Consequently, new approaches are needed to enable functional safety as an integral component in the development of E/E systems. It is important to consider all levels of system designs (Figure 1) and assure that safety goals of the systems are verifiably implemented according to the standard.

**Comprehensive perspective of system architectures**

A key requirement of all current safety standards in automotive and non-automotive industries (e.g. IEC 61511 for the process industry, IEC61513 for nuclear power plants, EN 50128 for railway systems) is that it must be verified that the developed system concept fulfills system safety goals. Safety goals are typically identified in hazard and risk analyses on the functional system level. The functional and technical safety requirements derived from the safety goals are then allocated to system components. Correct implementation of these safety requirements must be assured by a suitable combination of reviews, analyses and tests.

The attainment of system safety goals depends on many different factors. One example: faulty programming of software functions or random hardware failures in critical components. As recommended in ISO 26262, such isolated failures can be avoided relatively easily, or can at least be detected and overcome by current development methods. It becomes more problematic when safety goals are affected by a combination of different system factors on different architecture levels. However, in the case of complex systems, such interdependencies can hardly be revealed by conventional, document-based design methods. Here are two
examples of typical design errors:

> During software development, incorrect assumptions are made about the integrity of the communication medium between two functions. As a result, communication failures are inadequately considered. For example, later redistribution of software functions to different ECUs in different bus segments might violate system integrity due to the flawed original assumption – without the software developer being aware of it.

> A hardware component exhibits atypically high failure rates, because it is located in a vehicle area that is exposed to extreme environmental conditions, such as temperature mechanical vibration or electromagnetic interference. Elevated failure rates were not considered in the safety concept.

A comprehensive approach to system modeling is necessary to give due consideration to such complex interrelationships in the design phase. This approach combines all functional and nonfunctional requirements in one data model as well as the logical system design, network architecture and software and hardware component architectures. Similarly, it is necessary to consider the wiring harness and the topological distribution of components and the wiring harness in the vehicle (Figure 1). In this process, it is important to be able to describe the interdependencies between different architecture levels as well as domain-specific attributes of the modeled artifacts (e.g. bus latency times, hardware failure rates or temperature ranges of installation location). Based on this data, analysis – which may be performed semi-automatically – can then be used to formulate and answer questions such as: “Will wires transmitting signals relevant to the safety concept be routed in areas that are at risk of damage in a crash?”

### Model-based safety analyses

ISO 26262 requires that safety analyses be performed on the system, software and hardware levels, so that design weaknesses can be detected and actions can be taken to improve the design. One such analytical method is Failure Modes and Effects Analysis (FMEA). It is used to identify potential failures in individual components and analyze their effects on system goals as well as their probability of occurrence. This type of analysis is well suited to identifying components that are critical from the perspective of safety goals. Nonetheless, the results depend very much on the quality and scope of the modeled system design upon which the analysis is based. When system dependencies are inadequately documented, the results often depend on the individual experience levels and knowledge of engineers, and this often leads to the problems illustrated in the examples above.

Comprehensive modeling of the system is an optimal precondition for performing safety analyses. In conducting these analyses, the safety expert accesses information directly from the model. Dependencies, especially between different architecture levels, may be automatically analyzed, and their effects on system safety evaluated. Actions derived from the analysis are implemented directly in the model, and they are linked to the relevant analysis. This produces traceability between the design, analysis and affected safety goals, which are absolutely essential to provide the required safety verification and conduct impact analyses in response to system changes. Close intermeshing of the system design, safety analysis and design of the safety concept makes it possible to immediately analyze and evaluate the effects of model changes. This eliminates the need for time-consuming re-designs, which would otherwise be unavoidable in the case of sequential handling of the design and then the safety analysis. In addition, multiple implementation variants of a system may be compared and evaluated. This makes it possible to perform system optimization that incorporates safety-technical perspectives in an early phase of system development (Figure 2).

### Product line approach yields increased efficiency

From a system viewpoint, personalizing vehicles, i.e. offering different variants and configurations, leads to a number of variants that is simply unmanageable. The safety engineer is immediately faced with the challenge of providing the required safety validation for each system variant. One way to confront this challenge is to use a product line approach. This approach is based on the analysis (domain analysis) of variant-based systems (product lines) with

---

Figure 1:
Model-based system design: Comprehensive perspective of all elements of the system architecture and their dependencies
regard to identical parts (commonalities) and differences (variabilities). Identifying commonalities provides a foundation for re-using them over a number of products (vehicles). Furthermore, the work only needs to be performed once to create requirements analyses, implementations or tests.

To make the reusability concept feasible for the development of safety-critical systems, the product line approach must be extended to hazard and risk analyses as well as to safety concepts. These analyses and concepts are available for re-use, provided that they relate to a common set of features. Technical safety requirements for specific vehicle projects are derived from the functional safety concept. For example, specific vehicles are characterized by specific operating states, system architectures, etc. (Figure 3). Applying domain analysis to the technical safety requirements can make some of these requirements available for re-use.

To maximize the added value of re-use, domain analysis can also be extended to system components (software components, hardware components). Performance of the safety validation is supported by re-use of a portion of the argumentation structure (safety case argumentation structure). Assumptions about the specific vehicle environment are formulated as requirements whose implementation or validity must then be analyzed for the specific context.

A model-based approach is a prerequisite for performing variant-specific analyses and consistency checks. This approach ensures, for example, that all actions listed in the safety validation and technical requirements derived from the re-used safety concept can actually be implemented in the specific vehicle. If a redundancy that is provided in the safety concept were to be lack-

ing, for example, this would be detected as an unfulfilled requirement in a variant-specific consistency check.

**Summary**

Model-based methods and a comprehensive approach (Systems Engineering) give the system developer a method for understanding and mastering complex systems, which in the end leads to safe systems. The model-based approach promotes the increased efficiency to compensate for the additional work effort caused by safety relevant activities (analyses, implementation of actions resulting from them and safety validations). The re-use of entire portions of the safety architecture avoids work steps that are repeated one or more times, and this leads to further increases in efficiency.

The all decisive factor for success is the availability of proven tool support for implementing the paradigm shift described here in daily practice: from a document-centered approach to a model-based approach. A key requirement for a tool is its suitability for describing complex systems by means of a related semantic data model. But domain-specific graphic notations and support in analyses as well as performance of safety validation are also absolutely essential. Collaboration on large teams results in further requirements. The provision of a collaboration platform for data storage (single source principle) and data exchange among all project participants. In this process, competencies and responsibilities must lend themselves to modeling by a rights and roles concept. Chronological traceability (history of versions) requires integrated version and configuration management.
In its PREEvision product, the company Vector is offering a proven tool for model-based systems engineering that has been on the market for over five years. PREEvision also provides assistance in the areas of testing (test data management), planning (product and release management) and change management. In its latest version, PREEvision supports an ISO 26262 conformant approach to modeling, analysis and testing of functional safety concepts.

Translation of a German publication in ‘Automobil Elektronik’, issue 2/2012

Figures:
Vector Group

Links:
Home page Vector: www.vector.com
Product information PREEvision: www.vector.com/preevision_en

Authors:

Dr. Simon Burton
studied Computer Science at the University of York in England. He earned his doctorate degree in York as well with a thesis on Specification and Testing of Safety-Critical Systems. Focal points of his career include the introduction of systems engineering and model-based approaches in developing embedded, safety-critical systems. In 2006, he joined the Vector Group where he has served in the areas of safety consulting, product management and business management of the Automotive Solution.

Albert Habermann
studied physics at the Ludwig-Maximilians University in Munich. Focal points of his career include the introduction of model-based methods to software development and testing. In 2006, he joined Vector where he is employed as a project manager in the Customer Service area for the PREEvision architecture and systems engineering tool.

>> Your Contact:

Germany and all countries, not named below
France, Belgium, Luxembourg
Sweden, Denmark, Norway, Finland, Iceland
VecScan AB, Göteborg, Sweden, www.vector-scandinavia.com
Great Britain
Vector GB Ltd., Birmingham, United Kingdom, www.vector-gb.co.uk
USA, Canada, Mexico
Vector CANtech, Inc., Detroit, USA, www.vector-cantech.com
Japan
Vector Japan Co., Ltd., Tokyo, Japan, www.vector-japan.co.jp
Korea
India
Vector Informatik India Prv. Ltd., Pune, India, www.vector.in
China
Vector Automotive Technology Co., Ltd., Shanghai, China, www.vector-china.com

E-Mail Contact
info@vector.com