



Control Systems Under Attack !?

**...about the Cyber-Security
of modern Control Systems**

Dr. Stefan Lüders
FNAL Computer Security Seminar
September 10th 2009

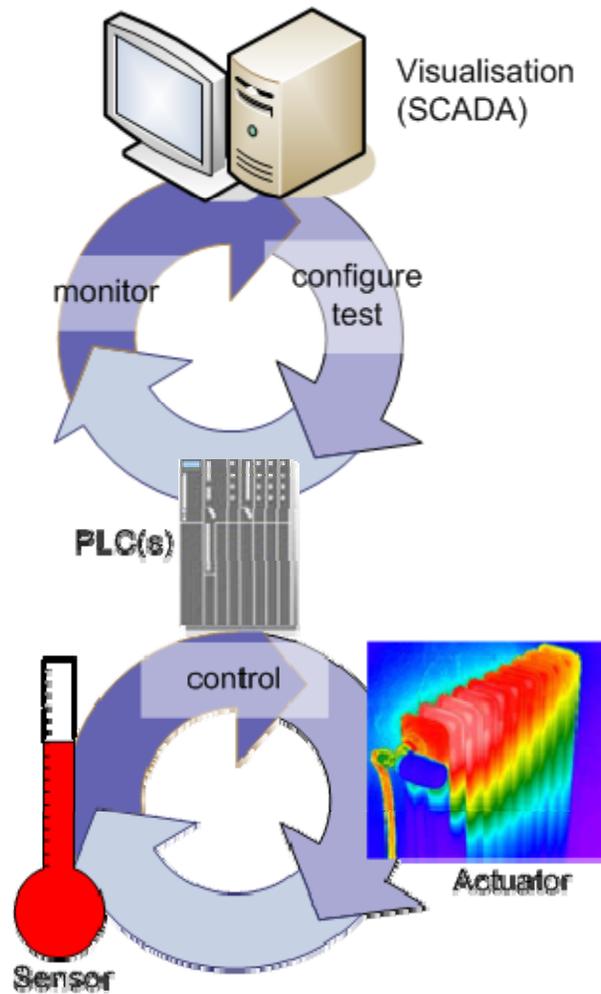




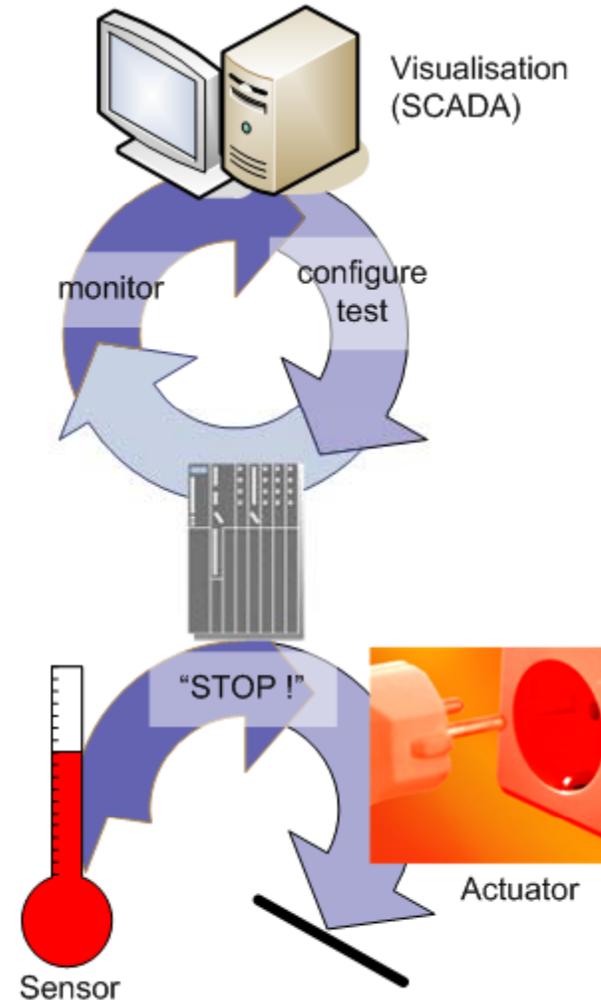
Control Systems for IT Experts

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

Control System



Safety System





Security for Controls Experts

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

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





Overview

"Control Systems Under Attack !?" — Dr. Stefan Lüders — September 10th 2009



The (r)evolution of control systems...



...omitted security aspects!



Why worry? The risk equation



Mitigation: Defense-in-Depth

Inheriting IT Standards

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009



**Ethernet & Wireless
Modbus/TCP, OPC & Telnet**

**Common of the shelf HW
Desktop PCs & Laptops**

Windows & Linux

WWW & Emails

C++, Java, XML, Corba...

Oracle, Labview...

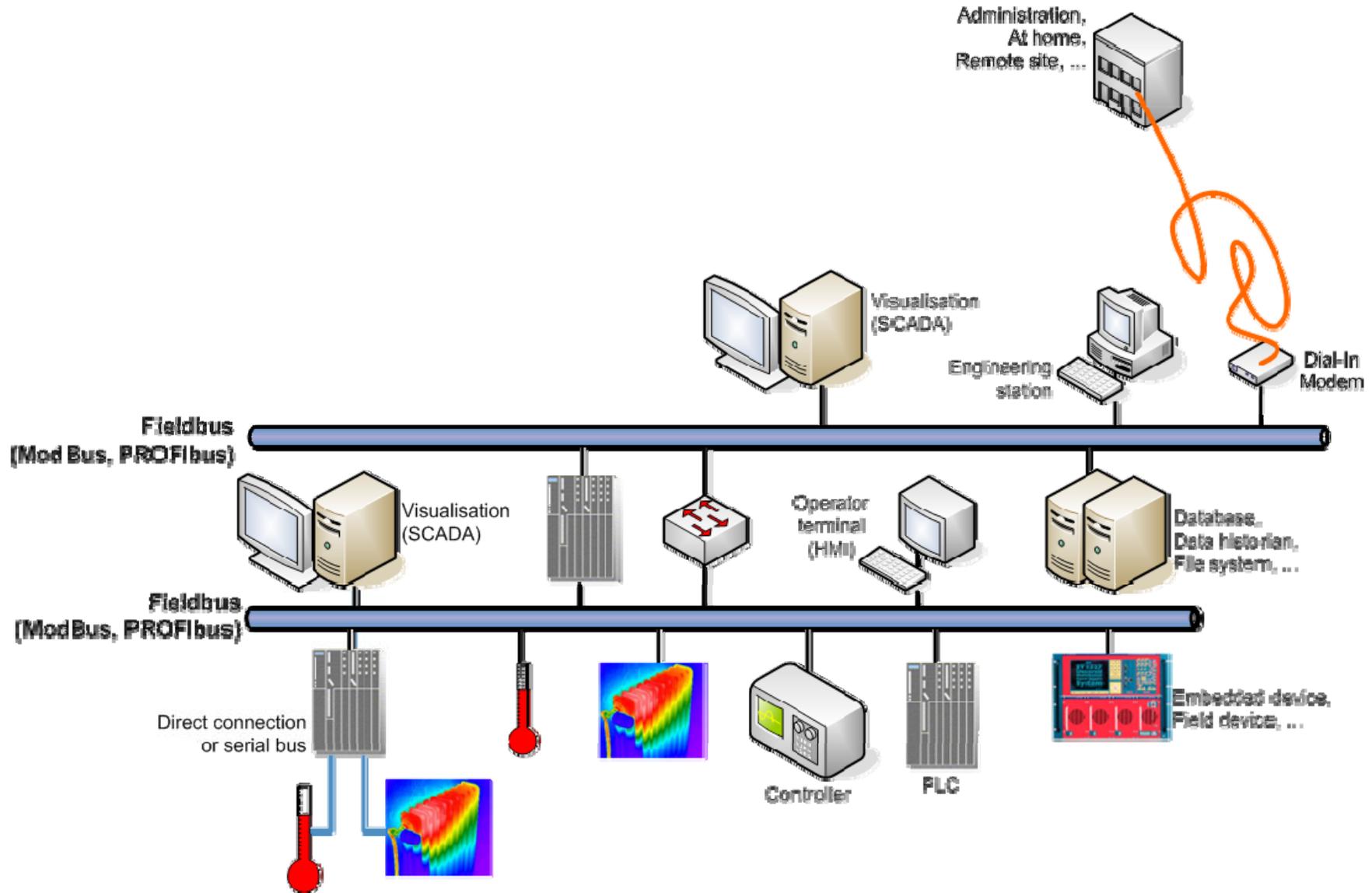
Shared Accounts & Passwords





(R)Evolution: The Past

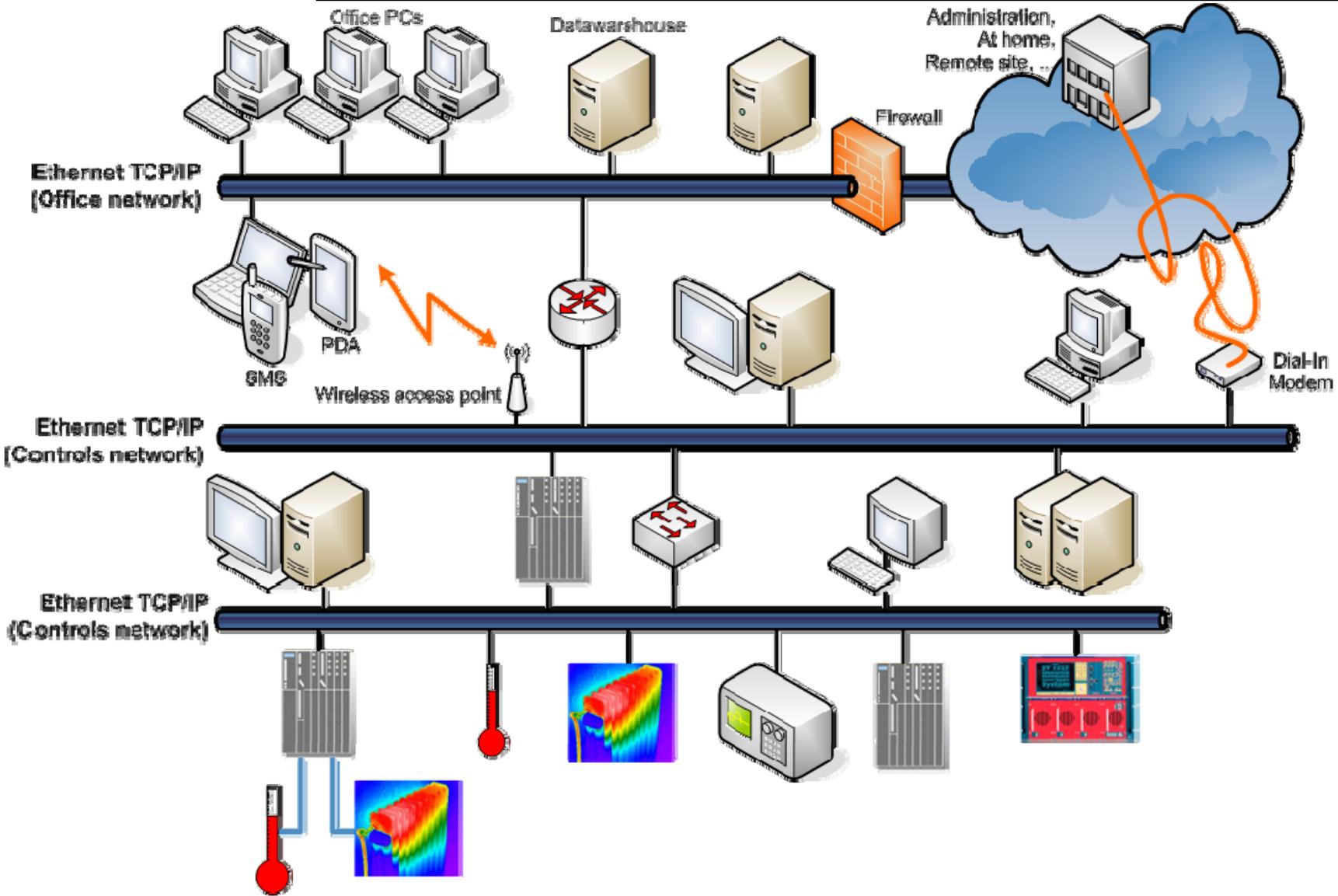
“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009





(R)Evolution: Today

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009





No (R)Evolution in Security (1)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

	“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





No (R)Evolution in Security (2)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

	“Office IT”	“Controls”
Changes	frequent, formal & coordinated	rare, informal & always
Patches & Upgrades	frequent	infrequent & impossible
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”)
	to be avoided	needs to run controls processes

“NEVER TOUCH A RUNNING SYSTEM!”



Inheriting IT Vulnerabilities

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

**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

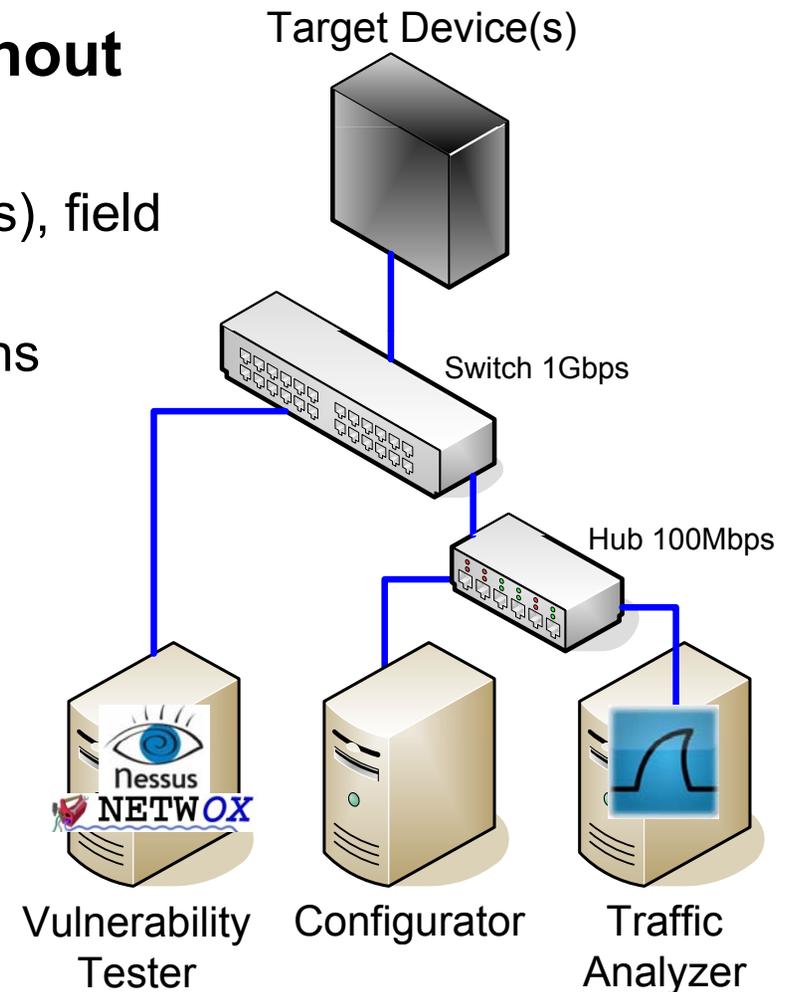
“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

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 !!!



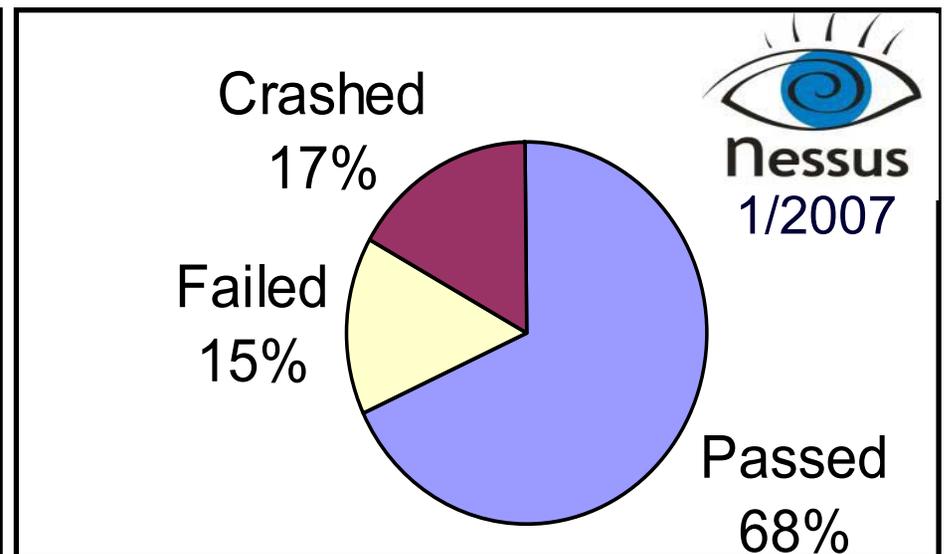
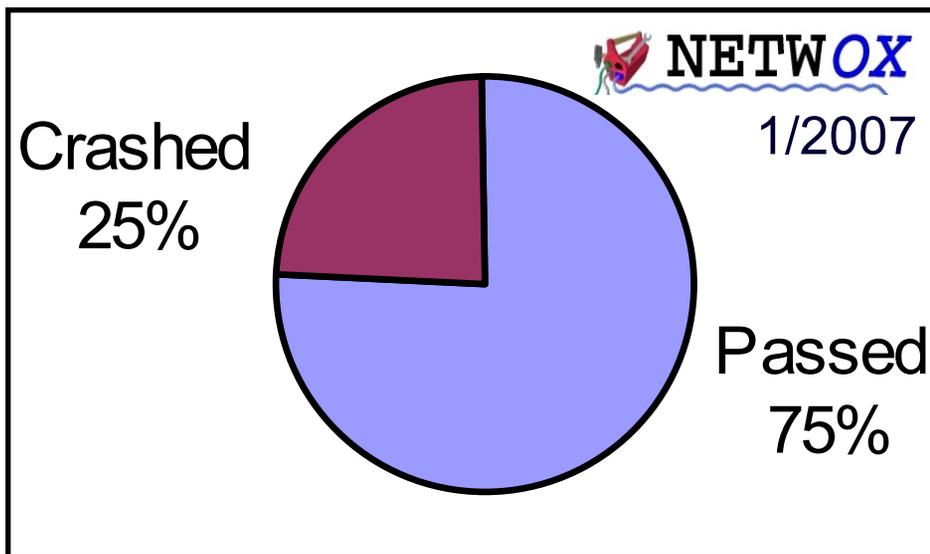


Control Systems under Attack !

"Control Systems Under Attack !?" — Dr. Stefan Lüders — September 10th 2009

CERN TOCSSiC Vulnerability Scans

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



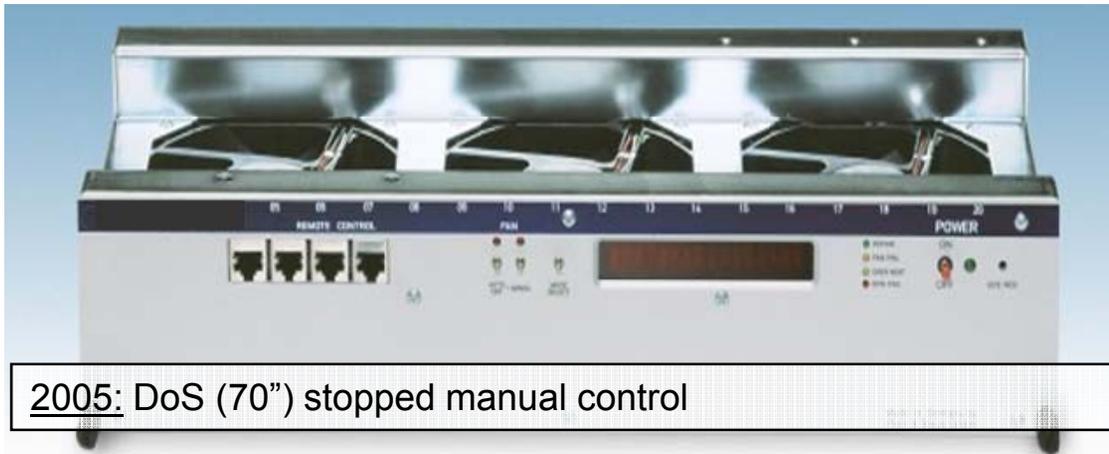
...PLCs under load seem more likely to fail !!!





TOCSSiC Findings (1)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009



The device crashed
while receiving special
non-conform packets

...violation of TCP/IP standards !!!

FTP server allows anonymous login or crashed

...legacy protocols introducing security risks !

HTTP server crashed or allowed 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”) !



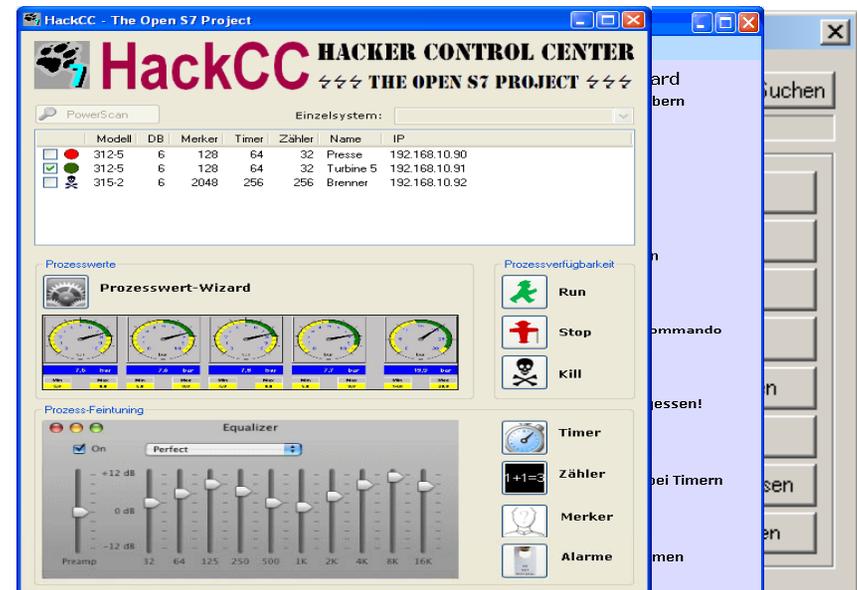


TOCSSiC Findings (2)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

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 !





Why worry ?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009



$$\begin{aligned} \text{Risk} &= \\ &\text{Vulnerability} \\ &\times \text{Threat} \\ &\times \text{Consequence} \end{aligned}$$



Who is the threat ?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

- ▶ Trojans, viruses, worms
- ▶ Disgruntled (ex-)employ
- ▶ Attackers (giving step-by-step providing freeware hack

Lack of procedures

- ▶ Flawed updates or patch
- ▶ Inappropriate test & mai

Lack of robustness

- ▶ Mal-configured or broke
- ▶ Developer / operator “fir

Ignorance...

Confidential data on Wiki, webpages, CVS..

Google search results for "samfox site:cern.ch".

Web

[DOC] [WHAT AND WHEN TO UPLOAD IN MTF](#)
File Format: Microsoft Word - [View as HTML](#)
... icon of <http://sm18-operation.web.cern.ch/sm18-operation> (sm18 operation page); When MTF page gets open, enter login 'sm18op' and password '**samfox**'. ...
www.cern.ch/sm18-public/sss/procedure/WHAT,%20WHEN%20&%20HOW%20TO%20UPLOAD%20IN%20MTF%20for%20SSS.doc - [Similar pages](#)

[PPT] [Slide 1](#)
File Format: Microsoft Powerpoint - [View as HTML](#)
"**samfox**". if some people. Have forgot. MTF my custom report. My custom reports. MTF my custom report. For dipole. For SSS. MTF my custom report. Magnet Name ...
www.cern.ch/sm18-public/presentation/Presentation%20Starting%20Up.ppt - [Similar pages](#)

[XLS] [Sheet1](#)
File Format: Microsoft Excel - [View as HTML](#)
70, sm18op, password - **samfox**. Click access equipt data. Type hcl% magnet no. in identifier and select assemblies only in type. Now click search, ...
www.cern.ch/sm18-public/dipole/procedure/SM18%20made%20easy%20in%20details%20for%20Dipole.xls - [Similar pages](#)

In order to show you the most relevant results we have omitted some entries very sim



Real or not ?!

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009



W32.Blaster.Worm
out three days earlier

Cracked road sign

THE WALL STREET JOURNAL. TECH

Europe Edition ▾ Today's Paper · Video · Columns · Blogs · Graphics

Home World Business Markets Market Data

Congress > Legislation > 2009-2010 (111th Congress) > S. 773

Text of S. 773: Cybersecurity Act of 2009

Show this version:
Introduced in Senate

Download PDF
Full Text on THOMAS
Go to Bill Status

GovTrack's bill text viewer has been updated. For the new viewer, archival legislative text will not be available. For the new viewer are welcome.

This version of the bill as introduced in the Senate. It may differ from the bill as it was written by its sponsor and may differ from the version of the bill as it was passed by the House of Representatives. The most recent version of the bill available on this website.

Compare to this version:

...America's failure to protect cyberspace is one of the most urgent national security problems facing the country.

IN THE SENATE OF THE UNITED STATES

We're HEP, nobody will attack us?!

Electrical grid in
Spardy (April 2009)

U.S. congress faces
this Wind of Change !





Attacks at CERN ☹

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

“In March Windows computers were compromised

...The initial compromised host was scanning the network and several compromise attempts were made to the

```

220-<<<<<<==< Haxed by A|0n3 >==<>>
220- ,,øα°°^°°αø, ,,øα°°^°°αø, ,,øα°°^°°αø, ,,øα°°^°°αø,
220-/
220-| Welcome to this free shell
220-| Today is: Thursday, 23 March 2006
220-|
220-| Current time: 12:00:14
220-| Speed: 58.57 MB/s
220-|
220-| 3 days, 10 hours, 31 min. and 31 sec.
220-| Connected : 1 Total : 15

```

Management Buy-in!!!

Unpatched oscilloscope (running Win XP SP2)



LHC First Beam Day

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

003/43

SAT GeoStar 45

Mozilla Firefox

Αρχείο Επεξεργασία Προβολή Ιστορικό Σελιδοδείκτες Εργαλεία Βοήθεια

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

Greeklish -> greek Systran Indymedia :: UNIVERSITY STUDENT... s3cmre.gr (l) Linuxfor...

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

Post a new topic http://[redacted]anthsh.html

GOST
GREEK SECURITY TEAM

10/09/08 03:00

Αυτήν την ώρα γίνεται 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 διαχείρισης που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυακός τόπος.

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
TMSYS 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* !

"Control Systems Under Attack !?" — Dr. Stefan Lüders — September 10th 2009

UPLOAD FORM

Browse...

Configuring [REDACTED], after the basic OS inst...
has been performed...

Boot into single user mode:

- . When "Booting Scientific Linux CERN" appears, stop the boot by pressing any key
- . Leave kernel selection on default -- should end in "s"
- . Press "a"
- . At the end of the boot line, add "single" at the end:
grub append> ro root=LABEL/ rhgb single
- . Continue booting

Find out MAC addresses of both network interfaces:
ifconfig eth0 (use for internal network)
ifconfig eth1 (use for external general public)
Write them down for later use

- . Set root password with "passwd" command from console

```
String q = qu.replaceAll(">", ">");  
out.println(q+"<P>");  
StringTokenizer st = new StringTokenizer(query);  
String firstWord = st.nextToken();  
String first = firstWord.toUpperCase();  
if (!first.equals("SELECT"))  
{  
    out.println("do nothing since it is not a SEL  
    return;  
}  
Statement stmt = null;  
+ ...
```

Neglected "Rule of Least Privileges":
Everyone could upload
whatever he/she wants...



Configuration well
documented on Google...



Lack of input
validation & sanitization





Who owns the consequences ?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

Who can allow for loss of

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



Who is prepared to take *full* responsibility?



Who is in the position to *really* take it ?



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



ZDNet Government
 Richard Koman
 Get ZDNet Government via: [Mobile](#) [RSS](#) [Email Alerts](#) [Bios](#)
 Pick a blog category
 September 12th, 2008
 Hackers deface LHC site, came close to turning off particle detector

Telegraph.co.uk
 Home News Sport Business Travel Jobs Motoring Telegraph TV
 Earth home Earth news Earth watch Comment
 Charles Greene
 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



Defence-in-Depth

"Control Systems Under Attack !?" — Dr. Stefan Lüders — September 10th 2009



Devices & Hardware

**Firmware & Operating Systems
(Network-) Protocols**

**Software & Applications
Third party applications**

**Operator & User
Vendor & Manufacturer**



Myths about Cyber-Security

"Control Systems Under Attack !?" — Dr. Stefan Lüders — September 10th 2009

"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 !"





Ground Rules for Cyber-Security

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009



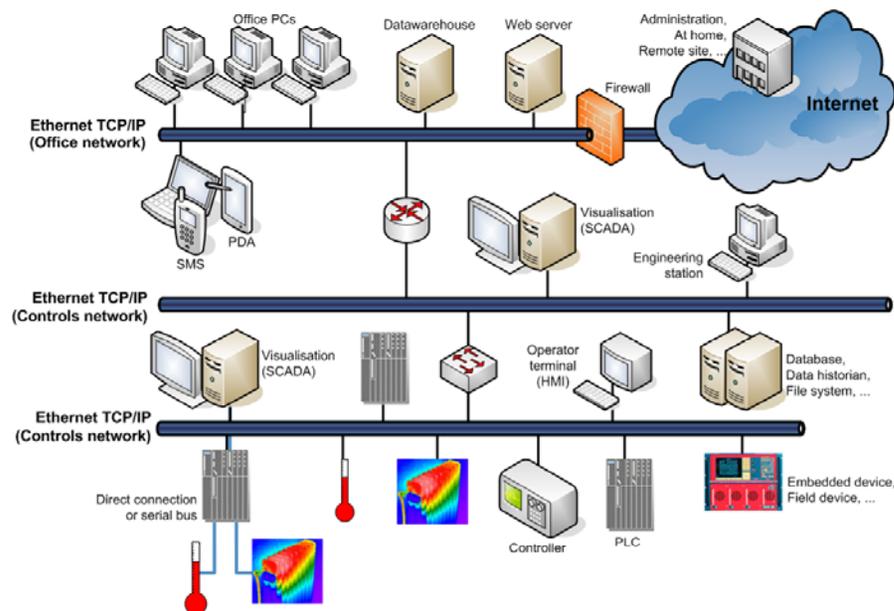


Separate Networks

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

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, and control web pages**
- ▶ Control remote access
- ▶ Deploy traffic monitoring & Intrusion Detection Systems

Control (Remote) Access

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

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



```
// If same day then simple query
if (($startDay == $endDay) && ($startMonth == $endMonth))
  $dateClause = " WHERE PROCESSINGDAY = TO_DATE(':$startDay-$startMonth-$startYear')";
else {
  $dateClause = " WHERE PROCESSINGDAY BETWEEN TO_DATE(':$startDay-$startMonth-$startYear')
  $dateClause .= " AND TO_DATE(':$endDay-$endMonth-$endYear')";
}

// do something with the results
$user = [REDACTED]
$pass = [REDACTED]
$db = [REDACTED]

$db_conn = oci_logon($user,$pass,$db);

$sqlstring = "Select sum(NROFRECORDS),execluster,jobstat
$sqlstring .= $dateClause;
```



Increase Robustness

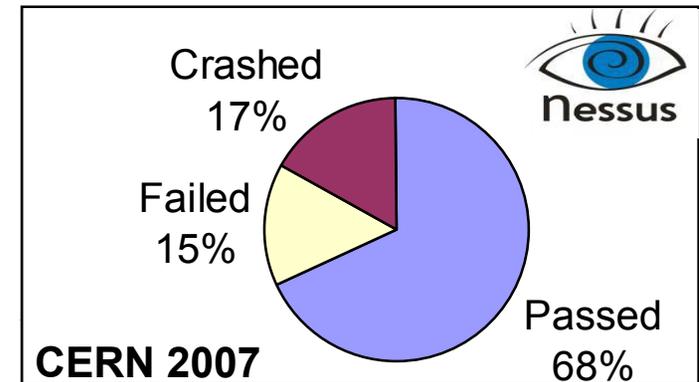
“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

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



HackCC HACKER CONTROL CENTER
THE OPEN S7 PROJECT

Modell	DB	Merker	Timer	Zähler	Name	IP
<input type="checkbox"/> 312-5	6	128	64	32	Presse	192.168.10.90
<input checked="" type="checkbox"/> 312-5	6	128	64	32	Turbine 5	192.168.10.91
<input type="checkbox"/> 315-2	6	2048	256	256	Brenner	192.168.10.92

Prozesswert-Wizard

Prozessverfügbarkeit

- Run
- Stop
- Kill

Prozess-Feintuning

Equalizer

Timer

- Zähler
- Merker
- Alarme





Review Development Life-Cycle

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

Review procedures for A Boeing 777 uses similar technologies to Process Control Systems



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



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



Foster Collaboration & Policies

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

Make security an objective

- ▶ Get **management buy-in** (security has a cost – successful attacks)
- ▶ Produce “Security Policy for Controls”
- ▶ **Follow** the **basic standards** of Industry

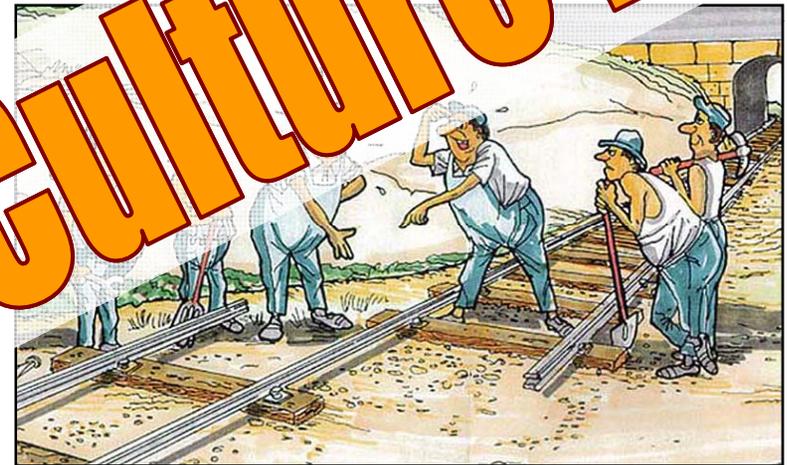
Bring together control & IT experts

- ▶ Control system experts know their systems by heart – but IT experts?
- ▶ IT people often don't know their systems – but IT security they do
- ▶ Win mutual trust in their domain
- ▶ Gain synergy

Change the culture

and raise awareness

Culture !!!





Force the Vendors on Board

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009

Manufacturers and vendors are part of the solution !

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



“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>





Summary

"Control Systems Under Attack !?" — Dr. Stefan Lüders — September 10th 2009



The (r)evolution of control systems...



...omitted security aspects!



Why worry ? The risk equation

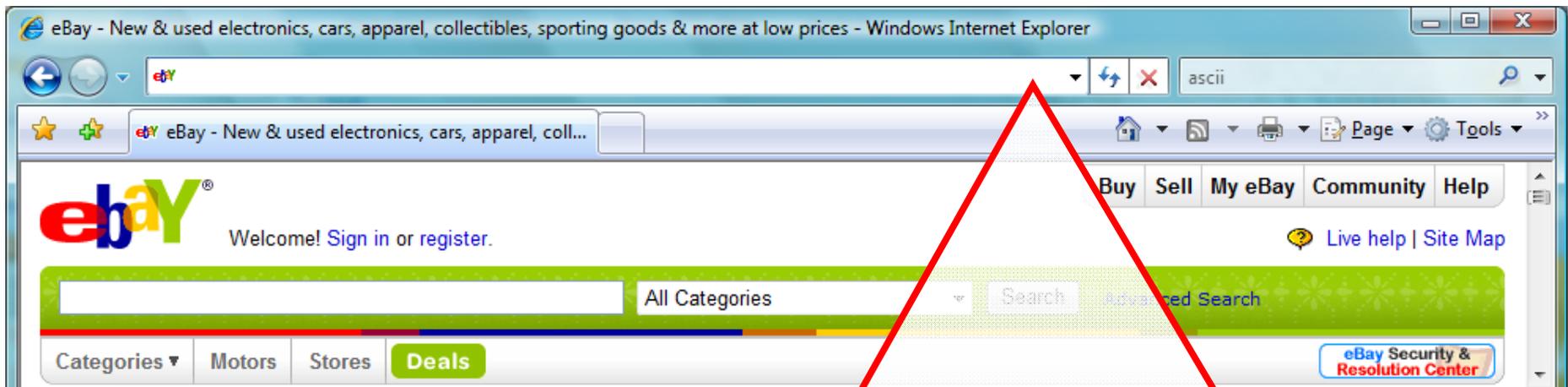


Mitigation: Defense-in-Depth



Thank you very much !!!

“Control Systems Under Attack !?” — Dr. Stefan Lüders — September 10th 2009



Quiz: Which link leads 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&raflid=0&encRaflid=default
- ▶ <http://secure-ebay.com>

