Critical software

Building Cybersecurity from Manufacturer to End User

A short roadmap for medical devices manufacturers

In partnership with:

FSQ EXPERTS FUNCTIONAL SAFETY & QUALITY EXPERTS GmbH

www.fsq-experts.com

A Rising Threat

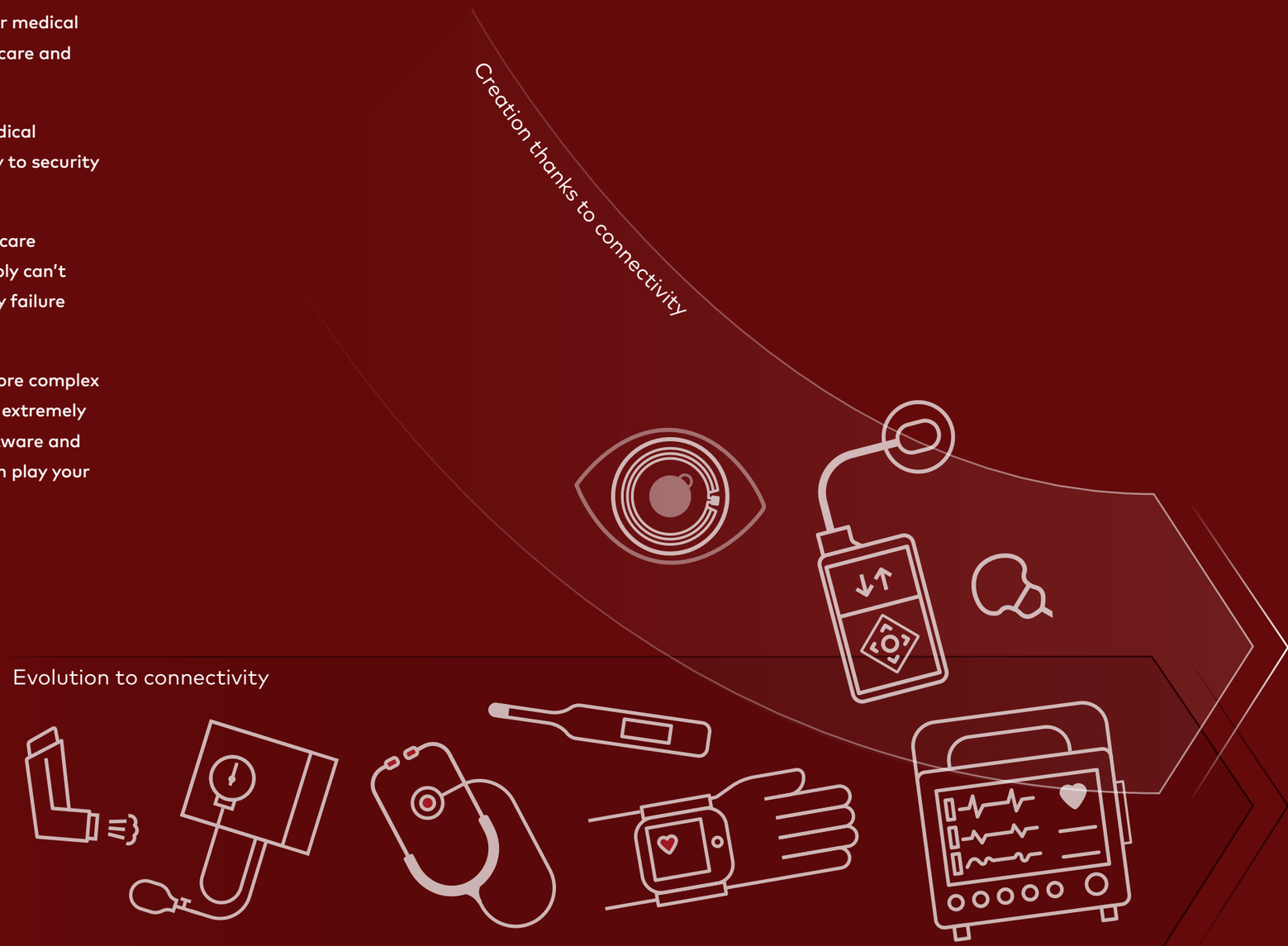
Hearing about new medical devices technology that doesn't include software in one way or another is becoming less and less common. In fact, the industry has taken things a step further, and medical devices are increasingly becoming connected to the internet, hospital networks, and other medical devices in the ever-expanding Internet of Things. The goal is, of course, to improve healthcare and help healthcare providers treat patients.

However, these features come with their own risks, specifically cybersecurity threats. Medical devices aren't different from other computer systems when it comes to their vulnerability to security breaches, and this can easily impact the safety and effectiveness of the device itself.

Thus it isn't surprising that news about cybersecurity breaches and attacks to the healthcare industry is growing considerably. The protection of people, assets and personal data simply can't and mustn't be compromised in this sector, which is why the rising threat of cybersecurity failure concerns manufacturers, governments and healthcare providers alike.

It is expected that cybersecurity threats will increase as more medical devices become more complex and connected, relying more heavily on software. While stopping the threat altogether is extremely hard to achieve, we can still do something to prevent and minimise the risks. Critical Software and FSQ Functional Safety and Quality Experts have come together to show you how you can play your part.

CONNECTED MEDICAL DEVICE EVOLUTION



Cybersecurity in Healthcare

Flying over to the US... Since 2015, the Food and Drugs Administration (FDA for short) and the US Department of Homeland Security have issued warnings about products that threaten patient safety due to their vulnerabilities. Most of these warnings relate to software problems, a growing trend in the industry as healthcare providers rely more on medical devices which employ software.

The impact of the Internet of Things (IoT for short) has meant that medical devices have become a gateway for cybersecurity attacks, given that they're now smarter and have features enabling them to connect wirelessly. Consequently, thanks to the increasing interconnectivity between medical devices and other systems, there's a higher risk of exploitation should the proper cybersecurity measures not be put in place.

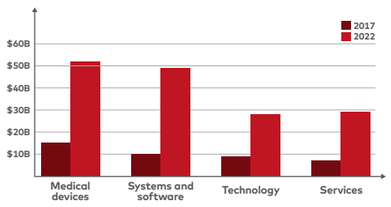


Figure 1 IoMT market expected growth

Not surprisingly, ensuring the security of embedded systems is an issue:

New, connected and embedded systems are being released into markets at such a rapid rate that the impact of these technologies has become unpredictable and, largely, uncontrollable.

Looking at the world map below, there's an evident low growth rate of connected medical devices in the USA, which is due to the fact that this kind of devices were first developed in that country, hence they now have a more mature and stable market. However, it was necessary for the US market to overcome exposure to cybersecurity threats in order to achieve this market stability.

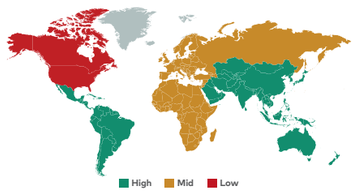


Figure 2 Connected medical device market growth by region (2019-2024)
Source: Mordor Intelligence

The FDA has implemented several measures to try to prevent or minimise the impact of cybersecurity issues. For example, in October 2019, the FDA issued a warning concerning medical devices that were vulnerable to being hacked because they were using a decades-old third-party software. At the time, researchers identified eleven vulnerabilities that would allow anyone to take remote control of a medical device, jeopardising patients' safety and data privacy. It's worth noting that these attacks are becoming so complex and well-designed that FDA members are struggling to create a comprehensive list of all affected devices.

Contrary to the USA, the growth rate of connected medical devices in Europe and Asia is high and has been increasing since 2019. It is expected that European countries face the same problems that the USA faced as the number of connected devices grows. Due to the delay on European manufacturers in dealing with cybersecurity threats in a proactive way, the FDA is prohibiting some "European" medical devices from entering the American market in order to protect the market's integrity.

This interconnectivity leaves medical devices vulnerable to security breaches. If hackers successfully tamper with these systems, patient safety is at risk, leading us to an important aspect to consider: the need to learn more about the hacking community in order to anticipate security issues, as hackers seem to move as fast as or even faster than the MD industry develops and refactors their products.

From 2015 to 2019, the USA was hackers' main focal point but, unfortunately, many of these cyberattacks now tend to cross borders and thus have a global impact.

From insulin pumps to cardiac implants like pacemakers, from imaging and diagnostic devices to data management systems – all were either the target of cybersecurity attacks or identified as presenting serious vulnerabilities.

The consequences of these attacks aren't surprising: device malfunction is the main concern, closely followed by personal data breaches and the inability to access data from medical devices.

Back in 2015, the FDA reported a case relating to the software code in infusion pumps which allowed an unauthorized user to remotely interfere with the pump's functioning, including modifying the dosage it delivers. More recently, the FDA alerted that communication software used in medical devices could be controlled remotely, causing denial of service and patient data leaks.

A recent Vanderbilt study found that there were as many as 36 additional deaths per 10,000 heart attacks occurring annually at the hospitals inspected, these caused by cybersecurity attacks which caused delays in treatments. It was found that it took an additional 2.7 minutes for suspected heart attack patients to receive an electrocardiogram following these cyberattacks.

One might wonder why medical devices are in a more vulnerable position when it comes to cybersecurity. Here are a few reasons why that might happen:

Equipment updates

Corrections can take a long time to be put in place so that the devices are once again compliant. Additionally, it's difficult to find a convenient time to apply these updates, as many hospitals are still running legacy operating systems that are no longer supported.

Lack of updates

Products that no longer receive updates provide an entry point for hackers since they no longer correct cybersecurity issues, putting the patients' safety and service availability at risk.

Medical device refitting

Many of these devices were refitted to become networked so that real-time data sharing could be leveraged. This data would be shared with relevant systems for process automation and can be remotely managed by vendors.

Interconnectivity

There can be adverse effects as a result of a hacker breaching into a hospital's internal network, such as personal data leakage and tampering with device functionality.

Undoubtedly, it's crucial that all entities are on the same page when it comes to these issues so they can find solutions and keep medical devices healthy and safe. But how do we do this? We need not go further than from having common regulations that apply to the medical device industry as a whole.

The Role of Regulation

REGULATION

Ensuring that everyone involved in the medical devices' lifecycle collaborates and remains vigilant is crucial when tackling cybersecurity issues. And that begins with regulation.

The first step to minimise risks is prevention, with proper regulation being the starting point to make this happen. The table on the right shows examples of existing regulations and guidelines concerning cybersecurity. As we can see, the FDA has taken a strong stance when it comes to publishing guidelines since 2005. In contrast, the European authorities took a while to publish theirs, with the first guidelines being published only from 2010.

Additionally, the GDPR [(EU) 2016/679] and NIS Directive [(EU) 2016/1148) were released in 2016, and the Cybersecurity Act – the first EU-wide cybersecurity certification framework – was approved by the European Parliament in 2019.

As these guidelines are relatively recent, manufacturers may be struggling with inconsistencies and lack of awareness. They may lack specific risk analysis or not be aware of some cybersecurity requirements, fail to know some of these requirements entirely or to include them on the devices' design and development processes. Additionally, the lack of guidelines or recommendations specifically for IT cybersecurity is also something to look out for.

Regulation is the way to reassure healthcare providers and patients that the devices they are using are trustworthy and will not endanger their safety, regardless of the manufacturer. Regulation standardises the rules for manufacturers, providing greater security and confidence in using medical devices produced by certain manufacturers.

For example, it is compulsory for medical devices in the European Market to bear a CE mark, which is helpful as leverage to enter other markets that consider the CE mark as having a guarantee of quality. With the MDR entering into play, the CE mark will go one step forward in regulating the European market.

Document title	Publisher	Publication date
Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software – guidance for industry	**FDA**	**January 2005**
Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices – guidance for industry and FDA staff	**FDA**	**May 2005**
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – guidance for industry and FDA staff (supplement of the two documents above)	**FDA**	**October 2014**
Postmarket Management of Cybersecurity in Medical Devices – guidance for industry and FDA staff	**FDA**	**December 2016**
UL 2900-2-1 – Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network-Connectable Components of Healthcare and Wellness Systems	**UL**	**September 2017**
IT Security Guidelines for Medical Devices	**TÜV, Siemens, Johner Institut**	**September 2018**
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – draft guidance for industry and FDA staff (update of the Dec. 2016 FDA document)	**FDA**	**October 2018**
Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices	**IMDRF**	**October 2018**
ANSM's Guidelines – Cybersecurity of Medical Devices Integrating Software During Their Lifecycle	**ANSM (France)**	**July 2019**
Medical Device Cybersecurity Guidance for Industry	**TGA (Austria, Health Department)**	**July 2019**
IEC 62443-4-2: Technical Security Requirements for Industrial Automation and Control Systems' Components	**Used by TÜV to assess MD cybersecurity**	**December 2019**
MDCG 2019-16 – Guidance on Cybersecurity for Medical Devices	**European Commission, GROW.R.2.DIR**	**January 2020**
MDR – Medical Devices Regulation	**European Parliament and Council**	**From April 2017 to be implemented in May 2020**

The Role of Manufacturers

There are still certain myths surrounding cybersecurity in the medical devices community. One of them being that cybersecurity may still be optional, since there is no harmonised standard offering guidance on this topic. Another outdated belief is to assign responsibilities exclusively to two parties: the software development team on the manufacturer's side, and the IT team at the side of the healthcare facility, where the devices are being used. Cybersecurity is a complex topic and needs a much more holistic approach than this.

Based on our experience supporting medical devices manufacturers, FSQ Experts and Critical Software have five practical tips for you:

1. Cybersecurity is multi-disciplinary

Due to its multi-disciplinary character, cybersecurity needs to be anchored to key processes in your organisation, for instance quality and complaint management. Moreover, during the development cycle, it should be integrated into already established activities, such as usability engineering, risk management and - of course - software development.

Our favorite approach is to address safety, security and human factors combined using as central documentation tool your risk management file.

Companies who have a well-established risk management process can implement and document safety, security and usability requirements in a more efficient way.

When it comes to methods and tools there are plenty of options. One can also learn from other industries, where the cybersecurity is already mature. One practical suggestion to the development team is to perform a Threat Assessment and Remediation Analysis (TARA) and incorporate these outcomes directly into the risk assessment in the risk management file (according to the standard DIN EN ISO 14971).

2. A technical approach

On the other hand, a more technical approach to tackling cybersecurity issues can be broken down into three layers. As some cybersecurity vulnerabilities can come from vague corporate policies, processes and, ultimately, technologies, the success of this structure is due to the enforcement of security policies across the company, from the top down. However, this structure isn't always easy to achieve for every organisation, and our approach bears this in mind. The three layers can exist separately and independently from one another, although they tend to work better together. Based on all these layers or on a combination of them, the foundations for the development of secure embedded systems can be set.

1. Corporate Information Security Management System. Focuses on supporting systems, as well as overall information security.

2. Secure Development Process Definition. Zooms in on the secure development process that needs to be defined and followed to ensure security later on.

3. Secure Embedded System Implementation. Looks at the practical side of creating an embedded cybersecurity solution.

In order to implement each of the three layers, elements of each one must be understood correctly:

• Corporate Information Security Management System (ISMS):

- Implementation of a full ISMS as a part of a complete management system
- Gap analysis
- Definition of security processes
- Day-to-day management focused on continuous improvement

• Secure Development Process Definition:

- Gap identification for a secure development process
- Secure development process definition
- Security management plan

• Secure Embedded System Implementation

- Secure system development as a general activity where experts support internal teams
- Security introduction in legacy systems through the addition of a safety layer
- Analysis of security threats and vulnerabilities
- Independent risk analysis
- Specific security analysis based on pre-defined checklists and security goals
- Requirements review
- Design review
- Software source code review
- Test case review
- Penetration test specification and execution

Although this approach helps set the foundations for the development of secure embedded systems, it's important to be aware that security threats are constantly evolving and generally faster than security barriers, thus achieving a secure system is an ongoing effort. Adapting processes and methodologies will be required, as will updating the system itself when new threats are detected.

3. Building better medical devices by knowing the users

Unlike other safety-critical products, medical devices have a wide range of users with different skills and backgrounds. These users can range from highly trained healthcare professionals, to patients, service technicians and even the cleaning staff.

It's important to understand who will use the device to make sure that it is operated correctly, safely and securely.

This is valid for any kind of misuse, including behaviour that may lead to potential unknown vulnerabilities of the device. Additionally, it's important to understand the context on which the device will be used: for example, there are many connected medical devices nowadays which are operated directly by the patient, or a relative of theirs, at home. One cannot expect that such private environment meets the same security levels as a healthcare facility.

Training is not enough in these situations. It is recommended that user-centric methods are applied during development of medical devices, such as design thinking. Users are subject-matter experts for the tasks where they interact with the medical device, so their input offers important details about user needs, context and foreseeable misuse. When compared to a reactive approach based mainly on post-market feedback, this way of developing devices has many advantages in terms of both safety and security implementation.

4. The importance of a strong partnership

Successfully implementing cybersecurity requires a strong partnership between the manufacturer and the healthcare institutions, as the responsibilities of each must be well-defined. Transparency can only be achieved when both parties co-operate closely while performing post-market surveillance activities.

One good source of information is the FDA recommendation for Postmarket Management of Cybersecurity in Medical Devices, which offers a more detailed overview than the Medical Device Regulation (MDR 2017/745). When it comes to reporting cybersecurity incidents, it is desirable to use a common legislative approach and encourage better standardisation between different regions, though this is only possible when cybersecurity is recognised as a main discipline in the healthcare industry.

5. Communication is key

Communicating with the authorities and stakeholders involved in the medical devices' lifecycle is important.

In the US, as we have mentioned, the FDA frequently shares a list of vulnerabilities on medical devices. In Europe, the new Medical Devices Regulation recommends that medical devices should be monitored for critical vulnerabilities, which means that manufacturers need to clearly communicate the end of life and end of support dates when devices are provided and implemented. Safety, security and effectiveness are integral design features of security mechanisms, so they must be considered by manufacturers from the early stages of development, manufacturing and throughout the device's whole lifecycle, including post- market.

On the other hand, manufacturers must provide clear usage instructions, which should include IT security features and configuration, guidelines for the operating environment IT security control, product specification, compatibility, recommended IT security measures and IT environment configuration (e.g. internet traffic monitoring). This is more than just training. Evaluating possible vulnerabilities in cybersecurity that could be caused by reasonably foreseeable misuse is crucial but it's also important to weigh these products' benefits against the risks posed by identified threats. It's rarely advantageous to entirely remove or disable vulnerable products, even though this eliminates the risk altogether.

Conclusion

According to a Deloitte study, in 2018, less than half of all medical devices had connectivity features. However, by 2023, 68% of all medical devices are forecast to be connected into the Internet of Things.

Although we are starting to see a clearer regulatory framework for introducing medical devices to the market, cybersecurity practices are still very inconsistent amongst manufacturers. It's important to bear in mind that everyone involved is responsible for the good functioning of these devices, including the users themselves, thus taking a proactive stance is crucial to avoid recalls or potentially cause harm to patients. This can be avoided if cybersecurity is present throughout the whole lifecycle of the device, instead of being a measure taken only once the threat has been identified.

In the end, it's essential for medical devices manufacturers to implement a solid post-market cybersecurity surveillance programme to address evolving risks. This programme should ensure that the device is operated in the intended environment, that knowledge and information of cybersecurity vulnerabilities and threats are shared and disseminated across multiple sectors. This should also include vulnerability remediation and incident response.

About FSQ Experts GmbH

FSQ Experts provides expert advice in the medical device field, particularly in the areas of quality management, systems engineering and regulatory affairs.

We work together with our partners and clients to help deliver high quality medical devices to market, with a focus on ensuring the most robust cybersecurity is also in place to protect the safety and privacy of patients and healthcare professionals.

About Critical Software

Critical Software provides systems and software services for safety, mission and business-critical applications. We work closely with our clients, helping them to meet the most demanding standards for performance reliability.

We were founded in 1998, with NASA our very first client. Today we work across many international industries and have offices across the globe.

We've tested and developed applications and software in markets that are highly regulated, complying with demanding international standards to a high-level of dependability. We have over twenty years' experience in embedded systems development and quality assurance, certified against international standards including ISO 13485:2016 and ISO 9001:2015.

We are CMMI Maturity Level 5 rated.
For a list of our certifications & standards visit our website.

criticalsoftware.com
info@criticalsoftware.com