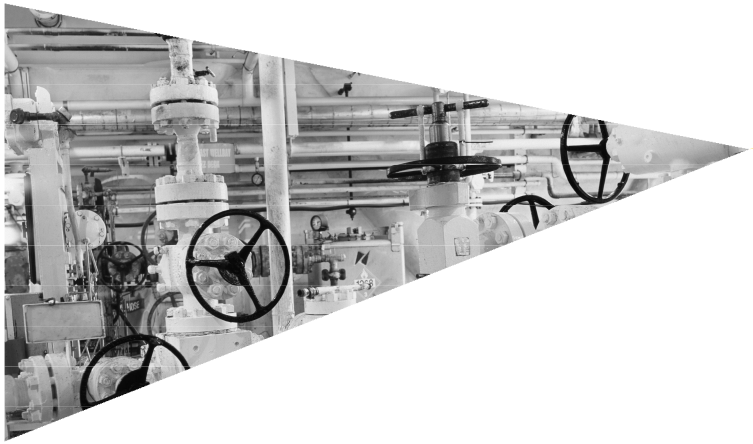
ISACA rudens konference

8 Novembris 2012



Procesa kontroles sistēmu drošība

Andris Lauciņš

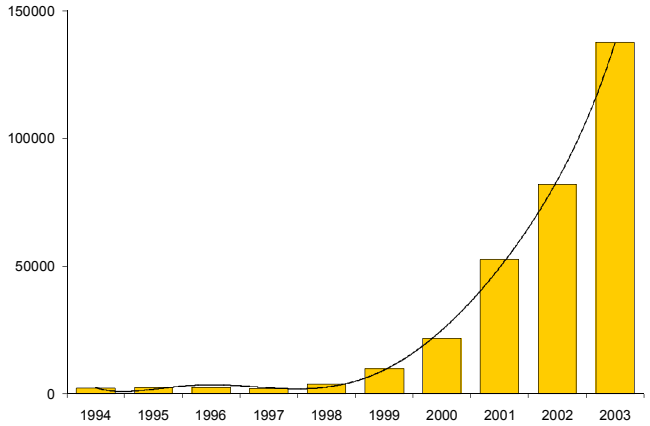
Ernst & Young
Quality In Everything We Do

Ievads – Kāpēc tēma par procesa kontroles sistēmām?

Ernst & Young
Quality In Everything We Do

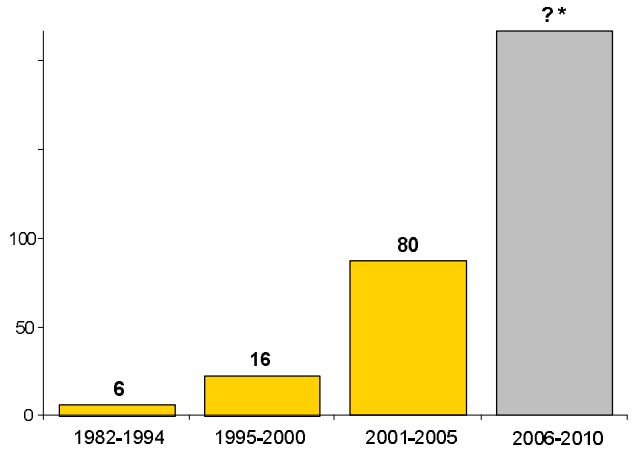
Statistics on incidents

Reality of the environment of industrial control systems:	Historically	Present
► ensuring high reliability and operationality	✓	✓
► Usa of dedicated, closed technology, inaccessible for public	✓	✗
► Operated by individuals with unique knowledge of these types of systems	✓	✗
► Phisical isolation of the industrial control network from external networks	✓	✗



Number of incidents reported to CERT/CC in the years 1994–2003

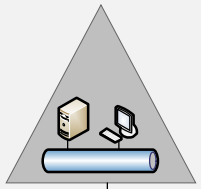
Source: CERT/CC, 2003



Number of occurrences affecting security of critical infrastructure supervision systems (SCADA)

Source: Security incidents and trends in SCADA and process industries, The Industrial Ethernet Book, May 2007

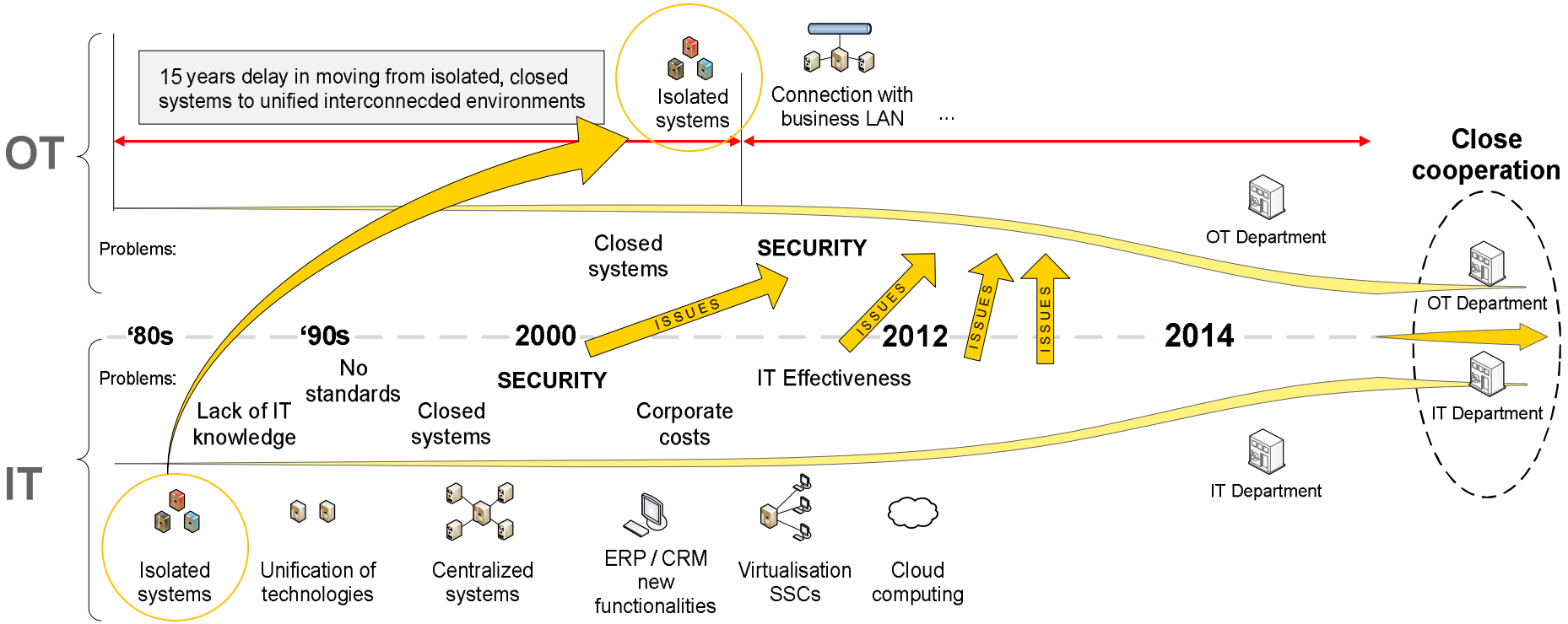
Setting the Scene
Operational Technology as a foundation of an industrial enterprise

	Layers of computer systems	Main components	Vendors
IT • Mature security approach • Knowledge widely available • **THE INFORMATION IS PROTECTED (Confidentiality first)**		• Application servers • Database servers • Workstations	Microsoft, SAP, ORACLE, IBM, hp
OT • Newly recognized area of concern • Speciffic industrial knowledge • Different approach ot security • **THE PROCESS IS PROTECTED (Availability first)**		• Control servers • **PHD** servers • Data historians • Alarm system serwers • **HMI** (Human Machine Interface) stations • Engineering workstaitons • **RTU** (Remote Terminal Unit) stations • **PLC** (Programable Logic Controlers)	Honeywell, Yokogawa, ABB, Rockwell Automation, Allen-Bradley, SIEMENS, YOKOGAWA, General Electric, Schneider Electric

ERNST & YOUNG
Quality In Everything We Do

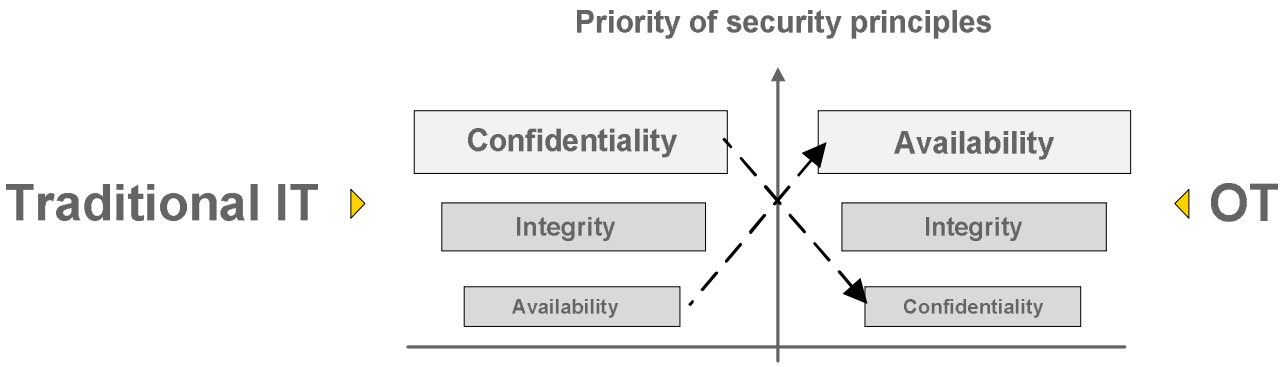
Setting the Scene

- Approach to security is being transferred from IT world to the OT assets.
- The problem organizations face is the lack of understanding of OT by IT based managers and lack of specific OT knowledge



ERNST & YOUNG
Quality In Everything We Do

Setting the Scene
OT vs. IT in terms of characteristics determining the approach to security



- IT systems process data only.
- Servers, network devices, printers, workstations, etc.
- Communication protocols: TCP/IP.
- Generally, versions of applications exist that are compatible with most of the independent operating systems.
- Implementations are made to last 3-5 years.

- OT systems process data and manage field devices.
- Apart from servers, network devices and workstations, there are PLCs, controllers, converters, devices collecting and distributing FrontEnd data.
- Communication protocols: ModBus, ProfiBus, FieldBus, DeviceNet, DNP3, IEC-60850-101/104.
- Dedicated systems are often coupled with the operating system.
- Implementations are made to last ~15 years.

ERNST & YOUNG
Quality In Everything We Do

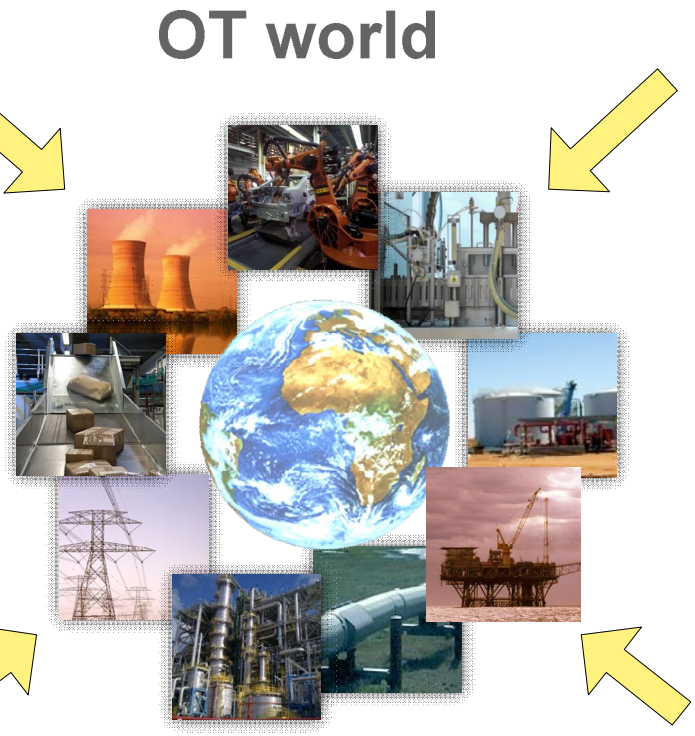
Setting the Scene
Factors influencing OT security

Convergence with IT

Transfer of technologies and evolution schemes from IT to OT, together with all related issues. OT will have, or already have introduced **Internet** connectivity, **mobile devices** access, etc.

Cyber Crime

Increasing number of attacks on critical infrastructure control systems such as SCADA **all over the world** resulting in power outages, destruction of equipment etc.



Legal Regulations

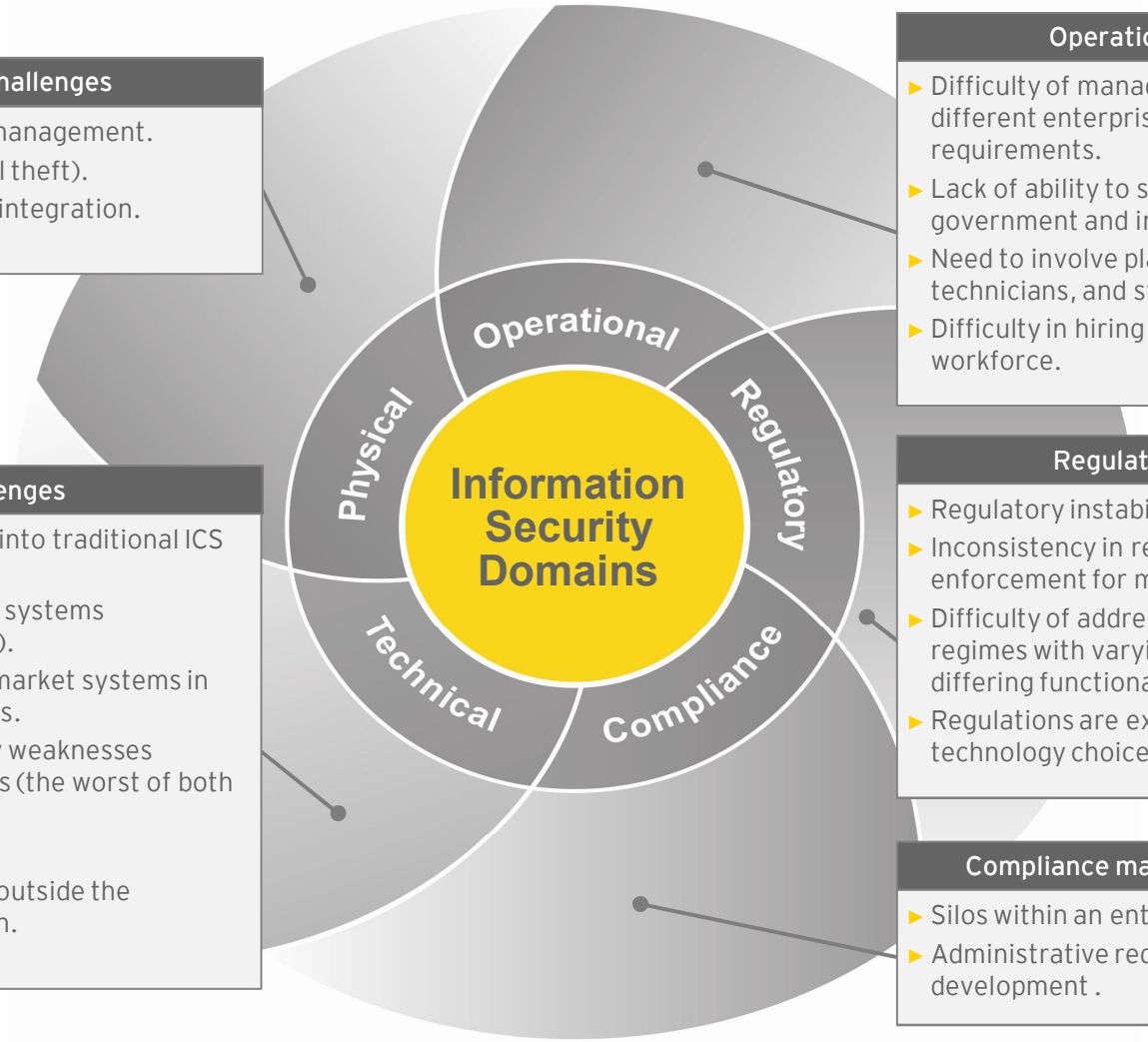
Specific regulatory guidance imposed by governments for in some sectors which will be moving towards **formal regulatory oversight** due to importance of the subject to national critical infrastructures.

New Technologies

Implementation of technologies like **Smart Fields,** causes current OT environments to change in order to provide new functionalities and increase the level of data exchange resulting in increased production effectiveness.

ERNST & YOUNG
Quality In Everything We Do

Setting the Scene
IT and OT holistic view across the major security domains



Physical security challenges
- Physical access and control management.
- Facility protection (e.g. metal theft).
- Physical security technology integration.

Technical challenges
- Integration of cyber security into traditional ICS model.
- Remote access into real-time systems (dependency on third parties).
- Convergence of control and market systems in safety and protection systems.
- Legacy systems with security weaknesses combined with newer systems (the worst of both worlds).
- Complexity.
- Technical devices are sitting outside the ownership of the organization.
- The Cloud.

Operational challenges
- Difficulty of managing security across different enterprise domains and functional requirements.
- Lack of ability to share information between government and industry.
- Need to involve planning engineers, field technicians, and system operators.
- Difficulty in hiring and retaining qualified workforce.

Regulatory challenges
- Regulatory instability.
- Inconsistency in regulatory audit and enforcement for multi-regional entities.
- Difficulty of addressing multiple regulatory regimes with varying requirements and differing functional focuses.
- Regulations are expensive and limit technology choices.

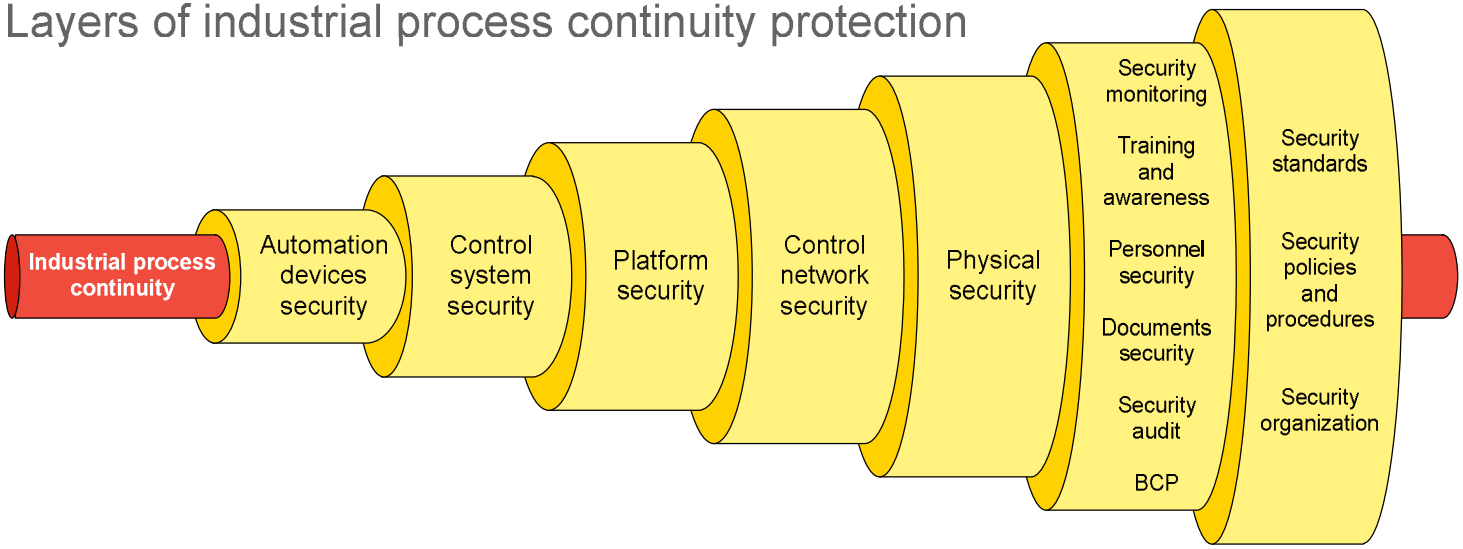
Compliance management challenges
- Silos within an entity.
- Administrative requirements and artifact development .

ERNST & YOUNG
Quality In Everything We Do

Setting the Scene
PCD chain of security

- The approach to protection of industrial process continuity at each layer must be compliant with OT requirements.
- Failure in each of the protection layers may cause disruption of the process and inability to recover.
- A Pin point approach to protection does not guarantee that the chain of security will be strong as a whole.
- In order for the Process Control Domain to work effectively, it must cover the whole chain of security on which the continuity of industrial processes depends.

Layers of industrial process continuity protection



ERNST & YOUNG
Quality In Everything We Do

What is seen
Issues we usually encounter – Process level examples

- Managements knowledge on the security of their control systems is based solely on the information they get from their SCADA/DCS administrators or directly from vendors.
- CIOs are in charge of IT and OT together, but their background is in IT and they have no understanding of OT characteristics.
- Lack of standardization.
- Any internal or external security audits are punctual and usually based on black-box penetration testing only.
- Most of the well organized security management practices cover only the area of business IT, while OT is unable or unwilling to implement them.
- No security monitoring inside the control network, even when it comes to remote activities of service providers or vendors. Lack of intruder detection in the control environment.
- Lack of incident response readiness.
- Faulty control systems and network architecture.

What is seen
Issues we usually encounter – Technical level examples

- We gained full access to critical control network from the business LAN.
- We took full control over PLC drivers, control system servers and operator's stations without having any credentials.
- We demonstrated the potential to cause Denial of Service of tested PLC drivers and critical control system servers.
- We identified a possibility to dump PLC drivers memory without logging into it.
- We took over HMI stations exploiting a vulnerable service running on it.
- We identified a network connection bypassing the firewalls and access control lists.
- We gained unauthorized access to major control environment supporting systems, such as UPS or backup storage.
- We identified a lack of adequate security on remote access channels, e.g. provided for system suppliers and service personnel.
- We identified lack of physical up-to-date network infrastructure documentation.

What is seen
Other companies approach to PCD

Organizations are starting to recognize control systems security as one of the top priorities. Sometimes due to awareness, sometimes due to government requirements or other regulations.

- Recognizing the necessity to monitor the security in the control environment and to be ready to react on incidents.
- Attempts to incorporate selected guidelines from best known norms and standards.
- Internal technical requirements for automation vendors, such as redundant power supply readiness.
- The will to transfer best security practices known from the IT world to the OT world while being aware of the requirement to adjust it to the OT specifics.
- Control systems security engagements are given "confidential" status in terms of agreements with service providers, scope of work and most of all - the results.

External Standards

- National Institute of Standards and Technology
  - NIST SP 800-82 Jun. 2011 Guide to Industrial Control Systems (ICS) Security
  - NIST 800-53 rev. 3 Aug. 2009 Recommended Security Controls for Federal Information Systems and Organizations (Appendix I – ICS Security Controls, Enhancements, And Supplemental Guidance)
- Instruments, Systems and Automation Society
  - ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models
  - ANSI/ISA-TR99.00.01-2007, Security Technologies for Manufacturing and Control Systems
  - ANSI/ISA–99.02.01–2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
  - Draft - ISA-99.03.03 - Security for industrial automation and control systems- System security requirements and security assurance levels
- North American Electrical Reliability Corporation - Critical Infrastructure Protection
  - NERC-CIP 002 - 009
- American Petroleum Institute
  - API-1164 – pipeline SCADA security
  - API-1165 - Recommended Practice for Pipeline SCADA Displays
  - API-1167 - Alarm Management (in development)
- American Gas Association
  - AGA-12 - SCADA encryption
- International Organization for Standardization / International Electrotechnical Commission
  - ISO/IEC 27001 / 27002

External Standards
NIST Guide to ICS Security

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

- Created by US National Institute of Standards and Technology (NIST).
- NIST SP 800-82 provides guidance for establishing secure industrial control systems (ICS).
- Is technical in nature however, provides the necessary background to understand the ICS.
- NIST 800-53 contains additions to the initial security control baselines for Federal Information Systems and Organizations that are required for ICS.

Focused on the Following Areas:

- Threats and Vulnerabilities (Threats, potential ICS Vulnerabilities, Risk Factors, Incidents)
- Security Program Development and Deployment (Business Case for Security, Developing a Comprehensive Security Program)
- Network Architecture (Firewall policies and rules, network segregation, NAT, Remote Access, Single Points of Failure, Man-in-the-Middle Attacks)
- Security Controls (Management Control, Operation Controls, Technical Controls)

Missing or Imprecisely Covered Areas:

- Organization structure (Roles and Responsibilities)
- A coherent approach to assets (identification, control, inventory)
- Encryption Technologies and Data Validation
- A coherent approach to Operating System and Application Updates
- Web Technologies
- Virus and Malicious Code
- Security Policies

Benefits

- Network security
- Authentication and authorization

External Standards
ISA 99

- Created by the International Society of Automation.
- Since 2008 developed and published by IEC (IEC 62433 series).
- Consists of best practices, technical reports and related information used to define procedures for implementing electronically secure manufacturing and control systems.

Focused on the Following Areas:

- Authentication & Authorization Technologies
- Filtering/Access Control/Blocking Technologies
- Encryption Technologies and Data Validation
- Management, Audit, Measurement, Monitoring, and Detection Tools
- Industrial Automation and Control Systems Computer Software
- Physical Security Controls

Missing or Imprecisely Covered Areas:

- Organization structure (Roles and Responsibilities)
- Business Continuity Plan
- Change Management Process

Benefits:

- Network zoning
- Filtering / blocking
- Authentication and authorization
- Password controls
- Antivirus protection

External Standards
NERC CIP

- Created by NERC North America Electric Reliability Corporation to improve physical and cyber security for the bulk power system of North America.
- NERC CIP is a set of cyber security standards created as an effort to offer solutions improving security of power generation, transmission and distribution companies.

Focused on the Following Areas:

- CIP 002: Critical Cyber Assets
- CIP 003: Security Management Controls
- CIP 004: Personnel & Training
- CIP 005: Electronic Security Perimeter
- CIP 006: Physical Security
- CIP 007: Systems Security Management
- CIP 008: Incident Reporting & Response Planning
- CIP 009: Recovery Plans for Critical Cyber Assets

Missing or Imprecisely Covered Areas:

- A coherent approach to assets and organization of energy industry (identification, control, inventory)
- Encryption Technologies and Data Validation
- A high level approach to technical solution
  - Operating System and Application Updates processes
  - Web Technologies
  - Virus and Malicious Code
  - Network security and segmentation

Benefits:

- Appropriate for high level management, describing basic principles of OT security

External Standards
API

- Created by American Petroleum Institute.
- API security provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security.

Focused on the Following Areas:

- Physical Security
- Communication System
- Network Design & Management
- Risk & Vulnerability Assessments
- Business Continuity Plan
- Incident Response Plan

Missing or Imprecisely Covered Areas:

- Network security (Filtering/Blocking/Access Control Technologies)
- Remote access

Benefits:

- Assets identification
- Assets management

External Standards
AGA-12

- Background, Policies and Test Plan for Cryptographic Protection of SCADA Communications.
- Describes cryptographic mechanisms viable to be implemented in the existing communications systems based on control protocols such as DNP3.

Focused on the Following Areas:

- Background, Polices and Test Plan
- Retrofit link encryption for Asynchronous serial communications
- Protection of Network System
- Protection Embedded in SCADA Components

Missing or Imprecisely Covered Areas:

- AGA 12 focuses only on ensuring the confidentiality of SCADA communications - lack of description of other areas.

Benefits:

- Complete description of cryptographic protection of SCADA communications.

External Standards
ISO / IEC 27001, 27002

- Developed by International Organization for Standardization / International Electrotechnical Commission.
- Defines requirements and sets guidelines for development, implementation and maintenance of an Information Security Management System.

Focused on the Following Areas:

- Security Policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Missing or Imprecisely Covered Areas:

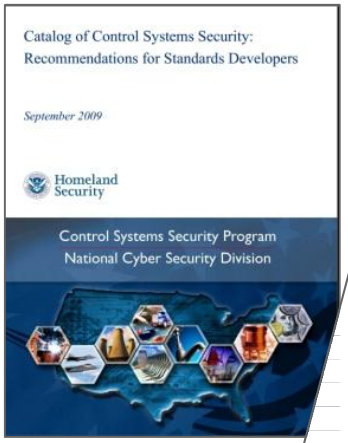
- Focused only on IT area
- Is more about "what" than "how"
- Process control
- Implementation testing

Benefits:

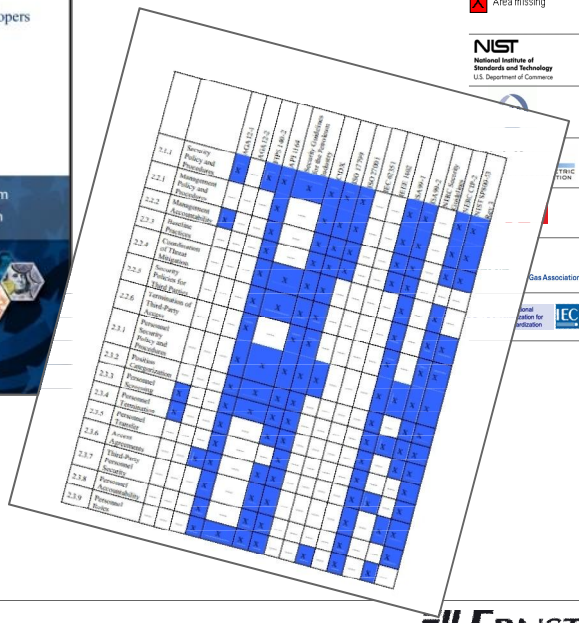
- Risk-driven approach

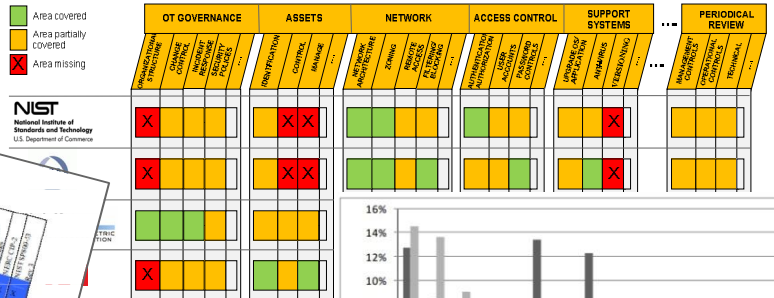
External Standards
Summary

- Currently none of the existing standards may be used straight out of the box and implemented in the OT environment in a way that ensures consistency and clear, precise interpretation of its requirements.
- Simply extracting the content from all the standards would result in design of requirements of basically all the required areas however the coverage in each area would not meet the requirements in terms of practicality for implementation purposes, not those in the area of particular security mechanisms to be used. - today's standards focus on "what" but miss the part about the "how".



Source: Depatment of Homeland Security





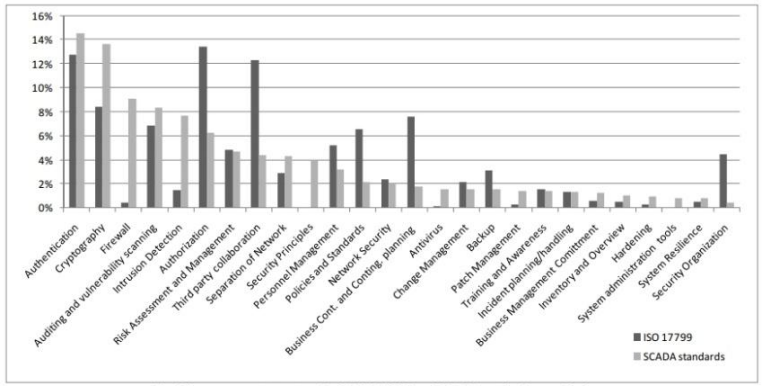


Fig. 3 **Focus on countermeasures for ISO/IEC 17799 and SCADA standard, normalized.**

Source: SCADA System Cyber Security – A Comparison of Standards ,Teodor Sommestad, Göran N. Ericsson, Senior Member, IEEE, Jakob Nordlander

ERNST & YOUNG
Quality In Everything We Do


Thank you!
ERNST & YOUNG
Quality In Everything We Do