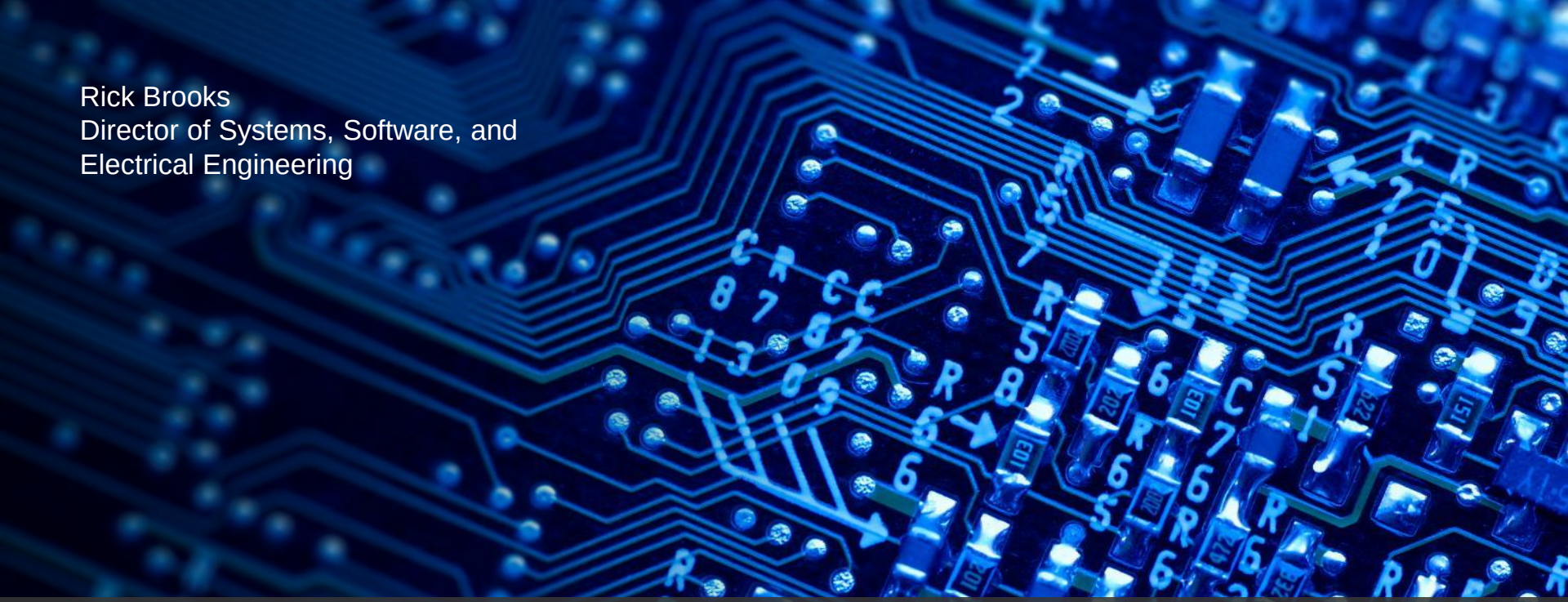
Rick Brooks
Director of Systems, Software, and
Electrical Engineering



Designing Secure Medical Devices

About Battelle

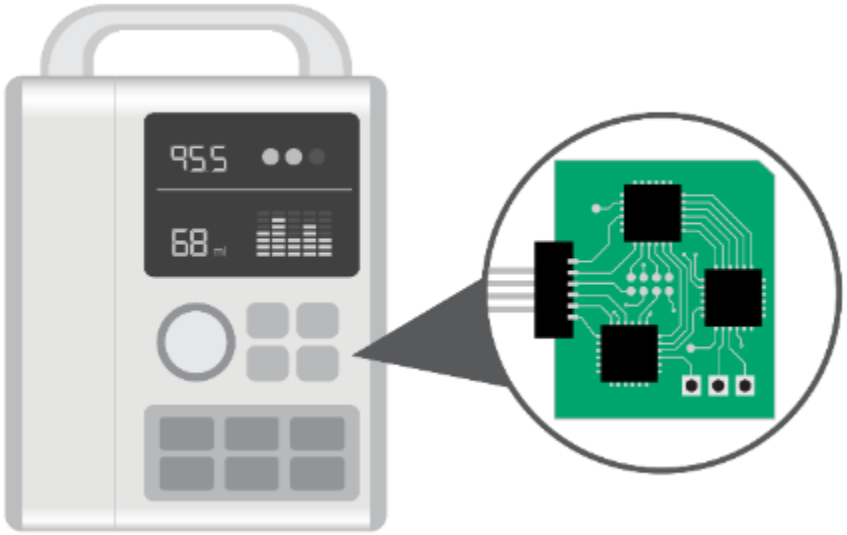
Our mission: To translate scientific discovery and technology advances into societal benefits

Gordon Battelle, Founder

- Nonprofit, charitable trust formed in 1925
- Largest private, independent R&D organization in the world
- Located in Columbus, OH
- Business pillars: Contract Research, Laboratory Management, and Philanthropy
- Profits reinvested in science & technology, STEM education

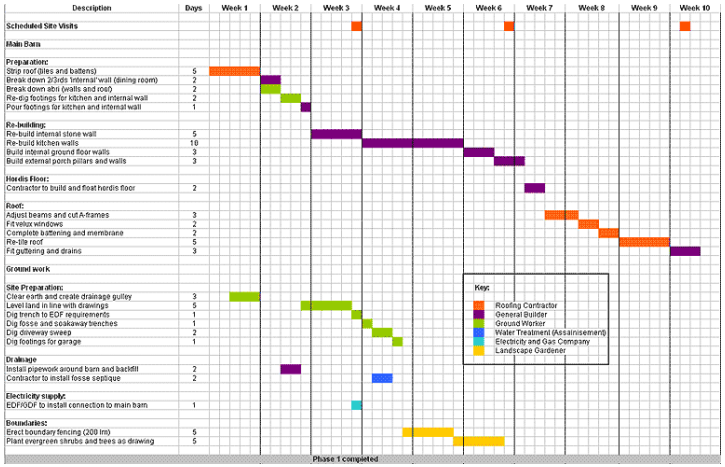
There is no such thing as a secure device

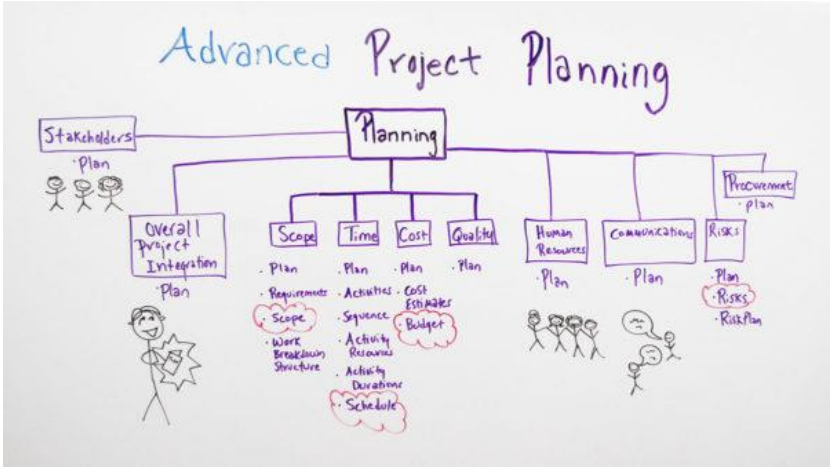
- **The Goal:** Stop an unauthorized or nefarious actor from manipulating your device or data
- With appropriate planning, the effort required to tamper, reverse engineer, manipulate, or counterfeit a device can be significantly increased



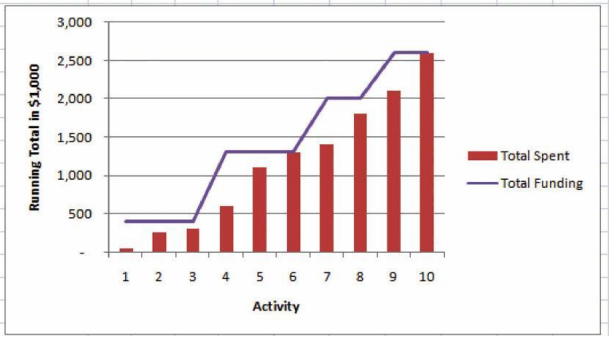
Patient Data
Billing Information
Intellectual Property
Network Access

Proactive vs Reactive Risk Management





Activity	1	2	3	4	5	6	7	8	9	10
Cost	50	200	50	300	500	200	100	400	300	500
Total Spent	50	250	300	600	1,100	1,300	1,400	1,800	2,100	2,600
Transfers	400			900			700		600	
Total Funding	400	400	400	1,300	1,300	1,300	2,000	2,000	2,600	2,600
Cash in Account	350	150	100	700	200	-	600	200	500	-

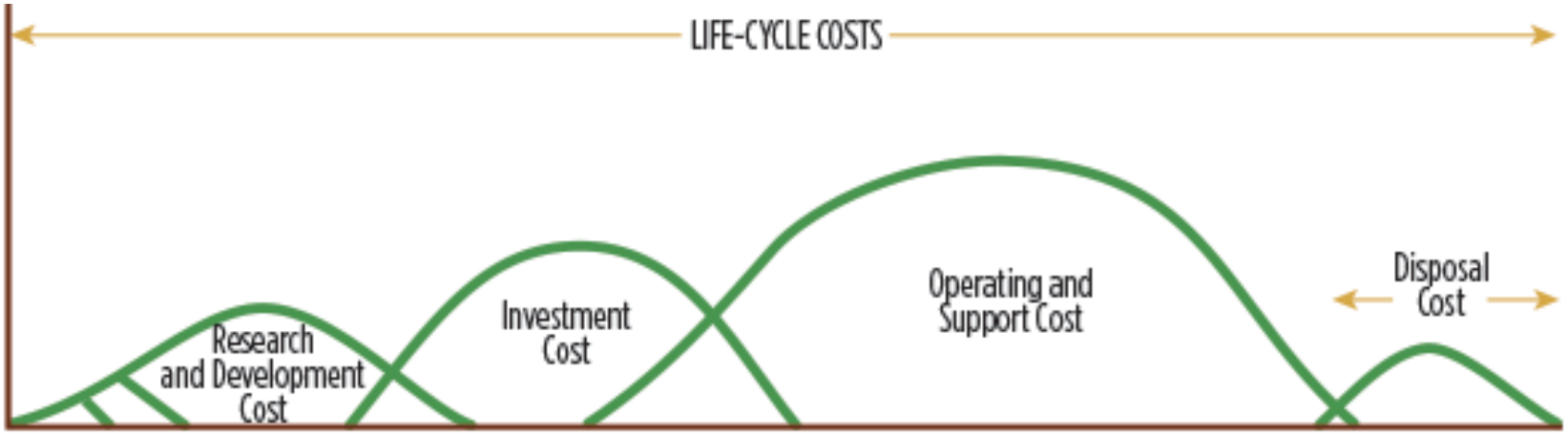


Sources: www.project-plan-templates.com/ www.projectmanager.com/ opentextbc.ca/ http://skyriverit.com/

BATTELLE

Proactive vs Reactive Risk Management

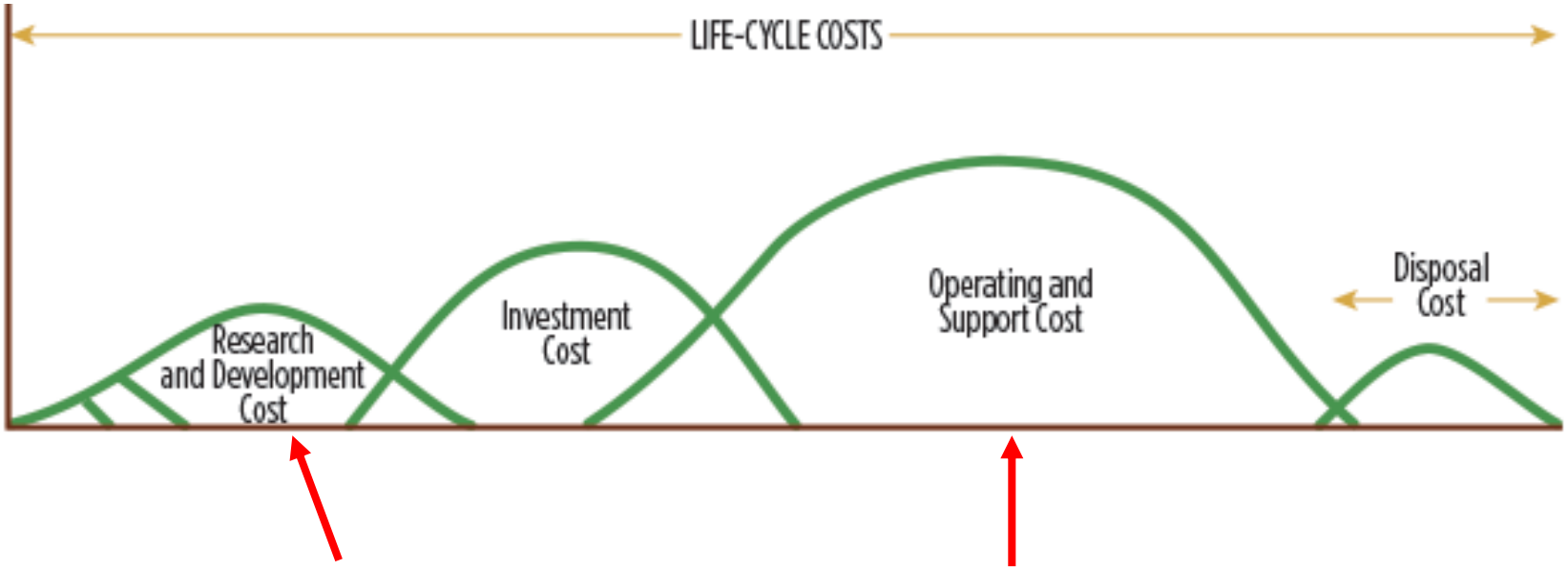
- Pay for it now, or pay for it later?



Source: http://dau.dodlive.mil/

Proactive vs Reactive Risk Management

- Pay for it now, or pay for it later?



Small increases here, will have big reductions here

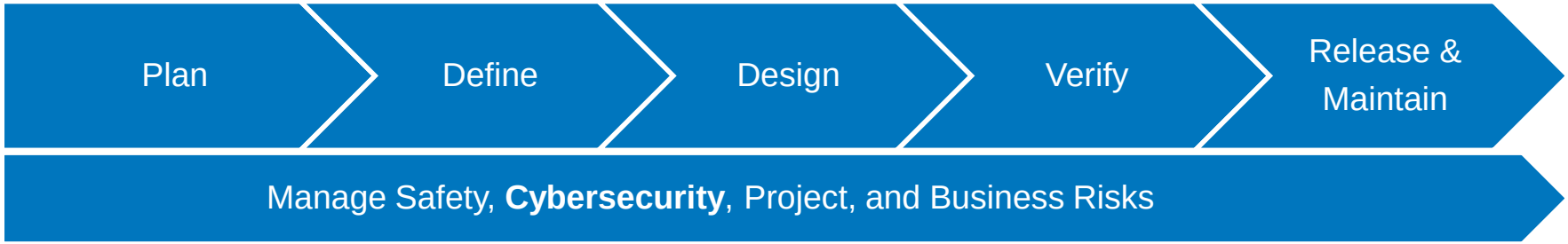
Source: http://dau.dodlive.mil/

Proactive vs Reactive Risk Management

- Security Risk must be considered similar to Safety Risk, Project Risk, Business Risk, etc.
- Effective Risk Control Approach: Expect the unknown and unexpected

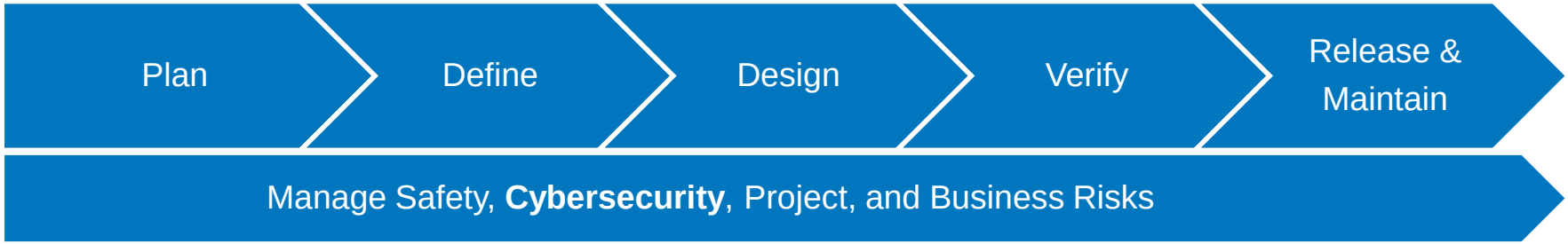
Source: curiosity.com

Product Development Lifecycle



BATTELLE

Product Development Lifecycle



- Most weaknesses in a system are the *result of poor design choice*, not implementation bugs.
- Making secure design choices *up front is critical*.
- Cybersecurity risk management should *integrate* with your company's *overall risk management plan*.
- Add a *cybersecurity engineer* to your team and involve them at each stage of the development process.

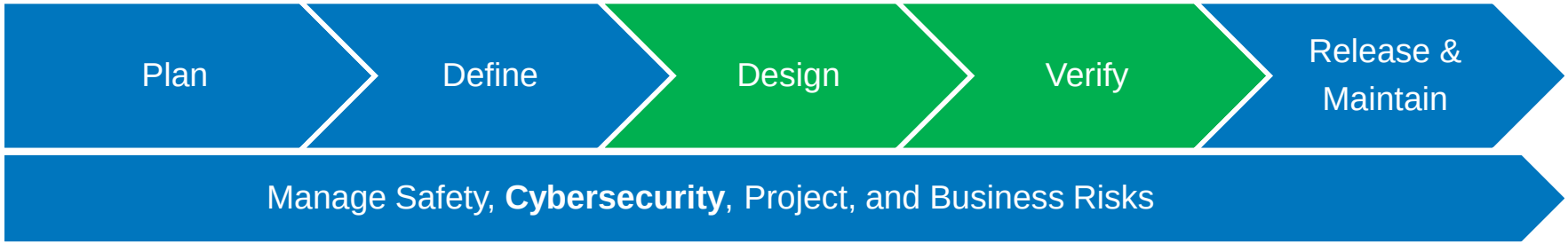
BATTELLE

Product Development Lifecycle
Some Practical Guidance

- Research defensive design techniques and extract applicable requirements;
  - Eliminate or close ports (hardware too!)
  - No hard-coded credentials
  - Don’t use root permissions in the OS
  - Validate data inputs
  - Grant permission; never assume trust
  - Encrypt transmissions, and data at rest
  - Many more…
- Create a Cybersecurity Management Plan

BATTELLE

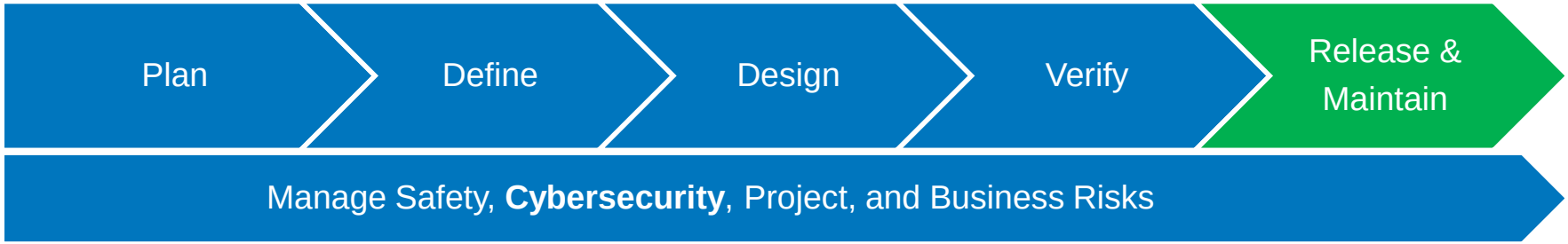
Product Development Lifecycle
Some Practical Guidance



- Robust Design Activities (security-specific);
  - Architecture & Design Reviews
  - Vulnerability Assessments
  - Pre-compliance Testing
  - Threat Assessments & Penetration Testing
  - Fuzz Testing
  - 3rd Party Security Reviews and Assessments

BATTELLE

Product Development Lifecycle
Some Practical Guidance



- Proactive Maintenance Considerations
  - Security Monitoring
    - Industry Monitoring
    - Information Sharing
    - Threat Monitoring
  - Security Incident Response
    - Incident Response Planning
    - Security Patch Management
    - External Communications (vendors, clients, users)

BATTELLE

Key Take-Aways

- There is no such thing as a secure device
- The landscape of cybersecurity is constantly changing
- Be proactive and plan ahead, to be adaptive
- The hard work in development will only pay off if a proactive security approach is maintained

Thank you for attending!
Share your experiences at #HWGSEC

BATTELLE

It can be done

800.201.2011 | solutions@battelle.org | www.battelle.org

INCOSE Healthcare Working Group

4th Annual Systems Engineering in Healthcare Conference

Balancing Safety, Security and Usability in the Design of Secure Medical Devices

Ken Hoyme
Director, Product Security
Boston Scientific
Ken.hoyme@bsci.com

Agenda

- Safety
- Safety & Usability
- Safety & Security
- Safety, Usability & Security
- System of Systems & Emergent Properties

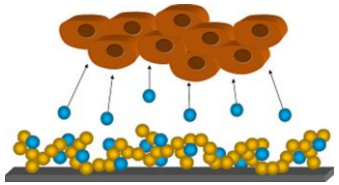
Medical Device Safety

Comets???

Usability

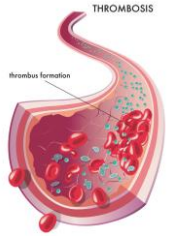
System Security

Electrical Shock

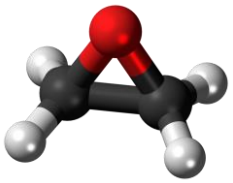


Biocompatibility

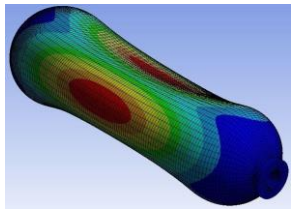
EMI



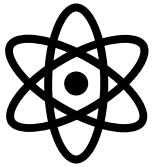
Thrombosis



Sterilization



Mechanical Failure



Radiation

14971 and 60601

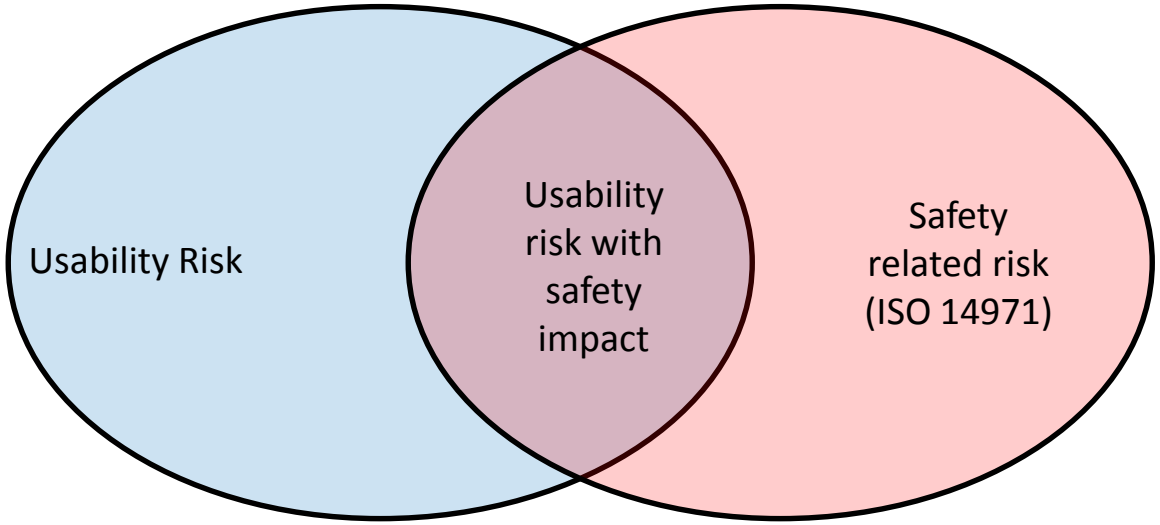
- 14971 defines the process for (safety) risk management
  - Defines harm, hazard and hazardous situation
  - Defines a process to evaluate risk, with or without protective measures
  - Documents means to assess acceptable residual risk
  - Establishes monitoring process requirements
  - Auditable but not testable
- 60601 defines “basic safety and essential performance”
  - Broadly and for individual device classes
  - Explicitly addresses usability
  - Addresses device response to failure
  - Generally testable

Usability recognized as a source of patient harm

- Order entry system confusion
- Surgery in the wrong location
- Ventilators left off accidentally (post X-ray)
- Tubing confusion in hospitals
- Alarm confusion/fatigue
- Similar device/different user interface designs

Usability and Safety Risks

- Usability risks that impact safety
  - User confusion leads to wrong pump setting
- Usability risks that don't impact safety
  - Wordiness, spelling errors
- Safety risks unassociated with usability
  - Power supply failure



Usability Analysis/62366

- Usability Engineering Process
  1. Specify application of device – Intended use & user
  2. Identify frequently used functions
  3. Identify hazards and hazardous situation related to usability – ISO 14971 – foreseeable misuse
  4. Identify device primary op. functions
  5. Develop usability specification
  6. Prepare usability validation plan
  7. Design & implement user interface
  8. Usability verification
  9. Validate usability of medical device

- Lifecycle stages
  - Concept development
  - User needs/requirements
  - Risk management
  - Verification and Validation
  - Post-market monitoring

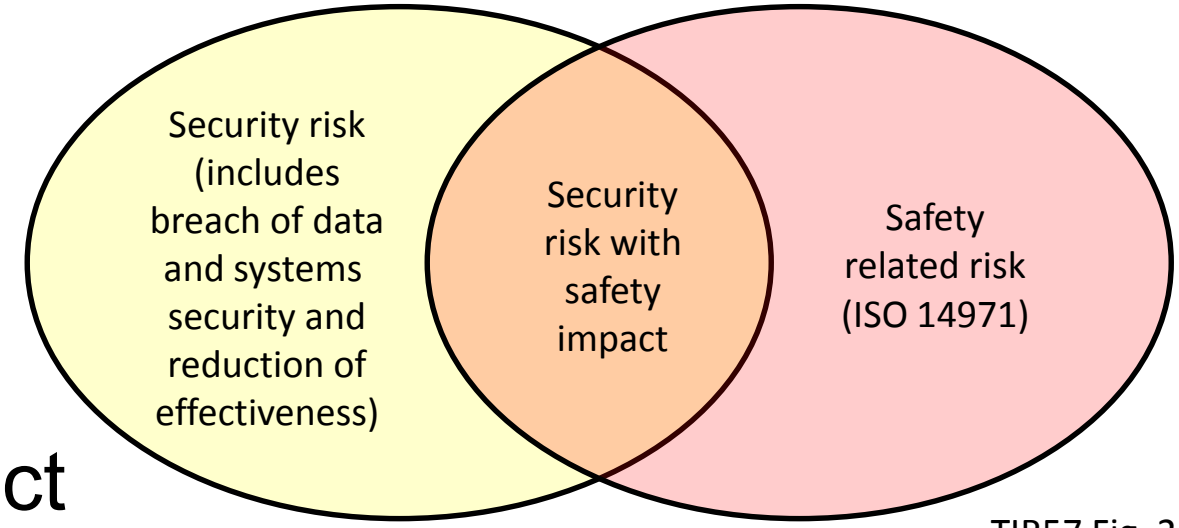
- No explicit references to “Usable security”

Security recognized as a source of patient harm

- Implantable Defibrillator hacking demonstrations (2008+)
- Wearable insulin pump hacking demonstrations (2010+)
- Cardiac company short sell (2016)
- WannaCry impacts on devices and hospital operations (2017)
- Ransomware hits hospitals (2017+)

Security and Safety Risks

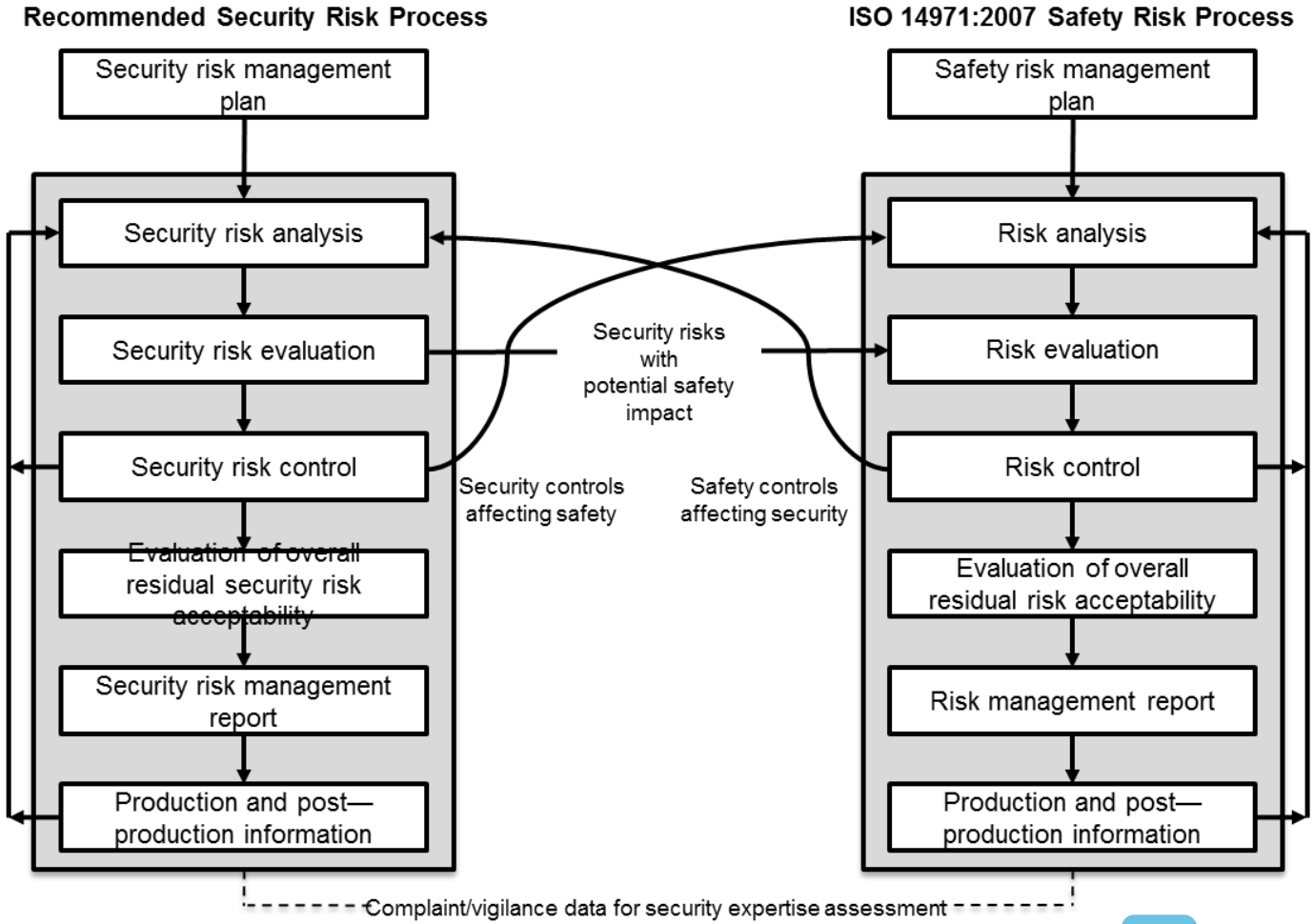
- Security risks that impact safety
  - Hacked pump changes drug flow rate
- Security risks that don't impact safety
  - PHI exposed
- Safety risks unassociated with security
  - Power supply failure



TIR57 Fig. 2

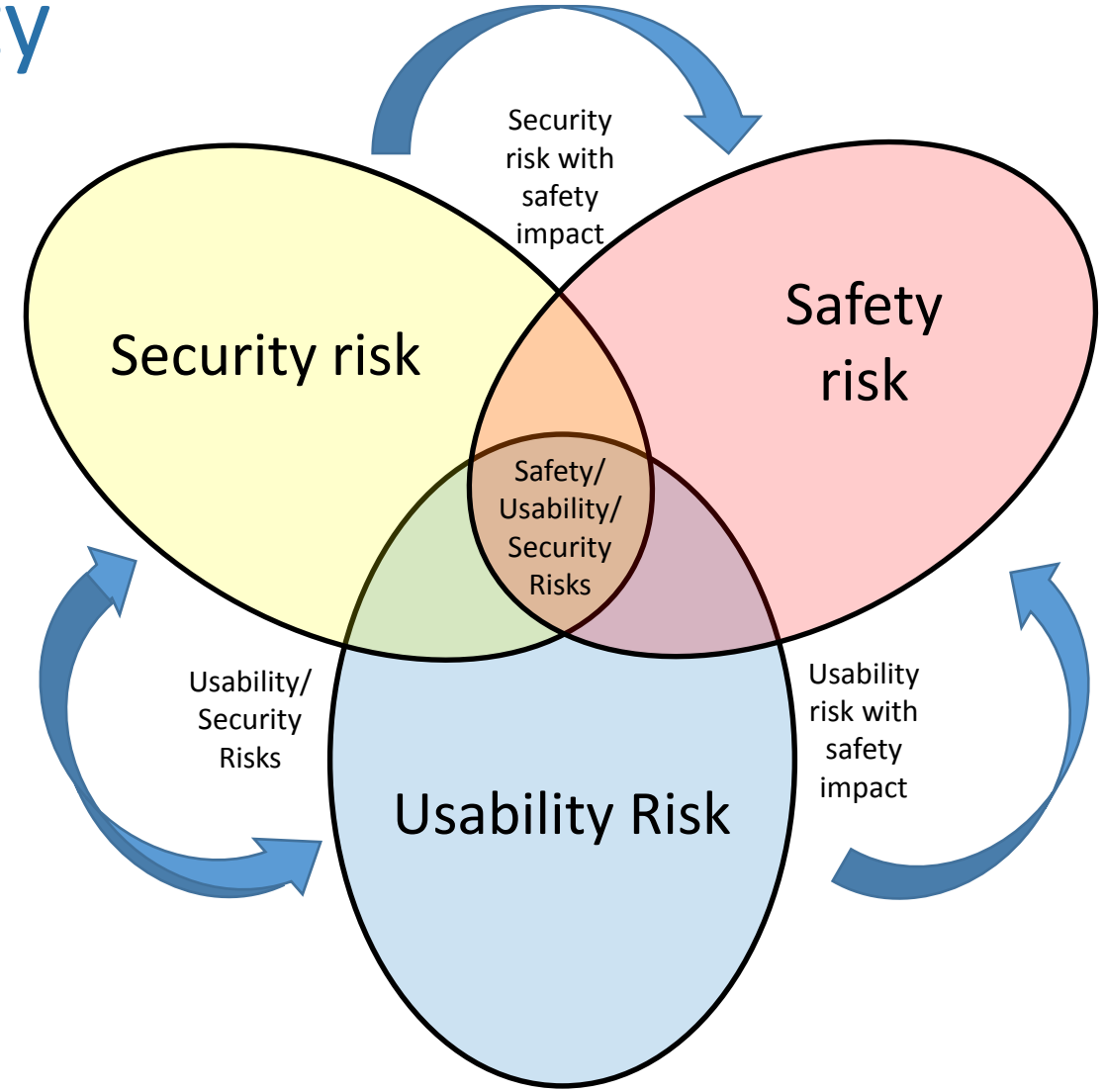
AAMI TIR57

- Addresses security risk management in the context of 14971.
- Creates clear linkages between the consideration of safety and security.
- Recognized by the FDA and referenced in their recent post-market guidance.



Safety, Usability and Security

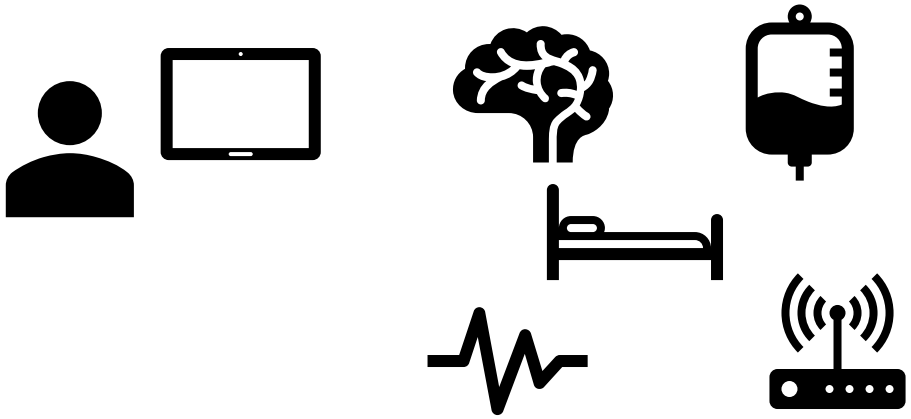
- All three can interact
  - Positively – good usable security can enhance safety
  - Negatively – elimination of a security control for fast access



Development Implications

- Early usability and security analysis must be done interactively
  - Early prototype assessment needs to have planned security controls in place
- Complete set of stakeholders/users need assessment
  - End user
  - Network/Device administrator (e.g. BMET department)
- Post-market monitoring and response to cyber-vulnerabilities needs to include usability analysis
  - Added controls to close a security hole might introduce user issues

System of Systems & Emergent Properties



- Safety, Usability and Security are all emergent systems properties
  - Can construct a system with property X from components without it
  - And vice-versa
- Regulatory processes encourage consideration of these properties only at a single device level.
- When integrated into a network, is the property preserved??

Healthcare System Implications

- Who serves the role of “systems integrator” in the creation of a network of heterogeneous medical devices?
- What new standards are needed will reduce the integration effort?
- What tools and methods can support ad hoc integrators?
  - E.g. Small to mid-sized hospitals with less experienced staff?

Conclusions

- Achieving system safety depends on a balance of supporting properties
  - Usability and Security need to be considered together

- Work is needed to better understand how to ensure safety, security and usability in networks of integrated heterogeneous devices

INCOSE
Healthcare Working Group
4th Annual Systems Engineering in Healthcare Conference

Thank you for attending!

Share your experiences at #HWGSEC