Establishing an Industrial Automation and Control Systems Security Program – An Overview of ISA-99.02.01

ISA EXPO 2008
Welcome

• Jim Gilsinn
  – Electronics Engineer
    National Institute of Standards & Technology (NIST) Manufacturing Engineering Laboratory (MEL)
    100 Bureau Drive, Stop 8230
    Gaithersburg, MD 20899-8230
    301-975-3865
    james.gilsinn@nist.gov
  – Editor, ISA-99.02.01 Standard
  – General Editor, ISA99 Committee

• Key Topics Covered
  – Introduction to ISA-99.02.01 standard
  – Update on status
## Restructuring of ISA99 Standards

<table>
<thead>
<tr>
<th>Work Group</th>
<th>Content Description</th>
<th>Previous ISA Number</th>
<th>Year</th>
<th>Revised ISA Number</th>
<th>Currently-approved IEC number</th>
<th>Proposed IEC Renumbering</th>
</tr>
</thead>
<tbody>
<tr>
<td>WG1</td>
<td>Technical report on security technologies</td>
<td>ISA–TR99.00.01</td>
<td>2007</td>
<td>ISA–99.01.02</td>
<td>IEC/TR 62443–5</td>
<td>IEC/TR 62443–1–2</td>
</tr>
<tr>
<td>WG3</td>
<td>Terminology, Concepts, and Models</td>
<td>ISA–99.00.01</td>
<td>2007</td>
<td>ISA–99.01.01</td>
<td>IEC/TS 62443–1</td>
<td>IEC 62443–1–1</td>
</tr>
<tr>
<td>WG2</td>
<td>Establishing an Industrial Automation and Control Systems Security Program</td>
<td>ISA–99.00.02</td>
<td>2008 (Est)</td>
<td>ISA–99.02.01</td>
<td>IEC 62443–2</td>
<td>IEC 62443–2–1</td>
</tr>
<tr>
<td>TBD</td>
<td>Operating an Industrial Automation and Control Systems Security Program</td>
<td>ISA–99.00.03</td>
<td>TBD</td>
<td>ISA–99.02.02</td>
<td>IEC 62443–3</td>
<td>IEC 62443–2–2</td>
</tr>
</tbody>
</table>
Introduction

- Cyber security management systems (CSMS) are nothing new to IT
  - ISO/IEC 17799 & the 27000 series
- Many organizations are looking at applying these IT security policies to industrial automations for a variety of reasons
  - Asset protection
  - Corporate policies
  - Government or industry regulations
- IT security policies cannot be applied blindly to industrial automation and control systems without understanding the risks
  - Risk analysis is a common process for industrial systems
  - The same diligence needs to be applied to the cyber security program
  - Work with entire organization to develop CSMS
- Absolute security is not really desirable
  - Locking things down to the point of being unusable is not necessary
  - Understanding the balance between risk and cost is important
Overall CSMS Architecture

- CSMS broken down into:
  - Categories
  - Element Groups
  - Elements

- Elements are not sequential
  - Some elements rely on parts of other elements
  - Many parts can be developed independently

- Document organization
  - Clauses define requirements
  - Annexes provide guidance on how to develop requirements
CSMS Category: Risk Analysis

- Description
  - Look at the risks associated with the industrial automation and control systems and analyze where those risks can be reduced by adding cyber security countermeasures
  - Provide background information and justification for CSMS

- Similar to other risk analysis processes
  - Many risk analyses may have already been conducted for financial, health, safety and environmental reasons
  - These risk analyses can feed into the cyber security risk analysis
CSMS Category: Addressing Risk with the CSMS

- **Description**
  - Requirements and guidance for developing and implementing the cyber security management system

- **Security policy, organization and awareness**
  - Basic security policies
  - Organizations responsible for cyber security
  - Awareness of cyber security within the organization

- **Selected security countermeasures**
  - Policies, procedures and practices related to some security countermeasures
  - Not an exhaustive list

- **Implementation**
  - Issues related to implementing the CSMS
CSMS Category: Monitoring and Improving the CSMS

- **Description**
  - Ensure that the CSMS has been implemented correctly
  - Ensure that the CSMS meets the expected goals
- Monitoring and improving do not seem to apply to establishing a program
  - Mechanisms to feedback changes into the CSMS need to be established
Status Update

- **Third Voting Draft**
  - September 2008
- **Second Voting Draft**
  - September 2007
  - 25 approval, 1 disapproval
  - 61% approval, enough votes to pass
  - 260 comments received from 17 reviewers
  - 106 technical, 86 editorial, 68 general comments
- **First Voting Draft**
  - April 2006
  - 19 approval, 2 disapproval
  - 46% approval, not enough votes to pass
  - 248 comments received from 16 reviewers
  - 130 technical, 77 editorial, 41 general comments
Review of Key Points

• Organizations are trying to apply cyber security to industrial automation and control systems
  – Do not apply IT programs blindly to IACS systems
  – Work with entire organization to develop CSMS
• Developing a CSMS program can be broken down into pieces
  – Many pieces can be developed in stages
• ISA-99.02.01 near completion
  – Has passed full committee voting
  – Finalizing comment resolution before publication
Q & A

- Tom Good
  ISA99, Working Group 2 Chair
  thomas.d.good@usa.dupont.com

- Jim Gilsinn
  ISA-99.02.01 Editor
  james.gilsinn@nist.gov

- Charley Robinson
  ISA Staff
  crobinson@isa.org