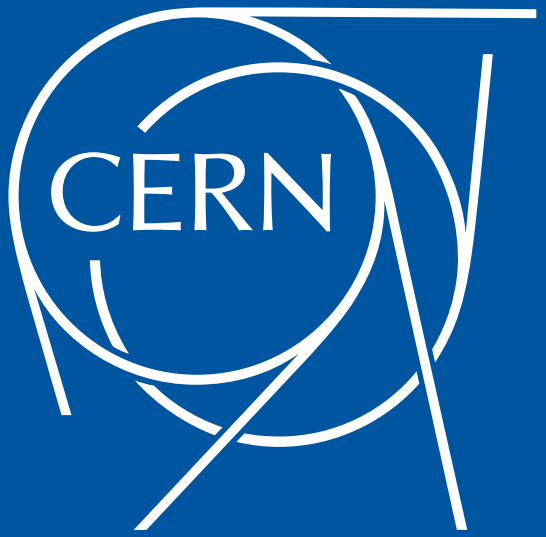
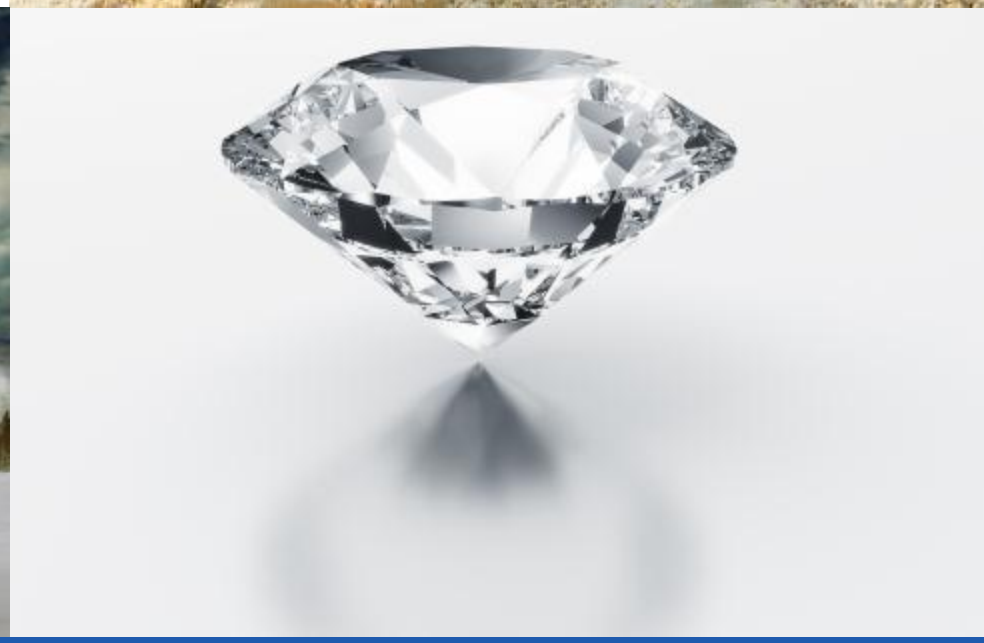

CERN

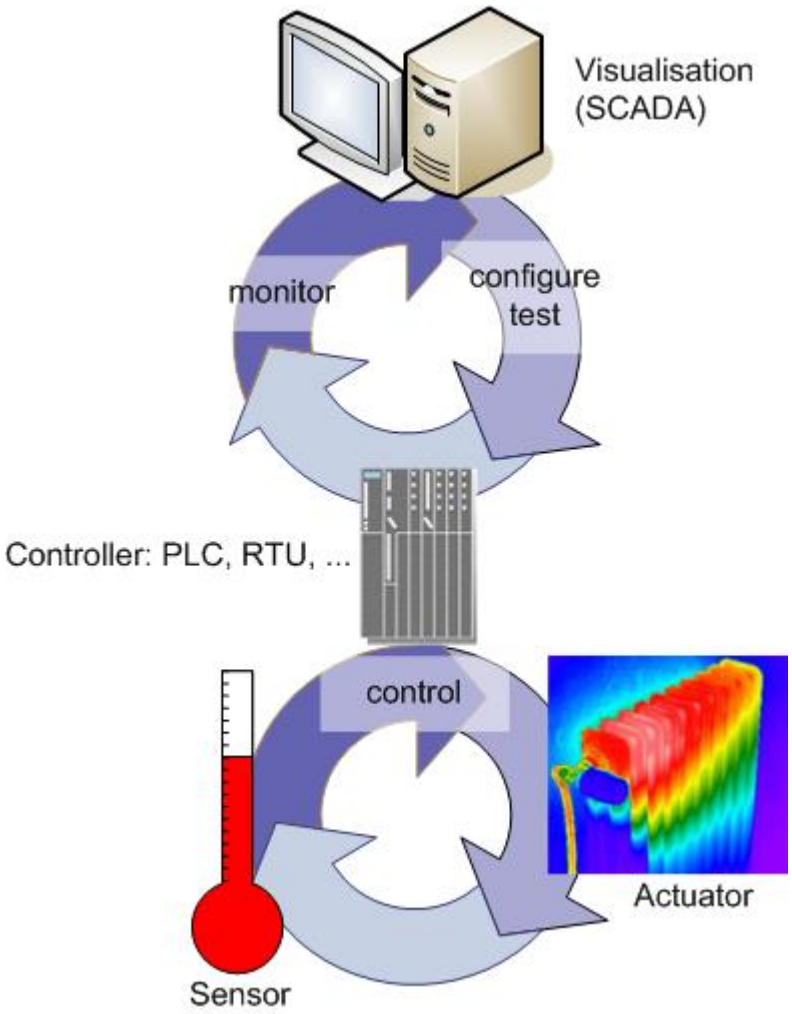
Why SCADA Security is NOT like Computer Centre Security

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

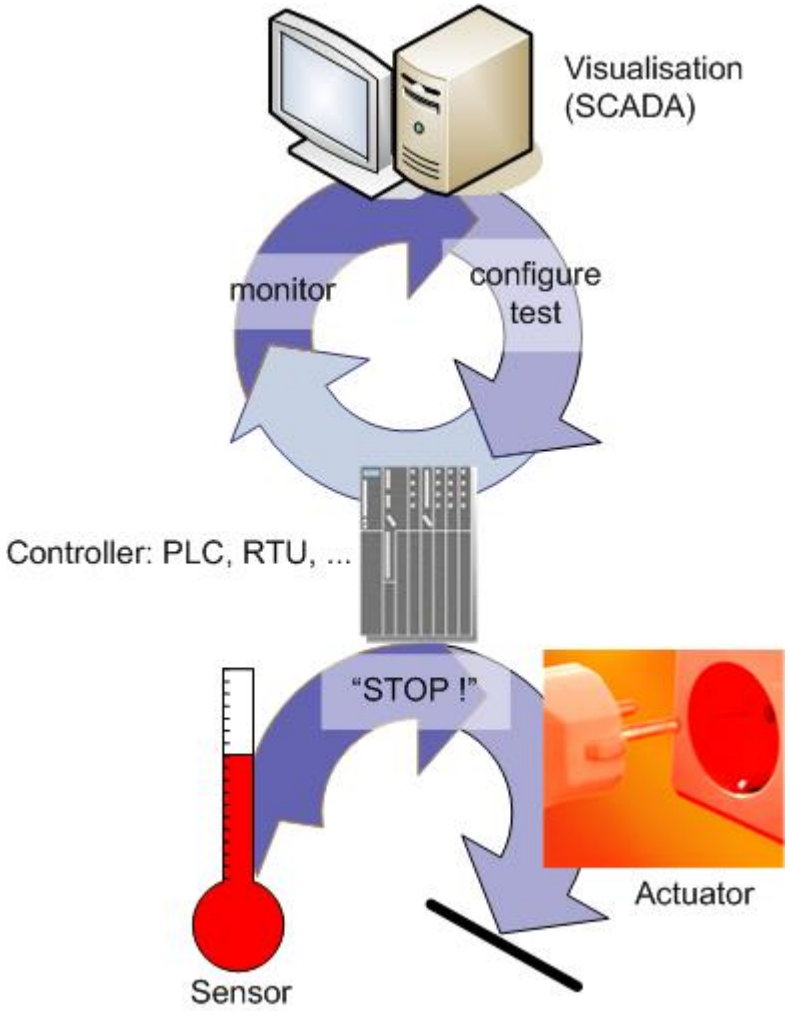


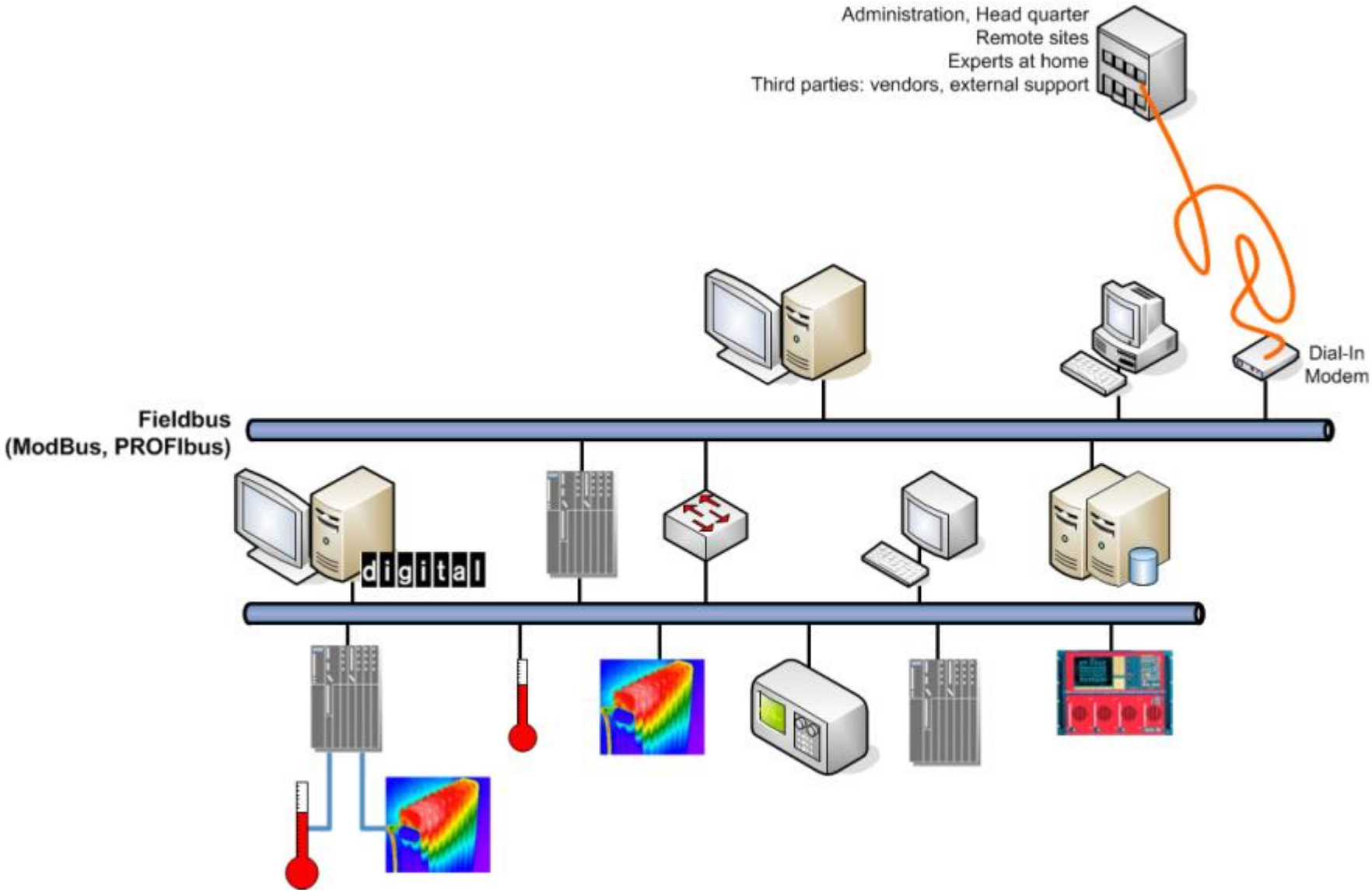
Overview

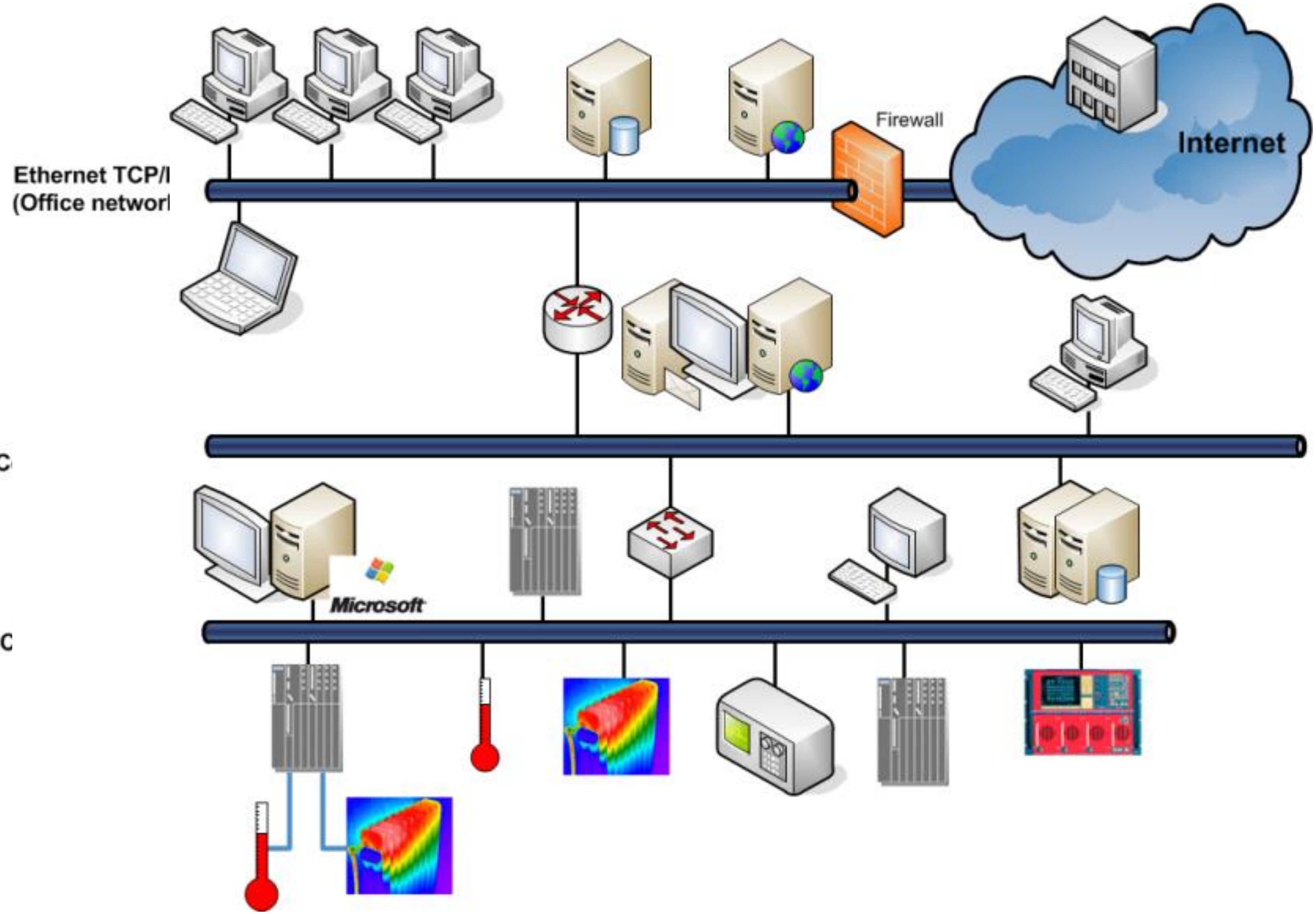
Process Control System (PCS)



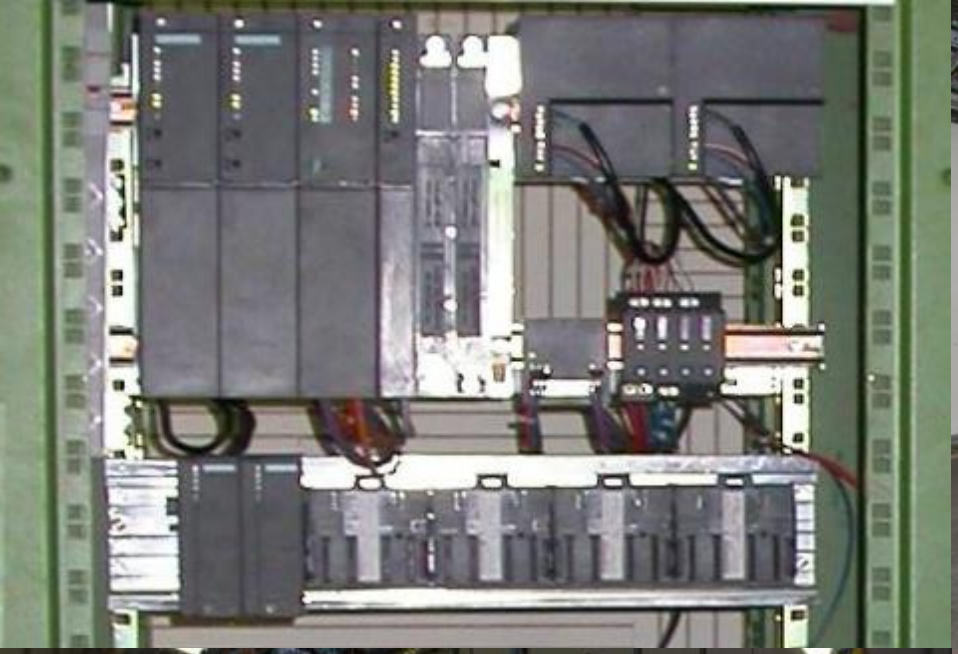
Safety System




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



Typical Control Systems & Devices

COBB County Electric, Georgia

Middle European Raw Oil, Czech Republic

Athens Water Supply & Sewage

CERN Control Centre

Critical (Cyber-)Infrastructures

Why SCADA Security is NOT like Computer Centre Security
Dr. Stefan.Lueders@cern.ch
Openlab Summer Student Lectures, August 28th 2014

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

BBC

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

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 n church lead
Easter qual downtown

Enter reality

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn | Twitter 5 | Facebook 2 | +1

By: Brian Prince
2010-07-16
Article Rating: ★★★★★ / 3
There are 0user comments on this IT Security & Netwo
Reviews story.

COMPUTERWORLD

News

Siemens: German customer hit by industrial worm

By Robert McMillan

1 Comment | Gefällt mir | +1 0

Siemens confirmed Tuesday that one of its customers
worm designed to steal secrets from industrial control

has been notified of one

SPIEGEL ONLINE

Mossad's Miracle Weapon

Stuxnet Virus Opens New Era of Cyber War

By Holger Stark

dpa

The Mossad, Israel's foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet. The first 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

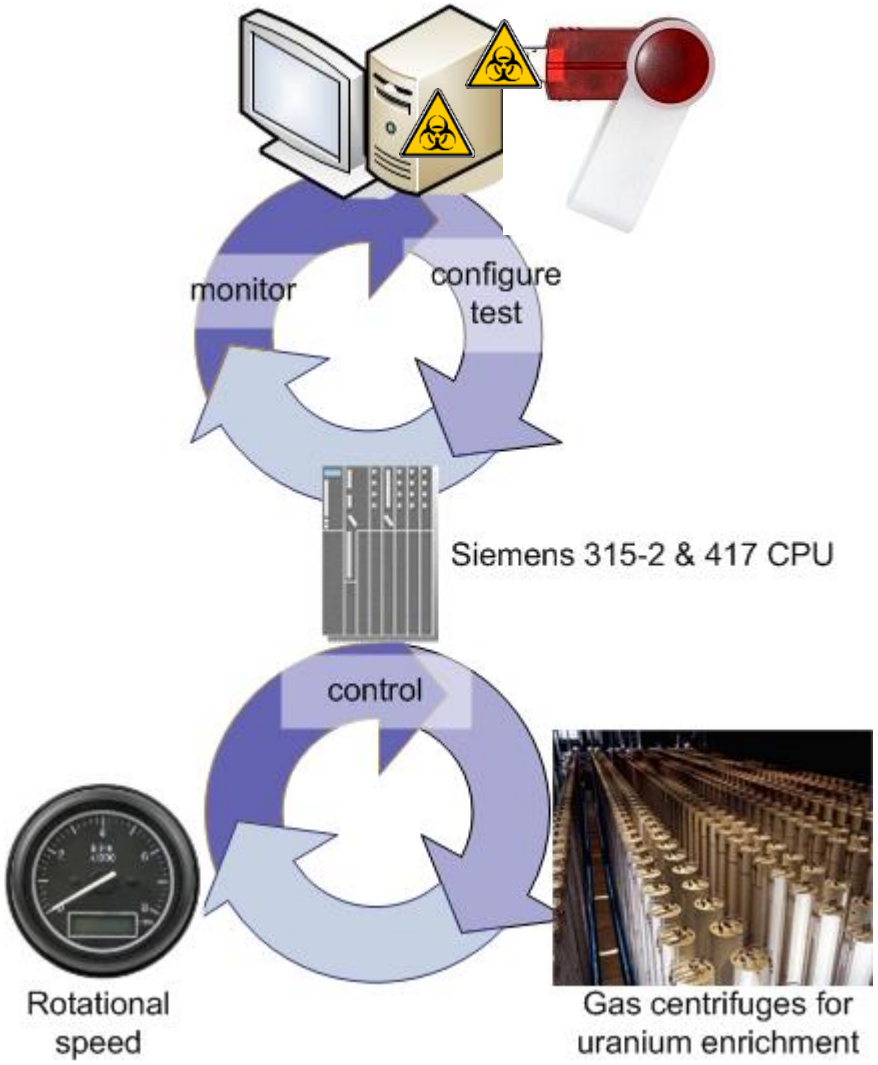
Sep 30th 2010 | from the print edition

Like 274 | Tweet 0

tified Iranian organization, according to Sergey Ulasen,
rus kernel department at VirusBlokAda, in Minsk, Belarus.
m, which does not own the type of SCADA (supervisory
uisition) systems targeted by the worm, "told us their
rebooted without any reason," Ulasen said in an e-mail

PC-Level:

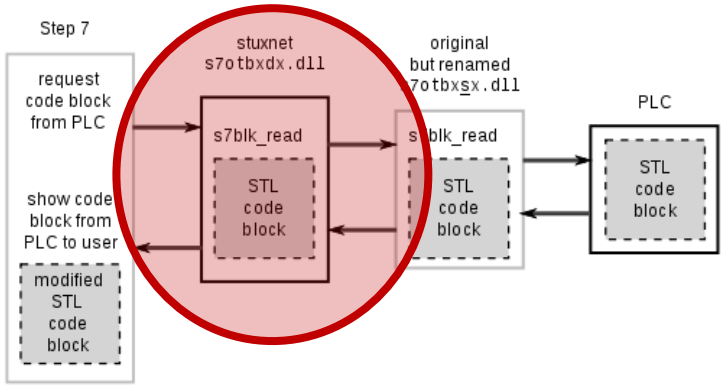
- Infiltration of infected USB stick into plant by malicious act or through social engineering.
- Compromizing Windows PCs with 4(!) zero-day exploits (worth >$100k)
- 4-5 evolutions starting 6/2009
- Infected 100.000 PCs (60% Iran,10% Indonesia)
- Hiding using “rootkit” techno & two stolen certificates
- Infecting other hosts and establishing connection “home”

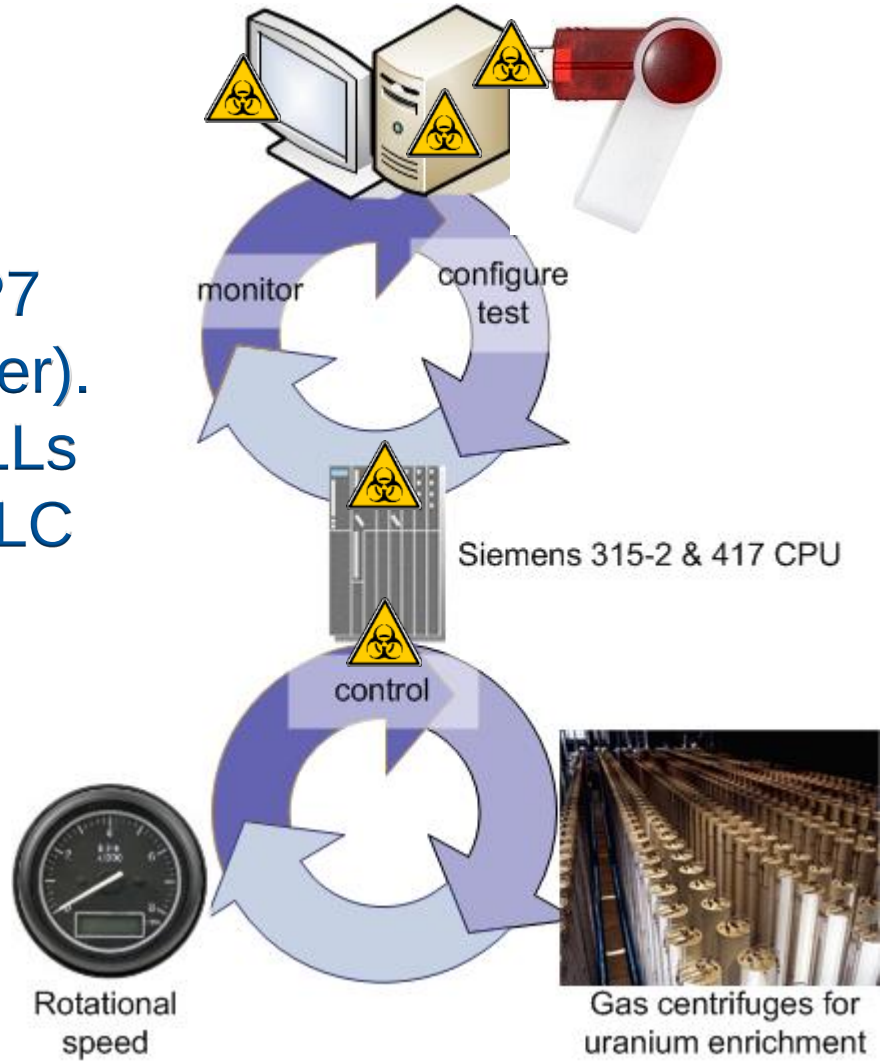


So far, nothing new: A standard, but expensive virus!

PLC Level:

- Checking local configuration for Siemens PCS7/STEP7/WINCC
- If found, copying into local STEP7 project folder (to propagate further).
- Replacing S7 communication DLLs used for exchanging data with PLC

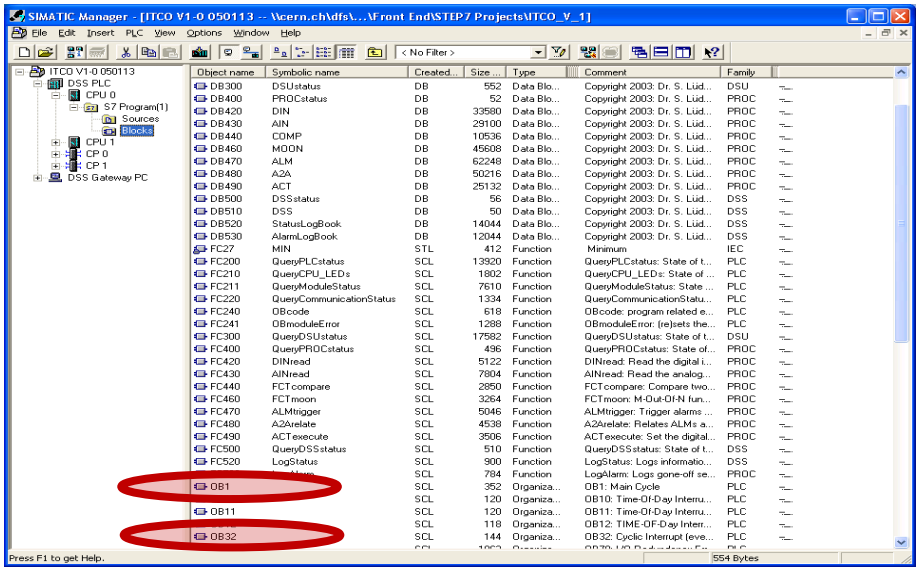


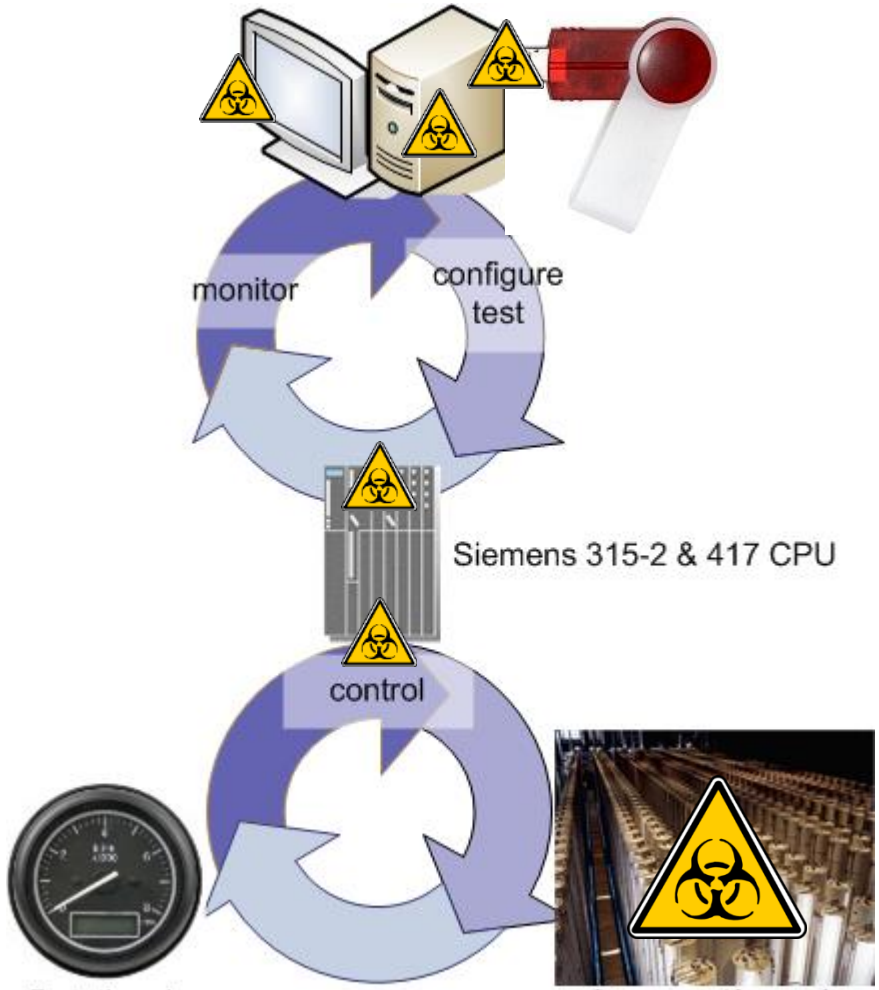


Stuxnet is now the "Man in the Middle" controlling the communication between SCADA & PLC.

Process Level:

- "Fingerprinting" connected PLCs
- If right PLC configuration, downloading/replacing code (between 17 and 32 FBs & DBs)





GAME OVER: varying rotational speed of centrifuges wearing them out and inhibiting Uranium enrichment.
"Man in the Middle" made SCADA displays look fine.

The Washington Post
NATIONAL

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

After Stuxnet, waiting on Pandora's box

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

Huffington Post UK | By Michael Ru
Posted: 16/05/2013 11:01 BST | Upda

HUFFPOST TECH

Iran hacks energy firms, U.S. says

The Washington Times

IRAN FOCUS

Obama hits pause on U.S. action in face of crippling cyber strikes from Syria, Iran

By Shaun Waterman - The Washington Times

Wednesday, August 28, 2013

Cyber
war

Associated P

Email

RELATED CONTENT

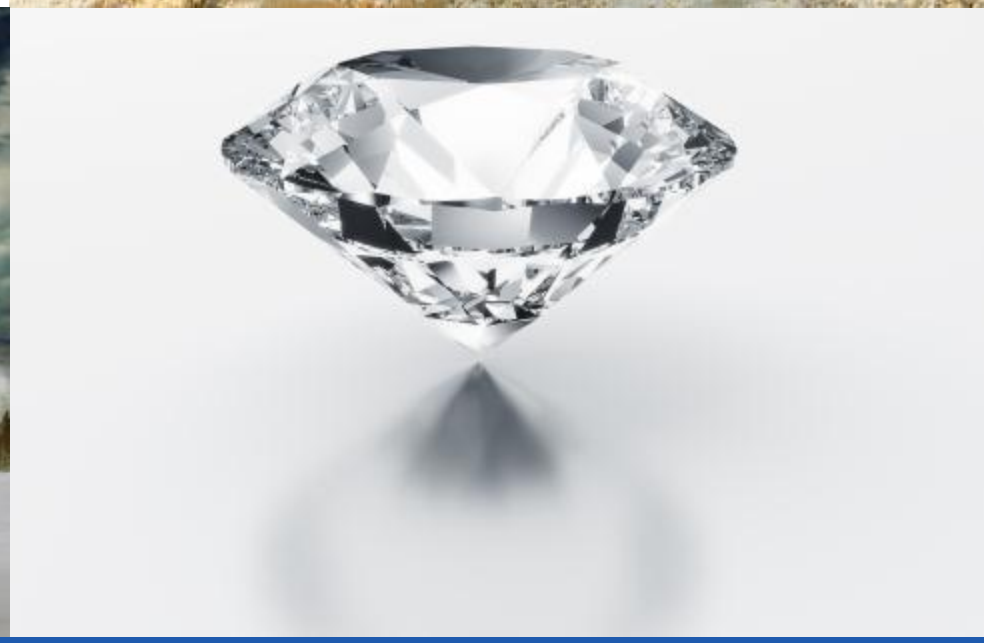
In this Feb. 19, 2010 photo, Richard A. Clarke, a former advisor to the president ...

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.

China, North Korea, Iran and Russ
could destroy power grids, bankin

The U.S. military, he said, is entire
conflict in which troops trot out or

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."



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


```
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

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)

Availability

- Redundancy & virtualization

Availability

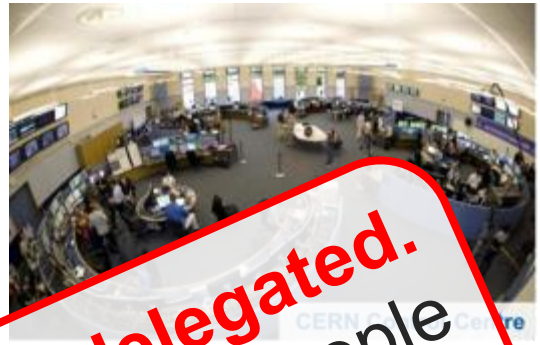
- Rare maintenance windows

Exceptions

- “One-offs”; stand-alone systems

Legacy

- Old or embedded devices



Integrity

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

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**.

Availability

- Rare maintenance windows

Legacy

- Old or embedded devices

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.

The Argus

Sluices, pumping stations & bridges poorly protected

Published on 14 February 2012 - 8:41pm

RNW RADIO NETHERLANDS WORLDWIDE

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..."

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

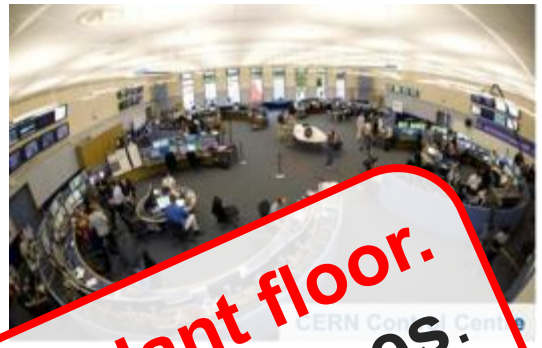
- We still deal with people
- Password vs. Phishing

Legacy

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

Complexity

- WLCG: a network of computer centres



Security

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

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

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.

Laziness

- We [illegible] dealing with people
- [illegible]. Pushing

Legacy

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

C[illegible]

- We [illegible] network of computer centres

"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

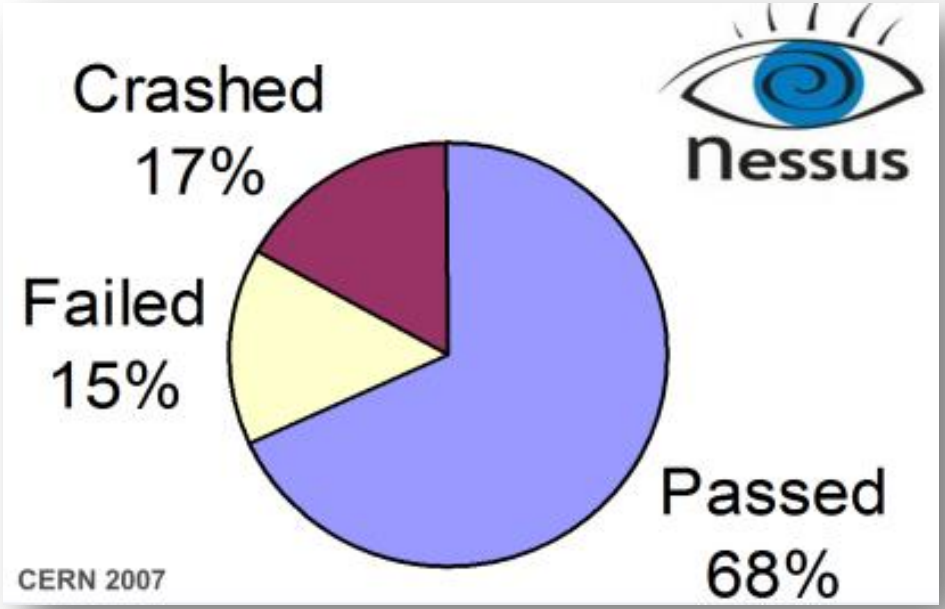
Fernwartung: Sicherheitslücke bedroht Hightech-Heizungen

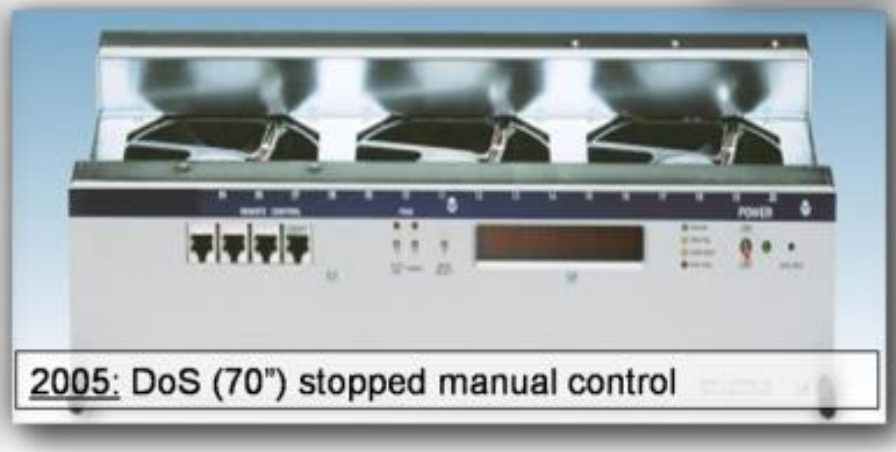
DHS investigates reported vulnerabilities in Siemens RuggedCom Tech

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





Robustness

- (Externally sponsored) penetration testing & vulnerability scanning

Robustness

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

Security

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

Security

- Not integral part…

…or through obscurity

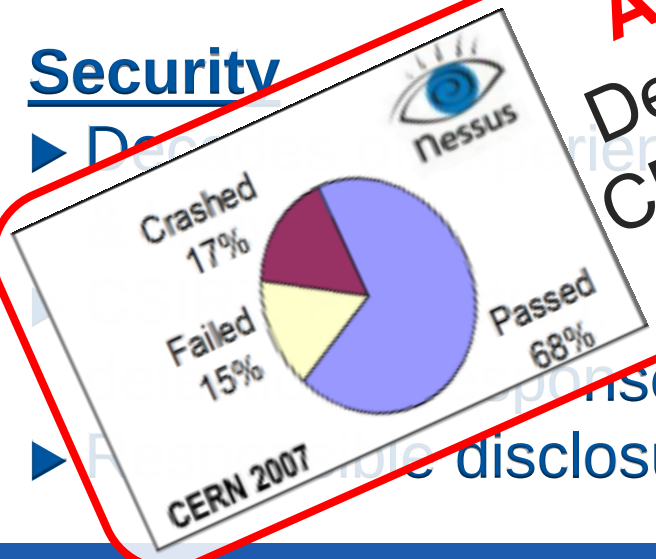
- Low priority, low knowledge
- Unwillingness to share incidents
- No laws; too many guidelines

Robustness

- (Externally sponsored) penetration testing & vulnerability scanning

Security

- Responsible disclosure



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

Security

- Not integral part…

…or through obscurity

- Low priority, low knowledge
- Unwillingness to share incidents
- No laws; too many guidelines

Confidentiality:

- Customer data available to others

Integrity:

- Manipulation of reading data
- Misuse of meter as an attack platform

Availability:

- Data not available in a timely manner…

Power Grid Is Found Susceptible to Cyberattack

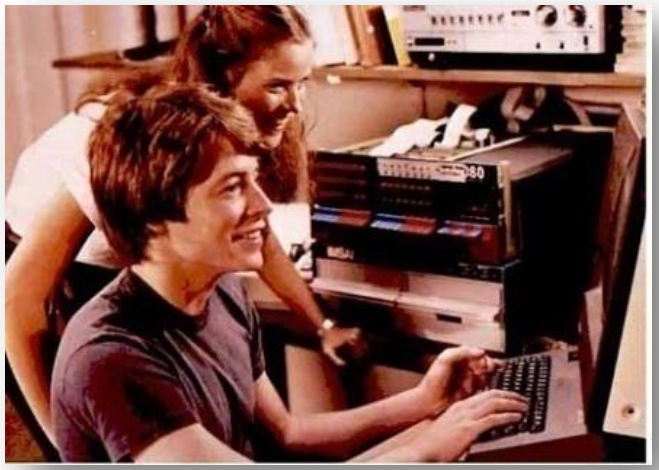
PCWorld

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.

PEOPLE WH
ALSO READ



PCS are (still) not designed to be secure.

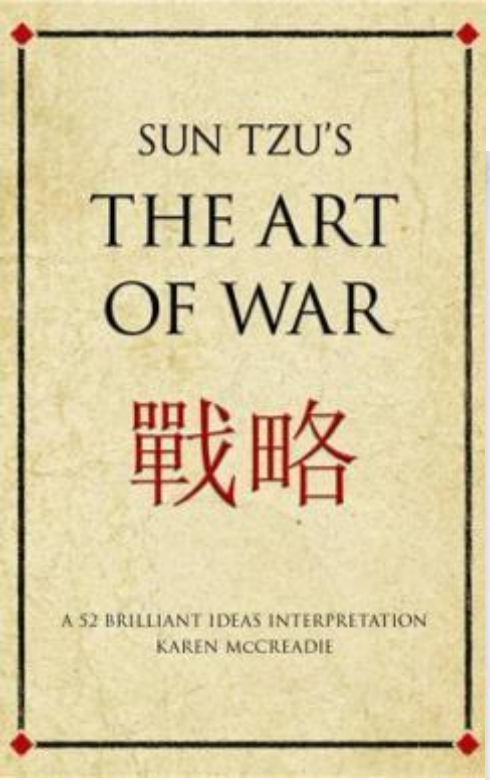
They fulfil use-cases *and* abuse cases.

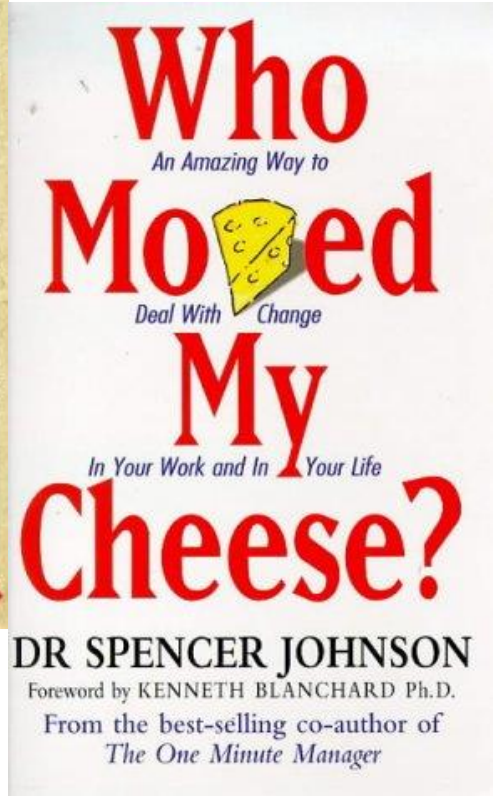
Defence-in-Depth is the key.
Make security part as functionality, usability, availability, maintainability, performance!

Align Control System Cyber-Security with IT security!
Patch procedures, access protection, robustness, certification & documentation need significant improvement.

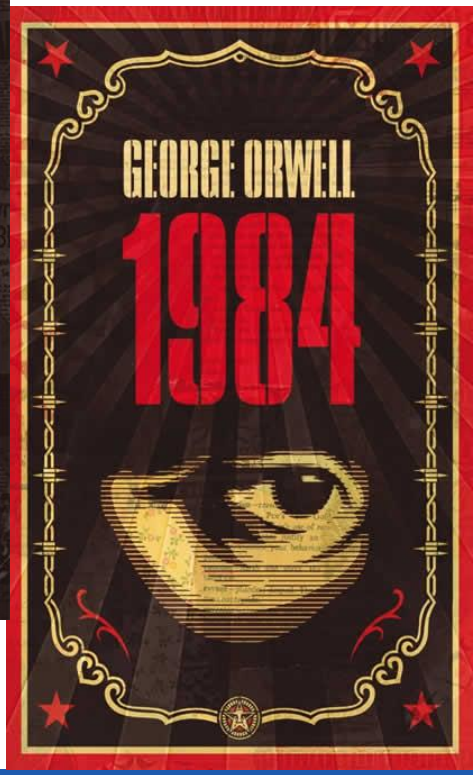
Hack the box!
Buy any PCS on ebay and throw your favourite pen suite at it.
Push vendors & start responsible disclosure

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


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


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


GEORGE ORWELL
1984

Literature