Holistic Cybersecurity for Industrial IoT Applications

Arun Siddeswaran
Sr. Manager, Solution Engineering
Cisco Systems, Inc.

Gregory Wilcox
Principal Engineer, Strategic Development
Rockwell Automation, Inc.

Presented at the ODVA
2018 Industry Conference & 19th Annual Meeting
October 10, 2018
Stone Mountain, Georgia, USA

Abstract

Industrial IoT (IIoT) offers the promise of business outcomes through the use of innovative technology. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices.

No single product, technology or methodology can fully secure IIoT applications. Protecting IIoT assets requires a holistic security approach to help address different types of threats. This approach uses multiple layers of diverse technologies for protection and detection, applied at different levels of IIoT architectures, while being implemented by different personas.

This paper, authored and presented by Cisco Systems and Rockwell Automation, will provide an overview of a holistic IIoT security framework. This framework incorporates aspects of IEC-62443 and NIST 800-82, leverages CIP Security™ for security zoning, addresses OT and IT personas, and enables secure connectivity from smart devices to smart machines/skids to cloud applications.

Keywords

OT-IT Convergence, IIoT, IoT, best practices, architecture, manufacturing, design, industrial, industrial security, cybersecurity

Industrial IoT (IIoT) Opportunities / Challenges

Industrial IoT (IIoT) offers the promise of business outcomes through the use of innovative technology such as mobility, collaboration, analytics and cloud-based services. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security and safety best practices.
There are many aspects that could impact the reliability and security of Industrial IoT architectures (Figure 1):

- **Connected Architectures** – smart IIoT devices which enable smart skids/equipment/machines, which in turn enables smart plants, but also smart IIoT devices connected to on premise applications (e.g. historians, analytics) or connected to cloud-based applications (e.g. analytics, dashboards).
- **Convergence** - not just technology and networks, but also cultural and organizational convergence of different personas, specifically IT and OT, groups that had little interaction in the past are now collaborating to share best practices.
- **Industrial standards** - for networking and security.
- **Cybersecurity Threats** – growing cybersecurity threats (types and actors) increase the risk to protect the availability, integrity and confidentiality of data within IIoT architectures. Powerful, yet simple to use tools are readily available to novice threat actors.
- **Scalable, Reliable, Safe, Secure and Future-ready Industrial IoT Architectures** requires an ecosystem.

![Industrial IoT Architectures](source: Rockwell Automation)

**OT-IT Collaboration**

Figure 2 is an architectural representation of the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE) reference architectures. CPwE has been helping industrial operations converge their many disparate operational, processing and production systems into a single control and information platform, utilizing a single Industrial IoT network technology, which is EtherNet/IP.

CPwE is a collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation. The content of CPwE is relevant to both operational technology (OT) and information technology (IT) disciplines. CPwE consists of documented architectures, best practices, design guidance and configuration settings to help industrial operations with development and
deployment of a scalable, reliable, safe, secure and future-ready plant-wide industrial network infrastructure.

Standard network and security technology by the IEEE and IETF is used by both IT at the Enterprise and operational technology (OT) for IIoT applications. However, there are cultural differences in how the technology is applied that should be accounted for. Examples of differences would be traffic types, data prioritization, time synchronization, resiliency and security policies and procedures.

Figure 2 - OT-IT Collaboration
Source: Cisco-RA CPwE

Cybersecurity – OT vs. IT

Due to IACS application requirements, there are differences (Figure 3) in how the technology, policies and procedures are applied between OT and IT that should be accounted for when developing an industrial security program. The following is a high-level summary:

- **Technology Differences:**
  - Software and hardware toolsets
  - Varying implementations of Layer 2/3 network services may create incompatibilities
    - Availability, Performance, Traffic Types, Security

- **Cultural Differences:**
  - Availability SLA (service level agreement)
    - Minutes/Hours vs. Hours/Days
  - Policies:
    - Security – Confidentiality, Integrity and Availability (CIA) vs. Availability, Integrity and Confidentiality (AIC)
    - QoS – prioritization of voice and video
    - NAT, Multicast

- **Skill-gaps – Workforce Development:**
  - OT personnel lacking knowledge of IT skills and requirements
  - IT personnel lacking knowledge of OT skills and requirements
  - Lack of Industrial IT personnel that bridge the gap between OT and IT
  - Challenges with Industrial IT talent recruitment, development and retention

- **Functional Differences and Incompatibilities between IT and OT:**
Technologies – e.g. resiliency, security
Products – e.g. QoS policies
Applications – e.g. WebEx and Skype vs. SCADA
Solutions – e.g. network access control vs. application access control

Industrial Security Trends

World Wide Threat Assessment -2015 (Figure 4):
- Director of National Intelligence James Clapper to the House Permanent Select Committee on Intelligence -September 10, 2015:
  - Cyber threats increasing in frequency, scale, sophistication and severity of impact.
  - Several nations have undertaken offensive cyber operations against private sector targets.
  - Cyber threat cannot be eliminated, rather, cyber risk must be managed.
  - The likelihood of a catastrophic attack is remote at this time; rather, we envision an ongoing series of low-moderate level cyber-attacks which will impose cumulative costs on U.S. economic competitiveness and national security.
According to the US DHS, industrial operations (Figure 5) led the way in 2016 for reporting cyber incidents – e.g. manufacturing, energy, water, transportation, chemical and food and agriculture. There was a broad range of infection vectors reported. Spear phishing, enabled by social engineering, was the most commonly reported.

Balancing Cost vs. Risk vs. Productivity

One continuing trend is the need to balance cost vs. risk vs productivity. Every industrial automation and control system (IACS) application is unique to some degree. One size does not fit all when it comes to risk tolerance and stance on availability, safety and security. What is acceptable by one industrial operator may be unacceptable to another and vice versa. IIoT architectures should support scalability, which includes the degree of holistic and diverse industrial security technologies applied at different levels of a plant-wide security architecture. Scalable security comes in many forms. Based on risk mitigation requirements, several diverse technology options are available for threat detection and prevention to help industrial operations meet their tolerance to risk.

The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security and safety best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry
security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.

Utilize safety and security standards to help assess the required security stance to meet the application requirements:

- Alignment with industrial functional safety standards such as IEC 61508, IEC 62061 (SIL), ISO 13849 (PL), CIP Safety
- Alignment with industrial security standards such as IEC-62443 (formerly ISA99), NIST 800-82, ICS-CERT and CIP Security

The need for early, open and two-way dialogue within industrial operations, especially between OT and IT, is critical for the success of IIoT projects. One size does not fit all when it comes to risk tolerance and stance on availability, safety and security.

**Established Industrial Security Standards**

There are multiple organizations, consortia and government agencies that provide or reference industrial security standards and recommended practices. Each has the common threads of:

- Security Zones – organizing industrial operations into functional or security zones, with strong segmenting of industrial operations from business (enterprise) networks.
- Defense-in-Depth - this approach uses multiple layers of diverse technologies for protection and detection, applied at different levels of IIoT architectures, while being implemented by different personas.

IEC 62443 and NIST 800-82 (Figure 6) is a series of standards, not just a single standard.

- **IEC 62443:**
  - General - general information which is applicable to industrial operations, System Integrators, and IACS vendors.
  - Policies and Procedures - most applicable to industrial operations.
  - System - most applicable to system designers (e.g. 3-2 for security zones and secure conduits) and system implementers (e.g. 3-3).
  - Component / Product – most applicable to IACS vendors.

- **NIST 800-82:**
  - Identify – development of policies and procedures to govern industrial operations, awareness and training for industrial operators, IACS asset inventory, IACS network discovery
  - Protect - multiple layers of diverse technologies for threat protection
  - Detect - multiple layers of diverse technologies for threat detection
  - Respond - policies and procedures to govern industrial operations, awareness and training for industrial operators
  - Recover - multiple layers of diverse technologies for IACS and network asset archiving,
Holistic and Diverse Plant-wide Security

No single product, technology or methodology can fully secure IIoT architectures. Protecting IIoT assets requires a holistic security approach to help address internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical), using diverse technologies for protection and detection, applied at different levels of IIoT architectures, while being implemented by different personas, by applying policies and procedures that address different types of threats.

To understand the security and network systems requirements of an industrial automation and control system (IACS), this document uses a logical model to describe the basic functions and composition of an IACS application. The Purdue Reference Architecture and ISA 95 are common and well-understood models that use Levels to segment devices and equipment into hierarchical functions. The concept of operational Levels has been incorporated into many other models and standards in the industry. Based on this segmentation of the plant operations, standards such as IEC 62443, NIST 800-82 and ICS-CERT recommended practices organize the operational Levels into Security Zones as shown in Figure 7. This is a representation of the CPwE Logical Model.
Multiple layers of defense-in-depth (Figure 7) for IIoT architectures include, but are not limited to:

- **Education and Awareness Programs** - training of OT personnel on established industrial security/safety policies and procedures including how to respond to a security incident.
- **Physical** – limit physical access to authorized personnel only: control room, cells/areas, control panels, IACS devices – e.g. locks, gates, biometrics.
- **Network** – restrictive access, hardening, traffic flow analysis and traffic inspection.
- **Computer Hardening** – patch management program, white listing of IACS applications, restrict admin privileges, removal of unused applications/protocols/services, closing unnecessary logical ports, and protecting physical ports.
- **Application** – restrictive access, trusted communications, hardening, and monitoring.
- **Device Hardening** – trusted communications, change management with disaster recovery, data encryption, and restrictive access.

The CPwE Industrial Security Framework (Figure 8) helps to provide a holistic, scalable, diverse and incremental architectural best practices:

- **Defense-in-Depth** - architectural best practices for holistic and diverse threat detection and protection
- **Alignment with industrial security standards:**
  - IEC 62443 - zones & conduits, availability, integrity, confidentiality.
  - NIST 800-82 - cybersecurity framework, identify, protect, detect, respond, and recover.
  - ICS-CERT - recommended practices for secure network architectures.
- **Different Personas:**
  - OT – e.g. Control System Engineers
  - Industrial IT - Control System Engineers (OT) in collaboration with IT Network Engineers, OT Engineers with IT skills, or IT with knowledge of OT requirements.
  - IT – e.g. security architects in collaboration with OT.
- **Scalability** – IIoT smart device to IACS application, IIoT smart device to Level 3 Site Operations, IIoT smart device to on premise analytics in the enterprise, and IIoT smart device to cloud-based applications.
Industrial security should be holistic (Figure 9) and not treated as a bolt-on afterthought for new IIoT architectures. However, there are many solutions available to help industrial operations incrementally improve the security stance for their legacy IIoT architectures.

- Hardening for Level 0-2 IACS devices - policies and procedures, physical measures, electronic measures, encrypted communications, trusted communications (CIP Security).
- Zoning – segmenting devices and applications into functional and security zones, CPwE Logical Model, Layer 2/3 switch hierarchy with access control lists (ACLs), virtual local area networks (VLANs) for Layer 2 networks, Layer 3 network address translation (NAT) devices, and industrial firewalls.
- Port Security – network and IACS devices, both physical and electronic.
- Application Hardening – application access control, trusted communications with possible whitelisting.
- Industrial Firewall – zoning (access control for protection) of OEM skids/equipment/machines, zoning (access control for protection) of legacy networks with legacy IACS devices which have little to no security capabilities, and inspection of both IIoT and non-IIoT traffic.
- Status and Monitoring – inventory and asset management of both IACS and network devices.
Plant-wide zoning (Figure 10) to support:

- Functional / Security Areas
- Smaller Connected LANs
  - Smaller broadcast domains
  - Smaller fault domains
  - Smaller domains of trust
  - Application micro-segmentation
- Alignment with IEC 62443-3-2 security zones and secure conduits model.
- Segmentation of different and potentially incompatible Industrial IoT Technology.
- Establish a building block approach for scalability.
Application / Device Security:
- CIP Security™, part of a holistic and diverse defense-in-depth security approach (Figure 11)
- Connections between Trusted Endpoints:
  - Reject data that has been altered (integrity).
  - Reject messages sent by untrusted people or untrusted devices (authenticity).
  - Reject messages that request actions that are not allowed (authorization).
- Capabilities:
  - System management
  - Micro-segmentation
  - Device-based firewall
- This does not replace the need for network security – e.g. firewalls, network access control, and zoning.
Figure 11 - Industrial IT (OT-IT) Persona – Application / Device Security

OT/IT Persona - Holistic and Diverse Plant-wide Security

Multiple layers of defense-in-depth (Figure 12) for IIoT architectures threat detection and prevention should include, but not limited to:

- Computer Hardening - patch management program, white listing of IACS applications, restrict admin privileges, removal of unused applications/protocols/services, closing unnecessary logical ports, and protecting physical ports.
- Network Infrastructure – hardening, access control (physical and electronic), and resiliency.
- Wireless LAN (WLAN)
  - Access Policy
    - Equipment SSID
    - Plant Personnel SSID
    - Trusted Partners SSID
  - WPA2 with AES Encryption
  - Autonomous WLAN
    - Pre-Shared Key
    - 802.1X - (EAP-FAST)
  - Unified WLAN
    - 802.1X - (EAP-TLS)
    - CAPWAP DTLS
- Remote Access Server – for central policy enforcement for plant, enterprise and remote access.
- Status and Monitoring – health status of IACS and network devices.
IT Persona - Holistic and Diverse Plant-wide Security

Multiple layers of defense-in-depth (Figure 13) for IIoT architectures threat detection and prevention should include, but not limited to:

- **Network Access Control** – centralized authentication, authorization and accounting (AAA), identity and mobility services, and software-defined segmentation.
- **Plant-wide Firewall Management** – industrial firewalls and firewalls within Industrial Demilitarized Zone (IDMZ).
- **Active Directory** – genesis of identity and access control policy.
- **Status and Monitoring** – traffic flow analysis and traffic inspection.
- **Plant Firewalls** - active/standby, inter-zone traffic segmentation, ACLS, IPS and IDS, VPN services, portal and remote desktop services proxy.
- **IDMZ best practices** – data brokers for reliable and secure communications, TLS proxy, application mirror, reverse proxy, remote desktop gateway server.

- Traditional method utilized VLANs (switch port based) with static ACLs (Figure 14a). This method lacked any dynamic nature and provided no programmability or automation capability.
- Authentication, Authorization and Accounting (AAA) services added the capability of dynamic ACLs to static VLANs (switch port based). This method provides for limited programmability and automation capability (Figure 14a).
- Source-Group Tag Exchange Protocol (SXP) with AAA services (Figure 14b) offers the capability of dynamic programmability and automation since the SXP is bound to the IACS endpoint and not the switch port.
Traffic Flow Analysis (Figure 15) for IIoT architectures.
- Flow - unidirectional stream of packets between a given source and destination.
- IP Flow Information Export (IPFIX), were a flow record is created and cached in the industrial Ethernet switch (IES).
  - Provides data about traffic flows: who, what, where, when, and how
    - Network Monitoring and Anomaly Detection
    - Application Monitoring and Profiling
    - User Monitoring and Profiling
    - Network Planning
    - Security Analysis
  - If one field within an incoming packet is different, a new IPFIX record is created in the local IPFIX cache.
  - Flow analysis, not packet analysis. Lightweight footprint, this is NOT a Full Packet Capture (PCAP).
- Various IPFIX Versions
  - Traditional NetFlow (TNF) – fixed info to identify a flow.
  - Flexible NetFlow (FNF) – user defines how to identify a flow.
- IPFIX Components –Generator, Flow Templates, Exporter, Collector
Cloud-based services help to enable data collaboration and remote monitoring of dashboards by plant personnel and/or trusted industry partners (for example, system integrator, OEM or contractor) for IACS applications within IIoT architectures (Figure 16). A holistic industrial security stance is necessary in order to help protect the integrity of safety and security best practices while also helping to enable restricted cloud-based services.

Industrial operations should also ensure that the cloud provider and internet service provider (ISP) are trusted. They are required to protect connectivity and data per the industrial operator’s security policies.

An IIoT Cloud Gateway should communicate with a Cloud application via Transport Layer Security (TLS). In keeping with the Industrial Demilitarized Zone (IDMZ) concept of brokered services, a TLS proxy should be located in the IDMZ. The IIoT security architecture should use the IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. Industrial Firewall(s) should also be implemented to enforce security policies within a Cell/Area Zone to protect the Industrial Zone from the IIoT Cloud Gateway ingress/egress point.

This is the security architecture recommended by Cisco and Rockwell Automation for industrial operators that require cloud-based connectivity yet have a lower tolerance to risk. Some industrial operators may already have a TLS proxy located in their Enterprise DMZ that buffers their Enterprise Zone from the Internet. This security architecture could be implemented to leverage that existing TLS proxy. A third option is to have a TLS Proxy located in the cloud like the Cisco Umbrella Intelligent Proxy.

Reliable and Secure Remote Access (Figure 17) for IIoT architectures.

- Balanced Security Stance
  - Multiple layers of diverse technology
  - Edge firewall with access policies
  - IDMZ best practices

Source: Cisco-RA CPwE
Identity services for AAA
- Remote access server
- Security zoning

- Enabling Remote Asset Management
- Protecting Integrity of Safety and Security Best Practices

No single product, technology or methodology can fully secure IIoT architectures. Protecting IIoT assets requires a holistic security approach to help address internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical), using diverse technologies for protection and detection, applied at different levels of IIoT architectures, while being implemented by different personas, by applying policies and procedures that address the different types of threats (Figure 18).

One size does not fit all when it comes to risk tolerance and stance on availability, safety and security. What is acceptable by one industrial operator may be unacceptable to another and vice versa. IIoT architectures should support scalability, which includes the degree of holistic and diverse industrial security technologies which are applied at different levels of a plant-wide security architecture. Scalable security comes in many forms. Based on risk mitigation requirements, several diverse technology options are available for threat detection and prevention to help industrial operations meet their tolerance to risk.

The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security and safety best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.
Key Takeaways

ODVA Members

Develop products that align with Industrial Automation and Control System (IACS) Security Standards and Technologies:

- IEC 62443
  - Education and awareness for your teams and customers
  - Strategy to address 4-1 and 4-2, where it makes sense for your business
- CIP Security
  - Harden EtherNet/IP products
  - Adopt CIP Security where it makes sense for your business
  - Conformance testing
  - Participate in PlugFest

End Users, System Integrators, OEMs

Utilize standards, reference models, and tested and validated reference architectures to help simplify your design, accelerate your deployment, and reduce your risk in deploying new technology.

No single product, technology or methodology can fully secure IIoT applications. Protecting IIoT assets requires a holistic security approach to help address different types of internal and external threats. This approach uses multiple layers (administrative, physical, and electronic) of diverse technologies for threat protection and detection, applied at different levels of IIoT applications, while being implemented by different personas.
Although industrial security should be holistic for Greenfield IIoT projects, there are many solutions available to help industrial operations incrementally improve the security stance for their legacy IIoT architectures.

Implement risk management policies for availability, safety and security: determination of risk tolerance, performing a risk assessment and implementing risk mitigation solutions.

Align with Industrial Automation and Control System (IACS) Security Standards.

**Definition of terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IIoT</td>
<td>Industrial Internet of Things</td>
</tr>
<tr>
<td>OT</td>
<td>Operation Technology</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>IES</td>
<td>Industrial Ethernet Switch</td>
</tr>
<tr>
<td>VLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>IACS</td>
<td>Industrial Automation and Control System</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>IDMZ</td>
<td>Industrial Demilitarized Zone</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication Authorization Accounting</td>
</tr>
<tr>
<td>CIP</td>
<td>Common Industrial Protocol</td>
</tr>
</tbody>
</table>

**References**

Cisco Design Zone for Manufacturing - Converged Plantwide Ethernet

Rockwell Automation – Industrial Network Architectures- Converged Plantwide Ethernet

Education / Awareness - Industrial IP Advantage (IIPA) eLearning
http://www.industrial-ip.org/en

National Cybersecurity & Communications Integration Center (NCCIC)

ODVA CIP Security

************************************************************************************
*

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of ODVA technologies and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because ODVA technologies may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying ODVA networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use. Copyright ©2018 ODVA, Inc. All rights reserved. For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on: TEL +1 734-975-8840 FAX +1 734-922-0027 EMAIL odva@odva.org WEB www.odva.org.  CIP, Common Industrial Protocol, CIP Energy, CIP Motion, CIP Safety, CIP Sync, CIP Security, CompoNet, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc. All other trademarks are property of their respective owners.