Sicherheitsmanagement in einem mittelständischen Bahnsystemunternehmen

Safety management in SME company supplying railway systems

Juha Turunen

Sicherheitsmanagement ist der Schlüsselfaktor im Eisenbahn-Signalling-Geschäft. Wenn man verschiedene Geschäftsbereiche, wo sicherheitskritische Anwendungen erforderlich sind, vergleicht, sieht man die Unterschiede bei der Bewertung der Verfahren und Risiken. Wenn man zum Beispiel sicherheitskritische Prozessautomatisierung in einem Kraftwerk oder einer Fertigungslinie plant und analysiert, so kann man diesen Prozess höchstwahrscheinlich umstellen, wenn das Risikomanagement anzeigt, dass das Verfahren, in dieser Weise implementiert, zu gefährlich wäre. Bei der Eisenbahn liegt es in der Natur der Sache, dass der Personentransport nicht umgestellt werden kann. Wir bei Mipro sind uns dieses Umstandes bewusst, dass die Geschäftstätigkeit im Bereich Eisenbahn-Signalling die höchstmögliche Qualität und Sicherheit erfordert.

1 Freiheit von Risiken

Um das Konzept des Sicherheitsmanagements komplett zu verstehen, bedarf es zunächst der Definition einiger Schlüsselbegriffe. Sicherheit ist die Freiheit von nicht tolerierbarem Risiko [1]. Diese Definition ist offensichtlich sehr allgemein und lässt ein numerisches oder sonstiges leicht messbares Kriterium, wonach man tolerierbares Risiko bestimmen könnte, aus. Dafür gibt es keine einfache Antwort oder Definition, weil das Risiko, das zu tolerieren man bereit ist, sich von Land zu Land unterscheiden kann. Für die schwersten Fälle ist das aber zumeist einfacher zu definieren: Der Verlust menschlichen Lebens ist nicht tolerierbar.

Das gesamte Sicherheitsmanagement besteht aus verschiedenen Sichtweisen auf die Sicherheit. Obwohl jeder Bereich der Sicherheit, wie er in dem Bild zum Gesamtsicherheitsmanagement (Bild 1) dargestellt ist, essentiell ist, so beschränkt sich dieser Beitrag auf den Bereich der funktionalen Sicherheit. Was ist mit Funktionale Sicherheit gemeint? Funktionale Sicherheit ist ein Teil der Gesamtsicherheit, die von einem System oder einer Ausrüstung abhängt und korrekt in Abhängigkeit von den Eingangsdaten betrieben wird [1]. Der korrekte Betrieb umfasst dabei das Konzept der Funktionalität des Systems, das in geeigneter Weise funktionieren muss, um sicheren Betrieb der entsprechenden Sicherheitsfunktion in einer sicherheitskritischen Anwendung zu gewährleisten.

Auf der Grundlage der obigen Definitionen können wir leicht die Aufgabe der funktionalen Sicherheit ersehen, so wie diese in international anerkannten Normen für die Implementierung von sicherheitskritischen Anwendungen definiert ist. Die Aufgabe ist, *„sicherzustellen, dass die Freiheit von Risiken auf physische Verletzung oder Gesundheitsschaden am Menschen durch ein nicht hinnehmbares Risiko durch unmittelbare oder mittelbare Einwirkung infolge von Zerstörung von Sachwerten oder der Umwelt, gegeben ist.“* [1] Die Priorität

Safety management is the key factor in the railway signalling business. The differences between the assessment of the process and the risks become apparent when comparing different industry domains where safety critical applications are required. For example, when planning and analysing safety critical process automation for a power plant or for a production line, the process can most probably be redesigned, if the risk assessment indicates that a process is too dangerous to be implemented as such. However, the nature of railways means that the process of transporting passengers cannot be changed. At Mipro, we are aware that conducting business in the railway signalling industry demands the highest possible level of quality and safety.

1 Freedom from risk

To fully understand the concept of safety management, certain key terms need to be defined first. Safety is freedom from risk which is not tolerable [1]. This definition is obviously somewhat general and it does not actually define any numerical or otherwise easily measured criteria as to what constitutes a tolerable risk. There is no simple answer or definition of a tolerable risk, because the tolerability may differ in different countries. However, it is typically easier to define this for the most severe cases: a loss of human life is not tolerable.

Overall safety management consists of several views of safety. Although each area of safety presented in the overall safety management figure (fig. 1) is vital, this article only considers safety from the point of view of functional safety. What does the expression functional safety mean? Functional safety is part of overall safety which depends on a system or equipment operating correctly in response to its inputs [1]. Operating correctly includes the concept of the functionality of the system, which must function correctly in order to guarantee the safe operation of a particular safety function in a safety critical application.

The aforementioned definition enables us to easily understand the objective of functional safety as it is defined in internationally recognised standards pertaining to the implementation of safety critical applications. The objective is *“to ensure the freedom from risk of physical injury or damage to human health caused by an unacceptable risk directly or indirectly as a result of the destruction of property or the environment.”* [1] The first priority is to protect human beings, but the safety of property and environment also has to be considered.

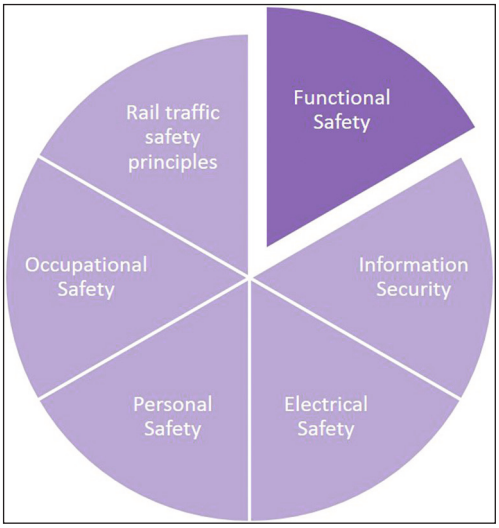

Bild 1: Funktionale Sicherheit ist ein Teil des Gesamtsicherheitsmanagements.
Fig. 1: Functional safety is part of overall safety management.

liegt auf dem Schutz des Menschen, wobei auch die Sicherheit von Eigentum und Umwelt zu berücksichtigen ist.

2 Unfallvorbeugung

Die wichtigste Aufgabe im Zusammenhang mit der funktionalen Sicherheit besteht in der Verhinderung von Unfällen. Aber wie können wir das erreichen? In der Eisenbahnbranche können wir dies zum Beispiel dadurch erreichen, indem wir funktional sichere Stellwerkssysteme zur Kollisionsverhinderung implementieren. In Kraftwerken können funktional sichere Verfahrenssteuerungen und Schutzsysteme zur Verhinderung von Explosionen zum Einsatz kommen. Die Schlüsselanforderung dabei liegt in der beständigen Risikoanalyse und -bewertung, und zwar während Planung, Entwicklung, Implementierung und Betrieb von sicherheitskritischen Ausrüstungen und Anwendungen.
Das Konzept „funktional sicher" ist eng verwandt mit der Sicherheitsstufe, die erreicht wird, indem die Anforderungen an die Integrität nach bestimmten Normen umgesetzt werden. Das bedeutet, dass wir eine angemessen sichere Implementierung mit der erforderlichen Integrität erreichen können, bedauerlicherweise gibt es jedoch keinen 100 %-Nachweis für funktional sichere Implementierung. Das ist etwas, was viele nicht verstehen. Die höchste definierte Sicherheitsstufe ist SIL4, bei dem aber immer noch ein sehr kleines Restrisiko bleibt. Um eine implementierte Sicherheitsfunktion zu erhalten, die einer bestimmten Sicherheitsstufe entspricht, müssen wir neben den ganzen technischen Anforderungen auch die Anforderungen der Normen hinsichtlich der systematischen Integrität und der Hardwareintegrität erfüllen. Die systematische Integrität betrachtet hauptsächlich qualitative Aspekte wie Prozesse und verwendete Techniken und Maßnahmen, wohingegen die Hardwareintegrität auch auf quantitative Belange eingeht, einschließlich der architektonischen Einschränkungen für eine konkrete Anwendung. An dieser Stelle werden selbst Personen, die nicht sonderlich mit dem Konzept der funktionalen Sicherheit vertraut sind, einen ersten Halt finden: den Wert der Wahrscheinlichkeit eines Gefährlichen Fehlers pro Stunde der Sicherheitsfunktion (PFH), der als die am besten bekannte Anforderung von SIL gilt. Daneben gibt es jedoch noch hunderte anderer Anforderungen, die zu berücksichtigen sind.
Wenn man die Akzeptabilität des Restrisikos betrachtet, so ist klar, dass das Restrisiko kleiner sein muss als das angestrebte zulässige Risiko. Das angestrebte zulässige Risiko wird normalerweise erreicht, indem das sicherheitskritische System in Übereinstimmung mit den Anforderungen der Sicherheitsstufe implementiert wird. In manchen Fällen, wenn das angestrebte zulässige Risiko geringer als das SIL4-Risiko ist, können

2 Accident prevention

The most important objective associated with functional safety is accident prevention. But how can we do this? In the railway business, for example, we can provide functionally safe interlocking systems to prevent train collisions. Or we can provide functionally safe process control and protection systems in power plants to prevent explosions. The key requirement is the continuous risk analysis and risk assessment during the planning, development, implementation and operation of any safety critical equipment and applications.
The concept of "functionally safe" is closely related to safety integrity which is achieved by fulfilling the integrity requirements of the specified standards. This means that we can achieve an adequately safe implementation with the required integrity, but 100 % proof of functionally safe implementation unfortunately does not exist. This is something that many do not understand. The highest specified level of safety integrity is SIL4, which still includes a very small amount of residual risk. In order to have an implemented safety function meet a certain specific level of safety integrity, we need to fulfil the systematic integrity and hardware integrity requirements set by the standards, in addition to all the technical requirements. Systematic integrity mainly considers qualitative aspects such as the processes and the used techniques and measures, while hardware integrity also considers the quantitative approach, including any architectural constraints on the specific implementation of the application. At this point, even people who are not too familiar with the concept of functional safety may be able to find a first stop: the value for the probability of a dangerous failure per hour per safety function (PFH) which is the best known SIL requirement. However, there are hundreds of additional requirements to be considered.
When considering the acceptability of the residual risk, the residual risk level needs to be lower than the target tolerable risk. The target tolerable risk is typically achieved by implementing a safety critical system according to the specified safety integrity level requirements. Other risk reduction measures may also be considered necessary in some cases, if the target tolerable risk level is lower than the SIL4 risk level. At the same time, we can also consider whether the process should be changed and the safety function re-designed, if SIL4 integrity is insufficient.

3 The concept of safety

Why do we talk about principles, risk management, standard processes and specific integrity requirements when we are dealing with safety management in railway system SME (small and medium sized enterprises)? The answer is quite obvious. We have to comply with all the specified requirements and follow the processes. There is no excuse or justification for smaller or bigger companies to ignore any requirements pertaining to the safety critical implementation. By specifying processes and applying the required techniques and measures, we can mitigate systematic failures and prevent human errors. As we know, systematic integrity is actually the most important driver behind the origin of the concept of "functional safety" and its evolution.

4 The safety culture

One key topic which defines the framework for safety thinking and integrates all the presented objectives and principles still has to be introduced. "Companies need to create and maintain a safety culture." The safety culture is the main enabler which makes the concept of functional safety meaningful. When considering culture in general, we can easily understand that this cannot be created over

weitere Maßnahmen zur Risikoreduzierung nötig werden. Gleichzeitig kann man auch hinterfragen, ob nicht der Prozess verändert werden sollte und die Sicherheitsfunktionen einer Überarbeitung bedürfen, wenn SIL4 nicht ausreichend ist.

3 Konzept der Sicherheit

Warum reden wir über Prinzipien, Risikomanagement, Standardprozesse und spezifische Integritätsanforderungen, wenn es um das Sicherheitsmanagement in einem KMB (Klein- und Mittelbetrieb), der Eisenbahnsysteme liefert, geht? Die Antwort ist ziemlich offensichtlich. Wir müssen den festgelegten Anforderungen entsprechen und den Prozessen folgen. Es gibt keine Entschuldigung oder Begründung, warum kleine oder große Unternehmen irgendwelche dieser Anforderungen an sicherheitskritische Implementationen ignorieren könnten. Indem man Prozesse spezifiziert und die erforderlichen Techniken und Maßnahmen zur Anwendung bringt, kann man systematische Fehler abmildern und menschlichem Irrtum vorbeugen. Wie wir wissen, ist die systematische Integrität gegenwärtig die wichtigste Triebkraft im Konzept der „funktionalen Sicherheit" und dessen Entwicklung.

4 Sicherheitskultur

Ein Schlüsselthema, das den Rahmen des Sicherheitsdenkens absteckt und alle dargestellten Ziele und Prinzipien integriert, muss jedoch noch eingeführt werden. „Unternehmen müssen eine Sicherheitskultur schaffen und leben." Sicherheitskultur ist der Hauptfaktor, der das Konzept der funktionalen Sicherheit mit Leben erfüllt. Wenn man sich allgemein mit Kultur beschäftigt, so ist klar, dass diese nicht innerhalb einer kurzen Zeitspanne entstehen kann und auch nicht durch einzelne Personen. Sicherheitskultur ist eher wie ein Modell, das aus einer Gruppe von Individuen, die Regeln und Normen durch eigenes Verhalten schaffen, besteht. Es kann eine oder mehrere einflussreiche Personen geben, die die Bedeutung von Sicherheit betonen und fördern können, aber keine derartige Person kann allein eine Sicherheitskultur schaffen oder leben. Die Güte bzw. Stärke der Sicherheitskultur ist nicht leicht zu messen, aber eine Sache ist immer klar, die Sicherheitskultur ist nur so gut wie das schwächste Glied in der Kette. Eine einzelne Person kann eine Sicherheitskultur allein weder erschaffen noch aufrechterhalten, aber eine Einzelperson ist immer verantwortlich, so zu denken und zu handeln, dass hohe Qualität und Sicherheit garantiert werden können. Eine gesunde Sicherheitskultur ist das Ergebnis der Zusammenarbeit einer Gruppe von Personen, die mit ähnlicher Grundhaltung zum Thema Sicherheit auf das Sicherheitsziel hinarbeiten.
Es ist offensichtlich, dass auch die oberen Leitungsebenen in Unternehmen in die Förderung der Sicherheitskultur einzubeziehen sind. Unternehmen, die sicherheitskritische Anwendungen liefern, sind sich im Klaren darüber, dass man mindestens einen Top-Influencer benötigt. Mit der Unterstützung des Top-Managements sind Influencer in der Lage, ihrer wichtigen Rolle bei der Förderung des Sicherheitsdenkens nachzukommen. Mipro hat zum Beispiel ein Programm zur Sicherheitsentwicklung, das als Werkzeug zur Förderung und Verbesserung der Sicherheitskultur dient. Da dies ein interessantes Thema ist, werden wir später in diesem Beitrag noch ausführlich darauf zurückkommen.

5 Angebote und Verkauf

Das Sicherheitsmanagement ist auch Teil des Verkaufsprozesses, was bedeutet, dass die Sicherheitsaspekte bereits in der Angebotsphase berücksichtigt werden müssen und deren Management sich über den gesamten Lieferzeitraum hinzieht. Der Prozess des Sicherheitsmanagements in der Verkaufsphase besteht aus mehreren Faktoren, von de-

a short period of time and by one individual person. Safety culture is rather like a model which consists of a group of individuals who create the rules and norms through their own behaviour. There may be one or more top influencers who can promote and highlight the importance of safety, but none of the individuals can either create or maintain a safety culture on their own. The goodness or strength of a safety culture is not easy to measure, but one thing is always clear; the safety culture is as strong as the weakest link in the chain. A single person cannot create or maintain a safety culture alone, but an individual person is always responsible for thinking and acting so that high levels of quality and safety can be guaranteed. A healthy safety culture is the outcome of a group of individuals working together towards a safety goal with a similar type of safety mind-set.
It is obvious that the highest management level in companies also has to be engaged in the promotion of the safety culture. Companies delivering safety critical applications definitely understand that at least one or more top influencers are needed. Influencers are able to perform their important role of promoting safety thinking when supported by the top management. For example, Mipro has established a safety development program which serves as a tool to improve and promote its safety culture. This interesting topic will be dealt with in more detail later in this article.

5 Bids and sales

The safety management process is also part of the sales process, which means that safety aspects need to be considered and managed starting already from the tender phase and continuing through the complete delivery. The safety management process in the sales phase consists of different factors, each of which has a specific influence on the sales process. The bid team should include members from its technical and commercial teams in order to ensure that safety aspects are appreciated and taken into account from the beginning. Each bid team member may have a different role, but everyone must be able to understand the key aspects of railway and safety systems. The bid team normally works with technical experts who attend to the assigned definitions and guide the other members in order to ensure that the offered system meets the safety requirements.

6 Understanding the safety systems and requirements

Sales of railway systems involve more than just selling systems to infrastructure owners or operators. This includes an understanding of the requirements, the accepted risk levels, the risk assessments, the safety methods, the safety definitions in railway systems and the compliance of railway systems with these factors. It is even more important to understand the aforementioned factors, if the delivery consists of a newly developed product.
The CENELEC railway application standards for communication, signalling and processing systems are typically part of tender materials and the supplier's proposal needs to comply with them. In addition to the formal safety integrity requirements, the supplier also needs to comply with any national and customer specific functional requirements. It is not possible to designate which requirements are more important since all these requirements must be met. Instead, it is understandable that the national and customer specific functional requirements have a far greater influence on the supplier's bid than the safety integrity requirements. These functional requirements may influence what can be offered to the customer and whether the function is already available in the offered system. Understanding the national and customer specific requirements and how they influence the proposed railway system is a key role in the sales phase; it

nen jeder einen spezifischen Einfluss auf den Verkaufsprozess hat. Das Angebotsteam muss auch Mitglieder aus den Bereichen Technik und Kommerzielles haben, um sicherzustellen, dass die Sicherheitsaspekte von Anfang an wahrgenommen und berücksichtigt werden. Jedes Mitglied des Angebotsteams kann eine andere Rolle haben, aber jeder muss in der Lage sein, die Kernpunkte von Eisenbahnsystemen und den Sicherheitssystemen zu verstehen. Das Angebotsteam arbeitet normalerweise mit technischen Experten zusammen, die auf die relevanten Definitionen achten und die übrigen Teammitglieder dabei anleiten, wenn es darum geht, die Sicherheitsanforderungen in dem angebotenen System einzuhalten.

6 Das Verstehen des Sicherheitssystems und der Sicherheitsanforderungen

Der Verkauf von Eisenbahnsystemen ist mehr als nur der Verkauf von Systemen an Eigentümer oder Betreiber von Infrastruktur. Es umfasst das Verständnis der Anforderungen, des akzeptierten Risikoniveaus, der Risikobewertung, der Sicherheitsmethoden, der Definitionen von Sicherheit in Eisenbahnsystemen und der Konformität der Eisenbahnsysteme, um all diesen Anforderungen gerecht zu werden. Die oben genannten Faktoren gewinnen noch an Bedeutung, wenn es sich bei der Lieferung auch um neuentwickelte Produkte handelt.
Die Normen der CENELEC zu Eisenbahnanwendungen für Kommunikation, Signalbetrieb und Datenverarbeitung sind normalerweise Bestandteil der Angebotsunterlagen und das Angebot eines Anbieters muss dazu konform sein. Zusätzlich zu den formellen Anforderungen an die Sicherheitsintegrität muss der Bieter auch den nationalen Bestimmungen und kundenspezifischen Anforderungen genügen. Dabei kann man keine Wertigkeit dieser Anforderungen festlegen, da alle essentiell sind und erfüllt werden müssen. Stattdessen ist es verständlich, dass die nationalen und kundenspezifischen funktionellen Anforderungen mehr Einfluss auf das Angebot haben als die Anforderungen an die Sicherheitsintegrität. Diese funktionellen Anforderungen haben darauf Einfluss, was man dem Kunden anbieten kann und ob in dem angebotenen System die geforderte Funktionalität bereits enthalten ist. Verständnis für die nationalen und kundenspezifischen Anforderungen und dafür, wie gerade diese das vorgeschlagene Eisenbahnsystem beeinflussen, ist ein Schlüsselfaktor in der Verkaufsphase; das erlaubt uns, die technische Sicherheit während der Lieferphase zu managen und die entsprechenden Modifikationen und Anpassungen im Zusammenhang mit den Sicherheitsanforderungen in jedem Land zu finden.

7 Lebenszyklus und Organisation der Sicherheit

In der Verkaufsphase muss der Bieter dem Kunden normalerweise Informationen zum Verfahren der Sicherheitsentwicklung beim Bieter geben sowie zum Lebenszyklusmanagement für Zuverlässigkeit, Verfügbarkeit, Wartbarkeit und Sicherheit (RAMS), indem spezifische Pläne als Evidenz für angemessene Qualität, Sicherheit und Projektmanagement unterbreitet werden. Um Sicherheit über den gesamten Lieferzeitraum zu gewährleisten, muss der Lieferant einen Lebenszyklusmanagementplan vorlegen, um zu demonstrieren, dass das gelieferte System angemessen gemanagt ist, auch nach der Übergabe, während des Betriebs und bei Wartung innerhalb des Lebenszyklus.
Mindestens so wichtig wie angemessene Sicherheit und Lebenszyklusmanagement ist das Kompetenzmanagement des Personals, die an der Entwicklung sicherheitskritischer Anwendungen teilhaben. Es muss sichergestellt werden, dass kompetente Personen für die verschiedenen Aufgaben zur Verfügung stehen und dass die Organisation die Kompetenz hat, alle verschiedenen Aufgaben und Verpflichtungen auszuführen. Daher muss der Lieferant bereits in einer frühen Phase des Angeenables us to manage the technical safety during the delivery phase and to ascertain any corresponding modifications and adjustments required by the safety requirements in each country.

7 The lifecycle and the organisation of safety

During the sales phase, the supplier normally needs to provide the customer with information about the supplier's safety development process and the reliability, availability, maintainability and safety (RAMS) lifecycle management by submitting specific plans as evidence of adequate quality, safety and project management. In order to ensure the safety throughout the entire delivery, the supplier needs to present a lifecycle management plan to demonstrate that the delivered system's safety will also be adequately managed after the commissioning and during the operation and maintenance lifecycle phases.
The competence management of the personnel participating in the development of any safety critical applications is at least as important as proper safety and lifecycle management. It is necessary to ensure that competent individuals will be available for different roles and that the organisation has the competence to implement all the different tasks and duties. Therefore, the supplier needs to name the individuals who will be responsible for the development of the safety aspects at an early stage of the bid phase and to provide CV and other personnel training records as evidence of their adequate professional know-how for the tasks at hand.
The organisation chart should at least name the key people involved in the project, quality and RAMS management, as well as the designers for the system design and implementation. Due to the nature of the functional safety development process, the organisation should also consider verification and validation roles and ensure their necessary independence from the project management and design roles. Testing and commissioning personnel can ensure that technical safety has been achieved and adequate quality has been secured.

8 Competence management and personnel training

The functional safety concept defines different roles for personnel participating in safety critical application development. The standards only define the key competencies at a high level. A typical high level requirement is that the person must be competent in engineering appropriate to the application area. Each company should determine and specify more detailed competence criteria for each role participating in the different development activities. For example, we have defined separate verifier roles in the Mipro hierarchy tree based on the competence and substance needed in various tasks. Competence criteria have been specified for the system verifier, the hardware verifier and the software verifier. The analogy is easily comparable to the designer or implementer roles, since not all people are typically able to perform both hardware and software development. There are also requirements which consider the knowledge regarding functional safety and safety management in general. Each person needs to understand at least the relevant parts of a specific standard or even the entire standard depending on his or her role. This leads to a situation in which all the people participating in any safety critical development activities should understand the same technical language, which means that they have to have mastered safety design principles and terminology at the very minimum.
On the basis of the previous requirements, Mipro launched an internal safety development program a few years ago to improve the functional safety knowledge of its personnel. The safety development program was launched for two reasons: to create a common professional language for Mipro personnel and to promote the safety

bots konkrete Personen benennen, die für die Entwicklung der Sicherheitsaspekte verantwortlich sind, und zu diesen die Lebensläufe und weitere Qualifikationsnachweise zum Nachweis der fachlichen Eignung für die anstehenden Aufgaben beibringen.
Das Organigramm sollte wenigstens die Schlüsselpersonen für das Projekt, die Qualitätssicherung und RAMS-Management benennen sowie die Designer für Systemdesign und Implementierung. Aufgrund der Natur des Entwicklungsprozesses bei der funktionalen Sicherheit sollte die Organisation auch Aufgaben zu Verifizierung und Validierung in Betracht ziehen und für die dafür notwendige Unabhängigkeit dieser Personen vom Projektmanagement und Design sorgen. Durch Prüfen und Zuweisen des geeigneten Personals wird sichergestellt, dass technische Sicherheit erreicht wird und angemessene Qualität gesichert ist.

8 Kompetenzmanagement und Personaltraining

Das Konzept der funktionalen Sicherheit sieht verschiedene Rollen für die Personen, die an der Entwicklung sicherheitskritischer Anwendungen arbeiten, vor. Die Normen definieren die Schlüsselkompetenzen nur auf einem hohen Niveau. Eine typische Anforderung auf hohem Niveau ist, dass die Person kompetent im Ingenieurwesen gemäß dem Anwendungsfeld sein muss. Jedes Unternehmen muss für jede beteiligte Rolle bei den verschiedenen Entwicklungsaufgaben konkretere Kompetenzkriterien definieren und spezifizieren. Wir in der Mipro-Hierarchie haben zum Beispiel verschiedene Prüfrollen definiert auf der Grundlage der Substanz, die für die verschiedenen Aufgaben benötigt wird. Kompetenzkriterien sind für den Systemprüfer, den Hardwareprüfer und den Softwareprüfer festgelegt. Die Analogie ist leicht vergleichbar mit den Rollen des Designers und des Umsetzenden, da typischerweise nicht alle Leute in der Lage sind, sowohl Hardware als auch Software zu entwickeln.
Es gibt zudem Anforderungen, die die Kenntnisse im Zusammenhang mit funktionaler Sicherheit und Sicherheitsmanagement allgemein in Betracht ziehen. In Abhängigkeit von der Rolle muss eine Person bestimmte Teile einer Norm kennen oder sogar die ganze Norm. Das führt zu einer Situation, wo alle Personen, die an einer Aktivität bei einer sicherheitskritischen Entwicklung teilnehmen, dieselbe technische Sprache verstehen sollten, was bedeutet, dass sie die Prinzipien und Terminologie des Sicherheitsdesigns zumindest in den Grundzügen verstehen müssen.
Auf der Basis der eben genannten Anforderungen startete Mipro vor einigen Jahren ein internes Sicherheitsentwicklungsprogramm, um die Kenntnisse zur funktionalen Sicherheit bei der Belegschaft zu verbessern. Das Sicherheitsentwicklungsprogramm war aus zwei Gründen gestartet worden: um eine gemeinsame Fachsprache für die Mipro-Belegschaft zu entwickeln und um die Sicherheitskultur zu befördern. Das Sicherheitsentwicklungsprogramm besteht aus einem Standard-Basistraining, das das Konzept der funktionalen Sicherheit, die grundlegende Terminologie und Prinzipien von Sicherheitsdesign umfasst. Mipro gestaltete sein Programm pragmatischer und entschied, dass Mitarbeiter, die in die Aktivitäten bei sicherheitskritischer Entwicklung involviert sind, eine Prüfung zur Terminologie absolvieren müssen, nachdem sie an den internen Standard-Trainings teilgenommen haben (Bild 2). Nach drei Jahren Erfahrung mit dem Sicherheitsentwicklungsprogramm und den Fachwortschatzprüfungen können wir stolz sagen, dass diese einen gewaltigen Einfluss auf die Kenntnis des Personals zum Sicherheitsmanagement und die Verbesserung der Einstellung zur Sicherheit hatten.
Mipro ist sich dessen bewusst, dass professionelles und kompetentes Personal der wichtigste Schlüssel für hohe Qualität und Sicherheit ist. Als Teil des Sicherheitsentwicklungsprogramms und des Personalkompetenzmanagements bietet Mipro jährlich mindestens zehn Personen die Möglichkeit, an externen Trainings zum Thema funktionale Sicher-

Bild 2: Bei Mipro wird durch das interne Entwicklungsprogramm für Wissen auf dem Gebiet der funktionalen Sicherheit gesorgt.
Fig. 2: The functional safety knowledge of the personnel at Mipro is ensured through the internal safety development program and training completed with a terminology exam.

culture. The safety development program consists of standard-based training which covers the functional safety concept, basic terminology and safety design principles. Mipro has made its program more pragmatic and decided that the personnel participating in any safety critical development activities should pass the terminology exam after they have participated in the internal standard training (fig. 2). After three years' experience of the safety development program and the terminology exams, we can proudly say that this has had a huge impact on the safety management knowledge of our personnel and enhanced their safety mind-set.
Mipro understands that professional and competent personnel are the most important enablers of high quality and safety. As part of its safety development program and personnel competence management, Mipro offers at least ten people a year the opportunity to participate in external functional safety training which leads to the internationally recognised, formal and personal functional safety professional certification. In this way we can manage our personnel competence so that not only senior Mipro employees are able to acquire formal certification, but that our younger professionals also participate in the certification training.

Bild 3: Das Sicherheitsmanagement in KMU unterscheidet sich nicht von den Zielen des Sicherheitsmanagements in großen Unternehmen. Alle Anforderungen, die für sicherheitskritische Anwendungen und deren Implementierung gelten, müssen erfüllt werden.
Fig. 3: Safety management in SME companies does not differ in principle from bigger companies' safety management targets and objectives. All the requirements set for the safety critical application implementation must be met, no matter what the size of the company.

heit teilzunehmen, was zu international anerkannten Zertifikaten im Bereich formelle und persönliche funktionale Sicherheit führt. Auf diese Art und Weise können wir persönliche Kompetenzen managen, sodass nicht nur die leitenden Mitarbeiter bei Mipro formell anerkannte Zertifikate bekommen, sondern auch jüngere Fachleute an diesen Trainings teilnehmen.

9 Entwicklung von Anwendungen und Änderungsmanagement

Aus technischer Sicht ist eine skalierbare Hardwareplattform und eine andere bewertete und zertifizierte Hardwareausstattung, die von Haus aus mit den Anforderungen an Sicherheitsintegrität konform ist, der Schlüssel zum Erfolg. Dadurch wird auch Sicherheitsmanagement in Lieferprojekten ermöglicht. Tatsächlich helfen sie nicht nur in der Entwurfs- und Realisierungsphase, sondern genauso in der Angebots- und Verkaufsphase. Kompetente Leute sind in der Lage, Eisenbahnsysteme auf der Basis dieser zertifizierten Hardwareausrüstung und generischer Anwendungslösungen zu designen. In der Verkaufsphase werden technische Lösungen und Systeme, die dem Kunden angeboten werden sollen, von verschiedenen Teammitgliedern des Angebotsteams verifiziert. Das ist ein Mittel dafür, dass die Konformität mit den Anforderungen der Ausschreibung und mit den Sicherheitsanforderungen, wie sie in der Ausschreibung festgelegt sind, gewährleistet wird.
Die Implementierung einer spezifischen Anwendung basiert üblicherweise auf einer bereits fertig entworfenen, geprüften und zertifizierten generischen Anwendung und generischen Produkten. Auch wenn diese generische Anwendung schon auf nationalen und kundenspezifischen Anforderungen aufbaut, so enthält die aktuelle spezifische Anwendungsimplementierung normalerweise einige Abweichungen in der Funktionalität und aus der Geometrie kann auch die Notwendigkeit entstehen, dass einige Eigenschaften in dem konkreten Fall der konkreten Umgebung angepasst werden müssen. Wenn man die Modifikationen der Funktionalität vom Standpunkt des Sicherheitsmanagements aus betrachtet, so sind die wichtigsten Faktoren das Änderungsmanagement, die Analyse der Auswirkungen und das Verfahren zur Versionskontrolle. Denn es ist wesentlich, dass alle Änderungen angemessen dokumentiert werden und damit die Versionsunterschiede

9 Application development and change management

A scalable hardware platform and other assessed and certified hardware equipment which already comply with the safety integrity requirements are the key to success from a technical point of view. They also facilitate safety management in delivery projects. In fact, they not only help in the design and implementation phase, but also equally in the bid and sales phases. Competent people are able to design railway systems based on certified hardware equipment and generic application solutions. The technical solutions and systems which are to be offered to the customer are verified by different bid team members in the sales phase. This is a means to ensuring that they correspond with the tender requirements and also comply with the safety requirements set out in the bid phase.
The implementation of a specific application is typically based on already designed, assessed and certified generic applications and generic products. Even though the generic application is based on national and customer specific requirements, the actual specific application implementation typically contains some exceptions to functionalities and the geometry may also result in the need to change some features in order to make them applicable in the specific environment. When considering any modifications to functionalities from a safety management point of view, the most important factors are change management, impact analysis and the version control procedure. It is essential that all the changes are properly documented and traceable between the modified versions. The impact analysis should indicate the direct effects which the change brings to the modified functionality and designate the effects on the adjacent interfaces. Once the effects of the change have been found through a proper change management and impact analysis procedure, the change request can be accepted for implementation.

10 So what is the difference?

The title of this article considers safety management in an SME sized company. This may lead the reader to the conclusion that there definitely should be some differences between the safety management

nachvollziehbar sind. Die Analyse der Auswirkungen muss dabei die direkten Wirkungen der Veränderungen aufgrund der Modifizierung der Funktionalität angeben und eventuelle Auswirkungen auf verbundene Komponenten benennen. Nachdem die Auswirkungen der Veränderungen durch angemessenes Änderungsmanagement und die Analyse der Auswirkungen gefunden wurden, kann dem Verlangen zu der Änderung stattgegeben und die Änderung implementiert werden.

10 Nun, was ist der Unterschied?

Der Titel dieses Beitrags bezieht sich auf Sicherheitsmanagement in einem KMU. Das mag vom Leser als Hinweis aufgenommen worden sein, dass es hier doch irgendwelche Unterschiede geben müsste, wenn man die Methoden des Sicherheitsmanagements bei kleineren und größeren Unternehmen betrachtet. Jetzt ist es an der Zeit zusammenzufassen und eine Frage zu stellen: Gibt es wirklich irgendwelche Unterschiede zwischen KMU und großen Unternehmen bei der Betrachtung des Konzeptes von Sicherheit und Sicherheitsmanagement? Ich wage zu behaupten, dass sich das Sicherheitsmanagement in KMU im Prinzip nicht von den Zielen und Aufgaben des Sicherheitsmanagements in großen Unternehmen unterscheidet (Bild 3). Wie bereits oben angemerkt, gibt es keine Entschuldigung oder Begründung, warum kleinere oder größere Unternehmen irgendwelche dieser Anforderungen an sicherheitskritische Implementationen ignorieren könnten. Zumindest aus der Sicht des Managements macht es keinen Unterschied, wie groß das Unternehmen ist. Der auffälligste Unterschied dürfte in der Zahl der Kollegen im Kaffeeraum liegen. ■

methods applied by smaller and larger companies. Now, it is time to conclude and to ask one question: is there actually any difference between SME and larger scale companies, when we consider the concept of safety and safety management? I dare say that safety management in SME does not differ in principle from bigger companies' safety management targets and objectives (fig. 3:). As noted earlier in this article, there is no excuse or justification for smaller or bigger companies to ignore any requirements set for the implementation of a safety critical application. It does not matter how big the company is, at least from the point of view of the management. The most prominent difference can be found in the number of colleagues congregating in the coffee room. ■

LITERATUR | LITERATURE

[1] Risknowlogy, X.: Zertifikationkurs zur funktionalen Sicherheit, Funktionale Sicherheit für Professionale und Ingenieure von sicherheitsbezogenen Systemen, Kursmaterial 2017

AUTOR | AUTHOR

Dipl.-Ing. Juha Turunen
Functional Safety Manager
MIPRO OY
Anschrift / *Address*: Bertel Jungin aukio 1, FI-02600 Espoo
E-Mail: juha.turunen@mipro.fi