Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality

Fubin Wu and Sherman Eagles

The need for effective cybersecurity to ensure safety and functionality of networks used for healthcare has become more important with increased use of wireless communication, Internet- and network-connected medical devices, and the frequent electronic exchange of medical device–related health information. It is well understood that responsibility for cybersecurity must be shared between medical device manufacturers and the organizations that control and manage networks. Manufacturers are expected to provide information, such as the Manufacturer Disclosure Statement for Medical Device Security,[1] to healthcare organizations (e.g., hospitals) and conduct cybersecurity risk analysis per Food and Drug Administration (FDA) guidance.[2]

Although cybersecurity is a relatively new subject to medical device manufacturers, safety risk management is not. Most medical device manufacturers have established safety risk management practices in compliance with applicable regulations and/or ANSI/AAMI/ISO 14971:2007.[3] How can manufacturers conduct cybersecurity risk analysis by leveraging their familiarity with the existing risk management framework? What cybersecurity documentation is needed to meet premarket submission requirements per the FDA guidance?[2]

Using examples, the current work illustrates how cybersecurity risk analysis can be performed by device manufacturers in leveraging safety risk analysis practices and how the cybersecurity risk analysis results can be documented to meet the premarket submission requirements and to communicate with other stakeholders. The methods are not meant to be exclusive. The examples are based on an insulin pump system (Figure 1) and previous research.[4,5] Also of note, the examples are based on highly abstract information and are meant to illustrate the cybersecurity analysis methods rather than the completeness and accuracy of the technical analysis results.

Furthermore, for the examples used in this article, the insulin pump system is defined as consisting of a pump that can deliver insulin programmatically and a meter remote. The meter remote is a combined device consist-

About the Authors

Fubin Wu is cofounder of GessNet risk management software in Sacramento, CA. Email: fubin.wu@gessnet.com

Sherman Eagles is partner at SoftwareCPR, lead instructor for the AAMI Safety Assurance Cases for Medical Devices course, and former technical fellow at Medtronic. Email: seagles@softwarecpr.com

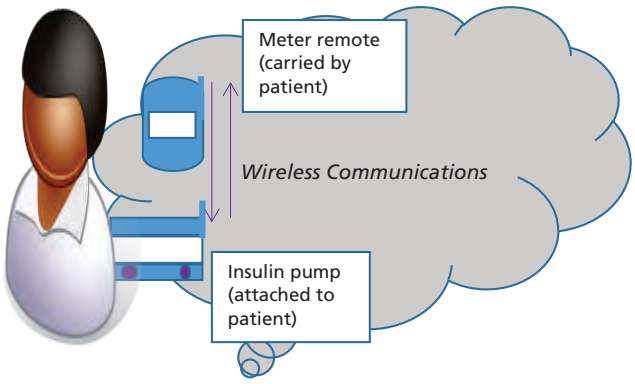

Figure 1. Example of an insulin pump system

ing of a remote control and a blood glucose meter that can program the pump remotely, take blood samples to check blood glucose levels, and send the results to the pump. The communications between the pump and meter remote occur wirelessly.

Medical Device Safety Risk Analysis

The ANSI/AAMI/ISO 14971–based risk analysis methodology is illustrated in Figure 2 (further explanation provided in Wu and Kusinitz[6]).

To ensure that a device is safe for its intended use, device manufacturers need to 1) have a comprehensive understanding of device-applicable hazards, hazardous situations, and causes (including conditions and events), as well as their roles in contributing to potential harm(s), and 2) identify and implement risk control(s) whenever appropriate to prevent the potential harm(s) from occurring. To accomplish these objectives, during the system design phase, device manufacturers typically begin by identifying top system hazards, hazardous situations, and potential harm(s) as applicable to a device and defining system-level risk controls. As subsystem and detailed design information become available, causes (including conditions and events in sequence) of hazardous situations can be further identified, analyzed, and mitigated. The typical methods to identify these causes, controls, and interrelationships (i.e., causal chains) include top-down analysis (e.g., fault tree analysis) and bottom-up analysis (e.g., failure mode effects analysis [FMEA]).[7] A risk control eliminates the causes, prevents the causes from becoming hazardous situations or harms, or reduces the severity of potential harms. It is possible to apply multiple risk controls at multiple stages of risk propagation throughout a causal chain leading to harm (Figure 2). An example of system hazard analysis is shown in Figure 3.

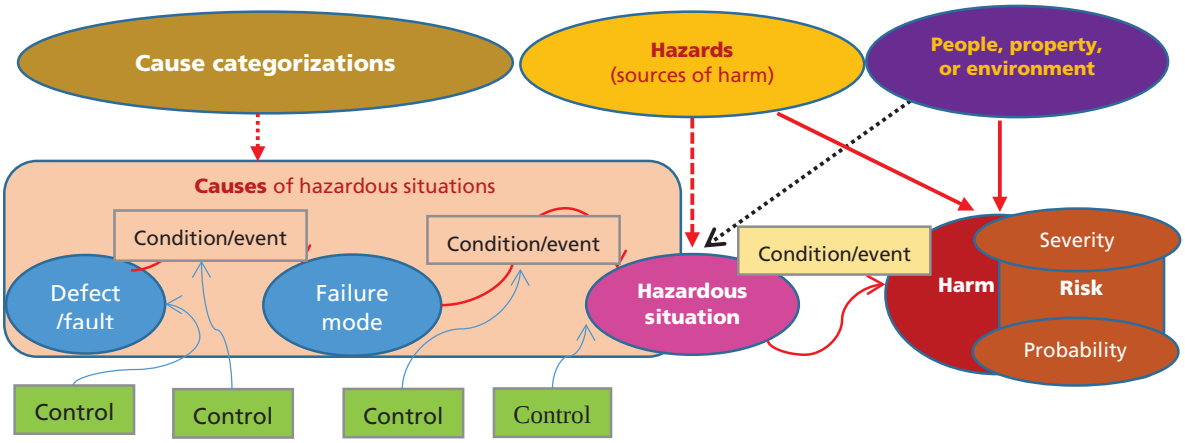

Figure 2. Causal chain illustration of risk analysis methodology, according to ANSI/AAMI/ISO 14971:2007

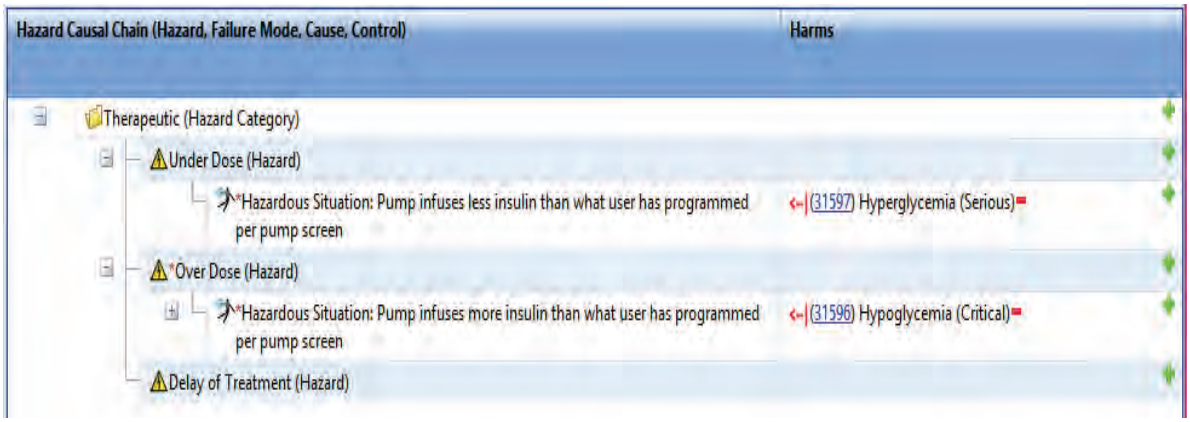

Figure 3. Example of system hazard analysis

Of note, "asset" (i.e., the subject in need of protection)—a term commonly used in security standards—is not used in ANSI/AAMI/ISO 14971. However, the definition of "harm" (i.e., physical injury or damage to people's health, damage to property or the environment) per ANSI/AAMI/ISO 14971 implies that subjects in need of protection include people, property, and the environment. In other words, people, property, and the environment are the "assets" to be protected according to ANSI/AAMI/ISO 14971.

Medical Device Cybersecurity Risk Analysis

Cybersecurity is necessitated by the proliferation of electronic computing (i.e., software), networking, and wireless communication technologies. Many of today's medical devices and healthcare systems use or rely on electronic technologies and therefore must address cybersecurity.

Per FDA guidance, "Cybersecurity is the process of preventing 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."[2] Generally speaking, cybersecurity can be regarded as the state of electronic information being protected from potential damage to its confidentiality, integrity, and availability (CIA). Cybersecurity analysis involves understanding the following:

- What needs to be protected (i.e., assets)
- What threats (and attacks) are potentially applicable
- What are the potential cybersecurity harms and associated effects if an exploit occurs, and how security harm is connected to safety risk
- What are the potential scenarios (i.e., system vulnerabilities) that expose assets (to the threats)
- What are the potential causes (e.g., basic vulnerabilities, conditions, events) that can result in system vulnerabilities
- What cybersecurity risk controls are needed to protect the assets and mitigate risks
- How cybersecurity risk is connected with safety risk
- How to document cybersecurity for internal or external review purpose (e.g., submissions to FDA)

A medical device manufacturer that already has established sound safety risk management practices can address cybersecurity through leveraging its experiences with safety risk management.

Similar to safety risk analysis per ANSI/AAMI/ISO 14971, a cybersecurity risk analysis can be illustrated using a causal chain concept (Figure 4). With this approach, a medical device manufacturer that already has established sound safety risk management practices can address cybersecurity through leveraging its experiences with safety risk management.

Identifying and Protecting Assets

Cybersecurity asset identification for a medical device can start with identifying the electronic information that needs to be protected based on the device's intended use,

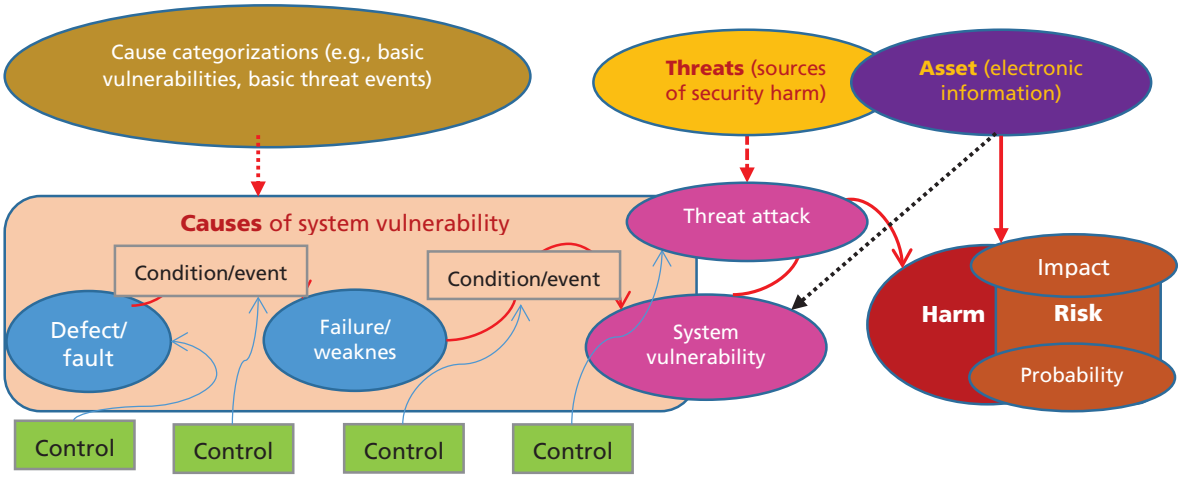

Figure 4. Causal chain illustration of cybersecurity risk analysis methodology

use environment, patient, user and customer needs, and other stakeholder interests (e.g., hospitals' requirements for personal health data privacy). The electronic information for a medical device in general can fit into one or more of the following categories: network-communicated information, health information, software information, and information that may need protection from a business perspective. These categories help to ensure adequate coverage and do not need to be orthogonal. Figure 5 provides an example of cybersecurity asset identification. Although there could be multiple layers of other systems, subsystems, and components that ought to be protected from a cybersecurity perspective, identifying the electronic information that ultimately needs to be protected would be beneficial. During development of a new medical device, this asset identification process should take place as early as the product concept phase, just as the safety risk management process should proactively identify the different groups of people and environments with which the device may interact so that their safety can be considered in the risk analysis.

For new product development, given the evolving nature of threats, an efficient approach is to assume that assets requiring protection will always be under threat.

Identifying Threats and Attacks

As illustrated in Figures 2 and 4, similarities exist between the ANSI/AAMI/ISO 14971 safety risk analysis methodology and the cybersecurity risk analysis methodology. ANSI/AAMI/ISO 14971 defines hazard as a potential source of harm. Different security standards may have slightly different definitions for cybersecurity threat, but for medical device manufacturers, threat can be viewed as a potential source of cybersecurity harm (i.e., potential sources of damage to electronic information's CIA). This source of cybersecurity harm (threat) is a person or thing (actor) that has the potential or intent (deliberate or undeliberate) to damage cybersecurity. Similar to hazard identification for safety risk, threat identification can start with commonly known categories of threat sources and identify specific potential threat actions/events (i.e., threat attacks) that can cause damage to security assets. As discussed previously,[6] similar to differentiating top-level hazards from low-level hazards (i.e., causes), it would be beneficial to differentiate threats that directly compromise the CIA of security assets from those that create vulnerabilities that can be exploited to compromise CIA and can indirectly cause security concerns. For new product development, given the evolving nature of threats, an efficient approach is to assume that assets requiring protection will always be under threat. With this approach, once assets are identified, the top threat attacks can be identified fairly easily. Preliminary threat analysis can be started as early as the product concept phase, in order to identify applicable threats and potential associated attacks to cybersecurity assets. System design documents, such as system/feature description, system architecture, and use cases, should be used to inform this analysis. An example of a threat analysis is shown in Figure 6.

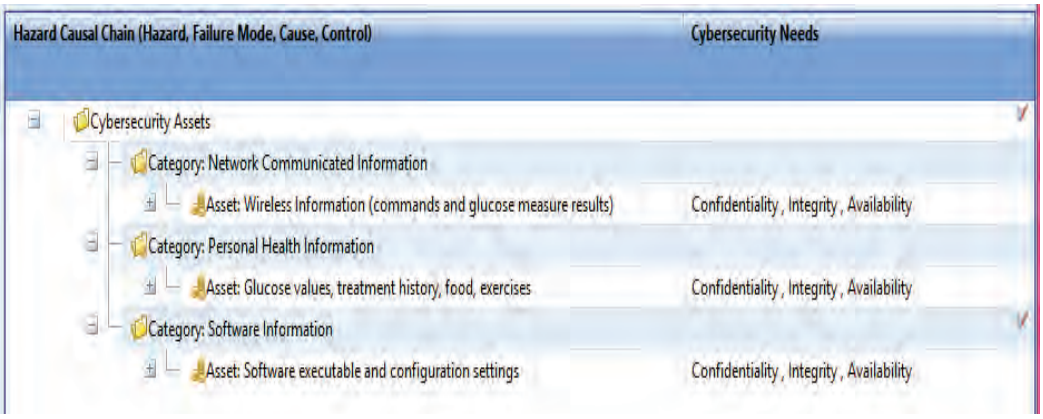

Figure 5. Example of cybersecurity asset identification

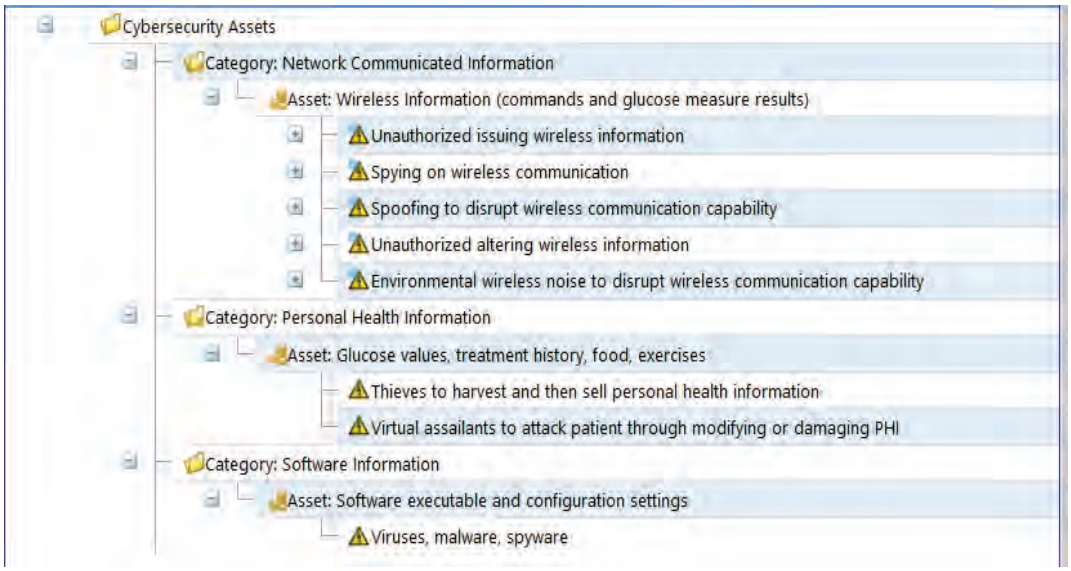

Figure 6. Cybersecurity threat identification

Identifying Security Harms and Potential Effects

In ANSI/AAMI/ISO 14971, harm is defined as damage to people, property, or the environment. Taking a similar approach, cybersecurity harm can be viewed as damage to an electronic information asset's CIA. For an identified asset, given a specific attack scenario, one should be able to identify potential associated cybersecurity harms. Common cybersecurity harms against electronic information include unauthorized access, use, or modification. For medical devices, cybersecurity harms should be further evaluated to determine whether they can cause a hazardous safety situation. This is particularly important from an FDA premarket regulatory perspective, as device safety is an important agency concern. When cybersecurity harm can affect safety, the cybersecurity system vulnerability must be recognized as a cause for safety harm and connected with safety risk analysis. Figure 7 is an example of how cybersecurity risks and safety risks can be connected for the insulin pump system.

Regardless of whether safety could be affected, cybersecurity harm remains a concern to medical device manufacturers and healthcare organizations. For example, hospitals may require medical device vendors to ensure that the confidentiality of personal health information is adequately protected. Therefore, device manufacturers should define cybersecurity risk ranking and acceptance criteria in addition to existing safety risk acceptance criteria.

Identifying Potential System Vulnerabilities

Vulnerability in cybersecurity analysis is defined as "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."[8] According to this definition, vulnerabilities as causes of cybersecurity harms can come from different sources, including use errors, malicious activities, system performance issues, inadequate device functionality, bad design choices, and software defects. From a security harm causal chain perspective, there must be an occurrence of vulnerability that directly exposes an asset to a top threat (attack) before security harm can occur. We call this vulnerability a system vulnerability.

System vulnerability in cybersecurity risk analysis is similar to a hazardous situation in safety risk analysis. Whereas hazardous situation is defined as a circumstance in which people, property, or the environment is exposed to a hazard, system vulnerability can be viewed as a circumstance in which a security asset(s) is exposed to one or more threats (attacks). The sequence of events and conditions leading to this exposure typically would include a combination of events (e.g., user errors, malicious activities) and lower-level vulnerable condition(s) (i.e., basic

vulnerabilities). For potential threat attacks identified, system vulnerability analysis works to identify anticipated potential scenarios of the exposures. Figure 8 provides an example of system vulnerability identification for an insulin pump system.

Causal Chain Analysis of System Vulnerabilities

Similar to safety risk analysis methods, to comprehensively understand cybersecurity harm causal chains (as shown in Figure 4), multiple analysis techniques should be considered. In general, these analysis techniques can be considered as either a top-down or bottom-up approach. As reported previously,[7] whenever possible, both top-down and bottom-up analyses should be considered.

A top-down analysis of cybersecurity can begin with identifying system vulnerabilities; then identifying causes, conditions, and events that can lead to system vulnerabilities; then further identifying where and what

Whereas hazardous situation is defined as a circumstance in which people, property, or the environment is exposed to a hazard, system vulnerability can be viewed as a circumstance in which a security asset(s) is exposed to one or more threats (attacks).

Claim: [Network Communicated Information is protected]	Security Harms	Safety Effect (Immediate Effect > Hazardous Situation > Harm)
*Network Communicated Information is protected		
Asset: Wireless Information (commands and glucose measure results)		
*Unauthorized issuing wireless information	<-|(31621) **Unauthorized wireless commands to infuse insulin (Major)**	(31706) Pump infuses more insulin than what user has programmed per pump screen > (31596) **Hypoglycemia (Critical)**
Spying on wireless communication	<-|(31620) **Patient PHI is disclosed (Major)**	
Spoofing to disrupt wireless communication capability	<-|(31622) **Compromised wireless communication capability (Moderate)**	(31707) User not able to issue remote commands due to non available or degraded wireless communications > (31623) **Delay of Insulin Treatment (Minor)** (31707) User not able to issue remote commands due to non available or degraded wireless communications > (31597) **Hyperglycemia (Serious)**
Unauthorized altering wireless information	<-|(31621) **Unauthorized wireless commands to infuse insulin (Major)**	(31706) Pump infuses more insulin than what user has programmed per pump screen > (31596) **Hypoglycemia (Critical)**
Environmental wireless noise to disrupt wireless communication capability	<-|(31622) **Compromised wireless communication capability (Moderate)**	

Figure 7. Security harm impact on safety

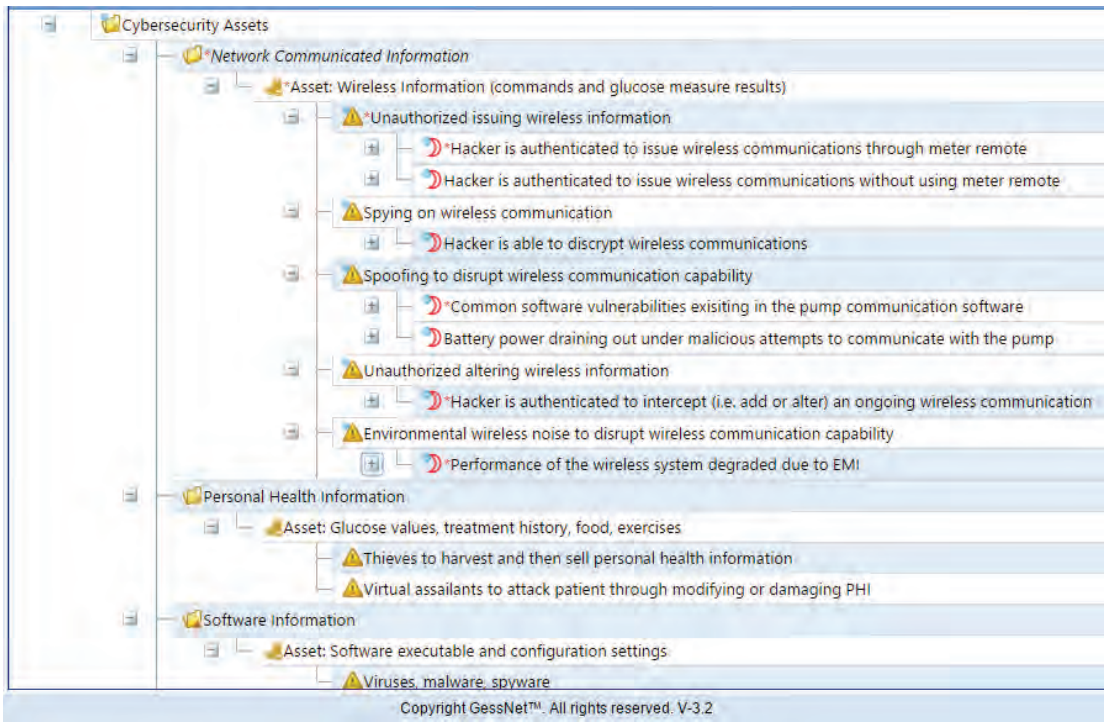

Figure 8. Example of cybersecurity threat exposure (i.e., system vulnerability) identification

cybersecurity control measure(s) can be applied. The result captured in this analysis could include a series of malicious activities from threat (sources) and corresponding vulnerable conditions. As such, this analysis also can be called an "attack tree" in the cybersecurity world. This top-down analysis approach can start as early as the product concept phase based on system level information. Figure 9 shows a conceptual example of this analysis.

A bottom-up analysis (e.g., FMEA, common cause analysis) of cybersecurity risk can begin with a particular subsystem, process, component, or category of common causes (e.g., common or known threat events and/or vulnerabilities), then identify potential failure modes, limitations, or degraded performance and associated local effect(s) and end effect(s) to electronic information assets. Figure 10 provides an example of how a bottom-up analysis can be performed.

For either top-down or bottom-up analysis, data visualization, such as data/information modeling diagrams, can be helpful. While not physically visible,

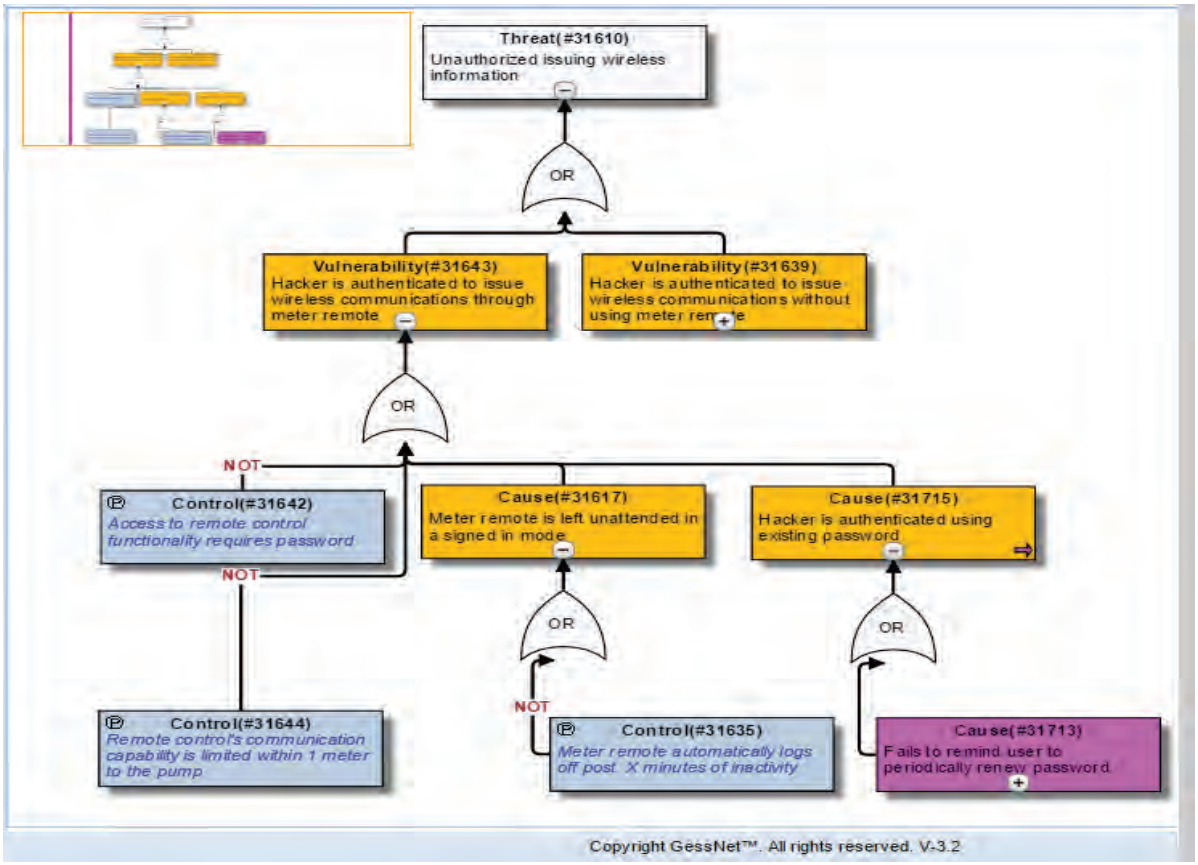

Figure 9. Example of fault tree/attack tree analysis for cybersecurity

Causal Chain (Failure Mode, Cause, Control)	Harms Local Effect >> End Effect	Security Harms Local Effect >> End Effect
Security FMEAs		
Sub-System or Component		
Function		
Failure Modes or Limitations		
Meter Remote Authentication Process		
Prevent unauthorized use of the meter remote		
Fails to remind user to periodically renew password	(31706) Hazardous Situation: Pump infuses more insulin than what user has programmed per pump screen >> (31596) **Hypoglycemia (Critical)**	(31715) Hackers is authenticated using existing password >> (31621) **Unauthorized wireless commands to infuse insulin (Major)**
Fails to automatically logout	(31617) Meter remote is left unattended in a signed in mode >> (31596) **Hypoglycemia (Critical)**	(31617) Meter remote is left unattended in a signed in mode >> (31621) **Unauthorized wireless commands to infuse insulin (Major)**

Figure 10. Failure mode effects analysis–like, bottom-up analysis of cybersecurity vulnerability and causes

electronic information (e.g., software) has a "life journey" in terms of its origination, storage, transmission, distribution, operational use, and disposition. To ensure causes of system vulnerabilities are adequately identified, visualizing the electronic information's journey, including interactions with other elements of the system, would be useful. Data modeling (e.g., data flow diagram) is a typical method for this visualization. A data modeling diagram can be at the system level or at a subsystem or component level and can be used as input to both top-down and bottom-up analysis, as well as serving as reference of context information for a reviewer to understand the cybersecurity analysis.

Cybersecurity Risk Controls and Security Capability

In general, risk controls are used to reduce the likelihood or severity of an undesirable event (e.g., a system vulnerability). From that perspective, cybersecurity risk controls are not different from safety risk controls. Referring to the causal chain analogies for safety and cybersecurity risk (Figures 2 and 4), it is possible to apply multiple risk controls at various stages of the causal chain to reduce the risk. Compared with safety risk controls, special considerations should be given when identifying and defining cybersecurity risk controls.

Considering potential malicious attacks on software, it would be realistic to assume that any software system may contain latent defects that will be exposed under malicious attack.

Risk Controls on Threat Attacks. Refer to Figures 2 and 4 for the safety and security harm causal chains. For safety risk, for the harm to occur, a hazardous situation must be present. To reduce the likelihood of safety harm, one can focus on reducing the probability of a hazardous situation occurring. For security risk, for the harm to occur, a system vulnerability and successful threat attack must be present. In addition to risk controls aiming at reducing the likelihood of system vulnerability, control options that can reduce the likelihood of threat attack initiation (e.g., reduce attractiveness) or reduce the likelihood of threat attack success also should be considered.

Risk Controls via Fail Safe Design. Refer to Figures 2 and 4 for the causal chain risk analysis methodology. Theoretically, the most desirable risk control is to eliminate the basic causes; however, this elimination is sometimes impossible or too costly. For example, software vulnerability is one of the common vulnerabilities that potentially cause system vulnerabilities to expose cybersecurity assets to ultimate threat attacks. Software vulnerability results from imperfection or unreliability of the software. From a software reliability engineering perspective, defect-free (i.e., perfect) software is almost impossible, or the cost to achieve defect-free software is too high to be practical. Considering potential malicious attacks on software, it would be realistic to assume that any software system may contain latent defects that will be exposed under malicious attack. Given that reality, in addition to minimizing software vulnerabilities, consideration should be given to control risks by preventing 1) a software defect from being exposed (i.e., being triggered), 2) the exposure of the defect (i.e., failure mode) from becoming a system vulnerability, or 3) the system vulnerability from becoming a cybersecurity harm.

For example, in a case of confidentiality of sensitive data potentially being compromised due to an attack exploiting an insulin pump's communication software, a fail-safe design can be applied to add additional encryption on the sensitive data.

Risk Controls via Proactive Detectability and Recovery. The purpose of cybersecurity is to protect electronic information assets. Electronic information is invisible, and damage to it is not necessarily as noticeable as damage to people or other physical assets. In addition, hackers are unlikely to report or claim their malicious intent or exploitation, whereas medical device users or patients likely would file complaints in case of harmful situations. These factors underscore the importance of detecting cybersecurity threat attempts and recovering from exploitation. The detectability and recoverability should be considered part of the inherent design features when possible, as well as proactive postmarket cybersecurity monitoring. Examples of risk controls through inherent design include 1) implementing features that allow for cybersecurity compromises to be recognized, logged, and acted upon and 2) providing methods for retention and recovery of device configuration by an

authenticated system administrator.

Existing medical device adverse event or complaint handling processes are mostly reactive. Postmarket cybersecurity vigilance should be proactive in monitoring cybersecurity attacks or related incidents.

Balance Cybersecurity Risk Controls and Usability. As pointed out in the FDA guidance, "manufacturers should also carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment of use (e.g., home use vs. healthcare facility use) to ensure that the security capabilities are appropriate for the intended users."[2] For an example, a cybersecurity feature, such as requiring a password in order to access certain functionality, can cause delay of treatment, potentially resulting in a hazardous situation. Before it is applied, a cybersecurity risk control needs to be analyzed to determine whether it has the potential to become a cause of a hazardous situation. Consideration also should be given to balance the level of cybersecurity control and its impact on usability and safety. As such, cybersecurity risk analysis and existing safety risk management need to be connected and synchronized so both cybersecurity and safety effects can be recognized and balanced. Figure 10 provides an example of how this integration and synchronization can be accomplished.

Cybersecurity Risk Control Decisions. The cybersecurity risk control decision-making process is complicated by the software involved, unidentified hackers, malicious attacks, continuously evolving threats, and potentially conflicting effects between security controls and safety. Adopting security standards can be helpful to this decision-making process. The National Institute of Standards and Technology (NIST) cybersecurity framework[9] identifies various security standards that can be applied by manufacturers. In addition, IEC/TR 80001-2-8,[10] which maps risk controls in standards to security capabilities identified in ANSI/AAMI/IEC TIR80001-2-2:2012,[11] is currently in press. However, no single standard provides all needed controls that suit all situations. This challenge makes it important to document the rationale behind cybersecurity decisions, regardless of whether risk control decisions are based on standards, good practices, or other factors. The rationales not only provide baseline knowledge for the manufacturers to continue to monitor and balance the security capability but also help both internal and external reviewers to perform effective reviews.

Proactive Implementation of Cybersecurity Capability. For a given device concept and intended use and use conditions, it is possible to foresee relevant threats (and threat attacks), how assets can potentially be exposed to threats, and the potential security impact without much detailed design information. This makes it possible for device designers to identify cybersecurity capability needs before actual design or implementation information is available. ANSI/AAMI/IEC TIR80001-2-2:2012 identifies 19 security capabilities appropriate for connected medical devices, and standards referenced in the NIST framework[11] provide rich resources for selecting which security capability level should be implemented and what security control requirements should be applied.

Ensuring Connectivity between Cybersecurity Risk and Safety Risk

Cybersecurity risk and safety risk should be connected, synchronized, and informed by each other due to their cause-effect relationships (examples in Figures 10 and 11). Accomplishing this can be a challenge because cybersecurity risk analysis and safety risk analysis require different technical expertise and may even be owned by different groups. Frequently, the technical expertise (e.g., network and information security) resides with information technology (IT) organizations or cloud vendors and expertise on device application and design resides with research and development organizations. Traditional IT security organizations may be good at securing the tunnels through which information travels. However, without adequate device knowledge, they may not have insight into the most critical assets, potentially resulting in security controls being added that impair a device's functionality and safety. On the other hand, device design and safety risk management personnel may not have the experience, skill set, or tools for dealing with cybersecurity.

How can potential gaps in expertise and among organizations be bridged? First, making one unit responsible for a manufacturer's overall risk management program would be helpful. This unit should oversee both device safety and cybersecurity risk to ensure the balance, consistency, and sharing between the two. Second, safety and cybersecurity critical information (e.g., safety risk management file and cybersecurity risk management file) need to be connected and readily available when needed. For example, when performing safety risk analysis, one should be able to see the corresponding effect on cybersecurity or vice versa. Figures 7, 10, and 11 show how safety and cybersecurity information can be linked electronically.

Demonstrating and Communicating Cybersecurity

The completeness and adequacy of the cybersecurity risk analysis needs to take into account the following layers of information:

- Are cybersecurity critical assets completely identified?
- Are applicable cybersecurity threats adequately identified?
- Are system vulnerabilities, subsystem vulnerabilities, and causes adequately identified?
- Are cybersecurity risk controls adequate and correctly implemented?

These are typical questions facing reviewers/stakeholders who want to know whether cybersecurity is adequately ensured for a medical device. Due to the typical involvement of software and malicious activities, having a scientifically quantitative cybersecurity risk assessment can be difficult. Lacking a quantitative assessment, the associated logic, qualitative criteria, and rationales should be documented. As discussed previously,[7] assurance cases provide a method for addressing these questions and presenting the information in a format that can facilitate the review process.

Table 1 shows the structure of a cybersecurity assurance case and Figures 12 and 13 provide examples with detailed content for the wireless communication asset assurance case.

Assurance cases are no longer new to the medical device industry, as FDA has been recommending infusion pump manufacturers to "submit your information through a framework known as a safety assurance case."[12] The FDA infusion pump guidance can serve as a good resource for medical device manufacturers to learn how to adopt the assurance case method on cybersecurity. Additional sources of information include an international standard for assurance cases (ISO/IEC 15026-2:2011[13]) and an international technical report (IEC/TR 80001-2-9[14]) that is being developed to provide guidance for medical device cybersecurity assurance cases.

Conclusion

Cybersecurity is a relatively new challenge facing medical device manufacturers. Although differences exist between cybersecurity and safety analyses, there are many similarities in the systems thinking, analysis techniques, and documentation methods required for each. By leveraging their familiarities with ANSI/AAMI/ISO 14971–based safety risk management practices, medical device manufacturers can overcome the cybersecurity challenge. Recognizing this, AAMI is developing a technical information report (TIR) for medical device cybersecurity risk management (ANSI/AAMI/ISO

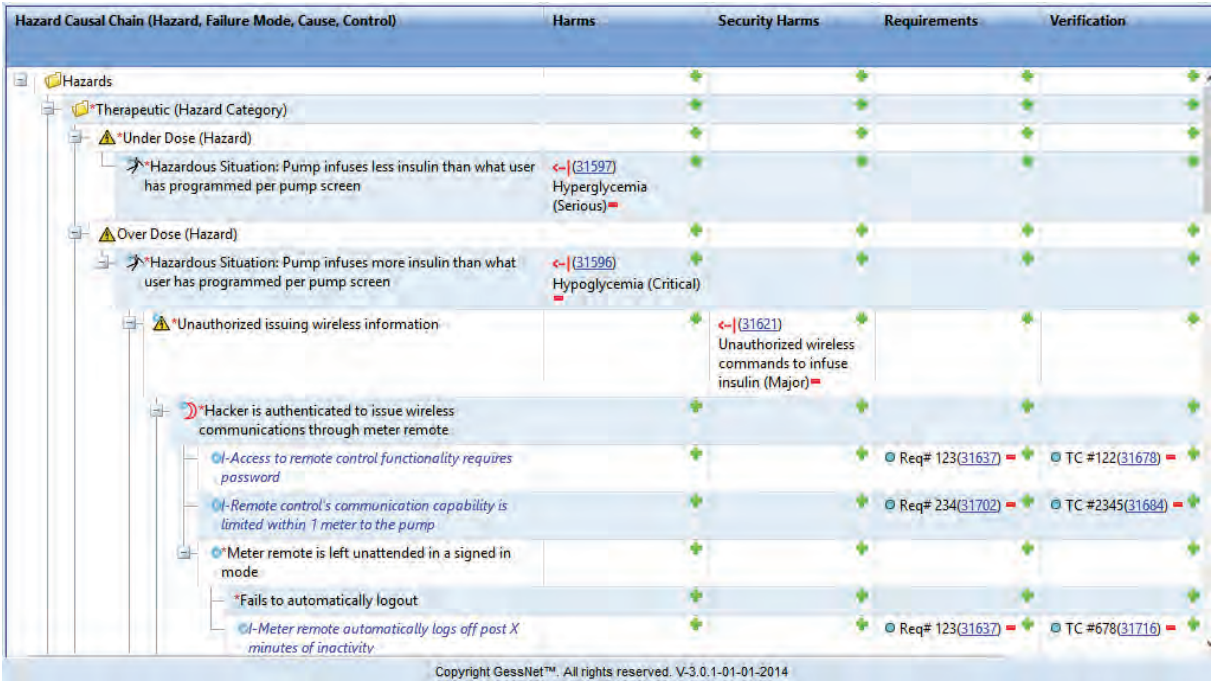

Figure 11. Example of integration of cybersecurity and safety analysis

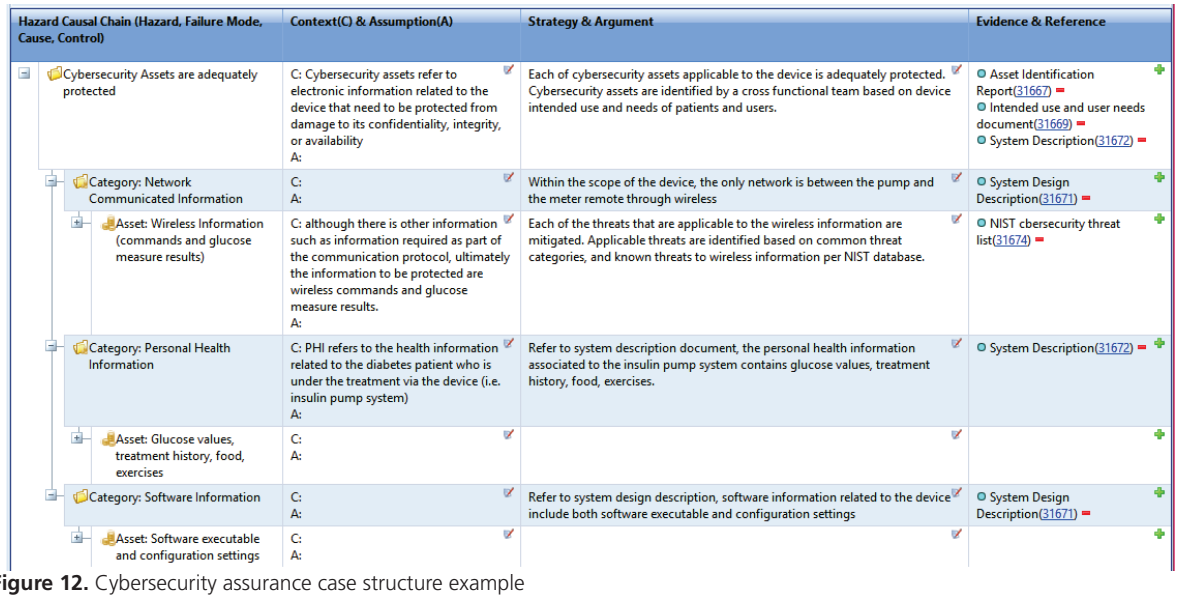

Figure 12. Cybersecurity assurance case structure example

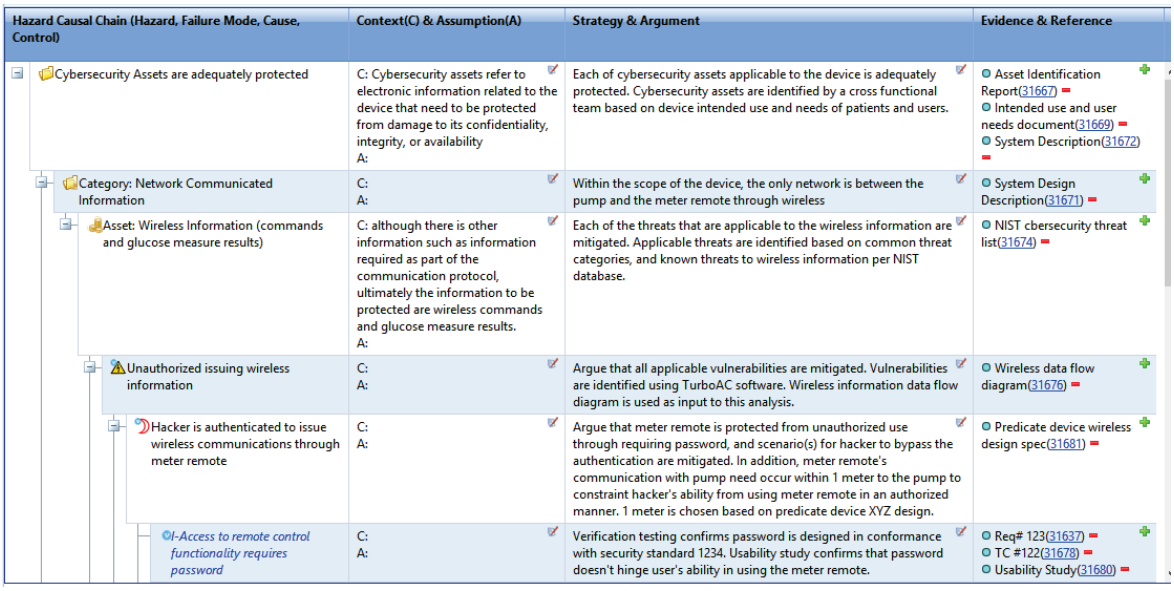

Figure 13. Cybersecurity assurance case example

Claim	Strategy and Argument	Evidence and Reference
Top claim: Cybersecurity for the medical device is adequately ensured.	Argue that all applicable assets are protected. Confidence argument on why assets are identified completely.	Asset identification records
Top subclaim: Each cybersecurity assets is protected.	Argue that all applicable threats for each asset are mitigated. Confidence argument on why threats are identified completely.	Threat identification records
Subclaim: Each applicable threat for each asset is mitigated.	Argue that all system vulnerabilities are mitigated. Confidence argument on why system vulnerabilities are identified completely.	Vulnerability identification and analysis records
Subclaim: Each applicable system vulnerability is mitigated.	Argue that all causes are mitigated. Confidence argument on why causes are identified completely.	Cause identification and analysis records
Subclaim: Each cause of system vulnerability is mitigated.	Argue that controls are established. Explain why controls are adequate.	Standards, good practices, analysis, validation
Subclaim: Cybersecurity risk controls are established.	Argument on why controls are implemented correctly.	Records of design and verification process

Table 1. Cybersecurity assurance case structure template

TIR57[15]) following the structure of ANSI/AAMI/ISO 14971.

To achieve adequate and balanced device cybersecurity and safety, cybersecurity and safety risk analyses should be connected and synchronized instead of being isolated. Due to its complexity, documenting the decisions and rationale related to cybersecurity is important. Assurance cases have been used to communicate risk management information and demonstrate medical device safety. They also can be used for documenting and communicating cybersecurity. ■

References

1. **National Electrical Manufacturers Association.** Manufacturer Disclosure Statement for Medical Device Security. Available at: www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx. Accessed Dec. 8, 2015.
2. **Food and Drug Administration.** Content of premarket submissions for management of cybersecurity in medical devices: guidance for industry and Food and Drug Administration staff. Available at: www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf. Accessed Dec. 8, 2015.
3. **Association for the Advancement of Medical Instrumentation.** ANSI/AAMI/ISO 14971:2007: *Medical devices – Application of risk management to medical devices*. Arlington, VA: Association for the Advancement of Medical Instrumentation; 2007.
4. **Zhang Y, Jones PL, Jetley R.** A hazard analysis for a generic insulin infusion pump. J Diabetes Sci Technol. 2010;4(2):263–83.
5. **Paul N, Kohno T, Klonoff DC.** A review of the security of insulin pump infusion systems. J Diabetes Sci Technol. 2011; 5(6): 1557–62.
6. **Wu F, Kusinitz A.** Best practices in applying risk management terminology. Biomed Instrum Technol. 2015;spring(suppl):19–24.
7. **Eagles S, Wu F.** Reducing risks and recalls: safety assurance cases for medical devices. Biomed Instrum Technol. 2014;48(1):24–32.
8. **National Institute of Standards and Technology.** NIST Special Publication 800-53. Available at: https://web.nvd.nist.gov/view/800-53/home. Accessed Dec. 8, 2015.
9. **National Institute of Standards and Technology.** Framework for improving critical infrastructure cybersecurity. Available at: www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. Accessed Dec. 8, 2015.
10. **International Electrotechnical Commission.** IEC/TR 80001-2-8: Application of risk management for IT networks incorporating medical devices – Part 2-8: Guidance on standards for establishing the security capabilities identified in IEC80001-2-2. Geneva: International Electrotechnical Commission. In press.
11. **Association for the Advancement of Medical Instrumentation.** ANSI/AAMI/IEC TIR80001-2-2:2012: *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*. Arlington, VA: Association for the Advancement of Medical Instrumentation; 2012.
12. **Food and Drug Administration.** Infusion pumps total product life cycle: guidance for industry and FDA staff. Available at: www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm209337.pdf. Accessed Dec. 8, 2015.
13. **International Electrotechnical Commission.** ISO/IEC 15026-2:2011: Systems and software engineering – Systems and software assurance – Part 2: Assurance case. Geneva: International Electrotechnical Commission; 2011.
14. **International Electrotechnical Commission.** IEC/TR 80001-2-9: Application of risk management for IT-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities. Geneva: International Electrotechnical Commission. Under development.
15. **Association for the Advancement of Medical Instrumentation.** ANSI/AAMI/ISO TIR57: *Principles for medical device information security risk management*. Arlington, VA: Association for the Advancement of Medical Instrumentation. Under development.