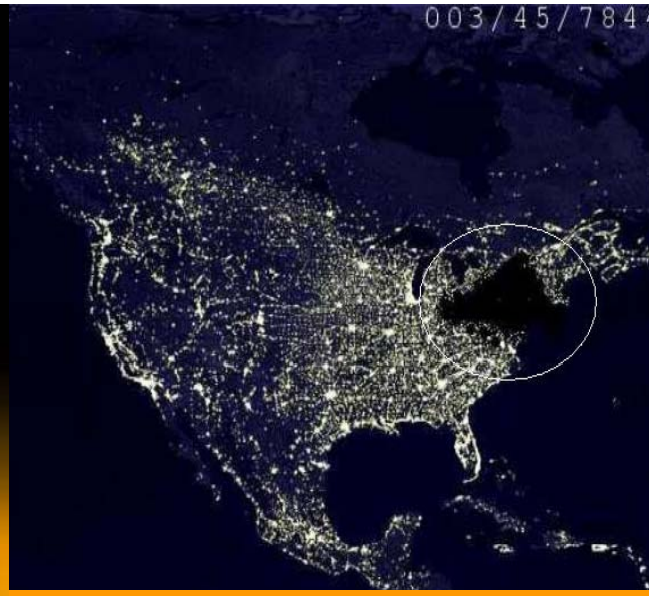




# Control Systems Under Attack !?

## …about the Cyber-Security of modern Control Systems

**Dr. Stefan Lüders (CERN IT/CO)**

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

October 14th 2007


# Overview



## The Past:
## The (R)Evolution of Control Systems

## The Present:
## What about Security !?

## The Future:
## Control System Cyber-Security


# Controls Goes IT



## Controls networks meet campus / business networks

- Proprietary field busses (PROFIBUS, ModBus)
  replaced by Ethernet & TCP/IP (PROFINET, ModBus/TCP)
- Field devices connect directly to Ethernet & TCP/IP
- Real time applications based on TCP/IP

## Migration to the Microsoft Windows platform

- MS Windows not designed for industrial / control systems
- OPC/DCOM runs on port 135 (heavily used for RPC)
- STEP7, PL7 Pro, UNITY, WINCC, VNC, PCAnywhere, …

## Use of IT protocols & gadgets

- eMails, FTP, Telnet, SNMP, HTTP (WWW), … directly on e.g. a PLC
- Wireless LAN, notebooks, USB sticks, webcams, …

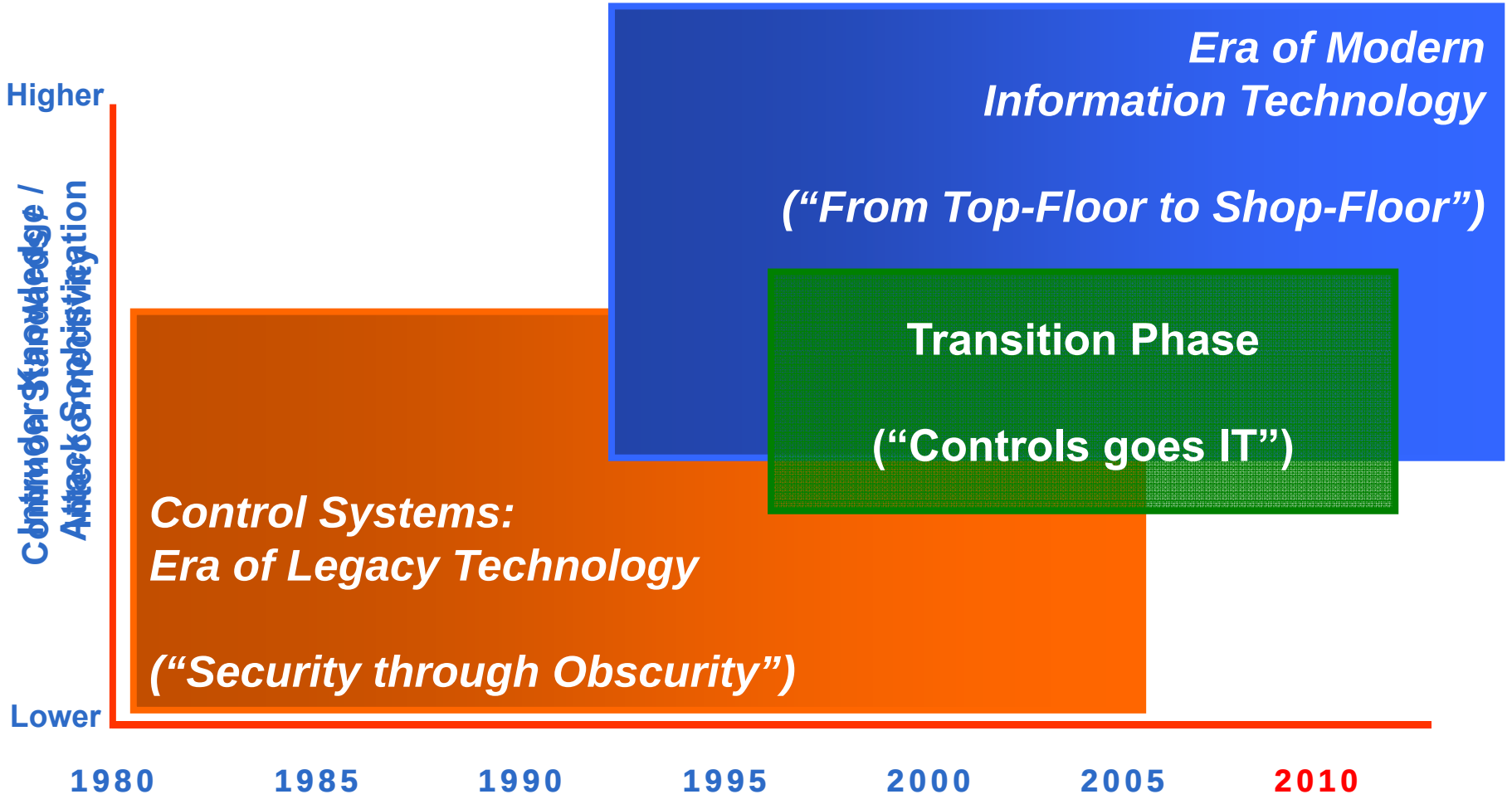



# The Past:
# The (R)Evolution of Control Systems

# The Present:
# What about Security !?

# Cyber Threats — Today's Peril






Shown at ICALEPCS2005


# The RISK Equation



## Risk = Threat

## × Vulnerability

## × Consequence


# *Who* is the threat ?



## Attacks performed by…

- Trojans, viruses, worms, …
- Disgruntled (ex-)employees or saboteurs
- Attackers and terrorists
  (first presentations on BlackHat conferences; free hacking tools; today's general security situation)

## Lack of robustness & lots of stupidity

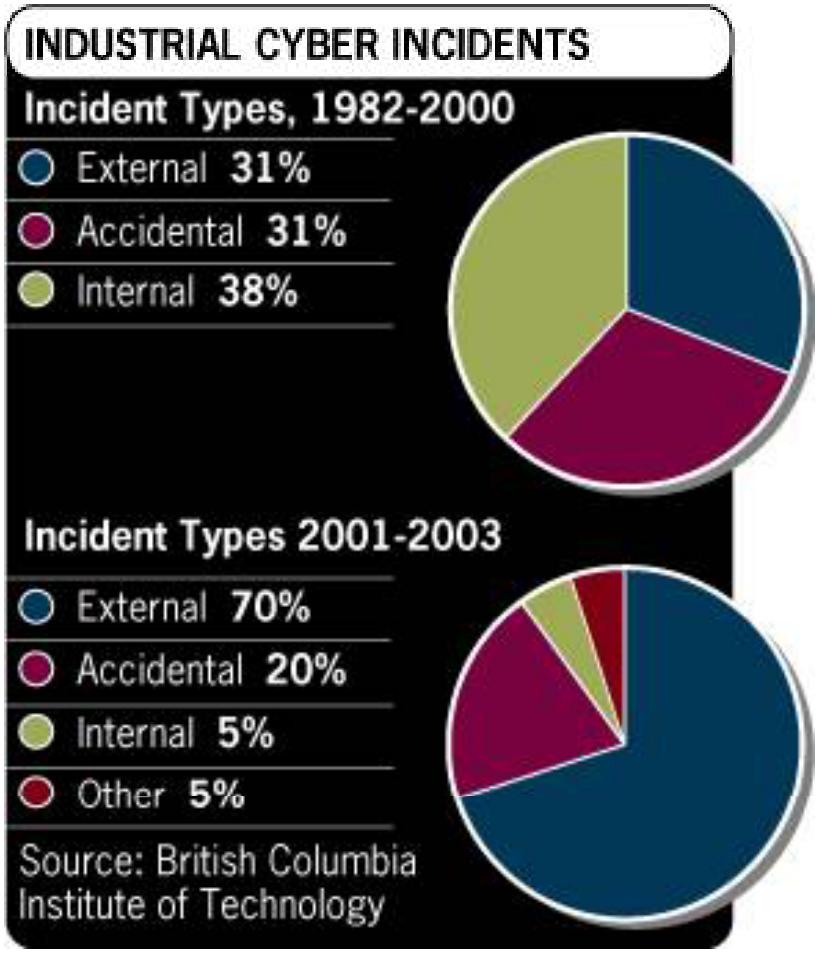
- Mal-configured or broken devices flood the network
- Developer / operator "finger trouble"

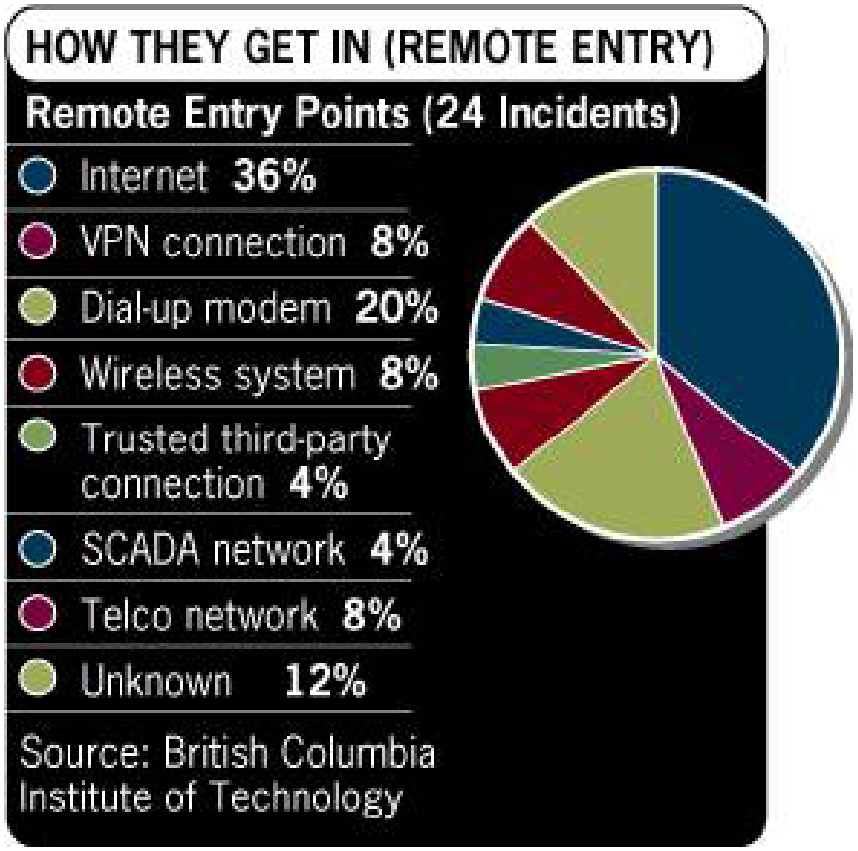
## Lack of procedures

- Flawed updates or patches provided by third parties
- Inappropriate test & maintenance rules or procedures

# “Industrial Security Intrusion DB”






**Based on 135+ documented incidents (2006)**




# Risk = Threat

# × Vulnerability


# Human Vulnerabilities (60%)



## Passwords are known to several (many?) people

- No traceability, ergo no responsibility

## People are increasingly the weakest link

- Use of weak passwords
- Infected notebooks are physically carried on site
- Users download malware and open "tricked" attachments

## Missing/default/weak passwords in applications

*…but how to handle **access control ?***

*…what about **traceability ?***


# Technical Vulnerabilities (40%)



## Poorly secured systems are being targeted

- Unpatched systems, OS, and applications
- Missing anti-virus software or old virus signature files
- No local firewall protection

## "Zero Day Exploits": security holes without patches

- Break-ins occur before patch and/or
- Anti-virus signature available
- Worms are spreading within seconds

*…but **how to patch/update** control/engineering PCs ?*

*…what about **anti-virus software & local firewalls** ?*

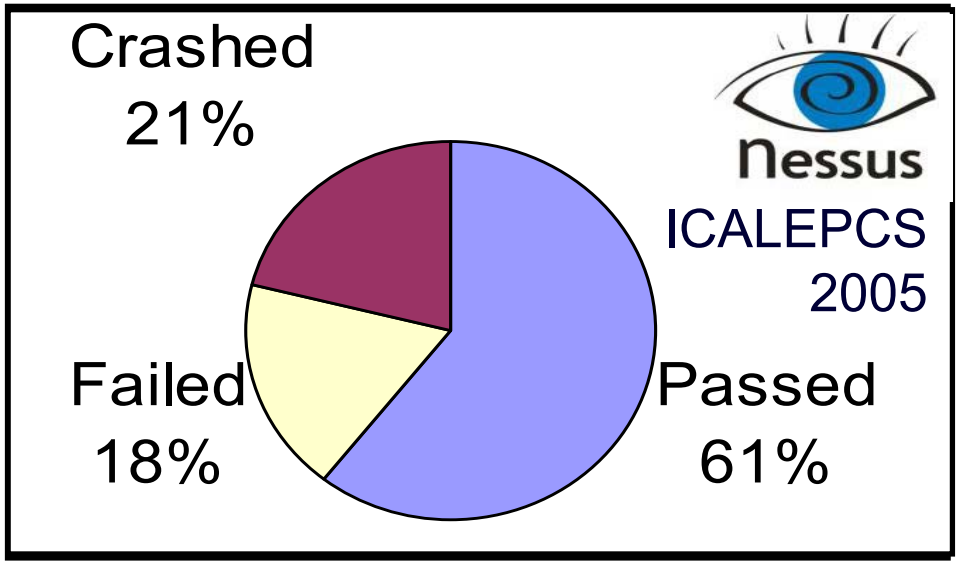
**Boeing 777 uses similar technology to Process Control Systems**

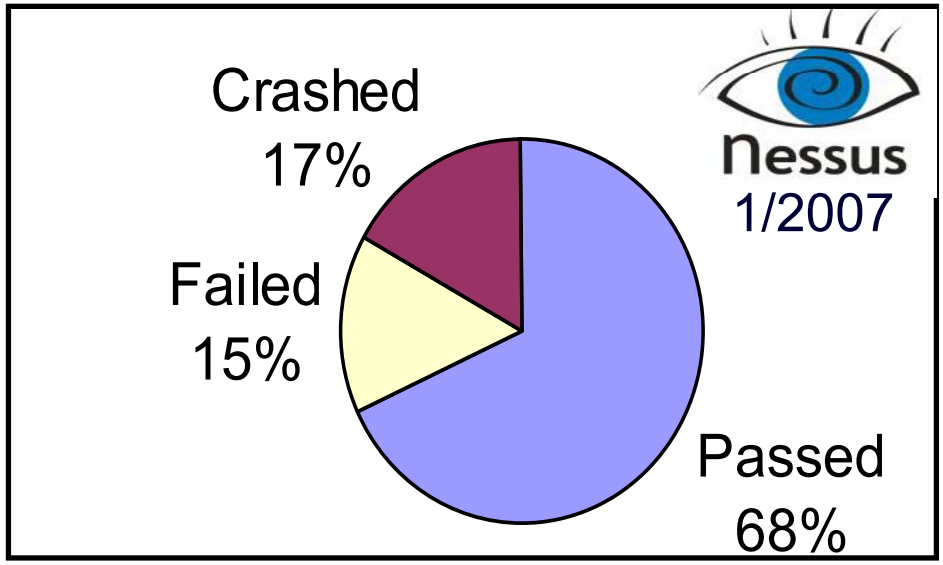

# Control Systems under Attack !



## CERN TOCSSiC Vulnerability Scans

- **31 devices** from 7 different manufacturers **(53 tests in total)**
- **All devices fully configured** but running idle
- see ICALEPCS 2005




*…PLCs under load seem **more likely to fail** !!!*

*…**results improve** with more recent firmware versions ☺*


# TOCSSiC Findings (1)

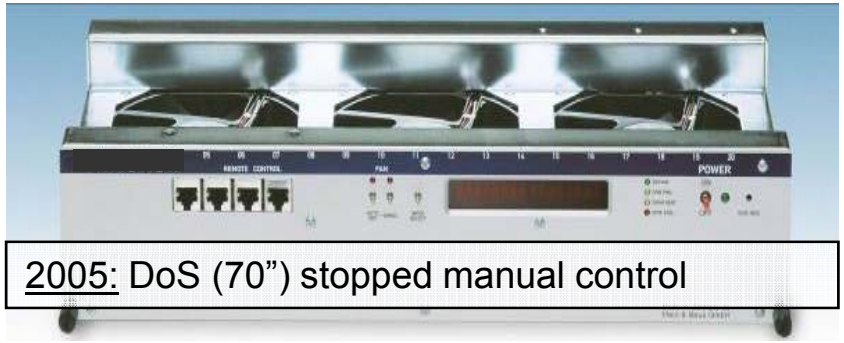


**The device crashed**

while receiving

special non-conform packets

*…violation of TCP/IP standards !!!*



2005: DoS (70") stopped manual control

**FTP server provides an attacker platform**

**FTP & Telnet servers crashed**

- Receiving very looooooooooong commands or arguments

*…both are legacy protocols w/o encryption !*

**HTTP server crashed**

- Receiving an URL with toooooooooooo many characters
- Using up all resources ("WWW infinite request" attack)

**HTTP server allows for directory traversal**

*…who needs web servers & e-mailing on PLCs ?*


# TOCSSiC Findings (2)



## ModBus server crashed

while scanning port 502

*…protocol is well documented !*


## PLCs are unprotected

- Can be **stopped w/o problems**
  (needs just a bit of Google )
- Passwords are not encrypted
- Lack of authorization schemes

*…authorization, data integrity checks, and encryption must become mandatory !*

## PLCs are *really* unprotected

- Services (HTTP, SMTP, FTP, Telnet, …) can not be disabled
- Neither local firewall nor antivirus software

*…default lock down of the configuration !*




# Anything out there ?


# *Where* is the threat ?



## CERN SCADA Honeypots

- Demonstrating the existence of the threat

## Simulating two brands of PLCs

- NMAP fingerprint, FTP, Telnet, SNMP, HTTP, S7 & Modbus

**No dedicated interaction with honeypots since March 2006:**

- **4 pots (à two PLCs) deployed inside CERN**
  - Only observation: the usual "slight fever" on CERN's campus network
- **3 pots deployed on the CERN controls network**
  - No interactions observed ☺
- **3 pots visible on ports 102/tcp & 502/tcp from the Internet**
  - Lots of "noise" observed, e.g. SSH scans, but nothing dedicated




# Risk = Threat

# × Vulnerability

# × Consequence


# Aware or Paranoid ? (1)



## Russia welcomes hack attacks

Script Kiddies cut teeth hijacking critical infrastructure

By Thomas C Greene in Washington → More by this author

Published Thursday 27th April 2000 12:25 GMT

Find you

Malici
specta
hacke
succe
Colon
The C
whethe

2000: Ex-Employe
46x into a sewage
basement of a Hya

2003: The "S
safety monit
Besse nucle

## 2003/08/11: W32.Blaster.Worm


# Aware or Paranoid ? (2)



eWEEK.COM SUBSCRIBE TO eWEEK RSS Feeds | Print | Newsletters

## Cyber security breaches threaten, 2006 forecasts

Date: **December 24, 2005**
Source: isa.org
By: BOB FELTON



**Cyber security breaches threaten, smarter factories and processes emerge, consulting business booms, and engineering talent base shrinks.**

and long run, availability of engineering talent is going to be a global issue," Bena said.

### Cyber security remains vulnerable

The electronic security of manufacturing systems has already become a global issue, with more than 100 documented instances of cyber events tha affected, or could have affected, process control. And because few companies willingly disclose breaches of security, experts believe the actual nu much higher.

* In Australia, a disgruntled contractor remotely arranged the release of one million liters of raw sewage into adjoining waterways.
* In Tempe, Ariz., an intruder gained access to the Salt River Project system, disrupting delivery of power and water to utility customers and stealing ac
* In
* H

"

> **"....penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours...."**
> **- Sandia National Labs, US [2005]**


# Aware or Paranoid ? (3)



CSO

The Resource for Security Executives

CSO 0

## "Data storm" blamed for nuclear-plant shutdown

*Robert Lemos*, SecurityFocus 2007-05-18

**May 2007**

The U.S. House of Representative's Committee on Homeland Security called this week for the Nuclear Regulatory the cause of excessive network traff plant.

During the incident, which happened last August at Unit 3 of the Browns Ferry nuclear power plant, operators manually shut down the reactor after two water recirculation pumps failed. The recirculation pumps control the flow of water through the reactor, and thus the power output of boiling-water reactors (BWRs) like Browns Ferry Unit 3. An investigation into the failure found that the controllers for the pumps locked up following a spike in data traffic -- referred to as a "data storm" in the NRC notice -- on the power plant's internal control system network. The deluge of data was apparently caused by a separate malfunctioning control device, known as a programmable logic controller (PLC).

PHYSORG.COM

SCIENCE : PHYSICS : TECH : NANO : NEWS

Home | Nanotechnology | Physics | Space & Earth science | Electronic Devices

Internet | Software | Business | Engineering | Semiconductors | Other | Telecom | Energy | Computer Sciences

Published: 07:03 EST, **March 25, 2007**

## Hole Found in Protocol Handling Vital National Infrastructure

**Systems that control dams, oil refineries, railroads and nuclear power plants have a vulnerability that could cause a system takeover, according to a recent research report.**

distribution, gas and oil pipelines and other distributed processes. Wikipedia has a schematic of SCADA here.

Neutralbit identified the vulnerability in NETxAutomation NETxEIB OPC (OLE for Process Control) Se Windows standard for easily writing GUI applications for SCADA. It's used for interconnecting proces running on Microsoft platforms. OPC servers are often used in control systems to consolidate field ar information.

Neutralbit reports that the flaw is caused by improper validation of server handles, which could be exp (different) network-connected devices,




# The Past:
# The (R)Evolution of Control Systems

# The Present:
# What about Security !?

# The Future:
# Control System Cyber-Security


# Myths about Cyber-Security



"Network security, that's it !"

"The firewall makes you secure..."

"Encryption protects you..." "VPNs protect you..."

"Field devices can't be hacked..."

"IDSs can identify possible control system attacks..."

"You are secure if attackers can't get in..."

"You can keep attackers out..."

"More and better gadgets can solve security problems..."

"Everything can be solved by technique !"


# How do you secure controls ?



- **How does your Security Policy for Controls integrate in the overall ?**
- What is your strategy for protection ?
  M&M ? Defense-in-Depth ? Using Office-IT ?
- **Have you adapted your network architecture ?**
- How do you exchange data with external users ?
- **What about remote access from the Internet ?**
  **VPN ? Modems ?**
- How do you manage, patch, and update control PCs ?
- **What have you put in place to detect incidents ?**
- How do you (plan to) deal with incident handling ?
- **What are your procedures for system recovery ?**


# How do you control their usage ?



- **What is your general access policy ?**
- How do you foresee to protect you control room (consoles) against unauthorized (physical) access ?
- **How do you distinguish between different classes of users (visitors, operators, experts, developers) ?**
- How do you ensure traceability of users and actions ?
- **Are there dependencies on external conditions (e.g. maintenance period, beam injection, data taking) ?**
- What is your remote access scheme ?
- **How do you think to manage user rights ?**
- What about synchronization with e.g. office accounts ?
- **How do you maintain this lot for the next years ?**

# (CS)² in HEP — The Agenda

"Control Systems Under Attack !?" — Dr. Stefan Lüders — (CS)2/HEP Workshop — October 14th 2007

| | | |
|---|---|---|
| 09:30-10:00 (00h30') | [5] **Control System Cyber Security Measures at the Advanced Photon Source** | Ms. Deborah QUOCK (Argonne National Laboratory) |
| 10:00-10:30 (00h30') | [12] **Perspective on secure network for control systems in SPring-8** | Dr. Toru OHATA (JASRI/SPring-8) |
| 10:45-11:15 (00h30') | [14] **Accelerator Control-System Network Security at Diamond Light Source** | Dr. Mike LEECH (Diamond Light Source) |
| 11:15-11:45 (00h30') | [9] **Network and computer security in the Fermilab Accelerator Control System** | Tim ZINGELMAN (Fermi National Accelerator Lab) |
| 11:45-12:15 (00h30') | [6] **Update on the CERN Computing and Network Infrastructure for Controls (CNIC)** | Stefan LUEDERS (CERN) |
| 14:00-14:30 (00h30') | [7] **Remote Access to Alice** | Peter CHOCHULA (CERN) |
| 14:30-15:00 (00h30') | [4] **Role Based Access Control for the Accelerator Control System at CERN** | Mrs. Suzanne GYSIN (FNAL) |
| 15:15-15:45 (00h30') | [8] **Secure Remote Operation of Light Source Beamline Controls with FreeNX** | Mr. Zhijian YIN (Brookhaven National Lab) |
| 15:45-16:15 (00h30') | [10] **WARCS -Wide Area Remote Control for SPring-8** | Dr. Akihiro YAMASHITA (SPring-8) |
| 16:15-16:45 (00h30') | [13] **Control System Cyber-Security in Industry** | Stefan LUEDERS (CERN) |
| 16:45-17:30 (00h45') | [3] **Discussion** | Stefan LUEDERS (CERN) |


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