WIND™

Cybersecurity for Medical Devices in a Connected Healthcare System

By Alex Wilson and Andreas Rollman

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

The drive toward digital business transformation that enables a digital healthcare system, with all of the benefits of shared healthcare data, is inevitable. This requires both medical device manufacturers and end users to consider the new concerns of cybersecurity, in order to meet regulatory requirements and mitigate risk for their company brand and reputation.

This is no longer a "nice to have" device feature. Cybersecurity response must be incorporated into the entire device lifecycle—not only in the design but also in development, manufacturing, operational maintenance and decommissioning, and how the device will operate in an IEC 80001 conformant healthcare environment. This becomes a crucial part of device manufacturers' success in operating against both existing and new competition.

Wind River® works with medical device manufacturers to ensure usage of the latest best practices. By properly designing security into medical devices, manufacturers can avoid financial damage, reputational damage, and potential risk to human lives.

TABLE OF CONTENTS

THE DIGITAL TRANSFORMATION OF HEALTHCARE

- Streamlining patient care and private information protection
- Better care decisions by ensuring the right data for the right people, at the right time
- Lower operational costs, especially in service, support, and maintenance expenses
- Increased uptime of technology-driven resources, including radiology, labs, and operating rooms
- Decreased investment enabled by new business models

CYBERSECURITY STRATEGY IS THE KEY TO DIGITAL TRANSFORMATION

With the drive toward increased workflow efficiency and unlocking Big Data analytics to better service patient needs, the digital business transformation trend is sweeping the global healthcare system. Interoperability of medical devices and integration of electronic medical records (both on premise and public) is now a critical requirement. Innovation in clinical applications and decision support systems are providing unprecedented access to medical data. Device security is at the forefront of device and system design, ensuring the successful digital transformation of medical businesses. For some 20 years, medical device manufacturers have wrestled with a common problem throughout the lifecycle: If a device cannot be updated, that device is not secure. Extended lifecycles, post-market device sales, and heterogeneous security practices with the hospital ecosystem have in turn created pressure to implement a comprehensive security strategy to protect medical devices and their data throughout their lifecycles.

In conversations with medical device manufacturers about innovation and the major business issues they have faced over the last 12 months, one topic stands out, having come up in every discussion: security, whether device security or cybersecurity.[1] Over the last few years, the awareness of cybersecurity threats has grown, but very few enterprises have established an end-to-end security strategy and a company-wide framework to execute on it.

The majority are adopting a "good enough" approach that leaves them uncovered at some point of the device lifecycle. Some have implemented isolated security features into specific products, but not into their full portfolio; and they have certainly not taken into account the bigger picture of where their devices fit into the healthcare infrastructure. Most software team leaders are well aware that this simple security protection is limited or outdated and that the overall approach does not solve the security demands of today or tomorrow.

Many companies have announced executive level responsibility for their security strategy or are in the process of implementing such a role. However, based on our own discussions with medical device customers, Wind River estimates that fewer than 10 out of the 30+ companies surveyed already implement some security features.

All of the executives agree that device security is extremely important, and they are concerned about being called out as the next company whose product security has been compromised. According to a recent survey,[2] 65 percent of companies think that their organization faces a significant level of security risk—namely, from the use of mobile, IT security, and cloud-based solutions in the enterprise. Despite this awareness, many have not defined an overall strategy with concrete actions, nor have they built a business justification to allocate budget to implement such a strategy. There are various reasons for this slow progress, including lack of understanding in top management, insufficient budgets, internal expertise gaps, stretched software developer resources, absence of a specific person responsible for device security, and the complexity of regulatory requirements.

MEDICAL DEVICES AND REGULATIONS

Device manufacturers used to have the luxury of stipulating that their devices would be deployed only on a network secured behind a firewall. Recent thinking has become more realistic, accepting that not every hospital network that is supposed to be secure truly is secure in practice. IT staff in hospitals, just as in other industries, struggle to keep their networks patched and up to date. Increasingly, they are asked to connect greater numbers and more diverse types of devices to that network, and now to cloud-based services outside of the hospital, resulting in many exceptions to the original rules of deployment. In fact, recent evidence suggests that even being behind the firewall no longer means being in a safe haven[3] from a security perspective, with rogue devices and poor security procedures in place in many establishments. Medical devices are also being deployed beyond the hospital walls in long-term care facilities or in the home, where there are no IT departments to build a security process and a secure network.

The Food and Drug Administration is taking cybersecurity seriously, and the guidance from October 2014, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,"[4] was the first step. This publication recommended that, prior to market submission, manufacturers consider security aspects of their devices, including:

- Identification of assets, threats, and vulnerabilities
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients
- Assessment of the likelihood of a threat and of a vulnerability being exploited
- Determination of risk levels and suitable mitigation strategies
- Assessment of residual risk and risk acceptance criteria

Of note, the guidance recognized several well-known security standards that could be used to achieve this goal, including IEC 80001 and IEC 62443. The recognition of the standards is a good start, but applying them to healthcare devices and infrastructure requires more knowledge and expertise.

Let's take IEC 80001, for example. From the IEC website: "IEC 80001-1:2010 applies after a medical device has been acquired by a responsible organization and is a candidate for incorporation into an IT-network. It applies throughout the life cycle of IT-networks incorporating medical devices. IEC 80001-1:2010 applies where there is no single medical device manufacturer assuming responsibility for addressing the key properties of the IT-network incorporating a medical device. IEC 80001-1:2010 applies to responsible organizations, medical device manufacturers and providers of other information technology for the purpose of risk management of an IT-network incorporating medical devices as specified by the responsible organization."

So what does this mean? For the medical device manufacturer, this does not apply to an individual device independently but rather to how their device supports and is incorporated into a connected healthcare system that is supporting IEC 80001. So an RFQ that says, "How does your medical device conform to IEC 80001?" may not immediately make sense, but what they are asking is how one operates the device in an IEC 80001 conformant environment.

Conversely, IEC 62443 covers many aspects of industrial control systems but is not specific to medical devices. So you need to understand how to apply it, and how it can assist you in applying a security strategy that meets the end user requirements in order to incorporate your device into an ISO 80001–based healthcare system.

The FDA guidance was also augmented in December 2016 with "Postmarket Management of Cybersecurity in Medical Devices,"[5] which addresses cybersecurity risk management for deployed devices. This guidance states, "Cybersecurity risk management programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm. Manufacturers should respond in a timely fashion to address identified vulnerabilities."

The postmarket guidance also states, "Effective cybersecurity risk management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity. An effective cybersecurity risk management program should incorporate both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to obsolescence. It is recommended that manufacturers apply the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity."[6]

The NIST was founded in 1901 and is now part of the U.S. Department of Commerce. The NIST Framework for Improving Critical Infrastructure Cybersecurity is a set of industry standards and best practices to help organizations manage cybersecurity risk. In particular, the Framework defines the following five Core Functions, which are high-level steps to follow for implementing cybersecurity: Identify, Protect, Detect, Respond, and Recover.

- **Identify:** Cybersecurity begins with identification of the cybersecurity risk to healthcare systems, assets, data, and capabilities.
- **Protect and Detect:** Once the potential threats are identified, manufacturers can start development of specific device security measures to meet the expected threats.
- **Respond and Recover:** Using defense in depth and security techniques, devices in the healthcare system will be able to protect themselves against known attacks and detect attacks in real time. To be truly effective, however, medical device security needs to do more than just detect attacks; it needs to be able to respond quickly to detected attacks. High-level security policies will dictate the actions that need to be taken for each type of detected security event.

CYBERSECURITY STRATEGY

We now have the impetus to consider a cybersecurity strategy, with the regulatory framework flowing down from government and the growing awareness among medical device manufacturers of the high importance of implementing security into their products. This will minimize risk and also secure investments in new business models and next-generation cloud-based solutions.

Let's start with the key stakeholders in the development and implementation of a successful security strategy, discuss their main pain points, and look at their goals.

These are:

- **Medical device manufacturers:** Those who design, build, deploy, and maintain medical devices
- **Healthcare institutions:** Hospitals and other healthcare establishments that use medical devices
- **Regulatory bodies:** Auditors from the FDA, Lloyd's Register, TÜVs, and others
- **Patients:** Those whose conditions are monitored with revolutionary therapies and medication delivery and care beyond hospital walls

Medical Device Manufacturers

Product managers, marketing managers, and service managers in the medical device industry have to make sure they build competitive devices that meet ever-changing regulatory requirements, especially around security. They must quickly find answers to these questions:

- How can we implement a security strategy that:
  - Is clearly and effectively messaged to medical device manufacturers, their sales organization, and their customers?
  - Meets both the end customer requirements (such as IEC 80001) and local security and disaster response laws (such as Katastrophenschutzgesetz in Germany or Federal Disaster Relief Act[7] in the USA)?
  - Supplies all of the correct documentation required by the regulatory authorities?
- Do we have trained staff who understand both safety and security requirements for medical devices?
- How do we support the IT manager of our customers in implementing an IEC 80001 strategy?
  - Further, how do we respond to medical device equipment tenders that specify IEC 80001 and provide the necessary information for the end user to remain IEC 80001 compliant?
- How do we respond to the hospitals' requirements, in terms of innovative methods of treatment, latest medical technology, cost-optimized services, or even completely new business models?
- Should we consider connected medical devices to support the drive toward smart hospitals?
  - How do we address the reservations of hospital operators?
  - How do we enable data transfer to these systems, and do we retain data ownership and privacy?
  - How do we maintain security when transferring data between these systems?

THE CHALLENGES OF CYBERSECURITY IN MEDICAL ENVIRONMENTS

- IT security realized through the full chain of medical devices to the wider IT landscape, from medical institutions to cloud-based applications
- Protection of patient data
- Separation of device data and protected health information
- Law and regulation compliance, e.g., IT Security Law, disaster control laws, international norm IEC 80001

Healthcare Institutions

Directors (business information systems and clinical information systems), IT managers of hospitals, and biomed engineers are confronted with a wave of massive challenges:

- **Pressure for innovation:** Innovation is crucial to survive the competition of hospitals and medical service suppliers.
- **Cost management:** This is vital to stay financially healthy despite increasing case numbers and decreasing funds in the healthcare system.
- **Liability, insurance, and legal requirements:** All of these are constantly increasing, along with demand on IT security, resulting in more complex risk management policies and greater risk aversion (Katastrophenschutzgesetz, IEC 80001).
- **Evolving regulatory agencies and norms:** These put a stronger focus on connectivity of medical devices (FDA, TÜVs, IEC 62304).
- **Implemented IT security:** Improved security has become a must in medical devices in order to respond to ever-increasing security threats, even as it increases the complexity of interoperability among medical device manufacturers.
- **Data generation:** Data can be increasingly used through IoT to help manufacturers become more attractive, spend less, and gain more with new businesses.

CERTIFYING BODIES

Due to the complexity of regulations for medical device security, it is vital while building a security strategy to engage early on with the certifying bodies. This way the device manufacturer or healthcare institution can confirm that the chosen route to a secure system aligns with current regulatory requirements and that they have taken a path that will lead to eventual approval by the certification bodies. This is just as true for verification and validation of safety systems.

WIND RIVER SOLUTIONS FOR MEDICAL DEVICES

As a global leader in embedded technology solutions, Wind River has been deeply involved since its inception in securing devices that perform life-critical functions and comply with stringent regulatory requirements. No single security principle by itself could provide complete protection for a medical device. Rather, it is the proper layering of these defense systems that will provide a much stronger, multifaceted protection. The concept of layering these principles together is known as defense in depth. It follows that the number of industry specifications can be overwhelming, requiring the need for a systematic approach to assessing the security posture of the device.

Wind River has developed, and continues to develop, capabilities built into the base software that add defense at the device level. From operating systems built on secure foundations to ongoing security protection provided by device updates and hot patches, the Wind River portfolio of commercial off-the-shelf products gives developers freedom and the access to rapid innovation promised by new connectivity development, while simultaneously ensuring manufacturers' peace of mind by mitigating security risks.

THE CIA TRIAD

The CIA triad is the foundational security principle for the protection of an asset. Its three components can be thought of as similar to the components of security for the contents of a hospital:

- **Confidentiality:** Defined as maintaining the privacy of an asset. Solid doors, walls, and window coverings provide privacy for the contents of a hospital.
- **Integrity:** Defined as maintaining the content of the asset. An alarm system, a security gate, and entry passes to departments and laboratories maintain the integrity of a hospital, such that the contents of the hospital are kept intact.
- **Availability:** Defined as the accessibility of the asset. The contents of the hospital are available to the healthcare professionals via pass codes to the alarm system and key cards or passes to the departments and laboratories.

In addition, Wind River has worked closely with medical device manufacturers to participate in medical safety and security assessments, providing guidance during the architecture phase; to build the hazard analysis to design and execute tests; and to provide an off-the-shelf (OTS) solution using our operating systems, along with a complete set of IEC 62304 documentation and IEC 62443 supporting evidence. Furthermore, Wind River can provide customized board support packages in an IEC 62304/62443 compliant manner with all tests and documentations for medical safety and security.

> "Wind River helped us develop customized documentation in accordance with IEC 62304 and FDA guidance. We passed the software audit easily and in a timely manner—and we launched the FDA-approved product to the market ahead of schedule."
>
> —Lutz Kersten, Department Manager, R&D
> Surgical Therapy Software, Olympus Surgical

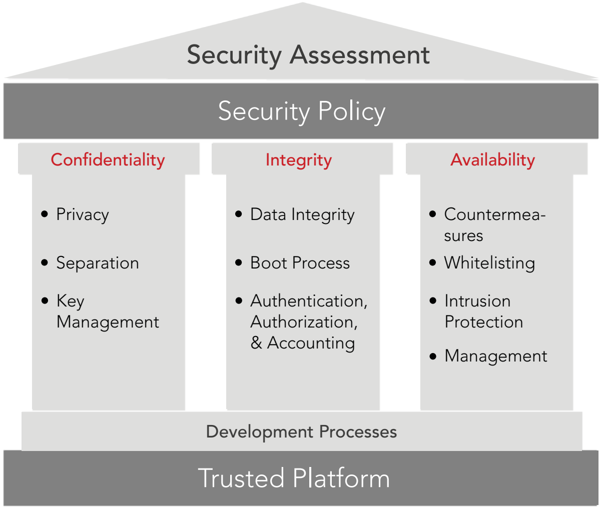


Figure 1. The CIA triad

In order to meet the many requirements of security standards across market sectors, a useful model to map various standards is the CIA triad of confidentiality, integrity, and availability (see Figure 1). This provides a comprehensive framework that allows device manufacturers to build a security strategy that suits their requirements.

Wind River provides security features that can be layered together to provide the level of security defined by a medical device's security requirements. For example, Wind River provides security profiles for our operating systems, VxWorks® and Wind River Linux:

VxWorks security profile features:

- Advanced user management
- Encrypted containers and disks
- TPM 1.2 and TrouSerS
- TPM 2.0 and TPM2-TSS
- Security events handler
- Secure boot
- Secure loader
- Extensions to IKE (SCEP and GDOI)
- Support for ARM TrustZone
- Achilles Level 2 certification
- Support for AD/LDAP
- Non-executable pages
- SSH client
- Digitally signed binaries

Wind River Linux security features:

- Mandatory access control (MAC)
- Integrity managed architecture (IMA) and secure remote management (SRM)
- Pluggable authentication modules (PAMs)
- Root of trust (RoT)
- Secure boot
- Trusted Platform Module (TPM)
- Package management
- Hardened kernel and secure user space
- OpenSCAP

PREDICTIVE MAINTENANCE AND SECURITY MONITORING

Device manufacturers are increasingly including security functionality at the earliest stage of design. That's a good thing—in fact, it's essential—but it's not enough. Threats are constantly evolving. Operators of medical systems need a mechanism to maintain security of devices over their entire useful life.

Manufacturers need to rethink their security strategies with an eye not only on system-level reinforcing but also on agile integration of new vulnerability patches. Unless systems are constantly updated, they run the risk of being vulnerable to emerging threats.

Common Vulnerabilities and Exposures (CVE) is the widely accepted, de facto industry standard for identifying, repairing, and reporting vulnerabilities. Using CVE identifiers, information about a vulnerability can be correlated to appropriate security patches or protection technologies, which is especially vital in the open source software world.

The Wind River security team is constantly monitoring security vulnerabilities, including specific security notifications from U.S. government agencies and organizations such as NIST, the United States Computer Emergency Readiness Team (US-CERT), and public and private security mailing lists, as well as the CVE database at cve.mitre.org. We also receive alerts from each of these organizations whenever a new security threat arises. Alerts include both community-confirmed and potential vulnerabilities, and we look into all of them. Constant monitoring lets us know about—and make patches available for—vulnerabilities that affect our products, sometimes even before the community publicly announces the vulnerability. When possible, we release patches to high-profile, critical vulnerabilities in coordination with the initial public disclosure.

Ongoing threat mitigation in deployed systems requires a four-step approach: monitoring, assessment and prioritization, notification, and remediation.

- **Monitoring:** Active monitoring of security alerts from reliable external sources, customers, and any other external submitters. During this stage, the team actively monitors specific security notification email lists.
- **Assessment and prioritization:** Assessment and prioritization of vulnerabilities based on severity, difficulty, and avoidability of alerts. Note that difficulty refers to the degree to which the vulnerability could be exploited, not the difficulty of fixing the issue.
- **Notification:** Notifying customers and the submitter of the level of susceptibility, within a short time frame.
- **Remediation:** Posting of the remediation action based on the classification of susceptibility, and within a short time frame (usually within 24 hours).

WIND RIVER PROFESSIONAL SERVICES

These security features can be augmented to meet specific customer requirements by Wind River Professional Services, which can provide:

- Security assessment and planning
- Safety, compliance, and security requirements
- Development and integration
- Long-term platform management

The Wind River security assessment offering is a systematic approach to defining the required security of the medical device. The security assessment provides a clear identification of assets, vulnerabilities, risks, and regulatory requirements of the device while balancing against cost, preformance, and the defined operational environment. The output of this security assessment is the security policy. The security policy defines what is meant to protect the identified assets in the system. This includes the security implementations to use, the security audit events to log, and the responses to those security audit events.

In order to meet the many requirements of security standards across market sectors, the security assessment uses the CIA triad (see Figure 1) to embody the security implementations required to be conformant to the various standards for the solution. This provides a comprehensive framework that allows our customers to build a security strategy that suits their requirements.

As an example, if the medical device manufacturer has chosen to use HIMSS/NEMA Standard HN 1-2013 in order to map to ISO 80001, then a consulting security assessment would lead to mapping as per Figure 2, CIA triad mapped to HIMSS/NEMA.

The security assessment contains the following major sections:

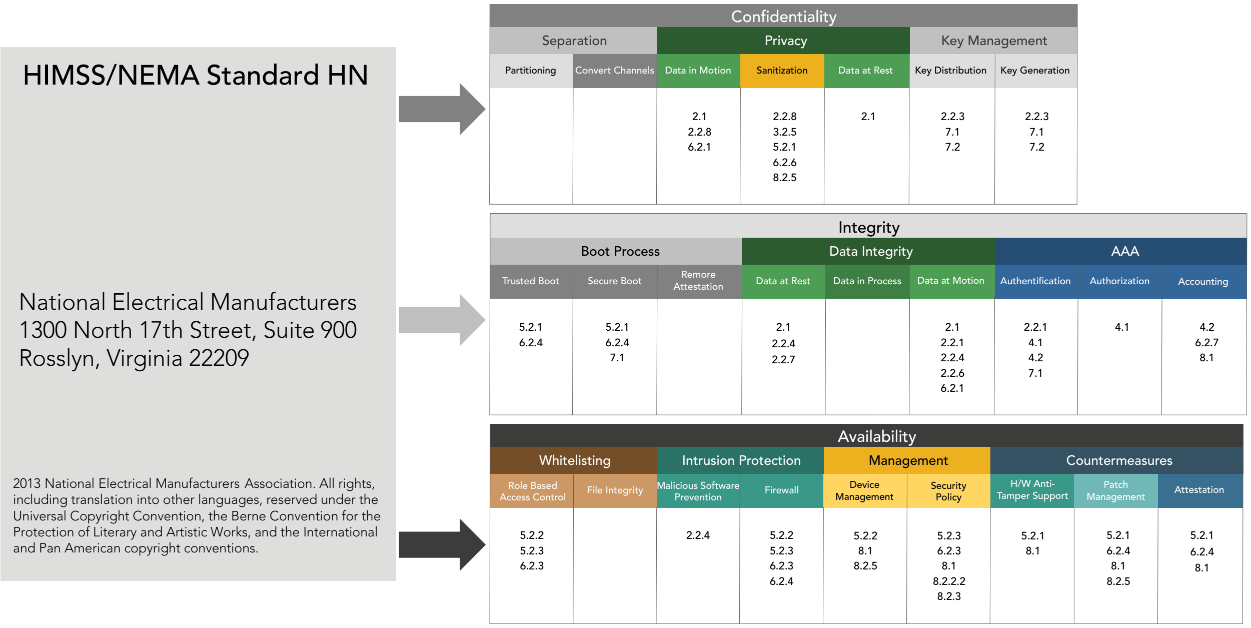
- **General information:** Because security means different things to different people, a baseline is defined.
- **Assets and vulnerabilities:** Assets within the device, and their vulnerabilities, are identified.
- **Security policy:** How those assets are protected from the vulnerabilities is described.
- **Implementation notes:** Specific security implementations are recommended.
- **Priority of recommendations:** The cost, performance, and operational environment are balanced and prioritized.

The security assessment leverages the security features of best-in-class products from Wind River to define a comprehensive security solution for the medical device.

WHEN IT MATTERS, IT RUNS ON WIND RIVER

The drive toward digital business transformation that enables a digital healthcare system, with all of the benefits of shared healthcare data, is inevitable. This requires both medical device manufacturers and end users to consider the new concerns of cybersecurity, in order to meet regulatory requirements and mitigate risk for their company brand and reputation.

This is no longer a "nice to have" device feature. It has to be built into the entire device lifecycle, not only in its design, development,



HIMSS/NEMA Standard HN

National Electrical Manufacturers
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

2013 National Electrical Manufacturers Association. All rights, including translation into other languages, reserved under the Universal Copyright Convention, the Berne Convention for the Protection of Literary and Artistic Works, and the International and Pan American copyright conventions.

Confidentiality						
Separation		Privacy			Key Management	
Partitioning	Convert Channels	Data in Motion	Sanitization	Data at Rest	Key Distribution	Key Generation
		2.1 2.2.8 6.2.1	2.2.8 3.2.5 5.2.1 6.2.6 8.2.5	2.1	2.2.3 7.1 7.2	2.2.3 7.1 7.2

Integrity								
Boot Process			Data Integrity			AAA		
Trusted Boot	Secure Boot	Remore Attestation	Data at Rest	Data in Process	Data at Motion	Authentification	Authorization	Accounting
5.2.1 6.2.4	5.2.1 6.2.4 7.1		2.1 2.2.4 2.2.7		2.1 2.2.1 2.2.4 2.2.6 6.2.1	2.2.1 4.1 4.2 7.1	4.1	4.2 6.2.7 8.1

Availability								
Whitelisting		Intrusion Protection		Management		Countermeasures		
Role Based Access Control	File Integrity	Malicious Software Prevention	Firewall	Device Management	Security Policy	H/W Anti-Tamper Support	Patch Management	Attestation
5.2.2 5.2.3 6.2.3		2.2.4	5.2.2 5.2.3 6.2.3 6.2.4	5.2.2 8.1 8.2.5	5.2.3 6.2.3 8.1 8.2.2.2 8.2.3	5.2.1 8.1	5.2.1 6.2.4 8.1 8.2.5	5.2.1 6.2.4 8.1

Figure 2. CIA triad mapped to HIMSS/NEMA

and manufacturing but also in operational aspects, such as security updates, and how the device will operate in an IEC 80001 conformant healthcare environment. This becomes a crucial part of device manufacturers' success in operating against both existing and new competition.

Wind River can help with medical device development and can ensure usage of the latest best practices. By properly designing security into medical devices, financial damage, reputational damage, and potential risk to human lives can be avoided.

As a global leader in embedded technology solutions, Wind River has been deeply involved since its inception in securing devices that perform life-critical functions and comply with stringent regulatory requirements. Our solutions and support have helped many medical device manufacturers meet their regulatory demands and time-to-market requirements throughout the product lifecycle.

REFERENCES

1. Wind River. "Internet of Things Security Is More Challenging Than Cybersecurity." www.windriver.com/whitepapers/security/iot-security-is-more-challenging-than-cybersecurity/#sthash.kIKPnaCE.dpuf.
2. Cisco 2016 Annual Security Report. www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html.
3. Lily Hay Newman. "Medical Devices Are the Next Security Nightmare." *Wired*. March 2, 2017. www.wired.com/2017/03/medical-devices-next-security-nightmare.
4. Food and Drug Administration. "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." October 2, 2014. www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf.
5. Food and Drug Administration. "Postmarket Management of Cybersecurity in Medical Devices." December 28, 2016. www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf.
6. National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." January 2016. www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
7. Federal Emergency Management Agency. "Overview of Federal Disaster Assistance." training.fema.gov/emiweb/downloads/is7unit_3.pdf.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.