Functional Safety system developments from MCU vendor point of view

By Thomas Kellermann, Renesas

This article highlights the importance of Functional Safety for system development, already a complex exercise and becoming even more complex. Component manufacturers will play a decisive role, especially MCU vendors. Application developers will need support for high-end functional safety systems, but they can accelerate development and save engineering costs.

The term Functional Safety has become a topic of great interest. Functional Safety generally means that malfunctions of the operating systems or applications that lead to any kind of threat or even accident have to be avoided. Of course, this basically includes human health and environment, but also material integrity can be of high interest. In other words, functional safety is that part of the overall safety that depends on failure-free operation of a system.

But how can such dangerous events be avoided? For sure, on the one hand it is quite important to minimize the risks. Actually, the risk minimization is only reasonable to a certain extent. Thus, it is fundamental in the field of functional safety to identify and understand potential risks and failure causes of a system. If ideally all potential failure causes are known and the consequences understood it is possible to define usable countermeasures. Thus, failures are detected before a hazardous event occurs and with the needed functional safety reaction the safe state is initiated. The safe states can be quite different depending on the application. A heater can be made safe by simple power-off, a safety barrier might need to be to be closed, a crane might be made safe by freezing the current position, and a motor control unit could need a specific power-down procedure. Just looking at the differences between safe states reveals the variety of functional safety applications. Every application is different and has its own peculiarities and thus potential failure causes and related safe states. This makes a functional safety analysis very complicated and interesting at the same time.

As mentioned at the beginning functional safety is currently one of the major trends in lots of industries. The topic is much more present than some years ago and still rapidly growing. Actually, functional safety should grow up together with the usage of IT in safety-critical applications. In reality it needed some experience and unfortunately also some accidents to lead to the beginning of functional safety in the early eighties. Since then we have had a significant and constant growth of IT and embedded systems that control safety-related applications.

For sure the presence of functional safety in the last few years is quite different for specific areas. In some special sectors, such as process industry, it has already been considered for a long time. Later the automotive area needed functional safety which is established and well known today. For getting embedded systems into our cars more and more functional safety was needed. The situation is similar in every sector where humans are transported by any kind of electric or electronic controlled device, no matter if on water, in the air or on railways. Human lives are reliant on correctly working systems thus functional safety is vital.

Today additional areas are accelerating the growth of overall functional safety devices. One reason is that it is driven by current major trends like Industry 4.0, Internet of Things and Smart Home/Building. A lot of new safety applications arise in these sectors due to increased integration of intelligence. In parallel the existing safety applications get much more complex.

Industry 4.0 moves factories to intelligent and flexible production clusters. Separation and encapsulation of safety-critical workflow steps is continuously being reduced. Man and machine are working side-by-side or even hand-in-hand. Autonomous systems in decentralized real-time production require build-in safety functionality to allow such safe human-machine collaborations to reduce physical safety barriers like safety locks or safety fences. All this leads to an increase in functional safety related applications. Due to the Internet of Things, embedded systems and generally IT are now conquering a wider area of home and building automation. This increases the potential risks of all this additional intelligence.

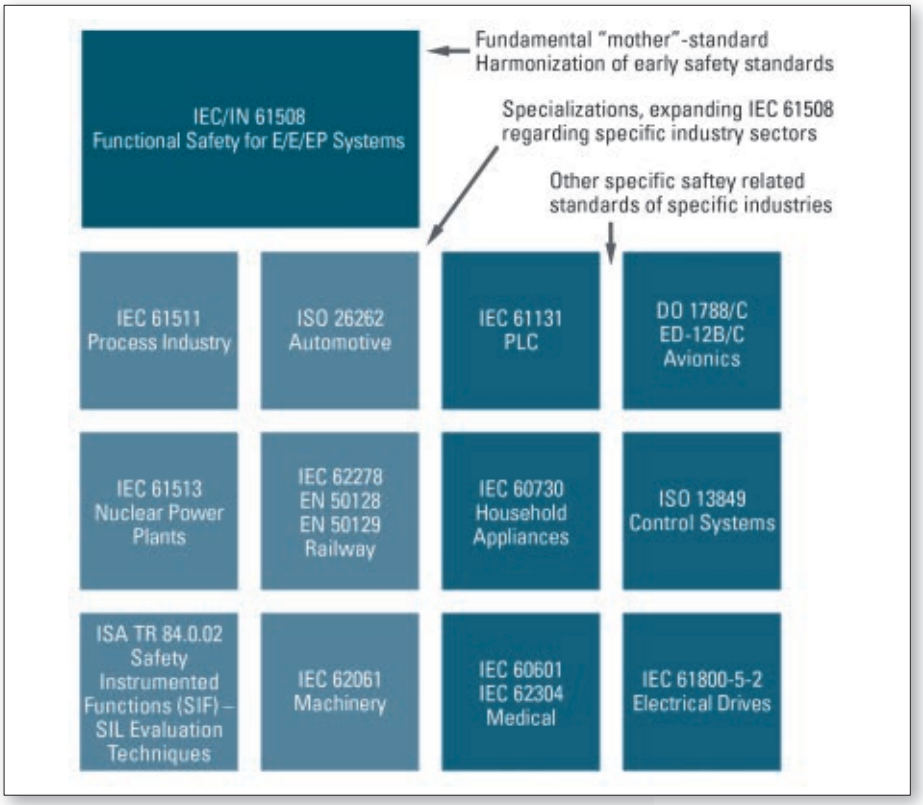

Figure 1. Functional Safety Standards

At first sight there are many standards related to functional safety. These standards have many similarities and differ often only slightly, e.g. in definitions. The most important standard is the IEC/EN 61508. This fundamental Functional Safety standard for E/E/EP (electrical, electronic or programmable electronic) applications harmonized former safety standards. This standard is usually the basis for Functional Safety developments and expanded by additional industry sector specific standards. Some of these additional standards are directly referred as an adaption or expansion of the IEC 61508.

Developing a safety application, especially with embedded systems inside, can be very complex. Historically, a lot of safety critical systems established safety simply by physical separation. In case of a not present separation like an opened access or flap the complete system was also physically separated from electricity. This guarantees a really high safety but can be quite inefficient from the productivity point of view and also expensive.The target of modern safety applications is to combine adequate functional safety with high performance of the system. A safety developer is always confronted with the compromise between functional safety and availability. Usually a higher availability and high performing system increases the complexity and the needed efforts of functional safety considerations. Therefore, a detailed hazard and risk analysis has to be done. The goal is to identify every potential failure, understand the consequences of it, estimate the probabilities of its occurrence, and lastly to identify countermeasures to detect any occurrence of each risk. For a safety analysis of a system all components and their interactions have to be considered. This includes the hardware components, the hardware design and also the application software. Based on this safety analysis countermeasures of all critical failure scenarios can be made.

Additionally, it is very important to get a complete understanding of the timings of a safety critical application. It is mandatory to understand in which time failures could occur and fit the timing of needed countermeasures. Here the so-called Process Safety Time (PST) related to the application has to be evaluated. This is the minimum time in which a failure leads to a hazardous event and for sure the needed countermeasure has to be faster. Looking on the variety of safety applications the PST can be in a lower millisecond range up to even multiple seconds. In a safety analysis the big picture always has to be understood with all its critical and partially high complex components. In modern systems one of the most critical and complicated hardware components are complex ICs and especially microcontrollers (MCUs).

In almost every modern electronic application a kind of MCU is integrated. All the different flavours of MCUs have in common that they usually are the complex heart of the

application. Developing a safety application or system requires special attention to these devices. But how deeply can developers, safety consultants or programmers understand the behaviour of an MCU? Plausibility checks of output data, watchdog usage, test calculation, cyclic notifications, software diversity for checks and much more are widely used safety mechanisms that are integrated to guarantee the correct operation of an MCU. Also, simply redundant MCUs are used performing the same operation; then the output data of both is compared to be equal. This hardware redundancy reduces the risk of a failure drastically without understanding the detailed MCU operation. In the end these are all quite good safety mechanisms. But unfortunately, from a safety analysis point of view this might be not sufficient. To develop a high-quality safety system a deeper understanding is mandatory to get realistic values of failure rates and safe failures. This is not only important to develop a hard deterministic safety application. Furthermore, it is mandatory regarding the different safety standards. For a safety qualification and classification real figures and values are needed as proof.

Detailed knowledge of the hardware is mandatory to develop a complex high performing safety application. This is even more true for complex devices like MCUs, where developers and external experts have a very limited insight. This is the moment when the MCU vendor needs to come into play. Optimally, a silicon vendor can provide FIT (Failure in Time) rates for the function blocks of the MCU. The silicon vendor therefore has to do a detailed MCU hardware safety analysis. This costs money and time but gives the customer – the final application developer – the best basis to make a solid failure probability calculation. Alternatively, the MCU vendor can also provide raw data e.g. chip area of function blocks. With this data and usage of common used formulas from standards (e.g. from IEC62380, SN 29500) FIT values can be estimated.

In addition to the theoretical values, a big MCU vendor can also record field data. A detailed analysis of faulty devices which are returned from the field can give additional information regarding permanent failures. At this point it should be noted that modern MCUs rarely show random damages apart from those caused by wrong operation conditions. Beside the supplying this safety related data, the MCU vendor may also offer solutions that support the final safety application development. This can be self-test software as for example is the case for the Renesas Safety Solution. This Safety Solution Package supports devices from Renesas RX MCU series. This self-test software which tests the CPU, RAM, and ROM could also be developed by an external software developer. Key is that the MCU manufacturer owns the design data, and therefore the coverage of the self-test software can be measured. By inserting discrete logical failures to the real MCU netlist and proofing the software detection of these logical failures the absolute coverage of a self-test software can be determined. This is not possible without the extensive chip design information. External core self-test software developments similar to the early versions of the Renesas self-test software do normally not reach a sufficient diagnostic coverage. During the development of the Renesas core self-test software, multiple test and improvement runs are therefore done to reach the target of more than 90% fault coverage. Such proven results help not only safety application development, they make the final certification process easier. This example shows on the one hand that a lot of effort is necessary to develop a highly efficient Functional Safety software especially self-test software. On the other hand it points out how important the support of an MCU manufacturer can be.

As said in the beginning, safety system development is very complex exercise, and in the future applications will become even more complex. Therefore, it will be very important to build up an application piece by piece with prepared Functional Safety considering hard- and software modules. Ideally the parts come with a certification. Though every application is different the usage of modular safety components, hard- as well as software, is a less extensive workload for safety developers. In the future, component manufacturers will play a decisive role especially MCU vendors. Application developers will need support to get high-end functional safety systems. Additionally, they can accelerate the development and save a lot of engineering costs. ■