Stephanie Domas
Lead Medical Security Engineer
domas@battelle.org

Cyber Risk Assessment

2017-09-27

Who am I?

- Stephanie Domas
- Battelle Memorial Institute
- Lead Medical Product Security Engineer

- Certifications
  - PE – Professional Engineer
  - CEH - Certified Ethical Hacker

- Adjunct Faculty - The Ohio State University College of Computer Engineering
  - Low level system programming (C/x86) & Ethics in Engineering


PERFORM FEASIBILITY STUDY
DEVELOP USER INPUTS
DEVELOP DEVICE REQUIREMENTS
DEVELOP DEVICE ARCHITECTURE
PERFORM RISK ANALYSIS
DEVELOP DESIGN OUTPUTS
DESIGN VERIFICATION AND VALIDATION
DESIGN TRANSFER
SUSTAINING ENGINEERING
= CYBERSECURITY

Security Risk Management

- Safety risk management, with a security perspective
- Threat modeling - Understanding the threat model of a device is essential to protecting it
  - Threat ≠ Vulnerability
    - A threat is the malicious action
    - A vulnerability is a weakness, that can be leveraged to carry out a threat

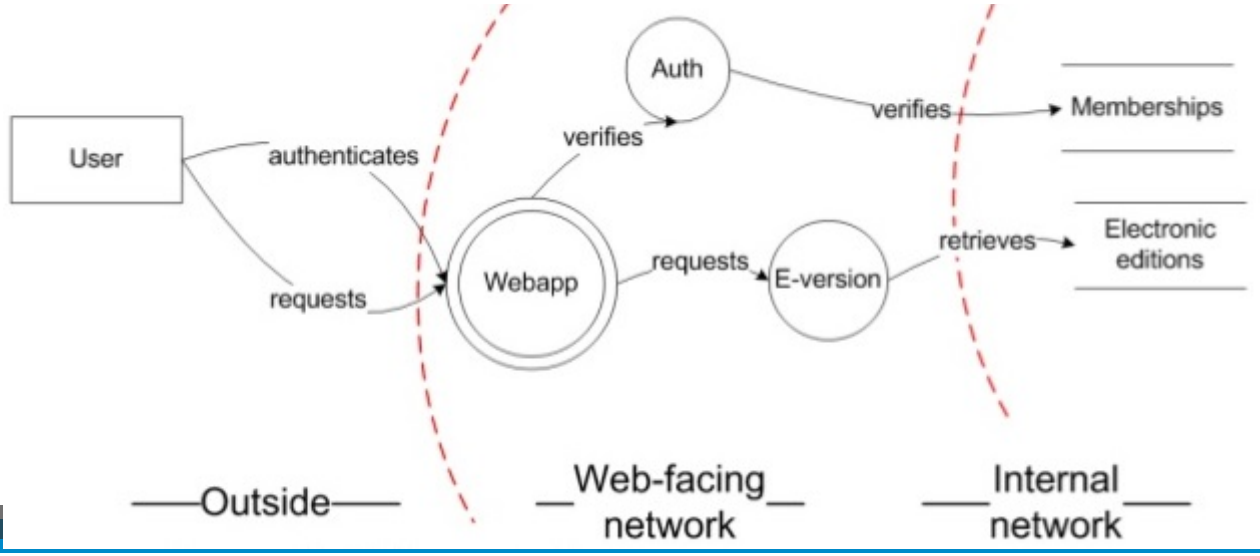

Image source: https://image.slidesharecdn.com/confoo2011-tam-110310101829-phpapp02/95/threat-modeling-web-application-a-case-study-43-728.jpg?cb=1299752523

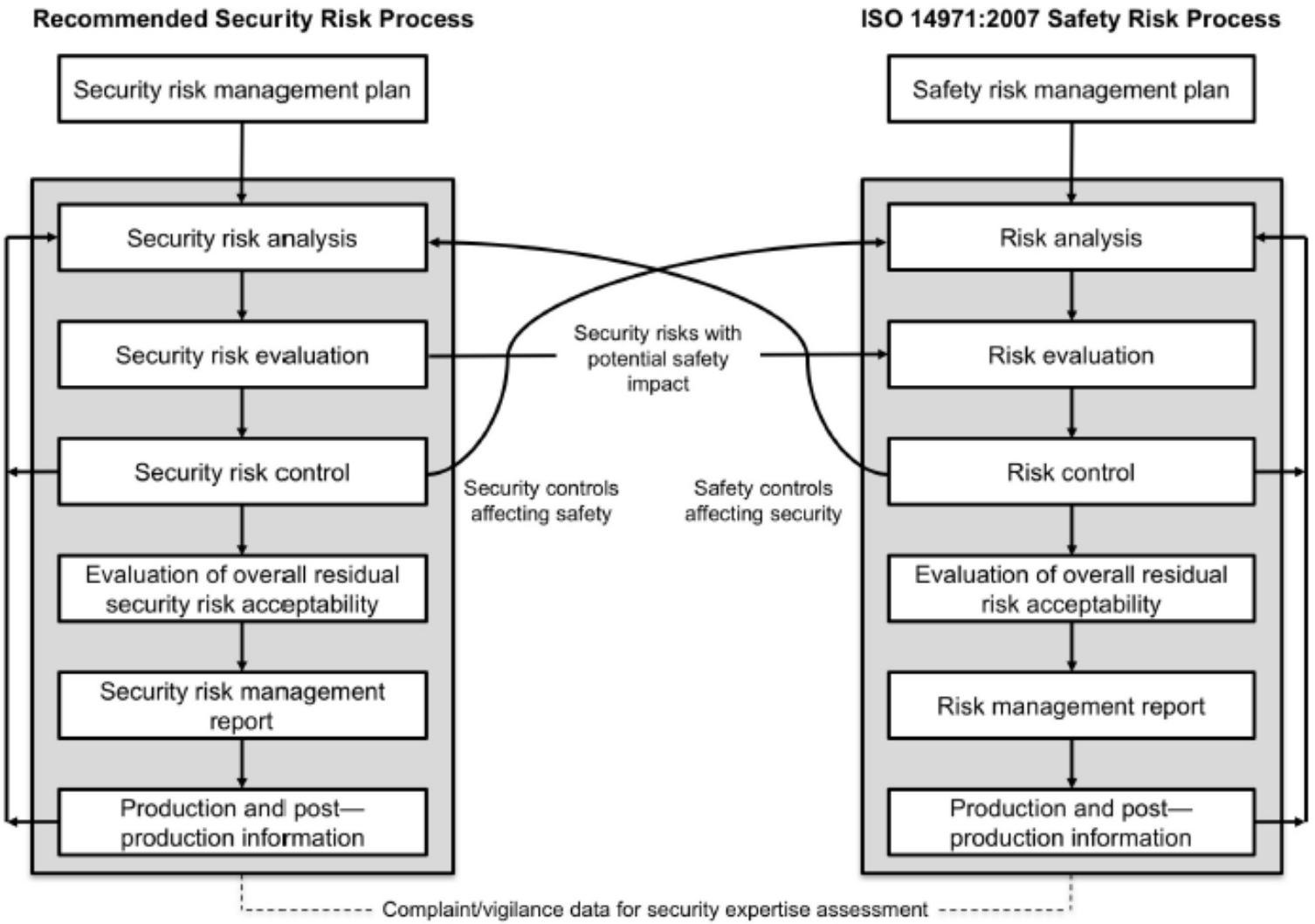

Figure 4 – Relationships between the security risk and safety risk management processes

Image Source: AAMI TIR-57:2016

Battelle
The Business of Innovation

NIST & AAMI TIR 57

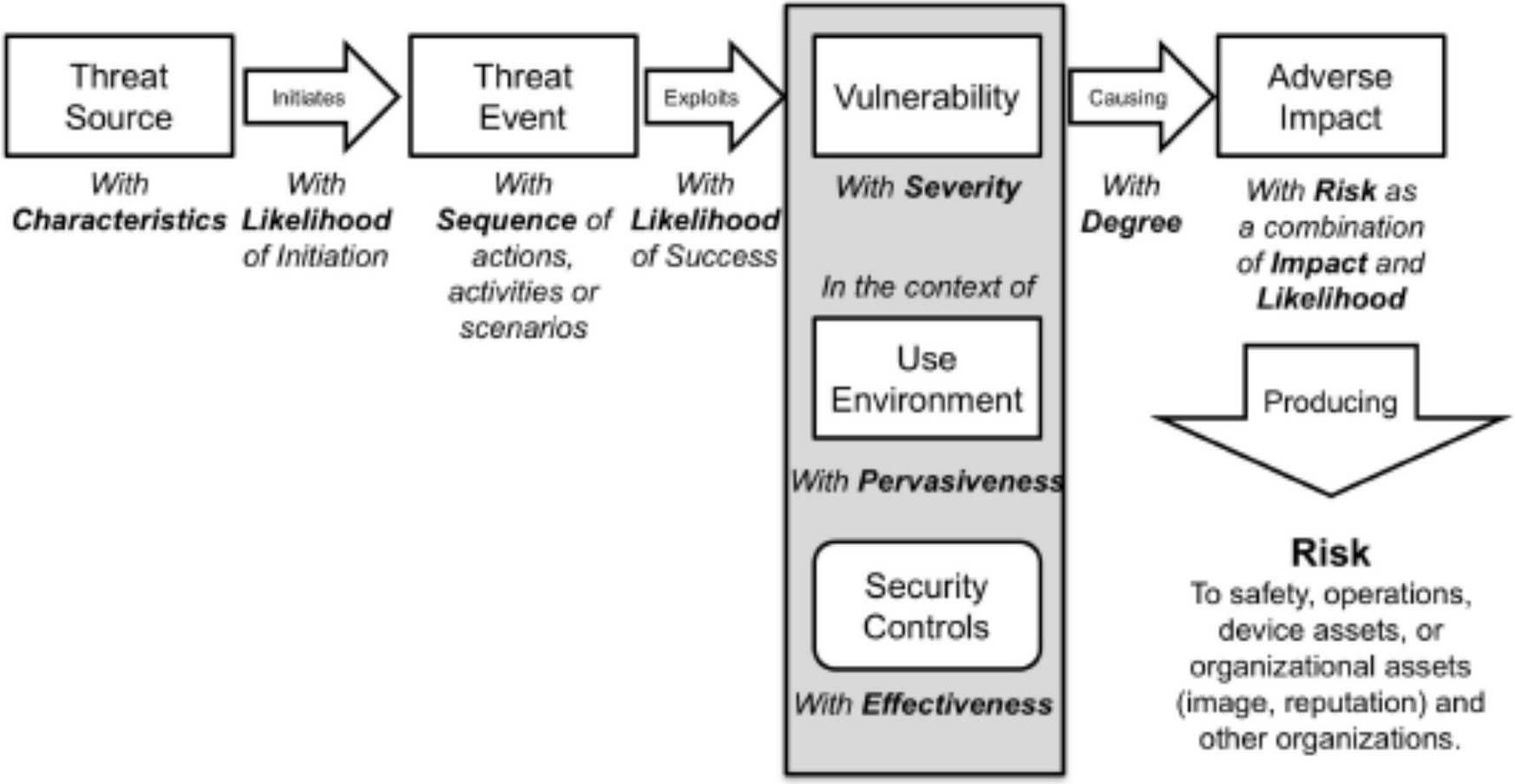

Figure B.5 - An example Threat-oriented Security Risk assessment approach[7]

Image Source: AAMI TIR-57:2016

Attacker/Threat Oriented

Iterate through the possible attackers and generate threats

a) Adversarial Actors
   1) Nation States
   2) Organized Crime
   3) Disgruntled/ex-employees
   4) Political Activists
   5) Emotionally unstable
   6) “Script kiddies”

b) Non-adversarial Actors
   1) Academic researchers
   2) Professional security researchers
   3) Unintentional Misuse
      i) Inexperienced users
      ii) Inexperienced installers
      iii) Inexperienced maintainers

c) Other threat sources
   1) Natural events
   2) Integration effects, such as
      i) RF Interference
      ii) Incompatible software
      iii) “Misbehaving” third party systems on network
      iv) Vulnerable systems or devices directly connected to the device (e.g., via RS-232, USB, or other “hardwired” non-network connections)

NIST & AAMI TIR 57

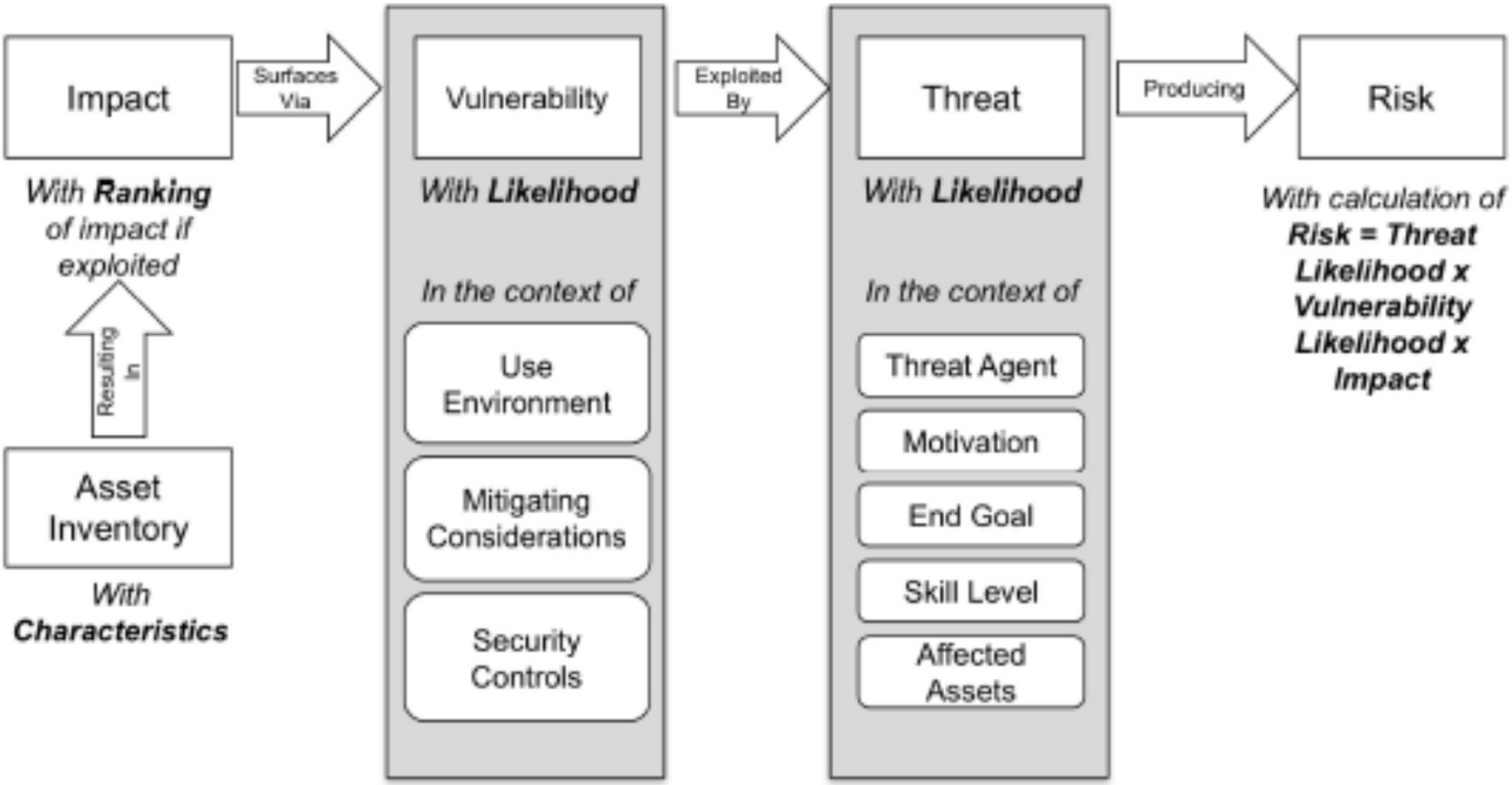

Figure B.6 - An example Asset-oriented Security Risk assessment approach

Image Source: AAMI TIR-57:2016

Asset Oriented

- **Identify all of the assets in the system**
- **Physical Assets**
- a) User interface
- b) Device assets
  - 1) Operating system
  - 3) Application software
  - 4) Keys/Certificates
  - 5) Device identity
  - 6) Device resources
  - 7) Physical interfaces
- d) Network interface
- **Information Assets**
  - a) Patient data
  - b) HDO data
  - d) Device settings/programming commands
  - e) Passwords
  - f) Configurations
    - 1) Network
    - 2) Infrastructure
  - i) Telemetry data

Why is risk assessment important?

- So you spent time and resources securing the right parts of your system
- *There is no such thing as a secure device*

BATTELLE

It can be done

- Stephanie Domas
  domas@battelle.org
- Lead Medical Product Security Engineer
- Battelle DeviceSecure™ Services