The Chronicles of Interoperability: Failures, Safety, and Security

Krishna K. Venkatasubramanian

Interoperability: Fellowship Of the Medical Devices

Medical devices are used in the diagnosis of disease or other conditions or in the cure, mitigation, treatment, or prevention of disease in humans or animals.[1] They allow caregivers (e.g., physicians, nurses) to be able to focus on their primary task of patient care.

Although medical devices were stand alone for many years, they have recently begun to move away from this configuration. Devices now have considerable communication capabilities that allow them to interact and *interoperate* with each other and other entities around them. This ability to interoperate has the potential to yield many improvements to care, including better performance, reduced false alarms, automatic decision/diagnosis support, and medication interaction checking in real time.[2]

Devices now have considerable communication capabilities that allow them to interact and *interoperate* with each other and other entities around them.

The most prominent effort to enable interoperability among medical devices is the ASTM F2761 standard architecture, which also is known as the MD PnP integrated clinical environment (ICE).[3] Logically, ICE is separated into three categories: supervisor, network controller, and medical devices. However, many components can be implemented on the same physical hardware. ICE allows coordination among devices from diverse manufacturers. Each device communicates with the network controller—a sort of "medical router" that does not have any medical/clinical functionality itself but is responsible for data routing, translation, and quality of service enforcement, thereby facilitating communication between devices and the supervisor. The supervisor is responsible for executing "clinical workflows," as well as more complex procedures such as medication interaction monitoring and suppression of false alarms.

As interoperability of medical devices increases, concern regarding patient safety also is growing. Harm to a patient can come in many ways: 1) immediate (untimely or wrong actuation), 2) intermediate (incorrect monitoring of patient physiological parameters leading to incorrect diagnosis or treatment), or 3) long-term (unauthorized disclosure of patient health information [i.e., privacy loss]). Failure of one or more of the constituent entities of an interoperability setup (e.g., medical devices, the network) is one of the main causes of patient harm. Hence, ensuring failure-free interoperable medical device operation is crucial.

Failure-free operation of interoperable medical devices can be viewed as satisfying both safety and security. To understand why, I will take a small detour to describe the interrelationship between the two.

About the Author

Krishna K. Venkatasubramanian, PhD, is assistant professor in the Department of Computer Science at Worcester Polytechnic Institute in Worcester, MA. E-mail: kven@wpi.edu

Safety and Security: Strangers on a Train?

Safety and security both deal with preventing failures. To understand the interrelationship between security and safety, we have to look at the causes of failures.

For failures to happen, two conditions generally need to be present: 1) existence of vulnerabilities in the system and 2) occurrence of *errors* in the system.[4]

Vulnerabilities are any system characteristic (known or unknown) that when activated, may lead to partial or complete failure of the system (e.g., presence of poor bounds checking in a device code leading to buffer overflow from extremely long input strings). Vulnerabilities need not be intrinsic to the device; they can be introduced from the context of operation well past deployment. Assuming the system design requirements are well understood, vulnerabilities introduced within the system mainly occur as a result of poor design, implementation, and/or deployment.

The interrelationship between safety and security and failures suggests that we need to consider both security and safety simultaneously when designing any critical system.

Errors occurring in the system usually fall into one of the following five categories[4]: 1) systemic (e.g., clogged tube in infusion device), 2) environmental (e.g., thermal noise–induced soft errors in device electronics), 3) lapse based (e.g., device operator forgot a step), 4) mistake based (e.g., device operator set the wrong dosage), or 5) inducement based (e.g., someone disables air-in-line sensor in a pump).

Errors are necessary but not sufficient for failures in the system. Vulnerabilities also have to exist. All safety and security requirements and solutions of a system essentially have to target these two conditions, albeit to varying extents. In general, the relationship between safety and security is defined in the literature as follows:

- **Subset relationship.** Here, safety is defined as preventing all five types of errors and associated vulnerabilities, while security is focused on inducement-based errors only. Security therefore can be seen as at least a partial subset (if we consider information loss to be a vulnerability in the system), if not a complete subset, of safety.[5,6]
- **Disjointed relationship.** If we view security requirements as specifically designed to prevent inducement-based errors and elimination of associated vulnerabilities, while safety is about all the other errors, then we have a model where the two are disjointed. In other words, safety is about preventing *accidental* failures, while security is about preventing *deliberate* failures in the system.[7]

Although other views of relating security and safety of systems exist, these are the two prominent ones. The interrelationship between safety and security and failures suggests that we need to consider both security and safety simultaneously when designing any critical system, including interoperable medical devices.

A Fistful of Safety

Considerable work is being done to design individual medical devices in a safe manner. This effort is particularly strong when it comes infusion pumps. The goal is to move beyond focusing on system-level testing and code review procedures to enable safety by design through model-based design and static analysis.[8–10]

However, when these safe devices are deployed in an interoperable setting, the overall interoperable setup itself is not necessarily safe.[11] For complex systems such as interoperable medical devices, interaction of various "safe" medical devices often leads to emergent situations that are unsafe, many of which cannot be anticipated a priori. Consequently, researchers are looking into designing interoperability architectures that enable safe interoperation.[12,13]

These efforts for promoting interoperability safety are focused on four fronts: 1) designing intelligent clinical alarm algorithms for the patient to detect patient health deterioration,[14,15] 2) designing algorithms for enabling closed-loop control of patient health,[16] 3) improving functional alarms for detecting deteriorating interoperability infrastructure performance,[17] and 4) instantiating the high-level description of the ICE architecture with a publish-subscribe system with clinical apps that promote safe interoperability.[16]

Safety clearly is very important for medical devices, regardless of whether they are interoperable. However, as we know, solutions developed for enabling safe interoperability are only part of the solution. They do not consider the potential of induced/intentional failures. If someone is intentionally causing a failure in the system, safety primitives alone cannot detect it. For example, consider a simple interoperability setting in which a patient-controlled analgesia pump is interoperating with a SPO_2 (pulse oximeter) sensor. A clinical app executing on the supervisor is providing safety interlock that prevents overdose of pain medication when the blood oxygenation of the patient is suppressed beyond a point. This is done automatically, without the presence of a caregiver and therefore presents one of the major advantages of enabling interoperability. A safe interoperable setup will ensure that no matter what the context, if the oxygenation goes below a certain point, the pump will stop infusing, stop boluses, or raise an alarm. However, if the sensor or its data stream are tampered with, then there is no way of knowing the current blood oxygenation of the patient and therefore no way to know whether the infusion should be stopped.

Oh Security, Where Art Thou?

As medical devices collect and exchange personal health data, securing them is very important. Lack of security may lead not only to loss of patients' privacy but also to physical harm of the patient by allowing adversaries to introduce bogus data or by modifying/suppressing legitimate data, thereby inducing erroneous diagnosis. Indeed, protecting health data also is a legal requirement. The HIPAA (Health Insurance Portability and Accountability Act)[18] and HITECH (Health Information Technology for Economic and Clinical Health Act)[19] regulations specify, among other things, a series of administrative, technical, and physical security procedures for covered entities to use in order to ensure the confidentiality and integrity of electronic health information. However, our analysis regarding the use of existing standards in the medical domain for interoperability security were found to be woefully inadequate.[20] Further, as the number of medical devices increases or the capability of individual devices increases in an interoperable setting, more attack venues will appear.

Lack of security may lead not only to loss of patients' privacy but also to physical harm of the patient by allowing adversaries to introduce bogus data or by modifying/suppressing legitimate data, thereby inducing erroneous diagnosis.

Safe and secure interoperability needs to be considered early on in the development of medical devices.

Thus, ensuring secure interoperability is as crucial as safe interoperability and needs to be addressed immediately, as architectural details for enabling interoperable medical devices are being developed.

The goal of attackers in safety-critical systems is to cause some form of physical harm to the patient, either immediately or in due course of time. This can be achieved by targeting various operational aspects of the medical device system such as sensing, processing, communication, and actuation. Adversaries can choose three broad classes of targets to attack in medical device systems. Security solutions are needed to address the following[21]:

- **Availability.** This category includes attacks that tamper with the data being generated by the various entities or mount a denial of service on the medical devices in some form so that they cannot perform their task properly. Sample attacks include physical destruction of the devices and sensors and modifying the environment of the device, causing it to measure incorrect values.
- **Privacy.** This category includes attacks that seek to access an individual patient's health data in an unauthorized manner. These data eventually can be used to harm the patient through availability violations. Patient data security can be breached in multiple ways (e.g., communication eavesdropping, physical theft of patient information). Sample attacks include a patient's health records being read by curious hospital staff.
- **Data.** This category includes attacks that seek to target the medical institution where the medical device system is deployed. The goal is to use the institution's network to tamper with data communicated among devices during interoperability. Sample attacks include analyzing the traffic of the hospital network to reveal that patients have a high rate of adverse events.

However, these security properties cannot be thought of in isolation, as they only target a subset of potential failure events.

Dial 'M' for Modeling

During the design of interoperable medical devices, simultaneously considering security and safety is vitally important. Safety and security and their integrated modeling have been studied in various domains, such as industrial control,[22] railroad signaling systems,[23–25] and avionics.[26] The lessons learned in these domains can be applied when designing safety and security for interoperable medical devices. Examples include:

- Extending the fault tree analysis and failure mode and effects analysis into including malicious (security) failures events (and associated sub-events) in parallel.[23]
- Developing a unified security and safety assurance framework,[27] which provides a means for certification of both safety and security properties of a system. It takes account of safety hazards and security threats, together with the operational requirements of the target system, to produce a risk model alongside the architectural model of the system.[27]
- Extending the life cycle model with methods from the domain of embedded security to protect the systems against sources of hazard.[28,29]

In any modeling tool used, one needs to consider that safety and security look at failures from a slightly different angle and therefore can lead to slightly different and sometimes overlapping (or even contradictory) actions. For example, one might include both checksum and message authentication code in a message for safety and security reasons, when just one would suffice.[28] Designing actions for interoperable medical devices that consider both security and safety requirements simultaneously is an open question that needs to be addressed.

In any modeling tool used, one needs to consider that safety and security look at failures from a slightly different angle and therefore can lead to slightly different and sometimes overlapping (or even contradictory) actions.

Conclusion

In conclusion, designing interoperable medical devices with both security and safety in mind is essential. Thus far, safety has been the primary focus as a means for failure mitigation in interoperable medical devices. As interoperability becomes pervasive in medical devices and they become interconnected, the threat surface also increases. The news about former Vice President Dick Cheney disabling his pacemaker's wireless communication comes to mind.[30] Instead of taking such drastic steps and losing an important capability of the medical devices, if we consider security and safety requirements simultaneously from the beginning, we can develop devices that are broadly failure resistant as well as useful. ■

References

1. **Library of Congress.** Safe Medical Devices Act of 1990. Available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d101:HR03095:@@@L&summ2=m&. Accessed Nov. 11, 2013.
2. **Arney D, Fischmeister S, Goldman J, et al.** Plug-and-Play for Medical Devices: Experiences from a Case Study. *BI&T*. 2009;43:313–317.
3. **ASTM International.** ASTM F2761. Medical Devices and Medical Systems—Essential Safety Requirements for Equipment Comprising the Patient-Centric Integrated Clinical Environment (ICE). ASTM International, West Conshohocken, PA; 2009.
4. **Brostoff S, Sasse MA.** 2001. Safe and sound: a safety-critical approach to security. In: Proceedings of the 2001 Workshop on New Security Paradigms. New York: Association for Computing Machinery; 2009:41–50.
5. **Pan D, Liu F.** Influence Between Functional Safety and Security. In: Proceedings of the Second IEEE Conference on Industrial Electronics and Applications. Washington, DC: IEEE; 2007:1323–1325.
6. **Burns A, McDermid J, Dobson J.** On the Meaning of Safety and Security. *The Computer Journal*. 1992;35:3-15.
7. **Alexander DS, Arbaugh WA, Keromytis AD, Smith JM.** Safety and Security of Programmable Network Infrastructures. *IEEE Communications Magazine*. 1998;36(10):84, 92.
8. **Arney D, Jetley R, Jones P, et al.** Formal Methods Based Development of a PCA Infusion Pump Reference Model: Generic Infusion Pump (GIP) Project. Proceedings of the High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play, Boston. 2007:23–33.
9. **Jetley R, Chelf B.** Diagnosing Medical Device Software Defects Using Static Analysis. Medical Device and Diagnostic Industry. 2009;31(5):72–83.
10. **Kim BG, Ayoub A, Sokolsky O, et al.** Safety-Assured Development of the GPCA Infusion Pump Software. In: Proceedings of the International Conference on Embedded Software (EMSOFT 2011), Taipei, Taiwan, Oct. 9–14, 2011.
11. **Cortès PA.; Krishnan SM, Lee I, Goldman JM.** Improving the Safety of Patient-Controlled Analgesia Infusions with Safety Interlocks and Closed-Loop Control. In: Proceedings of the 2007 Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability, Boston. 2007:149–150.

12. **King A, Procter S, Andresen D, et al.** An Open Test Bed for Medical Device Integration and Coordination. In: ICSE Companion. 2009:141–151.

13. **Kim C, Sun M, Mohan S, et al.** A Framework for the Safe Interoperability of Medical Devices in the Presence of Network Failures. In: Proceedings of the ACM/IEEE International Conference on Cyber-Physical Systems, Stockholm, Sweden, Apr. 12–15, 2010.

14. **King AK, Roederer A, Arney D, Chen S, et al.** GSA: A Framework for Rapid Prototyping of Smart Alarm Systems. In: Proceedings of the 1st ACM International Health Informatics Symposium. New York: Association for Computing Machinery; 2010:487–491.

15. **Park S, Roederer A, Mani R, et al.** Limitations of Threshold-Based Brain Oxygen Monitoring for Seizure Detection. *Neurocrit Care*. 2011;15:469–476.

16. **Lee I, Sokolsky O, Chen S, Hatcliff J, et al.** Challenges and Research Directions in Medical Cyber-Physical Systems. *Proceedings of the IEEE*. 2012;100:75–90.

17. **Venkatasubramanian KK, Vasserman E, Sokolsky O, Lee I.** Functional Alarms for Systems of Interoperable Medical Devices. In: Proceedings of the IEEE International Symposium on High Assurance Systems Engineering, Miami, FL, Jan. 9–11, 2014.

18. **Department of Health & Human Services.** HIPAA Report 2003: Summary of the Health Insurance Portability and Accountability Act. Washington, DC: Department of Health & Human Services; 2003.

19. **Department of Health & Human Services.** HITECH Act Enforcement Interim Final Rule. Available at: www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html. Accessed Nov. 11, 2013.

20. **Kune DF, Venkatasubramanian K, Vasserman E.** Toward a Safe Integrated Clinical Environment: A Communication Security Perspective. In: Proceedings of the Workshop on Medical Communication Systems, Helsinki, Finland: Aug. 13, 2012.

21. **Arney D, Venkatasubramanian K, Sokolsky O, Lee I.** Biomedical Devices and Systems Security. In Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Boston, Aug. 30 to Sep. 11, 2011.

22. **Novak T, Gerstinger A.** Safety- and Security-Critical Services in Building Automation and Control Systems. *IEEE Transactions on Industrial Electronics*. 2010;57:3614–3621.

23. **Silva N, Lopes R.** Practical Experiences With Real-World Systems: Security in the World of Reliable and Safe Systems. In: Proceedings of the Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop, Budapest, Hungary, Jun. 24–27, 2013.

24. **Smith J, Russell S, Looi M.** 2003. Security as a Safety Issue in Rail Communications. In: Proceedings of the Australian Workshop on Safety Critical Systems and Software. Darlinghurst, Australia: Australian Computer Society; 2003.

25. **Braband J, Seemann M.** On the Relationship of Hazards and Threats in Railway Signaling. System Safety. In: Proceedings of the International IET System Safety Conference, Edinburgh, UK, Oct. 15–18, 2012.

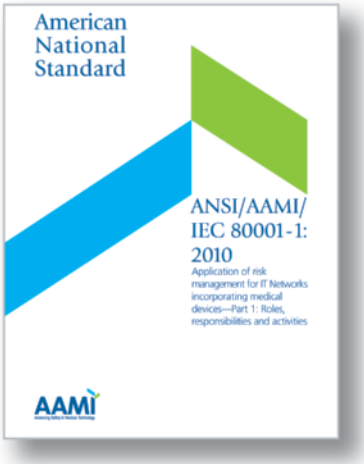
26. **Jacob JM.** High Assurance Security and Safety for Digital Avionics. In: Proceedings of the Digital Avionics Systems Conference, Salt Lake City, UT, Oct. 24–28, 2004.

27. **Lautieri S, Cooper D, Jackson D.** SafSec: Commonalities Between Safety and Security Assurance. In: Proceedings of the Safety Critical Systems Symposium, Southampton, UK, Feb. 8–10, 2005.

28. **Li H, Wang Y, Han J, Luo C.** The Merging Trend of Software Security and Safety. In: Proceedings of the International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, Xi'an, China, Jun. 17–19, 2011.

29. **Burton S, Likkei J, Vembar P, Wolf M.** Automotive Functional Safety = Safety + Security. In: Proceedings of the International Conference on Security of Internet of Things, Kerala, India, Aug. 17–19, 2012.

30. **Ford D.** Cheney's Defibrillator was Modified to Prevent Hacking. Available at: www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html. Accessed Nov. 11, 2013.


American
National
Standard
ANSI/AAMI/
IEC 80001-1:
2010
Application of risk management for IT Networks incorporating medical devices—Part 1: Roles, responsibilities and activities
AAMI