Control Systems Under Attack !?

…about the Cyber-Security of modern Control Systems

Dr. Stefan Lüders (CERN IT/CO)

EPICS Collaboration Meeting — April 25th 2007

Overview

The Past:
The (R)Evolution of
Control Systems

The Present:
What about Security !?

The Futur (!):
"Defence-In-Depth"
as Mitigation

Controls Goes IT

Controls networks mate 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

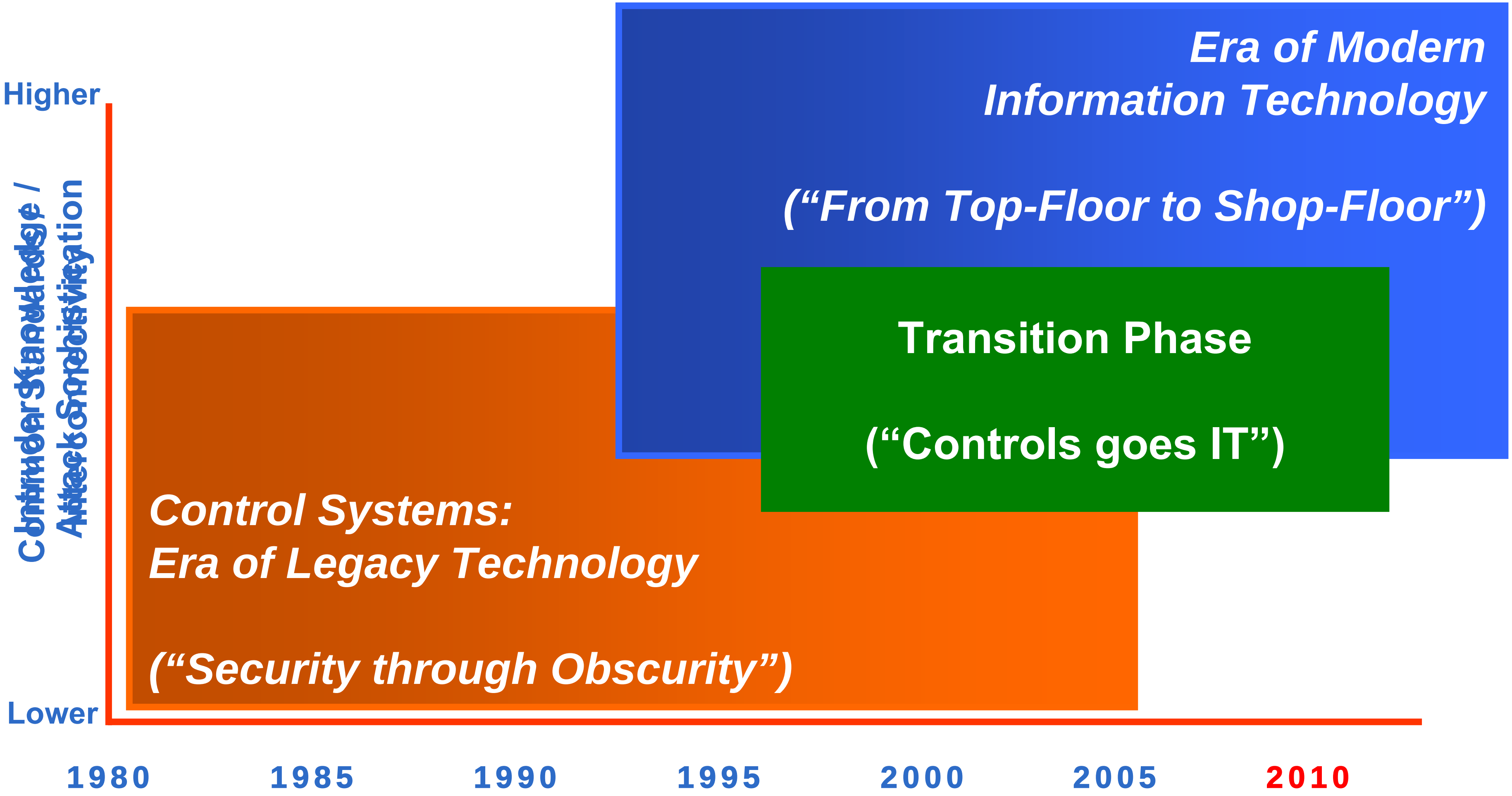
Use of IT protocols & gadgets

- eMails, FTP, Telnet, HTTP (WWW), … directly on the PLC
- Wireless LAN, notebooks, USB sticks, webcams, …

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, …

Cyber Threats — Today’s Peril


Higher
Lower
Intruder Knowledge / Attack Sophistication
Common Standards / Interconnectivity
1980
1985
1990
1995
2000
2005
2010

Era of Modern Information Technology

(“From Top-Floor to Shop-Floor”)

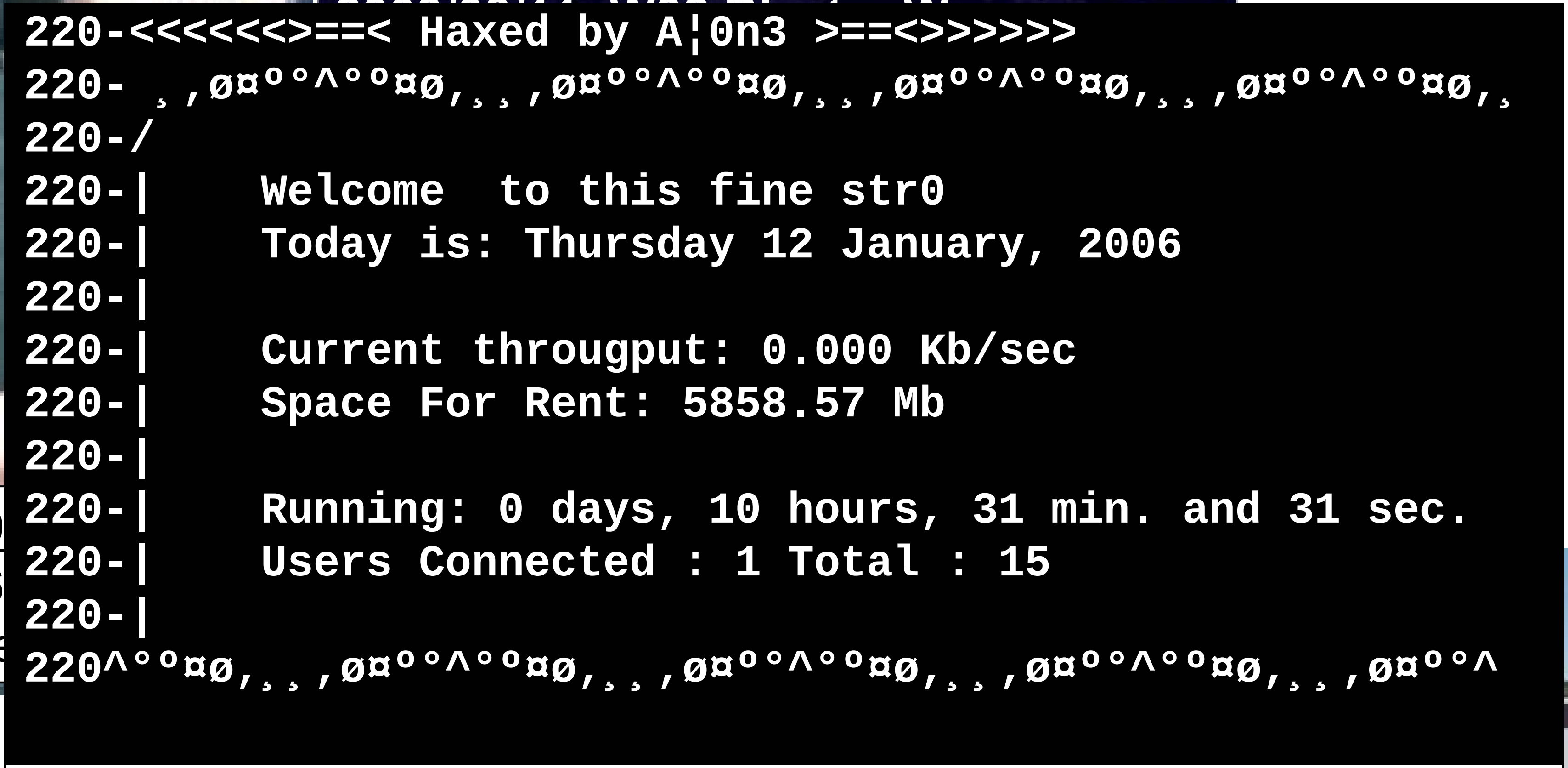
Transition Phase

(“Controls goes IT”)

Control Systems: Era of Legacy Technology

(“Security through Obscurity”)

Aware or Paranoid ?



```
220-<<<<<<>==< Haxed by A¦0n3 >==<>>>>>>
220- ¸,ø¤º°^°º¤ø,¸¸,ø¤º°^°º¤ø,¸¸,ø¤º°^°º¤ø,¸¸,ø¤º°^°º¤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^°º¤ø,¸¸,ø¤º°^°º¤ø,¸¸,ø¤º°^°º¤ø,¸¸,ø¤º°^°º¤ø,¸¸,ø¤º°^
```

2006: Hacked oscilloscope at CERN (running Win XP SP2)

20

46

the

ol

The Past:
The (R)Evolution of Control Systems

The Present:
What about Security !?

It’s up to YOU !!!

Risk = Vulnerability

× Threat

× Consequence

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 procures

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 ***Operator accounts ?***

…what about ***password rules ?***

Technical Vulnerabilities (40%)

Poorly secured systems are being targeted

- Unpatched systems, OS & 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** ?*

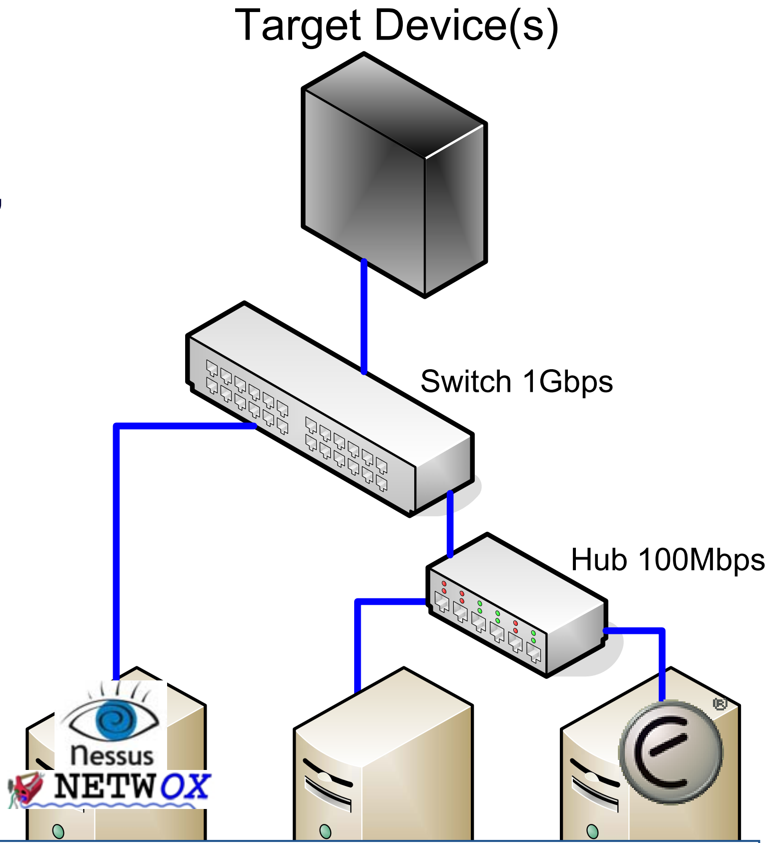
The “TOCSSiC” Teststand

COTS automation systems are without security protections

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

Creation of the Teststand On Controls System Security at CERN (TOCSSiC)

- Running “Nessus” vulnerability scan (used in Office-IT)

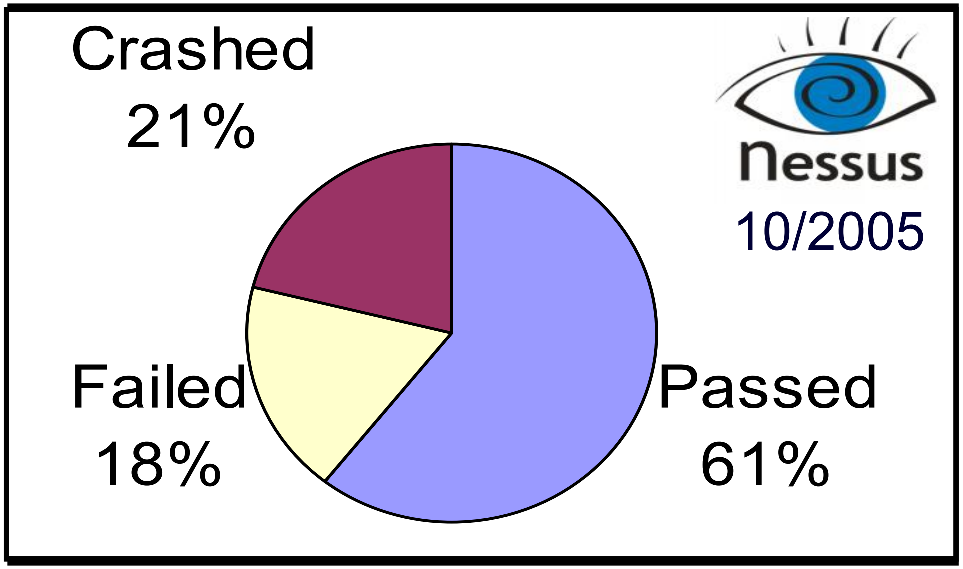


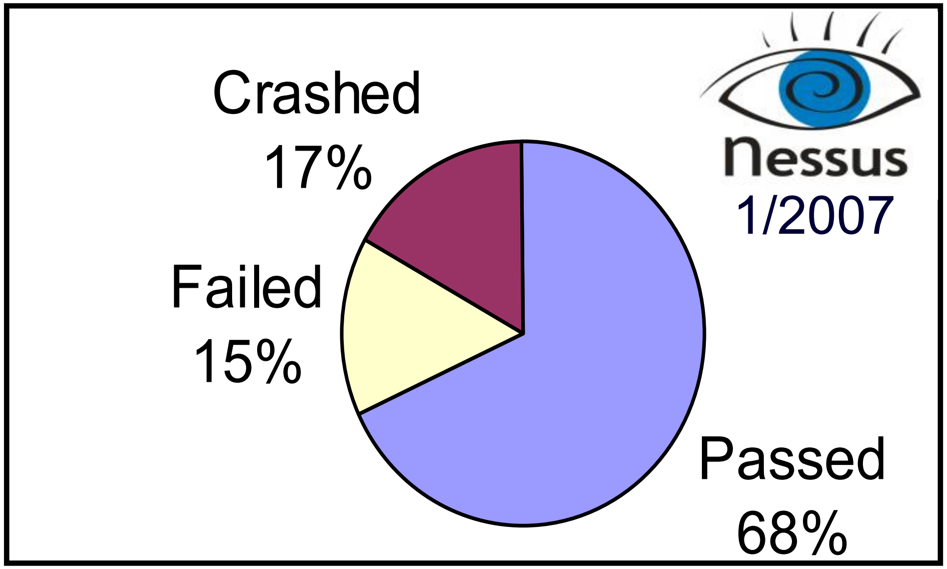
Going for the "low hanging fruits" !

Control Systems under Attack !

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

All devices fully configured <u>but running idle</u>

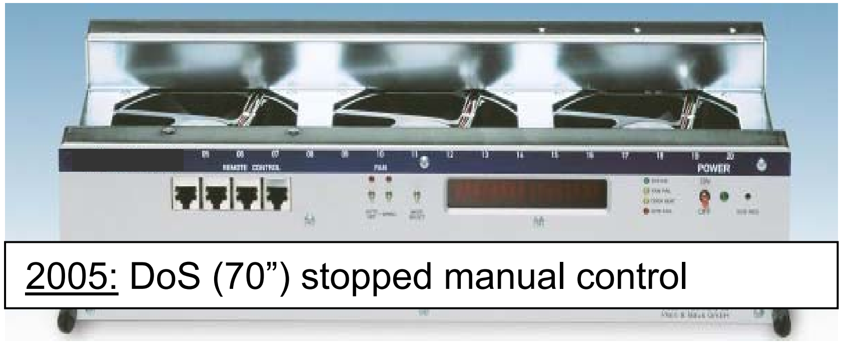




*…PLCs <u>under load</u> seem to **fail even more likely** !!!*

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

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 !!!

ModBus server crashed while scanning port 502

…protocols are well documented (“Google hacking”) !

TOCSSiC Findings (2)

FTP server allows anonymous login

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 tooooooooooooo many characters
- Using up all resources (“WWW infinite request” attack)

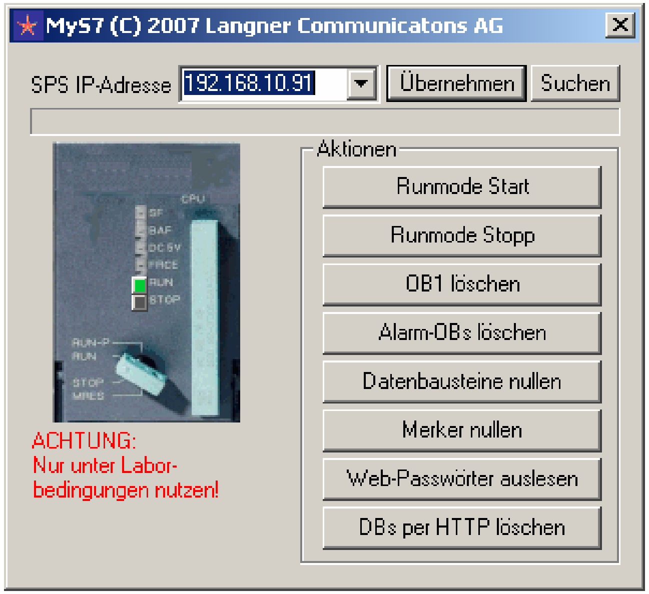
HTTP server allows for directory traversal

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

Fixed SNMP community names “public” & “private”

…community names must be changeable !

TOCSSiC Findings (3)



MyS7 (C) 2007 Langner Communicatons AG

SPS IP-Adresse 192.168.10.91

ACHTUNG:
Nur unter Labor-
bedingungen nutzen!

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

…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 !

Follow-Up of TOCSSiC

Discussions with corresponding manufacturers

- Acknowledgement only after a lot of persuasion
- Some now perform Nessus tests themselves

…results improve with more recent firmware versions ☺

Cooperation & Forwarding

CPNI Centre for the Protection of National Infrastructure

NISCC

- …together with governmental bodies
- …of the corresponding manufacturers to third parties

Nutzfahrzeuge

DESY

Presentations to Industry

PLCopen for efficiency in automation

- Discussions on
  "Requirements for the Cyber-Security of Control Systems"

ZVEI:

…but lots of ignorance ("There is no market demand !")

The Past: The (R)Evolution of Control Systems

The Present: What about Security !?

The Futur (!): "Defence-In-Depth" as Mitigation

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 hackers out..."

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

"Everything can be solved by technique !"

(Too?) Many Standards, …

- “Security for Manufacturing and Control Systems”
  “Integrating Electronic Security into Manufacturing…”
  (American National Standards Institute & Int'l Society for Measurement and Control)
  (ANSI/ISA SP99 TR1 & TR2)
- “Code of Practice for Information Security Management”
  (Int'l Organization for Standardization / Int'l Electrotechnical Commission / British Standard)
  (ISO/IEC 17799:2005, BS7799, ISO27000)
- Common Criteria (ISO/IEC 15408)
- “System Protection Profile for Industrial Control Systems”
  (U.S. National Institute of Standards and Technology NIST)
- “Cyber-Security Vulnerability Assessment Methodology Guidance”
  (U.S. Chemical Industry Data Exchange CIDX)
- “Good Automated Manufacturing Practices: Guideline for Automated System Security” (Int’l Society for Pharmaceutical Engineering ISPE)
- NERC standards (North American Electric Reliability Council)
- AGA standards (American Gas Association)

Defense-In-Depth

"Defence-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 should be included into orders and call for tenders

"Controls goes IT" — also for "Industrial Security" !!!

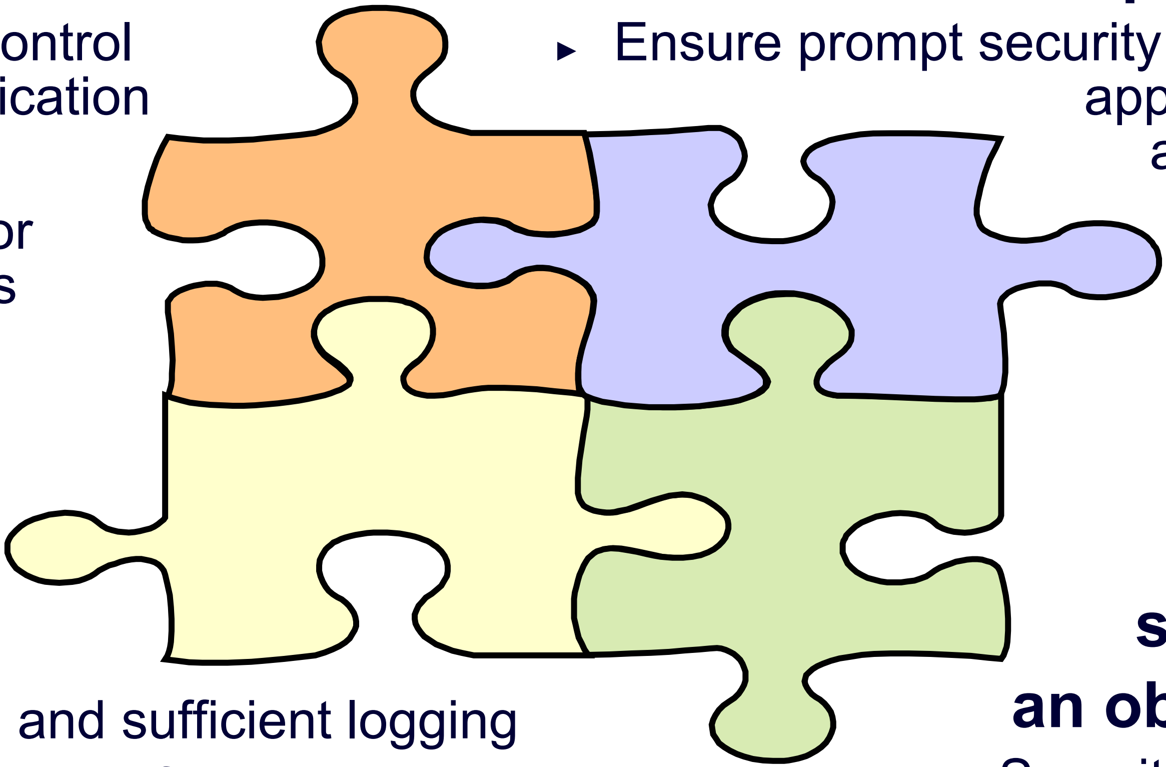
Ground Rules for Cyber-Security

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 people

Raising User Awareness

Dialog with user, organizations and governmental bodies

Nutzfahrzeuge Langner VATTENFALL

Bundesamt für Sicherheit in der Informationstechnik

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

NISCC

Awareness Campaigns

- …to inform Users of control systems about ‘Industrial Security’
- …at CERN and in the HEP community

IN2P3 Institut National de Physique Nucléaire et de Physique des Particules

Fermilab TRIUMF CCLRC DESY PAUL SCHERRER INSTITUT PSI

"Control System Cyber-Security in HEP" (CS²/HEP)

- Workshop during the ICALEPCS 2007
(October 2007 in Knoxville, Tennessee, USA)

07 ICALEPCS

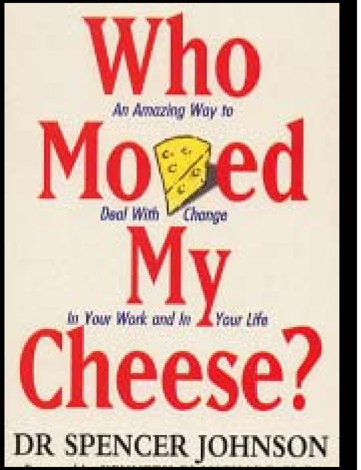
CERN

Summary

Controls Systems move towards IT-based solutions.

COTS Automation Systems are without security protections.

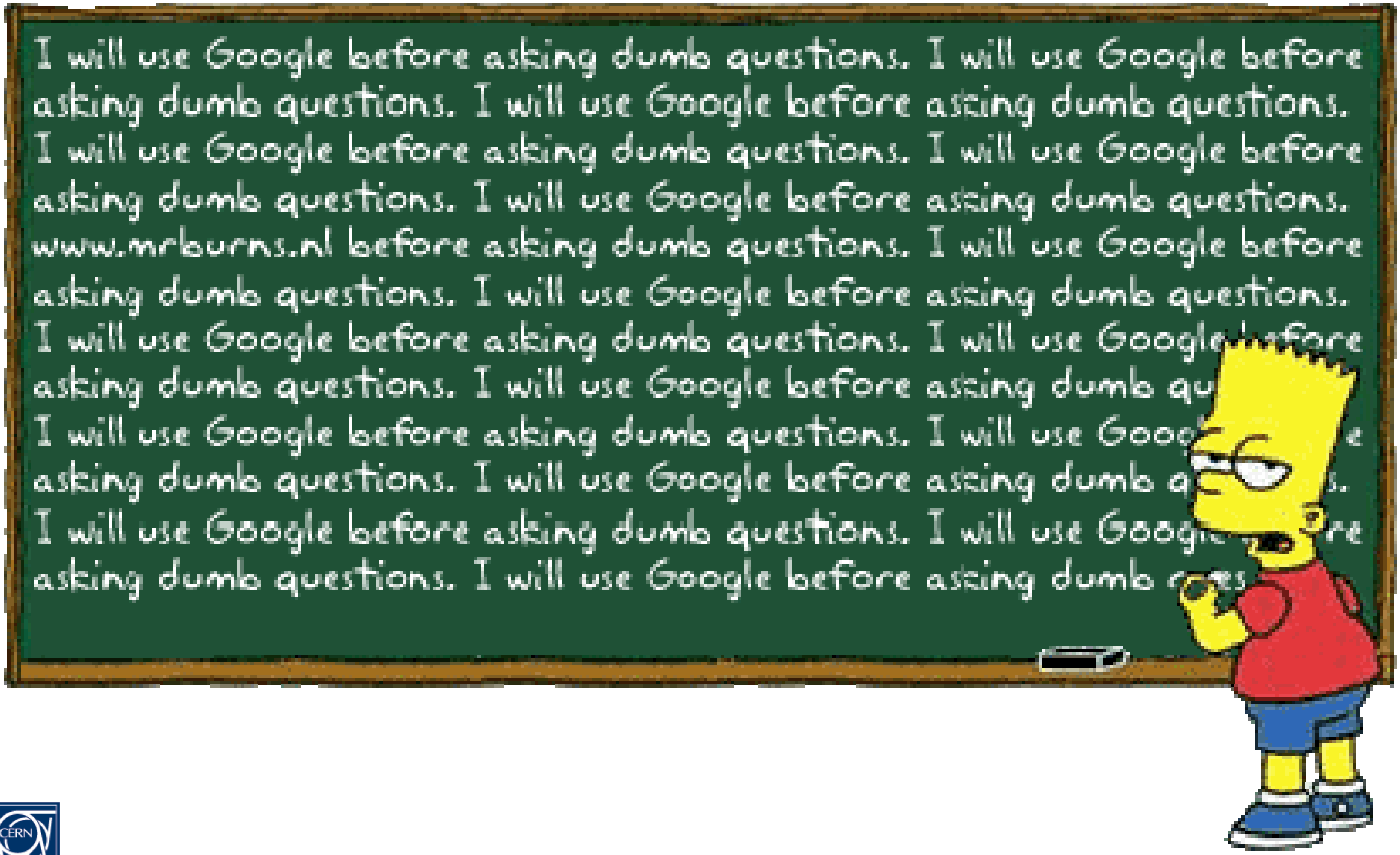
Do you want to act BEFORE or AFTER the incident ?



It's up to YOU !!!

A Defence-In-Depth approach offers 100%-ε mitigation.

Thanks a lot !


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