



Tufts Security & Privacy Lab

**Tufts**  
UNIVERSITY

**“There are rabbit holes I want to go down that I’m not allowed to go down”**

An Investigation of Security Expert Threat Modeling Practices for Medical Devices

**Ronald E. Thompson III**  
Tufts University

**Madeline McLaughlin**  
Tufts University

**Carson Powers**  
Tufts University

**Daniel Votipka**  
Tufts University

# Vulnerabilities in medical devices are a continued issue

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Insulin pumps are vulnerable to hacking, FDA warns amid recall

Nine Vulnerabilities in Critical Infrastructure Used by 80% of Major Hospitals



IEEE S&P

May. 2008

The Washington Post

Jun. 2019



Aug. 2021



# Medical Device Regulators are pushing for “secure-by-design”

Threat modeling includes a **PROCESS FOR IDENTIFYING SECURITY OBJECTIVES, RISKS, AND VULNERABILITIES** across the system, and then **DEFINING COUNTERMEASURES TO PREVENT, OR MITIGATE THE EFFECTS OF, THREATS** to the system throughout its lifecycle.

FDA Pre-Market Cybersecurity Guidance [2023]

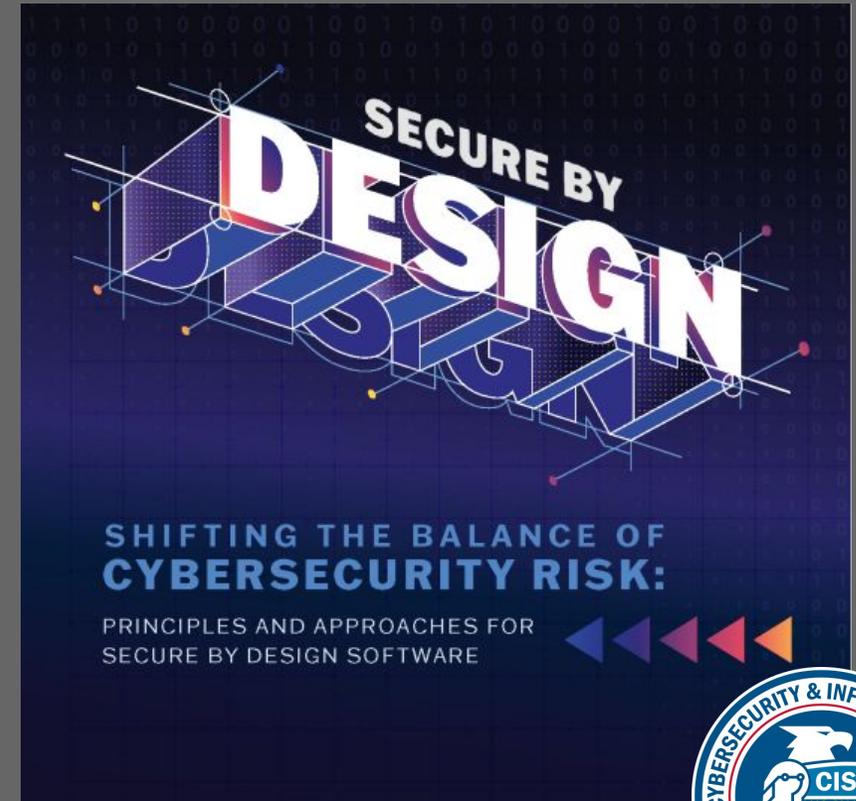


# Part of a larger trend by governments to use threat modeling

Use a tailored threat model during development to **PRIORITIZE THE MOST CRITICAL AND HIGH-IMPACT** products.

Threat models consider a product's specific use-case and enables development teams to fortify products.

Principles and Approaches for Secure by Design Software  
Signed by 19 Different National Agencies



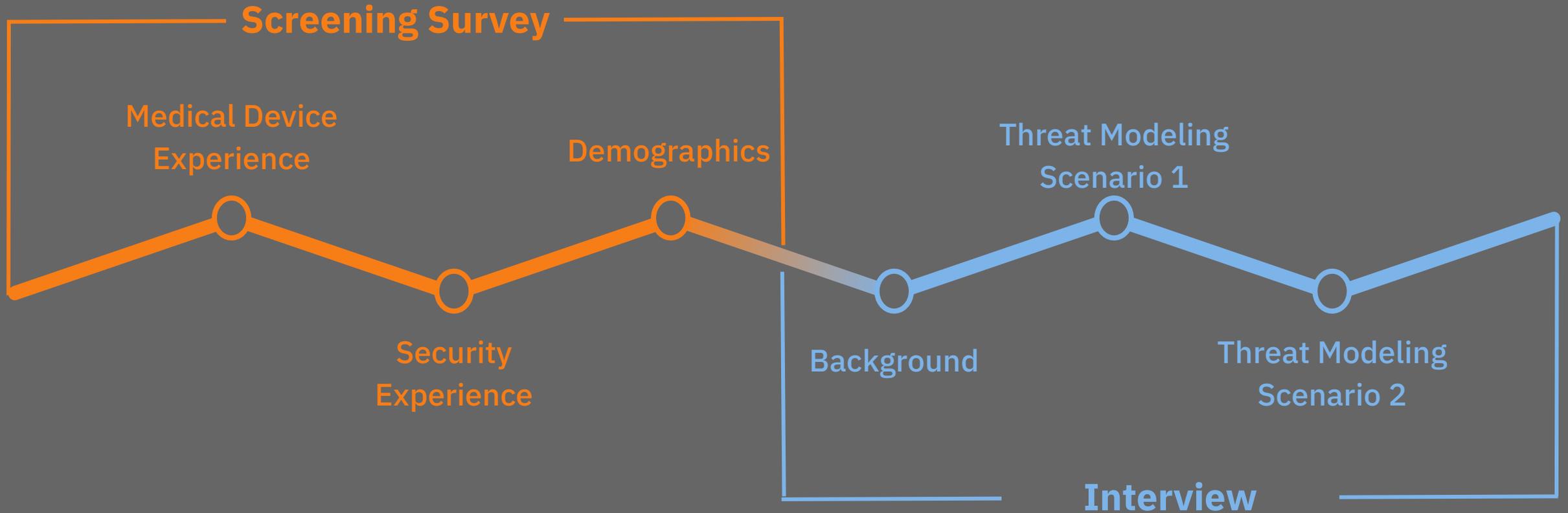
# We wanted to understand how threat modeling is done in practice by medical device manufacturers (MDM) security experts

How do MDM Security Experts identify specific threats and mitigations?

What processes do MDM Security Experts follow when navigating a system's design to identify threats?



# We screened participants and collected initial information before conducting 60 minute interviews



# With the help of experts, we developed three realistic mock device scenarios spanning various harms and settings

## Robotic Surgical System

Type: Surgical System  
Setting: Hospital  
Potential Harm: Patient Death  
Classification: Class II



## Next-Gen Sequencer

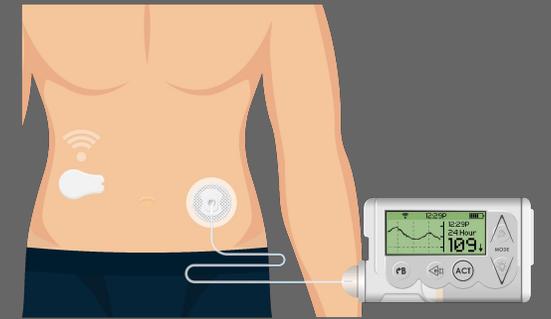
Type: Diagnostic Equipment  
Setting: Laboratory  
Potential Harm: Diagnostic Error  
Classification: Class II/IIa



## Artificial Pancreas

(Insulin Pump & Continuous Glucose Monitor)

Type: Implantable Medical Device  
Setting: Implant  
Potential Harm: Patient Death  
Classification: Class III



All three scenarios are based on devices that are currently being used on the market today  
Classifications are using FDA Guidance, EU MDR/IVDR, and Health Canada

# Each scenario included a set of requirements, a high level context diagram, and a data flow diagram

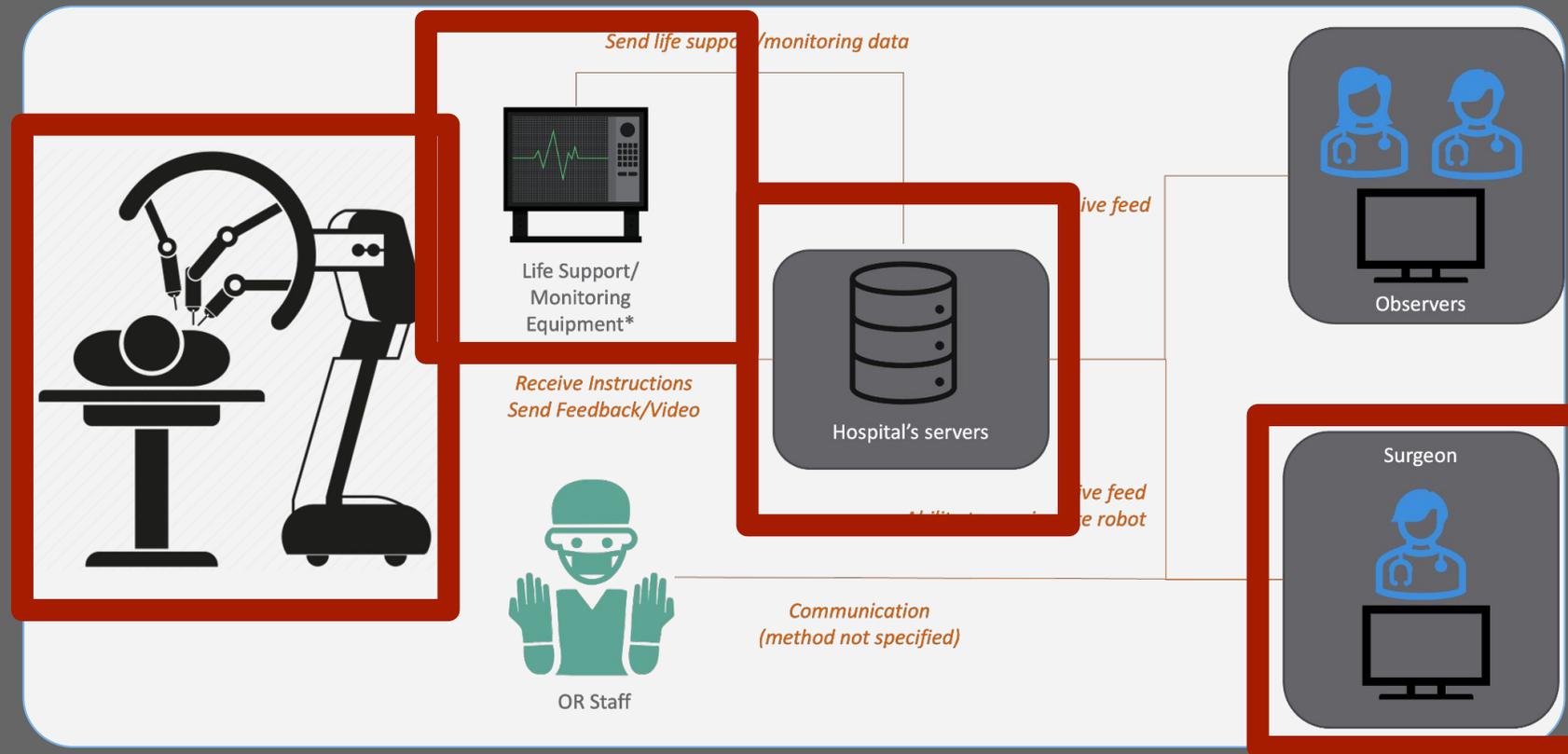
## Robotic Surgical System

Allow for remote surgery

Store surgical reports on hospital server

Observers are able to watch the surgery (including the surgeon's viewpoint) from their computers

Third-party monitoring equipment should send vitals to surgeon's console



Before recruiting, significant amount of time was invested in community engagement & building relationships



# We interviewed 12 experts involved in securing medical devices

Participants started their careers in...

...medical devices (6)

...security (6)

Participants hold roles in/as...

...large manufacturers (4)

...specialized manufacturers (4)

...consultants for manufacturers (4)

Participants had worked for...

...<5 years (2)

...5-10 years (1)

75%  
>10 years { ...10-20 years (2)  
                  ...20-30 years (4)  
                  ...30+ years (3)



# We developed a process model based on our results

Flexible process for brainstorming threats and controls

Safety considerations are critical, unclear how to integrate

Ad-hoc Navigation & Reliance on Use Cases for prioritization

} RQ1

RQ2

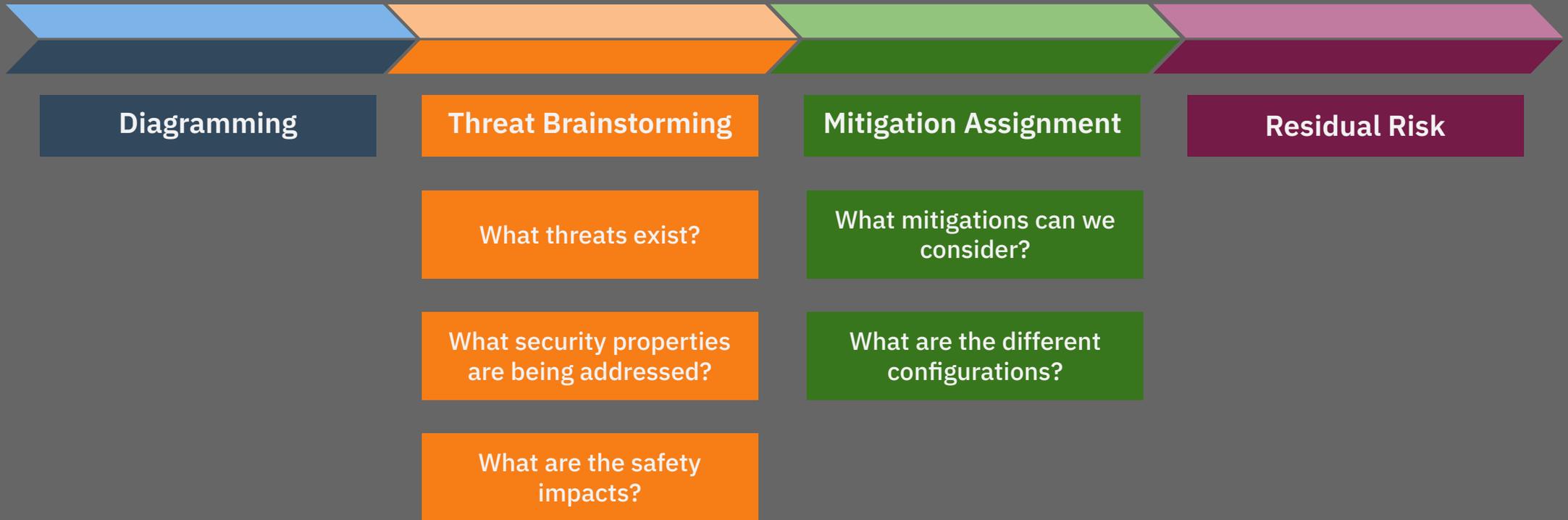


# We observed participants relying both explicitly and implicitly on Adam Shostack's Four Questions



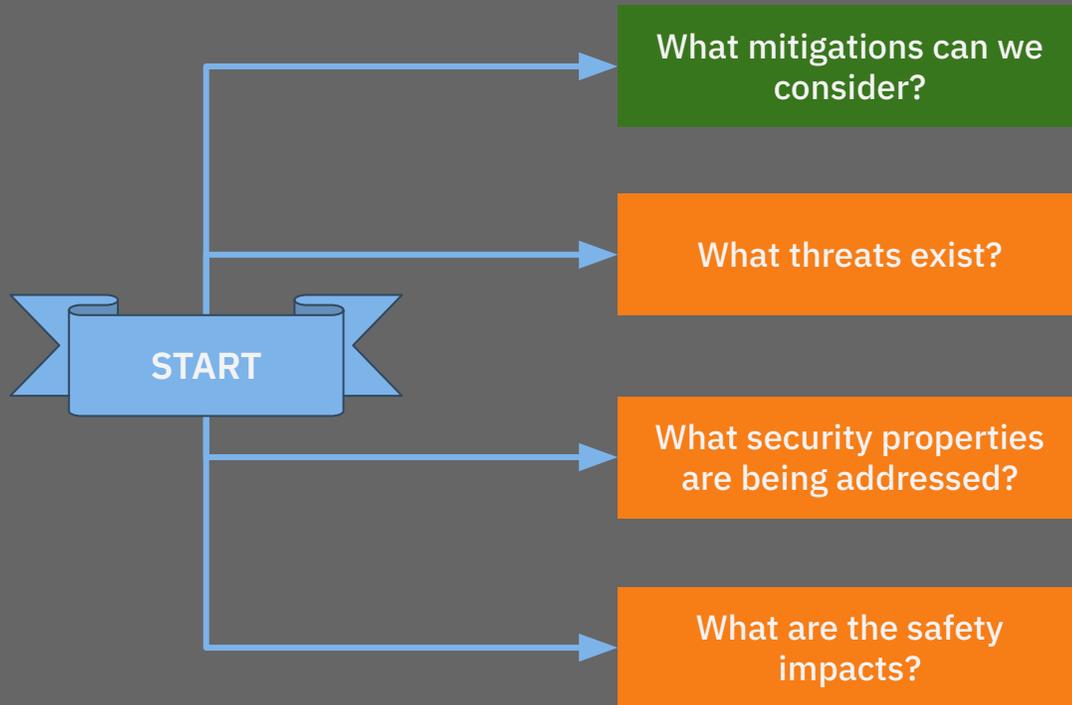
Flexible process for brainstorming threats and controls

# We found that participants answered common implicit and explicit threat related questions



Flexible process for brainstorming threats and controls

# When looking at a particular component of the system, participants initially answered different questions



Similar to the findings of prior work we found that these questions can be implicit assumptions [Van Landuyt & Joosen, *Softw Syst Model* 21]

Flexible process for brainstorming threats and controls

# Evaluating the component would involve answering the initial question and linking it to another question



“**INTEGRITY** of the data that flows across the system as well as the **AVAILABILITY** of the data flow and both could result in **HARM TO THE PATIENT**.”

Flexible process for brainstorming threats and controls

# It might also involve thinking about additional answers to the same question



“ If the hospitals in charge of setting it up themselves, ideally I'd say put it on a **SEPARATE VLAN** and then have more **INDIVIDUAL ACCESS** for that. And then obviously the researchers and providers only a couple would've access to that for the people who would actually need it. So it'd be more **ROLE BASED ACCESS**.

Flexible process for brainstorming threats and controls

# We developed a process model based on our results

Flexible process for brainstorming threats and controls

Safety considerations are critical, unclear how to integrate

Ad-hoc Navigation & Reliance on Use Cases for prioritization

} RQ1

RQ2



Despite suggestions from various standards to separate the two, security must consider the impact on safety and clinical efficacy

“We can't just look at where data resides, **WE CAN'T JUST SAY, 'HEY, HARDEN YOUR SERVERS,'** and things of that general statements. We have to really look at the function and what the data that's flowing between each component to understand and wrench its **IMPACT TO AFFECTING THAT CLINICAL WORKFLOW.**”

-Study Participant [emphasis added]

Safety considerations are critical, unclear how to integrate



Participants expressed concern about how safety and security teams operate independently and use different language

“The integration of this is very important, and we have **SEPARATE PROCESSES THAT HAVE SYNCHRONIZATION POINTS**, but without necessarily the two groups understanding each other, it **[POTENTIAL MISCOMMUNICATION] IS PRETTY DANGEROUS.**”

-Study Participant [emphasis added]

Safety considerations are critical, unclear how to integrate

# We developed a process model based on our results

Flexible process for brainstorming threats and controls

Safety considerations are critical, unclear how to integrate

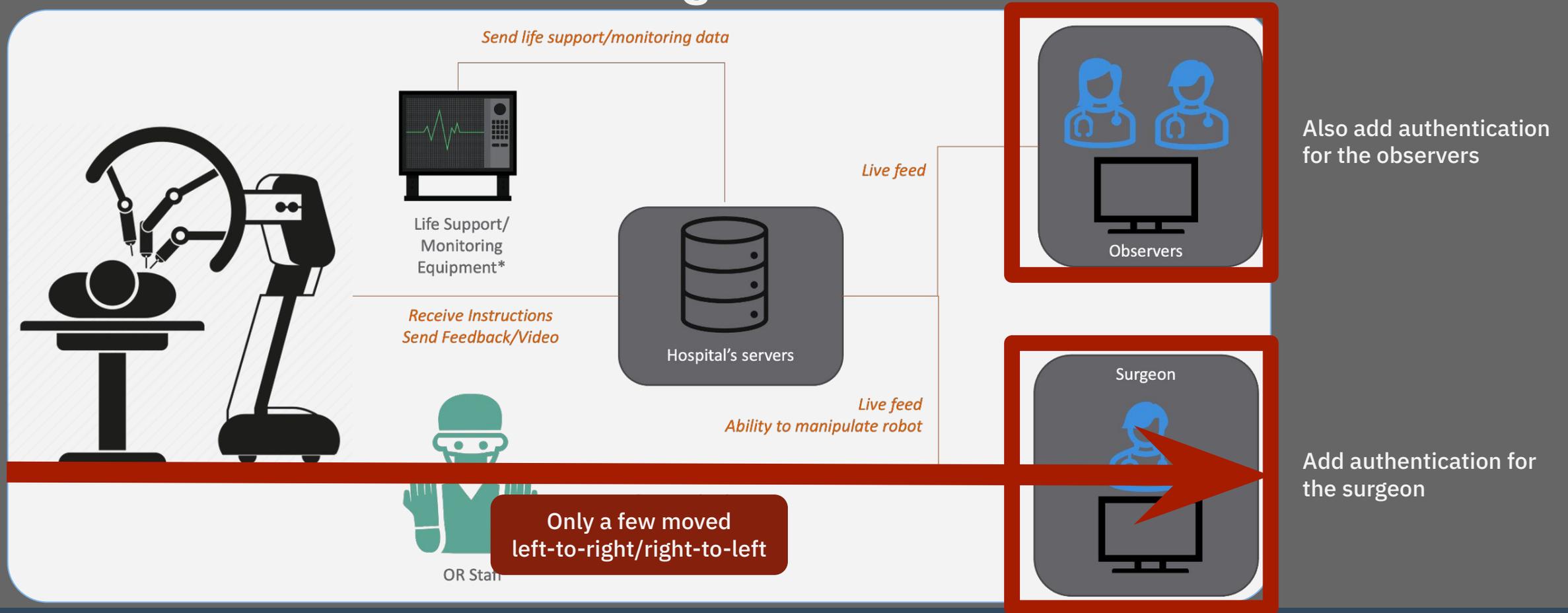
Ad-hoc Navigation & Reliance on Use Cases for prioritization

} RQ1

RQ2

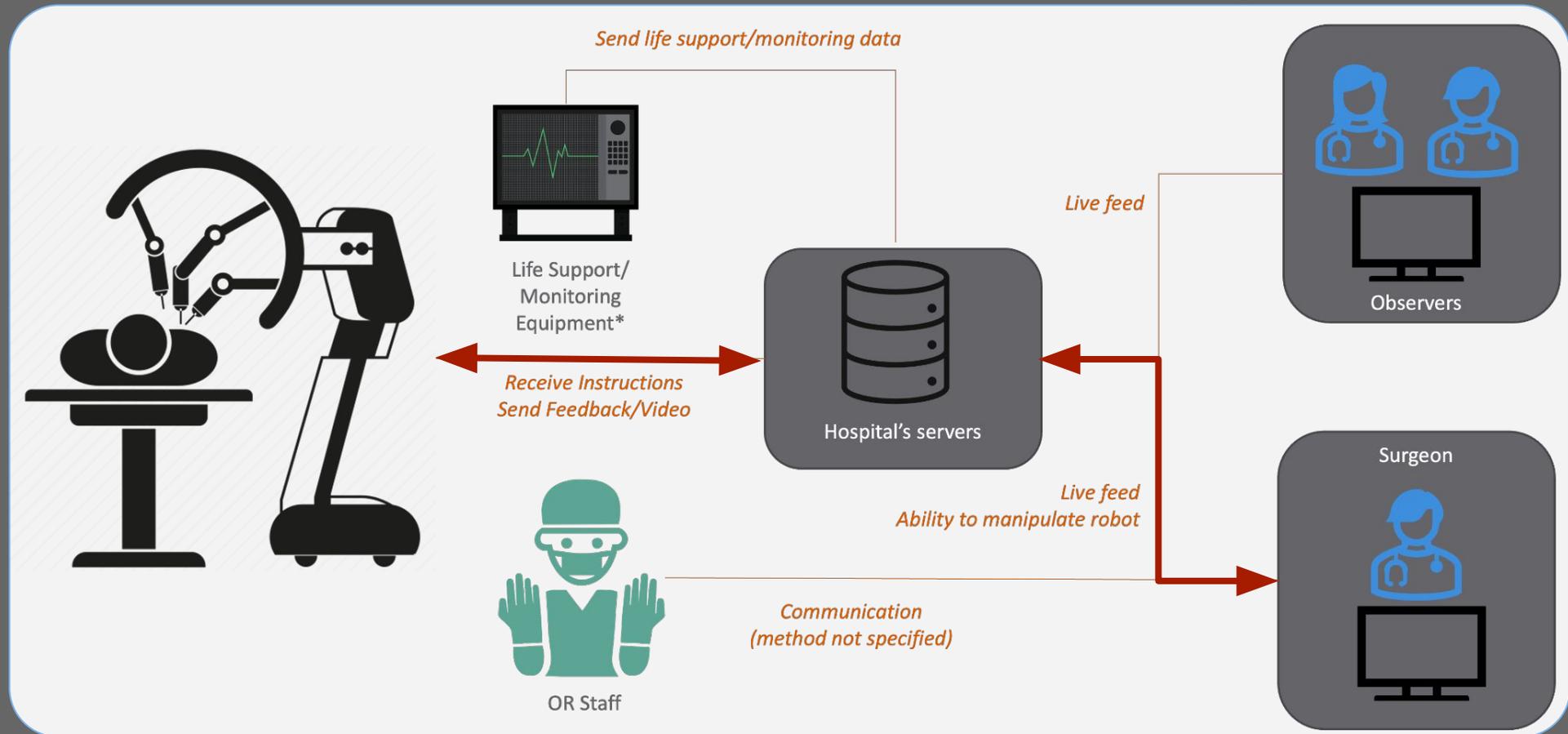


# Participants would bounce between parts of the system based on what they previously thought about



Ad-hoc Navigation & Reliance on Use Cases for prioritization

# Participants rely on Use Cases to help them focus, but this is not accounted for in formalized threat modeling processes



Adding more color to prior work that has found Data Flow Diagrams are not sufficient for threat modeling [Sion et al, ICSEW 20]

Ad-hoc Navigation & Reliance on Use Cases for prioritization

# Our recommendations include accommodating this “natural” process in threat modeling tools

## Automation & Tooling support the following:

Free-flowing process through interaction

Multiple configurations

Use-case views

Prompt for multi-patient harm

Integrate with safety risk processes

## FDA & Other Regulators should ensure that manufacturers:

Delineate internal vs. external architecture & explain which configurations are essential to what aspects of security

## Researchers are able to:

Build on top of the scenarios we developed to test frameworks and tools for medical device security & threat modeling

# Research Team



*Ronald Thompson  
Tufts University*



*Madeline McLaughlin  
Tufts University*



*Carson Powers  
Tufts University*



*Dan Votipka, PhD  
Tufts University*

# Acknowledgements



*Shannon Lantzy, PhD  
Independent Consultant*



*Rock Stevens, PhD  
US Army*



*Peter Ney, PhD  
University of Washington*



*Seth Carmody, PhD  
MedCrypt*



*Naomi Schwartz  
MedCrypt*



*Greg Garcia  
HSCC*

# Funding



# Takeaways

Flexible process for brainstorming threats and controls

Safety considerations are critical, unclear how to integrate

Use Cases/Workflows are useful tools for prioritization

## Supplemental Material

[osf.io/p9xky](https://osf.io/p9xky)

Includes scenarios, discussion on medical device regulations, codebook, and screening survey

# Questions?

[rthomp06@cs.tufts.edu](mailto:rthomp06@cs.tufts.edu)

[tsp.cs.tufts.edu](mailto:tsp.cs.tufts.edu)

## Funding Sponsors

