CampusEnergy2021

BRIDGE TO THE FUTURE

Feb. 16-18 | CONNECTING VIRTUALLY

WORKSHOPS | Thermal Distribution: March 2 | Microgrid: March 16

Cyber Security of Institutional Energy Systems

Tom McDonnell

Rockwell Automation, Power and Energy Industry Leader

Prepared by:

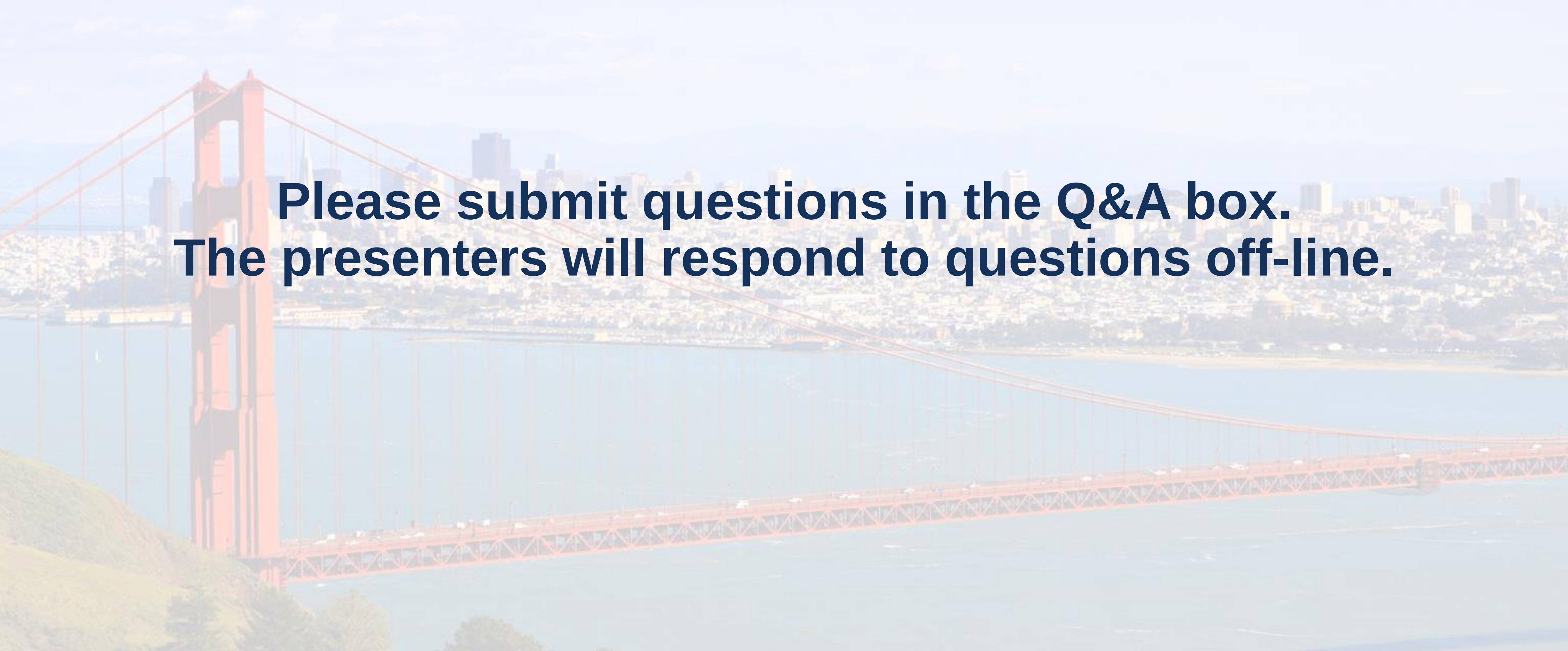
by Tom McDonnell and Tony Baker
Chief Product Safety & Security Officer

CampusEnergy2021
BRIDGE TO THE FUTURE
Feb. 16-18 I CONNECTING VIRTUALLY
WORKSHOPS I Thermal Distribution: March 2 I Microgrid: March 16

Rockwell Automation

INTERNATIONAL DISTRICT ENERGY ASSOCIATION

Q&A Will Not Be Answered Live



Please submit questions in the Q&A box.
The presenters will respond to questions off-line.

Challenges Facing Institutional Infrastructure

Why are colleges and universities easy targets for cyber attacks?

By their very nature, schools operate under an open-access IT environment. Thus, they are challenged with maintaining that environment for students, faculty and staff, thus making them frequent targets for cyber attack. As higher education changes how it operates, using more technology for education, student services, **facilities**, **research** and administration, the cyber risks multiply.

Skills Gap

- Dearth of qualified personnel [1]
- Achieving productivity goals
- Lack of staffing to expand operations [2]

Vulnerability

- Security is an after thought
- Aging Industrial Control Systems and Protocols
- Lack of proper policies and procedures
- Evolving Industrial Security Standards
- Broad Access with potentially hundreds of thousands of users

Inflexibility

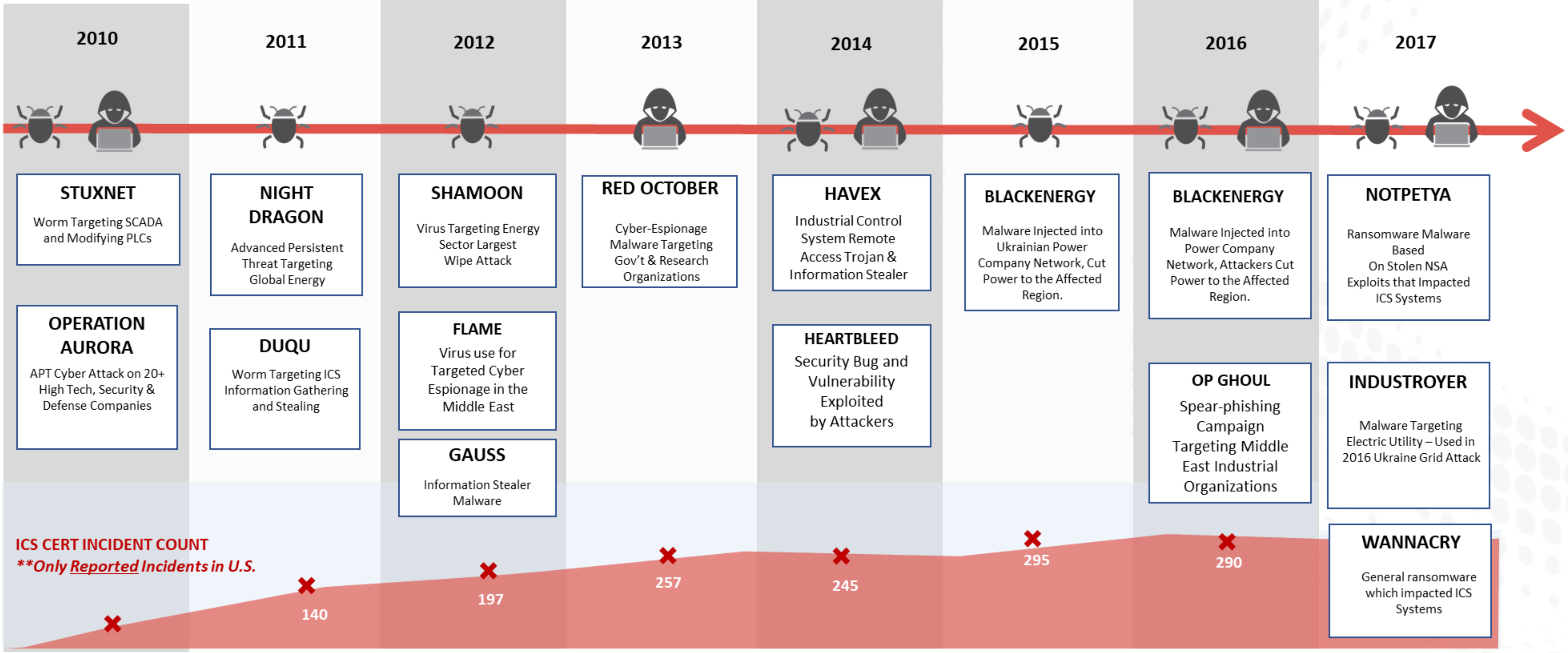
- Low Adoption of Risk Management Processes
- Shadow/Stealth IT
- Lack of tools to manage Infrastructure
- Too Much Data, Lack of Actionable Information

IT/OT Convergence

- Lack of comprehensive Asset Inventory
- Integration of new technologies
- Integrate: customer demand, supply chain and industrial processes

(1) ARC Supplier Provided Automation Services
(2) Aberdeen Group

ICS-Focused Campaigns, Attacks, Frequency



2010

STUXNET
Worm Targeting SCADA and Modifying PLCs

OPERATION AURORA
APT Cyber Attack on 20+ High Tech, Security & Defense Companies

2011

NIGHT DRAGON
Advanced Persistent Threat Targeting Global Energy

DUQU
Worm Targeting ICS Information Gathering and Stealing

2012

SHAMOON
Virus Targeting Energy Sector Largest Wipe Attack

FLAME
Virus use for Targeted Cyber Espionage in the Middle East

GAUSS
Information Stealer Malware

2013

RED OCTOBER
Cyber-Espionage Malware Targeting Gov't & Research Organizations

2014

HAVEX
Industrial Control System Remote Access Trojan & Information Stealer

HEARTBLEED
Security Bug and Vulnerability Exploited by Attackers

2015

BLACKENERGY
Malware Injected into Ukrainian Power Company Network, Cut Power to the Affected Region.

2016

BLACKENERGY
Malware Injected into Power Company Network, Attackers Cut Power to the Affected Region.

OP GHOUL
Spear-phishing Campaign Targeting Middle East Industrial Organizations

2017

NOTPETYA
Ransomware Malware Based
On Stolen NSA Exploits that Impacted ICS Systems

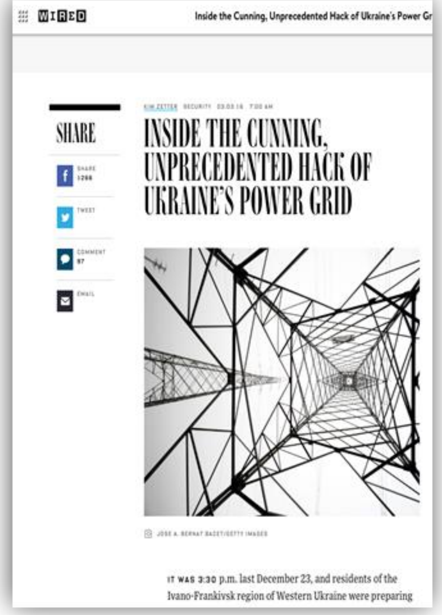
INDUSTROYER
Malware Targeting Electric Utility – Used in 2016 Ukraine Grid Attack

WANNACRY
General ransomware which impacted ICS Systems

ICS CERT INCIDENT COUNT
*****Only Reported Incidents in U.S.***

Industrial Control System Threat Actors

Nation States



WIRED
Inside the Cunning, Unprecedented Hack of Ukraine's Power Gr
SHARE
SHARE 1266
TWEET
COMMENT 97
EMAIL

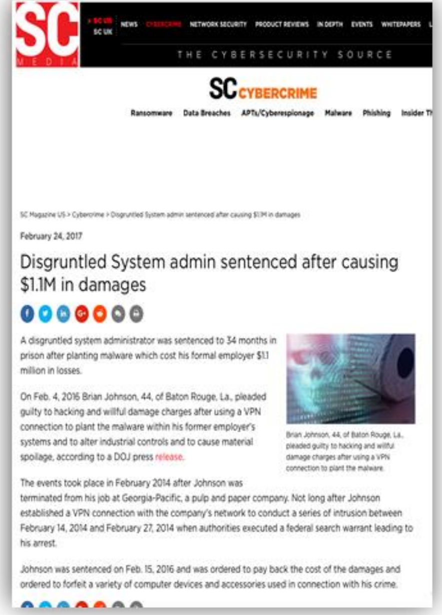
KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

JOSE A. BERNAT BACETE/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing

Insiders



SC MEDIA
> SC US
SC UK
NEWS CYBERCRIME NETWORK SECURITY PRODUCT REVIEWS IN DEPTH EVENTS WHITEPAPERS
THE CYBERSECURITY SOURCE
SC CYBERCRIME
Ransomware Data Breaches APTs/Cyberespionage Malware Phishing Insider Th

SC Magazine US > Cybercrime > Disgruntled System admin sentenced after causing $1.1M in damages

February 24, 2017

Disgruntled System admin sentenced after causing $1.1M in damages

A disgruntled system administrator was sentenced to 34 months in prison after planting malware which cost his formal employer $1.1 million in losses.

On Feb. 4, 2016 Brian Johnson, 44, of Baton Rouge, La., pleaded guilty to hacking and willful damage charges after using a VPN connection to plant the malware within his former employer's systems and to alter industrial controls and to cause material spoilage, according to a DOJ press release.

Brian Johnson, 44, of Baton Rouge, La., pleaded guilty to hacking and willful damage charges after using a VPN connection to plant the malware.

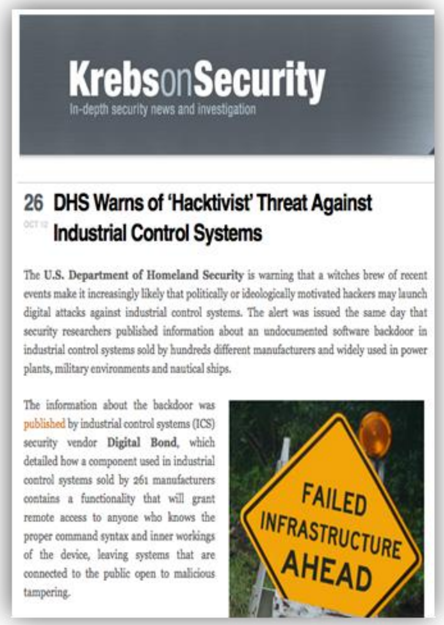
The events took place in February 2014 after Johnson was terminated from his job at Georgia-Pacific, a pulp and paper company. Not long after Johnson established a VPN connection with the company's network to conduct a series of intrusion between February 14, 2014 and February 27, 2014 when authorities executed a federal search warrant leading to his arrest.

Johnson was sentenced on Feb. 15, 2016 and was ordered to pay back the cost of the damages and ordered to forfeit a variety of computer devices and accessories used in connection with his crime.

Terrorists

Online Attacks on Infrastructure Are Increasing at a Worrying Pace

Hacktivists



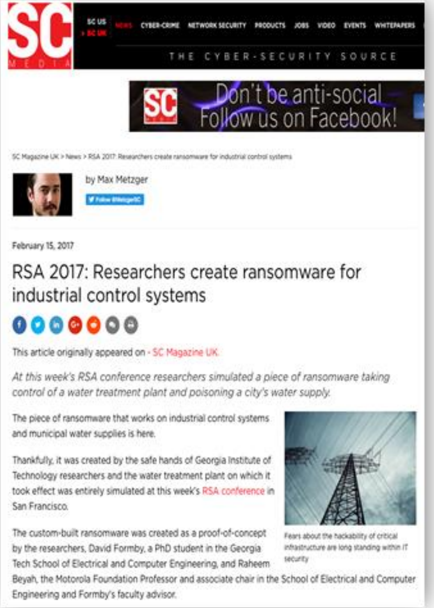
KrebsonSecurity
In-depth security news and investigation
26
OCT 12
FAILED INFRASTRUCTURE AHEAD

DHS Warns of 'Hacktivist' Threat Against Industrial Control Systems

The **U.S. Department of Homeland Security** is warning that a witches brew of recent events make it increasingly likely that politically or ideologically motivated hackers may launch digital attacks against industrial control systems. The alert was issued the same day that security researchers published information about an undocumented software backdoor in industrial control systems sold by hundreds different manufacturers and widely used in power plants, military environments and nautical ships.

The information about the backdoor was published by industrial control systems (ICS) security vendor **Digital Bond**, which detailed how a component used in industrial control systems sold by 261 manufacturers contains a functionality that will grant remote access to anyone who knows the proper command syntax and inner workings of the device, leaving systems that are connected to the public open to malicious tampering.

Cyber Criminals



SC MEDIA
SC US
> SC UK
NEWS CYBER-CRIME NETWORK SECURITY PRODUCTS JOBS VIDEO EVENTS WHITEPAPERS
THE CYBER-SECURITY SOURCE
SC
Don't be anti-social
Follow us on Facebook!
Follow @MetzgerSC

SC Magazine UK > News > RSA 2017: Researchers create ransomware for industrial control systems

by Max Metzger

February 15, 2017

RSA 2017: Researchers create ransomware for industrial control systems

This article originally appeared on - SC Magazine UK

At this week's RSA conference researchers simulated a piece of ransomware taking control of a water treatment plant and poisoning a city's water supply.

The piece of ransomware that works on industrial control systems and municipal water supplies is here.

Thankfully, it was created by the safe hands of Georgia Institute of Technology researchers and the water treatment plant on which it took effect was entirely simulated at this week's RSA conference in San Francisco.

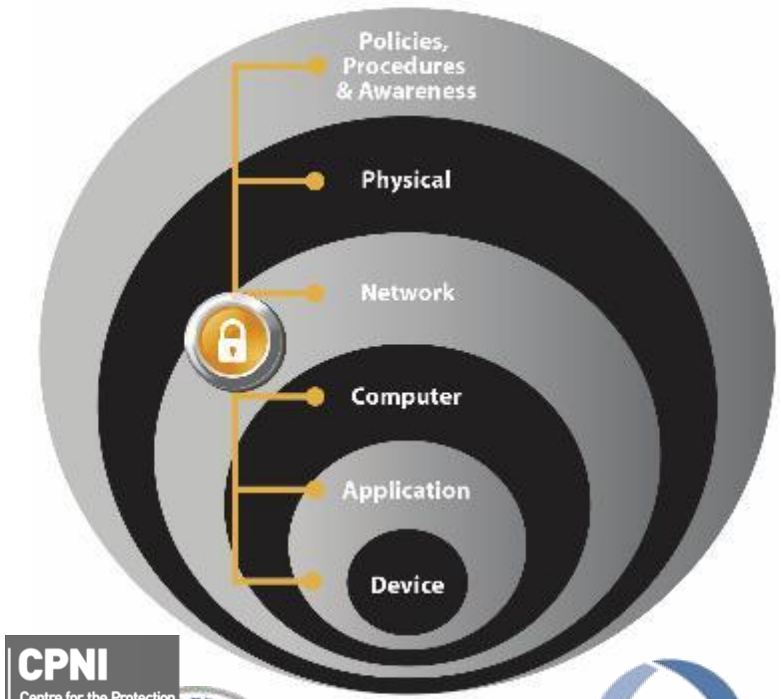
The custom-built ransomware was created as a proof-of-concept by the researchers, David Formby, a PhD student in the Georgia Tech School of Electrical and Computer Engineering, and Raheem Beyah, the Motorola Foundation Professor and associate chair in the School of Electrical and Computer Engineering and Formby's faculty advisor.

Fears about the hackability of critical infrastructure are long standing within IT security

Defense-in-Depth

A secure application depends on multiple layers of diverse protection and industrial security must be implemented as a system

Deploying Network Security Within A Converged Plantwide Ethernet Architecture

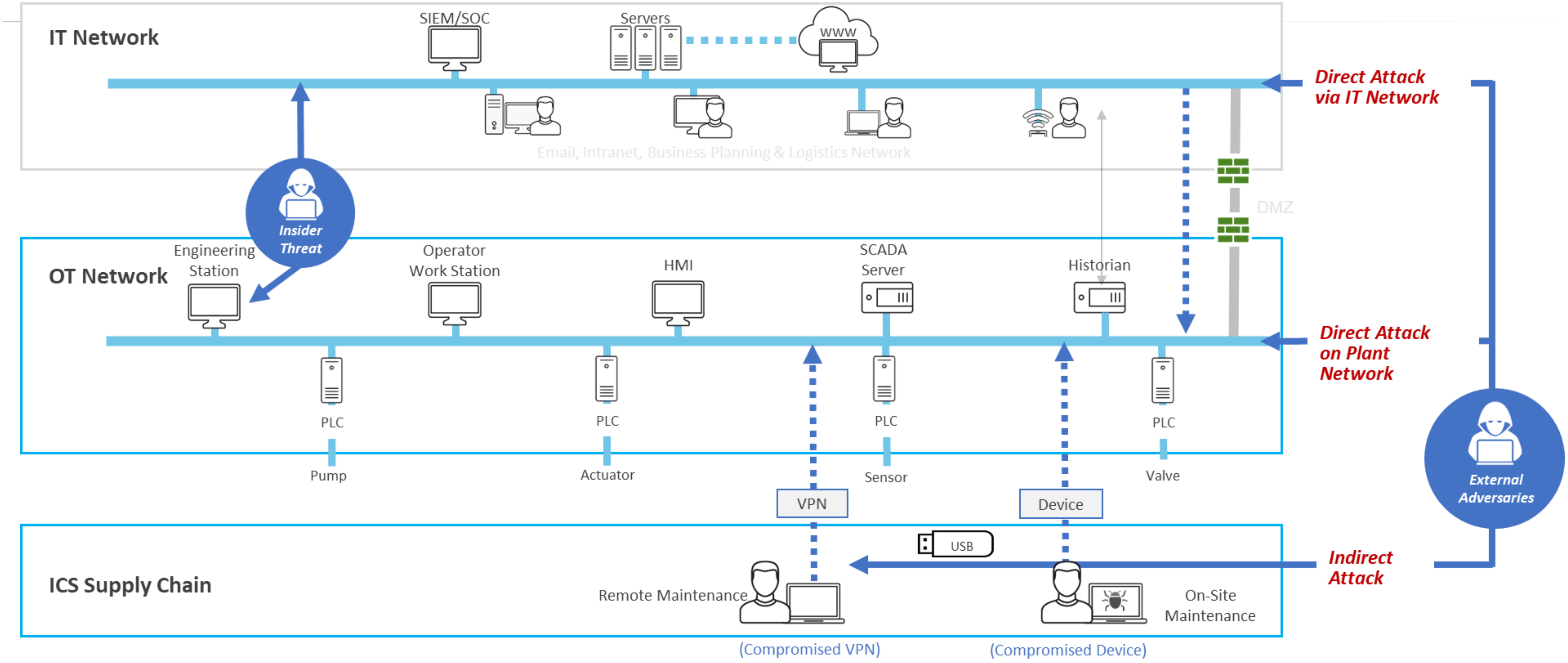


- **Defense in Depth**
  - Shield targets behind multiple levels of diverse security countermeasures to reduce risk
- **Openness**
  - Consideration for participation of a variety of vendors in security solutions
- **Flexibility**
  - Able to accommodate a customer's needs, including policies & procedures
- **Consistency**
  - Solutions that align with Government directives and Standards Bodies

CPNI Centre for the Protection of National Infrastructure

ISA IEC NIST

Industrial Control System Threat Vectors



Compliance & Standards

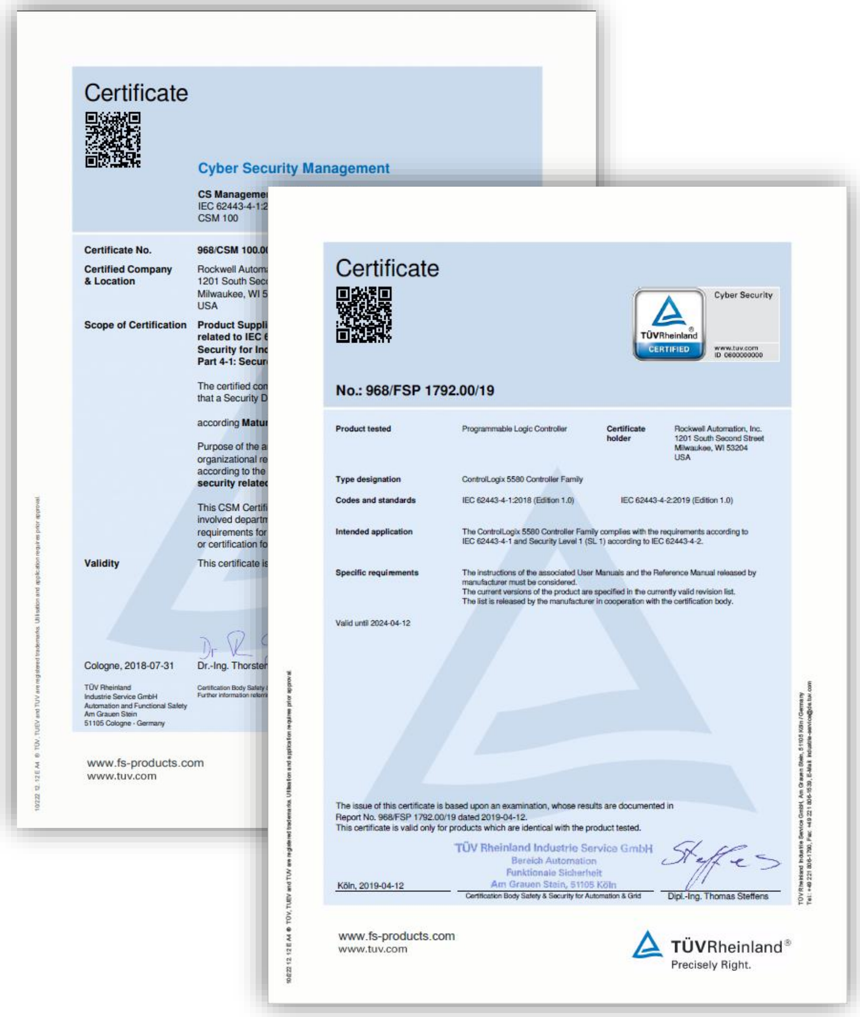
Certified Products, Architectures and Solution Delivery

ISA/IEC 62443: Series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

Applies to those responsible for ***designing, manufacturing, implementing, or managing*** industrial control systems:

- End-users (i.e. asset owner)
- System integrators
- Security practitioners
- ICS product/systems vendors

**Equivalence to ISO 27001 and NIST Cybersecurity Framework*



Certificate

Cyber Security Management

CS Managemen
IEC 62443-4-1:2
CSM 100

Certificate No.	968/CSM 100.0
Certified Company & Location	Rockwell Autom 1201 South Sec Milwaukee, WI 5 USA
Scope of Certification	**Product Suppli related to IEC 6 Security for Inc Part 4-1: Secur** The certified con that a Security D according **Matur** Purpose of the a organizational re according to the **security relatec** This CSM Certifi involved departm requirements for or certification fo
Validity	This certificate is

Cologne, 2018-07-31 Dr.-Ing. Thorster

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety
Further information referr

www.fs-products.com
www.tuv.com

10/222 12.12 E A4 © TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

Certificate

TÜVRheinland® CERTIFIED Cyber Security www.tuv.com ID 0600000000

No.: 968/FSP 1792.00/19

Product tested	Programmable Logic Controller	**Certificate holder**	Rockwell Automation, Inc. 1201 South Second Street Milwaukee, WI 53204 USA
Type designation	ControlLogix 5580 Controller Family		
Codes and standards	IEC 62443-4-1:2018 (Edition 1.0)	IEC 62443-4-2:2019 (Edition 1.0)	
Intended application	The ControlLogix 5580 Controller Family complies with the requirements according to IEC 62443-4-1 and Security Level 1 (SL 1) according to IEC 62443-4-2.		
Specific requirements	The instructions of the associated User Manuals and the Reference Manual released by manufacturer must be considered. The current versions of the product are specified in the currently valid revision list. The list is released by the manufacturer in cooperation with the certification body.		

Valid until 2024-04-12

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1792.00/19 dated 2019-04-12.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

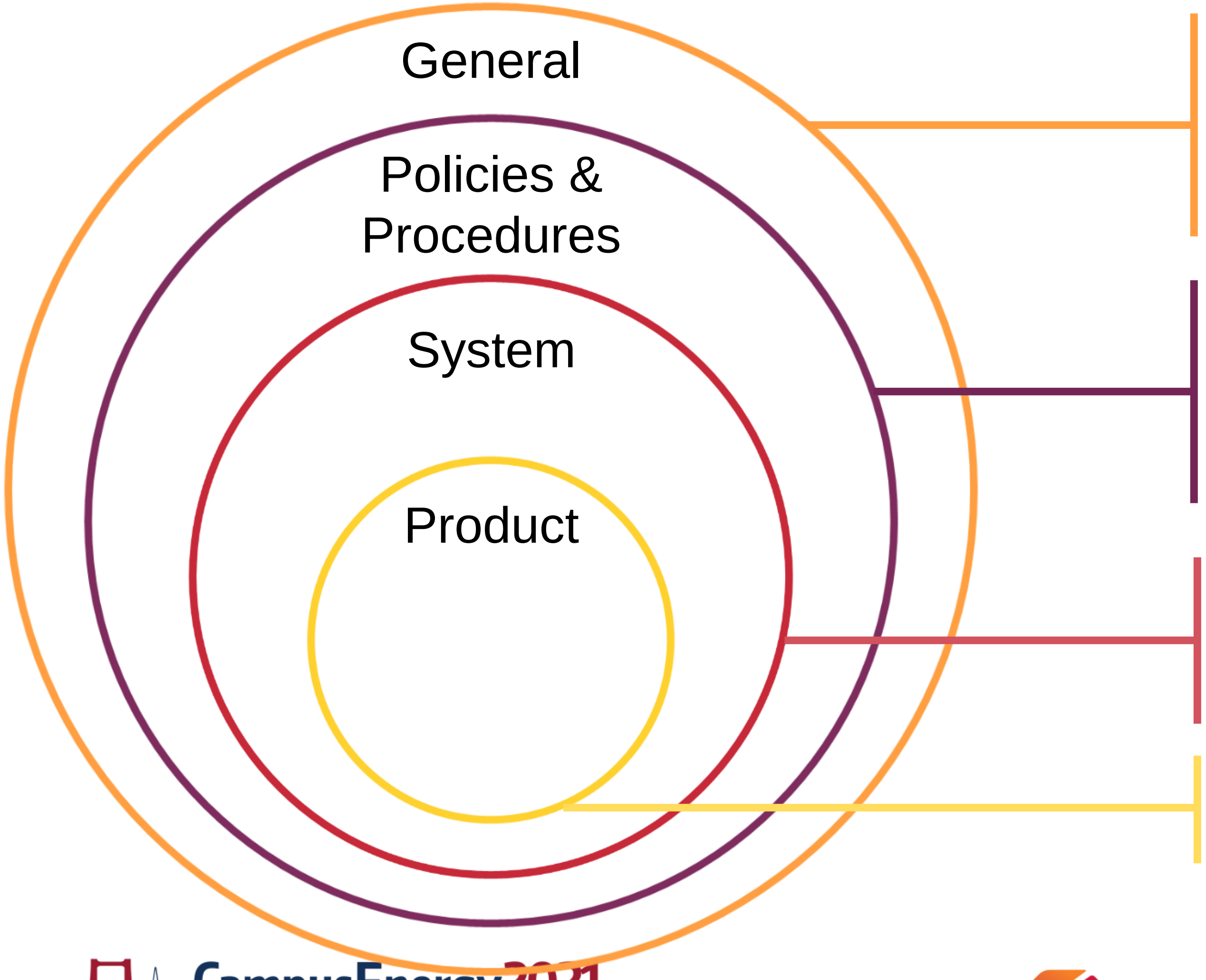
Köln, 2019-04-12 | Certification Body Safety & Security for Automation & Grid | Dipl.-Ing. Thomas Steffens

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

IEC 62443

Series of standards that define procedures for implementing electronically secure IACS.



1-1: Models & Concepts
1-2: Master Glossary
1-3: System Security Compliance Metrics
1-4: IACS Security Lifecycle & Use-Cases

2-1: Requirements for IACS Security Management System
2-2: Implementation guidance
2-3: Patch management guidance
2-4: Installation and maintenance guidance

3-1: Security Technologies for IACS
3-2: Security Risk Assessment and System Design
3-3: System Security Requirements and Security Levels

4-1: Product development requirements
4-2: Technical security requirements for IACS

ISA/IEC 62443 Structure

General	Policies & Procedures	System	Component / Product
1-1 Models and concepts	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidance for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements for IACS service providers		

Asset Owner

Service Provider

Integration Provider

Product Supplier

Supplier Chain EO13920 and NERC CIP-013-1

Key Items for Automation Suppliers

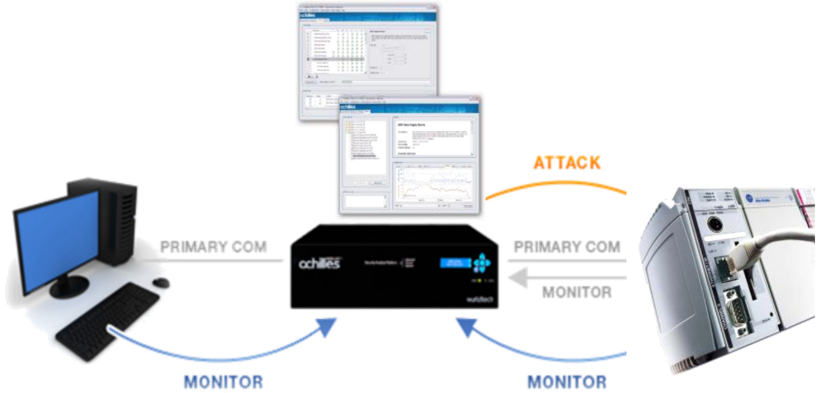
- This is serious
- “foreign adversary”
- Regulated entity compliance and by proxy impact to Suppliers
- NERC CIP-013, calls for a plan to protect a utility’s supply chain
- Impact to design, development, manufacturing, testing, implementation, and chain of custody
- Assessment of current and future vendor relationships by preparing and issuing questionnaires.
- For the purposes of **Supply Chain Risk Management (SCRM**), a vendor is described as
    - The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract to supply BES Cyber Systems and related services.
    - It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards).
    - A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

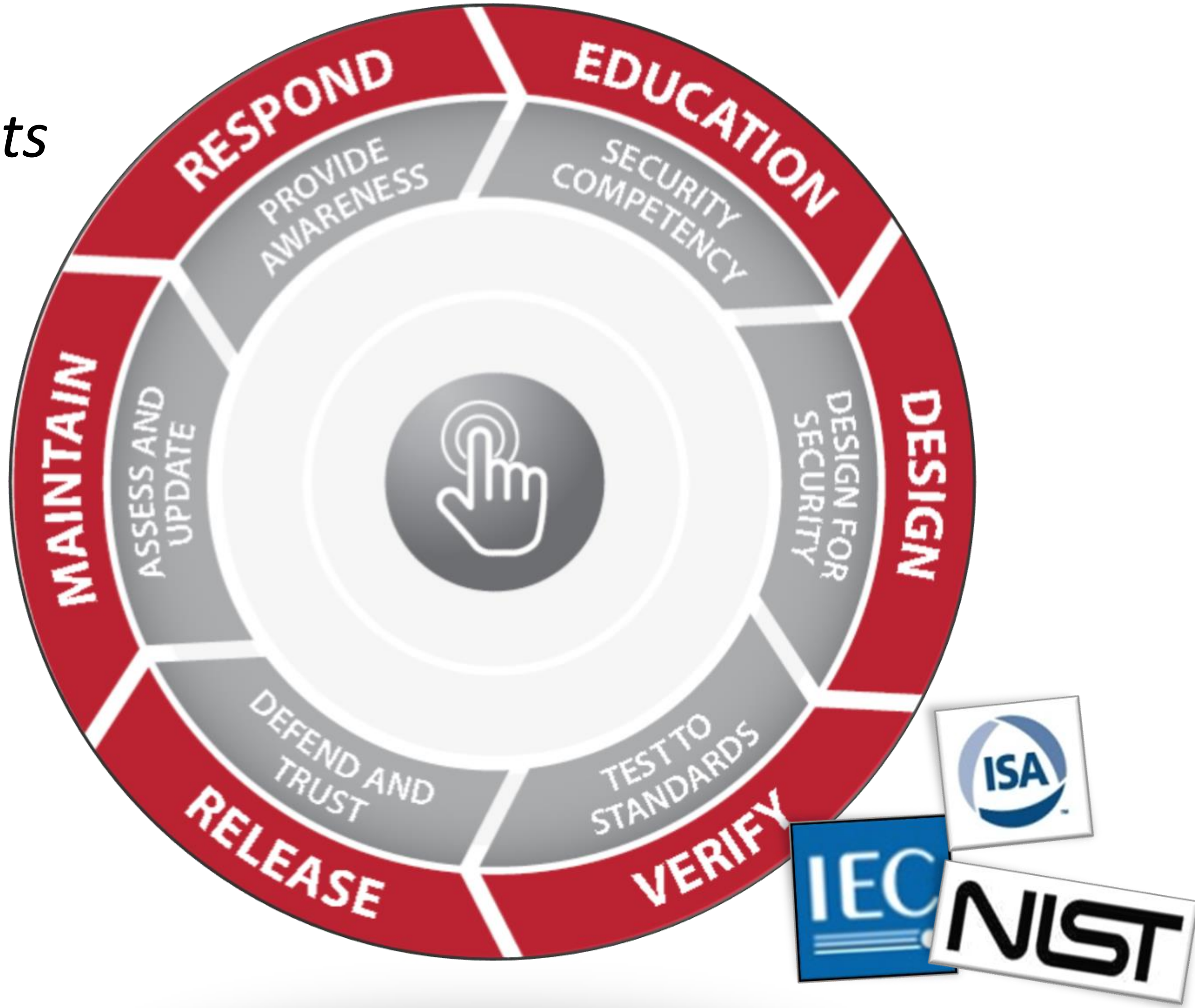
Trusted Supplier

Security Built-in

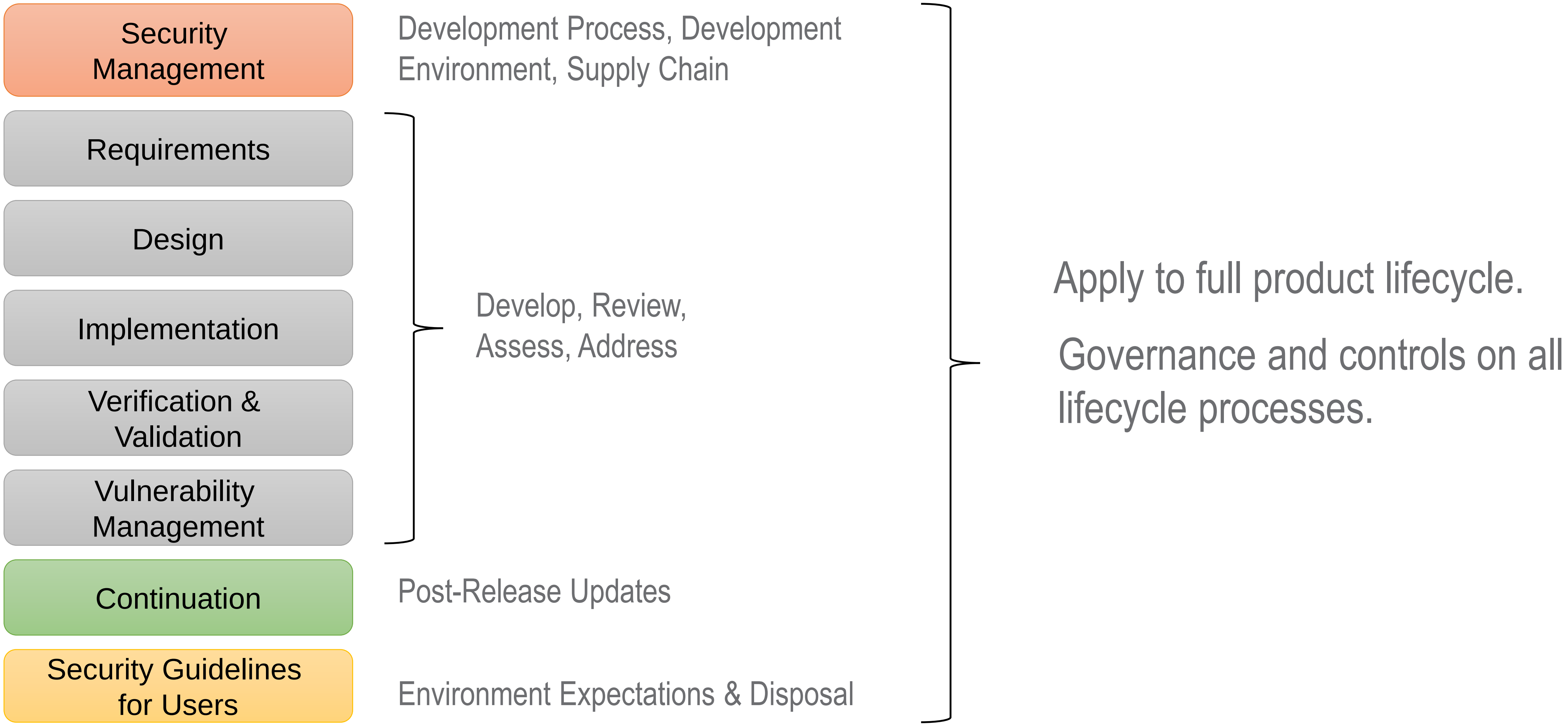
Vendors must build security into products with a focus on security throughout the products lifecycle…

Secure Development Lifecycle





Secure Development Lifecycle - Practice Areas



Security Management

Requirements

Design

Implementation

Verification & Validation

Vulnerability Management

Continuation

Security Guidelines for Users

Development Process, Development Environment, Supply Chain

Develop, Review, Assess, Address

Post-Release Updates

Environment Expectations & Disposal

Apply to full product lifecycle.

Governance and controls on all lifecycle processes.

Requirements - Design for Security

- Security requirements for all products (including factored)
  - Establishes a common baseline for the security of hardware and software products
  - Ensures products are consistently developed, enhanced and delivered
- Continuous improvement program
  - Changes reviewed by the SME community and other extended security team members
  - Updated by end of each fiscal year, as new threats and vulnerabilities emerge.

Design for Security - Examples

- ‘No back doors’ or ‘hidden passwords’ policy
- Prevent disruptive operations
- Minimize open TCP / UDP ports
- Web server hardening
- SNMP policy
- Ethernet Protocol Testing TCP/IP
- CIP Protocol Compliance Testing
- Trusted Binaries (Firmware, Software)
- OS Platform Hardening

- Protected Mode for Disruptive Ops
- Hardening common Ethernet Services
  - SMTP, SNMP, FTP, SSH
- Secure Coding Best Practices
  - No static passwords, coding standards, code reviews
- Secure Training for SMEs and Team
- Cryptography Standards

Product Security Incident Response Team (PSIRT)

Key items of the PSIRT function:

- Provides governance and oversight consistent w/ appropriate government agencies and standards
- Leads the process for evaluating both internally and externally reported potential vulnerabilities
- Accepts input from any/all sources, with responsible disclosure
- Leads a strong partnership with affected product teams and business units, legal, marketing and communications, and customer support
- Inform customers and provide mitigations for product security vulnerabilities, to enable them to take action and reduce their risk.
- Coordinate company internal teams to drive continuous improvement and process enhancements

What to do - Increased Assessment

- Institutions will have to dig deeper to get the information
  - Increases cost
    - Personnel
    - Direct - Cost transferred from vendor

- Increases time to production
  - Due to increased assessment
  - Due to increased time to negotiate contracts

- May need to review all existing technology deployed
  - Would be recommended

- May need to replace some technologies
  - Unplanned and Additional costs
  - Risk of failure of systems due to incompatibility

What to do - Increased Monitoring

- Institutions will need to continuously monitor vendors
  - Determine where they are conducting business
  - Who influences their manufacturing
  - Where are they getting their components
  - Where are they assembling the product

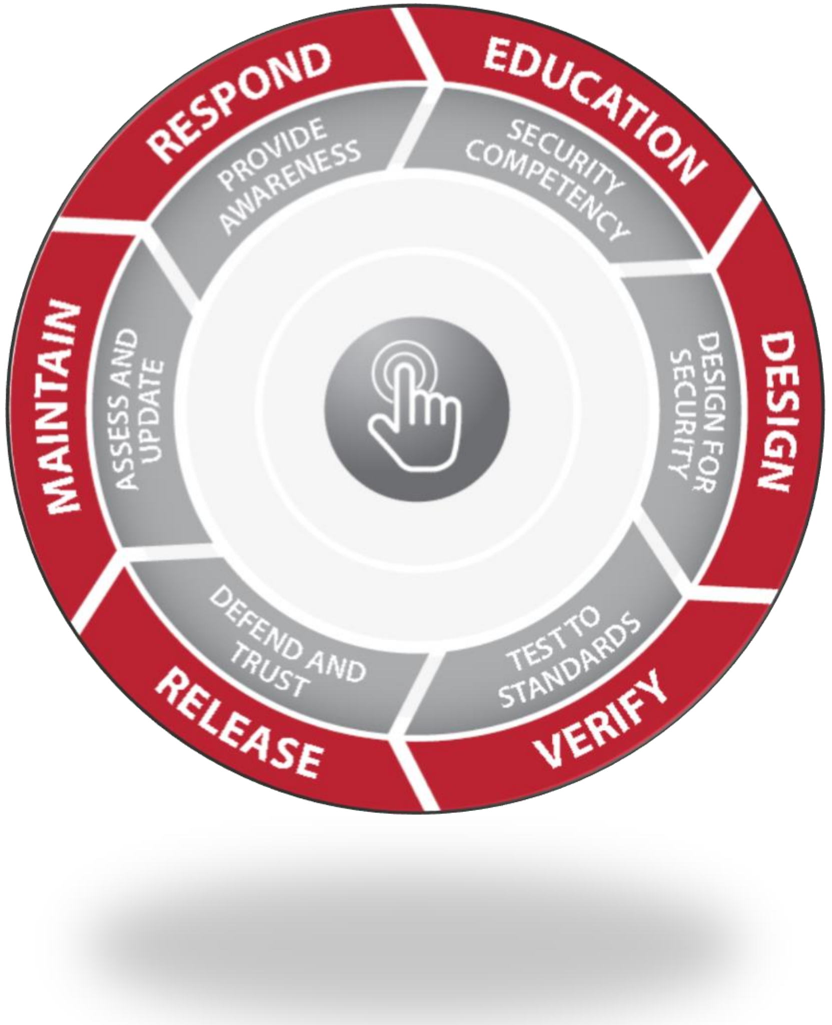
- Institutions will need to be aware of updates
  - Where are they produced
  - How are they produced
  - How are they distributed
  - Integrity management
  - Source verification

What to do - Increased Auditing

- Ensure you have contractual agreements
  - Product development, assembly, control, etc.
  - Notification of change of ownership, control or influence
    - Are new foreign entities involved in the process
    - Who are they
    - Are they acceptable to the utility

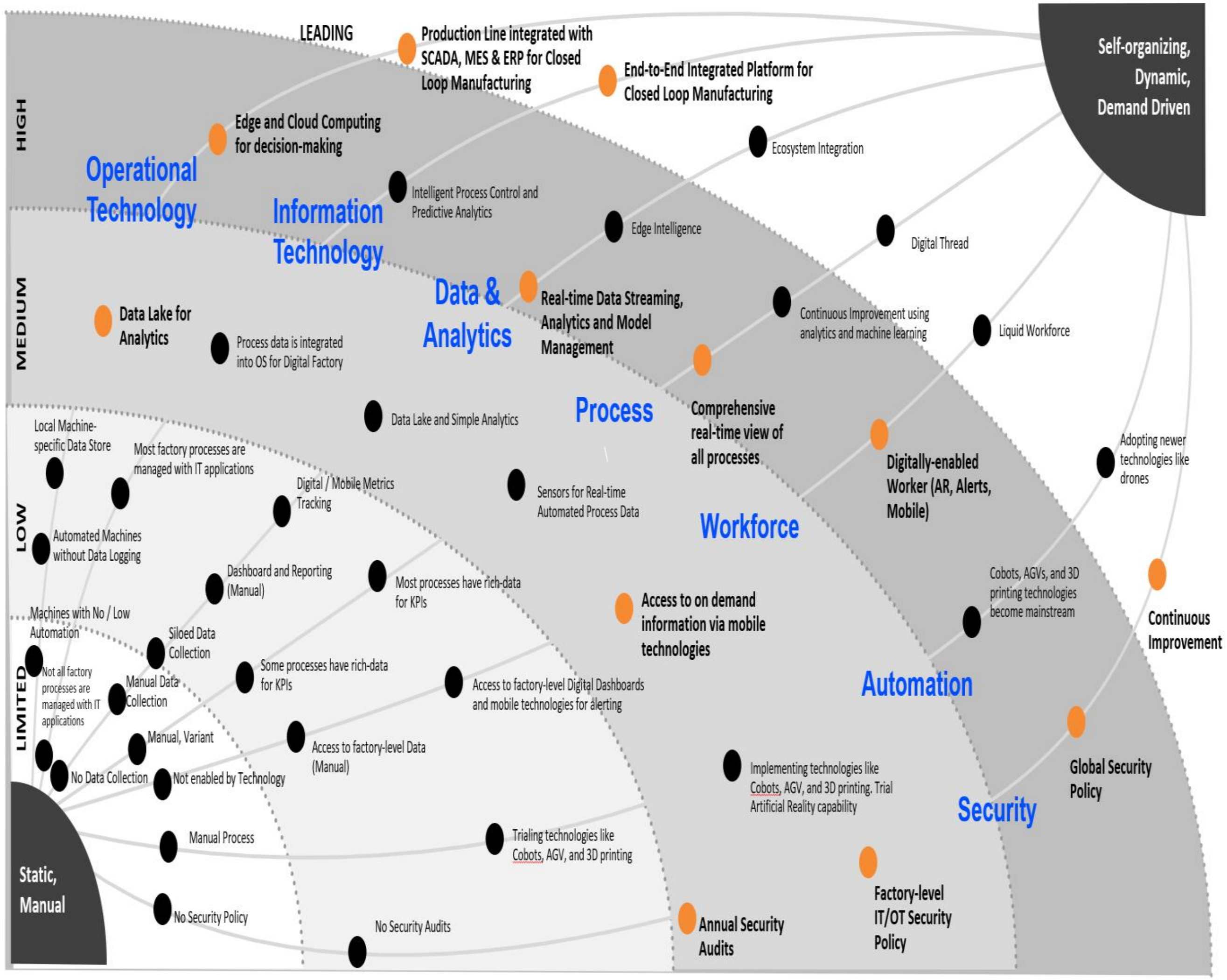
- Institutions will have to ensure they audit their vendors
  - Accept Third Party Audits
  - Perform your own
  - Attestations

- Continuous Process



What to do - Summary

- Understand your organization's digital maturity
- Review technology supplier's cyber security program
- Require a secure development lifecycle
- Review Supply Chain Risk Management
- Define Standards (e.g. IEC 62443, NIST, NERC, etc.)
- Require a certified solution delivery
- Define Recognized Risk
  - Analysis
  - Mitigate
  - Informed decisions



HIGH
MEDIUM
LOW
LIMITED
LEADING
Static, Manual
Self-organizing, Dynamic, Demand Driven
Operational Technology
Information Technology
Data & Analytics
Process
Workforce
Automation
Security
Production Line integrated with SCADA, MES & ERP for Closed Loop Manufacturing
End-to-End Integrated Platform for Closed Loop Manufacturing
Edge and Cloud Computing for decision-making
Ecosystem Integration
Intelligent Process Control and Predictive Analytics
Edge Intelligence
Digital Thread
Data Lake for Analytics
Process data is integrated into OS for Digital Factory
Real-time Data Streaming, Analytics and Model Management
Continuous Improvement using analytics and machine learning
Liquid Workforce
Data Lake and Simple Analytics
Comprehensive real-time view of all processes
Local Machine-specific Data Store
Most factory processes are managed with IT applications
Digital / Mobile Metrics Tracking
Sensors for Real-time Automated Process Data
Digitally-enabled Worker (AR, Alerts, Mobile)
Adopting newer technologies like drones
Automated Machines without Data Logging
Dashboard and Reporting (Manual)
Most processes have rich-data for KPIs
Access to on demand information via mobile technologies
Cobots, AGVs, and 3D printing technologies become mainstream
Continuous Improvement
Machines with No / Low Automation
Siloed Data Collection
Not all factory processes are managed with IT applications
Manual Data Collection
Some processes have rich-data for KPIs
Access to factory-level Digital Dashboards and mobile technologies for alerting
Manual, Variant
Access to factory-level Data (Manual)
No Data Collection
Not enabled by Technology
Implementing technologies like Cobots, AGV, and 3D printing. Trial Artificial Reality capability
Global Security Policy
Manual Process
Trialing technologies like Cobots, AGV, and 3D printing
No Security Policy
No Security Audits
Annual Security Audits
Factory-level IT/OT Security Policy

Tom McDonnell

Rockwell Automation,

Power and Energy Industry Leader

TMMcDonnell@RA.Rockwell.com

Rockwell Automation