AABC Commissioning Group

AIA Provider Number 50111116

Cybersecurity for Energy Managers

Course Number: CXENERGY1919

Jesse Wiegand
Christopher Markstein, PE, CEM
Schneider Electric

April 17, 2019

Credit(s) earned on completion of this course will be reported to AIA CES for AIA members. Certificates of Completion for both AIA members and non-AIA members are available upon request.

This course is registered with AIA CES for continuing professional education. As such, it does not include content that may be deemed or construed to be an approval or endorsement by the AIA of any material of construction or any method or manner of handling, using, distributing, or dealing in any material or product.

Questions related to specific materials, methods, and services will be addressed at the conclusion of this presentation.

Copyright Materials

Course Description

Cybersecurity is an important aspect of project implementation and support today, and will become increasingly critical as information and operations technology convergence continues.

In the current threat landscape, vulnerabilities can quickly lead to the loss of availability of critical infrastructure, exposure of confidential data or an interruption of business function. This discussion will seek to inform on both the current state and developments in the field of cybersecurity within facilities operations, building management, systems integration, and remote connectivity and support.

Topics covered include common deficiencies leading to avenues of compromise as well as approaches to achieving and maintaining end-to-end cybersecurity within your projects.

Learning Objectives

At the end of the this course, participants will be able to:

1. Describe fundamental aspects of cybersecurity pertinent to project stakeholders including facility energy managers, building automation & systems engineers, and commissioning agents.

2. Identify potential risks inherent to networked systems such as building automation and energy management systems and the possible liabilities held by the stakeholders above.

3. Discuss cybersecurity lifecycle processes to mitigate and manage risk during project design, implementation, and long-term support phases.

4. Investigate the applicability of prominent regulatory and industry standards including the NIST Risk Management Framework (RMF) and NERC Critical Infrastructure Protection (CIP) standards.

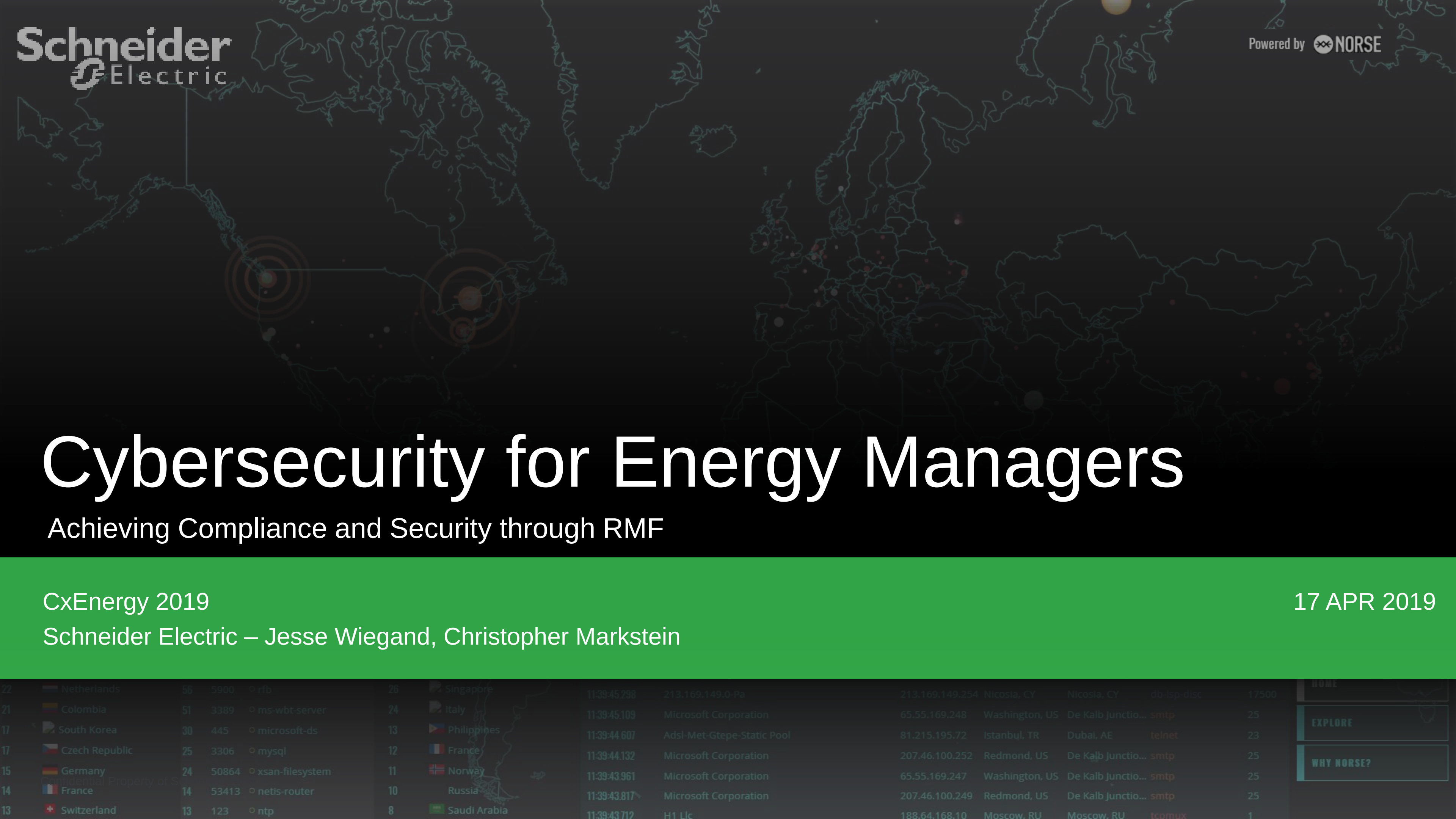
Cybersecurity for Energy Managers

Achieving Compliance and Security through RMF

CxEnergy 2019

17 APR 2019

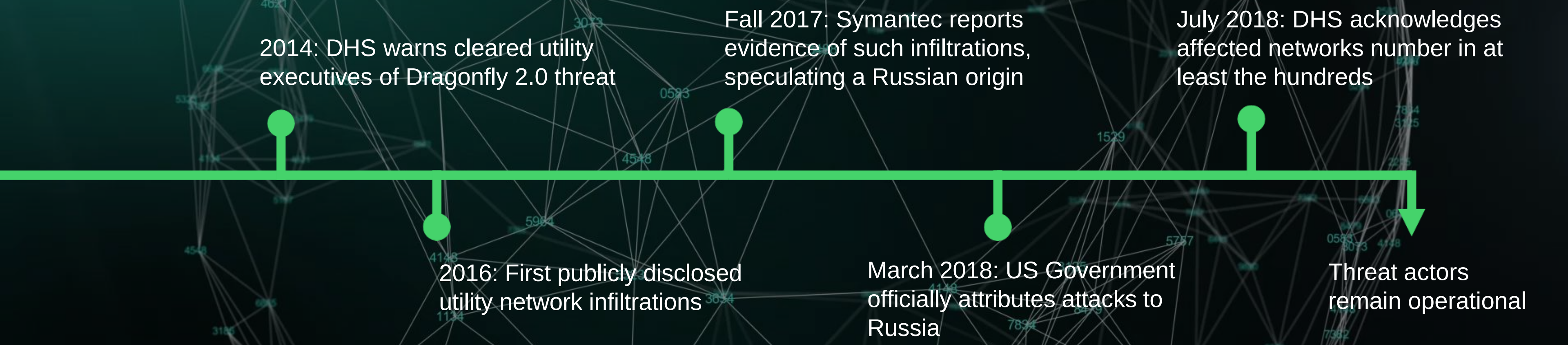
Schneider Electric – Jesse Wiegand, Christopher Markstein



22	Netherlands	56	5900	rfb	26	Singapore
21	Colombia	51	3389	ms-wbt-server	24	Italy
17	South Korea	30	445	microsoft-ds	13	Philippines
17	Czech Republic	25	3306	mysql	12	France
15	Germany	24	50864	xsan-filesystem	11	Norway
14	France	14	53413	netis-router	10	Russia
13	Switzerland	13	123	ntp	8	Saudi Arabia

11:39:45.298	213.169.149.0-Pa	213.169.149.254	Nicosia, CY	Nicosia, CY	db-lsp-disc	17500
11:39:45.109	Microsoft Corporation	65.55.169.248	Washington, US	De Kalb Junctio...	smtp	25
11:39:44.607	Adsl-Met-Gtepe-Static Pool	81.215.195.72	Istanbul, TR	Dubai, AE	telnet	23
11:39:44.132	Microsoft Corporation	207.46.100.252	Redmond, US	De Kalb Junctio...	smtp	25
11:39:43.961	Microsoft Corporation	65.55.169.247	Washington, US	De Kalb Junctio...	smtp	25
11:39:43.817	Microsoft Corporation	207.46.100.249	Redmond, US	De Kalb Junctio...	smtp	25
11:39:43.712	H1 Llc	188.64.168.10	Moscow, RU	Moscow, RU	tcpmux	1

State-sponsored Hacking of Critical Infrastructure



2014: DHS warns cleared utility executives of Dragonfly 2.0 threat

2016: First publicly disclosed utility network infiltrations

Fall 2017: Symantec reports evidence of such infiltrations, speculating a Russian origin

March 2018: US Government officially attributes attacks to Russia

July 2018: DHS acknowledges affected networks number in at least the hundreds

Threat actors remain operational

Insider Threats:

28%

of all attacks perpetrated by insiders

46%

responded that the damage
from insider attacks was more severe
than outsider attacks

75%

of insider incidents handled internally,
without law enforcement or legal action
(and often without media coverage)

Source: Carnegie Mellon SEI CERT 2014 US State of Cybercrime Survey

Non-compliant systems are subject to disconnection

A sample case:

“I wish this email was coming to you on better terms, but I am in full out panic mode. I just got told an hour ago, that I basically have one month before our [EMCS] will be removed from the network and [our] devices will be blacklisted… [this] kills my whole program.”

Email communication received August, 2017

Cybersecurity applies to your entire operation

Protect your business

Protect your image and reputation

Ensure business continuity

Avoid regulatory penalties

Protect critical digital assets

Improve robustness to cyberattacks

Optimize inventories and assets

What’s driving digitization in industry?

CONNECTIVITY

- Smart connected devices (products)
- Standards-driven connectivity
- Lower cost of measurement

MOBILITY

- Pervasive and affordable communication
- Remote access
- User-driven interfaces

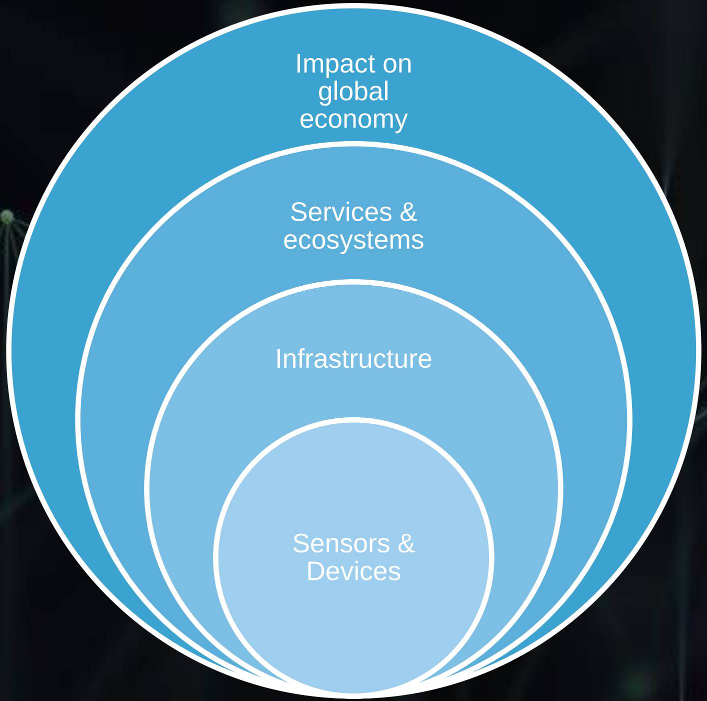
CLOUD

- Massive aggregation of data
- Data access by specialists
- Industrial application developer ecosystem

ANALYTICS

- Cognitive applications
- Artificial intelligence optimizing performance at all levels

Size and market impact of IIoT



IIoT market by 2020

$110bn

Morgan Stanley (2015):
$90 billion to $110 billion by 2020

IIoT market by 2021

$123bn

Industry ARC(2016):
$123.89 billion by 2021

Impact on global economy by 2030

$14.2tn

Accenture estimates the IIoT could add $14.2 trillion to the global economy by 2030.

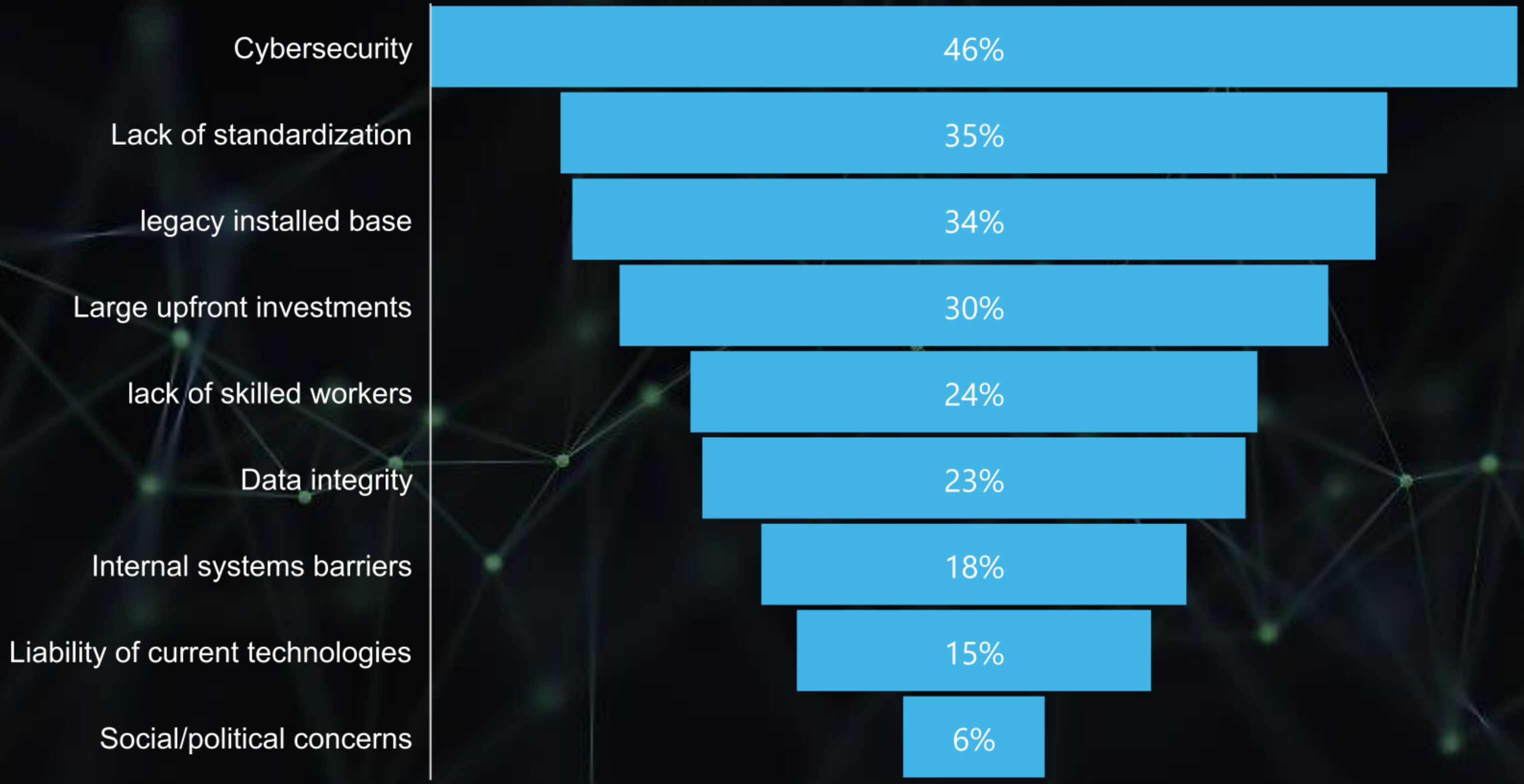
CAGR until 2020

7.3%

Global IIoT market report:
global IIoT market to grow at a CAGR of 7.3% until 2020

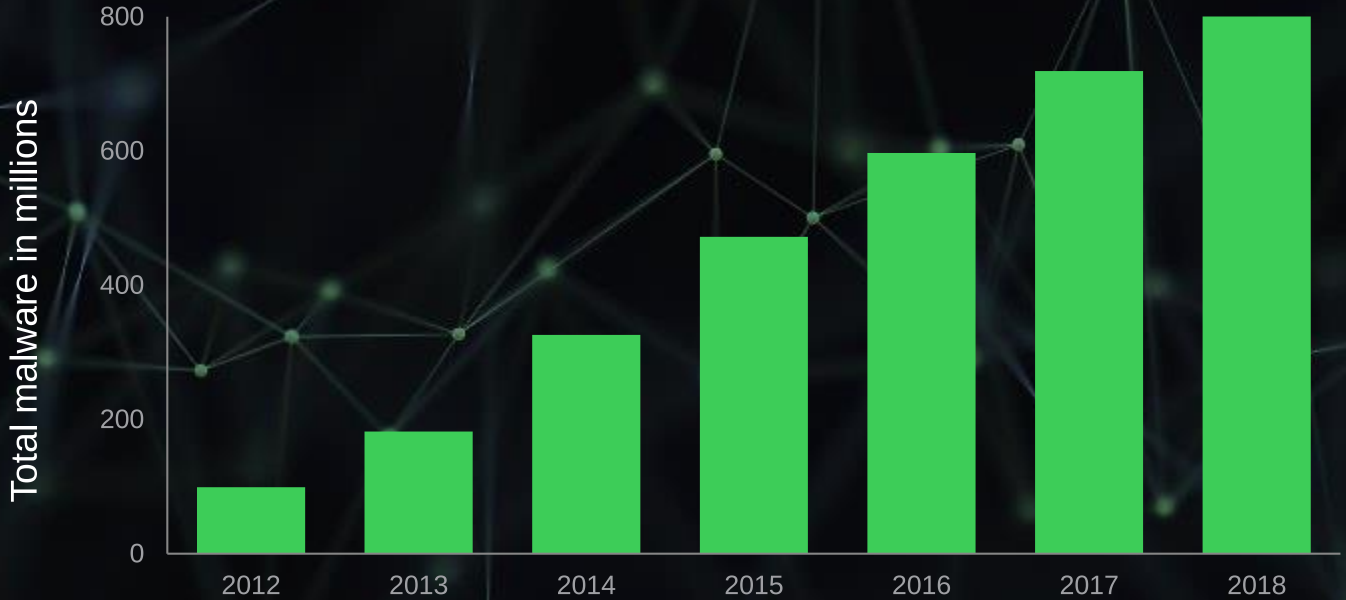
Size and market impact of the Industrial Internet of Things – source: Morgan Stanley, IndustryARC, Accenture and Research and Markets.

Challenges to IIoT Adoption



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

Cybersecurity threat landscape



AV-Test.org August 2018

The Risk Management Framework (RMF)

Common Security Framework for Federal Information Systems as defined by NIST SP 800-37

RMF Goal

Reduce & mitigate vulnerabilities until the risk is acceptable to the System Owner (SO) and the Authorizing Official (AO)

- ***FISMA Compliance***
- *RMF reduces cybersecurity risk while considering resource constraints and mission requirements*
- *Risk reduction must also account for risks to system functionality due to the application of security controls*

Security Controls

Specific actions taken to secure a system

- *Detailed in NIST Special Publication 800-82*
- *Main focus of RMF steps 2-4: includes IT controls but also personnel and management policies and procedures plus physical security*
- *Usage of the word 'control' not to be confused with control systems engineering*

Inheritance

An inherited security control is addressed by others in such a way that it applies to your system

Three primary methods for inheritance:

- *By existing within a physical security boundary*
- *By being covered by policies and procedures already in place*
- *By connection to another system which addresses the security controls*

Six-step system life cycle process:

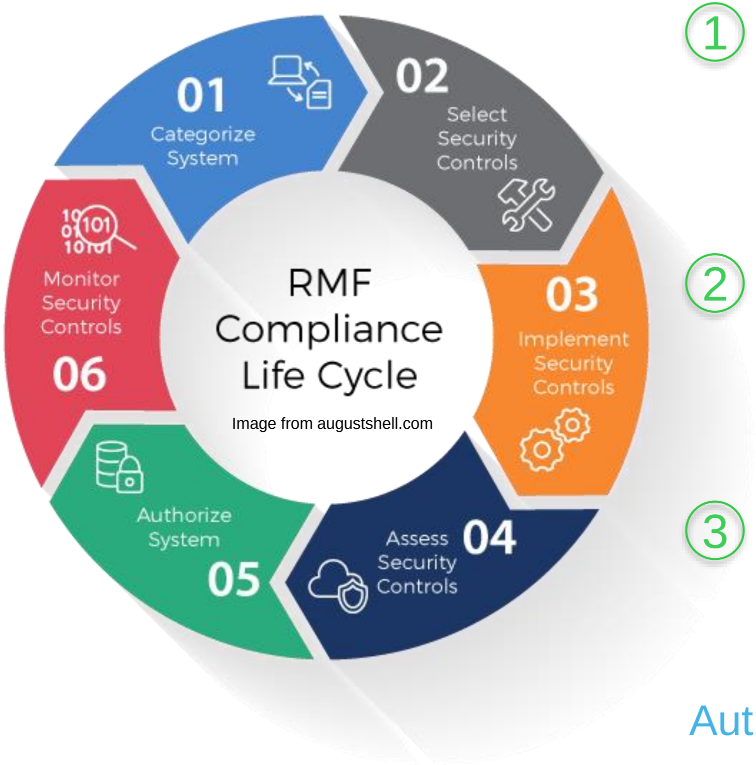


Image from augustshell.com

1 **Categorization**
of information systems

Determine C-I-A Impact levels (LOW-MODERATE-HIGH)

2 **Selection**
of security controls

Pulled from NIST SP 800-82 based on categorization

3 **Implementation**
of security controls

4 **Assessment**
of security controls

3rd party Security Controls Assessor & Validator (SCA-V)

5 **Authorization**
of information systems

6 **Monitoring**
of security controls (ongoing)

Must have a plan for system administration including scanning and patching

Authorization to Operate (ATO) must be periodically renewed

Foundational Concepts

Vulnerability

a weakness that could lead to a security breach either through accidental trigger or intentional exploitation.

Exploit

a specific means of using a vulnerability to gain control of or damage a system.

Threat

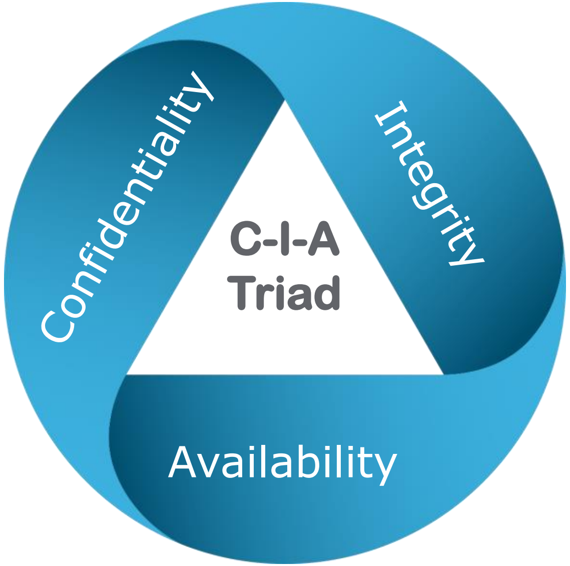
the potential for a threat agent or threat actor to "exercise" a vulnerability. The path or tool used by the threat actor can be referred to as the threat vector.

Risk

the likelihood and impact (or consequence) of a threat actor exercising a vulnerability.

Source: gtslearning.com

Foundational Concepts: Categorization

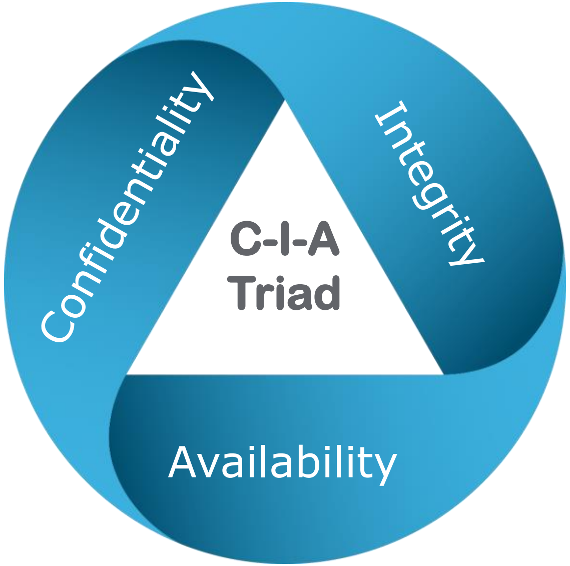


Confidentiality

A loss of confidentiality is the unauthorized disclosure of information

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542]

Foundational Concepts: Categorization

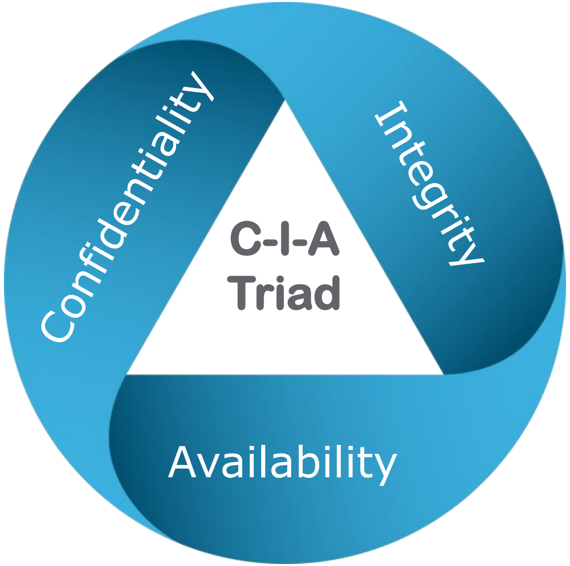


Integrity

A loss of integrity is the unauthorized modification or destruction of information

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

Foundational Concepts: Categorization



Availability

A loss of availability is the disruption of access to or use of information or an information system.

“Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542]

Design & operate systems
for security & compliance

End-to-end Cybersecurity

Applying Security Controls

Isolate

Stand-alone (air-gapped) network

- Does not eliminate RMF compliance required by DoD Instruction 8510.01, but generally subject to fewer applicable security controls
- Requires a plan and funding for on-going system administration and maintenance including scanning, patching, & remediation
- Can be more costly as new physical network infrastructure must be created
  - *Point-to-point wireless could be an option in lieu of cross-installation fiber*

Platform Enclaves

- Uses the existing NIPRNet wide area network infrastructure (switches, routers, fiber, etc.)
- Network segmentation through Virtual LANs (VLANs), subnetting, and/or VPNs: same physical network but logically separate
- More applicable security controls but many of these can be inherited from existing ATO
- Interconnections to non-VLAN resources possible if part of authorization

Applying Security Controls

Harden your Devices and Services

1. **Change all default credentials and assign individual accounts with only the needed permissions**
   Wherever possible, enforce password complexity rules through Active Directory integration or other means

2. **Disable all unneeded IP ports and services at both the host and network level**

3. **Physically secure all equipment and device ports**

4. **Encrypt data and use secure protocols (TLS)**

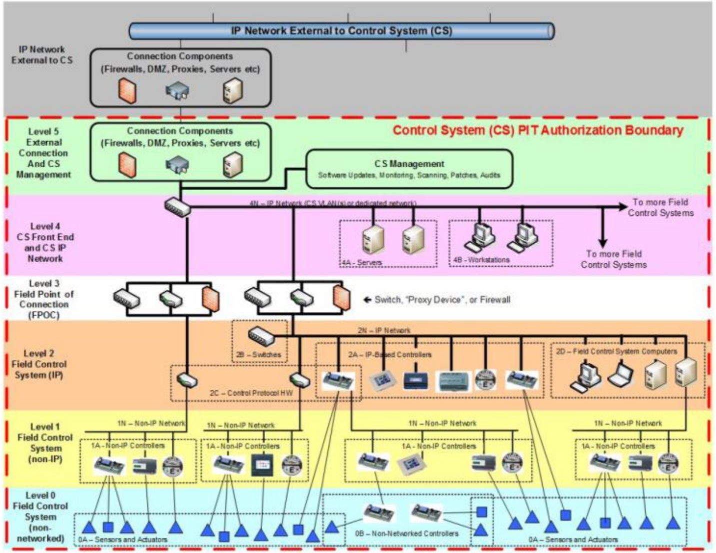
5. **Employ host-based and network based anti-malware and content filtering applications**
   Use GFE or VM servers/workstations or disk images (i.e. Army Golden Master) whenever possible

6. **Consider the risk before deploying a wireless solution and if approved, use only WPA2 encryption**

Unpacking RMF

5-Level Control System Architecture:

As Presented in UFC 04-010-06


IP Network External to Control System (CS)
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control System (CS) PIT Authorization Boundary
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
4N – IP Network (CS VLAN(s) or dedicated network)
To more Field Control Systems
Level 4 CS Front End and CS IP Network
4A - Servers
4B - Workstations
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
← Switch, "Proxy Device", or Firewall
Level 2 Field Control System (IP)
2N – IP Network
2B – Switches
2A – IP-Based Controllers
2D – Field Control System Computers
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
Level 0 Field Control System (non-networked)
0A – Sensors and Actuators
0B – Non-Networked Controllers
0A – Sensors and Actuators

Applying to ICS & Networked Systems in Energy Projects

As presented in UFC 4-010-06, the 5-level architecture represents a broad range of possible ICS solutions

- *Not every system will have every level or type of component within a level*
- *Some devices may reside in multiple sublevels (for example, controller/routers)*

The architecture consists of both “Standard IT” elements and “Non-Standard IT” elements

- *Security controls for standard IT elements are addressed using standard cybersecurity practices and are often inherited through a Platform Enclave or similar means*
- *Non-standard elements are in large part what makes control system cybersecurity challenging as they do no resemble typical IT systems – these must be addressed by the designer*

The UFC covers systems with C-I-A impacts of LOW or MODERATE severity. HIGH impact systems generally require more expertise and attention to detail than a UFC can provide

Unpacking RMF

5-Level Control System Architecture:

As Presented in UFC 04-010-06

Authorization Boundary
Includes entire PIT system

L0: non-networked devices
Sensors, actuators, etc.

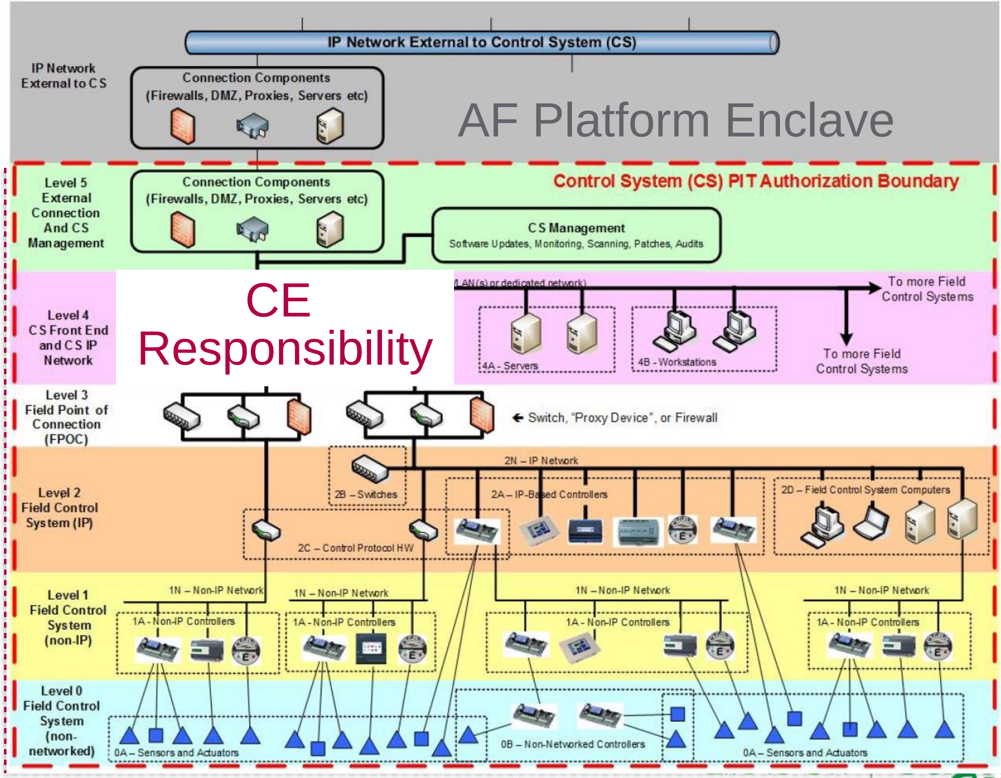
L1: non-IP networked controllers
Sensors, actuators, etc.

L2: Controllers on IP network

L3: Field Point of Connection (FPOC)

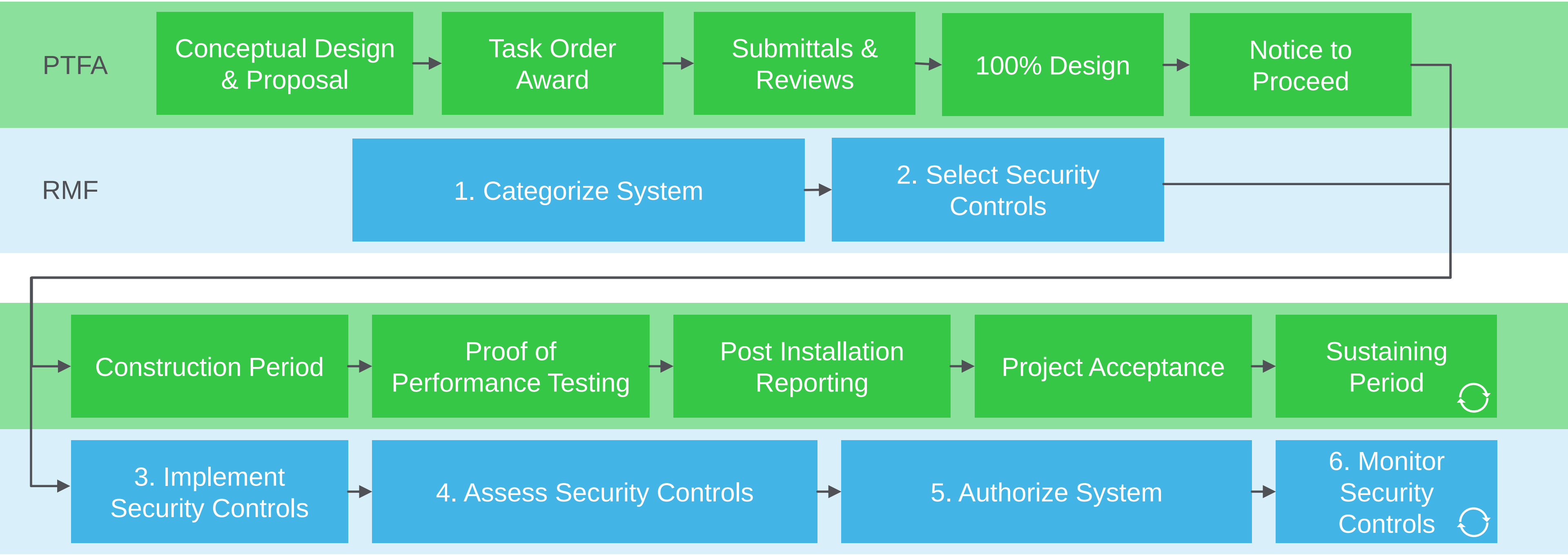
L4: Site-wide CS IP network

L5: Interfaces to external networks


IP Network External to Control System (CS)
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
AF Platform Enclave
Control System (CS) PIT Authorization Boundary
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 CS Front End and CS IP Network
CE Responsibility
LAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
← Switch, "Proxy Device", or Firewall
2N – IP Network
2B – Switches
2A – IP-Based Controllers
2D – Field Control System Computers
Level 2 Field Control System (IP)
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1N – Non-IP Network
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
E
Level 0 Field Control System (non-networked)
0A – Sensors and Actuators
0B – Non-Networked Controllers
0A – Sensors and Actuators

Path to Final Acceptance (PTFA)

Incorporating the Risk Management Framework (RMF) into your Project Roadmap



PTFA

Conceptual Design & Proposal → Task Order Award → Submittals & Reviews → 100% Design → Notice to Proceed

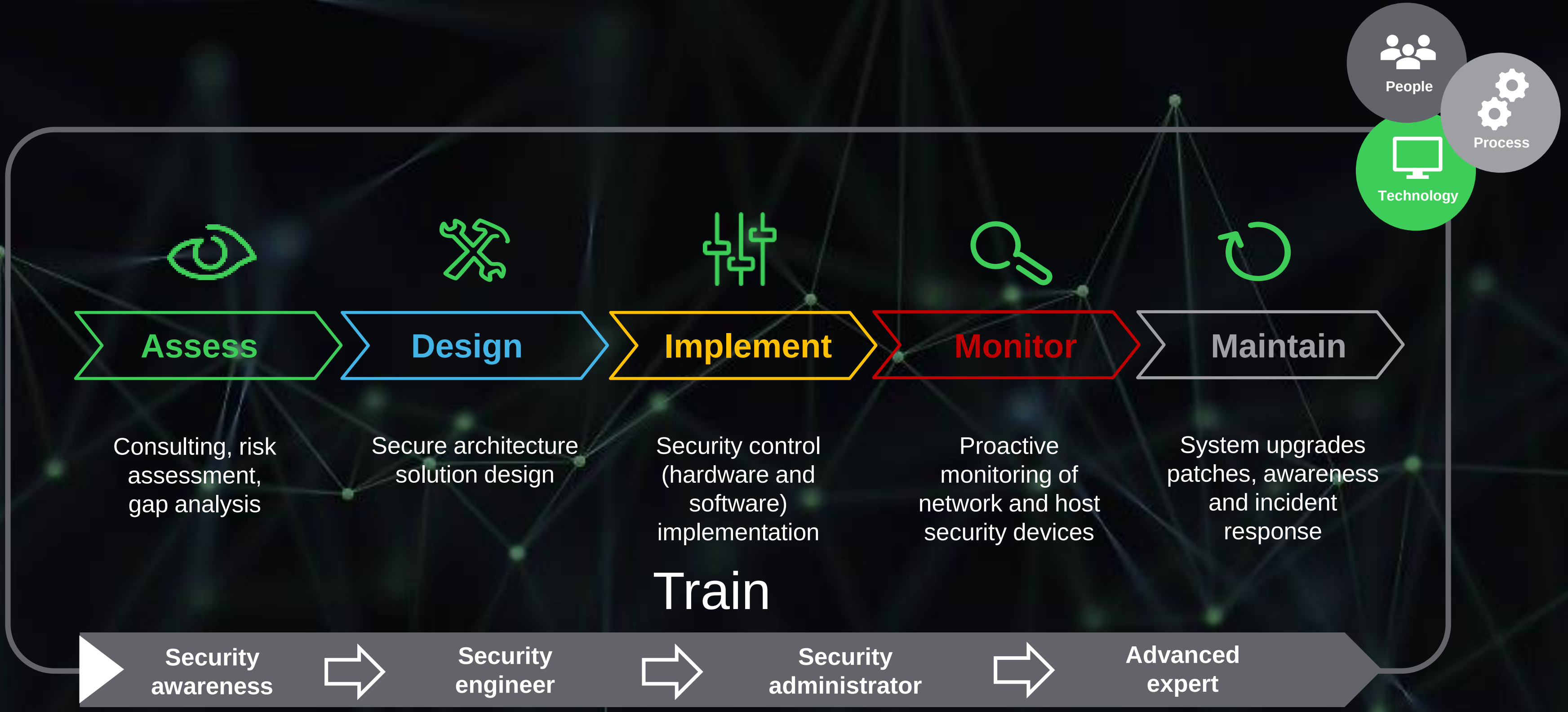
RMF

1. Categorize System → 2. Select Security Controls

Construction Period → Proof of Performance Testing → Post Installation Reporting → Project Acceptance → Sustaining Period

3. Implement Security Controls → 4. Assess Security Controls → 5. Authorize System → 6. Monitor Security Controls

Cybersecurity solutions for the operational life cycle:



Assess

Consulting, risk assessment, gap analysis

Design

Secure architecture solution design

Implement

Security control (hardware and software) implementation

Monitor

Proactive monitoring of network and host security devices

Maintain

System upgrades patches, awareness and incident response

Train

Security awareness → **Security engineer** → **Security administrator** → **Advanced expert**

Cybersecurity Solutions Portfolio

Permit	Manage access to Operations systems and information through network and physical controls
Protect	Specific controls as part of the operations systems for ongoing protection.
Detect	Active processes that monitor the operating environment to detect and communicate threats
Respond	Capabilities and systems to support rapid response to cyber incidents to contain and mitigate attacks

Cybersecurity Solutions Portfolio

Permit

- Authentication, Authorization, Accounting
- Multi-Factor Authentication
- Network Segmentation
- Secure Remote Access
- Physical Security

Protect

- Endpoint protection anti-virus, anti-malware,
- DLP, HIPS, whitelisting
- Central Device Control
- CPU/PID Protection
- Patch Management

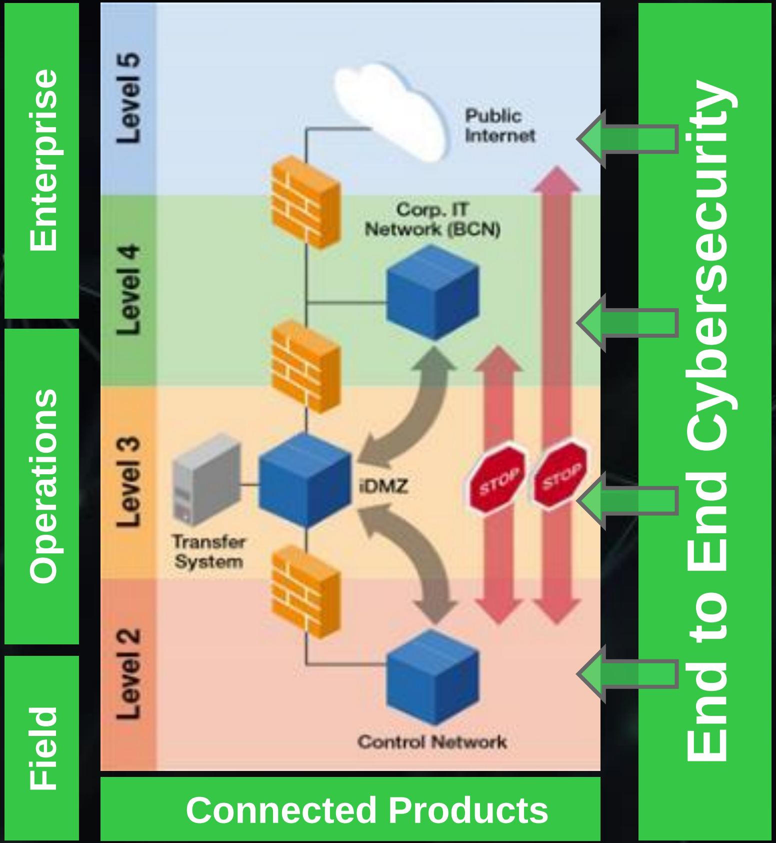
Detect

- Security Information & Event Management (SIEM)
- Network performance monitoring
- Anomaly Detection
- Intrusion Detection (IPDS)
- SOC / NOC

Respond

- Backup / Disaster Recovery
- Forensics
- Incident Response

Cybersecurity from the ground up



Enterprise

Operations

Field

Connected Products

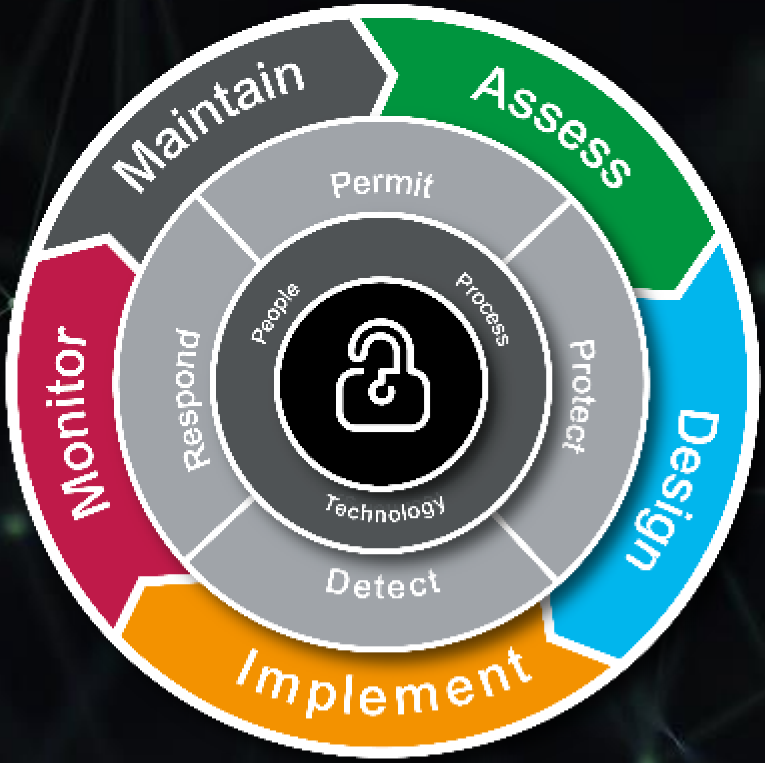
End to End Cybersecurity

Cybersecurity is an essential consideration throughout your operation

Cybersecurity lifecycle enables the digital world

The value of a comprehensive cybersecurity culture

- Mitigating the risk of data exposure and downtime
- Commitment of your employees
- Maintaining a high degree of market trust and confidence
- Being an **enabler** of IIoT applications
- Proactive design of solutions that will grow with business needs
- Ongoing value from a lifecycle perspective



Government Resources

- DoD CIO RMF Portal (CAC ID required): https://rmfks.osd.mil/login.htm
- serdp-estcp.org: process guidance plus links to NIST publications and other pertinent documentation
  - *Navigate to Tools & Training > Installation Energy & Water > Cybersecurity (Start with UFC 4-010-06*)
- Service POCs: all support requests must be initiated by the Contracting Officer’s Representative (COR)
  - *Army: ICS Cybersecurity Center of Expertise, Huntsville Engineering and Support Center*
  - *Navy & Marines: Naval Facilities Engineering Command, Command Information Office (CIO)*
  - *Air Force: Civil Engineer Maintenance, Inspection, and Repair Team (CEMIRT) ICS Branch, Tyndall AFB*

Private Sector Resources:

Vendors, Consultants, Academia, and Non-Profits

- Must know which specific standards and regulations apply to your systems and end-users
- Project specifications are increasingly including cybersecurity requirements – ensure familiarity and understanding before bidding
- The North American Electric Reliability Corporation Critical Infrastructure Protection standards (NERC-CIP) are a great starting point and are broadly incorporated intro projects across the utility and private sectors
- Your hardware/software manufacturers can be a great reference for additional information and implementation assistance

Life Is On

Schneider Electric

This concludes The American Institute of Architects Continuing Education Systems Course

Jesse Wiegand

Cybersecurity Program Director

Schneider Electric

jesse.wiegand@se.com

Christopher J. Markstein, PE, CEM, CEA

Global Solution Architect

Schneider Electric

christopher.markstein@se.com