Cybersecurity for Smart Manufacturing Systems

World Manufacturing Forum 2014
Milan, Italy

Keith Stouffer
Project Leader,
Cybersecurity for
Smart Manufacturing
Systems, NIST

July 2, 2014

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

ICS Security Standards and Guidelines Strategy

- Add control systems domain expertise to:
  - Already available Information Security Risk Management Framework
  - Provide workable, practical solutions for manufacturing control systems – without causing more harm than the incidents we are working to prevent
- This expertise takes the form of specific cautions, recommendations & requirements for application to control systems - throughout both technologies and programs
  - NIST SP 800-82 *Guide to Industrial Control System (ICS) Security*
  - ISA/IEC 62443 Industrial Automation & Control Systems Security

NIST SP 800-82

- Guide to Industrial Control Systems Security
  - Provide guidance for establishing secure ICS, including implementation guidance for NIST SP 800-53 security controls
- Content
  - Overview of ICS
  - ICS Risk Management and Assessment
  - ICS Security Program Development and Deployment
  - ICS Security Architecture
  - Applying Security Control to ICS
  - Threat Sources, Vulnerabilities and Incidents
  - Current Activities in Industrial Control Systems Security
  - ICS Security Capabilities and Tools
  - ICS Overlay for NIST SP 800-53, Rev 4 security controls
- Downloaded over **2,500,000** times since 2006 initial release and is heavily referenced by the public and private ICS security community worldwide

Major ICS Security Objectives

- **Restrict logical access to the ICS network and network activity**
  - Demilitarized zone (DMZ) network architecture
  - Separate authentication mechanisms and credentials for users of the corporate and ICS networks.
  - Network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restrict physical access to the ICS network and devices**
  - Unauthorized physical access to components could cause serious disruption of the ICS's functionality.
  - Combination of physical access controls should be used, such as locks, card readers, and/or guards.

Major ICS Security Objectives

- **Protect individual ICS components from exploitation**
  - Deploy security patches in as expeditious a manner as possible
  - Disable unused ports and services
  - Restrict ICS user privileges to only those that are required
  - Tracking and monitor audit trails
  - Implement antivirus and file integrity checking software where feasible to prevent, deter, detect, and mitigate malware
- **Maintain functionality during adverse conditions**
  - Design ICS so that critical components have redundant counterparts
  - Component failure should not generate unnecessary traffic on the ICS or other networks, or should not cause another problem elsewhere, such as a cascading event
- **Deploy security solution based on potential impact**
  - Not a one size fits all solution

Low Impact System

ICS Impact Level Examples

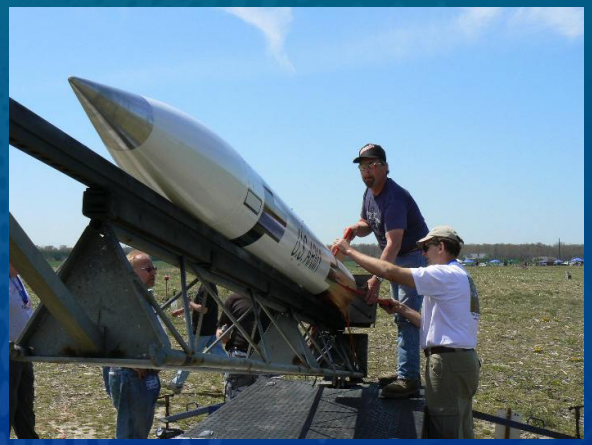
- Low Impact ICS
  - **Product Examples:** Non hazardous materials or products, Non-ingested consumer products
  - **Industry Examples:** Plastic Injection Molding, Warehouse Applications
  - **Security Concerns:** Protecting people, Capital investment, Ensuring uptime

Moderate Impact Systems

ICS Impact Level Examples

- Moderate Impact ICS
  - **Product Examples:** Some hazardous products and/or steps during production, High amount of proprietary information
  - **Industry Examples:** Automotive Metal Industries, Pulp & Paper, Semi-conductors
  - **Security Concerns:** Protecting people, Trade secrets, Capital investment, Ensuring uptime

High Impact System



High Impact System !!!

ICS Impact Level Examples

- High Impact ICS
  - **Product Examples:** Critical Infrastructure, Hazardous Materials, Ingested Products, Military components
  - **Industry Examples:** Utilities, Petrochemical, Food & Beverage, Pharmaceutical, Defense
  - **Security Concerns:** Protecting human life, Ensuring basic social services, Protecting environment

World Record High Impact System ☺

NIST SP 800-82, Rev 2 Schedule

- International public comment period on NIST SP 800-82, Rev 2 Initial Public Draft is May 15 – July 18, 2014
- Final Public Draft expected September 2014 – 30 day comment period
- NIST SP 800-82, Rev 2 expected to be final by end of 2014

ISA99 Committee

- The International Society of Automation (ISA) Committee on Security for Industrial Automation & Control Systems (ISA99)
  - 500+ members
  - Representing companies across all sectors, including:
    - Chemical Processing
    - Petroleum Refining
    - Food and Beverage
    - Energy
    - Pharmaceuticals
    - Water
    - Manufacturing

Copyright © ISA

ISA99 and ISA/IEC 62443

- ISA/IEC 62443 is an international series of standards for ICS cybersecurity
- Being Developed by 3 Groups
  - ISA99 → ANSI/ISA-62443
  - IEC TC65/WG10 → IEC 62443
  - ISO/IEC JTC1/SC27 → ISO/IEC 2700x

Copyright © ISA

The ISA/IEC-62443 Series

General

ISA-62443-1-1	ISA-TR62443-1-2	ISA-62443-1-3	ISA-TR62443-1-4
Terminology, concepts and models	Master glossary of terms and abbreviations	System security compliance metrics	IACS security lifecycle and use-case

Published as ISA-99.00.01-2007

Policies & procedures

ISA-62443-2-1	ISA-TR62443-2-2	ISA-TR62443-2-3	ISA-62443-2-4
Requirements for an IACS security management system	Implementation guidance for an IACS security management system	Patch management in the IACS environment	Requirements for IACS solution suppliers

Published as ISA-99.02.01-2009

System

ISA-TR62443-3-1	ISA-62443-3-2	ISA-62443-3-3
Security technologies for IACS	Security levels for zones and conduits	System security requirements and security levels

Published as ISA-TR99.00.01-2007

Component

ISA-62443-4-1	ISA-62443-4-2
Product development requirements	Technical security requirements for IACS components

Copyright © ISA

NIST ICS Cybersecurity Testbed

- Goal of the testbed is to measure the performance of ICS when instrumented with cybersecurity protections in accordance with practices prescribed by national and international standards and guidelines such as ISA/IEC 62443 standards and NIST SP800-82
- Research areas include
  - Perimeter network security
  - Host-based security
  - User and device authentication
  - Packet integrity and authentication
  - Encryption
  - Zone-based security
  - Field bus (non-routable) protocol security
  - Robust/ fault tolerant systems
- Research outcomes will provide guidance to industry on best practices for implementing cybersecurity standards and guidelines without negatively impacting ICS performance

Testbed Scenarios

- Continuous Processes
  - Chemical Processing
  - Oil & Gas Refinery
- Advanced Discrete Processes
  - Dynamic Robotic Assembly
  - Additive Manufacturing
- Distributed Operations
  - Smart Transportation
  - Smart Grid
  - Gas and Water Pipelines

Key Takeaway

- The most successful method for securing an ICS
  - Engage in a proactive, collaborative effort between
    - Management
    - Controls engineers and operators
    - IT organization
    - Trusted automation advisor
  - This team should gather industry recommended practices and draw upon the wealth of information available from ongoing government, industry group, vendor and standards organizational activities

Contact Info

Keith Stouffer

+1-301-975-3877
keith.stouffer@nist.gov

Engineering Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8230
Gaithersburg, MD 20899-8230 USA