Cybersecurity in Industrial IoT Systems

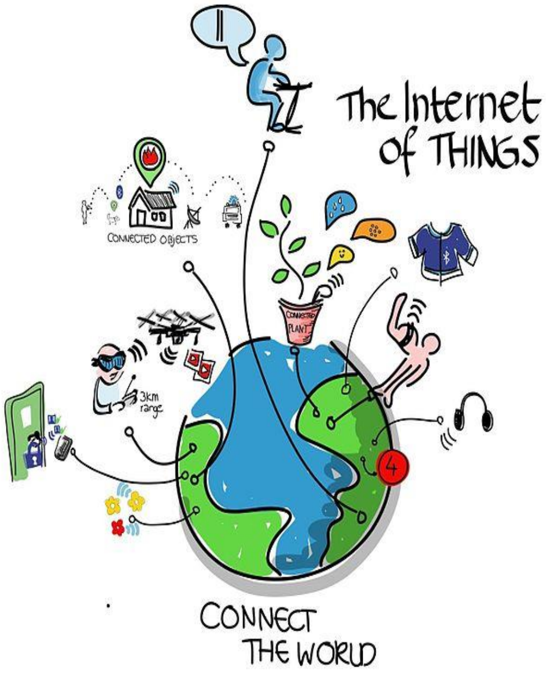
Reza Abdolee, Ph.D.
IoT and Cybersecurity Lab.

Dept. of Computer Science
California State University Channel Islands
Email: reza.abdolee@csuci.edu

IoT Definition

IEEE-IOT:

- An IoT is a network that connect uniquely identifiable "things" to the Internet.
- The things have sensing/actuating and can be potentially programed.
- Through exploitation of the unique identification, and sensing, information can be collected, and the state of the "thing" can be changed from anywhere, anytime.



Source: http://en.wikipedia.org/wiki/Internet_of_Things

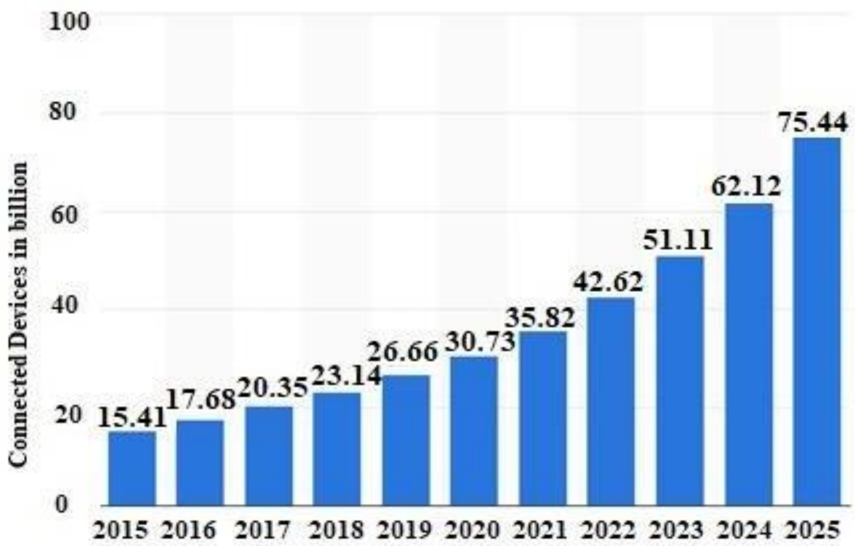
IoT can be defined as the latest evolution of the Internet!

Evolution of IoT

Pre-Internet	Internet of CONTENT	Internet of SERVICES	Internet of PEOPLE	Internet of THINGS
"HUMAN TO HUMAN"	**"WWW"**	**"WEB 2.0"**	**"SOCIAL MEDIA"**	**"MACHINE TO MACHINE"**
• Fixed & mobile telephony • SMS	• E-mail • Information • Entertainment	• E-productivity • E-commerce • …	• Skype • Facebook • YouTube • Twitter • ….	• Identification, tracking, monitoring, metering …. • Semantically structured and shared data …
+ Smart networks	**+ Smart IT platforms & services**	**+ Smart Phones & applications**	**+ Smart Devices, objects & tags**	**+ Smart Data & ambient context**

Importance of IoT

- According to Lucero's analysis from IHS, there will be nearly 75 billion devices connected to the Internet of Things network by 2025.
- According to Ericson, there will be 3.5 Billion Cellular IoT by 2022 (long range IoT devices).
- As per CISCO Research, every second 127 IoT devices are connected to the Internet.
- And as per the MarketsandMarkets Analysis, forecasts that the global IoT market will grow up to 457 billion by 2020.

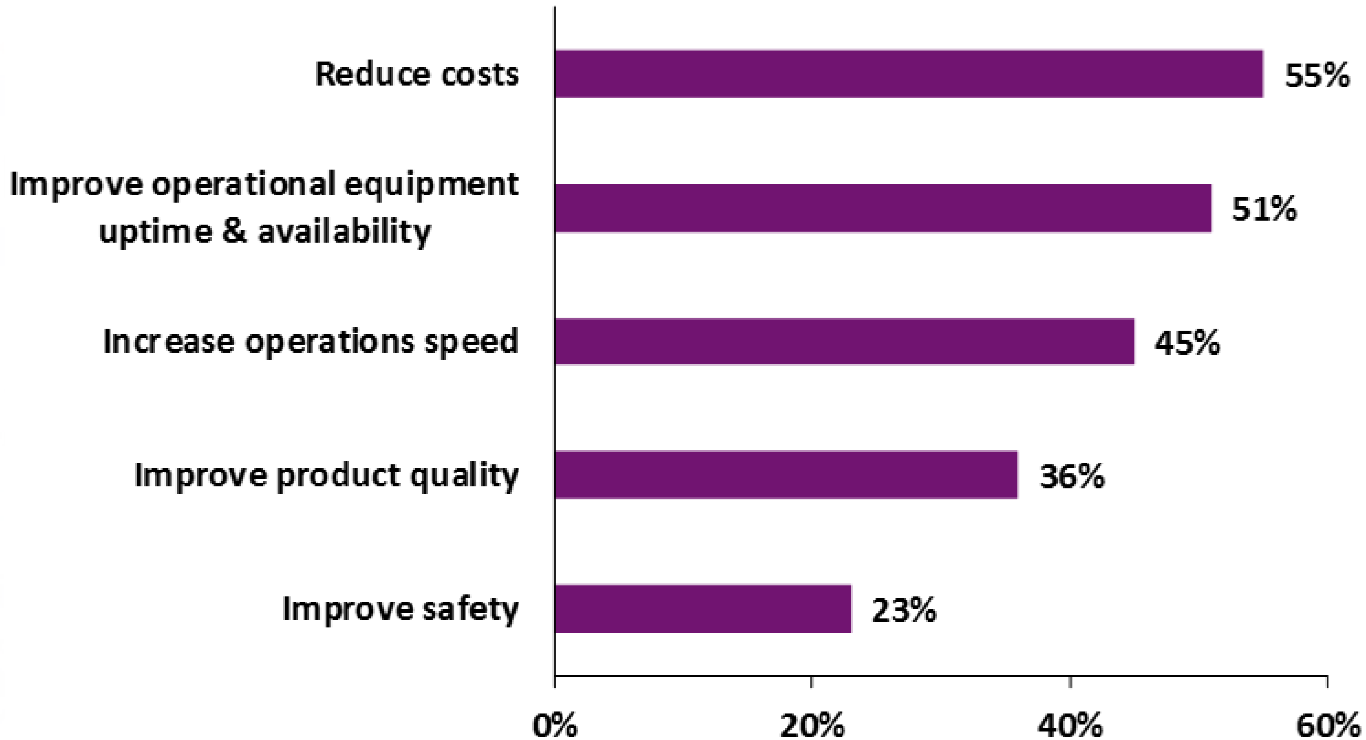


Researchgate.net by Tanweer Alalam

Industrial Internet of Things (IIoT)

- **Industry applications:**
    - Energy sector, e.g. Oil and Gas
    - Manufacturing industry
    - Agriculture (Digital farming)
    - Transportation
    - Smart cities
    - Healthcare

Benefits of IIoT



SOURCE: Aberdeen Group, March 2017

Where We Are on IIoT Technology?

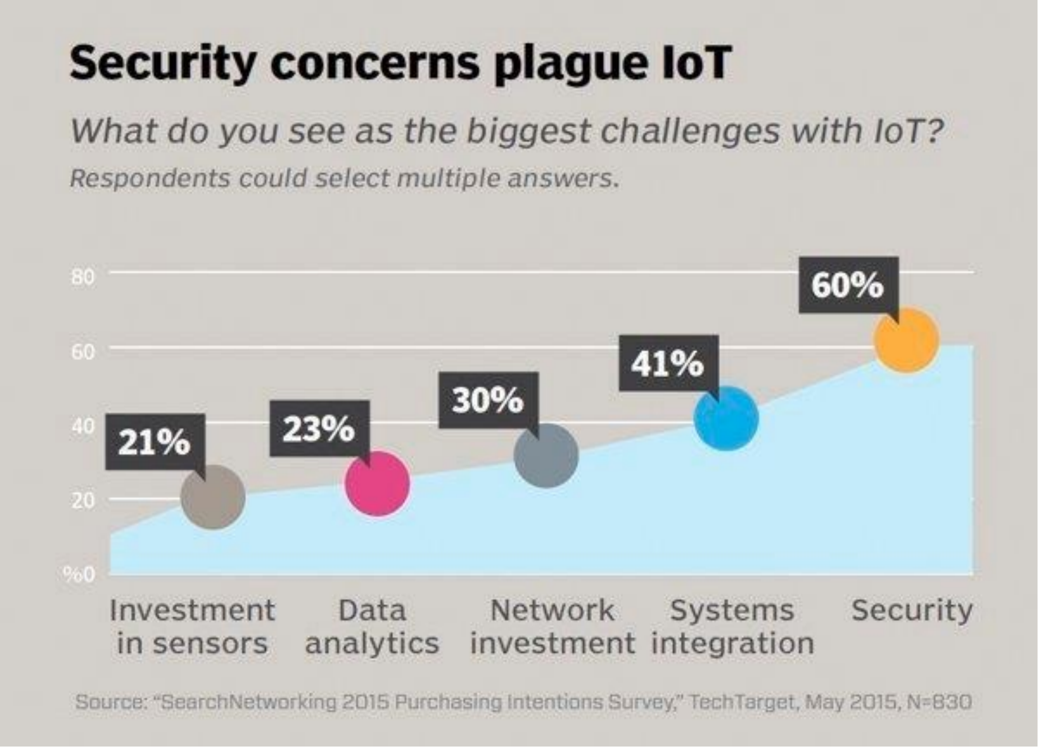
Delivery drones

Smart cities

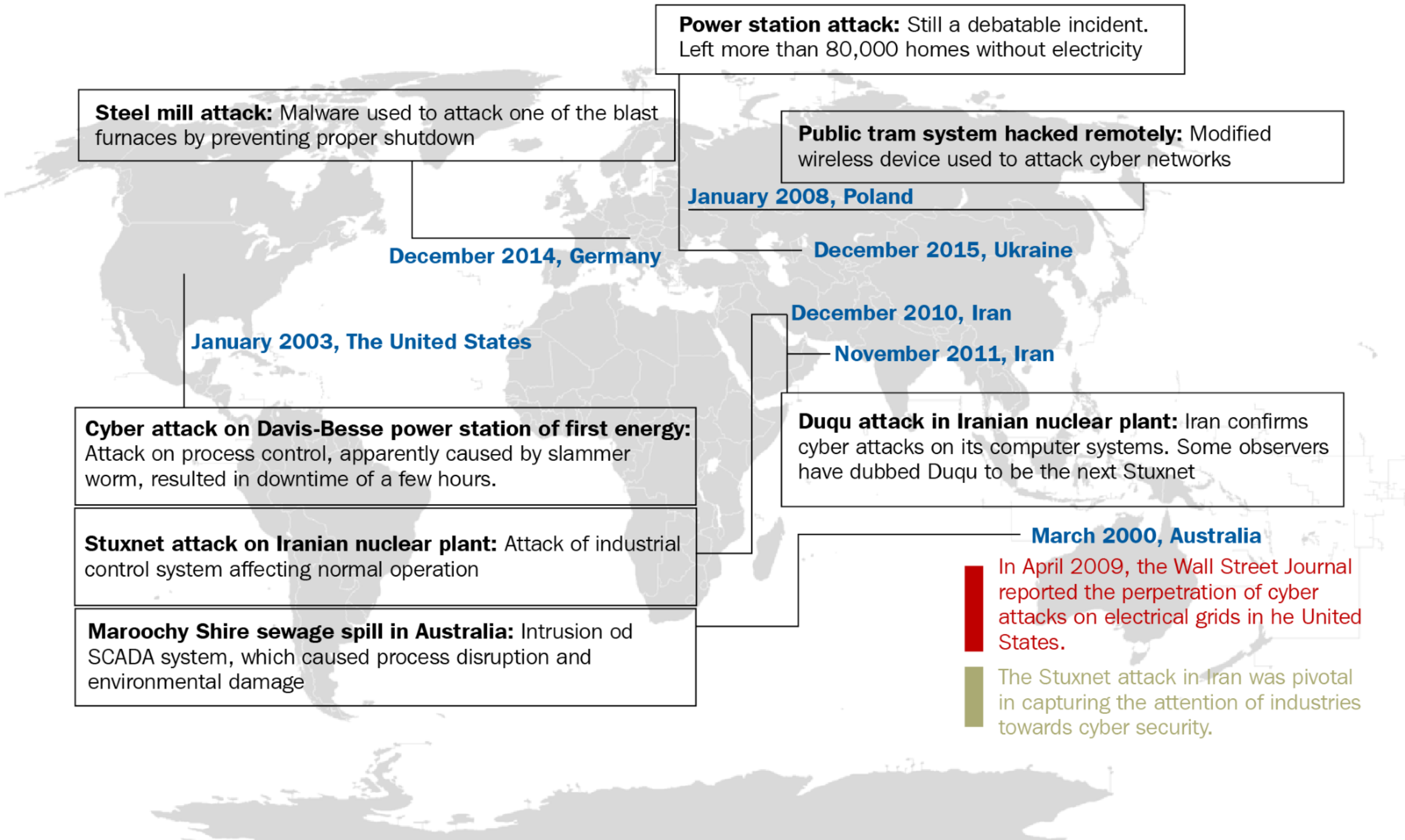
Flying taxis

Major IIoT Challenges

a) Cybersecurity
b) System implementation and interoperability due to lack of uniform policies and standards.
c) Legacy systems and brownfield implementations

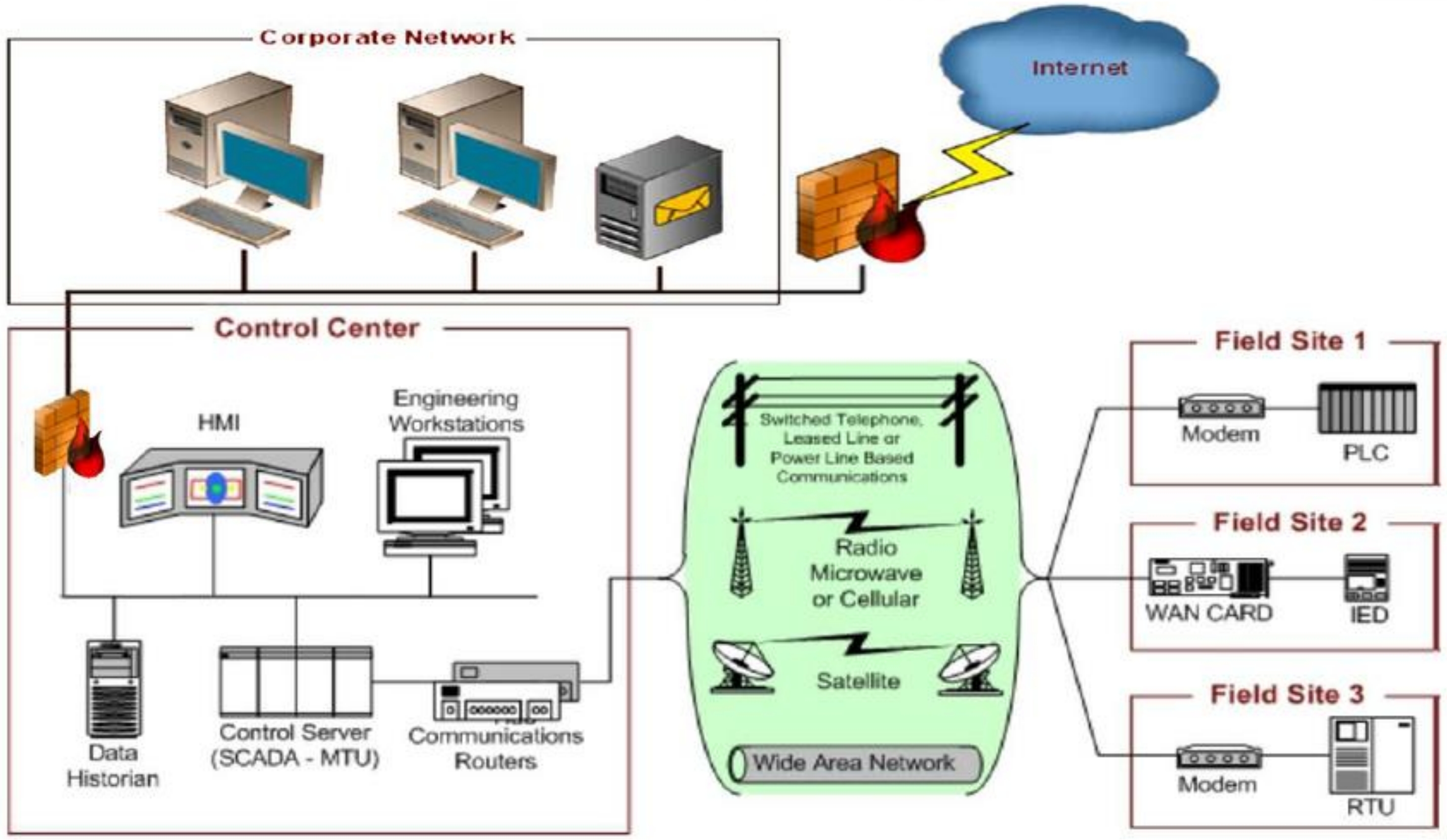


History of Cyber-Attacks in the IIoT



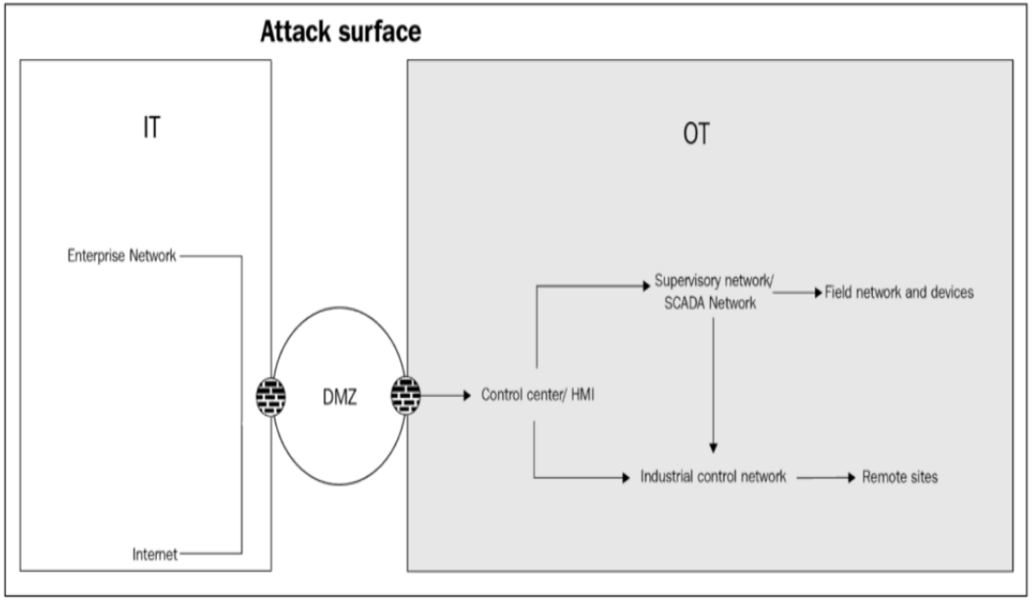
Reference: Practical Industrial Internet of Things Security

ICS/SCADA network components



Source: National Institute of Standards and Technology(NIST)-800-82r2

Attack Surface in IIoT



Reference: Practical Industrial Internet of Things Security

Attack differ in IT and OT considerably

IT: Software environment (input field, network, interfaces and protocols)

OT: attack surface is vast and scary. The diverse deployment foster several avenues for intentional and unintentional cyber incidence.

Vulnerabilities in IIoT

1) **Policy and procedure vulnerability**
2) **Platform vulnerability**
3) **Software platform vulnerability**
4) **Network vulnerability**
5) **End-device vulnerability**

Top 10 OWASP IoT Cybersecurity concerns 2018

1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

OWASP
Open Web Application Security Project

Industrial IoT Cybersecurity

- Traditional industrial setting:

  -obscurity ensures security

  -air-gapping was a prevalent security strategy

- In digital era air-gapping is a questionable security strategy
- In modern industrial setting, connectivity is the key to stay competitive

Solution: 4-tier cybersecurity architectures

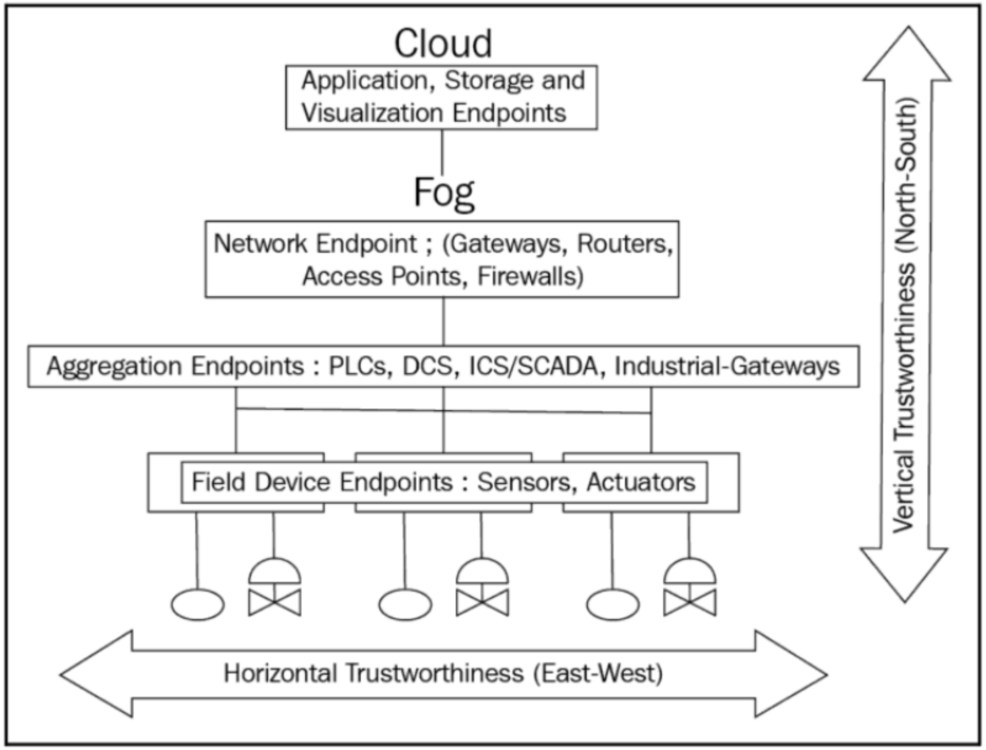
Four-Tier IIoT Cybersecurity Architecture

Data Governance Policy	Security Standards	System Security Guideline	Security Policies	Security Threat Analysis		Tier 4: Process and governance
Data Center Security	Secure Application Platforms	Secure Analytics Platforms	Saas/Iaas/Paas Cyber Security			Tier 3: Cloud platform and applications
Gateway Protection	Secure Edge Intelligence	Media Protocol Security	Cryptographic Protection	Configuration, Monitoring. Management	IDS and IPS Engines	Tier 2: Communication and connectivity
Endpoint Identify	Secure Configuration and Management	Root of Trust Sandboxing	Access Control Secure Boot	Physical Security		Tier 1: Endpoints and embedded software

Reference: Practical Industrial Internet of Things Security

End-Point Security and Trustworthiness

-The trustworthiness of an IIOT systems is rooted in end-point protection.
- Inadequate trustworthiness at any point in the value chain poses major threat to security



Reference: Practical Industrial Internet of Things Security

Enhance Trustworthiness of End-Points

a) Crypto accelerators and coprocessors (**FPGA, HSM and TPM**)

b) **Light cryptographic** algorithms that offers comparable security strength

c) Security functions can be delegated to a **security gateway**

d) **Incremental update** instead of full update

Trust in Hardware vs Software

- The trust anchor can be implemented either in software or hardware.
- The choice calls for a trade-off between the complexity and the level of assurance

	Hardware	Software
Level of Trust	High (IEC 62433 Level 3 and 4)	Low (IEC 62433 Level 1, 2, and 3)
Battery Performance	More efficient	Less efficient
Management complexity	High	Low
Crypto Algorithm Reprogramming Complexity	High	Low
Security Updates	More complex when supported	Less complex
Computational Cost	Less burden on CPU	CPU- and memory-intensive
Storing of Secrets	More secure	Less secure

Hardware Security Components

- Field programmable Gate Array (FPGA)
  - Support firmware updates
  - Can include CPU co-processor
  - Crytoaccelarator occupy a small space on chip
- Hardware Security Modules (HSM)
  - Designed to provide physical isolation for security function
  - Plug into computer or server
- Trusted Platform Modules (TPM)
  - Built into motherboard
  - Strong tamper resistance key generation and storage using hardware random num. gen.

Brownfield Scenarios Consideration

Every industrial systems has legacy devices in it such as:

Pump, motors, and turbins

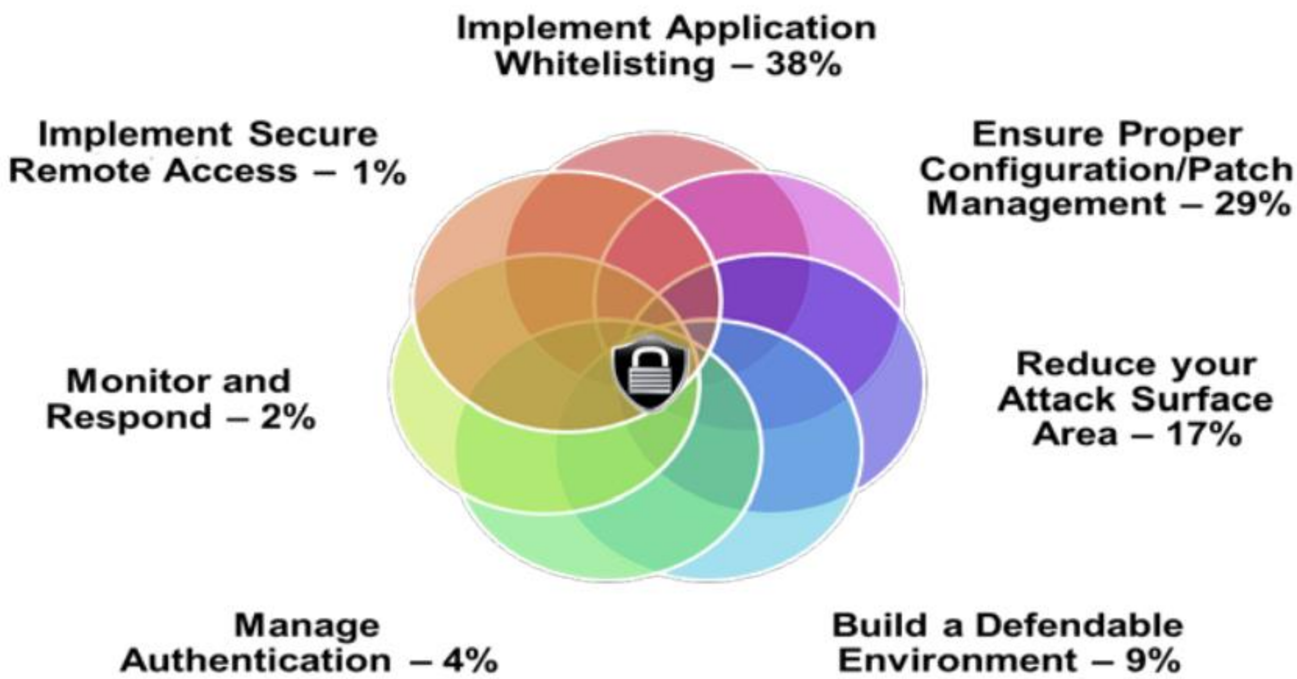
How to reduces vulnerabilities in such cases?

1) International society of automation (ISA) defines securing assurance level using **zone and Conduits**: This technique introduces isolation

2) **Security gateways** to protect legacy devices

a) mutual authentications
b) Identity management and storage
c) Network whitelisting to allow only defined flow between two devices
d) Gateway resolve interoperability problems due to vendor-specific inconsistency
e) Gateways makes security agnostics to vender-specific platforms

Cybersecurity Recommendation for IIOT



Source: US homeland security - NCCIC

Cybersecurity Research

Research in “IoT and Cybersecurity Lab.” at CSUCI:

- **Lightweight reconfigurable cryptographic algorithms for resource-constrained IoT end-devices**
  - parameters of a given cryptographic algorithms changes
  - the cryptographic algorithms itself changes in run time
- **5G Enabled-IoT architecture using Blockchain concepts and Technology**
  - Blockchain provides a tamper-resistance security ecosystem
  - However, IoT are resource-constrained with low computation and storage value
- **Machine learning enabled end-point security**
  - Cybersecurity countermeasures are traditionally reactive
  - Vaccine comes after the virus has infected the system
  - Blacklisting happened after the incident
  - ML can be used to detect anomaly and update whitelisting and blacklisting dynamically
  - Challenge are “accuracy of prediction”, “vast quantity of training data”, and zero-day threat.

CS plan to Help Local Industry

- Research collaboration in cybersecurity area with local industry and the navy
- Launch a cybersecurity program in Computer Science department and train local workforce
- Offer cybersecurity crash courses to industry partners and government agencies

Suggestions and Questions!

Email: reza.abdolee@csuci.edu