

# **Security Standards:**

## **Those Available Today and Future Directions**

**October 4, 2004**

**Houston, TX**

Session Developer:

**Bryan L Singer**

Chairman, ISA SP-99  
Rockwell Automation

[blsinger@ra.rockwell.com](mailto:blsinger@ra.rockwell.com)



# Introductions

- Bryan L Singer – Chairman ISA SP-99, Rockwell Automation
- Joe Weiss – Member, ISA SP-99 Kema Consulting, IEEE, IEC, ISA
- Dick Oyen, Member ISA SP-99, ABB

# Agenda

- Introductions – Bryan Singer
- Purpose behind industry standards – Bryan Singer
- Brief overview of available standards bodies, what do they have to offer? Bryan Singer, Dick Oyen
- Impact of standards in the industry – Joe Weiss
- Future Directions of Standards – Bryan Singer, Dick Oyen
- Panel Discussion/Q&A - All

# Ground Rules

- Speakers will present information, a panel discussion at the end of the presentation will be provided for Q&A
- Comments are welcome and encouraged, during the panel discussion
- Keep comments and discussion as short and concise as possible

# Purpose Behind Industry Standards

- Provide a common means by which vendors and customers can communicate
- Reduce complexity of implementing security
- Capitalize on the best guidance available in the industry
- Reduce industry-wide risk

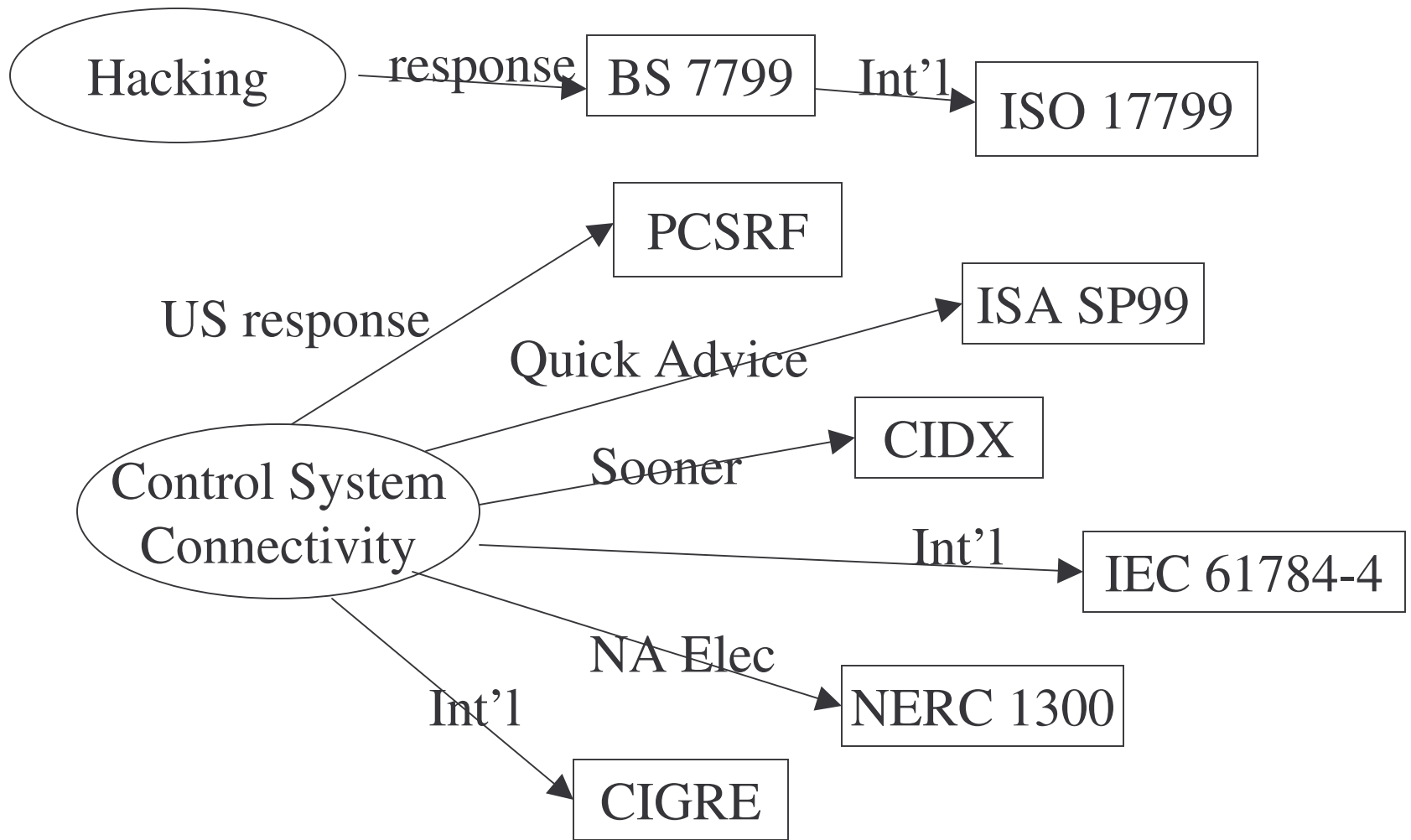
# Available Standards – Current State

- Most so far are of a “guidance” nature
- Some describe technical architectures
- Very formative stages
- Government groups are closely monitoring standards work while working on their own guidance
- Standards bodies such as ISA are publishing industry non-specific guidance, and relying on industry specific groups (e.g. CIDX) to extend their information to specific industries

# Available Standards and Industry Bodies

- ISA SP-99
- NIST PCSRF (Process Control Security Req's Forum)
- IEC (65C WG's)
- ANSI
- IEEE (Various technical standards)
- ISO (ISO 17799, BS 7799, BS 7799-2)
- CIDX
- Regulatory (food bioterrorism, 21CFR 11)
- Government (DHS)

# A Quick History



# ISO 17799

- Standard of ISO/IEC JTC1 SC27
- Domain: IT Security
- No control system considerations
- “Should”
- Mature in 2000

<http://www.iso-17799.com/>

# ISO 17799 Content

- **Policy:** management direction and support
- **Organization:** establish org to manage security
- **Assets:** account for assets
- **Personnel:** screening and training
- **Physical:** premises
- **System Operations:** security procedures, incident response
- **Access:** information dissemination and alteration
- **Development:** security designed into the system
- **Continuity:** avoid or counteract business interruption
- **Compliance:** statutory, regulatory, contractual

# PCSRF

## Process Control Security Requirements Forum

- Sponsored by (US) NIST
- Domain: Control System Security
- New products and systems
- Follows Common Criteria (ISO 15408)
- “Shall”
- April 2004
  - SPP-ICS Version 1.0  
“System Protection Profile – Industrial Control System”
- Next
  - SCADA Protection Profile
  - Other protection profiles

# PCSRF SPP-ICS Comparison

	PCSRF SPP-ICS
Policy	
Organization	
Asset	X
Personnel	
Physical	
System Operations	X
Access	X
Development	X
Continuity	
Compliance	
<b>Ctrl Sys Oriented</b>	X
<b>Products</b>	X

\* Preliminary Comparison

# ISA SP99

## Manufacturing and Control System Security

- Scope
  - Multi-industry
  - Multi-national
- Focus
  - Recommend practices first, then write standard
  - Pertains to existing (and new) plant systems
- April 2004
  - Issued reports TR99.00.01 and 02
- 2005
  - Draft parts 1 & 2 of the standard

# Report TR99.00.01

## Security Technologies for Manufacturing and Control Systems

- Technology areas:
  - Authentication, Authorization
  - Filtering/Blocking/Access Ctrl
  - Encryption & Validation
  - Audit, Measure, Mon, Detect
  - Software
  - Physical
- for each technology:
  - Vulnerabilities addressed
  - Typical deployment
  - Known issues and weaknesses
  - Use in control systems
  - Future directions
  - Recommendations

# Report TR99.00.02

## Integrating Electronic Security into the Manufacturing and Control Systems Environment

- Developing a Security Program
- Define Risk Goals
- Assess and Define Existing Systems
- Design or Select Countermeasures
- Procure or Build Countermeasures
- Conduct Risk Assessment and Gap Analysis
- Testing
- Finalize Operational Security Measures
- Routine Security Reporting and Analysis
- Periodic Audit and Compliance
- Reevaluate Security Countermeasures

# ISA SP99 Standard

## ■ Part 1

- Assets
- Policy
- Risk
- Reference Model
- Physical Models
- Functional Models
- Zones - Conduits
- Countermeasures

## ■ Part 2

- Will derive from TR99.00.02
- And add material
- Programmatic aspects of security

## ■ Part 3

- Running and Maintaining a Security Program
- Scheduled to begin next year

## ■ Part 4

- Technical standard for specifying precise relationship between security requirements and controls
- Common reference for vendors and end-users

# ISA SP99 Standard Comparison

	ISA SP-99
Policy	X
Organization	X
Asset	X
Personnel	
Physical	
System Operations	X
Access	X
Development	
Continuity	X
Compliance	X
Ctrl Sys Oriented	X
Products	
<b>Risk Analysis</b>	X

\* Preliminary Comparison

# IEC 65C WG13

- International Electro-technical Commission (IEC)
  - Industrial-Process Measurement and Control (TC65)
    - Digital Communications (SC65C)
      - Cyber Security (WG13)
- Domain: Manufacturing and Control System Security
- Will take ISA SP99 as Publicly Available Specs
- 2004-2007
  - 61784-4 “Profiles for secure communications in industrial networks”
    - A Fieldbus Profile

# IEC 61784-4 Content - PRELIMINARY

- Reference model
  - Guidance on threat and consequence analysis
  - Communication security system level requirements
  - Profiles
    - Inter-control center
    - Corporate intranet
    - Upper level network within a control center
    - Remote operation through the Internet or corporate Intranet
    - Dial-up remote access
    - Lower levels within the control center
  - Case studies and other supporting analysis
-

# IEC 61784-4 Comparison

	IEC 61784-4
Policy	
Organization	
Asset	X
Personnel	
Physical	
System Operations	
Access	X
Development	
Continuity	
Compliance	
Ctrl Sys Oriented	X
Products	
Risk Analysis	

\* Preliminary Comparison

# CIDX

- Chemical Industry Data Exchange
- 2004
  - Interests similar to other groups
  - Members take leadership roles in other groups

<http://www.cidx.org/>

# NERC 1300

North American Electric Reliability Council

- Domain: Electric generation and transmission – control system security
- Region: Canada and US
- “Levels of Noncompliance”
- 2003
  - Standard 1200
- Current
  - 1300 Draft for review through 1 Nov 2004

# NERC 1300 Content

- Security Management Controls
  - Critical Cyber Assets
  - Personnel & Training
  - Electronic Security
  - Physical Security
  - Systems Security Management
  - Incident Response Planning
  - Recovery Plans
-

# NERC 1300 Comparison

	NERC 1300
Policy	X
Organization	
Asset	X
Personnel	X
Physical	X
System Operations	
Access	X
Development	
Continuity	X
Compliance	
Ctrl Sys Oriented	X
Products	
Risk Analysis	

\* Preliminary Comparison

# CIGRE

- International Council on Large Electric Systems (CIGRE)
- Started in Europe, now world-wide
- Decided to observe and participate in ISA SP99

# Comparison

	ISO 17799	PCSRF SPP-ICS	ISA SP99 std	IEC 61784-4	NERC 1300
Policy	X		X		X
Organization	X		X		
Asset	X	X	X	X	X
Personnel	X				X
Physical	X				X
System Operations	X	X	X		
Access	X	X	X	X	X
Development	X	X			
Continuity	X		X		X
Compliance	X		X		
Ctrl Sys Oriented		X	X	X	X
Products		X			
Risk Analysis			X		

\* Preliminary Comparison

# A Word from the Sponsor

## ISA SP99 WG7

- Liaison working group
  - Identifies specific liaisons: person \* organization
  - Database of Control System Standards Related Organizations
  - Coordinates Standards Comparison Efforts

Many control system users, vendors, and the public would benefit from a coherent set of standards.

# Conclusion

Several control system security standards are evolving

- The differences are issues of “Frame of Reference”
  - Industries
  - Associations
  - Standards methodologies
  - Rigor
- The similarities are the set of security issues
- The similarities are much more significant than the differences

# NERC Cyber Security Standards

- 1200
  - Control center only
    - 16 tasks
  - No detailed metrics
  - No penalties
  - Self-certification
  
- 1300
  - Control Center, Power Plants, and Substations
    - Any power plant participating in market
    - 8 tasks
  - Detailed metrics
  - Penalties
  - Audits

# Implementation Schedule

- In draft
- Frequently Asked Questions available
- Comments due November 1
- Expectation is Standard final by 8/05

# 1300 – Cyber Security

- 1301 Security Management Controls
- 1302 Critical Cyber Assets
- 1303 Personnel & Training
- 1304 Electronic Security
- 1305 Physical Security
- 1306 Systems Security Management
- 1307 Incident Response Planning
- 1308 Recovery Plans

# Applicability

- Power plant control systems
  - Except nuclear plants
- Dial-up modems
- Routable protocols
  - Not control system protocols

# Hardware

- None required, but firewalls and intrusion detection implied

# References

- NIST Firewall and Intrusion Detection standards
- Not included
  - Northeast Blackout Final Report\*
  - ISA SP99

\*Several recommendations beyond 1300

# Expected Tough Issues

- Electronic Security Perimeter
- Periodic assessments
  - Potential unintentional impacts
- Background checks
- Security Policies
- Event identification/Disclosure
- Recovery Plans

# Recommendation

- Be prudent!
  - Prudent design will make you more reliable and secure as well as meet the intent of 1300



# Panel Discussion