Dr. Stefan Lüders (CERN IT/CO) with slides from P. Chochula (ALICE), S. Gysin (FNAL), T. Lahey (SLAC), M. Leech (Diamond), T. Ohata (JASRI/SPring-8), D. Quock (ANL), A. Yamashita (SPring-8), Z. Yin (BNL), and T. Zingelman (FNAL)

ICALEPCS, Knoxville (U.S.), October 15th 2007
Changing Times

The Past:
The (R)Evolution of Control Systems

The Present:
What about Security !?*

The Future:
Control System Cyber-Security
Risk = Threat × Vulnerability × Consequence
<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:05-09:30 (00h25')</td>
<td>[11] Cyber-Threats, Cyber-Vulnerabilities, and Cyber-Risks</td>
<td>Dr. Stefan LUEDERS (CERN)</td>
</tr>
<tr>
<td>09:30-10:00 (00h30')</td>
<td>[9] Network and computer security in the Fermilab Accelerator Control System</td>
<td>Tim ZINGELMAN (Fermi National Accelerator Lab)</td>
</tr>
<tr>
<td>10:00-10:30 (00h30')</td>
<td>[5] Control System Cyber Security Measures at the Advanced Photon Source</td>
<td>Ms. Deborah QUOCK (Argonne National Laboratory)</td>
</tr>
<tr>
<td>10:45-11:15 (00h30')</td>
<td>[12] Perspective on secure network for control systems in SPring-8</td>
<td>Dr. Toru OHATA (JASRI/SPring-8)</td>
</tr>
<tr>
<td>11:15-11:45 (00h30')</td>
<td>[6] Update on the CERN Computing and Network Infrastructure for Controls (CNIC)</td>
<td>Dr. Stefan LUEDERS (CERN)</td>
</tr>
<tr>
<td>11:45-12:15 (00h30')</td>
<td>[7] Remote Access to Alice</td>
<td>Peter CHOCHULA (CERN)</td>
</tr>
</tbody>
</table>

http://indico.cern.ch/conferenceDisplay.py?confId=13367
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker and Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:05-09:30</td>
<td>[11] Cyber-Threats, Cyber-Vulnerabilities, and Cyber-Risks</td>
<td>Dr. Stefan LUEDERS (CERN)</td>
</tr>
<tr>
<td>09:30-10:00</td>
<td>[9] Network and computer security in the Fermilab Accelerator Control System</td>
<td>Tim ZINGELMAN (Fermi National Accelerator Lab)</td>
</tr>
<tr>
<td>10:00-10:30</td>
<td>[15] SLAC Controls Security Overview</td>
<td>Terri LAHEY (SLAC)</td>
</tr>
<tr>
<td>10:45-11:15</td>
<td>[4] Role Based Access Control for the Accelerator Control System at CERN</td>
<td>Mrs. Suzanne GYSIN (FNAL)</td>
</tr>
<tr>
<td>11:15-11:45</td>
<td>[10] WARC S -Wide Area Remote Control for SPring-8</td>
<td>Dr. Akihiro YAMASHITA (SPring-8)</td>
</tr>
<tr>
<td>11:45-12:15</td>
<td>[8] Secure Remote Operation of Light Source Beamline Controls with FreeNX</td>
<td>Mr. Zhijian YIN (Brookhaven National Lab)</td>
</tr>
<tr>
<td>16:15-16:45</td>
<td>[14] Accelerator Control-System Network Security at Diamond Light Source</td>
<td>Dr. Mike LEECH (Diamond Light Source)</td>
</tr>
<tr>
<td>16:45-17:15</td>
<td>[13] Control System Cyber-Security in Industry</td>
<td>Dr. Stefan LUEDERS (CERN)</td>
</tr>
<tr>
<td>Time</td>
<td>Session</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>09:30-10:00</td>
<td>[9] Network and computer security in the Fermilab Accelerator Control System</td>
<td></td>
</tr>
<tr>
<td>10:00-10:30</td>
<td>14:00-14:30 [15] SLAC Controls Security Overview</td>
<td></td>
</tr>
<tr>
<td>10:00-10:30</td>
<td>[4] Role Based Access Control for the Accelerator Control System at CERN</td>
<td></td>
</tr>
<tr>
<td>11:15-11:45</td>
<td>15:00-15:30 [10] WARCS -Wide Area Remote Control for SPring-8</td>
<td></td>
</tr>
</tbody>
</table>

http://indico.cern.ch/conferenceDisplay.py?confId=13367
APS Control System

- Linac, PAR, Booster and Storage Ring
  - 80 Workstations (Solaris, Linux, Windows, Apple Mac)
  - Approximately 300 distributed Input/Output Controllers (IOCs)
  - EPICS supervisory real-time controls software is interfaced by 96 PLCs, FPGAs, and Johnson Controls distributed control systems
  - More than 30,000 replaceable hardware components
  - Over 100,000 IOC points that are monitoring and controlling more than 450,000 technical parameters
  - Nearly 700 unique control system software applications

- Beamlines
  - Beam diagnostics control roughly 60 X-ray beams simultaneously with >500 ultra-high resolution beam position monitors, each resolving beam motion to a fraction the size of the period at the end of this sentence.
  - Nearly 100 remote computers collect data from the 500 monitors & re-steer the X-ray beams 1,500 times per second
APS Control System

- Linac, PAR, Booster and Storage Ring
  - 800M
  - App
  - EPIC
  - Dist
  - MoI
  - OxI
  - Net
- Beamline
  - Bet
  - Pos
  - Net

Standards, if possible!

Commercial off the shelf hardware
- Tektronix
- Schneider Electric
- Beckhoff
- National Instruments
- Hirschmann
- LeCroy
- Siemens
- CAEN
- Linde
- Sun

Standard (controls) software
- ORACLE
- PVSS II
- Microsoft
- MySQL
- SONICMO

Standard communication protocols
- OPC Foundation
- WorldFIP
- CAN
- W3C
- PROFIBUS
- Modbus-IDA
- PCI EXPRESS
- VMEbus
 Variety & Diversity in Products

APS Control System

- Linac, PAR, Booster and Storage Ring
  - 80'
  - App.
  - EPI dist
  - MoI
  - OvI
  - Net

- Beamline
  - Bet pos sen
  - Net peri

Multitude of hardware, ...

Standards, if possible

Commercial off the shelf hardware

- Tektronix
- Schneider Electric
- Beckhoff
- National Instruments

... O/S, applications, and protocols!
Balance Risk, Safety & Usability

Vulnerabilities ARE fact!

Management buy-in!
II. Balancing Risks vs. Usability

- Reducing disruption to operations by cyber threats is important, however, reducing disruption to operations by cyber protections is also very important!

- More accelerator downtime due to effects of cyber protection than from cyber attacks
Balance Risk, Safety & Usability

II. Balancing Risks vs. Usability

- Reduced threat to personnel, but still a risk of disruption of operations
- More emphasis on cyber security

Machine Protection Systems and (HW) Interfaces

- Beam Current Monitors
- DCCT Dipole Current 1
- DCCT Dipole Current 2
- RF turn clock
- Beam Energy Tracking
- Injection Kickers
- Safe LHC Parameters
- SPS Extraction Interlocks
- TL collimators
- BLMs aperture
- BLMs arc
- Collimators / Absorbers
- BPMs for Beam Dump
- NC Magnet Interlocks
- BPMs for $dE/dt + dy/dt$
- $dI/dt$ beam current
- $dI/dt$ magnet current
- Screens
- RF + Damper
- LHC Experiments
- Vacuum System
- Operators
- Software Interlocks

Access Safety System

Discharge Switches

Cryogenics
- Quench Protection
- Power Converters
- AUG
- UPS

Powering Interlock System

Essential circuits

 Auxiliary circuits

Timing

PM Trigger
II. Balancing Risks vs. Usability

- Reducing threats due to disruptions.
- More focus on cyber

Machine Protection Systems and (HWS)

| Beam Current Monitors | Current |
| DCCT Dipole Current 1 | Beam Energy Tracking |
| DCCT Dipole Current 2 | Injection Kickers |
| RF turn clock |

- Beam Dumping System
- Safe LHC Parameter
- Injection Flag

LHC Beam Interlock System

| Cryogenics |
| Power Converters |
| Power Protection |
| Powering Interlock System |

Safety goes along, too !!!
**Ground Rules for Cyber-Security**

**Separate controls and campus networks**
- Reduce and control inter-communication
- Deploy IDS
- Apply policy for remote access

**Use centrally managed systems wherever possible**
- Ensure prompt security updates: applications, anti-virus, OS, etc.

**Deploy proper access control**
- Use strong authentication and sufficient logging
- Ensure traceability of access (who, when, and from where)
- Passwords must be kept secret: beware of “Google Hacking”

**Make security an objective**
- Security training
- Management buy-in
- Bring together IT and Controls experts
Defense-In-Depth

Summary on the (CS)²/HEP Workshop — Dr. Stefan Lüders et al. — ICALEPCS — October 15th 2007

Ground Rules for Cyber Security

Security Layers in ALICE DCS

- Which roles are granted to current user?
- Which resources are accessible from where?
- Authentication and authorization at the level of control system
- Access control at the level of network
- Authorization at the level of OS
- Authentication at the level of OS
- Which applications can be started?
- Who can logon where?

Separate campus
- Read
- Inter
- Deploy
- Applicant
- Remote

Deploy policies and access control
- Use
- Authorize
- Ensure
- (who, what, when, where and why)
- Password strength and behavio...
Security Layers in ALICE DCS

Conclusion

- Security of the worst node can cause problems for all – real or perceived
- Implement secure computers, networks and practices using local experts that work with central experts.
- Build secure architecture - know what is happening on your systems/network
- Create good procedures, and revise as needed
Defense-In-Depth

Security Layers in ALICE DCS

Conclusion

- Security of the worst node can cause problems for all – real or perceived.
- Implement secure computers, networks and practices using local experts that work with central experts.
- Build secure architecture - know what is happening on your systems/network.
- Create good procedures, and revise as needed.
Network Segregation

Cybersecurity Requirements at BNL:
Perimeter Defense
Network Segregation

Cybersecurity Requirements at BNL:

AD Enterprise 1.3
10-4-07

FNAL

AD border-1

AD border-2

AD Backbone

AD firewall-primary

Failover Serial Cable

Failover Gigabit Link

AD firewall-secondary

AD controls subnet

dmz1

Outback

Outland

dmz2

v-ad-3030

AD general subnet

DB servers DAEA/DPE Web Server

Linux Cluster Frontends MCR consoles

Wireless APs Netlog Print Server Web Server File server KDC
Network Segregation

Cybersecurity Requirements at BNL:

AD Enterprise 1.3
10-4-07

Network topology

Control system cybersecurity workshop at Knoxville, USA
October 14, 2007
Network Segregation

Cybersecurity Requirements at BNL:

Network topology

Strong perimeter protection...
...with firewalls and shielding routers...
...plus dedicated controls networks!
Dual Homed Servers:
- SSH Bastion: Allows remote access during shutdown and emergency remote access during operation to fix faults.
- EPICS Channel Access archiver: Allows office access to archived data.
- Bootserver: Allows office read-only access to software (3.14).
- Relational Database: Allows access to ELog, cable schedules etc.
Rules for Remote Access

Remote Access to the DCS Network

Access to ALICE DCS is based on application gateways
No direct logon from outside
1. User logs into the gateways
2. From the gateway user logs into the destination host
Rules for Remote Access

Remote Access to the DCS Network

Statistics on IPS

- 300 incidents/year
- Fewer suspicious hosts, shutdown period in SPring-8
- Most incidents had shown undesirable behavior such as sweep port scan

We recommend IPS!!

When checked “quarantine list” and go to the host, we found “Trojan Horse”

"miss setting" was caused by the wrong detection of pattern string.
A pattern string for detection worm is simple.
- The detection strings of Sasser worm is "\lsarpc$".
- Normal connections such as Active Directory of Microsoft uses this string.

Control system cyber-security workshop at Knoxville, USA
October 14, 2007
Rules for Remote Access

Remote Access to the DCS Network

Statistics on IPS

- suspicious host
- miss setting
- identified worm

We recommend IPS!!

Most incidents had shown undesirable behavior such as sweep port scan.

When checked "quarantine list" and go to the host, we found "Trojan Horse"

"miss setting" was caused by the wrong detection of pattern.

A pattern string for detection worm is simple.
- The detection strings of Sasser worm is "\lsarpc6".
- Normal connections such as Active Directory of Microsoft uses this string.

Control system cyber-security workshop at Knoxville, USA
October 14, 2007

Controlled data exchange...
...w/o visibility from outside...
...and surveilled & protected!
V. Access Options

- **VPN**
  - Software client, controls ‘key’ & login required
  - Authenticated & time limited network access
  - Remote system becomes a ‘Controls’ node
  - Full **inbound** and **outbound** firewall restrictions apply (no ‘split tunnel’) all traffic is ‘inside’
  - Still requires further login to get command line access or to start a control system console
VNC (Virtual Network Computer)

- Screen sharing program
  - With multiple users (not only 1-1, 1 to many)
- Free
- Multi platform
  - Not only Win, Mac, UNIX but also PDA
- Open standard
  - Many implementation
  - UltraVNC for Win
    - Shrink large screen to fit small screen
    - 20" screen into 11" note PC's screen
- Image compression level can be selected.
  - Select by connection condition.
Remote Access Tools

The TSSHELL

Standard Windows Shell

User can interact with system in several ways

TSShell

User cannot interact with system - TSSHELL is the only available interface
Remote Access Tools

Remote Operations with NX:
Putting together

- Create ssh tunnel:
  remote host port 22 map to localhost: 3322
  through ssh gateway,
  zyin@ssh.bnl.gov

- Leave the terminal open
- Configure NoMachine NX client
  localhost port 3322
Remote Operations with NX:
Putting together

- Create ssh tunnel:
  remote host port 22 maps to
  through ssh gateway,
  zylin@ssh.bnl.gov

- Leave the terminal open
- Configure NoMachine NX client
  localhost port 3322

...VNC (ev.
inside SSH), ...
terminal
server, or...
customized remote X via SSH!
Central PC Management

Central Installation Schemes (2)

Install...
- Centrally managed OS & SW
- User applications
- Automatically & network-based
- On many PCs in parallel

Configure...
- Look & Feel
- Access rights & restrictions

Full remote control of...
- Configuring
- Installation
- Patching
- Rebooting

... this works even for oscilloscopes !!!
Central Installation Schemes (2)

IV. OS/Application Layer Protection

- Linux systems use Site autoYUM service for OS and Applications and Site MIT Kerberos

- Windows systems use Division patching services and Site W2K Domain, plus Control System Anti-Virus service

- FreeBSD and Solaris systems use ‘portaudit’ and vendor email notification – these systems have ‘professional’ administrators
Central PC Management

Central Installation Schemes (2)

IV. OS/Application Layer Protection

- Linux system and Application
- Windows services
- FreeBSD and various others have ‘patch management’

Patch management

- Windows update, anti-virus software update server
  - push patches into clients
  Target:daq front-end with LabVIEW, Oscilloscope, etc.

- Linux mirror servers
  - YaST mirror of SuSE Linux Enterprise 10
  - apt mirror of Ubuntu and Debian
  Target: operator consoles,daq front-end, etc.
Central PC Management

“Summary on the (CS)²/HEP Workshop” — Dr. Stefan Lüders et al. — ICALEPCS — October 15th 2007

Central Installation Schemes (2)

IV. OS/Application Layer Protection

- Linux system and application patch management

Patch management

- Windows update, anti-virus software server
  - push patches into clients
  - Target:daq front-end with LabVIEW, Oscillos etc.

- Linux mirror servers
  - YaST mirror of SuSE Linux Enterprise 10
  - apt mirror of Ubuntu and Debian
  - Target: operator consoles, dq front-end, etc.

Do it centralized...

...for Linux & Windows...

...with patches & anti-virus!
Web-based Controls Applications

- Security Strategies

- Web Server
  - Secure Web server, HTTPS
    - Deter session hijacking
    - HTTPS uses Secure Sockets Layer (SSL) to encrypt the request and response

- User Authentication
  - LDAP, Lightweight Directory Access Protocol
    - Standard for communicating record-based, directory-like data between programs
  - SSO, Single Sign-On service
  - Sun Java System Access Manager (also provides for real-time auditing)

- PHP
  - Message-Digest algorithm 5 (MD5) cryptographic hash PHP function
    - Transfer user authenticated phrase
  - PHP session feature (PHP-created cookie)
    - Deter session fixation
    - Customize with PHP functions
      - `$_SESSION_save_handler()`
      - `$_SESSION_set_cookie_params()`
  - PHP `htmlentities()` function
    - Prevent cross-site scripting attacks
  - PHP `mysql_real_escape_string()`
    - Prevent SQL injection
Web-based Controls Applications

- Web-based Controls Applications
  - Security Issues

- Use
  - User authentication and roles
    - Web site access
    - Relational database access
  - Web site session fixation
    - Force the creation of a known valid session
  - Web site session hijacking
    - Cross-site scripting
    - SQL injection
    - Network eavesdropping
    - Unwitting exposure
    - Forwarding, Proxies, and Phishing
    - Reverse proxy attack
  - Real-time auditing of users’ activities
Web-based Controls Applications

- Web-based Controls Applications
  - Security Issues

- Use
  - L
  - F

- PHF
  - F

- Web
  - F
  - F
  - F
  - F

Apache Reverse Web Proxy:
- Enables one web server to provide content from another transparently.
- Gives encrypted and authenticated access to certain internal web pages. Such as, Elog, archiver, Machine status.

http://internal.com -> https://external.com/internal
Web-based Controls Applications

Apache Reverse Web Proxy:
- Enables one web server to provide content from another transparently.
- Gives encrypted and authenticated access to certain internal web pages, such as, Elog, archiver, Machine status.

http://internal.com -> https://external.com/internal
How does it work?

- RBAC works by giving people roles and assigning the roles permissions to make settings.

- Terminology
- Defining roles
- Defining permissions
What about Industry?

Overview

Critical Infrastructure Protection

Standards & Regulations

The Silence of the Lambs

Raising Awareness
What about Industry?

Overview
(Too?) Many Standards, ...

- "Manufacturing and Control Systems Security"
  (American National Standards Institute & Int'l Society for Measurement and Control)
  (ANSI/ISA SP80)
- "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 17799:2005, BS7799, ISO27000)
- "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)
Overview
(Too?) Many Standards, ...

“Procurement Language”

Manufacturers and vendors are part of the solution!
- Security demands must be included into orders and call for tenders

“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, ...

http://www.msisac.org/scada
What about Industry?

Overview

(Too?) Many Standards, ...

“Procurement Language” document

Manufacturers and vendors are part of the solution!

Security demands must be included into orders and contracts.

Industry & govs start to realize...

...and produced lots of standards:

It's up to you to act!

http://www.msisac.org/cs2/
An overdue technology change:

- Modern control systems take advantage of “office”-IT standards…
- …but also inherit the inherent cyber-risks!

For mitigation, major labs follow a “Defense-in-Depth” approach:

- Network segregation & remote access procedures
- Central installation schemes
- Generalized Authentication & Authorization schemes
Thank you very much!

I would like to thank all presenters and participants, making this workshop such a success.

► Special thanks go to Karen, Lori, David & colleagues for the organization !!