# Improving IT Security of Medical IoT Devices:

# A Maturity Evaluation and a Labeling Approach

Michael Gleißner[1,2], Johannes Dotzler[1], Juliana Hartig[1], Andreas Aßmuth[2], Clemens Bulitta[1] and Steffen Hamm[1]

*Technical University of Applied Sciences OTH Amberg-Weiden*
[1] Hetzenrichter Weg 15, 92637 Weiden, Germany
[2] Kaiser-Wilhelm-Ring 23, 92224 Amberg, Germany

Email: {m.gleissner | jo.dotzler | j.hartig | a.assmuth | c.bulitta | s.hamm}@oth-aw.de

***Abstract*—The healthcare industry worldwide is currently being transformed by digitization and the Internet of Things. As the level of digitization increases, the number of devices within a network of a healthcare facility grows exponentially. The consequential complexity of the infrastructure poses a substantial challenge for IT professionals to keep their networks secure. This paper aims to provide two different ways to aid administrators and decision makers to help integrate the increasing amount of interconnected medical devices into their infrastructure more securely. Additionally, two mobile ultrasonic scanners were tested in regard to their security as well as privacy to show where problems with such devices might occur.**

***Keywords*—*Internet of Things; healthcare; Medical IoT; cloud services; IT security; IoT labeling; IoT evaluation.***

## I. Motivation

With the rise of the Internet of Things (IoT), IT security has become an ever increasing challenge. Additionally, one of the main reasons why the focus on IT security is going to be amplified is the fact that future communication networks will be based on software-defined networks (SDN). SDNs will be exposed to a large number of known attack vectors, which are already available on the market since SDNs are increasingly implemented using architectures similar to the Representational State Transfer (REST) schematic. Therefore, attacks can be carried out by anyone without specific expert knowledge. This risk is consciously accepted, and solutions are developed for it. The reasoning is that potential gains for industries that come with Next Generation Mobile Networks (NGMNs) exceed the known risks. Potential benefits of NGMNs include, for example, network-slicing or SIM provisioning. From an economic point of view, NGMNs require new use cases, e.g., the density of connected IoT devices, to make it a profitable investment for adopters. The most promising adoption of 5G networks in that context is the so-called "massive Machine Type Communication" (mMTC) [2]. New use cases are still evolving, for example, for branches like public safety, the automotive industry, healthcare, factory automation etc. These use cases are based on the concepts of IoT and promise a steep increase in productivity across a variety of business processes and industries [3]. To implement these use cases, it will be necessary to integrate and administrate up to 100,000 devices per 1 km² [4] in the future. This is going to present a challenge that needs to be carefully considered. Undoubtedly, managing such a massive IoT ecosystem demands highly secure architectures and certified processes with a strong focus on IT security, particularly for healthcare providers. The goal of this paper is to provide two different methods for healthcare facilities to improve their IT security posture. A maturity model is presented, which provides guidance on how an environment for Medical IoT (MIoT) integration needs to be shaped in order to maintain a secure infrastructure while still reaping the benefits of the devices. Additionally, a labeling concept is shown. This concept allows personnel responsible for procuring MIoT devices to quickly assess if a product fulfills the minimum requirements to be considered secure for integration. It is meant as a supporting tool for gaining a brief overview rather than a replacement for an in-depth security analysis of the MIoT device. The rest of the paper is structured as follows. In Section II, a brief review of currently published IoT security-related reference models from accredited stakeholders, e.g., industry associations, consortia and alliances, are presented. Section III highlights the background to understand the topic and underlines essential aspects. Section IV introduces a majority model focusing specifically on the healthcare sector. Section V presents a labeling approach for technology to empower healthcare facilities and consumers. Section VI outlines a security test of two IoT devices in detail. At last, an outlook and future thoughts are given.

## II. Recent Works

This section presents a brief literature overview of common standards and reference models targeting IoT-related security models and architectures by accredited consortia, alliances and standardization bodies. During the literature research, it turned out that relevant standardization efforts mainly originate from the manufacturing and production sector. Consequently, it is not surprising that most (industrial) IoT reference models, architectures and blueprints target manufacturing and production sites and are, therefore, not fully compatible with the healthcare sector. A possible reason for these one-sided efforts could be the fact that several government programs, e.g., "Industrie 4.0" from Germany [5] or the "Made in China 2025" initiative from the Chinese government [6] have been established.

Literature research of already existing IoT reference models targeting manufacturing and surrounding topics has already been conducted by many researchers. Some examples are the research from Nakagawa et al. with the title "Industry 4.0 reference architectures: State of the art and future trends" [7] and the work of Mazon-Olivo and Pan titled "Internet of Things: State-of-the-art, Computing Paradigms and Reference Architectures" [8]. For the sake of completeness, some well-recognized reference models are mentioned. These are the "Referenzarchitekturmodell Industrie 4.0" (RAMI4.0) [9], the "NIST Smart Manufacturing Ecosystem" [10] and the advanced IoT reference models for the Internet of Things from the "IoT World Forum Reference Model" [11]. Also, the European Union published a consolidated IoT standard and announced the "3D Reference Architecture Model" [12].

Those architectures and frameworks targeting IoT security all share that security cannot be achieved by merely applying software and / or technologies, e.g., blockchain, alone. Security has to be an integral part even before the beginning of the actual development process. During this process, the type of users and the intended use cases are vital parameters to consider. Some alliances apply security-relevant topics to the entire supply chain. Starting with the component manufacturer (producer of hardware, e.g., chips and processors), over to retailers and operational users. The goal is to provide recommendations targeting those specific groups to security by design into practice, which results, for example, in the (Hardware) Root of Trust ((H)RoT) [13]. Others shed light on detailed processes, e.g., on an auditable and verifiable boot process [14], when setting up and integrating IoT devices in an existing network.

From a German perspective, the Federal Office for Information Security published in their recommendations several useful proposals for how IoT devices can be used safely in institutions [15] and how they can be operated securely [16]. These recommendations might find attention in well-financed production industries with up-to-date IoT devices, which are intended to perform their tasks in a network. But the reality shows an entirely different picture because other industries, e.g., the German healthcare industry, cannot rely on up-to-date equipped departments, and thus, some outdated medical devices will be modified to act as IoT devices. This approach leads to a very error-prone infrastructure. A scenario has been considered in this manner neither by the publications of the Federal Office for Information Security nor by other sources listed above. Another critical topic is the kind of data in the healthcare industry. Health data or data related to patients need to be treated with special care because this data describes various medical conditions of people and can cause damage in the wrong hands. In order to implement a legal basis, the EU states in its General Data Protection Regulation (GDPR) [17] a set of regulations which enforces compliant handling of personal data. This is done to handle potential misconduct of such sensitive information (e.g., healthcare data). A proper application of the GDPR needs to be considered, especially in the healthcare sector, where highly sensitive data is collected [18]. Additionally, a certain set of rules and requirements need to be defined in order to provide a minimum in the safety and security of the technology used in practice. Therefore, it is imperative to answer the corresponding questions about what IoT devices will be deployed and thus purchased and integrated in a future healthcare environment. This paper aims to outline the common understanding and need for the definition of references related to safety and transparency labeling models, focusing on the healthcare industry in Germany. Complementary to this, a maturity model for Medical IoT devices is proposed, which allows to evaluate if a secure integration of these products by the corresponding actor is possible. Section V proposes a concept that will enable consumers to obtain a comprehensive picture of the functionality, built-in components, generated data and responsible parties of an IoT device. This allows customers to gain an overview of the corresponding product even before purchase. Last but not least, two exemplary Medical IoT devices are examined to show the current deficits of the industry in regards to IT security. In the following section, the mentioned assessment model is introduced.

## III. Background

IoT is now influencing many areas of business and private life and is gaining increasingly technical, social and economic importance. IoT can be defined as "an emerging concept comprising a wide ecosystem of interconnected services and devices, such as sensors, consumer products and everyday smart home objects, cars, and industrial and health components" [19]. This work focuses on IoT devices in the healthcare sector. It aims to be an extension to our previous work in [1] with the goal of analyzing MIoT with a focus on IT security. Especially in the healthcare sector, device failure can have devastating consequences for human beings.

The reason for this is the increasing focus on digitization in the healthcare sector. The introduction of the new 5G mobile network will enable better and more efficient connectivity between IoT devices, which means that the number of these devices in the sensitive healthcare environment is expected to grow exponentially over the next few years. In numbers, this means that USD 60.83 billion were spent on IoT devices in the healthcare sector in 2019, whereas in 2027, the investment is expected to reach USD 260.75 billion [20]. The goals of MIoT devices are, among others, to reduce the workload of medical staff, to make diagnostics more efficient and safer, and to make everyday life easier for patients. One possible way might be monitoring interconnected devices in the network to analyze utilization, location or maintenance intervals. A reduction in search times and an increased efficiency in the use of equipment (e.g., mobile ultrasound scanners) are potential benefits.

## IV. Maturity Model for Secure Medical IoT Integration

The following model is embedded in the 5G4Healthcare research project, which is briefly presented below to provide context.

### A. Project 5G4Healthcare

The 5G4Healthcare project (5G4HC) at the Technical University of Applied Sciences Amberg-Weiden (OTH-AW) is one of six research projects funded under the 5G Innovation Program of the German Federal Ministry for Digital and Transport. The project's objective is to establish a platform based on 5G technology on what digital applications can be integrated into healthcare scenarios. The scenarios will focus on measurable improvements in the effectiveness and efficiency of healthcare delivery. The project also aims to explore opportunities and limitations in improving healthcare delivery through 5G. Primarily related to the two defined use cases "Homecare" and "Integrated Care", the opportunities and potentials of the 5G technology in healthcare will be explored. Part of the 5G4HC project is developing an evaluation model specifically for the digital health sector. Based on the work done on the general evaluation model, the following model was developed for Medical IoT devices with a focus on the secure integration of MIoT devices in healthcare facilities. The methodology of the general model is explained below.

### B. Methodology of the General Evaluation Model

The model developed takes the essential aspects of established evaluation systems in a mixed-method approach and combines them to form a new evaluation model. Initially, the basis for this system is the model of the European Foundation for Quality Management (EFQM) [21]. The EFQM model is based on a comprehensive analysis of elements in three levels: structure, process and result relevant to quality. In its original model, it is divided into a total of nine criteria and subdivisions (e.g., management, personal, law and regulatory, etc.). These criteria have been adapted for the Medical IoT model (see Section IV-C). In the next step, the sub-dimensions of the EFQM model are assessed using the systems of a maturity model. These five maturity levels are divided into beginnings (1), first steps (2), on the way (3), developed organization (4) and mature organization (5).

The essential novelty of the developed evaluation model consists in the systems that a holistic consideration will take place by means of the nine sub-dimensions. The intention is to ensure that the results provide a weighted statement about the development status of a technology, a process or even an entire system.

### C. Methodology of the Medical IoT Model

The generic evaluation model is modular. One module was adapted Medical IoT devices, with IT security as the main criterion. There are many recommendations on IT security of IoT devices in the international literature (see Section II). However, the market has lacked a separate elaboration tailored to integrating Medical IoT devices into a healthcare environment so far. The following assessment model is intended to fill this gap. Based on the recommendations for general IoT devices from industrial and other sectors [22], an overview was created that includes special conditions for the medical industry. The available literature includes recommendations and guidelines from organizations such as the IoT Security Foundation, Industrial Internet Consortium (IIC), Online Trust Alliance (OTA), European Union Agency for Cybersecurity (ENISA), and many other official entities. The criteria found in these guidelines were thus adapted to this specific use case in the healthcare sector and divided into five maturity levels. Before explaining the model, the specifics of the healthcare sector will be discussed.

Normally, Medical IoT devices are used by medical personnel. Both doctors and nurses operate diagnostic and therapeutic IoT devices. It can therefore be assumed that the user has a low level of digital competence. Furthermore, medical personnel is under time pressure in their daily work. Due to staff shortages or acute indications of patients, seconds can play a decisive factor in care. In the context of Medical IoT devices, this means that failures or complex handling are not suitable to be an actual relief for the staff. Dedicated IT personnel are also typically few to nonexistent and require a broad knowledge of medical devices. It is common, especially in outpatient practices, that no trained IT staff is on site. Instead, separate external companies that have a 24-hour response time are used. In the medical sector, the availability of IoT devices must therefore be close to 100 %, especially for critical applications. Otherwise, the well-being of patients is at risk. Another critical point is the environment the Medical IoT devices have to be integrated into. The IoT devices must be embedded into existing infrastructure. However, in most cases, that infrastructure is outdated, especially in hospitals, nursing homes and outpatient practices, which directly impacts IT security. Even if an IoT device was developed and sold by the manufacturer using the security-by-design approach, there is still a risk of unauthorized access or tampering simply because of the infrastructure in the healthcare facility. To minimize this risk, investments in infrastructure need to be made, highlighting the next problem in the healthcare sector: Lack of financial means. Depending on the country, healthcare facilities have a different financing structure. Facilities can be governmental, private or public nonprofit. Government health facilities, in particular, often lack the money for new investments. Primarily, financial investments are made in more urgently needed areas, such as additional staff or an expansion of treatment services. Investment in infrastructure is rarely the first priority. These particular problems make it clear that, from an IT security perspective, a good and trustworthy environment cannot be assumed. However, there is hope for the future. Many countries (e.g., Germany with the Hospital Future Act) are switching to state support for digitization in healthcare facilities. The potential funding amounts are enormous depending on the country (e.g., in Germany, 4.3 billion euros in 2021). These subsidies should be used urgently

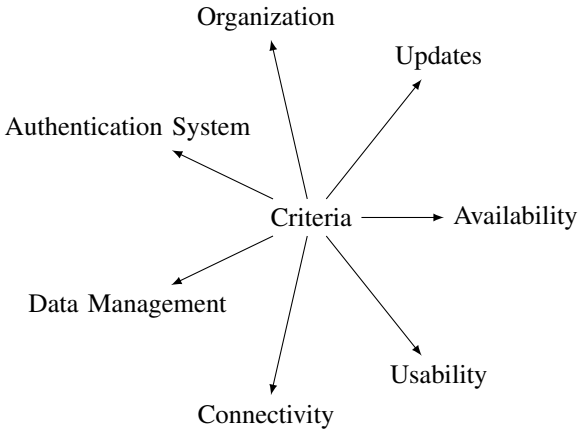


Figure 1. Criteria as basis for the evaluation model

to make the environment in healthcare facilities more secure, as the potential risk here is exceptionally high for the reasons mentioned. In the following, however, we will still focus on Medical IoT devices, as many threats can be prevented through good preparation and a structured approach. To structure the evaluation of the Medical IoT integration process and thus reduce complexity, seven criteria were formed similar to the generic evaluation model (see above). These can be seen in Figure 1.

These criteria were divided into the dimensions of structure, process, and outcome according to the Donabedian approach [23]. Following the approach, means that with a good structure and a good process based on it, a good result is automatically achieved. The dimensions thus build on each other and influence each other. All criteria were deliberately chosen to provide a controlled setting for Medical IoT devices to be embedded into. By providing such an environment, security and safety for staff and patients can be significantly improved both during the implementation phase and during regular operation. All detailed criteria can be seen in the appendix.

The system in the maturity model states that all criteria of one level must be fulfilled to attain the next higher level. For example, even if individual criteria of level four are fulfilled, but one criterion from level three is still not fulfilled, the IoT device is only awarded level three. The three matrices for evaluation can be found in the appendix. After shedding light on the maturity model, the upcoming sections refer to a concept that aids consumers in their decision-making regarding IoT products.

## V. Sovereign Technology Labeling

The idea is to provide visual indications for products (e.g., IoT devices) to help consumers and decision-makers in sensitive and critical industries. The healthcare industry must provide accessible and understandable information about MIoT devices that go beyond price and functionality. That information needs to be even more detailed if IoT interacts closely with humans. To be able to perform an adequate evaluation of MIoT devices, some kind of additional labeling (obligation) might be helpful. A system of this kind could be a beneficial addition to the evaluation model presented in Section IV, making it easier to assess criteria such as data management or updates. The labeling should reflect key figures that best represent individual IT security-related aspects. Looking at hardware, labels should be displayed on the respective product packaging or the devices themselves. For software, on the other hand, a digital indication should be given before the final purchase / sign-up is made. Furthermore, future IoT devices must also be equipped with an expiry date that clearly reflects a time frame for action to be taken in order to further continue the use of integrated hardware components, installed software and intended operating environments.

An already applied and working analogy, which proves the increase of safety and security, can be noticed in the food industry and their products. The food industry must ensure that its products do not cause any harm to consumers. That is the reason why various procedures have been developed to increase the safety of food. To make the safety aspect transparent to consumers, various information and visual labels have been developed and put on products. Guidelines and labels could also be a foundation and possible approach to evaluate different technologies and their adaptations in products, e.g., IoT, software, or services. These guidelines and labeling requirements for food products are defined precisely and even required by law. Almost every country has governmental regulations for food safety, for example, the food regulations introduced by the European Union [24]. The quality assurance tools and mechanisms for the food industry have already proven that it is possible to shift the issue of safety to the manufacturer and, thus, away from the consumer. It would be appropriate to establish such guidelines for technology as well. An example of a mapping of food safety scenarios applied to technology is presented as follows:

$$\text{Nutrition Facts Label} \rightarrow \text{IoT Components Facts Label}$$
$$\text{Food Handling} \rightarrow \text{IoT Lifecycle Facts}$$
$$\text{The Best Before Date} \rightarrow \text{IoT Best Before Inspection Date}$$

A first approach is presented to map necessary information from the nutrition to the IoT domain by declaring precisely what components, protocols etc., were integrated or used during operation. It should be noted that this approach is not supposed to end up with a confusing set of different labels. One or two labels that make the most important indicators available must be sufficient to allow the consumer to make a quick and comprehensive assessment. A QR code will be provided should there be a need for more in-depth details. At the moment of writing, a list of parameters, which should be displayed, has not been defined. It is emerging that the areas affecting the human in this context will be a focus point. Until now, these areas are hardware, software and data (flow). The standard IoT component facts label suggested above would be a first step towards a more transparent evaluation of an IoT device itself and supports decision-makers to evaluate IoT devices in more detail. Specifications may vary depending on the

| IoT Components | Used in Item |
|---|---|
| **Sensors / Detectors** | **real time, post processing** |
| 1. Temperature Sensor | Temperature in Celsius |
| 2. Location Sensor | GPS, Latitude and Longitude |
| **Actuators** | |
| 1. Electric Motor | Rotation |
| Connectivity / Network | Cloud / Local |
| 1. Protocol Name | MQTT |
| 2. Protocol Name | Bluetooth |
| **Gateways** | |
| Cloud Location | Italy, EU |
| Storage Location | Netherlands, EU |
| Responsible Entity | Company name, phone, email, country |
| **Stored Attributes** | **Name / Cycle** |
| 1. Attribute | GPS (latitude and longitude) / every minute |
| 2. Attribute | Temperature / every minute |
| User Control | App, device itself |
| **Deletion of Date** | **Easy to complex** |
| 1. Electric Motor | Rotation |

TABLE I. An example of a possible IoT component labeling approach

product category, intended use and criticality. The following section presents the second part of the presented approach with all relevant runtime facts of a specific MIoT device that needs to be measured and labeled by the manufacturers.

### A. IoT Runtime Facts

The IoT runtime facts provide information about nominal or target values for different stages of usage of an IoT device. Those stages are presented as follows:

*1) Integration Stage (Initial Setup):* This stage of an IoT device represents the initial integration into an existing environment by recording the boot process of the IoT device in detail. Reference values should be specified by the manufacturer. These values are to be expected during the initial boot process. Examples are CPU usage, energy consumption, standard boot time, successful boot loader verification, etc. Having reference points would help detect tampered IoT devices from the beginning. Comparing the original values (manufacturer's specifications) with the actual values when a device is first set up allows the detection of anomalies. This approach can not only be applied during initial integration into an IoT environment, but it can also be utilized in the day-to-day monitoring efforts of IoT devices during operation. Threshold values could also be defined and specified by the manufacturer which are not exceeded during everyday use.

*2) Operating Stage:* This stage should reflect the IoT device metric in operation mode. It should list the same parameters as mentioned in the integration stage but with adjusted values. Additional values when operating in a production environment could be listed. An example might be the data throughput (amount of processed data). Furthermore, the IoT runtime facts in operation enable responsible parties to identify malicious IoT devices by monitoring the given reference values with the current information when in use. This allows for the detection of misconfiguration or of tampered devices without having to shut down an entire MIoT infrastructure as a precaution. To meet the above requirements, the IoT Device IdentificAtion and RecoGnition (IoTAG) [25] approach might present a possible solution. The IoTAG approach proposes that all IoT devices used in an IoT environment report their security-relevant parameters, such as a unique ID, a device name, the current software version, active services, etc., in order to manage IoT networks securely [25].

*3) Fail Safe Stage:* Within this stage, extreme values for security-relevant parameters need to be defined by the manufacturer. Those extreme values (maxima and minima) should never be exceeded in any operation stage of a MIoT device. Should this still happen, a reaction chain must be invoked, and the MIoT device has to automatically be removed from the operating stage and be forced to pause operation.

### B. Best Before Inspection Date

To support a more transparent labeling and thereby strengthen the role of consumers, an additional important indicator is suggested: the best-before-inspection date. This date is not a fixed value as known from food safety. Instead, it is intended as an indication for decision-makers. It represents how long the IoT device can securely operate, at least without the need to apply changes. The date can be extended by updates, patches, etc. The best-before-inspection date for MIoT proposed depends largely on the activities and reaction time in terms of further development by the manufacturers. Parameters, which influence the best-before-inspection date, are, among others, the following:

- Update cycle
- How many new product variants were newly developed by the manufacturer?
- What is the average end of lifetime period for this particular manufacturer?
- etc.

Many more parameters could be mentioned to modify the best-before-inspection date. The mentioned parameters are used to get the idea across. The approach to calculating an accurate best-before-inspection date is quite difficult, as no average values regarding the lifetime of individual hardware components are available. This is amplified by the fact that the lifetime is also dependent on its operating time and operating environment. If average values were available for the lifetime of individual components considering the actual operating time and operating environment, it would be possible to calculate the best-before date of hardware. Results could be based on the component with the shortest life time. It should also be noted that a fixed best-before date could negatively impact our ecological environment, as IoT devices would be disposed of when the best-before date is exceeded. Reevaluating whether the IoT device can still be used for its intended purpose from a technical point of view might not be done. Hence, there is a need to develop a more flexible best-before-inspection date. The best-before-inspection date is intended to specify a point in time when it becomes necessary to reevaluate the IoT device for the first time after its initial integration. Otherwise, IoT turns into an avoidable risk. With this definition in mind, it is more comprehensible to calculate an accurate best-before-inspection date. The calculation starts with the date of manufacturing or, if not available, with the date of purchase.

After a starting point is declared, the best-before-inspection date can vary based on certain parameters. Parameters that have a positive effect could be the frequency of updates, if the product or software is still purchasable or if the product line still exists. Parameters with a negative effect could be that the manufacturer does not provide support or updates anymore. This kind of behavior of a manufacturer would automatically lead to a negative label. Labeling a product in such a way provides decision-makers an indicator that the manufacturer does not provide continuous and recurring updates. This might influence the decision of whether buying an IoT or MIoT is beneficial. The precise definition of parameters that can be used to classify values as positive or negative in relation to the best-before-inspection date will be identified in future research efforts.

The approach of determining an approximate best-before-inspection date enables IT security managers to initiate various actions. The best-before-inspection date is primarily intended to initiate an action on a specific day. An action can be a comprehensive screening of the IoT device by checking if the firmware is up to date. Restarting the IoT device and then comparing the measured values during the reboot process with the original ones provided by the manufacturer is also possible. Another option is ensuring that actual support activities offered by the manufacturer are still active. Furthermore, the best-before-inspection date can also be used to start a new threat modeling or the maturity modeling process. The latter is suggested in Section IV.

Ultimately, it can be said that the three proposed labeling approaches have the potential to provide two benefits. On the one hand, the decision-making power of end consumers is increased. On the other hand, decision makers in critical businesses, for example, hospitals, can be strengthened as well. Above all, the MIoT components facts label contributes to greater transparency and thus increases trust in MIoT devices, the manufacturers and the technologies themselves. To achieve a labeling system for technology and to encourage manufacturers to participate, the government is in charge of establishing incentives and / or regulations, as it can be observed in the food industry. In the following section, two specific MIoT devices have been examined. The focus of the examination is on security in order to emphasize the relevance of the previous suggestions.

## VI. Security Testing of Ultrasonic Scanning Equipment

In our previous work [1] we concluded that common security guidelines for Medical IoT devices are needed to build the resilience necessary to provide a safe and secure environment for patients in the long term. But is a need for such guidelines and recommendations warranted? To answer this question, we monitored the connections of two mobile ultrasonic scanners. Analyzing only two MIoT devices does not allow drawing conclusions on how security is handled in the MIoT industry as a whole. However, as it is already laid out in [1] other entities did take a look at a larger number of devices and deduced that many MIoT devices lack basic security features. This section is meant to see if those results are still relevant for up-to-date products currently sold on the market.

Both scanners require smartphones for operation. On each smartphone, the respective app needs to be installed. These apps allow connecting to the scanner and provide additional functionalities such as

- saving previous scans,
- creating patient records,
- live video conferencing whilst sharing the image of the ultrasonic scanner,
- synchronizing patient records with the cloud of the manufacturer or
- sharing patient records through the cloud.

The scanners are multi-purpose ultrasonic imaging systems. They allow the examination of different organs of the human body, such as the abdomen, bladder, lung or prostate. One product uses a WiFi connection, while the other requires a wires USB Type-C connection to communicate with the corresponding smartphone app.

### A. The Security Test Setup

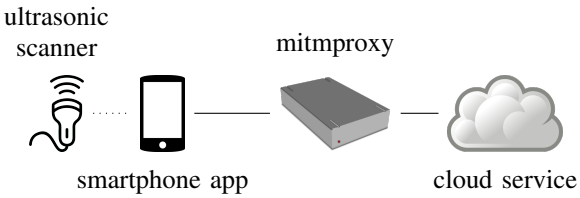


Figure 2. Abstract structure how app traffic is intercepted

The apps of both scanners require the user to log in with an account at the respective cloud service. A connection to the cloud services is mandatory to use the products. Monitoring the connection between the smartphone and the cloud service is therefore of interest in order to gain information about how connections are being handled and what type of information is being sent.

The smartphone used for testing was a rooted Android device. For intercepting the traffic between the smartphone and the cloud services, the software mitmproxy [26] has been set up. The traffic can be decrypted on the fly by installing the root certificate generated by mitmproxy on the smartphone as a system-level certificate. The traffic of the scanner app is being redirected towards the proxy by leveraging the firewall rules of the smartphone. A simplified structure of how the traffic is intercepted can be seen in Figure 2. To ensure that any outgoing connections can be attributed correctly, only traffic from and towards the respective app is being redirected to the mitmproxy software.

### B. Pitfalls and Limitation During Testing

Both tested devices and apps presented certain challenges when trying to intercept their communications. In the following section, these will be presented to give an understanding

of the limitations of the security tests within the scope of this specific work.

*1) Communication Interfaces:* Each scanner uses a different way to establish a connection with the smartphone. One scanner opens up a WiFi access point. The respective smartphone needs to connect to that. The other scanner uses a wired USB Type-C connection to exchange data with the smartphone. Both ways put certain restrictions on the means of how the connections can be monitored.

The wireless scanner reserves the WiFi connection for the data exchange with the smartphone. A simultaneous connection with the cloud services is therefore only possible by using the mobile broadband connection of the smartphone. Hence, it was tried to build a reverse tethering connection between the smartphone and the device where the mitmproxy software is running [27]. This approach came with its own issues. Since the software used generates the reverse tethering connection by tunneling all network traffic through a Virtual Private Network (VPN) client towards the proxy device, all network communication is forced to go through this proxy computer. As a result, the app cannot communicate with the scanner while the reverse tethering connection is active. No signals can be exchanged even if the wireless device is connected to the smartphone via WiFi.

Due to these constraints, it was only possible to evaluate the connections made by the app itself. Connections made while using the wireless scanner were not the subject of the evaluation.

*2) Root Detection:* The scanner, which uses the wired connection, allows for a simultaneous connection of the smartphone with the computer where the mitmproxy software is running in order to intercept the traffic. However, this device puts mechanisms in place to detect if the app is running on a rooted smartphone. If the app detects that the smartphone has root access enabled, it then simply refuses to start. Extra steps had to be taken to trick the scanner app into accepting the rooted environment. After hiding the root privileges, the app successfully started. Still getting past the app's login screen was not possible, even with all these modifications in place. This only allowed inspecting connections made right after first starting the app, as well as authentication attempts made when trying to use login credentials. Rooting the device was required to install the TLS certificate of mitmproxy as a system-level certificate, which allows the inspection of TLS-encrypted traffic. Decrypting the TLS traffic on a non-rooted device was not possible.

### C. Results of the Traffic Monitoring

All connections captured were secured using Transport Layer Security (TLS) 1.2 or higher. No plaintext communication between the manufacturers' apps and cloud services was discovered.

The smartphone app of the wireless scanner only connected to two different URLs:

- https://cloud.-manufacturer-.com and
- https://*.amazonaws.com.

Taking a look at the second domain reveals that the corresponding IP address belongs to the Amazon Web Services (AWS) platform. The entire cloud service for the wireless scanning system is therefore hosted on servers belonging to the company Amazon. The IP addresses can be assigned to the city of Montreal, Quebec, Canada, according to the service IP2Location [28].

On the wired ultrasonic scanning system, significantly more communication activity can be seen. After first starting the app, connection attempts to the following URLs can be observed:

- https://firebase-settings.crashlytics.com
- https://firebaseinstallations.googleapis.com
- https://crashlyticsreports-pa.googleapis.com
- https://clientstream.launchdarkly.com
- https://mobile.launchdarkly.com
- https://firehose.us-east-1.amazonaws.com
- https://cdn-settings.segment.com

The first three URLs listed belong to the Firebase product provided by the company Google. The connections captured infer that the Firebase cloud service is mainly used to process application-related logging events, such as crash reports. A report sent to Firebase contains additional meta data besides the error message created by the application. The metadata consists, among other things, of the build number of the app, the smartphone model, the smartphone fingerprint, the built-in chipset, the language of the operating system, the manufacturer name and the operating system version.

The next two URLs belong to Launchdarkly. Launchdarkly is a feature management platform for mobile app development. It allows the developer to enable or disable certain features through an online portal without needing to redeploy or update the application. The app is told by the Launchdarkly server, whose features are supposed to be enabled or displayed. A regular synchronization mechanism between smartphone and server is therefore leveraged. It should be mentioned that similar metadata to what is sent to the Google Firebase service is sent to the Launchdarkly servers. The IP addresses of Launchdarkly suggest that their servers are located in the US and are part of the AWS infrastructure.

Amazon Kinesis Data Firehose is a platform by Amazon that allows data streams of high volumes and from many sources to be saved and processed within the Amazon infrastructure. This is most likely the service used to store all user information, such as previous scans or patient data. The data streams sent and received during the tests could not be decoded. Therefore, it was not possible to reconstruct what kind of data was actually sent. The servers are located in the US and are part of AWS's infrastructure.

The last service monitored during testing was Segment. Segment is a service dedicated to giving the app developer the ability to collect user analytics data. The focus is on tracking user and device behavior to optimize the user experience. While Firebase and Launchdarkly both collect some user information, the number of parameters sent was far less than what Segment is transferring to their servers. The additional

information is, for example, the screen resolution of the smartphone, active wireless connections, mobile carrier information or the timezone the user is in. Again, the location of the Segment servers is in the US, and they belong to the AWS infrastructure.

### *D. Implications of the Monitoring Results on Security and Privacy*

The security of both ultrasonic scanners can not be sufficiently evaluated to make a qualified statement about their resilience against an attacker. This is either due to technical constraints or obstacles put in place by the developer to restrict tampering with or evaluating the software used with the scanner. It can be said that all connections observed were using at least TLS 1.2 or higher to encrypt the traffic between the apps and the cloud services. This ensures a sufficient level of confidentiality when transferring data from one endpoint to another.

However, in terms of privacy, bigger issues become apparent. In both cases, third parties save and process metadata and patient data directly. None of the vendors tested were hosting their own cloud solution. Instead, both manufacturers decided to use the AWS solution, which is apparently hosted in Canada and the US. The wired ultrasonic scanning system shares information with four different companies, which are not part of the manufacturer or vendor. All data observed was secured via TLS but was not end-to-end encrypted. That means all information stored in the cloud servers is stored in plain text. Patient data is also saved in plain text. This was verified by creating a dummy patient record in the app of the wireless scanning system and monitoring the connection activity. It is worth mentioning that cloud synchronization of patient data is an optional feature of the device.

Storing sensitive patient data in plain text on cloud services can be an issue. Both manufacturers state on their website that they comply with the European GDPR. However, the data is being stored on foreign servers in plain text. Therefore, the data could be accessed by foreign entities or agencies. Additionally, every actor with access to the cloud storage could read and manipulate any data they want. In both cases, the manufacturer of the ultrasonic scanner, as well as Amazon, have access to the medical data provided to them by their customers. This can be a problem if customers want to ensure a high level of privacy for their patients. The customer must trust the vendor or service provider to handle the information given with absolute discretion. Misuse of the data stored can not be prevented on a technical level. It is up to the service provider to adhere to the contractual agreements. Furthermore, the service provider needs to ensure that their infrastructure has state-of-the-art IT defense mechanisms in place to prevent cyber attacks. In a worst-case scenario, a security breach at a vendor could lead to a data leak of all customers.

But patient data is not the only information transmitted to third parties. In Section VI-C it was shown that additional metadata is being sent to Google, Launchdarkly and Segment. These companies are able to see what equipment was used at a certain time in a specific location. They might even be able to retrace usage statistics of employees handling these devices. So, not only is information about patients given to third parties, but it is also plausible to argue that employees' privacy using these scanners might be compromised.

In conclusion, the customer needs to trust that all parties linked to these ultrasonic scanners handle the data given to them responsibly. No technical precautions have been put in place to prevent misuse of the given data. Given the sensitivity of the handled data, better security mechanisms can be expected from the manufacturers in question.

## VII. Outlook

As presented in this work, it is applicable that many efforts will be spent on future security topics, e.g., architectures and processes, starting with best practices for manufacturers. Trustworthy security, safety and trust begin not by signing contracts, e.g., Service Level Agreements (SLA). The trust root starts long before. Politicians and official authorities should consider the derived proposed labeling concepts from the food industry. Of course, those labeling concepts require further research and broad consensus among manufacturers and global technology consortiums. But as we all know, it is possible to agree on labeling and enclosed concepts that provide more transparency for consumers and additionally strengthen safety, security and trust. The National Institute of Standards and Technology (NIST) is already discussing labeling IoT products targeting mostly security-related aims [29].

Research already provides different processes, methods and models that can be used to realize a more secure, safe and trustworthy technological evolution; for example, the process described by Roots of Trust (RoT) [3] is a promising and practical way to achieve absolute trust in a hyper-stakeholder environment targeting manufacturers from the first breath up to the retailers. Bringing the roots of trust into action requires a non-editable approach to audit and trace. A promising technological fundament would be distributed ledger technology to fulfill the required needs. Actual Blockchain-enhanced RoT solutions are already discussed [30], [31]. Another well-promising enhanced version of the "roots of trust" is the "hardware roots of trust" to validate and ensure trust in hardware components. Also, this approach is being researched by Javaid et al. [32]. With the mentioned RoT processes, it would also be relatively easy to accurately define a best-before-inspection date, which can be, for now, only roughly estimated.

Unquestionably, all the above-mentioned suggestions are worth further exploration to foster security, safety and trust in the IoT domain. This paper should not only summarize already existing efforts. Instead, it is intended to present a (Medical) IoT labeling approach and a new paradigm that seems worth focusing on.

## VIII. Conclusion

In this paper, we pointed out that while advisories, guidelines and certain regulations for common IT networks exist, the Medical IoT sector still severely lacks these documents and frameworks. This has the potential to become a severe issue in the future since the amount of IoT devices in operation is rapidly growing, and the data processed is very sensitive information which requires robust protection mechanisms.

To provide guidance for stakeholders and authorities, we proposed an evaluation system to help actors within the healthcare sector. This methodology aims to identify the current Medical IoT security posture. Additionally, this maturity model can be used to understand which steps are necessary to bring the IT security of the infrastructure in question to the next level.

Furthermore, a labeling system for Medical IoT devices was proposed. With such a system, stakeholders should be able to get an overview of the key facts and components of a MIoT system to ascertain the risks and benefits it provides. With that information, decision-makers can manage risk more reliable and faster. However, such a system needs to be standardized. It is the responsibility of governments and regulatory bodies to define the rules for creating such a label to guarantee the sufficiency of the values included and ease of use for the stakeholders.

Finally, two Medical IoT devices were subjected to a basic security test. This test showed that for the connections of the IoT devices to their respective cloud services, sufficient security mechanisms had been put in place. However, in terms of privacy and confidentiality of patient data, it is not clear to the consumer or stakeholder what parties are involved to provide the services. Since the security posture between different parties can vary significantly, it is misleading to think that the security of the IoT device only depends on the vendor or manufacturer.

That is why it is essential for stakeholders to have the tools available to assess the security of their networks and to have a concise overview of the components and parties involved in providing a Medical IoT service.

## IX. Acknowledgment

This research is funded as part of recently granted 5G4Healthcare project by the German Federal Ministry for Digital and Transport within the 5x5G Initiative.

## References

[1] M. Gleißner, J. Dotzler, J. Hartig, A. Aßmuth, C. Bulitta, and S. Hamm, "It security of cloud services and iot devices in healthcare," in *CLOUD COMPUTING 2021*, B. Duncan, Y. W. Lee, and M. Popescu, Eds. Wilmington, DE, USA: IARIA, 2021, pp. 1–7.

[2] S. Dahmen-Lhuissier, "Etsi - technologies - 5G," 2022. [Online]. Available: https://www.etsi.org/technologies/5g?tmpl=component&jjj=1642854003450 [retrieved: 2022.12.15].

[3] National Institute of Standards and Technology, "roots of trust," 2022. [Online]. Available: https://csrc.nist.gov/glossary/term/roots_of_trust[retrieved:2022.12.15] [retrieved: 2022.04.11].

[4] ITU Radiocommunication Sector, "Minimum requirements related totechnical performance for IMT-2020 radio interface(s)," ITU Radiocommunication Sector, Nov. 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf [retrieved: 2022.12.15].

[5] Bundesministerium für Bildung und Forschung, "Industrie 4.0 [industry 4.0]," Jan. 2016. [Online]. Available: https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/industrie-4-0/industrie-4-0.html [retrieved: 2022.12.15].

[6] Harvard University, "Made in china 2025 explained," 2022. [Online]. Available: https://projects.iq.harvard.edu/innovation/made-china-2025-explained [retrieved: 2022.12.15].

[7] E. Y. Nakagawa, P. O. Antonino, F. Schnicke, R. Capilla, T. Kuhn, and P. Liggesmeyer, "Industry 4.0 reference architectures: State of the art and future trends," *Computers & Industrial Engineering*, vol. 156, p. 107241, 2021.

[8] B. Mazon-Olivo and A. Pan, "Internet of things: State-of-the-art, computing paradigms and reference architectures," *IEEE Latin America Transactions*, vol. 20, no. 1, pp. 49–63, 2022.

[9] R. Heidel, M. Hoffmeister, M. Hankel, and U. Döbrich, Eds., *Industrie 4.0: The reference architecture model RAMI 4.0 and the Industrie 4.0 component*, ser. Beuth Innovation. Berlin and Wien and Zürich and Berlin and Offenbach: Beuth Verlag and VDE Verlag, 2019.

[10] Y. Lu, K. C. Morris, and S. Frechette, "Current standards landscape for smart manufacturing systems," Feb. 2016.

[11] Juxtology, "Iot: Architecture." [Online]. Available: https://www.m2mology.com/iot-transformation/iot-world-forum/ [retrieved: 2022.12.15].

[12] IoT European Large-Scale Pilots Programme, "Create-IoT." [Online]. Available: https://european-iot-pilots.eu/create-iot/consortium/ [retrieved: 2022.12.15].

[13] National Institute of Standards and Technology, "Roots of trust." [Online]. Available: https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust [retrieved: 2022.12.15].

[14] IoT Security Foundation, "Device secure boot." [Online]. Available: https://www.iotsecurityfoundation.org/best-practice-guide-articles/device-secure-boot/ [retrieved: 2022.12.15].

[15] Bundesamt für Sicherheit in der Informationstechnik, "SYS.4.3 Eingebettete Systeme [SYS.4.3 Embedded Systems]," 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/07_SYS_IT_Systeme/SYS_4_3_Eingebettete_Systeme_Edition_2021.pdf [retrieved: 2022.12.15].

[16] Bundesamt für Sicherheit in der Informationstechnik, "Sys.4.4: Allgemeines iot-gerät," 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/07_SYS_IT_Systeme/SYS_4_4_Allgemeines_IoT_Geraet_Edition_2021.pdf [retrieved: 2022.12.15].

[17] European Union, "Regulation (eu) 2016/679 of the european parliament and of the council," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3265-1-1 [retrieved: 2022.12.15].

[18] Public Health, "Factsheet - european health data space (ehds)," 2022. [Online]. Available: https://ec.europa.eu/health/latest-updates/factsheet-european-health-data-space-ehds-2022-05-03_en [retrieved: 2022.12.15].

[19] European Union Agency for Cybersecurity, "Baseline security recommendations for IoT," Nov. 2017, [retrieved: 2022.12.15].

[20] BioSpace, "IoT in healthcare market to reach USD 260.75 billion by 2027– reports and data," Jul. 2021. [Online]. Available: https://www.biospace.com/article/iot-in-healthcare-market-to-reach-usd-260-75-billion-by-2027-reports-and-data/ [retrieved: 2022.12.15].

[21] EFQM, "Efqm_model_2020_v2_german_summary: 2. überarbeitete ausgabe," 2021. [Online]. Available: https://mailchi.mp/b505ea74b885/61o67uatr8 [retrieved: 2022.12.15].

[22] Brookfield, "Mapping of iot security recommendations, guidance and standards to the UK's code of practice for consumer IoT security," Oct. 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973928/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018_V2.pdf [retrieved: 2022.12.15].

[23] Avedis Donabedian, "Evaluation the quality of medical care," p. 166–206, 1965. [Online]. Available: https://www.jstor.org/stable/3348969

[24] European Union, "EUR-Lex - 32018r0775 - EN," May 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1568299917869&uri=CELEX:32018R0775 [retrieved: 2022.12.15].

[25] L. Hinterberger, S. Fischer, B. Weber, K. Neubauer, and R. Hackenberg, "Iot device identification and recognition (iotag)," in *CLOUD COMPUTING 2020, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*, 2020, pp. 17–23.

[26] A. Cortesi, M. Hils, and T. Kriechbaumer, "mitmproxy - an interactive HTTPS proxy," 2022. [Online]. Available: https://mitmproxy.org/ [retrieved: 2022.12.15].

[27] R. Vimont, J. Shuali, S. Testa, and A. Aslanyan, "Gnirehtet (v2.5)," 2022. [Online]. Available: https://github.com/Genymobile/gnirehtet [retrieved: 2022.12.15].

[28] IP2Location, "IP address to IP location and proxy information | IP2Location," 2022. [Online]. Available: https://www.ip2location.com/ [retrieved: 2022.12.15].

[29] National Institute of Standards and Technology, "IoT product criteria," Feb. 2022. [Online]. Available: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria [retrieved: 2022.12.15].

[30] *2018 International Conference on Smart Communications and Networking (SmartNets)*. IEEE, 2018.

[31] Elisa Bertino, Dan Lin, and Jorge Lobo, Eds., *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, ser. ACM Conferences. New York, NY: Association for Computing Machinery, 2018. [Online]. Available: http://dl.acm.org/citation.cfm?id=3205977

[32] U. Javaid, M. N. Aman, and B. Sikdar, "Defining trust in IoT environments via distributed remote attestation using blockchain," in *Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*. New York, NY, USA: ACM, 2020.

## APPENDIX

TABLE II. Criteria dimension structure

| Maturity / Criteria | Organisation | Data Management | Authentication System |
|---|---|---|---|
| 1 | • Health facility's management commitment to the implementation of IT security for all IoT devices in the whole healthcare area | • Detailed description of end-to-end-security and cryptographic principles<br>• Utilize crypto coprocessors for key creation and storage<br>• All products related to web servers have their HTTP trace and trace methods disabled | • No default credentials for Medical IoT devices<br>• No use of any function by unauthorized user or guest users incl. patients (also changing credentials)<br>• Applications operated at the lowest privilege level possible |
| 2 | • Definition of basic objectives, scope, roles and tasks regarding IT security of Medical IoT devices<br>• Determining contractual clauses with Medical IoT suppliers about IT security | • Encrypted data on application layer<br>• All communications keys are stored with industry standards (e.g., FIPS 140)<br>• All communication ports (e.g., USB, RS232) only communicate with authorized and authenticated entities<br>• Minimized sharing principle of resources | • Different secret keys for each Medical IoT or product family<br>• Complex password management (no blanks, no containing user account name, etc.) for all Medical IoT devices |
| 3 | • Definition of all Medical IoT processes including risk level<br>• All products contain a unique and tamper-resistent device identifier (e.g., chip serial number) | • Key management incl. generation, distribution, storage and maintenance<br>• Utilize trusted platform modules (TPM) and hardware security modules (HSM)<br>• Communication protocols are at most secure version (e.g., Bluetooth 4.2 rather than 4.0) | • No hard coded passwords in IoT software code<br>• 2-Factor authentication for all Medical IoT devices |
| 4 | • Training for medical staff about IT security of IoT devices<br>• All OS non-essential services have been removed from product's software | • Storage of sensitive data in hardware (not software)<br>• Only use secure boot methods | • Multi factor authentication or certificates for all Medical IoT devices<br>• Secure mechanism for updated credentials (fixed time intervals) for all medical stuff |
| 5 | • Manufacturers consider compliance with ISO 30111 for vulnerability report handling | • Encrypt data parameters using a Direct Acess Recovery (DAR) encryption key stored I a physically locked module<br>• Using Root of Trust (certificates, signing keys) | • No secret credentials left in application code of Medical IoT devices<br>• Biometric authentication for all medical staff |

TABLE III. Criteria dimension process

| Maturity / Criteria | Updates | Malfunction Management | Usability |
|---|---|---|---|
| 1 | • Regular updates of security measures of all Medical IoT devices<br>• User notification when updates and patches modify user-configured preferences, security and privacy settings | • Defined use of error handlers<br>• Generic error messages and use of custom error pages<br>• Enable restore secure state after security breach<br>• Runtime Protection mechanism | • Basic training for medical staff is done |
| 2 | • Agile and prompt response to new security or other flaws of IT in the health facility<br>• Validation of authenticity and integrity of all updates (e.g., signing certificate)<br>• Restore secure state (if update was not successful or occurred) | • Log all authentication attempts and failures of the medical staff<br>• Log all access control failures of the medical staff<br>• Log all apparent tampering events | • Advanced training for staff is done |
| 3 | • Automated update process for all Medical IoT devices<br>• Use of libraries that are actively maintained and supported | • Defined bug reporting system from Medical IoT suppliers<br>• Log all backend TLS connection failures<br>• Automated alerting system for tampering events | • Regular training sessions incl. innovations are taught for medical staff |
| 4 | • Defined limitation of device functionality for all Medical IoT devices after security support period ends (e.g., remote control)<br>• Backward compatibility of updates (compatible with previous versions) for all Medical IoT devices | • Mechanisms for self-diagnosis and self-repair for all Medical IoT devices | • No training necessary for usage or all medical staff is trained for usage |
| 5 | • Updates include cryptographic checks and cipher suites<br>• Complete end-to-life update strategy for all Medical IoT devices incl. awareness of potential risks beyond its expected expiry date | • Participation in information sharing platform to report vulnerabilities and current cyber threats of Medical IoT devices | • No training necessary for usage or all medical staff is trained for usage incl. IT security handling |

TABLE IV. Criteria dimension outcome

| Maturity / Criteria | Costs for IT Security | Downtime reg. criticality | Failsafe | Threats and attacks |
|---|---|---|---|---|
| 1 | • Less than 1 % of the complete health facility budget | • All Medical IoT devices with low criticality have a max. downtime of 3 days | • Failure affects the whole system / the whole Medical IoT device / the whole IoT product family | • there were less than 25 security-related events (e.g., threats, attacks) last year in the health facility |
| 2 | • Less than 2 % of the complete health facility budget | • All Medical IoT devices with low criticality have a max. downtime of 24 hours | • Failure affects parts of the system / the whole Medical IoT device / the whole IoT product family | • there were less than 20 security-related events (e.g., threats, attacks) last year in the health facility |
| 3 | • Less than 4 % of the complete health facility budget | • All Medical IoT devices with medium criticality have a max. downtime of 3 days | • Failure affects the availability of operation or use of the system / the whole Medical IoT device / the whole IoT product family | • there were less than 15 security-related events (e.g., threats, attacks) last year in the health facility |
| 4 | • Less than 6 % of the complete health facility budget | • All Medical IoT devices with medium criticality have a max. downtime of 24 hours | • Failure has no effect on the medical operation (no human damage possible) | • there were less than 10 security-related events (e.g., threats, attacks) last year in the health facility |
| 5 | • More than 8 % of the complete health facility budget | • All Medical IoT devices with high criticality have a max. downtime of 24 hours | • Failure has no effect on the operation or use of the whole system / the whole Medical IoT device / the whole IoT product family | • there were less than 5 security-related events (e.g., threats, attacks) last year in the health facility |