White Paper

HIMA – 50 Years of Safety Certification

(Brühl, November 2020)

In 1970, HIMA launched the world's first TÜV certified safety controller. This means that the safety company and TÜV Rheinland have already been working together for 50 years maintaining an excellent cooperation - both in terms of communication within committees and certification of safety controllers. Alongside TÜV Rheinland, HIMA also plays a decisive role as a standards driving force when it comes to safety and security. The major challenges for the future are here cyber security and technological development. Looking back over the past 50 years, we may wonder: "How have challenges evolved over time? Which aspects had to be considered in the past compared to today?" In this paper, experts from TÜV Rheinland and HIMA report impressively on their long-standing partnership.

Functional safety has a high status in Germany, and this is no coincidence. With their collaboration, HIMA and TÜV Rheinland have significantly contributed to achieving this result. Functional safety systems protect people, plants and the environment within the process industry, and just about every industrial environment. Safety controllers, for example, cause systems to enter a safe state if suddenly dangerous situations occur. This is particularly important when people cannot respond quickly enough or other safety measures do not work. Functional safety aims at preventing accidents or undesirable, costly system downtimes. After all, a lot is at stake: the employees' health, the company's physical assets and the environment.

In Germany, functional safety is practiced at a very high level and "is considered exemplary around the worldwide," says Merlin Hilger from TÜV Rheinland. The standard-compliant protection of people, plants and the environment is a priority for German enterprises. IEC 61508, the basic standard for safety-related systems, has now been in force for around 20 years and applies to all safety-related systems (electrical, electronic and programmable electronic devices) across all industries - whether in process industry, burner, marine, or

railway applications. “It prescribes a very high level of safety” states Hilger. Further enhancements to this basic standard have been achieved with the last amendments 10 years ago. Boris Betz from HIMA shares this view: “In Germany, we operate at a very high level in terms of functional safety. However, there is no upper limit, and it is also a challenge to keep standard-compliant products on the market for a long time. In development, we have to observe about 150 standards altogether.”

Hilger explains that, as a result, people in Germany can rely on safety in their workplaces, and it is unsurprising that countries with less advanced functional safety levels are recognizing these advantages and will now follow suit in a significant manner. Former TÜV officer Heinz Gall adds that the perception of risk is also a key concern, noting that “personal safety is certainly a top priority in Germany”.

TÜV experts such as Heinz Gall, Jana Klaes and Merlin Hilger emphasize that fortunately, in their careers to date, no serious accidents or catastrophes have occurred that might have acted as additional drivers for standardization in functional safety. Things can be quite different, however, as the disaster of the Piper Alpha oil platform in 1988 clearly demonstrates. In response to this major incident, in which 167 people lost their lives, Health, Safety and Environment (HSE) management systems were developed to prevent these catastrophes from occurring in the future. According to Jana Klaes from TÜV Rheinland, the fact that functional safety is so important in Germany has a lot to do with the corporate sense of responsibility, which goes beyond the safety and protection of industrial plants. “Nor does anyone want to hit the headlines when people or the environment are harmed”, so the TÜV expert.

Cooperation between HIMA and TÜV Rheinland - then and now

The cooperation between HIMA and TÜV Rheinland is a proven success story. In order to conduct tests, TÜV Rheinland is accredited by the German accreditation body. The procedures and processes required to perform certification testing are strictly regulated. “This also covers the documentation of the various test steps. In this respect, far more regulations apply today than in the past”, says Hilger.

At HIMA, TÜV Rheinland is mainly involved in change testing, which are conducted during further developments and maintenance of proven safety controllers. Tests within the scope of product maintenance usually require much less time than testing of completely new product developments. “That said, also the time required for product maintenance testing always depends on which type of change has been performed”, so Hilger.

Boris Betz from HIMA adds that because HIMA's safety controllers have extremely long product lifetimes, modernization and mandatory recertifications are recurring issues related to product maintenance. This includes, of course, submission of all relevant documentation. In the past, this was done by sending manageable quantities of paper documents by mail. Today, data transfer at HIMA is completely digital – but there are also considerably differences in the amount of data. When recertifying existing HIMA solutions, only few megabytes of data need to be transferred to inspection bodies such as TÜV Rheinland. In contrast, new developments and in particular software components involve extremely high data volumes. 20 to 30 gigabytes of documentation and data are achieved very quickly.

With tools and processors becoming ever more powerful, one would think that the overall processes may be accelerated as well. Hilger points out that although the idea that better tools mean less effort seems rather obvious, the reality is different. “The reason is the increasing complexity, which may also result in higher personnel, coordination and time efforts required for new products. In the past, teams were often smaller than today. Back then, just a few people were involved in testing. In today’s (online) meetings, far more specialists must be consulted on the customer’s side”, notes Hilger. The proportion of service functions that are not developed in-house by the manufacturer, but outsourced to external partners, is on the rise. This also leads to higher testing and personnel costs.

The TÜV Rheinland performs test and certifications for both new product developments and recertification of existing safety controllers. The solid relationship that TÜV Rheinland and HIMA have maintained over the last five decades has built up an important fundamental trust that benefits the professional work of the experts on both sides. “Based on our long-lasting cooperation, we know how work is done at HIMA," remarks Jana Klaes. This can be seen, for example, in the document review that TÜV Rheinland performs at HIMA. Thanks to the accurate and diligent work at HIMA, deviations from the standard are seldom. Gall also recalls the excellent cooperation between HIMA and TÜV Rheinland in the past certification work.

For new products, TÜV Rheinland is already involved in the concept phase. As the focus of functional safety is on failure avoidance, it is important to address any potential faults or errors that may occur at the beginning of the product’s development. TÜV Rheinland covers this aspect during the concept inspection phase, where the TÜV provides the manufacturer with their assessment of the measures implemented to avoid and control failures: Are the planned safety measures appropriate for this type of project? Another factor is the complexity of the product, which determines when TÜV Rheinland will be involved again by the manufacturer. For example, a safety controller has a significantly longer development

time than a safety sensor. The duration of an overall test can take three months to several years, whereby the specialists from TÜV Rheinland usually guide their customers from start to completion. Towards the end, "paper-based" work increases sharply: At this point, test reports, design specifications and other documents are first analyzed and checked to see whether planning and implementation comply with the applicable standards.

Together with the customer, TÜV Rheinland then performs so-called fault injection tests with respect to functional safety, which may take several days. The tests are intended to verify the failure avoidance measures planned during the concept phase by intentionally induced faults. In this respect, for example, a safety controller is expected to respond safely and standard-compliant during the fault injection tests.

On the side of HIMA, Boris Betz has been involved in the certification process with TÜV Rheinland since 2014 and emphasizes the excellent cooperation with the inspection body during the development phase. “On both sides, we have a good feeling on as to when we should start working together on an upcoming certification or recertification”. An immense advantage is that HIMA has a fixed core group of contact persons at TÜV Rheinland, which makes many things easier: “The TÜV experts are always excellent in the subject field, and if something is to be clarified, it is usually solved directly, quickly and efficiently”.

In his current position, Merlin Hilger is enjoying a “very positive, constructive and professional teamwork with HIMA in a wide spectrum of areas”. These include the planning and implementation of joint training courses, change testing for existing HIMA solutions or testing of new, smart safety solutions that complement the current HIMA portfolio. TÜV Rheinland also certifies the functional safety management system at HIMA.

“New product developments such as HIQuad X or the HIMax are likely to take five to eight years at HIMA,” Betz explains. For HIMA as a manufacturer, involving TÜV Rheinland as a notified body for new product developments from the very beginning also means to minimize the economic risk potential. “Irrespective of the experience gained, it makes no sense to simply build something new, if there are significant concerns with respect to the Machinery Directive. This is why a regular exchange with the TÜV during the development process is of utmost importance for us”. Of course, there are always last-minute questions from the testers immediately before certification - but everything is done in a positive and constructive manner, remarks Betz. The high level of competence of all the HIMA experts involved not only contributes to the high quality and high level of co-operation, but it also makes sure there is the required level of fun at work, explains Hilger. “Certifications are always the result of a tremendous amount of work that a whole team of HIMA employees has accomplished over long periods of time”, concludes Betz.

In the beginning there was the single fault consideration

Today's high level of functional safety was preceded by decades of development efforts on the standards applicable today. From the 1970s to the 1980s, work was mainly done with low-complexity and at the same time hard-wired technology, which was certified by TÜV Rheinland. At that time, various techniques based on a deterministic approach existed and there were no classifications regarding safety classes or safety integrity levels (SIL). Accordingly, no risk assessments were performed, but just calculations of failures and failure rates, and not in terms of failure probability, explains Gall. Starting in the 1980s, the focus shifted first to programmable technology and then increasingly to microcomputers.

“The deterministic approach used in the past relied on single fault analysis, which is no longer an option today,” says Gall. “We could look at individual parts and components and determine what would happen if a failure were to occur there.” This FMEA (Failure Mode and Effects Analysis) was always performed at component level. The question was: What would be the response to this single fault in the output signal? The standards to be observed were application-specific: Is the component still safe with respect to the application? Gall recalls: “If the application was still safe despite the fault, we add another fault - up to three faults in combination were considered”.

The application could be anything, from presses to elevators, i.e., any kind of machine. To ensure that the technology was functioning safely, the primary concern was always to analyze the failure and contain the faults by implementing the measures described in the standards. Dynamic systems came then into use in the 1980s: “Everything seems to be fine as long as a dynamic signal was sent from a unit under consideration”, says Gall. “The circuits were designed such that faults in individual components caused all dynamics to be lost. This allowed us to determine whether the application was still operating safely - or not.”

Microcomputers eventually changed many things. In 1984 a research project dealing with microcomputers in safety technology was published by TÜV Rheinland and TÜV Bayern. For the first time, five safety classes were defined in the standards applicable at the time and failure counting was used in the approach. These safety classes, however, cannot be compared with today's SILs. “We looked at fault models in integrated circuits and also discussed potential redundancies and diagnostic measures, e.g., for CPU, RAM and ROM,” explains Gall retrospectively. “The guide, though, did not yet address the probability of failure and risk considerations. Instead, the attention was directed for the first time to programmable technology in the context of safety-relevant applications”.

In mid 1980s, after the guide's publication, standardization activities in Germany began to intensify significantly. "In the DIN standards, hazards and risk classes were defined - whereby the probabilities were still missing," recalls Gall. Individual standards in the field of combustion technology, for instance, described the use of programmable technology. "Finally, the two German standards DIN V 19250 and DIN V VDE 0801 for safety with computer technology were published at the end of the 1980s."

If we have a look at the German pre-standard DIN V 19250, we can see that requirement classes (RC) were used at that time, which correspond to today's SIL levels defined in IEC 61508 or IEC 61511. The IEC standards were published in the early 1990s and adopted essential parts of the German standards. "They now also included the probability of failure and methods for risk reduction," explains Gall. "The necessary risk reduction was determined based on the calculated extent and likelihood of failures and was then described by the SILs," continues Gall.

"If risks were to be reduced, we had to implement measures intended to contain and avoid spurious and systematic faults - and that already during a product's or solution's development. The objective was now to design faultless systems", says Gall. By applying appropriate diagnostic procedures, we were then able to determine the probability of failure. These concepts were basically defined in IEC 61508, which, together with IEC 61511, served as the basic functional safety standard for a wide range of application standards.

Another important point is the development of a structured safety management system. Again, there were initially neither standards nor any official procedure to which users or manufacturers had to conform. Gall looks back: "Of course, there were quality assurance measures in every company, but these depended more on the people than on the system. No structured safety management like the one we have today – which is followed throughout the company and all employees working in development can refer to – existed back then."

Over the decades, the mindset has changed: "The deterministic approach, which considers single faults in components, moved to the analysis of the probability of failure and risk reduction in highly complex systems," says Gall summarizing the development. "The complexity that exists today makes it impossible to test with the same methods of the past, just more extensively. That has simply become too expensive."

HIMA and TÜV Rheinland - crucial contributors to the world of standards

The standards were discussed and jointly developed by the parties participating in the standardization committees. As of 1984/85, Heinz Gall was active in the committee explicitly dealing with functional safety with one or two HIMA representatives. Each party offered their own perspectives and expertise: TÜV Rheinland the viewpoint of the inspection body and HIMA the expertise as a manufacturer of safety controllers. Gall explains: “The committees were staffed by representatives of the various TÜV units as well as experts from the industry, associations, institutes of the professional bodies and academic institutions. The standardization committees have always maintained a sound, close and interactive cooperation with HIMA's experts over the decades”, recalls Gall. From the point of view of HIMA's testing specialist Betz, it is also essential that manufacturers introduce and discuss the industry's insights to the standardization committees. “Particularly when standards are being drafted, these are indeed very dynamic processes involving a great deal of discussion and coordination,” says Betz.

A good historical example of the successful interactive partnership is the development of standards for furnaces such as the VDE 0116, which was early on dealing with computer technology and has meanwhile become DIN EN 50156. The relationship between TÜV Rheinland and HIMA also continued with IEC 61508 and IEC 61511. “In particular, with the three standards - VDE 0116 for furnaces, IEC 61508 as the basic functional safety standard and IEC 61511 for the process industry on the user side - I have been working in person with HIMA engineers for years,” concludes Gall.

In Europe, the EU defines the directives that eventually result in the standards. “Safety in Europe must always be based on the state-of-the-art,” says Gall. According to Hilger, the standards committees must seek a reasonable balance in order to establish a framework, especially for basic standards such as IEC 61508, which is not only currently valid, but will remain so for years to come. Here, too, the rapidly developing technologies are the reason why the standards could not keep pace with them. Hilger explains: “This is also why standards such as IEC 61508 do not go into technical details, but rather describe procedures from which one can also derive how to deal with new technologies.” A good example of this is multicore technology in processors to which the procedures of the standard are applicable and therefore have to be used. Multicore processors are extremely powerful because their cores run in parallel. In addition to the increased performance, this also results in new fault patterns that a processor with only one core does not have. “As functional safety is about controlling failures, the fault patterns of multicore processors are a

challenge," explains Hilger. "Here it is necessary to adapt the standards to the reality of the new fault patterns".

"We already feel that the number of standards to be taken into account in a test is increasing, but this is not necessarily due to the legal requirements or the standards themselves. Rather, it is due to the pace of technological development. One product should cover as many markets and applications as possible. In the case of HIMA, its controllers are not only suitable for the process industry, but also for other areas, such as railway applications, machine safety and the offshore industry," explains Hilger.

For Betz, the standards have increased both in terms of quality and quantity: "When HIMA started to certify its safety controllers, there were nothing more than a few standards. Today, everything is defined and documented in much more detail. From HIMA's point of view, the standards must be adapted to keep pace with technological developments". "Ideally, the standards should reflect the actual technological conditions. This is one of HIMA's concerns as a manufacturer, and that's why we see our role here as a standards driving force. Standardization and the further development of standards are dialogical processes, which is why the parties involved should present a good argumentation and substantiation beforehand to have a chance of success in the ensuing standards discussion."

Due to the variable fields of application of modern products, they must also comply with a growing number of standards. "This increase in standards is therefore also manufacturer-driven", concludes Hilger. Different standards are used for these different areas, but all of them are based on the same basic standard. "Here the standardization committees have contributed their thoughts, so that we are still able to cope with this at all," Hilger says.

The challenges of technology development and cyber security

From a technological perspective, a lot has changed over the decades. "In the past, technology was completely hard-wired, partly based on relays. Software that can be found everywhere today was hardly available," explains Betz. "The individual processors are smaller and also much more powerful than before. However, the modern safety controllers as a whole have not become smaller, which is mainly due to the increased complexity. This must be mapped in both the software and the hardware."

The safety controllers cover more applications and functions. As a result, functional safety is facing growing challenges as well.

Whereas the concepts of functional safety, i.e., fault avoidance, have hardly changed, the extremely rapid technological development is the major challenge of today. “Technology is clearly driving the standards,” says Gall. His colleague Hilger cites again multicore processors as an example. The technology is already available and ready for the market, therefore companies want to use it. However, when standards such as IEC 61508 were last updated, multicore processors did not play a significant role in safety technology and were therefore not addressed by the standard.

“Manufacturers, who had been dealing with functional safety for many years, have their diagnostics and solutions very easily under control”, says Klaes. “We can quantitatively determine how high the likelihood is that a safety function on demand will not operate as intended by the user”. Although everything is “under control” within the solution, or calculate failure probabilities well, cyber security actually acts as a game changer. Cyber security only came into play through networking. In the past, it was only about pure failure avoidance (FMEA). Attacks from outside and the manipulation of a system were - if at all - only possible if the attacker had direct physical access, e.g., to the control cabinets or hard wiring. “This direct attack via the hardware is no use today, as attackers can now choose the path via the network,” says Gall.

For Gall, the increased communication and also the network capability of the systems are the most crucial reason to become very active, in terms of cyber security as well. “Under whatever circumstances, we shouldn’t make things more complex than required. Just because we still have to keep track of everything ourselves. The same also applies to functional safety,” remarks Gall. “Proper structures are important to get an overview and evaluate the overall system. However, if the structures are not designed properly, the complexity and difficulties of keeping an overview and meeting the required safety level increase unnecessarily. Also, we should not rely too much on internal diagnostics and testing”.

The basic requirements for safe operation have not changed, says Gall. At the same time, the challenges posed by the increased complexity have grown significantly over time. The use of more software also results in higher fault potential – “Safety is clearly turning towards software,” concludes Gall. Edition 2 of the IEC 61508 standard is the logical response to this. The systems design is ever more flexible and modular, and HIMA’s Smart Safety Platform provides a good example of this development. Software is gaining in importance compared to hardware, which also means avoiding obsolescence: “Safety is shifting towards software and this is attributable to the higher dynamics,” says Betz.

For Gall as well, software plays a very important role in preventing failures. “In software, you must consider systematic rather than random faults. This means that you really need to work hard to avoid faults and reduce risks, and, consequently, to focus on a clear structure and architecture,” concludes Gall.

For Betz, too, cyber security used to be a purely physical access control. Today, cyber security is a layered overall concept with a systematic threat analysis, in which factors such as social engineering also play an important role. “In cyber security, the systematic threat analysis represents what FMEA stands for in safety,” says Betz. Risk assessment is fundamental here, but can be performed applying systematic approaches that lead to a sound overall concept. A good example is the use of the STRIDE approach (**s**poofing, **t**ampering, **r**epudiation, **i**nformation disclosure; privacy breach or data leak, **d**enial of service, **e**levation of privilege). “In this respect, the responsibility is in the hands of the users. They must think about what must happen for a certain attack scenario to occur. As a manufacturer, we can suggest the use of suitable solutions in the overall concept,” recaps Betz. In some cases, reliable hard-wired solutions such the Planar systems offered by HIMA may be suitable options to counter the threat of cyber attacks. According to Betz, hard wiring remains crucial at neuralgic points and retains its importance, e.g., for use in critical infrastructures. “The hard-wired controllers employed here are not upgraded as regards networking; they have very clear tasks and, with this in mind, they are kept as simple as possible,” says Betz.

External attacks on safety functions with the potential of compromising them creates new challenges for all parties involved - manufacturers and operators the like. Years ago, no one would have expected that someone would deliberately manipulate the safety functions. Similarly, networking has also increased dramatically to offer users more options, such as access from home. According to Klaes, the manufacturers would have been happy to meet these requests for their industrial customers, but this would also have created many points of attack for potential cyber attacks. From Klaes' standpoint, the biggest challenge at the moment is to think about functional safety in terms of cyber security: “Consequently, great efforts have been made recently to make safety solutions not only 'safe' but also 'secure' at the same time”.

The lifecycles of functional safety systems are completely different from those of cyber security systems, where ongoing security updates are necessary to provide the best possible protection. The lifecycle of cyber security is very short compared to that of functional safety and is characterized by continuous modifications.

It is therefore vital to include, right from the start, cyber security aspects in the development of functional safety systems. The segregation of layers should also be built in to ensure that a small change to Security cannot affect Safety. These challenges must be aligned within the industry.

During Hilger's time at TÜV Rheinland, no certified product was ever involved in an accident that fell within the scope of safety. The situation is completely different with cyber security. Latest since active cyber attacks like Stuxnet, potential hazards are taken very seriously by manufacturers of safety controls. As a consequence, cyber security has become an important area of activity for TÜV Rheinland as a certification body due to the rising threat level. “If you as a user detect a cyber security risk, you must observe the standard. Ultimately, the initiative is up to you,” says Hilger. “If networking is in place and functional safety could be threatened by cyber attacks, then the situation must be considered according to IEC 61508,” adds Gall. “The IEC 61508 standard includes a further reference to cyber security standards such as IEC 62443.”

Networking is becoming more and more important today, as customers need it for communication and increased productivity. Good examples are the demands for decentralization, more remote maintenance or effective remote controls in industry. To accommodate these customer needs, HIMA is currently working on an API for its programming tool SILworX. SILworX API will enable customers to automate their processes remotely and platform-independently. Also the HIMA Smart Safety Platform meets the market's requirements. Tools such as HIMA's programming tool are gaining in value - both for the internal development environment and for the subsequent user operation. Tools must be qualified accordingly. Since they are based on software, particular attention must be placed on cyber security.

After strategic attacks such as those by Stuxnet, HIMA tests all existing products for vulnerability to cyber attacks and protects them accordingly. Threats are taken very seriously: “So far, we can prove that no HIMA safety controllers have ever been corrupted by attacks - and we are working hard to ensure that this remains the case. However, it is unserious to claim that there can ever be an absolutely safe control system,” says Betz. “In the end, it always depends on the efforts attackers intend to invest. States dispose of completely different resources than 'script kiddies' or small groups of cyber criminals.”

“Over the past five years, cyber security has clearly moved into focus - for a good reason,” says Klaes. IEC 61508 already referred to IEC 62443 ten years ago. Threat and vulnerability analysis are examples of these references. Unquestionably, the strong networking has significantly increased the foreseeable risk of cyber attacks, and the

IEC 62443 standard is also used far more than before in the functional safety context. IEC 62443-4-1 concerning management processes and lifecycle and IEC 62443-4-2 concerning technical requirements has been available since 2018 and 2019, respectively. For components such as control systems, Part 4 of IEC 62443 (published in 2019) is relevant. According to Klaes, this shows how seriously cyber security has been assessed by the relevant standards committees.

“There is a clear trend in the market that many companies and providers are addressing cyber security to make their solutions 'secure'. In view of the real threats, a completely new market is emerging here, to which manufacturers of security solutions are responding,” Klaes notes. Betz shares this view and emphasizes: “IEC 62443-4-1 and IEC 62443-4-2 are of the utmost importance to us as a manufacturer in terms of cyber security when it comes to product maintenance and new product development. Especially Part 4-1 is important in this context: security must be considered from the very beginning.”

Further future challenges

The Covid-19 crisis hardly impacts the work of TÜV Rheinland. This is because manufacturers can digitally provide all the documents that have to be reviewed for the audit and compared with the standards. In the past, the documents to be reviewed were sent by mail. Today, everything is available digitally and is previously generated with the aid of tools. Only activities where the meeting of people is absolutely necessary are affected by the current crisis.

Face-to-face calls to customers are easier, in particular, for product maintenance testing, than for the more extensive testing of brand new products. Many tests, especially those performed internally by manufacturers such as HIMA, are being increasingly automated. Scripts and automated test environments in test fields have been used for years. As a result, test reports are no longer handwritten as in the past, but are now generated entirely by one tool.

The test procedures are fixed and until a few years ago everything was checked by hand, remembers Betz. “These were tedious procedures involving many people.” Almost half of the development time is spent on proofs, inspections, tests and verifications. A few years ago, HIMA started to automate as many of the test functionalities as possible in order to optimize them. Thanks to automation, what used to take half a year or more can now be done in a few weeks, sometimes even days, saving several man-years of time during development. Compared to the past, the time required for testing can be maintained

constant, which Betz considers as a good success: “The additional complexity simply means that much more effort is required.”

Digitization at HIMA is already progressing apace, which, in the current Covid-19 crisis, is very helpful for the test procedures. The existing infrastructure enables HIMA experts to run tests from home, i.e., remotely, such that they only need to be on site personally for a few tests. As for TÜV Rheinland, it has not yet been clarified whether the physical presence of a TÜV employee is mandatory for fault injection testing. Typically, TÜV experts should be physically on site for some tests, but not for others, i.e., they only need to be personally on site for some tests.

When it comes to proving the safety functions, i.e., to demonstrating a successful shutdown, there is the so-called “witness testing”, where witnesses from the test institute were required to be present on site. “Recently we implemented something completely new along these lines: With the help of a very good camera and a secure video conferencing tool, we have been able to successfully implement witness testing remotely. The inspector was thus also able to join virtually, and that was sufficient in terms of recertification as part of product maintenance,” says Betz. “We are confident that we can also use these remote tests for other certifications. The digitization boost provided by Covid-19 is clearly visible here and opens up new opportunities for us: using video transmissions, witness tests can simply be performed much more efficiently and directly than in the past.

“It certainly would be worthwhile to be able to perform even more tests digitally,” remarks Hilger. As for fault injection tests, there is no decision yet whether the TÜV will continue to perform them remotely in the future. The progress in VR technology creates new opportunities as well. However, the law should first define the framework conditions: Is a test using VR technology even legally permitted? The crux of the matter: is an inspection even possible without physical presence, regardless of whether the law (or the accrediting body) would allow it? How can one ensure that the test results are determined properly? The law notwithstanding, it still comes down to the judgement of the assessor and his expertise.

Conclusion

Thanks to their outstanding cooperation in standardization committees, HIMA and TÜV Rheinland have acted as a driving force and contributed significantly to ensuring that functional safety in Germany is state-of-the-art. Milestones were the German pre-standard DIN V 19250, interim endpoint standards such as IEC 61508, IEC 61511 and IEC 62443. Today’s standards have increased both in terms of quality and quantity, which also impacts

the audits and certification procedures that TÜV Rheinland performs for companies like HIMA. The approach to testing has changed dramatically over the decades: Instead of a deterministic approach of single fault consideration for components, the focus is now on the analysis of highly complex systems in terms of failure probability and risk reduction. The primary challenges on this ongoing journey are posed by the continuous technological progress, which standards can hardly cope with, new threats through cyber attacks and the current Covid-19 situation. Remote testing and automation are in use and radically change the day-to-day work of all parties involved.

(approx. 5.695 words, 36.411 characters)

About the authors

Jana Klaes

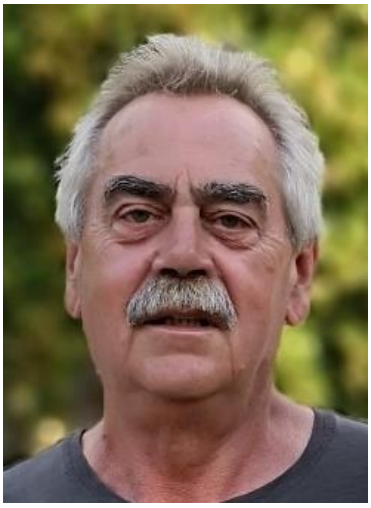
Jana Klaes is electrical engineer at TÜV Rheinland Industrie Service GmbH (specialist area: Cyber Security). She has been working as an assessor at TÜV Rheinland for functional safety for two years. In cooperation with HIMA, she is responsible for cyber security and functional safety.

Picture © TÜV Rheinland Industrie Service GmbH

Merlin Hilger

Merlin Hilger is Expert for functional safety at TÜV Rheinland Industrie Service GmbH (specialist area: functional safety). He has been with TÜV Rheinland for four years and cooperates with HIMA in the areas of training, change management and testing of new products.

Picture © TÜV Rheinland Industrie Service GmbH



Heinz Gall

From the 1980s onward, Heinz Gall was employed by TÜV Rheinland as an expert for functional safety and cyber security. He retired in 2019.

Picture © Private

Boris Betz, HIMA Paul Hildebrandt GmbH

Boris Betz has been working for HIMA since 2013 and is manager for software testing, systems and certifications.

Picture © HIMA Group

About HIMA

The HIMA Group is the world's leading independent provider of smart safety solutions for industrial applications. With more than 40,000 installed TÜV-certified safety systems worldwide, HIMA qualifies as the technology leader in this sector. Its expert engineers develop customized solutions that help increase safety, cyber security and profitability of plants and factories in the digital age. For over 50 years, HIMA has been a trusted partner to the world's largest oil, gas, chemical, and energy-producing companies. These rely on HIMA solutions, services and consultancy for uninterrupted plant operation and protection of assets, people and the environment. HIMA's offering includes smart safety solutions that help increase safety and uptime by turning data into business-relevant information. HIMA also provides comprehensive solutions for the efficient control and monitoring of turbomachinery (TMC), burners and boilers (BMC) and pipelines (PMC). In the global rail industry, HIMA's CENELEC-certified SIL4 COTS safety controllers are leading the way to increased safety, security and profitability. Founded in 1908, the family-owned company operates from over 50 locations worldwide with its headquarters in Bruehl, Germany. With a workforce of approximately 800 employees, HIMA generated a turnover of approximately €123 million in 2018. For more information, please visit: www.hima.com

Editorial contact / specimen copies Please send to:

Mark Herten, Publitek
P.O. Box 12 55, 21232 Buchholz, Germany
Phone: +49 (0)4181 968 09820
Cell: +49 (0)1520 748 3901
E-mail: mark.herten@publitek.com

Carsten Otte, Publitek
Phone: +49 (0)4181 9680 09880
Cell: +49 (0)1520 915 8629
E-mail: carsten.otte@publitek.com

Press contact, HIMA Headquarters
HIMA Paul Hildebrandt GmbH
Daniel Plaga
Group Manager Global PR

Albert-Bassermann-Straße 28
68782 Brühl, Germany
Phone: +49 6202 / 709-405
Fax: +49 6202 / 709-123
E-mail: d.plaga@hima.com

www.hima.com