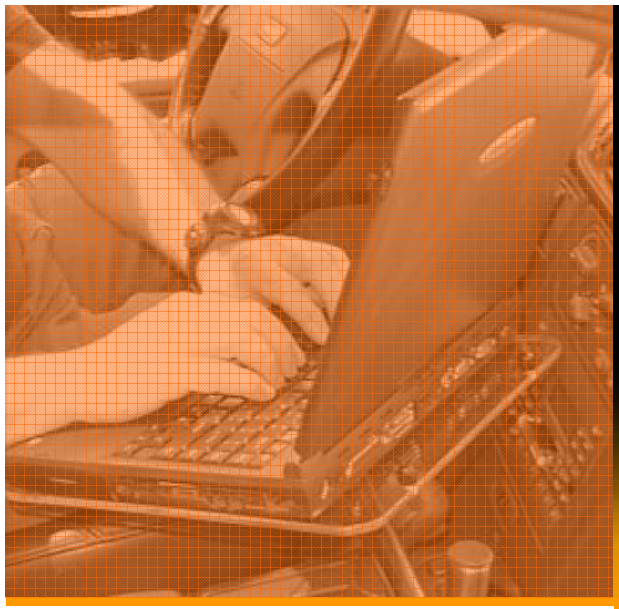
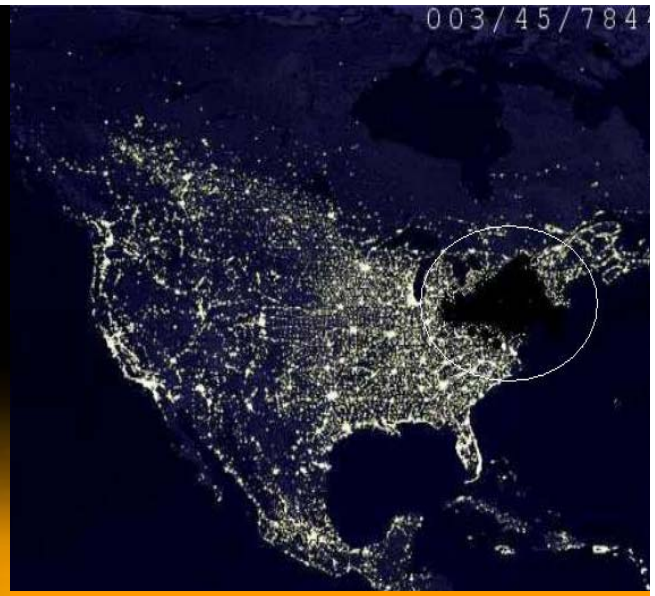




(CS)² HEP Control System Cyber-Security Workshop

A Summary of Yesterday's Meeting

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

The Past:
The (R)Evolution of Control Systems

The Present:
What about Security !?

The Future:
Control System Cyber-Security

Risk = Threat

× Vulnerability

× Consequence

(CS)² in HEP — The Agenda

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

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

(CS)² in HEP — The Agenda

09:05-09:30 (00h25')	[11] **Cyber-Threats, Cyber-Vulnerabilities, and Cyber-Risks**	Dr. Stefan LUEDERS (CERN)
09:30-10:00 (00h30')	[9] **Network and computer security in the Fermilab Accelerator Control System**	Tim ZINGELMAN (Fermi National Accelerator Lab)
10:00-10:30 (00h30		
10:45-11:15 (00h30		
11:15-11:45 (00h30		
11:45-12:15 (00h30		
14:00-14:30 (00h30')	[15] **SLAC Controls Security Overview**	Terri LAHEY (SLAC)
14:30-15:00 (00h30')	[4] **Role Based Access Control for the Accelerator Control System at CERN**	Mrs. Suzanne GYSIN (FNAL)
15:00-15:30 (00h30')	[10] **WARCS -Wide Area Remote Control for SPring-8**	Dr. Akihiro YAMASHITA (SPring-8)
15:45-16:15 (00h30')	[8] **Secure Remote Operation of Light Source Beamline Controls with FreeNX**	Mr. Zhijian YIN (Brookhaven National Lab)
16:15-16:45 (00h30')	[14] **Accelerator Control-System Network Security at Diamond Light Source**	Dr. Mike LEECH (Diamond Light Source)
16:45-17:15 (00h30')	[13] **Control System Cyber-Security in Industry**	Dr. Stefan LUEDERS (CERN)

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

(CS)² in HEP — The Agenda

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

09:05-09:30 (00h25') [11] **Cyber-Threats, Cyber-Vulnerabilities, and Cyber-Risks** Dr. Stefan LUEDERS (CERN)

09:30-10:00 (00h30') [9] **Network and computer security in the Fermilab Accelerator Control System** Tim ZINGELMAN (Fermi National Accel

10:00-10:30 (00h30

14:00-14:30 (00h30') [15] **SLAC Controls Security Overview**

14:30-15:00 (00h30') [4] **Role Based Access Control for the Accelerator Control System at CERN**

10:45-11:15 (00h30

15:00-15:30 (00h30') [10] **WARCS -Wide Area Remote Control for SPring-8** Dr. Akihiro YAMASHITA (SPring-8)

11:15-11:45 (00h30

15:45-16:15 (00h30') [8] **Secure Remote Operation of Light Source Beamline Controls with FreeNX** Mr. Zh

11:45-12:15 (00h30

16:15-16:45 (00h30') [14] **Accelerator Control-System Network Security at Diamond Light Source** Dr. Mike LEECH (Diamond Light Source)

16:45-17:15 (00h30') [13] **Control System Cyber-Security in Industry**

Security Strategies

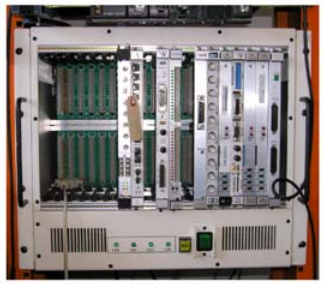
Mrs. Suzanne GYSIN (FNAL)

Authentication & Authorization

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

APS Control System

Accelerator IOC



- 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

Variety & Diversity in Products

APS Control System

Accelerator IOC

- Linac, PAR, Booster and Storage Ring
  - 80
  - App
  - EPI dist
  - Mor
  - Ove
  - Nea
- Beamline
  - Bea pos sen
  - Nea per

Standards, if possible !

"CNIC Status Report" — Dr. Stefan Lüders — (CS)2/HEP Workshop — October 14th 2007

Commercial of the shelf hardware

standard desktop PCs

SIEMENS, TRANE, Sun microsystems, CAEN, Linde, AIR LIQUIDE, WAGO, CES, applicom, iseg, Tektronix, Schneider Electric, BECKHOFF, acqiris, NATIONAL INSTRUMENTS, HIRSCHMANN, LeCroy, WIENER

Standard (controls) software

CORBA, redhat LINUX, CVS, WinCC, PcVue, ORACLE, PVSS II, Microsoft, LynxOS, Wizcon, MySQL, SONICMQ®

Standard communication protocols

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

Argonne NATIONAL LABORATORY

Variety & Diversity in Products

APS Control System

Accelerator IOC

- Linac, PAR, Booster and Storage Ring
  - 80
  - App
  - EPI dist
  - Mo
  - Ove
  - Nea
- Beamline
  - Bea pos sen
  - Nea per

Standards, if possible

"CNIC Status Report" — Dr. Stefan Lüders — (CS)2/HEP Workshop — October 14th 2007

Commercial of the shelf hardware

standard desktop PCs

SIEMENS, TRANE, CAEN, Linde, AIR LIQUIDE, WAGO, CES, applicom, Tektronix, Schneider Electric, BECKHOFF, acqiris, NATIONAL INSTRUMENTS, HIRSCHMANN, LeCroy, WIENER

Standard (controls) software

CORBA, redhat LINUX, CVS, WinCC, PcVue, ORACLE, PVSS II, Microsoft, LynxOS, Wizcon, MySQL

Standard communication protocols

OPC FOUNDATION, WorldFIP, IEEE 1394, BUS, W3C, PROFIBUS, Modbus-IDA, PCI EXPRESS, VMEbus

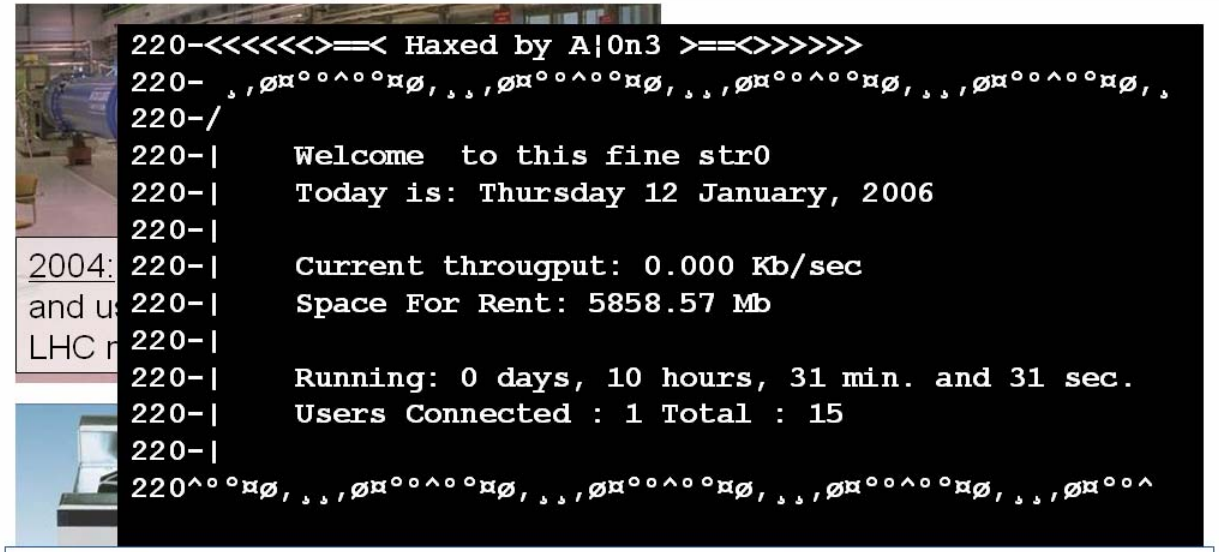
Multitude of hardware, ...

...O/S, applications, and protocols !

Argonne NATIONAL LABORATORY

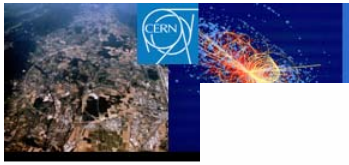
Balance Risk, Safety & Usability

Vulnerabilities ARE fact !



Management buy-in !

Balance Risk, Safety & Usability



Vulnerabilities ARE fact !

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

Vulnerabilities ARE fact !

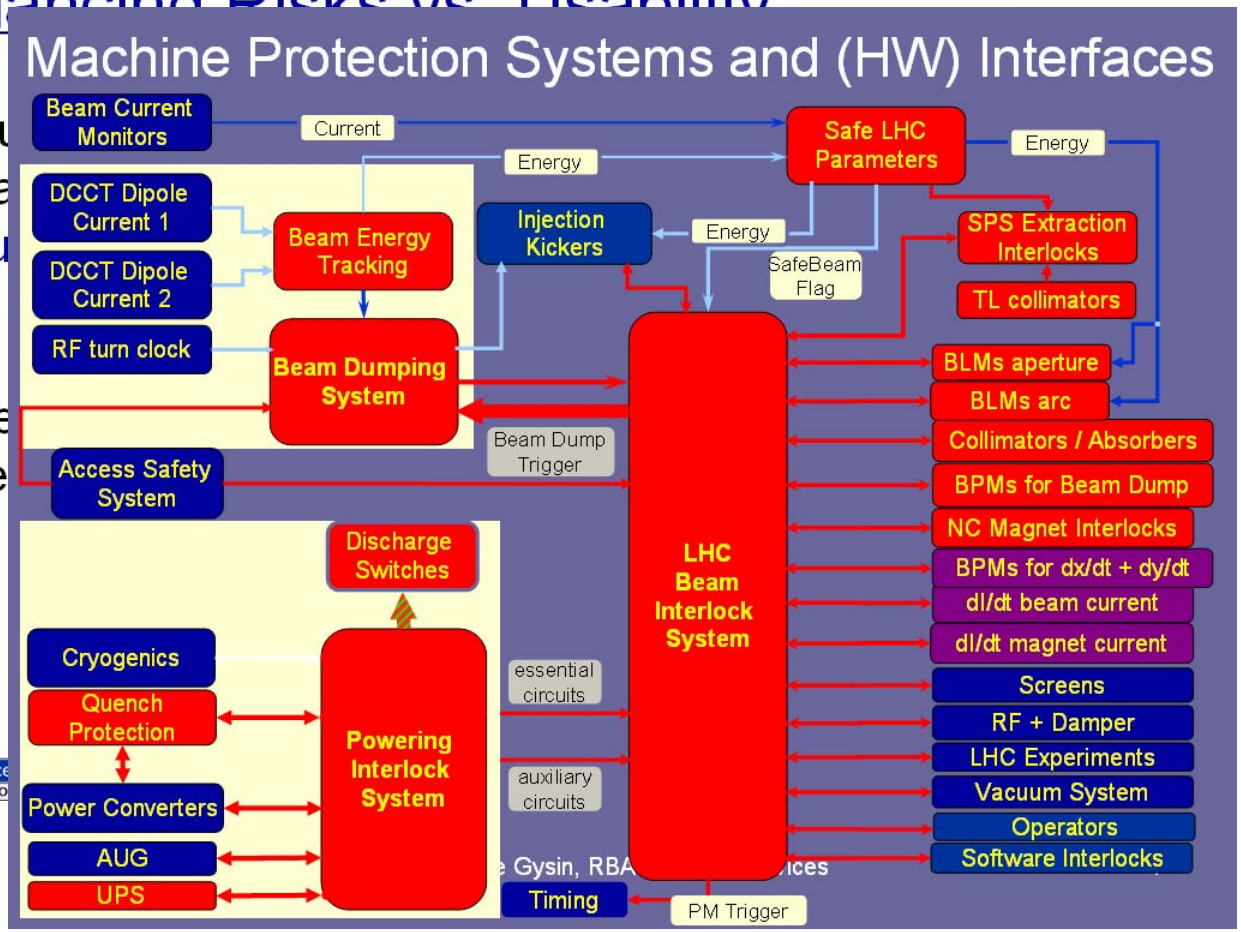
II. Balancing Risks vs. Usability

- Redu
  threa
  disru
  also
- More
  cybe

Ma

Fermi National Acce
ACCELERATO

Machine Protection Systems and (HW) Interfaces



Balance Risk, Safety & Usability

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

Vulnerabilities ARE fact !

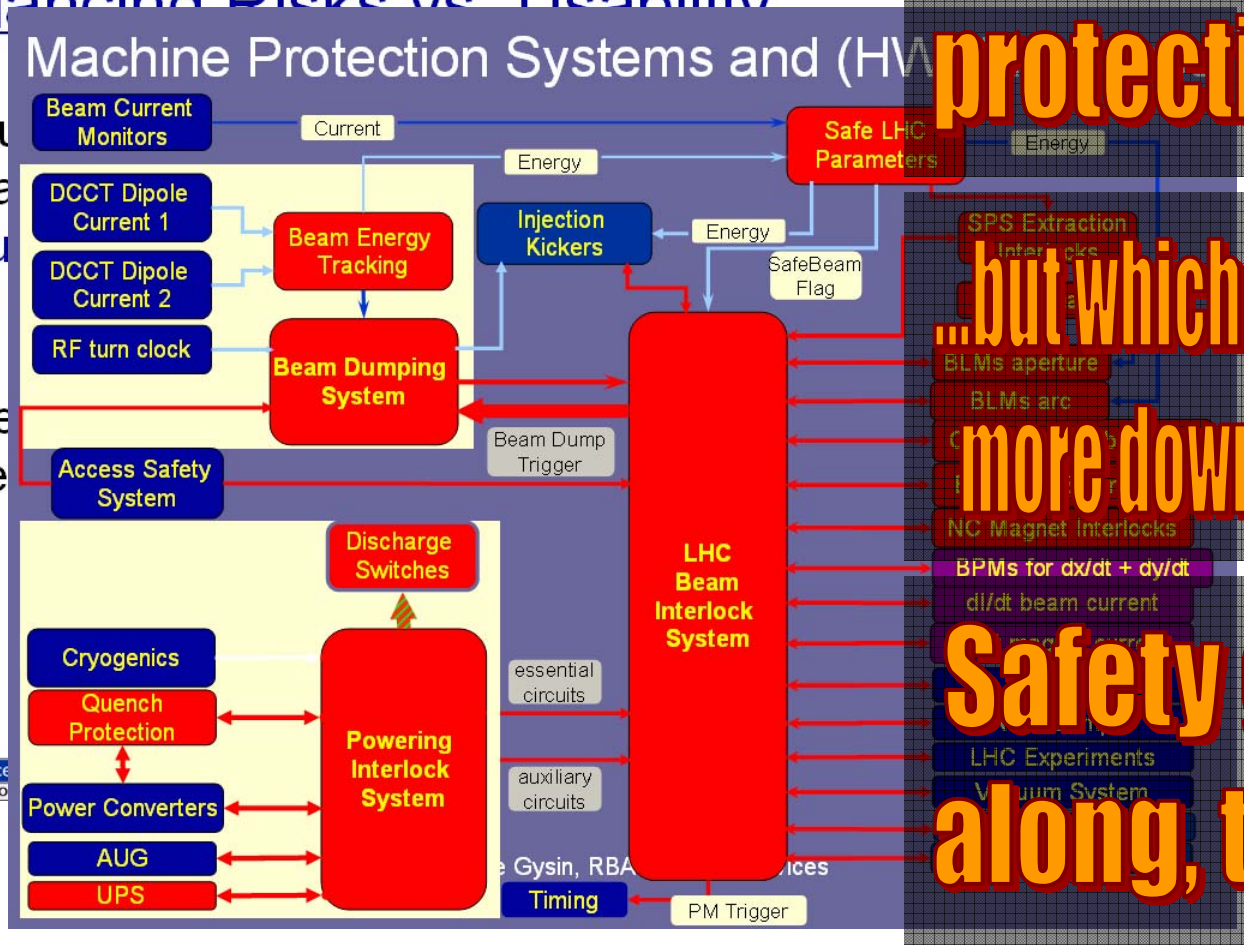
II. Balancing Risks vs. Usability

- Redu
  threa
  disru
  also
- More
  cybe

Ma

Fermi National Acce
ACCELERATO

Machine Protection Systems and (HW

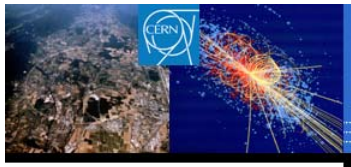


Threats & protections...

...but which creates more downtime ?

Safety goes along, too !!!

Defense-In-Depth



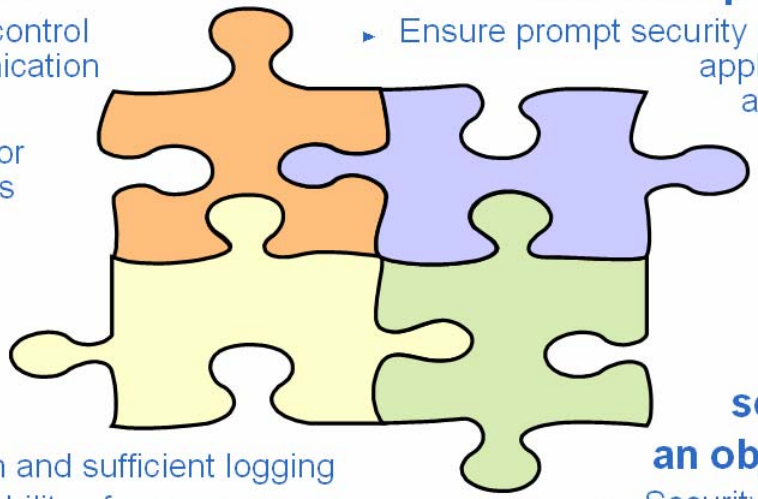
Ground Rules for Cyber-Security

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.



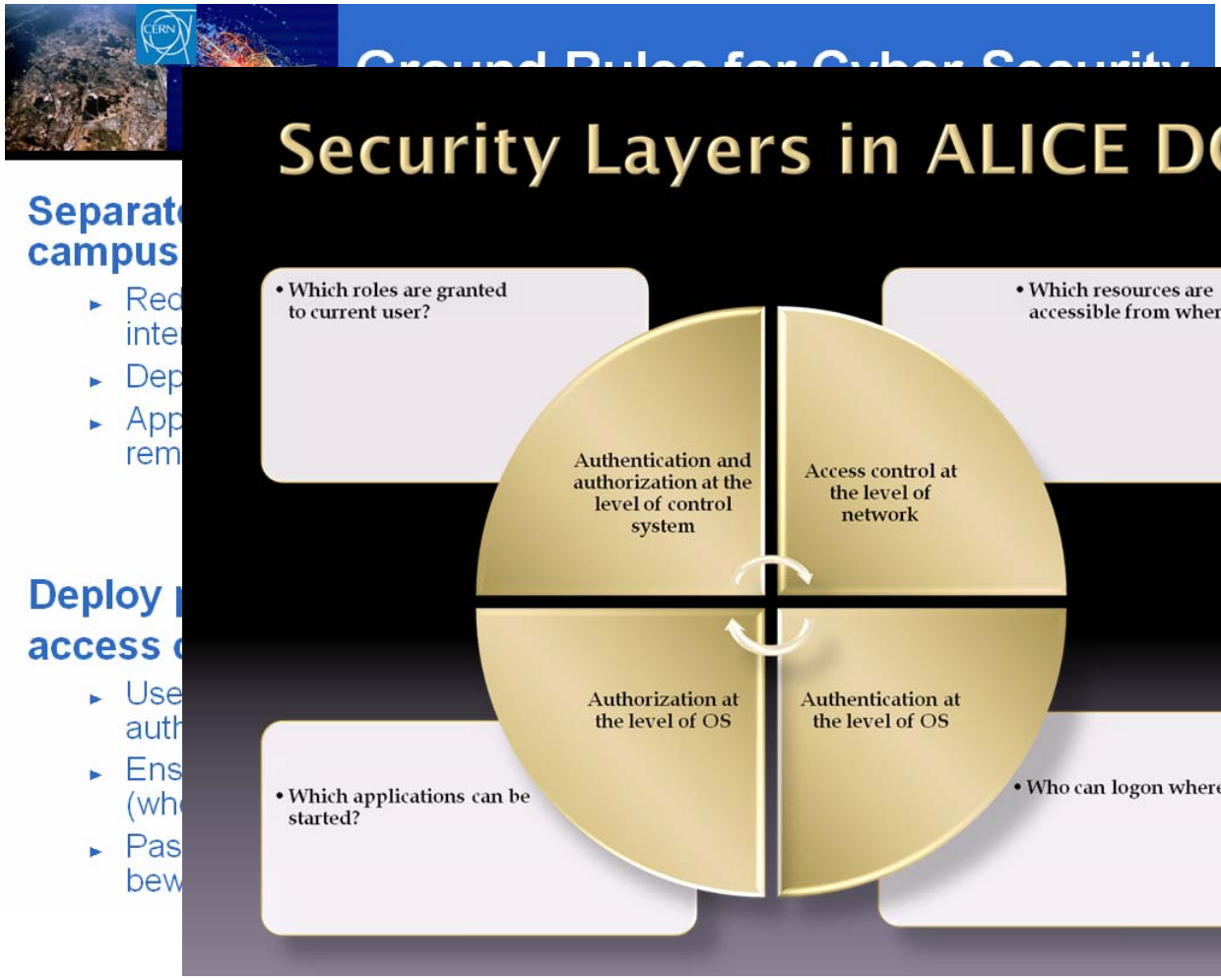
Deploy proper access control

- Use strong authentication and sufficient logging
- Ensure traceability of access (who, when, and from where)
- Passwords must be kept secret: beware of "Google Hacking"

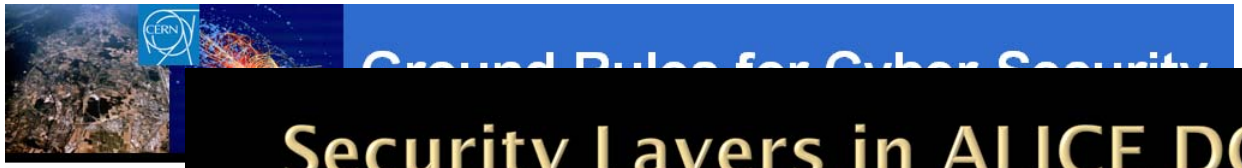
Make security an objective

- Security training
- Management buy-in
- Bring together IT and Controls experts

Defense-In-Depth



Defense-In-Depth



Ground Rules for Cyber Security

Separat
campus
- Red
inte
- Dep
- App
rem

Deploy
access
- Use
auth
- Ens
(wh
- Pas
bew

Security Layers in ALICE DCS

• Which roles
to current us

• Which appli
started?

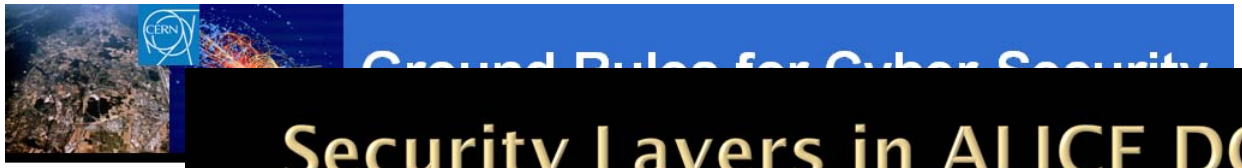
LCLS

Stanford Linear Accelerator Center
Stanford Synchrotron Radiation Laboratory

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



Ground Rules for Cyber Security

Separat
campus
- Red
inte
- Dep
- App
rem

Deploy
access
- Use
auth
- Ens
(wh
- Pas
bew

Security Layers in ALICE DCS

- Which roles
to current us

- Which appli
started?

Stanford Linear Acc
Stanford Synchrotron Radiat

Conclusion

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

October 14, 2007 8 Ter
Control System Cyber-Security Workshop lahey@slac.

Network Segregation

Central PC Management

Authentication &

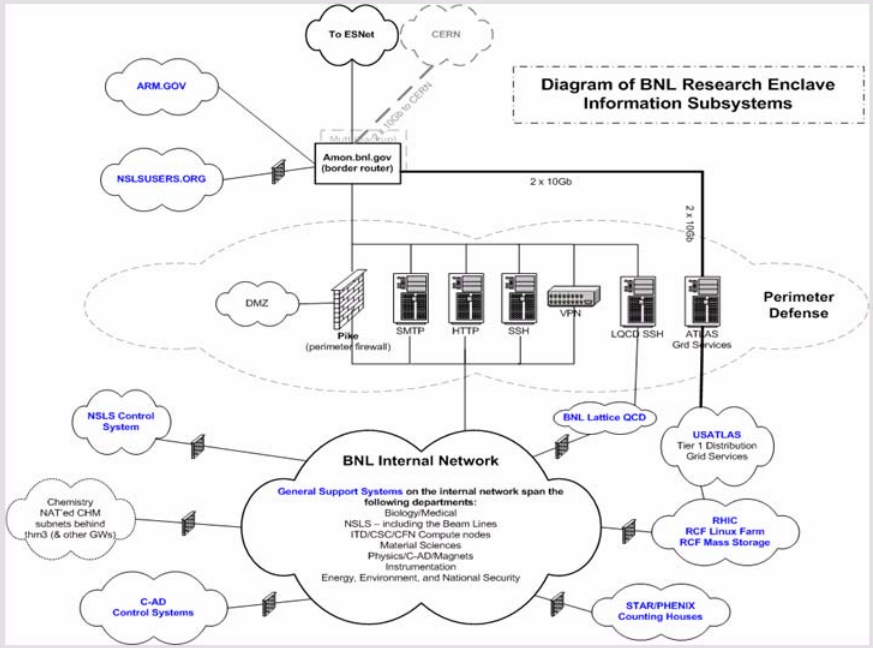
Authorization

Controls & IT

experts together

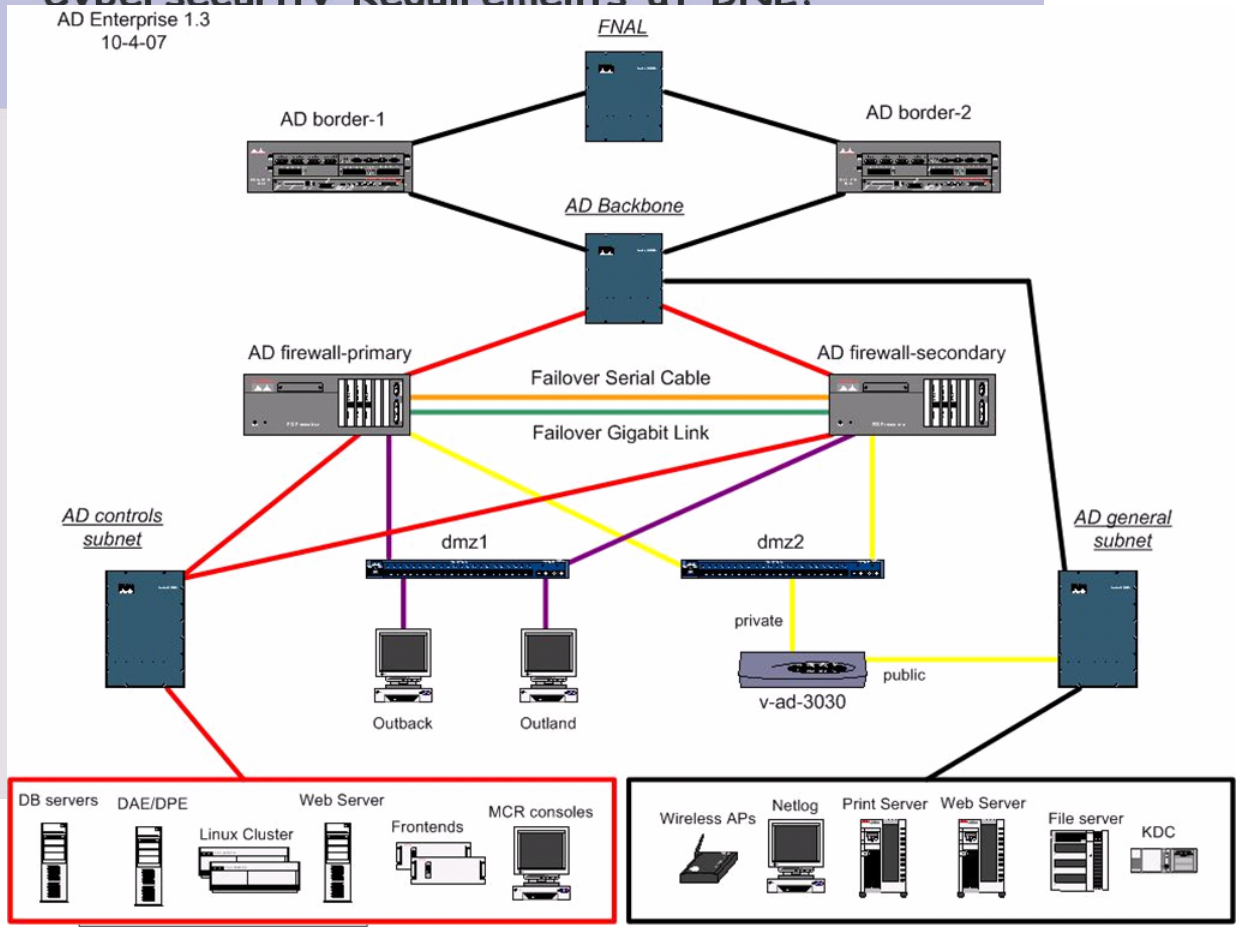
Network Segregation

Cybersecurity Requirements at BNL: Perimeter Defense



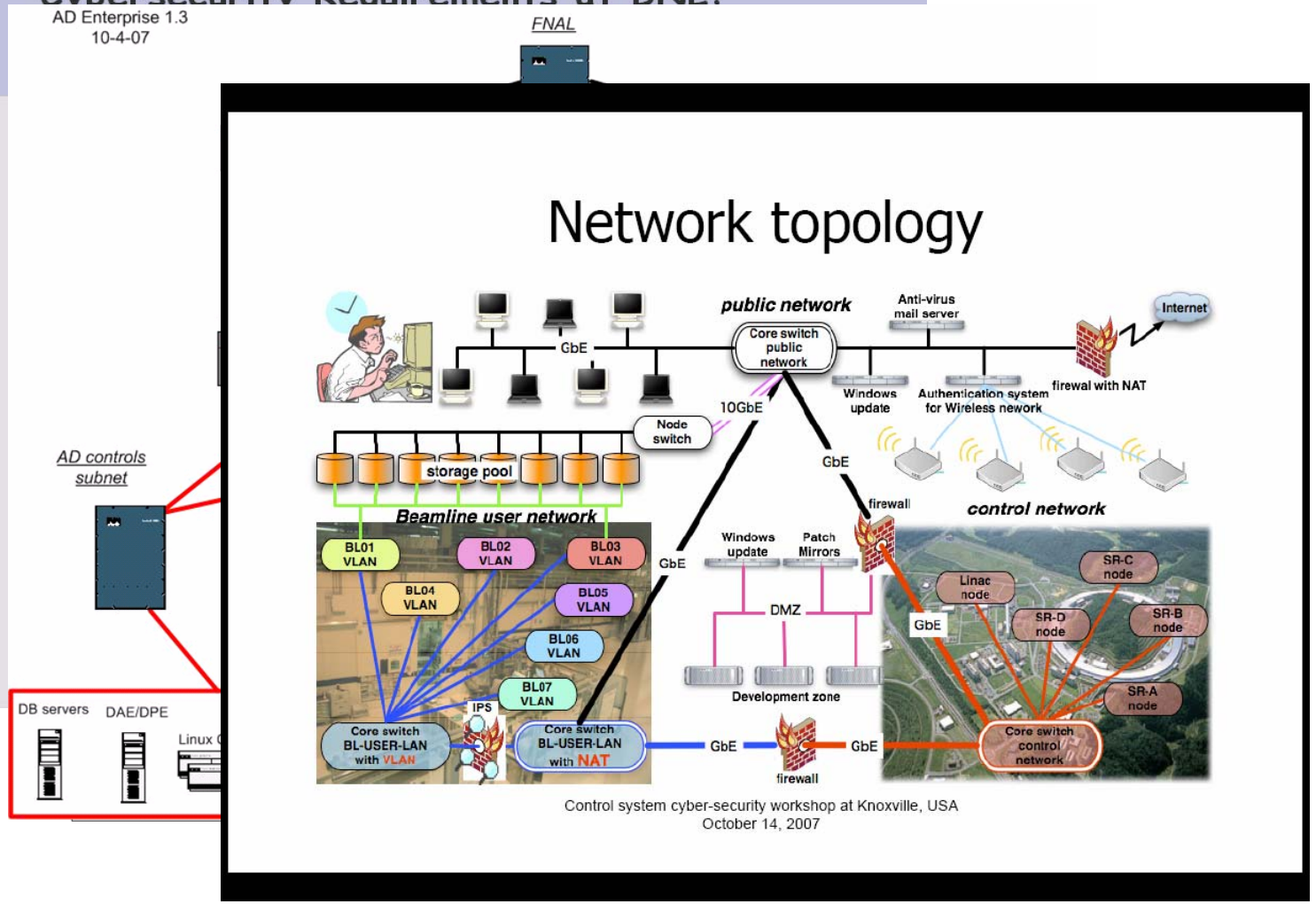
Network Segregation

Cybersecurity Requirements at BNL:



Network Segregation

Cybersecurity Requirements at BNL:



Network Segregation

Cybersecurity Requirements at BNL:

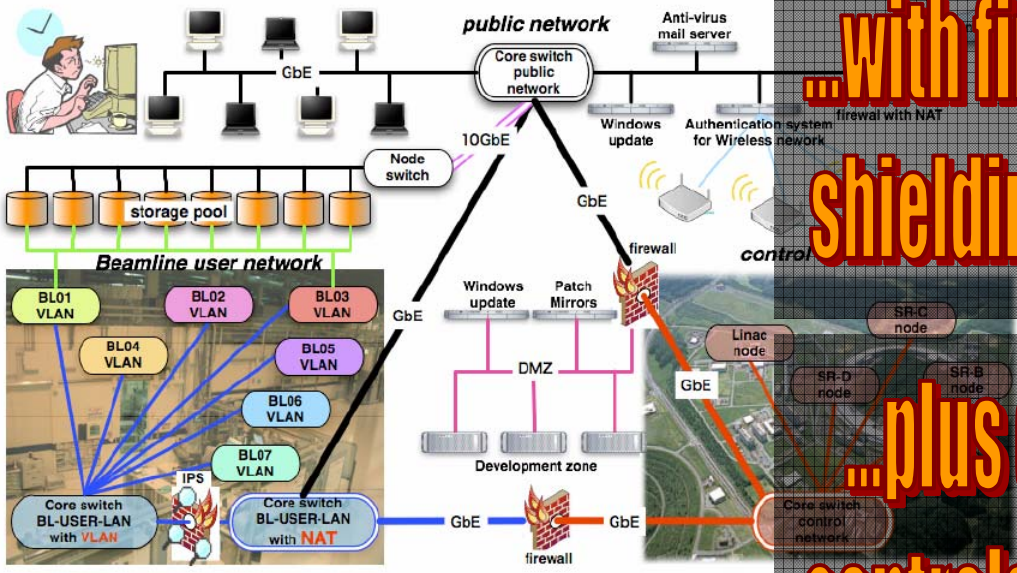
AD Enterprise 1.3
10-4-07

FNAL

AD controls subnet

DB servers DAE/DPE Linux

Network topology



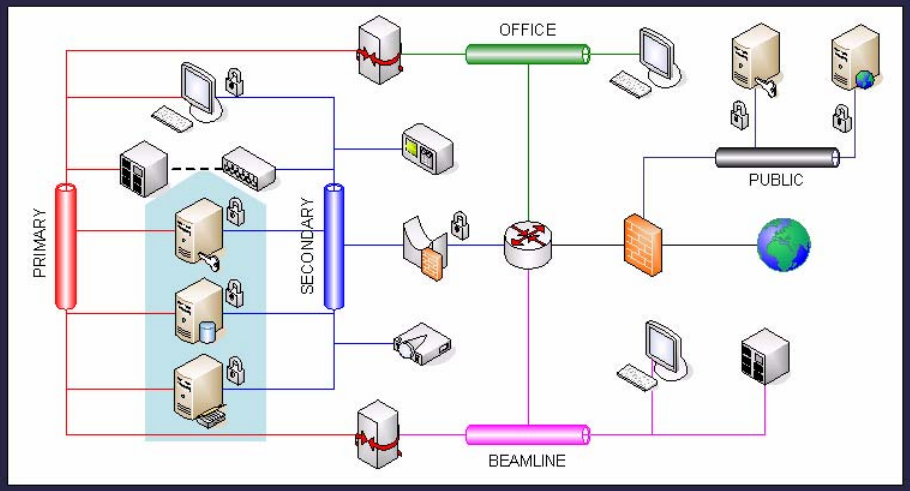
Control system cyber-security workshop at Knoxville, USA
October 14, 2007

Strong perimeter protection...

...with firewalls and shielding routers...

...plus dedicated controls networks!

Rules for Remote Access

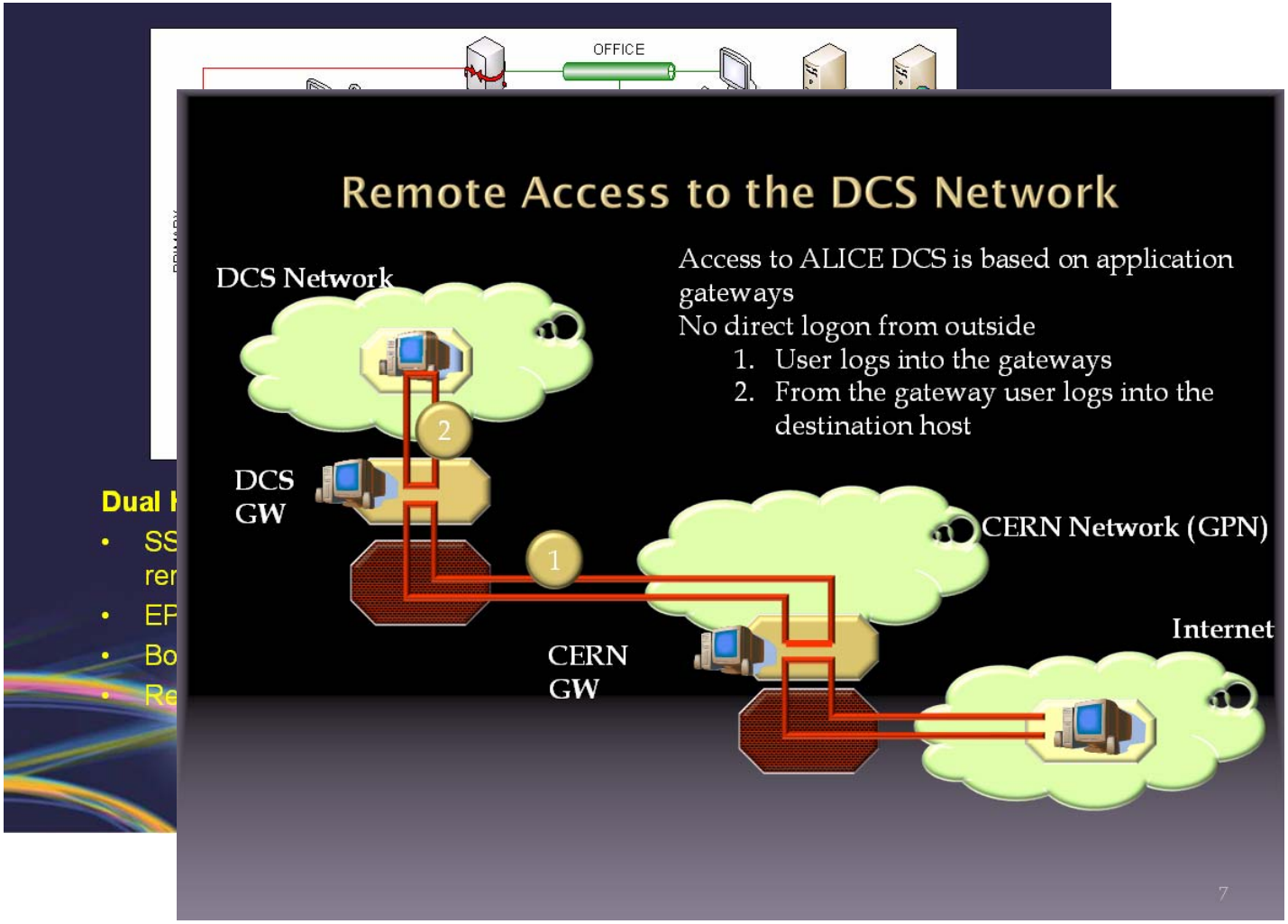


Dual Homed Servers:

- 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

diamond

Rules for Remote Access



Rules for Remote Access

OFFICE

Remote Access to the DCS Network

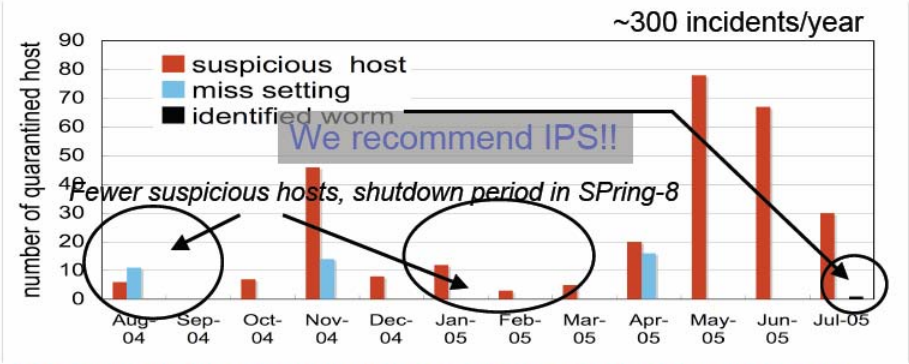
DCS Networ

DCS GW

Dual

- SS
- EF
- Bo
- Re

Statistics on IPS



Most incidents had shown undesirable behavior such as sweep port scan

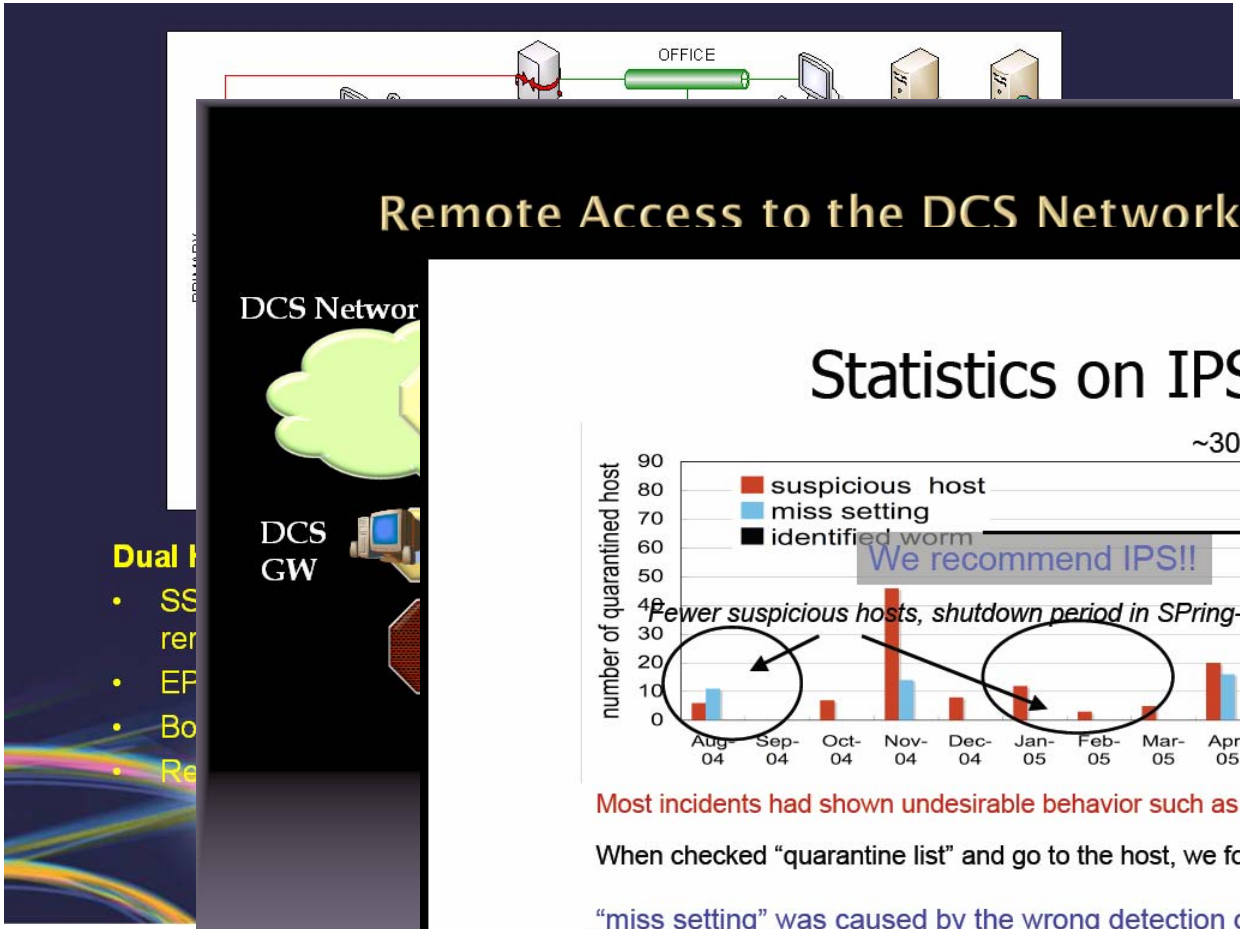
When checked "quarantine list" and go to the host, we found "Trojan Horse"

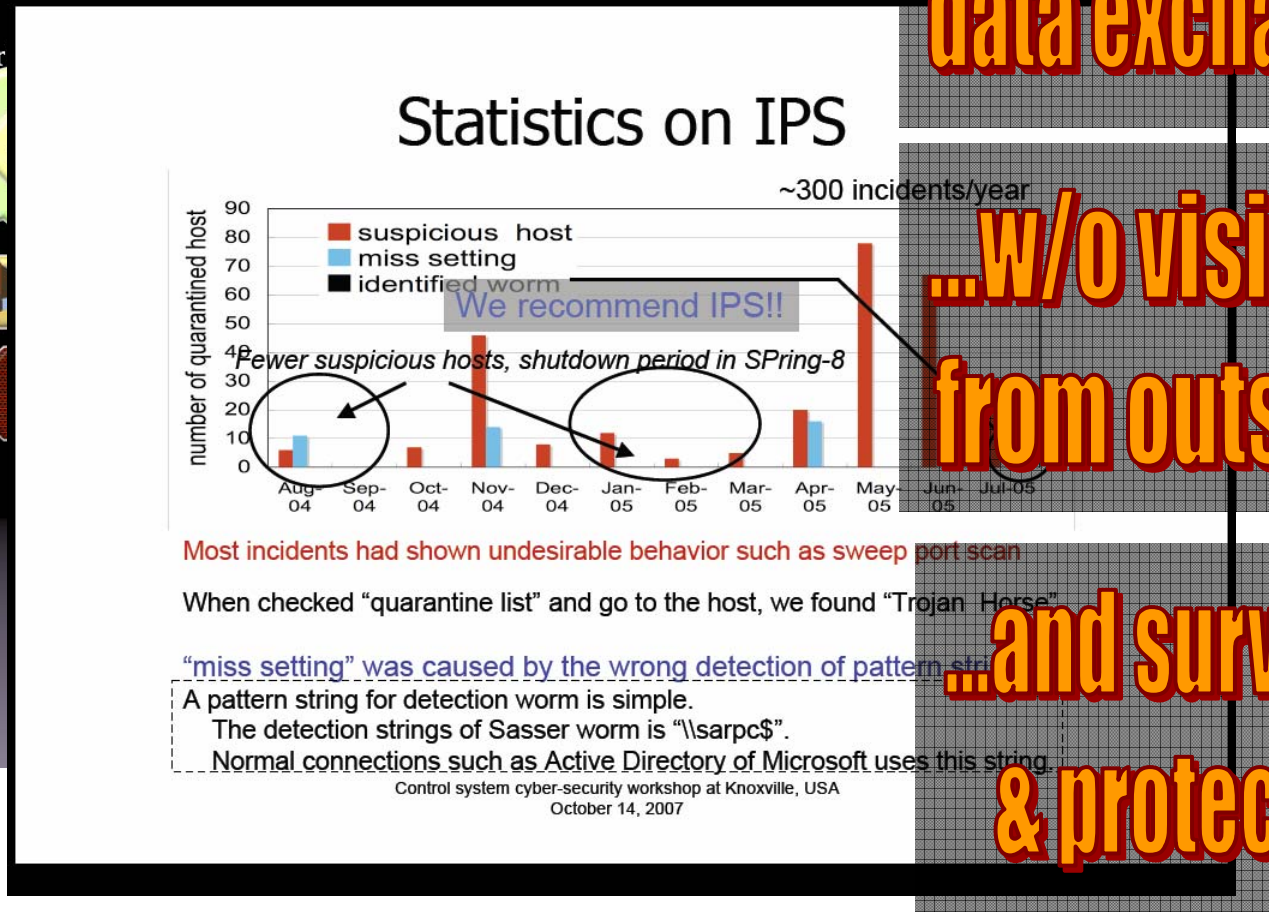
"miss setting" was caused by the wrong detection of pattern string.

A pattern string for detection worm is simple.
The detection strings of Sasser worm is "\\sarpc$".
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





Controlled data exchange...

...w/o visibility from outside...

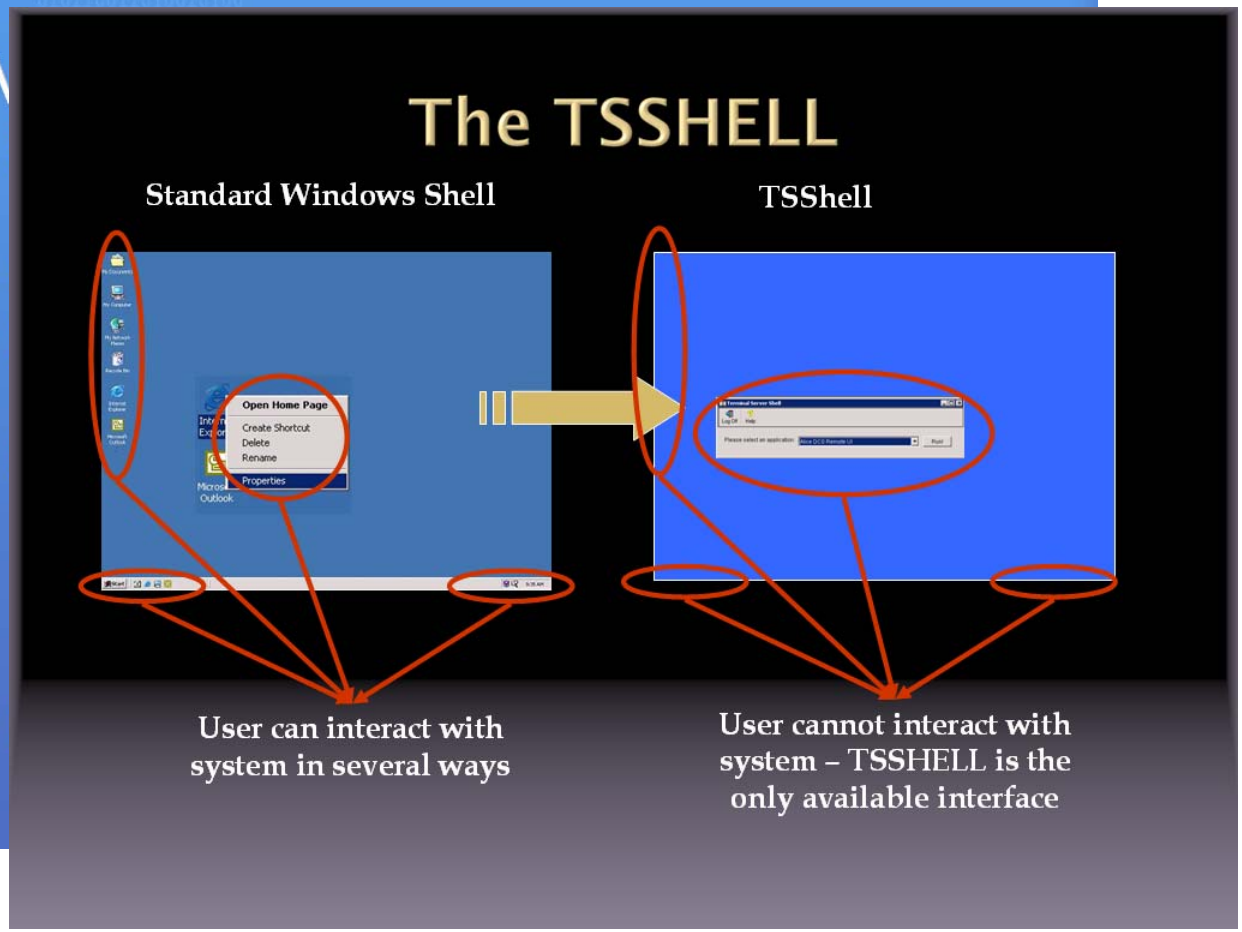
...and surveilled & protected !

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

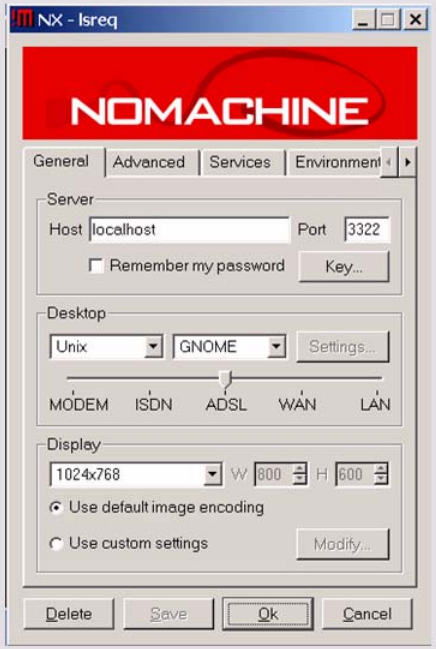
VNC (Virtual Network Computer)

- 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
  - Ultr@VNC 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.


The TSSHELL
Standard Windows Shell
TSShell
Open Home Page
Create Shortcut
Delete
Rename
Properties
User can interact with system in several ways
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,
  ssh -L 3322:lsx21pc.nsls.bnl.gov:22
  zyin@ssh.bnl.gov
- Leave the terminal open
- Configure NoMachine NX client
  localhost port 3322

Remote Access Tools

Standards like VPN, ...

...VNC (ev. inside SSH), ...

...terminal server, or...

...customized remote X via SSH !

Central PC Management

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

Central Installation Schemes (2)

"CNIC Status Report" — Dr. Stefan Lüders — (CS)2/HEP Workshop — October 14th 2007

Install…

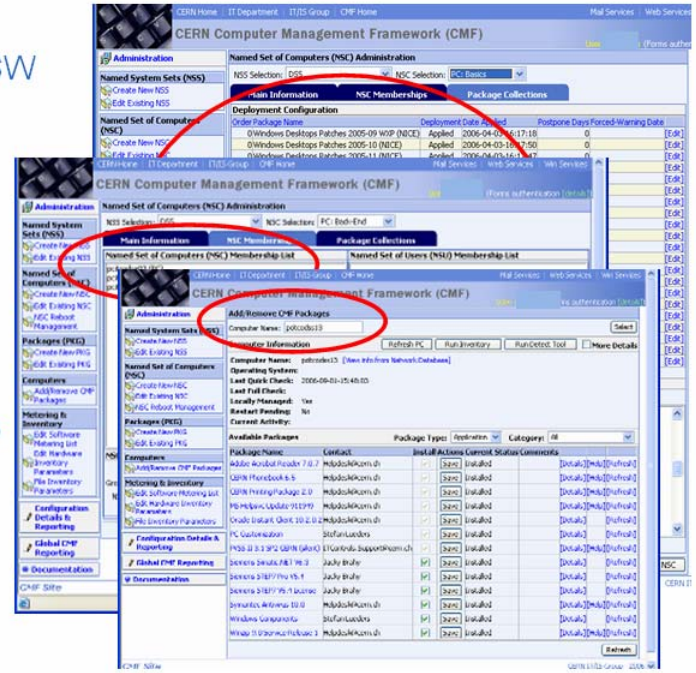
- Centrally managed OS & SW
- User applications
- Automatically & network-based
- On many PCs in parallel

Configure…

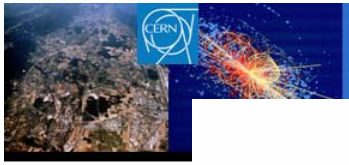
- Look & Feel
- Access rights & restrictions

Full remote control of…

- Configuring
- Installation
- Patching
- Rebooting



… this works even for oscilloscopes !!!



Central Installation Schemes (2)

Install…

- Cent
- User
- Autc netw
- On r

Configur

- Look
- Acce

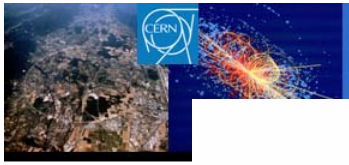
Full rem

- Conf
- Insta
- Patc
- Reb

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)

Install…

- Cent
- User
- Autc netw
- On r

Configur

- Look
- Acce

Full remo

- Conf
- Insta
- Patc
- Reb

IV. OS/Application Layer Protection

- Linux s and Ap
- Windo service Syster
- FreeB and ve have 'p

Fermi National Accelera
ACCELERATOR DIV

Patch management

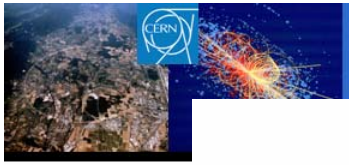
- Windows update, anti-virus software update server
  - push patches into clients

  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.

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

Central PC Management



Central Installation Schemes (2)

Install...
- Cent
- User
- Autc netw
- On r

Configur
- Look
- Acce

Full rem
- Conf
- Insta
- Patc
- Reb

IV. OS/Application Layer Protection

- Linux s and Ap
- Windo service Syster
- FreeB and ve have 'p

Fermi National Accelera
ACCELERATOR DIV

Patch management

- Windows update, anti-virus software update 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, daq front-end, etc.

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

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_set_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

- 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

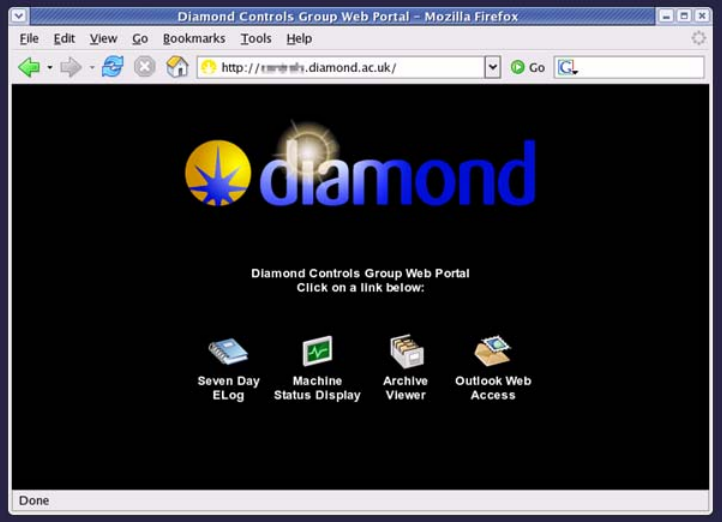
Web-based Technologies

Web-based Controls Applications

- Web
- Use
- PHP
- Rea

Web-based Controls Applications - Security issues

- Use
- Web
- Web



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

diamond

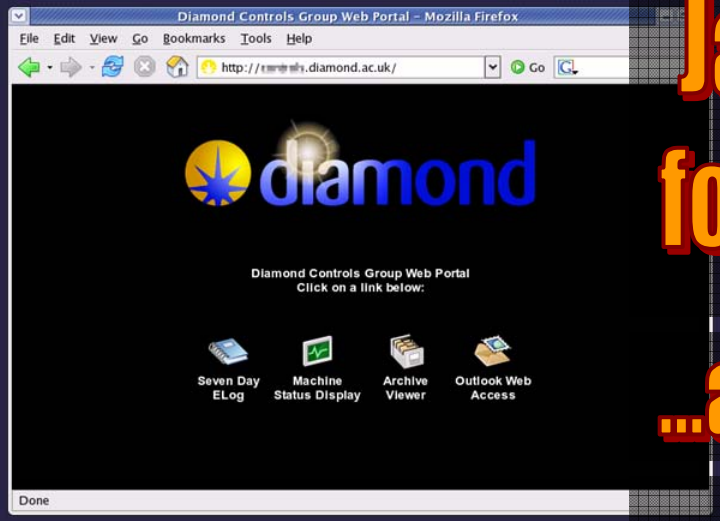
Argonne NATIONAL LABORATORY

Argonne NATIONAL LABORATORY

Web-based Technologies

Web-based Controls Applications

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

XML, PHP, Java, MySQL, for controls ...

...are risky and...

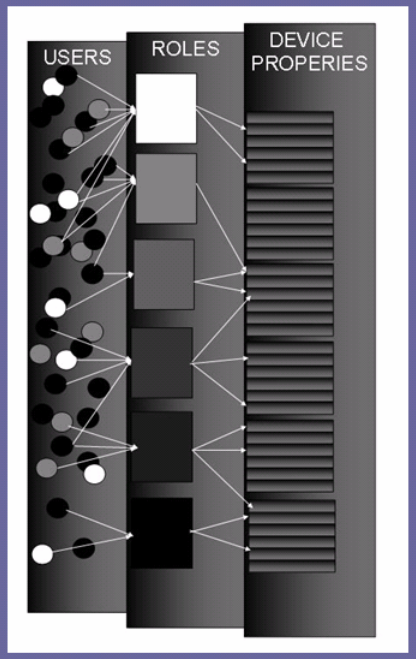
...need special security strategies!

Authentication & Authorization

How does it work?

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

- Terminology
- Defining roles
- Defining permissions



2007-10-15 Suzanne Gysin, RBAC for LHC devices 6

RBAC...

...on the O/S level, ...

...the SCADA system, and...

...at the front-end !

What about Industry ?

Overview

Critical Infrastructure Protection

Standards & Regulations

The Silence of the Lambs

Raising Awareness

What about Industry ?

Overview

(Too?) Many Standards, …

Critic

Stan

The

Rai

- "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 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)

What about Industry ?

Overview

(Too?) Many Standards, …

"Procurement Language"

Critic

Stan

The

Rai

- "Manufa
  (American
  (ANSI/ISA
- "Good P
  (U.K. Cent
- "Code c
  (Int'l Organ
  (ISO/IEC 1
- "Guide
  Industri
  (U.S. Natio
- "Systen
- Commc
- "Cyber-
  (U.S. Chen
- "Good A
  System
- NERC 8
  (North Ame

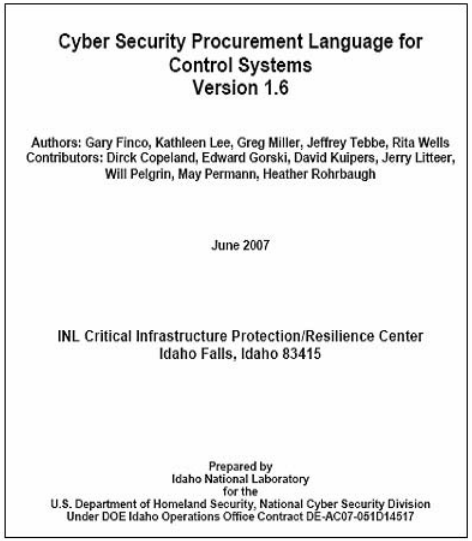
Manufacturers and vendors are part of the solution !

- 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

What about Industry ?

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

Overview

(Too?) Many Standards, …

"Procurement …

Industry & govs start to realize…

…and produced lots of standards:

It's up to you to act !

Critic…

Stan…

The …

Rai…

- "Manufa… (American… (ANSI/ISA…
- "Good P… (U.K. Cent…
- "Code o… (Int'l Organ… (ISO/IEC 1…
- "Guide … Industri… (U.S. Natio…
- "Systen…
- Commo…
- "Cyber-… (U.S. Chen…
- "Good A… System…
- NERC &… (North Ame…

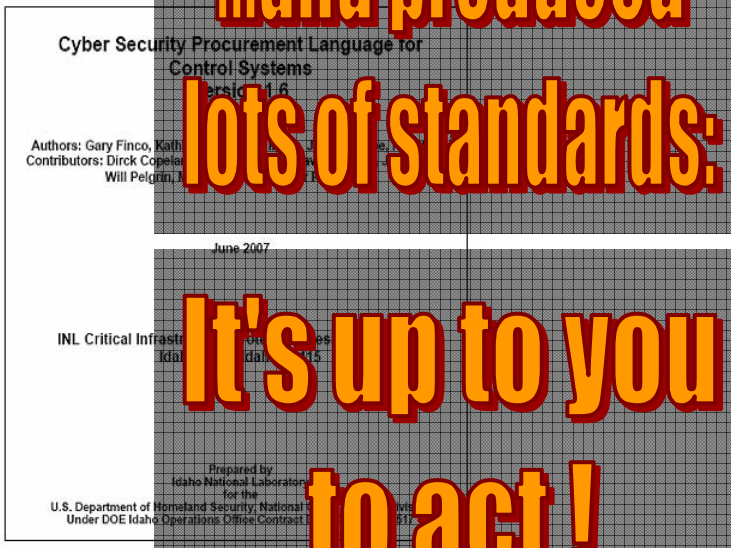
Manufacturers and vendors are part of the solution !

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

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, …



http://www.msisac.org/scada

Summary

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

You are not alone !

Let's tackle the problem together !!!

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 !!!