# Safe & Secure Connectivity

Interview with Hannes Molsen,
Product Security Manager and Developer at Dräger

 

The first important step – create standards.


# Minimizing vulnerabilities and possible points of attack for hackers

**Digitalization in the healthcare sector continues to move forward. The industry is endeavoring to provide manufacturer-independent interoperability between various devices and systems. At the same time, there are more and more reports about cyberattacks on hospitals. How do you see these developments?**

Comprehensive networking undoubtedly increases the vulnerability of systems. The segmenting of networks in hospitals that is already practiced provides security and should be maintained in the future. The challenge is to move beyond the situation where each device manufacturer tends to require a separate network. To achieve this, many medical technology providers, including Dräger, are employing communication protocols based on harmonized standards in their devices and systems. As an important first step to this end, the new communication protocol SDC was issued in January 2019 as part of the IEEE 11073 series of standards. In this context, a new form of controlling access to networks is important that demands authentication – for example through digital security certificates – from the network itself or from the end device. Regarding the known attacks on hospitals in recent times, it is said that they have tended not to be targeted actions but rather the result of malware circulating in the Internet. Hospitals have often been hit particularly hard because their software is frequently outdated.

**Doesn‘t manufacturer-independent connectivity carry the risk of faster proliferation of malware through the whole system?**

Increased network connectivity is always associated with higher risks. We deal with this risk by taking into account the security of

each individual end device and not only the security at the network level.* The core functionality of devices must be maintained even in the event of an attack. Especially for care-relevant medical technology, we should operate according to the maxim that the network should always only represent an additional function of such devices. And if this additional functionality should fail, the core therapeutic function should remain intact. Only on this basis is it possible to ensure patient safety at all times.

**What role does the "hardening of software components" have for the cybersecurity of care-relevant medical devices in the reduction of overall vulnerability?**

In medical devices it is important to only integrate software components that are accessible from outside when they are really necessary for the functioning of the device. Unnecessary elements should not be included. To put it simply: A ventilation device based on a Windows operating system does not need to have the same features as a computer in a doctor's office with an email inbox, text programs, etc. This makes for a sharp reduction in possible points of attack for hackers. And these can be further reduced through a modular construction of the operating systems. In summary, one can say the less software is visible from outside the device, the more secure the technology and the device will be.

**What is the status of the requirement proposed by experts that a technical separation of functional and network components be in place for therapy devices?**

This is a subject that gets a lot of discussion. With some of our devices, we have already realized this separation. On the software side, a strict separation is necessary in every case. Finally, it cannot be that Component A will be affected if Component B happens to crash.

**In the overall context of digitalization and interoperability in the healthcare sector, the question is also posed about the role of software-supported security solutions (e.g. firewalls) in addition to the cybersecurity measures that you have already mentioned.**

That is an important issue where there is a variety of opinions. What is in any case clear is that firewalls and antivirus programs are essential for consumer computers as used in doctors' offices or by the hospital administration. For medical devices, on the other hand, such features are of less relevance. Firewalls prevent certain software components from being addressed by incoming signals. This assumes, however, that these components are present in the system. With lots of medical technology this tends not to be the case. Here, I'll make reference to the principle of the hardened system that is the reduction of software elements to the absolute minimum required for the functionality of the device. Antivirus programs are also intended more for dynamic systems with diverse applications – like personal computers. In future, the quantity of applications included in medical devices will also increase so that the requirement profile for appropriate security software may change. Then firewalls and antivirus security software may come to be of more significance in this area. Here is a realistic scenario as an example: The data created with a therapy device are transmitted via a network to the computer in the physician's office, analyzed there, converted into an application command – for example "Change medication" – and sent back to the therapy device.



*Not applicable to all legacy products.

It seems that cybersecurity can be most improved through the reduction of potential points of attack. In IT circles there's lots of talk in this connection about the importance of interface management. How does that come into play here?

Physical interfaces are changing constantly. In the field of medical technology, however, this subject is still at a more preliminary stage. Today in the medical field a very conservative approach is being taken with these developments as in the past, and that will continue for the foreseeable future. For example, the classic serial cable is still often used instead of a network cable. The physical interfaces will likely become of less significance, however, as more data exchange takes place via networks. Nonetheless, it is still the case that the likelihood of attacks via interfaces can be reduced when systems are hardened.

With all this fast-paced progress, how can hospital personnel who are not specialized in IT keep up with developments?

Training is very important. In training sessions, employees can learn about the correct way to handle email attachments, flash drives and links. Another topic that is covered is how to conduct oneself in public Internet forums. It is also especially important to explain what happens when a given technology does fail and how such failures can be recognized. The larger and more dynamic networks become, the higher the risk of errors and failures. Personnel must learn how to handle technical malfunctions of various types, even if it's something as simple as a person stumbling over a cable and severing a connection. The important thing is not to panic. When there is a well thought out cybersecurity concept with hardened systems, secure networks and well trained personnel, then panic will certainly not be the response.



**IMPRESSUM**

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Tel +49 (0) 451 / 882 0
Fax +49 (0) 451 / 882 2080
Mail: info@draeger.com
www.draeger.com

PDF-9311 | 20.03.2