ISA Standards Program
- Over 55 years of standards development
- Over 100 committees and 3,000 volunteers
- Over 33,000 members worldwide
  - Available pool of technical expertise
- ANSI accreditation to produce American National Standards
  - Committee method
  - canvass method
ISA Standards Program (cont.)

- **Types of standards publications:**
  - Standards
  - Draft Standards for Trial Use
  - Technical Reports
  - Recommended Practices
  - Online material

- **ISA holds 3 international IEC Secretariats**

- **ISA administers 8 US Technical Advisory Groups**
SP-99: security
SP-99, Manufacturing and Control Systems Security

- First face-to-face meeting at ISA Expo, October 2002
- 243 participants, 48 contributing/voting (max one vote per company)
- Two published technical reports
- Four standards in preparation
SP-99 Scope: A Broad View

- ISA has taken a broad view:
  - Based on function, not industry or type of control

- Includes
  - SCADA/EMS
  - DCS
  - PLCs
  - RTUs/IEDs
  - Transmitters, meters, control valves, enterprise wide HMIs, …
  - Enterprise applications, to the extent they can affect control

- Not limited to one or a few industries or technologies
  - In other words, a very broad encompassing definition
Scope of Security Standards

Purdue reference Model Levels

Level 5
- Company Management Data Presentation
- Company Production Assignment Scheduling Supervision
- Company Management Information
- Company Production Scheduling Assignment

Level 4
- Operational & Production Supervision
- Production Scheduling & Operational Management

Level 3
- Supervisor’s Console
- Inter-Area Coordination

Level 2
- Supervisor’s Console
- Supervisory Control

Level 1
- Operator’s Console
- Direct Digital Control
- Controllers
- Process

IT Security Policies and Practices (ISO 17799)
Mfg Security Policies and Practices (ISA 99)
Process Safety (ISA 84, IEC 61508, IEC 61511)
Common technologies, policies and practices
SP-99: Published Technical Reports


Technical Report 1 – Technologies

Security Technologies for Manufacturing and Control Systems

Approved 11 March 2004
TR99.00.01–2004, Security Technologies for Manufacturing and Control Systems

Technology areas:

- Authentication and Authorization
- Filtering/Blocking/Access Control
- Encryption and Data Validation
- Audit, Measurement, Monitoring and Detection Tools
- Computer Software
- Physical Security
Role Based Authorization Tools
Password Authentication
Challenge Response Authentication
Physical/Token Authentication
Smart Card Authentication
Biometric Authentication
Location Based Authentication
Password distribution and Management Technologies
Device to Device Authentication
TR99.00.01 Filtering/Blocking/Access Control

- Dedicated Firewalls (Hardware Based)
- Host-based Firewalls (Software Based)
- Virtual Local Area Networks (VLANs)
TR99.00.01 Encryption Technologies and Data Validation

- Symmetric (Private) Key Encryption
- Public Key Encryption and Key Distribution
- Virtual Private Networks (VPNs)
- Digital Certificates
TR99.00.01 Audit, Measurement, and Monitoring and Detection Tools

- Log Auditing Utilities
- Virus/Malicious Code Detection
- Intrusion Detection Systems
- Network Vulnerability Scanners
- Network Forensics and Analysis Tools
- Host Configuration Management Tools
- Automated Software Management Tools
TR99.00.01 Computer Software

- Sever and Workstation Operating Systems
- Real-time and Embedded Operating Systems
- Web and Internet Technologies
TR99.00.01 Physical Security Controls

- Physical Protection
- Personnel Security
Technical Report 2 – Programs

Integrating Electronic Security into the Manufacturing and Control Systems Environment

Approved 12 April 2004
Contents
- Developing a Program
- Defining Risk Goals
- Assessing and Defining Existing System
- Conducting Risk Assessment and Gap Analysis
- Design or Select Countermeasures
- Procure or Build Countermeasures
- Define Component, Integration, Post Installation Test Plans
- Test Components, Integration, and System
Contents (cont.)

- Finalize Operational Security Measures
- Routine Reporting and Analysis
- Periodic Audit and Compliance
- Reevaluation
- Working with suppliers and consultants
- Working with industry
- References
- Annex A – Sample Policies and Procedures
Security lifecycle from TR99.00.02

1. Define Risk Goals
2. Assess & Define Existing System
3. Conduct Risk Assessment & Gap Analysis
4. Design or Select Countermeasures
5. Procure or Build Security Countermeasures
6. Define Component Test Plans
7. Test Countermeasures
8. Define Integration Test Plan
9. Perform Pre-Integration test
10. Define System Validation Test Plan
11. Installation and Perform Validation test on installed system
12. Finalize Operational Security Measures
13. Routine Security Reporting and Analysis
14. Periodic Audit And Compliance Measures
15. Reevaluate Security Countermeasures (Break-in or Major Plant Change)

System goes operational here
SP-99 Standards (in preparation)

Manufacturing and Control Systems Security –

- Part 1: Models and Terminology
- Part 2: Establishing a Manufacturing and Control System Security Program
- Part 3: Operating a Manufacturing and Control Systems Security Program
- Part 4: Specific Security Requirements for Manufacturing and Control Systems
SP99.01 – Part 1: Models and Terminology

- Definitions of Manufacturing and Control Systems security terms
- Description of the terminology used in security as it applies to Manufacturing and Control Systems
- A Common Model for specifying security requirements for Manufacturing and Control Systems program
- A reference architecture for describing the security environment
Summary of SP99 activities

- SP99 has published significant guidance on:
  - Unique needs of control systems
  - Improving security in control systems

- SP99 is continuing to expand and update this guidance

- SP99 is now developing standards for terminology, models and programs
SP-100: wireless
SP-100, Wireless Systems for Automation

- Organizational meeting at ISA Expo, October 2004
- First official face-to-face at ISA Expo, October 2005
- 49 participants, 26 contributing/voting
  (max one vote per company)
- Outgrowth of DOE Wireless Sensors development program
  - Three DOE contractors: Eaton, GE, Honeywell
- Four studies / reports underway in SP-100
SP-100 studies / reports

- Physics of Radio
- Requirements
- Interoperability of Sensor Networks
- Users Guide
Taxonomy of use of wireless automation networks

- **Monitoring group**
  - Class 5: Logging
    *No immediate operational consequence*
    (e.g., history collection, SOE, preventive maintenance)
  - Class 4: Flagging
    *Short-term operational consequence*  
    (e.g., event-based maintenance)

- **Control group**
  - Class 3: Open loop control
    (human in the loop)
  - Class 2: Closed loop supervisory control
    (non-critical)
  - Class 1: Closed loop regulatory control
    (often critical)

- **Safety group**
  - Class 0: Emergency action
    (always critical)

- **Alarms**
  - Any class
    (human or automated action)

- **Wireless worker**
  - Class 3 – 5
    (access may be proxied)
Required security functionality
(from new IEC NP+CD titled “SECURITY FOR INDUSTRIAL PROCESS MEASUREMENT AND CONTROL – Network and system security”)

- Device identity
- Session endpoint authentication and authorization
- Message integrity
- Message source (and source set) authentication
- Message freshness and ordering
- Message timeliness
- Message data confidentiality
  - Semantic security to conceal relationships between messages
Recommended Key Management Functionality

- **Specialized key center**
  - Centralized key management
  - Separate data keys for unicast pairings and multicast groups identified from the automation system’s configuration
  - Support for key escrow, deep inspection firewalls and NIDS
  - Can be outsourced (remote from automation site)

- **Initial symmetric key establishment via plant-issued**
  - public key certificates, or
  - “resurrecting duckling” out-of-band bootstrap key injection

- **Frequent rekeying or key update of all comm. keys**
  - Daily rekeying / key update recommended
Cryptography in wireless field devices

- Devices designed to meet Intrinsic Safety standards
  - Peak instantaneous power $\leq 100$ mW

- 3 yr battery life requires duty cycles of 1% to 0.1%

- Typical microcontroller: TI MSP430

- Extensive use of multicast communications, complicating authentication of message sources

- Cryptography is dominant compute-power load

- Urgent need for resource-sparing single-pass authenticated encryption with associated data (AEAD)
Thank you!

Contact information:
Tom Phinney (tom.phinney@honeywell.com)
Honeywell  ms: N21
2500 W. Union Hills Dr
Phoenix, AZ  85027-5139  USA
+1 (602) 313-5989 (desk)

Questions?