CONNECTED BUT PROTECTED – SECURELY CONNECTING DRUG DELIVERY DEVICES

Dr Joachim Wilke of ITK Engineering discusses wireless connectivity in novel drug delivery devices, highlighting the possibilities for improved patient outcomes and care. The associated security risks, as well as examining the wide range of cyber security solutions and standards to mitigate these issues.

Healthcare is no longer confined to hospitals and doctors' surgeries; it is increasingly expanding into everyday environments such as homes, workplaces and public spaces. To keep pace with this evolution, drug delivery devices must be intelligently connected. This enables seamless integration of medical care into daily life, improving both treatment outcomes and patient comfort – all while meeting stringent safety and compliance standards (Figure 1).

SECURING DATA TRANSMISSION RELIABLY

One key technical feature of modern drug delivery devices is their wireless connectivity. Interfaces such as Bluetooth Low Energy (BLE), Wi-Fi, and Near Field Communication (NFC) are essential for enabling interaction between the device and external systems such as mobile apps, health platforms and cloud-based analytics services. However, this connectivity also introduces new security risks – unencrypted or poorly secured transmission channels can compromise sensitive patient data or, in extreme cases, even affect the device's functionality. Therefore, implementing advanced encryption standards for data security in transit and at rest.

Additionally, robust authentication methods, such as multi-factor authentication and biometric procedures, are becoming the new standard to control access to devices and their data. This is particularly critical

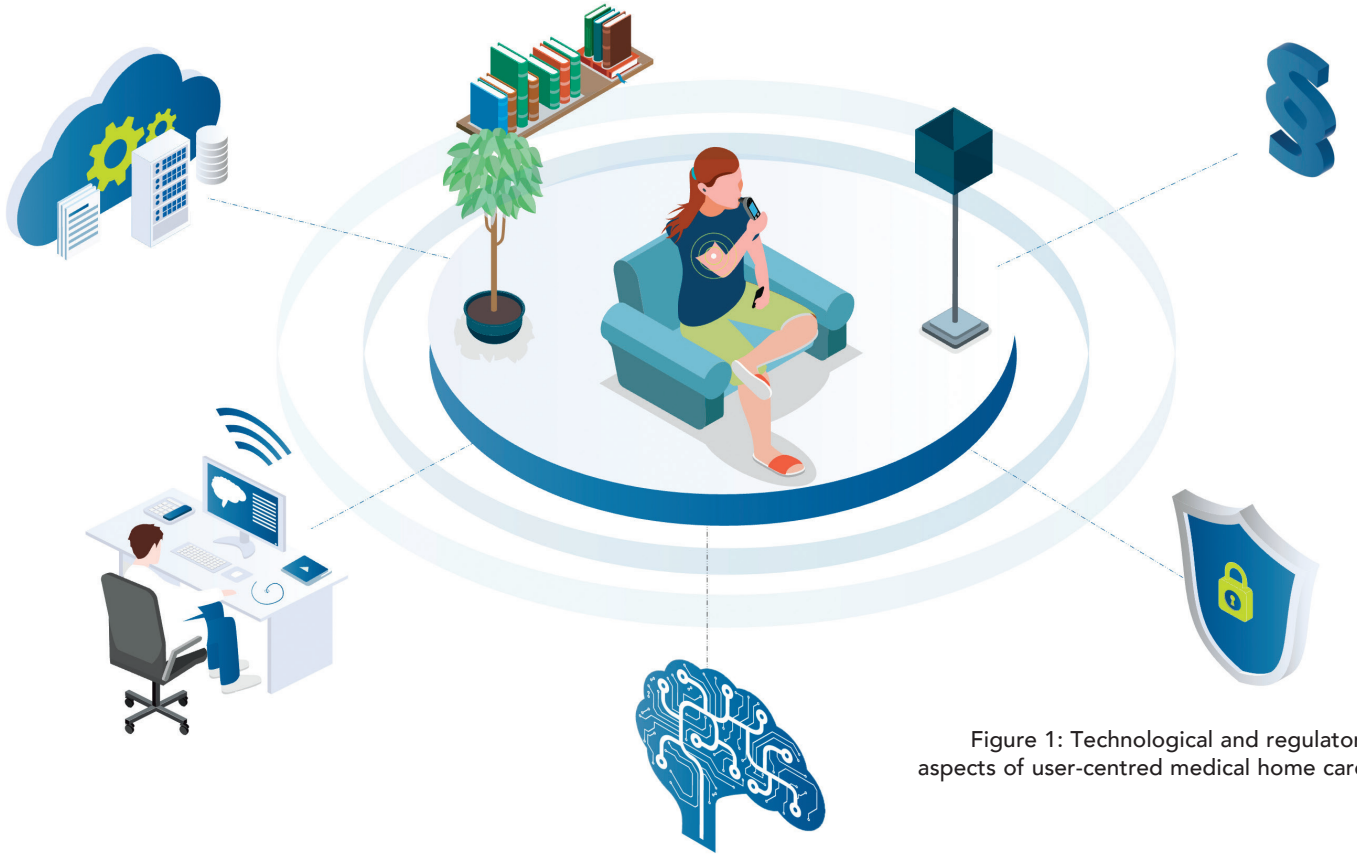


Figure 1: Technological and regulatory aspects of user-centred medical home care.

"TO ENSURE THE RELIABILITY OF DRUG DELIVERY DEVICES EVEN UNDER THREAT SCENARIOS, IT IS CRUCIAL TO INTEGRATE CYBER SECURITY PROACTIVELY THROUGHOUT THE ENTIRE LIFECYCLE."

for drug delivery devices involving patient-specific dosing, where only authorised individuals should be able to operate the device. Increasingly, device-bound digital certificates, challenge-response methods and hash- and time-based one-time passwords are being employed.

Another trend is the local validation of sensitive actions directly within the device itself, for example, by using hardware security modules or secure elements. These components protect private keys and perform cryptographic operations in a hardware-supported manner.

IDENTIFYING RISKS BEFORE THEY ARISE

To ensure the reliability of drug delivery devices even under threat scenarios, it is crucial to integrate cyber security proactively throughout the entire lifecycle – from development and design to commissioning and ongoing maintenance. Standards such as IEC 81001-5-1, which focuses on secure design principles,[1] and ISO 14971,[2] which governs risk management for medical devices, provide important guidelines for manufacturers. Cyber security measures may also become relevant in the context of the new post-market surveillance requirements introduced by the UK Medicines and Healthcare products Regulatory Agency (MHRA), which will come into effect on 16 June 2025.[3]

STRIDE

Proactive cyber security means already conducting threat and risk analyses during the development phase, for example, by using the STRIDE methodology (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege). STRIDE systematically identifies potential threats through the creation of data flow diagrams, enabling comprehensive yet efficient risk assessments.

CVE scanning

Since no single method can guarantee full coverage of all potential risks, it is advisable to combine several identification techniques. Alongside STRIDE, a common vulnerabilities and exposures (CVE) scan of the software components used can be performed. CVE refers to publicly known vulnerabilities in software and hardware documented in the international CVE database. These vulnerabilities can cause serious risks, such as data leaks or system manipulations. Regulatory bodies, including the EU and the US FDA, have set clear requirements: manufacturers must integrate CVE scanning processes into their workflows and produce reports listing affected components, their criticality and the mitigation measures taken. These analyses are essential to detect security risks early. Furthermore, all decisions must be traceably documented, helping to minimise liability risks and meet auditor requirements.

Conducting a CVE scan requires a software bill of materials (S-BOM) – a comprehensive list of all the software components comprising the system under review. Often, S-BOMs must be maintained manually. However, automation tools can assist in both creating S-BOMs and performing scans – only the subsequent assessment of discovered vulnerabilities still demands meticulous manual work (Figure 2).

Penetration testing

Another essential building block for ensuring cyber security is penetration testing (pentesting). This is a structured security test explicitly required by IEC 81001-5-1,

"THE PRIMARY GOAL OF PENTESTING IS TO IDENTIFY WEAKNESSES THAT MIGHT HAVE BEEN OVERLOOKED DESPITE THOROUGH RISK MANAGEMENT AND SECURE IMPLEMENTATION – OR THAT WERE INHERENTLY UNDETECTABLE BEFOREHAND."

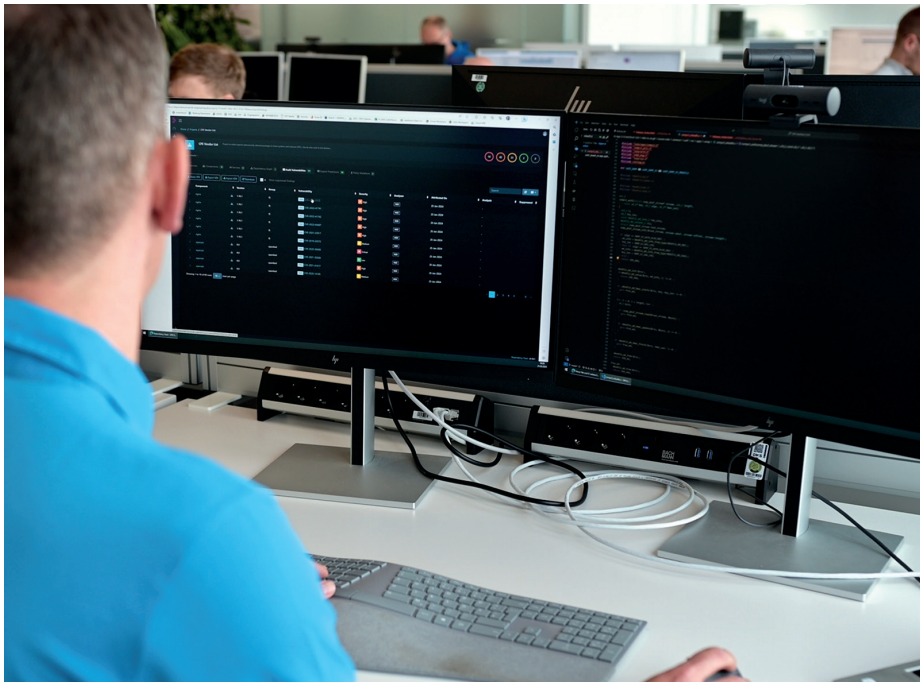
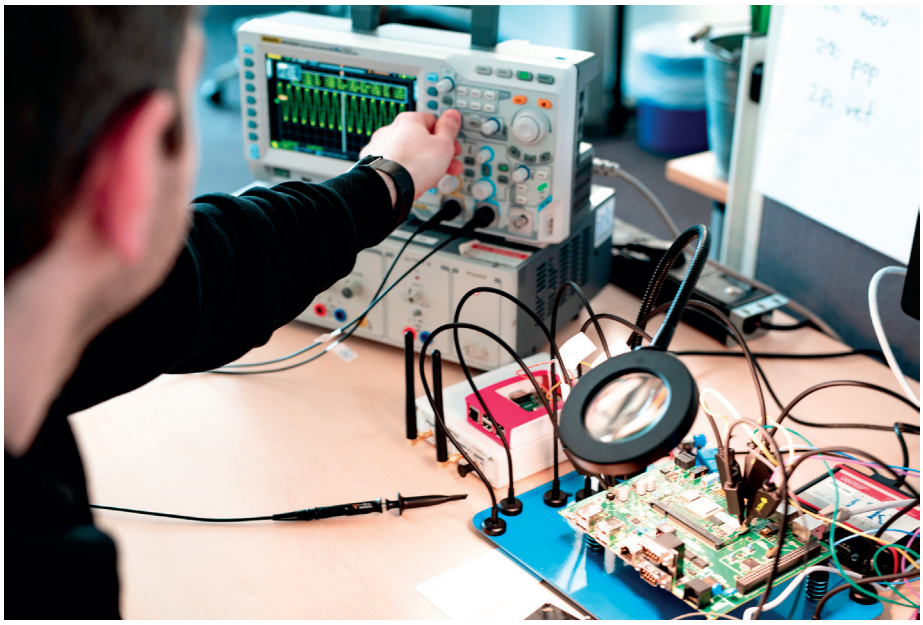


Figure 2: Setting up a CVE scan requires considerable manual work, such as converting software components into a machine-readable S-BOM.



"ZERO TRUST ARCHITECTURES ENABLE FINE-TUNED CONTROL OVER THE DATA FLOW BETWEEN DEVICES, APPLICATIONS, AND USERS, THEREBY SUPPORTING THE SECURITY OF SENSITIVE DATA AND COMPLIANCE WITH REGULATORY REQUIREMENTS."

Figure 3: In-depth penetration testing of a connected medical device.

designed to uncover vulnerabilities within a product. The primary goal of pentesting is to identify weaknesses that might have been overlooked despite thorough risk management and secure implementation – or that were inherently undetectable beforehand, which is more often the case in practice. Additionally, pentesting offers a valuable opportunity to validate a product's security from an independent perspective, particularly towards the end of the development phase. In practice, a combination of black-box and white-box testing has proven to be effective (Figure 3).

MANAGING DATA SECURELY WITH THE RIGHT INFRASTRUCTURE

The choice of data infrastructure significantly impacts the security of connected drug delivery devices. Whether opting for public cloud, private cloud or hybrid solutions, decisions should be based on several factors, such as data sensitivity, regulatory requirements and cost considerations. Infrastructure decisions must also take into account the energy demands of data processing, ensuring that data management remains robust without placing an undue burden on device energy resources. Encrypting data both during transmission and at rest is essential to prevent unauthorised access.

Dr Joachim Wilke

Joachim Wilke, PhD, Cyber Security Specialist, Healthcare, at ITK Engineering, has played a key role as a group leader and project manager in the connectivity of medical devices for various renowned clients in the healthcare sector since 2013. He is an expert in identifying security vulnerabilities and implementing comprehensive security concepts in medical systems. Prior to this, he conducted academic research in the field of telematics and earned his doctorate studying wireless sensor-actuator networks at the Karlsruhe Institute of Technology (Germany).

T: +49 162 1057339
E: joachim.wilke@itk-engineering.de

ITK Engineering
Im Speyerer Tal 6, 76761 Ruelzheim, Germany
E: healthcare@itk-engineering.de
www.itk-engineering.de/en/

Role-based access control and zero trust architectures are effective strategies to enforce strict role-based access permissions and ensure continuous validation and adjustment of authorisation rights. Especially in healthcare, zero trust architectures enable fine-tuned control over the data flow between devices, applications and users, thereby supporting the security of sensitive data and compliance with regulatory requirements.

CONCLUSION: CONNECTIVITY REQUIRES SECURITY FROM THE START

The increasing connectivity of drug delivery devices offers tremendous potential – for personalised therapies, improved care outside traditional medical institutions and enhanced quality of life for patients. However, this progress can only succeed if security is embedded from the very beginning. A comprehensive "security by design" approach ensures that drug delivery devices are equipped with robust security mechanisms right from the start. Regular vulnerability analyses, structured threat modelling and targeted penetration testing can help identify risks early – before they can escalate into real dangers.

As the use of cloud technologies and artificial intelligence-based analytics increases, so too does the complexity of potential attack scenarios. It is therefore all the more important to regularly review and adapt cyber security strategies to new risk landscapes, keeping them flexible and resilient. This way, connected drug delivery devices can be developed that not only impress technically but also sustainably build trust among users, healthcare professionals and regulatory authorities – ensuring long-term market success.

ABOUT THE COMPANY

ITK Engineering, a global tech company and wholly owned subsidiary of Robert Bosch, draws on methods-driven expertise to provide standards-compliant and platform-independent software and system development services to customers across several industries. In its healthcare branch, which is certified according to EN ISO 13485:2016, ITK Engineering implements standards-compliant system and software solutions for medical products – from medical devices and robotic systems to diagnostic solutions.

REFERENCES

1. *"IEC 81001-5-1: Health software and health IT systems safety – Part 5-1: Security – Activities in the product life cycle". IEC, 2021.*
2. *"ISO 14971: Medical devices – Application of risk management to medical devices". IEC, 2019.*
3. *"The Medical Devices (Post-market Surveillance Requirements) (Amendment) (Great Britain) Regulations 2024". UK Government, 2024.*