Automotive Systems Engineering und Functional Safety: The Way Forward

Simon Burton, Albert Habermann

Automotive Systems Engineering und Functional Safety: The Way Forward

Dr. Simon Burton
Albert Habermann
Vector Informatik GmbH
Ingersheimer Strasse 24
70499 Stuttgart, Germany
+49 711 80670 1529
albert.habermann@vector.com

ABSTRACT

The increasing of complexity of safety relevant functions, as well as their implementation on distributed components is one of the major issues in automotive engineering. The situation is additionally tightened by challenges arising from the introduction of ISO26262 standard.

It is discussed how a model based systems engineering approach enables the integration of the safety activities into the development process to deal with growing complexity and to improve efficiency as well. Finally the extension of the product line engineering approach to work products of safety activities can lead to the step change required to match the capabilities of engineering departments to the complexities of the task at hand.

Keywords

Automotive systems engineering, functional safety, product-line development, model-based engineering, safety case.

1. INTRODUCTION

During the last 25 years, the automotive industry has seen an exponential rise in the number of safety-relevant E/E enabled vehicle functions. These functions are not only increasing in number, but also in complexity, authority over the control of the vehicle and the level of interaction between (see Figure 1, based on personal experience and observations).

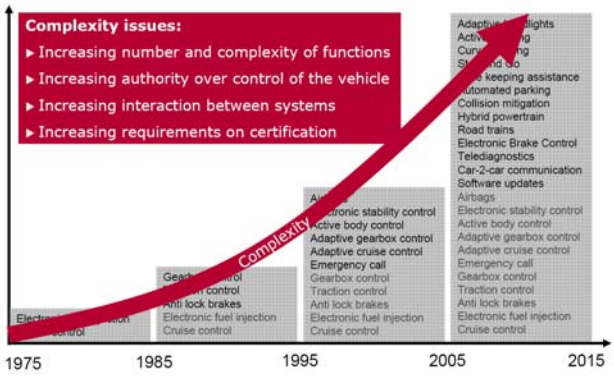

Figure 1: Complexity issues in automotive systems

Decontentisation, i.e., reducing the number and behavioural scope of the functions themselves is one method of reducing complexity. However, this approach is limited due to market pressure on the differentiation between vehicle manufacturers and therefore the need for ever more innovative functions, in particular in the area of active and passive safety, which by definition can lead to safety-related incidents if they malfunction.

With the introduction of the automotive industry specific standard on functional safety, ISO 26262 [1], currently released as a draft international standard, there is also an increasing need to ensure that best practice has been applied during the development of the systems and to provide a convincing argument that the developed systems are safe.

We see a number of factors that limit the capability of the industry to fulfil the above mentioned requirements with given development practices and resources. The sheer number of systems to be developed and the rate of technological change combined with a lack of sufficiently trained and experienced safety engineers result in development projects being insufficiently supported. In addition, despite increasing efforts to adhere to models such as CMMI [2] and SPICE [3], the process discipline required to efficiently and effectively perform the systems engineering with the necessary level of rigour is often lacking. This is, however, often more due to inappropriate processes and tools rather than an ingrained resistance to the engineering principles themselves.

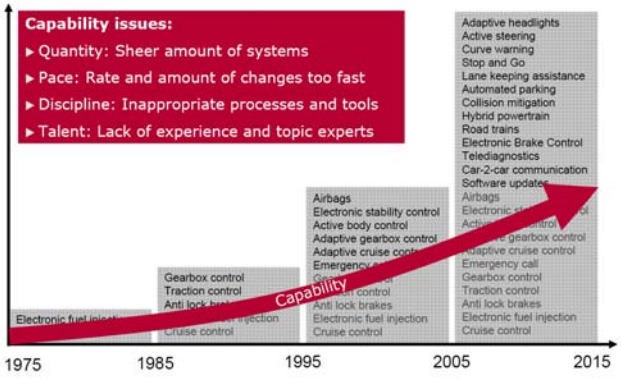

Figure 2: Capability issues in automotive systems engineering

Due to the issues described above and summarized in Figure 2, we see a strong need for major changes in the approaches taken to the systems engineering of safety-relevant automotive E/E functions. On the one hand, to provide the efficiency to allow for the number, size and complexity of functions to be developed to a sufficiently high standard and on the other to provide a clear framework within which a convincing argument for the functional safety of the systems can be made. The rest of this paper discusses how a stronger integration of the safety case into the development activities, progress in the areas of product-line development and model-driven systems engineering can lead to the step-change required to match the capabilities of the systems engineering departments to the complexities of the task at hand.

2. MODEL-BASED SYSTEMS ENGINEERING AND SAFETY

A major requirement of all safety standards is the ability to demonstrate the fulfilment of system level safety goals through the implementation of an appropriate system safety concept. Safety goals are typically derived based on hazard analyses and then refined into functional and technical safety requirements that can be allocated to individual system components.

The fulfilment of the safety goals can depend on a number of factors such as incorrectly implemented software functions or random hardware failures. Such isolated failures are relatively simple to detect and protect against using standard development techniques as prescribed by the standards. The real difficulty however lies in securing the system against failures resulting from a combination of factors from different layers of the architecture. Classical, document based processes are not well suited for coping with these types of system interdependencies, as these two examples show:

- During software development, incorrect assumptions are made about the integrity of the communication medium over which two functions interact. Communication faults, latencies etc. are not sufficiently considered in the software design. This may be due to a re-allocation of pre-existing functions across ECUs and buses.
- A hardware component shows unexpectedly high rates of failure due to a use in an installation space in the vehicle that is subject to unusually high levels of environmental (e.g. temperature, vibration, electro-magnetic interference) stress.

The approach we suggest to handling these types of complexity issues is the use of holistic model-based systems engineering techniques. These approaches allow a system to be specified from a number of different viewpoints, linked and made consistent by the use of a common underlying model. This data model should cover all aspects of EE-System design, from requirements specification, through functional architecture and technical hardware and software design (see Figure 3). A critical aspect of this approach is the ability to model the dependencies between these different architectural layers as well as domain specific attributes of the modelled artefacts (e.g. bus load, hardware fault rates, safety integrity levels, temperature ranges of installation locations, etc.). On the basis of this level of modelling analysis questions can be formulated such as, “are there any cables that run through areas of the vehicle that are particularly sensitive to crash situations and that carry signals between components for whom the correct communication is critical for the implementation of safety related functions?”.

Figure 3 Overview architectural layers

With such an approach it becomes possible to achieve a much richer integration of the engineering activities than with traditional document-based traceability based on requirements tags. This in turn leads to a greater level of coherency between the engineering artefacts, an important attribute when constructing a convincing safety case.

3. SAFETY "ROUND-TRIP ENGINEERING"

Safety standards require that analyses are performed at the system, software and hardware levels to identify weaknesses in the design and to determine the necessary improvement measures. Examples of such analysis are FMEA (failure mode and effects analysis) and FTA (fault tree analysis). In such analyses the fault behaviour of individual components is determined and their impact on the safety gaols and their failure rates analysed. A holistic approach to systems modelling which refines the system goals through a number of layers while retaining the functional dependencies between them is an optimal pre-requisite for performing the safety analyses. Whilst performing the safety analyses, the engineers can use this information to better identify the potential hazardous effects associated with the component failures. The resulting improvement measures suggested during the analysis can be directly linked to the appropriate parts of the system model, thus ensuring traceability for the safety case and improvement the efficiency of later impact analyses should parts of the design model be changed.

An extension of the model-based systems engineering approaches with elements describing the safety case and safety concept could lead to a highly interactive "round-trip engineering" approach to safety engineering whereby changes for example in the system design will immediately point to elements in the safety concept, associated analyses and safety case that require rework. Furthermore by associating particular design patterns with safety analysis and safety case patterns, parts of the safety case structure could be automatically generated based on an analysis of the design. This could lead to the ability to perform "what-if" analyses on the design, by formulating an alternative design solution and then analysing the impact this would have on creating the necessary evidence required for the safety case.

With the publication of ISO 26262 [1], the automotive industry has committed itself to implementing the principles of functional safety. Whilst contributing to providing a common understanding of the development processes required to ensure a consideration of functional safety in the development of automotive E/E systems, the standard contains only weak requirements regarding the construction of a safety case as a means of providing a convincing argument that the functional safety of the developed system has been achieved.

Experience at a number of automotive manufacturers and suppliers currently implementing the standard shows little consensus on the role, value and methods for developing, maintaining and documenting the safety case. This is not helped by the disconnect between the requirements given in Part 2 of the standard, which are vague at best, and the guidance in Part 10, which describes a proven approach established in other industries, but bears little relation to Part 2. As a result, current practices are often restricted to interpreting the safety case as a list of safety-related documents to be provided at the end of the development project. Due to the complexity of the systems being developed, it is easy to see the inherent risk associated in this approach both in terms of the development project losing sight of its progress in achieving the safety goals as well as the difficulties in convincing an external assessor of the approach taken. The potential benefits of a safety case to provide a coherent and convincing argument of the functional safety of the system as well for steering the development activities are therefore not realized.

We believe that a structured approach to constructing a safety case has the potential for tangible benefits both in terms of demonstrating the safety of the system as well as increasing the efficiency of the development.

We propose that safety cases in the form of structured arguments that combine both product and process evidence are adapted to the development of automotive E/E systems

and extended in the way that they are integrated into the systems engineering lifecycle.

In this approach, a safety case would be constructed for each system safety goal describing the strategies for meeting the goals and referencing assumptions, justification and evidence in a structured, top-down manner. In doing so, the safety case would "knit together" the evidence contained within the system model to provide a coherent and defensible argument for functional safety.

4. PRODUCT-LINE BASED SAFETY ENGINEERING

One major hurdle to safety-relevant systems development is the additional effort associated with engineering activities otherwise not required for standard development projects. In the concept phase, these activities involve performing hazard and risk analyses, developing an appropriate system safety concept and deriving the technical safety requirements on the system and its components. This additional effort is typically not planned for in current, ever shortening vehicle development project schedules leading either to delays in the project or more commonly safety activities being retrospectively performed when deficits found late in the system architecture may lead to significant additional costs.

One way of addressing this problem is to use a product-line approach to systems engineering to make use of proven, domain-specific safety concepts. Such an approach would drive systematic reuse across the whole development lifecycle based on a set of common development work products that are then tailored to take into account the vehicle specific functionality, operating conditions and architecture. To maximise the benefits of a product-line approach for safety related systems, the assets associated with the common vehicle features should be extended to include hazard and risk analyses and safety concepts. This would allow for project specific technical requirements to then be derived based on an impact analysis of the variations in function, operating conditions and architecture and the subsequent adaptation of the common requirements specifications.

By strictly controlling the commonalities and variabilities associated with the features, the reuse of technical requirements derived from the safety concepts can be maximised which in turn will drive the reuse of pre-developed components and software, thus further reducing the efforts associated with implementation and test.

5. THE WAY FORWARD

To migrate towards this vision of a model-based, safety-case driven systems engineering paradigm a number of issues must first be addressed:

- Systems engineering approaches need to be extended with the ability to model a safety case (here the integration of the Goal structuring notation would be ideal) as well as the notion of a safety concept (based on architecture and behavioural models).
- Product-line approaches must be integrated into the models (at requirements, design and safety case level).
- The approaches must not require manual effort to create and manage dependencies between the development artefacts. This should be done automatically by the underlying tool set that supports the development methods. This also includes the development and maintenance of the safety case.
- Lastly, industrial strength tool support is required not only for allowing engineers to create the graphical specifications but also to manage the underlying data to ensure consistency between the model elements, create baselines, allow for cross-site collaborative development etc.

For meeting the step change required to match the capabilities of engineering departments to the complexities of the task at hand and to meet the predicted benefit, from the suggested methods, an industrial strength tool support is a key success factor.

In detail, a development tool chain should supports by

…managing the complexity in the E/E system design by providing an approved semantic data model with domain specific attributes (e.g. bus load, latency times)

…supporting bidirectional traceability between each step of development and related artifacts (e.g. from safety goal to system safety concept, see Figure 4)

…ensuring safety analysis and development activities are performed on a single source model of the system

…ensuring consistency between all work products referenced by the safety case (configuration management)

…ensuring the completeness and consistency of the model by automatically performed rule based checks

…providing predefined elements (e.g. operation scenarios, operation modes, generic safety goals)

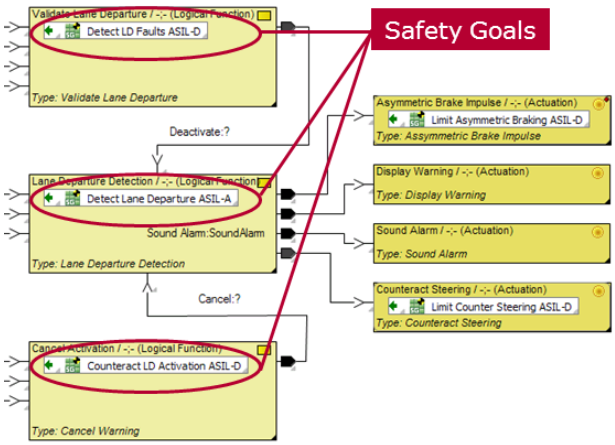

Figure 4 Vitalization: Allocation of safety goals to system safety concept

Vector Informatik GmbH offers PREEvision as an industrial strength tool support for model based systems engineering. Integrated business logic and one comprehensive data model enables a seamless EE-development process from requirements, through system, SW- and HW-design to test.

Figure 5 Model description layers in PREEvision

PREEvision enables model-based architecture development on the following layers (Figure 5)

- Product Goals (Requirements, Features), logical architectures (function networks)
- SW-architectures according to AUTOSAR
- Network topology (ECUs, bus-systems, sensors, actuators)
- Electrical circuits, wiring harness, and geometrical topology

Applying the model based systems engineering approach using PREEvision enables the following benefit

- Seamless process support from concept phase to production
- Data reuse, traceability, and impact analysis in product line context – single point of truth for E/E development
- Supports frontloading, automatic validation, and consistency checks in early development phases
- Reduced development effort through integrated design and safety process
- System level optimization leads to smarter architectures and lower product costs
- Tool-based concept evaluation and Rapid prototyping leverages validation of cost intensive decisions in early development phase
- Complete modeling and documentation of entire architecture
- Support of team collaboration and cross-organizational data exchange

6. CONCLUSIONS

Industry is in a period of change, the focus on functional safety is drawing attention to a number of areas in systems engineering where significant improvements are needed if effective solutions to problems are to be found.

Vector's **PREEvision Tool Suite** will offer the optimal solution for safety with its combination of **model-based systems engineering** with **integrated process and engineering data management**.

7. LITERATURE

[1] International Organization for Standardization, 2009. ISO DIS 26262 “Road Vehicles – Functional Safety”. Draft International Standard.

[2] Chrissis, M.B., Konrad M., Shrum, S., 2006. CMMI: Guidelines for Process Integration and Product Improvement (2nd Edition). Addison-Wesley Professional. ISBN 0321279670

[3] Joint Technical Subcommittee between the International Organization for Standardization and the International Electrotechnical Commission, 2004. ISO/IEC 15504 “SPICE (Software Process Improvement and Capability Determination)”. International Standard.