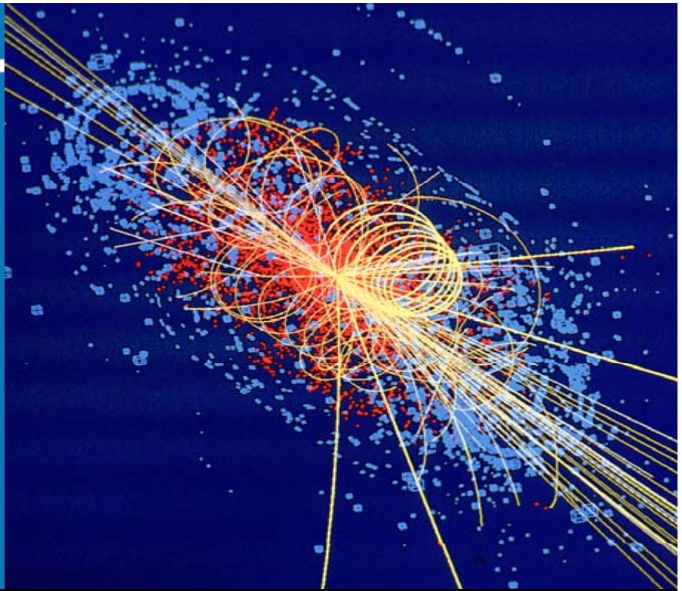
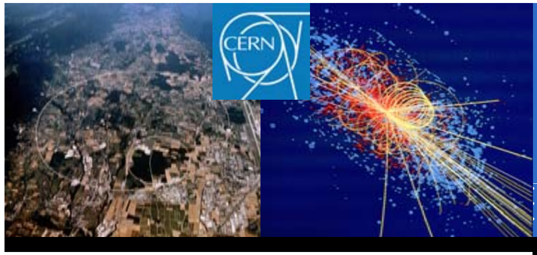


CERN Computing and Network Infrastructure for Controls (CNIC)

Status Report on the Implementation

Dr. Stefan Lüders (CERN IT/CO)

(CS)^2/HEP Workshop, Knoxville (U.S.)
October 14th 2007

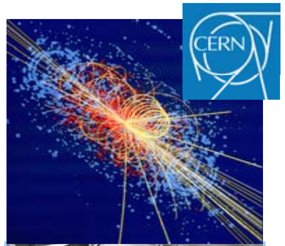


Overview

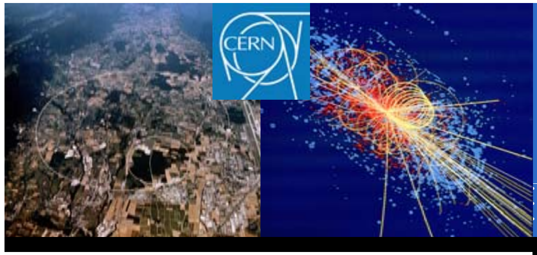
Risk = Consequence

× Threat

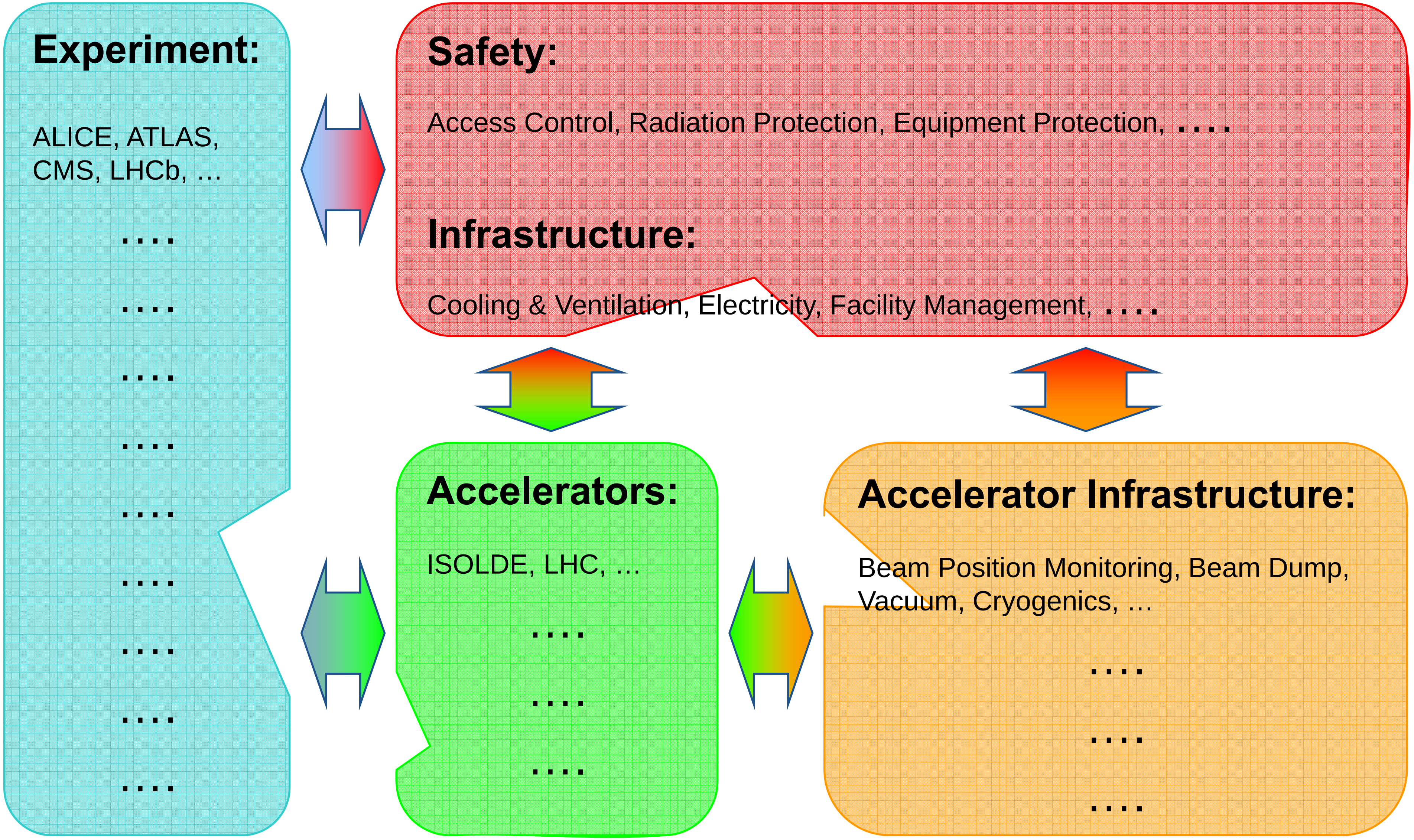
× Vulnerability



Mitigation:
"Defense-in-Depth"



Control Systems at CERN



Experiment:

ALICE, ATLAS,
CMS, LHCb, …

. . . .

. . . .

. . . .

. . . .

. . . .

. . . .

. . . .

. . . .

. . . .

Safety:

Access Control, Radiation Protection, Equipment Protection, ...

Infrastructure:

Cooling & Ventilation, Electricity, Facility Management, ...

Accelerators:

ISOLDE, LHC, …

. . . .

. . . .

. . . .

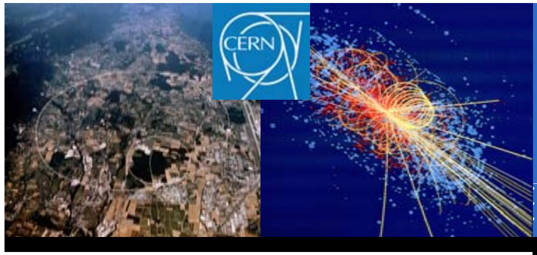
Accelerator Infrastructure:

Beam Position Monitoring, Beam Dump,
Vacuum, Cryogenics, …

. . . .

. . . .

. . . .



Standards, if possible !

- Commercial of the shelf hardware

standard desktop PCs

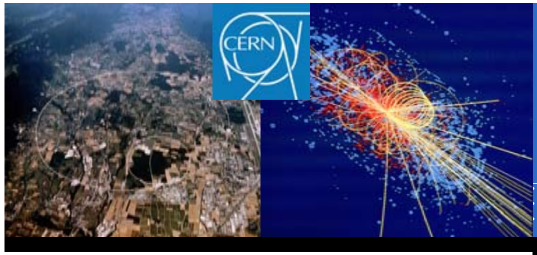
SIEMENS TRANE Sun microsystems CAEN Tools for discovery Linde AIR LIQUIDE WAGO CES CREATIVE ELECTRONIC SYSTEMS applicom iseg Tektronix Schneider Electric BECKHOFF INDUSTRIE ELEKTRONIK acqiris NATIONAL INSTRUMENTS HIRSCHMANN LeCroy WIENER

- Standard (controls) software

CORBA redhat LINUX CVS WinCC PcVue Gnu Savannah LynxOS ORACLE PVSS II Microsoft Wizcon Systems MySQL SONICMQ®

- Standard communication protocols

OPC FOUNDATION WorldFIP CAN I²C BUS W3C World Wide Web Consortium PROFI BUS PROCESS FIELD BUS Modbus-IDA PCI EXPRESS VMEbus Technology



CERN Assets at Risk

Equipment being affected or even destroyed

- Some very expensive, e ents & accelerators
- Sometimes imposs

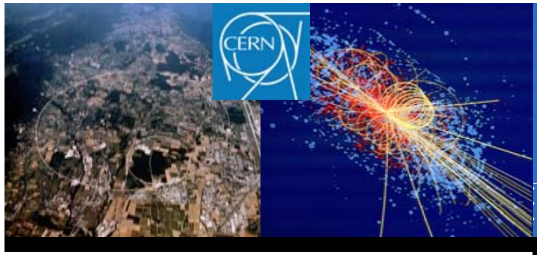
Processes bein

- High interco bances
  - *A coolin elerator*
  - *A power ctor*
- Difficult to co

Time being waste

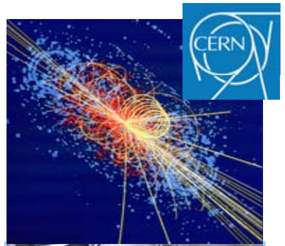
- Downtime reduces s in experiments)
- Time needed to re-install, re-configure, test and/or re-start
- Requires many people working, possibly outside working hours

Consequences are significant !



Risk = Consequence

× Threat



Who is the threat ?

Attacks performed by…

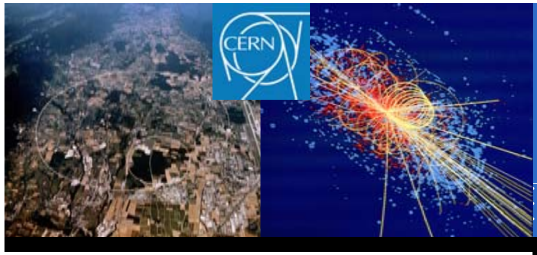
- Trojans, viruses, worms, …
- Disgruntled (ex-)employees or saboteurs
- Attackers and terrorists

Lack of robustness & lots of stupidity

- Mal-configured or broken devices flood the network
- Developer / operator “Finger trouble”

Lack of procedures

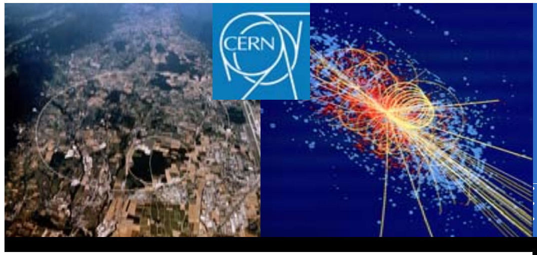
- Flawed updates or patches provided by third parties
- Inappropriate test rules and procedures



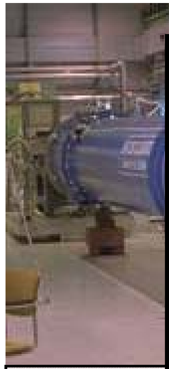
Risk = Consequence

× Threat

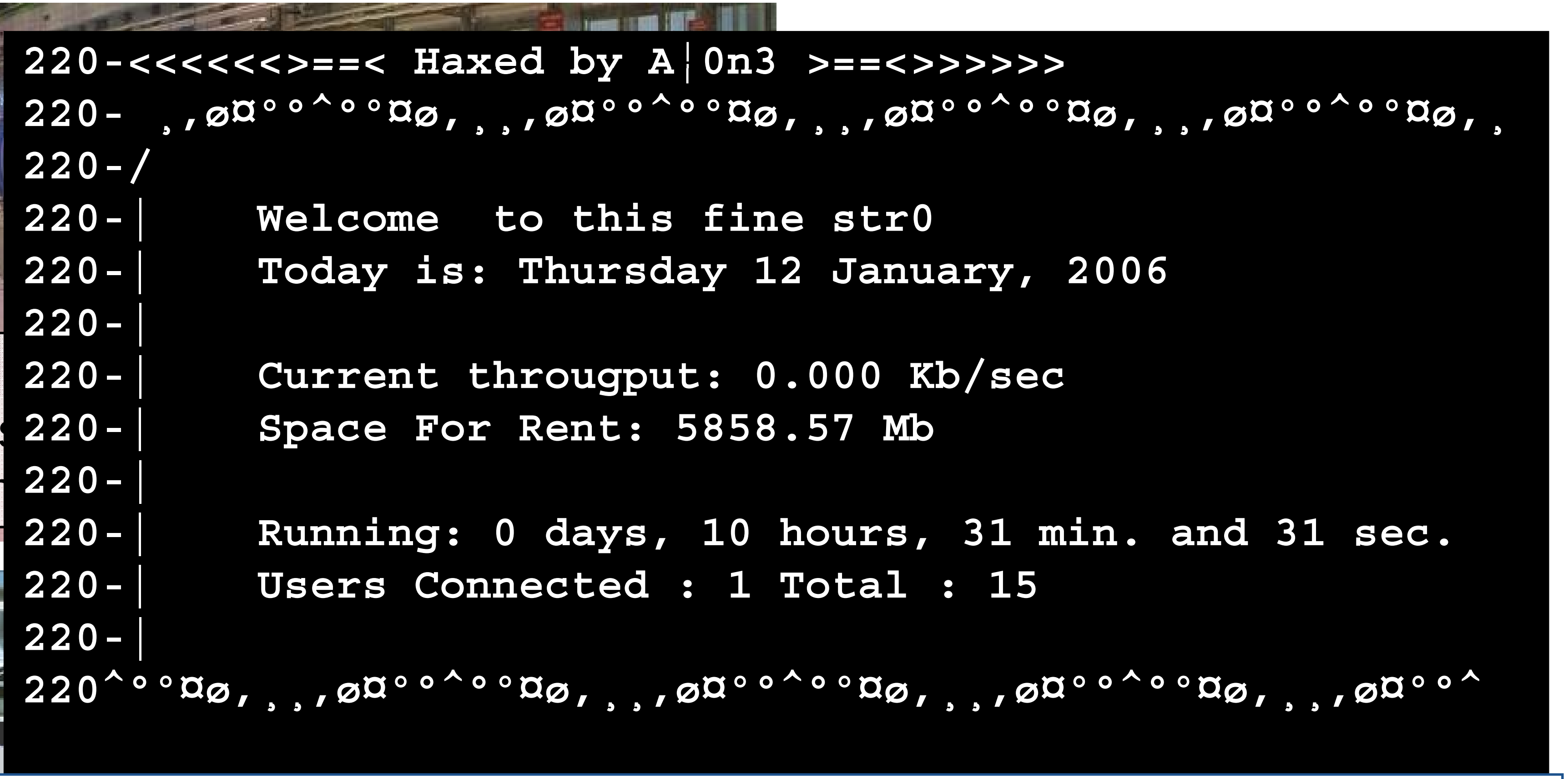
× Vulnerability



Vulnerabilities ARE fact !



2004:
and u
LHC r



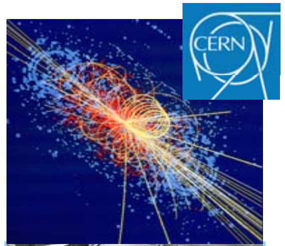
```
220-<<<<<<>==< Haxed by A¦0n3 >==<>>>>>>
220- ¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸
220-/
220-|     Welcome  to this fine str0
220-|     Today is: Thursday 12 January, 2006
220-|
220-|     Current througput: 0.000 Kb/sec
220-|     Space For Rent: 5858.57 Mb
220-|
220-|     Running: 0 days, 10 hours, 31 min. and 31 sec.
220-|     Users Connected : 1 Total : 15
220-|
220^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^
```

Management buy-in !

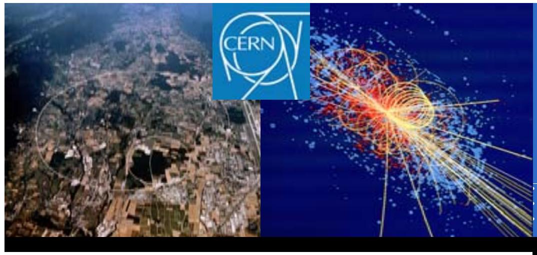
Risk = Consequence

× Threat

× Vulnerability



Mitigation: "Defense-in-Depth"



“Defense-in-Depth”

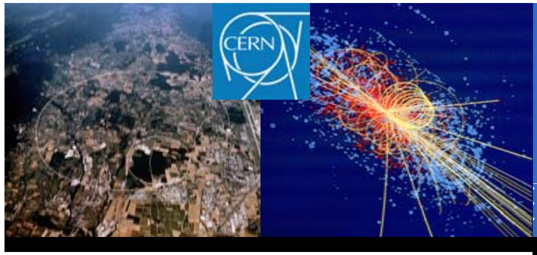
“Defense-in-Depth” means security on *each* layer !

- …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

Manufacturers and vendors are part of the solution !

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

"Control System Cyber-Security" needed !!!



9/2004: Development of a security policy for controls

- Major stakeholders from experiments, accelerator, infrastructure, and IT
- Management buy-in & support

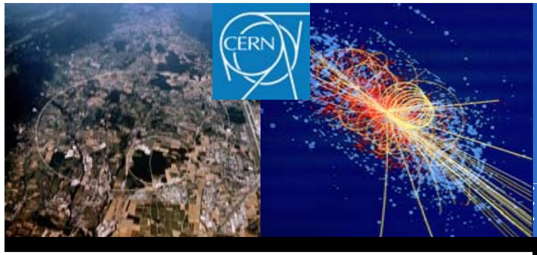
4/2005: CNIC Security Policy & implementation proposals

- Approved by all parties involved
- See ICALEPCS2005

10/2005: Implementation of major security measures

- Technical implementation done by IT:
  Network, Windows, and Linux experts
- Controls expert became part in CERN's Computer Security Team
- Huge effort in getting buy-in from developers, operators, and users

7/2007: Review of security policy & re-assessment of goals



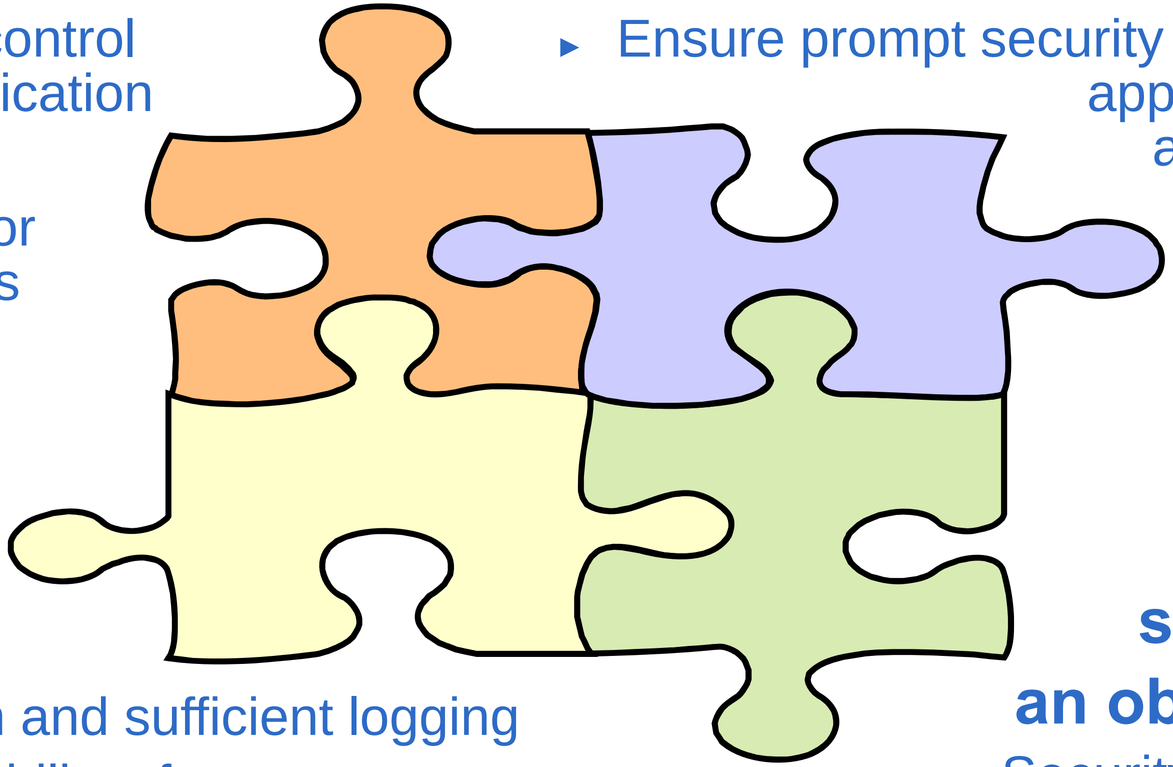
Ground Rules for Cyber-Security

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

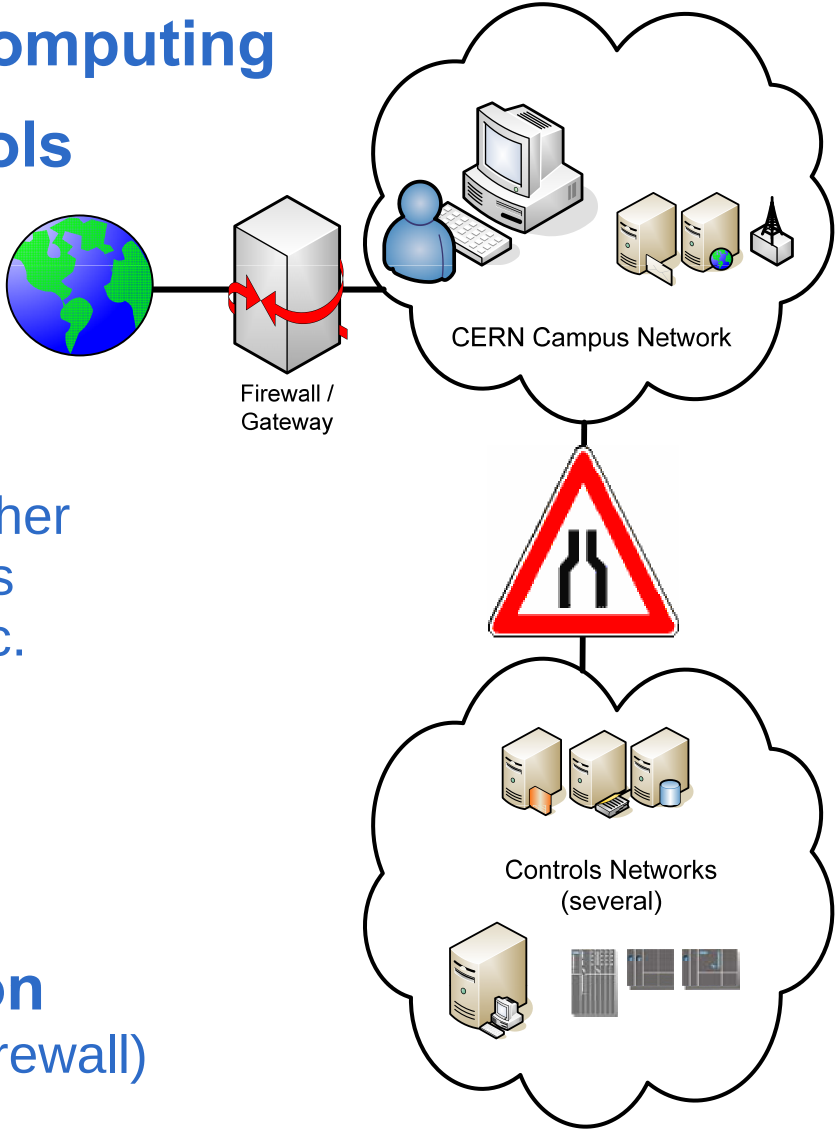
- Security training
- Management buy-in
- Bring together IT and Controls experts

Network Segregation

Campus network for desktop computing

"Networks Domains" for Controls

- Domain Manager with technical responsibility
- Authorization procedure for new connections
- MAC address authentication
- Only operational devices, but neither laptops nor wireless access points
- Additional protection for PLCs, etc.



Network monitoring

- Statistics & intrusion detection
- Disconnection if threat for others

Restricted cross-communication

- Traffic filtering (ACL-based plus firewall)
- Application gateways plus DMZ

Restricted Inter-Communication

Remote interactive access *from* "outside"

- "outside" means "office", "home", "wireless"
- Using (Windows) Terminal Servers
- Methods to access controls applications
- Methods to access local control PCs

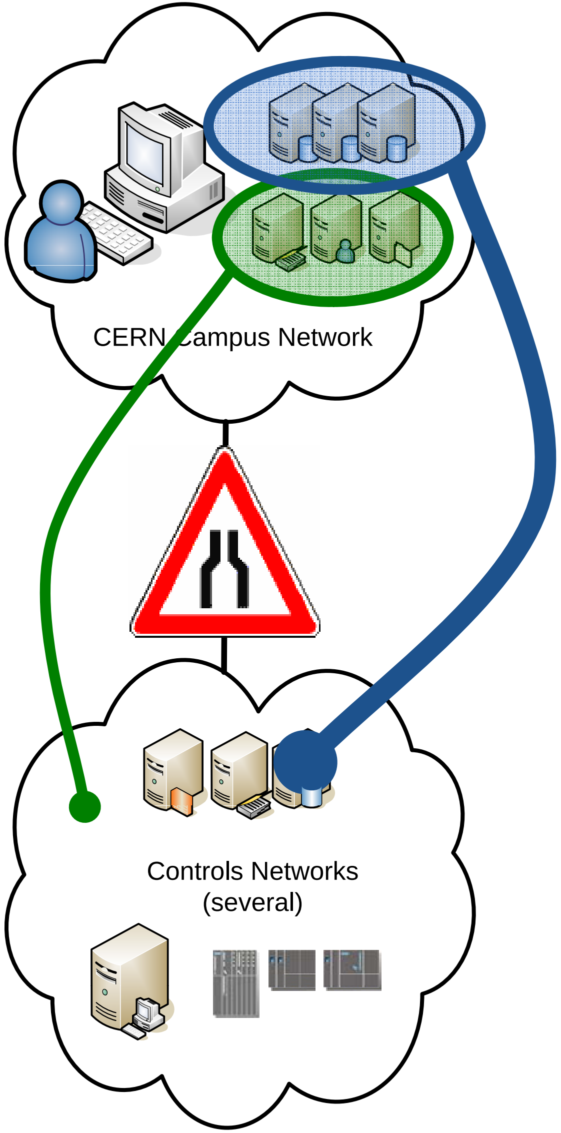
Interactive access *to* the "outside"

- Rules for web-browsing, automatic e-mails, file transfer, etc.

"Fat-Pipe" data transfer to "the GRID"

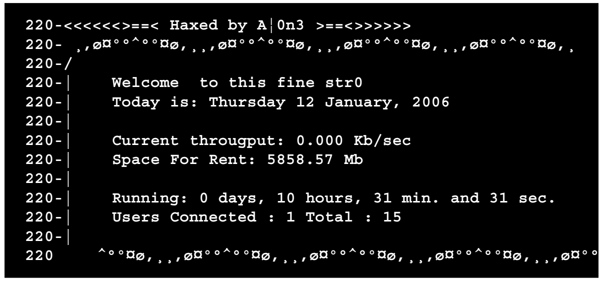
Essential services are "trusted"

- DNS, NTP, Oracle, data storage, …



Central Installation Schemes (1)

"Poorly secured systems are being targeted."



```
220-<<<<<<>==< Haxed by A¦0n3 >==<>>>>>>
220- ¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸
220-/
220-|     Welcome  to this fine str0
220-|     Today is: Thursday 12 January, 2006
220-|
220-|     Current througput: 0.000 Kb/sec
220-|     Space For Rent: 5858.57 Mb
220-|
220-|     Running: 0 days, 10 hours, 31 min. and 31 sec.
220-|     Users Connected : 1 Total : 15
220-|
220     ^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°
```

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 department)
- IT will send out email notifications of new patches to be installed
- ***HE*** has to ensure security
- However, PCs might be blocked if threat for others

Implementations for

- Windows XP, Windows Server (web-based interface)
- CERN Scientific Linux 3/4 (terminal-based) using quattor

Central Installation Schemes (2)

Install…

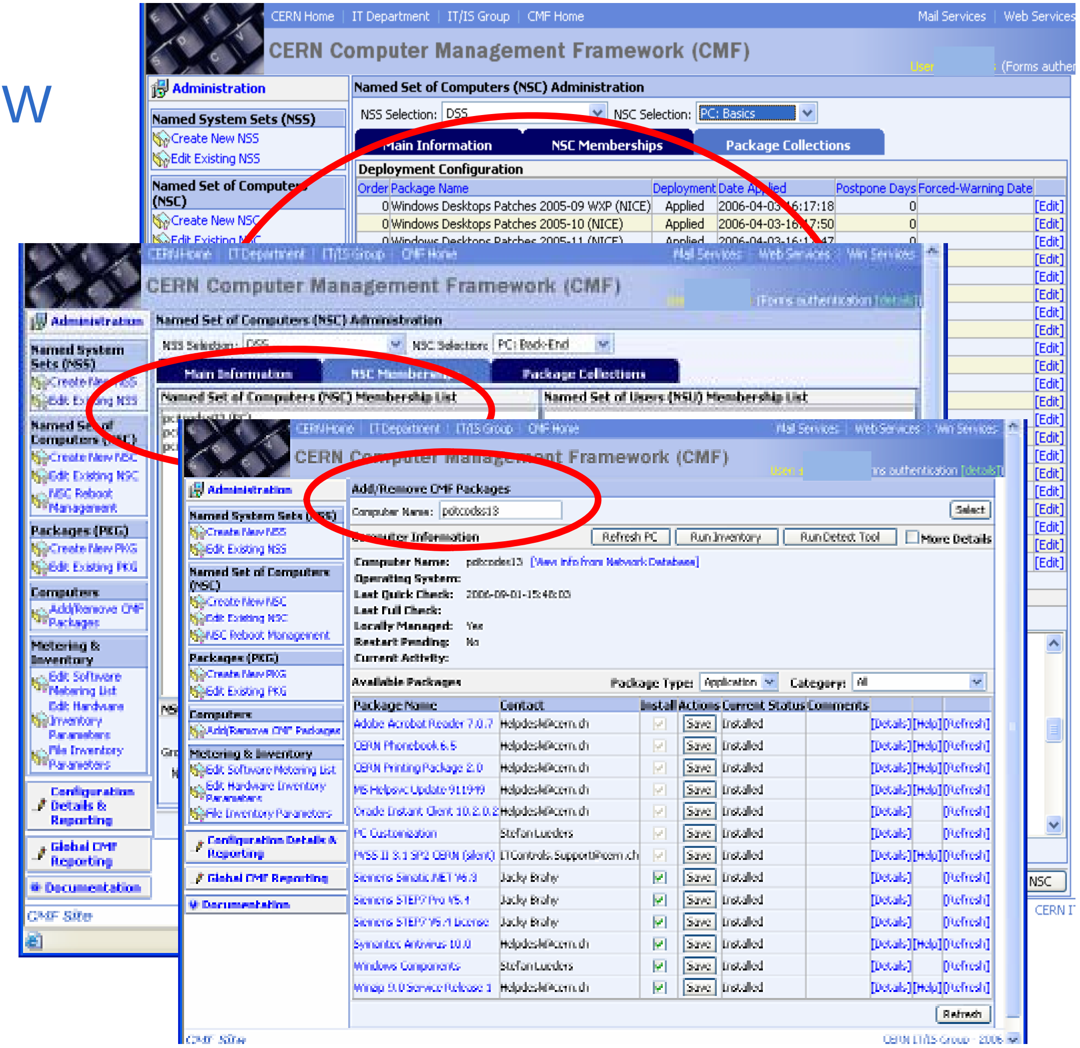
- Centrally managed OS & SW
- User applications
- Automatically & network-based
- On many PCs in parallel

Configure…

- Look & Feel
- Access rights & restrictions

Full remote control of…

- Configuring
- Installation
- Patching
- Rebooting



CERN Home | IT Department | IT/IS Group | CMF Home — Mail Services | Web Services

CERN Computer Management Framework (CMF)

Named Set of Computers (NSC) Administration

NSS Selection: DSS — NSC Selection: PC: Basics

Main Information | NSC Memberships | Package Collections

Deployment Configuration

Order	Package Name	Deployment	Date Applied	Postpone Days	Forced-Warning Date	
0	Windows Desktops Patches 2005-09 WXP (NICE)	Applied	2006-04-03-16:17:18	0		[Edit]
0	Windows Desktops Patches 2005-10 (NICE)	Applied	2006-04-03-16:17:50	0		[Edit]
0	Windows Desktops Patches 2005-11 (NICE)	Applied	2006-04-03-16:1?:47	0		[Edit]

Named Set of Computers (NSC) Administration

NSS Selection: DSS — NSC Selection: PC: Back-End

Main Information | NSC Memberships | Package Collections

Named Set of Computers (NSC) Membership List — Named Set of Users (NSU) Membership List

Add/Remove CMF Packages

Computer Name: pdtcodes13 — Select

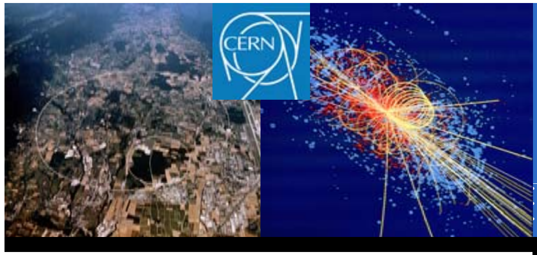
Computer Information — Refresh PC | Run Inventory | Run Detect Tool | □ More Details

Computer Name: pdtcodes13 [View info from Network Database]
Operating System:
Last Quick Check: 2006-09-01-15:48:03
Last Full Check:
Locally Managed: Yes
Restart Pending: No
Current Activity:

Available Packages — Package Type: Application — Category: All

Package Name	Contact	Install	Actions	Current Status	Comments			
Adobe Acrobat Reader 7.0.7	Helpdesk@cern.ch	✓	Save	Installed		[Details]	[Help]	[Refresh]
CERN Phonebook 6.5	Helpdesk@cern.ch	✓	Save	Installed		[Details]	[Help]	[Refresh]
CERN Printing Package 2.0	Helpdesk@cern.ch	✓	Save	Installed		[Details]	[Help]	[Refresh]
MS Helpsvc Update 911949	Helpdesk@cern.ch	✓	Save	Installed		[Details]	[Help]	[Refresh]
Oracle Instant Client 10.2.0.2	Helpdesk@cern.ch	✓	Save	Installed		[Details]		[Refresh]
PC Customization	Stefan Lueders	✓	Save	Installed		[Details]		[Refresh]
PVSS II 3.1 SP2 CERN (silent)	ITControls.Support@cern.ch	✓	Save	Installed		[Details]	[Help]	[Refresh]
Siemens Simatic.NET V6.3	Jacky Brahy	☑	Save	Installed		[Details]		[Refresh]
Siemens STEP7 Pro V5.4	Jacky Brahy	☑	Save	Installed		[Details]		[Refresh]
Siemens STEP7 V5.4 License	Jacky Brahy	☑	Save	Installed		[Details]		[Refresh]
Symantec Antivirus 10.0	Helpdesk@cern.ch	☑	Save	Installed		[Details]	[Help]	[Refresh]
Windows Components	Stefan Lueders	☑	Save	Installed		[Details]		[Refresh]
Winzip 9.0 Service Release 1	Helpdesk@cern.ch	☑	Save	Installed		[Details]	[Help]	[Refresh]

… this works even for oscilloscopes !!!



Policies on Access Control

"People are increasingly the weakest link."

Restricted emailing or web browsing on controls networks

Role Based Access Control

- User credentials for authentication
- Role assignment for authorization
- Strict rules for remote access
- See talks by S. Gysin & P. Chochula

However, still problematic areas

- Lack of access control in standard communication protocols
- Problem controlling user privileges in commercial controls applications
- Generalisation to one common central scheme at CERN

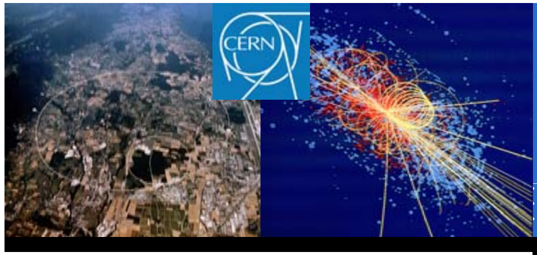
Incident Response & System Recovery

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

Incident handling on a Domain

- Part of CERN's general procedures
- Jointly by Domain Administrator & CERN's Computer Security Team
- In emergencies, the acting
  CERN Security Officer has the right to take appropriate actions

CERN's Central Installation Schemes CMF and L4C allow for fast system recovery.



Review & Re-assessment

Recent review of the CNIC Security Policy:

- Review threat scenarios and priorities
- Review assumptions being made initially
- Take more realistic perspective
- Document and review the implementation
- Regular annual reviews of the CERN CNIC Security Policy and its implementation planned for the future

Still some construction sites:

- Large DMZ & lots of exceptions (*"We're still in commissioning phase"*)
- Some control systems still on campus network (e.g. some fixed-target experiments)
- Single sign-on and a coherent CERN-wide solution (still too many authentication & authorization schemes around)

Summary

Control Systems at CERN

Experiment:

Safety:

Infrastructure:

Cooling & Ventilation, Electricity, Facility Management, ….

CERNs control systems are complex, expensive & unique.

Vulnerabilities ARE fact !

The risk is not zero.

```
220-/
220-|     Welcome  to this fine str0
220-|     Today is: Thursday 12 January, 2006
220-|
220-|     Current througput: 0.000 Kb/sec
220-|     Space For Rent: 5858.57 Mb
220-|
```

Management buy-in !

Better tackle the problem before it's too late !!!

- …of the network connections & protocols,
- …of the software applications (for PLC programming, SCADA, etc.),
- …of third party software, and
- …together with users, developers & operators
- Security demands should be included into orders and call for tenders

"Control System Cyber-Security" needed !!!

A "Defense-in-Depth" approach offers 100%-ε mitigation.

Ground Rules for Cyber-Security

- Reduce and control inter-communication
- Deploy IDS
- Apply policy for remote access
- Ensure prompt security updates: applications, anti-virus, OS, etc.

Deploy access control

- Use strong authentication
- Passwords must be kept secret: beware of "Google Hacking"

Make security an objective

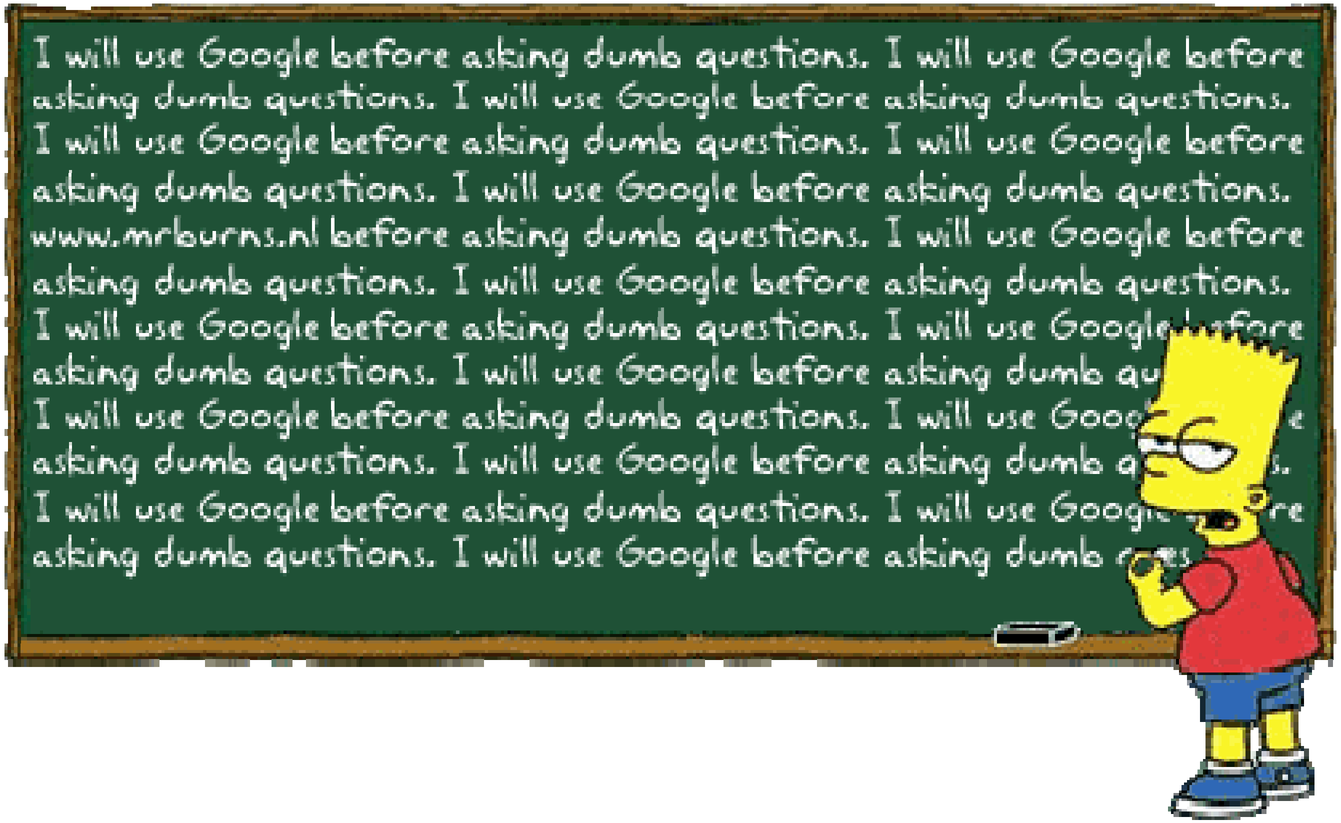
- Bring together IT and Controls experts

Security measures are applied on multiple-levels.

Thanks a lot !

Special acknowledgements go to:

- The CNIC working group
- A. Bland, P. Charrue (AB), I. Deloose, N. Høimyr, M. Schröder (IT), M. Dobson (ATLAS), U. Epting, S. Poulsen (TS)



I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google efore
asking dumb questions. I will use Google before asking dumb qu
I will use Google before asking dumb questions. I will use Goog e
asking dumb questions. I will use Google before asking dumb q s.
I will use Google before asking dumb questions. I will use Goog re
asking dumb questions. I will use Google before asking dumb ques