

Control Systems Under Attack !?

…about the Cyber-Security of modern Control Systems

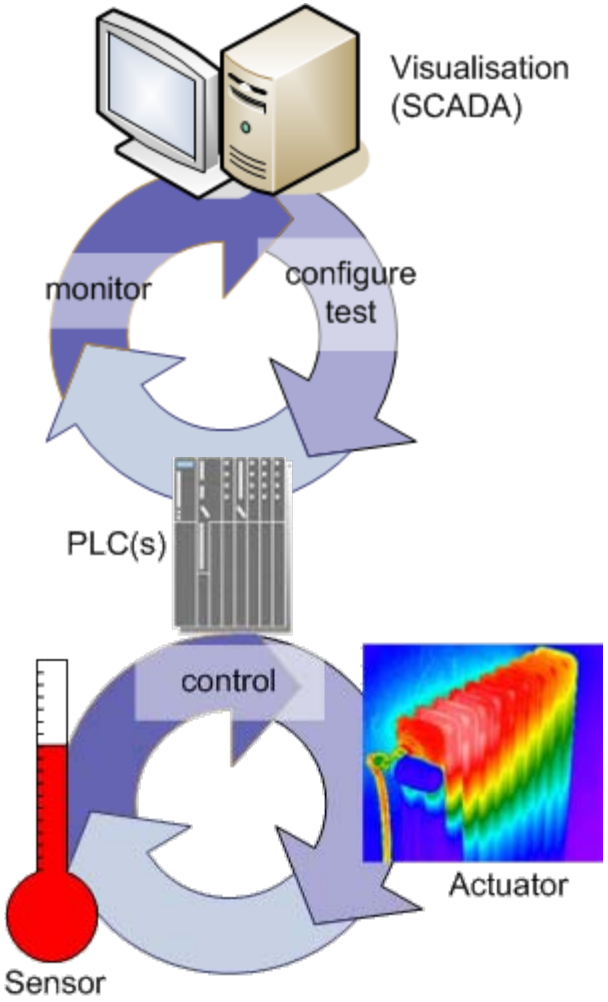
Dr. Stefan Lüders (CERN Computer Security Team)

"Protecting Office Computing, Computing Services, GRID & Controls"

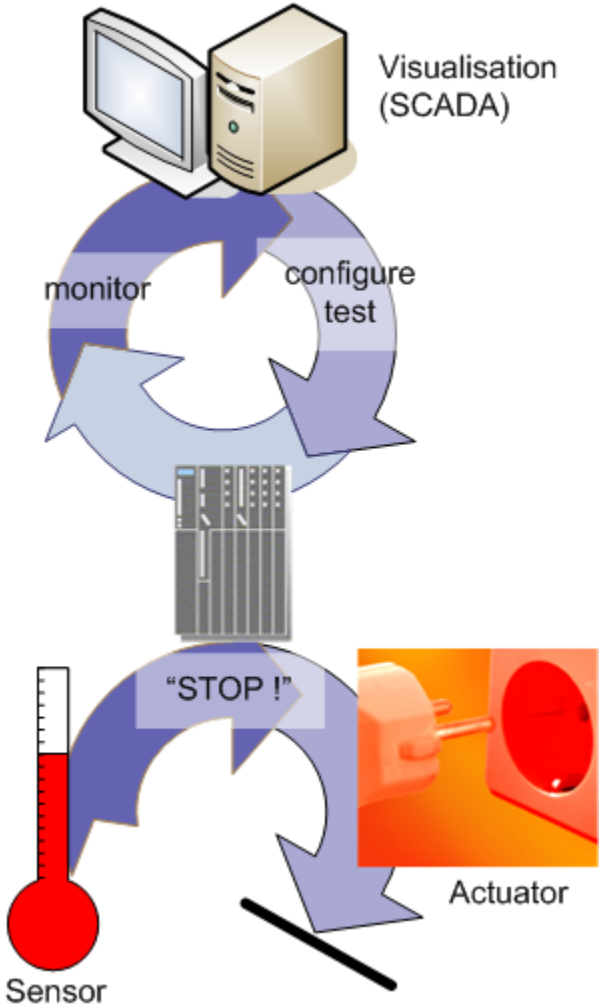
Openlab Students Lectures July 7th 2009


Control Systems in a Nutshell

Control System

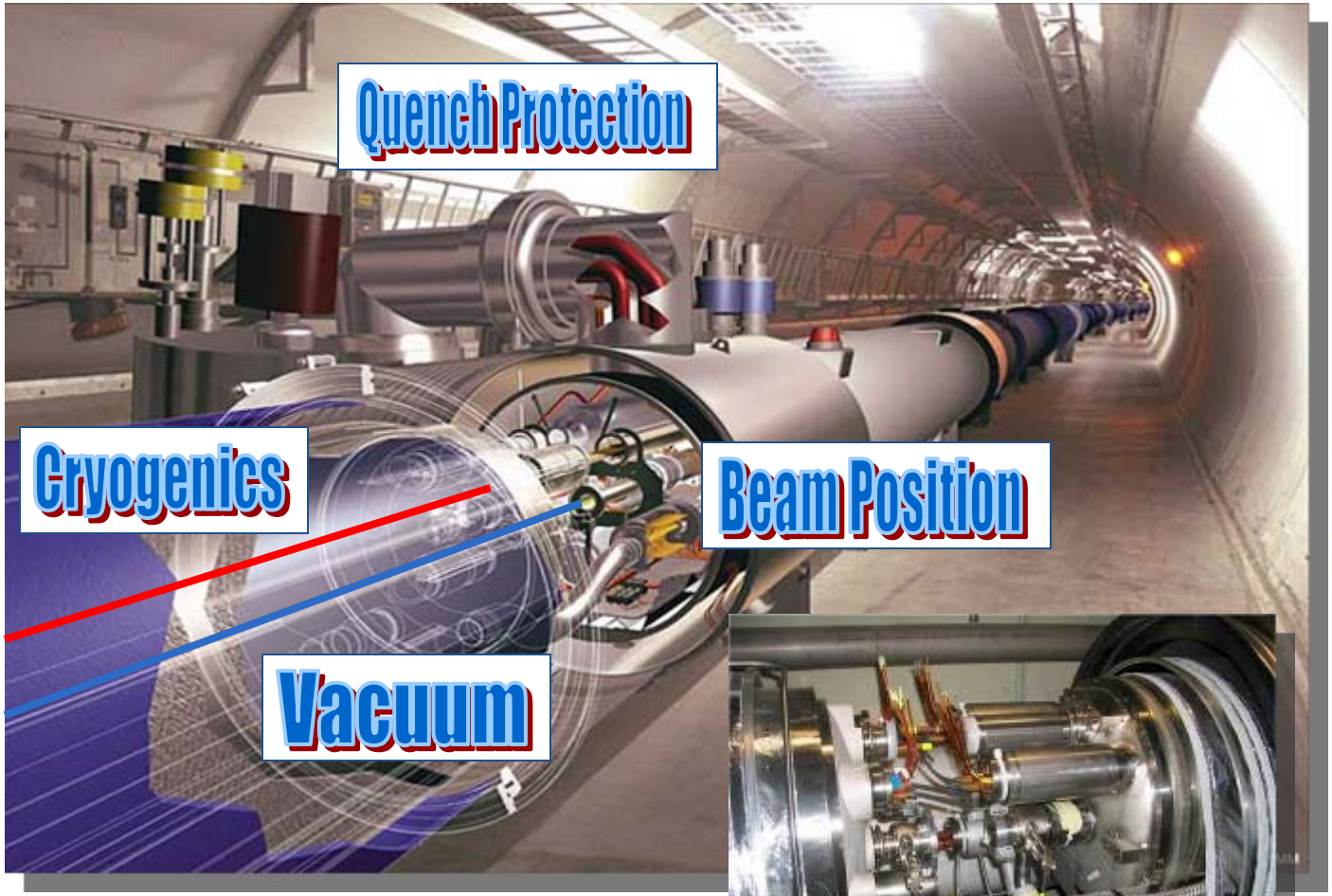


Safety System



The Large Hadron Collider (LHC)

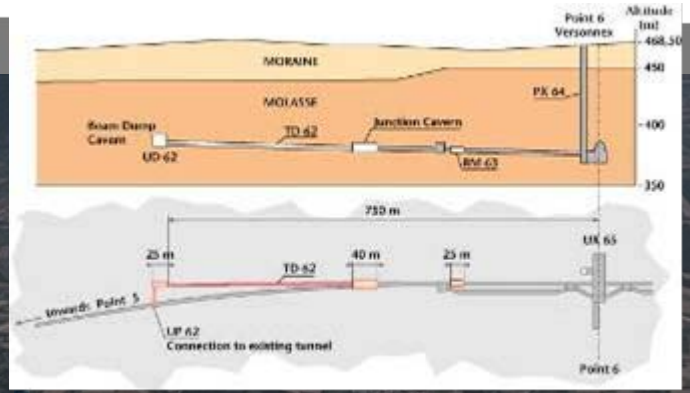

LHC Beam Optics



Steer a beam of 85 kg TNT through a 3mm hole 10000 times per second !

World's largest superconducting installation (27km @ 1.9°K) worth 2B€


CERN Accelerator Complex



Radio Frequency

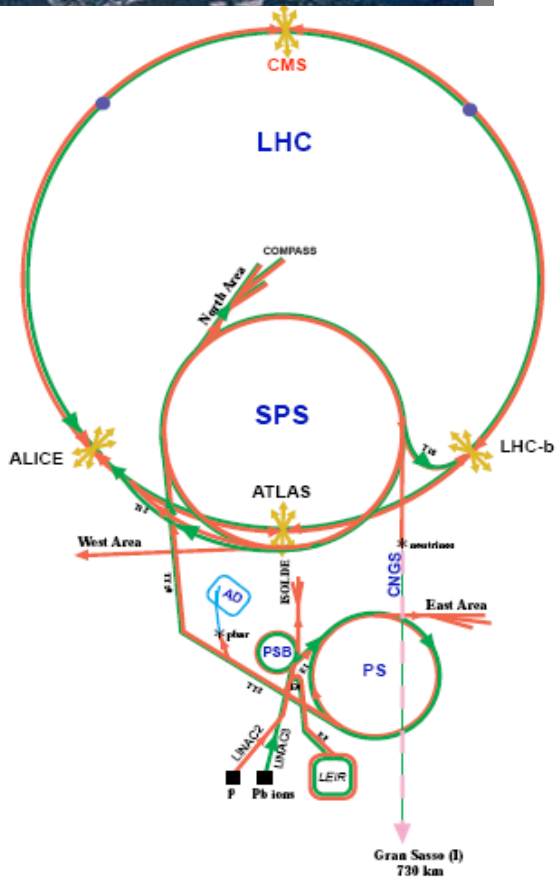
Machine Protection

Beam Dump

Beam Orbit

Timing

Pre-Accelerators



General Infrastructure

Access Control

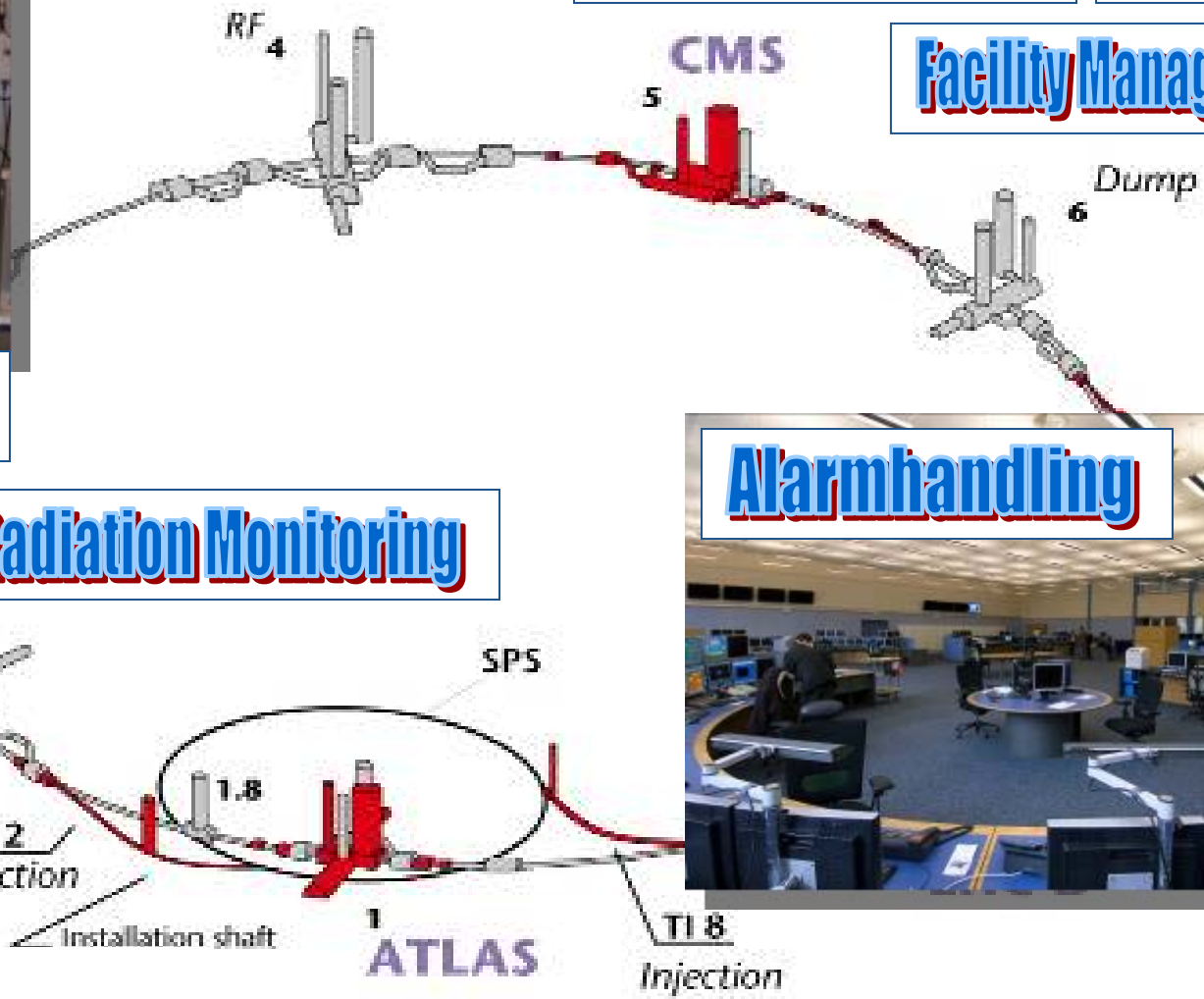
Cooling & Ventilation

Electricity

Facility Management

Safety

Radiation Monitoring



Alarmhandling

Data Acquisition Control

(Sub-)Detectors

Data Acquisition

Triggering

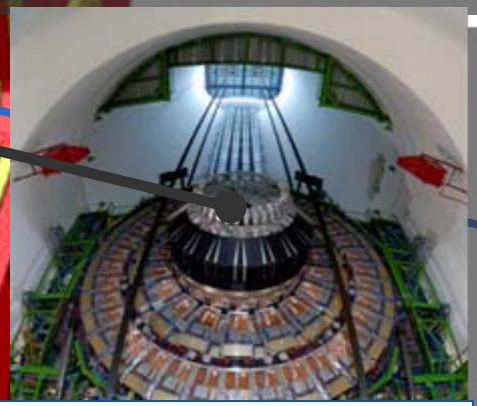
Experiment

Run Control

About 100 million data channels

Control Systems for Experiments

- Electricity
- Gas Distribution
- Cooling & Ventilation
- High Voltage
- Magnet
- Cryogenics
- Safety
- Radiation
- Smoke
- Sniffer



About one million control channels


Control Systems at CERN

Experiment:

ALICE, ATLAS, CMS, LHCb, LHCf and TOTEM

ALPHA (AD-5), Cast, Collaps, Compass, Dirac, Gamma Irradiation Facility, ISOLTRAP, MICE R&D, Miniball, Mistral, NA48/3, NA49, NA60, nTOF, Witch, …

GCS, MCS, MSS, and Cryogenics System

Safety:

ACIS, AC PS1, AC PS2, AC SPS1, AC SPS2, Alarm Repeater, ARCON, ADS, CSA, SGGAZ, SFDIN, CSAM, CESAR, DSS, LACS, LASS, LASER, Radmon, RAMSES, MSAT, Radio Protection Service, Sniffer System, SUSI, TIM, and Video Surveillance

Infrastructure:

CV, ENS, FM, DBR, Gamma Spectroscopy, TS/CSE, and YAMS

Accelerators:

AB/OP, AD, CNGS, CCC, CLIC, ISOLDE, ISOLDE offline, LEIR, LHC, Linac 2, Linac 3, PS, PS Booster, REX, SM18, and SPS

Accelerator Infrastructure:

ADT, ACS, BQE, BPAWT, BDI, BIC, BLM, BOF, BPM, BOB, BSRT, BTV, BRA, CWAT, Cryo (Frigo, SM18 & Tunnel), BCTDC, BCTF, FGC, LEIR Low Level RF, LHC Beam Control System, LBDS, HC, LHC Logging Service, LTI, MKQA, APWL, BPL, OASIS, PIC, QDS/QPS, BQS, SPS BT, BQK, Vacuum System, WIC, and BWS


Overview

The (r)evolution of control systems...

...omitted security aspects!

Why worry ? The risk equation

Mitigation: Defense-in-Depth

Team Up: Risks & Mitigations are int'l !


Standard Hard and Software



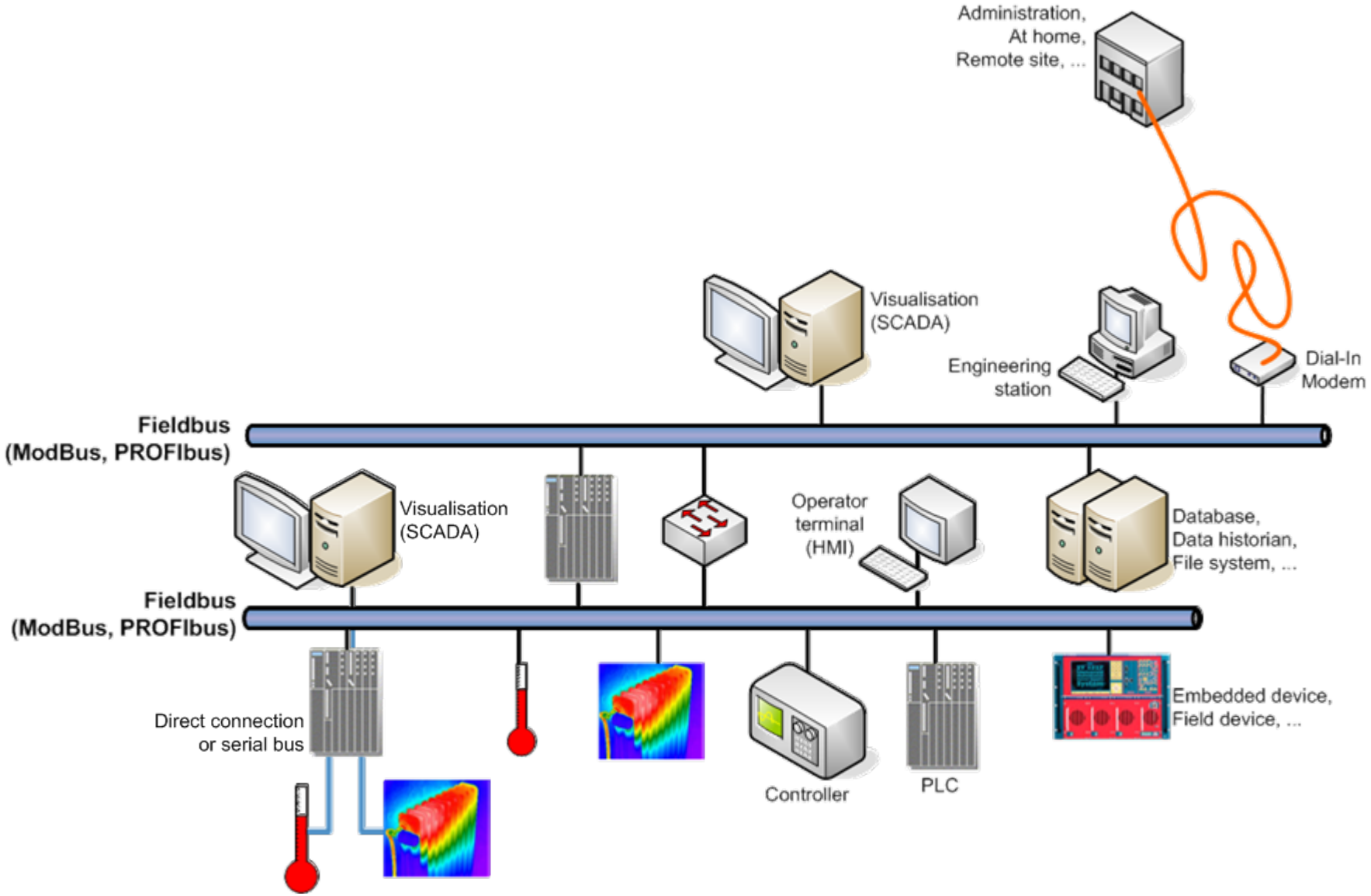

Ethernet & Wireless
Modbus/TCP, OPC & Telnet

Common of the shelf HW
Desktop PCs & Laptops
Windows & Linux

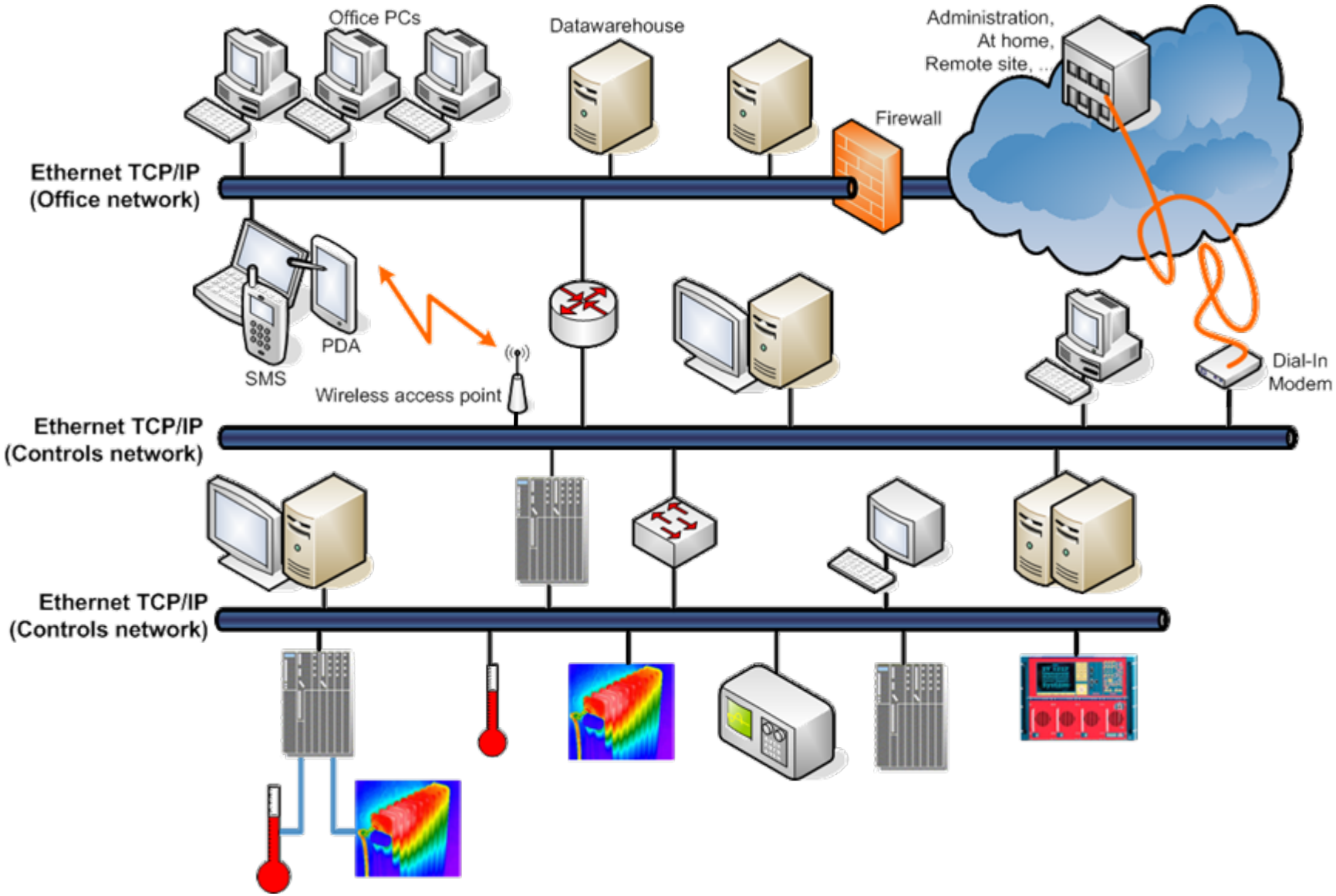
WWW & Emails
C++, Java, XML, Corba...
Oracle, Labview...

Shared Accounts & Passwords


(R)Evolution: The Past




(R)Evolution: Today




“Controls” is *not* IT ! (1)

	“Office IT”	“Controls”
System Life Cycle	3 – 5 years	5 – 20 years
Availability	scheduled interventions OK	24h / 7d / 365d
Confidentiality	high	low
Time Criticality	delays tolerated	critical
Security Knowledge	exists	usually low
Intrusion detection	standard	…no signatures…
DHCP	standard	Fixed IPs in hardware configurations
Usage of wireless	frequent	increasing use


“Controls” is *not* IT ! (2)

	“Office IT”	“Controls”
Changes	frequent, formal & coordinated	rare, informal & not always coordinated
Patches & Upgrades	frequent	infrequent or impossible (needs extensive tests)
Antivirus Software	standard	rare or impossible (might block CPU)
Reboots	standard	rare or impossible (processes will stop)
Password Changes	standard	rare or impossible (password “hardwired”)

"Do not touch a running system !!!"


Standard Vulnerabilities




Ethernet & Wireless
Modbus/TCP, OPC & Telnet

Common of the shelf HW
Desktop PCs & Laptops
Windows & Linux

WWW & Emails
C++, Java, XML, Corba...
Oracle, Labview...

Shared Accounts & Passwords

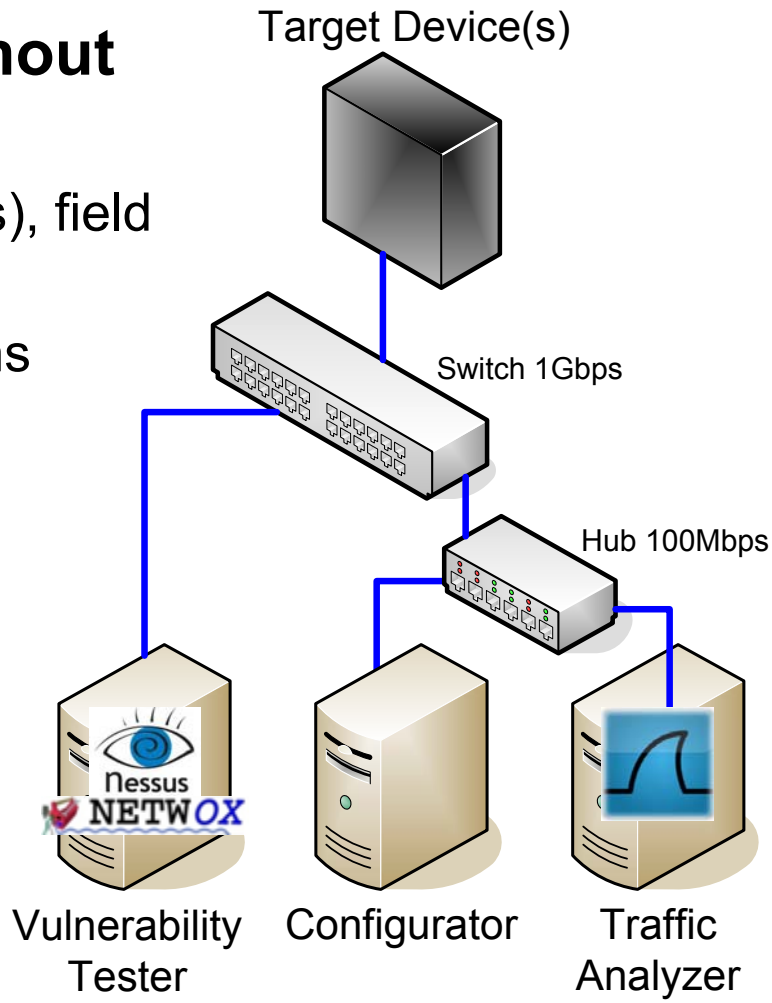

The TOCSSiC

COTS Automation Systems are without security protections.

- Programmable Logic Controllers (PLCs), field devices, power supplies, …
- Security not integrated into their designs

Teststand On Controls System Security at CERN (TOCSSiC)

- "Nessus" vulnerability scan (used in Office IT)
- "Netwox" DoS attack with random fragments
- "Wireshark" network sniffer

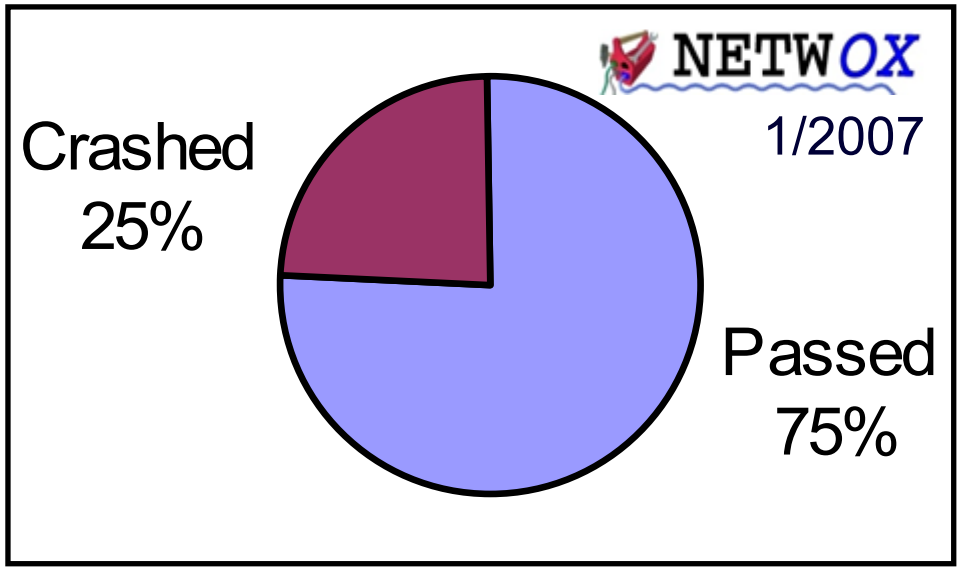


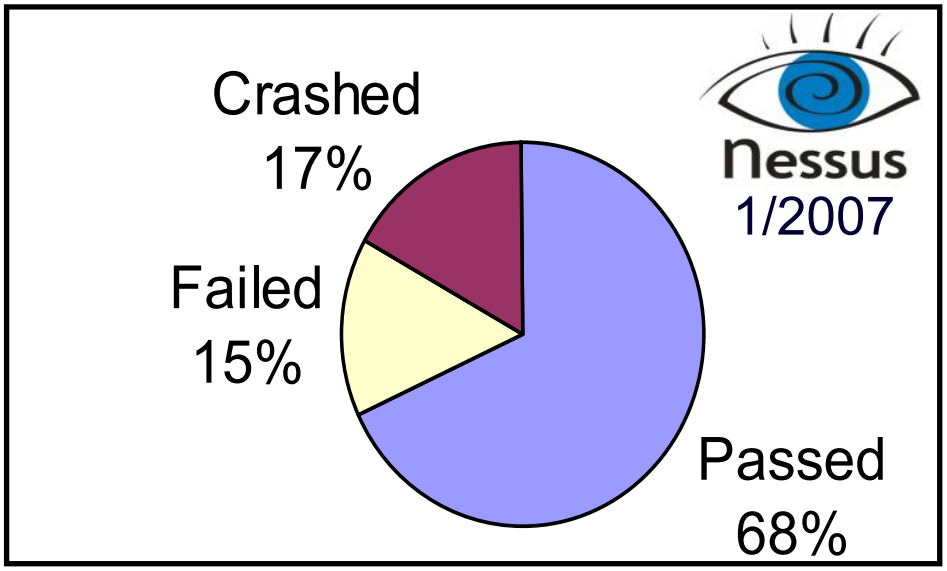
…going for the low-hanging fruits !!!


Control Systems under Attack !

CERN TOCSSiC Vulnerability Scans

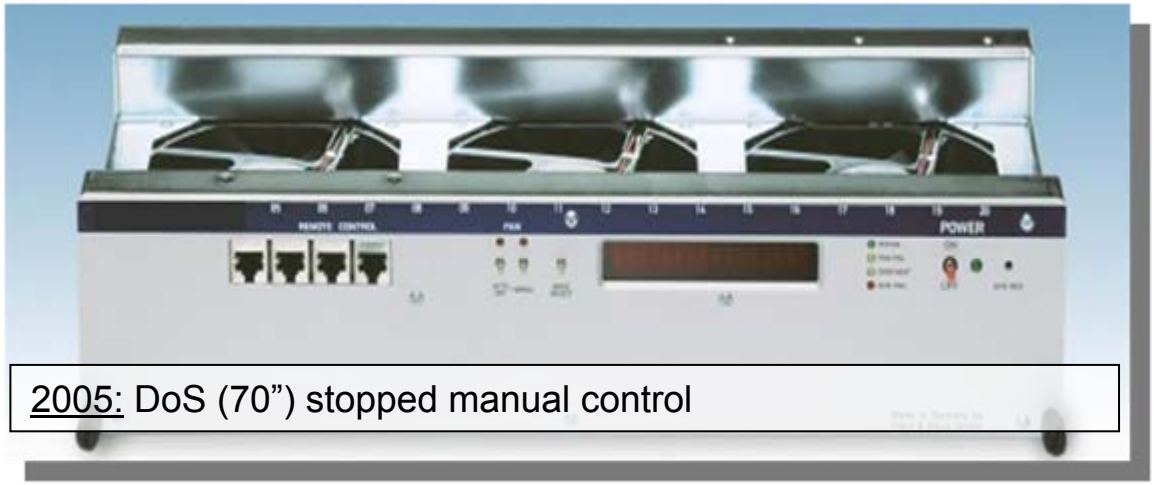
- **31 devices** from 7 different manufacturers **(53 tests in total)**
- **All devices fully configured** but running idle





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


TOCSSiC Findings (1)



2005: DoS (70") stopped manual control

The device crashed

while receiving special non-conform packets

- Consumption of all CPU resources ("jolt2" DoS attack)
- Failure to properly handle overlapping IP fragments ("Nestea" attack)
- Loss of network connectivity (Linux "zero length fragment" bug)
- Unable to deal with special malformed packets ("oshare" attack)

…violation of TCP/IP standards !!!


TOCSSiC Findings (2)

FTP server allows anonymous login

FTP & Telnet servers crashed

- Receiving very looooooooooong commands or arguments

…legacy protocols introducing security risks !

HTTP server crashed

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

HTTP server allows for directory traversal

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

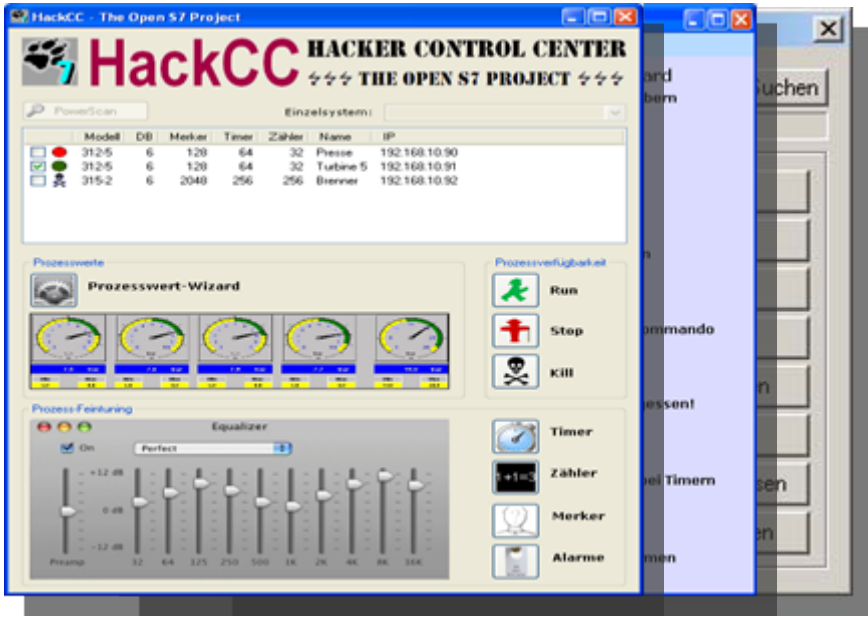
ModBus server crashed while scanning port 502

…protocols are well documented ("Google hacking") !

TOCSSiC Findings (3)

PLCs are unprotected

- Can be **stopped w/o problems** (needs just a bit of Google)
- Passwords are not encrypted
- PLC might even come without authorization schemes



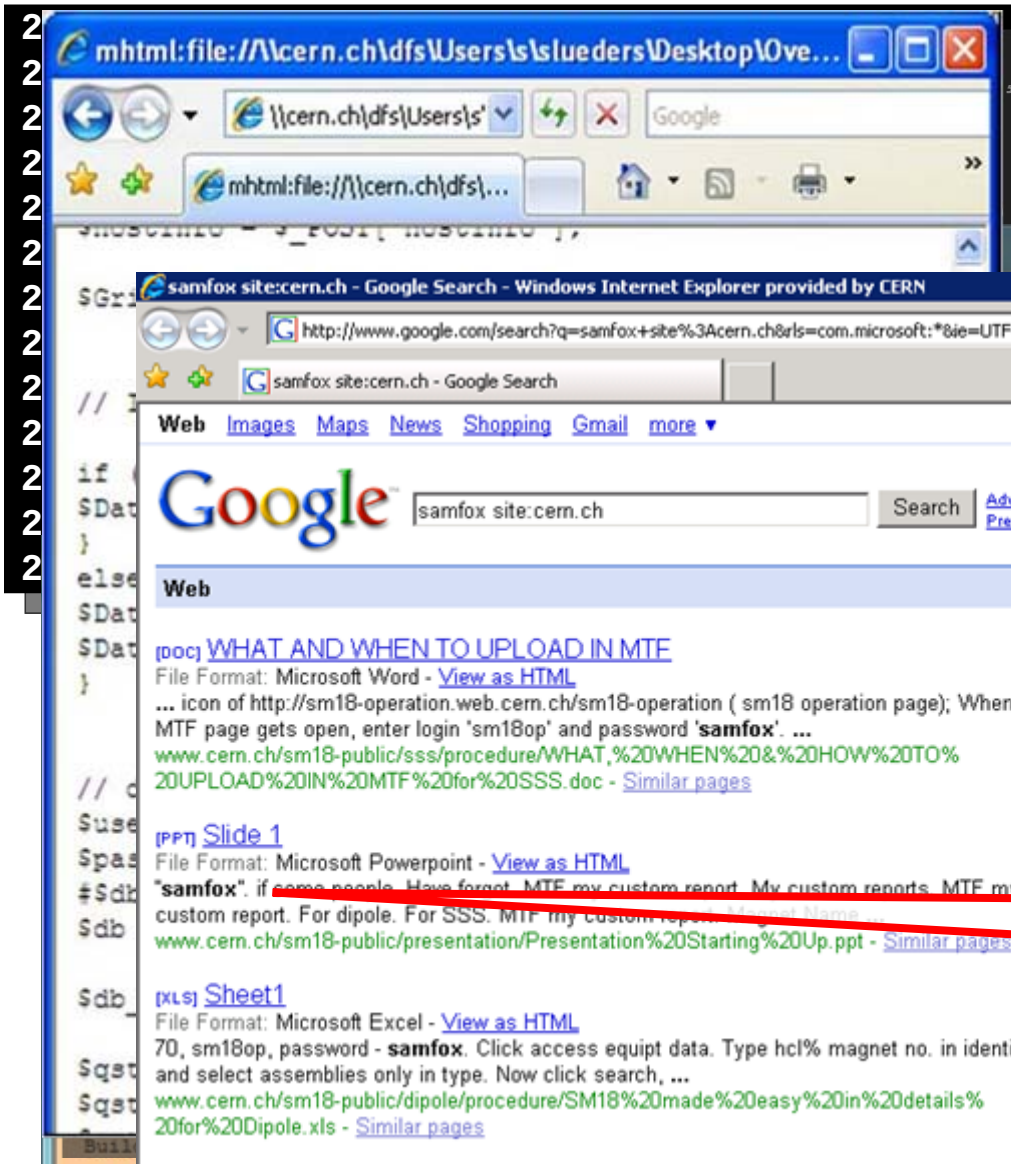
…robustness/resilience (security?) must become part of life-cycle !

PLCs are *really* unprotected

- Services (HTTP, SMTP, FTP, Telnet,…) can not be disabled
- Usually no local firewall or ACLs

…lock down of configuration by default !

Vulnerabilities are everywhere !!!



Unpatched oscilloscop
(running Win XP SP2)

Lack of input
validation & sanitizatio

Confidential data on
Wiki, webpages, CVS.

Free passwords
on Google…


Why worry ?





Risk =

Vulnerability

× Threat

× Consequence


Who is the threat ?

Attacks performed by…

- Trojans, viruses, worms, …
- Disgruntled (ex-)employees or saboteurs
- Attackers and terrorists
  (step-by-step instructions on BlackHat conferences;
  freeware hacking tools for "Script Kiddies")

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


CERN Under Permanent Attack

CERN is under permanent attack… even now !!!

- CERN servers visible to the Internet are permanently probed
- Incidents happen frequently
- On the office network, there are always devices being infected or compromized
- Many systems are still/again vulnerable, new vulnerabilities are discovered frequently, and there are lots or areas to improve


Damage by Viruses / Worms ?

2003: The "Sla
safety monitor
Besse nuclear

2003/08/11: W32.Blaster.Worm

Home > Topics > Security > News > **Zotob, PnP Worms Slam 13 DaimlerChrysler Plants**

Security

eWEEK.COM

Zotob, PnP Worms Slam 13 DaimlerChrysler Plants

By Paul F. Roberts

August 18, 2005

TALKBACK
Comment on this article
4 comments posted
Add your opinion

A round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. auto manufacturing plants offline for almost an hour this week, stranding some 50,000 auto workers as infected Microsoft Windows systems were patched, a company spokesperson told eWEEK.

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 50 minutes, according to spokesperson Dave Elshoff.

Damage by Lack of Robustness ?

"Your software license
(Not at CERN ☺)

"Data storm" blamed for nuclear-plant shutdown

Robert Lemos, SecurityFocus 2007-05-18

The U.S. House of Representative's Committee on Homeland Security called this week for the Nuclear Regulatory Commission (NRC) to further investigate the cause of excessive network traffic that shut down an Alabama nuclear 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).

If you want to stop a hacker...

" If you were to test any control systems that have any more than three or four (different) network-connected devices,

Damage by Insiders ?

Duo deny LA traffic hack charges

The Register®

The Hollywood Job

By John Leyden – More by this author

Published Wednesday 10th January 2007 17:46 GMT

A pair of Los Angeles traffic system engineers have been charged with manipulating traffic signals to disrupt transportation across the city in the run-up to a union protest last August.

The Argus

Rude awakening for dawn drivers

*By **Louise Acford***

Early morning motorists got a shock yesterday when digital car park signs were tampered with by computer hackers and were left displaying an obscene message.

The message appeared on all similar signs around Crawley at about 6.45am.

Thousands of motorists travelling into the town would have been subjected to the unsavoury advice.

The signs normally display the number of spaces available in the town's car parks and were installed about four years ago.

One of the car park signs

A spokeswoman for Crawley Borough Council said the authority had received no complaints from the public, just calls advising them what had happened.

2000: Ex-Employee hacked "wire
46x into a sewage plant and floo
basement of a Hyatt Regency hotel.

Damage by Attackers ?

Russia welcomes hack attacks

Script Kiddies cut teeth hijacking critical infrastructure

By Thomas C Greene in Washington →

Published Thursday 27th April 2000 12:25 GMT

Malicious hack attacks
spectacularly, Russian a
hackers last year. Gazp
succeeded in defeating
Colonel Konstantin Mac
The Colonel said the int

"....penetration test locked up the SCADA
not able to send gas through it"
- Sandia National Labs, US [2005]

CSO
cso online.com
The Resource for
infrastr
service, transpo
risk from very simple h

CNN.com
Next Article in U.S. »
VIDEO
WASHINGTON (CNN) -- Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned.

Department of Homeland Security video shows a generator spewing smoke after a staged experiment.

Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power.

Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix.

CNN has honored a request from the Department of Homeland Security not to divulge certain details about the experiment, dubbed "Aurora," and conducted in March at the Department of Energy's Idaho lab

In a previously classified video of the test CNN obtained, the generator shakes and smokes, and then stops.

Most Popu

We're HEP, so who will attack us ?!

...also at CERN ☹

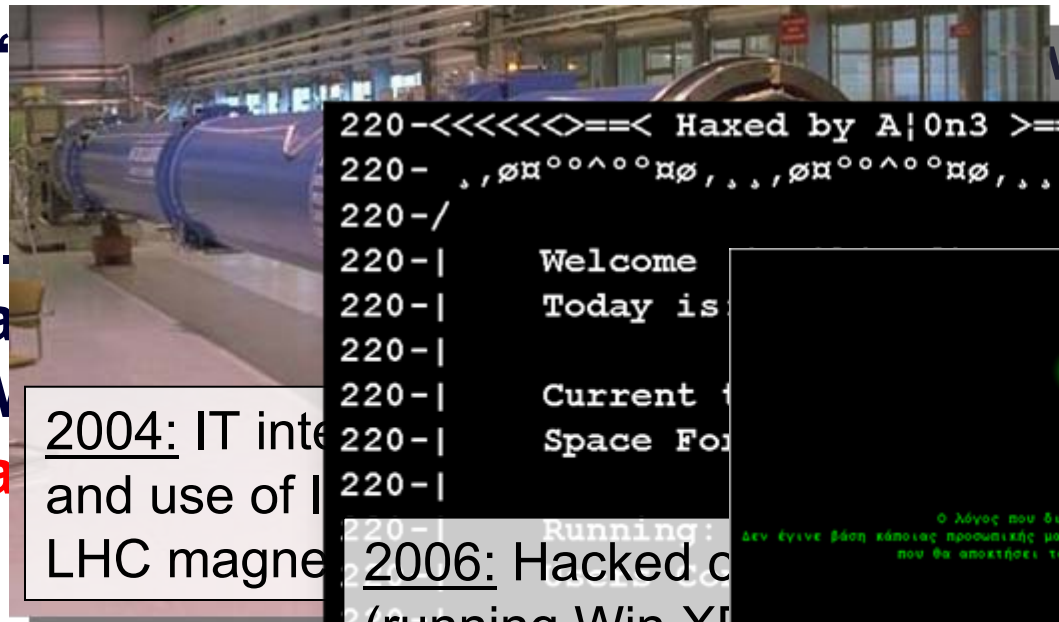
"...vere compromised...

...twork

a...

M...

a...



2004: IT inte... and use of I... LHC magne...

2006: Hacked c... (running Win XP...

...Analysis...

installation left the passv...

2008: Control system historian of LHC experiment defaced

Management Buy-In !!

LHC First Beam Day

Mozilla Firefox

http://[redacted].cern.ch[redacted]/apanthsh.html

Proxy: None Apply Edit Remove Add Status: Using None Preferences

• Post a new topic

http:[redacted]anthsh.html

GREEK SECURITY TEAM

10/09/08 03:00

Αυτήν την ώρα γίνετε η απόπειρα πειράματος στο CERN.

Ο λόγος που διαλέξαμε αυτή τη σελίδα είναι για να σας θυμίζουμε

Δεν έγινε βάση κάποιας προσωπικής μας αντιπαράθεσης με την ομάδα διαχείρισ

που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυα

Μερικά στοιχεία απ' τη βάση :

USERNAME	USER_ID	CREATED
SYS	0	2008-02-18 16:19:25.0
SYSTEM	5	2008-02-18 16:19:25.0
OUTLN	11	2008-02-18 16:19:28.0
DIP	19	2008-02-18 16:21:17.0
TSMSYS	21	2008-02-18 16:23:27.0
DBSNMP	24	2008-02-18 16:24:25.0
WMSYS	25	2008-02-18 16:24:53.0
EXFSYS	34	2008-02-18 16:27:55.0
XDB	35	2008-02-18 16:28:04.0
PDB_ADMIN	46	2008-02-18 17:26:32.0
GLEGE	49	2008-02-19 10:13:07.0
PDBMON	45	2008-02-18 17:25:24.0
BALYS	44	2008-02-18 17:25:24.0
USERMON	48	2008-02-18 17:59:26.0

..etc...etc....

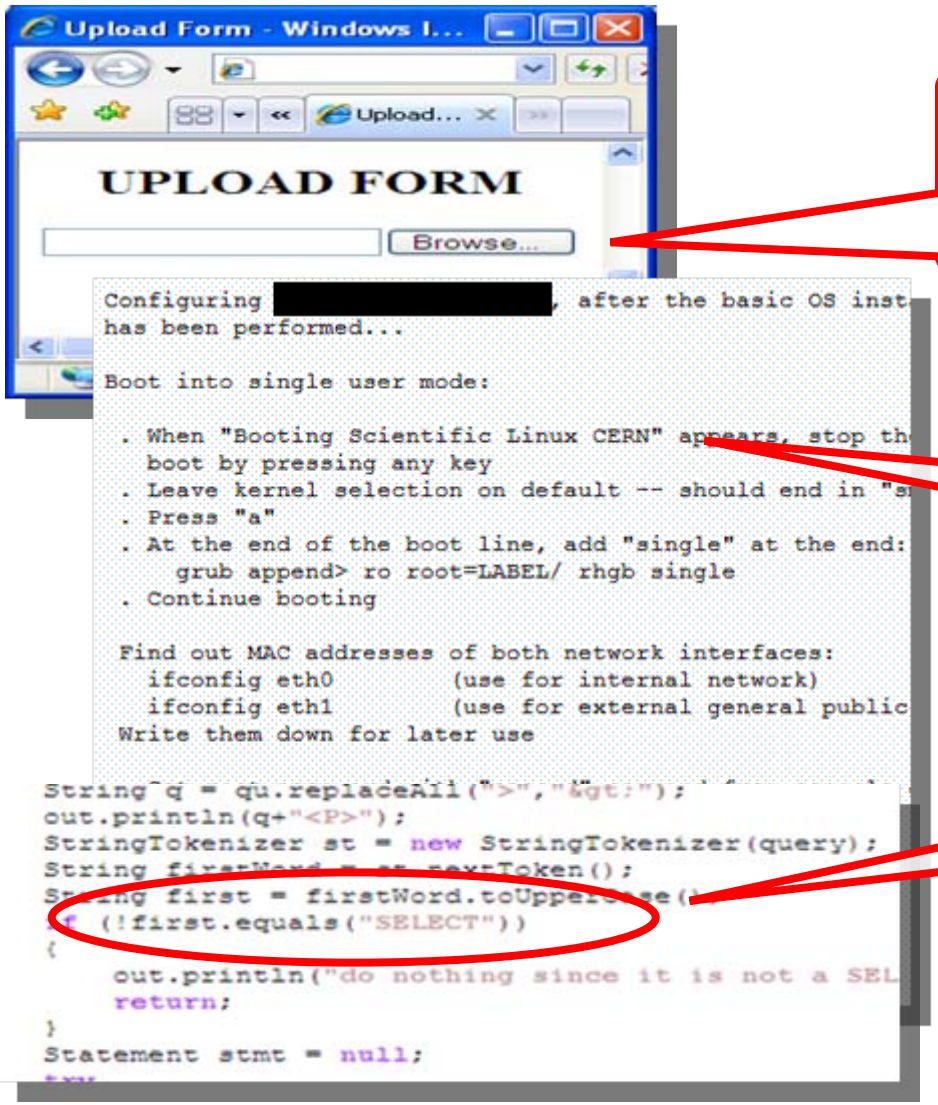
Hmm…
A defaced web-page
at an LHC experiment…

…on 10/09/2008:
Just coincidence ?

A "flame" message
to some Greek
"competitors"…

…user accounts !?!

Violation of *Basic* Principles !



Neglected "Rule of Least Privileges":

Everyone could upload whatever he/she wants…

Configuration well documented in Google..

Lack of input validation & sanitization

http://cern.ch/security/webapps

http://cern.ch/security/Recommendations/sysadmin-checklist.html

Who owns the consequences ?

ZDNet Government

Richard Koman

Get ZDNet Government via: Mobile RSS Email Alerts Bios:

Pick a blog category view

September 12th, 2008

Hackers deface LHC site, came close to turning off particle detector

Telegraph.co.uk

BEST CONSUMER ONLINE PUBLISHER aop uk

Home News Sport Business Travel Jobs Motoring Telegraph TV

Earth home
Earth news
Earth watch
Comment

Hackers infiltrate Large Hadron Collider systems and mock IT security

News Site of the Year | The 2008 Newspaper Awards

TIMESONLINE

NEWS COMMENT BUSINESS MONEY SPORT LIFE & STYLE TRAVEL DRIVING

UK NEWS WORLD NEWS POLITICS ENVIRONMENT WEATHER TECH & WEB TIMES ONLINE

Where am I? Home News UK News Science News

From The Times

September 13, 2008

Hackers break into CERN computer show up its 'schoolkid' security

Can you allow for loss of

- functionality
- control or safety
- efficiency & beam time
- hardware or data
- reputation…?

Are you prepared to take *full* responsibility?

Are you in the position to *really* take it ?

How long does it take you to reinstall your system, if requested *right now* ?


Defence-in-Depth




Devices & Hardware

Firmware & Operating Systems
(Network-) Protocols

Software & Applications
Third party applications

Operator & User
System Integrator & Manufacturer


Myths about Cyber-Security

"Network security, that's all you need !"

"Firewall protection is sufficient..."

"Encryption protects you..."

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

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

"You can keep attackers out..."

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

"Everything can be solved by technique !"


Wanted: Defense-in-Depth

Security is as high as the weakest link:

- ►Attacker chooses the time, place, method
- ►Defender needs to protect against all possible attacks (currently known, and those yet to be discovered)

Security is a system property (not a feature)

Security is a permanent process (not a product)

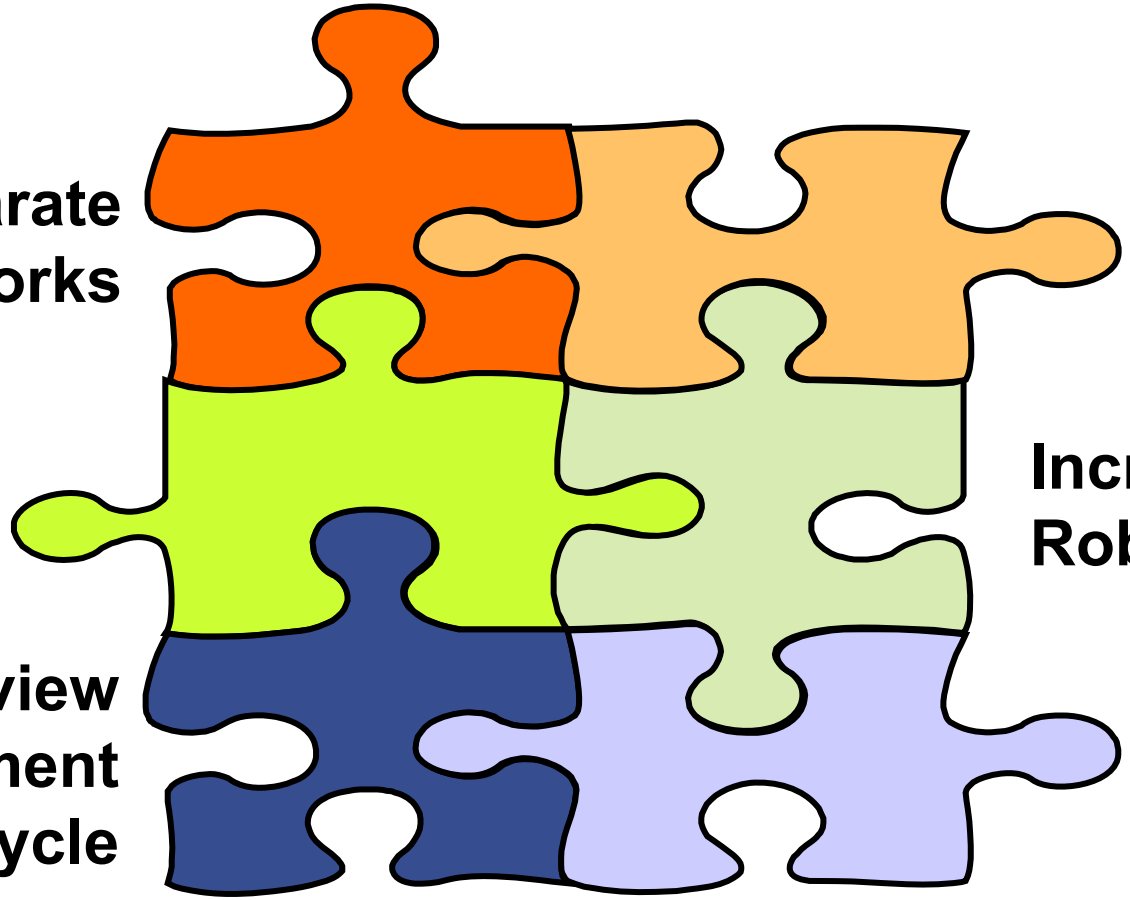
Security cannot be proven (phase-space-problem)

Security is difficult to achieve, and only to 100%-ε

- ►YOU define ε as user, developer, system expert, admin, project manager

BTW: Security is *not* a synonym for safety


Ground Rules for Cyber-Security

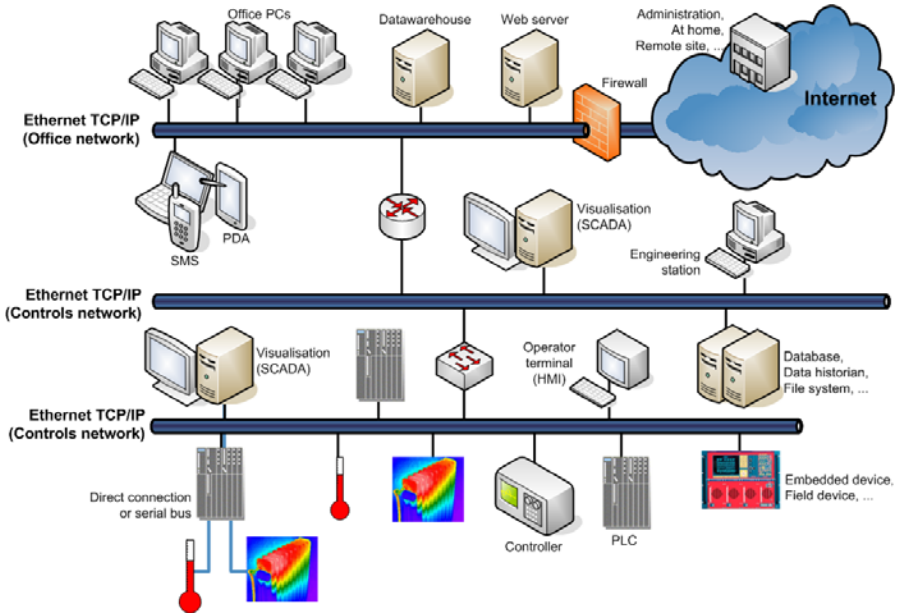


- *Valid for CERN Control Systems (ongoing), but also standard IT systems.*
- *What about your systems ?*

Separate Networks

Deploy different networks for different purposes:

- …for operations
  with sub-nets for different functions
- …for development and basic testing
- …for beam-lines & experiments
- Campus network for office computing



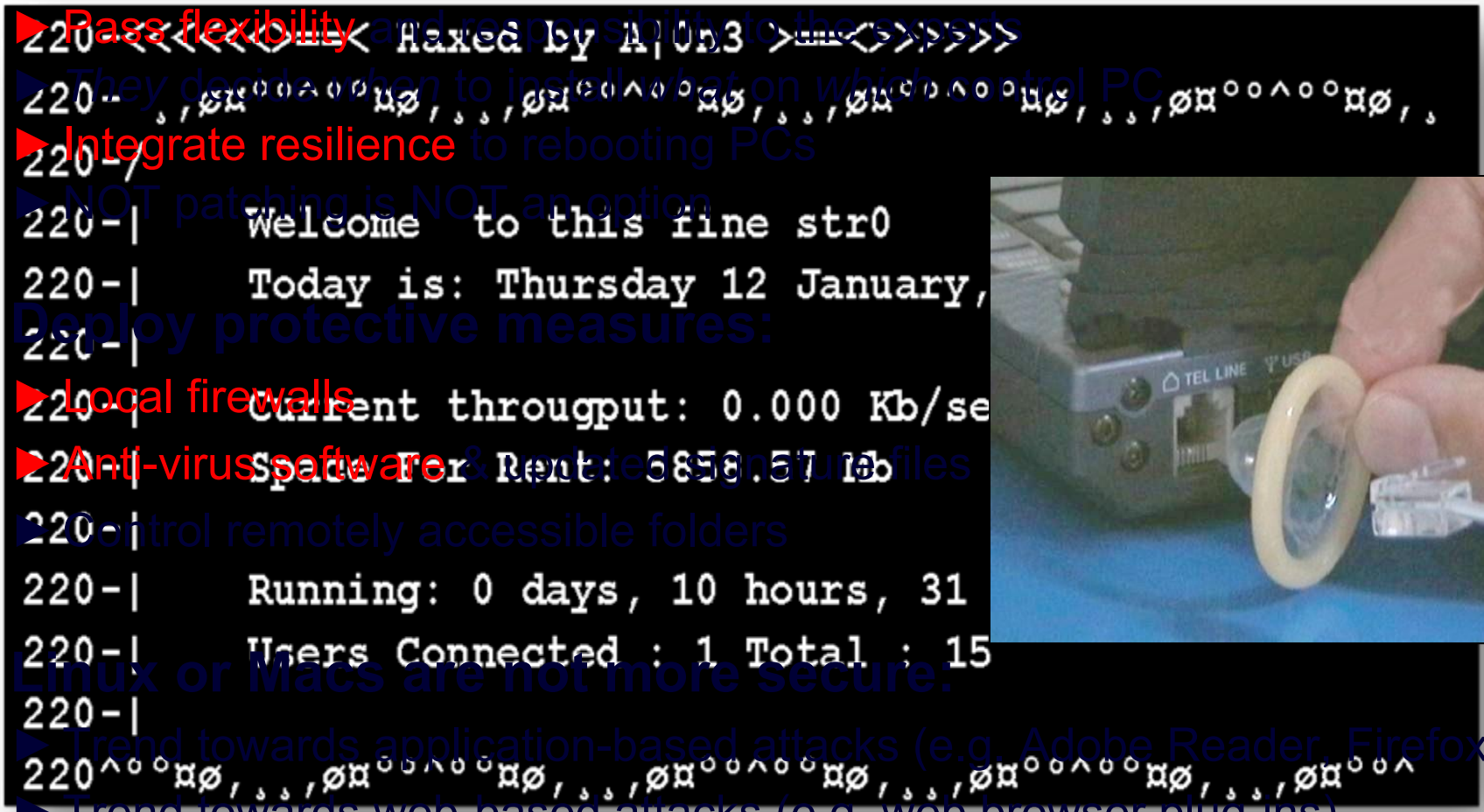
Restrict their usage:

- Assign responsibilities and deploy authorization procedures
- Drop Internet connectivity, (GPRS) modems, wireless access points
- Control inter-communication between networks
- Block laptops, email & control web pages
- Control remote access
- Deploy traffic monitoring & Intrusion Detection Systems


Patch, Patch, Patch !!!

Ensure prompt security updates:

- Pass flexibility
- Integrate resilience



Deploy protective measures:

- Local firewalls
- Anti-virus software

Linux or Macs are not more secure:

- Trend towards application-based attacks (e.g. Adobe Reader, Firefox)
- Trend towards web-based attacks (e.g. web browser plug-ins)


Control (Remote) Access

Follow "Rule of Least Privilege":

- Restrict all access to minimum
- Ensure traceability (who, when, and from where)
- Keep passwords secret

…for all assets:

- Control PCs & operating systems
- SCADA applications & user interfaces
- Procedures, documentation, etc.

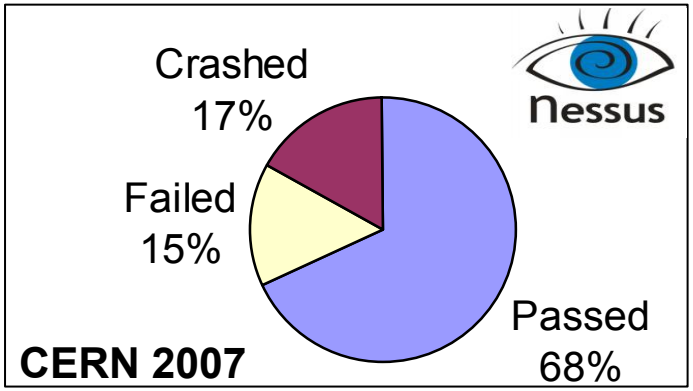
"Role Based Access Control" for op's:

- Avoid "shared" accounts
- Multi-factor authentication for critical assets
- Full control for the shift leader of operations

Increase Robustness

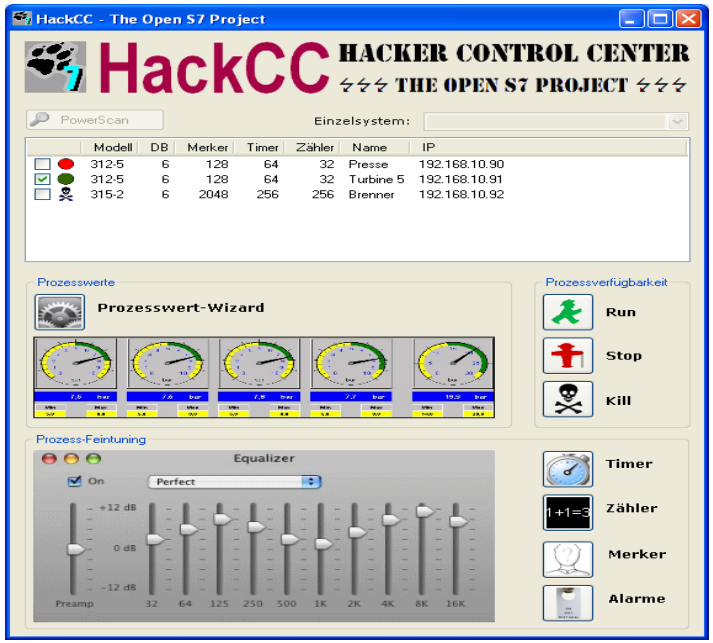
PLCs and other controls devices are completely unprotected:

- No firewall, no anti-virus, nothing



Assess your systems:

- Run vulnerability tools on everything (e.g . PLCs, control PCs, SCADA, data bases. web servers)
- Review configurations settings and remove unnecessary services (e.g. emailing, web servers, Telnet, FTP)
- Deploy additional protective measures if needed (VPN, ACL, …)
- Make your installations resilient & robust




Review Development Life-Cycle

Review procedures for

- ...development of hardware & applications
- ...system testing
- ...deployment
- ...operations
- ...maintenance & bug fixing
- Use software versioning systems configuration management and integration frameworks (CVS, SVN, Git)

A Boeing 777 uses similar technologies to Process Control Systems

Protect operations

- Keep development separated from operations (eventually debugging might need access to full accelerator hardware)
- Avoid online changes for the sake of safe operations. Online changes must be authorized by the shift leader for operations

WWW.FOTN.IN

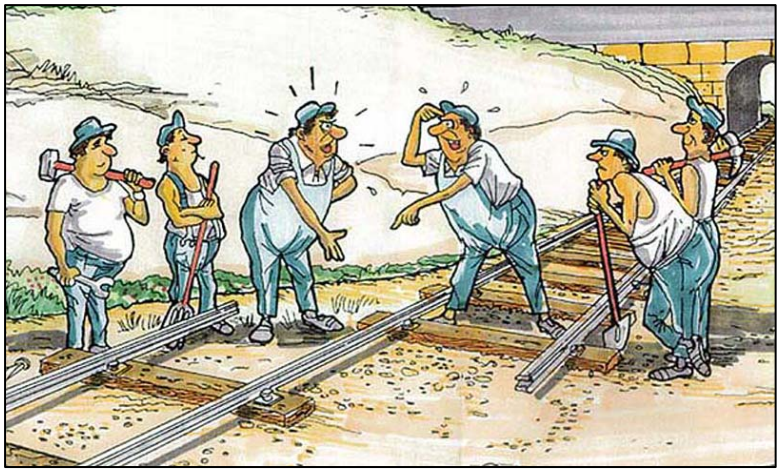

Deepen Collaboration & Policies

Make security an objective

- Get management buy-in (security has a cost – successful attacks, too)
- Produce "Security Policy for Controls"
- Follow the basic standards of Industry

Bring together control & IT experts:

- Control system experts know their systems by heart – but IT concepts ?
- IT people often don't know controls – but IT security they do
- Win mutual trust & get their buy-in
- Gain synergy effects



Train users and raise awareness


Team up: The *International* Risk

Risk =

Vulnerability

× Threat

× Consequence


Control Systems for Living

…in the electricity sector
- ► transmission & distribution, fossil, hydro, nuclear

…in the oil & gas sector

…in the water & waste sector

…in the chemical and pharmaceutical industry

…in the transport sector

…for production:
- ► e.g. cars, planes, clothes

…in supermarkets
- ► e.g. scales, fridges

…for facility management
- ► electricity, water, C&V

COBB County Electric, Georgia

Middle European Raw Oil, Czech Republic

Athens Water Supply & Sewage

Merck Sharp & Dohme, Ireland

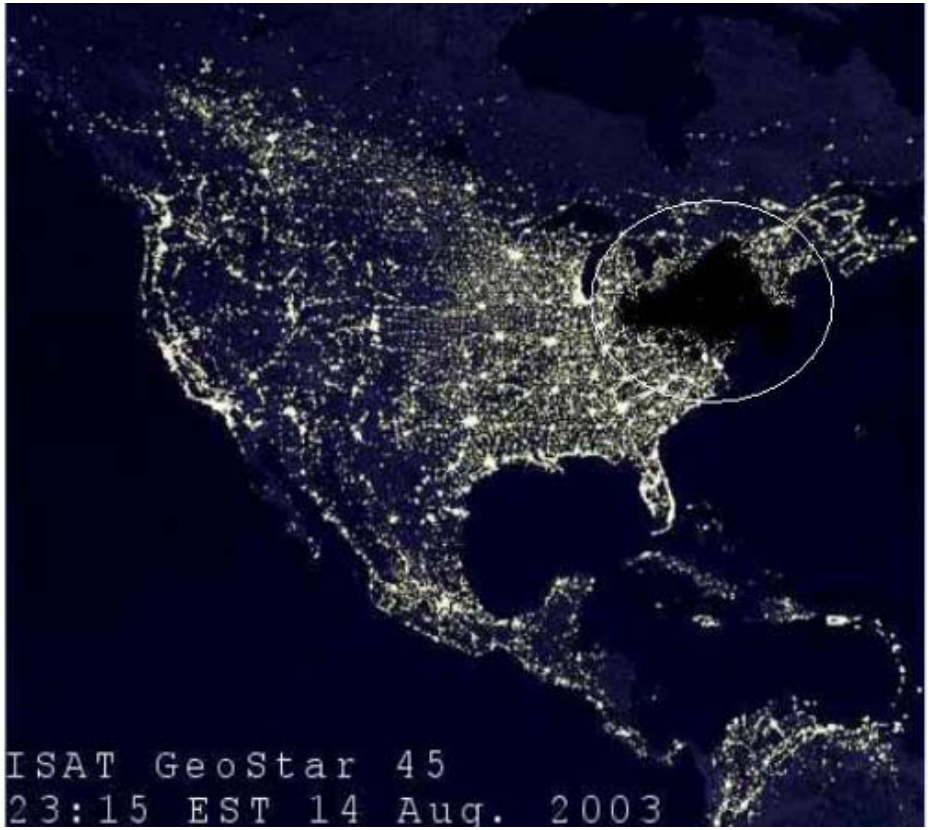
CCTV Control Room, UK

Reuters TV Master Control Room

Critical Infrastructure

Increased focus since 9/11 and due to today's general security situation:

- Electricity
- Oil & Gas
- Water & Waste
- Chemical & Pharmaceutical
- Transport



Critical Infrastructure Protection (CIP)


(Too) Many Standards... ?

"Good Practice Guidelines Parts 1-7"
U.K. Centre for the Protection of National Infrastructure (CPNI)
http://www.cpni.gov.uk/Products/guidelines.aspx

"Manufacturing and Control Systems Security"
ANSI/ISA SP99 TR99.00.01-04
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

"Guide to SCADA and Industrial Control Systems Security"
NIST SP800-82
http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

"Critical Infrastructure Protection CIP-002 to CIP-009"
U.S. Federal Energy Regulatory Commission (FERC)
http://www.nerc.com/page.php?cid=2%7C20

"Information Technology — Security Techniques"

"Systems and Software Engineering — Software Life Cycle Processes"
ISO/IEC 27001:2005 and ISO/IEC 12207:2009

+ Common Criteria, AGA, CIDX, ISPE, OLF #104, bdew whitepaper…


“Procurement Language”

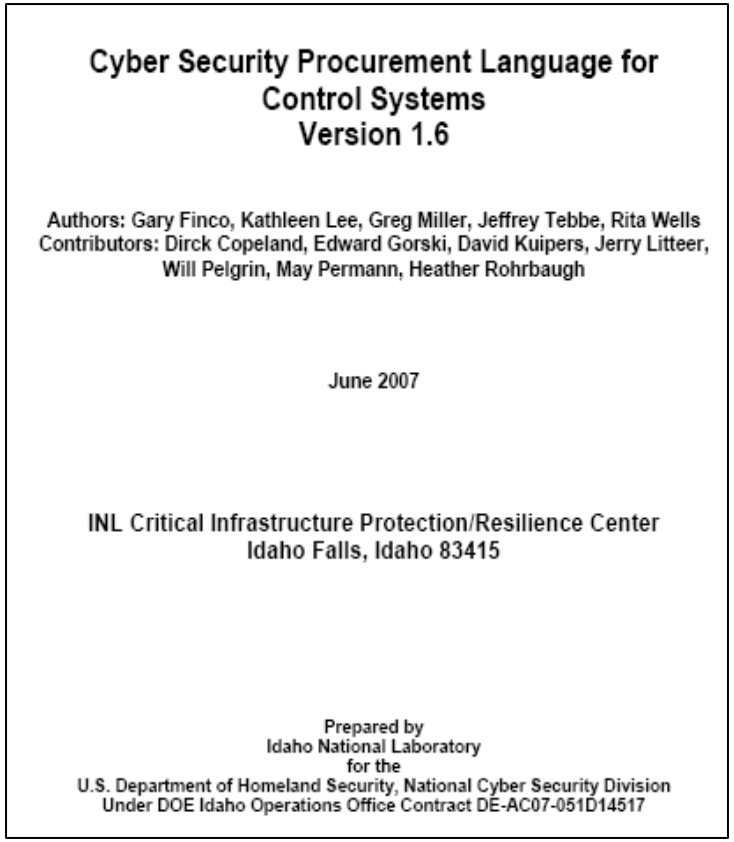
Manufacturers and vendors are part of the solution !

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

Idaho National Laboratory

“Procurement Language” document

- *“… collective buying power to help ensure that security is integrated into SCADA systems.”*
- **“Copy & Paste” paragraphs** for System Hardening, Perimeter Protection, Account Management, Coding Practices, Flaw Remediation, …



Cyber Security Procurement Language for Control Systems
Version 1.6

Authors: Gary Finco, Kathleen Lee, Greg Miller, Jeffrey Tebbe, Rita Wells
Contributors: Dirck Copeland, Edward Gorski, David Kuipers, Jerry Litteer, Will Pelgrin, May Permann, Heather Rohrbaugh

June 2007

INL Critical Infrastructure Protection/Resilience Center
Idaho Falls, Idaho 83415

Prepared by
Idaho National Laboratory
for the
U.S. Department of Homeland Security, National Cyber Security Division
Under DOE Idaho Operations Office Contract DE-AC07-051D14517

http://www.msisac.org/scada


Team Up !

"European Information Exchange on SCADA and Control System Security"

EuroSCSIE

- *"…is for those 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..."*
- 19 members from 13 European countries (50% authorities, 50% users)

Government Initiatives:

samen tegen cybercrime NICC

Bundesamt für Sicherheit in der Informationstechnik

MSB Myndigheten för samhällsskydd och beredskap

Informatikstrategieorgan Bund ISB
Unité de stratégie informatique de la Confédération USIC
Organo strategia informatica della Confederazione OSIC
Organ da strategia informatica da la Confederaziun OSIC

CPNI Centre for the Protection of National Infrastructure

U.S. Department of Homeland Security

Global Players:

ISA–The Instrumentation, Systems, and Automation Society

SANS INSTITUTE

wurldtech security technologies

byres security inc intrinsically secure

BCIT British Columbia Institute of Technology

Digital Bond:

Conferences: European SCADA Summit (10/2009, Stockholm)

SCADA Security Scientific Symposium (1/2010, Miami)

CERN


Summary

The (r)evolution of control systems...

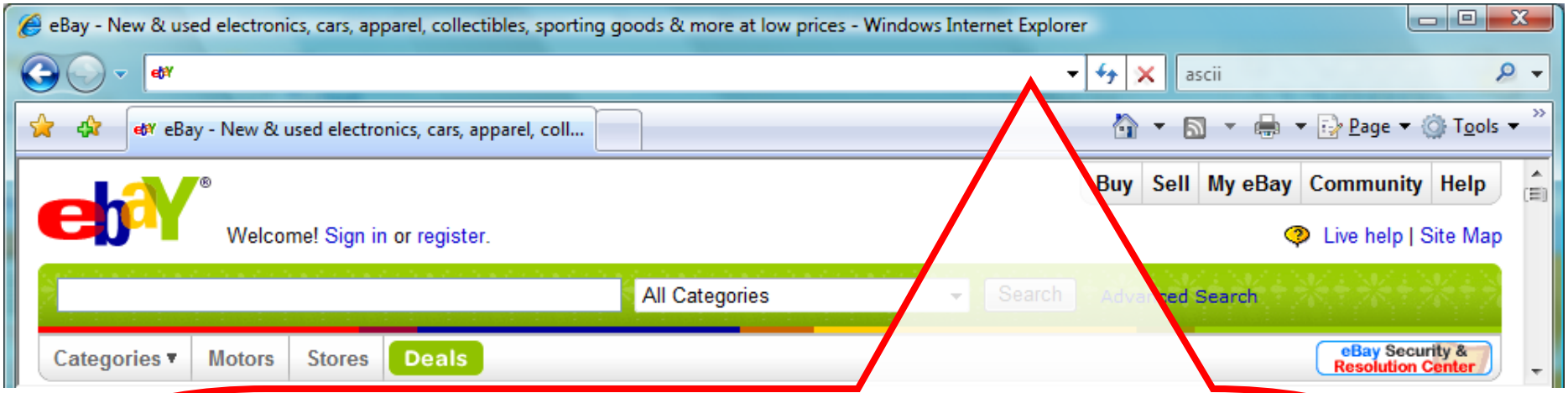
...omitted security aspects!

Why worry ? The risk equation

Mitigation: Defense-in-Depth

Team Up: Risks & Mitigations are int'l !

Thank you !!!



Quiz: Which link leads you to www.ebay.com ?

- http://www.ebay.com\cgi-bin\login?ds=1%204324@%31%33%37%2e%31%33%38%2e%31%33%37%2e%31%37%37/p?uh3f223d
- http://www.ebay.com/ws/eBayISAPI.dll?SignIn
- http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&rafld=0
  &encRafId=default
- http://secure-ebay.com