CYBERSECURITY AND CONNECTED DRUG DELIVERY – AN INTEGRATED RISK-BASED APPROACH

In this article, John Whitehouse, Senior Software Engineer, Rob Veasey, Senior Sector Manager, Medical and Scientific, and Shane Day, Electronics and Software Skills Leader, of DCA Design, discuss the value of integrating cybersecurity into a holistic, multidisciplinary approach to risk management for connected medical devices.

> "Reports by cybersecurity researchers have demonstrated the potential vulnerability of safety-critical devices, such as wireless-connected insulin pumps and pacemakers, to hacking, raising the genuinely sinister prospect of targeted, remote, life-endangering attacks on individuals."

We are all becoming increasingly aware of concerns about the security of digital information impacting our lives. Most people routinely communicate online and, in the wake of covid-19, many of us now also extensively work, shop, bank and socialise in the digital space. This inexorable trend is revolutionising the way we live and is impacting the medical industry as both healthcare providers and device companies embrace digital technology as a means to improve patient outcomes and streamline service efficiency.

Of course, electronically programmable medical devices have been around for decades; what is different now is the widespread integration of these devices with a patient's own electronic products and systems, such as mobile phones and home networks. This integration significantly increases the vulnerability of personal medical data to cyber-snooping and raises the very serious prospect that malicious attacks could be made that disrupt safe and effective operation of devices that are critical to the health and well-being of patients.

In 2017, the WannaCry ransomware attack affected hundreds of thousands of computers around the world. Whilst this attack was not specifically targeted at medical systems, it exposed the vulnerability of large, interconnected healthcare providers, such as the UK's NHS. The attack resulted in the cancellation of thousands of appointments and operations within the NHS. It was also reported that some staff had to revert to pen and paper and the use of private mobile phones, as centralised IT systems had become completely disrupted. Perhaps even more alarmingly, reports by cybersecurity researchers have demonstrated the potential vulnerability of safety-critical devices, such as wireless-connected insulin pumps and pacemakers, to hacking,[1]

John Whitehouse
Senior Software Engineer
T: +44 1926 499461
E: medical@dca-design.com

Rob Veasey
Senior Sector Manager,
Medical and Scientific
T: +44 1926 499461
E: medical@dca-design.com

Shane Day
Electronics and Software Skills Leader
T: +44 1926 499461
E: shane.day@dca-design.com

DCA Design International
19 Church Street
Warwick
CV34 4AB
United Kingdom

www.dca-design.com

> "The device developer should aim to generate a comprehensive list of cybersecurity risks that require consideration and mitigation during the development of the detailed design for the device."

raising the genuinely sinister prospect of targeted, remote, life-endangering attacks on individuals.

Whether inadvertently or deliberately, it is clear that cyber-attacks have the potential to inflict serious harm on patients. In response, regulators expect that cybersecurity vulnerabilities are adequately identified and addressed by developers and manufacturers of all electronically programmable medical devices.

WHAT NEEDS TO BE PROTECTED?

When determining how to protect the cybersecurity of a medical device, the first step is to understand the data assets that the device manages. Data records, especially sensitive patient data, need protection from snooping and manipulation for both privacy and safety reasons. Additionally, the software running on the device may be a key intellectual property asset that needs to be protected from theft or tampering.

As a second step, one needs to consider the environment in which the device will be used. For example:

- Will the device be connected to the internet?
- Does sensitive data need to be transferred to, as well as from, the device?
- Does the device need to be operating at all times?
- Will the device be used in public or private spaces?

The answers to these questions will help to inform decisions on the most appropriate type of communications technology for the device, such as Bluetooth, near-field communication (NFC) or cellular, which in turn enables the developer to explore potential system risks and vulnerabilities.

Consider a hypothetical scenario, wherein a new drug delivery device is being designed with connectivity features to support a patient in tracking their medication and to enable live monitoring by clinicians (Figure 1). In this scenario, a patient interacts with their device using an app on their smartphone via a short-range, personal area network (e.g. Bluetooth Low Energy), which allows the patient to read a log of their dose history. Additionally, the device has an internet connection that allows data to be uploaded to a cloud-hosted database server. The patient's clinician can access the data from the database for remote patient monitoring. The device also includes a wired access port for device maintenance and diagnostics by the manufacturer.

An initial cybersecurity assessment identifies that there are a number of possible points of interest for a potential attacker. Data records, including the details of a patient's medication history and any sensitive personal data, could be of interest to an attacker looking to profile or track

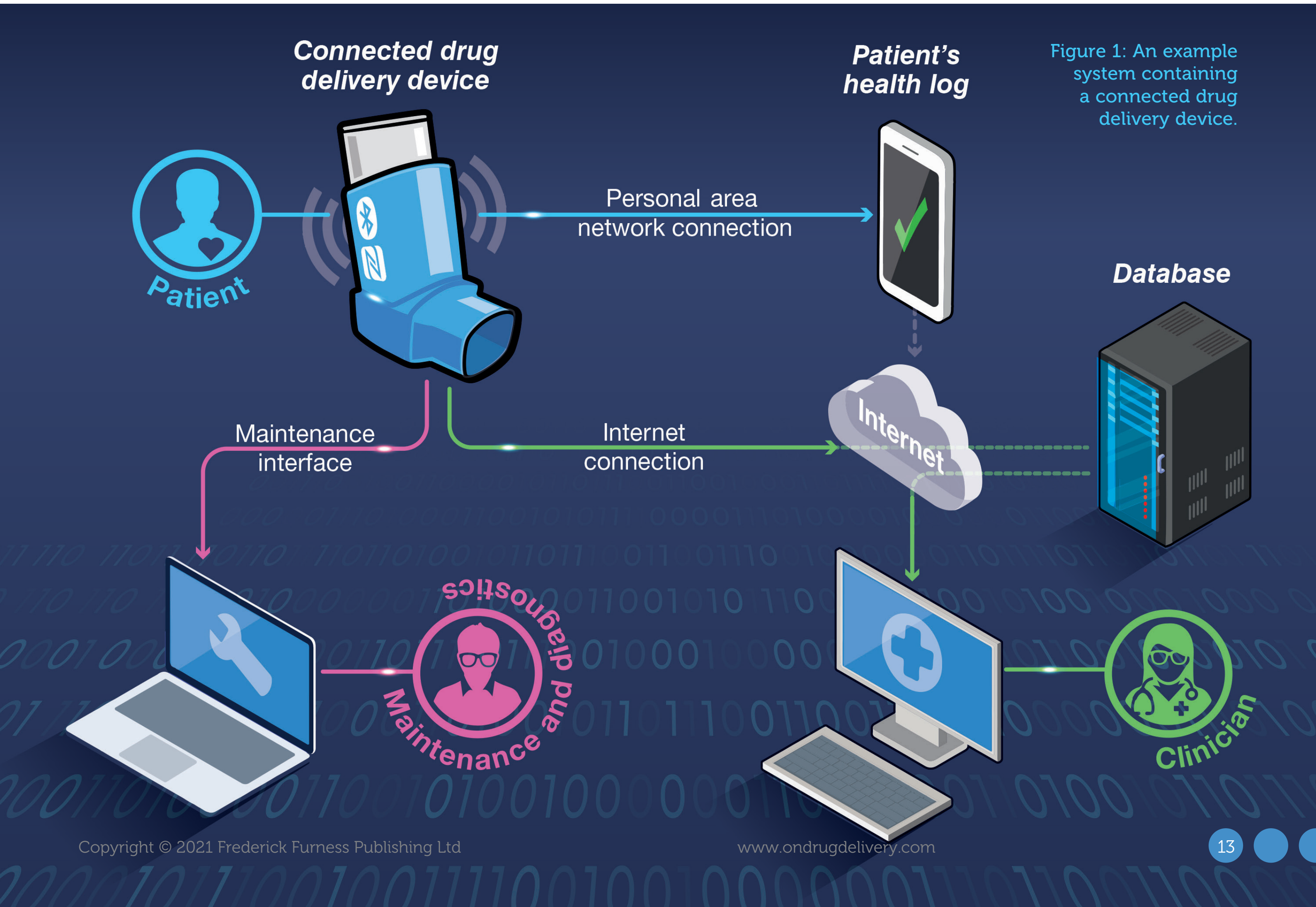

Figure 1: An example system containing a connected drug delivery device.

an individual. Access to the software and configuration settings that control the device's behaviour, either via the wired access port or wirelessly, could provide an avenue for malicious attacks, as well as theft of intellectual property. The presence of an internet connection could also make the device vulnerable to a variety of attacks, such as "denial-of-service", where the device is flooded with superfluous requests in an attempt to make it unavailable to its intended users.

> "After identifying potential cybersecurity risks, DCA's approach is to manage and review the identified vulnerabilities as part of the overall risk management process for the device. This approach helps to ensure that all aspects of performance are considered and appropriately balanced."

IDENTIFYING VULNERABILITIES

Once the device and its system architecture are defined, threat modelling should be applied methodically to identify potential vulnerabilities that need to be addressed. By examining the potential for cyber-attacks, such as spoofing (disguising a communication from an unknown source as being from a known and trusted source), tampering, data repudiation (hidden manipulation or invalidation of data), information leaks, unauthorised use or denial-of-service, the potential impacts on device behaviour can be explored. The device developer should aim to generate a comprehensive list of cybersecurity risks that require consideration and mitigation during the development of the detailed design for the device.

When evaluating the potential severity of cybersecurity risks and assessing possible risk controls, a common approach is to consider confidentiality, integrity and availability (CIA) for each scenario. The US National Institute of Standards and Technology (NIST) defines these terms as follows:[2]

- **Confidentiality:** Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.
- **Availability:** Ensuring timely and reliable access to and use of information.

	Risk	Confidentiality	Integrity	Availability
1	Dose data transmitted via the wireless link is intercepted, manipulated or corrupted in transit.	Data sent via the internet connection is likely to transit untrusted networks, so could be monitored by a third party. Data sent via the personal area network could likewise potentially be visible outside of the target app on the patient's smartphone. **SEVERITY: HIGH**	Data sent via the internet connection could be manipulated on an untrusted network. Data sent via the personal area network could be manipulated before reaching the target app on the smartphone. **SEVERITY: HIGH**	Attempts at manipulation or corruption of data might stop it reaching the patient or clinician at all. **SEVERITY: MEDIUM**
2	Dose data stored on the device is accessed or manipulated via a wired or wireless link.	Unauthorised data access results in a leak of sensitive dose data. **SEVERITY: HIGH**	Access to dose data could result in it being manipulated without the patient's knowledge. **SEVERITY: HIGH**	Dose data is irrecoverably corrupted or deleted. **SEVERITY: HIGH**
3	Software on the device has a bug, resulting in a cybersecurity vulnerability.	If the vulnerability can be exploited, unauthorised data access may result in a leak of sensitive dose data. **SEVERITY: HIGH**	If the vulnerability can be exploited, dose data could be manipulated without the patient's consent or knowledge. **SEVERITY: HIGH**	If the vulnerability can be exploited, device behaviour could be modified, resulting in loss of connectivity. **SEVERITY: HIGH**
4	Spoofing (mimicking) of the device means that the patient or clinician unknowingly receives invalid data.	An unauthorised user discloses false dose data information to the patient and clinician. **SEVERITY: HIGH**	False dose data sent to patient / clinician. **SEVERITY: HIGH**	Spoofing by another device could deny genuine device access to a patient's smartphone or clinician's database. **SEVERITY: MEDIUM**
5	Denial-of-service attack prevents the patient or clinician receiving dose data.	Depending on the nature of the attack, dose data may not be directly exposed, so there may be no significant confidentiality risk. **SEVERITY: LOW**	Unauthorised user able to interfere with device behaviour. **SEVERITY: MEDIUM**	Dose data may not be retrievable from the device. Risk that timing of safety-critical device functions could be impacted. **SEVERITY: HIGH**

Table 1: Example cybersecurity risks identified using the CIA framework.

The relative importance of each criterion will depend on the intended use of a medical device. For a connected drug delivery device, integrity of data, such as records of drug delivery activity, may often be considered more important than confidentiality or availability. However, availability of data might be more important in scenarios where the drug delivery device needs to provide real-time updates, such as alerting a clinician to an occurring problem.

Taking our hypothetical drug delivery device example, we have identified a few example cybersecurity risks and evaluated their potential impact using the CIA framework in Table 1. Having identified cybersecurity risks in this way, they can then be resolved within the overarching connected device risk analysis.

When developing electronically programmable medical devices at DCA, the company also performs detailed research into known issues and published vulnerabilities for the hardware and software used in a medical device to support further risk identification. This includes examining supporting software documentation and assessing published information in open-source databases, such as the Common Vulnerabilities and Exposures (CVE) database. DCA also consults any appropriate guidance on the secure use of data communication protocols, such as Bluetooth Low Energy, that has been published by authorities like NIST.[3]

CYBERSECURITY AS A PART OF MULTIDISCIPLINARY RISK MANAGEMENT

After identifying potential cybersecurity risks, DCA's approach is to manage and review the identified vulnerabilities as part of the overall risk management process for the device. This approach helps to ensure that all aspects of performance are considered and appropriately balanced. It is important to remember that a secure device is not necessarily a safe one, as shown in Figure 2, adapted from the Association for the Advancement of Medical Instrumentation's (AAMI's) technical report on the principles of medical device cybersecurity.[4] The application of a cybersecurity-focused risk control measure in isolation from safety-related risk management could compromise essential performance of the device, for example by negatively impacting usability. One possible situation where this might arise is if extra authentication steps are added to improve the security of the data shared from the device.

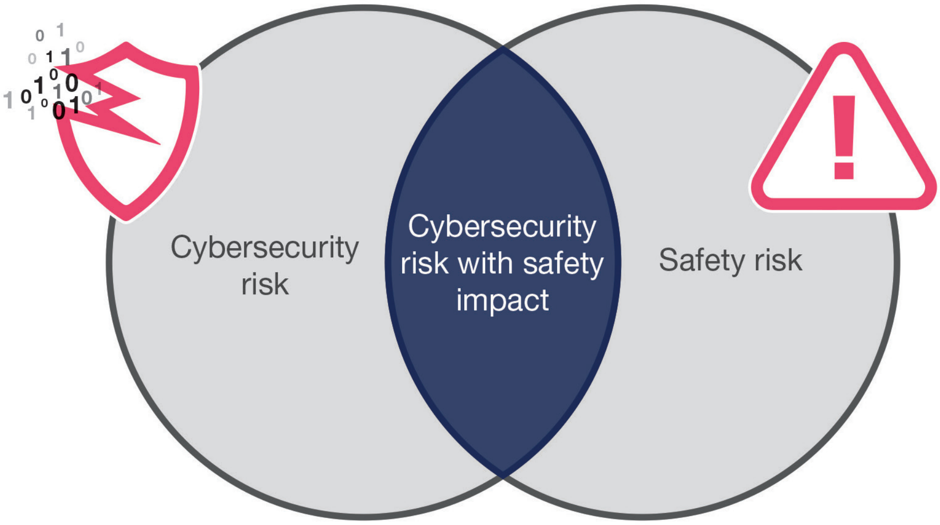

Figure 2: The relationship between cybersecurity and safety risks.

Returning to our hypothetical example device, let us consider some potential mitigations to the cybersecurity risks highlighted in Table 1 and the wider design impacts that their adoption could involve.

Risk 1 – Dose Data Transmitted Via the Wireless Link is Intercepted, Manipulated or Corrupted in Transit

In the case of dose data interception, manipulation or corruption in transit, one mitigation could be to specify and implement end-to-end encryption when dose data is transferred from the device to a smartphone or database. This could be supported by some form of pre-shared encryption key, though a better approach would probably be to use a secure key agreement protocol, such as Diffie-Hellman, for generating a shared encryption key across an insecure communications channel.

In reviewing this proposed mitigation, a relevant safety consideration would be whether the use of a computationally intensive encryption algorithm could impact on the timing of safety-critical functions, such as generating new dose activity records. This may require new design constraints to be specified to ensure that other device functions which impact patient safety are not compromised, such as the segregation of data transfer functionality from dose delivery or monitoring activities.

Risk 2 – Dose Data Stored on the Device is Accessed or Manipulated Via a Wired or Wireless Link

When considering this risk, minimising the opportunities for data to be changed from outside of the device after manufacture would provide a useful mitigation. This could include restricting access to dose data via the wireless and wired links, such as making it read-only. Adding integrity checks, such as error detection codes, could provide an additional detection mechanism in case of inadvertent data manipulation due to a device fault. In these cases, cybersecurity and safety mitigations are likely to be complementary, though the impact on essential performance should always be considered.

Implementing a user authentication scheme could provide a further mitigation for this risk, as well as for risks involving spoofing of a device. Authentication could, for example, involve the patient using their smartphone to scan a unique identifier printed on the device. Data from this identifier would subsequently be used to cryptographically confirm that the data is coming from the expected device. When reviewing this potential mitigation, however, there is a usability trade-off that needs careful consideration. The developer must assess whether the addition of this type of authentication means that the device remains usable and accessible for all target patients. Requiring additional authentication steps via a smartphone app may well be beyond the capabilities of some elderly or cognitively impaired users.

Risk 3 – Software on the Device Has a Bug, Resulting in a Cybersecurity Vulnerability

Where a software bug is published that may result in cybersecurity vulnerability, a couple of mitigation strategies can be employed. To improve monitoring and detection of such risks, a cybersecurity bill of materials

(CBoM) can be prepared, which holds a list of software and hardware components that are, or could become, susceptible to cybersecurity vulnerabilities. The CBoM can be used to support risk management through the device's lifecycle. This includes assessment of purchasing controls and supply chains during manufacture and monitoring exposure to new vulnerabilities when the device is on the market.

Additionally, a device could be designed such that it supports remote software updates to patch software bugs associated with cybersecurity vulnerabilities. However, design of such a capability needs to be carefully considered to prevent the introduction of new cybersecurity risks. Such an update feature may provide a "back door" into the device for data manipulation, allowing pathways for unauthorised software changes or reloading of an old version of the software that has exploitable vulnerabilities. The remote software update protocol also needs to be sufficiently secure to avoid inadvertent loss of intellectual property. Microprocessor manufacturers are improving their capabilities for supporting secure remote software updates, but these should be carefully reviewed and evaluated as part of device risk management, as well as in design verification and validation planning.

Risk 4 – Spoofing of the Device Means That the Patient or Clinician Unknowingly Receive Invalid Data

Considering the risk of device spoofing, a potential cybersecurity mitigation could be to authenticate a patient's device before accepting data from it. As with Risk 2, this could take the form of the patient using their smartphone to scan a unique identifier printed on the device, to confirm that the data is coming from the expected source.

Risk 5 – Denial-Of-Service Attack Prevents the Patient or Clinician Receiving Data

Denial-of-service attacks can be mitigated by implementing a firewall to filter out opportunistic attacks on the wired or wireless interfaces. Consideration of the intended use and careful design is then required to ensure that the risk is appropriately mitigated. Essential performance could still be impacted if most of the on-board computing resource on the device is required to service the firewall. A failsafe function could be considered in this situation too, which temporarily disables data communications to ensure essential performance is not compromised. However, this may not be appropriate where high availability is required; in this situation, a means of prioritising communications, such as alerts, might be required if the device needs to communicate whilst under a denial-of-service attack.

CONCLUSION

This overview only scratches the surface, as there are many technical solutions available to combat potential cybersecurity threats. When developing a connected drug delivery device, these solutions must be carefully considered in the context of the intended use, so that potential impacts on safety and usability are also appropriately balanced.

DCA believes that a detailed multidisciplinary approach to identifying and countering cybersecurity risks should be deployed throughout the development and lifecycle management of connected drug delivery devices, seeking to identify potential problems early, untangle conflicts and thereby achieve optimised design solutions. An effective development process is one that couples risk identification with informed design decision making to deliver safe, usable and cyber-secure connected devices.

ABOUT THE COMPANY

Founded in 1960, DCA is a leading product design and development consultancy. Its multidisciplinary service offering includes systems engineering, mechanical engineering, industrial design, insight and strategy, UX/UI, human factors, electronics, software and prototyping.

With a range of global pharmaceutical, biotech and device companies amongst its long-standing clients, DCA has deep experience in the field of drug delivery devices. Work undertaken in this area includes design, development, analysis and industrialisation support for injection devices, inhalers, wearables and intranasal devices and applicators, including smart and connected devices. DCA has won multiple major industry awards and contributed to over 1,000 granted patents in the last 10 years. The company's development service is certified to ISO 9001 and ISO 13485 standards.

REFERENCES

1. *Ngak C, "Black hat hacker can remotely attack insulin pumps and kill people". CBS News, Aug 2011.*
2. *"Security and Privacy Controls for Information Systems and Organizations". NIST Special Publication 800-53 Rev 5, Sept 2020.*
3. *Padgette J et al, "Guide to Bluetooth Security". NIST Special Publication 800-121 Rev 2, May 2017.*
4. *"Technical Information Report: Principles for medical device security – Risk management". AAMI, 16th Ed, 2019.*

ABOUT THE AUTHORS

John Whitehouse is a Senior Software Engineer at DCA, with experience of leading software design and verification activities in the development of connected drug delivery devices. Mr Whitehouse's experience includes performing cybersecurity assessments as part of an IEC 62304-compliant risk management lifecycle.

Rob Veasey is Senior Sector Manager, Medical and Scientific, leading drug delivery device development projects within DCA's medical device sector. He has 30 years' experience in engineering, design and management roles for leading manufacturing and consultancy businesses and has worked exclusively on development of drug delivery devices for 20 years. Mr Veasey's experience encompasses mechanical and electromechanical drug delivery devices, including work in the fields of injection, body-worn devices, metered dose inhalers, dry powder inhalers, intranasal sprays and topical applicators for global pharmaceutical and medical device companies.

Shane Day is the Electronics and Software Skills Leader at DCA, with a background in systems engineering and over 30 years of medical device development experience. Mr Day has in-depth knowledge of the software development lifecycle and the associated standards and regulations. He believes that, by adopting a pragmatic, risk-based approach to software and system development, we can develop better, safer connected devices.

DCA

Helping our clients
connect with the future

www.dca-design.com