Security for medical devices - a shared responsibility

D-45345-2021

At Dräger, we develop technology for life. This technology is subject to constant change and the digitization of healthcare is advancing rapidly. We are helping to shape this change in order to make digital technology have a positive impact for patient care and hospital economics.

1. INTRODUCTION

At Dräger, we develop technology for life. This technology is subject to constant change and the digitization of healthcare is advancing rapidly. We are helping to shape this change in order to make digital technology have a positive impact for patient care and hospital economics. Today and even more so in the future, medical devices and systems will be connected to networks to interact with each other, enabling new clinical applications. These new clinical applications include decision-supporting technologies, remote control capabilities or automated processes. However, this needs to happen in a safe and secure network environment in order to safeguard device function and data protection. Hospitals are making massive efforts to secure their networks and manufacturers should contribute to this secure environment by providing products that are resilient to cyber-attacks and can be securely integrated into the hospital's networks. As the cybersecurity threats and risks to internal and external healthcare environments continue to increase, well-established security controls are necessary for adequate protection of patients and patient data.

Medical devices are different from the standard networked devices. They are fixed-function devices designed to perform a specialized task and are optimized to minimize processing cycles and memory usage. Although the level of security required for a medical device varies depending upon the function of the device, all devices must have appropriate security controls in place to protect the device, its data, and the connected patient from cyber-attacks. This is ideally being achieved by building in security from the early stages of product lifecycle using a multifaceted approach with respect to cybersecurity standards and best practices. At Dräger, this multifaceted approach is being deeply integrated in the development processes as well as in the technical controls.

Our medical devices and systems are being developed following current cybersecurity best practices as outlined in this document. This applies to all products currently being developed. This does not necessarily apply to all currently marketed portfolios. For these portfolios please request a MDS2 form from your local sales representative.

This paper will provide you with details on how security is being implemented in the development of our medical devices. Additional information on the security of cloud-based product solutions and services will be provided in a separate paper.

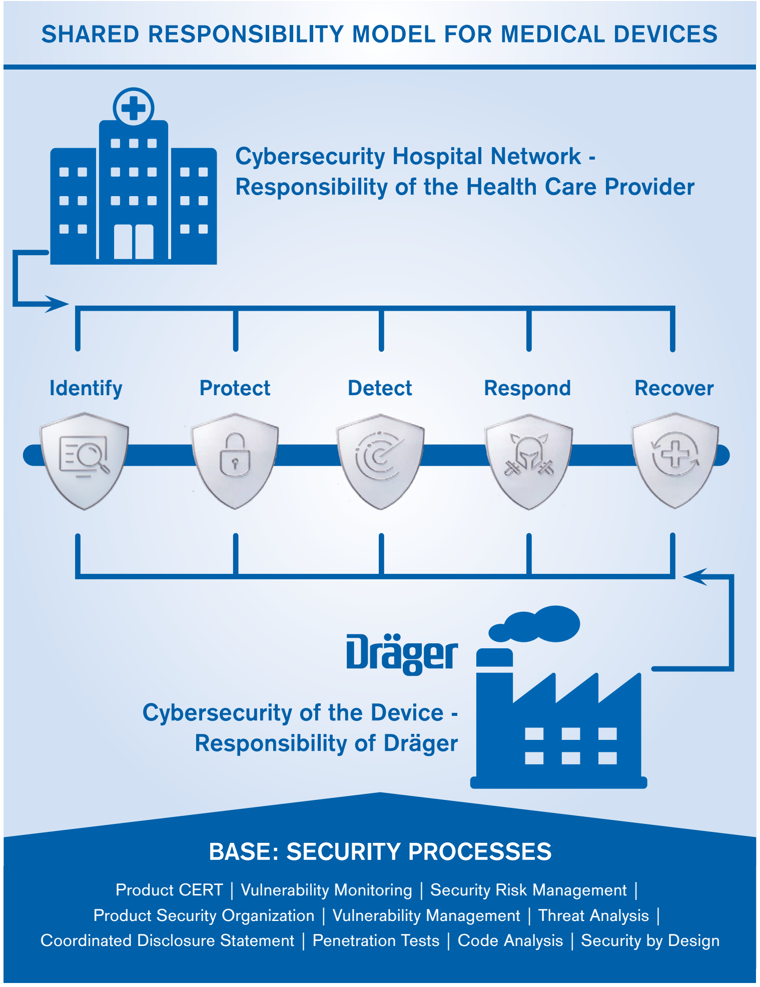
It is our responsibility to make sure that our devices can be securely operated in the hospital network. You, as our customer, are responsible for the security within your hospital network. Therefore, cybersecurity needs to be understood as a shared responsibility and needs to be managed in a joined effort.

2. CYBERSECURITY – A SHARED RESPONSIBILITY

There is no such thing as a "cybersecurity silver bullet." Cybersecurity requires comprehensive administrative, logical, and physical controls in place to protect medical devices, avoid patient harm and financial damage. It is neither a short-term project nor is it once and done but is a continuous, multi-layered process to minimize the risks of threats to medical devices to avoid patient harm.

As healthcare systems become increasingly digital, the security of hospital networks become increasingly important in order to minimize the risk resulting from attacks. Therefore, we at Dräger are aware that hospitals put shields up by adopting cybersecurity best practices in order to protect their networks and their assets. It is our responsibility as a provider of networked medical devices and systems to make sure that our products can be securely integrated into your hospitals' network.

Security Framework. Our multifaceted security strategy can best be described as "Defense-in-Depth." We don't have a single solution or process for cybersecurity, rather we employ a layerbased strategy for the development of defenses throughout our devices and systems. This strategy follows the same cybersecurity best practices more and more hospitals adopt in their security strategies so that you can integrate our devices and systems seamlessly into your networks and security concepts.



SHARED RESPONSIBILITY MODEL FOR MEDICAL DEVICES

Cybersecurity Hospital Network - Responsibility of the Health Care Provider

Cybersecurity of the Device - Responsibility of Dräger

BASE: SECURITY PROCESSES

Product CERT | Vulnerability Monitoring | Security Risk Management | Product Security Organization | Vulnerability Management | Threat Analysis | Coordinated Disclosure Statement | Penetration Tests | Code Analysis | Security by Design

The security best practices framework we follow consists of the following functions:

IDENTIFY

Assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. It enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

PROTECT

Outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

DETECT

Defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

RESPOND

Includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

RECOVER

Supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Shared Responsibility

In order to achieve the most effective protection possible against cyber-attacks, best practice safeguards should ideally be implemented on both sides: the hospital to manage the security of the network and at Dräger for the development of secure networked medical devices and systems. Therefore, cybersecurity becomes a shared responsibility. As a hospital it is your responsibility to integrate medical devices in a secure network environment based on your security policies. Our responsibility as a provider of medical devices and systems is to protect the medical device internals to the perimeter of the medical device to ensure that the hospitals can monitor activity and changes to and from our medical devices. Furthermore, we need to provide you with all information and support you require for the secure implementation into your network environment.

In the following pages we will provide insights into the technical controls, our security organization and our processes along the secure development lifecycle which together form our layer-based approach to secure our medical devices and systems and to make the secure integration into your networks seamless.

3. TECHNICAL CONTROLS

We have implemented numerous technical controls and safeguards into our medical devices to protect them against cyber-attacks and to limit risks. The controls are based on best-practices as outlined in this document for the categories: Identify, Protect, Detect, Respond and Recover.

The software of our medical devices is a closed system that verifies itself upon boot and during normal operation. All executables of the subsystem are validated before manufacturing of the device and the subsystem is locked down to prevent execution of all further executables.

IDENTIFY

We provide you as our customer with all the information you need to identify your assets and the known cyber risks that threaten our medical devices. This information covers:

- A Software Bill of Material (SBOM) that lists all 3rd party software components used in the product.
- Disclosure of security advisories in case new vulnerabilities of the product are found.
- Instructions for Use that describe, among other things, cybersecurity aspects of integrating the device into the customer network.
- Manufacturer Disclosure Statement for Medical Device Security (MDS2) to assist customers in assessing the security-risks associated with the management of medical devices.

PROTECT

We follow a Security-by-Design approach for protecting our medical devices against cyber-threats. The goal of Security-by- Design is to minimize the attack surface that the devices expose. The protection controls are preventive measures to reduce the risk of a device being compromised in the event of an attack. Our technical controls are designed to prevent unauthorized use by denying unauthorized access and by incorporating the principles of “need to know” and “least privilege.” Authentication and authorization controls for medical devices is developed using:

- **Restricted remote access.** This best practice is recommended to restrict any access, especially remote access, for the purpose of limiting the risk of unauthorized and unauthenticated access to the medical device or system.
- **Authenticated access.** Authenticated access is required, and our devices are designed to balance the requirement for secure authentication with the requirement for ease of use to support the workflows in the acute care medicine.
- **Passwords.** Passwords provide the first line of defense against unauthorized access to Dräger devices and systems. Where feasible, strong passwords shall be used.
- **Session timeouts.** When there is no activity for a set period, the session will timeout. This configuration helps to limit the risk of a medical device or system being exposed to unauthorized access. Insufficient session expiration by a medical application, device, or system increases the exposure of other session-based attacks, such as the reuse of a valid session ID or hijack of the associated session. The shorter the session interval is, the less time an attacker has to use the valid session ID.
- **Changing of default passwords.** Default passwords are a pre-configured password for medical devices and software can easily be found on the Internet. Changing a default password can ensure access is protected and restricted to authorized individuals or systems. Such passwords are the default configuration for many existing devices and, if left unchanged, present a serious security risk. Many default passwords are publicly documented and widely available. Default passwords should be changed prior to connecting the devices or systems to a network.
- **Encrypted authentication.** To ensure user IDs and passwords cannot be monitored when coming across the network, encrypted authentication is used on the medical device.

We ensure that only trusted software signed by us can be executed on our medical device by using the following techniques:

- Secure / Trusted boot chain, which is ensuring the integrity of firmware and software running on the medical device. In this way, a medical device can guard against malicious attacks, rootkits, and unauthorized software updates that could happen prior to the operating system (OS) launching. Dräger uses secure boot to keep Dräger medical devices and systems attack resistant. Secure boot detects tampering with boot loaders, operating system kernel and executable files as well as static configuration files by validating their digital signatures.
- Internal encryption key management, including the protection of the keys in an internal secure key store.
- Software integrity, meaning that the code does what it should: is tested, has security features, is robust, and is easy to edit and upgrade without introducing new errors. Software integrity matters to Dräger because it demonstrates the safety, security, and maintainability of our device and system code. Our software integrity is crucial for compliance with coding standards and industry regulations.

Data transfers to and from the devices are protected via the usage of encrypted transport channels and cryptographic checksums. Thus, the confidentiality and integrity of the exchanged data can be ensured and our devices are protected against malicious attacks, data exfiltration, and other security risks.

By omitting unnecessary software components and deactivating all unused network ports, the devices configuration is hardened in order to reduce the attack surface. ”Deny all by default” ensures that undefined ports cannot be used to access the medical device or system. Dräger ensures that open TCP/IP ports are restricted to only allow authorized access and communication.

DETECT

In addition to preventive technical controls that protect a device from attacks, it is important that attempts to compromise a device can be detected. The ability to discover anomalous actions or cybersecurity events in a timely manner is crucial for an effective response in the event of an attack.

Dräger medical devices maintain a Security Event Log that contains all of the security-related events an administrator needs to analyze potential compromises and for forensic evidence. Possible security events include, but are not limited to, authentication events, software installation events, configuration events and network anomalies.

To achieve tamper resistance each individual log entry is accompanied by a cryptographic checksum (hash-based message authentication code) which is generated using the log message and a device-specific secret key. This approach allows to detect tampering of log entries, including modification and deletion.

In case of security events with an impact to the device integrity and an influence of the therapy is possible, the clinical user of the device receives urgent warnings indicating that the device is not suitable for clinical use. Security events which indicate abnormal technical behavior are notified to the administrative user of the device or to the hospital’s IT department.

Configuration change notifications. A change in the device or system configurations can have an impact on performance, security, availability, and operation. Change notifications in the form of alerts can prove to be a lifesaver by alerting the administrator about the changes and their details in real-time.

RESPOND

To enable you as our customer to respond quickly and effectively to a detected cybersecurity event, each event notification sent to your IT administrators includes information about the cause of the security event and recommended action.

Our devices contain a component called System Health Monitor (SHM) which measures the resource consumption of the software running on the device during operation. For example, the SHM measures continuously the memory usage and the processor load. If the consumption violates the limits set by SHM, the last resort reaction will be a reboot of the system. During the reboot, several checks will be performed before starting again.

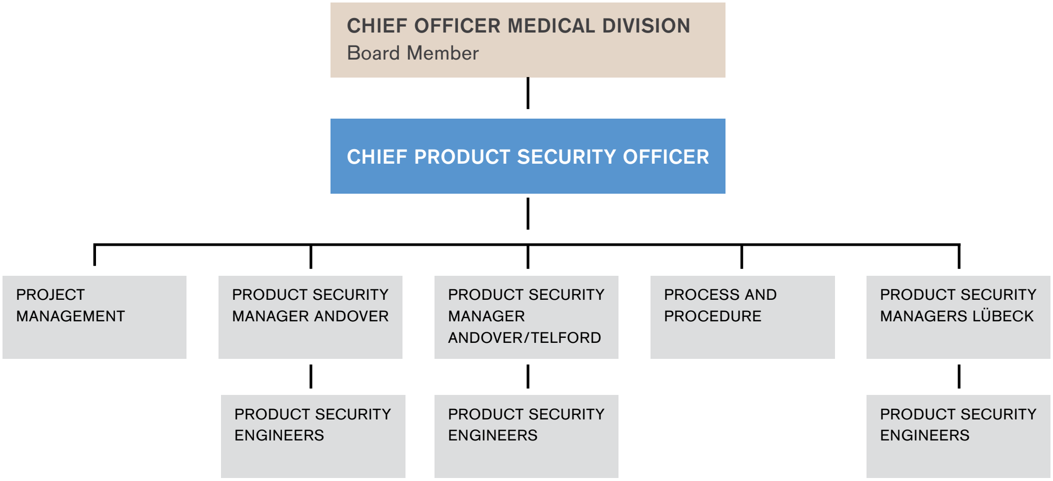
The system load caused by interface traffic is measured by monitoring the resource used by the device network protocol stack. If that resource usage exceeds a certain level, so the runtime behavior of other system parts might be influenced, the network adapter is disabled automatically until the next reboot.

RECOVER

After a cyber-attack is successfully eradicated, the device must recover to good health in order to continue normal operation. Our medical devices support the recovery by the following safeguards:

- The device supports the storage of clinical configurations on USB mass storage devices for distribution and backup purposes.
- If the device detects a software runtime error caused by a cyber-attack, it will initiate a system restart to restore it to a known-good-state.
- As a last resort Dräger Service will be able to restore hardware and/or software components.

DRÄGER'S PRODUCT SECURITY ORGANIZATION


CHIEF OFFICER MEDICAL DIVISION
Board Member
CHIEF PRODUCT SECURITY OFFICER
PROJECT MANAGEMENT
PRODUCT SECURITY MANAGER ANDOVER
PRODUCT SECURITY MANAGER ANDOVER/TELFORD
PROCESS AND PROCEDURE
PRODUCT SECURITY MANAGERS LÜBECK
PRODUCT SECURITY ENGINEERS
PRODUCT SECURITY ENGINEERS
PRODUCT SECURITY ENGINEERS

Our product security organization employs a layered protection approach to ensure security design and control for our products.

The product security organization is separate from product development and located in USA and Europe thereby allowing autonomy for the product security organization to be focused on security instead of the product development process.

The Chief Product Security Officer is accountable for all Dräger products and reports directly to the Executive Board who has the overarching responsibility and accountability to ensure Dräger products are secure when a healthcare organization implements into their environment.

The Product Security Managers report to the Chief Product Security Office and are responsible for the security of all products.

Product Security Engineers report to product security managers and are responsible for all security controls and processes within a specific product.

5. SECURE PRODUCT DEVELOPMENT LIFECYCLE

Our secure development lifecycle places security front and center during the medical device and firmware development process. From requirements to design, from development to testing, the secure development lifecycle strives to build security into our medical devices and firmware at every step in the development process.

We have six key components integrated into our secure product development lifecycle:

- Training
- Design
- Development
- Verification / Testing
- Release
- Maintenance / Monitoring

Training

Technical training of staff involved is needed for any secure product development lifecycle. It includes numerous topics that focus on secure design, secure coding, and minimizing the risks and threats to firmware.

Secure products cannot be developed by bolting on security requirements to the medical devices and firmware. That type of development may produce additional risks and vulnerabilities within the development of products. The integration of security requirements to limit risks to our products is a result of teamwork. Every Dräger team member is aware of risks existing in our very connected world. Additionally, our team members have the training to neutralize these risks and build more robust security into the medical device. To continually improve security training, we have established a multistage training concept, providing in-depth education.

Dräger Product Security Engineers are also responsible for staying up to date regarding current topics and developments in the security world, ensuring that Dräger will not be surprised by sudden incidents threatening the security of you as our customer.

Design

We design security into product requirements from the very beginning. A well-designed security architecture is the foundation for the resilience and the secure operation of our products. While the complete absence of vulnerabilities is unrealistic, we put a tremendous amount of effort into the process of securing our devices to make them withstand the risks in a connected environment.

To ensure that every design decision takes security into account, we follow a guideline that we call our cybersecurity ten guiding principles. These commandments reflect the ten most important things to consider with respect to the integration of cybersecurity into our products and systems. Our products shall:

- Not ship with (or rely on) discontinued, unsupported, or vulnerable components
- Run on the least possible privilege
- Ship in the securest state by default
- Not ship with hard coded credentials
- Have security designed in from the beginning
- Be resilient against unexpected inputs on any of their interfaces
- Be designed to protect all data, at rest and in transit
- Have no hidden backdoors, debug ports, or unnecessary software running
- Be designed to receive security patches
- Protect critical functions from unauthorized access.

We ensure that our products and systems are designed in this way for the desired level of security. We create threat models, which is an analysis of the system from the viewpoint of an attacker, by following best practices. Finding possible motives and leveraging the STRIDE[1] framework for the motivation to identify possible security vulnerabilities and issues. Security threats can thereby be assessed and mitigated early in the design phase of the systems.

Develop

Writing a paper on security product architecture alone does not guarantee a secure development of a product or system. While documentation aids to minimize the exploitability and impact of vulnerabilities in the product or system when developed to the requirements, it cannot prevent vulnerabilities being introduced into the system during the development phase. Steve McConnell states that the industry average is 15 to 50 programming errors per 1000 lines of source code. While most of these errors have no impact on the security of the product or system, some vulnerabilities are among them. This range of vulnerabilities from buffer overflows to cross site scripting, from denial-of-service errors to flawed access controls, are still present in many products and systems. We have taken several steps to minimize the number of this kind of vulnerabilities.

At Dräger no line of code is shipped unreviewed. In most of our teams the four plus one (4+1) principle is followed: Four (4) is the minimal number of approvers that have seen and reviewed shipped code in peer-to-peer or group code reviews, and plus one (+1) is the static code analysis software, which we use to check code for automatically detectable defects.

With these efforts, we can bring the number of security vulnerabilities down to a minimal level.

Verify / Test

During the code verification phase we ensure that the product or system, whether new developed or enhanced, functions as intended during the design step. This focus is not only on the actual functionality but also on the security capabilities. As part of the verification and release process, we also use a set of systematic test methods like Fuzz-Testing of Inputs and Interfaces, automated vulnerability scanners, and static code analysis software.

The final stage of test and verification is the assignment of independent external security experts to carry out penetration testing on our medical devices and systems. During these tests professional White-Hats try to infiltrate the medical device or system without being pre-influenced by the background knowledge Dräger developers have, paired with their high expertise in hardware and software security technology. If vulnerabilities are found, we are able to fix them before bringing the medical device or system to market. These tests are also an independent confirmation of the reliability of our products and Dräger Secure Development Life Cycle, and a proof of quality for you as our customer.

Release

After our team completes the verifications and remediations are completed and re-verified, our products enter the release phase where the Software Engineering team takes over to perform the release phase. During the release phase, the Dräger product and system documentation is finalized, and a Software Bill of Material (SBOM) is created. Furthermore, the SBOM links the software components versions to Dräger specific release and enables us to perform an effective vulnerability monitoring. The final software build is frozen and bundled with its documentation, signed to prevent unauthorized changes, and released for distribution.

Product Maintenance and Vulnerability Monitoring

We understand the importance of monitoring public information for vulnerabilities. Our product security team monitors continuously a variety of information sources for published security vulnerabilities in third party components and maps these to the possibly affected Dräger products. Our sources include the National Vulnerability Database (NVD), MITRE's CVE List, VulnDB, and several vendor specific RSS feeds, mailing lists, and websites. Furthermore, Dräger is member of the German Alliance for Cybersecurity ("Allianz für Cybersicherheit"), which provides timely information on current threats and vulnerabilities.

We maintain a product security page at **draeger.com/security** in order to provide contact details and information concerning the procedures to follow to test and report vulnerabilities or security issues. This page also provides information concerning the procedures that follow any incident and public product related security advisories.

6. CLOSING STATEMENT FROM OUR CHIEF PRODUCT SECURITY OFFICER

Dräger is deeply aware of its responsibility towards patients and hospitals. That is why my Product Security Team and I are working passionately to ensure that cyber-attacks on hospitals will not affect the care of patients or the integrity of patient data on our medical devices and systems. As the specialists in critical care, you can count on us to provide expertise to help you and your hospital keep our medical devices running securely on your networks.

It is our mission to implement cybersecurity best practices for our solutions in order to provide industry-leading protection and security. Along the way, we strive to make tomorrow's connected healthcare more secure. Our personal values of honesty, integrity, professionalism and mutual respect play a central role in this. This is what I and my team stand for.

Jeff Moore, Chief Product Security Officer

Jeff Moore

Discover more on our website: draeger.com/en-us_us/Hospital/Healthcare-Cybersecurity

[1] STRIDE security is the mnemonic for six threat categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege.

DMC-100396 | 22.01-1 | NW | GT | Subject to modifications | © 2022 Drägerwerk AG & Co. KGaA

CORPORATE HEADQUARTERS
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23558 Lübeck, Germany

www.draeger.com

USA
Draeger, Inc.
3135 Quarry Road
Telford, PA 18969-1042, USA
Tel +1 800 4DRAGER
(+1 800 437 2437)
Fax +1 215 723 5935
info.usa@draeger.com

Manufacturer:
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23558 Lübeck, Germany