Security Lifecycles in ISA/IEC 62443 Cybersecurity Standards

Johan B Nye
ICS Guru LLC
September 23, 2020
About the Speaker

- Johan Nye
- johan.nye@ICS.guru
- Experience
  - Currently an independent ICS cybersecurity consultant
  - Currently part of ISA 99 committee leadership
  - Previously ICS Cybersecurity Advisor @ major petrochemical company
  - Previously Chairman @ ISA Security Compliance Institute (ISASecure.org)
  - MIT, BS/MS Mechanical Engineering
Agenda

- Key messages
- Principal roles and responsibilities
- Industrial Automation and Control Systems (IACS)
- ISA/IEC 62443 series of standards
- Product Security Lifecycle
- Automation Solution Security Lifecycle

Note: this presentation is based on ISA 99 Committee draft documents and is subject to change.
Key messages

- Asset Owner is accountable for the cybersecurity risk of the IACS and the Equipment Under Control.
- IACS cybersecurity is a shared responsibility between Asset Owner, Product Supplier and Service Providers.
- IACS cybersecurity is required throughout the Product Security Lifecycle.
- IACS cybersecurity is required throughout the Automation Solution Security Lifecycle.
IACS Principal Roles

- **Asset owner**
  - is accountable and responsible for one or more IACSs
  - operates the IACS and the Equipment under Control

- **Product Supplier**
  - manufactures and supports an IACS hardware and/or software product

- **Service Providers**
  - Integration Service Provider (System Integrator)
    - provides system integration activities for an Automation Solution
      - design, installation, configuration, testing, commissioning and handover to the Asset Owner
  - Maintenance Service Provider (Support Provider)
    - provides support activities for an Automation Solution

- **Remember roles and organizations are different**
  - An individual or organization can have multiple roles
  - The responsibilities for a role can be split between organizations
  - The Asset Owner is responsible for documenting roles and responsibilities
Defining Industrial Automation and Control

- **Component**
  - an embedded device, host device, network device, or software application
  - e.g. field devices, PLC, historian, HMI

- **Control System (or System)**
  - the hardware and software components of an IACS
  - e.g. DCS, SIS, SCADA

- **Automation Solution**
  - a set of zones and conduits
  - an integrated set of System and Component products
  - an instance at an end user’s facility

- **Security Program**
  - People (training) and Processes (policies and procedures) to manage IACS security

- **Industrial Automation and Control System (IACS)**
  - a collection of personnel, hardware, software and policies involved in the operation of the Equipment Under Control and that can affect or influence its safe, secure and reliable operation
  - Automation Solution + Security Program
IACS Principal Roles and Responsibilities

Roles
- Asset Owner
- Maintenance Service Provider
- Integration Service Provider

IACS environment

Industrial automation and control system (IACS)
Operation and routine maintenance according to security policies and procedures

Automation Solution
- Essential functions
- Control functions
- Safety functions
- Complementary functions

Includes configured products (control systems and components)

Product Supplier

Develops and supports
Independent of IACS environment

Components
- Supporting software applications
- Embedded devices
- Network devices
- Host devices

Control systems (as a combination of components)
ISA/IEC 62443 Series
### ISA/IEC 62443 Series Details

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>TS</td>
<td>Terminology, concepts, and models</td>
<td>2007</td>
</tr>
<tr>
<td>1-2</td>
<td>TR</td>
<td>Master glossary of terms and abbreviations</td>
<td></td>
</tr>
<tr>
<td>1-3</td>
<td>IS</td>
<td>System security conformance metrics</td>
<td></td>
</tr>
<tr>
<td>1-4</td>
<td>IS</td>
<td>IACS security lifecycle and use cases</td>
<td></td>
</tr>
<tr>
<td>2-1</td>
<td>IS</td>
<td>Establishing an IACS security program</td>
<td>2009</td>
</tr>
<tr>
<td>2-2</td>
<td>IS</td>
<td>IACS security program ratings</td>
<td></td>
</tr>
<tr>
<td>2-3</td>
<td>TR</td>
<td>Patch management in the IACS environment</td>
<td>2015</td>
</tr>
<tr>
<td>2-4</td>
<td>IS</td>
<td>Security program requirements for IACS service providers</td>
<td>2018</td>
</tr>
<tr>
<td>2-5</td>
<td>TR</td>
<td>Implementation guidance for IACS asset owners</td>
<td></td>
</tr>
<tr>
<td>3-1</td>
<td>TR</td>
<td>Security technologies for IACS</td>
<td></td>
</tr>
<tr>
<td>3-2</td>
<td>IS</td>
<td>Security risk assessment for system design</td>
<td>2020</td>
</tr>
<tr>
<td>3-3</td>
<td>IS</td>
<td>System security requirements and security levels</td>
<td>2013</td>
</tr>
<tr>
<td>4-1</td>
<td>IS</td>
<td>Product security development life-cycle requirements</td>
<td>2018</td>
</tr>
<tr>
<td>4-2</td>
<td>IS</td>
<td>Technical security requirements for IACS components</td>
<td>2018</td>
</tr>
</tbody>
</table>
# IACS System Lifecycle View

## Automation Solution Security Lifecycle

<table>
<thead>
<tr>
<th>Integration</th>
<th>Operation and Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify</td>
<td>Operate</td>
</tr>
<tr>
<td>Design</td>
<td>Maintain</td>
</tr>
<tr>
<td>Implement</td>
<td>Decommission</td>
</tr>
<tr>
<td>Verify &amp; Validate</td>
<td></td>
</tr>
</tbody>
</table>

## Part 1: Terminology, Concepts and Models

- Part 1-1: Terminology, Concepts and Models

## Part 2: Establishing an IACS Security Program

- Part 2-1: Establishing an IACS Security Program
- Part 2-2: IACS Security Program Rating
- Part 2-3: Patch Management in the IACS environment
- Part 2-4: Security program requirements for IACS service providers
- Part 3-2: Security risk assessment for system design

## Part 3: Security risk assessment for system design

- Part 3-3: System security requirements and security levels

## Part 4: Product security development lifecycle requirements

- Part 4-1: Product security development lifecycle requirements
- Part 4-2: Technical security requirements for IACS components
security-related activities are adequately planned, documented and executed throughout the product’s lifecycle

user documentation is available that describes how to integrate, configure and maintain the defense in depth strategy within the product security context

security updates associated with the product are tested for regressions and made available in a timely manner

handling of security-related issues of a product that has been configured to employ its defense in depth strategy within the product security context

documentation of security capabilities of the product along with the expected security context

security has been designed into the product including a defense in depth strategy

product features are implemented securely

security testing required of a product that has been configured to employ its defense in depth strategy within the product security context

user documentation is available that describes how to integrate, configure and maintain the defense in depth strategy within the product security context

security updates associated with the product are tested for regressions and made available in a timely manner

handling of security-related issues of a product that has been configured to employ its defense in depth strategy within the product security context

security testing required of a product that has been configured to employ its defense in depth strategy within the product security context

security has been designed into the product including a defense in depth strategy

product features are implemented securely

security testing required of a product that has been configured to employ its defense in depth strategy within the product security context

user documentation is available that describes how to integrate, configure and maintain the defense in depth strategy within the product security context

security updates associated with the product are tested for regressions and made available in a timely manner

handling of security-related issues of a product that has been configured to employ its defense in depth strategy within the product security context

documentation of security capabilities of the product along with the expected security context

security has been designed into the product including a defense in depth strategy

product features are implemented securely

security testing required of a product that has been configured to employ its defense in depth strategy within the product security context

user documentation is available that describes how to integrate, configure and maintain the defense in depth strategy within the product security context

security updates associated with the product are tested for regressions and made available in a timely manner

handling of security-related issues of a product that has been configured to employ its defense in depth strategy within the product security context

documentation of security capabilities of the product along with the expected security context

security has been designed into the product including a defense in depth strategy

product features are implemented securely

security testing required of a product that has been configured to employ its defense in depth strategy within the product security context
Automation Solution Security Lifecycle

Security Program throughout the Automation Solution Lifecycle

- Specification
- Design
- Implementation
- Verification & Validation
- Operation
- Maintenance
- Decommissioning

AO: Asset Owner
PS: Product Supplier
SI: Integration Service Provider
SM: Maintenance Service Provider
AC: Accountable
AR: Responsible
CR: Contributor
ISASecure and the Security Lifecycle

- **Product Security Lifecycle**
  - Product Supplier submits products and receives certificates that their products conform to ISA/IEC 62443
    - ISASecure Security Development Lifecycle Assurance (SDLA)
    - ISASecure System Security Assurance (SSA)
    - ISASecure Component Security Assurance (CSA)

- **Automation Solution Security Lifecycle**
  - Specification phase
    - Asset Owner requires that products used in the Automation Solution have been certified to conform to ISA/IEC 62443
  - Design and Implementation phases
    - System Integrator selects products that have been certified to conform with ISA/IEC 62443
Quick Start Guide: An Overview of the ISA/IEC 62443 Series of Standards
- www.isa.org/cyberguide

Quick Start Guide: An Overview of ISASecure® Certification
- TBD

Security Lifecycles in the ISA/IEC 62443 Series
- TBD

ISA/IEC 62443—Security for Industrial Automation and Control Systems

ISASecure Product Certification
- https://ISASecure.org

ISA Training

Security PHA Review for Consequence-Based Cybersecurity

Phone: +1 919-549-8411
E-mail Address: info@isa.org