Impact of new IoT technologies for diagnostics and maintenance purposes in buildings

Veit, Stefan, Steiner, František
Faculty of Electrical Engineering/
University of West Bohemia
Pilsen, Czech Republic
veit@fel.zcu.cz

2022 International Conference on Diagnostics in Electrical Engineering (Diagnostika) | 978-1-6654-8082-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/Diagnostika55131.2022.9905138

***Abstract*— New technologies are having an ever-greater influence on maintenance and diagnostic applications in technical building equipment. The networking of many sensors for the detection of ambient and operating conditions via the Internet of Things [IoT] has here an important role to play. Safety-critical systems therefore also form an important use case. This paper will present the influence of new IoT-based technologies on maintenance and diagnostic applications in safety-critical systems of buildings. Fire alarm systems [FAS] are used as an example to analyse and illustrate the mentioned impact. Possible opportunities and risks of the new technologies are highlighted.**

Keywords*— *Internet of Things (IoT), safety-critical systems, cyber physical systems (CPS), maintenance, diagnostic applications, buildings, fire alarm systems (FAS), risks

I. INTRODUCTION

The starting point for the investigations is that the Internet of Things (IoT) and the associated technologies are increasingly being used in safety-critical systems [1]. This concerns the increased use of IoT technologies for diagnostic applications in buildings and their technical equipment and facilities.

The networking of intelligent sensors is used here to continuously monitor plant and operating conditions, but also environmental conditions. The properties of cyber-physical systems (CPS) are used here [2]. In particular, the new technology offers advantages in terms of the greater computing power that can be made available by the distributed systems of the IoT. In peculiar, the use of these features enables data processing in real time.

Due to these new achievements in technology, new sensor technologies can be used to improve existing applications [3, 4]. However, the increased use of IoT also creates new risks that need to be considered.

Due to the variety and relevance of possible future influences, this paper will present the impact of new IoT-based technologies on maintenance and diagnostic applications in safety-critical systems of buildings. For this purpose, we will first analyse which possibilities exist to use IoT technologies for these applications. The example of fire alarm systems (FAS) will then be used to show what influence this technological change could have. This will be followed by an analysis of the risks involved.

II. BACKGROUND

Today many individual standalone systems are operated and used in classic technical building equipment. The systems often operate autonomously without communication interfaces to other similar systems. This applies both to general building services equipment - such as HVAC systems - and to safety-critical equipment such as fire alarm systems.

The stand-alone systems each have their own sensors to detect environmental conditions for the control and regulation of their internal system functions. In addition, the systems have their own sensors, which can diagnose faulty system conditions.

In the past, these systems mainly stood on their own. Interfaces to other systems and equipment existed only where this was necessary to fulfil the functional scope. This can be demonstrated very well using the example of a fire alarm system in accordance with the specifications of EN 54. As can be seen from figure 1, the essential functions of the fire alarm system - in particular the detection of fire parameters and the corresponding evaluation of sensor data - are located within the plant. This is symbolized by the red marking in the figure. All functions of external systems are produced via interfaces - but exclusively via local links. This is done classically by means of potential-free contacts and wire-bound transmission.

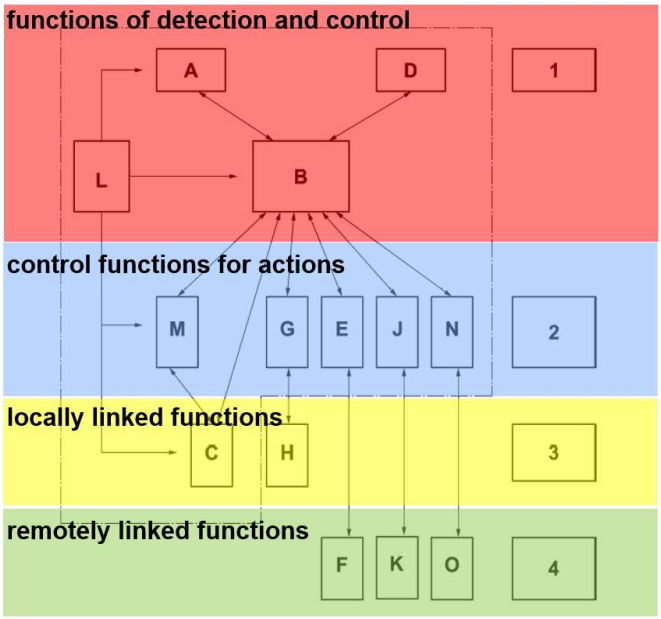
This existing system approach produces many problems in practice. On the one hand, setting up the large number of individual systems is costly. For example, several sensors of the different systems are used for the detection of individual parameters, since a plant-wide data exchange is not guaranteed.

Especially in the case of fire alarm systems, there is the problem of false alarms [5]. In this application, a fire alarm condition is detected by the safety-critical system, although no real fire event is detected. The reason therefore is that decoy variables are present, which are recognized and classified by the system as a parameter for the detection of a fire event. A cross-system plausibility check of the detected events - e.g., the comparison of different sensor data - is not possible due to the missing networking of the system.

These false alarms lead to great risks, which are mainly caused by an additional load and binding of emergency forces

applicable funding agency: TÜV SÜD Industrie Service GmbH .

as well as the panic situations during the evacuation of the buildings, which may be triggered by the alarm [6].



***Legend**: **A** automatic fire detection function; **B** fire alarm control panel transmission function; **F** function for receiving fire alarms; **G** Control function for fire protection device(s), **H** Fire protection system or device; **J** Transmission function for fault messages; **K** Function for receiving fault messages; **L** Power supply function; **M** Control and display function for fire alarm system(s); **N** additional input or output functions; **O** additional management function information exchange between functions*

Figure 1: Functional assemblies of fire detection systems according to EN54-1:2011-06

The following figure 2 shows the high proportion of false alarms in the total number of alarms triggered by fire alarm systems. Shown here is the number of fire alarms from fire detection and alarm systems (FDAS) reported to a professional fire department as a function of the total number of installed systems together with the actual fire conditions found during the operations. According to this evaluation, a false alarm rate of sometimes more than 95 % occurs.

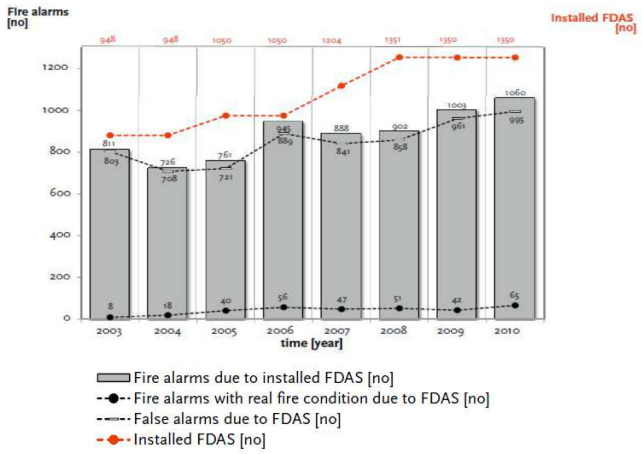


Figure 2: Development of fire alarms from FDAS of a professional fire brigade from [5]

Cross-plant networking can solve many of these challenges. Networking can provide an overarching plausibility check of data to avoid false alarms [7]. In addition, the overall cost of plant installation can be reduced because data from individual sensors can be used for multiple plants. This cross-system networking is based on the Internet of Things (IoT).

III. IoT-BASED TECHNOLOGIES ON MAINTENANCE AND DIAGNOSTIC APPLICATIONS IN SAFETY-CRITICAL SYSTEMS OF BUILDINGS

The use of IoT technologies for a wide range of building services equipment is an approach that has already found its way into many areas of our life. In the private sector, the technology is already widely known as "smart home".

The constant further development of the systems means that the Internet of Things is finding its way further and further into professional building applications - including safety-critical systems. The overall integration of these technologies is to be evaluated as a cyber-physical system approach and a great opportunity to sustainably increase the safety of buildings. Figure 3 shows one example for the possibilities of integration.

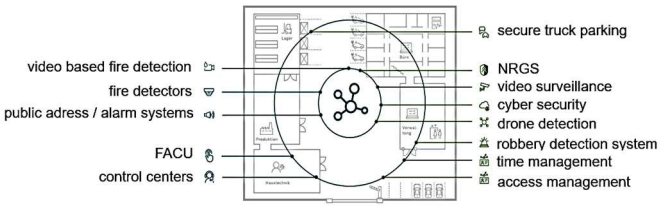


Figure 3: Networked security technology through IoT approaches from [3]

Smart building technology provides a new level of safety. Networked fire alarm technology, for example, makes it possible to detect fires at an early stage, to alert people in the danger zone in a more targeted and efficient manner, to support emergency services more effectively in fighting firesand to document damage events more completely than it was previously possible with the given effort [3].

The influences of IoT technologies on technical building equipment as well as the associated changes in systems engineering are different and have different stages. There are basically three different currents in the associated developments.

A. IoT technology for increased plant networking

One of the central flow directions of IoT applications for technical building equipment is the stronger, higher-level networking of individual systems.

The entire technical equipment - including safety technology - is conceived here as a holistic approach - as a superordinate system networked via the IoT.

In this approach, many individual subsystems still exist - for example, ventilation systems, heating systems, air-conditioning units, fire alarm systems, energy management systems and many more. All these systems can initially operate independently. However, the individual systems are networked and communicate with each other.

Through this approach, the individual plants form a large cyber-physical system. They communicate with each other to

verify changes in status and thus optimize control and regulation processes. In particular, the plants can react specifically to detected fault conditions - for example, the failure of a sensor point - and use data from other plants as a substitute [1].

B. Maintaining the Integrity of the Specifications

Another part of the developments in building technology deals with the use of IoT technologies for real-time processing of large amounts of data. This approach addresses the use of IoT technology to enable new diagnostic methods in building technology [7].

This is very much advanced in fire alarm technology. In most cases, current fire alarm systems use sensors that detect fire events based on fire characteristics - which result from fire consequence products. Examples are smoke or smoke-like aerosol mixtures, heat, flames and their characteristic UV or IR radiation as well as fire gases such as carbon monoxide (CO) or carbon dioxide (CO2).

However, all these currently deployed detector technologies have one major drawback. Every fire is different - because depending on the ambient conditions and the burning material, the fire products that can be recognised by the detectors are produced in a different constellation. Under certain circumstances, this can mean that fires cannot be detected at all or that detection is severely delayed.

IoT technology opens the door to new techniques here: For example, many research efforts together with major manufacturers focused on the use of video technology for the detection of fire events.

Modern image processing techniques can detect fires at a very early stage [8]. The great advantage is that through the image processing techniques not only a specific fire characteristic can be detected. Thus, through the targeted evaluation of video material by new algorithms, both smoke and radiation, can be detected in the wake of flames.

This technology can be used not only for fire detection. IoT approaches can also be used in building technology to monitor systems for other faulty operating conditions.

The major advantage of the new technological approaches is the availability of computing capacity to process large amounts of data. Previous standalone systems - fire alarm systems, for example - were unable to process the vast amounts of data emerging from video-based asset monitoring with the computing capacity made available to them internally within the system [9].

IoT devices can either analyse the recorded monitoring data themselves or use cloud services for this purpose. This creation of the availability of more computing capacity means that computationally intensive algorithms can now also be used for fault detection - especially in combination with artificial intelligence technologies and machine learning approaches [10].

C. IoT as a new holistic system approach

In addition to the directions of flow already outlined regarding the influences of IoT technology on building technology, the most holistic approach is the development of fully IoT-based overall systems.

Here, the individual building technology systems are no longer understood as independent control centres and individual systems, but the systems are formed virtually.

This is an approach in which intelligent IoT sensors are combined into virtual networks and the data can be evaluated by algorithms in a targeted manner regarding a wide range of requirements - including fire detection [7].

On site, such systems simply consist of various networked sensors that can detect different parameters and environmental conditions in the building. For example, the data obtained from the sensor genes can be the room temperature, the composition of the room air from different gases (CO, CO2, O2, etc.) and the humidity.

This data can be evaluated – for one thing - to determine whether air conditioning systems are required to heat or cool the rooms, whether the air humidity is in the optimum range or whether humidification of the air is necessary. On the other hand, however, an evaluation can also be made from a safety point of view - for example, whether there is a fire event or an excessively high CO content in the room.

The original control centre functions of the safety systems are thus virtually taken over by the IoT - making separate control centres obsolete.

New radio-based transmission technologies are playing a key role in networking smart sensors with the IoT. As the number of sensors in buildings increases, wired data transmission of the systems is becoming an increasingly ineffective approach. Radio-based transmission technologies are becoming increasingly important here.

Examples of transmission technologies used in the building sector are already well-known technologies such as ZigBee, Wi-Fi or Lora. Furthermore, however, the introduction of 5G technology is driving the market considerably, since the mMTC family of uses strongly favours IoT technologies and enables real-time-supported communication based on high-frequency connections. Furthermore, an important standard to mention is NB-IoT [7].

IV. RISKS OF IOT TECHNOLOGIES IN BUILDING SERVICES ENGINEERING

As outlined in the previous sections, IoT approaches - regardless of their depth and scope - will influence buildings and their technical equipment in many ways in the future.

However, the use of new technologies is always associated with risk factors that must be considered. The development of IoT-based building technology as distributed, safety-critical, real-time systems is challenging because of its high complexity, the potentially large number of components and especially because of the complicated requirements and environmental assumptions that may arise from national or international standards and guidelines [1].

The risks arising from the use of IoT technologies are based on the need for a minimum level of availability and reliability of the systems. This is particularly important when the sub-applications are safety-critical systems. A qualitative risk analysis was conducted to highlight what risks exist when using IoT technologies.

A. Risk identification

First and foremost, in the qualitative risk analysis is the identification of potential risks. When considering and identifying risks, only those risks are considered that arise from the additional use of IoT technology for safety-critical applications. Special reference is made in the context of the consideration to the example shown of fire alarm systems.

To obtain a complete overview of possible risks, a consideration was made since the layer model of an IoT network, which could be applied for comparable purposes. Figure 4 shows the layer model used.

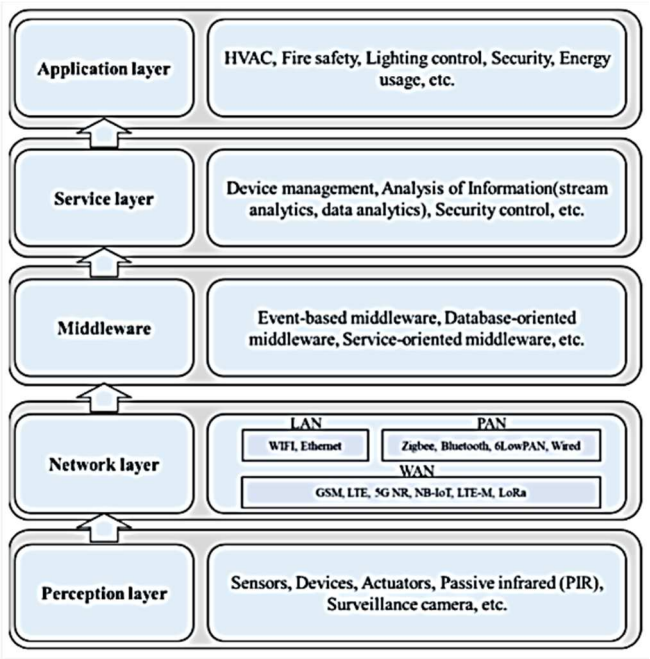


Figure 4: Possible construction of an IoT-based fire detection and evacuation system for buildings from [7]

a) Risk identification for the perception layer

Starting with the perception layer - in which the sensor technology used in the diagnostic applications is located - the topic of energy supply must be considered. The sensor technology itself does not differ - or does not differ significantly - from systems currently in use. However, current systems usually have a wired energy supply. Some manufacturers also rely on a battery-based backup power source. Due to the large number of sensors used and the associated high cost of the wired energy supply, IoT sensors are often powered by batteries as a sole source of energy. This represents a risk that must be considered, since a single failure of the energy supply (battery) would result in a possible sensor failure - and thus a failure or impairment of the diagnostic application (R1).

b) Risk identification for the network layer

Continuing the identification of possible risks, communication at the network layer must be considered. This is where the main part of the sensors' communication with the higher-level IoT network takes place. Here, too, there is a great deal of focus on the changed communication media. This is because high-frequency transmission paths are increasingly being used here instead of line-based communication.

Risks to be considered here are:

- General connection errors during normal operation (e.g., when sending status messages, fault messages) (R2)
- Transmission errors during the sending of data (transmission of incorrect data due to e.g., protocol errors - falsification of sensor data) (R3)
- Connection restrictions in case of danger due to changed environmental conditions (restriction of radio connections e.g., due to smoke) (R4)
- Disturbance of signal transmissions due to unintentional interference with other high-frequency transmission protocols (R5)
- Interference by deliberate, malicious system influences to deliberately disrupt connections and communication paths (hacker attacks, jammers, etc.) (R6)
- Disruption by deliberate, malicious system influences to deliberately manipulate data, e.g., to implement / install false alarms and trigger associated event chains (R7)

c) Risk identification for the middleware

In the next layer - the middleware, the targeted tailoring of sensor data for the application software takes place. Here, the flood of different sensor data is prepared in such a way that the data for evaluation by the IoT application on the service layer has the right format as well as the necessary framework conditions in terms of scope, depth, and representation. Risks arise here as well:

- Incorrect data cutting by the stored algorithms, which leads to the fact that not all necessary data can be evaluated optimally, or necessary data is lost - possibly also induced by deliberate software manipulation (R8)
- Limited software availability resulting in extended runtimes and limited real-time capability of the system (R9)

d) Risk identification for the service layer

The main analytical task of an IoT-based fire alarm system - but also of all other IoT-based diagnostic applications - occurs at the service layer level. Here, the data is evaluated with (intelligent) algorithms and corresponding damage events are detected. The following possible risk factors arise:

- Lack of computing capacity to perform the analytical task in real time, resulting in delayed detections. (R10)
- Faulty algorithms fail to detect malicious events or fail to do so within the required service time. (R11)
- Algorithms are deliberately influenced by malicious unauthorized access in such a way that detection of malicious events does not occur - or occurs even under normal operating conditions (e.g., due to malware, hacker attacks, etc.). (R12)
- False alarms / deceptive alarms occur due to faulty algorithms. (R13)

e) Risk identification for the application layer

The top layer that needs to be examined in terms of identifying potential risks is the application layer. This is about the actual provision of a concrete service - in our example a fire alarm system - for other applications. At this level, the results of the service are communicated in such a way that they can be used for other applications. The following risks must be considered:

- Data is not usable for other systems because interfaces do not work correctly. (R14)
- Errors in data exchange with other systems are not detected. (R15)
- Prioritization of messages is incorrect. Safety-relevant events and results are not forwarded with the correct priority and are inadmissibly delayed. (R16)
- Sufficient data integrity is not guaranteed, and sensitive system data can be viewed by unauthorized persons. (R17)
- False alarm messages can be implied into the system through malicious manipulation or correct alarm messages can be deliberately suppressed (e.g., through hacking attacks). (R18)

When considering the specific risks for fire alarm systems, a distinction can be made between two basic groups of risk factors. The first group considers the failure of the system and the associated failure of early fire detection in the part of the system considered by the failure. The second group is formed by the scenarios of deliberate implication of false alarms. On the one hand, this can disrupt industrial processes, deliberately trigger panics, or disable entire safety-related infrastructures if, for example, all fire alarm systems in a city report an alarm almost simultaneously.

B. Analysis of the causes of risk

After the identification of possible risks, the next step in the risk analysis is the evaluation of the possible causes. The causes of the collected risks can be summarized here, since the effects and the sub-risks on the layer levels are different, but causes are often the same. Identified causes are:

- Technical defect (C1)
- Faulty data connection of high frequency links (C2)
- Environmental influences on communication paths (C3)
- Malicious system interventions / hacking attacks (C4)
- System overloads / lack of computing capacity (C5)
- Faulty algorithms / software (C6)
- Lack of IT security (C7)
- Faulty (human/manual) system interventions (C8)

C. Analysis of damage impact

In addition to the causes, as well as the identification of possible risks, the analysis of the possible extent of damage forms an important role.

Basically, it is to be considered here that the extent of damage in numbers naturally always depends on the considered building and the situation. In the context of a qualitative consideration, however, a distinction can be made between:

- Damage factors, which lead to a delayed function of the plant. (S1)
- Damage factors, which influence parts of a plant and can lead to a failure of the plant. (S2)
- Damaging factors that influence an entire plant and can lead to its failure. (S3)
- Damaging factors, which can influence whole infrastructures (of several buildings) and can endanger their entire safety concept. (S4)

D. Findings of qualitative risk analysis

In risk analysis, risks are assessed as the product of the likelihood of occurrence and the severity of a potentially resulting damaging event. If a quantitative risk analysis is performed, this can be calculated and quantified using appropriate factors.

In the qualitative risk analysis carried out here, the findings are evaluated using a risk matrix. Here, the probability of occurrence as well as the severity of the consequences if the risk were to occur are shown in a diagram. In this way, it can be shown graphically in a clear and simple manner which are the greatest risk factors and must therefore be considered in a prioritized manner.

The following illustration in figure 5 shows graphically the assessed distribution of risks in the use of IoT technology for diagnostic applications in safety-related systems in buildings regarding the probability of occurrence as well as the possible extent of damage.

As the results of the qualitative risk analysis - emerging from the graphical risk matrix - show, the greatest risk comes from malicious implied false alarms into a system [11]. The severity of the impact depends on whether only one system is affected or whether an entire infrastructure is affected by numerous maliciously implied false alarms at the same time, effectively rendering it incapable of action.

The highest risk is still posed by deceptive alarms because of false algorithms. Furthermore, relevant risks can be analysed in incorrect prioritization of damage reports, malicious hacking attacks from damage detection algorithms and errors in the detection of system errors.

Overall, low risks arise from individual data transmitted with errors, individual erroneous data cuts of the algorithms or errors in the data integrity of the systems.

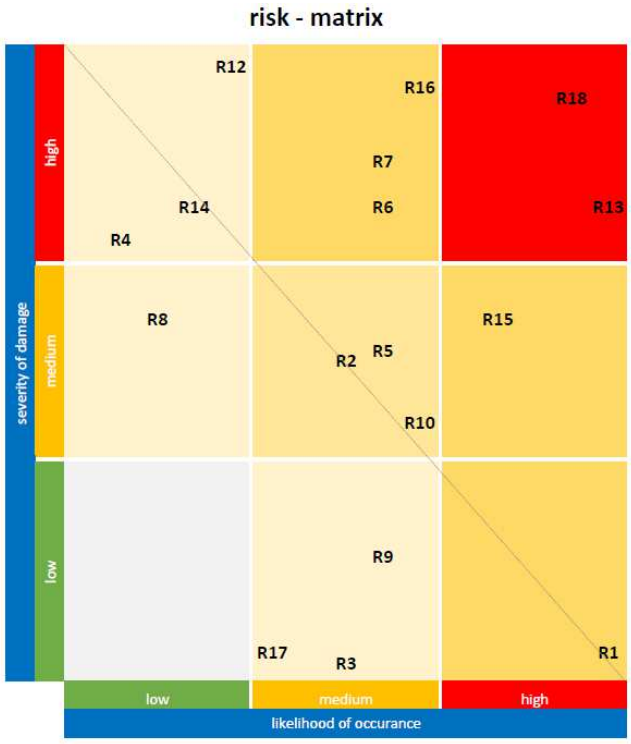


Figure 5: Risk matrix on IoT-Technologies for diagnostic purposes for safety critical systems in buildings

E. Countermeasures

After the risk analysis has been carried out, the question now arises which countermeasures exist to reduce the analysed risks to an acceptable residual risk. It is important to consider those risks which simultaneously have a high likelihood of occurrence and a large amount of damage.

In this respect, the risks based on technical system conditions can be considered first. These are, for example, R5 - Disturbance of signal transmissions due to unintentional interference with other high-frequency transmission protocols or R10 - Lack of computing capacity to perform the analytical task in real time, resulting in delayed detections. Furthermore, the risks R6 and R15 would be classified in this category.
This kind of risks can be counteracted very well by the appropriate selection of communication protocols for data transmission with the corresponding priorities of alarm messages. Corresponding regulations already exist in current installation and product standards, for example in the EN-54 standard.

Unfortunately, there are also risks for which no standardized countermeasures have yet been introduced. This concerns malicious system interventions, as it is the case in some of the most highly classified risks. This affects, for example, risk R18. - False alarm messages can be implied into the system through malicious manipulation or correct alarm messages can be deliberately suppressed (e.g., through hacking attacks). In science, this circumstance has already been recognized and research work exists - how such system influences could be prevented [11]. However, these have not yet been implemented in practice's analysis, risks are assessed as the product of the likelihood

V. CONCLUSION

This article focused on the impact of IoT technologies and resulting new approaches on diagnostic and maintenance applications in buildings - related to the technical building equipment and its safety-critical system components.

This paper showed that there are various approaches through which IoT could influence building technology. This begins with increased networking of systems via the IoT together with the enabling of new diagnostic procedures for real-time data processing. A fully comprehensive approach is offered by the overarching networking of sensors to form "virtual plants" - and the associated elimination of on-site central functions by physical plants.

The example of fire alarm systems was used to explain which technologies have already found their way onto the market and that the use of new technology can solve many problems of existing plant technology.

As the main part of the scientific work, a qualitative risk analysis of the new IoT approaches in the listed topic area was carried out. Through this qualitative analysis, it can be presented that the use of IoT technology for diagnostic processes in safety-critical systems in buildings poses non-negligible risks. In particular, the attack paths for malicious system interventions - especially the deliberate implication of false alarms or the falsification of detection algorithms - are important risk factors with high damage potential.

The results of the work also show that effective countermeasures are already presented in some cases in the standards. However, some risks, which are to be classified as very critical due to the technological innovations, are not yet considered by standardized countermeasures. Further consideration is required here reducing these to an acceptable level.

The findings of the work show that for the practical use of IoT-based distributed systems for safety-critical applications in buildings, new regulations and test procedures must be created to limit the risks and their potential damage to an acceptable level. The equivalence of the systems with today's systems cannot be assessed with existing test procedures commonly used in practice. This requires new methods and regulations for the planning, evaluation, and assessment of these systems.

[1] SERGIO ALEJANDRO FEO ARENIS. A Formal Approach to the Development of Industrial Cyber-Physical Systems.

[2] ZHANG, J., R. R.A. ISSA a R. LIU. A Cyber-Physical System Approach for Intelligent Building Emergency Evacuation Signage Guidance. In: C. Wang, C. Harper, Y. Lee, R. Harris a C. Berryman, ed., 2018, s. 535-541.

[3] SAYURI GUNAWARDENA. Der Brandschutz der Zukunft. Digitalisierung, Innovationen und verändertes Sicherheitsbedürfnis: neue Perspektiven für den Brandschutz. Ein Whitepaper von Bosch Energy and Building Solutions. 2021.

[4] ALTOWAIJRI, A. H., M. S. ALFAIFI, T. A. ALSHAWI, IBRAHIM, AB a S. A. ALSHEBEILI. A Privacy-Preserving Iot-Based Fire Detector [online]. IEEE ACCESS. 2021, 9, 51393-51402. Dostupné z: 10.1109/ACCESS.2021.3069588.

[5] FESTAG, Sebastian, ed. False Alarm Study: False Alarm Data Collection and Analysis from Fire Detection and Fire Alarm Systems in Selected European Countries. 1st ed. Berlin : Erich Schmidt Verlag GmbH & Co, 2018. 978 3 503 18101 8.

[6] FESTAG, S. False alarm ratio of fire detection and fire alarm systems in Germany - A meta analysis [online]. FIRE SAFETY JOURNAL. 2016, 79, 119-126. Dostupné z: 10.1016/j.firesaf.2015.11.010.

[7] FANG, H. Q., S. M. LO a J. T.Y. LO. Building Fire Evacuation: An IoT-Aided Perspective in the 5G Era [online]. BUILDINGS. 2021, 11[12]. Dostupné z: 10.3390/buildings11120643.

[8] SHARMA, A., P. K. SINGH a Y. KUMAR. An integrated fire detection system using IoT and image processing technique for smart cities [online]. SUSTAINABLE CITIES AND SOCIETY. 2020, 61. Dostupné z: 10.1016/j.scs.2020.102332.

[9] PARK, J. H., S. LEE, S. YUN, H. KIM a W. T. KIM. Dependable Fire Detection System with Multifunctional Artificial Intelligence Framework [online]. SENSORS. 2019, 19[9]. Dostupné z: 10.3390/s19092025.

[10] GERRY CHRISTENSEN. Artificial Intelligence of Things [AIoT] [online]. Dostupné z: https://internetofthingsagenda.techtarget.com/definition/Artificial-Intelligence-of-Things-AIoT.

[11] SHIN, H., J. NOH, D. KIM a Y. KIM. The System That Cried Wolf: Sensor Security Analysis of Wide-area Smoke Detectors for Critical Infrastructure [online]. ACM TRANSACTIONS ON PRIVACY AND SECURITY. 2020, 23[3]. Dostupné z: 10.1145/3393926.