

# Cyber-Security at CERN

- ▶ High Energy Physics & CERN Control Systems
- ▶ “TOCSSiC” Vulnerability Tests
- ▶ SCADA Honeynets

Dr. Stefan Lüders (CERN IT/CO)  
PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006



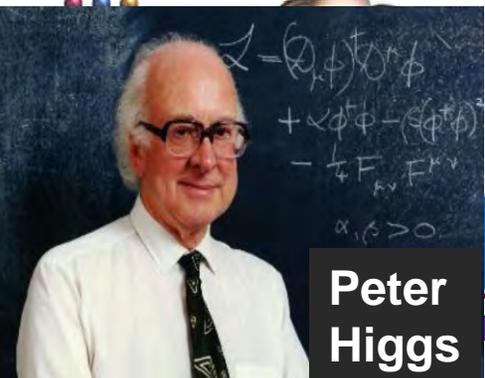
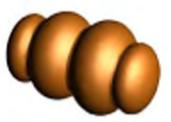


# The Standard Model of HEP

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

## Strong

**Gluons (8)**



**Peter Higgs**

**Graviton ?**

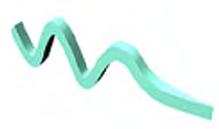


Solar system  
Galaxies  
Black holes

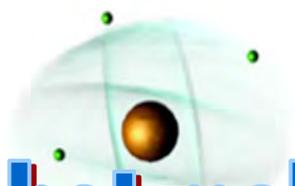


## Electromagnetic

**Photon**

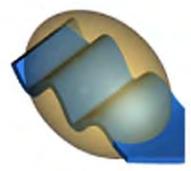


Atoms  
Light  
Chemistry

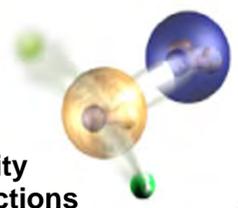


## Weak

**Bosons (W,Z)**



Neutron decay  
Beta radioactivity  
Neutrino interactions  
Burning of the sun



## Leptons

Electric Charge

**Tau** -1    0 **Tau Neutrino**

**Muon** -1    0 **Muon Neutrino**

**Electron** -1    0 **Electron Neutrino**

# But what makes them weightless?

## Quarks

Electric Charge

**Bottom** -1/3 2/3 **Top**

**Strange** -1/3 2/3 **Charm**

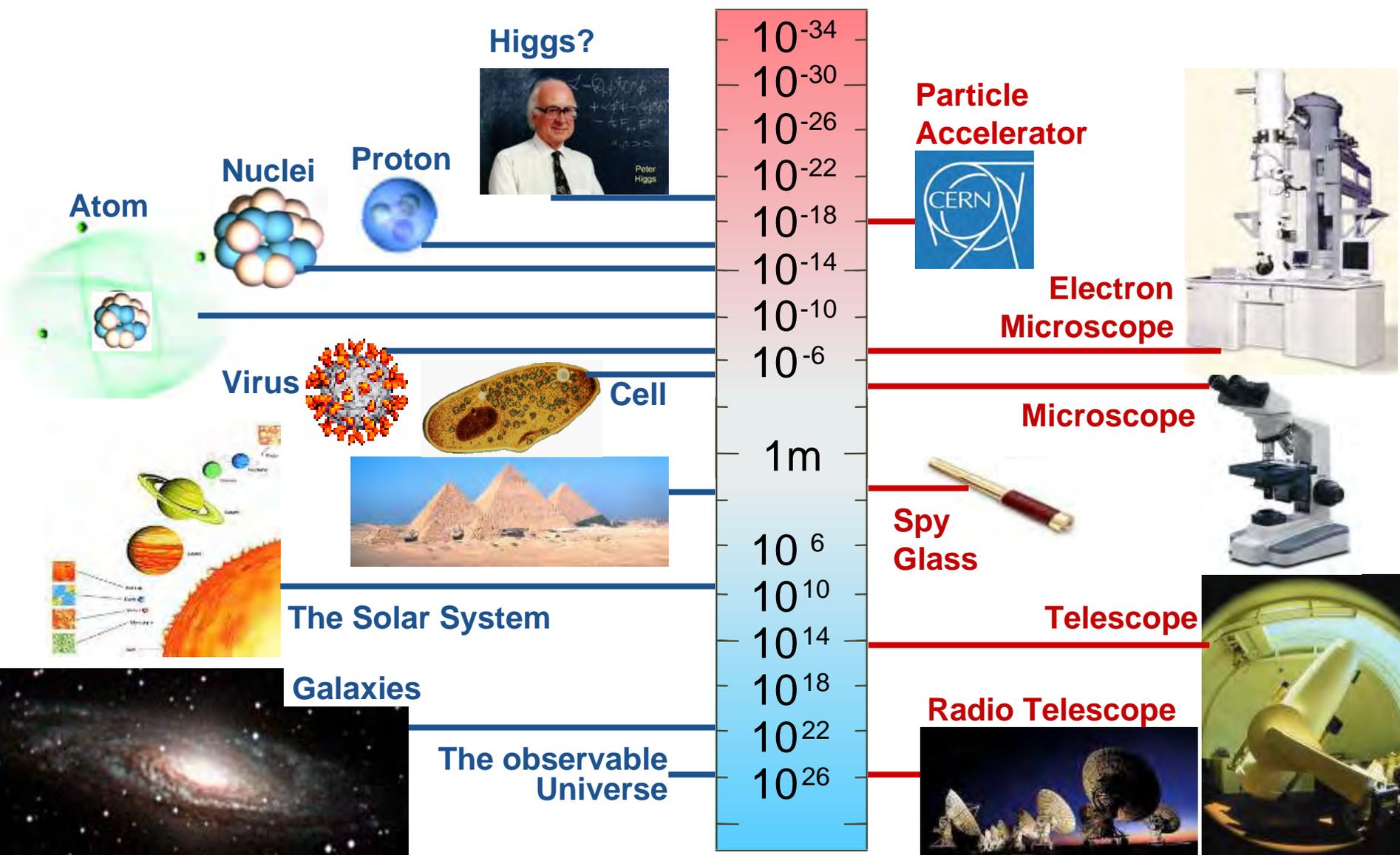
**Down** -1/3 2/3 **Up**

each quark: *R*, *B*, *G* 3 colors

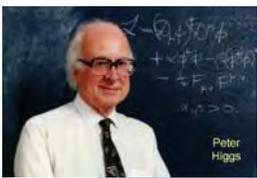


# Observables & Instruments

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006



Higgs?



Nuclei

Proton

Atom

Particle Accelerator



Electron Microscope



Virus

Cell

Microscope



1m

Spy Glass



The Solar System

Telescope



Galaxies

Radio Telescope



The observable Universe





**Dan Brown's**  
*Angels & Demons*

**European Organization  
for Nuclear Research**

**20 European Members**

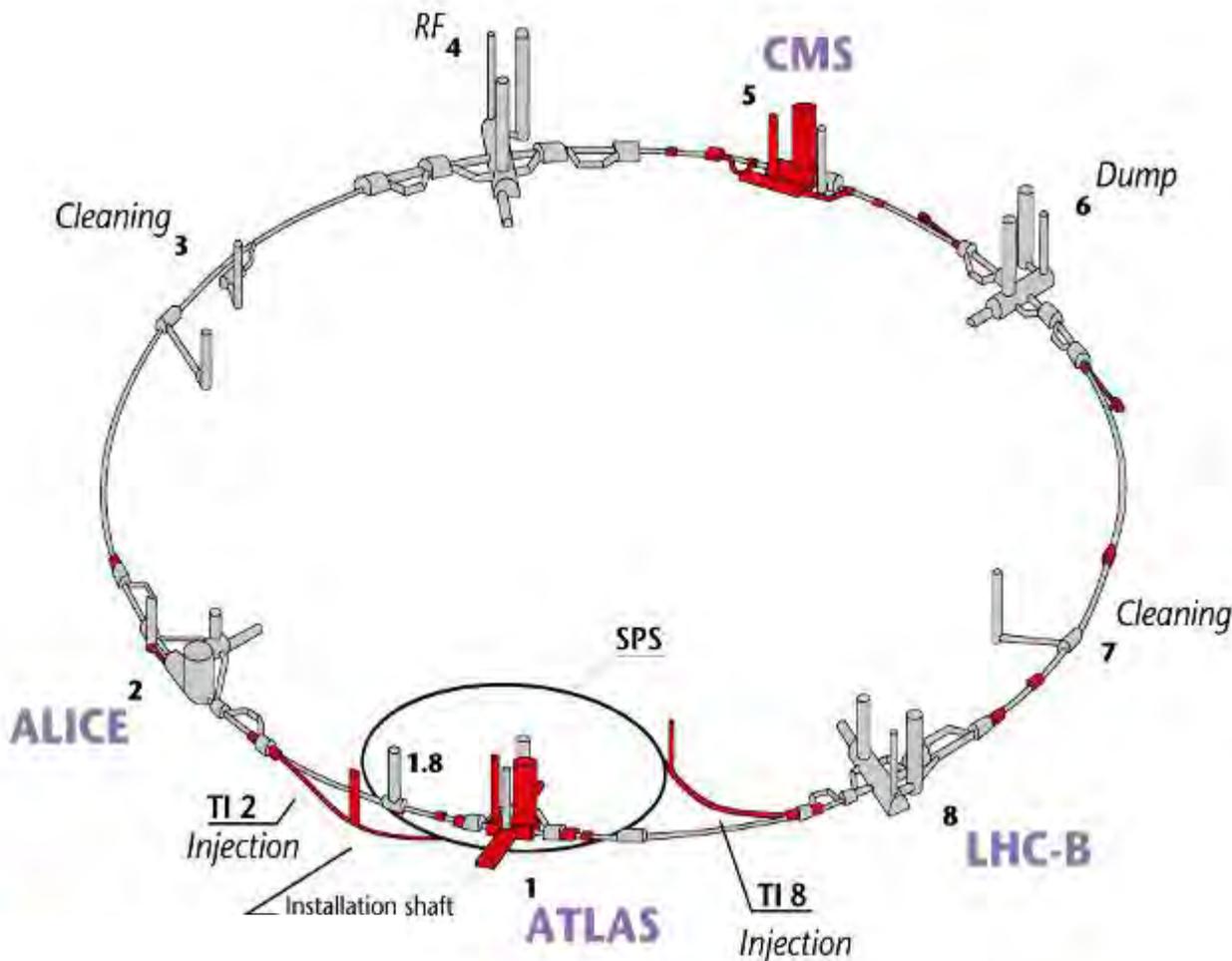
**2500 staff + 5000 users**

**600M€ annual budget**



# The “Large Hadron Collider”

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006



Steer a beam of 85 kg TNT through a 3mm hole 10000 times per second !



World's largest superconducting installation (27km @ 1.9°K) worth 2B€



# The "ATLAS" Experiment

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

# million data channels

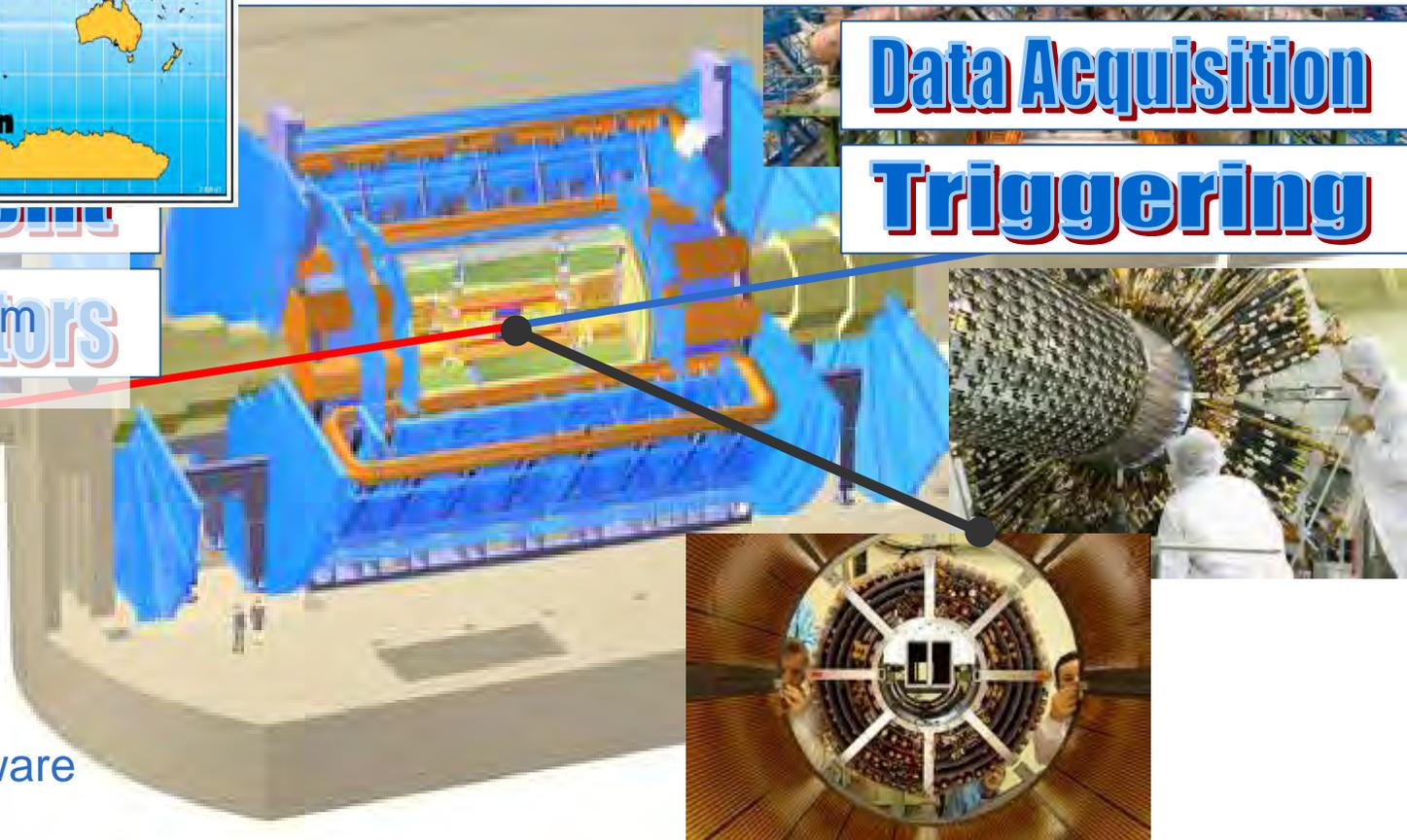
## Data Acquisition

## Triggering



2000 members of  
151 institutions from  
34 countries

**The Experiment**  
7000 tons  
Ø22m × 43m  
500M€ pure hardware  
<http://atlas.ch>





# The "CMS" Experiment

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006



**Safety**

**Radiation**

**Smoke**

**Sniffer**

**Gas Distribution**

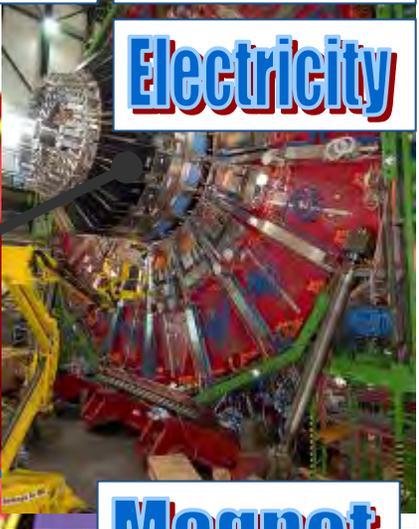
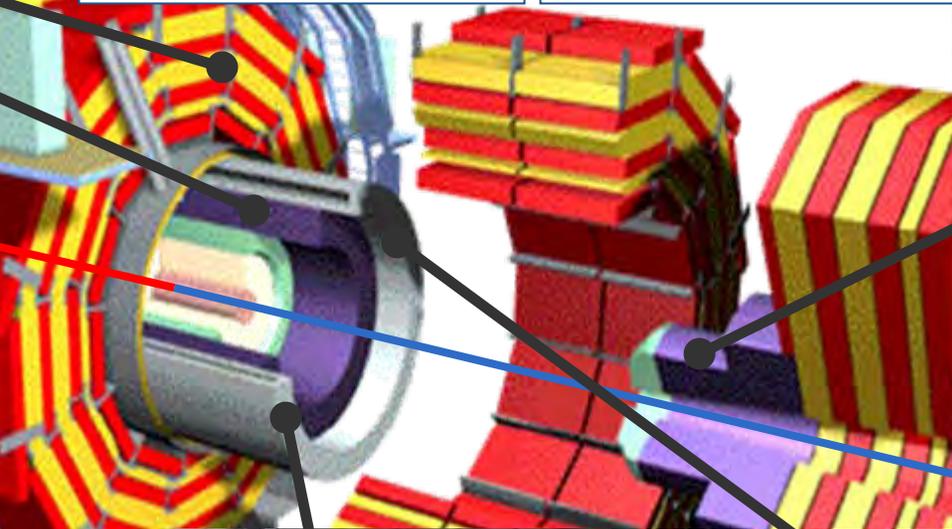
**Cooling & Ventilation**

**High Voltage**

**Electricity**

**Cryogenics**

**Magnet**



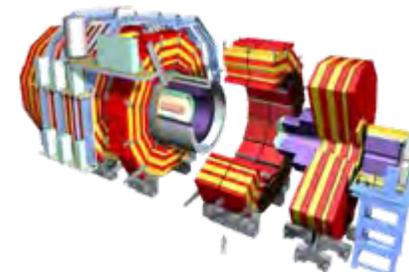
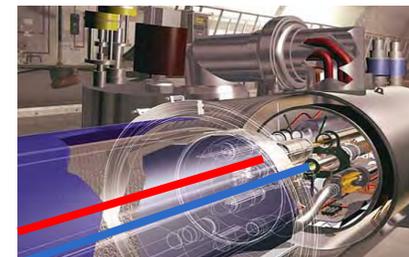
**About one million control channels**



# Concerned about Cyber-Security

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

- ▶ **High number of control systems**
- ▶ **Complex, expensive & unique**
- ▶ **Highly interconnected & interdependend**
- ▶ **COTS & standards where possible**

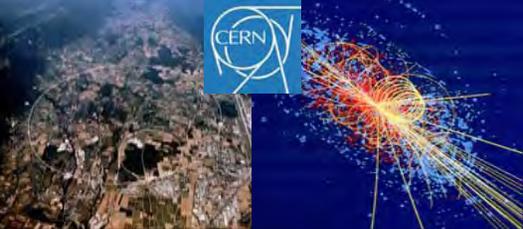


▶ **Very high external bandwidth**

▶ **World Wide Processing**

▶ **Large external user community**

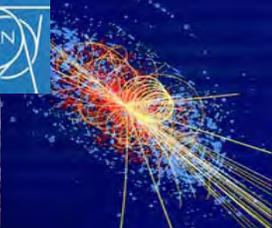




# Cyber-Security Ground Rules

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

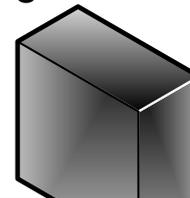
- ▶ **Apply a “Defence-in-Depth” approach**
  - ▶ Protect *each* layer of Control Systems
  
- ▶ **Separate Controls and Campus Networks**
  - ▶ Reduce and control inter-communication
  
- ▶ **Use centrally managed systems where ever possible**
  - ▶ Ensure prompt security updates: OS, applications, anti-virus, ...
  
- ▶ **Use strong passwords and sufficient logging**
  - ▶ Ensure traceability of access (who and from where)
  - ▶ Passwords must be kept secret: beware of “Google Hacking”
  
- ▶ **Make security an objective**
  - ▶ Raise awareness in the User community



## COTS Automation Systems are without security protections.

- ▶ Programmable Logic Controllers (PLCs), field devices, power supplies

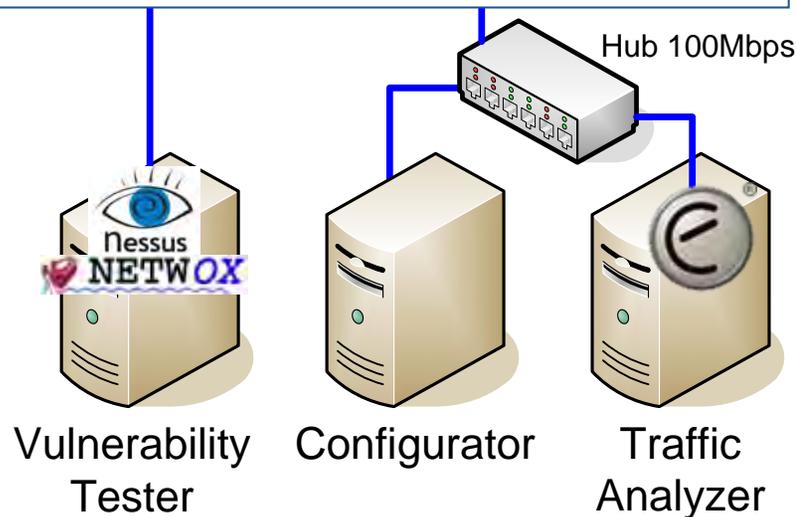
Target Device(s)

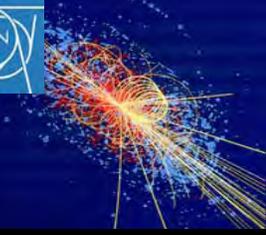


# Going for the "low hanging fruits"!

## Teststand On Controls System Security at CERN (TOCSSiC)

- ▶ Running "Nessus" vulnerability scan (used in Office IT)
- ▶ Running "Netwox" DoS attack with random fragments
- ▶ Running "Ethereal" network sniffer

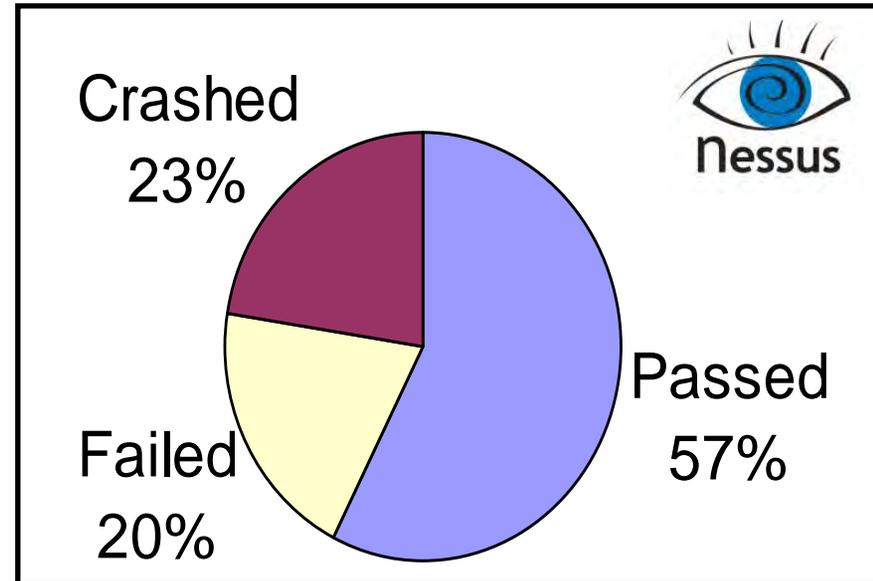
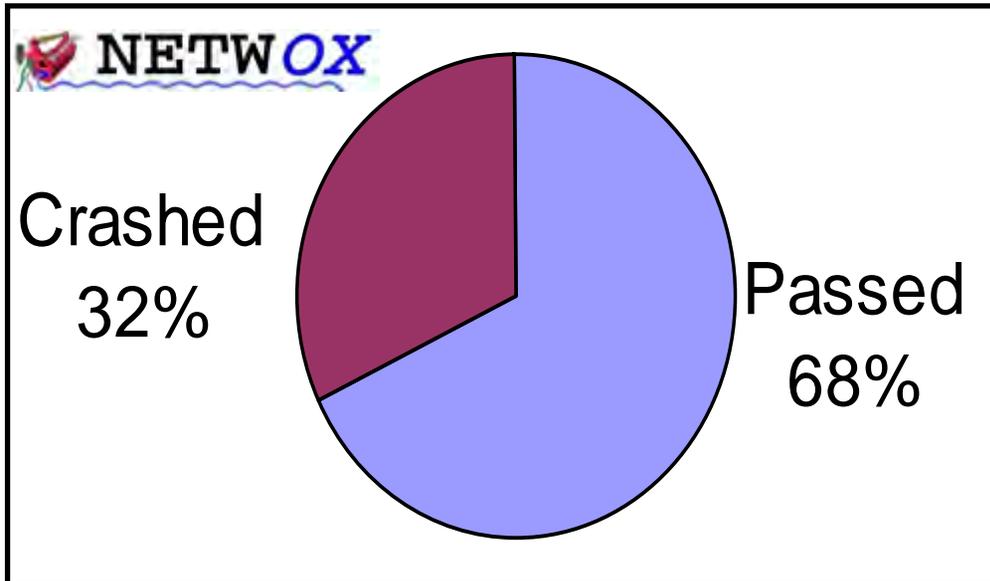




# Control Systems under Attack !

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

- ▶ 25 devices from 7 different manufacturers (42 tests in total)
- ▶ All devices fully configured but running idle



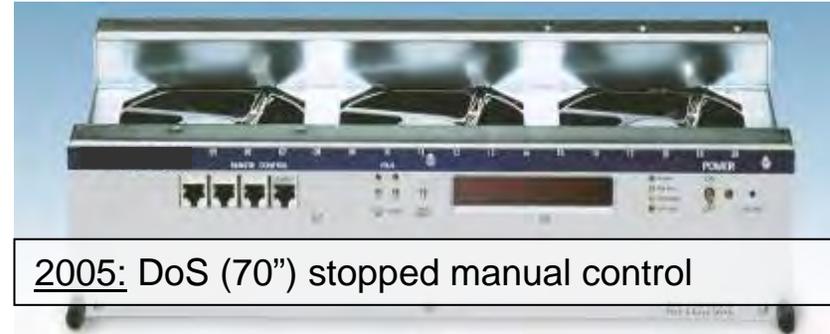
*...PLCs under load seem to **fail even more likely** !!!*  
*...results improve with more recent firmware versions ☺*



# TOCSSiC Findings (1)

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

- ▶ **The device crashed because of mal-formed TCP/IP packets**



*...violation of TCP/IP standards !!!*

- ▶ **PLCs are un-protected**

- ▶ Can be stopped w/o problems (needs just a bit “googling”)
- ▶ Passwords are not encrypted
- ▶ Might even come without authentication

*...authentication, integrity checks & encryption should be mandatory !*

- ▶ **Modbus server crashed by scanning port 502**

*...protocols are well documented (“Google hacking”) !*



# TOCSSiC Findings (2)

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

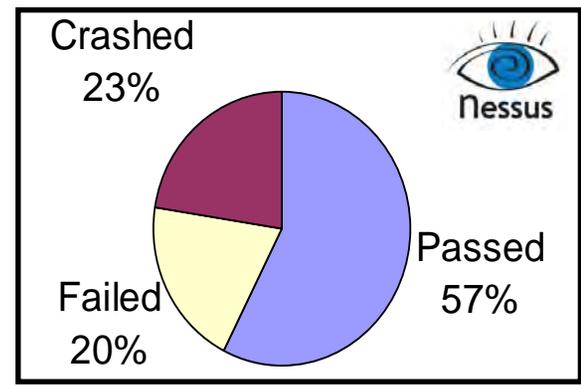
- ▶ **Fixed SNMP community names “public” and “private”**  
*...why can community names not be changed ?*
- ▶ **FTP server offered attacker platform**
- ▶ **FTP & Telnet servers crashed**  
because of too long commands / arguments  
*...both are legacy protocols w/o encryption !*
- ▶ **HTTP server crashed** because of a too long URL
- ▶ **HTTP server allowed for **directory traversal****  
*...who needs web servers & e-mailing on PLCs ?*



# TOCSSiC Follow Up

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

- ▶ **Controls goes IT...**
- ▶ **...but COTS automation systems are without security protections.**
- ▶ **'Industrial Security' must become fundamental ingredient.**
- ▶ **CERN has already followed up with vendors, government bodies & research.**





# CERN's SCADA Honeynet Project

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

## ► Understanding of mal-traffic on CERN's network

## ► Demonstrating the existence of the risk

- ▶ Vulnerabilities already proven by e.g. TOCSSiC

*...threats have not been demonstrated (yet)...*

## ► Features

- ▶ Emulation of several PLCs
- ▶ Logging & reporting of all activity
- ▶ Easy deployment (thus easy shareable)
- ▶ Limited resources
- ▶ Avoid compromising
- ▶ Detect compromising

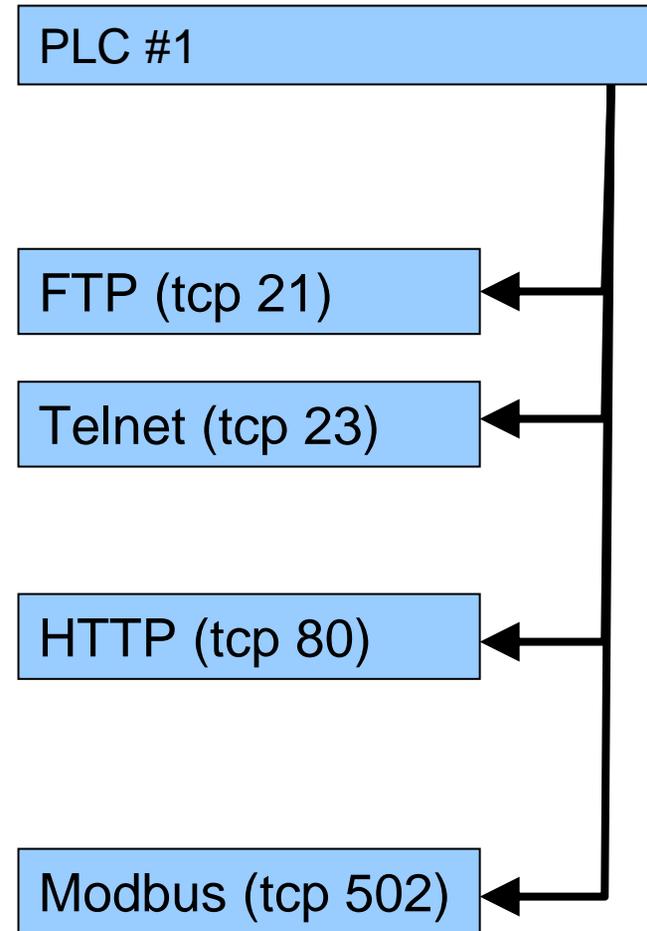


# Honeyd Simulation (1)

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

## Python scripts for:

- ▶ **Nmap signature**
- ▶ **FTP** (login only)
- ▶ **Telnet**  
(login only; improved existing scripts)
- ▶ **HTTP**  
(identical functionalities as the real PLC web server)
- ▶ **Modbus**  
(all functions available; persistent in memory)



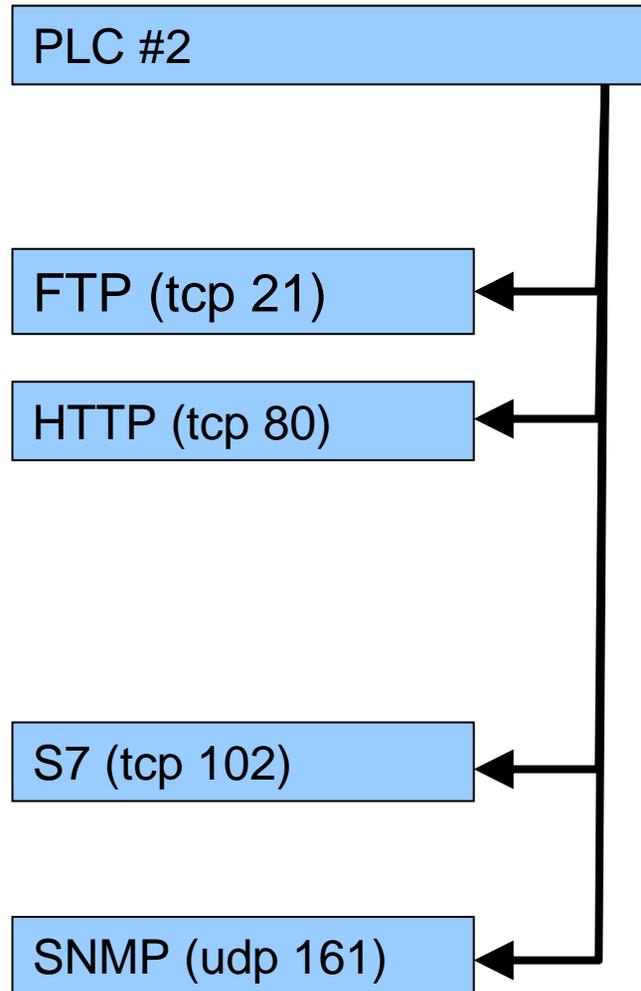


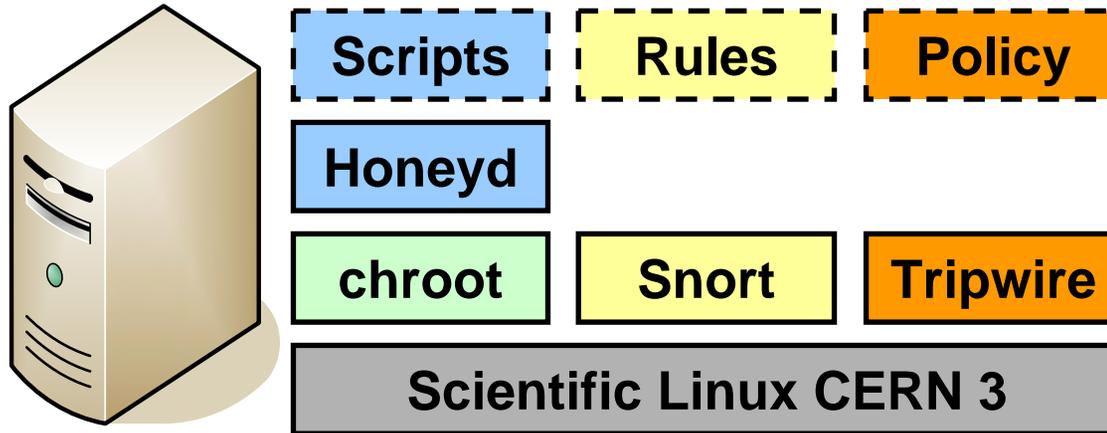
# Honeyd Simulation (2)

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

## Python scripts for:

- ▶ **Nmap signature**
- ▶ **FTP** (login only)
- ▶ **HTTP**  
(identical functionalities as the real PLC web server, incl. directory traversal vulnerability)
- ▶ **Siemens S7**  
(Reverse-engineered by Th. Hergenbahn; allows “read”, “write”, and “switch on/off”)
- ▶ **SNMP**  
(status values cloned from real PLC)





- ▶ **PLC simulation & logging of interactions with the honeypot**
- ▶ **Recording of all traffic**
- ▶ **Periodic file checks**
- ▶ **Daily reports**
- ▶ **Installation tool**
- ▶ **Plans to publish on [sourceforge.net](http://sourceforge.net)**

The work has been done by **Joël Arnold** (EPFL). Credits go to **Venkat Pothamsetty & Thomas Hergenbahn**.



# (No) Results so far...

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

▶ Nov. 2005:

**4 pots (à two PLCs) deployed inside CERN**

- ▶ Only observation: the usual “slight fever” on CERN’s campus network

**3 pots deployed on controls network**

- ▶ No interactions observed 😊

▶ Mar. 2006:

**3 pots visible on ports 102 & 502 from the Internet**

- ▶ Lots of “noise” observed, e.g. SSH scans, but nothing on 102 nor 502

**▶ No dedicated interaction with honeynet so far...**



# Summary

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

► **Fundamental research to understand the world (from a physicist's point of view)**

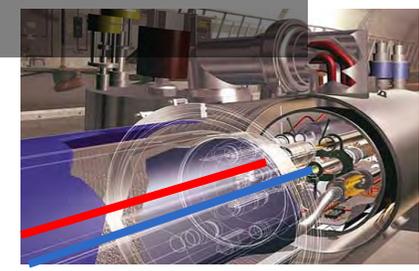
THE STANDARD MODEL

	Fermions			Bosons		
Quarks	$u$ up	$c$ charm	$t$ top	$\gamma$ photon	Force carriers	
	$d$ down	$s$ strange	$b$ bottom	$Z$ Z boson		
Leptons	$\nu_e$ electron neutrino	$\nu_\mu$ muon neutrino	$\nu_\tau$ tau neutrino	$W$ W boson		
	$e$ electron	$\mu$ muon	$\tau$ tau	$g$ gluon		

► **'Industrial Security' must become fundamental ingredient !!!**

► **CERNs control systems are complex, expensive & unique.**

\*Yet to be confirmed  
Higgs\* boson  
Source: AAAS

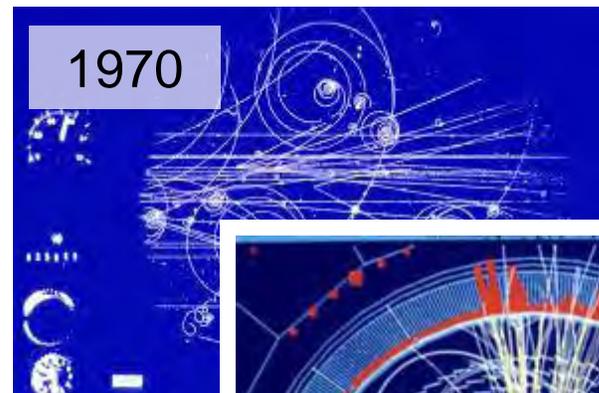




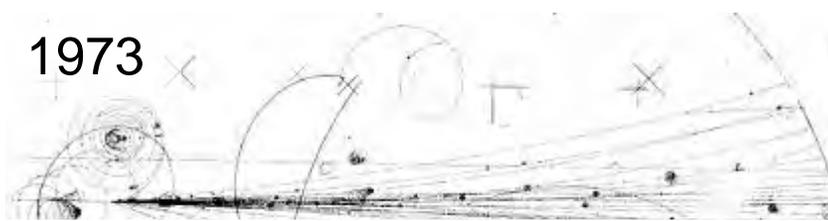
# Nature is beautiful !!!

Dr. Stefan Lüders (CERN IT/CO) — PCSF Spring Meeting — June 6<sup>th</sup>/7<sup>th</sup> 2006

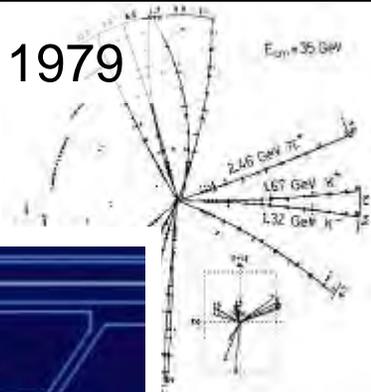
1970



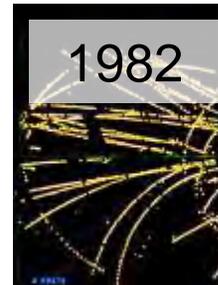
1973



1979

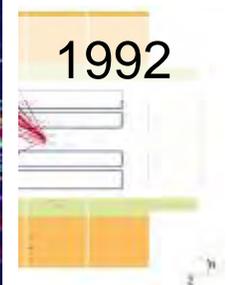


1982



**Thank you  
very much.**

1992



2008?

1995



2000



2001

