



# Control Systems Under Attack !?

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

**Dr. Stefan Lüders**  
Openlab Summer Student Lectures, July 19<sup>th</sup> 2010



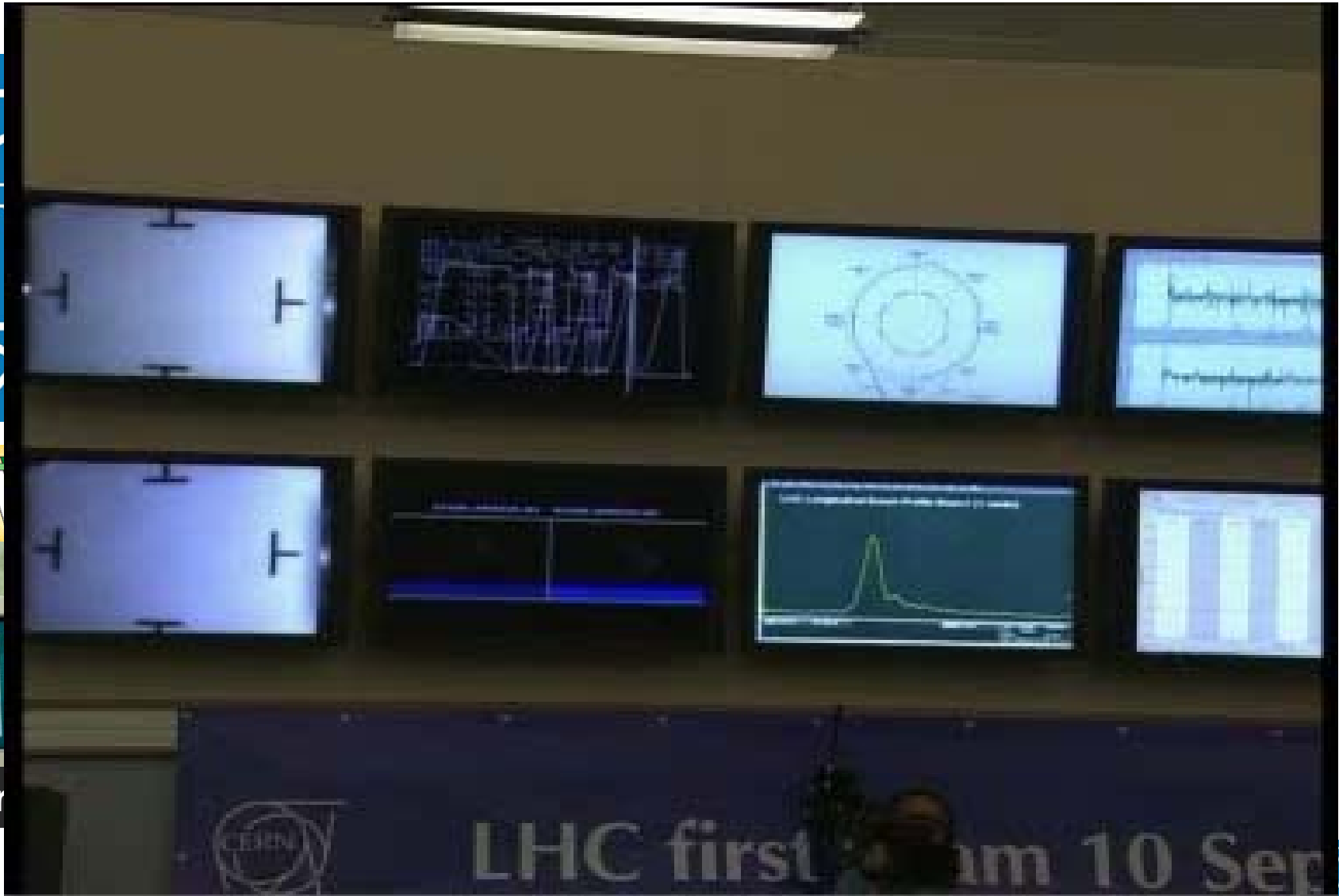


# CERN in a Nutshell

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



Tim Berners-Lee

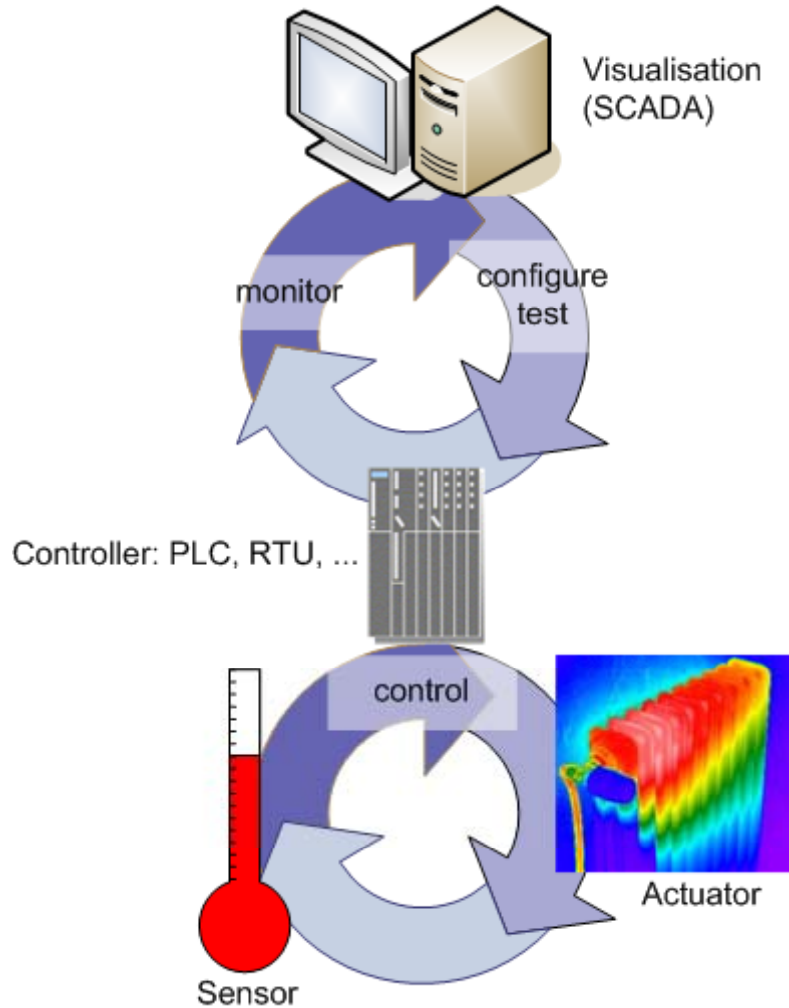




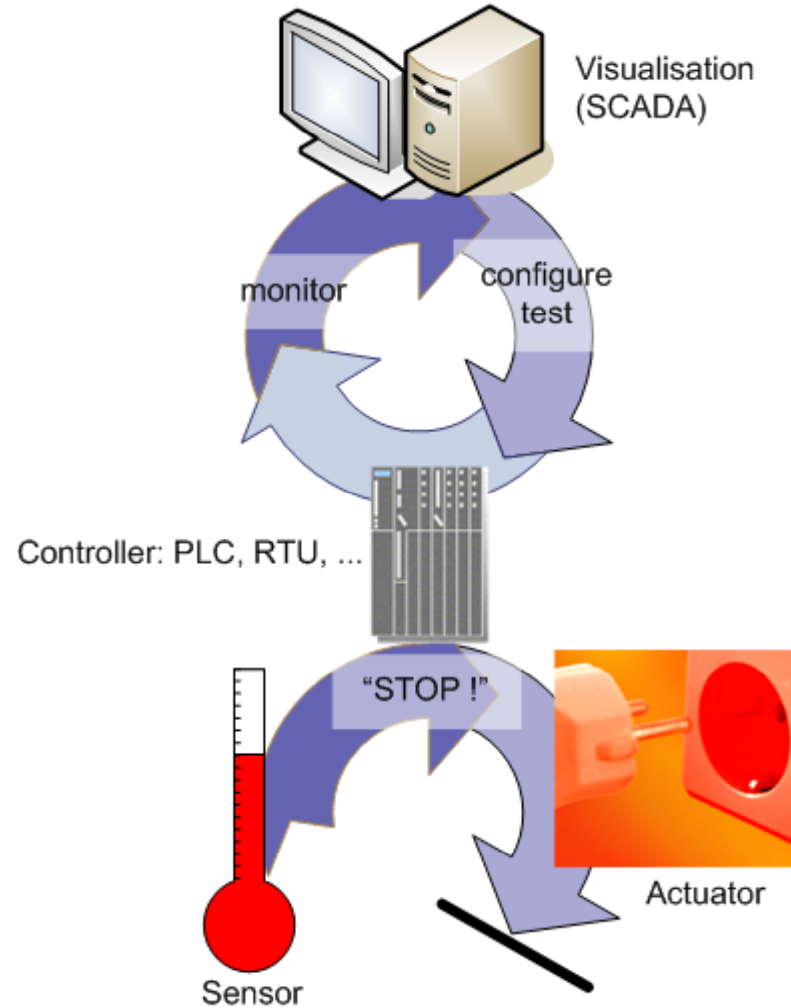
# “Control Systems” in a Nutshell

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## Process Control System (PCS)



## Safety System





# “Security” in a Nutshell

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

**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**



**BTW: Security is *not* a synonym for safety**





# Overview

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



**“Control Systems” go “IT”...**



**...but omitted security aspects!**



**Why worry? The Risk Equation**



**Mitigation: Today's Cacophony**



# “Control Systems” go “IT” ...

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



## In the past, PCS were

- ▶ **stand-alone** & interconnected using proprietary networks only
- ▶ accessed via modems, if at all
- ▶ using **own standards**, technologies & means
- ▶ **largely proprietary**



*"He's the only person who knows how to program our 20 year old PLCs."*

## Today, PCS

- ▶ base on **custom-of-the-shelf** hardware and software (“office IT”)
- ▶ are **highly inter-connected**
- ▶ **determine & impact widely on our daily life**





# Control Systems for Living

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

- ...in the electricity sector
- ...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, news
- ...in supermarkets
  - ▶ e.g. scales, fridges

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

CERN Control Centre



In the aftermath of the 9/11 attacks & today's “terroristic” fears:

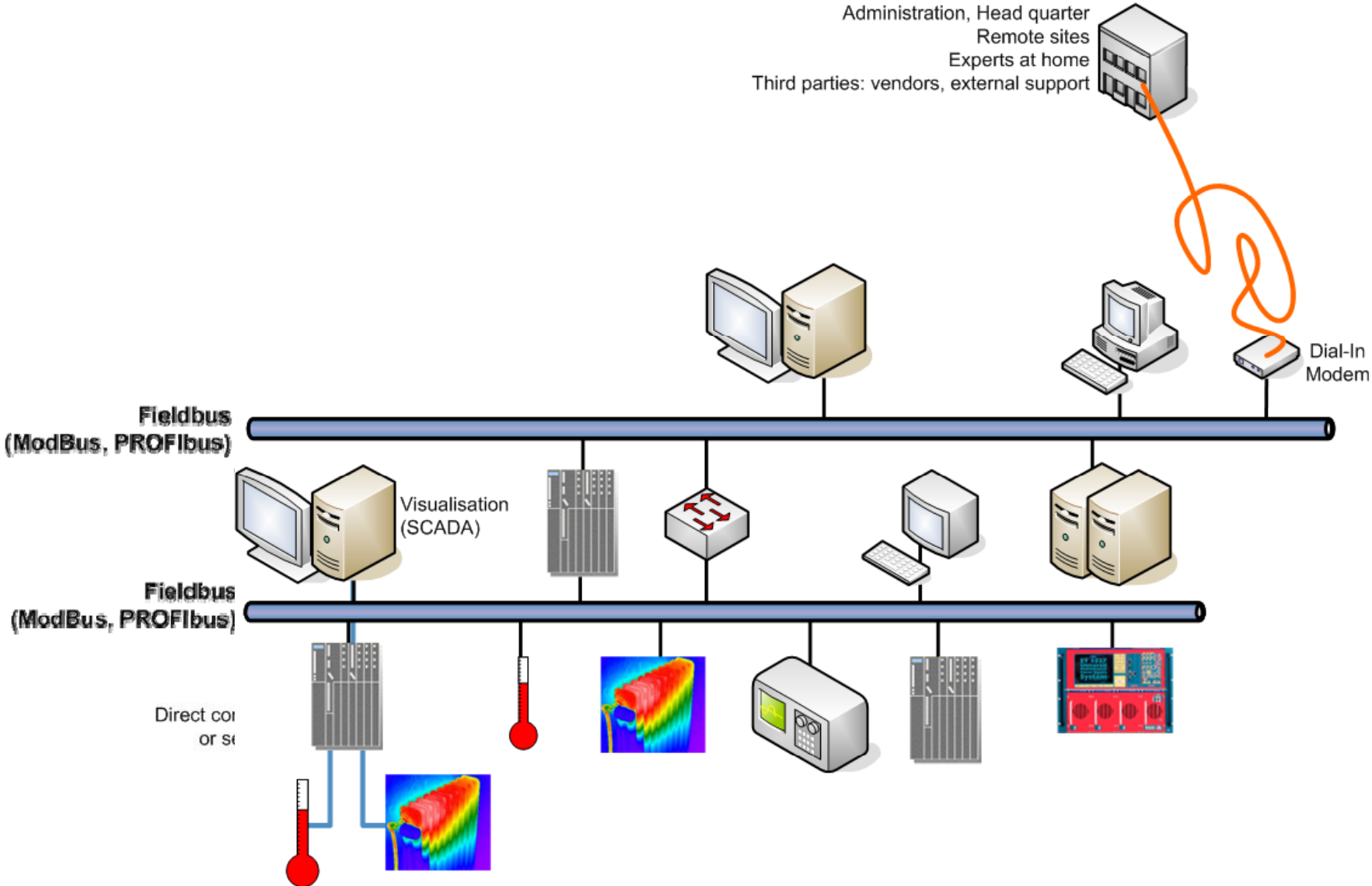
## Critical Infrastructure Protection (CIP)





# (R)Evolution: The Past

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

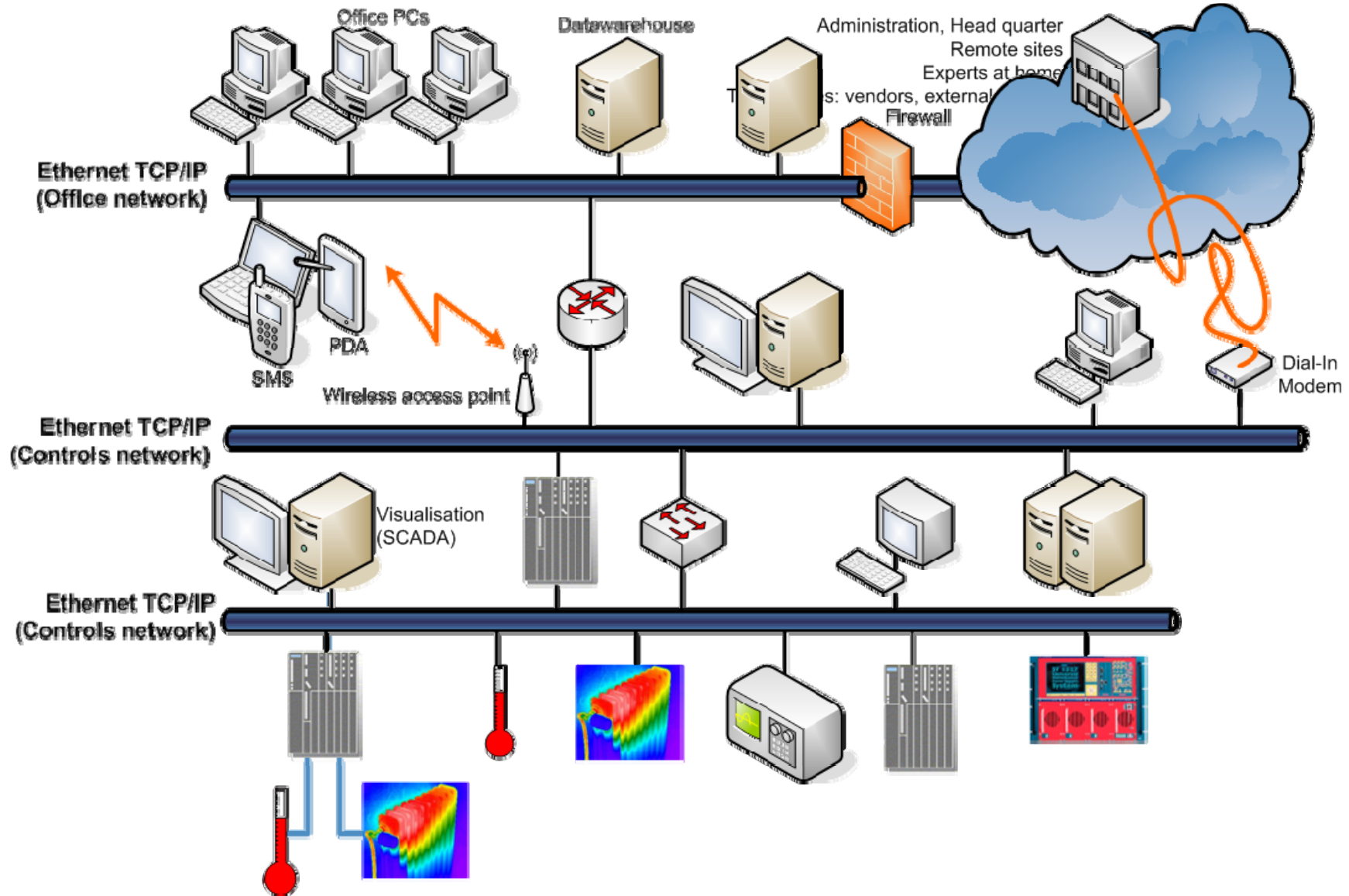






# (R)Evolution: Today

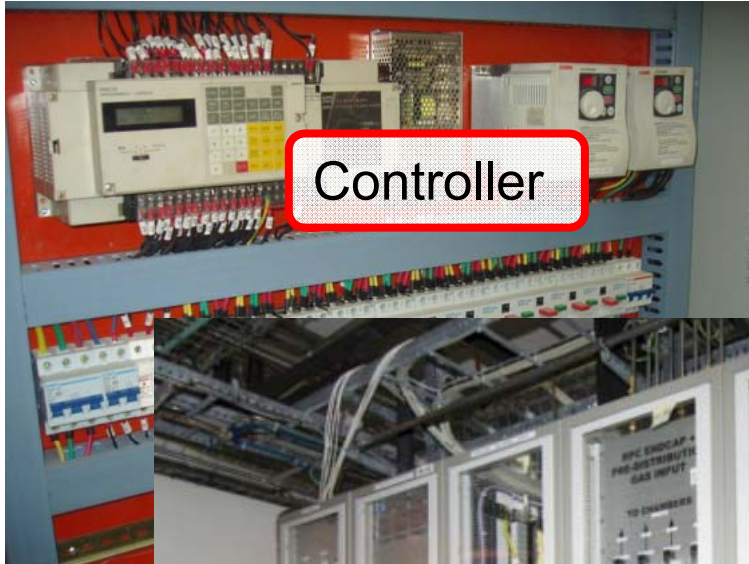
“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010





# This is how PCS can look like

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



Controller



Controller

Sensors & actuators





# Standard Hard and Software

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



**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**





# Standard Security Risks

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



**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**





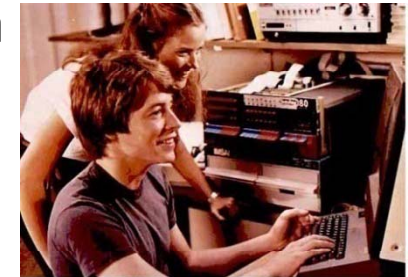
# PCS omitted security aspects!

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



## PCS security was

- ▶ hidden (“**security through obscurity**”)
- ▶ never a real concern
- ▶ a target for nerds



## Today,

- ▶ **Same “office IT”-risks** inherent for PCS
- ▶ **Same “office IT”-attackers** targeting PCS

## But also, today,

- ▶ many entities are paranoid on this  
– in particular after 9/11





# “Controls” is *not* IT ! (1)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

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





# “Controls” is *not* IT ! (2)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



“Office IT”: “CIA” (Confidentiality – Integrity – Availability)

“Controls”: “AIC” (Availability – Integrity – Confidentiality)

A Boeing 777 uses similar technologies to PCS....

Admin Rights to be avoided needs to run controls  
**“Never touch a running system !!!”**



# Why worry? The Risk Equation

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$





# Who is the threat ?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## 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 / procedures





# Damage by Viruses & Worms?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## 2003/08/11: W32.Blaster.Worm

### 'Sinister' Integral Energy virus outbreak a threat to power grid

ASHER MOSES  
October 1, 2009

smh.com.au

### Linux saves Aussie electrical grid

A virus outbreak is wreaking havoc on a computer network, forcing it to rebo

Open source to the rescue  
By Nick Farrell

the **INQUIRER**

### Zotob, PnP Worms Slam 13 DaimlerChrysler Plants

By: Paul F. Roberts  
2005-08-18  
Article Rating: ☆☆☆☆☆ / 0  
Share This Article

eWEEK.COM

... have saved an Australian power supply network got infected with a virus

SecurityFocus™

There are 0 user comments on this Security story.

ris-Besse nu  
by plant pers

infopackets  
Deliciously Addictive Tech News Served Daily

The latest worm attacks, exploiting holes in the Windows Plug and Play service, are causing grief to major corporations.

### Hospital Equipment Infected with Conficker

The bre: 5-inch h analog b the nucl permitte

A round of Internet worm infections knocked 13 of DaimlerChrysler auto manufacturing plants off almost an hour this week, str some 50,000 auto workers as infected Microsoft Windows sy spokesperson told eWEEK.

by Bill Lindner on 20090428 @ 02:13PM EST | google it | send to friends  
Filed under Security | (related terms: conficker/downadup worm , hospitals , computers infected , internet , critical )



# Damage by Insiders?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



**ParanoidProse**  
reading to keep you up at night

## hacking California canal system

software

Jul 17

### new windows 0-day targets SCADA, threatens us all

By alberghacks

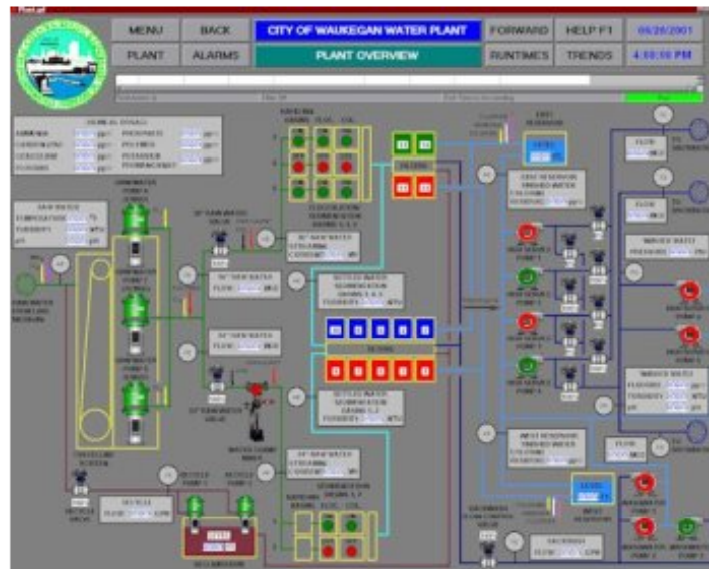
↓ Add comments

Duo deny L  
The Hollywoc  
By John Leyd  
Posted in Enterj  
Free whitepaper-

2000:  
46x in  
basen

A pair of Los A  
signals to disru

Gabriel Murillo,  
access of a col  
accused of rou  
LA's Automate  
commands to r



Over the past few days, reports of a new attack against Windows based SCADA systems (the computer software which control power plants, water treatment facilities and other parts of the critical infrastructure) have been making the rounds of the security blogosphere. While the payload carried in the new attacks is aimed specifically at these vital control systems (specifically a system called Siemens SCADA WinCC + S7), the vulnerability used to deliver it looks

COMPUTERWORLD

net.

kers

could make

contractor

court with

on oil-rig

site for not

the

other

ed

they

charge, though, fortunately, no leaks.





# Damage by Attacker? (1)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## CIA slipped bugs to Soviets

### Memoir recounts Cold War

By David E. Hoffman

washingtonpost.com

updated 12:13 a.m. ET Feb. 27, 2010

Russia welcomes hack attacks

Script Kiddies cut teeth hijacking critical ir

By Thomas C Greene in Washington DC • G

Posted in Business, 27th April 2000 12:25 GMT

Free whitepaper – Taking control of your data demons:

Malicious hack attacks are on the rise in Russia  
Interfax news service reports. Most spectacular  
that Gazprom, a state-run gas utility, came und  
Gazprom is the world's largest natural gas prod  
The intruders succeeded in defeating the comp  
controlling gas pipelines, Interior Ministry spok  
The flow of natural gas was under the control  
reported. The C  
name it. The Int  
crime. ©

TECHNOLOGY | APRIL 8, 2009

## Electricity Grid in U.S. Penetrated By Spies

Article Video Comments (145)

Email Print

The Register

CONTENT

## Report: Cyber Attacks Caused Power Outages in Brazil

By Kevin Poulsen November 7, 2009 | 12:55 am | Categories: Cybarmageddon!

WIRED

Electrical blackouts impacting millions of people in Brazil in 2005 and 2007 were caused by hackers targeting control systems, according to the CBS news magazine 60 Minutes.

(Update: Brazilian Blackout Traced to

In a show set to air Sunday night, CBS  
Espirito Santo in 2007 on a hack attac

## Hackers hit Pennsylvania water system

A foreign hacker who penetrated security at a Harrisburg, Pa., water filtering plant is under investigation for planting malicious software capable of affecting the plant's water treatment operations, the FBI said.

The hacker did not attempt to take control of the system; instead the intruder tried to use the system as its own distribution system for e-mails or pirated software, officials said.

sought to damage the power grid or other key infrastructure, but officials warned they could try

# InTech



st surfaced last year, based on  
ed to identify any country or the  
month, former cybersecurity czar  
ime, but didn't go into details.





# Damage by Attacker? (2)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

May 7, 2009 3:59 PM PDT

## Report: Hackers broke into FAA air traffic control systems

by Elinor

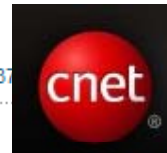
0 twe

Hackers Adminis

In Febru  
identifical  
report s



Font size Print E-mail Share 37



ACHTUNG:



## The Argus

### Rude awakening for dawn drivers

7:38am Friday 27th October 2006

Print Email Share

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.





# No Damage, yet? (1)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

“....penetration test locked up the system and was not able to send gas through its pipes”  
- Sandia National Labs, US [2005]

September 26, 2007 -- Updated 0306 GMT (1106 HKT)

Sources: Staged cyber attack reveals vulnerability in power grid



FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack

By Kim Zetter 01.04.08



Security

## America's Hackable Backbone

Andy Greenberg, 08.22.07, 6:00 PM ET

### TVA Power Plants Vulnerable to Cyber Attack Regulators Want Authority to Require Security Upgrades In

By Brian J. ... Safety

washington  
Wednesd:

You are in: Home > Safety > News Article

The Tenn  
public po  
could sab  
than 8.7  
Accounta

DATE: 06/05/09

SOURCE: Air Transport Intelligence news

### US air traffic exposed to “serious attacks

By John Croft

Federal investigators were able to hack into an air traffic and traffic flow management computers as part of a wide-scale test of the US FAA's air traffic control infrastructure.

The audit results, published 4 May by the Transportation Department's Inspector General (OIG), concluded that “web applications used in air traffic control are not properly secured to prevent attacks or unauthorized access.”



The Boeing 787 Dreamliner aircraft makes its public debut July 8, 2007, amidst employees and special guests outside the Boeing assembly plant in Everett, Washington.  
Photo: Robert Sorbo / Corbis

Boeing's new 787 Dreamliner passenger jet may have a serious security vulnerability in its onboard computer networks that could allow passengers to access the plane's control systems, according to the U.S. Federal Aviation Administration.





# No Damage, yet? (2)

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## Hole Found in Protocol Handling Vital National Infrastructure

March 25, 2007

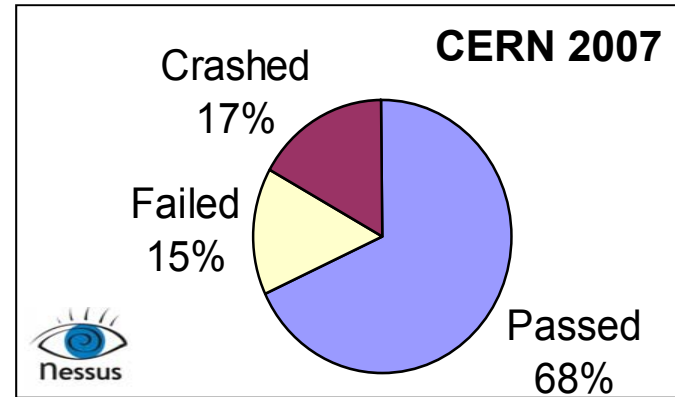
Systems that control dams, oil refineries, railroads, power plants have a vulnerability that could cause takeover, according to a recent research report.



**Secure SCADA Syst**  
Realtime software you

7 May 2008, 14:37

## Denial of service hole in WonderWare SCADA systems



## A Heart Device Is Found Vulnerable to Hacker Attacks

By BARNABY J. FEDER  
Published: March 12, 2008

### CIP VIGILANCE

This Blog is about Critical Infrastructure Protection (CIP) and Information Security issues.

### SCADAmobile for iPhone

November 25, 2009 CIIP [Go to comments](#) [Leave a comment](#)

I just came across this iPhone App (ScadaMobile) from SweetWilliam Automation. (Company Website)

The App description states that the product can Monitor (display and change) PLC variables (tags) through local or remote wireless access.



The Manual which can be downloaded here describes how the App will access internet.

“ScadaMobile is designed to communicate with PLCs without using dedicated specific software installed on a PC.

ScadaMobile communicates with OMRON PLC by sending FINS protocol commands. A remote connection, a GPRS or ADSL router is needed at the PLC site, which bridge between the PLC LAN (Local Network) and the WWAN or WAN (Internet). (Source: Section 4.1 in the manual.)



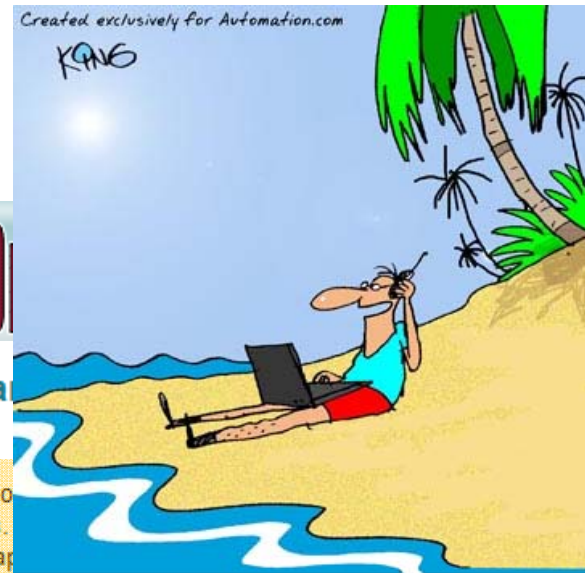
### The New York Times

- TWITTER
- SIGN IN TO E-MAIL OR SAVE THIS
- PRINT

### Technology news: February 2008

## BlackBerry-based SCADA puts plant in your hands

A German software developer and systems integrator has developed a SCADA system based on BlackBerry smartphones. The system, called Extend 7000, which relies on Java applications running on BlackBerries, can control and monitor industrial processes and S7 PLCs.



“I designed a program that allows me to run the entire plant from my computer. By the way, how’s the weather back there?”





# Damage due to Lack of Procedures?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

**"Data storm" blamed for nuclear-plant shutdown**  
 Robert Lemos, SecurityFocus 2007-05-18

The U.S. House of Representative's Committee on Energy and Commerce (NRC) to further investigate the cause of excessive network traffic at the plant.

## Cyber Incident Blamed for Nuclear Power Plant Shutdown

August 26, 2008 -- Updated 0152 GMT (0952 HKT)

**FAA computers delay hundreds of flights**

STORY HIGHLIGHT  
 • NEW: FAA says si...

**CNN.com/travel**

Next Article in Travel

READ VIDEO

ATLANTA, Georgia (CNN) -- Air traffic delays began to clear up Tuesday evening after computer problems left travelers across the United States waiting in airports, the Federal Aviation Administration said.

## The Washington Post

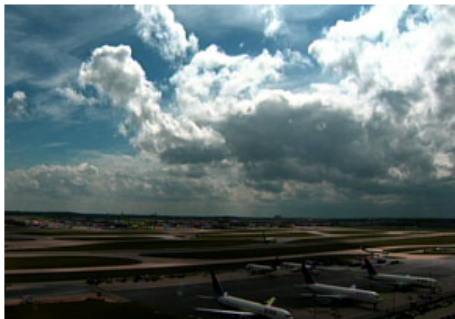
COMMENT

15 Comments | View All »

COMMENTS ARE CLOSED

WHO'S BLOGGING powered by

» Links to this article



Airports experienced hours of flight delays Tuesday afternoon after a communications breakdown at a Federal Aviation Administration facility, the administration said.

The facility south of Atlanta had problems processing data, requiring that all flight-plan information be processed through a facility in Salt Lake City, Utah, overloading that facility.

The two facilities process all flight plans for commercial and general aviation flights in the United States, FAA spokeswoman Kathleen Bergen said.

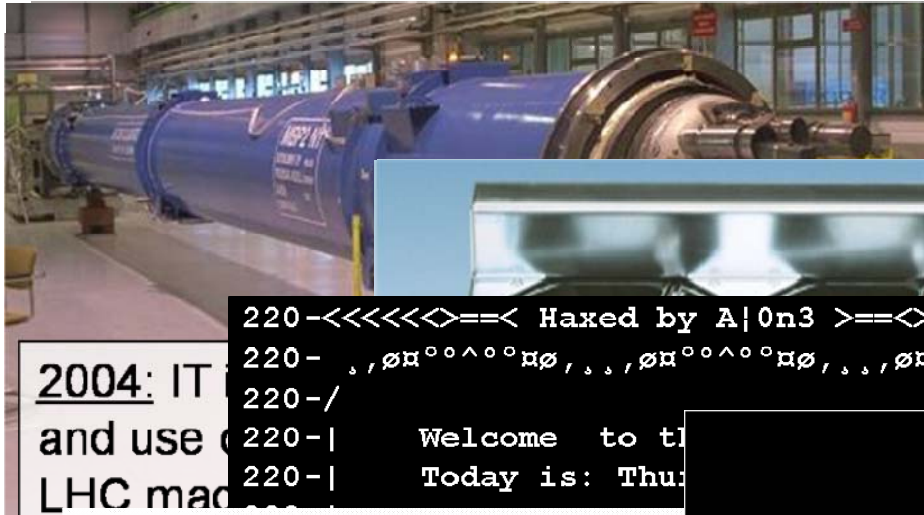






# No Damage at CERN

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



2004: IT  
and use of  
LHC machine

“In March .... Windows computer

...The initial compromised hardware and several compromise MS-SQL servers (port 1433) and 'sa' account...

...Analysis indicated that the installation left the password

2008: Control system historian of LHC experiment defaced





# Smart Meters: Risk & Hype

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



## Use case:

- ▶ Measuring your consumption at home
- ▶ Online with the grid: Optimizing the power usage
- ▶ Publicly accessible, off-the-shelf, open networks

## Risks:

- ▶ **Exploitation** of meter vulnerabilities: registration process, firmware, data, ...
- ▶ **Loss of confidentiality:** customer data available to others
- ▶ **Loss of integrity:** manipulation of reading data
- ▶ **Loss of availability:** data not available in a timely manner
- ▶ **Misuse** as attack platform

## Power Grid Is Found Susceptible to Cyberattack

Robert McMillan, IDG News Service

Saturday, March 21, 2009 12:10 PM PDT

An emerging network of intelligent power switches, called the Smart Grid, could be taken down by a cyberattack, according to researchers with IOActive, a Seattle security consultancy.

IOActive researchers have spent the past year testing Smart Grid devices for security vulnerabilities and have discovered a number of flaws that could

**PCWorld**



courtesy of M. Tritschler (KEMA)





# Mitigation: Today's Cacophony

"Control Systems Under Attack !?" — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



## Using "office"-IT *must* also mean using "office"-security technology":

- ▶ Apply same security measures
- ▶ Inherent differences need to be taken care of separately
- ▶ Defence-in-Depth as a basis
- ▶ Influence you vendor !!!

## Too many stakeholders:

- ▶ A cacophony in standards & guidelines
- ▶ A cacophony in interest
- ▶ No *real* directions by legislators



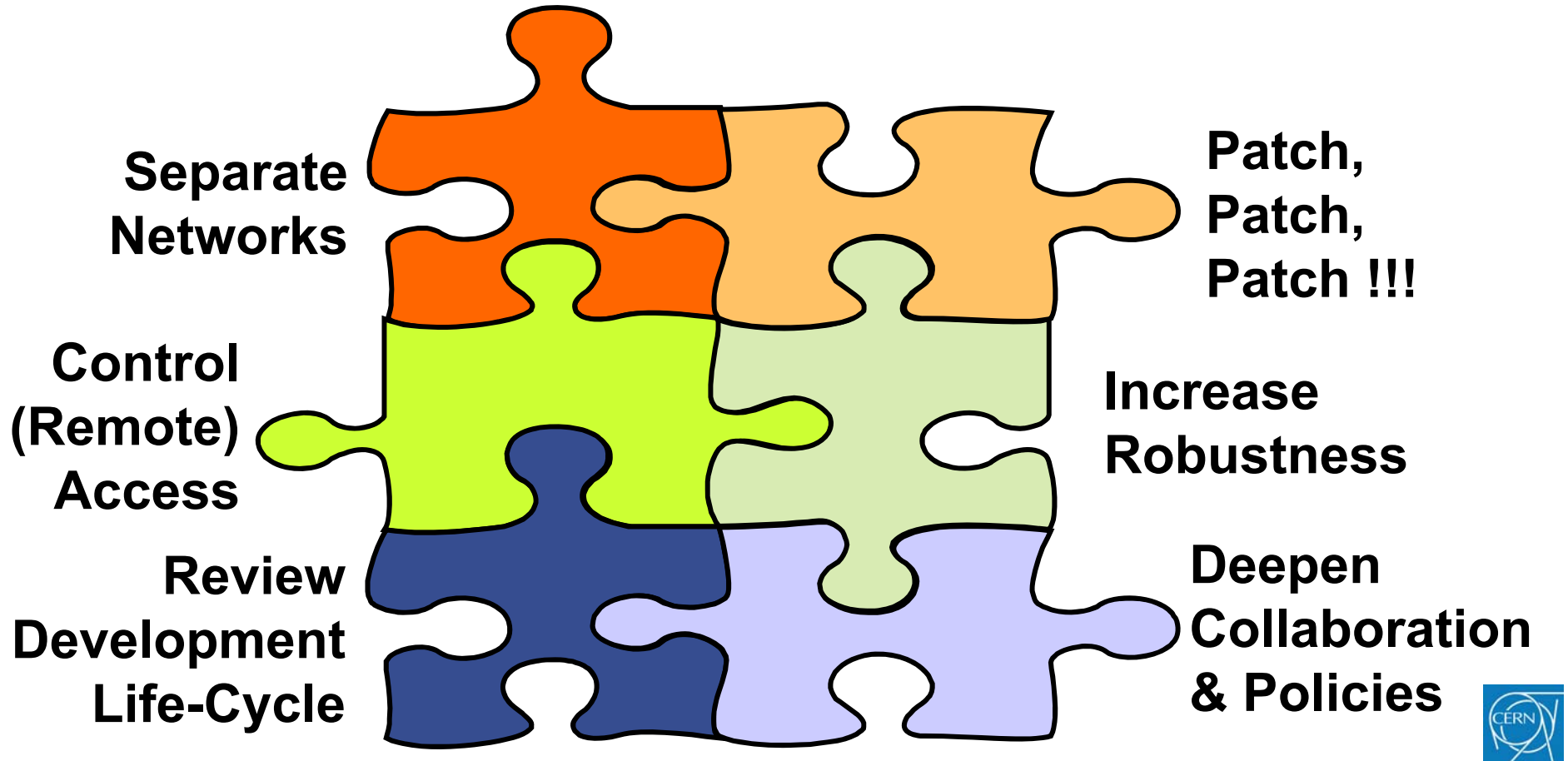


# Ground Rules for Cyber-Security

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## “Defence-in-Depth” protection on every layer:

device/hardware, firmware/operating systems/network protocols,  
software/applications, user/integrator/developer



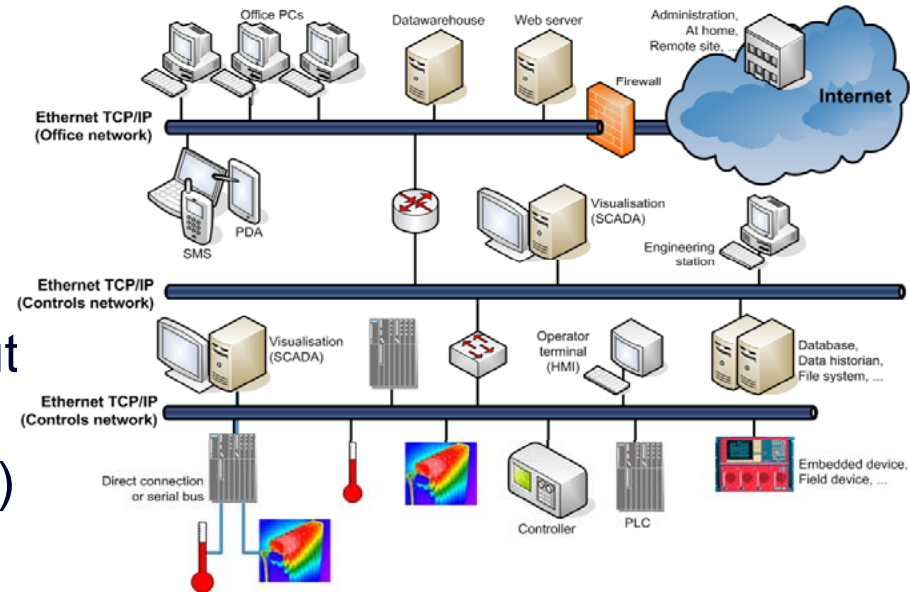


# Network Segregation

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## Different networks for different purposes:

- ▶ ...for accelerator operations
- ▶ ...and for experiments
- ▶ Campus network for office comput
- ▶ Additional **protective measures** where needed (“VPNs”, ACLs, ...)



## Restrictions on Controls Networks:

- ▶ **Assignment of responsibilities** and usage of authorization procedures
- ▶ **No** Internet, no (GPRS) modems, no wireless access points or laptops
- ▶ **Controlled inter-communication** between networks
- ▶ **Blocked incoming emails & control over visible web pages**
- ▶ Controlled remote access, e.g. for maintenance, development & testing
- ▶ Traffic monitoring & intrusion detection at the gates



# Patch, Patch, Patch !!!

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

```
220- <<<<<< Hacked by A10n3 >>>>>>>>
220-  .o00^o0ng .o00^o0ng .o00^o0ng .o00^o0ng
220- / They decide when to install what on which control PC
220- | Welcome to this fine str0 Windows XP/7 & Linux
220- | NOT watching is NOT an option
220- | Today is: Thursday 12 January,
220- |
220- | current throughput: 0.000 Kb/s
220- | Local Space for Rent: 5858.57 Mb
220- | Anti-virus software & updated signature f
220- | Running: 0 days, 10 hours, 31
220- | Users Connected : 1 Total : 15
220- | also on embedded devices !
220- | Checking with vendors patching procedures for oscilloscopes
```





# Control (Remote) Access

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## Following “Rule of Least Privilege”:

- ▶ Restricting all access to minimum
- ▶ Ensuring traceability (who, when, from where)
- ▶ Keeping passwords secret

## ...for all assets:

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

## “Role Based Access Control” for op’s:

- ▶ Reduction of “shared” accounts
- ▶ Full control for the shift leader of operations
- ▶ Multi-factor authentication for critical assets (planned)



```
// 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 the query and show tables
$User = 
$Pass = 
#Sdb = 
Sdb = "

Sdb_conn = oci_logon($User,$Pass,$Sdb);

Sqlstring = "Select sum(NROFRECORDS),exclcluster,jobstat
Sqlstring .= $DateClause;
```



# Review Development Life-Cycle

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## Reviewing procedures for Boeing 777 uses similar technologies to Process Control Systems



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



## Protecting operations

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





# Understand the Risks

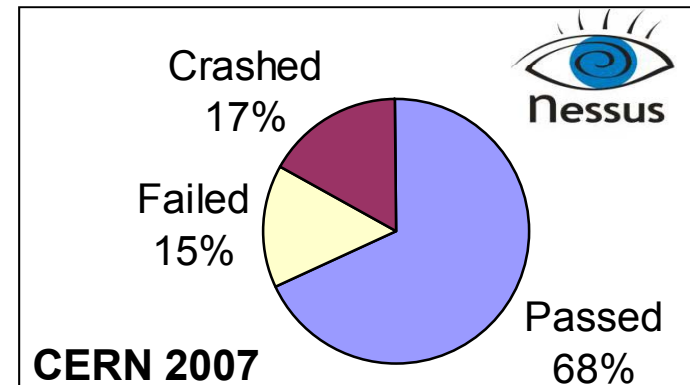
“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## PLCs and other controls devices are completely **unprotected**:

- ▶ No firewall, no anti-virus, nothing

## Thorough Risk Assessment:

- ▶ Building asset inventory
- ▶ Understanding dependencies
- ▶ **Running vulnerability tools** on everything (e.g . PLCs, control PCs, SCADA, data historians, Web servers)
- ▶ **Determination of weaknesses & risks**
- ▶ Applying “**Security Baselines**”  
i.e. a contract on security with recommendations for configuration settings, protective means, procedures & training



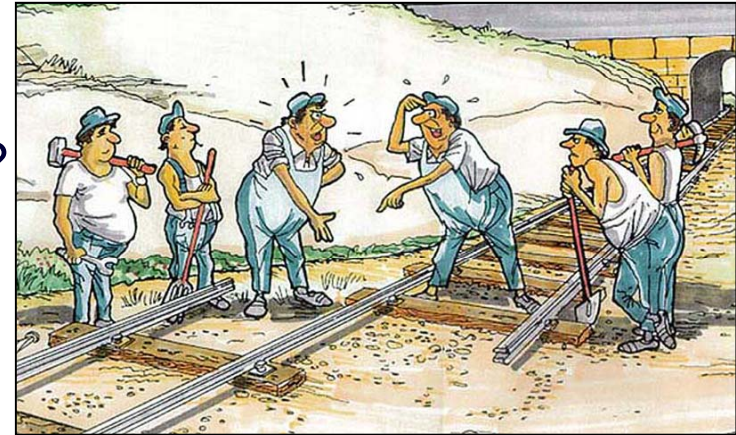


# Deepen Collaboration

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## Bringing together 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










## Training of users and raise awareness

### Looking outside!

- ▶ Following the **basic standards** of Industry
- ▶ Establishing contacts inside the HEP community with governments, with industry, ...
- ▶ Spread the word to the vendors, and...



Quelques astuces pour protéger votre ordinateur et vos données

-  **Utilisez les systèmes d'exploitation fournis par le département IT du CERN :** ils sont configurés de manière sûre et mis à jour automatiquement pour vous.
-  **Soyez prudent lorsque vous naviguez sur le Web :** ne cliquez pas sur des liens suspects et n'installez pas de plug-in douteux.
-  **Protégez vos mots de passe :** ne les partagez jamais; prenez garde au phishing (technique qu'utilisent les escrocs en ligne pour voler votre mot de passe); ne les réutilisez pas (utilisez des mots de passe différents pour des applications différentes); ne les tapez pas sur des ordinateurs ou des sites Web suspects.
-  **Protégez votre ordinateur privé :** utilisez l'antivirus du CERN; appliquez les mises à jour logicielles; n'installez pas de logiciels douteux.
-  **Protégez vos fichiers et données :** limitez l'accès à vos documents et répertoires; appliquez le principe du droit d'accès minimal.
-  **Suivez les règles informatiques du CERN :** respectez le droit d'auteur; n'utilisez pas de logiciels non-autorisés; consultez <http://cern.ch/ComputingRules>.
-  **Demandez conseil :** l'équipe de sécurité informatique vous propose des cours de formation, des analyses de codes logiciels, des balayages Web ou serveur etc., et est là pour vous aider: contactez [Computer.Security@cern.ch](mailto:Computer.Security@cern.ch) ou consultez <http://cern.ch/Computer.Security>.





# (Too) Many Standards... ?

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## “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](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”

ISO/IEC 27001:2005 and following

**Lot's of money dumped (wasted?) to have better CIP...**

**“Too many cooks spoil the broth”**





# Some more cooks...

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

## Government Initiatives:



## Global Key Players:



## Mixed Communities:



(This list is not intended to be complete.)





# Today's only (?) regulation

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010

**NIST**  
National Institute of  
Standards and Technology

## NIST 800-53 & 53A

- ▶ Help to identify, control, mitigate risks to information and information systems
- ▶ Recommendations and guidelines for selecting and specifying safeguards & countermeasures
- ▶ Foundation for risk assessment

...how does this apply to PCS  
(e.g. NIST SP800-82) ?

### FEDERAL INFORMATION SECURITY MANAGEMENT ACT

#### IMPLEMENTING SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard developed in response to the Federal Information Security Management Act of 2002. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in Special Publication 800-53.

This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems (other than national security information and information systems). The agency's risk assessment validates the security control set by determining if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), agency assets, or individuals. The resulting set of security controls establishes a level of "security due diligence" for federal agencies and their contractors.

In addition to the security requirements established by FISMA, there may also be specific security requirements in different business areas within agencies that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These requirements may not be equivalent to the security requirements and implementing security controls required by FISMA or may enhance or further refine the security requirements and security controls. It is important that agency officials (including authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and acquisition authorities) take steps to help ensure that: (i) all appropriate security requirements are addressed in agency acquisitions of information systems and information system services; and (ii) all necessary security controls are implemented in agency information systems when determining the tailored and supplemented control baselines described in this publication.

See <http://csrc.nist.gov/sec-cert/ca-compliance.html> for additional information on compliance.



# Summary

“Control Systems Under Attack !?” — Dr. Stefan Lüders — July 19<sup>th</sup> 2010



**“Control Systems” go “IT”...**



**...but omitted security aspects!**



**Why worry? The Risk Equation**



**Mitigation: Today's Cacophony**