Control System Cyber-Security in Industry

Dr. Stefan Lüders (CERN IT/CO)

(CS)^2/HEP Workshop, Knoxville (U.S.)

October 14th 2007

Overview

Critical Infrastructure Protection

Standards & Regulations

The Silence of the Lambs

Raising Awareness

Control Systems for Living

…in the electricity sector

- transmission & distribution, fossil, hydro, nuclear

…in the oil & gas sector

…in the water & waste sector

…in the chemical and pharmaceutical industry

…in the transport sector

…for production:

- e.g. cars, planes, clothes

…in supermarkets

- e.g. scales, fridges

…for facility management

- electricity, water, C&V

COBB County Electric, Georgia

Middle European Raw Oil, Czech Republic

Athens Water Supply & Sewage

Merck Sharp & Dohme, Ireland

CCTV Control Room, UK

Reuters TV Master Control Room

CERN: Standards, if possible !

- Commercial of the shelf hardware

standard desktop PCs

SIEMENS CAEN Tektronix Schneider Electric BECKHOFF INDUSTRIE ELEKTRONIK acqiris NATIONAL INSTRU WIENER

- Standard (controls) soft

PcVue WinCC CVS LynxOS Microsoft Wizcon MySQL SONICMQ®

- Communication protocols

OPC FOUNDATION WorldFIP CAN FIP BUS W3C PROFIBUS Modbus-IDA PCI EXPRESS VMEbus Technology

Used elsewhere, too !!!

Severe Consequences

Loss of control or safety:

- Blocking of CPU or other resources
- Dysfunction or interruptions of process
- Halt of equipment

Perturbations in a factory / industry:

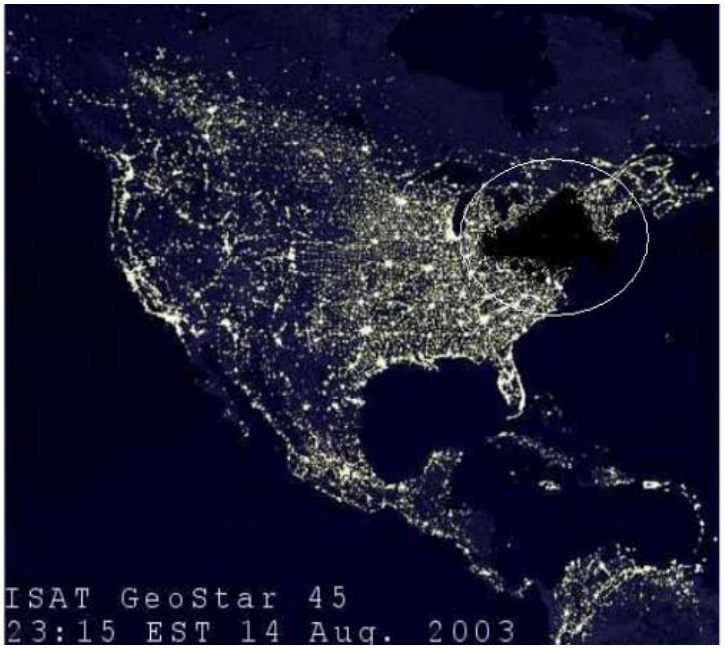
- Reduction or **loss of production**
- Damage or **destruction of equipment**
- Injuries or **casualties**
- **Bad PR** or loss of confidence

€€€ CHF £££ $$$

Critical Infrastructure

Increased focus since 9/11 and due to today's general security situation:

- Electricity
- Oil & Gas
- Water & Waste
- Chemical & Pharmaceutical
- Transport



Critical Infrastructure Protection (CIP)
Critical Information Infrastructure Protection (CIIP)

Critical Infrastructure Protection

Standards & Regulations

(Too?) Many Standards, …

- "Manufacturing and Control Systems Security"
  (American National Standards Institute & Int'l Society for Measurement and Control)
  (ANSI/ISA SP99)
- "Good Practice Guidelines"
  (U.K. Centre for the Protection of National Infrastructure CPNI)
- "Code of Practice for Information Security Management"
  (Int'l Organization for Standardization / Int'l Electrotechnical Commission / British Standard)
  (ISO/IEC 27002 aka. 17799:2005, BS7799)
- "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security"
  (U.S. National Institute of Standards and Technology NIST SP800-82)
- "System Protection Profile - Industrial Control Systems" (NIST)
- Common Criteria (ISO/IEC 15408)
- "Cyber-Security Vulnerability Assessment Methodology Guidance"
  (U.S. Chemical Industry Data Exchange CIDX)
- "Good Automated Manufacturing Practices: Guideline for Automated System Security" (Int'l Society for Pharmaceutical Engineering ISPE)
- NERC & AGA standards
  (North American Electric Reliability Council, American Gas Association)

ISA SP99: “Manufacturing and Control Systems Security”

ISA–The Instrumentation, Systems, and Automation Society

Standards 01 to 04:

- “Scope, Concepts, Models and Terminology” (ISA 99.00.01)
- “Establishing a Manufacturing and Control Systems Security Program“ (ISA 99.00.02)
- “Operating a Manufacturing and Control Systems Security Program” (ISA 99.00.03)
- “Specific Security Requirements for Manufacturing and Control Systems” (ISA 99.00.04)

Technical Reports 01 & 02:

- “Technologies for Protecting Manufacturing and Control Systems” (ISA TR 99.00.01)
- “Integrating Electronic Security into the Manufacturing and Control Systems Environment” (ISA TR 99.00.02 — obsolete)

http://www.isa.org/MSPrinterTemplate.cfm?MicrositeID=988&CommitteeID=6821

CPNI Good Practice Guidelines

CPNI
Centre for the Protection of National Infrastructure

www.cpni.gov.uk

PA Consulting Group

www.paconsulting.com

Good Practice Guide

Process Control and SCADA Security

This guide is designed to impart good practice for securing industrial control systems such as: process control, industrial automation, distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Such systems are used extensively across the nation's Critical National Infrastructure. The paper provides valuable advice on protecting these systems from electronic attack and has been produced by PA Consulting Group for NISCC.

TABLE OF CONTENTS 2

http://www.cpni.gov.uk/Products/guidelines.aspx

Regulations

NIST
National Institute of Standards and Technology

Special Pub's 800-53 and 53A

- Help to identify, control, and mitigate risks to information and information systems
- Recommendations and guidelines for selecting and specifying safeguards & countermeasures
- Foundation for risk assessment

…how does this apply to "Controls" (e.g. SP800-82) ?

http://csrc.nist.gov/publications/nistpubs

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

IMPLEMENTING SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard developed in response to the Federal Information Security Management Act of 2002. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems (other than national security information and information systems). The agency's risk assessment validates the security control set by determining if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), agency assets, or individuals. The resulting set of security controls establishes a level of "security due diligence" for federal agencies and their contractors.

In addition to the security requirements established by FISMA, there may also be specific security requirements in different business areas within agencies that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These requirements may not be equivalent to the security requirements and implementing security controls required by FISMA or may enhance or further refine the security requirements and security controls. It is important that agency officials (including authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and acquisition authorities) take steps to help ensure that: (i) all appropriate security requirements are addressed in agency acquisitions of information systems and information system services; and (ii) all necessary security controls are implemented in agency information systems when determining the tailored and supplemented control baselines described in this publication.

See http://csrc.nist.gov/sec-cert/ca-compliance.html for additional information on compliance.

Critical Infrastructure Protection

Standards & Regulations

The Silence of the Lambs

Follow-Up of CERN's TOCSSiC

Discussions with corresponding manufacturers

- Acknowledgement only after a lot of persuasion
- Some now perform vulnerability scans themselves

…results improve with more recent firmware versions ☺

Cooperation & forwarding

- …together with governmental bodies
- …of the corresponding manufacturers to third parties
- …"Hamburger Liste" on www.langner.com

CPNI Centre for the Protection of National Infrastructure

Informatikstrategieorgan Bund ISB
Unité de stratégie informatique de la Confédération USIC
Organo strategia informatica della Confederazione OSIC
Organ da strategia informatica da la Confederaziun OSIC

DESY

Nutzfahrzeuge

Langner

Presentations to industry

- Discussions on "Requirements for the Cyber-Security of Control Systems"

PLCopen for efficiency in automation

ZVEI

*…but lots of ignorance: **"There is no market demand !"***

"European Information Exchange on SCADA and Control System Security"

EuroSCSIE

- *"…members from European based government, industry and research institutions depending upon and/or whose responsibility it is to improve the security of SCADA and Control Systems…"*
- Currently chaired by CERN

Objectives:

- Exchange good practices & recommendations, incidents & mitigations
- Provide interface between governmental regulators & end-users
- Channel information between regional information exchange groups
- Address cyber-security issues jointly to vendors & manufacturers
- In preparation:
  "Questionnaire on Cyber-Security for Control Systems"

“Procurement Language”

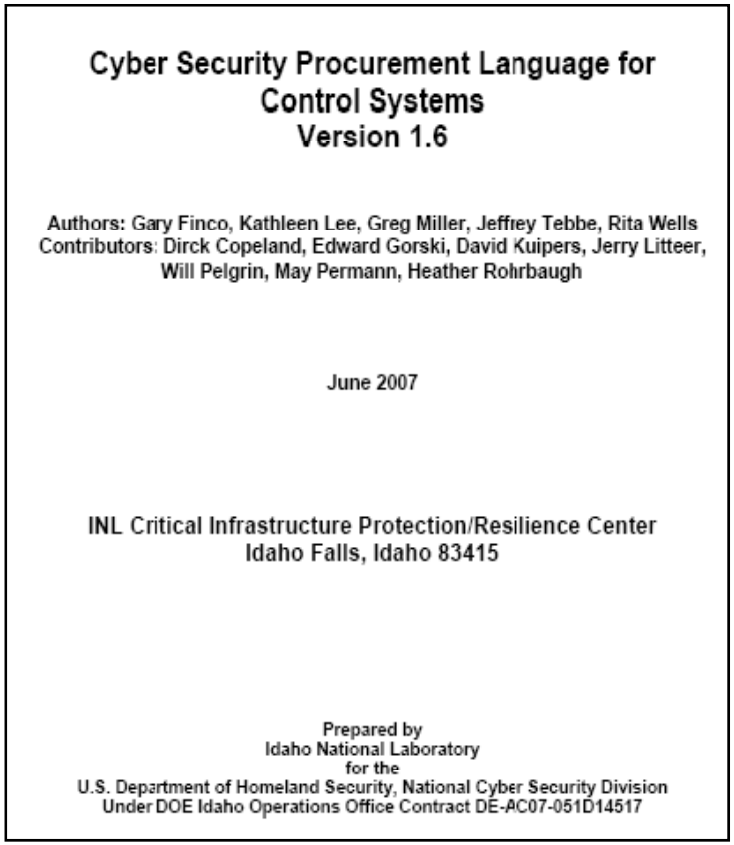
Manufacturers and vendors are part of the solution !

- Security demands must be included into orders and call for tenders

Idaho National Laboratory

“Procurement Language” document

- *“… collective buying power to help ensure that security is integrated into SCADA systems.”*
- **“Copy & Paste” paragraphs** for
  System Hardening,
  Perimeter Protection,
  Account Management,
  Coding Practices,
  Flaw Remediation, …



Cyber Security Procurement Language for Control Systems
Version 1.6

Authors: Gary Finco, Kathleen Lee, Greg Miller, Jeffrey Tebbe, Rita Wells
Contributors: Dirck Copeland, Edward Gorski, David Kuipers, Jerry Litteer, Will Pelgrin, May Permann, Heather Rohrbaugh

June 2007

INL Critical Infrastructure Protection/Resilience Center
Idaho Falls, Idaho 83415

Prepared by
Idaho National Laboratory
for the
U.S. Department of Homeland Security, National Cyber Security Division
Under DOE Idaho Operations Office Contract DE-AC07-051D14517

http://www.msisac.org/scada

Penetration Tests & Certification

Sandia National Laboratories

www.sandia.gov/scada

"....penetration test I
not able to send gas
- Sandia National Labs

Full scale penetration test

- …on complete control systems used e.g. in power plants
- Manufacturers can participate

wurldtech™
security technologies

"Achilles" black box tester

- Random testing of protocol fields' possible values & combinations
- Product certification: "OSI Stack", "Modbus/TCP", …

Documents

The following are a list of SCADA and related reports.

- "Analysis of Operations and Cyber Security Policies for a System of Cooperating Flexible Alternating Current Transmission System (FACTS) Devices," SAND 2005-7301, December 2005.
- "Agent-Based Control of Distributed Infrastructure Resources," SAND 2005-7937, January 2006.
- "Cyber Security for Utility Operations," April 2005.
- "A Summary of Control System Security Standards Activities in the Energy Sector," October 2005.
- "Network Security Infrastructure Testing," October 2005.
- "Reference Model for Control and Automation Systems in Electrical Power," October 2005.
- "Penetration Testing of Industrial Control Systems," SAND2005-2846P, March 2005.
- "Key Management for SCADA," SAND2001-3252, March 2002.
- "Sandia SCADA Program - High-Security SCADA LDRD Final Report," SAND2002-0729, April 2002.
- "A Scalable Systems Approach for Critical Infrastructure Security," SAND2002-0877, April 2002.
- "Common Vulnerabilities in Critical Infrastructure Control Systems," SAND2003-1772C, May 2003. (Presented at SANS SANSFIRE 2003 and National Information Assurance Leadership Conference V - (NIAL), July 14-23, 2003, Washingdon, DC).
- "An Introduction to and Evaluation of Information Control Models," SAND2002-1405, October 2003.
- "A Classification Scheme for Risk Assessment Methods," SAND 2004-4233, August 2004.
- "A Reference Model for Control and Automation Systems in Electric Power," SAND 2005-1000C
- "Framework for SCADA Security Policy," SAND 2005-1002C
- "Sustainable Security for Infrastructure SCADA"
- "An Introduction to Information Control Models," SAND2002-1031, September 2003.

The following are a list of upcoming SCADA and related reports.

- "Best Practices for SCADA Networks," SAND2004-xxxx, Completion expected 1Q2004.
- "Agent-Based Control of Distributed Infrastructure Resources," LDRD #03-

Contains commands for working with the selected items.

Critical Infrastructure Protection

Standards & Regulations

The Silence of the Lambs

Raising Awareness

Major Players

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

"To accelerate the design, development, and deployment of more secure control and legacy systems."

On Board: Chemical industry, U.S. government, vendor community, water & waste management

Reference Library	Resources
Securing your SCADA and Industrial Control Systems by The Department of Homeland Security and the Technical Support Working Group (TSWG)	Control Systems Security Program (CSSP)
	Technical Support Working Group (TSWG) SCADA Site
SCADA Honeynet Results from the PCSF 2007 Annual Meeting by Dale Peterson and Landon Lewis	Energy Roadmap Initiative
	DHS Daily Open Source Infrastructure Report
Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research by D. Dudenhoeffer, S. Hartley, M. Permann	SCADA and Control Systems Procurement Project
	SCADA Security Blog
Applying NIST SP 800-53 to Industrial Control Systems by Stuart Katzke, Keith Stouffer, et al.	SCADA and Control System Security Links
PCSF Project Plan to Execute Liaison D with IEC TC65WG10 by Dennis Holstein, OPUS Publishing	
Critical Utility Infrastructure Resilience - Extended Abstract	

https://www.pcsforum.org

Digital Bond:

wurldtech™ security technologies

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

- Tests on OPC vulnerabilities
- Dedicated "Snort" rule-sets for Controls
- Dedicated plug-ins for "Nessus" on Modbus/TCP, OPC, DNP3, ICCP
- SCADA Honeynets

Conferences

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

- **Annual spring meetings**
  - Next: March/April 2008

Digital Bond:

- **"SCADA Security Scientific Symposium"**
  - Next: January 2008, Miami

ISA
ISA–The Instrumentation, Systems, and Automation Society

- **Annual exposition**
  - Incl. dedicated "Security Exchange"
  - Last: October 2007, Houston

SANS INSTITUTE

- **Irregular workshops and webcasts**

- **Lots of regional workshops by consulting services, governments, etc.**

YOU ARE NOT ALONE !!!

Dialog to discuss Control System Cyber-Security

- …at CERN
- …with industry, consultants, governments
- …in the HEP community

Thank you for being here…

…Let's tackle the problem together !!!

DESY · PAUL SCHERRER INSTITUT PSI · Fermilab · TRIUMF · CCLRC · IN2P3 Institut National de Physique Nucléaire et de Physique des Particules

(CS)² HEP