ISA-99 – Industrial Automation & Control Systems Security

Jim Gilsinn
National Institute of Standards & Technology (NIST)
Engineering Laboratory
ISA99 Committee

• Addresses Industrial Automation and Control Systems

• Compromise could result in:
  – Endangerment of public or employee safety
  – Loss of public confidence
  – Violation of regulatory requirements
  – Loss of proprietary or confidential information
  – Economic loss
  – Impact on entity, local, state, or national security
• Over 500 members
• Sectors include:
  – Chemical Processing
  – Petroleum Refining
  – Food and Beverage
  – Power
  – Pharmaceuticals
  – Discrete Part Manufacturing
  – Process Automation Suppliers
  – IT Suppliers
  – Government Labs
  – Consultants
Connecting with Others

ISA84 (Safety)

ISA100 (Wireless)

MSMUG

IEC & ISO (International)

ISCI (Compliance)
ISA-99 Work Products

- 4 Main Series
  - General
  - Policies & Procedures
  - System
  - Component

- IEC 62443 Series Matches

Current as of December 2011
ISA-99 Work Products

- Terminology, concepts and models
  - Foundational Material
  - Consistent Terminology

Current as of December 2011
ISA-99 Work Products

- Security Compliance Metrics
  - Consistent
  - Usable
  - Quantitative
  - Non-trivial
  - Measure Achieved SALs

Current as of December 2011
ISA-99 Work Products

- Establishing & Operating a Security Program
  - Asset Owner Focused
  - Non-Technical
  - Based upon ISO/IEC 27002
  - IACS-Specific Requirements & Guidance

Current as of December 2011
ISA-99 Work Products

- Patch Management
  - Applying Well-Established Practices to IACS
  - XML Schema for Patch Descriptions
ISA-99 Work Products

- Security Technologies
  - Guidance on Applying Existing Tools, Technology and Controls to IACS
ISA-99 Work Products

- Zones & Conduits
  - Defining Logical Architecture Breakdown
  - Determine Target SALs
ISA-99 Work Products

- System-Level Security Requirements
  - Technical Controls
  - IACS-Specific Requirements & Guidance
  - Specifies Capability SALs

Current as of December 2011
ISA-99 Work Products

- Product Development Lifecycle
  - Requirements for Each Development Phase
  - Building Security in From Ground Up

Current as of December 2011
## ISA-99 Work Products

### Component-Level Security Requirements

- Technical Controls
- Expand System-Level Reqs. For Individual Components
- IACS-Specific Requirements & Guidance
- Specifies Capability SALs

### General

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 62443-1-1 (Ed. 2)</td>
<td>ISA-62443.01.01 (99.01.01)</td>
</tr>
<tr>
<td>IEC/TR 62443-1-2</td>
<td>ISA-TR62443.01.02 (TR99.01.02)</td>
</tr>
<tr>
<td>IEC 62443-1-3</td>
<td>ISA-62443.01.03 (99.01.03)</td>
</tr>
</tbody>
</table>

- Terminology, concepts and models
- Master glossary of terms and abbreviations
- System security compliance metrics

Published as ISA-99.00.01-2007

### Policies & procedures

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 62443-2-1 (Ed. 2)</td>
<td>ISA-62443.02.01 (99.02.01)</td>
</tr>
<tr>
<td>IEC 62443-2-2</td>
<td>ISA-62443.02.02 (99.02.02)</td>
</tr>
<tr>
<td>IEC/TR 62443-2-3</td>
<td>ISA-TR62443.02.03 (TR99.02.03)</td>
</tr>
</tbody>
</table>

- Establishing an IACS security program
- Operating an IACS security program
- Patch management in the IACS environment

Published as ISA-TR99.00.01-2007

### System

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC/TR 62443-3-1</td>
<td>ISA-TR62443.03.01 (TR99.03.01)</td>
</tr>
<tr>
<td>IEC 62443-3-2</td>
<td>ISA-62443.03.03 (99.03.03)</td>
</tr>
<tr>
<td>IEC 62443-3-3</td>
<td>ISA-62443.03.03 (99.03.03)</td>
</tr>
</tbody>
</table>

- Security technologies for IACS
- Security assurance levels for zones and conduits
- System security requirements and security assurance levels

Published as ISA-TR99.00.01-2007

### Component

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 62443-4-1</td>
<td>ISA-62443.04.01 (99.04.01)</td>
</tr>
<tr>
<td>IEC 62443-4-2</td>
<td>ISA-62443.04.02 (99.04.02)</td>
</tr>
</tbody>
</table>

- Product development requirements
- Technical security requirements for IACS components

Current as of December 2011
IEC 62443 Document Series

- **IEC 62443-2-4**
  - Additional Document in IEC Series
  - Outside ISA99 Structure
  - Vendor Certification Requirements

Current as of December 2011
Additional Technical Working Groups

- WG7 – Security & Safety
- WG8 – Communications & Outreach
- WG9 – Wireless Security
- WG11 – Nuclear Plant Security
Applying the ISA-99 Work Products

• Several organizations using
  – Concepts as defined in ISA-99.01.01
  – Programs as defined in ISA-99.02.01
  – Zone & Conduit model
• Case studies are becoming available
• Overall, the feedback is quite good!
More Information

• ISA99 Wiki

• Contacts
  – Eric Cosman, eric.cosman@gmail.com
  – Bryan Singer, bryan.singer@kenexis.com
  – Jim Gilsinn, james.gilsinn@nist.gov

• ISA Staff
  – Charley Robinson, crobinson@isa.org