FDA U.S. FOOD & DRUG ADMINISTRATION

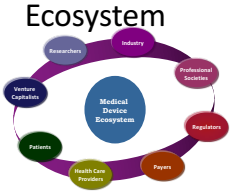
Technical Aspects of System Safety: Interoperability and Cybersecurity

- Sandy Weininger, Ph.D.
- Office of Science and Engineering Labs, CDRH, FDA

www.fda.gov

FDA

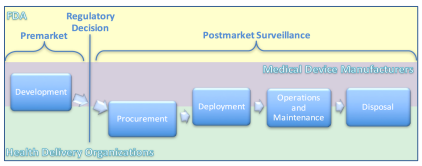
Medical Device Ecosystem



2

FDA

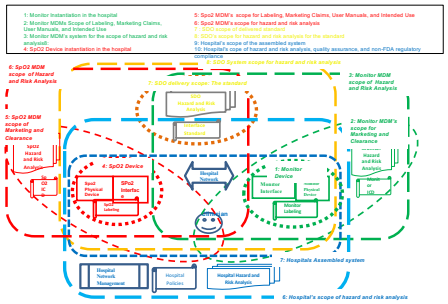
Device Lifecycle: Ecosystem Challenges



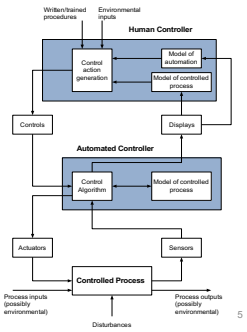
www.fda.gov

3

What is the System?



Higher Level Diagram



Template configuration for a higher-level system view for use in STPA, modified Fig. 8.8 from Leveson. (©2011 by Nancy G. Leveson. All rights reserved. Used with permission.)

Highest Level Diagram

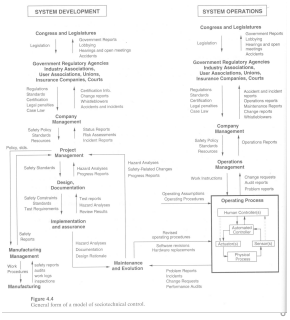
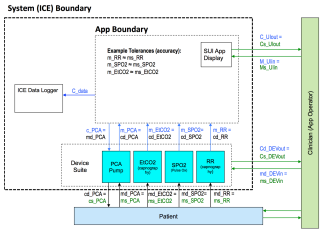


Fig. 4.4 from Leveson. (©2011 by Nancy G. Leveson. All rights reserved. Used with permission.)

boundaries

- Boundary – a means of demarking a responsibility
- boundaries, what information passes thru the boundaries, what types of interactions happen in the system, and what control you have (or don't) over other elements inside and outside the boundaries

Boundaries and Interface Content (MDIDs)



What do you want your standards to do?

- Provide safety acceptance criteria for individual devices when "connected" or when "interacting"
- Provide performance measures
- Establish lifecycles for product development
- Establish an "ecosystem" [who are the stakeholders and what are their roles]

FDA Goals for Cyber and Interop Safety

- Meet our mission: safe and effective devices
- Raise cybersecurity and interop awareness
- Promote safety and security by design through establishing clear regulatory expectations
- Promote coordinated vulnerability disclosure & proactive vulnerability management
- Minimize reactive approaches
- Foster ***'whole of community'*** approach

10

Premarket Cybersecurity Guidance

- Draft June 2013
- Final October 2014
- Key Principles:
  - #1 Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
  - #2 Address cybersecurity during the design and development of the medical device
  - #3 Establish design inputs for device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g)

www.fda.gov

11

Design Stage Activities (security)

- **Design in** the security of your device
- Understand the attack surface of your device
  - What ports and connections are available
  - What third party components/software are used in your device
- Incorporate security principles into the risk assessment
  - Create a threat model
  - Plan to continually update this model throughout life of your device
- Plan for software updates to support the security of the device in the field
- Plan for how you will learn about vulnerabilities
- Plan for how you will conduct an assessment

12

Deployment Activities (security)

- Provide adequate labeling for your device
  - End user needs to know the use expectations
- Develop processes to assure that device is shipped without malware
  - Manufacturing processes are free of malware
  - Deployment method is free of malware

13

FDA interop guidance doc

- Address scoping and boundaries
- Data integrity and reliability , whose responsibility is it
  - Who owns the data as it is generated and passes thru
  - Pulse ox has to send correct data; hospital has to assure network is protected

www.fda.gov 14

Key Definitions

- ***Interoperable medical devices:*** devices that have the ability to exchange and use information through an electronic interface with another medical/nonmedical product, system, or device. Interoperable medical devices can be involved in simple unidirectional transmission of data to another device or product or in more complex interactions, such as exerting command and control over one or more medical devices. Interoperable medical devices can also be part of a complex system containing multiple medical devices.

15

Key Definitions

- ***Electronic Interface***: the medium by which systems interact and/or communicate with each other thereby allowing the exchange of information between systems. It includes both the type of connection (e.g. USB port, wireless connection) and the information content. It is a medium by which a medical device exchanges and uses information with other equipment or other medical devices.

16

Purpose of the Interop Guidance

- To promote the availability of safe and effective interoperable medical devices.
- To provide considerations to use in the development and design of interoperable medical devices.
- To clarify the contents to submit in a pre-market submission to support interoperable medical devices.
- To provide recommendations for labeling.

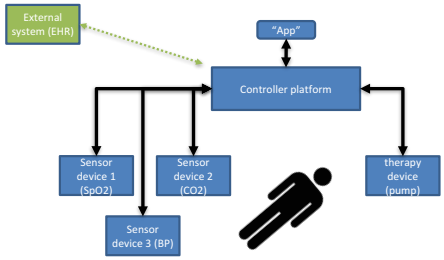
17

Considerations for Medical Device Manufacturers

- Designing systems with interoperability as an objective
- Conducting appropriate verification, validation and risk management activities
- Specifying the relevant functional, performance, and interface characteristics in a user available manner such as labeling

18

Closed loop example



19

What should an interoperability standard address? And how?

interoperability concepts

- physiological observation (esp. semantics; integrity/continuity, timeliness, validity);
- significant event [e.g. medical/clinical alarming] (esp. validity, timeliness, audial/visual "noisiness");
- analytics (/decision support);
- remote (settings; transaction) control; and
- system management, including:
  - Patient/operator/machine identification and authorization
  - [Cyber]Security/Privacy
  - Time bases and synchronization
  - Data logging/forensics.

risk concerns

- product safety, security, and essential performance
- requirements for achieve risk controls
- testing and assurance objectives for demonstrating the effectiveness of the associated risk controls
- labelling and use and operating instructions for guiding others in achieving issue-relevant safety and security in an integrated and operational context.

20