European Organization for Particle Physics

Exploring the frontiers of knowledge

CERN Control Centre

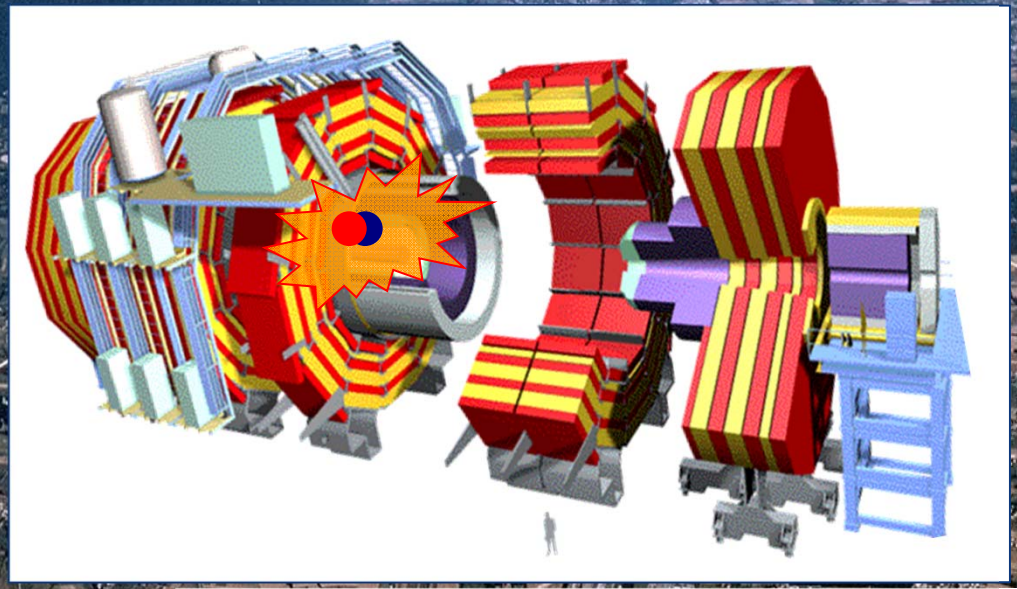
CERN Computer Centre

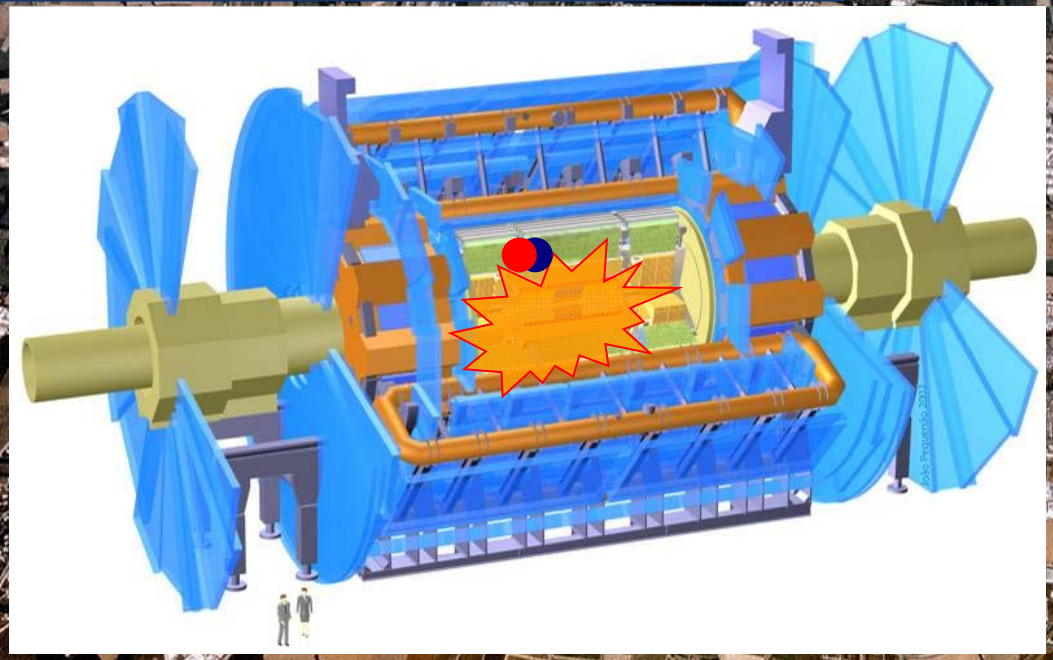
Why Control System Cyber-Security Sucks

Dr. Stefan.Lueders@cern.ch

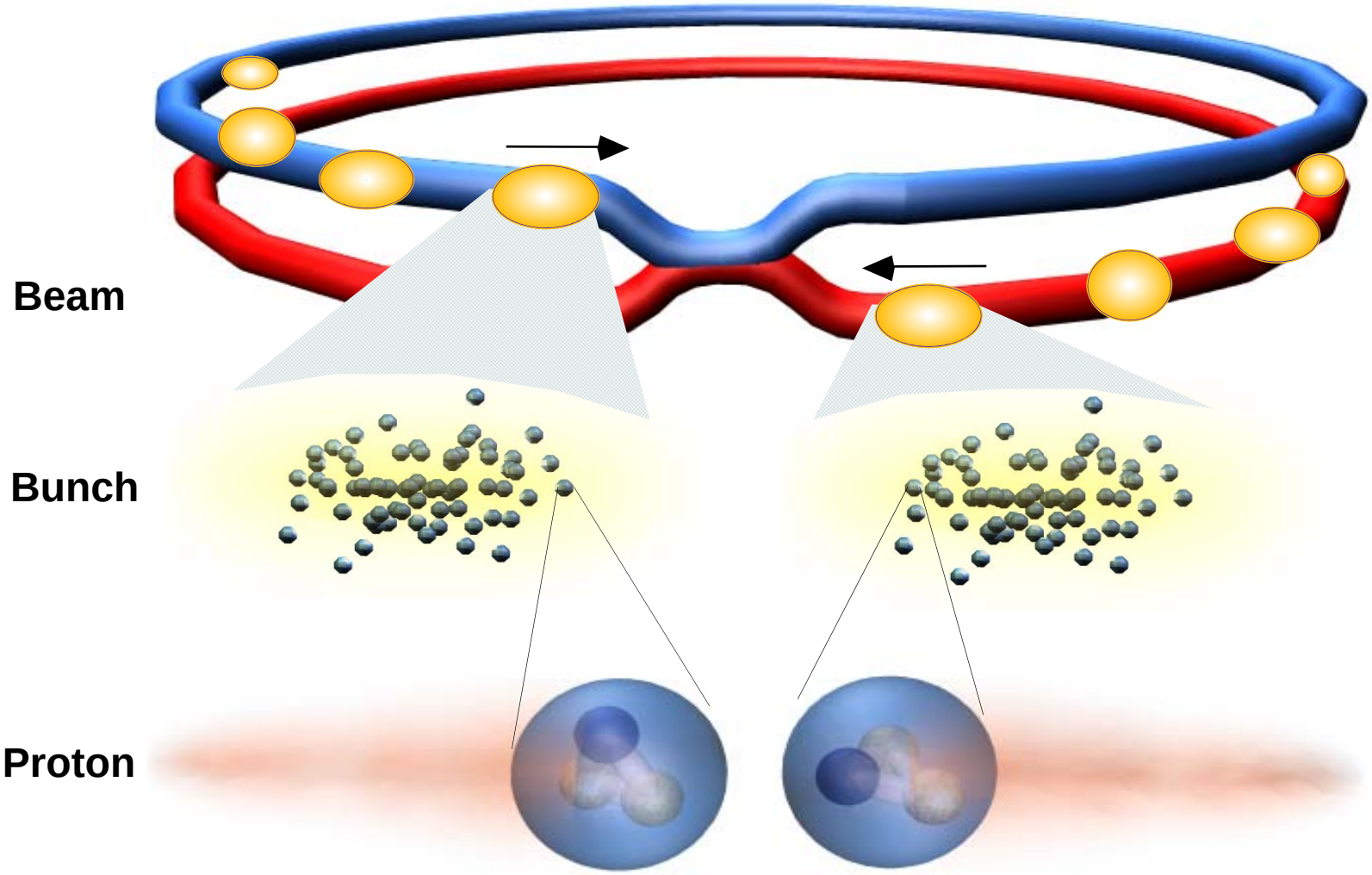
European Organization for Particle Physics

Exploring the frontiers of knowledge

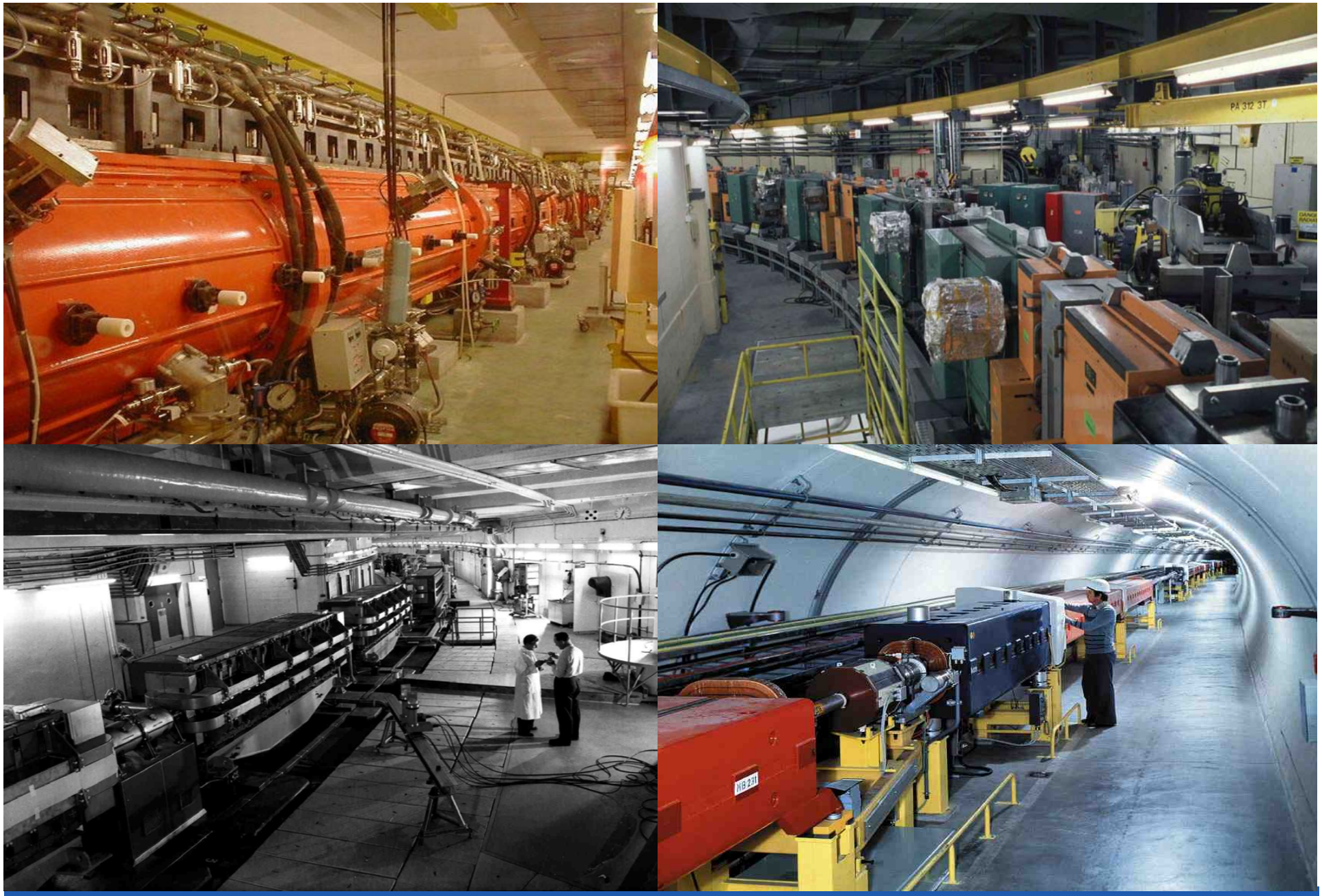




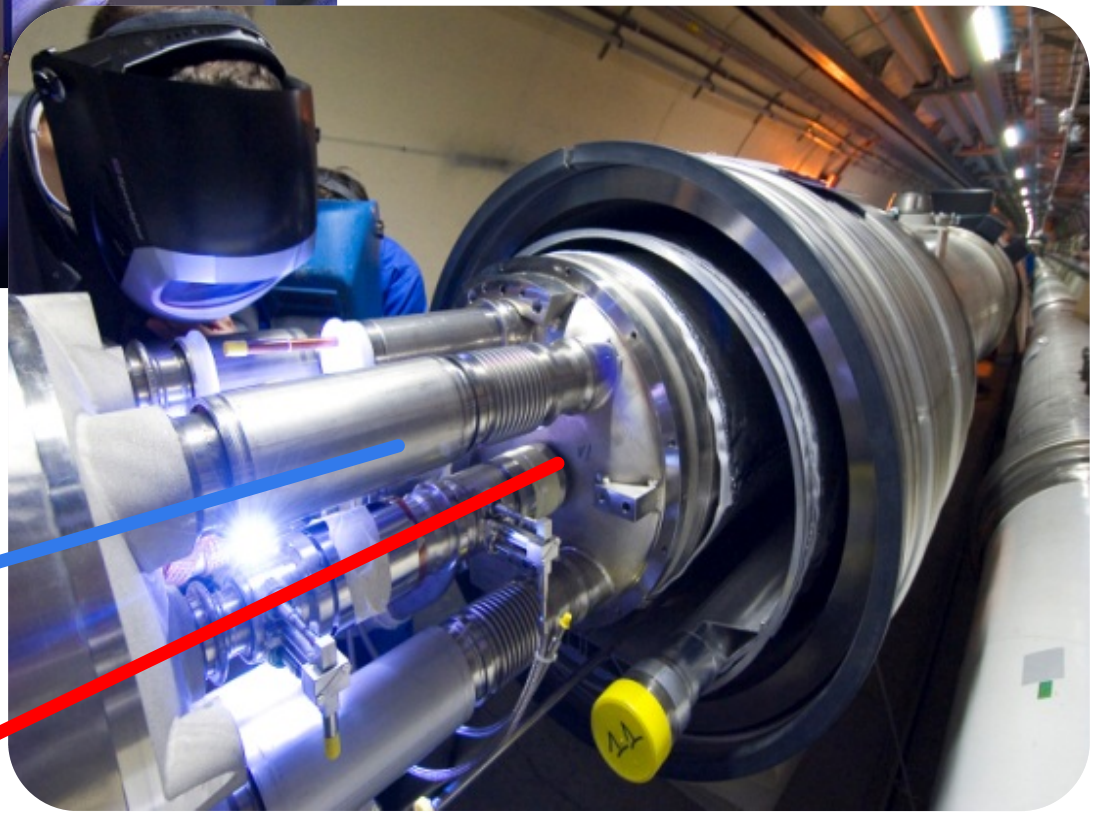
CERN Business Modell



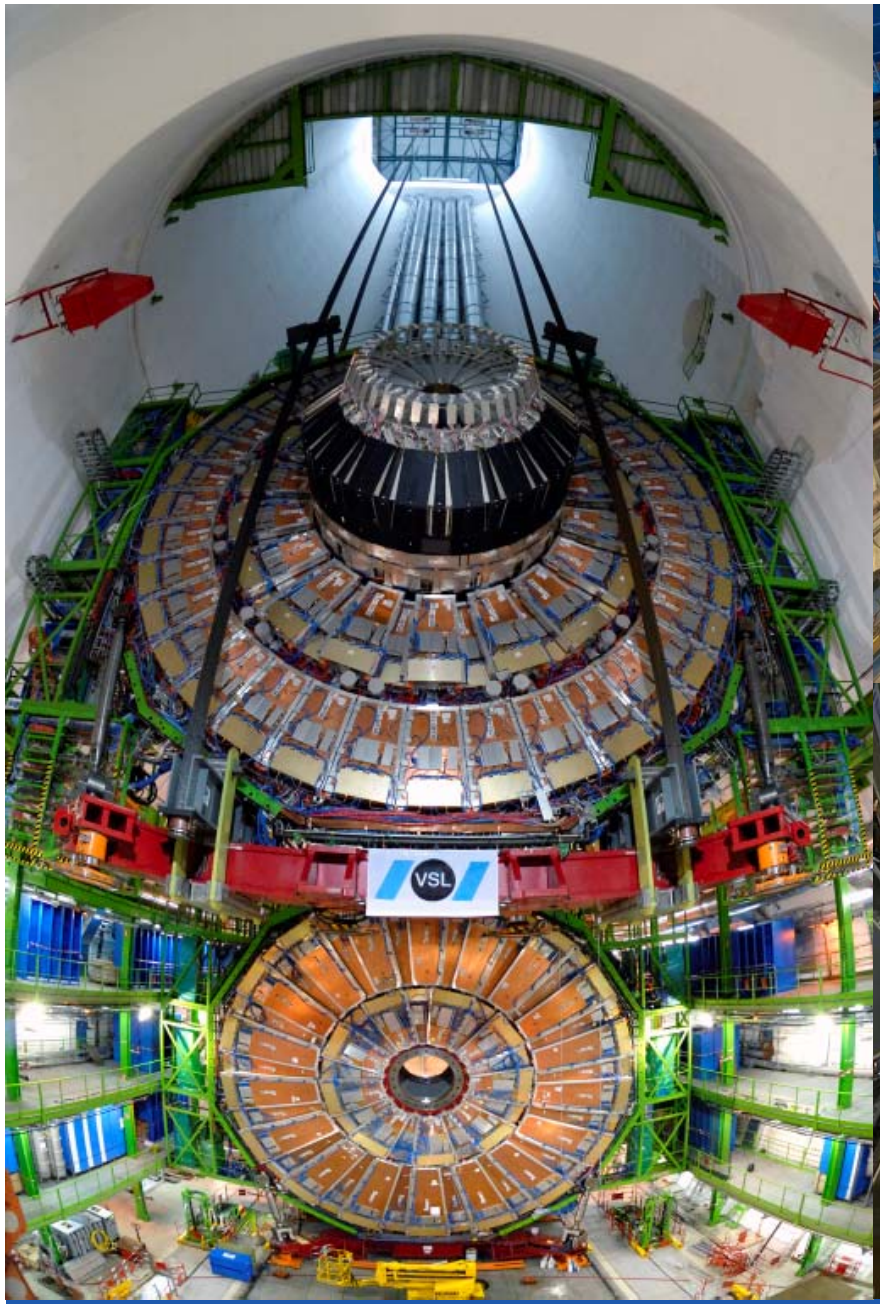
Accumulate protons, …

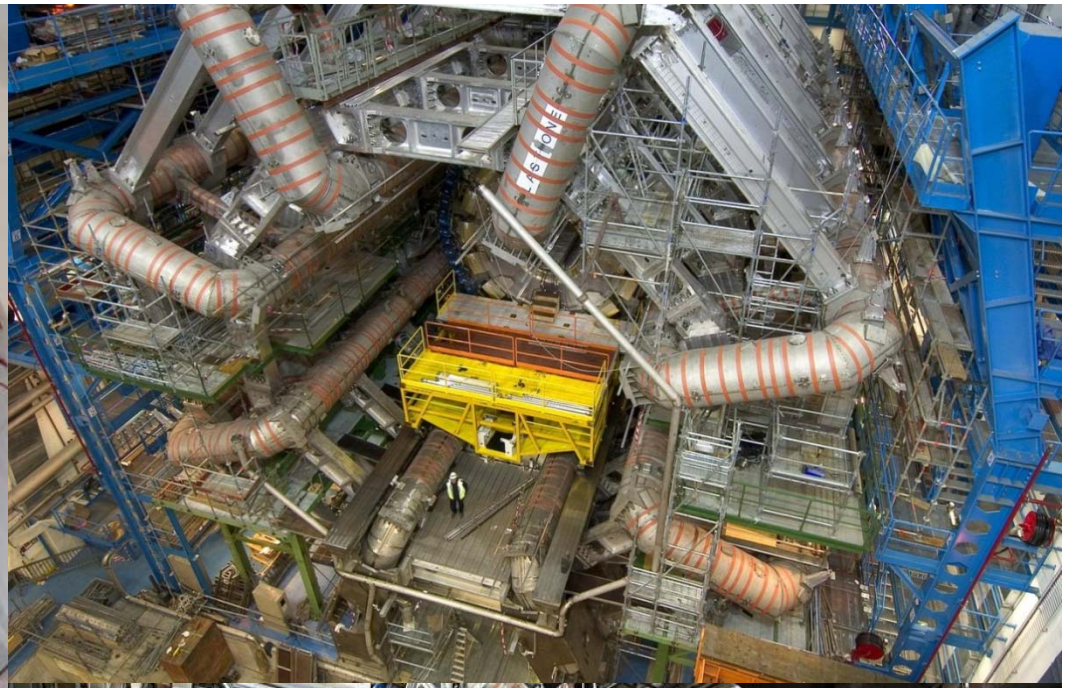


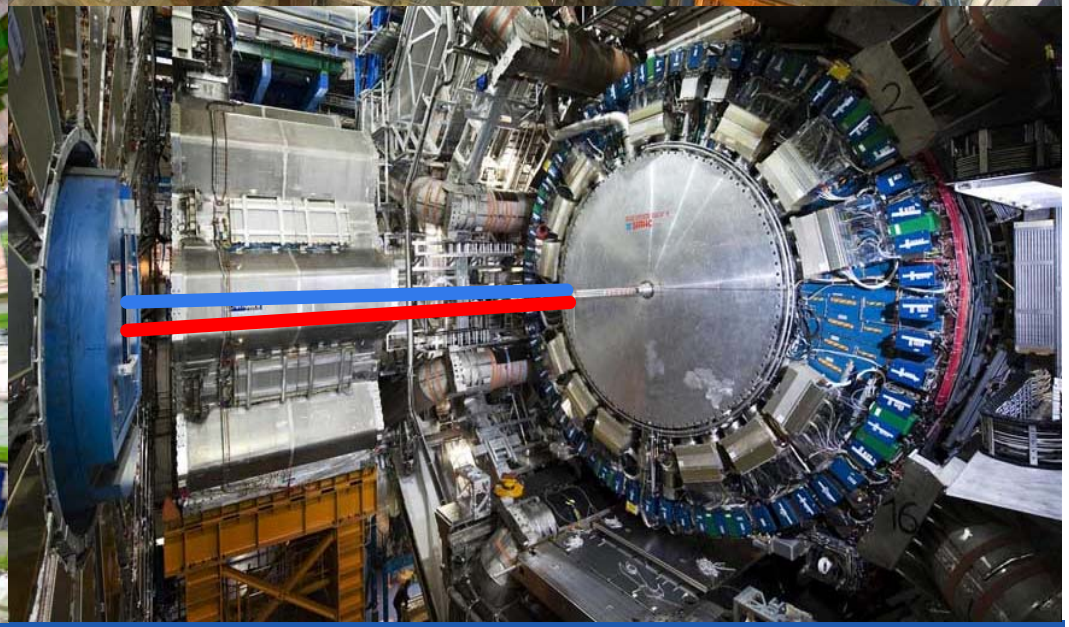
…accelerate them…



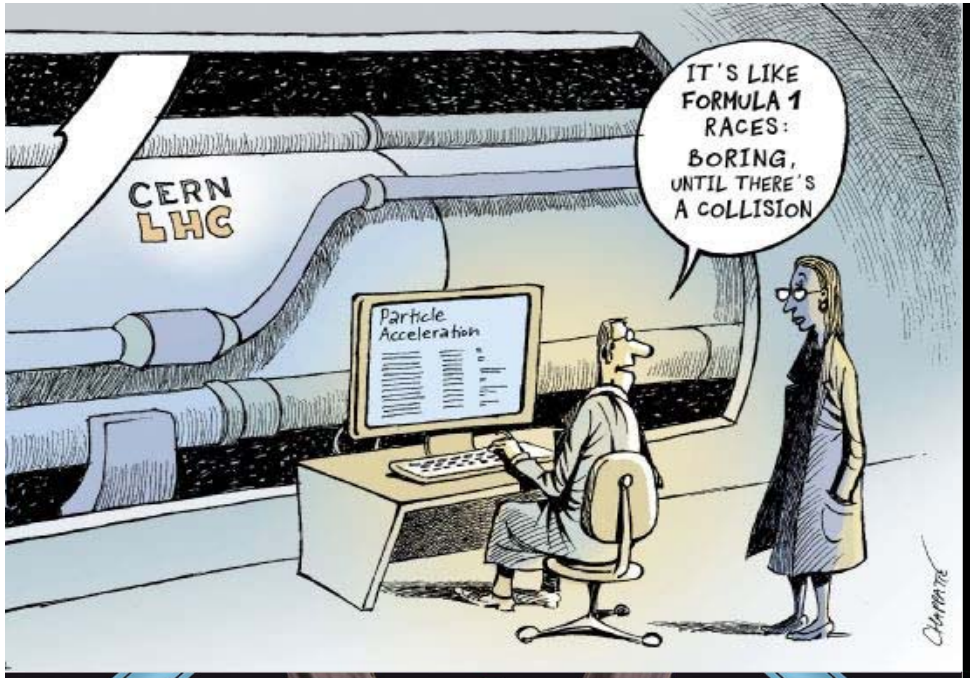
…to highest energies…

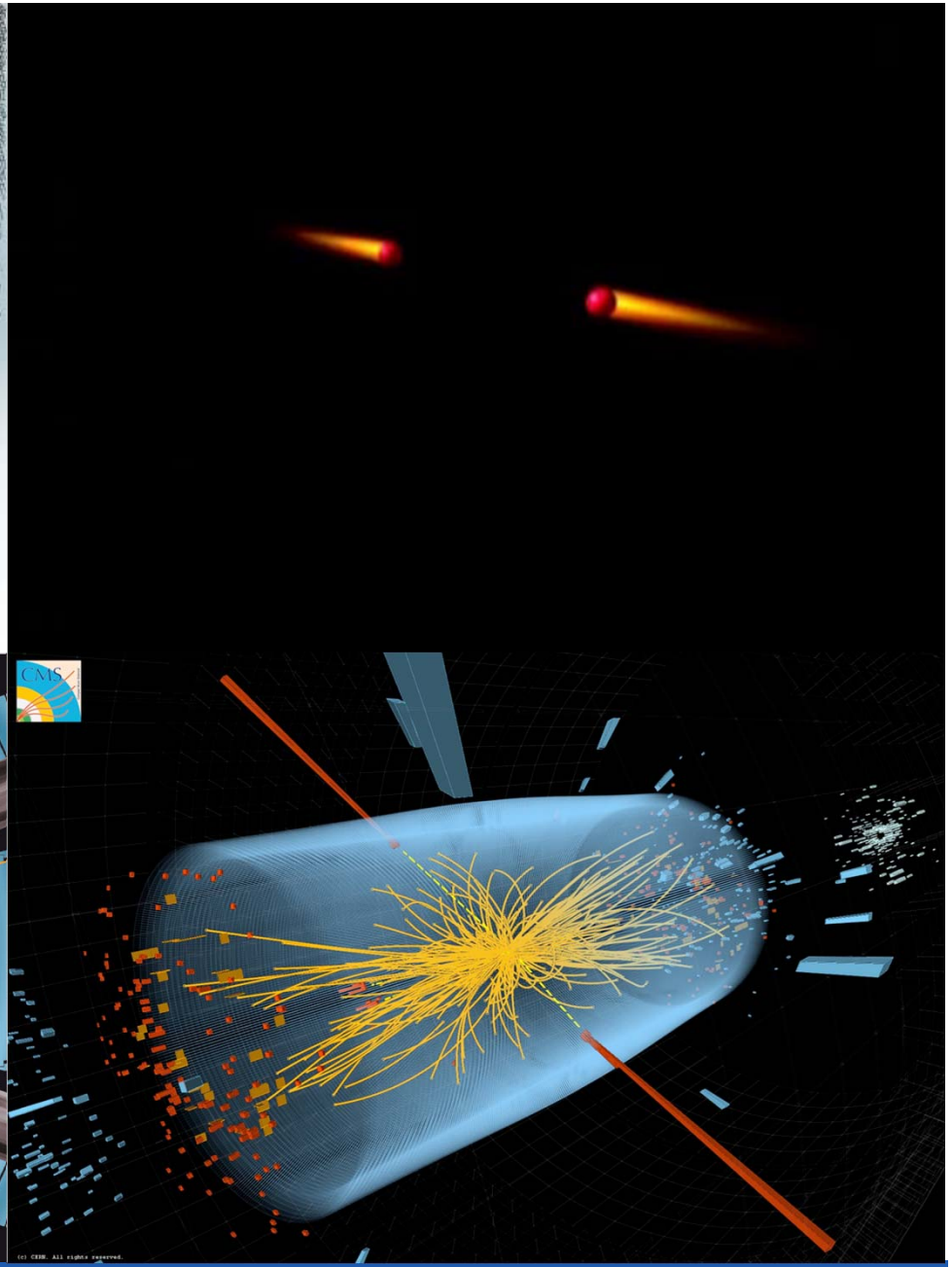


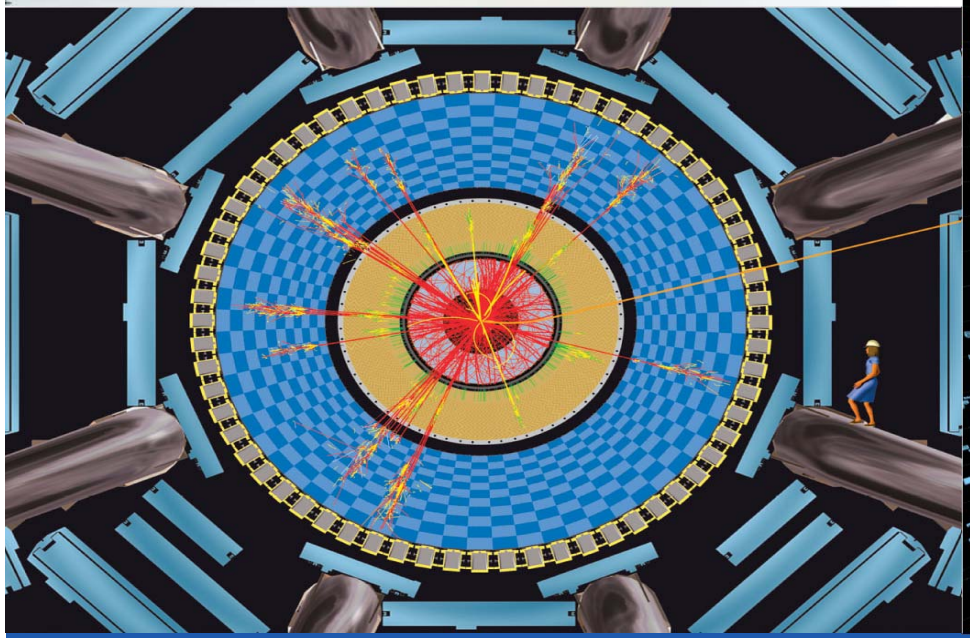




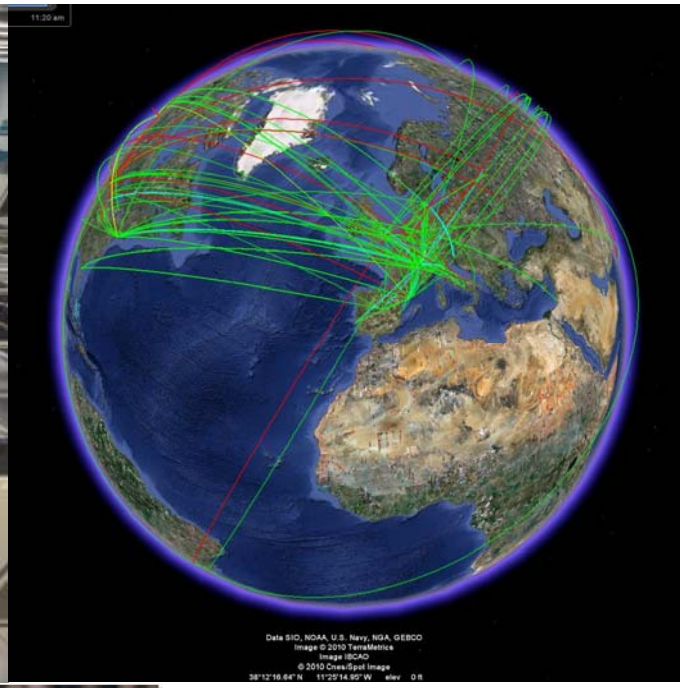
…& continuously take photos…



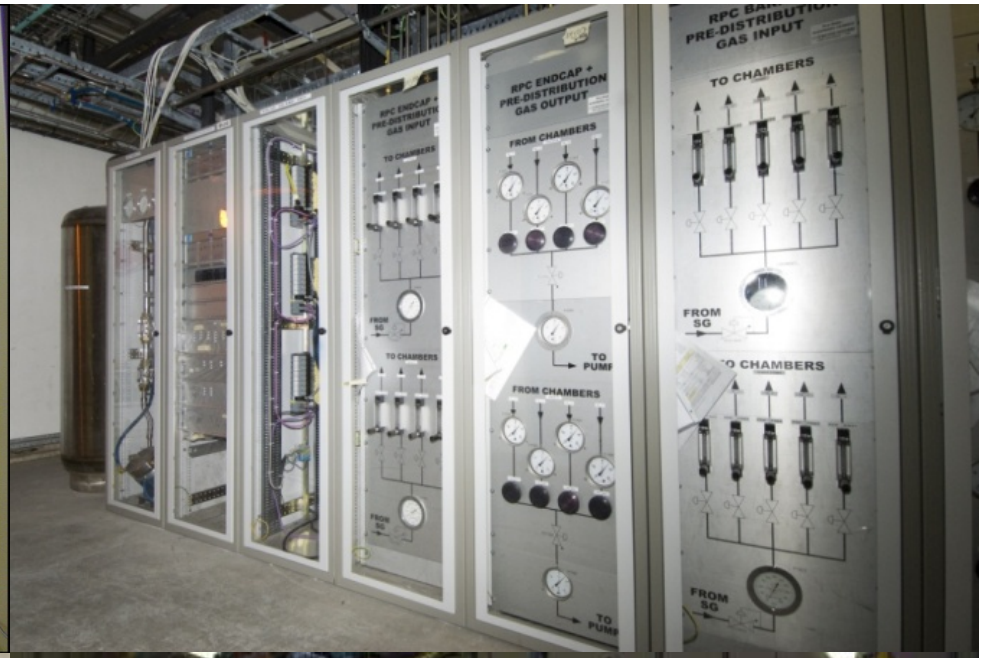




…of their collisions…



…to get the Nobel Prize ☺



Typical Control Systems (1)

Typical Control Systems (2)

CERN Control Centre

CERN Computer Centre

Why Control System Cyber-Security Sucks

Dr. Stefan.Lueders@cern.ch

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

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

COMPUTERWORLD TECHWORLD

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

WIRED

Report: Cyber Attacks Caused Power Outages in Brazil

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

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

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

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

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

Russia welcomes hack attacks

Script Kiddies cut teeth hijacking critical infrastructure

The Register®

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

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

Zotob, PnP Worms Slam 13 DaimlerChrysler Plants

By: Paul F. Roberts
2005-08-18

eWEEK.COM

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

Sluices, pumping stations & bridges poorly protected

Published on 14 February 2012 - 8:41pm

RNW RADIO NETHERLANDS WORLDWIDE

"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™

Malware on oil rig computers raises security fears

HOUSTON CHRONICLE ENERGY

CERN

Why Control System Cyber-Security Sucks
Dr. Stefan.Lueders@cern.ch
Black Hat, August 6-7th 2014, Las Vegas (US)

Why worry?

RISK ASSESSMENT / SECURITY & HACKTIVISM

ars technica

Bug can cause deadly failures when anesthesia device is connected to cell phones

No, it's not clear why anyone would ever connect a phone to a medical device.

UPDATE 1-All at sea: global shipping fleet exposed to hacking threat

Jeremy Wagstaff

Wednesday, 23 Apr 2014 | 9:54 PM ET

CNBC

Cyber weaknesses should deter US from waging war

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

YAHOO! NEWS

U.S. utility's control system was hacked, says Homeland Security

REUTERS By Jim Finkle

May 20, 2014 6:42 PM

THREAT LEVEL | WIRED

It's Insanely Easy to Hack Hospital Equipment

BY KIM ZETTER 04.25.14 | 6:30 AM | PERMALINK

Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable

BY KIM ZETTER 06.25.14 | 6:30 AM | PERMALINK

4 April 2014 Last updated at 09:50 GMT

BBC

Power plants put at risk by security bugs

Iran hacks energy firms, U.S. says

FRIDAY, 24 MAY 2013

IRAN FOCUS NEWS & ANALYSIS

UPDATE 1-Malicious virus shuttered U.S. power plant -DHS

Wed Jan 16, 2013 5:53pm EST

REUTERS

National Electric Grid Remains at Significant Risk for Cyber-attack

06 March 2014

infosecurity

STRATEGY /// INSIGHT /// TECHNIQUE

SPIEGEL ONLINE

Fernwartung: Sicherheitslücke bedroht Hightech-Heizungen

Really! Why worry?

Houston,
we have a problem…

…since years, but
who really cares?

Computer Centre:

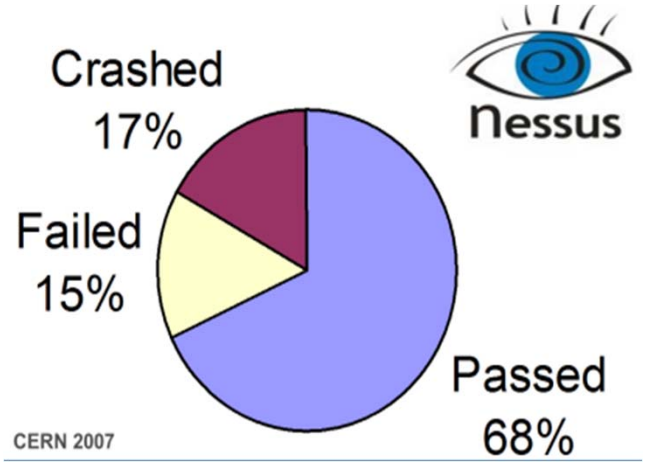
- SDLC, regression testing, nightly builds
- Full configuration mgmt.
- Redundancy & virtualization
- Few exceptions

Control Systems:

- Heavy compliance testing (vendor & utility) to keep warranties & certification (e.g. SIL)
- Rare maintenance windows
- Fear to brick a $100k device
- Lots of legacy, old or embedded devices

Why “Patching” Sucks

With an Internet of Things, how “prompt and agile” must (should?) patching be done?



Computer Centre:

skipfish
web application security scanner

- (Externally sponsored) pen testing & vulnerability scanning
- Decades of experience/knowledge
- Responsible disclosure & CSIRTs

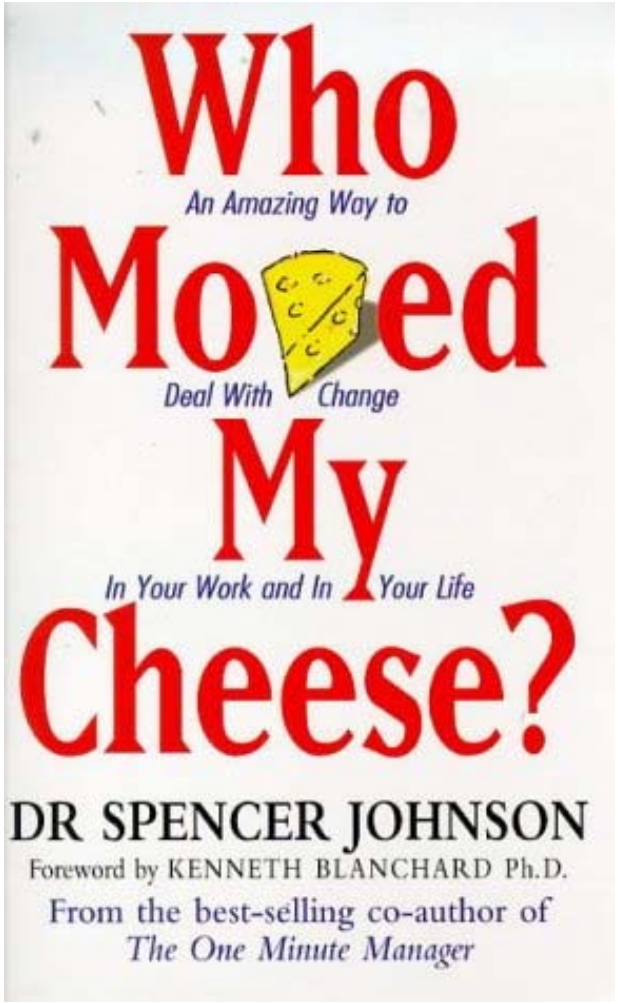
NMAP.ORG
Nessus
w3af
Web Application Attack and Audit Framework

Control Systems:

- Security not integral part… or thru obscurity
- Fulfil use-cases, but fail to abuse-cases
- Default passwords & undoc'd backdoors
- Few laws; too many guidelines
- Unwillingness to share incidents
- No security certification (yet?)

Why "Ignorance" Sucks

Why do I have to do due diligence and bear the costs(!) instead of those vendors shipping insecure applications/devices?



Computer Science:

- Our kids are the users/programmers of tomorrow
- Why are students still weak on "security"?

  BSc CV: programming, O/S, DBs, web, …

  MSc CV: ditto, now add "security"
- Do we need more professionalism?

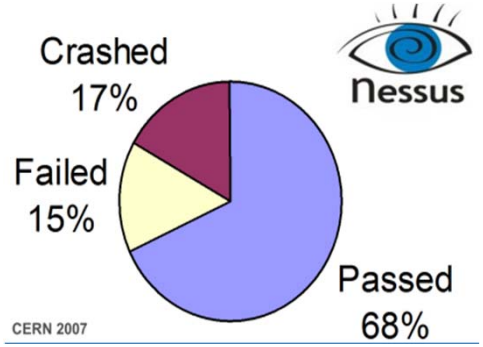
Control System Engineering:

- Get a "Computer Science" education
- Stop reinventing standard IT, …
- …but embrace IT methods

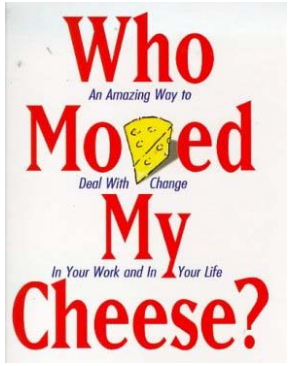
Why "Unprofessionalism" Sucks

Why is “security” still separated from functionality, usability, availability, and maintainability?

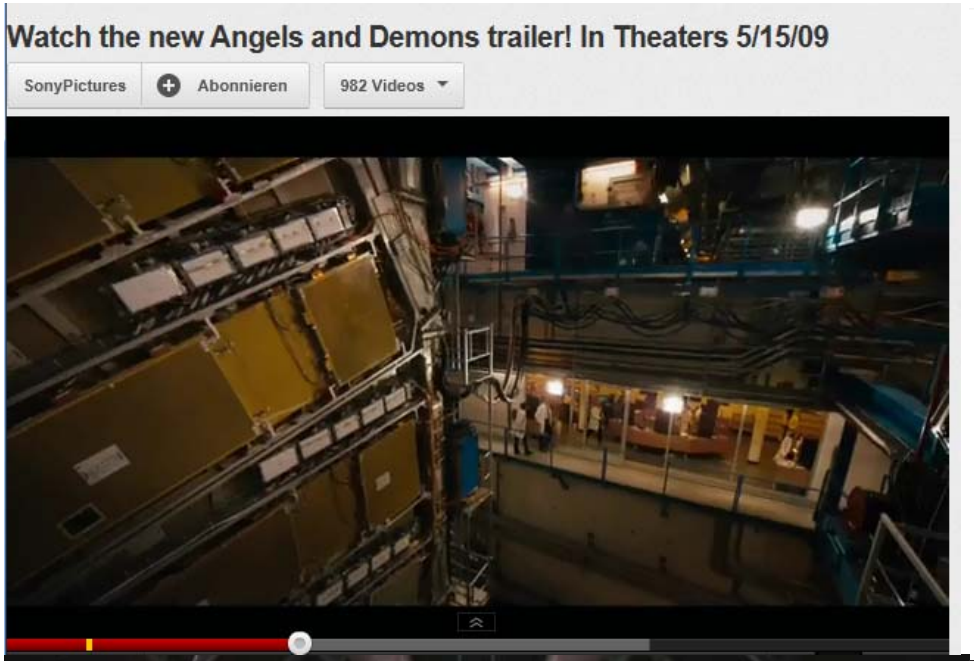
Patch promptly:
Merge control system IT with standard IT



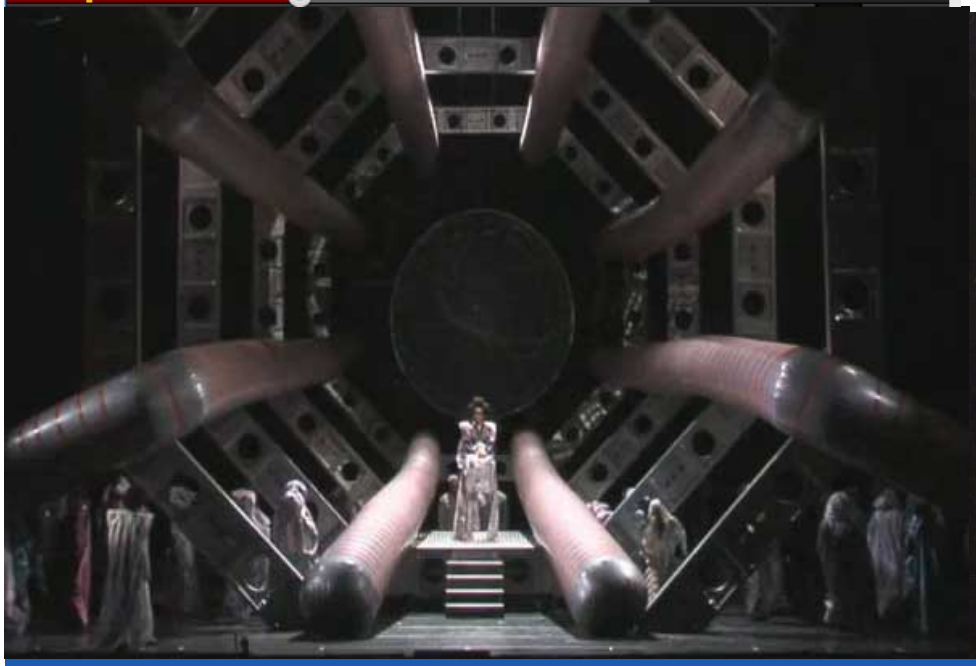
Robustify:
Hack.the.box!
…& disclose responsibly



Change of Minds:
Make "security" part of everyone's CV!


Watch the new Angels and Demons trailer! In Theaters 5/15/09
SonyPictures
Abonnieren
982 Videos


THE MUPPETS - Full Trailer 2011
19melyk87
143 Videos
Abonnieren
Blockieren...




BE THE NEXT!
cern.ch/jobs

Thx!

www.cern.ch