Overcoming IT and Cybersecurity Challenges With IOMT in Hospital-Based Medical Devices

Dave Saunders

CTO, Galen Robotics, Inc

Dave Saunders, Co-Founder, CTO Galen Robotics, Inc.

Twenty-five years experience product development and engineering and has taken over 40 products to market; product development experience ranging from startup to Fortune 500

Marketing/Technical Chair, AODI

Line Manager, Access Concentration, Ascend Communications

Technical manager, Access Concentration, Voice Gateway, Lucent Bell Labs

VP Product Manager, Navigated Orthopedics, Trak Surgical

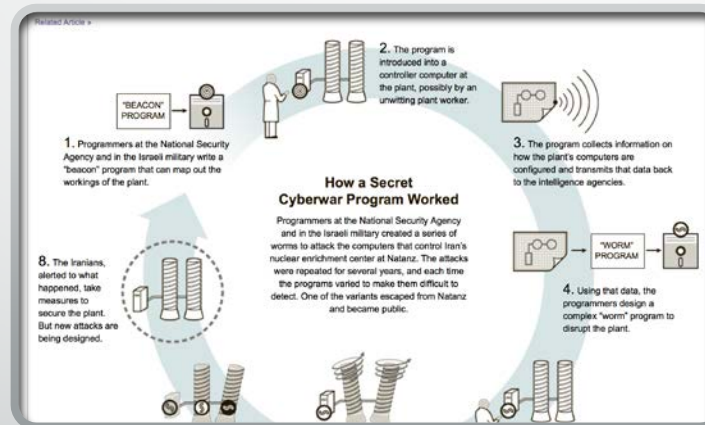Co-Founder & CTO, Surgical Robotics, Galen Robotics

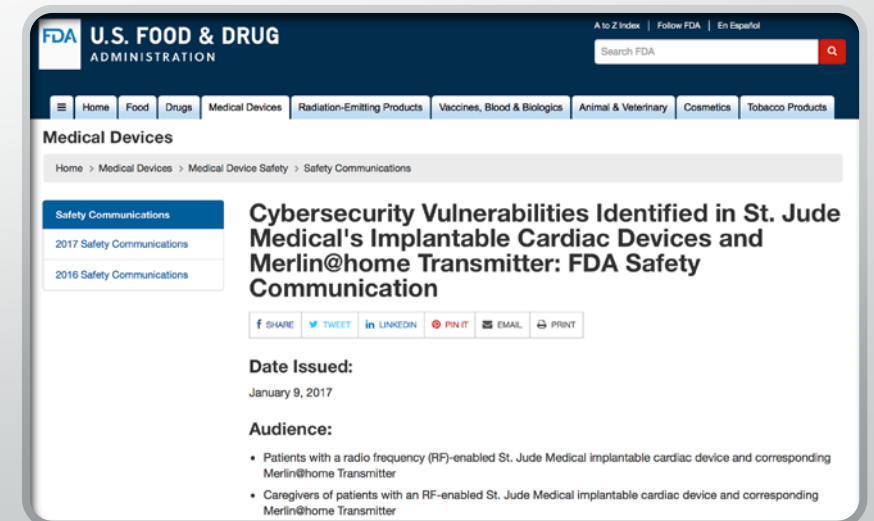# Medical Device & Industry Cybersecurity

Is the risk real?

Dave Saunders -- Galen Robotics, Inc.

Vulnerabilities in the News

- Do you want to be next?

Dave Saunders -- Galen Robotics, Inc.

THE HILL

FDA, industry fear wave of medical-device hacks

BY CASEY HARPER, THE HILL EXTRA - 04/10/17 01:05 PM EDT

289 SHARES

2 COMMENTS

Just In...

Offensive trademark requests up since Supreme Court ruling: report
BLOG BRIEFING ROOM — 05 AGO

Time to change US approach on the nuclear weapons ban treaty
CONTRIBUTORS — 29M 57S AGO

Scaramucci clarifies make-up artist comment: 'I need all the help I can get'
ADMINISTRATION — 60M 40S AGO

Pence: Trump is just getting started

Regulators and medical-device-makers are bracing for an expected barrage of hacking attacks even as legal and technical uncertainties leave them in uncharted territory.

More videos:

Most Popular

Related Article ▶

How a Secret Cyberwar Program Worked

Programmers at the National Security Agency and in the Israeli military created a series of worms to attack the computers that control Iran's nuclear enrichment center at Natanz. The attacks were repeated for several years, and each time the programs varied to make them difficult to detect. One of the variants escaped from Natanz and became public.

1. Programmers at the National Security Agency and in the Israeli military write a "beacon" program that can map out the workings of the plant.

"BEACON" PROGRAM

2. The program is introduced into a controller computer at the plant, possibly by an unwitting plant worker.

3. The program collects information on how the plant's computers are configured and transmits that data back to intelligence agencies.

4. Using that data, the programmers design a complex "worm" program to disrupt the plant.

"WORM" PROGRAM

8. The Iranians, alerted to what happened, take measures to secure the plant. But new attacks are being designed.

Pharmaceutical giant rocked by ransomware attack

By **Hamza Shaban** and **Ellen Nakashima** June 27

Decoding Internet Security: Ransomware

DECODING INTERNET SECURITY:
RANSOMWARE

▶ Play Video 2:24

Here is what you need to know about ransomware: software that locks down your files and demands payment to release them. (Sarah Parnass, Dani Player, Daron Taylor/The Washington Post)

FDA Warnings and Recalls

Attacks on Networks

- If the network you're on, is compromised, how is your device affected?
  - Operations
  - Monitoring
  - License Control

Hacker group Anonymous targets Children's Hospital

By Michael B. Farrell and Patricia Wen | GLOBE STAFF APRIL 24, 2014

Fair Warning to Do Your Part

11739

Federal Register
Vol. 78, No. 33
Tuesday, February 19, 2013

Presidential Documents

Title 3—

The President

Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. *Critical Infrastructure.* As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic

Dave Saunders -- Galen Robotics, Inc.

Baking Security Into Your Products

Dave Saunders -- Galen Robotics, Inc.

A Robot Alone, Isn't a Product

Today's tech medical devices should be online to provide the customers with a richly integrated experience

Mantra

There is no security but the security you make.

Michael W Wellman, CEO, Virgil Security

Our Mission and Responsibility

Protect

- Take steps to add cybersecurity consideration to the design and development process
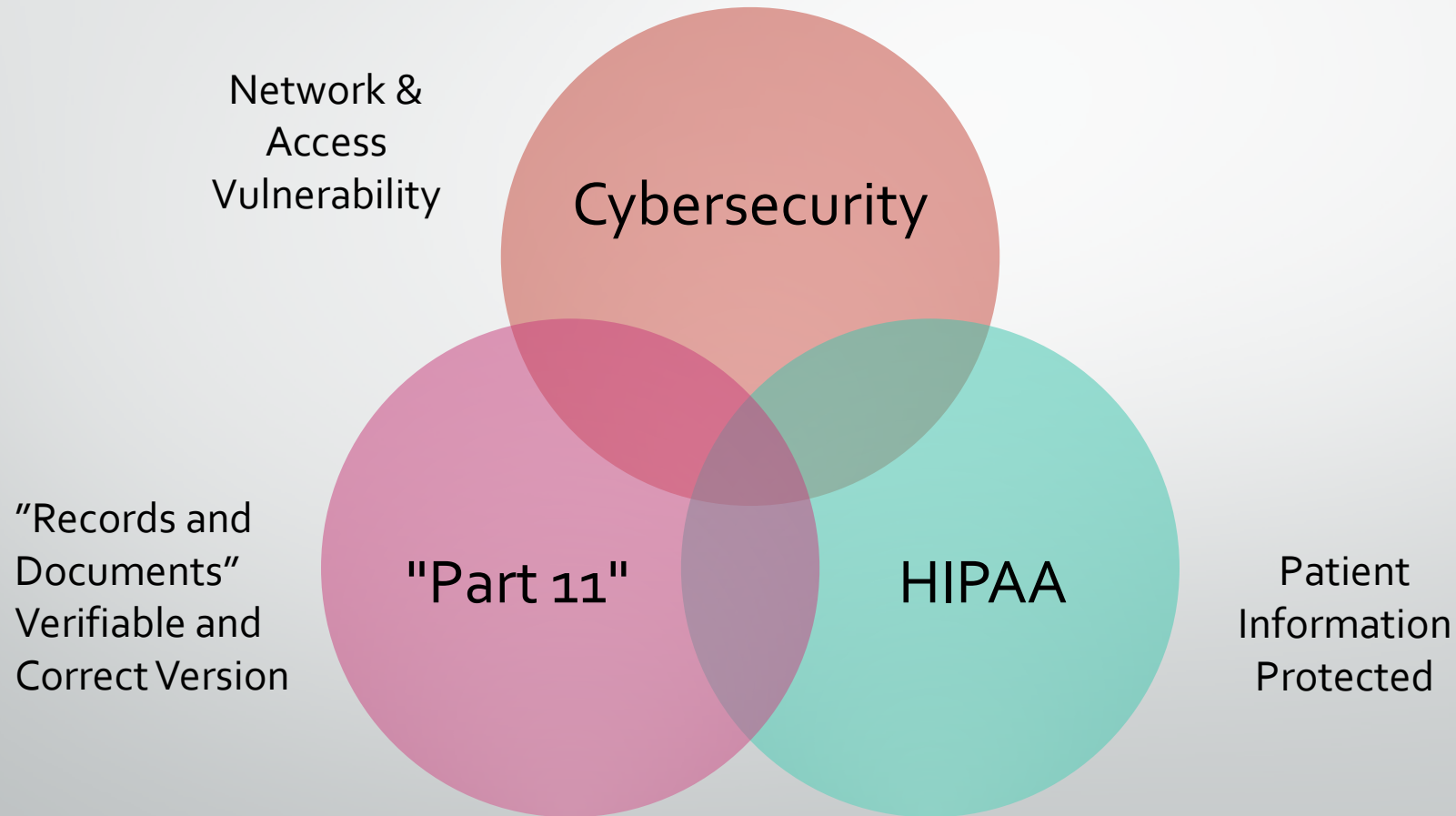- Identify all points of potential vulnerability and employ best efforts to secure them

Detect

- Build intrusion detection (when possible) into the architecture
- Perform penetration testing regularly

Inform

- Inform the public when something unexpected happens with production equipment

Dave Saunders -- Galen Robotics, Inc.

Addressing Vulnerabilities Multiple Contexts

Network & Access Vulnerability

Cybersecurity

"Records and Documents" Verifiable and Correct Version

"Part 11"

HIPAA

Patient Information Protected

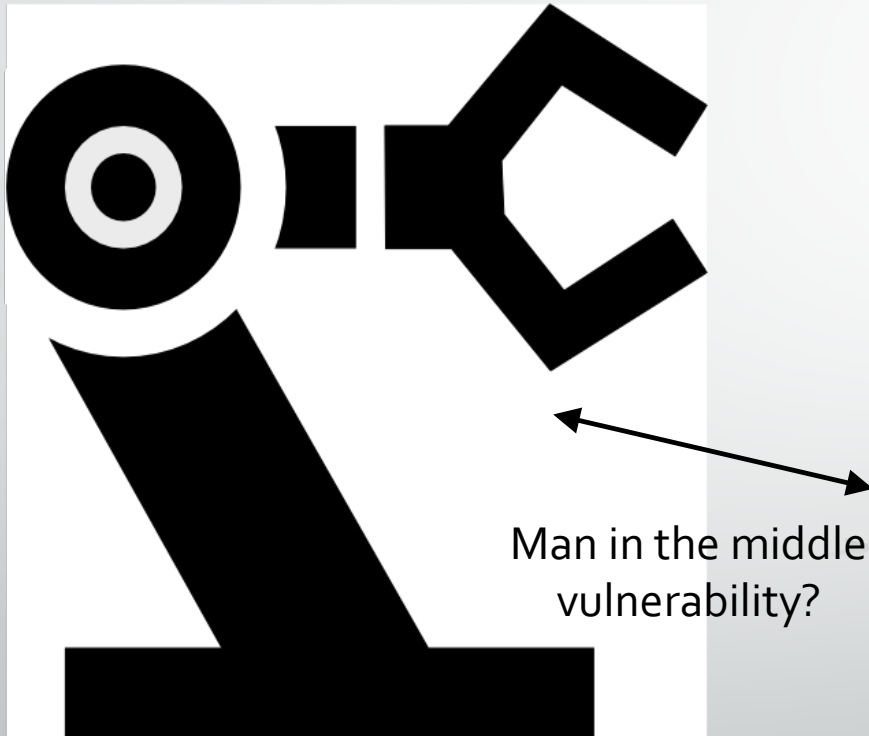Dave Saunders -- Galen Robotics, Inc.

The Basic Robot

A basic "slave" and "master" robotic architecture.

Similar to many medical devices – A "brain" communicates with, coordinates & controls combinations of sensors and "actors"
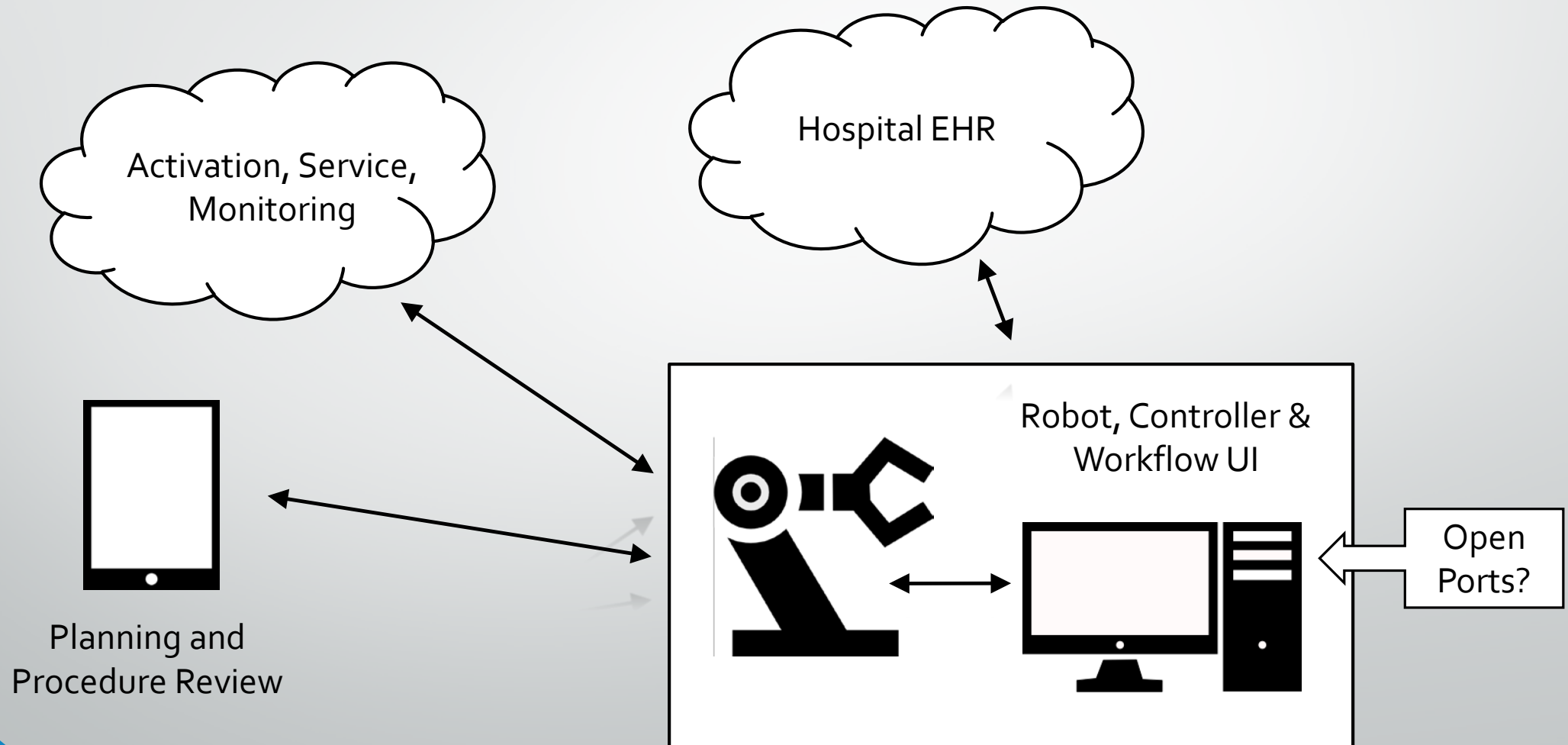
How does data flow between them?

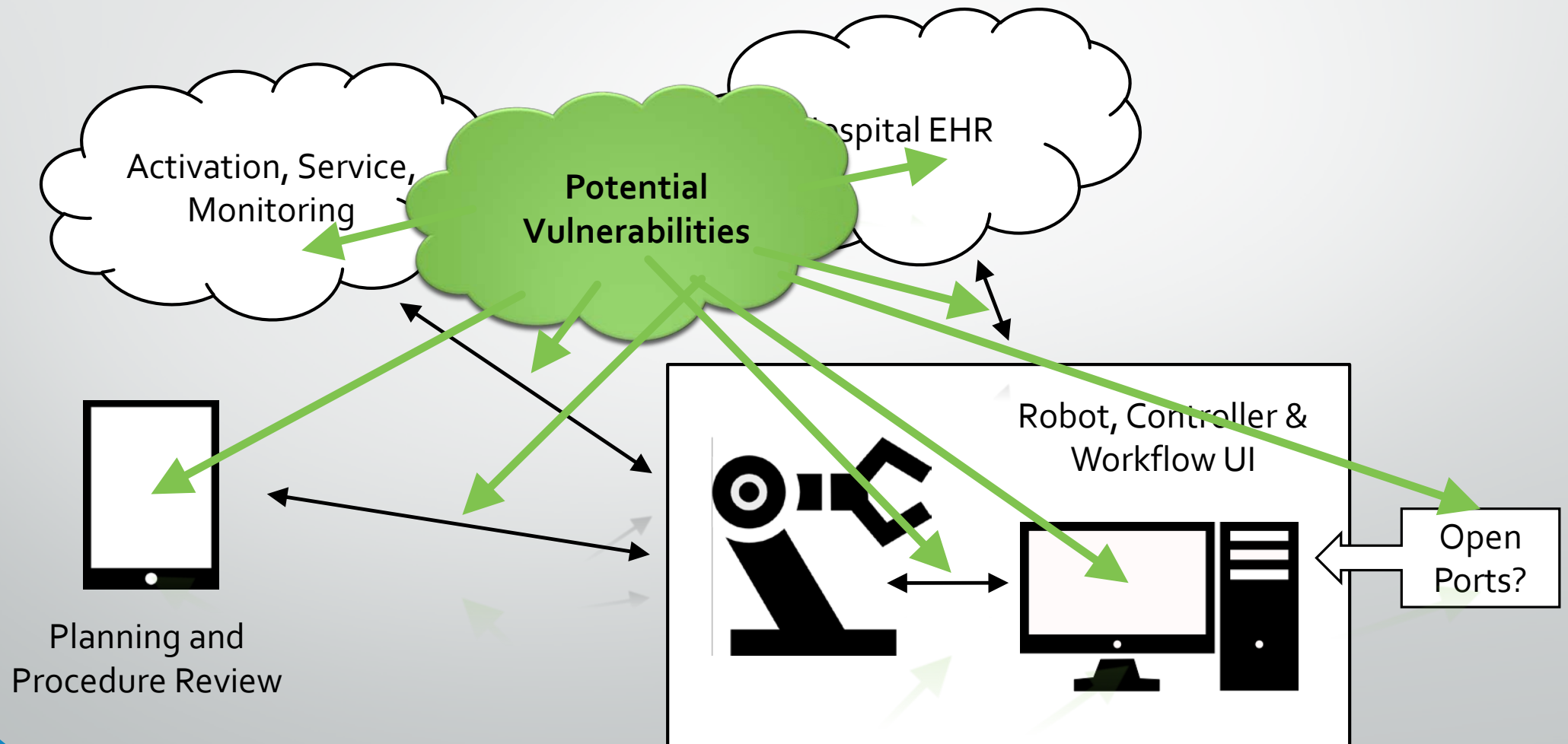Man in the middle vulnerability?

Dave Saunders -- Galen Robotics, Inc.

Today's Market Expects More IT Integration for Medical Devices

Activation, Service, Monitoring

Hospital EHR

Planning and Procedure Review

Robot, Controller & Workflow UI

Open Ports?

Dave Saunders -- Galen Robotics, Inc.

Today's Market Expects More IT Integration for Medical Devices – more risks for vulnerabilities

Activation, Service, Monitoring

Potential Vulnerabilities

Hospital EHR

Robot, Controller & Workflow UI

Open Ports?

Planning and Procedure Review

Dave Saunders -- Galen Robotics, Inc.

InfoSec Strategies

- **Do assume the network you're on is not secure**
  - Encrypt and authenticate whenever possible
- **Don't assume your only risks are network-based**
- **Do remain vigilant and make**
- **Don't assume those with physical access to your device will only to the "right thing"**
  - Be creative with failure modes for unexpected events; they're not always done with ill-intent
  - E.g., what if someone tries to charge their phone with an open USB port on your system?
- **Your device brings a greater benefits to patient care and the Industry as a connected part of the IOMT ecosystem, than sealed away**

Dave Saunders -- Galen Robotics, Inc.

https://www.dhs.gov/isao

Get Help

Dave Saunders -- Galen Robotics, Inc.

Learn Best Practices

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Dave Saunders -- Galen Robotics, Inc.