



# UPDATE ON THE CERN COMPUTING AND NETWORK INFRASTRUCTURE FOR CONTROLS (CNIC)

S. Lüders on behalf of the CNIC WG

CERN IT/CO, Geneva, Switzerland

**ABSTRACT** Over the last few years modern accelerator and experiment control systems have increasingly been based on commercial-off-the-shelf products (VME crates, PLCs, SCADA systems, etc.), on Windows or Linux PCs, and on communication infrastructures using Ethernet and TCP/IP. Despite the benefits coming with this (r)evolution, new vulnerabilities are inherited too: Worms and viruses spread within seconds via the Ethernet cable, and attackers are becoming interested in control systems. Unfortunately, control PCs cannot be patched as fast as office PCs. Even worse, vulnerability scans at CERN using standard IT tools have shown that commercial automation systems lack fundamental security precautions: Some systems crashed during the scan, others could easily be stopped or their process data be altered [1]. During the two years following the presentation of the CNIC Security Policy at ICALEPCS2005 [2], a "Defense-in-Depth" approach has been applied to protect CERN's control systems. This presentation will give a review of its thorough implementation and its deployment. Particularly, measures to secure the controls network and tools for user-driven management of Windows and Linux control PCs will be discussed.

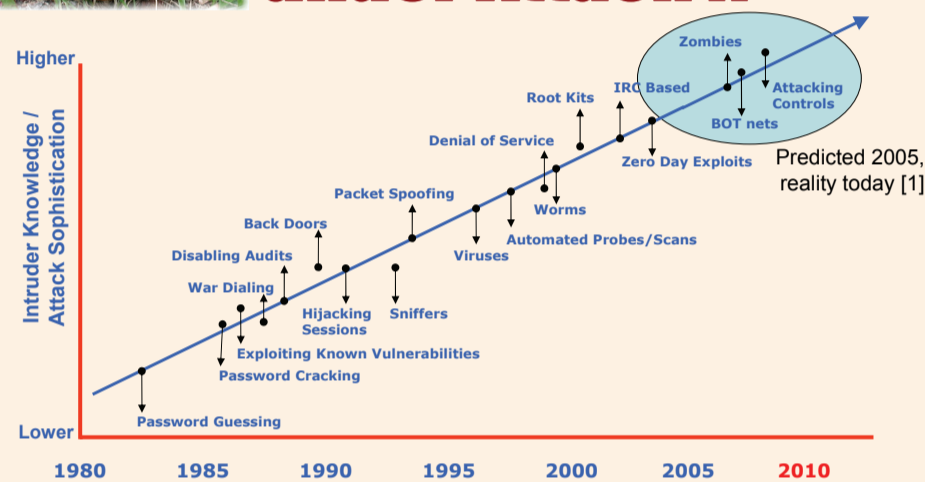
## The (R)Evolution of Control Systems

- Controls networks meet campus / business networks**
- Proprietary field buses (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, ...

## Control Systems under Attack !?



**Control Systems: Era of Legacy Technology ("Security through Obscurity")**

**Transition Phase ("Controls goes IT")**

**Era of Modern Information Technology ("From Top-Floor to Shop-Floor")**

## Risk = Threat × Vulnerability × Consequence

**CSO The Resource for Security Executives**

**Russia welcomes hack attacks**  
Secret kiddies cut both heading critical infrastructure  
By Thomas C. Greene in Washington — May 15, 2007  
Published Thursday, 27th April 2007 12:25 GMT  
The new perspective: data from thousands of tech websites

**U.S. Critical Infrastructure in Serious Jeopardy**  
Our electrical services, transportation, telecommunications and drinking water are at serious risk from very simple hacker attacks.

**Hole Found in Protocol Handling Vital National Infrastructure**  
Systems that control dams, oil refineries, railroads and nuclear power plants have a vulnerability that could open a system takeover, according to a recent research report.

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

**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 that affected, or could have affected, process control. And because few companies willingly disclose breaches of security, experts believe the actual number is much higher.

**Zotob, PNP Worms Slam 13 DaimlerChrysler Plants**  
penetration led 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]

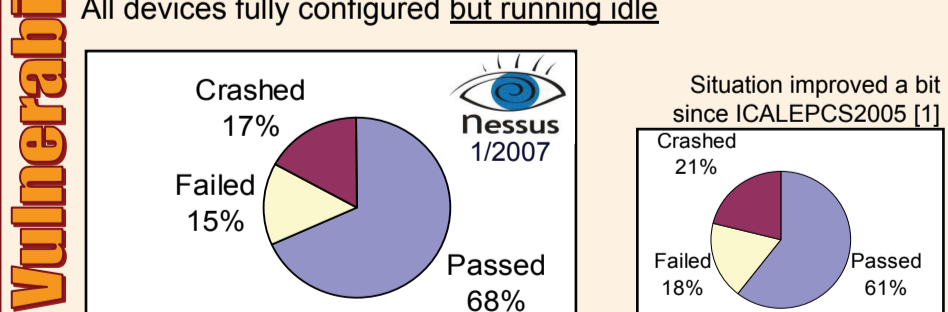
**Spreads of Internet worm infections knocked 11 of DaimlerChrysler's U.S. auto manufacturing plants**  
Several for four hours. The worm, spreading since the end of last week, attacked Windows XP systems were patched, a company spokesperson told ENR.

**Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware and Michigan were knocked offline at around 3:00 PM on Tuesday, stopping vehicle production at those plants for up to 30 minutes, according to the company's press release.**

**CERN TOSSIC Vulnerability Scans [1]**

31 devices from 7 different manufacturers (53 tests in total)

All devices fully configured but running idle



- Equipment being affected or even destroyed**
- Some very expensive, esp. in experiments & accelerators
  - Sometimes impossible to repair / replace

- Processes being disturbed**
- High interconnectivity, thus very sensitive to disturbances
  - A cooling process PLC failure can stop the accelerator
  - A power controller failure can stop a (sub-)detector
  - Difficult to configure

- Time being wasted**
- Downtime reduces efficiency (esp. data loss in experiments)
  - Time needed to re-install, re-configure, test and/or re-start
  - Requires many people working, possibly outside working hours

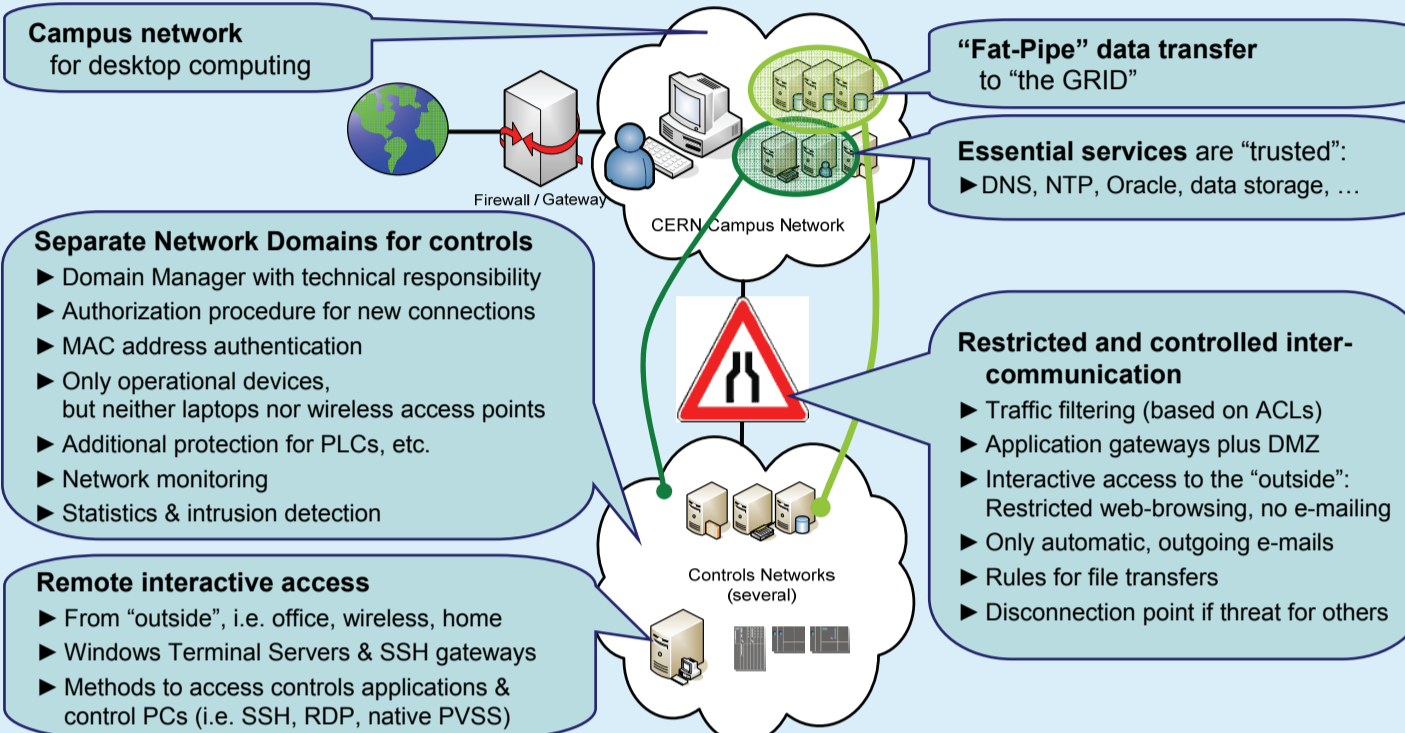
## CERN's Mitigation: "Defense-in-Depth"

"Defense-in-Depth" means security on each layer:

...of the security of the device itself, ...of the firmware and operating system, ...of the network connections & protocols, ...of the software applications (for PLC programming, SCADA, etc.), ...of third party software, and ...together with users, developers & operators.

CERN's solution is based on the "Good Practice Guidelines Parts 1-7" of the U.K. Centre for the Protection of the National Infrastructure (CPNI) [3].

## Network Segregation



- From experience at CERN, only centrally managed and patched PCs have shown to be secure in the long run.**
- Use centrally managed systems wherever possible
  - Ensure prompt security updates: OS, applications, anti-virus, etc.

### Development of a User-driven PC management

- Pass flexibility and responsibility to the User
- HE decides WHEN to install WHAT on WHICH control PCs (instead of the IT people)
- IT will send out email notifications of new patches to be installed
- HE has to ensure security
- PCs might be blocked if threat for others

**Web-based Computer Management Framework (CMF)** for Window XP and Windows Server [4]

**Template-based Linux For Controls (L4C)** for CERN Scientific Linux 3/4 using quattor

**Automatic & network-based installation**

- Centrally managed OS & applications
- User applications, settings, and Look & Feel
- Configuration of access rights & restrictions

**On many PCs in parallel**

**Full remote control of...**

- Installation & configuration
- Patching
- Reboots

... this works even for oscilloscopes !!!

## Central Installation Schemes

## Authentication & Authorization

- People are always the weakest link.**
- Need for a proper, coherent, and CERN-wide access control
  - Ensuring traceability of access (who, when, and from where)
  - Passwords must be kept secret: beware of "Google Hacking"
  - In exceptional cases using strong authentication

Still problematic areas: e.g. problems controlling user privileges in commercial controls applications, no generalization to one common central scheme at CERN, lack of access control in standard communication protocols

### Making security an objective

- Security training for users, operators, and system experts
- Bringing together IT and controls people
- Management buy-in due to incident at CERN's magnet test-stand
- Manufacturers and vendors became part of the solution. Security demands will be soon included into orders and call for tenders

### Discussion with governments, industry, and users

- Control System Cyber-Security (CS<sup>2</sup>/HEP) workshop [6]
- CERN is chairing the EuroSCSIE, with members from European governments, industry and research institutions that are dependent upon and, or whose responsibility it is to improve the security of SCADA and Control Systems.



## Incident Handling & System Recovery

Even with a stringent Security Policy incidents can never be prevented completely.

- Incident handling became part of CERN's general procedures
- Handling incidents on a Domain have been and will be jointly performed by CERN's Computer Security Team and the corresponding Domain Administrator
- The acting Computer Security Officer has the right to take appropriate actions in justified emergency cases
- CERN's Central Installation Schemes CMF and L4C allow for prompt system recovery

## Auditing & Assessment

### Keeping and raising the level of security

- Annual reviews of the CNIC Security Policy and its implementation planned for the future; the last being held in summer 2007

**SUMMARY** Due to the continuing integration of common IT technology into control systems, the corresponding IT security vulnerabilities and cyber-attackers end up threatening control systems, and, thus, CERN's operation and assets. However, control systems demand a different approach to security than office systems do. This poster presents a thorough rule-set to secure CERN's control systems. Its implementation uses a "Defense-in-Depth" approach based on network segregation, central installation schemes, authentication & authorization, user training, incident response & system recovery, and security auditing

**ACKNOWLEDGEMENTS** The author would like to thank all his colleagues at CERN involved in the realization of CNIC making it such a success; in particular A. Bland, P. Charrue, I. Deloose, M. Dobson, U. Epting, N. Høimyr, S. Poulsen, and M. Schröder.

### REFERENCES

- S. Lüders, "Control Systems Under Attack ?", ICALEPCS, Geneva, October 2005.
- U. Epting et al., "Computing and Network Infrastructure for Controls", ICALEPCS, Geneva, October 2005.
- Centre for the Protection of the National Infrastructure (CPNI), "Good Practice Guidelines Parts 1-7", London, 2006.
- I. Deloose, "The Evolution of Managing Windows Computers at CERN", HEPIx, Rome, April 2006.
- S. Gysin et al., "Role-Based Access Control for the Accelerator Control System at CERN"; K. Kostro et al., "Role-Based Authorization in Equipment Access at CERN"; A. Petrov et al., "User Authentication for Role-Based Access Control"; and P. Chocula, "Cyber Security in ALICE", these proceedings.
- S. Lüders, "Summary of the Control System Cyber-Security CS<sup>2</sup>/HEP Workshop", these proceedings.