Medical Device Design for Safety, Security, and Privacy

National Academy of Sciences

Steve Abrahamson
Director, Product Security Engineering
GE Healthcare

September 10, 2014

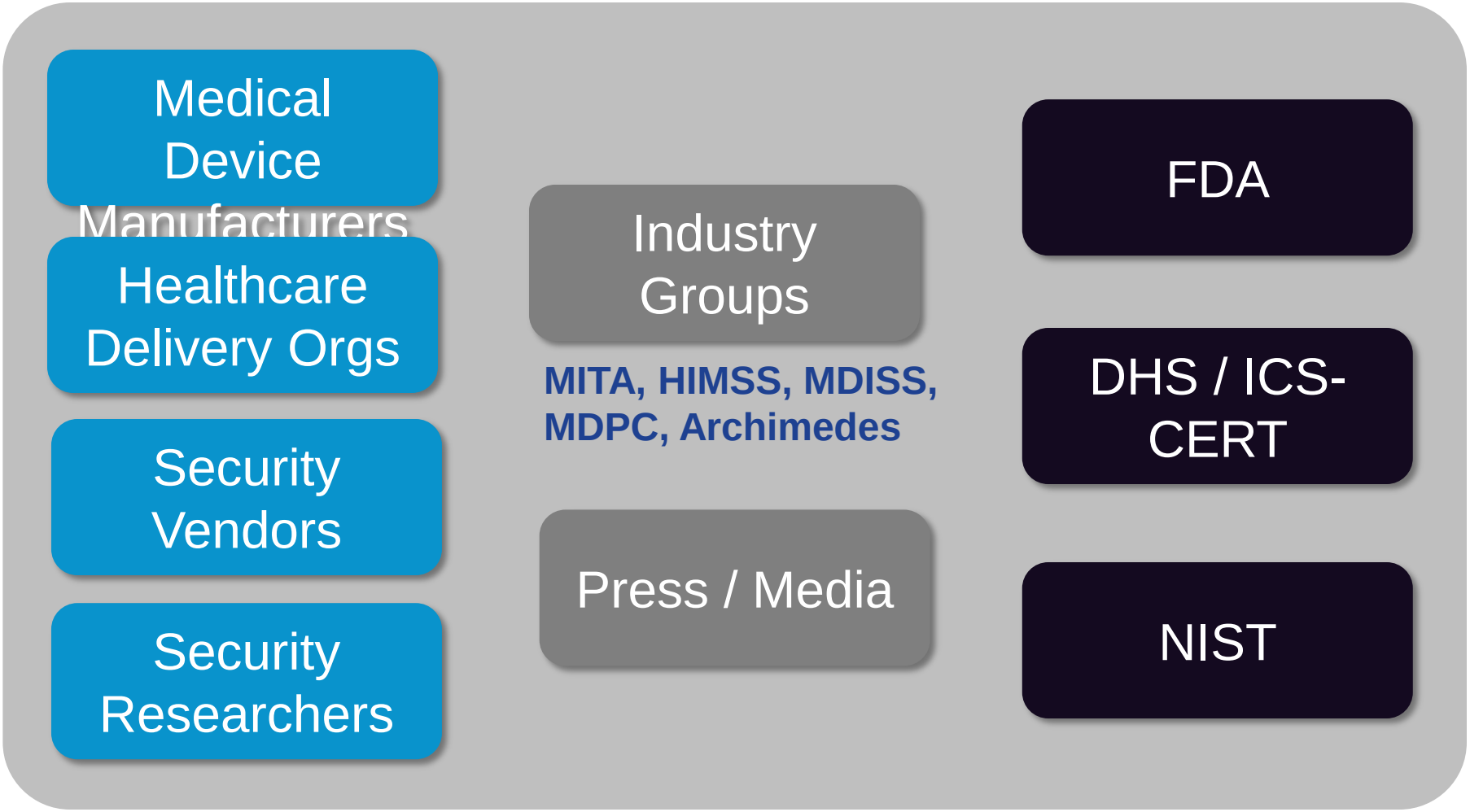
GE imagination at work

Definition

Medical Device Product Security: Controls applied within the design, installation, and maintenance of a product intended to manage risk to the product and information stored, created, or transmitted by the product, from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide integrity, confidentiality, and availability, consistent with function and intended use.

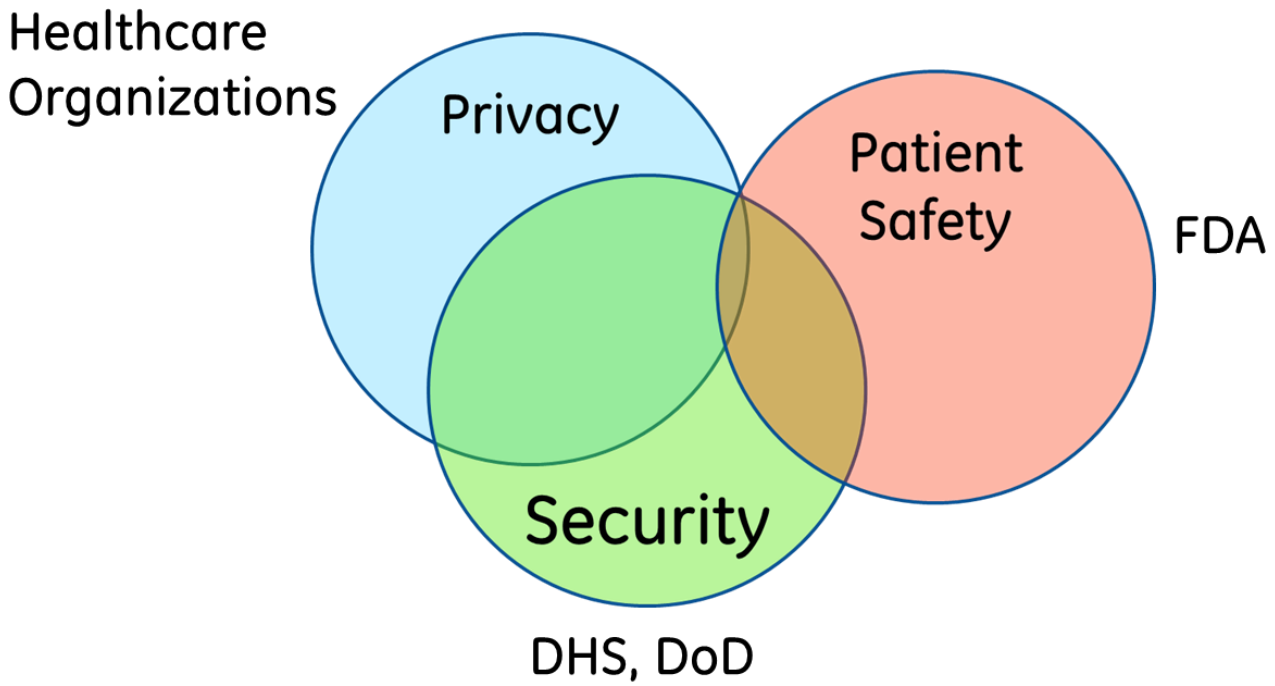
A secure medical device will enable the information security capabilities of Healthcare Delivery Organizations

Medical Device Security Ecosystem



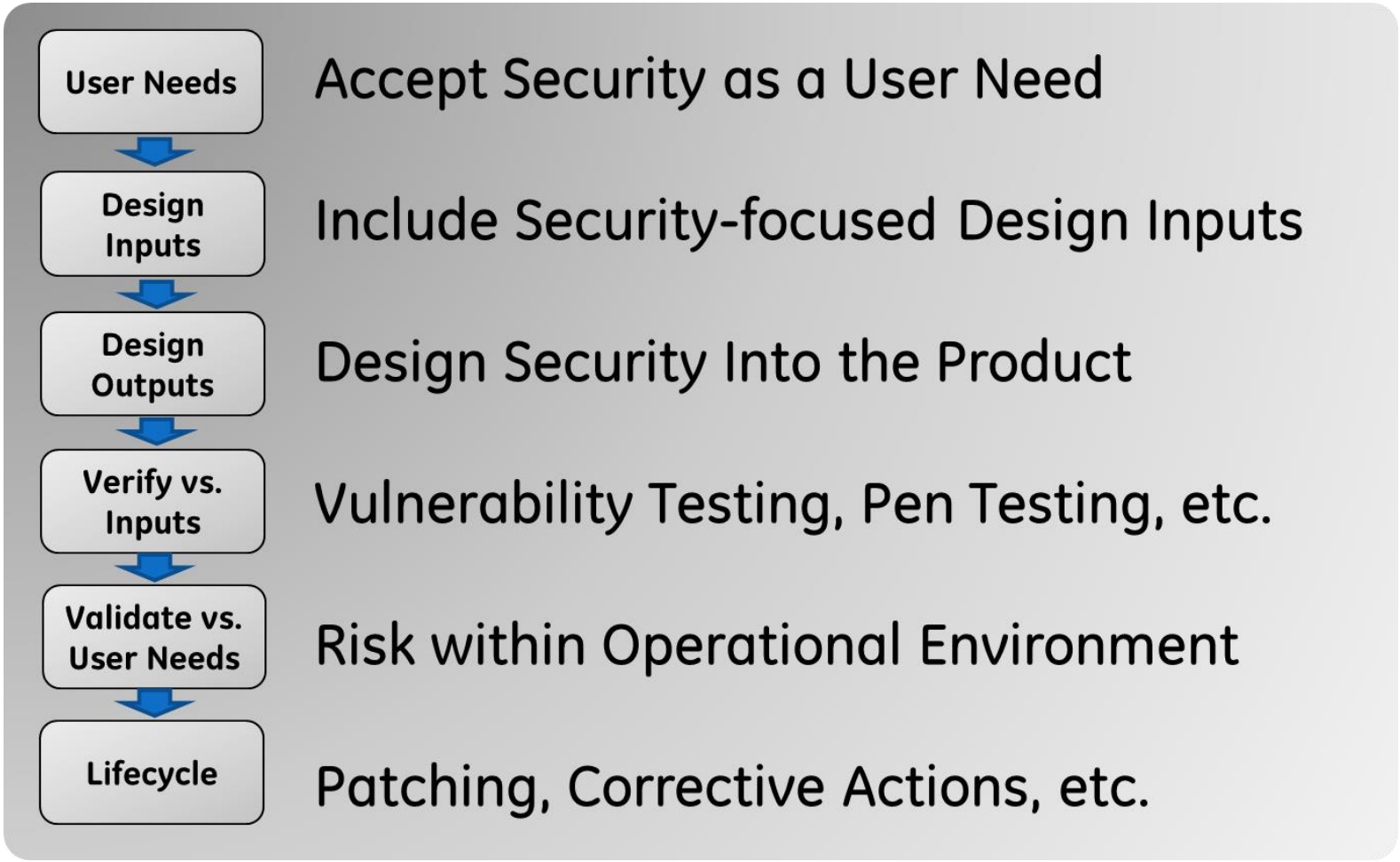
GE imagination at work

Broader Risk View for Manufacturers

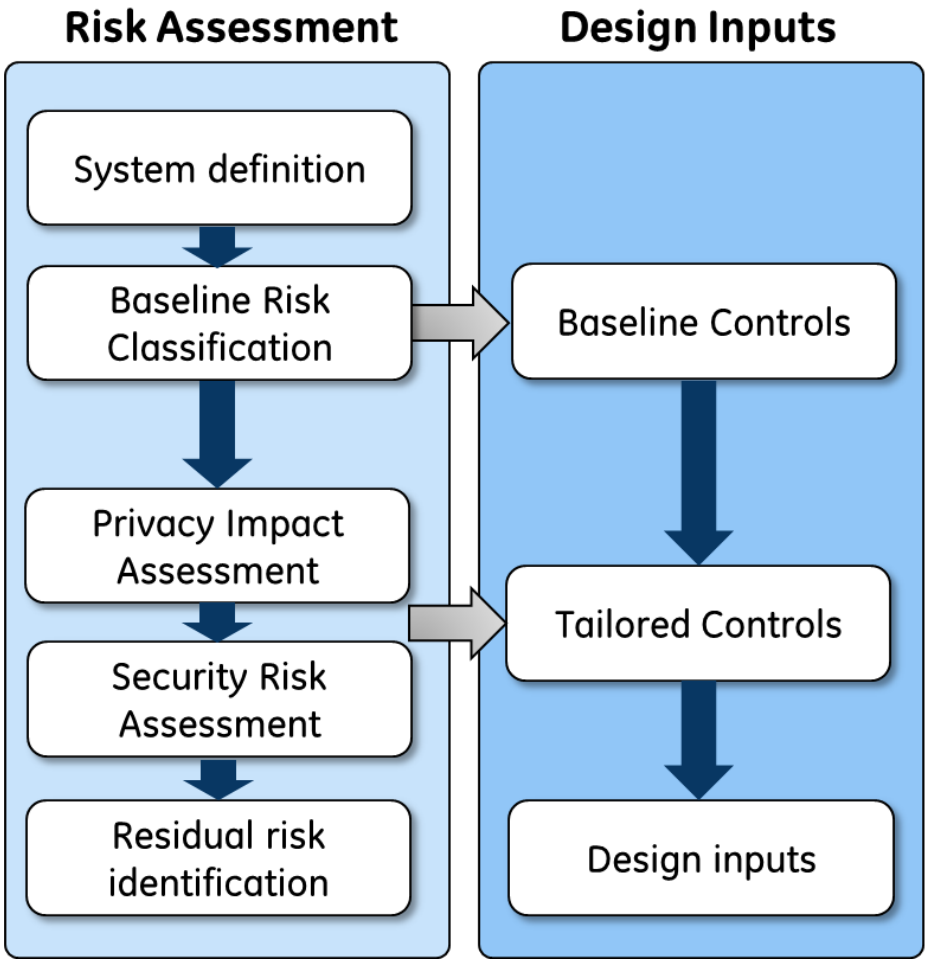


Need to address all risks within Engineering processes…

Design Engineering for Security



Defining the Correct Design Inputs



Three-step risk assessment to identify risk-based controls tailored to product use and operational environment.

Recommend controls based on a standard such as NIST 800-53.

Medical Device Environment

Medical Device Ownership

- Multiple owners with different priorities

FDA Quality System Regulation

- Regulated change management process

Life Cycle Support

- Long product life cycles

Operational Security in the User Environment

- Device security within layered security

Medical Device Security: Moving Forward

Collaboration – build momentum

Proactive – security by design

Technical and non-technical – need both

Risk Management - not “one-size-fits-all”

Safety and Security

Collaboration, not competition