CERN

Why SCADA Security is NOT like Computer Centre Security

Finding vuln's is easy — finding solutions is the challenge!

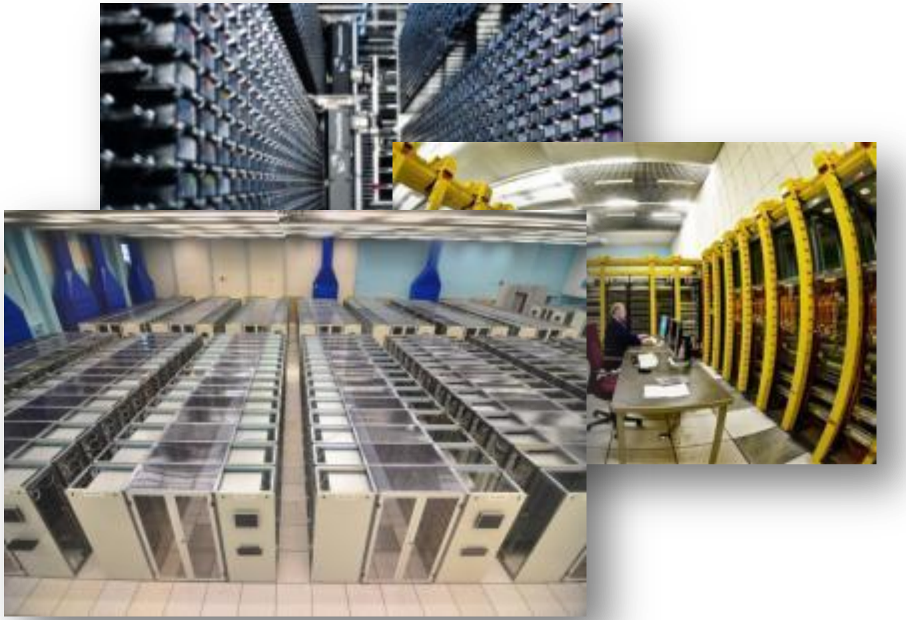
CERN Sectors of Operation

Office Computing Security

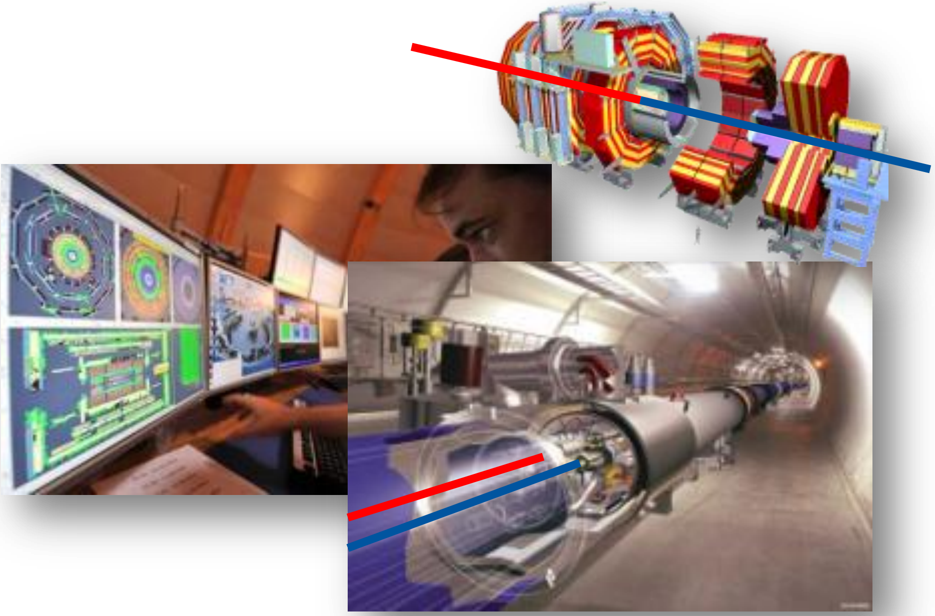
Balloon
30 Km
CD stack with
1 year LHC data
≈ 20 Km
Concorde
15 Km
Mt Blanc
4.8 Km

Grid Computing Security

Computing Services Security

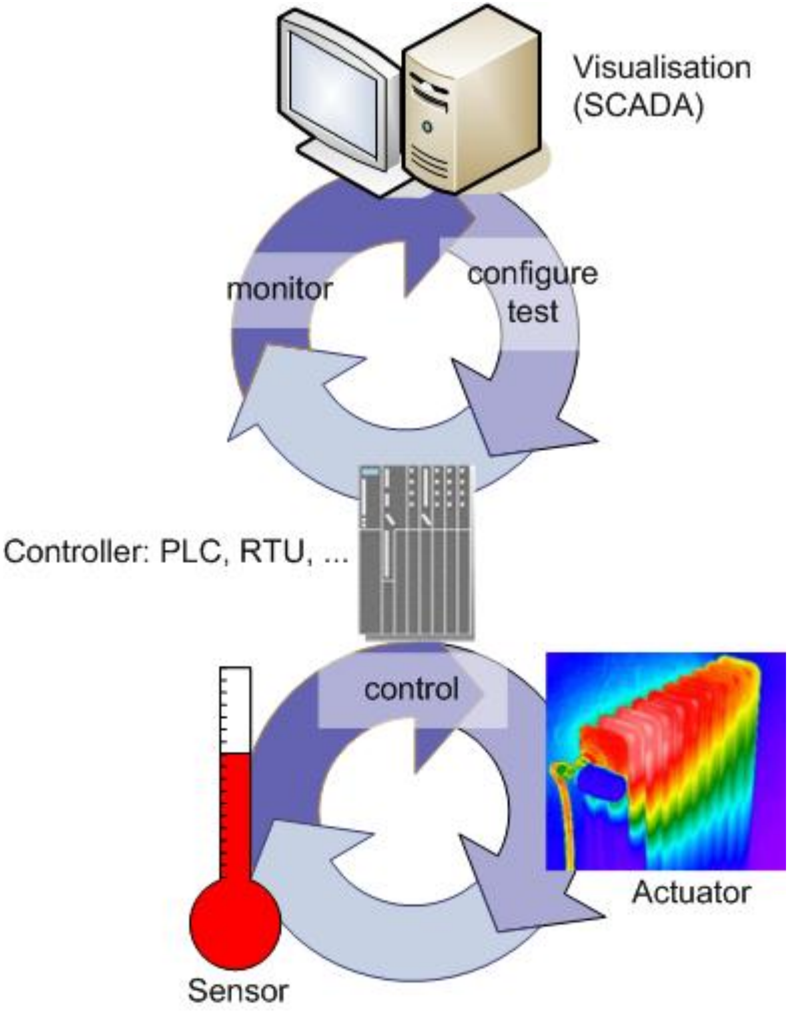


Control Systems Security

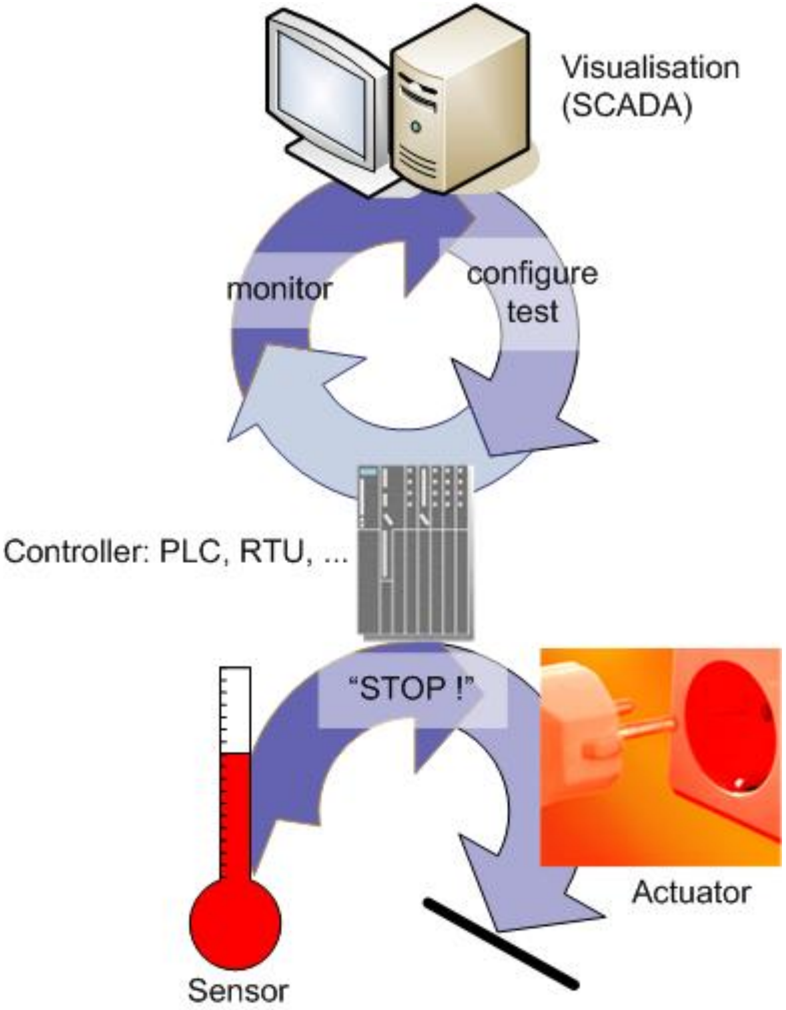


Overview

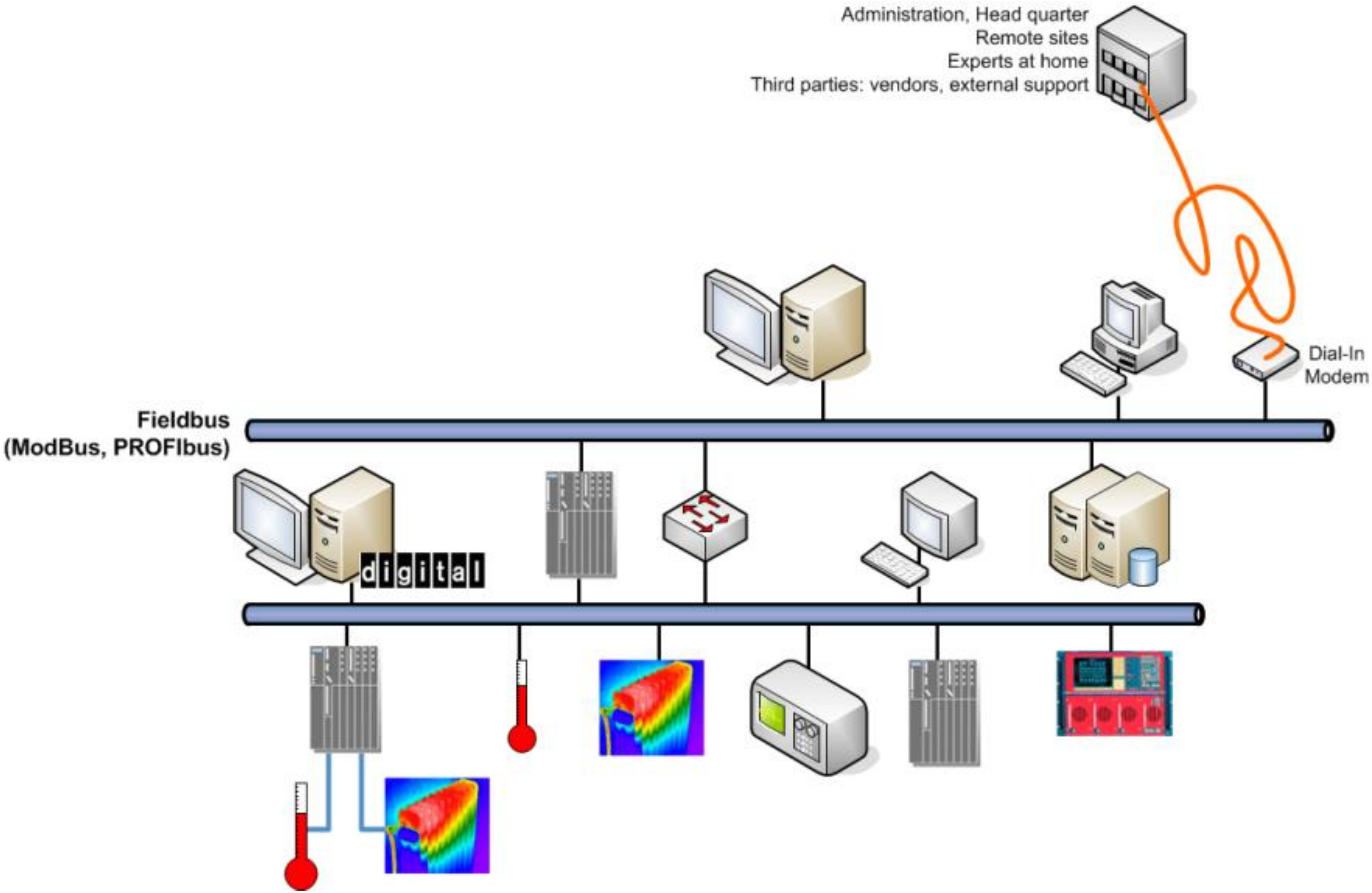
Process Control System (PCS)



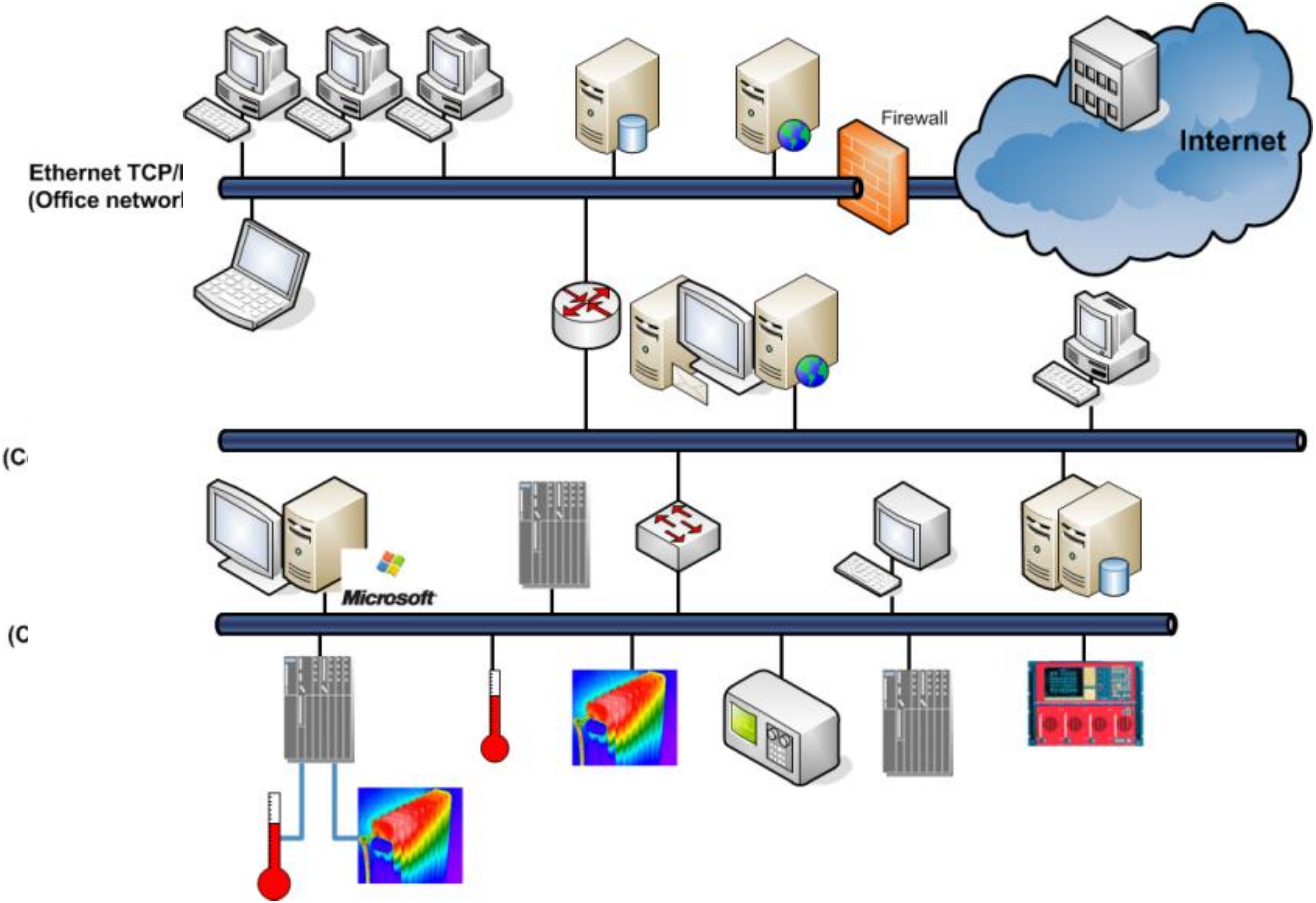
Safety System



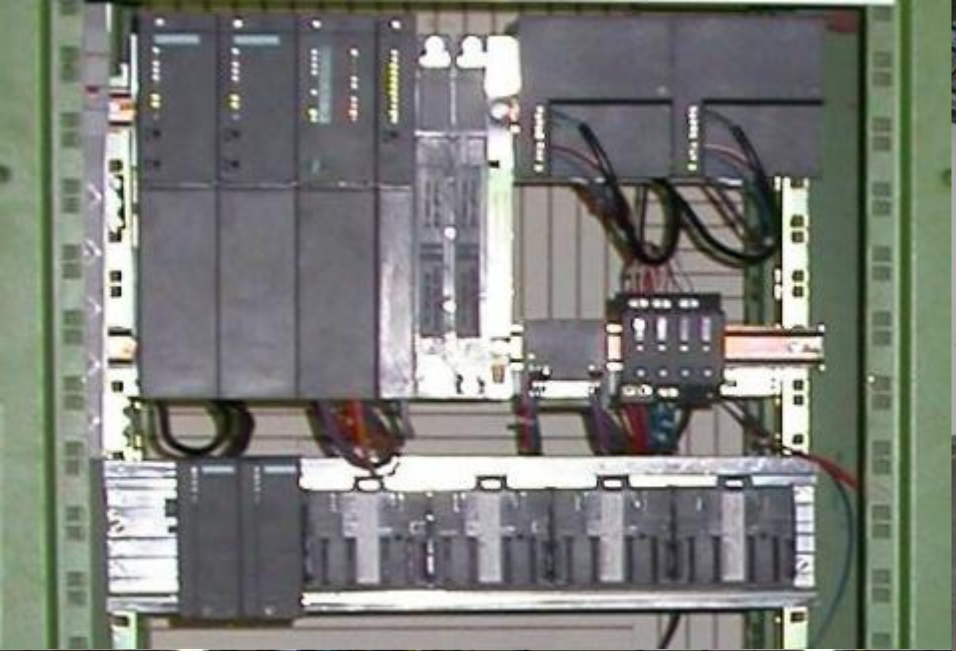
Control System in a Nutshell


Administration, Head quarter
Remote sites
Experts at home
Third parties: vendors, external support
Dial-In Modem
Fieldbus (ModBus, PROFIbus)
digital

(R)Evolution of Control Systems



(R)Evolution of Control Systems



Typical Control Systems & Devices

Critical (Cyber-)Infrastructures

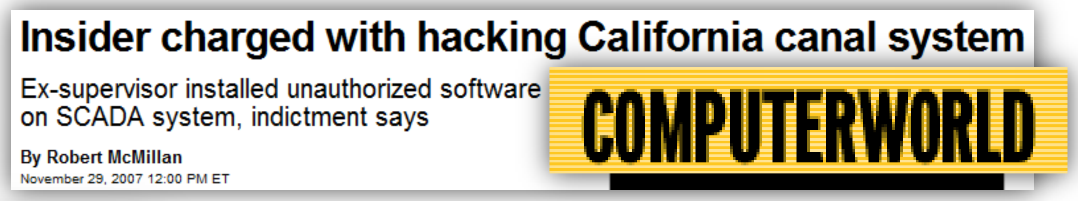
COBB County Electric, Georgia

Middle European Raw Oil, Czech Republic

Athens Water Supply & Sewage

CERN Control Centre

Overview



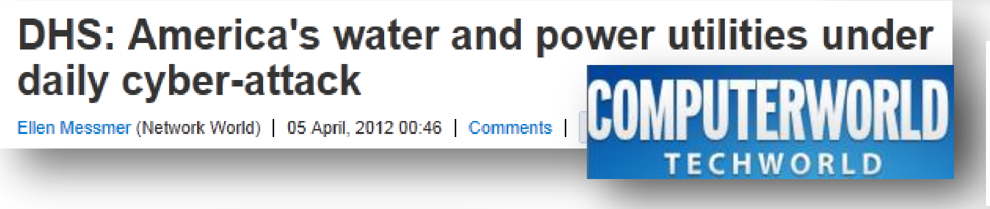
Insider charged with hacking California canal system

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

By Robert McMillan

November 29, 2007 12:00 PM ET

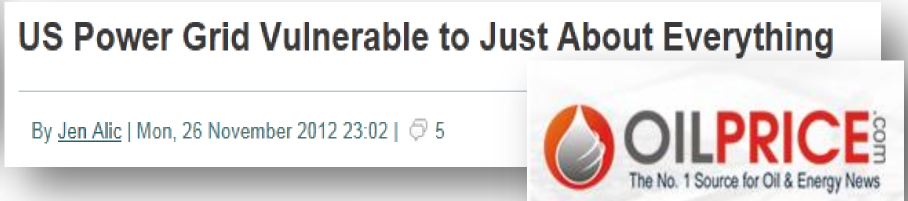
COMPUTERWORLD



DHS: America's water and power utilities under daily cyber-attack

Ellen Messmer (Network World) | 05 April, 2012 00:46 | Comments |

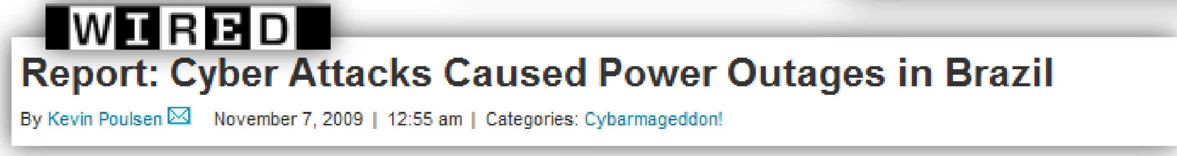
COMPUTERWORLD TECHWORLD



US Power Grid Vulnerable to Just About Everything

By Jen Alic | Mon, 26 November 2012 23:02 | 5

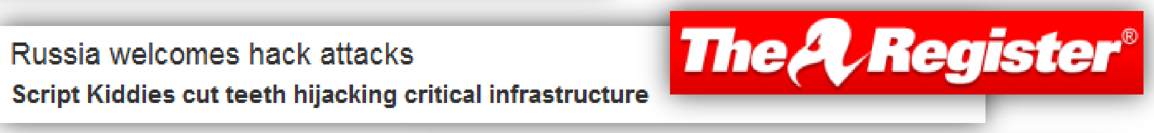
OILPRICE.com The No. 1 Source for Oil & Energy News



WIRED

Report: Cyber Attacks Caused Power Outages in Brazil

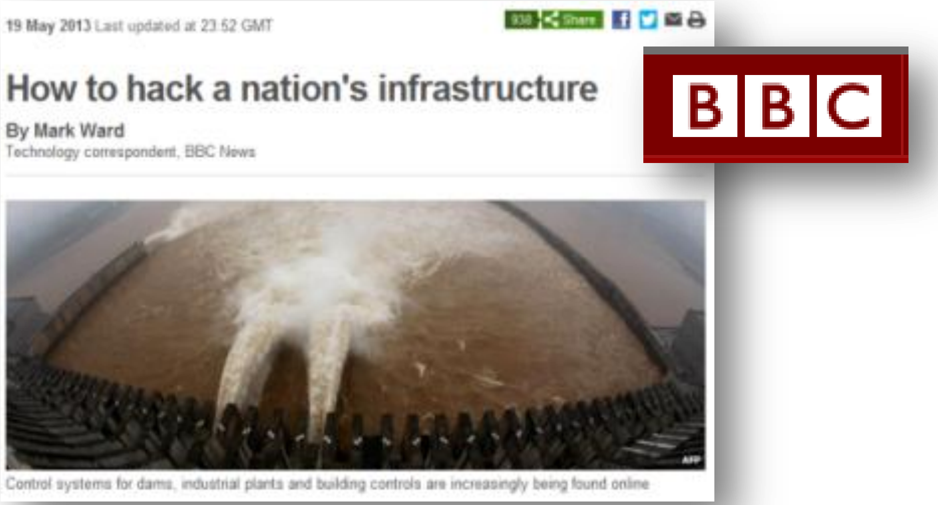
By Kevin Poulsen ✉ November 7, 2009 | 12:55 am | Categories: Cybarmageddon!



Russia welcomes hack attacks

Script Kiddies cut teeth hijacking critical infrastructure

The Register®



19 May 2013 Last updated at 23:52 GMT

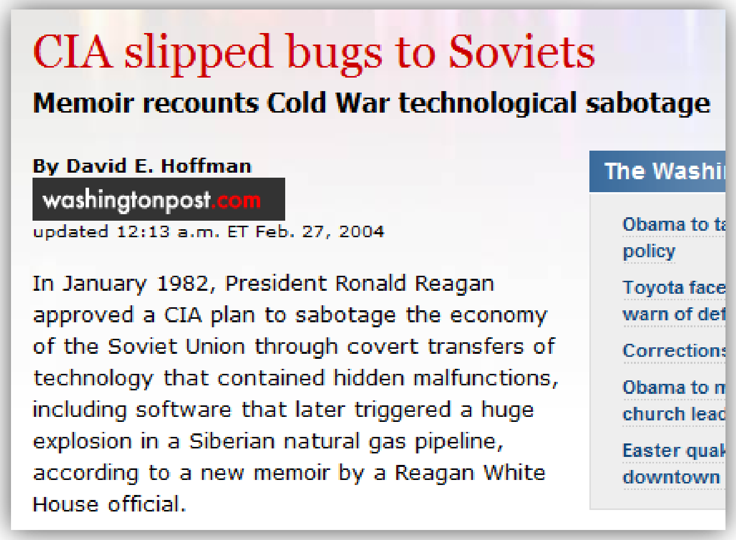
How to hack a nation's infrastructure

By Mark Ward

Technology correspondent, BBC News

Control systems for dams, industrial plants and building controls are increasingly being found online

BBC



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

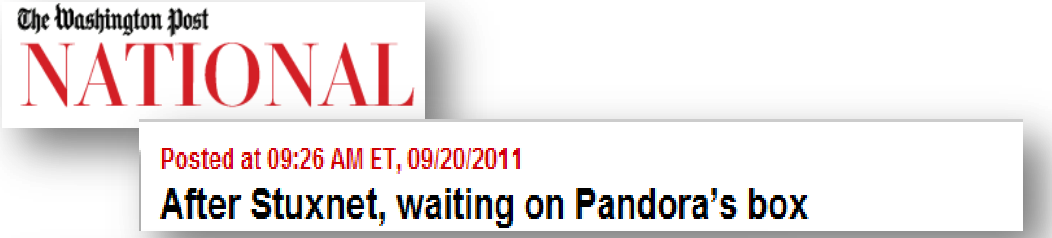
Toyota face warn of def

Corrections

Obama to m church lead

Easter quak downtown

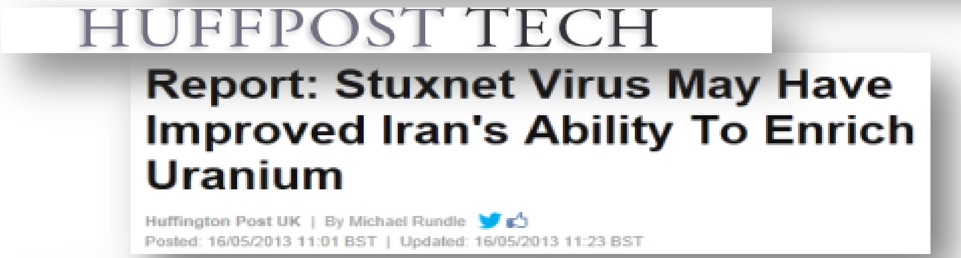
Enter reality



The Washington Post
NATIONAL

Posted at 09:26 AM ET, 09/20/2011

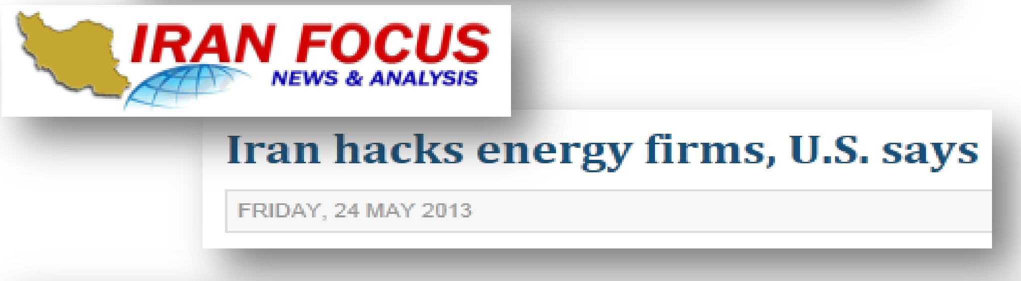
After Stuxnet, waiting on Pandora's box



HUFFPOST TECH

Report: Stuxnet Virus May Have Improved Iran's Ability To Enrich Uranium

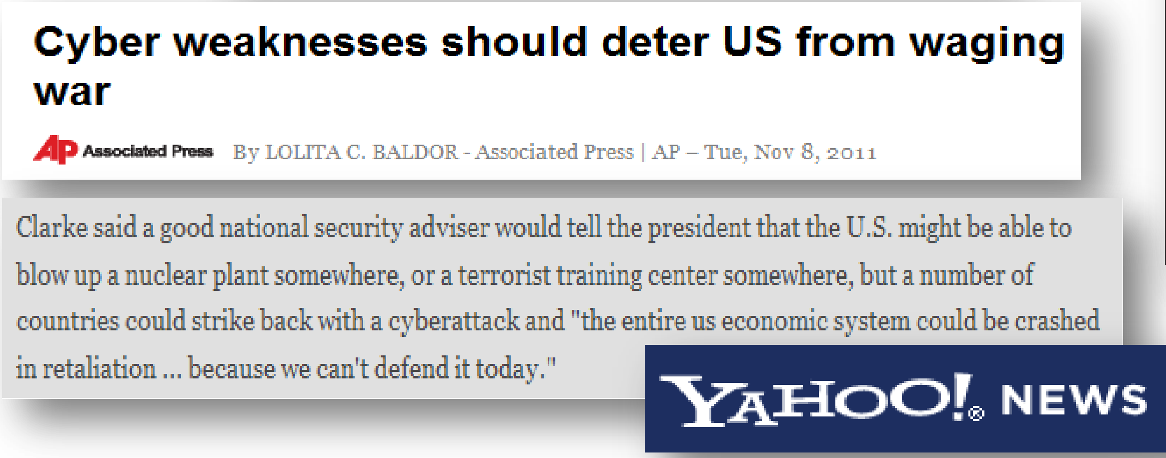
Huffington Post UK | By Michael Rundle
Posted: 16/05/2013 11:01 BST | Updated: 16/05/2013 11:23 BST



IRAN FOCUS
NEWS & ANALYSIS

Iran hacks energy firms, U.S. says

FRIDAY, 24 MAY 2013

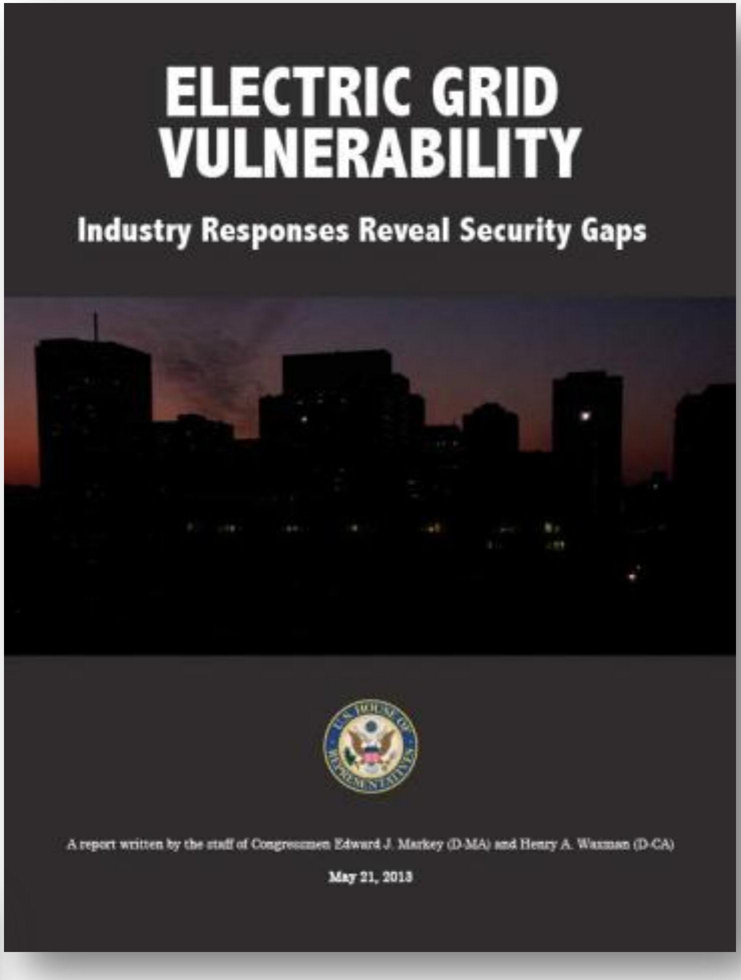


Cyber weaknesses should deter US from waging war

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

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."

YAHOO! NEWS



ELECTRIC GRID VULNERABILITY

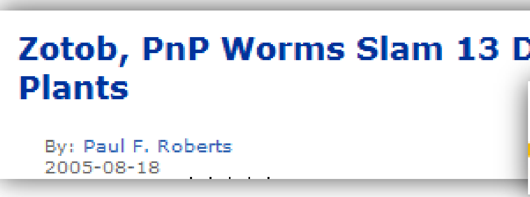
Industry Responses Reveal Security Gaps

A report written by the staff of Congressmen Edward J. Markey (D-MA) and Henry A. Waxman (D-CA)

May 21, 2013

The Dawn of the Cold Cyber-War Era

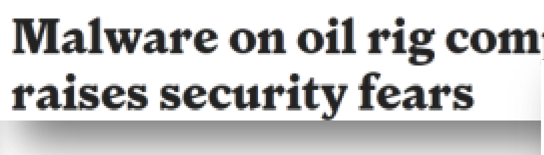
Overview



Zotob, PnP Worms Slam 13 DaimlerChrysler Plants

By: Paul F. Roberts
2005-08-18

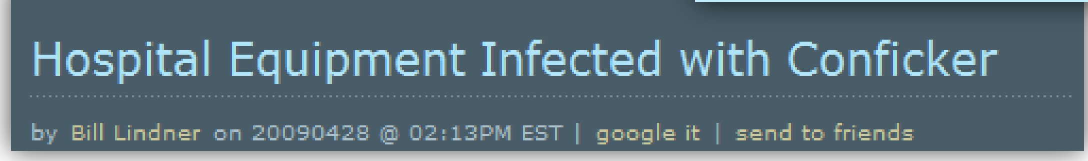
eWEEK.COM



Malware on oil rig computers raises security fears

HOUSTON CHRONICLE
ENERGY

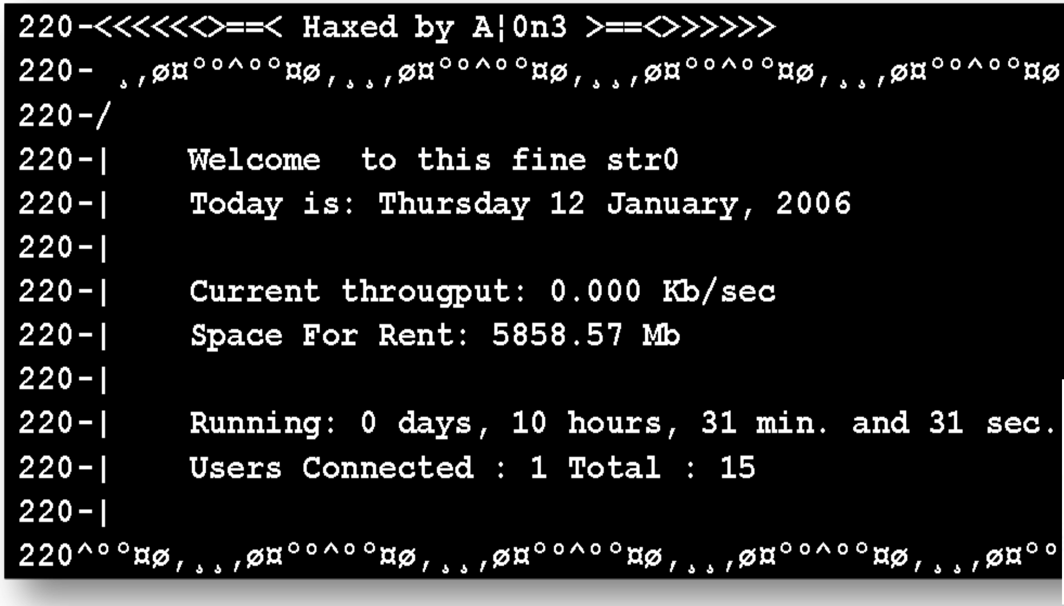
infopackets
Deliciously Addictive Tech News Served Daily



Hospital Equipment Infected with Conficker

by Bill Lindner on 20090428 @ 02:13PM EST | google it | send to friends

```
ight (c) Microsoft Corporation, 1991-1993.  All rights reserved.
ight (c) Hewlett-Packard Corporation, 1985-1993.  All rights reserved
ight (c) 3Com Corporation, 1985-1993.  All rights reserved.
```



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

The Lack of Patching

CERN Computer Centre

Integrity

- S/W development live-cycles
- Thorough regression testing
- Nightly builds
- Full configuration management

Availability

- Redundancy & virtualization

Exceptions

- “One-offs”; stand-alone systems

CERN Control Centre

Safety!

- Needs heavy compliance testing (vendor & utility)
- Potential loss of warranties & certification (e.g. SIL)

Availability

- Rare maintenance windows

Legacy

- Old or embedded devices

The Problem of Patching

Integrity

- ▶ S/W development live-cycles
- ▶ Thorough regression testing
- ▶ Nightly builds
- ▶ Full configuration management

Safety!

- ▶ Needs heavy compliance testing (vendor & utility)
- ▶ Potential loss of warranties & certification (e.g. SIL)

Availab

- ▶ cy & virtualization

- ▶ ons"; stand-alone systems

Availability

- ▶ Rare maintenance windows

Legacy

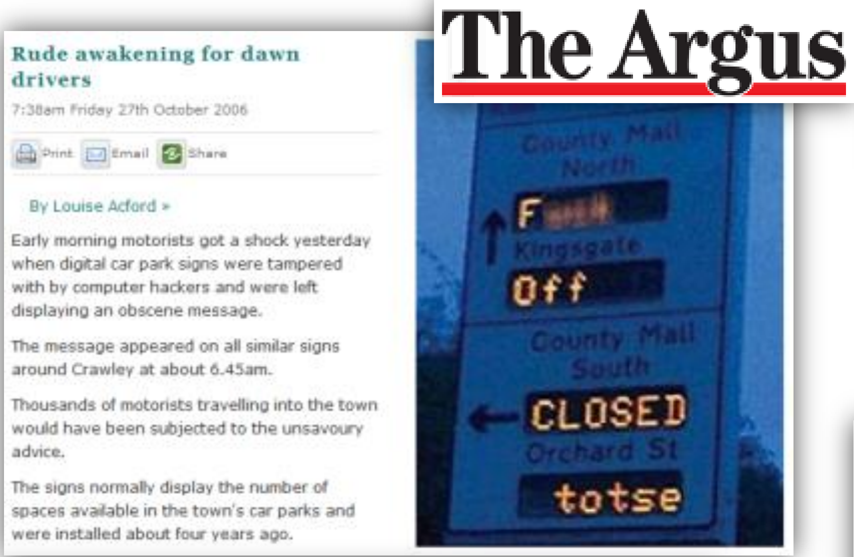
- ▶ Old or embedded devices

Security at CERN has been delegated.

We (work hard to) **enable & assist** our people **to fully assume** that responsibility!

They decide **when** to install **what** and **where**.

The Problem of Patching



The Argus

Rude awakening for dawn drivers

7:38am Friday 27th October 2006

Print Email Share

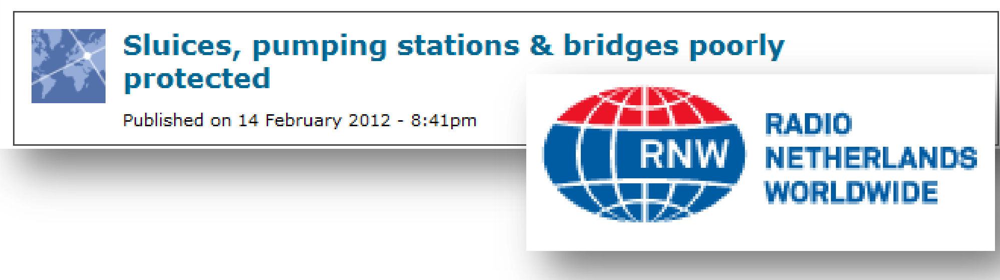
By Louise Acford »

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.

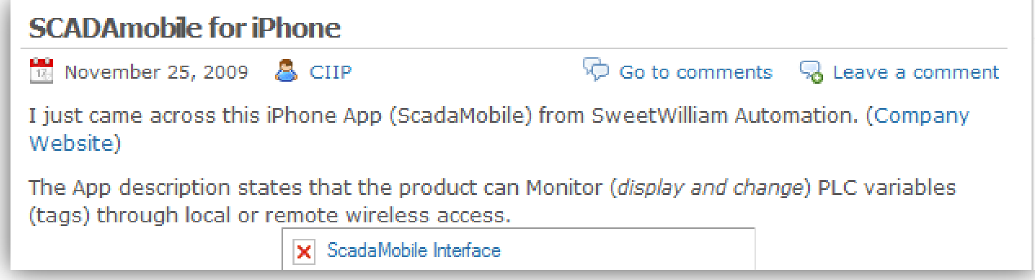
Thousands of motorists travelling into the town would have been subjected to the unsavoury advice.

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



Sluices, pumping stations & bridges poorly protected

Published on 14 February 2012 - 8:41pm



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.

☒ ScadaMobile Interface

"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…"

The Lack of Access Controls

CERN Computer Centre

CERN Control Centre

Security

- Split of AuthN & AuthZ
- SSO, LDAP & AD
- Kerberos, x509 & 2-factor AuthN

Laziness

- We still deal with people
- Password vs. Phishing

Complexity

- WLCG: a network of computer centres

Safety!

- Access always to be guaranteed
- Shared accounts
- Encryption too “heavy”

Legacy

- Default passwords
- Undocumented backdoors
- Impossible IdM integration
- No ACLs, iptables, etc.

The Problem of Access Control

Security

- ▶ Split of AuthN & AuthZ
- ▶ SSO, LDAP & AD
- ▶ Kerberos, x509 & 2-factor AuthN

Safety!

- ▶ Access always to be guaranteed
- ▶ Shared accounts
- ▶ Encryption too "heavy"

Laziness

- ▶ Wo[illegible]ling with people
- ▶ [illegible]s. Phishing

Legacy

- ▶ Default passwords
- ▶ Undocumented backdoors
- ▶ Impossible IdM integration
- ▶ No ACLs, iptables, etc.

Co[illegible]

- ▶ W[illegible] a network of computer centre

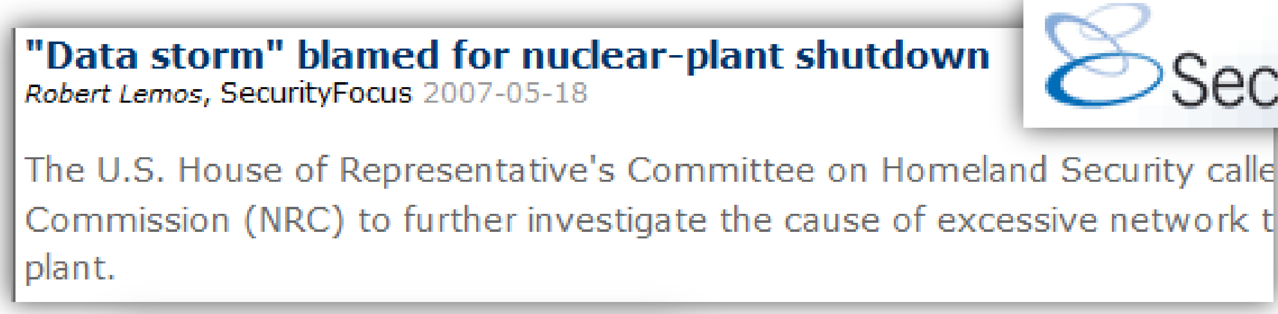
CERN strives to bring IT to the plant floor.

CERN IT provides **general services**.

CERN CERT provides **general protections**.

CERN controls experts run the show.

The Problem of Access Control



"Data storm" blamed for nuclear-plant shutdown

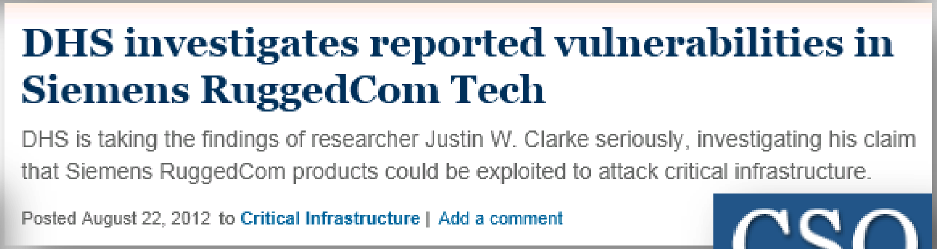
Robert Lemos, SecurityFocus 2007-05-18

The U.S. House of Representative's Committee on Homeland Security calle
Commission (NRC) to further investigate the cause of excessive network t
plant.

SecurityFocus™

SPIEGEL ONLINE

Fernwartung: Sicherheitslücke bedroht Hightech-Heizungen

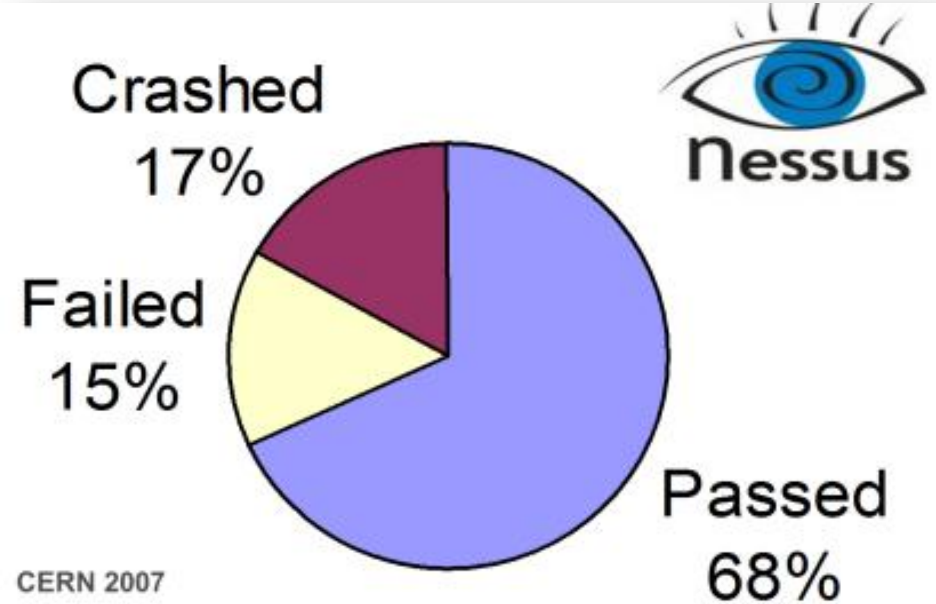


DHS investigates reported vulnerabilities in Siemens RuggedCom Tech

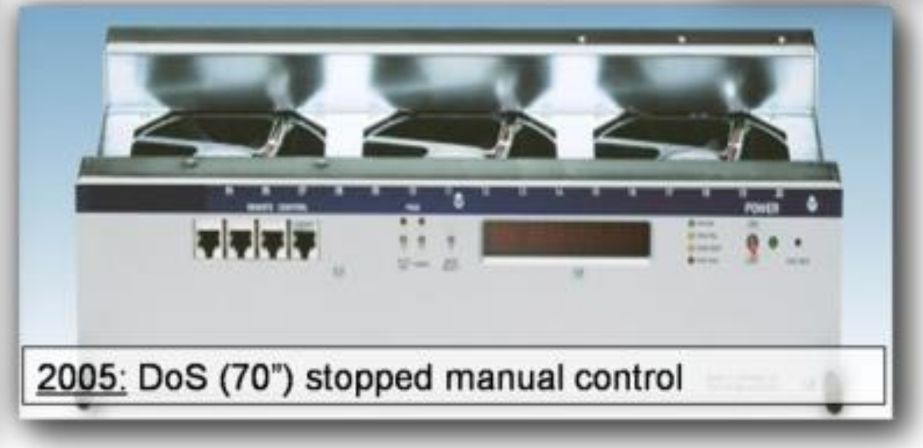
DHS is taking the findings of researcher Justin W. Clarke seriously, investigating his claim that Siemens RuggedCom products could be exploited to attack critical infrastructure.

Posted August 22, 2012 to Critical Infrastructure | Add a comment

CSO SECURITY AND RISK



CERN 2007



2005: DoS (70") stopped manual control

The Lack of Robustness

Robustness

- ▶ (Externally sponsored) penetration testing & vulnerability scanning

Security

- ▶ Decades of experience & knowledge
- ▶ CSIRT: Protection, detection & response
- ▶ Responsible disclosure

Robustness

- ▶ Use-cases ***and*** abuse-cases
- ▶ Not always compliant to standards
- ▶ No certification (yet?)

Security

- ▶ Not integral part… …or through obscurity
- ▶ Low priority, low knowledge
- ▶ Unwillingness to share incidents
- ▶ No laws; too many guidelines

The Problem of Robustness

CERN Computer Centre

CERN Control Centre

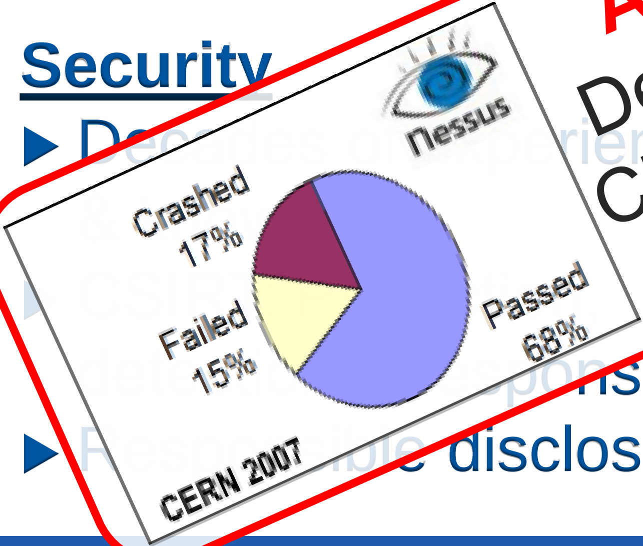
Robustness
- ▶ (Externally sponsored) penetration testing & vulnerability scanning

Security
- ▶ Dec[illegible]rience
- ▶ CS[illegible]
- [illegible]ponse
- ▶ R[illegible]ble disclosure

Robustness
- ▶ Use cases and abuse cases
- ▶ Not always compliant to standards
- ▶ No certification (yet?)

Security
- ▶ Not integral part… …or through obscurity
- ▶ Low priority, low knowledge
- ▶ Unwillingness to share incidents
- ▶ No laws; too many guidelines

Asset inventories are key to CERN:
Devices, websites, S/W, dependencies.
CERN **pen tests everything** (we can get hands on).
(IPv6 is our next nightmare.)



The Problem of Robustness

PCS are (still) not designed to be secure.

They fulfil use-cases *and* abuse cases.

Defence-in-Depth is the key.

Make security part as functionality, usability, availability, maintainability, performance!

Align Control System Cyber-Security with IT security!

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

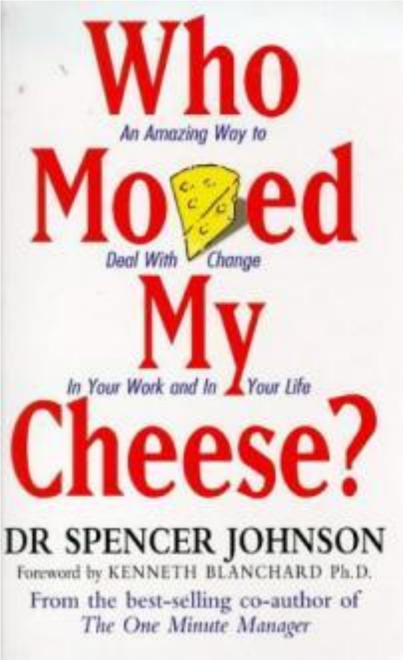
Hack the box!

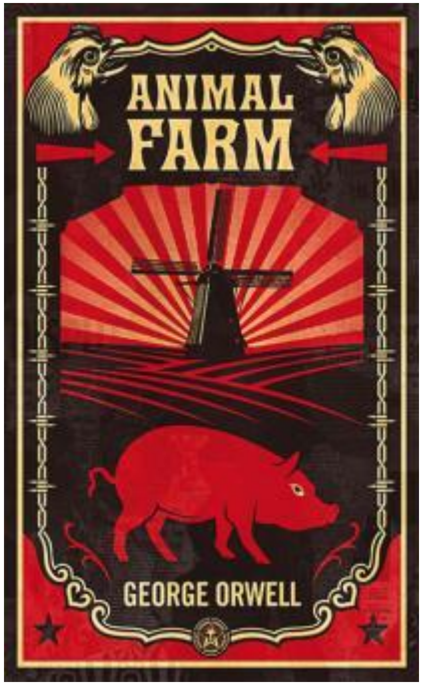
Buy any PCS on ebay and throw your favourite pen suite at it.

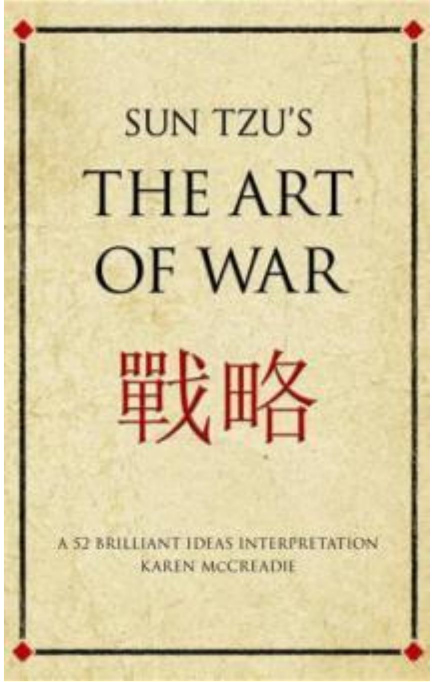
Push vendors & start responsible disclosure

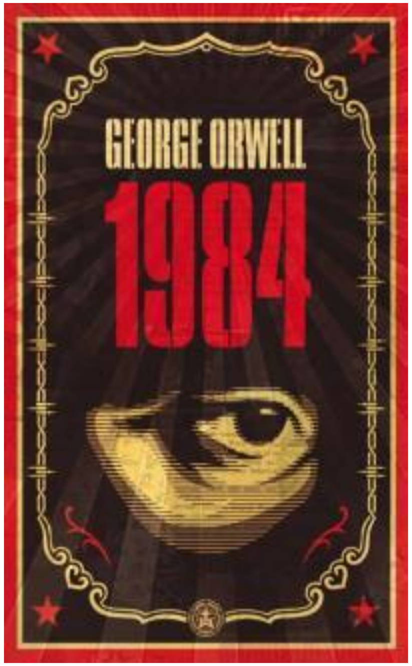
P.S. Why do I have to do due diligence (and bear the costs) instead vendors shipping out insecure applications/devices?

Summary


Who
An Amazing Way to
Moved
Deal With Change
My
In Your Work and In Your Life
Cheese?
DR SPENCER JOHNSON
Foreword by KENNETH BLANCHARD Ph.D.
From the best-selling co-author of
The One Minute Manager


ANIMAL
FARM
GEORGE ORWELL


SUN TZU'S
THE ART
OF WAR
戰略
A 52 BRILLIANT IDEAS INTERPRETATION
KAREN MCCREADIE


GEORGE ORWELL
1984

Literature