls. This forms the foundation for defining safety goals with the associated ASIL. Spreadsheet editors can be used to specify functional safety requirements that are derived from the safety goals. Checks of the model, which the tool executes continuously in background, give immediate feedback on any violations of the standard, such as invalid decompositions of safety requirements. On the logical architecture level, causal chains serve to describe the functional safety concept. Sensor, actuator and logical function blocks are used whose ports are specified by interface definitions. It is also possible to classify logical functions hierarchically. A proven method here is to describe and implement one causal chain per safety goal. The safety requirements can easily be linked to objects on the logical level. This means that early in the concept phase the engineer is already able to take the proper actions for fulfilling safety goals with the associated ASIL.

Technical Safety Concept

In the framework of product development on the system level, the functional and technical safety requirements are fine-tuned, and the technical safety concept is worked out in accordance with ISO 26262. The next step in the development of a safety-relevant vehicle system – according to the reference phase model – is to subdivide product development into hardware and software development, and they are reunified in the framework of integration on the system level. PREEvision follows this approach in modeling the technical safety concept by using the hardware and software modeling levels. The technical safety requirements then result in specific hardware and software safety requirements. PREEvision supports users with diagrams and editors which let them work on different levels of detail.

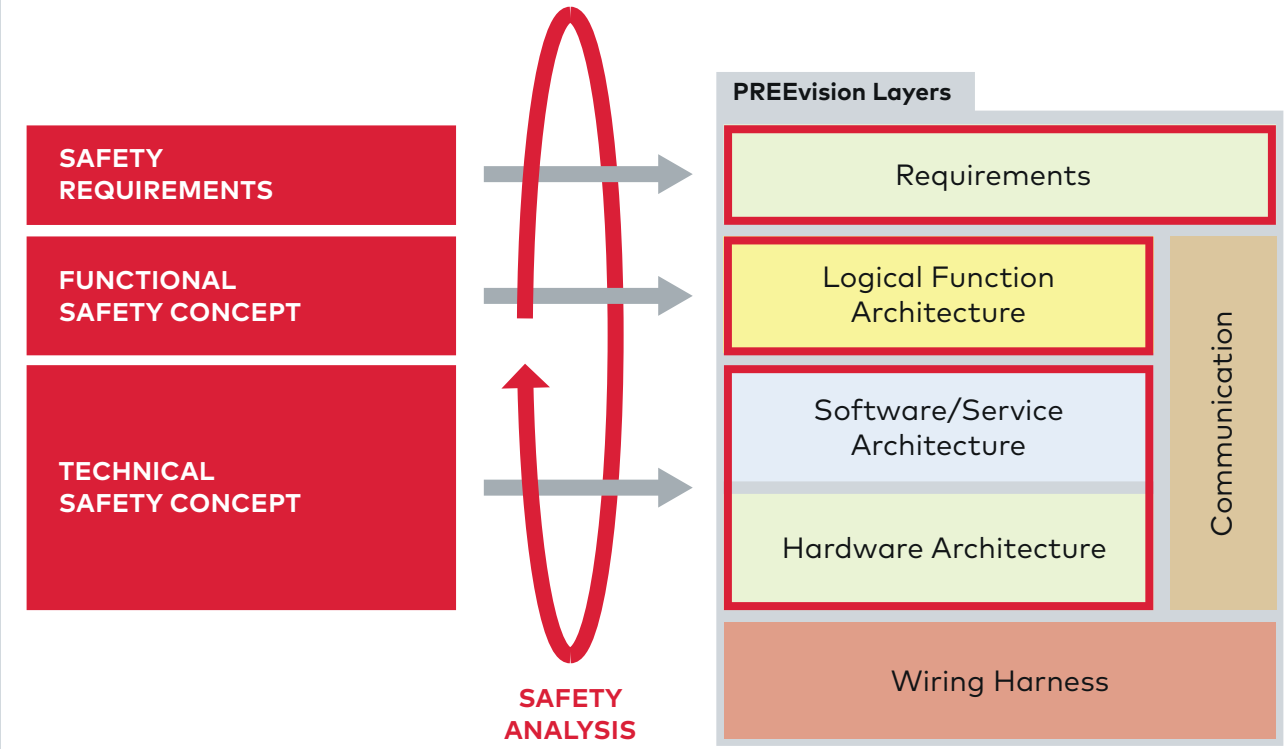

Figure 2: The functional safety concept and technical safety concept are modeled on these levels in PREEvision: logical functional architecture, software/service architecture and hardware architecture. Safety requirements can be linked to their related components on these levels. Tool-supported safety analyses can be used to refine the safety concept iteratively and harmonize it with requirements.

This makes it possible to create both the architecture design and the detailed design of hardware and software components. In this process, libraries are used in which the failure rates and types are already stored for each component. In a similar way, safety mechanisms can be integrated with their associated degrees of diagnostic coverage (Figure 3).

Safety Analysis

In safety analysis of the design, PREEvision supports the inductive methods FMEA (Failure Mode and Effects Analysis), FMEDA (Failure Mode, Effects and Diagnostic Analysis) and the deductive FTA method (Fault Tree Analysis). In executing an FMEA, suitable editors may be used to fill out the form sheets manually. As an alternative, the user can have PREEvision automatically fill in portions of an FMEA form sheet based on information from the model. For the FTA, the user can construct fault trees with the help of diagrams and reference them to specific safety requirements. When a qualitative FTA is executed, it identifies lower-level events that lead to the occurrence of the top event being analyzed. This makes it possible to improve the design in specific ways. This can be optimized by showing additional relevant design elements from the model in the diagram. To check whether the designs achieve the required target values, a quantitative FTA can be performed by linking the lower-level events of the qualitative FTA together with their probability of occurrence. The fault trees can also be reused in PREEvision – like subsystems. In the context of system variants, fault trees can be analyzed in a variant-sensitive manner. The FMEDA is especially important to Tier-1 suppliers. In PREEvision, the hardware can be broken down to the level of electronic circuit diagrams of a component for this purpose. Individual component types such as microcontrollers and resistors are supplemented by fault information stored in a library (Figure 3).

After instantiating these components in the circuit diagram, the engineer can classify the individual failure types of components as single, residual or multiple errors. Building upon this, the required safety analyses can be performed: the Hardware Architectural Metrics and Failure Rate Class Method. After integrating all the necessary information into the PREEvision model, the safety requirements, their ASIL classifications and the required target values are known. This gives the engineer direct feedback on whether they have been fulfilled. Specific changes can then be made to the hardware design, e.g. introducing additional safety mechanisms or using other components from the library.

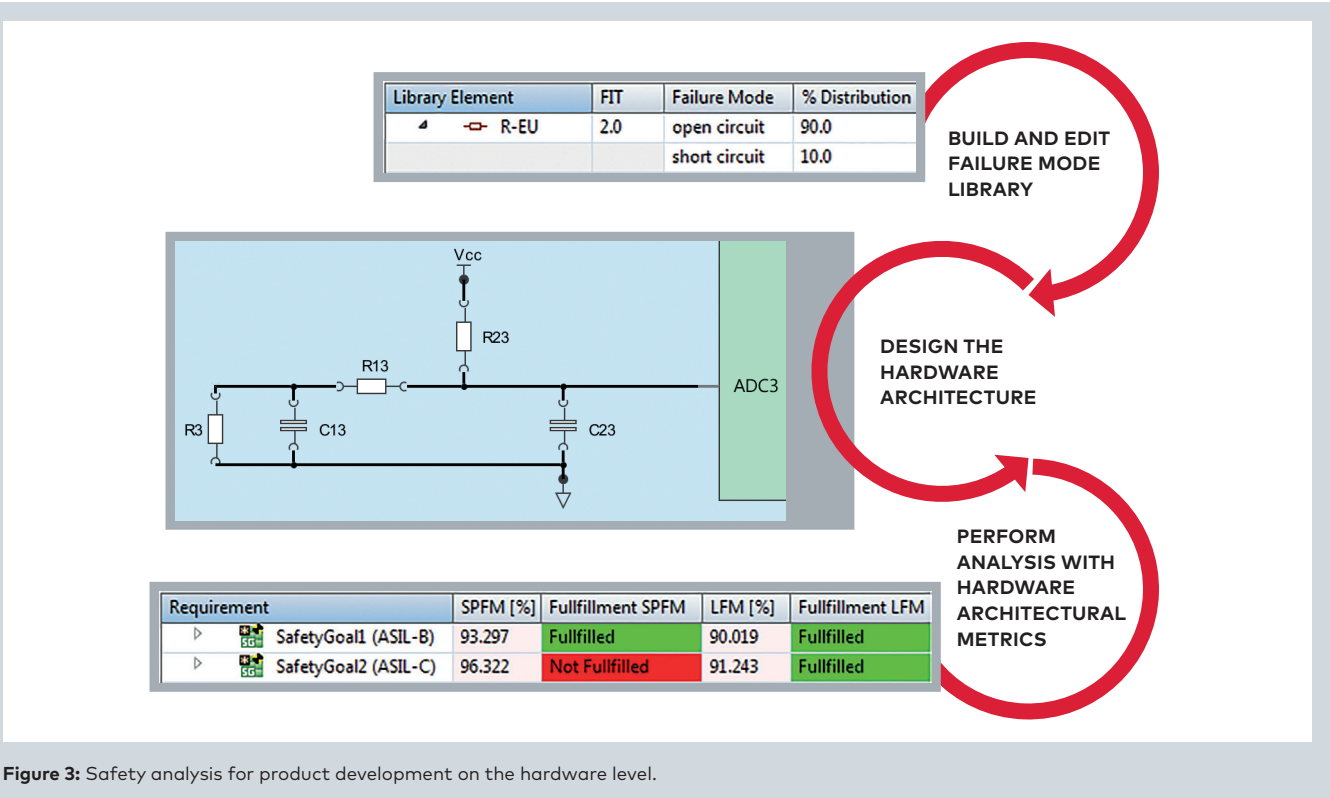

Figure 3: Safety analysis for product development on the hardware level.

Verification and Validation

PREEvision may also be used for integration and testing on the hardware, software and system levels. Test specifications can be derived from requirements and customer functions. They can be used to design tests and implement them. It is possible to plan test activities and to input or import the results of individual test executions into them – whether they are manual tests or automated tests. The tool presents the results in the form of reports and diagrams.

Cooperation between OEM and Suppliers

Change management with a ticket system enables transparent tracking of change requests and defects, since tickets can be linked to model elements. In addition, customer-specific life cycles can be set for tickets. Integrated release management supports project planning and tracking. In addition, it is possible to review subsets of all model contents such as safety requirements. The import/export interface, which extends the established ReqIF exchange format, can be used to simultaneously initiate external coordination of requirements between an OEM and multiple suppliers. This mechanism supports the Development Interface Agreement for data exchange mentioned in ISO 26262.

Iterative Process for Safety Verification

The verification documents required by ISO 26262 can be automatically created by a report generation function that can be customized. Hyperlinks to the E/E model may be saved in the texts of the verification documents. This simplifies internal reviews, safety assessments and audits. ISO 26262 recommends treating the safety verification as an incremental activity rather than as an activity that is started toward the end of the safety life cycle. With PREEvision, engineers can perform development tasks related to functional safety iteratively. During different development phases, work products can be checked for consistency, and an interim report on the safety verification can be generated. In the end, this procedure leads to a safety verification which demonstrates that all safety goals are complete and have been fulfilled (Figure 4).

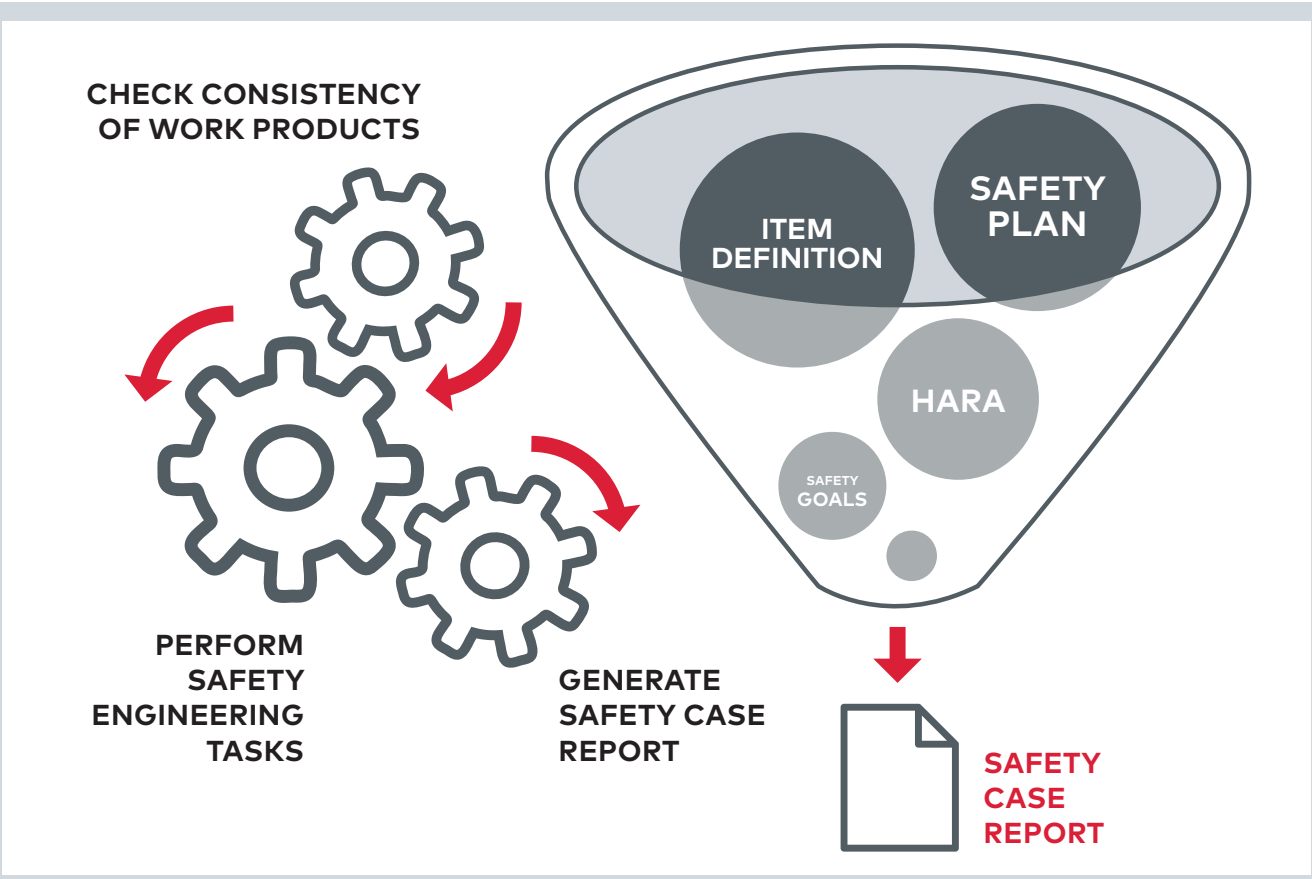

Figure 4: Safety verification as an incremental activity.

Summary

Model-based environments provide different views of a vehicle's E/E content and are a powerful tool in development. They enable consistent design of functionally safe systems and help engineers to focus on the core activities of their work. Powerful tools like PREEvision also offer process support which can be adapted to the specific needs of OEMs and Tier-1 suppliers. An integrated approach results in traceability: from the requirements specification to the safety verification.

Authors

Dr. (Engineering) Nico Adler
Vector Informatik GmbH
Product Management Engineer
PREEvision Functional Safety

Originally published in "Elektronik automotive" magazine Special issue "Software" – November 2018