IIA CHICAGO
CHAPTER
58TH ANNUAL
SEMINAR
2018

TRANSFORMING...
OURSELVES.
OUR WORKPLACE.
OUR PROFESSION.

NTAC:4UC-11

AUDITING ROBOTICS AND THE INTERNET OF THINGS (IOT)

APRIL 9, 2018

PRESENTERS

Kara Nagel
Manager, Information Security
Accenture

Ryan Hopkins
Assistant Director, Internal Audit Services
Packaging Corp. of America

AGENDA

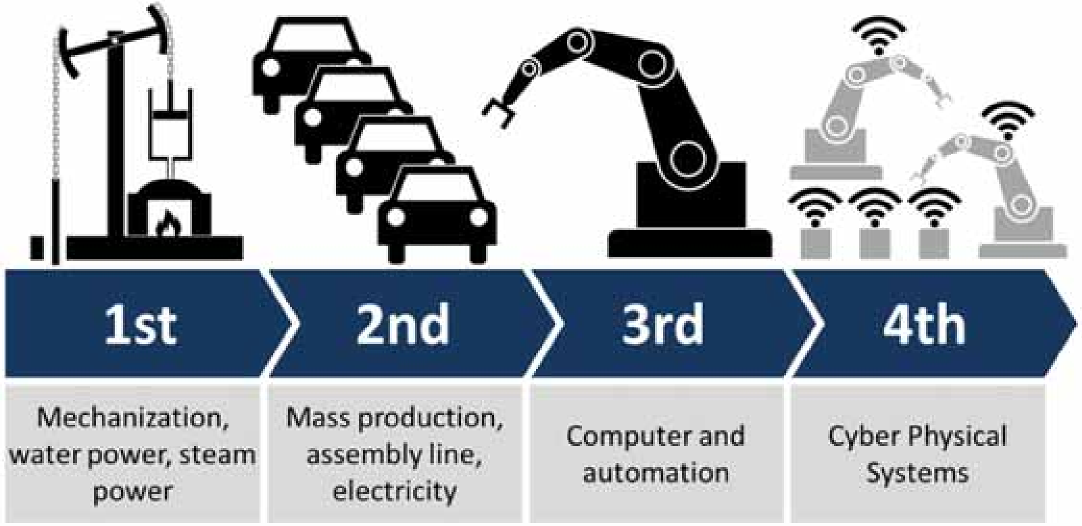
Topics
1. Introduction
2. What is Robotics & IOT?
3. News Worthy Breaches and New Regulations
4. Case Study 1: Auditing Manufacturing Control Networks
5. Case Study 2: Auditing Embedded Software
6. Key Takeaways
7. Q&A

OBJECTIVES

- By the end of this course, you will be able to:
  - Identify Robotics and IOT applications within organizations.
  - Assess and audit the unique risks associated with Robotics and IOT.
  - Communicate the likelihood and impact of common risks.

WHAT ARE ROBOTICS?

- Robotics is an interdisciplinary branch of engineering and science that includes mechanical engineering, electrical engineering, computer science, and others. Robotics deals with the design, construction, operation, and use of robots, as well as computer systems for their control, sensory feedback, and information processing. (Source: https://en.wikipedia.org/wiki/Robotics)


1st
2nd
3rd
4th
Mechanization, water power, steam power
Mass production, assembly line, electricity
Computer and automation
Cyber Physical Systems

(Source: http://www.innovationmanagement.se/2016/12/29/industry-4-0-and-the-internet-of-things-iot/)

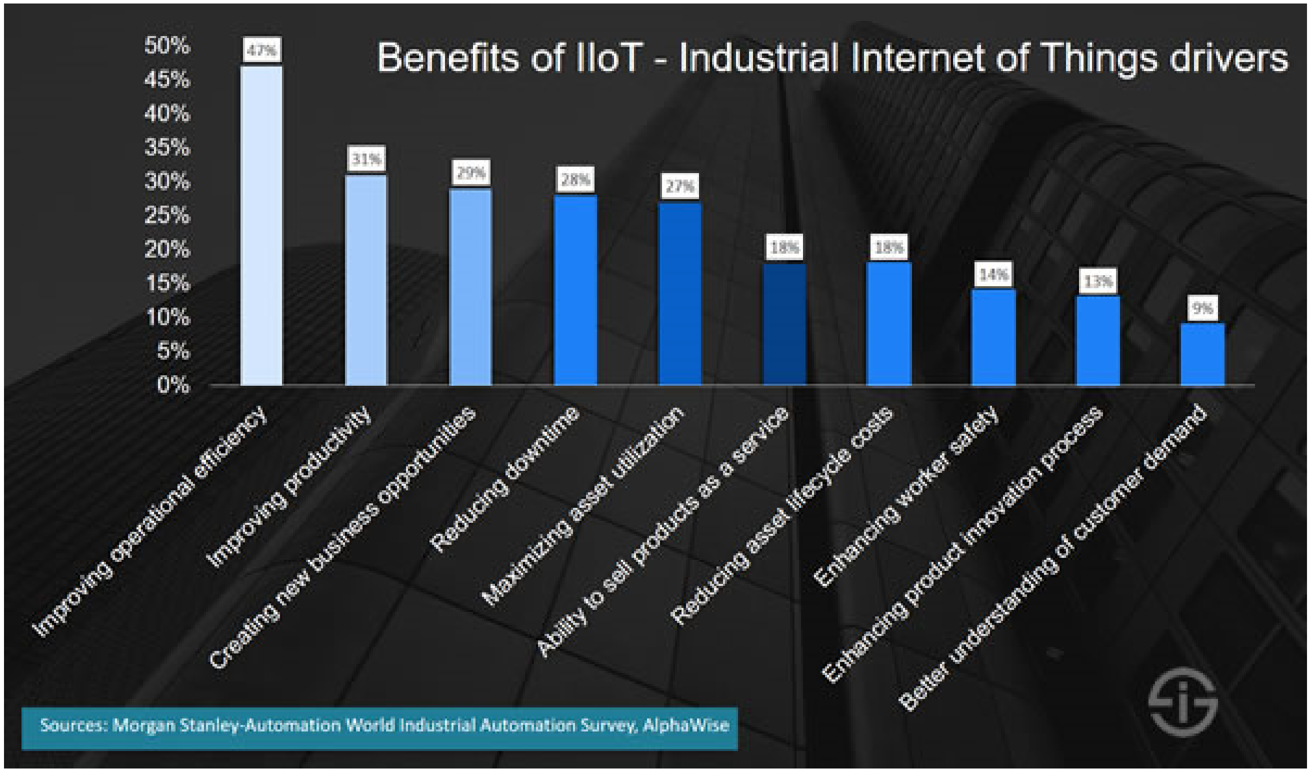
WHAT IS THE INTERNET OF THINGS (IOT)?

- The Internet of things (IoT) is the network of physical devices, vehicles, appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. (Source: https://en.wikipedia.org/wiki/Internet_of_things)

SMART Automobile
SMART Energy
SMART Health Care
SMART Manufacturing
SMART Retail
SMART Surveillance
SMART Home
SMART Agriculture

(Source: https://www.letsnurture.com/solutions/internet-things-iot-solutions.html)

BENEFITS DRIVING ADOPTION

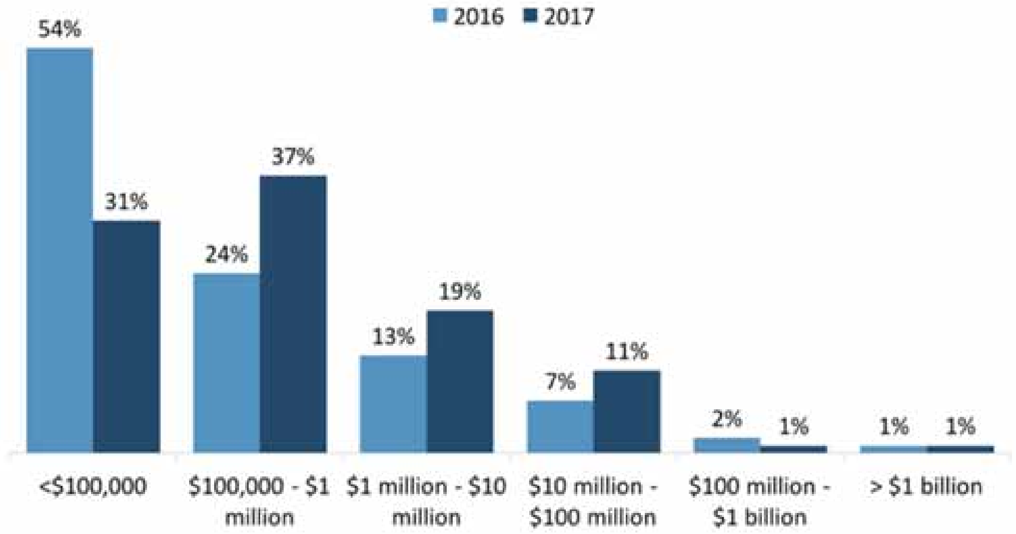

Benefits of IIoT - Industrial Internet of Things drivers

Sources: Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

ADOPTION RATE

Companies' Planned 5-Year Investment In IoT Solutions

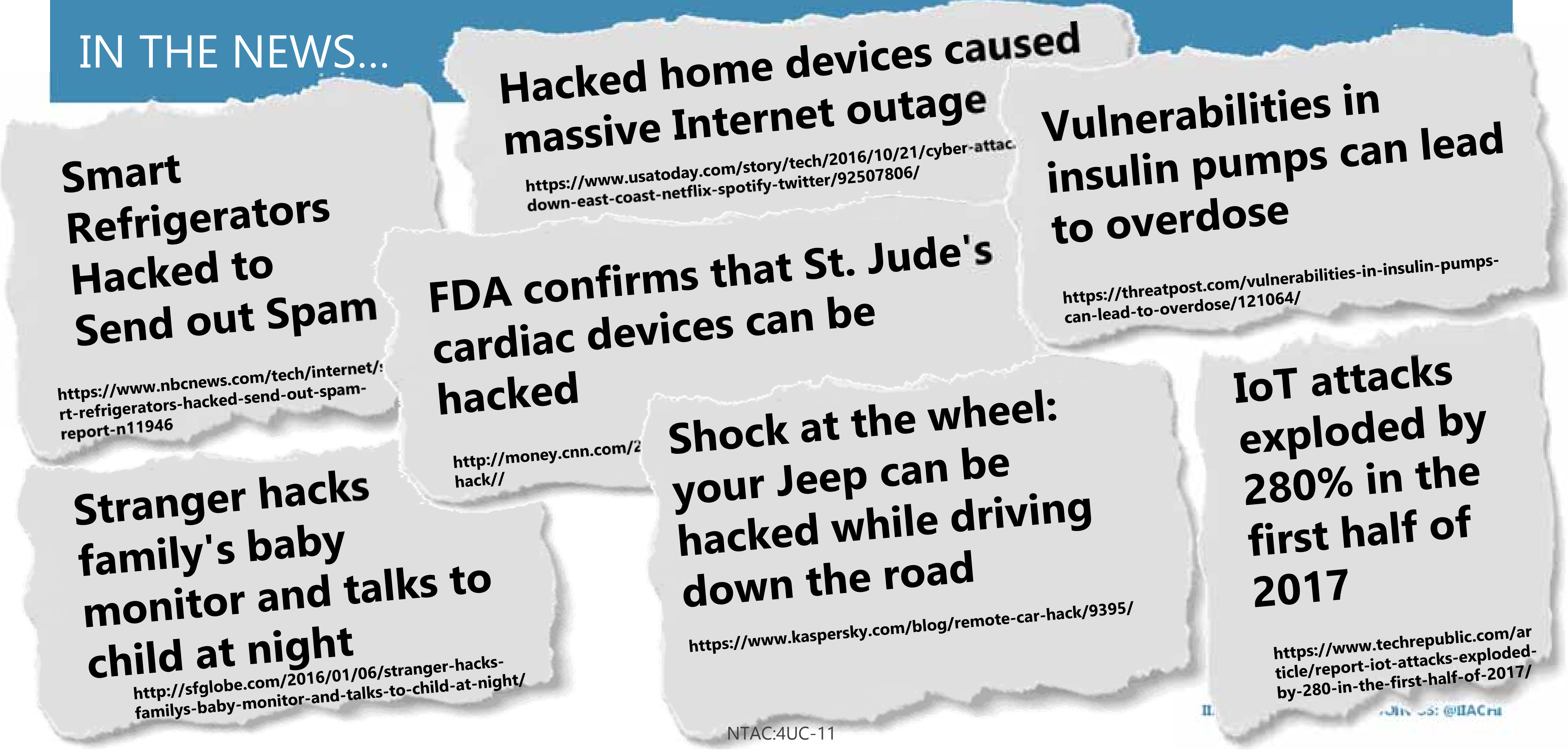
Global



Source: Business Insider Global IoT Executive Surveys, n=235 IoT users, 2016; n=75 IoT users, 2017

EXCLUSIVE DATA FROM BI INTELLIGENCE

IN THE NEWS…



Hacked home devices caused massive Internet outage

https://www.usatoday.com/story/tech/2016/10/21/cyber-attac down-east-coast-netflix-spotify-twitter/92507806/

Vulnerabilities in insulin pumps can lead to overdose

https://threatpost.com/vulnerabilities-in-insulin-pumps-can-lead-to-overdose/121064/

Smart Refrigerators Hacked to Send out Spam

https://www.nbcnews.com/tech/internet/s rt-refrigerators-hacked-send-out-spam-report-n11946

FDA confirms that St. Jude's cardiac devices can be hacked

http://money.cnn.com/2 hack//

Stranger hacks family's baby monitor and talks to child at night

http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/

Shock at the wheel: your Jeep can be hacked while driving down the road

https://www.kaspersky.com/blog/remote-car-hack/9395/

IoT attacks exploded by 280% in the first half of 2017

https://www.techrepublic.com/ar ticle/report-iot-attacks-exploded-by-280-in-the-first-half-of-2017/

INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2017

- Scope:
  - Limited to U.S. Government-purchased devices.
  - Relies heavily on NIST 800-53 standards.
  - Applies to any device that has an internet connection and can transmit data.

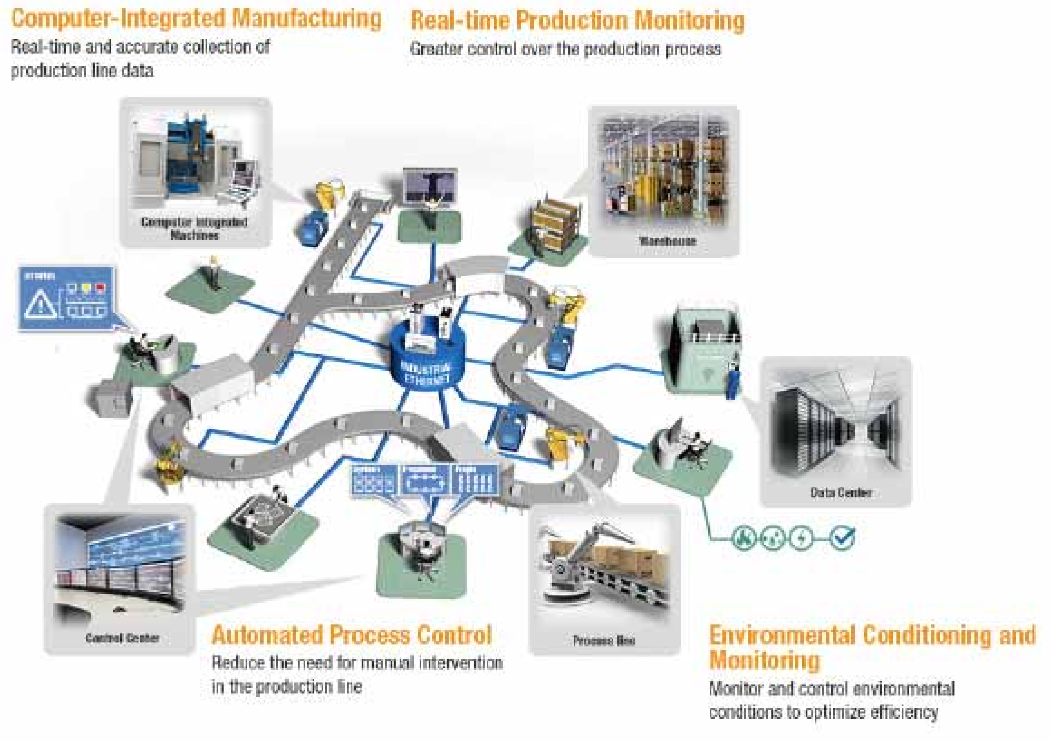
- Regulatory Requirements:
  - Requires that any device sold to the US must be patchable / allow for security updates.
  - Not have any known security vulnerabilities.
  - Permit users to change default passwords.

https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

CASE STUDY 1: MANUFACTURING CONTROL NETWORKS

WHAT ARE MANUFACTURING CONTROL NETWORKS?

- Manufacturing control systems monitor and operate industrial equipment that support automated manufacturing processes.
- The control room operator terminals, process engineering workstations, and control system servers on the control networks use proprietary software and specialized controller devices to monitor and operate sensors, valves, breakers, pumps, and other automated components of industrial equipment.



Computer-Integrated Manufacturing
Real-time and accurate collection of production line data

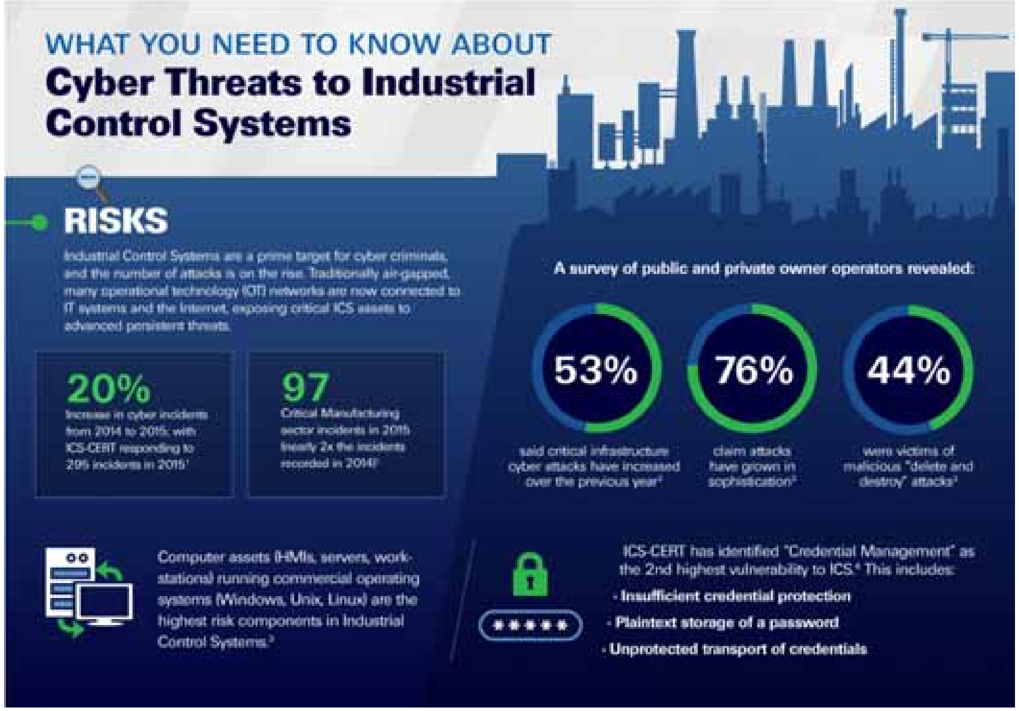
Real-time Production Monitoring
Greater control over the production process

Automated Process Control
Reduce the need for manual intervention in the production line

Environmental Conditioning and Monitoring
Monitor and control environmental conditions to optimize efficiency

WHY AUDIT MANUFACTURING CONTROL NETWORKS?

- Legacy control systems were not designed with the same level of security as business systems and modern control systems.
- Manufacturing companies are leveraging data analytics and data visualization to optimizing manufacturing processes. There is an increasing demand for large volumes of real-time data from manufacturing control systems that requires additional integration between the control networks and other business systems.
- A cyber-attack or other control system incident could damage critical equipment and result in unscheduled manufacturing downtime.



WHAT YOU NEED TO KNOW ABOUT
Cyber Threats to Industrial Control Systems

RISKS

Industrial Control Systems are a prime target for cyber criminals, and the number of attacks is on the rise. Traditionally air-gapped, many operational technology (OT) networks are now connected to IT systems and the Internet, exposing critical ICS assets to advanced persistent threats.

20% Increase in cyber incidents from 2014 to 2015; with ICS-CERT responding to 295 incidents in 2015[1]

97 Critical Manufacturing sector incidents in 2015 (nearly 2x the incidents recorded in 2014)[1]

A survey of public and private owner operators revealed:

53% said critical infrastructure cyber attacks have increased over the previous year[2]

76% claim attacks have grown in sophistication[2]

44% were victims of malicious "delete and destroy" attacks[2]

Computer assets (HMIs, servers, work-stations) running commercial operating systems (Windows, Unix, Linux) are the highest risk components in Industrial Control Systems.[3]

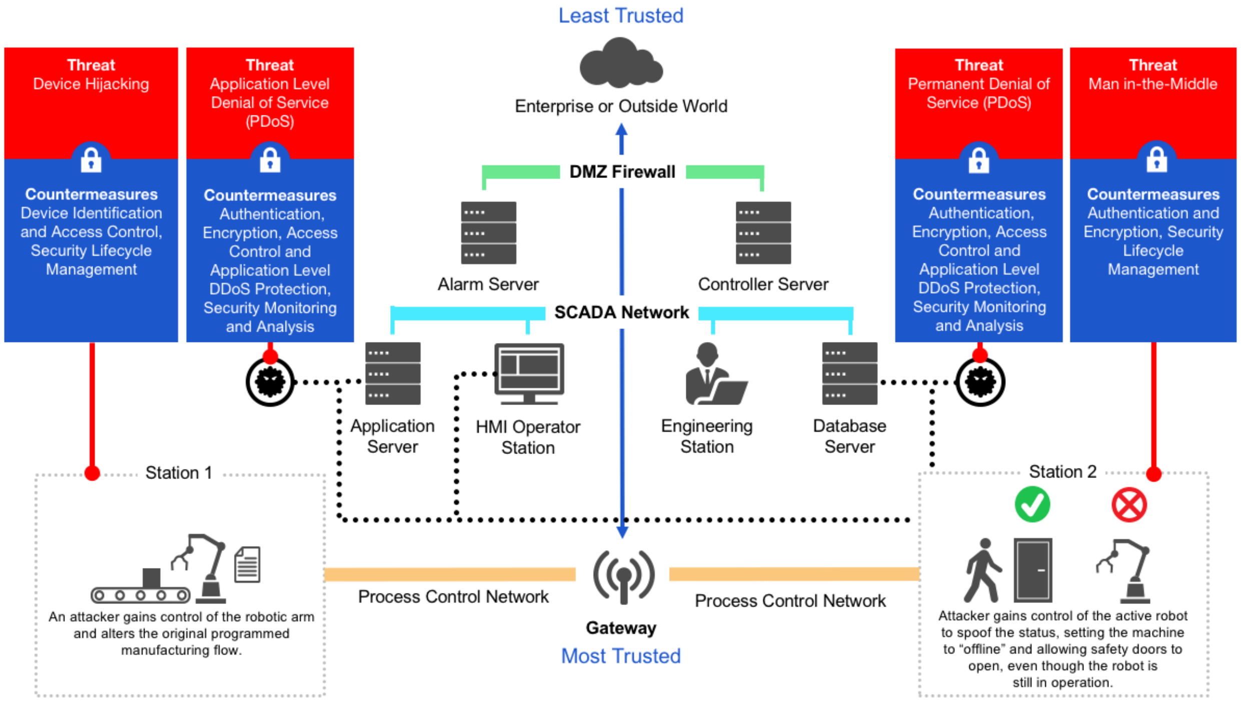
ICS-CERT has identified "Credential Management" as the 2nd highest vulnerability to ICS.[4] This includes:

- **Insufficient credential protection**
- **Plaintext storage of a password**
- **Unprotected transport of credentials**

(Source: http://www.cyberark.com/wp-content/uploads/2016/06/Cyber-threats-to-ICS_FINAL-060216.jpeg)

RELEVANT NETWORK SECURITY AUDIT AREAS AND RISKS

- **Evaluate Network Segmentation** – Integrated open network architectures significantly increases the risk that a virus or attacker could migrate from a company's business network and other network segments onto the control network and disrupt manufacturing processes.
- **Assess Network Device Configuration and Patch Management** – Network devices route network traffic between network segments and an attacker could exploit vulnerable network devices and obtain unauthorized access to the control network.



Least Trusted

Enterprise or Outside World

DMZ Firewall

Alarm Server

Controller Server

SCADA Network

Application Server

HMI Operator Station

Engineering Station

Database Server

Threat
Device Hijacking

Countermeasures
Device Identification and Access Control, Security Lifecycle Management

Threat
Application Level Denial of Service (PDoS)

Countermeasures
Authentication, Encryption, Access Control and Application Level DDoS Protection, Security Monitoring and Analysis

Threat
Permanent Denial of Service (PDoS)

Countermeasures
Authentication, Encryption, Access Control and Application Level DDoS Protection, Security Monitoring and Analysis

Threat
Man in-the-Middle

Countermeasures
Authentication and Encryption, Security Lifecycle Management

Station 1

An attacker gains control of the robotic arm and alters the original programmed manufacturing flow.

Process Control Network

Gateway

Most Trusted

Process Control Network

Station 2

Attacker gains control of the active robot to spoof the status, setting the machine to "offline" and allowing safety doors to open, even though the robot is still in operation.

(Source: https://www.rambus.com/iot/industrial-iot/)

RELEVANT PHYSICAL ACCESS AUDIT AREAS AND RISKS

- **Review Access to Device Input Ports** – If device input ports (e.g. Universal Serial Bus) are not locked or disabled a vendor or an unauthorized employee could connect an untrusted device and intentionally or unintentionally load malicious software onto the control network systems.
- **Evaluate Location Physical Access Management** – An unauthorized employee or vendor could gain access to control systems and damage hardware and create unplanned downtime.

RELEVANT LOGICAL ACCESS AUDIT AREAS AND RISKS

- **Review Access User Access Management** – Unauthorized personnel can use a default account and unused accounts if not removed or disabled in a timely manner.
- **Evaluate Password Management** – Unauthorized users could exploit default passwords, shared passwords and other password configuration weaknesses and gain unauthorized access to control systems.

RELEVANT SOFTWARE MANAGEMENT AUDIT AREAS AND RISKS

- **Review Access Software Update, Patch, and Change Management** – If software updates and patches are not applied in a timely manner, vulnerabilities increase the risk of an attacker gaining unauthorized access, or rendering a system inaccessible.
  - **Evaluate Testing Process for Proprietary Software** - As new vulnerabilities are identified, software vendors release software updates and patches to remediate vulnerabilities, but those updates are not tested and verified by software vendors at the same frequency. Some updates require significant capital investments and can only be implemented during a full manufacturing outages.

CASE STUDY II: EMBEDDED SOFTWARE

EMBEDDED SOFTWARE / IOT

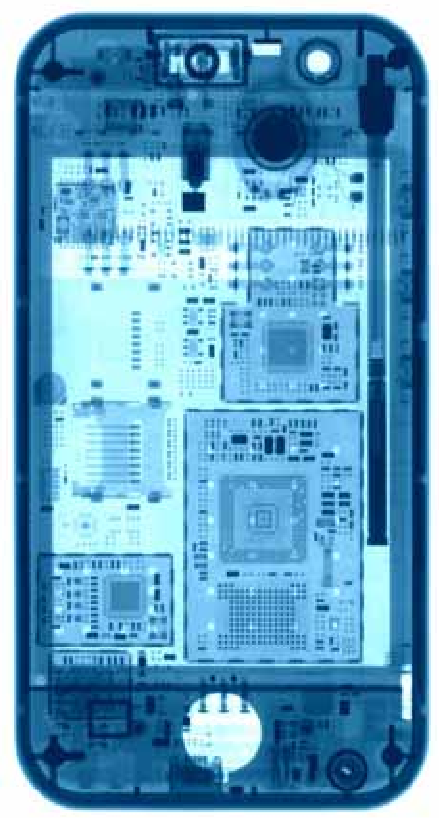
- **Embedded Software:** Piece of software that is embedded in hardware or non-PC devices, including IOT and Robotics. It is written specifically for the particular hardware that it runs on and usually has processing and memory constraints because of the device’s limited computing capabilities.

High Speed Trains – Have you considered the reliance placed on automated train track signals and controllers and impacts if those automated controllers were compromised?

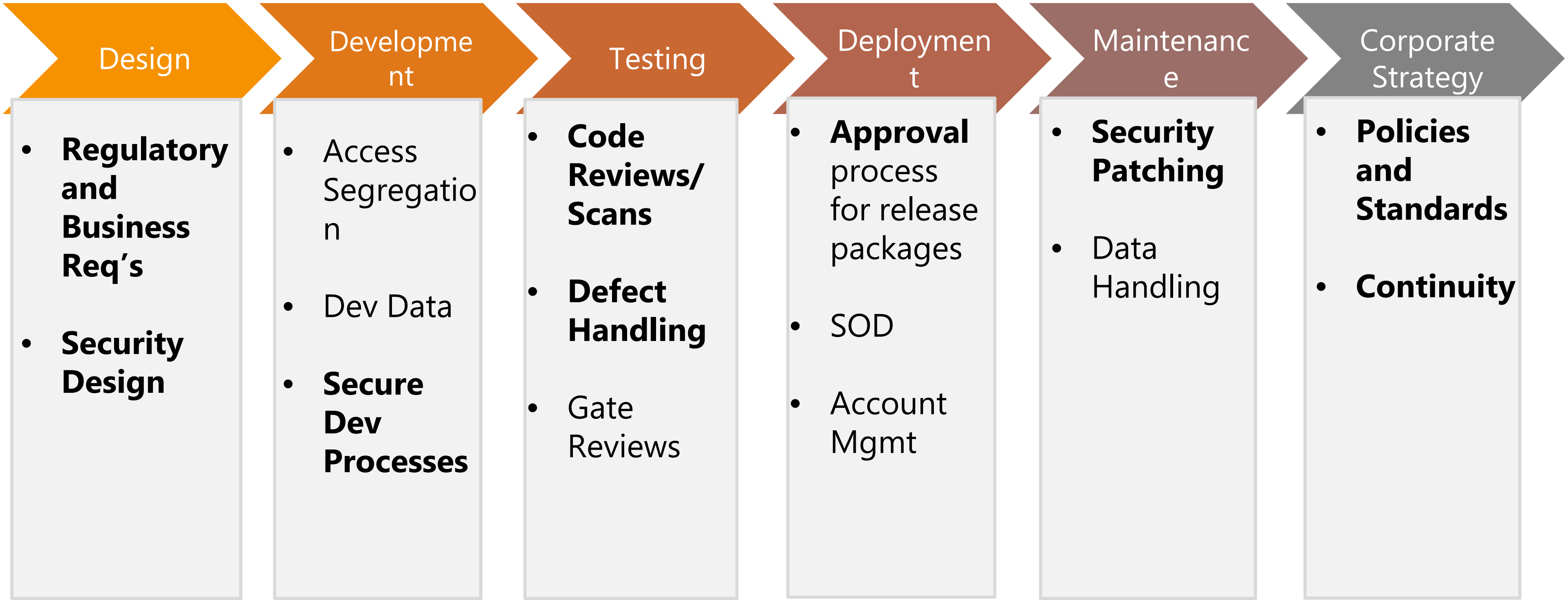
Blood Tests – Have you considered the reliance placed on automated medical testing devices and the inaccurate results that could be produced if device was compromised?

WHY AUDIT IOT & EMBEDDED SOFTWARE?

- Embedded software can be in everyday objects, mission critical devices, or devices with life and death impact.
- Security is not always considered throughout the design and development phase. **But it should be.**
- Common Arguments:
  - Security increases design cost
  - Security decreases innovation
  - Security impacts performance
  - Security is not a requirement for this IOT device
  - IOT consumers don’t care about Security



KEY COMPONENTS OF THE IOT DEVELOPMENT LIFECYCLE



Design

- **Regulatory and Business Req's**
- **Security Design**

Development

- Access Segregation
- Dev Data
- **Secure Dev Processes**

Testing

- **Code Reviews/ Scans**
- **Defect Handling**
- Gate Reviews

Deployment

- **Approval** process for release packages
- SOD
- Account Mgmt

Maintenance

- **Security Patching**
- Data Handling

Corporate Strategy

- **Policies and Standards**
- **Continuity**

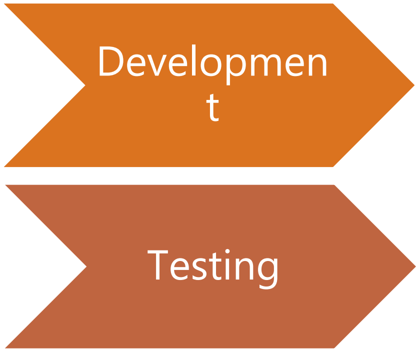
RELEVANT IOT DEVELOPMENT LIFECYCLE AUDIT AREAS & RISKS

Design

- **Regulatory & Business Requirements** – Certain regulations may exist that will need to be considered in the design phase. Regulations may include country-specific data privacy or access stipulations, safety or health requirements (FDA), or industry-specific controls (PCI).

- **Security Design** – IOT development typically focuses on developing quickly based on functionality requirements. Security considerations need to be integrated into the design to ensure compliance with regulations. Key security design components include how users and other connecting systems will **authenticate**, how **passwords** are managed, and how firmware **updates** can be pushed to the embedded software / IOT device.

RELEVANT IOT DEVELOPMENT LIFECYCLE AUDIT AREAS & RISKS


Developmen
t

Testing

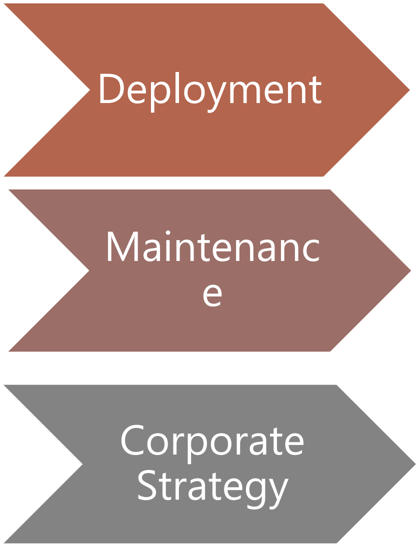
- **Secure Development** – Developers should follow a development methodology, which includes requirements relating to types of data used in lower environments, automation permitted, and ongoing testing/peer code reviews.

- **Code Reviews / Scans** – Code reviews and scans will assess for vulnerabilities or exploits in a small code base. These reviews should happen throughout the development process.

- **Defect Handling** – As defects are identified through development and testing, a process should be implemented to log the defects, assess the defects for impact to the greater project, and remediate defects through future development waves or releases.

RELEVANT IOT DEVELOPMENT LIFECYCLE AUDIT AREAS & RISKS

- **Approval Process** – Formal approvals from the business stakeholders should be collected during the design, development, testing, and release process.
- **Security Patching / Firmware Updates** – A process exists to patch or provide updates for IOT devices and embedded software. If this cannot be performed centrally, guidance should be provided and updates readily available to consumer.
- **Policies & Procedures** - Appropriate usage guidelines for IOT should be defined in policy or standards.
- **Continuity** – If any IOT is considered critical to your business, an impact analysis and continuity strategy should be in place to determine work-arounds and remediation steps if that IOT is unavailable.



Deployment

Maintenanc
e

Corporate
Strategy

KEY TAKEAWAYS

- IOT is everywhere. It connects our world and reliance upon it will continue to expand in our professional and personal lives.
- Based on the connected nature, vulnerabilities present on an IOT devices impact not only the device, but everything connected to it.
- IOT devices have not historically been developed with Security in mind.
- IOT is utilized throughout organization's business functions and across industries. **This is not just an IT risk**; it impacts key stakeholders across the organizations business functions.

QUESTIONS AND ANSWERS?

END OF PRESENTATION

THANK YOU FOR YOUR TIME AND ATTENTION!

IIA CHAPTER CHICAGO | 58TH ANNUAL SEMINAR