

Industrial Systems Security

Gary Rathwell

November 24, 2006

Topics

- Introduction
- What are ISA S99 & IEC 62443
- What other standards groups are relevant
- Summary

Introduction – Gary Rathwell

- President, [Enterprise Consultants, Inc.](#) (ECI)
- Long experience in Industrial Controls & Telecom
 - Fluor - Functional Leader of Controls and Automation
 - H.A. Simons – Director, Mill Wide Systems
 - ICI and Texaco Manager process control and optimization
- Proponent of [PERA](#) (Purdue Enterprise Reference Architecture) Architecture and Master Planning
 - Lead more than 12 large master planning studies
 - Contributed to many more smaller plans & studies
- Member of S95, S99 and IEC TC184 Standards Teams.
- Author of many engineering tools and standards.

What are ISA S99 and IEC 62443 ?

- [ISA S99](#) – guidance documents and standards on security of industrial control and automation Systems
 - Part 1 – Defines terms and models used in automation security
 - Part 2 – Establishing Cyber Security Management Systems
 - Part 3 - Operating a Security Program
 - Part 4 - Specific Security Requirements for Control Systems
- [IEC 62443](#) – mainly addresses technical aspects of system security architecture

What is the Threat ?

- Terrorists, Hackers and Organized Crime Threats
- Must defend against both internal and external threats
 - For small companies most threats are external
 - For large companies most threats are internal

What kind of Attacks Have Occurred?

- Nuclear Plant shutdown (virus)
- Massive release of human sewage (malicious employee)
- Shutdown of major US airport (technical and contract failure)
- Many banking system breaches (many more not publicized e.g. Russia in 1999)
- Tests of North American Power grid showed many openings.

What has changed?

- Hackers, Terrorists and Organized Crime are becoming more sophisticated.
- Increased use of Standardized LANs and Operating Systems in ICD mean many more people know how to attack them
- Wireless technologies present major new challenges
- 911 and increased terrorist activity

Why is a Security Standard Needed ?

- Need to have a standard to audit against
- Need standards to train next generation of engineers.
- Need standards so security products can work compatibly together.

Example Security Policies

- No non-critical applications in ICD
- Eliminate unstructured applications
 - e.g. email
- Eliminate communication access points
 - e.g. maintenance dial-ins
- Single point of control
 - every new application adds vulnerabilities
 - Must be auditable

What Security Practices are Needed ?

- Manufacturing organizations need ICD (Industrial Control Domain) policies and effective implementation
- A well-documented and managed Corporate Control and Information Systems architecture, particularly for the ICD
- If processes are critical or dangerous, need a regular audit of ICD security
- The Firewalls between MES & ICD and MES and IT must be very carefully designed, managed, and audited.
- If ICD links traverse external networks, require secure VLAN and monitoring.
- Medium to large companies may require a secured Industrial Data Center where MES and SCADA systems reside.

Why Can't Existing Information Systems Standards be Used for ICD Security ?

- Authentication and Authorization Technologies
 - Operator's ability to recall and enter a password may be impacted by the urgency of the situation
- Filtering/Blocking/Access Control Technologies
 - Adds delay to control system communications
 - Lack of firewall products for non-IP based protocols
- Encryption Technologies
 - Slows down communication as additional time is required to encrypt, decrypt, and authenticate messages
- Auditing Tools
 - Many legacy control devices don't have logs

ISA S99 Standard

Part 1 - Models & Terminology

- Theme
 - Establish the scope and define terminology
- Typical Questions Addressed
 - What is a control system?
 - How is it different from a typical business system?
 - What are the different levels of data confidentiality for control systems applications?
 - How can these levels be established?
 - What are the key security terms and concepts and how are they defined in this context?

Part 1 - Models & Terminology

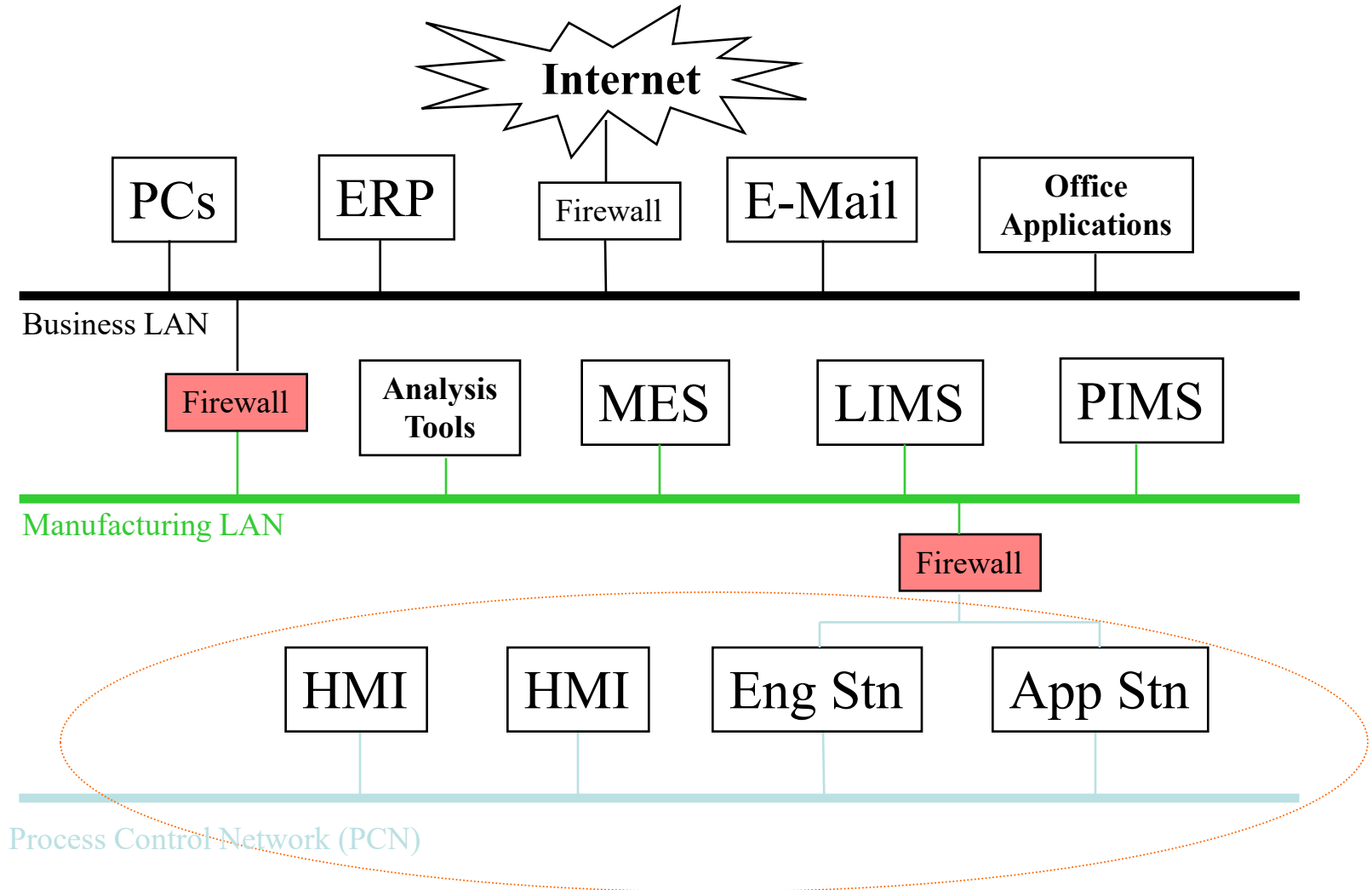
- References

- Purdue CIM Reference Model
- ISA S84 – Safety Instrumented Systems
- ISA S88 – Batch Control
- ISA S95 – Enterprise- Control Systems Integration

- Models

- Identify threats and vulnerabilities
- Classify assets
- Define architectural boundaries and information flows
- Define security policy

Part 1 Application Example



Part 2 - Establishing a Security Program

- Theme

- Give practical guidance and direction on how to establish business case for a security program and how to design the program to meet business needs.

- Typical Questions Addressed

- How to make a business case for security in Manufacturing & Control Systems environment?
- What is the step-by-step process for building such a program?
- What skills and organizations should be involved?

- Proposed Timeline

- First committee vote expected in July 2005

Part 3 - Operating a Security Program

- Theme

- Details of how a program is run after it is designed and implemented

- Typical Questions Addressed

- What should the short-term and long-term responsible organization look like?
- What do I do when the project team goes away?
- How do I keep a program relevant and effective in the face of changing technology and business needs?
- How do I work effectively with my IT and audit organizations?

- Proposed Timeline

- First Draft December 2005

Part 4 – Specific Security Requirements for Control Systems

- Theme
 - Focus on those operational and design requirements that set apart manufacturing and control systems from IT systems
- Typical Questions Addressed
 - What is so special about the Manufacturing and Controls Environment that it requires a different response and design?
- Timeline
 - First Draft March 2006

Other Groups Working in this Area

- The National Strategy to Secure Cyberspace published in Feb. 2003
- DHS Initiatives (Fact Sheet – Published Feb. 2005)
 - Established the US Computer Emergency Readiness Team (CERT) Control Systems Center
 - Established, the Control Systems Security and Test Center (CSSTC) in conjunction with Idaho National Environmental and Engineering Laboratory
 - Launched a new Process Control Systems Forum as a joint effort between National Cyber Security Division (NCSD) and Science & Technology (S&T) Directorate
- Other Standards Organizations
 - IEC, NERC, NIST, CIDX and several others

Other Groups Working in this Area

- ISA Working Group 7

- Proactively seeks partnerships and coordinate activities with pertinent outside groups
- Participate in meetings of outside organizations, as well as monitor progress and review published documents
- Report back to ISA areas of overlap and viewpoints that are either cooperative or conflicting

- Organizations

- DHS (Department of Homeland Security)
- IEC (International Electrotechnical Commission)
- NIST PCSRF (Process Control Security Requirements Forum)
- CIDX (Chemical Industry Data eXchange)
- NERC (North American Electric Reliability Council)
- Other standards organizations

Summary

- Rapidly increasing industrial systems integration market.
- Complexity and risks are also increasing
- S95 represents the ONLY efficient way to implement links between automation, MES and ERP (e.g. SAP etc.)
- S99 and Security architectures are essential at all enterprise levels.
- Failures have legal implications if best technology was not applied