



4th Control System Cyber-Security Workshop

More “discipline” is what we need.

Dr. Stefan Lüders (CERN Computer Security Officer)

with contributions from

S. Banerin (UW School of Medicine), E. Bonaccorsi (LHCb),
E. Carrone (SLAC), P. Chochula (ALICE), S. Gysin (ESS),
R. Krempaska (PSI), T. Sugimoto (Spring8), F. Tilaro (CERN)

ICALEPCS, San Francisco (California), October 7th 2013





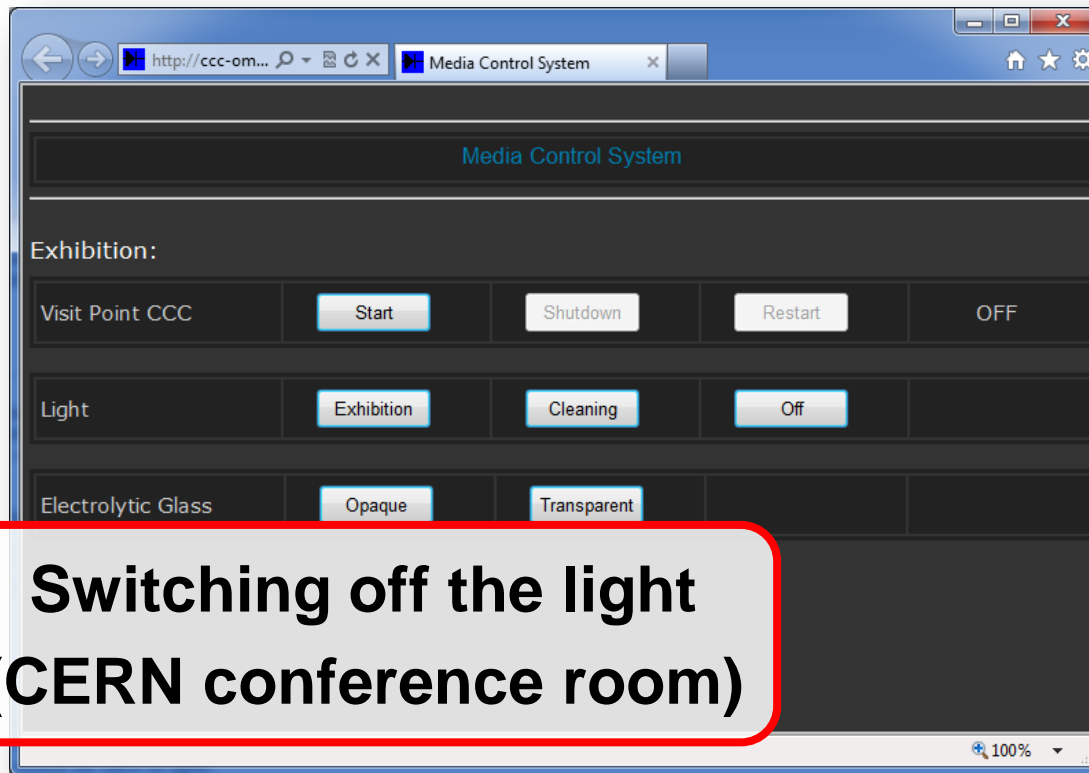
Why Control System Cyber-Security...

“4th CS2/HEP Workshop Summary” — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013



Why Control System Cyber-Security...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

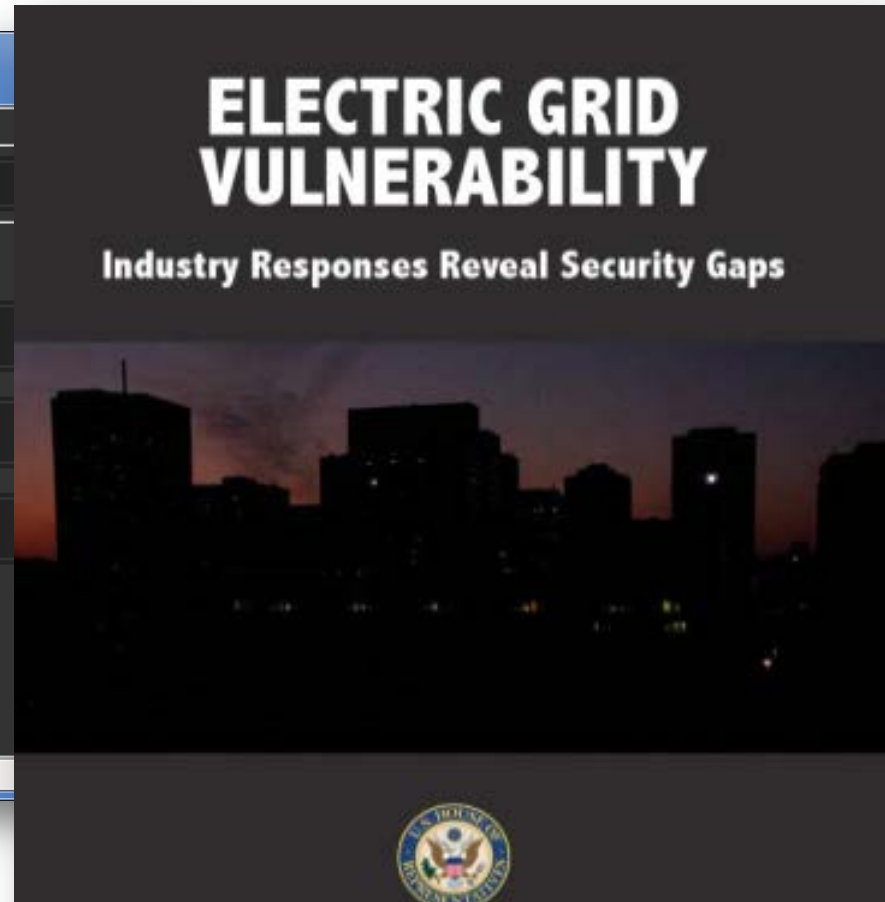
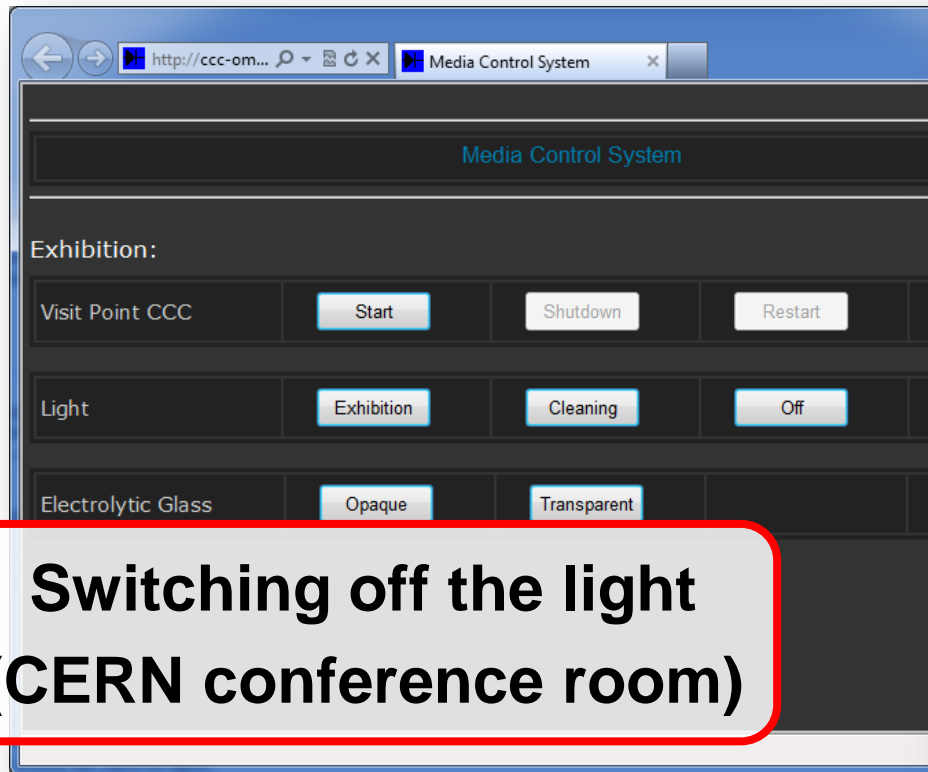


**Switching off the light
(CERN conference room)**



Why Control System Cyber-Security...

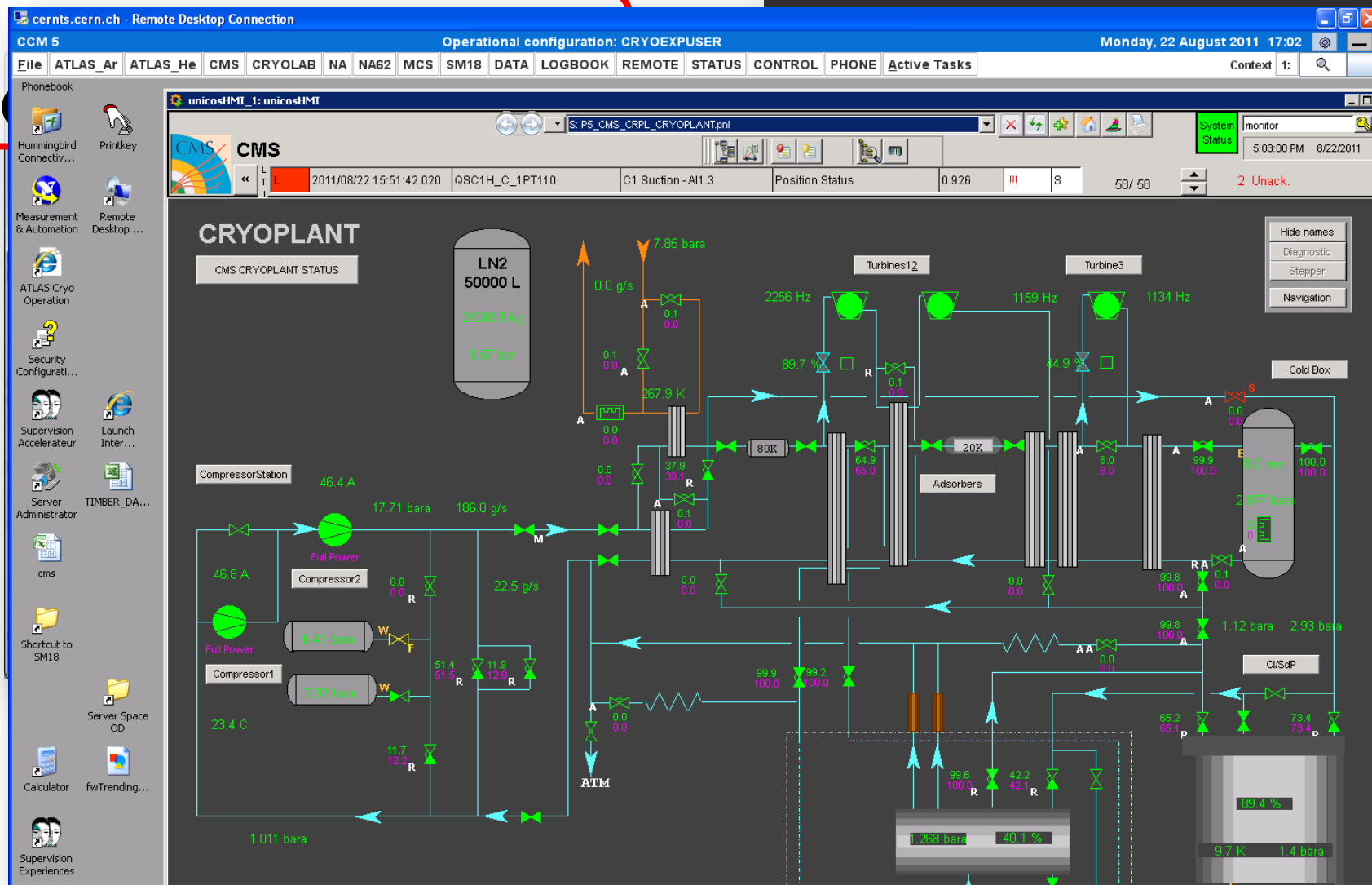
"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013



Switching off the light (US cities)
<http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf>



“4th CS2/HEP Workshop Summary” — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013





Why Control System Cyber-Security...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

cernts.cern.ch - Remote Desktop Connection

Operational configuration: CRYOEXPUSER

Monday, 22 August 2011 17:02

File ATLAS_Ar ATLAS_He CMS CRYOLAB NA NA62 MCS SM18 DATA LOGBOOK REMOTE STATUS CONTROL PHONE Active Tasks

Phonebook

Hummingbird Connectiv... Printkey

Measurement & Automation Remote Desktop ...

ATLAS Cryo Operation

Security Configurati...

Supervision Accelérateur Launch Inter...

Server Administrator TIMBER_DA...

cms

Shortcut to SM18

Calculator fwTrending...

Supervision Experiences

unicosHMI_1: unicosHMI

CMS

2011/08/22 15:51:42.020 QSC1H_C_1PT110

CRYOPLANT

CMS CRYOPLANT STATUS

LN2 50000 L

21048.5 kg

6.57 bar

CompressorStation 46.4 A

17.71 bara 186.0 g/s

Full Power

Compressor2 46.8 A

22.5 g/s

Compressor1 51.5 R 120 R

1.011 bara

ATM

1.265 bara 40.1 %

9.7 k 1.4 bara

Twitter / @reversemode: Writing a post involving CERN, LHC, SCADA, passwords... one of the most curious cases I've found.

Don't miss any updates from Rubén Santamarta

Get your account on Twitter today to stay up-to-date with what interests you!

Sign up »

Text follow reversemode to 40404 in the United States

@reversemode Rubén Santamarta

Writing a post involving CERN, LHC, SCADA, passwords... one of the most curious cases I've found.

9 Aug via TweetDeck

About Help Blog Status Jobs Terms Privacy Advertisers Businesses Media Developers Resources © 2011 Twitter

Switching off accelerators!



...needs a disciplined approach!

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Acceptance Factors

SLAC

Implementation of Cyber Security is hard:

Not much love from **users** (aka "*I need to access the machine and change the beam parameters on my iphone while I'm waiting for the traffic light to become green*" syndrome).

Not much love from **organizations removed from Engineering**: we do theoretical [*insert any hard science here*] and data analysis, we don't need all this CS controls.

Not much love from **Cost Account Managers**: Whoa! These **Cyber Security** guys are so expensive! This facility has been up from [*insert any time after WWII*] without any problem...!



With some discipline, people managed to have...

“4th CS2/HEP Workshop Summary” — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013





Are we really autonomous?

- Absence of external services could trigger immediate shutdown

- Pixel detectors might melt in absence of cooling
- Photon spectrometer might freeze if frontend electronics turns off while cooling is present

...full network segregation & firewalling (*Alice, LHCb, PSI*)

Network Security implementation



PAUL SCHENNER INSTITUT **Control System Network Security**

Controls Network and Rules

- Control system for accelerators is separated in private machine networks.
- Control system for SLS beamlines is in separated sub-nets, behind a firewall. Users from one beamline cannot influence the control system of another beamline.

Alice, LHCB, PS



With some discipline, people managed to have...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Are we really autonomous?

- Absence of external services could trigger immediate shutdown
 - Pixel detectors might melt in absence of cooling
 - Photon spectrometer might freeze if frontend electronics turns off while cooling is present
- We are almost autonomous.....

Network Security implementation

- General public and log in services/ Terminal services
 - RDP windows remote desktops
 - SSH gateways
 - VPN gateways



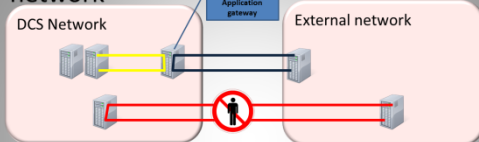
Control System Network Security

Controls Network and Rules

- Control system for accelerators is separated in private machine networks.
- Control system for SLS beamlines is in separated sub-nets, behind a firewall. Users from one beamline cannot influence the control system of another beamline.
- Remote access from the PSI office network to machine and beamline networks is possible through a dedicated ssh gateway.

...full network segregation & firewalling (Alice, LHCb, PSI)

Remote interactive access to the DCS network



- No direct user access to the ALICE network
- Remote access to ALICE network is possible via the application gateways
 - User makes RDP connection to the gateway
 - From the gateway further connection is granted to the network

Enrico Bonaccorsi — 4th Control System Cyber-Security Workshop (CS2/HEP) ICALEPCS — San Francisco

Local and Remote Access

Local access

- Connected devices must be registered in the PSI central DNS.
- No direct wireless access to the private machine networks

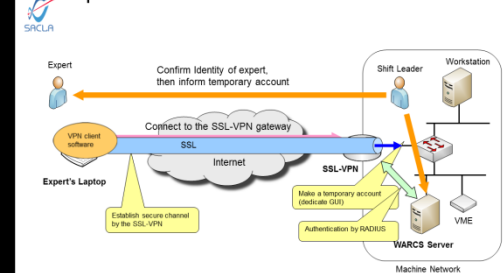
Remote access to a private machine network

- Access only from the PSI net through the gateways
- No direct access from one machine network to another
- No access to users home directories

R. Krempaska, October, 2013

R. Krempaska, October, 2013

Operation Process of WARCSv2



Connection between the laptop and VPN gateway is server-authenticated encrypted tunnel. Therefore, secure channel is to be established by client authentication. This process is very different from that of WARCSv1.

October 6, 2013

4th Control System Cyber-Security Workshop

36



With some discipline, people managed to have...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Are we really autonomous?

- Absence of external services could trigger immediate shutdown
 - Pixel detectors might melt in absence of cooling
 - Photon spectrometer might freeze if frontend electronics turns off while cooling is present
- We are almost autonomous.....

Network Security implementation

- General public and log in services/ Terminal services
 - RDP windows remote desktops
 - SSH gateways
 - VPN gateways
- Network segmentation and firewall



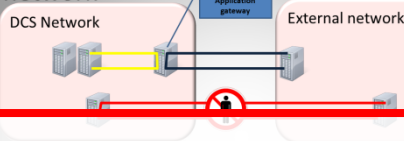
Control System Network Security

Controls Network and Rules

- Control system for accelerators is separated in private machine networks.
- Control system for SLS beamlines is in separated sub-nets, behind a firewall. Users from one beamline cannot influence the control system of another beamline.
- Remote access from the PSI office network to machine and beamline networks is possible through a dedicated ssh gateway.

...full network segregation & firewalling (Alice, LHCb, PSI)

Remote interactive access to the DCS network



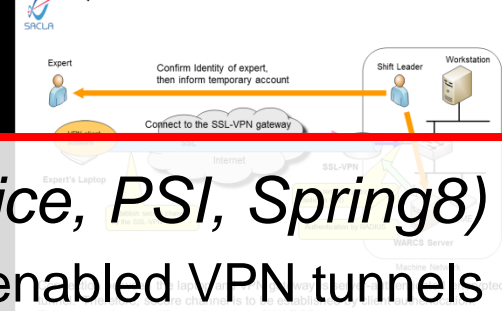
...tightly controlled remote access (Alice, PSI, Spring8)

2FA-Authentication; SSH gateways; shift leader enabled VPN tunnels

Local and Remote Access

- Local access**
 - Connected devices must be registered in the PSI central DNS.
 - No direct wireless access to the private machine networks
- Remote access to a private machine network**
 - Access only from the PSI net through the gateways
 - No direct access from one machine network to another
 - No access to users home directories

Operation Process of WARCSv2





With some discipline, people managed to have...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Are we really autonomous?

- Absence of external services could trigger immediate shutdown
 - Pixel detectors might melt in absence of cooling
 - Photon spectrometer might freeze if frontend electronics turns off while cooling is present
- ...full network segregation & firewalling (Alice, LHCb, PSI)
- We are almost autonomous.....

Network Security implementation

- General public and log in services/ Terminal services
 - RDP windows remote desktops
 - SSH gateways
 - VPN gateways
- Network segmentation and firewalling
- Access control

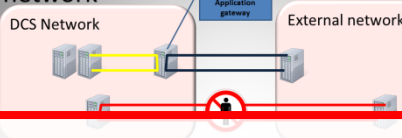


Control System Network Security

Controls Network and Rules

- Control system for accelerators is separated in private machine networks.
- Control system for SLS beamlines is in separated sub-nets, behind a firewall. Users from one beamline cannot influence the control system of another beamline.
- Remote access from the PSI office network to machine and beamline networks is possible through a dedicated ssh gateway.
- Access to ssh gateway is restricted for a well defined list of users and machines. The ssh gateway is a dedicated machine with a dedicated IP address. It is not possible to access the ssh gateway from the Internet. The ssh gateway can only be accessed from the internal network.

Remote interactive access to the DCS network

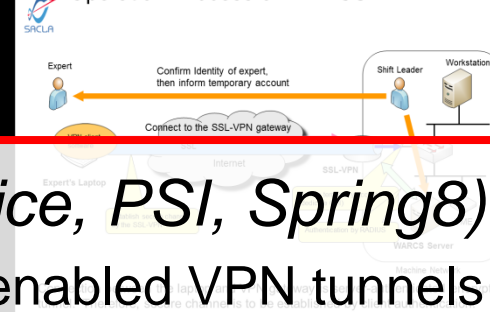


- ...tightly controlled remote access (Alice, PSI, Spring8)
- 2FA-Authentication; SSH gateways; shift leader enabled VPN tunnels

Local and Remote Access

- Local access
 - Connected devices must be registered in the PSI central DNS.
 - No direct wireless access to the private machine networks
- Remote access to a private machine network
 - Access only from the PSI net through the gateways
 - No direct access from one machine network to another
 - No access to users home directories

Operation Process of WARCSv2



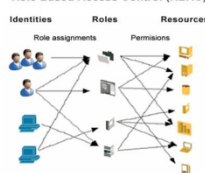
Authorization and authentication

- User authentication is based on CERN domain credentials
 - No local DCS accounts
 - All users must have CERN account (no external accounts allowed)
- Authorization is managed via groups
 - Operators have rights to logon to operator nodes and use WINCC OA
 - Experts have access to all computers belonging to their detectors
 - Super experts have access everywhere
- Fine granularity of user privileges can be managed by detectors at the WINCC OA level
 - Only certain people are for example allowed to manipulate very high voltage system etc.



Role Based Access Control (RBAC)

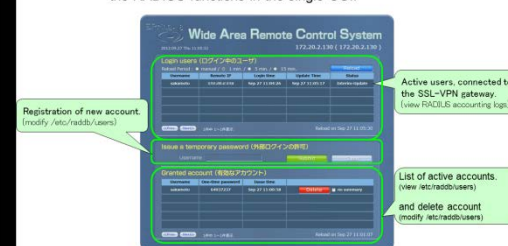
Role Based Access Control (RBAC)



- Machine Safety
 - ESS's 5 MW is powerful and potentially very damaging
 - RBAC protects from crippling machine damage
 - RBAC is proactive rather than reactive, it prevents invoking machine protection system
- Machine Performance
 - Don't mess with a fine tuned system
 - Access is denied during certain machine states

Account Registration GUI

Since shift leader is not IT expert, we wrapped the RADIUS functions in the single GUI.





With some discipline, people managed to have...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Are we really autonomous?

- Absence of external services could trigger immediate shutdown
 - Pixel detectors might melt in absence of cooling
 - Photon spectrometer might freeze if frontend electronics turns off while cooling is present
- ...full network segregation & firewalling (Alice, LHCb, PSI)
- We are almost autonomous.....

Network Security implementation

- General public and log in services/ Terminal services
 - RDP windows remote desktops
 - SSH gateways
 - VPN gateways
- Network segmentation and firewalling
- Active backup (redundant)

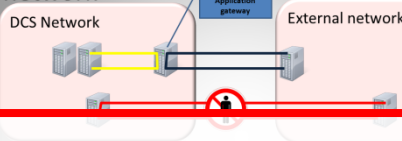


Control System Network Security

Controls Network and Rules

- Control system for accelerators is separated in private machine networks.
- Control system for SLS beamlines is in separated sub-nets, behind a firewall. Users from one beamline cannot influence the control system of another beamline.
- Remote access from the PSI office network to machine and beamline networks is possible through a dedicated ssh gateway.
- Access to ssh gateway is restricted for a well defined list of users and is subject to strict access control. The gateway is managed by a dedicated team. The gateway can be closed from the shift leader operator in case of an emergency and can close the remote network access at any time.

Remote interactive access to the DCS network



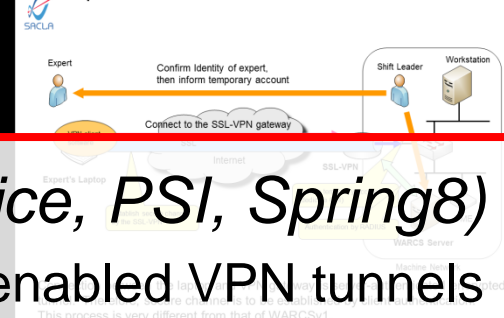
- ...tightly controlled remote access (Alice, PSI, Spring8)
- 2FA-Authentication; SSH gateways; shift leader enabled VPN tunnels

Local and Remote Access

Local access

- Connected devices must be registered in the PSI central DNS.
- No direct wireless access to the private machine networks
- Remote access to a private machine network
 - Access only from the PSI net through the gateways
 - No direct access from one machine network to another
 - No access to users home directories

Operation Process of WARCSv2



Authorization and authentication

- User authentication is based on CERN domain credentials
 - No local DCS accounts
 - All users must have CERN account (no external accounts allowed)

Role Based Access Control (RBAC)

Role Based Access Control (RBAC)

Identities Roles Resources

1. Machine Safety

- ESS's 5 MW is powerful and potentially very damaging
- RBAC protects from crippling machine damage
- RBAC is proactive rather than reactive

2. Machine Performance

- Don't mess with a fine tuned system
- Access to certain machine states

Account Registration GUI

Since shift leader is not IT expert, we wrapped the RADIUS functions in the single GUI.



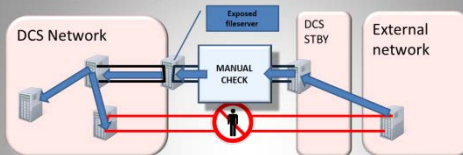
- ...fine-grained local access control (Alice, ESS, SPring8)
- User vs. experts vs. admins; down to Channel Access; role-based



With some discipline, people managed to have...

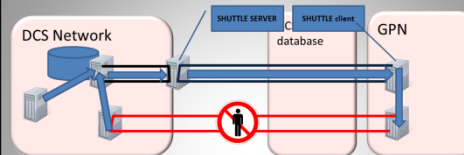
"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Uploading files to DCS network



- No direct user access to DCS filesystems
- Files are uploaded on request
- No teleport

Exposing DCS database to OFFLINE



- Database replication latency would delay processing
 - Trusted OFFLINE client requests data
 - SHUTTLE server retrieves data from database and sends it to OFFLINE
 - Protection against excessive requests

Data Security

- Shared filesystem
 - served by a cluster of five nodes on redundant hardware
 - High Availability granted by Cluster of NFS/SMB servers that export the filesystem to the entire experiment
 - Data protection:
 - Short term based on different storage raid set using RSYNC for immediate user access (file deleted by mistake by the user, etc)
 - Long Term based on tape using CASTOR for... ever? ☹
 - Backup sent to CASTOR and stored on tape
- Servers and Control PCs
 - High availability granted by RAID 1
 - SW RAID used when HW raid is not available
 - Daily Backup based on Tivoli (Thanks to IT dep.)

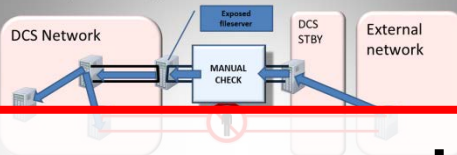
• Enrico Bonaccorsi — 4th Control System Cyber-Security Workshop(CS2/HEP) ICALEPCS - San Francisco • 14



With some discipline, people managed to have...

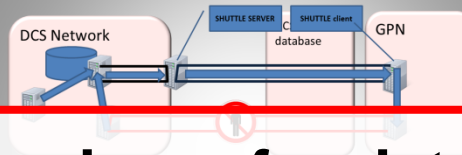
"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Uploading files to DCS network



- No direct user access to DCS servers
- Files are uploaded on request
- No teleports

Exposing DCS database to OFFLINE



- Database replication latency would delay processing
 - Trusted OFFLINE client requests data
- Protected against excessive requests

Data Security

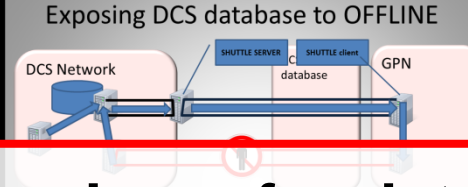
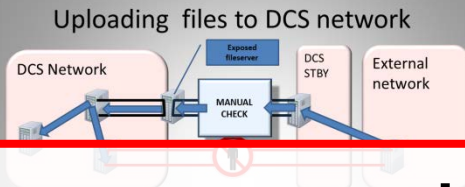
- Shared filesystem
 - served by a cluster of five nodes on redundant hardware
 - High Availability granted by Cluster of NFS/SMB servers that export the
- Data protection
 - Short term backup of control storage on tape using RSYNC for
 - Long term backup of control storage on tape by the user, etc)
 - Backup of control storage on tape by the user, etc)
- Servers and control PCs
 - Servers are protected by RAID 1
 - Control PCs are protected by RAID 1

...agreed procedures for data transfer (*Alice*)
Data replication (outgoing), manual file inspection (incoming)



With some discipline, people managed to have...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013



- ### Data Security
- Shared filesystem
 - served by a cluster of five nodes on redundant hardware
 - High Availability granted by Cluster of NFS/SMB servers that export the

...agreed procedures for data transfer (*Alice*)
Data replication (outgoing), manual file inspection (incoming)

- No direct user access to DCS servers
- Files are uploaded on request
- No teleports

- Database replication latency would delay processing
- Trusted OFFLINE client requests data
- Protected against excessive requests

- Data protection
 - Short term backup of control system data using RSYNC for
 - Long term backup of control system data using tape by the user, etc)

Servers and control PCs

- Hardware is committed by SAO 1

• Enrico Bonaccorti — 4th Control system Cyber-security Workshop (CS2/HEP) ICALEPCS - San Francisco • 14

TN Disco Test

Cut the cable between GPN and TN.

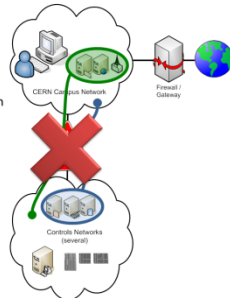
Control systems should be able to continue running.

Objectives:

- Reassure people that disconnection does not do harm;
- Understand extent of dependency on external services;
- Confirm autonomy;
- Confirm that disconnection is valid preventive action in case of major security incidents e.g. in the CC.

Downer:

This is LS1 — many systems were in maintenance mode...



Control System Infrastructure

Installation and Configuration

Linux PCs

- Scientific Linux (SL) distribution is used at PSI
- PSI Central Computing Division is in charge for SL core and rpm packages
- We use Redhat **kickstart** mechanism to deploy the base SL and **puppet** to configure computers according to the Controls requirements

Windows PCs

- OS installation according to the PSI Central computing division standard mechanism
- Extra software is installed by the Controls IT

R. Krempaska, October, 2013

Suggestions for Discussion

On the managerial side:

- ☐ With tight budgets, how to trigger incentives on management level?
- ☐ Can/should "standard" IT take over basic services?
- ☐ Did the Snowden revelations changed anything in your organization?

On the human side:

- ☐ How to trigger best incentives with system developers?
- ☐ Do we need to wait for a new generation of engineers?

On the technical side:

- ☐ How do you address patching/AV of Windows-based oscilloscopes?
- ☐ With commodity systems, how to give remote access to support hot-lines?
- ☐ Is splitting dev., test & operation of accelerator/experiment controls feasible?
- ☐ Who has experience with virtualization of controls? ...or usage of "Clouds"?
- ☐ Is IPv6 the new threat?

The diagram is divided into three main sections: 'Uploading files to DCS network', 'Exposing DCS database to OFFLINE', and 'Data Security'.

- Uploading files to DCS network:** Shows a 'DCS Network' connected to an 'Exposed Firewall' (labeled 'MANUAL CHECK'). This firewall is connected to a 'DCS STBY' and an 'External network'.
- Exposing DCS database to OFFLINE:** Shows a 'DCS Network' connected to a 'SHUTTLE SERVER' and a 'SHUTTLE client database'. This is connected to a 'GPN' (Global Positioning Network).
- Data Security:** Lists several security measures:
 - Shared filesystem:
 - served by a cluster of five nodes on redundant hardware
 - High Availability granted by Cluster of NFS/SMB servers that export the
 - Short term backup and recovery:
 - Short term backup and recovery using RSYNC for
 - Short term backup and recovery using RSYNC for
 - Short term backup and recovery using RSYNC for
 - Servers and control PCs:
 - High availability and redundancy (RAID)
 - High availability and redundancy (RAID)
 - High availability and redundancy (RAID)

Below the diagram, a large red box contains the text: **...agreed procedures for data transfer (Alice)**. Below this box, the text reads: **Data replication (outgoing), manual file inspection (incoming)**.

TN Disco Test

Cut the cable between GPN and TN.

Control systems should be able to continue running.

Control System Infrastructure

Installation and Configuration

Linux PCs

- Scientific Linux (SL) distribution is used at PSI
- PSI Central Computing Division is in charge of SL core and rpm packages

Suggestions for Discussion

On the managerial side:

- With tight budgets, how to trigger incentives on management level?
- Can/should "standard" IT take over basic services?
- Did the Snowden revelations changed anything in your organization?

On the human side:

- What are the best incentives for IT?
- How do you address the "AM" of Windows and applications?
- Is it a good idea to have a "standard" IT department?
- Who has experience with virtualization of controls?
- Is IPv6 the new threat?

...inventories & configuration management (CERN, PSI)

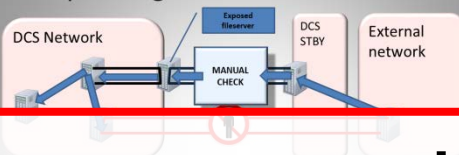
Dependency analysis; Kickstart & Puppet; but patching still too infrequent



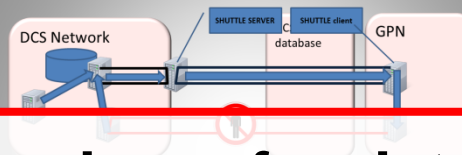
With some discipline, people managed to have...

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Uploading files to DCS network



Exposing DCS database to OFFLINE



Data Security

- Shared filesystem
 - served by a cluster of five nodes on redundant hardware
 - High Availability granted by Cluster of NFS/SMB servers that export the

...agreed procedures for data transfer (*Alice*)
Data replication (outgoing), manual file inspection (incoming)

TN Disco Test

Cut the cable between GPN and TN.

Control systems should be able to continue running.



Control System Infrastructure

Installation and Configuration

Linux PCs

- Scientific Linux (SL) distribution is used at PSI
- PSI Central Computing Division is in charge for SL core and rpm packages

Suggestions for Discussion

On the managerial side:

- ☐ With tight budgets, how to trigger incentives on management level?
- ☐ Can/should "standard" IT take over basic services?
- ☐ Did the Snowden revelations changed anything in your organization?

On the human side:

- ☐ How do you address the lack of training for new hires?
- ☐ How do you address the lack of training for new hires?

On the technical side:

- ☐ How do you address the lack of training for new hires?
- ☐ How do you address the lack of training for new hires?
- ☐ Is IPv6 the new threat?

...inventories & configuration management (*CERN, PSI*)
Dependency analysis; Kickstart & Puppet; but patching still too infrequent

Analyzed Security Standards

NERC
The North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) provides a list of guidelines to identify and protect critical cyber assets to support the reliability of the Bulk Electric System.

NIST
The National Institute of Standards and Technology (NIST) NISTIR 7628 presents an analytical framework to develop effective cyber security strategies specifically tailored for Smart-Grids.

ISA Secure
ISA Security Compliance Institute (ISCI) Communication Robustness Testing (CRT) program which has been produced on the basis of ISA-99 security standards specifications.

IEC
The technical specification IEC 62351 represents another effort to secure the IEC 61850 communication.

Your interface with IT

Key to success is to engage in a proactive, collaborative effort between management, controls engineers, IT Department and security.

NIST 800-53 is king.
Along came NIST 800-82.

- Many times a CS team (an "enclave") exists already.
- "Ah, we're not sure we can share such information with you" ...
- They might even tell you that it is impossible to gain access.
- You are the bridge between 800-53 and 800-82.
- You will have to provide the expertise to implement it.

Approaches to Security and Privacy

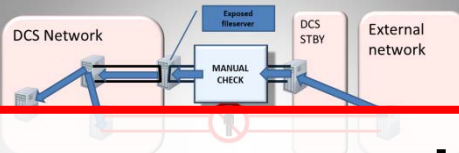
- Legal Methods
 - Contracts: (issue: what will vendor agree to?)
 - Laws: statutory (HIPAA, FERPA, ACA); administrative (FDA); case (rulings by courts).
 - Who interprets these in the workplace?
- Professional Organizations
 - AAPM (Physicists); AMA and ASTRO (Physicians); ONS (Nurses); ASRT (Radiation Technologists)
 - Overlapping authority, differing interpretations



With some discipline, people managed to have...

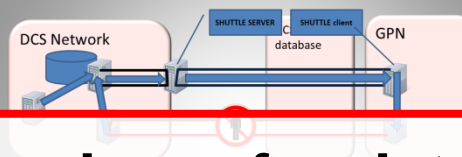
"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

Uploading files to DCS network



- No direct user access to DCS servers
- Files are uploaded on request
- No teleports

Exposing DCS database to OFFLINE



- Database replication latency would delay processing
- Trusted OFFLINE client requests data
- Protected against excessive requests

Data Security

- Shared filesystem
 - served by a cluster of five nodes on redundant hardware
 - High Availability granted by Cluster of NFS/SMB servers that export the
- Data protection
 - Short term backup of critical data using rsync for
 - Long term backup of critical data using tape by the user, etc)
- Servers and control PCs
 - High availability granted by RAID 1
 - High availability granted by RAID 1

...agreed procedures for data transfer (*Alice*)
Data replication (outgoing), manual file inspection (incoming)

TN Disco Test

Cut the cable between GPN and TN.

Control systems should be able to continue running.



- Reassure people that disconnection does not harm;
- Understand the impact of disconnection on the system;
- Confirm that disconnection is valid preventive action in case of major maintenance mode...

Control System Infrastructure

Installation and Configuration

Linux PCs

- Scientific Linux (SL) distribution is used at PSI
- PSI Central Computing Division is in charge for SL core and rpm packages

to configure computers according to the Controls requirements

Windows PCs

...inventories & configuration management (*CERN, PSI*)
Dependency analysis; Kickstart & Puppet; but patching still too infrequent

Suggestions for Discussion

Dr. Stefan Lüders — 4th CS2/HEP Workshop — October 6th 2013

On the managerial side:

- ☐ With tight budgets, how to trigger incentives on management level?
- ☐ Can/should "standard" IT take over basic services?
- ☐ Did the Snowden revelations changed anything in your organization?

On the human side:

- ☐ How do you address the lack of IT skills in the control room?
- ☐ How do you address the lack of IT skills in the control room?

On the technical side:

- ☐ How do you address the lack of IT skills in the control room?
- ☐ How do you address the lack of IT skills in the control room?
- ☐ Is IPv6 the new threat?

R. Krempaska, October, 2013

Analyzed Security Standards

NERC
The North America Electric
Reliability Corporation (NERC)
Critical Infrastructure Protection

NIST
The National Institute of
Standards and Technology (NIST)
NISTIR 7628 presents an analytical

Your interface with IT

Key to success is to engage in a proactive,
collaborative effort between management,
controls engineers, IT Department and security.

...standards & regulations compliance (*CERN, SLAC, UW*)
IEC61850 robustness; 800-53(IT) vs. 800-82(ICS); HIPAA/FERPA/FDA

Approaches to Security and Privacy

- Legal Methods
 - Contracts: (issue: what will vendor agree to?)

case (rulings by courts).

Who interprets these in the workplace?

On the technical side:

AAPM (Physicists), AMA and ASTRO (Physicians), ONS (Nurses), ASRT (Radiation Technologists)



Control System Cyber-Security is feasible!!

“4th CS2/HEP Workshop Summary” — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013



Control System Cyber-Security is feasible!!

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

**You just need to be
disciplined...**



Control System Cyber-Security is feasible!!

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

**You just need to be
disciplined...**

...able to prioritize...

1. Safety 2. Availability 3.
Security



Control System Cyber-Security is feasible!!

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

**You just need to be
disciplined...**

...able to prioritize...

1. Safety 2. Availability 3.
Security

**...and bring together
what belongs together:**

Functionality, usability,
availability, maintainability,
and *security*



Control System Cyber-Security is feasible!!

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

**You just need to be
disciplined...**

...able to prioritize...

1. Safety 2. Availability 3.
Security

**...and bring together
what belongs together:**

Functionality, usability,
availability, maintainability,
and *security*

Let's tackle it JOINTLY!!!



Control System Cyber-Security is feasible!!

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

**You just need to be
disciplined...**

...able to prioritize...
1. Safety 2. Availability 3.
Security

**...and bring together
what belongs together:**
Functionality, usability,
availability, maintainability,
and *security*

Let's tackle it JOINTLY!!!

The screenshot shows a web browser displaying the Indico conference page for the 4th Control System Cyber-Security Workshop (CS)2/HEP. The page title is "4th Control System Cyber-Security Workshop (CS)2/HEP" and the date is "6 October 2013" at "The Hyatt Regency Embarcadero Center". The left sidebar contains links for "Overview", "Timetable", "Registration & Accommodation", and "Support". The main content area shows the "Sun 06/10" timetable. The timetable lists various sessions with their start and end times and speakers. The sessions are:

Time	Session Title	Speaker
09:00	Introduction to the 4th Control System Cyber-Security Workshop	Dr. Stefan LUEDERS
09:30 - 09:45	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	
09:45 - 10:10	Controls Cyber Security at PSI	Renata KREMPASKA
10:00	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	
10:10 - 10:35	IEC 61850 Industrial communication standards under test	Filippo Maria TILARO
10:35 - 11:00	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	
11:00	Remote Access to Experiment Controls	Peter CHOCHULA
11:00 - 11:25	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	
12:00	Renewal of the remote maintenance system for the SPRING-3 control system	Dr. Takashi SUGIMOTO
12:10 - 12:35	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	
12:35 - 13:50	Authentication and Authorization for the ESS Control System	Suzanne GYSIN
13:00	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	
13:50 - 14:15	Lunch Break	
14:00	IT Security for the LHCb experiment	Enrico BONACCORSI
14:15 - 14:40	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	
14:40 - 15:00	Seacliff D, Bayview Level, The Hyatt Regency Embarcadero Center	

The URL in the address bar is <https://indico.cern.ch/conferenceDisplay.py?confId=217457>.



Thank you very much!!!

"4th CS2/HEP Workshop Summary" — Dr. Stefan Lüders — ICALEPCS2013 — October 6th 2013

**In particular to
~35 participants &
esp. to all presenters...**



Protect your passwords

A cybercriminal, who knows your password,
will abuse your computing account.



**Be careful when surfing the Web
and with e-mails**

Cybercriminals are trying to trick you!

**...as well as to the
Organizing Committee!!!**

