Digitalization in fire protection

Sebastian Brose, Bettina Bormann
VdS Schadenverhütung, Cologne, Germany

Abstract

A noticeable trend in today’s product development is the close convergence of mechanics, electronics and the Internet. This means that the Internet of Things is spreading to almost all areas of life. Even in modern safety technology, more and more products are interconnected – with all the advantages and disadvantages.

Digitalization offers enormous potential to simplify our lives in many ways. In the business environment, this often refers to the acceleration and optimization of processes through automation or virtualization, for example. Our decisions for action are also becoming increasingly well-founded and logical through the collection and evaluation of digital data. In summary, digitalization makes us faster and smarter – but it does not automatically make us safer. In addition to all its advantages, the strong interconnection of more and more components also opens up new, far-reaching potential hazards. Digitalized processes, systems and products offer a broad attack surface for hackers who can gain unauthorized access. The risks of disruption and failure are also significantly increased.

Keywords: IoT, digitalization, Cyber Security, remote services, risk management

Changing conditions for product development in the safety industry

The safety technology sector may not be considered a pioneer of the digital revolution, but the trend of the “Internet of Things (IoT)” is demonstrably noticeable there as well. The safety industry is experiencing significant changes in the field of extinguishing systems, for example. Their vital parameters, such as temperature, pressure or filling levels, are collected around the clock and stored in clouds. Another step will be autonomously operating systems that perform certain test routines fully automatically and transmit the results.

Video-based fire detection is also developing rapidly - with the help of intelligent algorithms and interconnection of different systems, not only are global reading and control functions possible, but the systems can also learn from each other and hopefully benefit. The desire of many operators for remote support (remote service) also contributes to increasing interconnection and is flanked by current standardization projects such as the upcoming EN 50710.

The highest benchmark in the development of all safety products: They must provide protection - under all circumstances, without restriction. This credo must of course also apply to new, digitalized safety products such as self-monitoring fire extinguishing systems. The changed risk conditions and hazard potentials must be taken into account in order to rule out a failure of protection, even through hacking, for example. What is a highly secure detection and effective extinguishing technology worth if it can be disabled in the blink of an eye through vulnerabilities in the IT-based control system?

To make matters worse, fire protection systems now also have to withstand manipulation attacks (tamper). This is an attack scenario that has long been known in the world of burglary protection, but was previously irrelevant in fire protection. But in the case of an interconnected fire alarm system, it must also be ensured that blackmailers cannot trigger the alarm remotely and thus cause operational disruptions - in order to extort "protection money" from the operator.

Status Quo: Dealing with new, digital risks

The functionality and resilience of safety devices are tested by institutes such as VdS against defined standards and guidelines. VdS has been pursuing an integrated approach to safety for more than 110 years. Only products that are consistent with the approach of comprehensive and holistically considered safety are allowed to bear the VdS seal.

The following four pillars must be taken into account when testing and approving safety technology products and are also part of every VdS guideline:

1. functionality (the promised function must be given)
2. manipulation safety (tamper, if relevant, must be prevented or detected)
3. operating safety (expected operating steps must not trigger an unexpected function)
4. environmental behavior (the device must function properly under the relevant influences)

However, the products are not used in a vacuum, but are usually part of a system or are them-selves interconnected in the sense of IoT and thus connected to the Internet or other networks. In the age of digitalization, this approach must therefore be consistently supplemented by the aspect of information security.

To stay with the example of the networked fire alarm system: Here, the reality is that there is as yet no European standard according to which the protection aspect of fire alarm systems connected to the Internet could be holistically tested. Therefore, in most cases, the work begins at the forefront: the evaluation of the dangers and possibilities of attack, as well as the development of the corresponding safety requirements.

Support on the way to a secure Industry 4.0

Together with industry, associations and authorities, VdS has therefore developed its own, well-founded requirements for this context. The guidelines VdS 3836 "Cyber security for systems and components of fire protection and security technology" examine the new risk conditions of the IoT in detail and regulate the information security of safety and fire protection products - in a practical and straightforward manner.

The guidelines are based on the internationally approved IEC 62443 series standard and for the first time enable appropriate cyber security for interconnected fire protection and safety products/systems. For this purpose, VdS has broken down and specified the complex IEC requirements to the concrete application cases of fire protection and safety technology. This procedure has already proven to be effective and practical, for example, in the case of cyber security for SMEs with VdS 10000. The special characteristics of fire protection and security technology were taken into account, as were specific requirements from standards and guide-lines. The requirements are designed to be class-specific, so that different security needs can be addressed.

The guidelines provide a practical framework for testing information security that is specifically tailored to fire protection and security technology products. They can be applied as horizontal guidelines alongside other standards or VdS guidelines. This means that, in addition to the product-specific requirements, for example for a fire alarm control panel, the IT security aspect is also directly tested and certified. The requirements complement each other thereby.

For the first time, the VdS regulations allow the aspect of IT security to be considered holistically. The guidelines formulate practicable requirements for user and access management as well as for secure data storage and transmission or the validation of interface input by users or other devices. They focus on the device, its functions and its ecosystem. Management system standards such as ISO 27001 or VdS 10000, which primarily regulate the organization of in-formation security, must be distinguished therefrom.

Testing is performed both on the basis of documentation as well as by practical laboratory tests. Depending on the respective software architecture, automated tests, e.g. port scans or brute force attacks are carried out to (thoroughly) test the claimed security features such as firewall functions or hardening mechanisms. VdS has set up a completely new test infrastructure with high performance components and virtualization engines. Even a partial code review is part of the set of test methods, which are used to review the compliance with the requirements.

Certified products are marked with the VdS SecIoT logo. According to the WIK-Enquête, a VdS certificate is the most important purchase criterion for decision-makers and safe-ty/security experts. Manufacturers achieve competitive advantages for their product through the internationally renowned VdS quality seal. By using the additional logo, it becomes apparent at first glance that a product not only meets the VdS requirements for its actual function, but has provided proof that it is also cyber-secure.

VdS SecIoT

Professional installation and maintenance of smart products

A safety product is only truly safe if it is installed and operated properly. But what does this mean for the handling of smart safety products? At the very least, a shift or expansion of competencies. The fact is that the installation and maintenance of an interconnected safety system works differently than with an analog device. The training of specialists at installer companies must therefore take the digital aspect into account.

Whereas in the past mechanics and electronics engineers had to "learn" the aspects of information technology and safety/security at a later stage, in the future (depending on the product and its complexity) it could also be the case that computer scientists gain increasing entry into the industry and then, conversely, have to learn aspects of mechanics and electronics. Perhaps even new professions will develop.

Another factor that should not be underestimated is the interconnection or interaction of several trades in a building. In highly interconnected, digitalized buildings, there can be not only friction losses, but also very specific risks of malfunction/failure and attack. In the worst case, this also affects the interconnected fire and intrusion alarm systems, sprinkler and access systems, which contribute significantly to the protection of life and limb. What is missing in most cases at this point is the complete overview and the overall responsibility as well as the knowledge of the possibilities and limits of the individual trades of a smart building.

This requires a specialist who knows the typical risks and is trained to avoid interdependencies and interaction difficulties, to minimize attack vectors and to optimize the overall processes. In this way, customer requirements can be reconciled with the technical possibilities and what is justifiable in terms of protection, and the specific security gaps in smart buildings can be closed. In order to meet this need, VdS offers the possibility of concrete further training in the field of loss prevention for digitalized buildings with the Specialist for Smart Building Safety & Security.

Smart products must be protected smartly

As discussed in depth, cyber security must be given even greater importance in the future. Progressive digitalization may be a truism, and quite a few people (still) regard it as an empty buzzword in safety and security technology. But even though the great revolution may not yet have taken place, this should not disguise the fact that there is already a great deal of digitalization contained in the products on a small scale. The claim of VdS approvals to provide a practical and holistic statement about the quality of a product and ultimately in combination with other requirements of the overall system therefore requires the systematic inclusion of cyber security requirements.

References

[1] IEC 62443 standard series.

[2] VdS 3836en:2019-12 (01), VdS-Guidelines for Cyber Security - Cyber Security for Systems and Components of Fire Safety and Security Technologies – Requirements.

[3] VdS 10000:2018-12 (02), VdS guidelines for information processing - Information security management system for small and medium-sized enterprises (SMEs) – Requirements.

[4] prEN 50710:20XX, Guidelines and requirements for Remote Services for fire safety and security systems.

[5] EN ISO/IEC 27001:2017-06, Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015).