Software in Medical Devices

Module 4: Special Topics

- Off The Shelf Software (OTS)
- Cybersecurity

Pat Baird
Head of Global Software Standards
Philips
Disclosure: Philips has applications pending before FDA. I am not involved in the submission or direct support of those applications.

Pat Baird
Head of Global Software Standards
Philips
Agenda

Off The Shelf Software (OTS)
Cybersecurity
Agenda

Off The Shelf Software (OTS)

Cybersecurity
Expectations for OTS

Many products incorporate Software Of Unknown Provenance ("SOUP") or Off The Shelf software ("OTS") components into their code base. This could be an operating system, graphics library, network protocols, legacy code, etc., that are acquired externally and are incorporated into the final software, but there might not be access to the source code, design files, or verification activities.

The manufacturer of the final product is responsible for identifying how OTS impacts the final product, and is responsible for evaluating and taking action when necessary.

Remember the 4 Steps:
1. What is the OTS trying to do?
2. What can go wrong?
3. What are you doing about it?
4. Did it work?
OTS Consumption is Increasing

- Products have more features and are being developed at a faster pace than they used to be.
- OTS is a key enabler.
- Some products may contain no OTS, other products may be primarily made from OTS with a small amount of custom software was created to integrate the OTS elements.
Supplier Quality

- Just like other domains, software quality is impacted by supplier quality.
- You need to make sure that any software components that you use in your product actually work, but you often don’t have access to the design documentation nor source code.
- “Open Source” Source code has unique challenges.
FDA Guidance (circa 1999)

“Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices”

• Published in 1999, but currently has a disclaimer that it might be revisited as a result of the 21st Century Cures Act

• Asks for version control, a description of what OTS does, test, verification, and validation, risk assessment, and a list of known bugs.
Cumulus Example

• Should you write your own cloud-storage solution, or simply license an existing one such as Dropbox, OneDrive, etc?

• What verification activities would you require for a cloud solution?

• How will your cloud handle multiple versions (because not every patient would update their software on the same day..)
Agenda

Off The Shelf Software (OTS)

Cybersecurity
Cybersecurity Definitions

**Threat**: Threat is any circumstance or event with the potential to adversely impact the device, organizational operations, organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threat exercise vulnerabilities, which may impact the safety or essential performance of a device.

Source: Postmarket Management of Cybersecurity in Medical Devices
Cybersecurity Definitions

**Vulnerability**: A vulnerability is a weakness in an information system, system security procedures, internal controls, human behavior, or implementation that could be exploited by a threat.

**Exploit**: An exploit is an instance where a vulnerability or vulnerabilities have been exercised (accidentally or intentionally) by a threat and could impact the safety or essential performance of a medical device or use a medical device as a vector to compromise a connected device or system.

Source: Postmarket Management of Cybersecurity in Medical Devices
**Cybersecurity Definitions**

**SBOM:** Software Bill of Materials. A list of components in a piece of software. Because vulnerabilities can exist in different software components, having an “inventory” of what components & their version number is useful in evaluating the product.

**ISAO:** Information Sharing & Analysis Organization

From Postmarket Guidance: “ISAOs gather and analyze critical infrastructure information in order to better understand cybersecurity problems and interdependencies, communicate or disclose critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of cyber threats, or voluntarily disseminate critical infrastructure information to its members or others involved in the detection and response to cybersecurity issues.”

**NH-ISAC:** National Health Information Sharing & Analysis Center, which is a well-known medical device & Health IT ISAO
Confidentiality: data, information, or system structures are accessible only to authorized persons and entities and are processed at authorized times and in the authorized manner, thereby helping ensure data and system security. Confidentiality provides the assurance that no unauthorized users (i.e. only trusted users) have access to the data, information, or system structures.

Integrity: In this document means that data, information and software are accurate and complete and have not been improperly modified.

Availability: data, information, and information systems are accessible and usable on a timely basis in the expected manner (i.e. the assurance that information will be available when needed.)
CIA Priority?

There is sometimes a difference in priority between medical device and non-device security priorities. For example, in non-medical IT systems, to preserve **Confidentiality**, a decision is made that adversely impacts **Availability**.

However, for critical medical devices, **Availability** might be the most important characteristic. Some medical devices may reverse “CIA” into “AIC”:

1. **Availability**: The system starts and runs.
2. **Integrity**: System data and results are accurate.
3. **Confidentiality**: Patient data is secure.
Example

Source: Eliciting security requirements with misuse cases, G. Sindre, A. L. Opdahl, Requirements Engineer (2005) 10: 34-44
Safety & Security Must Work Together

Safety is about keeping the product from affecting the environment.

Security is about keeping something in the environment from affecting the product.

Security risks should be shared with safety team.

Source: IEC Guide 120 “Security Aspects – Guidelines for their inclusion in publications”
Differences in Security Risk Evaluation

Similar to how software failures are different than hardware failures, security failures can also be different than software failures.

**Probability** for **Safety** Risk Management is a function of **design** – material selection, tolerances, design margin, and a function of **manufacturing** – Cpk, etc.

**Probability** for **Security** Risk Management is a function of **motivation** – financial gain, mayhem, and a function of **opportunity** – open vulnerabilities, etc.

**Probability** for **Safety** Risk Management largely stays the same over time, and only change as the design or manufacturing changes.

**Probability** for **Security** Risk Management can increases over time and can immediately change.
Severity of Harm for Safety Risk Management is substantially driven by the intended use.

Severity of Harm for Security Risk Management can be completely unrelated to your product – it may be related to what your device connects to.

Of course, security can lead to physical harm (e.g. through disruption or a malicious agent intent on harm.)

Interesting Read: “Everything is a Target, Everything is a Weapon” [Control System Cyber Security How to Properly Protect and Maintain, I. Verhappen, S. Gold, CP 2013 Panel Discussion]
Differences in Human Factors

In **Safety** Risk Management, a product that is easy to use is often safer to use.

In **Security** Risk Management, there can be a complex tradeoff of being easy to use and being secure.

Need to strike a balance..

Also note that Security risk can interact with physical location – a mobile x-ray might not have passwords in the OR because physical security is there, but passwords might be wanted when the device sits in a hallway.
Cybersecurity Resources

- IEC Guide 120 Security Aspects – Guidelines for their inclusion in publications
- AAMI TIR57:2016 Principles for medical device security – Risk management
- UL 2900-1: General requirements for software cybersecurity for network-connectable devices and products (testing requirements)
- UL 2900-2-1: Particular requirements for network-connectable healthcare system components including medical devices and software (testing requirements)
- “Common Weakness Enumeration” (CWE)
- NIST SP800-30, -39, -53A, ...
IEC Guide 120 “Security Aspects – Guidelines for their inclusion in publications”

Principles for interrelation between security and functional safety are:

• security controls should not affect functional safety (e.g. no change of existing proof of functional safety);
• in particular, security controls should not affect the performance of functional safety measures beyond an acceptable level (e.g. integrity of data relevant for functional safety);
• functional safety measures should be designed in a way that they are reasonably protected from failures of security controls (e.g. update of vulnerable software without re-validation);
• in particular, security controls should mitigate identified hazards caused by security threats in order to achieve the requested level of safety

Examples:

• Hypothetical: A medical device requires security access controls (security function) but to avoid impacting availability in an emergency situation (safety function), there is a button to disable the security function (break glass feature.)
• GermanWings flight 9525 incident where the co-pilot used a physical security measure to protect the safety of the passengers against a hijack was misused against the passengers.
AAMI TIR57:2016 Principles for medical device security – Risk management

- AAMI TIR57 provides guidance on how to perform cybersecurity analysis, evaluation, and mitigations for medical devices.
- Cybersecurity risk management is modeled after ISO/IEC 14971
- Includes relationship between security and safety

Source: AAMI TIR57:2016 Principles for medical device security – Risk management
TIR57 modeled after ISO/IEC 14971

To make it easy to adopt, TIR57 was modeled after the process steps in 14971 – plan, identify vulnerabilities, threats, assets, evaluate risks, implement controls, assess overall residual risk, report, and continue into postmarket.
TIR57 also based on existing NIST & Military publications

TIR57 Figure B.3 - Security risk assessment process; adapted from “Resilient Military Systems and the Advanced Cyber Threat”
The security of your product is only as good as your least secure product.

With the growing use of OTS components, this makes for interesting security challenges – lack of support from a software vendor can delay deployment of patches.
What can Medical Device Software learn from Fur Traders in the 1800s?
What can we learn?

Never Give UP
Questions?