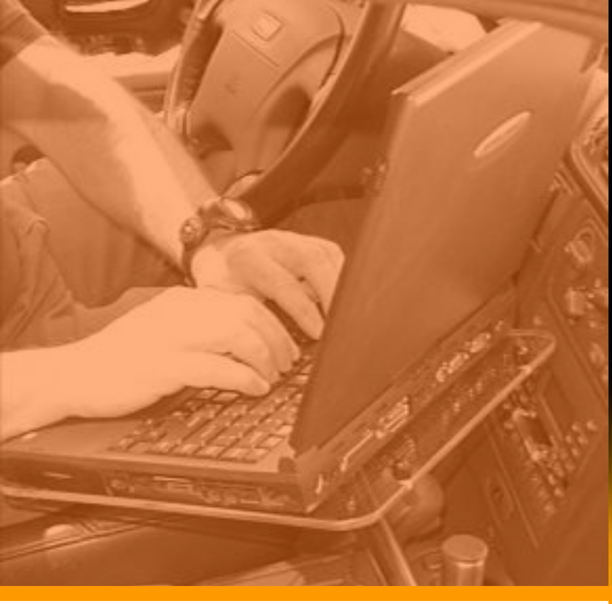


# Control Systems Under Attack !?

## …about the Cyber-Security of modern Control Systems

**Dr. Stefan Lüders (CERN Computer Security Officer)**

Openlab Summer Student Lectures

July 23rd 2012

# Security in a Nutshell

**Security is as good 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.**

- ► At CERN, every single computing resource owner defines ε !!!

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

# Security in a Nutshell

**Security is as good 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.**

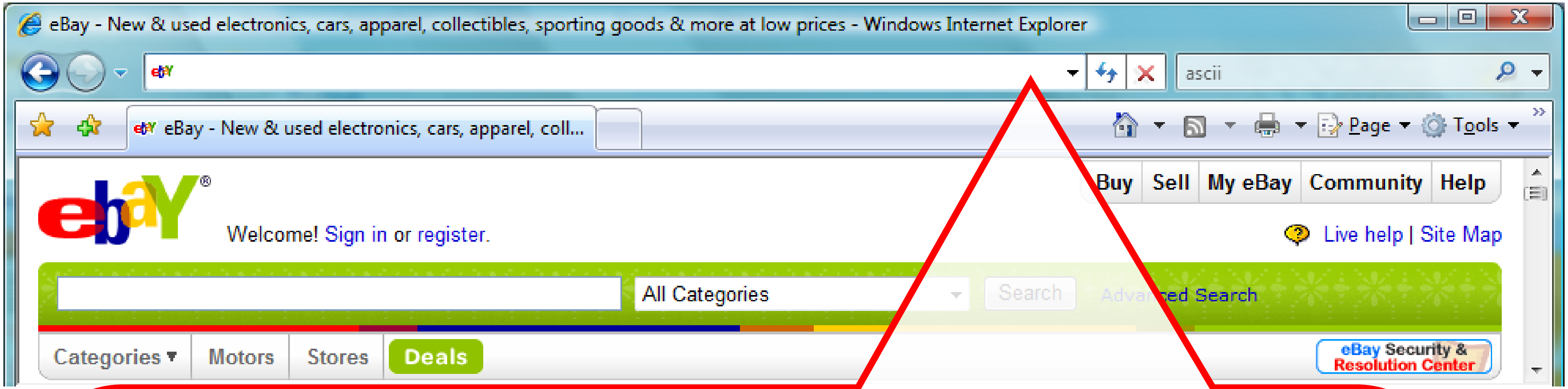
- ► At CERN, every single computing resource owner defines ε !!!

YOU are responsible for securing your services & systems:

- ► As user, developer, system expert or administrator
- ► As a project manager or line manager
- ► As part of the CERN or your experiment hierarchy

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

# Warm-Up: A small quiz


eBay - New & used electronics, cars, apparel, collectibles, sporting goods & more at low prices - Windows Internet Explorer
ebY
ascii
eBay - New & used electronics, cars, apparel, coll...
Page
Tools
ebY
Buy
Sell
My eBay
Community
Help
Welcome! Sign in or register.
Live help | Site Map
All Categories
Search
Advanced Search
Categories
Motors
Stores
Deals
eBay Security & Resolution Center

**What links to www.ebay.com?**

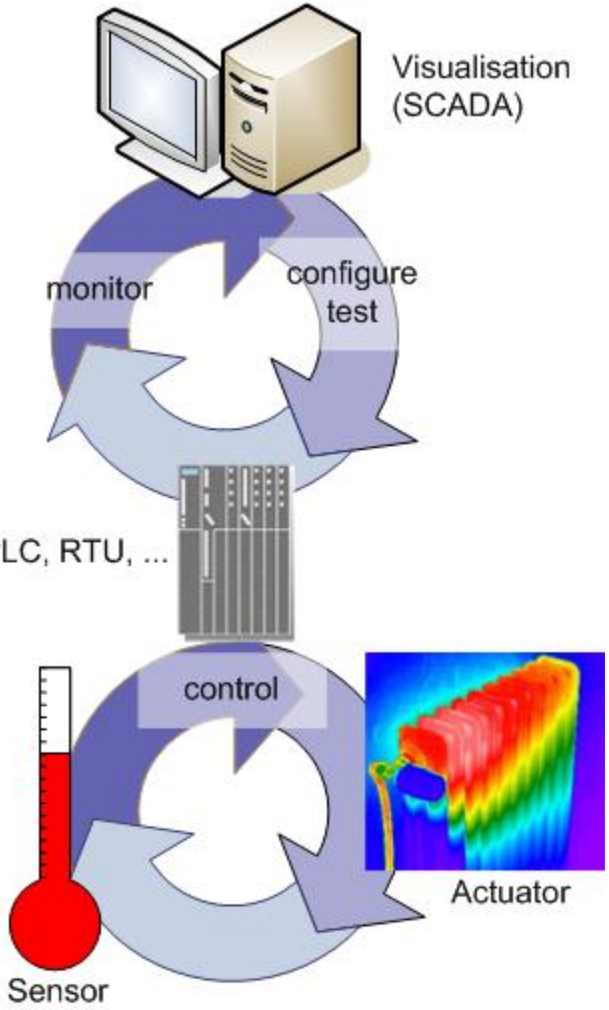
- ✘ http://www.ebay.com\cgi-bin\login?ds=1 %2e%31%33%38%2e%31%33%37%2
- ✘ http://www.ebay.com/ws/eBayISAPI.dll?
- ✓ http://scgi.ebay.com/ws/eBayISAPI.dll?l co_partnerid=2&usage=0&ru=http =0 &encRafId=default
- ✘ http://secure-ebay.com

100 % 100 % 100 %

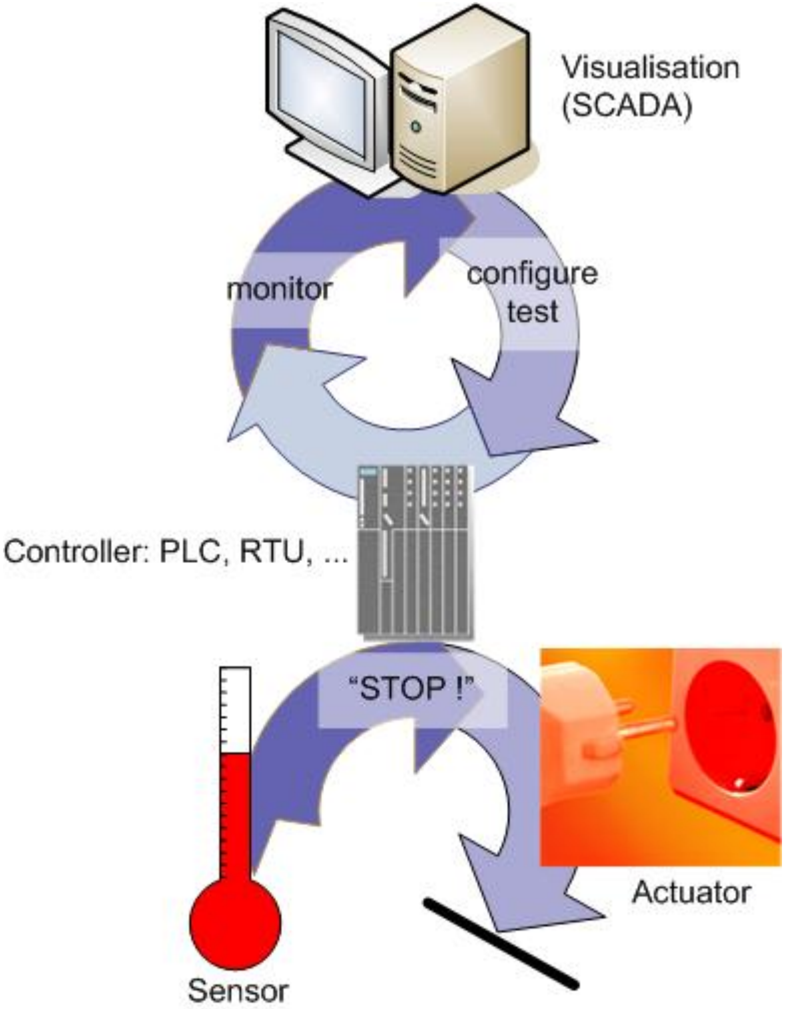
THIS IS NOT EVEN OBVIOUS FOR PROFESSIONALS!

# “Control Systems” in a Nutshell

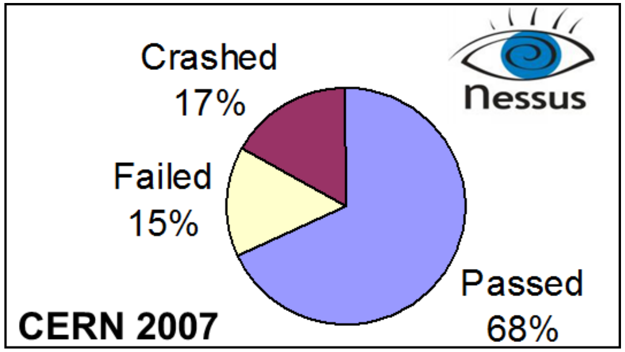
## Process Control System (PCS)

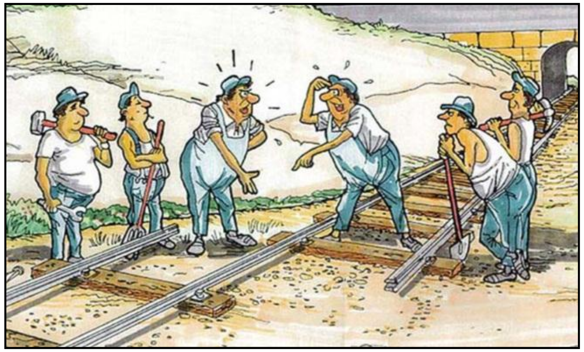


## Safety System



# Roadmap for Today





# “Control Systems” go “IT”...

## In the past, PCS were

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

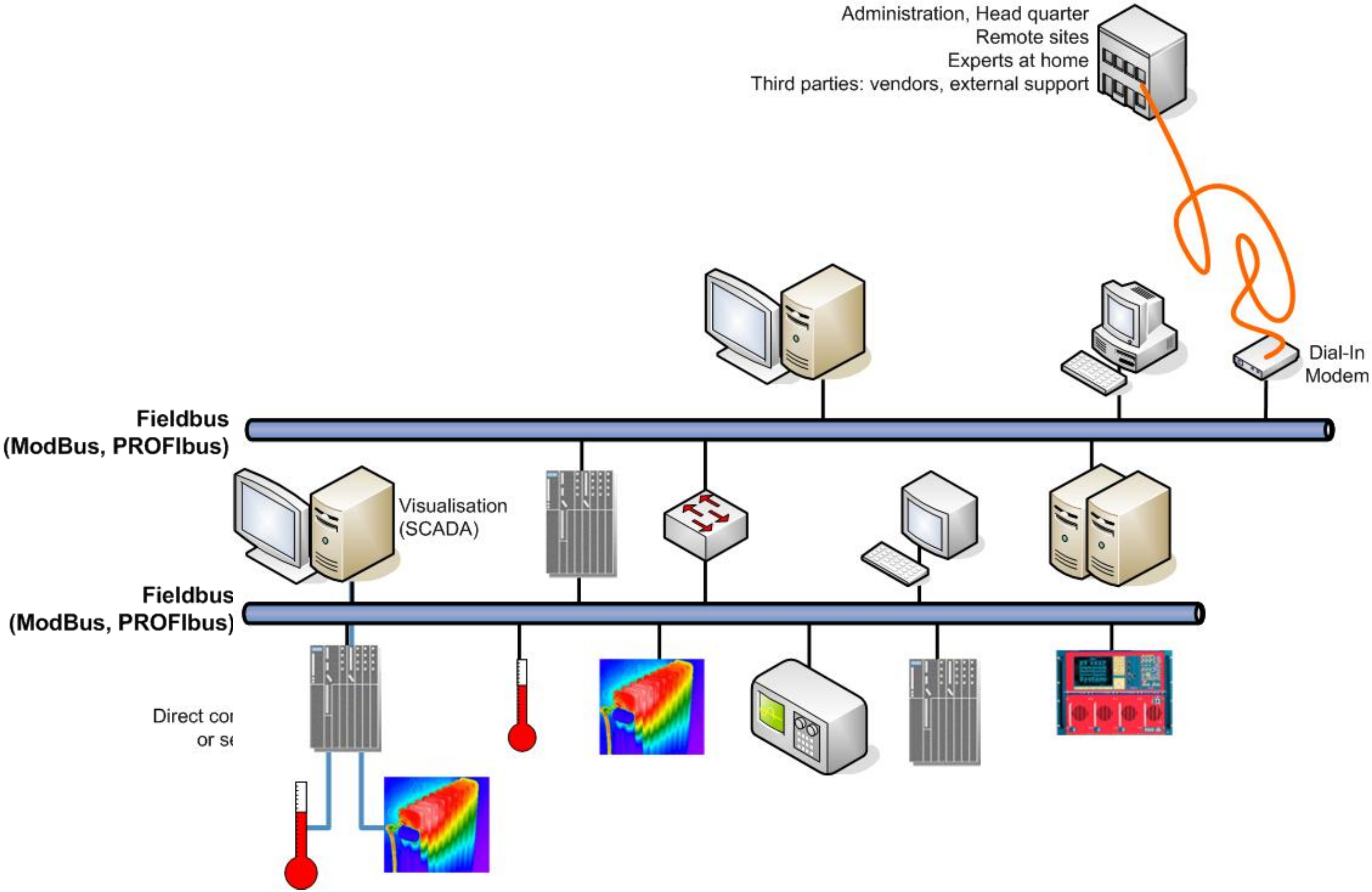
Created Exclusively for Automation.com
BREAK GLASS INCASE OF EMERGENCY

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

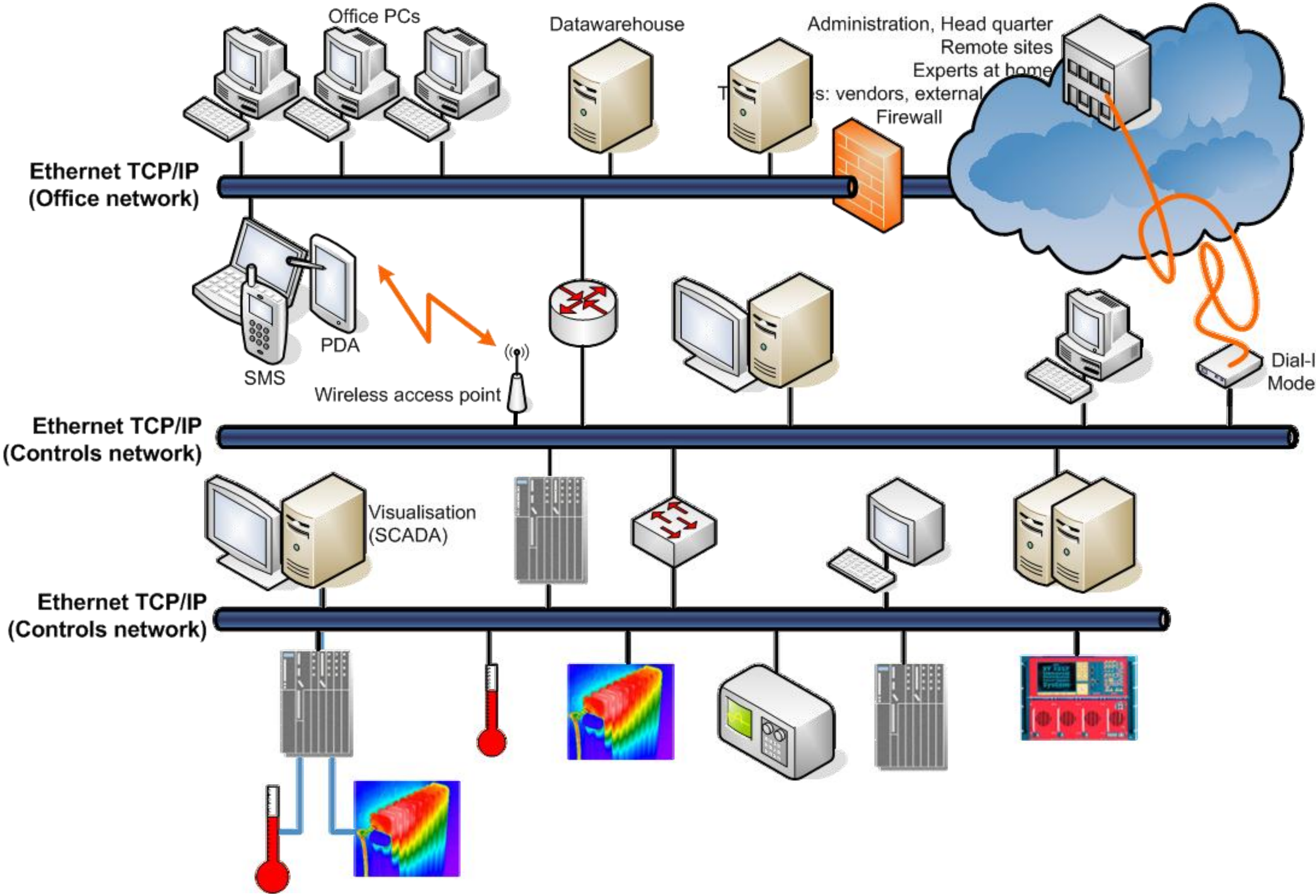
## Today, PCS

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

# (R)Evolution: The Past


Administration, Head quarter
Remote sites
Experts at home
Third parties: vendors, external support
Dial-In Modem
Fieldbus (ModBus, PROFIbus)
Visualisation (SCADA)
Fieldbus (ModBus, PROFIbus)
Direct cor
or se

# (R)Evolution: Today



# Control Systems for Living

- …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
- …for facility management
  e.g. [illegible]
- …for accelerator controls

COBB County Electric, Georgia

Middle European Raw Oil, Czech Republic

Athens Water Supply & Sewage

Merck Sharp & Dohme, Ireland

CCTV Control Room, UK

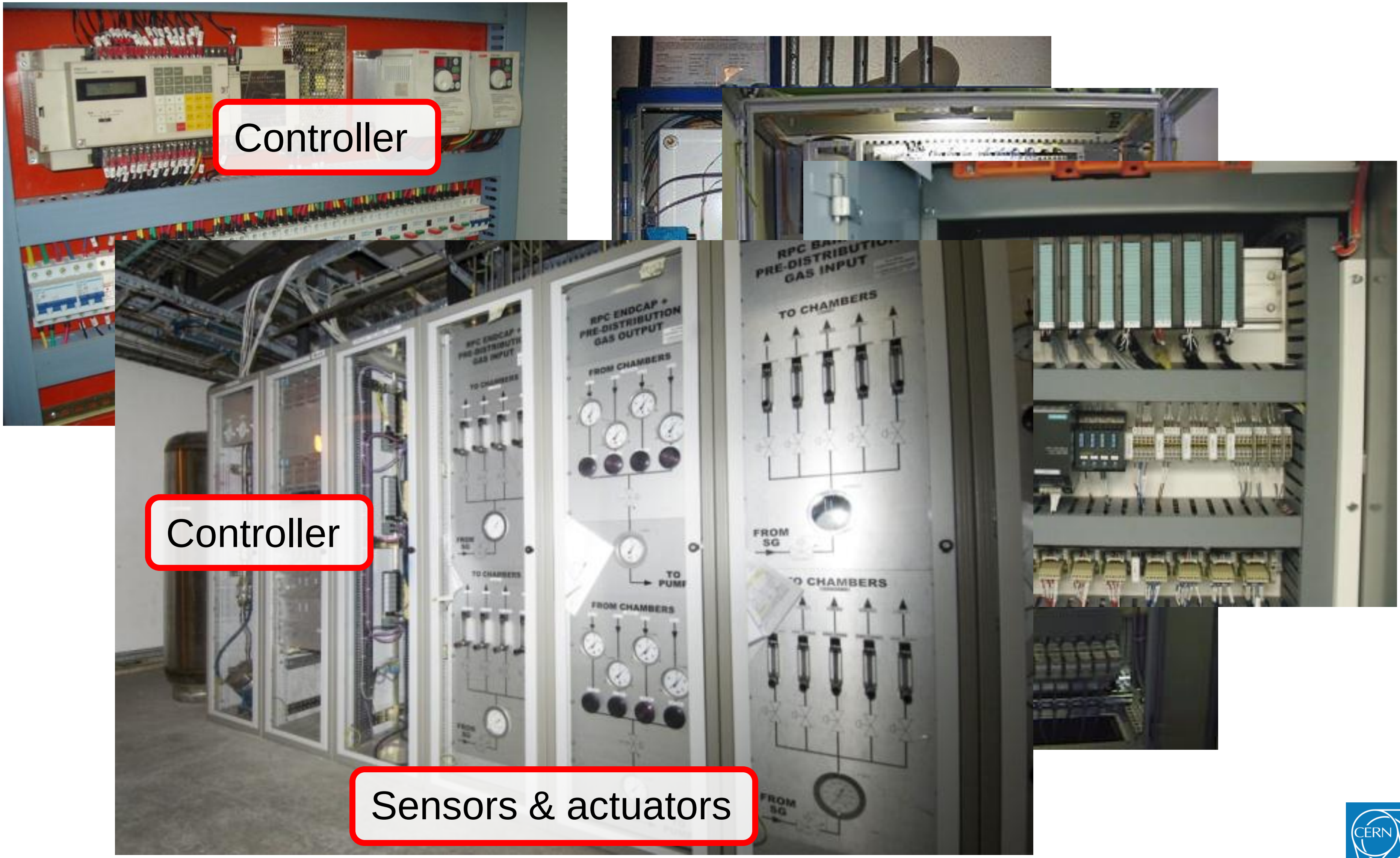
Reuters TV Master Control Room

CERN Control Centre

The claimed No. 1 goal for cyber-security in the 21st century:

**Critical Infrastructure Protection (CIP)**

# This is how PCS can look like


RPC ENDCAP + PRE-DISTRIBUTION GAS INPUT
TO CHAMBERS
FROM SG
RPC ENDCAP + PRE-DISTRIBUTION GAS OUTPUT
FROM CHAMBERS
TO PUMP
RPC BARREL PRE-DISTRIBUTION GAS INPUT

Controller

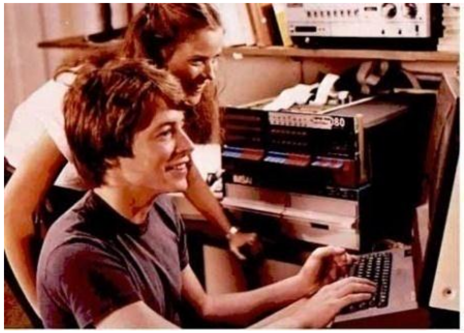
Controller

Sensors & actuators

# PCS omitted security aspects!

## In the past, PCS security was

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



## Today,

- ► Same “office IT”-risks inherent in PCS (TCP/IP, Windows PCs, WWW & mail, C++, …)
- ► Same “office IT”-attackers targeting PCS (viruses/worms, saboteurs, attacker, stupidity, …)

# Why worry? The Risk Equation

Risk =
Threat
× Vulnerability
× Consequence

# *Who* is the threat?

## Attacks performed by…

- Disgruntled (ex-)employees or saboteurs
- Attackers and terrorists, but also since “Stuxnet”: (Western) countries (step-by-step instructions on BlackHat conferences; freeware hacking tools for “Script Kiddies”)
- Trojans, viruses, worms, …

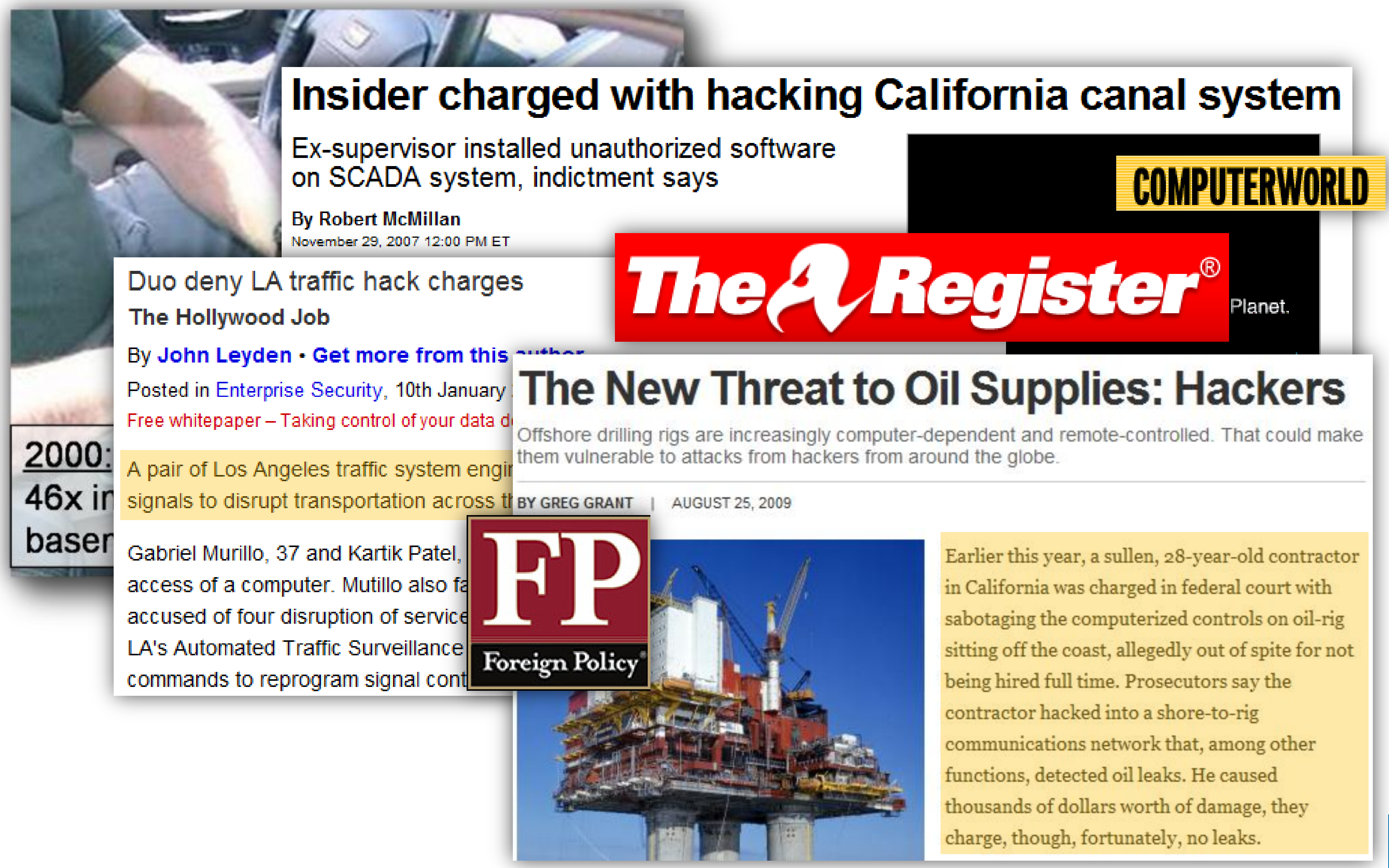
## Lack of robustness & lots of stupidity

- 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 Insiders?



2000:
46x in
baser

## Insider charged with hacking California canal system

Ex-supervisor installed unauthorized software on SCADA system, indictment says

By Robert McMillan
November 29, 2007 12:00 PM ET

COMPUTERWORLD

The Register®

Planet.

## Duo deny LA traffic hack charges

**The Hollywood Job**

By John Leyden • Get more from this author

Posted in Enterprise Security, 10th January

Free whitepaper – Taking control of your data d

A pair of Los Angeles traffic system engi
signals to disrupt transportation across th

Gabriel Murillo, 37 and Kartik Patel,
access of a computer. Mutillo also fa
accused of four disruption of service
LA's Automated Traffic Surveillance
commands to reprogram signal cont

FP
Foreign Policy®

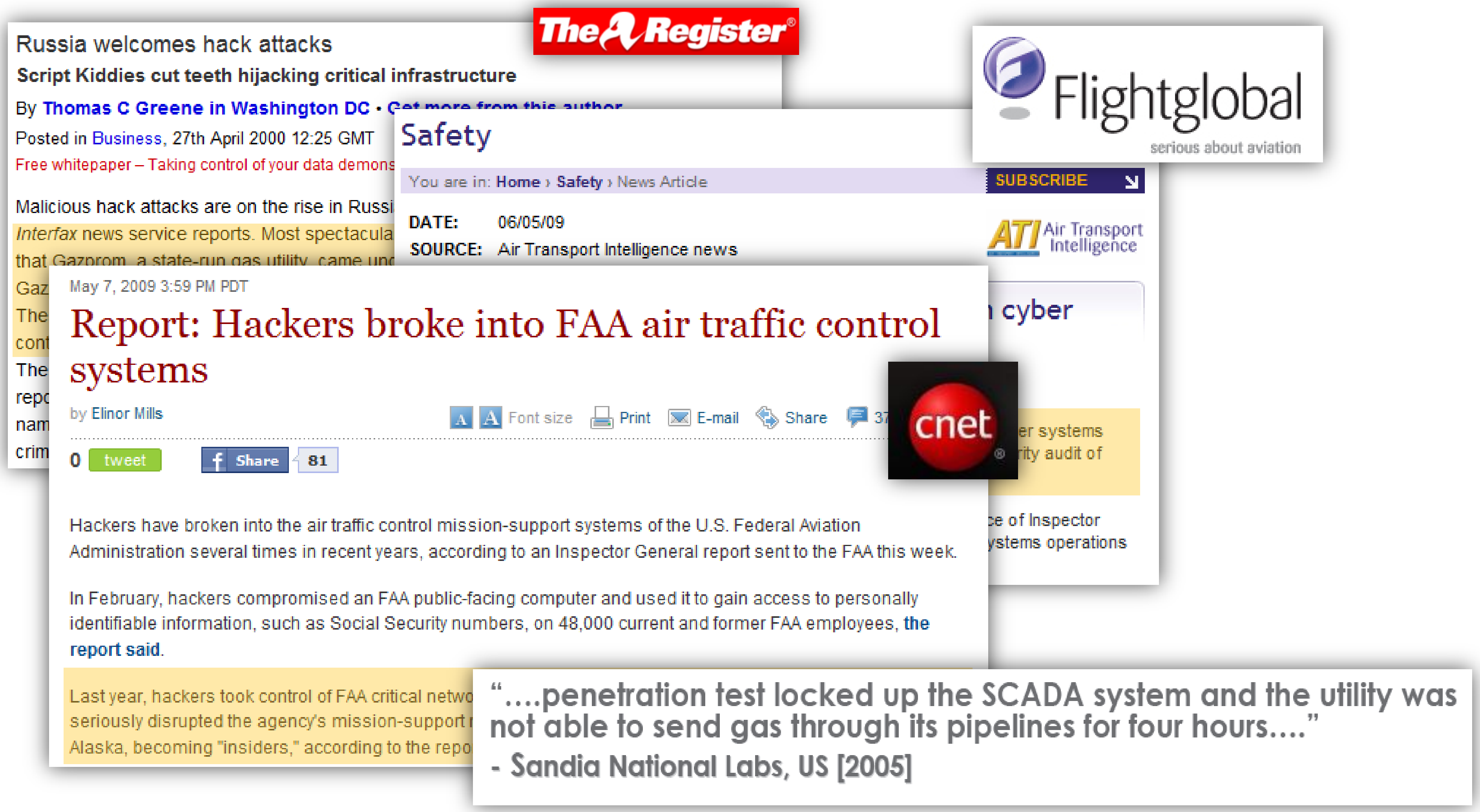
## The New Threat to Oil Supplies: Hackers

Offshore drilling rigs are increasingly computer-dependent and remote-controlled. That could make them vulnerable to attacks from hackers from around the globe.

BY GREG GRANT | AUGUST 25, 2009

Earlier this year, a sullen, 28-year-old contractor in California was charged in federal court with sabotaging the computerized controls on oil-rig sitting off the coast, allegedly out of spite for not being hired full time. Prosecutors say the contractor hacked into a shore-to-rig communications network that, among other functions, detected oil leaks. He caused thousands of dollars worth of damage, they charge, though, fortunately, no leaks.

# Damage by Attacker?



The Register®

Russia welcomes hack attacks

**Script Kiddies cut teeth hijacking critical infrastructure**

By Thomas C Greene in Washington DC • Get more from this author

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 Russi

*Interfax* news service reports. Most spectacula

that Gazprom, a state-run gas utility, came und

Gaz

The

cont

The

repo

nam

crim

Flightglobal

serious about aviation

Safety

You are in: Home › Safety › News Article

SUBSCRIBE

DATE: 06/05/09

SOURCE: Air Transport Intelligence news

ATI Air Transport Intelligence

n cyber

er systems

rity audit of

ce of Inspector

ystems operations

May 7, 2009 3:59 PM PDT

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

by Elinor Mills

A A Font size Print E-mail Share 37

0 tweet Share 81

cnet

Hackers have broken into the air traffic control mission-support systems of the U.S. Federal Aviation Administration several times in recent years, according to an Inspector General report sent to the FAA this week.

In February, hackers compromised an FAA public-facing computer and used it to gain access to personally identifiable information, such as Social Security numbers, on 48,000 current and former FAA employees, the report said.

Last year, hackers took control of FAA critical netwo

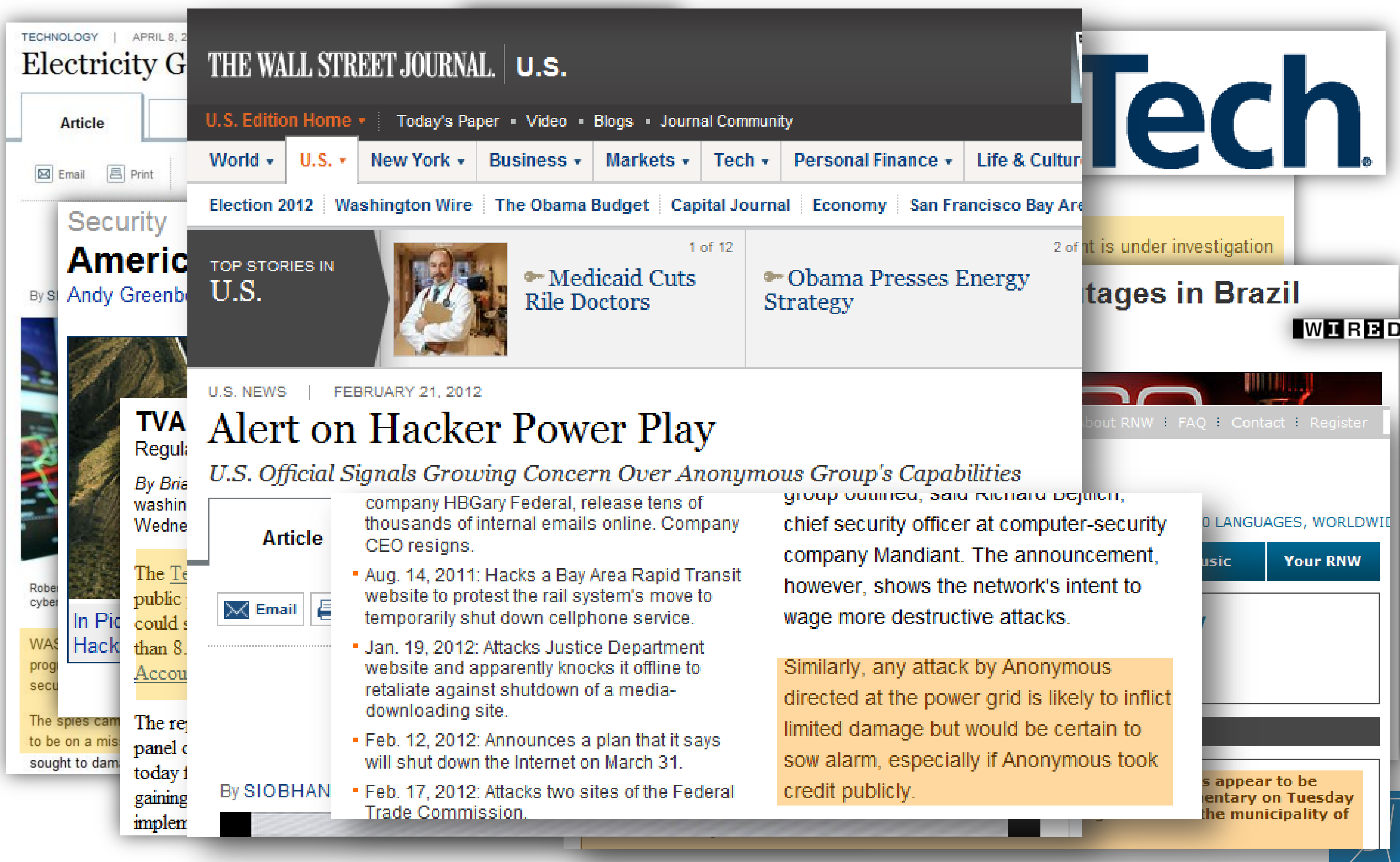
seriously disrupted the agency's mission-support

Alaska, becoming "insiders," according to the repo

“….penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours….”

- Sandia National Labs, US [2005]

# Damage due to CI No-P?



THE WALL STREET JOURNAL. | U.S.

U.S. Edition Home ▾ | Today's Paper • Video • Blogs • Journal Community

World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life & Cultur

Election 2012 | Washington Wire | The Obama Budget | Capital Journal | Economy | San Francisco Bay Are

TOP STORIES IN U.S.

1 of 12 Medicaid Cuts Rile Doctors

2 of Obama Presses Energy Strategy

U.S. NEWS | FEBRUARY 21, 2012

## Alert on Hacker Power Play

*U.S. Official Signals Growing Concern Over Anonymous Group's Capabilities*

Article

Email

By SIOBHAN

company HBGary Federal, release tens of thousands of internal emails online. Company CEO resigns.

- Aug. 14, 2011: Hacks a Bay Area Rapid Transit website to protest the rail system's move to temporarily shut down cellphone service.
- Jan. 19, 2012: Attacks Justice Department website and apparently knocks it offline to retaliate against shutdown of a media-downloading site.
- Feb. 12, 2012: Announces a plan that it says will shut down the Internet on March 31.
- Feb. 17, 2012: Attacks two sites of the Federal Trade Commission.

group outlined, said Richard Bejtlich, chief security officer at computer-security company Mandiant. The announcement, however, shows the network's intent to wage more destructive attacks.

Similarly, any attack by Anonymous directed at the power grid is likely to inflict limited damage but would be certain to sow alarm, especially if Anonymous took credit publicly.

TECHNOLOGY | APRIL 8, 2

Electricity G

Article

Email Print

Security

Americ

By S

Andy Greenb

In Pic

Hack

Robe

cyber

WAS

prog

secu

The spies cam

to be on a mis

sought to dam

TVA

Regul

By Bria

washin

Wedne

The Te

public

could

than 8

Accou

The re

panel

today

gaining

implem

Tech®

nt is under investigation

tages in Brazil

WIRED

bout RNW : FAQ : Contact : Register

0 LANGUAGES, WORLDWID

usic

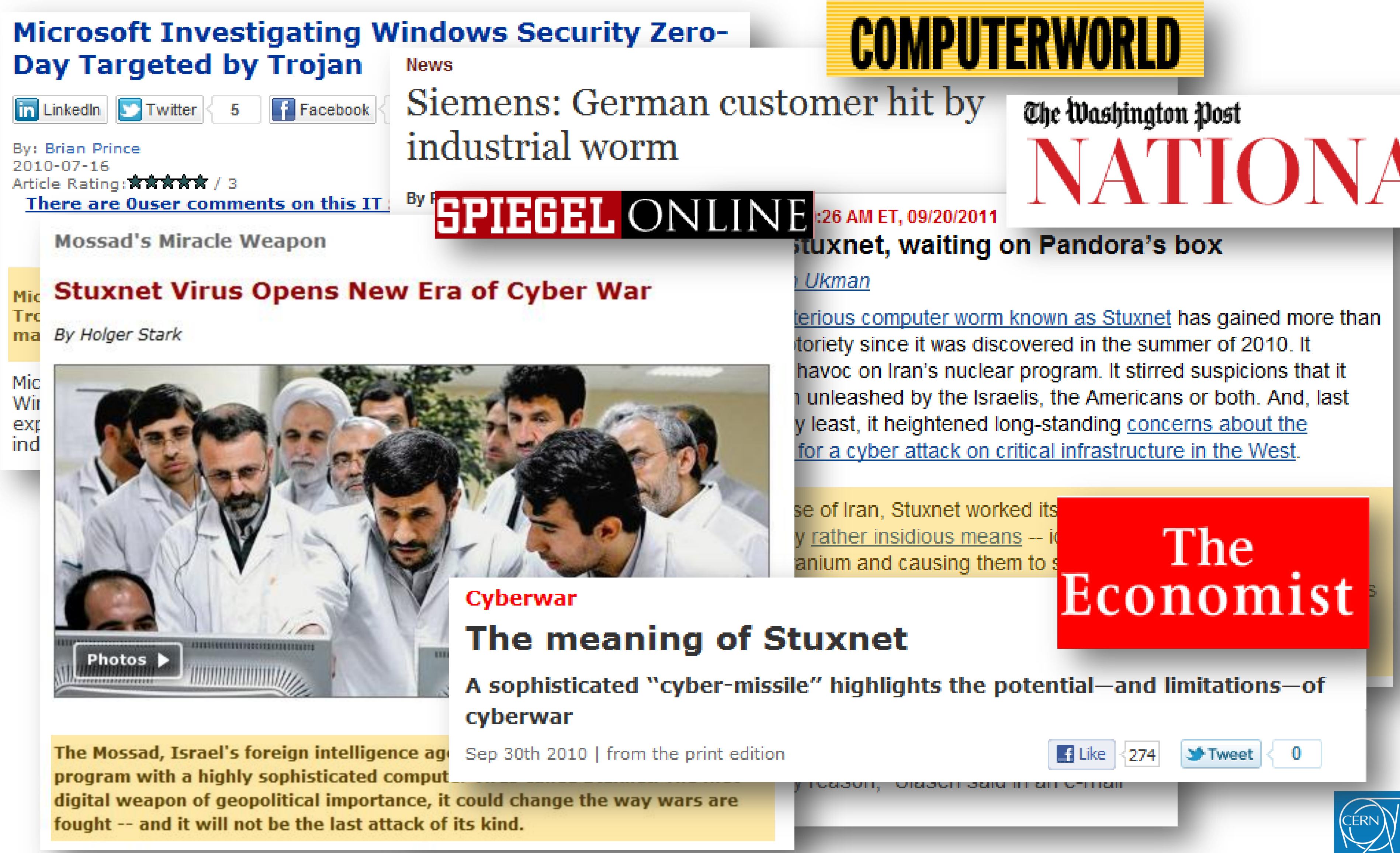
Your RNW

s appear to be

entary on Tuesday

the municipality of

# Natanz, we have a problem.



## Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn Twitter 5 Facebook

By: Brian Prince
2010-07-16
Article Rating: ★★★★★ / 3
There are 0user comments on this IT

Mic
Tro
ma

Mic
Wi
exp
ind

COMPUTERWORLD

News

## Siemens: German customer hit by industrial worm

By

The Washington Post

NATIONA

:26 AM ET, 09/20/2011

## tuxnet, waiting on Pandora’s box

Ukman

terious computer worm known as Stuxnet has gained more than toriety since it was discovered in the summer of 2010. It havoc on Iran’s nuclear program. It stirred suspicions that it unleashed by the Israelis, the Americans or both. And, last y least, it heightened long-standing concerns about the for a cyber attack on critical infrastructure in the West.

se of Iran, Stuxnet worked its
y rather insidious means -- i
anium and causing them to

y reason,” Glasen said in an e-mail

SPIEGEL ONLINE

Mossad's Miracle Weapon

## Stuxnet Virus Opens New Era of Cyber War

*By Holger Stark*

The Mossad, Israel's foreign intelligence ag program with a highly sophisticated comput digital weapon of geopolitical importance, it could change the way wars are fought -- and it will not be the last attack of its kind.

The Economist

Cyberwar

## The meaning of Stuxnet

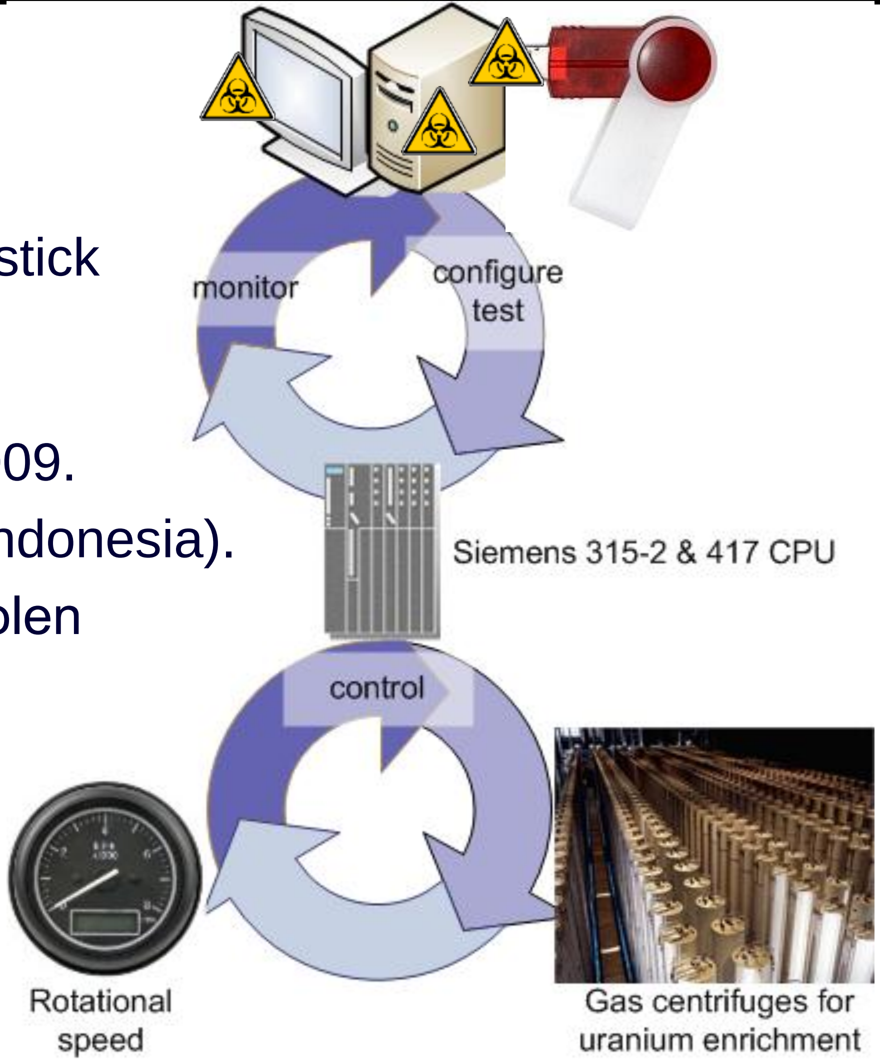
A sophisticated “cyber-missile” highlights the potential—and limitations—of cyberwar

Sep 30th 2010 | from the print edition

Like 274 Tweet 0

# The Workings of Stuxnet (I)

- An infected USB stick was infiltrated into the plant either by malicious act or through social engineering.
- Once inserted into a Windows PC, the stick tried to compromize the O/S with up to 4(!) zero-day exploits (worth >$100k).
- There were 4-5 evolutions starting 6/2009.
- Infected 100.000 PCs (60% Iran,10% Indonesia).
- Using "rootkit" technologies and two stolen certificates, it hid from being detected.
- It tried to infect other hosts and establish a P2P connection "home".

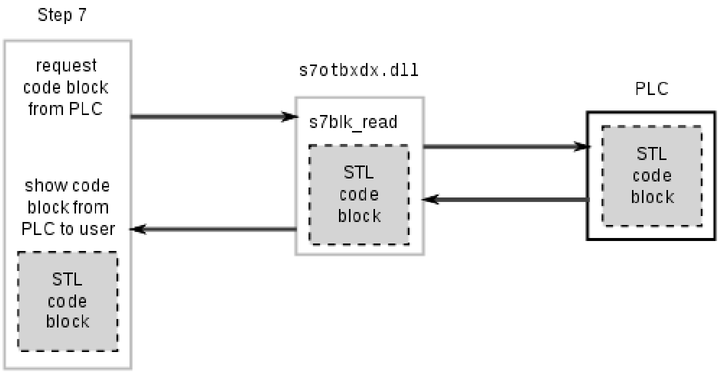


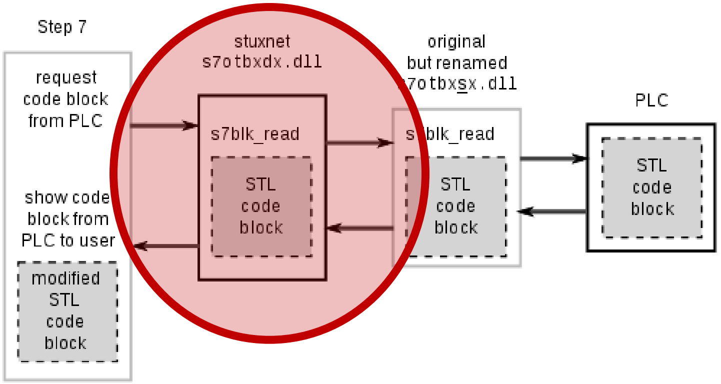
**So far, nothing new:
A standard,
but expensive virus!**

# The Workings of Stuxnet (II)

- Stuxnet then checked the local configuration looking for the presence of Siemens PCS7/STEP7/WINCC SCADA software.
- If so, it copied itself into the local STEP7 project folder (to propagate further).
- It replaced the S7 communication libraries (DLLs) used for exchanging data with a PLC.
- Stuxnet can now manipulate values to be send to the PLC or displayed by the SCADA.

**Stuxnet is now the "Man in the Middle" controlling the communication between SCADA & PLC.**





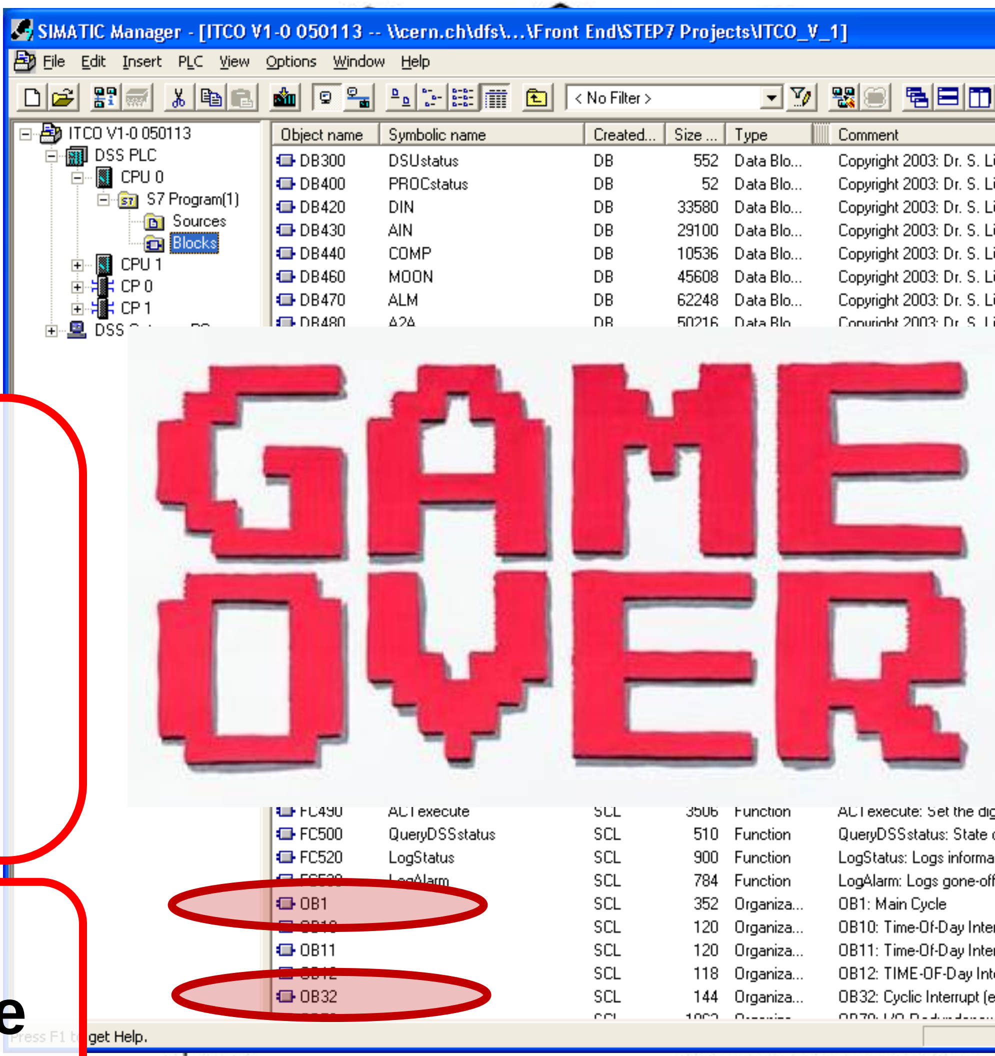
- If not, Stuxnet got idle and would expire on 2012/06/24.

# The Workings of Stuxnet (III)

- Next, Stuxnet was "fingerprinting" connected PLCs.
- If right PLC configuration, it downloaded/replaced code between 17 and 32 FBs & DBs.

**This code varied the rotational speed of the centrifuges over months wearing them out and inhibiting uranium enrichment.**

**The "Man in the Middle" made everything looked fine at the SCADA level…**

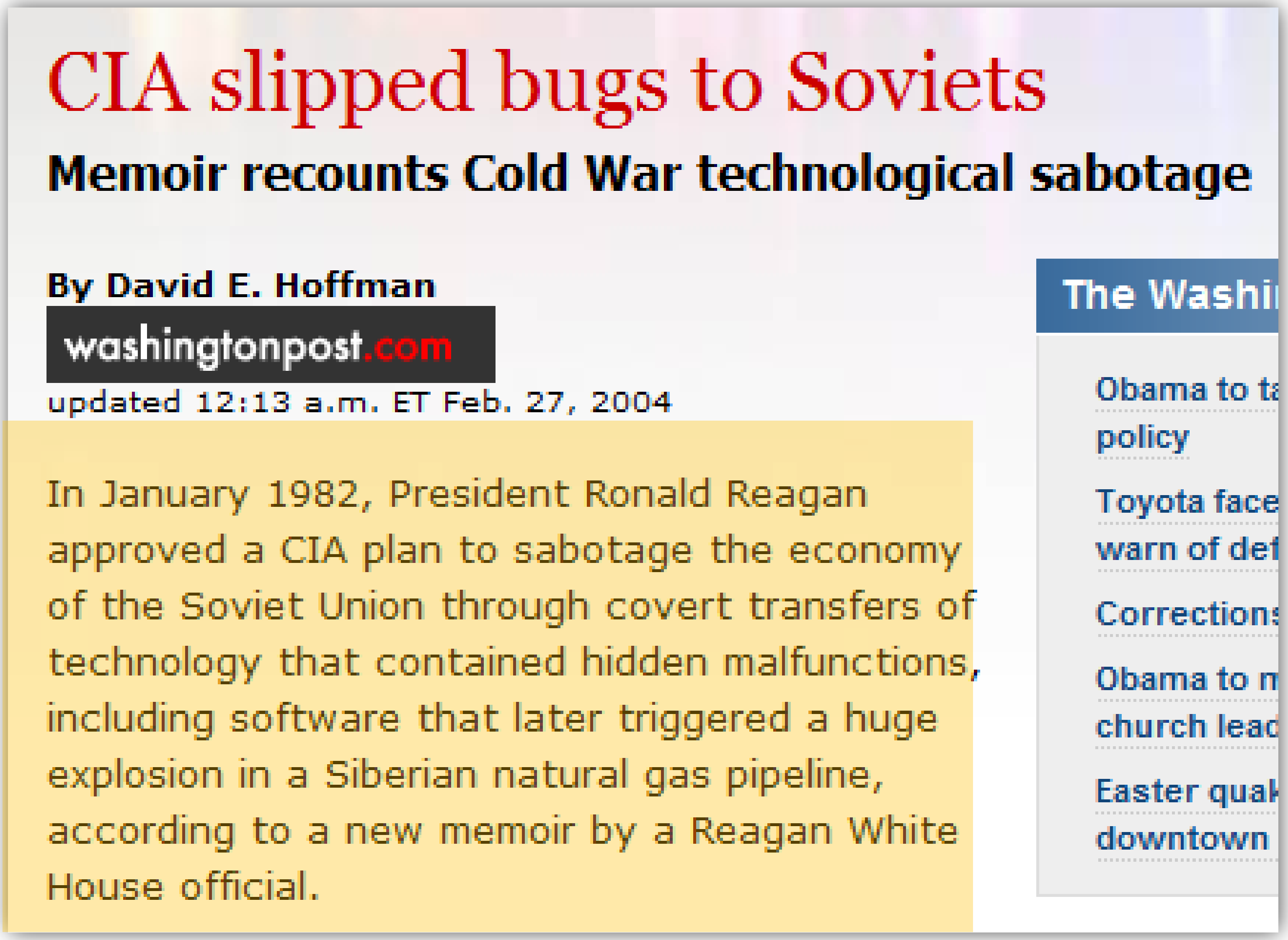


SIMATIC Manager - [ITCO V1-0 050113 -- \\cern.ch\dfs\...\Front End\STEP7 Projects\ITCO_V_1]

| Object name | Symbolic name | Created... | Size ... | Type | Comment |
|---|---|---|---|---|---|
| DB300 | DSUstatus | DB | 552 | Data Blo... | Copyright 2003: Dr. S. Li |
| DB400 | PROCstatus | DB | 52 | Data Blo... | Copyright 2003: Dr. S. Li |
| DB420 | DIN | DB | 33580 | Data Blo... | Copyright 2003: Dr. S. Li |
| DB430 | AIN | DB | 29100 | Data Blo... | Copyright 2003: Dr. S. Li |
| DB440 | COMP | DB | 10536 | Data Blo... | Copyright 2003: Dr. S. Li |
| DB460 | MOON | DB | 45608 | Data Blo... | Copyright 2003: Dr. S. Li |
| DB470 | ALM | DB | 62248 | Data Blo... | Copyright 2003: Dr. S. Li |
| DB480 | A2A | DB | 50216 | Data Blo... | Copyright 2003: Dr. S. Li |
| FC490 | ACTexecute | SCL | 3506 | Function | ACTexecute: Set the dig |
| FC500 | QueryDSSstatus | SCL | 510 | Function | QueryDSSstatus: State c |
| FC520 | LogStatus | SCL | 900 | Function | LogStatus: Logs informa |
| FC530 | LogAlarm | SCL | 784 | Function | LogAlarm: Logs gone-off |
| OB1 | | SCL | 352 | Organiza... | OB1: Main Cycle |
| OB10 | | SCL | 120 | Organiza... | OB10: Time-Of-Day Inter |
| OB11 | | SCL | 120 | Organiza... | OB11: Time-Of-Day Inter |
| OB12 | | SCL | 118 | Organiza... | OB12: TIME-OF-Day Inte |
| OB32 | | SCL | 144 | Organiza... | OB32: Cyclic Interrupt (e |
| [illegible] | | SCL | 1062 | Organiza... | OB70: I/O Redundancy |

Press F1 to get Help.

# Stuxnet was not the first one!



## CIA slipped bugs to Soviets

### Memoir recounts Cold War technological sabotage

By David E. Hoffman

washingtonpost.com

updated 12:13 a.m. ET Feb. 27, 2004

In January 1982, President Ronald Reagan approved a CIA plan to sabotage the economy of the Soviet Union through covert transfers of technology that contained hidden malfunctions, including software that later triggered a huge explosion in a Siberian natural gas pipeline, according to a new memoir by a Reagan White House official.

The Washi

Obama to ta policy

Toyota face warn of def

Correction

Obama to m church lead

Easter quak downtown

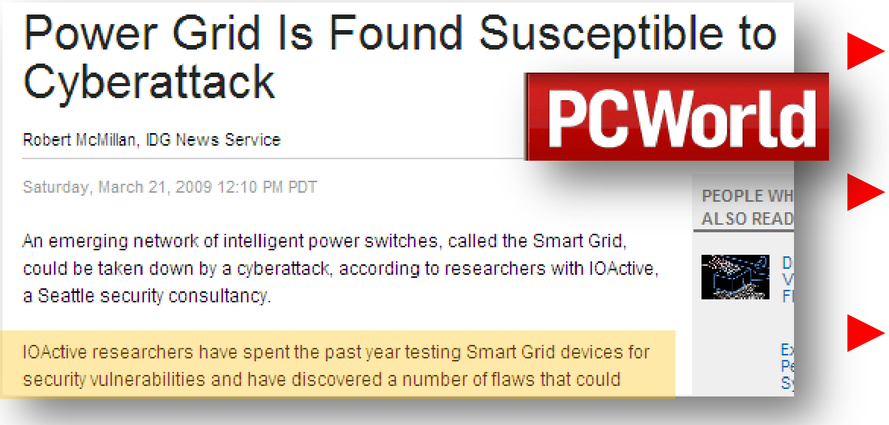
# Smart Meters: Nothing Learned?

## 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.

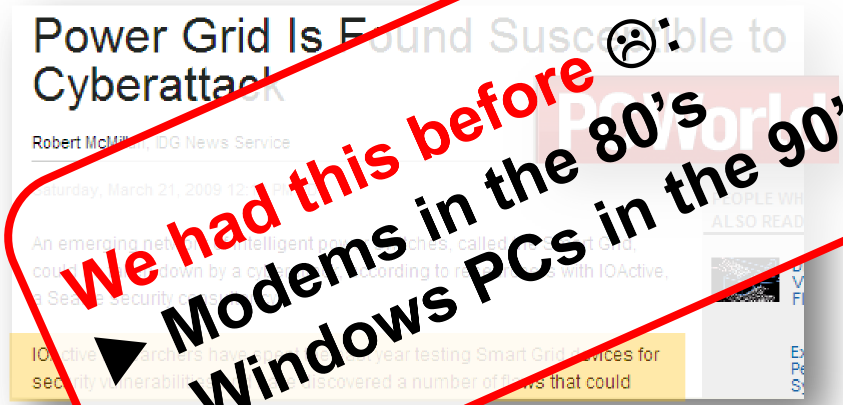
IOActive researchers have spent the past year testing Smart Grid devices for security vulnerabilities and have discovered a number of flaws that could

courtesy of M. Tritschler (KEMA)

# Smart Meters: Nothing Learned?

## Use case:

- ▶ Measuring your consumption at h
- ▶ Online with the grid: Optimi e
- ▶ Publicly accessible, off-th



Power Grid Is Found Susceptible to Cyberattack

Robert McMillan, IDG News Service

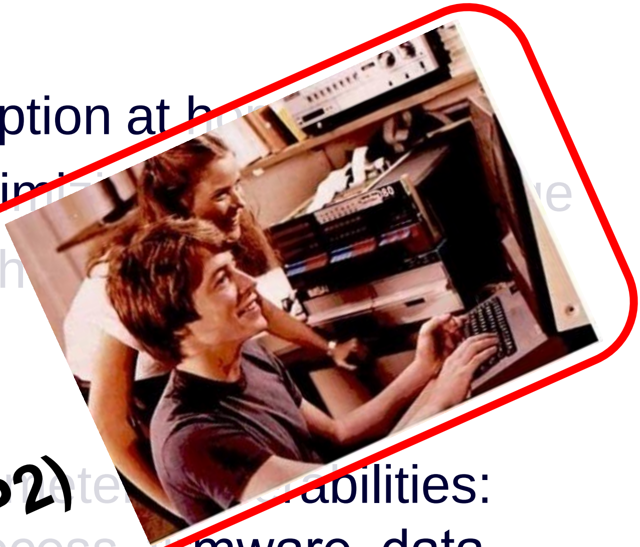
Saturday, March 21, 2009 12:1 PM

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

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

We had this before ☹:

- ▶ Modems in the 80’s
- ▶ Windows PCs in the 90’s (before XP SP2)

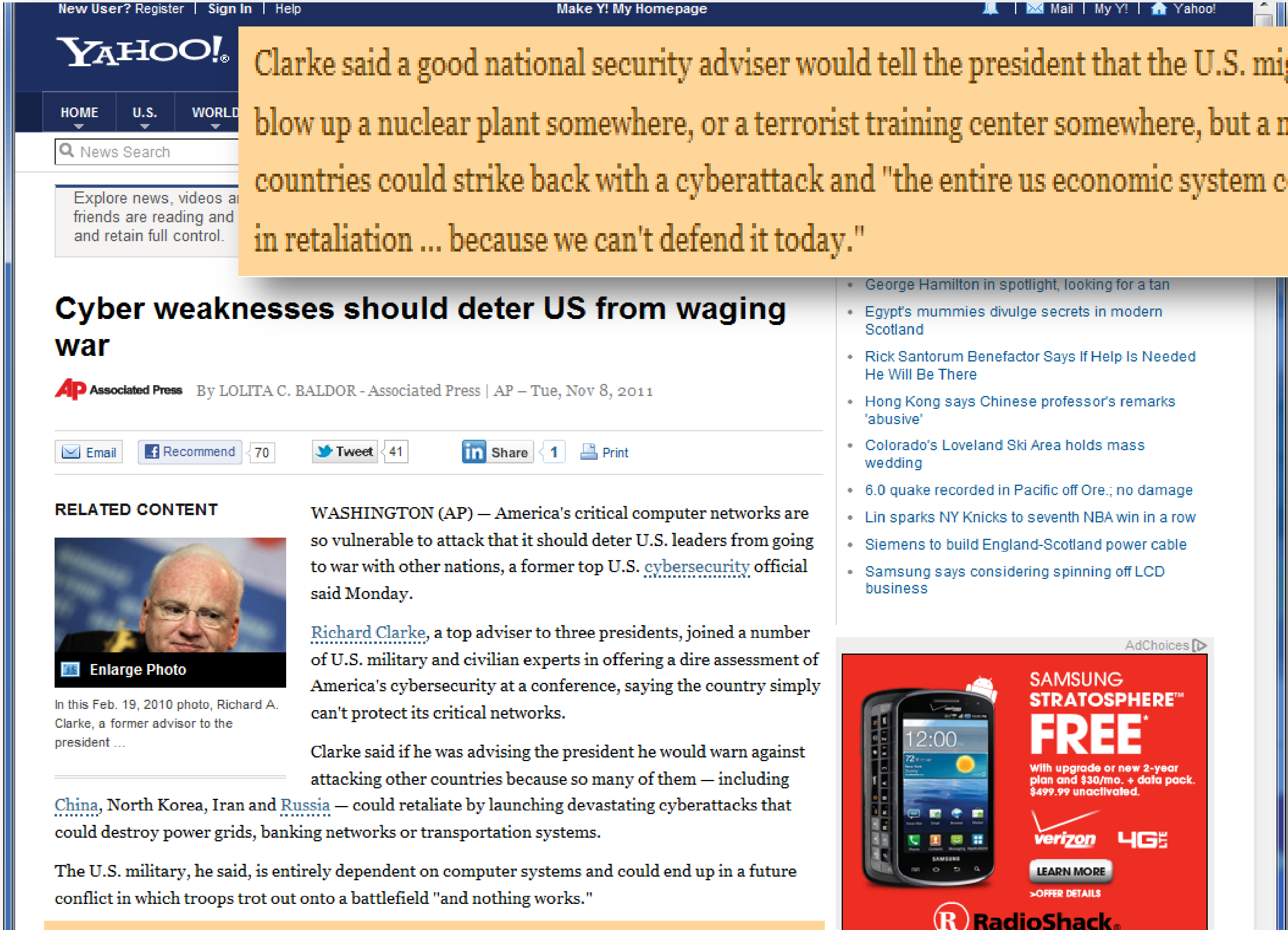


## Risks:

- ▶ Exploitation of meter abilities: 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

courtesy of M. Tritschler (KEMA)

# Why care?



Explore news, videos a… friends are reading and… and retain full control.

> Clarke said a good national security adviser would tell the president that the U.S. might be able to blow up a nuclear plant somewhere, or a terrorist training center somewhere, but a number of countries could strike back with a cyberattack and "the entire us economic system could be crashed in retaliation … because we can't defend it today."

## Cyber weaknesses should deter US from waging war

Associated Press By LOLITA C. BALDOR - Associated Press | AP – Tue, Nov 8, 2011

RELATED CONTENT

In this Feb. 19, 2010 photo, Richard A. Clarke, a former advisor to the president ...

WASHINGTON (AP) — America's critical computer networks are so vulnerable to attack that it should deter U.S. leaders from going to war with other nations, a former top U.S. cybersecurity official said Monday.

Richard Clarke, a top adviser to three presidents, joined a number of U.S. military and civilian experts in offering a dire assessment of America's cybersecurity at a conference, saying the country simply can't protect its critical networks.

Clarke said if he was advising the president he would warn against attacking other countries because so many of them — including China, North Korea, Iran and Russia — could retaliate by launching devastating cyberattacks that could destroy power grids, banking networks or transportation systems.

The U.S. military, he said, is entirely dependent on computer systems and could end up in a future conflict in which troops trot out onto a battlefield "and nothing works."

- George Hamilton in spotlight, looking for a tan
- Egypt's mummies divulge secrets in modern Scotland
- Rick Santorum Benefactor Says If Help Is Needed He Will Be There
- Hong Kong says Chinese professor's remarks 'abusive'
- Colorado's Loveland Ski Area holds mass wedding
- 6.0 quake recorded in Pacific off Ore.; no damage
- Lin sparks NY Knicks to seventh NBA win in a row
- Siemens to build England-Scotland power cable
- Samsung says considering spinning off LCD business

# Mitigation: Today’s Cacophony

**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 your vendor!!!

**Too many stakeholders:**

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

# 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..."

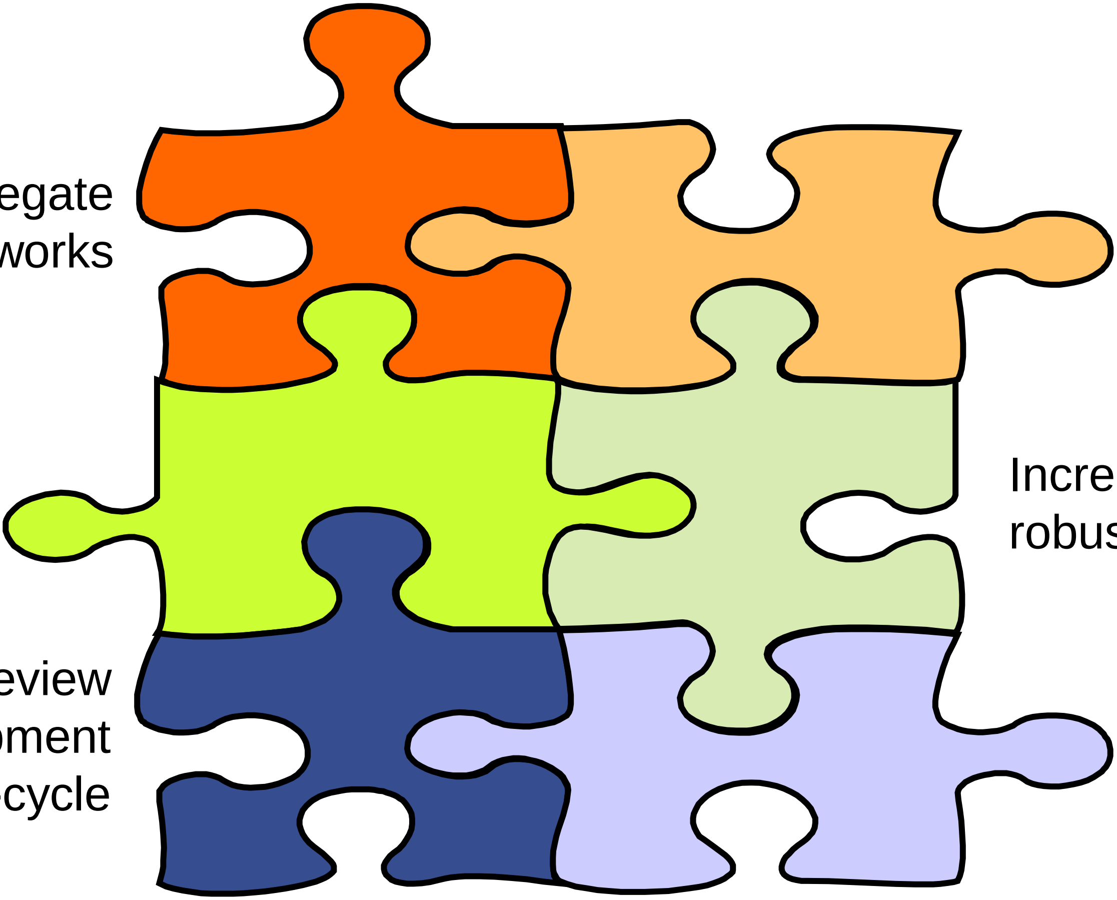
"More and better gadgets can solve security problems..."

"Everything can be solved by technique !"

# Ground Rules for Cyber-Security

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

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



Segregate networks

Patch, patch, patch!!!

Control (remote) access

Increase robustness

Review development life-cycle

Deepen collaboration & policies

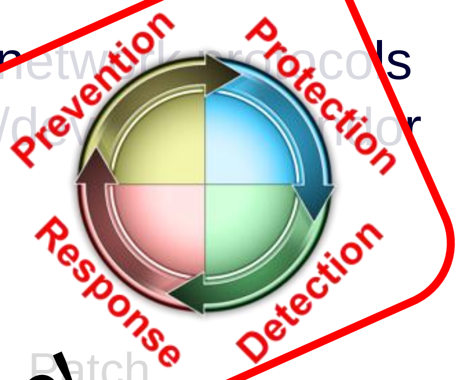
# Ground Rules for Cyber-Security

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

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

**Control Systems use COTS IT hard/software.**

**Control System Cyber-Security must employ/allow for COTS IT security measures, too!**

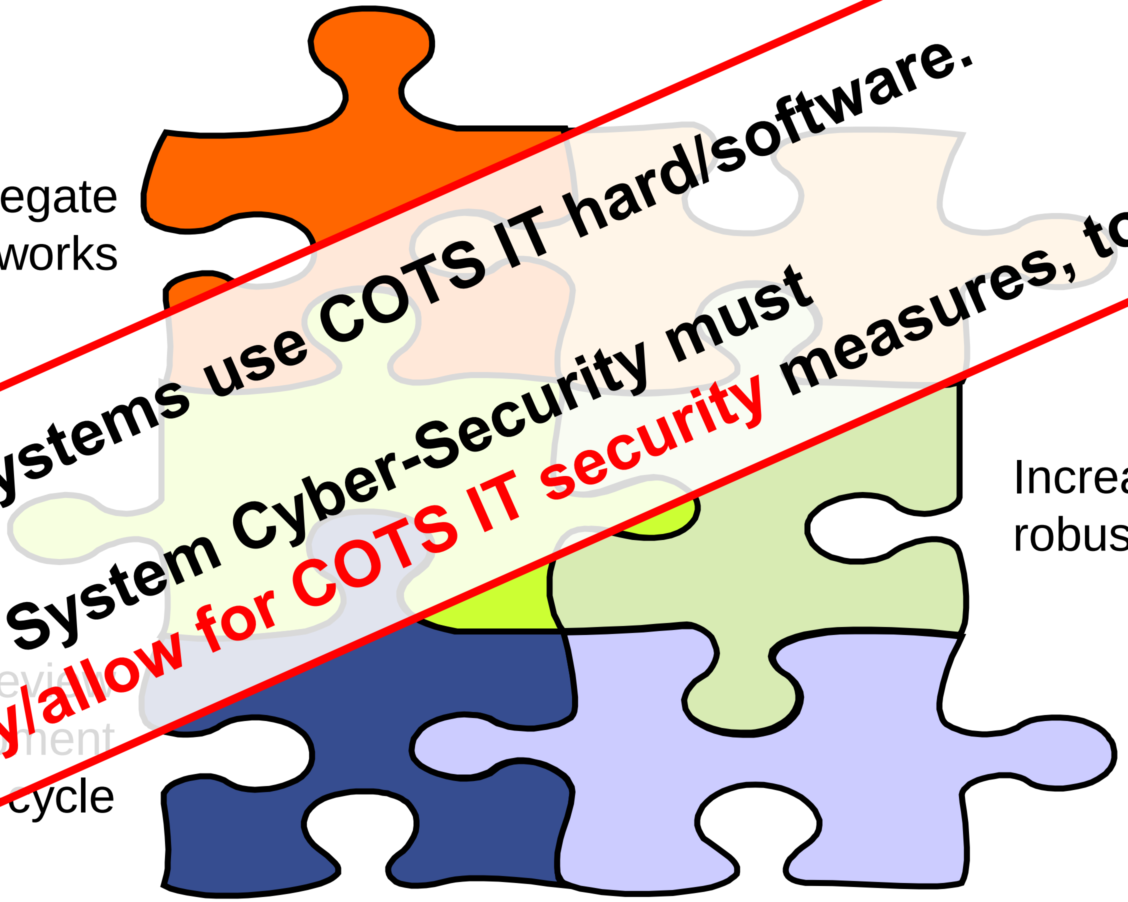


Prevention

Protection

Detection

Response



Segregate networks

Control (remote) access

Review development life-cycle

Patch, patch, patch!!!

Increase robustness

Deepen collaboration & policies

# Damage due to Interconnectivity?

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

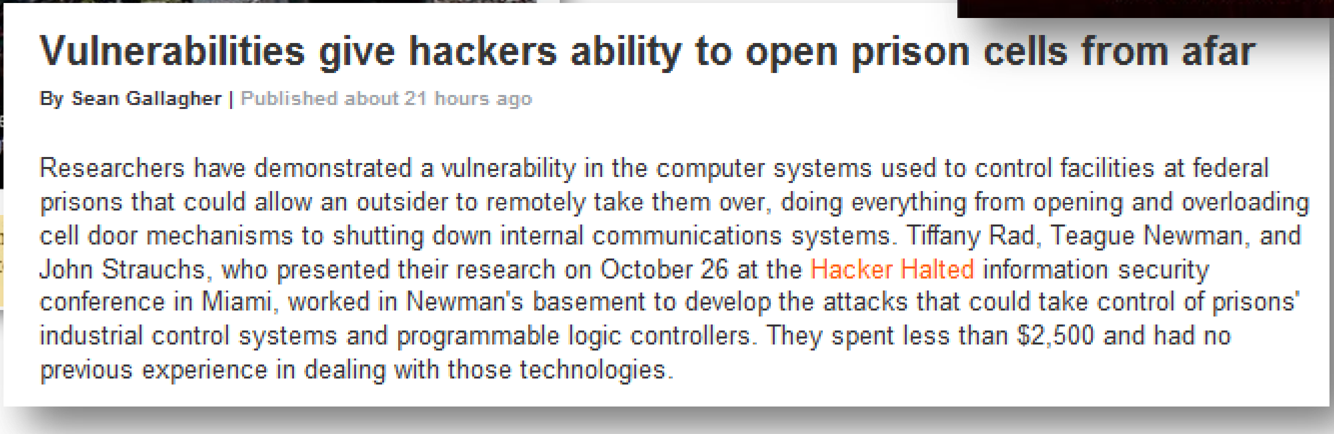
WIRED

By Kim Zetter 01.04.08

The Boeing 787 Dreamliner aircraft makes its public de
outside the Boeing assembly plant in Everett, Washing
*Photo: Robert Sorbo / Corbis*

Boeing's new 787 Dreamliner passenger jet may h
computer networks that could allow passengers t
the U.S. Federal Aviation Administration.

ars technica



## Vulnerabilities give hackers ability to open prison cells from afar

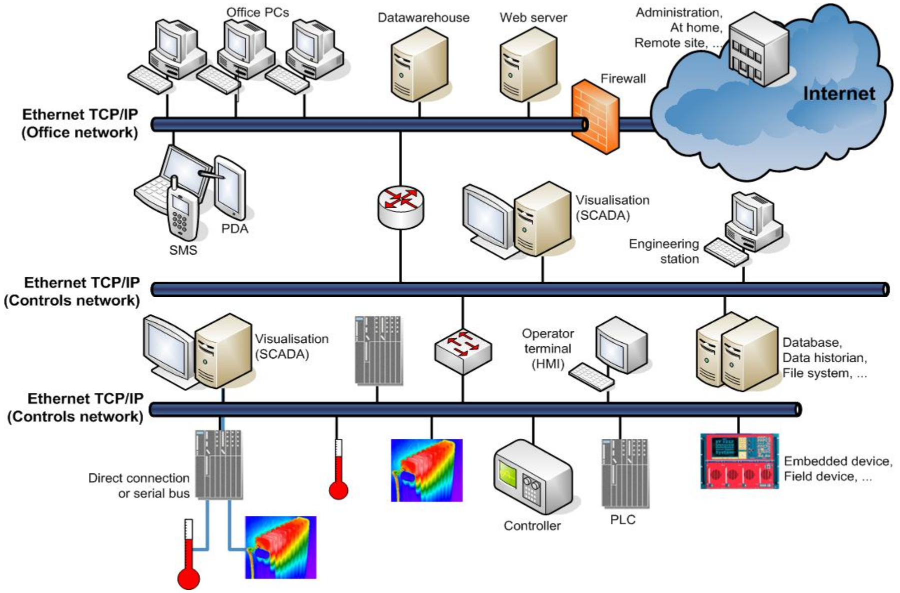
By Sean Gallagher | Published about 21 hours ago

Researchers have demonstrated a vulnerability in the computer systems used to control facilities at federal prisons that could allow an outsider to remotely take them over, doing everything from opening and overloading cell door mechanisms to shutting down internal communications systems. Tiffany Rad, Teague Newman, and John Strauchs, who presented their research on October 26 at the Hacker Halted information security conference in Miami, worked in Newman's basement to develop the attacks that could take control of prisons' industrial control systems and programmable logic controllers. They spent less than $2,500 and had no previous experience in dealing with those technologies.

# Network Segregation at CERN

## Different networks for different purposes:

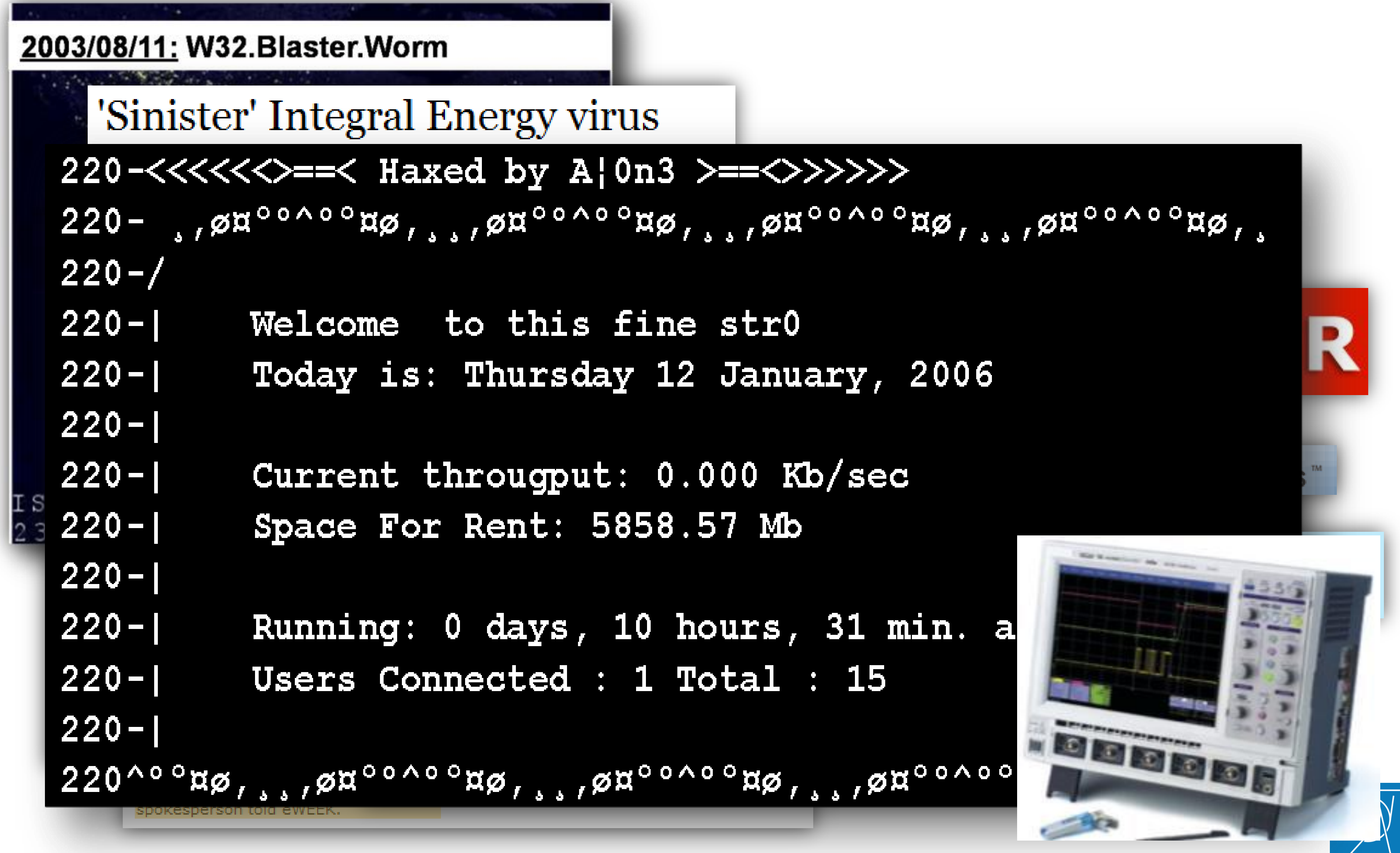
- ► …for accelerator operations
- ► …and for experiments
- ► Campus network for office computing
- ► Additional protective measures where needed ("VPNs", ACLs, …)


Office PCs
Datawarehouse
Web server
Administration, At home, Remote site, …
Firewall
Internet
Ethernet TCP/IP (Office network)
PDA
SMS
Visualisation (SCADA)
Engineering station
Ethernet TCP/IP (Controls network)
Visualisation (SCADA)
Operator terminal (HMI)
Database, Data historian, File system, …
Ethernet TCP/IP (Controls network)
Direct connection or serial bus
Embedded device, Field device, …
Controller
PLC

## 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

# Damage by Viruses & Worms?



2003/08/11: W32.Blaster.Worm

'Sinister' Integral Energy virus

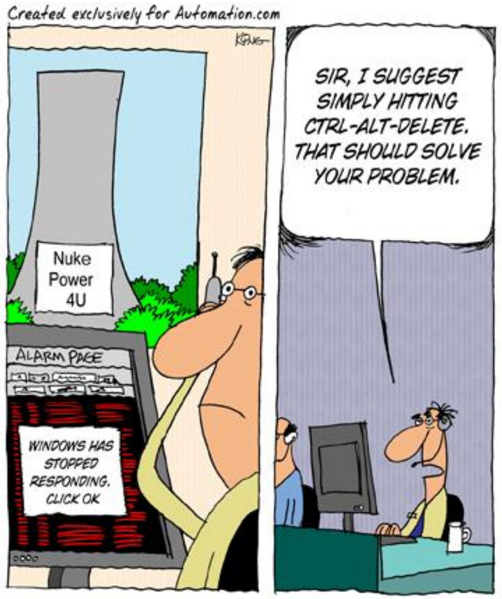
```
220-<<<<<<>==< Haxed by A¦0n3 >==<>>>>>
220- ¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸
220-/
220-|    Welcome  to this fine str0
220-|    Today is: Thursday 12 January, 2006
220-|
220-|    Current througput: 0.000 Kb/sec
220-|    Space For Rent: 5858.57 Mb
220-|
220-|    Running: 0 days,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

spokesperson told eWEEK.

# Patch, Patch, Patch!!!

**Prompt patching essential… but problematic:**

- Compliance statement needed (vendor-side testing)
- Integrator might decline responsibility if PCS is touched
- PCS might need to be re-certified (e.g. SILx)
- True impact on PCS unknown: thorough on-site testing!
- Difficult (impossible?) to patch embedded devices!


Created exclusively for Automation.com
Nuke Power 4U
ALARM PAGE
WINDOWS HAS STOPPED RESPONDING. CLICK OK
SIR, I SUGGEST SIMPLY HITTING CTRL-ALT-DELETE. THAT SHOULD SOLVE YOUR PROBLEM.

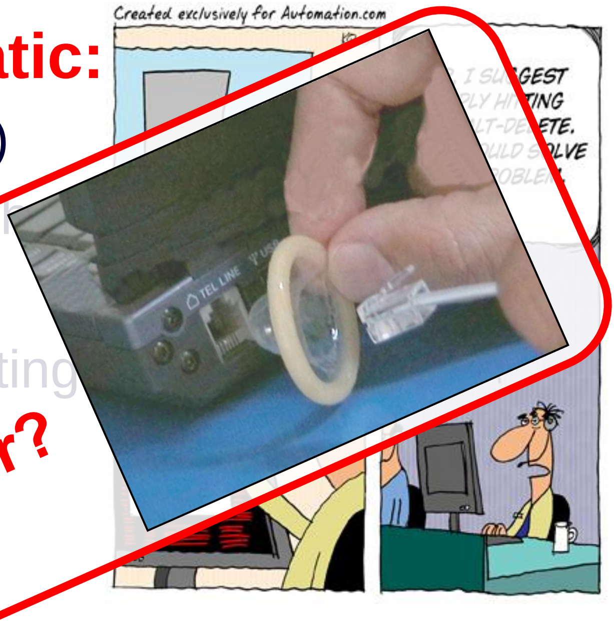
## CERN delegates patching:

- Passing flexibility and responsibility to the experts
- They decide *when* to install *what* on *which* control PC
- NOT patching is NOT an option, but delays are tolerated
- Running up-to-date anti-virus software and local firewalls is a must
- However, processes are still not optimal:
  Applications still depend too much on the O/S!

# Patch, Patch, Patch!!!

## Prompt patching essential… but problematic:

- ► Compliance statement needed (vendor-side testing)
- ► Integrator might decline responsibility if PCS is touc
- ► PCS might need to be re-certified (e.g. SIL x)
- ► True impact on PCS unknown: thorough on-site testing
- ► Difficult (impossible?) to patch embedded devices!


Created exclusively for Automation.com
I SUGGEST ... PLY HITTING ... LT-DELETE. ... ULD SOLVE ... OBLEM
TEL LINE

## CERN delegates patching:

- ► Passing flexibility and responsibility to the experts
- ► They decide *when* to install *what* on *which* control PC
- ► NOT patching is NOT an option, but delays are tolerated
- ► Running up-to-date anti-virus software and local firewalls is a must
- ► However, processes are still not optimal: Applications still depend too much on the O/S!

**Review you PCS.**

**How can you make patching easier/quicker?**

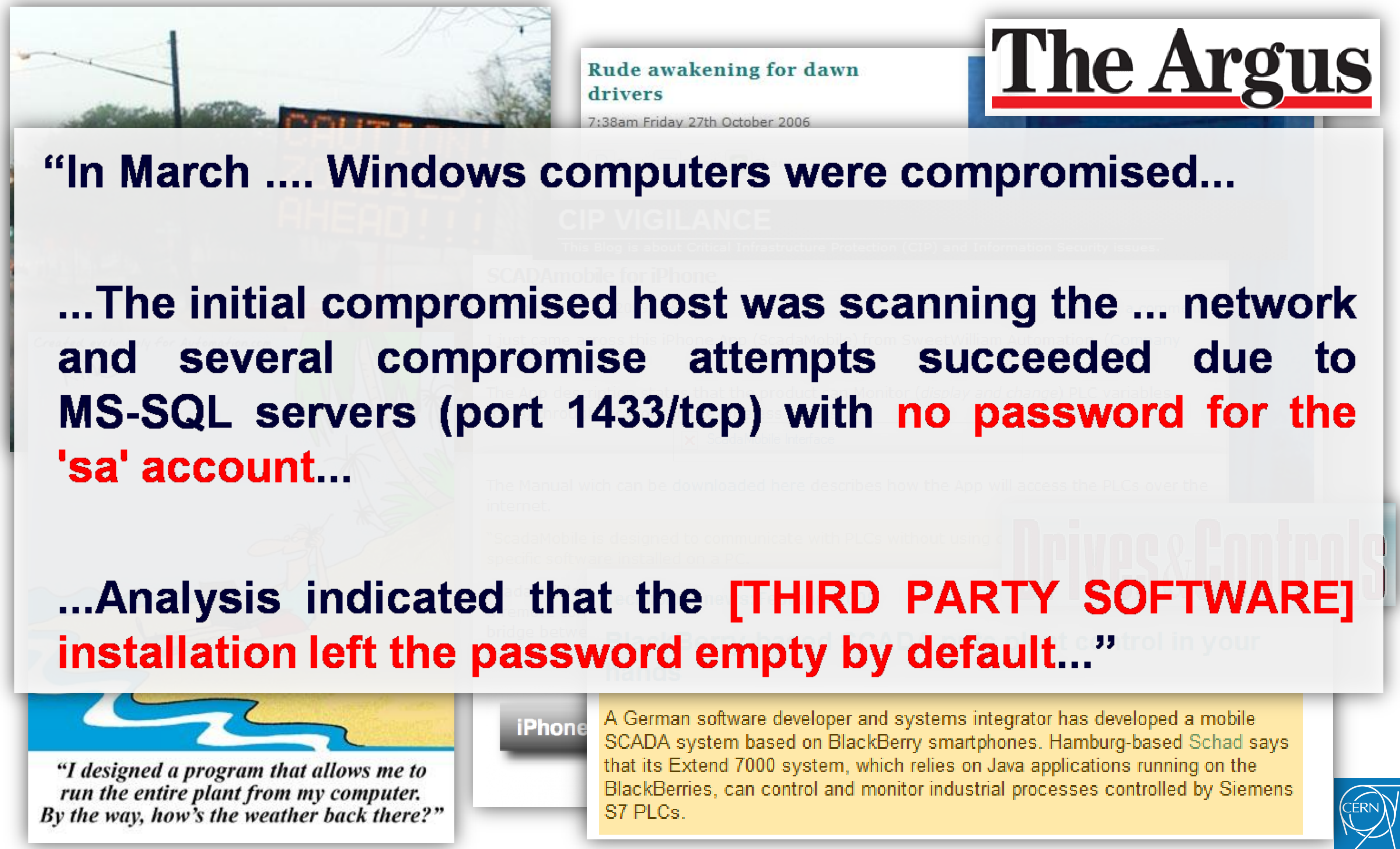
**Do you have test systems in place?**

# Damage due to Openness?

“In March …. Windows computers were compromised…

…The initial compromised host was scanning the … network and several compromise attempts succeeded due to MS-SQL servers (port 1433/tcp) with **no password for the 'sa' account**…

…Analysis indicated that the **[THIRD PARTY SOFTWARE] installation left the password empty by default**…”


CAUTION
ZOMBIES
AHEAD!!
CIP VIGILANCE
This Blog is about Critical Infrastructure Protection (CIP) and Information Security issues.
SCADAmobile for iPhone
Drives&Controls
BlackBerry-based SCADA puts plant control in your hands
iPhone

Rude awakening for dawn drivers

7:38am Friday 27th October 2006

The Argus

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

A German software developer and systems integrator has developed a mobile SCADA system based on BlackBerry smartphones. Hamburg-based Schad says that its Extend 7000 system, which relies on Java applications running on the BlackBerries, can control and monitor industrial processes controlled by Siemens S7 PLCs.

# Apply the Rule of Least Privilege

## Can't follow the "Rule of Least Privilege":

► Default passwords still widely used – not incentive/force to change

► Backdoors might be present – not communicated to user

► Still need for shared accounts instead of personal accounts

► No modern access protection for PLCs and field devices like certificates, challenge/response, granular access control, …
(The RUN-P key switch disappeared again from Siemens S7-400 PLCs)

► Difficult to integrate into standard IdM: OIM, FIM, LDAP/AD/Kerberos

► Cacophony of different solutions for remote access:
Is this user or vendor driven???

## CERN uses PVSS (ETM/Siemens):

► Full integration with CERN SSO/AD/LDAP (i.e. central IdP)

► Multi-factor to come (SmartChip certificates, mobile apps, Yubikeys)

► More difficult with home-grown SCADA software ☹

# Apply the Rule of Least Privilege

## Can’t follow the “Rule of Least Privilege”:

- ► Default passwords still widely used – not incentive/force to cl
- ► Backdoors might be present – not communicated to u
- ► Still need for shared accounts instead of personal ac
- ► No modern access protection for PLCs and field devic , challenge/response, granular access control, … (The RUN-P key switch disappeared again from Siemens -400 PLCs)
- ► Difficult to integrate into standard IdM: OIM, FIM, LDAP/AD/Kerberos
- ► Cacophony of different solutions for remote access: Is this user or vendor driven???

## CERN uses PVSS (ETM/Siemens):

- ► Full integration with CERN SSO/AD/LDAP (i.e. central IdM)
- ► Multi-factor to come (SmartChip certificates, mobile apps, Yubikeys)
- ► More difficult with home-grown SCADA software ☹

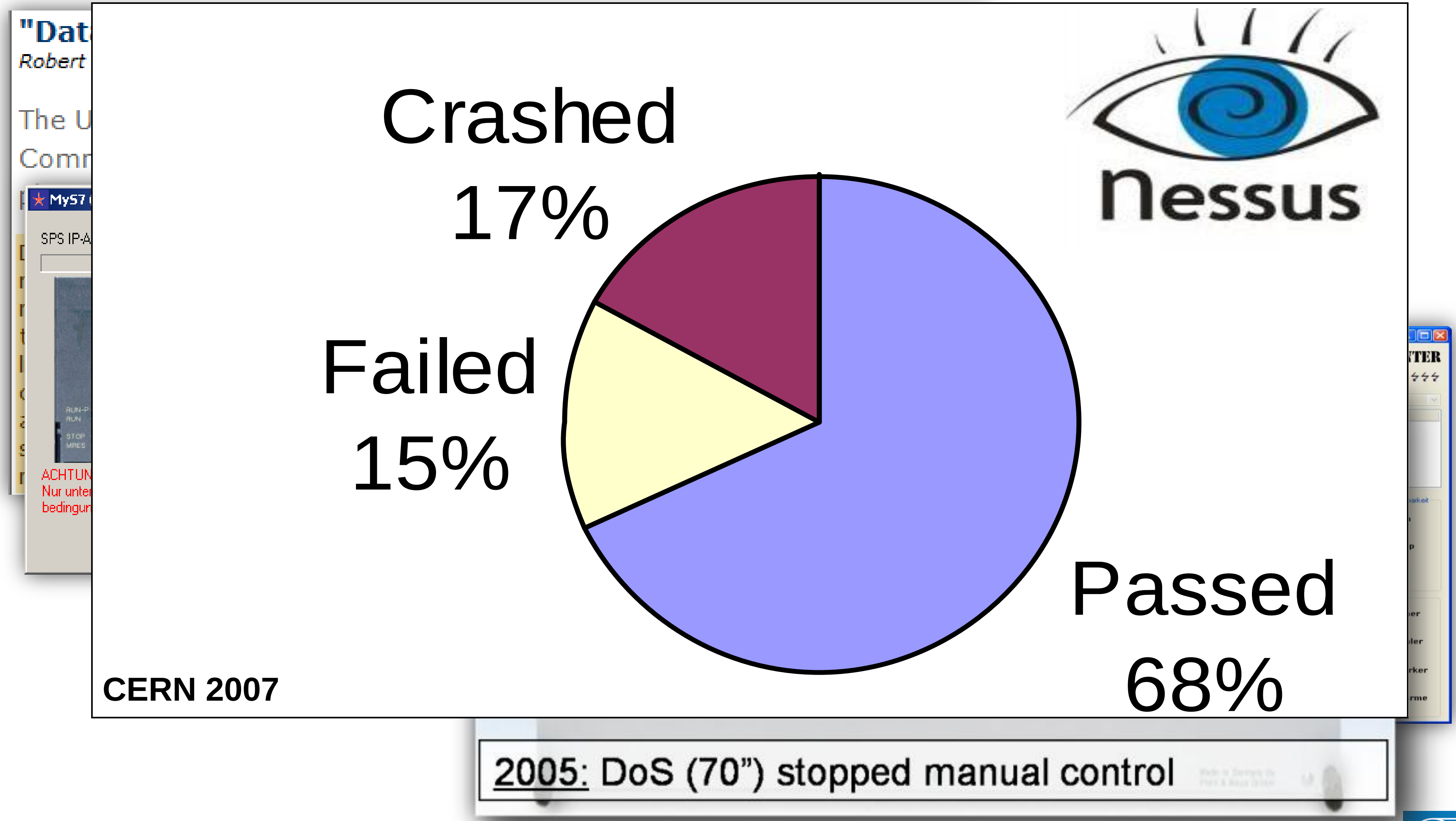
**Review & restrict access rights.**

**Access should be personalized.**

**Keep passwords secret!**

**Ask your vendor of default/hidden accounts.**

# Damage due to lack of resilience?



CERN 2007

2005: DoS (70”) stopped manual control

# Robustify!

## Many PLCs, etc. are completely unprotected:

- Legacy & even today’s systems fail basic security scans (nmap, Nessus).
- No firewall, no anti-virus, nothing.
- Wrong defaults: everything should be disabled, first.
- Violating standards: They fulfill use-cases, but not *abuse*-cases.
- No data sheets of default configuration, open ports, default accounts.
- There is no certification. Nothing mandatory.
  (INL & Wurldtech/Archilles procedures & results are proprietary to vendors)

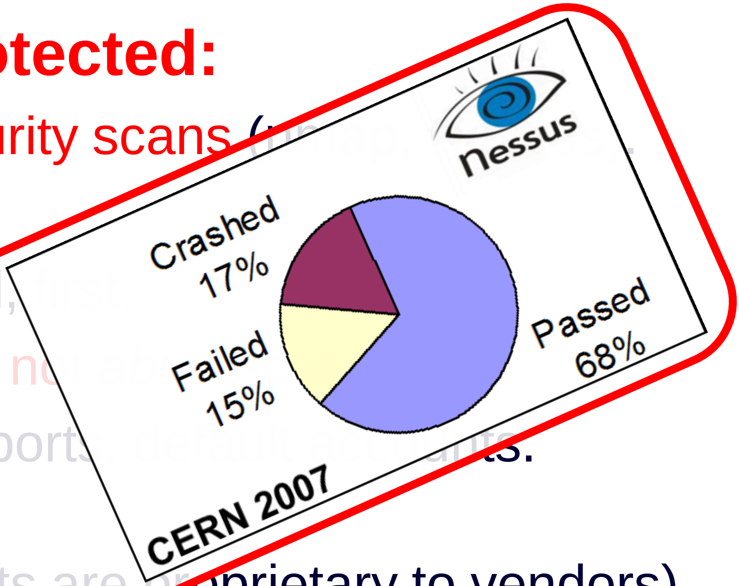
## Understanding is the key at CERN:

- Building asset inventory & understanding dependencies
- Running vulnerability tools on everything
- Applying “Security Baselines”
  i.e. a contract on security with recommendations
  for configuration settings, protective means, procedures & training

# Robustify!

## Many PLCs, etc. are completely unprotected:

- ► Legacy & even today’s systems fail basic security scans (nmap, nessus, etc.).
- ► No firewall, no anti-virus, nothing.
- ► Wrong defaults: everything should be disabled, first.
- ► Violating standards: They fulfill use-cases, but not abuse-cases.
- ► No data sheets of default configuration, open ports, default accounts.
- ► There is no certification. Nothing mandatory.
  (INL & Wurldtech/Achilles procedures & results are proprietary to vendors)



## Understanding is the key at CERN:

- ► Building asset inventory & understanding dependencies
- ► Running vulnerability tools on everything
- ► Applying “Security Baselines”
  i.e. a contract on security with recommendations
  for configuration settings, protective means, procedures & training

**Review you field devices.**
**Scan them (if not in production ;-).**
**Return failing ones to your vendor!**

# Damage due missing procedures?

Hole Found in Protocol Handling Vital National Infrastructure

March 25, 2007

A Boeing 777 uses similar technologies to Process Control Systems

7 May 2008, 14:37

CADA systems

are industrial
trochemicals, food,
nponent of its software
are systems using

reatens

Add comments

s, reports of a
ndows based
omputer
ol power plants,
ties and other
frastructure)
e rounds of the
While the
new attacks is
hese vital control
system called
C + S7) , the
vulnerability used to deliver it looks

# Review Development Life-Cycle

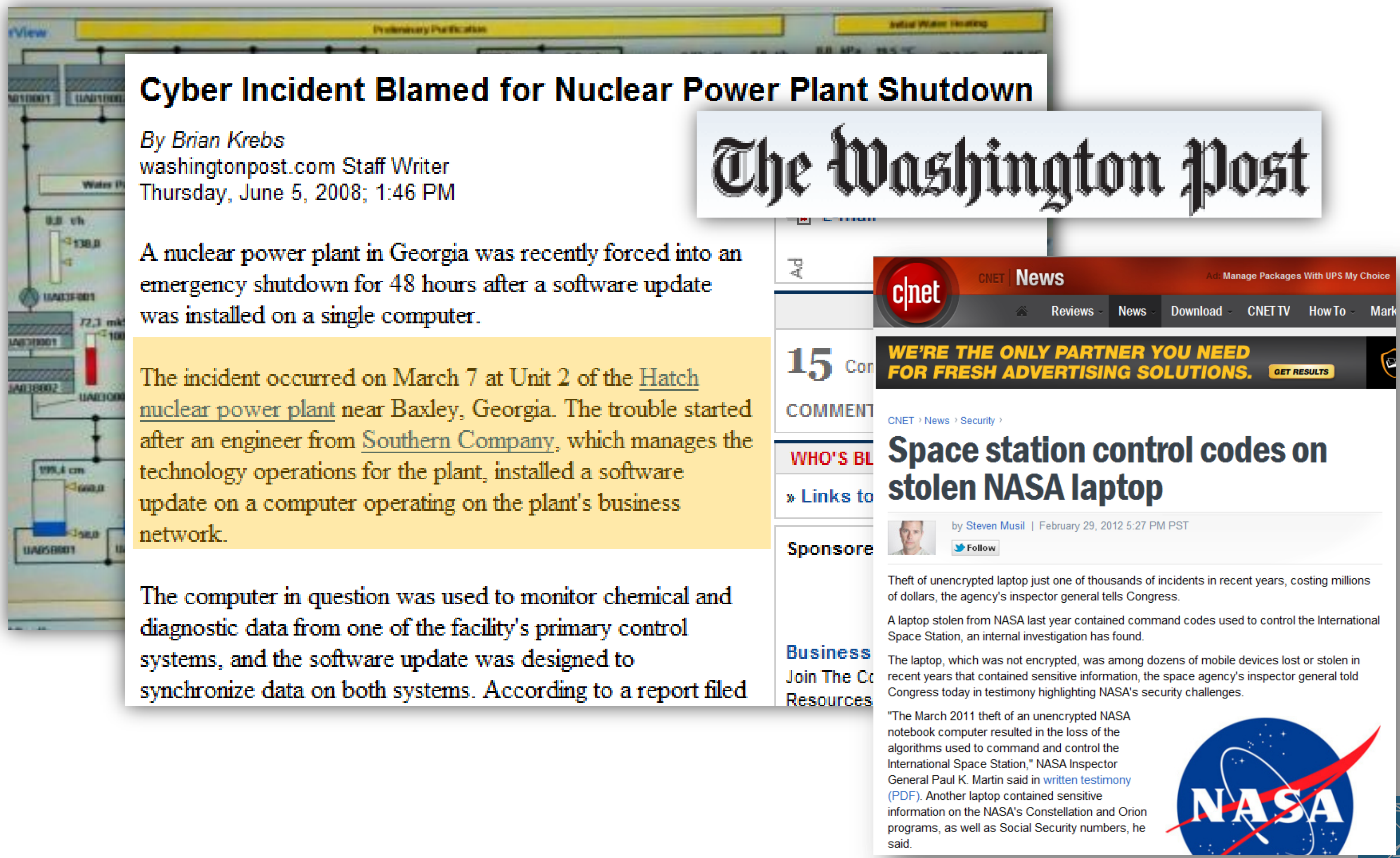
## Reviewing procedures for

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

## Protecting operations

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

# Damage due to Unawareness?



## Cyber Incident Blamed for Nuclear Power Plant Shutdown

*By Brian Krebs*
washingtonpost.com Staff Writer
Thursday, June 5, 2008; 1:46 PM

A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer.

The incident occurred on March 7 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. The trouble started after an engineer from Southern Company, which manages the technology operations for the plant, installed a software update on a computer operating on the plant's business network.

The computer in question was used to monitor chemical and diagnostic data from one of the facility's primary control systems, and the software update was designed to synchronize data on both systems. According to a report filed

CNET › News › Security ›

## Space station control codes on stolen NASA laptop

by Steven Musil | February 29, 2012 5:27 PM PST

Theft of unencrypted laptop just one of thousands of incidents in recent years, costing millions of dollars, the agency's inspector general tells Congress.

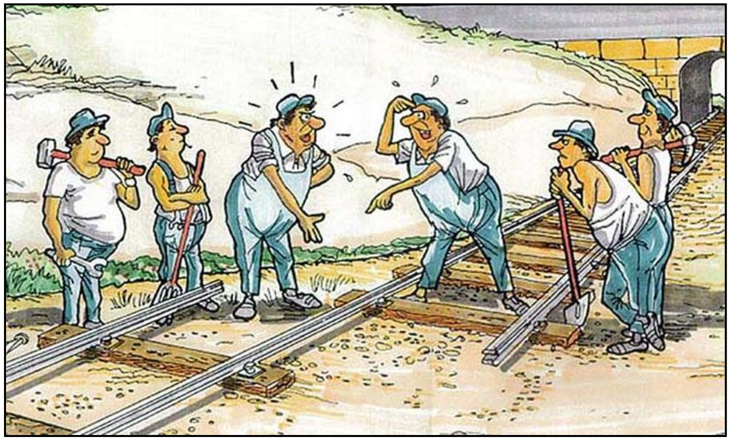
A laptop stolen from NASA last year contained command codes used to control the International Space Station, an internal investigation has found.

The laptop, which was not encrypted, was among dozens of mobile devices lost or stolen in recent years that contained sensitive information, the space agency's inspector general told Congress today in testimony highlighting NASA's security challenges.

"The March 2011 theft of an unencrypted NASA notebook computer resulted in the loss of the algorithms used to command and control the International Space Station," NASA Inspector General Paul K. Martin said in written testimony (PDF). Another laptop contained sensitive information on the NASA's Constellation and Orion programs, as well as Social Security numbers, he said.

# This is a People Problem! (I)

## Bringing together experts:



- ►Control system experts know their systems by heart – but IT concepts?
- ►IT people (should) know IT security – but don't know controls!
- ►Synergy between both is often poorly/not really exploited!

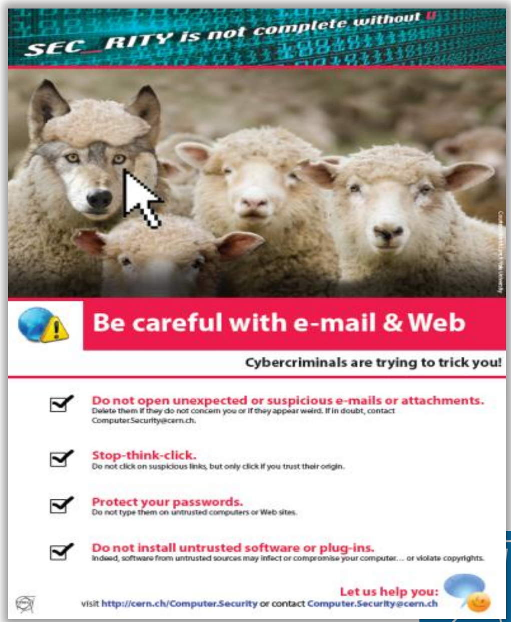
## Openly discuss vulnerabilities:

- ►Attackers are better networked than we are!
  Attackers know of vuln's probably long before we do.
- ►"Responsible disclosure" also for PCS vulnerabilities.
- ►Create "SCADA_BugTraq" (ideally join BugTraq, CVE, & Co.).
- ►Deploy/train CERT/CSIRTs to understand PCS.
- ►More activism of the vendors needed (outside standardization bodies)!

# This is a People Problem! (II)

## CERN aims to for a “change of culture” & “a new mind set”

- ► Basic awareness training to everyone, esp. newcomers
- ► Every owner of a computer account must follow an online security course every 3 years.
- ► Provisioning of static code analyzers
- ► Dedicated training on secure development (Java, C/C++, Perl, Python, PHP, web, ...)
- ► Baselines & consulting
- ► The Security Team as facilitator and enabler: Making security part of the overall.


SEC_RITY is not complete without U!

**Be careful with e-mail & Web**

Cybercriminals are trying to trick you!

☑ **Do not open unexpected or suspicious e-mails or attachments.** Delete them if they do not concern you or if they appear weird. If in doubt, contact Computer.Security@cern.ch.

☑ **Stop-think-click.** Do not click on suspicious links, but only click if you trust their origin.

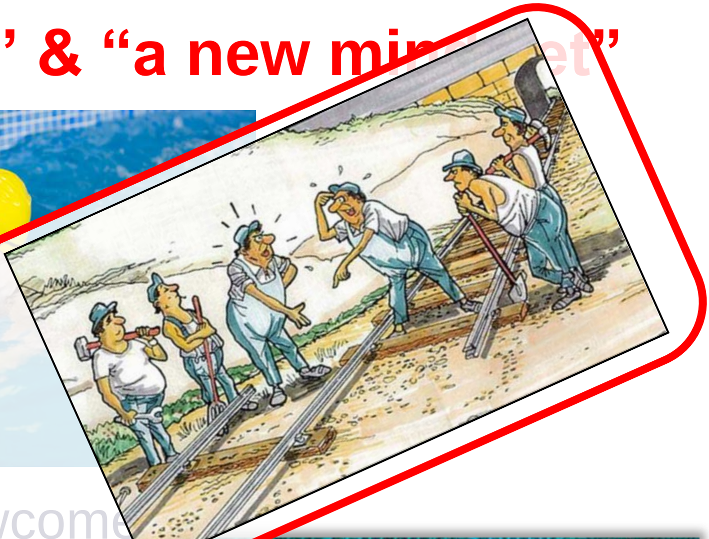
☑ **Protect your passwords.** Do not type them on untrusted computers or Web sites.

☑ **Do not install untrusted software or plug-ins.** Indeed, software from untrusted sources may infect or compromise your computer… or violate copyrights.

Let us help you: visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

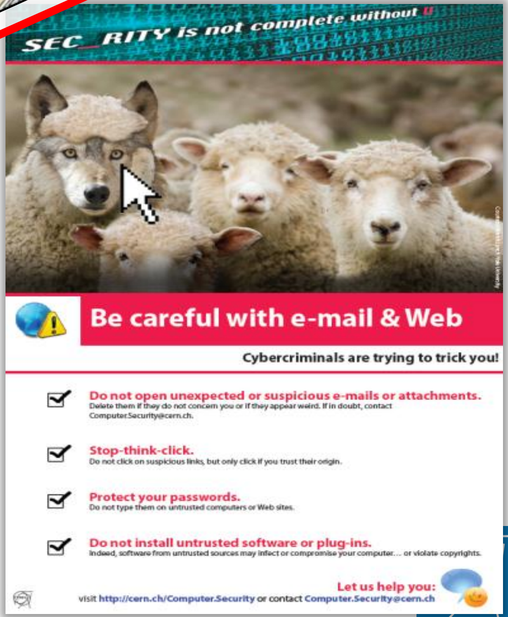
# This is a People Problem! (II)

## CERN aims to for a “change of culture” & “a new mind set”



- ► Basic awareness training to everyone, esp. newcomers
- ► Every owner of a computer account must follow an online security course every 3 years
- ► Provisioning of static code analyzers
- ► Dedicated training on secure development (Java, C/C++, Perl, Python, PHP, web, ...)
- ► Baselines & consulting
- ► The Security Team as facilitator and enabler: Making security part of the overall.

**Communication is the key.**
**Bring together experts.**
**Change the culture & the mind set.**
**Make “security” part of the overall!**


SEC_RITY is not complete without U

**Be careful with e-mail & Web**

Cybercriminals are trying to trick you!

☑ **Do not open unexpected or suspicious e-mails or attachments.**
Delete them if they do not concern you or if they appear weird. If in doubt, contact Computer.Security@cern.ch.

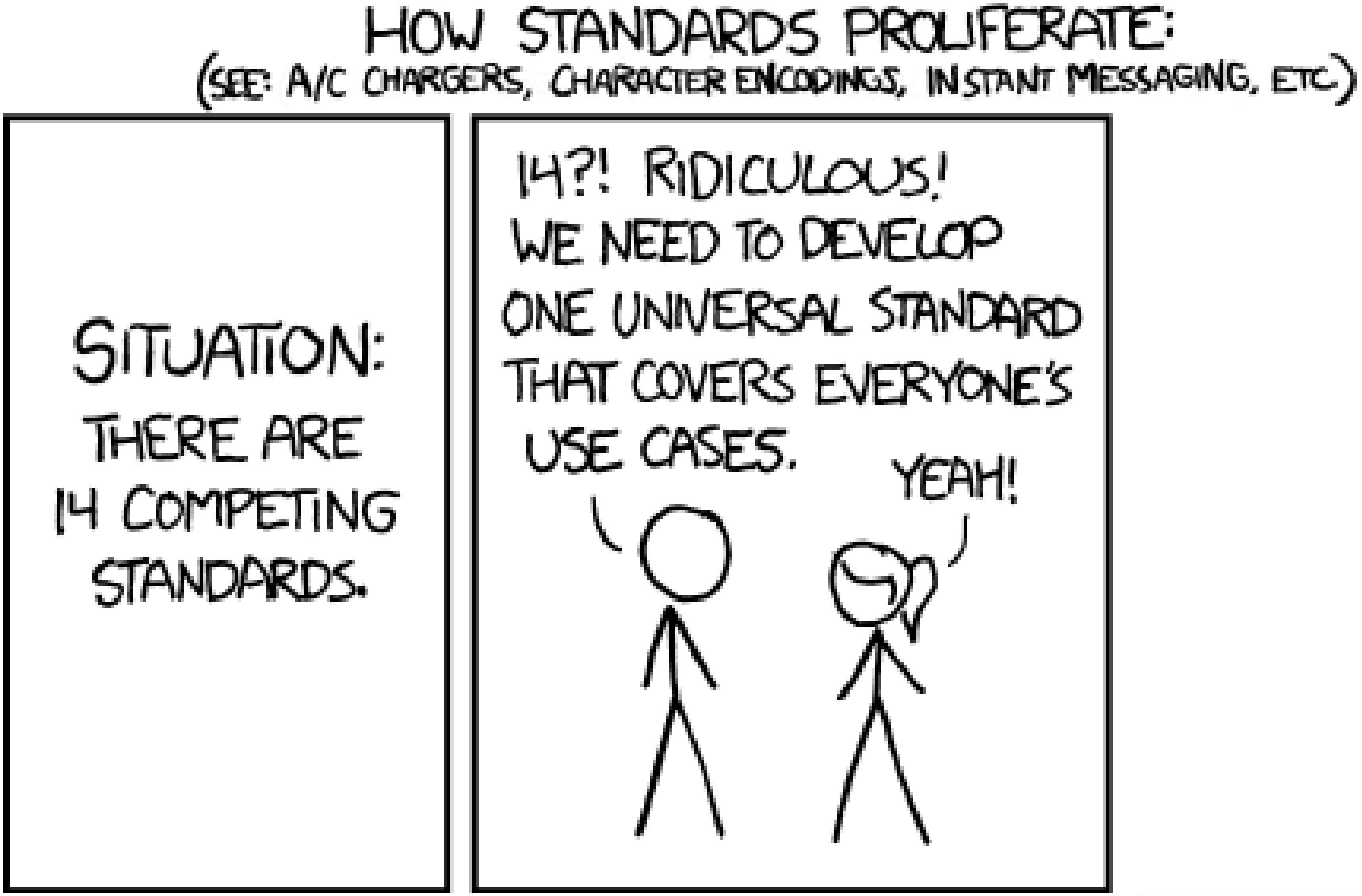
☑ **Stop-think-click.**
Do not click on suspicious links, but only click if you trust their origin.

☑ **Protect your passwords.**
Do not type them on untrusted computers or Web sites.

☑ **Do not install untrusted software or plug-ins.**
Indeed, software from untrusted sources may infect or compromise your computer… or violate copyrights.

**Let us help you:**
visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

# (Too) Many Standards…? (I)


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!

# (Too) Many Standards...? (II)

## “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”

ISO/IEC 27001:2005 and following

## *Plus standards of:*

American Gas Association (AGA)
U.S. Chemical Industry (CIDX)
German Federal Association of the Gas and Water Industries
Int’l Society for Pharmaceutical Engineering (ISPE)
Norwegian Oil Industry Association (OLF)
...

# (Too) Many Standards...? (II)

## “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”

ISO/IEC 27001:2005 and following

**Plus standards of:**

American Gas Association (AGA)
U.S. Chemical Industry (CIDX)
German Federal Association of the Gas and Water Industries

Int’l Society for Pharmaceutical Engineering (ISPE)
Norwegian Oil Industry Association (OLF)
...

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-AC07-05ID14517

http://www.msisac.org/scada

**Pick one.** **It doesn’t really matter which one.**
**Apply its recommendations.**
**Note down where you can’t.**
**Cross-check with a second one.**

# Some keyplayers…

## 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 Key Players:

ISA
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:

ABB

invensys

SIEMENS

KEMA

INL
Idaho National Laboratory

Honeywell

## Mixed Communities:

EuroSCSIE

ISASecure

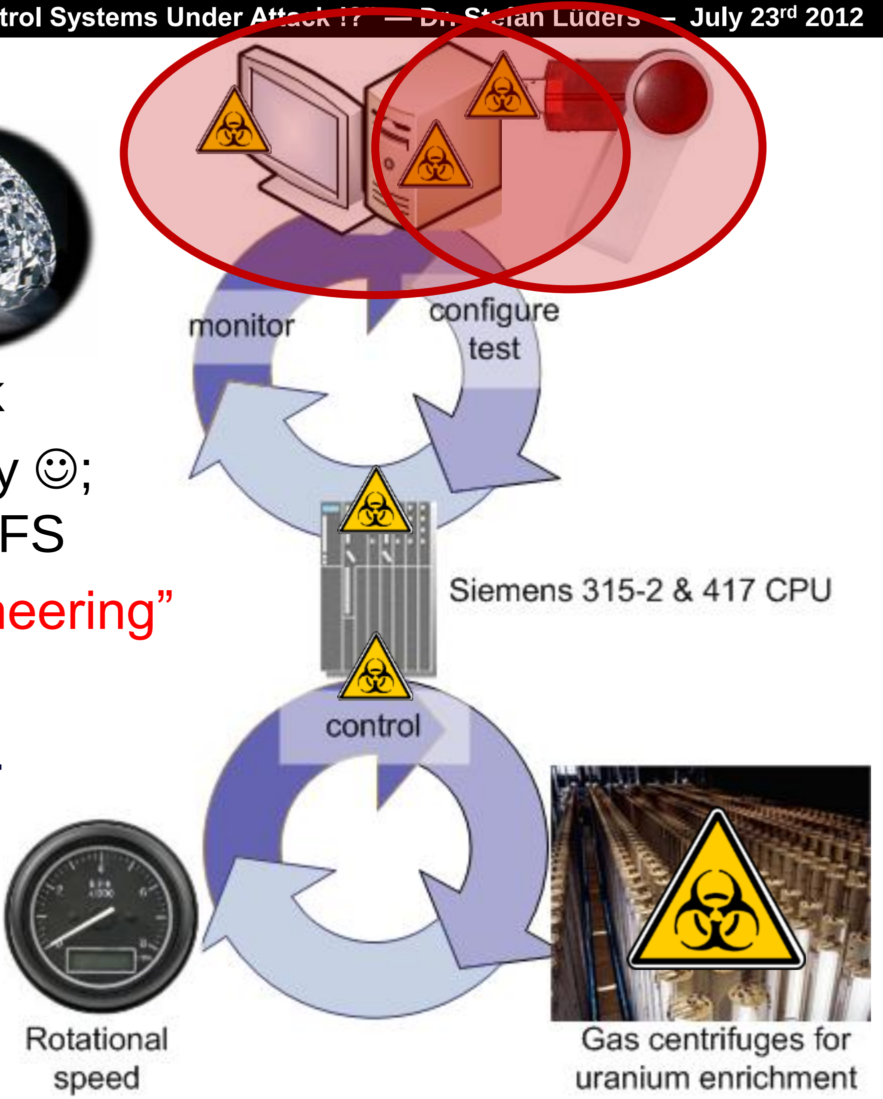
WIB
International Instrument
Users' Association

(This list is not intended to be complete.)

# Stuxnet: Protective Measures (I)

- ► Deploy a Defense-in-Depth protection

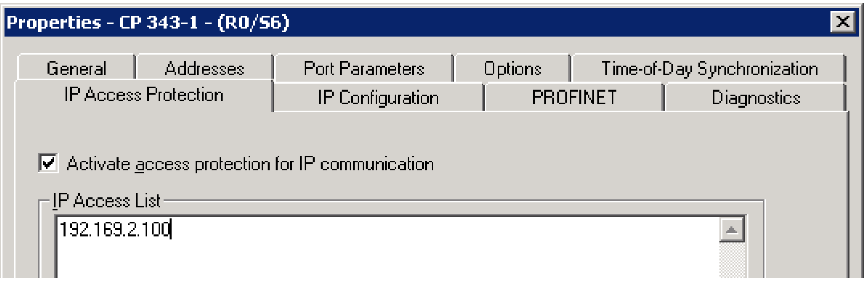
- ► Establish security cells on your network
- ► Forbid usage of USB keys or use Epoxy ☺; restrict usage of CDs, open shares & DFS
- ► Teach your experts about "Social Engineering"
- ► Screen your experts: alcohol/drugs, financial, psychological/social/family, …
- ► Patch, patch, patch… …and run up-to-date antivirus software (wouldn't have helped here ☹)



**Apply Defense-in-Depth!!!**
**…and follow a standard.**

# Stuxnet: Protective Measures (II)

- Scan you PLCs on vulnerabilities & robustness
- Lock down the PLC configuration: Enable firewall, disable unneeded services



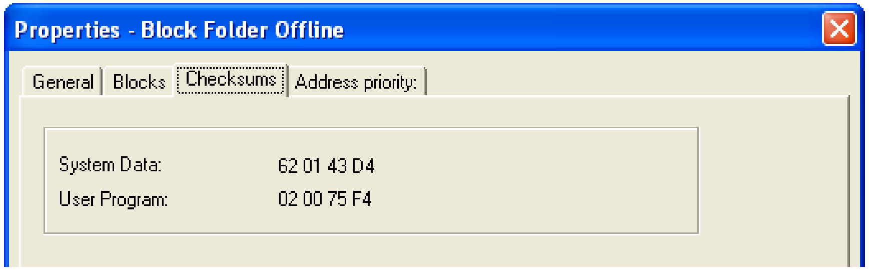
Properties - CP 343-1 - (R0/S6)

☑ Activate access protection for IP communication

IP Access List

192.169.2.100

- Enable PLC intrusion detection

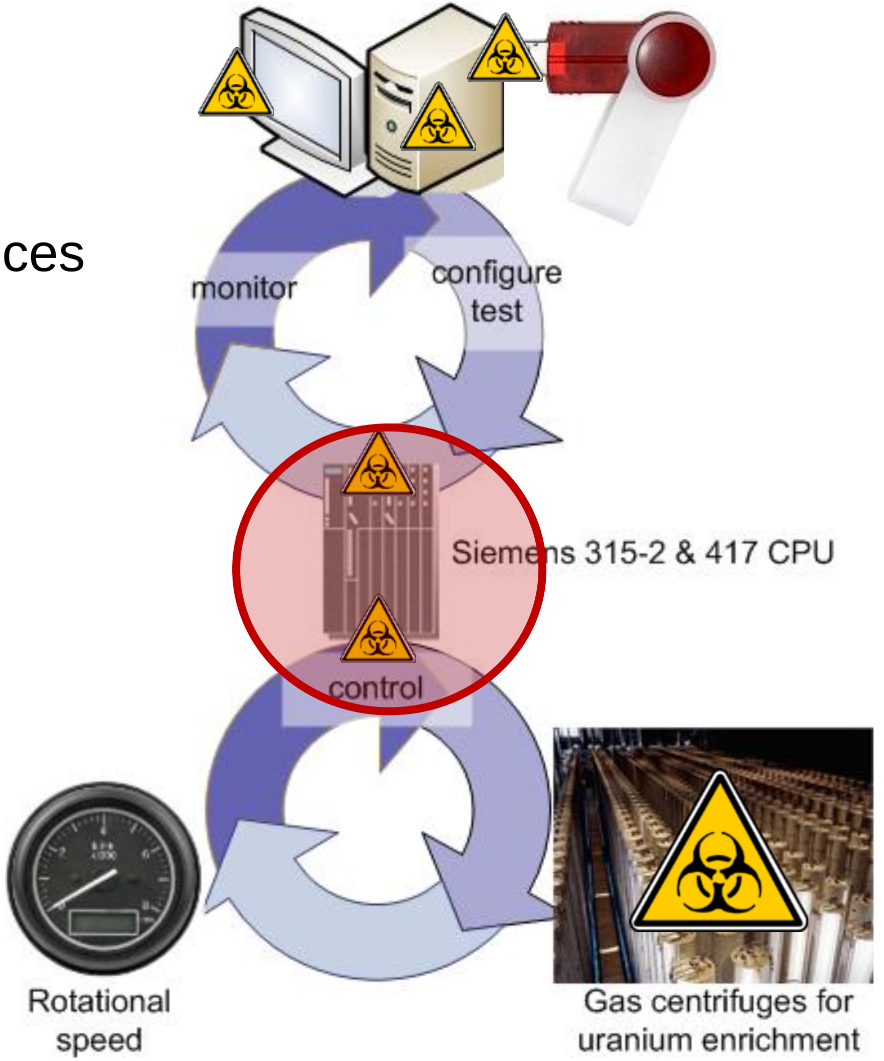


Properties - Block Folder Offline

System Data: 62 01 43 D4

User Program: 02 00 75 F4

**Talk to your vendor!**
**Accept the residual risk.**

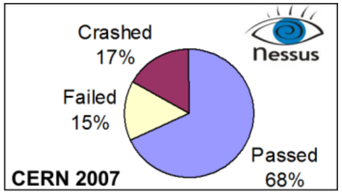


# Summary

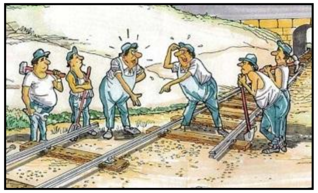
PCS are (still) not designed to be secure.

They fulfill use-cases but not *abuse* cases.

Defence-in-Depth is the key.
Protective means must be applied on *every* layer.
Control System Cyber-Security should align with IT security.



Patch procedures, access protection, robustness,
security certification & documentation
need significant improvement.

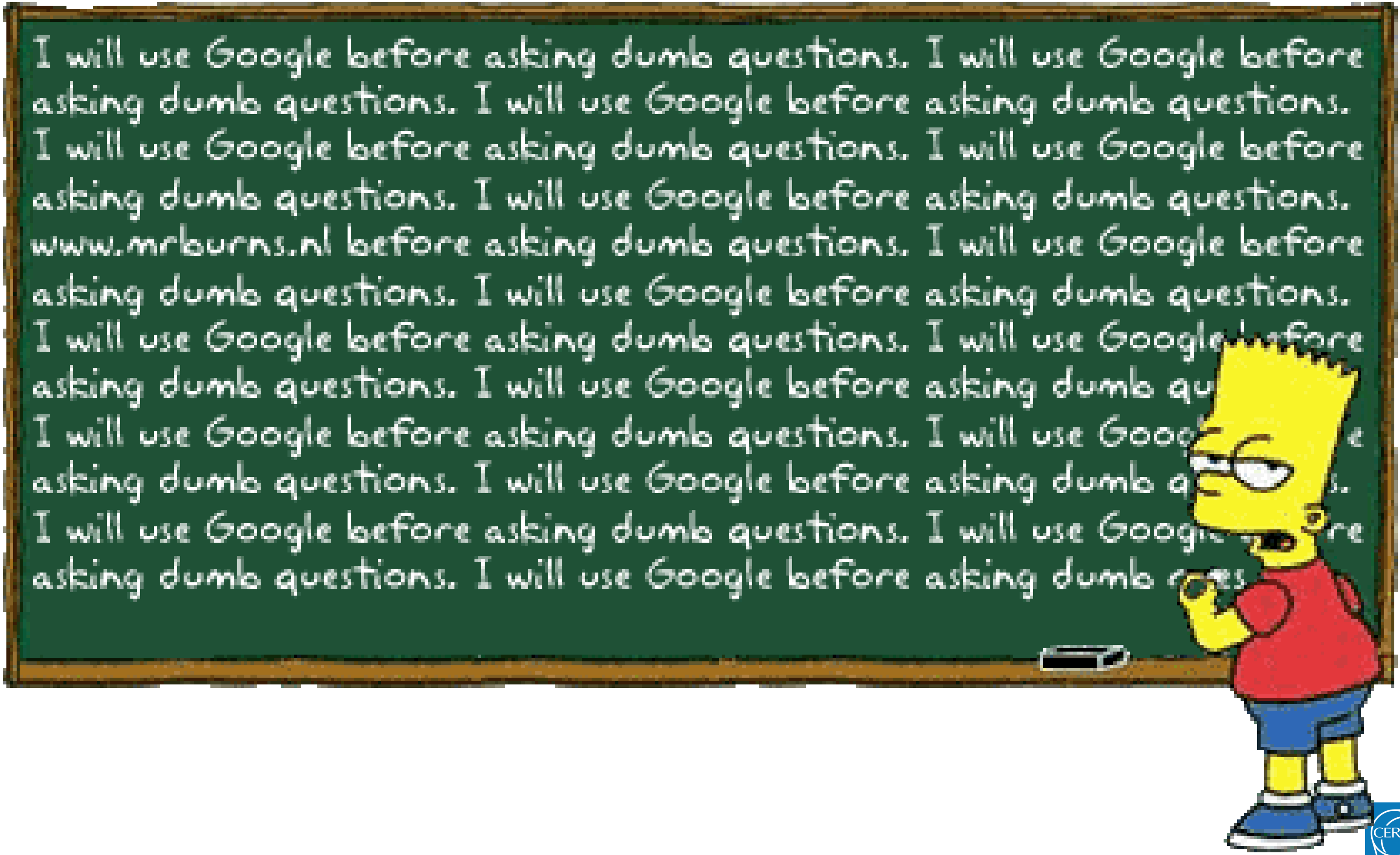


Open communication, e.g. on vuln’s, is essential.

Get your vendors/integrators/IT people on board.

There was (is?) lots of hype on PCS security since Stuxnet.
Many vendors quickly rolled out “security solutions”.
Assess first. Choose a standard and apply.

# Thanks a lot !


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