

Introducing automotive E/E safety engineering: Challenges and solutions

Abstract:

Functions such as adaptive cruise control, crash protection systems, active body control and ESP are increasing in complexity and taking an ever more active role in controlling the car. These functions are realized by systems of sensors, actuators and interconnected electronic control units. The systems must be designed to function under a variety of operating conditions and must adhere to a number of mechanical, hardware and software constraints. In order to be able to manage the emerging product liability risks associated with such systems as well as ensuring the high level of quality required of automotive systems, significant improvements to engineering processes are necessary. In this article, we describe our experiences in adapting companies' development processes to conform to safety standards and to cope with the challenges mentioned above. We detail key success factors in overcoming these challenges and provide practical examples from working with global OEMs and tier-one suppliers on implementing safety standards in E/E development.

Authors:

Dr. Christof Ebert, Dr. Simon Burton, Dr. Klaus Amsler, Dr. Dieter Lederer

Lead authors CV:

Dr. Christof Ebert is managing director and partner at Vector Consulting Services. He is helping clients worldwide to improve technical product development. Prior to that, he held engineering and management positions for more than a decade in telecommunication and aerospace. As author of articles and several books, speaker and consultant, his results-driven contributions have influenced numerous companies.

Dr. Simon Burton is a Manager at Vector Consulting Services. His current focus is on advising automotive manufacturers and their suppliers on achieving conformance to safety standards such as IEC 61508 and ISO 26262. Prior to this position, he led the pre-development of infotainment system architectures and performed internal consulting in the area of software and systems engineering at a premium automotive manufacturer.

Contact information:

Dr. Christof Ebert
Vector Consulting Services GmbH
Ingersheimer Straße 24
D-70499 Stuttgart
Germany
www.vector-consulting-services.com
Mailto:christof.ebert@vector-consulting.de
Phone Number: +49 711 80670-175
Fax Number : +49 711 80670-444

Introducing automotive E/E safety engineering: Challenges and solutions

Abstract

Functions such as adaptive cruise control, crash protection systems, active body control and ESP are increasing in complexity and taking an ever more active role in controlling the car. These functions are realized by systems of sensors, actuators and interconnected electronic control units. The systems must be designed to function under a variety of operating conditions must and adhere to a number of mechanical, hardware and software constraints. In order to be able to manage the emerging product liability risks associated with such systems as well as ensuring the high level of quality required of automotive systems, significant improvements to engineering processes are necessary. In this article, we describe our experiences in adapting companies' development processes to conform to safety standards and to cope with the challenges mentioned above. We detail key success factors in overcoming these challenges and provide practical examples from working with global OEMs and tier-one suppliers on implementing safety standards in E/E development.

Introduction

Some years ago an electronic parking brake system was introduced in order to assist the driver as well as to save on weight and mechanical overhead and cost. The principle was very simple. Once the brake was activated it would prevent the car from rolling and as soon as the driver activated the throttle, it would release, thus relieving the driver from handling the synchronization of releasing the brake while simultaneously pushing the throttle. The concept worked fine and of course, the electronic parking brake had two redundant channels straight from the parking button to the brakes. During a test drive on a hot summer day, the driver stopped the car to check something outside and activated the electronic parking brake. He left the engine running as it was a short stop and he only intended to briefly leave the vehicle. The car was, after all, secured by the parking brake. A few seconds after he had left the vehicle, it suddenly accelerated and crashed into a wall. What had happened? The electronic parking brake system just worked fine. But, when the driver left the car, he naturally opened the door. This allowed hot air into the vehicle. The air condition activated itself to sustain the desired interior climate. Since it needed more power, it slightly increased the throttle – which released the brake...

Safety-critical systems have the potential to cause physical harm should they fail in their intended function. Failures can be due to random hardware faults (e.g. short circuits) or systematic design errors (e.g. software defects). The risk associated with the system is reduced by minimizing the probability of a failure occurring and limiting the consequences of unavoidable failures. With the increasing complexity of the vehicle, its electronic components and their interworking, safety concepts will therefore be at the core of any new design, be it for the change of an existing function, such as in above example, or be it for a completely new function.

Functional safety is dependent on the correct functioning of the system [1,2]. It is a property of the system as a whole rather than just a component property, i.e., it depends on the integrated operation of all sensors, actors, control devices, etc. The goal is to reduce the residual risk associated with a functional failure of the system to "As Low As Reasonably Practicable" (ALARP) [3,4].

Safety as a basic concept has a long tradition in specific disciplines, such as the design of the passenger cell to protect drivers or the anti-blocking braking system that has strongly reduced fatal accidents [4]. However, today we have to acknowledge that safety has reached a new level of impact and risk. It is not anymore individual components that add to safety, but rather their interworking at the system level, that is the entire vehicle with its physical assembly of mechanical and electronic subsystems.

This article provides experience and guidance on how automotive E/E safety engineering can be successfully introduced. Standards such as IEC 61508 [1] and ISO 26262 [2] provide some guidance, but a thorough understanding of what safety means on engineering and management levels is absolutely critical to achieve a culture of safety within product development! Note in this context, that IEC 61508 is still widely used in practice, specifically by suppliers, but there is a fast move towards the recently released ISO 26262 which will quickly evolve to the leading standard in functional safety for the automotive industry. Most OEMs and tier-1 suppliers prepare since two years for this migration and acknowledge that ISO 26262 is much more specific to automotive needs and also is more precise as to which methods to apply depending on the ASIL-level and environment (e.g., embedded software, supportive software, tools).

Our experiences from safety engineering in industries such as automotive, transport and automation show that safety engineering is only successful when considering three needs in parallel (see Fig. 1), namely

1. System-oriented development
2. Safety methods engrained to engineering
3. Improved process maturity

This article will detail these three needs and show how they can be translated into concrete development practices. With practical examples from working with global OEMs and tier-one suppliers on implementing safety standards in E/E development, the article will be of help to those engineers and companies just starting with safety engineering or optimizing their current practices towards more efficiency and effectiveness.

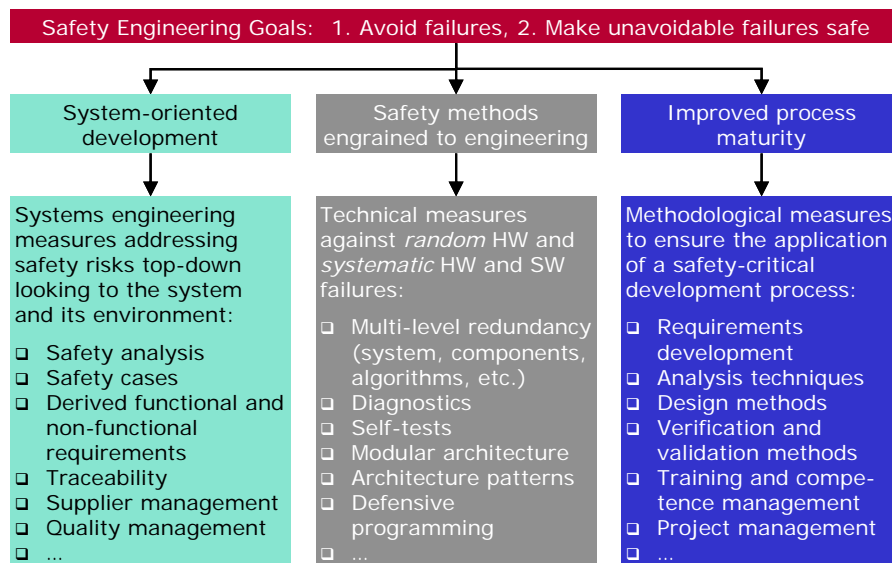


Fig. 1 Practical Safety Engineering

Challenges in applying safety standards in the automotive industry

Engineering safety-critical automotive systems is still a major challenge and often is associated with significant development overheads. The main obstacles towards achieving effective and efficient safety-engineering in the automotive industry can be summarized as follows:

1. Component-oriented development
2. Inadequate process capabilities
3. Abstract standards

The development of automotive E/E systems is still too component-orientated. Safety, however, is a property of the system as whole. The consideration of safety aspects across a number of components often requires a more systematic approach to requirements and quality management than is currently practiced as well as organizational changes in the development departments. It is often not possible, with current processes to ensure the traceability from top level safety goals at the system level (e.g. the electronic parking brake must not activate above certain speeds) to software safety requirements (e.g. plausibility checks on sensor values).

Safety-engineering is only achieved when following a strict process-oriented development with a rigorous application of project, quality and supplier management practices. These prerequisites are often missing in the development processes we have observed and must first be established to form a basis upon which the safety-specific measures can be effectively applied. As a typical example, requirements on supplier development practices are often included in the requirements specification but not verified or enforced by the OEM during the development of the systems.

Current safety standards are rather abstract and do not give concrete guidance as to how the required measures can be efficiently integrated into existing processes [3]. The detailed changes and extensions to the processes required to achieve conformity need to be identified on a case by case basis for each organization. On the other hand, there is a trend visible in the recent evolution of the standards towards prescriptive details on how engineering processes, specifically formalized safety requirements and safety case specifications and their verification should be treated. The risk with this approach in standards is that engineers would just follow what is described and not really consider what is pragmatically necessary, looking to safety needs, risks and economic trade-offs. In consequence, safety engineering will be expensive and complex but not necessarily exhibit improved safety to the user.

This can be best understood when taking the example of accidents such as the London ambulance system (causing deaths during a reconfiguration activity) or the Therac medical radiation system (causing deaths due to radiation overdose) [11]. Both have been designed following the required standards, and still failed to exhibit safety because they lacked in usability. With untrained drivers that do not understand the complexity of underlying devices, this problem will accumulate. The message clearly is that safety standards do not provide sufficient guarantee for safety if above criteria of systems engineering and thinking paired with disciplined high-maturity processes are followed.

Success factors for safety engineering

From our experiences in introducing safety concepts to automotive OEMs and tier-one suppliers around the world, we see three needs to establish a safety engineering culture – on top of already institutionalized disciplined management and engineering practices, namely

1. System-oriented development
2. Safety methods engrained to engineering
3. Improved process maturity

Safety demands a systems engineering perspective. Complexity growth within the electrical subsystems of the car, their networked interconnection, and increasing variability of features make embedded E/E systems more and more vulnerable. Such risks demand strong protection on various levels along the entire life-cycle. Most relevant above all is to identify the relevant safety risks how they can be avoided or mitigated against at a system and software level. Especially for automotive embedded systems, safety must be handled starting with system specification, analysis and design. Once initial architecture and design is complete, the multitude of different components and their interaction will not anymore allow to retrospectively design for safety.

In the relationship management of automotive supply chains the principle of divide and conquer is hierarchically established and deeply engrained into the management and engineering culture. This obviously had its merits while nuts and bolts were being acquired that were selected from supplier catalogues. However, an electronic steering system, for example, cannot be acquired by referencing such standard specifications. It must be designed as an integral part of the vehicle, taking into consideration its physical, dynamical and mechanical behavior as well as electronic and many other constraints. Nevertheless, OEMs are still overly prudent not to disclose too much systems information, while their tier-1 suppliers are often looking towards their specific subsystems and trying to verify features on that level only.

The V-model with all its merits must be understood not from a piecemeal perspective where verification happens only on the lowest level, but rather as an integrated framework, where requirements and specifications for safety design, implementation and verification are derived top-down from systems requirements and design principles. Fig. 2 provides some examples of safety engineering techniques and how they are driven from a systems engineering perspective.

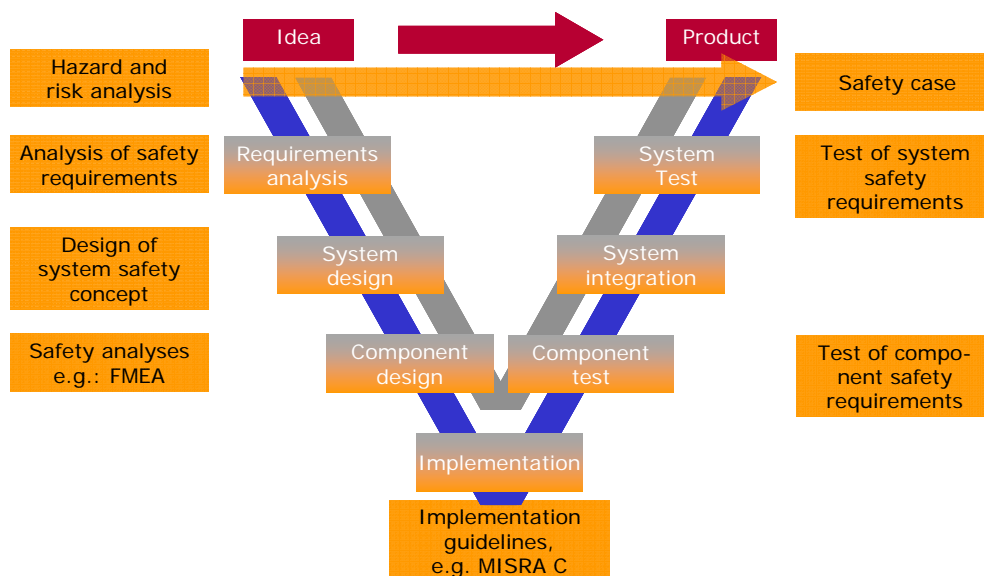


Fig. 2 Safety concepts evolve top-down

Safety concepts must be defined at the system architecture level. A systematic requirements management is required to document the safety requirements derived from the system level safety analyses (using methods such as FMEA, FTA etc.), the allocation of these safety requirements to individual components and, after successive application of safety analyses at the component (hardware and software) level, to specific safety-related technical requirements on each component.

Each single engineering activity must be enhanced by adequate safety methodologies. Fig. 3 described the derivation of component specific technical requirements from the safety analysis and top-level safety goals. Vertical and horizontal requirements traceability provides a solid basis for managing the dependencies between safety requirements at various levels of the product architecture.

Due to the shift from component towards system-oriented development a re-allocation of responsibilities within the organization and between manufacturer and supplier is often required. There must be a clear responsibility for functional safety at a system level and the provision of the system safety case (to demonstrate the adequate implementation of functional safety). From a supplier perspective the critical requirements must be agreed with

the OEM early in the proposal phase to evaluate the impact on BOM and development costs. Management and commercial analysis is heavily impacted by safety engineering. Tender analysis for instance demands close interaction to evaluate which requirements are appropriate given the level of risk and which measures might not justify the additional cost involved. From a legal perspective, the identified and agreed critical requirements must be documented in the product specification or product requirements specifications as applicable while ensuring throughout the development process that they are traceable to technical requirements at the hardware and software level.

The development of safety-critical software will require placing more emphasis on excluding systematic errors through software architecture design, software implementation guidelines, and software verification and validation. Specific safety methods and techniques must be deeply engrained into the engineering methods. This is obvious when it comes to using coding standards and rules for programming safety-critical software [3,5]. But coding is not enough. The high quality demands of modern E/E systems can only be ensured with systematic engineering processes. Starting late and looking only to components as many were used to, is not the answer. A high overall quality level and thus early defect detection and removal is only feasible by combining a multitude of cascaded design, verification and validation activities starting with requirements engineering and only ending with end of service and retirement of a product or service.

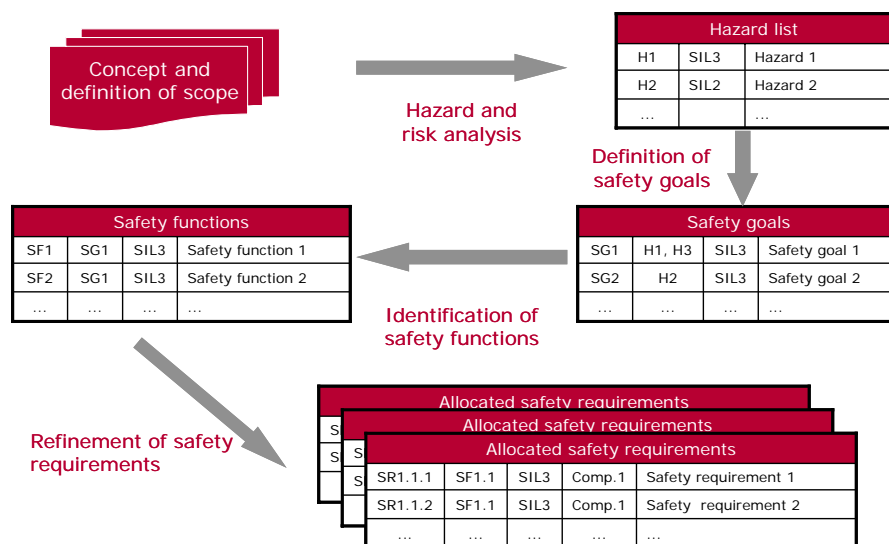


Fig. 3 Safety analyses and safety requirements

Hardware development demands a documented development process including the use of analysis techniques for assessing the reliability of the hardware such as design FMEAs and worst case tolerance calculations. Potential hardware failure rates must be quantitatively modeled and used to apply hardware diagnostic measures in order to provide a more arguably robust design.

Safety engineering during design demands systematic defect prediction, detection, correction and prevention. The first step is to identify risks and hazards as they would relate to malfunctions and how defects would be critical to performance. The underlying techniques are statistical methods of defect estimation, reliability prediction and criticality assessment [8]. Systematic defects in the design or implementation have to be detected by quality control activities, such as inspections, reviews, unit test, etc. [9,10]. Each of these techniques has their strengths and weaknesses which explains why they ought to be combined to be most efficient. It is of not much value to allocate a large number of engineers to testing, when in-depth requirements reviews would be much faster and cheaper. Once defects are detected and identified, the third step is to remove them. This sounds easier than it actually is due to

the many ripple effects each correction has to a system. Regression tests and reviews of corrections are absolutely necessary to assure that quality won't degrade with changes. A look to cost of non-quality and efficiency demands focus on preventing defects from re-occurring. Often engineers and their management state that this actually should be the first and most relevant step. We agree, but experience tells that again and again, people struggle with defect avoidance simply because their processes won't support it. In order to effectively avoid defects, engineering processes must be defined, systematically applied and quantitatively managed. This being in place, defect prevention is a very cost-effective means to boost both customer satisfaction and business performance, as many high-maturity organizations have shown [8,10].

In order to fulfill the requirements of the standards, process maturity is required. In other words, planned tasks for safety are tracked until completion, safety requirements are systematically identified and traced throughout the entire process and it must be shown that all necessary activities were performed conform to the process and that the product meets all its requirements (i.e., the safety case). In our experience, the CMMI [6] and SPICE [7] process improvement frameworks provide a good basis for implementing safety processes. Adapting development processes to conform to the safety standards as part of a CMMI or SPICE process improvement program ensures that the necessary pre-requisites are achieved which then form a solid basis for ensuring that additional measures for safety are effectively introduced in a controlled and sustainable manner.

Fig. 4 provides an overview how the practices of CMMI support to requirements from currently mostly used safety standard in automotive industry, namely IEC 61508. The same "translation" could be done for ISO 26262. Many requirements demanded by a thorough safety process are covered by the CMMI framework. Given the current focus of OEMs on supplier management and demanding the use of CMMI, this framework is thus a good – and cost-effective – basis for implementing safety standards. Note though, that the process framework needs to meet maturity level 3 requirements as this is where engineering is detailed. In addition safety specific practices are required (e.g. hazard analysis, safety assessments, compilation of a safety case) which can be integrated in process areas such as requirements development or product integration.

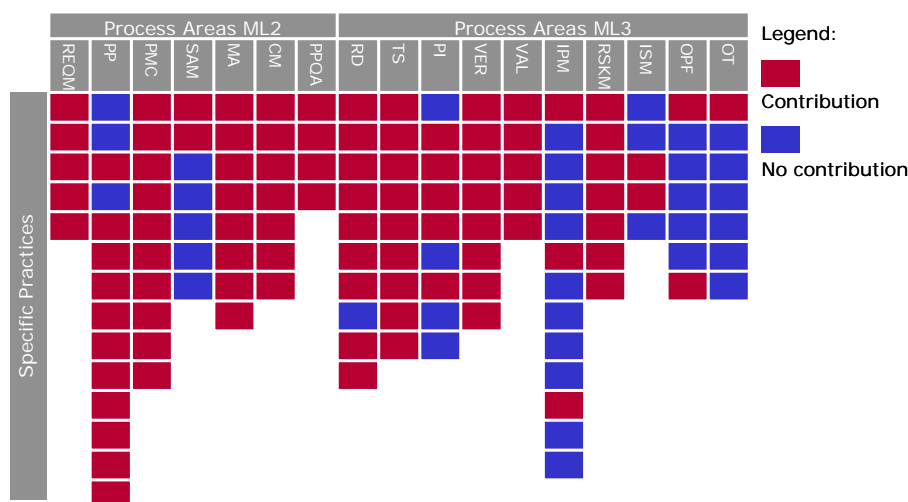


Fig. 4 Mapping between CMMI practices and safety standards

By addressing the safety aspects in combination with other process improvement measures, an efficient process realization can be achieved [8]. For example, a safety plan can be realized as an extension to existing project and quality management plans and a safety case can be realized by instantiating these plans with reference to the results of the various analysis, verification and validation measures. Fig. 5 shows how the traditional development

plans can be enhanced with safety-related extensions. The column on the left shows some examples from the development plan as it is today practiced, looking to areas such as project planning, quality assurance and configuration management. The middle column shows extensions for these three areas to design for safety. The column on the right shows which evidence, related to the plans, can be used in building the safety case. The “command and control” principle which we know from aerospace obviously applies to automotive safety engineering as well. Needless to say that the three mentioned areas of planning, QA and CM are just examples, and all process areas have to be extended, including domains such as training or measurement.

Systematic process improvement means organizational change management. For the reasons described above (i.e., move towards system-oriented development and the need to establish basic process capabilities) adapting development processes to conform to the safety standards nearly always needs to be addressed as part of a systematic and wider ranging process improvement effort. This includes:

- Aligning process improvement measures to the organization’s business goals to ensure that safety-related improvements are not introduced at the expense of other goals such as cost and efficiency.
- A detailed understanding of the strengths and weaknesses of the existing processes. It is rarely possible to redefine development processes “from scratch” in working organizations. The additional measures required by the safety standards must therefore be intelligently integrated into the existing development practices.

In order to address the organizational changes associated with the move toward a system-oriented development, the improvement of basic process capabilities, as well as the establishment of safety-specific roles and development activities, an early consideration of organizational change management aspects is essential. This includes ensuring support of senior management in terms of communication of the organizational goals, the provision of resources and the authority to enforce the changes.

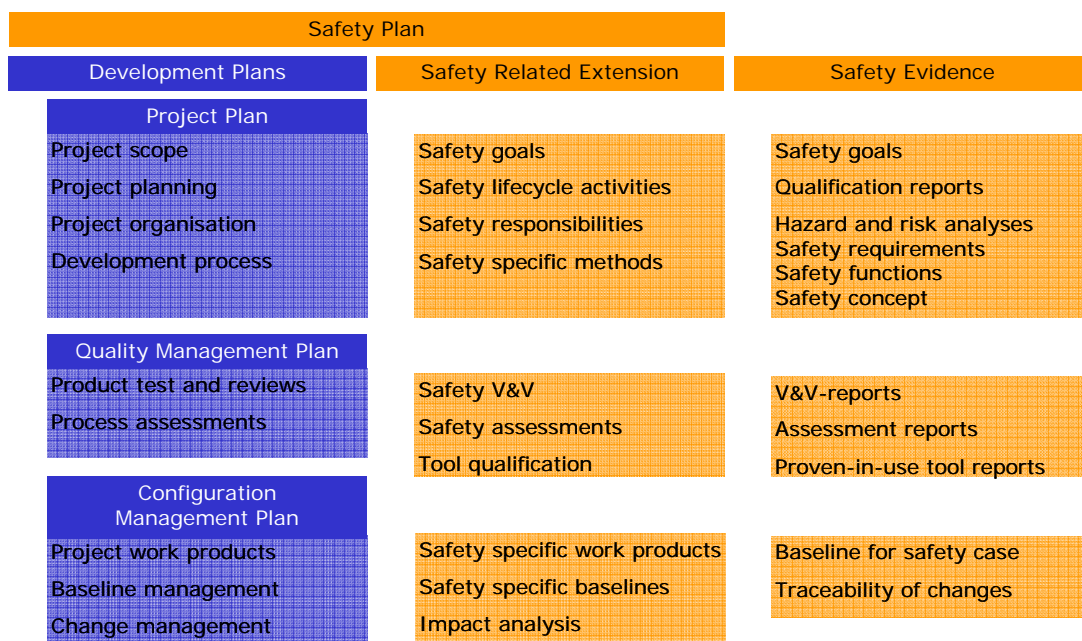


Fig. 5 Safety plan and safety case: A pragmatic approach

Conclusion

Safety engineering and thus the adoption of safety standards such as IEC 61508 and ISO 26262 in the development of automotive systems is no rocket science and is absolutely

necessary to avoid severe product liability risks in the future! We highlighted three key components for sustainable safety engineering in automotive systems, namely system-oriented development, safety methods engrained to engineering and improved process maturity.

Let's go back to our introductory example to show what would be different. System-oriented development would have helped to consider the entire system and its signals, thus not using the throttle signal on the CAN-bus but rather taking the breaking pedal position. Engraining safety methods across the life-cycle would for instance create test cases in parallel to establishing the safety case. Those would be broken down to ensure on component and product level a full traceability from safety requirements and safety case to design decisions and their verification. Finally a higher process maturity would have demanded to review operational scenarios from different perspectives and evaluate alternative designs before implementing what looks most cost-effective but does not fulfill safety standards.

An efficient implementation of the standard requirements can be achieved through the systematic management and improvement of development processes combined with the introduction of few focused safety-specific measures. In introducing a safety culture to OEMs and suppliers we found two efficiency handles to reduce cost of safety engineering:

- A maturity level 1 organization wanting to ramp up towards SIL 3 typically pays 30-50% more for engineering. A combined introduction of safety engineering with improving process maturity to maturity level 3 would still create this cost, but additionally yield immediate returns through defect phase containment, easier change management and improved predictability – each contributing with 10-20% to reducing engineering cost.
- Having a system perspective when specifying and implementing SIL-3 requirements and designing components top-down in a distributed architecture achieves substantial benefits due to not demanding SIL-3 on each component and controller but achieving trade-offs by allocating cost factors to safety designs and then comparing overall system cost. We found at an OEM with this method that a combined electric and mechanical solution was from a life-cycle perspective much cheaper than having the same function fully implemented electrically.

Migrating to a safety-conform development will only be successful if it is understood and performed as a cultural and thus organizational change. However, too often, safety is understood primarily as a technical challenge where few additional requirements are added to an already overly long specification. A safety culture needs to be established.

Management and engineering needs to understand the challenge of safety as a multidimensional need which impacts management processes, responsibilities and engineering methods. Functional safety needs to be seen as a critical product liability issue with all consequences on disciplined and formalized development. Engineers need to understand safety needs on the system level and adopt their engineering methods towards systematic and traceable decision-making from architectural to functional and component-levels.

For organizations starting towards a safety culture across their engineering we recommend an integrated and incremental approach to achieving safety standards while at the same time improving basic process capabilities. Fig. 6 provides an approach for facilitating step-wise yet deterministic migration towards a full safety coverage.

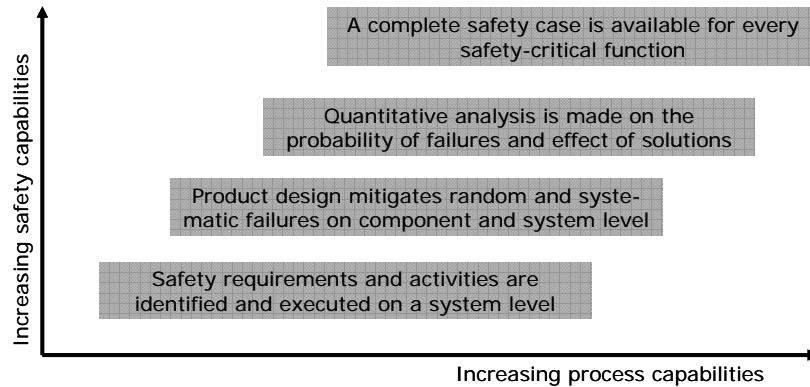


Fig. 6 Migrating towards safety-critical development

Necessary improvements towards systematic safety engineering in automotive systems need to be made in coordination with other organizational goals such as cost, quality and efficiency. The good news though is that state of the practice techniques, such as engineering and management processes following CMMI Maturity Level 3 goes a long way in achieving many of the pre-requisites for fulfilling the requirements of the standards.

Literature

- [1] IEC 61508: Functional safety of electrical / electronic / programmable electronic safety-related systems (E/E/PES), IEC, <http://www.iec.ch>, 1998. See also: <http://www.iec.ch/zone/fsafety/scope.htm>
- [2] ISO 26262: Automotive Functional Safety, ISO, <http://www.iso.org>, 2011.
- [3] Smith, D. J. and K.G.L. Simpson: Functional Safety: A Straightforward Guide to Applying IEC 61508 and Related Standards. Elsevier, New York, USA, 2004.
- [4] Pimentel, J.R., ed.: Safety-Critical Automotive Systems, Soc. of automotive engineers. SAE books international, Warrendale, USA, 2006.
- [5] Bärwald, A.: IEC 61508 & MISRA C – The Benefits of Utilising IEC 61508 and MISRA C for Automotive Applications. 1st IEE Automotive Electronics Conference, London, UK, 2005.
- [6] Chrissis, M.B., M. Konrad and S. Shrum: CMMI. Guidelines for Process Integration and Product Improvement, ed. 2. Addison-Wesley, Reading, USA, 2006.
- [7] ISO/IEC 15504:2004. Information technology – Process assessment. ISO, <http://www.iso.org>, 2004.
- [8] Ebert, C. and R. Dumke: Software Measurement. Springer, Heidelberg, New York, 2007.
- [9] Vector Informatik: Efficient Testing in Automotive Electronics - A test environment from HIL simulation to diagnostics. ATZ, No. 7-8, 2007. Accessible at: http://www.vector-worldwide.com/portal/medien/cmcc/press/PND/Testing_ATZ_200708_PressArticle_EN.pdf
- [10] Shull, F. et al: What we have learned about fighting defects. Proceedings of the 8th International Symposium on Software Metrics. IEEE, Los Alamitos, USA, pp. 249-258, 2002.
- [11] Leveson, N. G.: Safeware: System Safety and the Computer Age. Addison-Wesley. Reading, MA. 1995.