Challenges and Trends in the Engineering of Electric Automotive Systems

Thomas Illgen, Stefan Ortmann

Carmeq GmbH
Carnotstr. 4-6
10587 Berlin
thomas.illgen@carmeq.com
stefan.ortmann@carmeq.com

Abstract: The complexity of automotive systems continuously increased in the past fifteen years. Prognoses predict that 90% of future innovations in the car are based on software, and more and more safety critical functions are based on electronic systems. Factors of influence increasing the complexity are the growing numbers of networking functions, driving assistant systems, mechatronic components, comfort systems, law and environment requirements and the need of integration of consumer electronics. Especially the different life cycles of consumer electronics and vehicle systems are challenges for future engineering processes. The challenge to handle software-driven architectures of embedded systems is managing the complexity of technical solutions as well as the complexity of engineering processes and organisational barriers. This paper will introduce and discuss the aspects of complexity in embedded automotive systems. After a brief analysis of problems and challenges today and in the future, some trends managing the complexity are presented.

1 Introduction

Today's high class cars contain up to 80 electronic control units (ECU) and up to 7 different network systems. Different networks are coupled by gateways. Many of the functions are time critical and more and more functions are becoming safety critical. Figure 1 outlines a historical and future dimension of technologies and shows the increasing density of new systems. New technologies like time triggered networks (i.e. TTP, Flexray) are building the fundamentals for future X-By-Wire-Systems [ESR97] without mechanical fall back mechanisms. But still systems like ESP (Electronic Stability Program) are safety critical. Today's quality improvement depends on standardisation and reusability of dependable components as well as the improvement of the engineering processes and organisational constraints. There are lots of activities for standardisation of processes and technologies like:

- AUTOSAR (AUTomotive Open System ARchitecture) [Au06]
- Automotive SPiCE [Si06]
- FAKRA [Ju05]

Beyond the technologies a process oriented engineering organization is essential to develop complex high quality embedded systems.

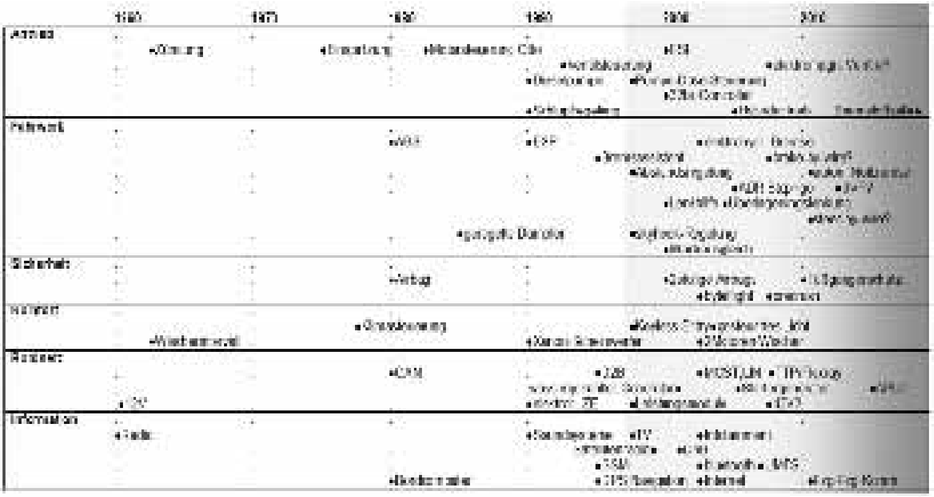

Figure 1: Historical and future technologies

2 Challenges

There are basically three top challenges:

- Complexity due to increasing number of functions and networking
- Outsourcing of development causes problems, e.g. with regard to integration
- Implementation of innovative processes based on huge organisations

To handle the increasing number of electronic control units, networking and new functions in several domains like engine, chassis, infotainment and comfort is the top challenge in automotive systems. The increasing number of new functions causes a high busload of signals on bus systems. This causes timing problems located very late in the integration process up to now. Constraints of this process are the increasing requirement of high quality and dependability as well as the enormous pressure on cost reduction. Additionally the extreme outsourcing of the development of electronic parts like ECU's, sensors or software is a main challenge for the systems planning and integration process.

A further challenge beyond technology solutions is to handle the complexity of engineering processes. Typical development cycles of three to five years for a new car have to be synchronised with extreme short life cycles of electronic components like processors or consumer electronics. Innovative processes have to be implemented and fixed by organisational structures. This causes especially in huge, established organisations a cost intensive improvement program. Additionally the implementation of safety processes and technologies based on the constraints below to secure the dependability is a top challenge for the future.

3 Trends

The top three trends are:

- New architectures
- Standardisation and Reusability
- Process improvement based on experiences of other industries

New technologies like time triggered networks (TTP, Flexray) [Fl06] or networks with high bandwidth are architectural, but expensive solutions for an inadequate bandwidth. A further trend to reduce costs and increase dependability is reusability of artefacts like requirements, models, software code or test cases. A constraint to handle the reusability in complex embedded systems is the standardisation of interfaces or components. There are several initiatives in the automotive community to standardise interfaces and to enable an interchange of engineering artefacts. These are for example requirement interchange formats based on XML (RIF), testing technologies (TTCN3), process capability determination (Automotive SPiCE) or open system architectures (AUTOSAR). But very individual and established engineering processes at car manufacturers and suppliers require time and cost intensive process improvement programs. Especially for safety critical systems like X-by-wire systems a high level engineering process is a very important constraint. It is a base to reduce the risk of failures and cost intensive service recalls or liability and a precondition for the implementation of new architectures, technologies and reusability. Therefore a main future trend of process improvement to handle safety critical systems is presented next. As a further precondition of each development and reusability process the key process of requirements engineering is outlined.

3.1 Safety and dependability

Up to now there is no official certification standard for safety critical functions in automotive systems established. Nevertheless there are activities to define an automotive standard based on the IEC 61508 called FAKRA [Ju05]. The norm defines safety integrity levels based on system criticality, e.g. frequency of situations or of event occurences, impairment and the degree of controllability. Depending on the safety integrity level, methods and processes for the engineering of safety critical systems are defined. These requirements take place as non-functional requirement in the product or process requirement specification. A risk analysis process predicts the potential harm depending on the failure of the system. To define what a top failure event causes, a deductive analysis based on fault trees (FTA) is an effective and efficient method. Based on a top event (a failure causes a critical system down time) the steps what this top event causes are analysed and the critical path is isolated. The path that causes the event has to be break down on the system structure and mechanisms of fault tolerance or well defined engineering processes have to be used to reduce the risk. The other view is a bottom up view on the causes of system defects (Functional Hazard Analysis FHA). In a moderated session the influence of a breakdown of the system or parts of the system (for example: low energy or processor breakdown) on the functional correctness has to be analysed. The critical parts have to be isolated and fault tolerance mechanisms have to be defined. Figure 2 shows the two approaches of system analysing.

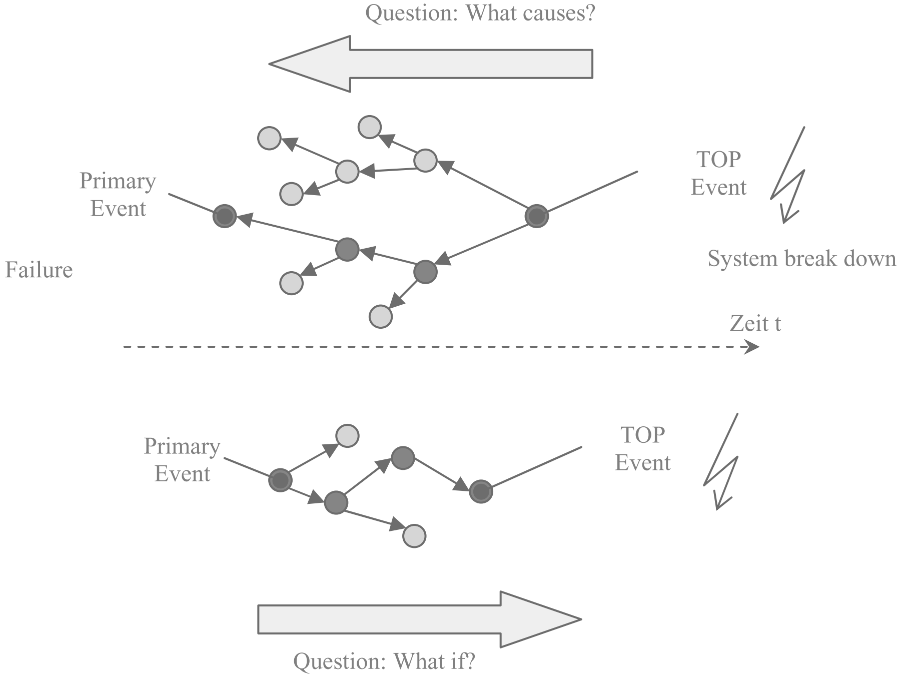

Figure 2: FTA and FHA for safety critical systems

The analysis based on these established methods utilizes on knowledge of the system behaviour. The analysis is difficult for new systems without existing experiences. An approach to handle this is the incremental analysis of the systems specification and the technical solution, e.g. the system behaviour. Bases are the well known requirements of basic safety aspects. In each incremental step a cost analysis based on risks and efficiency has to be done. Figure 3 shows the generic process of this approach.

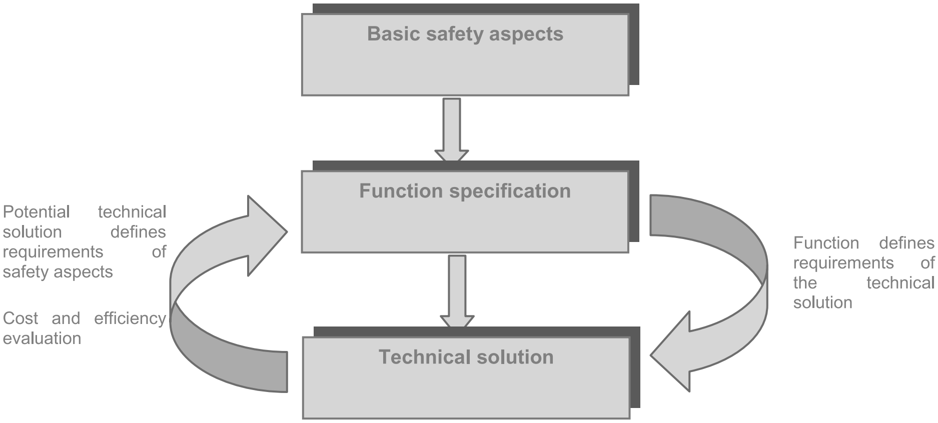
Basic safety aspects
Function specification
Technical solution
Potential technical solution defines requirements of safety aspects
Cost and efficiency evaluation
Function defines requirements of the technical solution

Figure 3: Incremental process of safety analyses and specification

The results of the safety analysis process have an influence on the systems architecture, design steps and engineering processes. The initial phase in the system engineering process is the requirements elicitation and engineering process. The results of the safety analysis are reported in the safety plan as a part of the quality plan. But safety requirements, especially requirements relevant for the architecture, function or other behaviours of the system have to take place in the system specification as shown in Figure 3.

3.2 Requirements Engineering

There are three main trends to handle requirements in automotive systems engineering:

- Writing “good” requirements: Good requirements are atomic, clear and testable [Ru04].
- Functional view on requirements: To enable new architectures, reduce cost and reduce the number of electrical control units, a requirements engineering process, traceable from the first definition of a new product line to each part of an electric, electronic system, has to be defined. The hierarchical layers in this functional decomposition process have to be well defined and adopted to the testing process and methods.
- The complexity of variants and product lines has to be handled. Invariants over different products have to be defined. This is a key requirement of reusability of all engineering steps [PBL05].

The functional view on the system architecture is completely different from the present engineering process. Instead of a bottom-up view from electronic control units to the integration of implemented functions a top-down approach from marketing aspects over functionality to the implementation of required resources like sensors, processor power, control units or bandwidth should be established. The main goals of this approach are:

- Closer system view in early engineering phases
- Reduction of resources
- Later distribution of functionality on resources
- Reusability of encapsulated artefacts, e.g. specifications, code, test cases
- Traceability of functionality in the system life cycle
- Variants or product line management

Aspects of the safety process or new technologies as described below are based on the changing of thinking from component implementation to function orientation. This new thinking has many influences on the system engineering process and organisational structures. It couples the non-technical view of marketing aspects with technical solutions as well as the phases in the design, implementation, integration and functional decomposition process. Therefore new responsibilities like for example function specialists in charge have to be established.

This includes an intensive process improvement program. The key approaches of successful process improvement programs are outlined in chapter 4.

4 Process Improvement

In large organisations like car manufacturers the improvement of processes is a very sensible and difficult challenge. Beyond technical innovations, human aspects of changing daily work and management aspects are often different. There are some basic aspects in software improvement programs:

- Analysing existing processes and daily work of employees
- Define and realise quick wins
- Planning and negotiation of the improvement program
- Piloting of the developed solutions and artefacts
- Developing and planning of a roll-out concept

- Timing and endurance

It is important to find a distribution channel for new processes and methods in the organisation. First the management has to commit the planning. The improvement concept depends on the organisation. In strong hierarchical organisations an improvement program could be realised by order. Normally a trust of help has to be established. This help is identified by analysing the largest problems in the project and realisation of quick wins, e.g. a quick help for this problem. A roll-out concept has to be developed in an early phase of the improvement program to define realistic goals. The roll-out concept has to include training concepts and distributors as multipliers and supporters in the project.

5 Conclusion

The top challenge of the future development of automotive systems is to handle the complexity of the increasing number of functions, networking and safety criticality. Today's solutions to handle this complexity are based on:

- Standardisation
- Architectures
- Processes

These solutions are interdependent. That is the main problem for the change process. We have shown some top trends in early phases of the engineering process to handle this problem. These are aspects of safety and dependability, requirements engineering and process improvement as concepts of implementing the solutions. Even if technical solutions are well defined and understood, innovation is also a changing of thinking and behaving of people and organisations. To break these human and organisational barriers might be the largest challenge in the future.

6 References

[ESR97] E. Dilger, L.-A. Johansson, H. Kopetz, M. Krug, P. Liden, G. McCall, P. Mortara, B. Müller, U. Panizza, S. Poledna, A. Schedl, J. Söderberg, M. Strömberg and T. Thurner: Towards an Architecture for Safety Related Fault Tolerant Systems in Vehicles, In: Proceedings of the ESREL' 97 InternationalConference on Safety and Reliability, Volume II, June 1997, (pp. 1021-1030), Lisbon. [ABC01] Abraham, N.; Bibel, U.; Corleone, P.: Formatting Contributions for LNI. In (Glück, H.I. Hrsg.): Proc. 7th Int. Conf. on Formatting of Workshop-Proceedings, New York 1999. Noah & Sons, San Francisco, 2001; S. 46-53.

[Au06] AUTOSAR.ORG: http://www.autosar.org, 2006

[Si06] Automotive SPiCE: http://www.automotivespice.com, 2006

[Ju05] C. Jung: Stand des Automotive Standards für funktionale Sicherheit – FAKRA-Entwurf, In: Safetronic 2005, Munich 2005

[Fl06] Flexray: http://www.flexray.com, 2006

[Ru04] C. Rupp, Requirements Engineering and Management, Hanser, 2004

[PBL05] Pohl, K.; Böckle, G.; van der Linden, Frank: Software Product Line Engineering – Foundations, Principles and Techniques, Springer, 2005.