4th Control System Cyber-Security Workshop

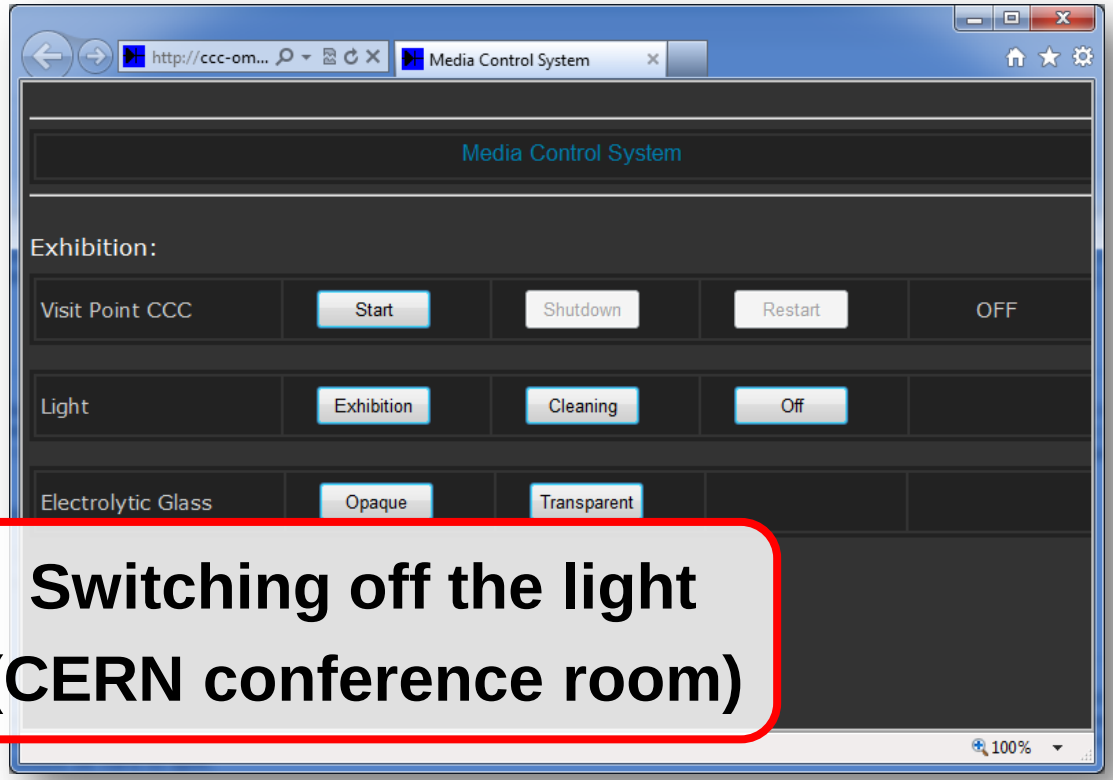
More “discipline” is what we need.

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

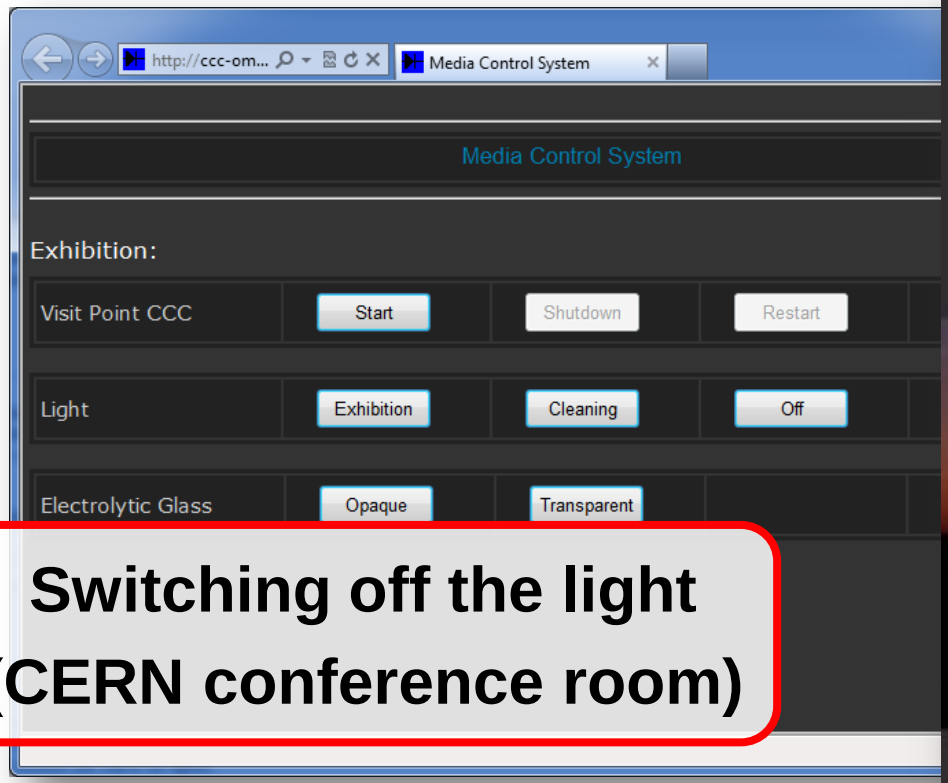
Why Control System Cyber-Security…

Why Control System Cyber-Security…

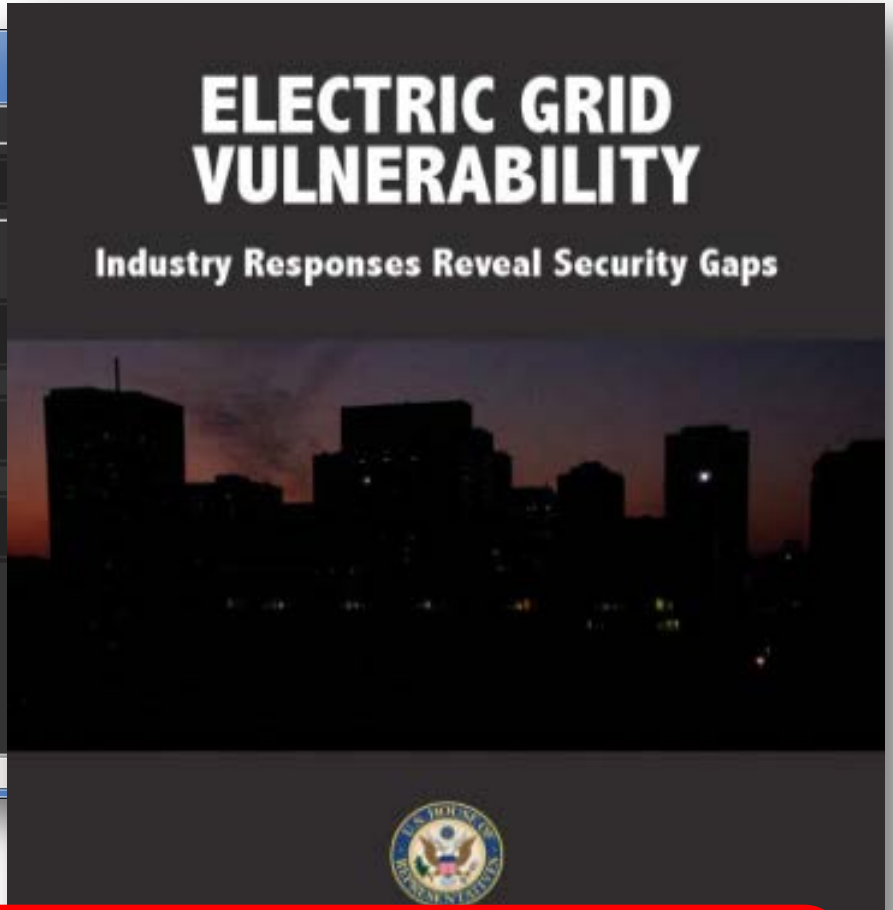


Switching off the light (CERN conference room)

Why Control System Cyber-Security…



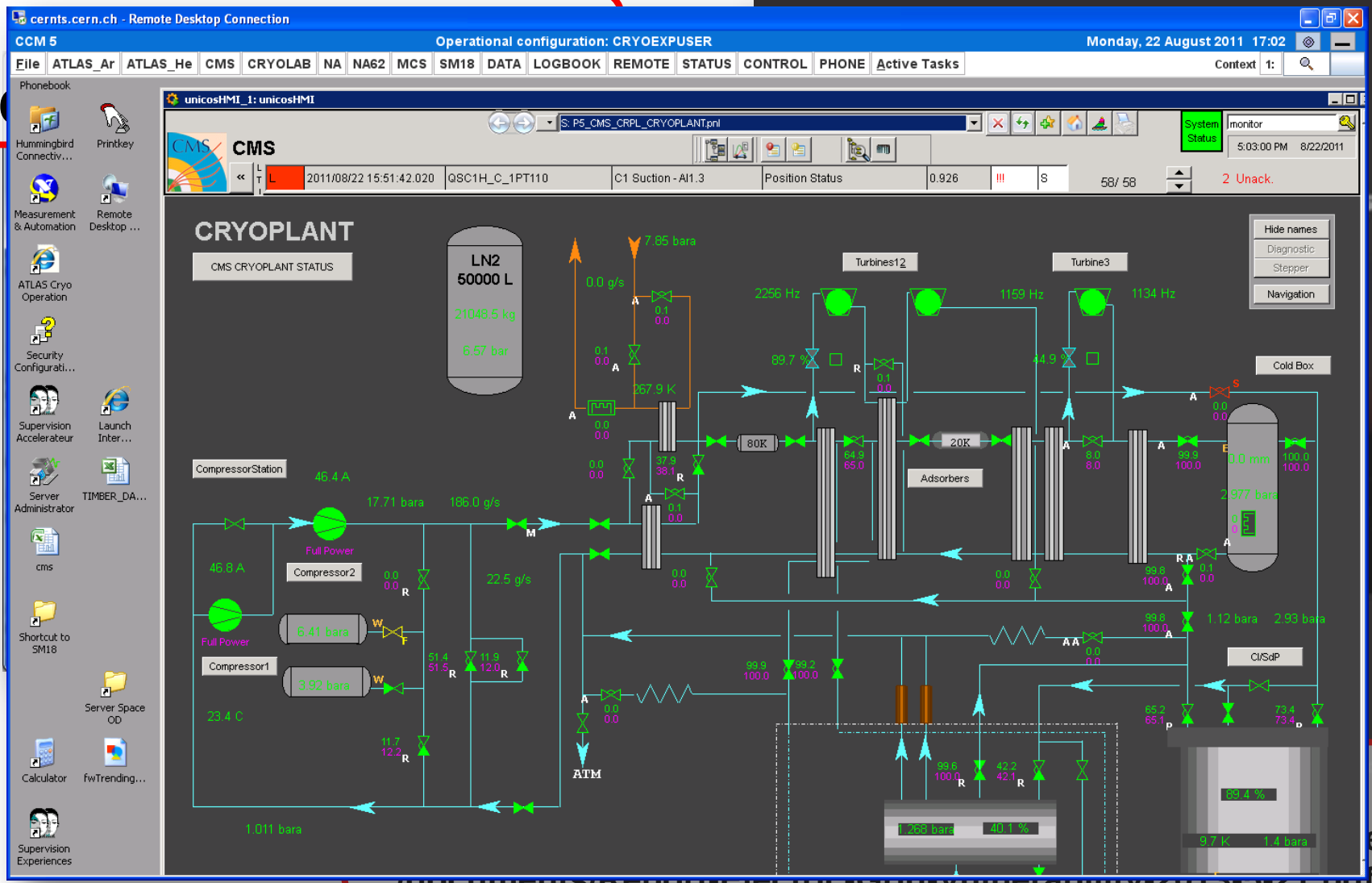
Switching off the light (CERN conference room)



Switching off the light (US cities)

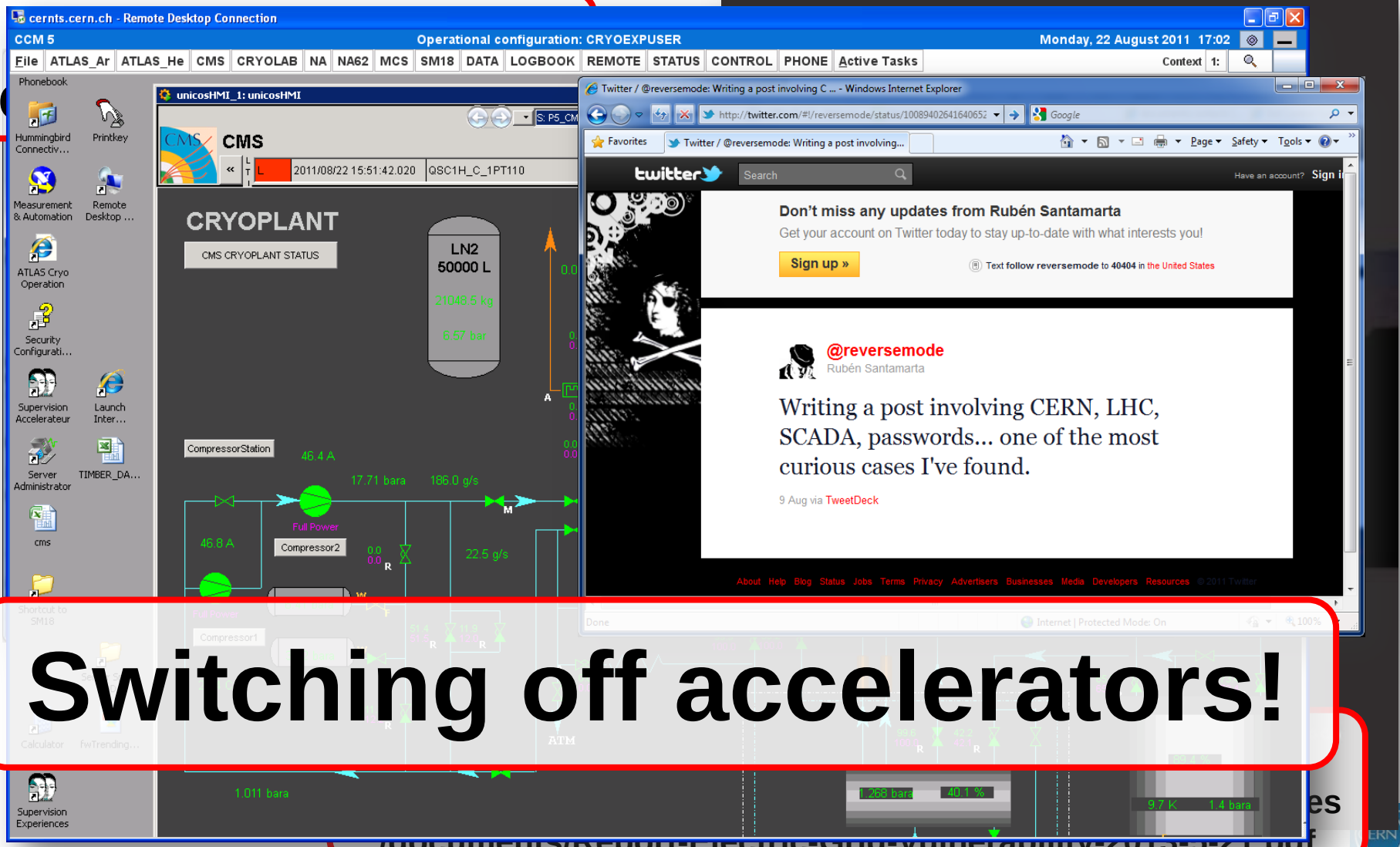
http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf

Why Control System Cyber-Security…



/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf

Why Control System Cyber-Security…



Switching off accelerators!


…needs a disciplined approach!

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…

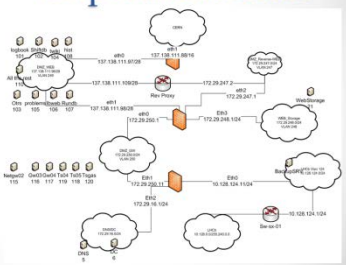
With some discipline, people managed to have…

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
- ALICE operation is impossible without DCS feedback
- We are almost autonomous……

Network Security implementation

- General public and log in services/ Terminal services
  - RDP windows remote desktops
  - SSH gateways
  - NX linux remote desktops
  - Web services
- Network segmentation and trusted zones
  - three tiers level of trust based on the sensitivity of the data being processed



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.
- Login to ssh gateway is restricted for a well defined list of users and allowed only during facilities shutdown and machine shifts. The „on-call" service Controls members can get the access on request from the control room. The shift leader operator in the Control room can close the remote network access at any time.

With some discipline, people managed to have…

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
- Network segmentation and trusted

Enrico Bonaccorsi –4th Control System Cyber-Security Workshop(CS)2/HEP ICALEPCS – San Francisco 12

Control System Network Security

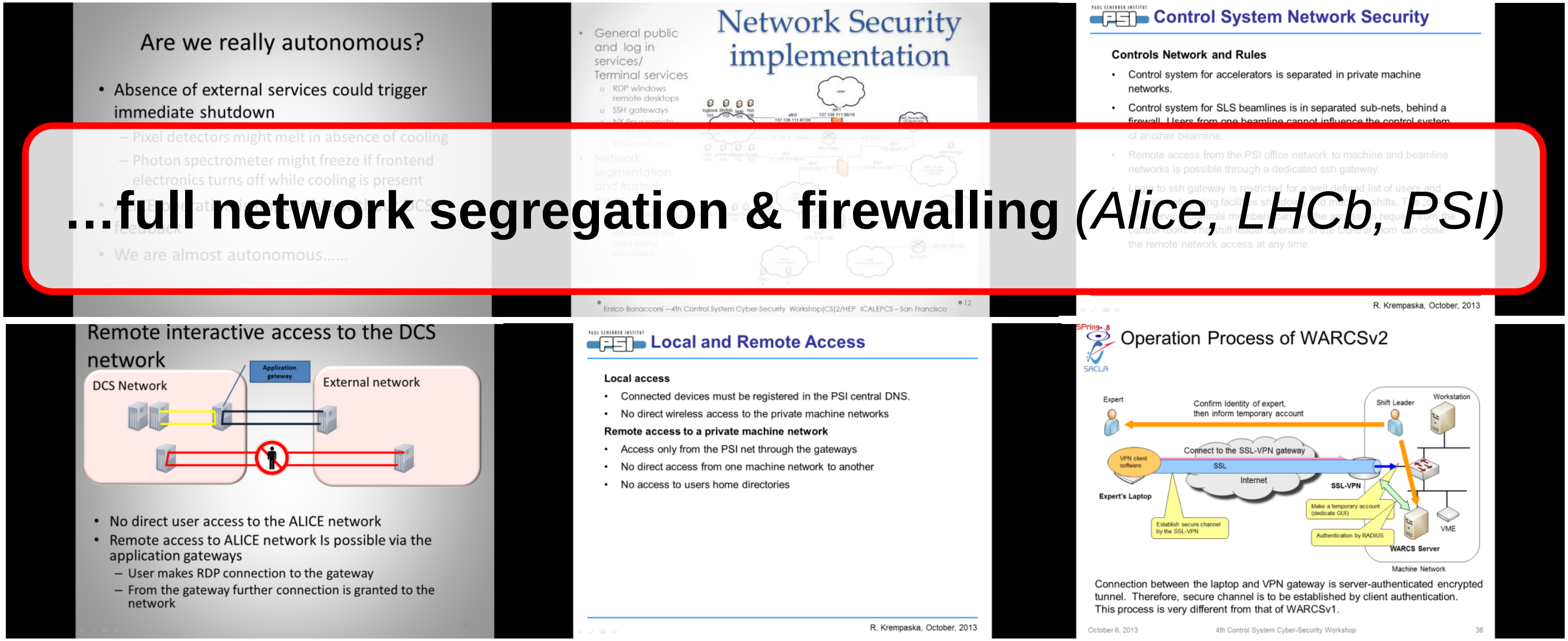
Controls Network and Rules

- 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 the corresponding facility's shifters. The control room shift leader operator in the control room can close the remote network access at any time.

R. Krempaska, October, 2013

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

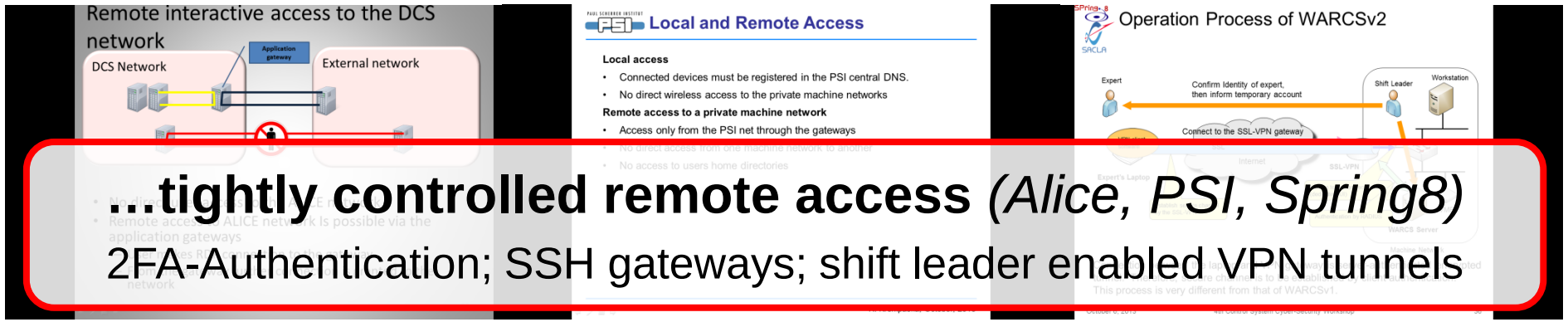
With some discipline, people managed to have...



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


With some discipline, people managed to have…

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



…tightly controlled remote access *(Alice, PSI, Spring8)*

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

With some discipline, people managed to have…

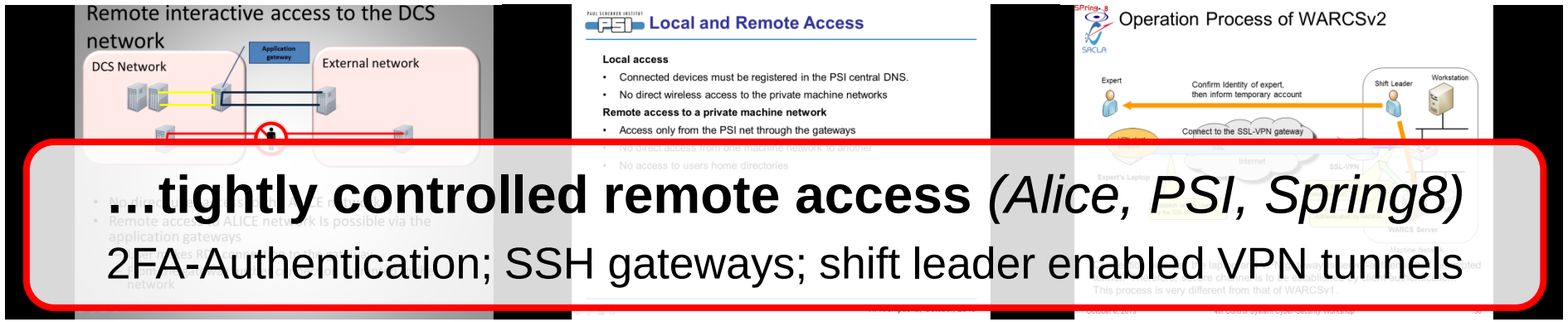
…full network segregation & firewalling *(Alice, LHCb, PSI)*

…tightly controlled remote access *(Alice, PSI, Spring8)*

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

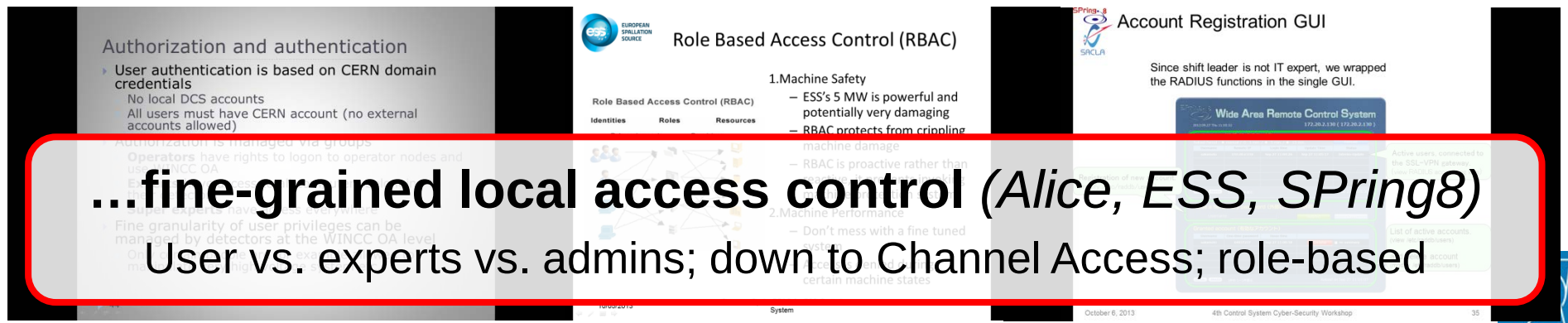
With some discipline, people managed to have…

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



…tightly controlled remote access *(Alice, PSI, Spring8)*

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

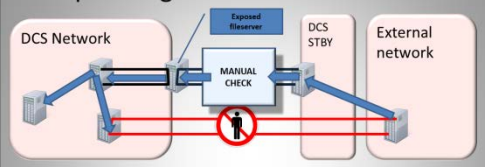


…fine-grained local access control *(Alice, ESS, SPring8)*

User vs. experts vs. admins; down to Channel Access; role-based

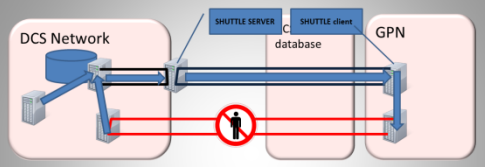
With some discipline, people managed to have…

Uploading files to DCS network



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

Exposing DCS database to OFFLINE

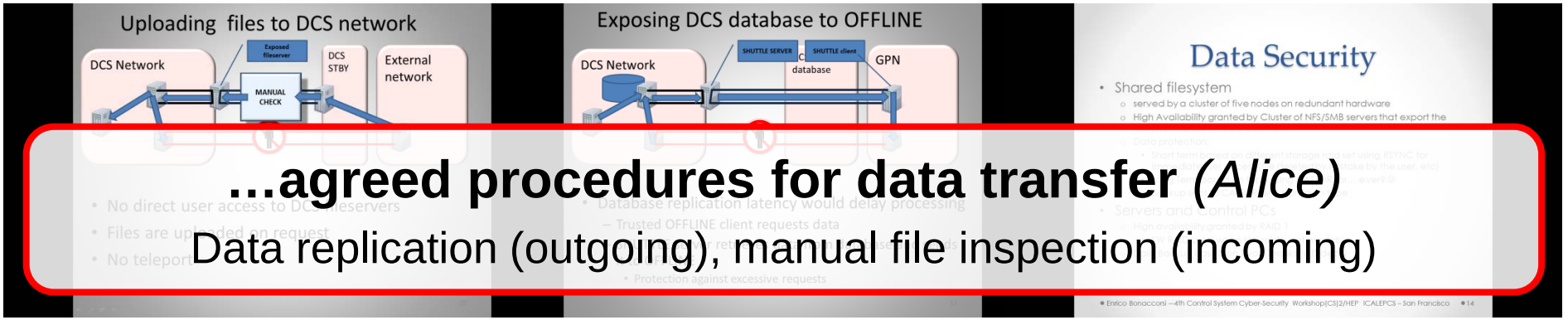


- Database replication latency would delay processing
  - Trusted OFFLINE client requests data
  - SHUTTLE server retrieves data from database and sends it to OFFLINE
    - Protection against excessive requests

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 type
- 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.)

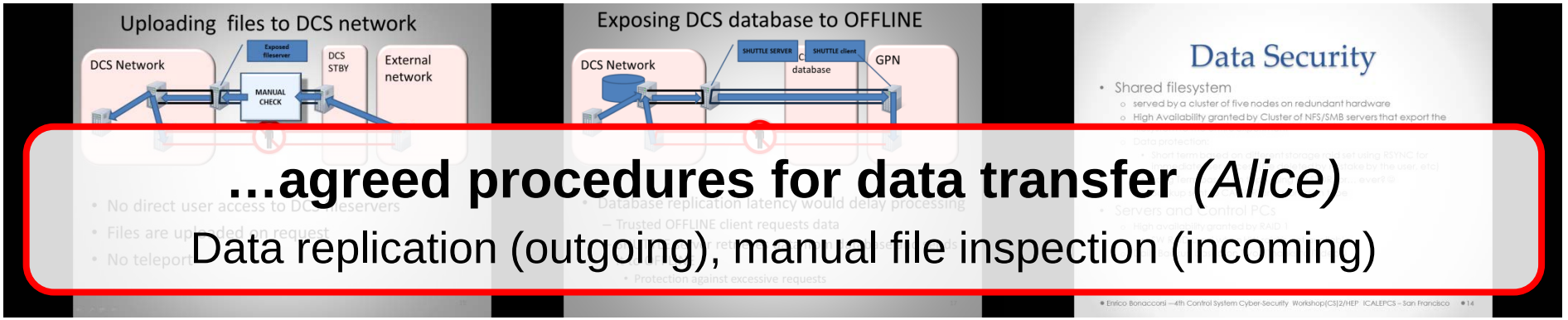
With some discipline, people managed to have…



…agreed procedures for data transfer *(Alice)*

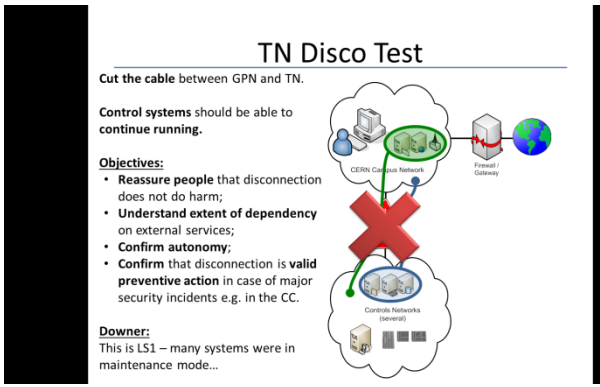
Data replication (outgoing), manual file inspection (incoming)

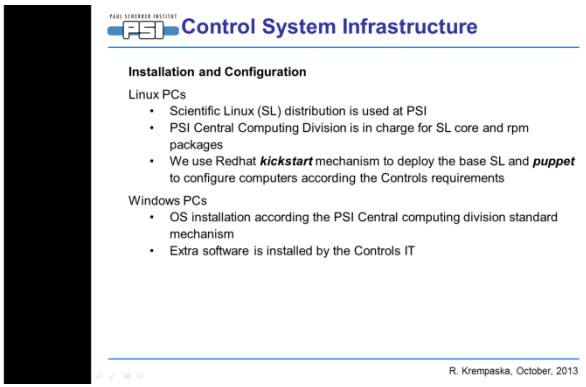

With some discipline, people managed to have…

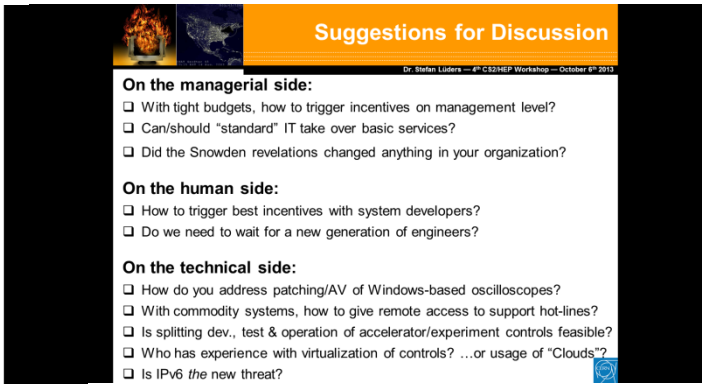


…agreed procedures for data transfer *(Alice)*

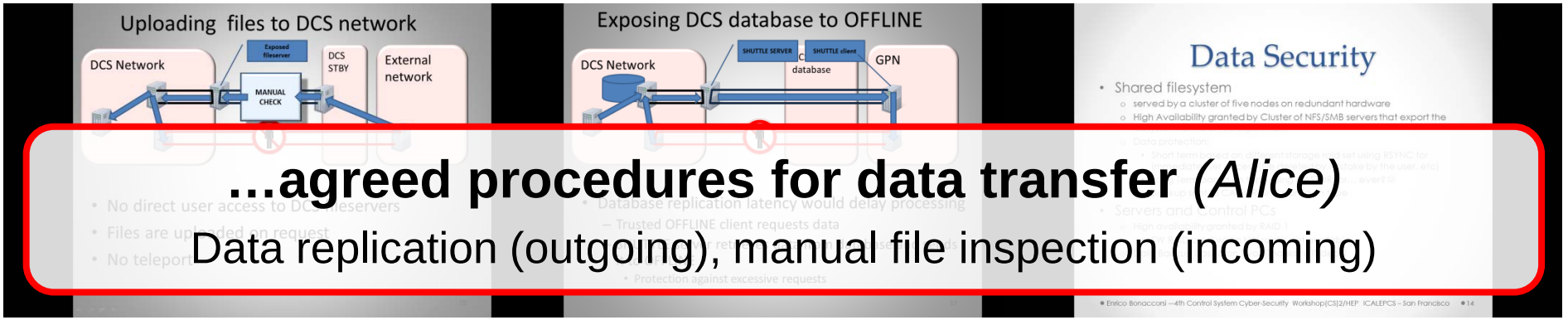
Data replication (outgoing), manual file inspection (incoming)





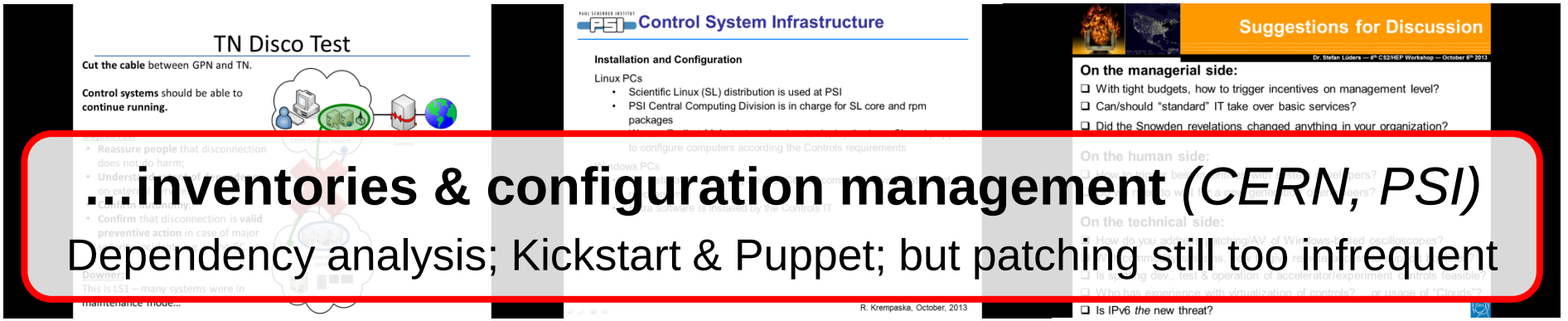



With some discipline, people managed to have…



…agreed procedures for data transfer *(Alice)*

Data replication (outgoing), manual file inspection (incoming)



…inventories & configuration management *(CERN, PSI)*

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

With some discipline, people managed to have…

…agreed procedures for data transfer *(Alice)*

Data replication (outgoing), manual file inspection (incoming)

…inventories & configuration management *(CERN, PSI)*

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


With some discipline, people managed to have…

…agreed procedures for data transfer *(Alice)*

Data replication (outgoing), manual file inspection (incoming)

…inventories & configuration management *(CERN, PSI)*

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

…standards & regulations compliance *(CERN, SLAC, UW)*

IEC61850 robustness;800-53(IT) vs. 800-82(ICS); HIPPAA/FERPA/FDA


Control System Cyber-Security is feasible!!


Control System Cyber-Security is feasible!!

You just need to be disciplined…


Control System Cyber-Security is feasible!!

You just need to be disciplined…

…able to prioritize…

1. Safety 2. Availability *3. Security*


Control System Cyber-Security is feasible!!

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!!

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!!!

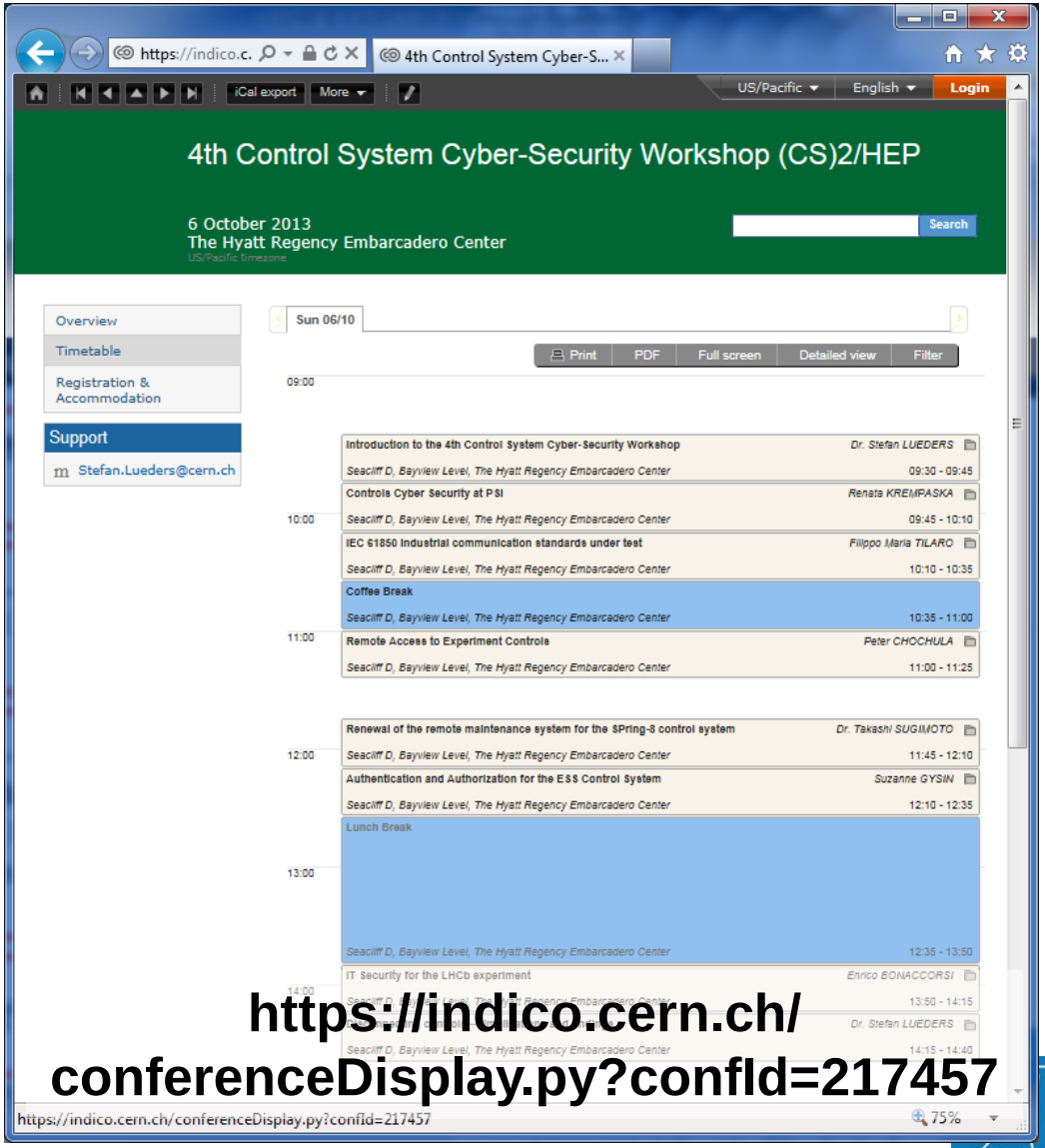
Control System Cyber-Security is feasible!!

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!!!



https://indico.cern.ch/conferenceDisplay.py?confId=217457


Thank you very much!!!

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

…as well as to the Organizing Committee!!!