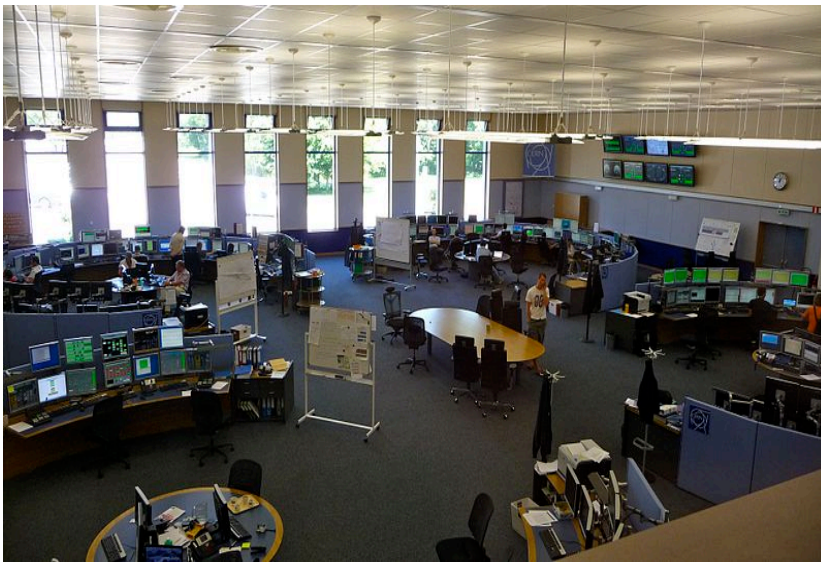




European Organization for Particle Physics
Exploring the frontiers of knowledge



Pain Points of Securing Modern Industrial Control Systems



Pain Points of Securing Modern ICSES

Dr. Stefan.Lueders@cern.ch

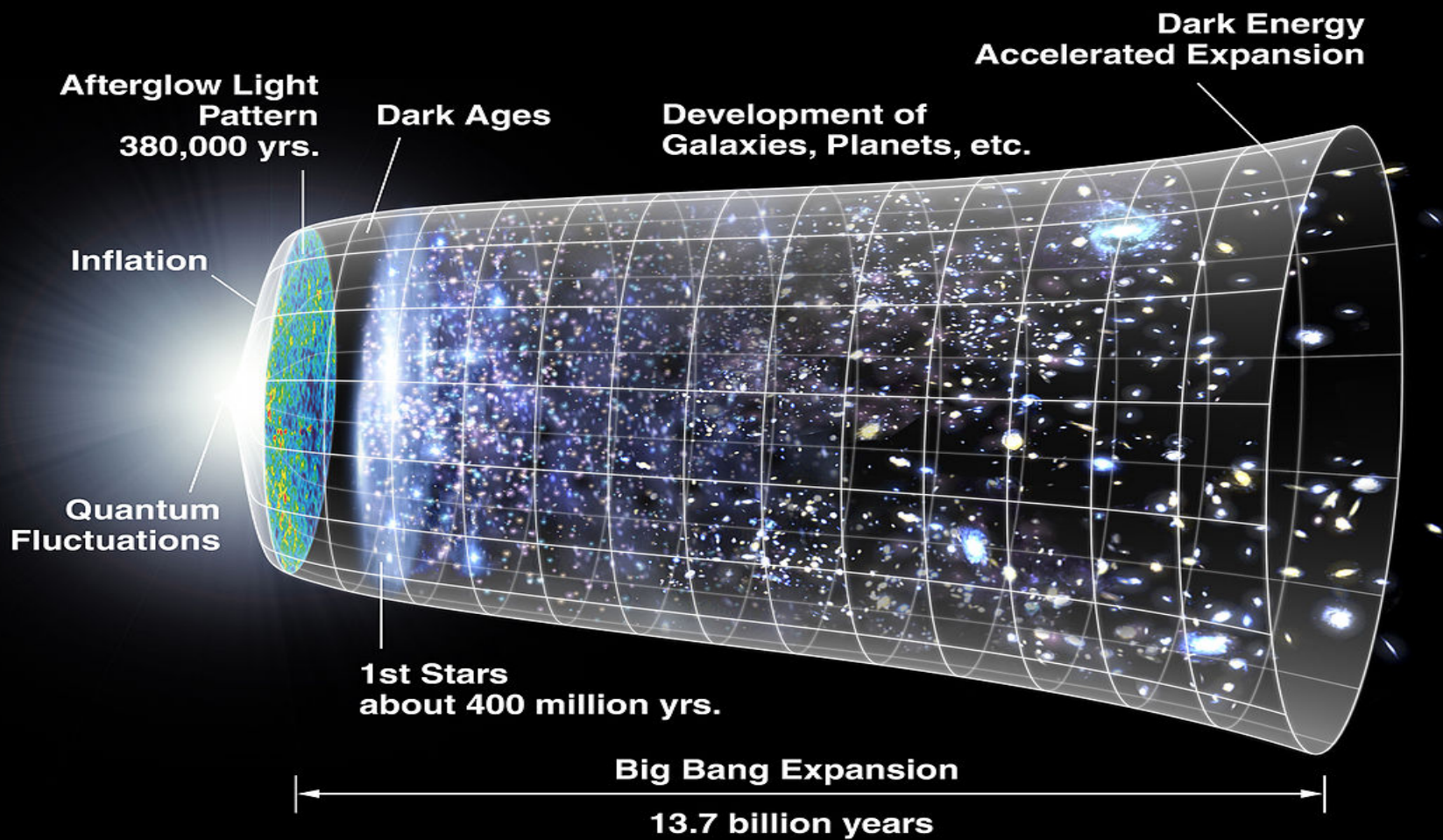
Swiss Cyber Storm, October 18th 2017, Lucerne (CH)

The LHC: A One-Time Prototype

**The Revolution of ICS:
Old paradigms don't hold
anymore.**

ICS & IT: Towards a joint future





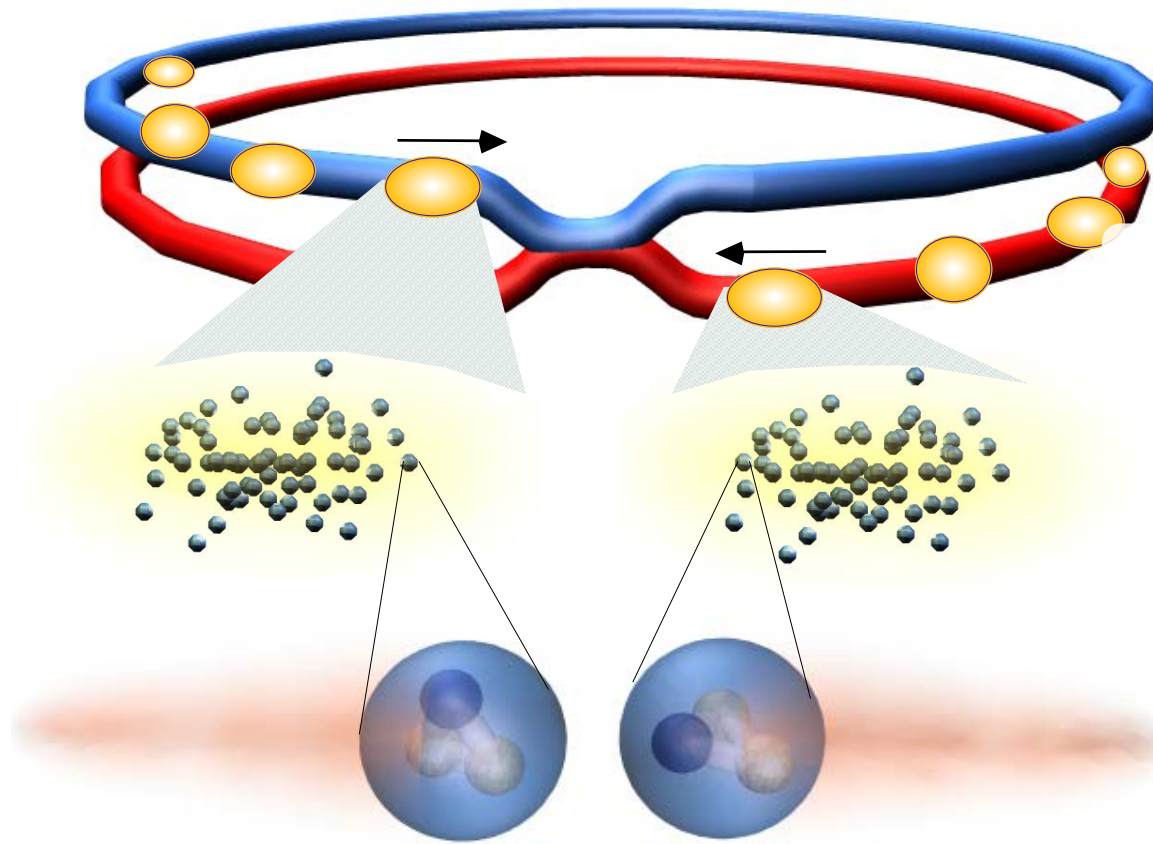
"CMB Timeline300 no WMAP" by NASA/WMAP Science Team - Original version: NASA, modified by Ryan Kaldari. Licensed under Public Domain





Pain Points of Securing Modern ICSES
Dr. Stefan.Lueders@cern.ch
Swiss Cyber Storm, October 18th 2017, Lucerne (CH)

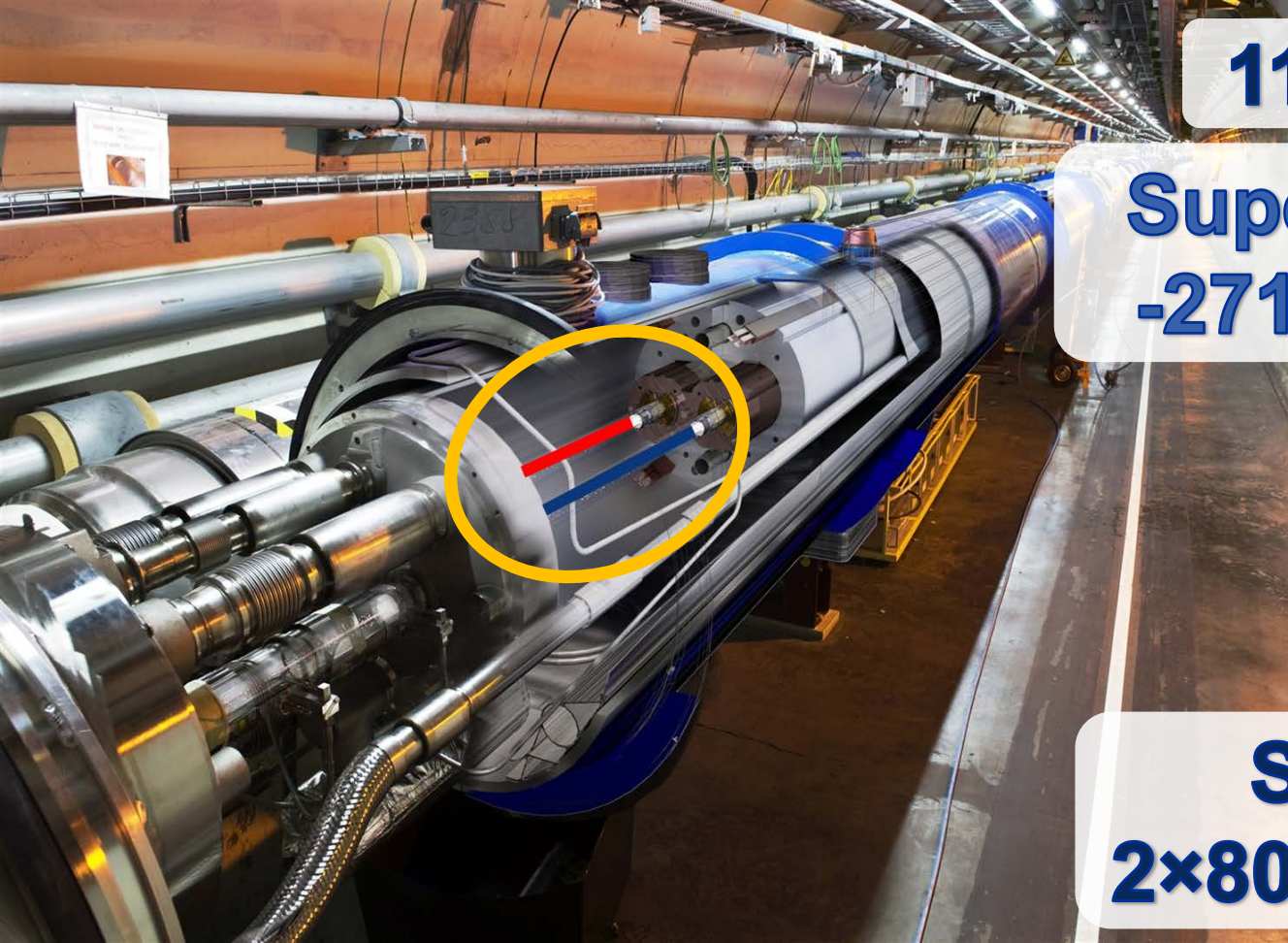
Mankind. Literally.



“Beam”: $2 \times 2076b$

“Bunch”: $10^{11}p$

Protons/Quarks



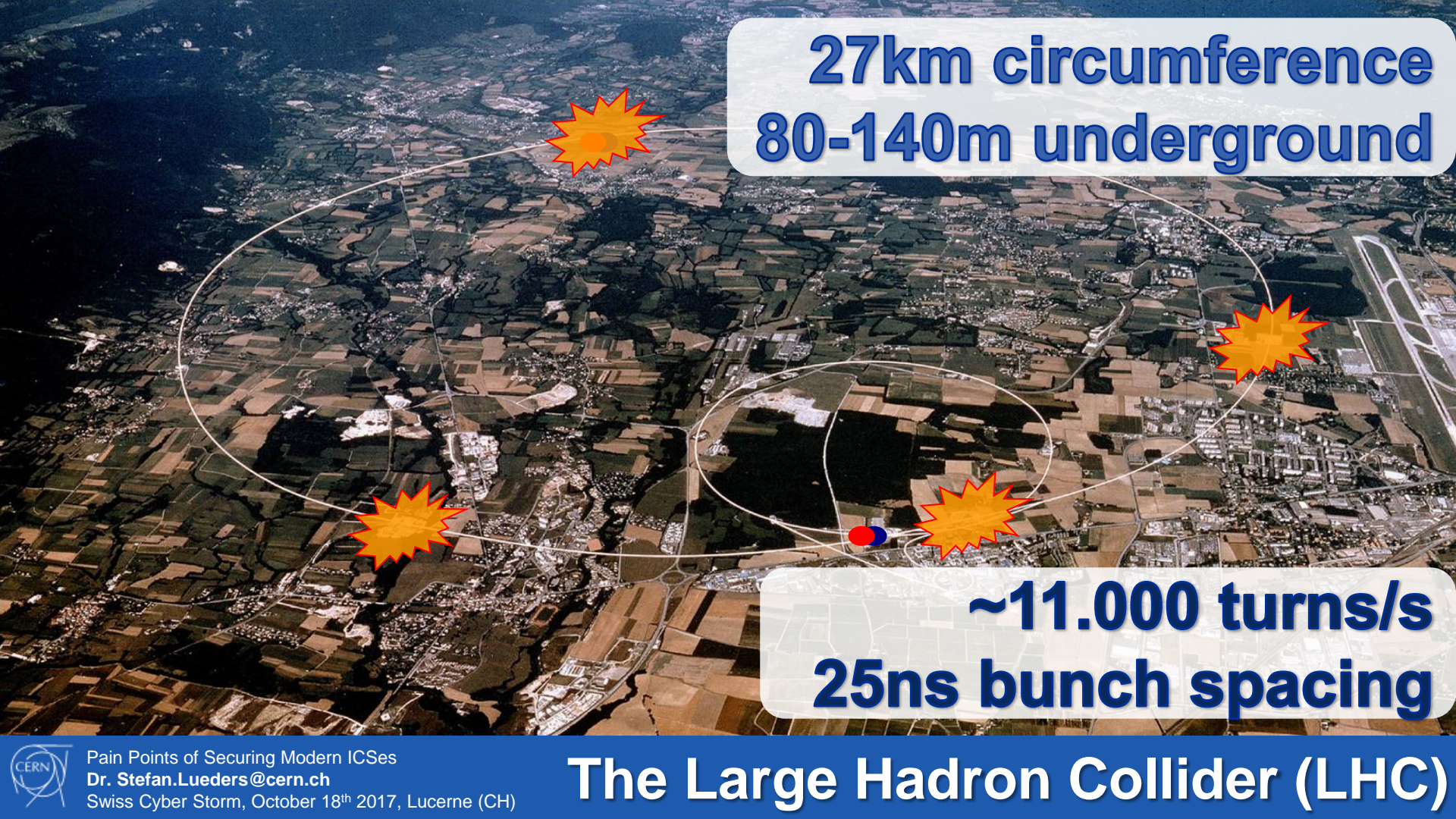
11.000A current

**Superconducting:
-271°C (1.9K) cold**



**Stored energy:
2×80kg TNT equiv.**

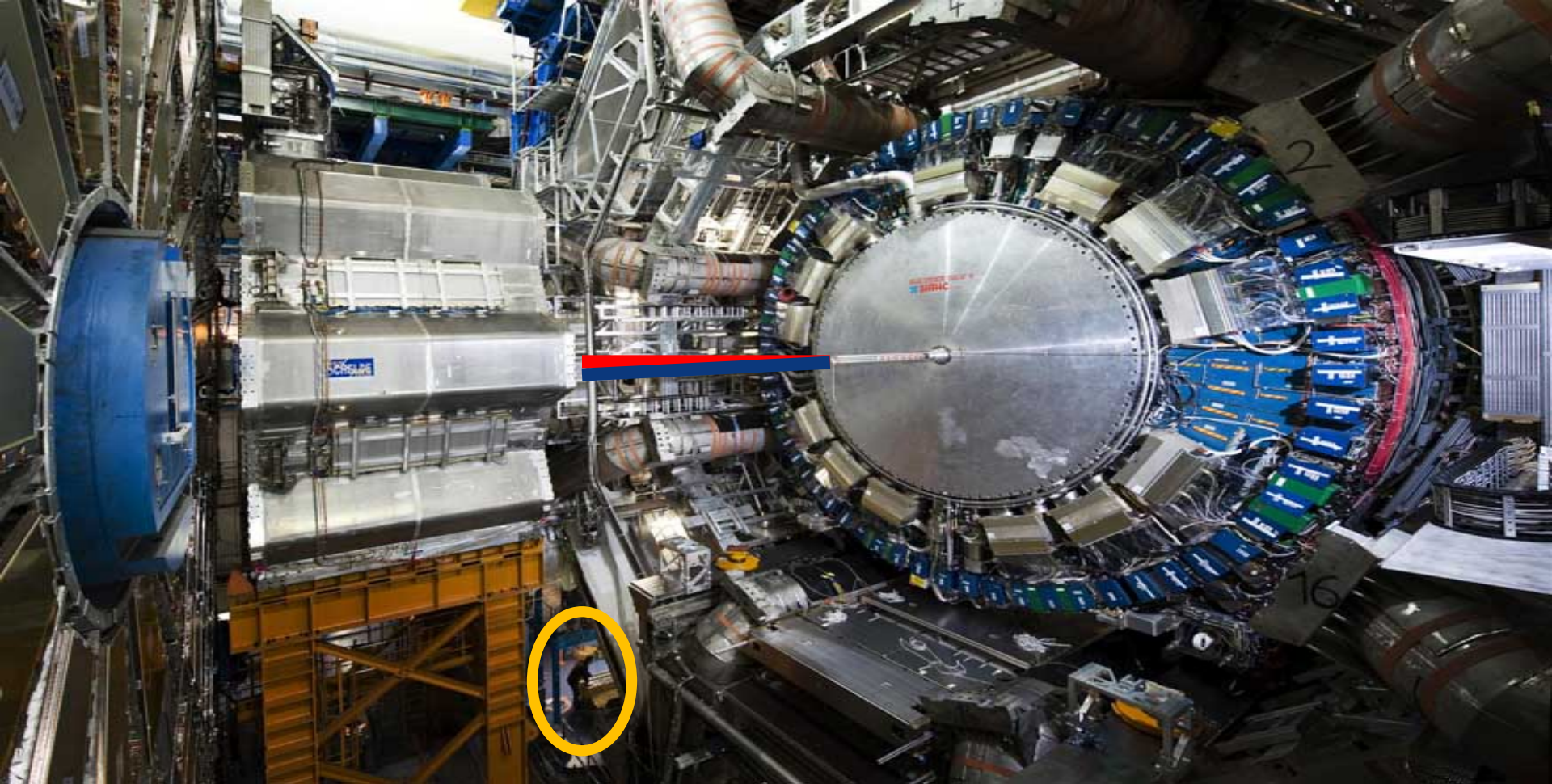




27km circumference
80-140m underground

~11.000 turns/s
25ns bunch spacing



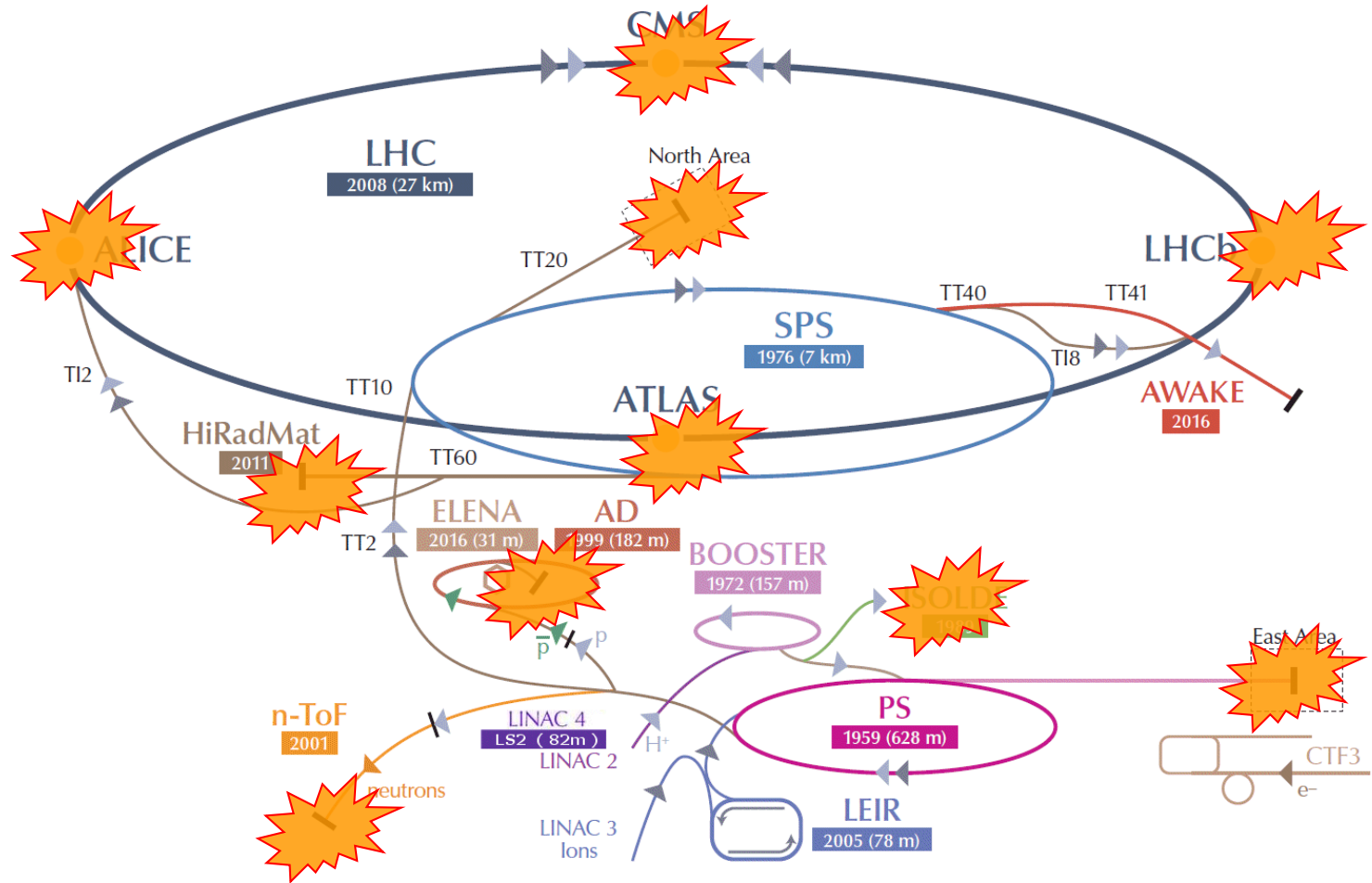


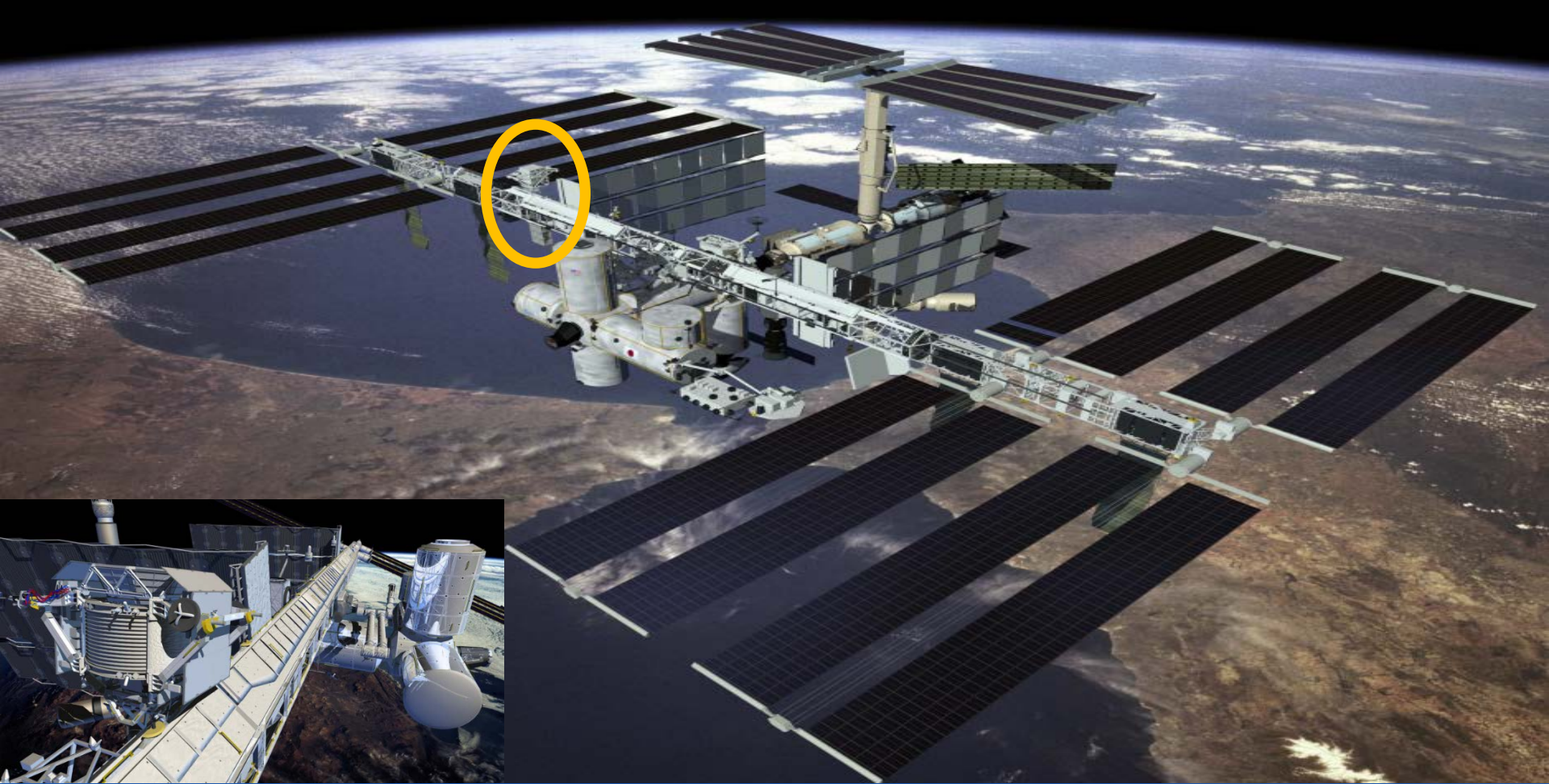
Pain Points of Securing Modern ICSeS

Dr. Stefan.Lueders@cern.ch

Swiss Cyber Storm, October 18th 2017, Lucerne (CH)

The ATLAS “camera” (open)



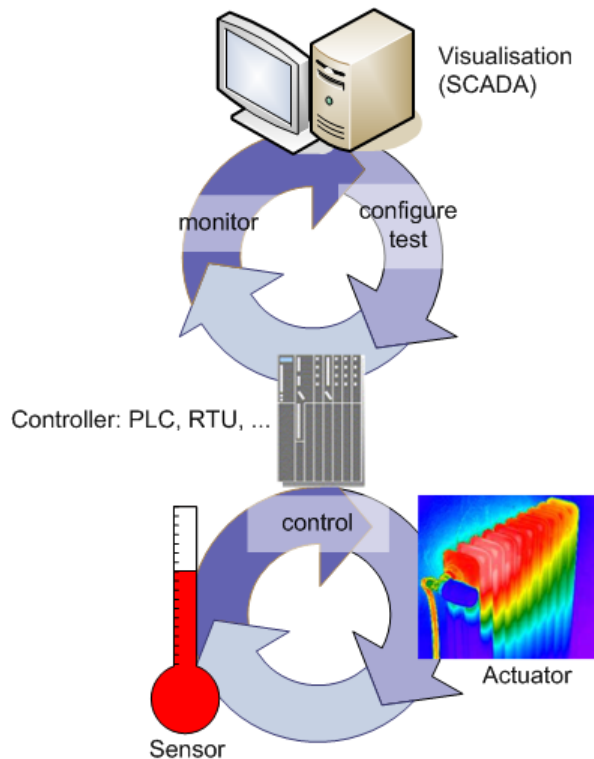


The LHC: A One-Time Prototype

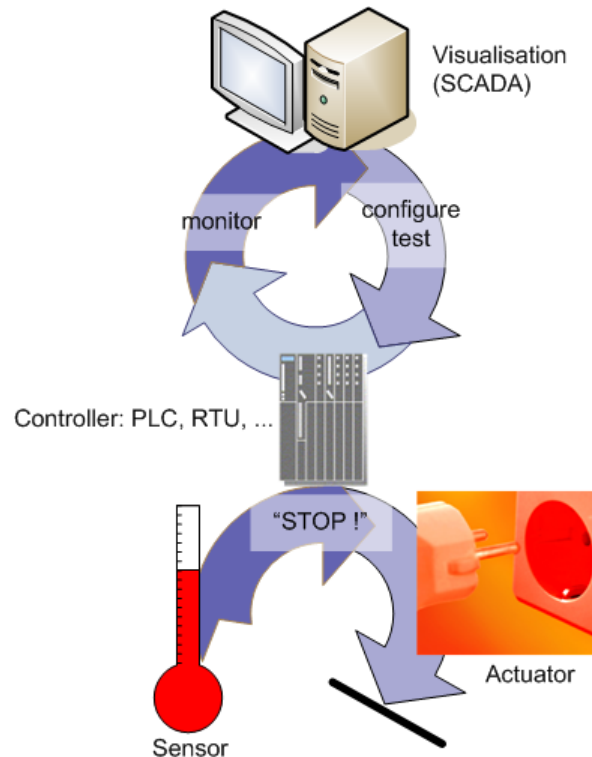
**The Revolution of ICS:
Old paradigms don't hold
anymore.**

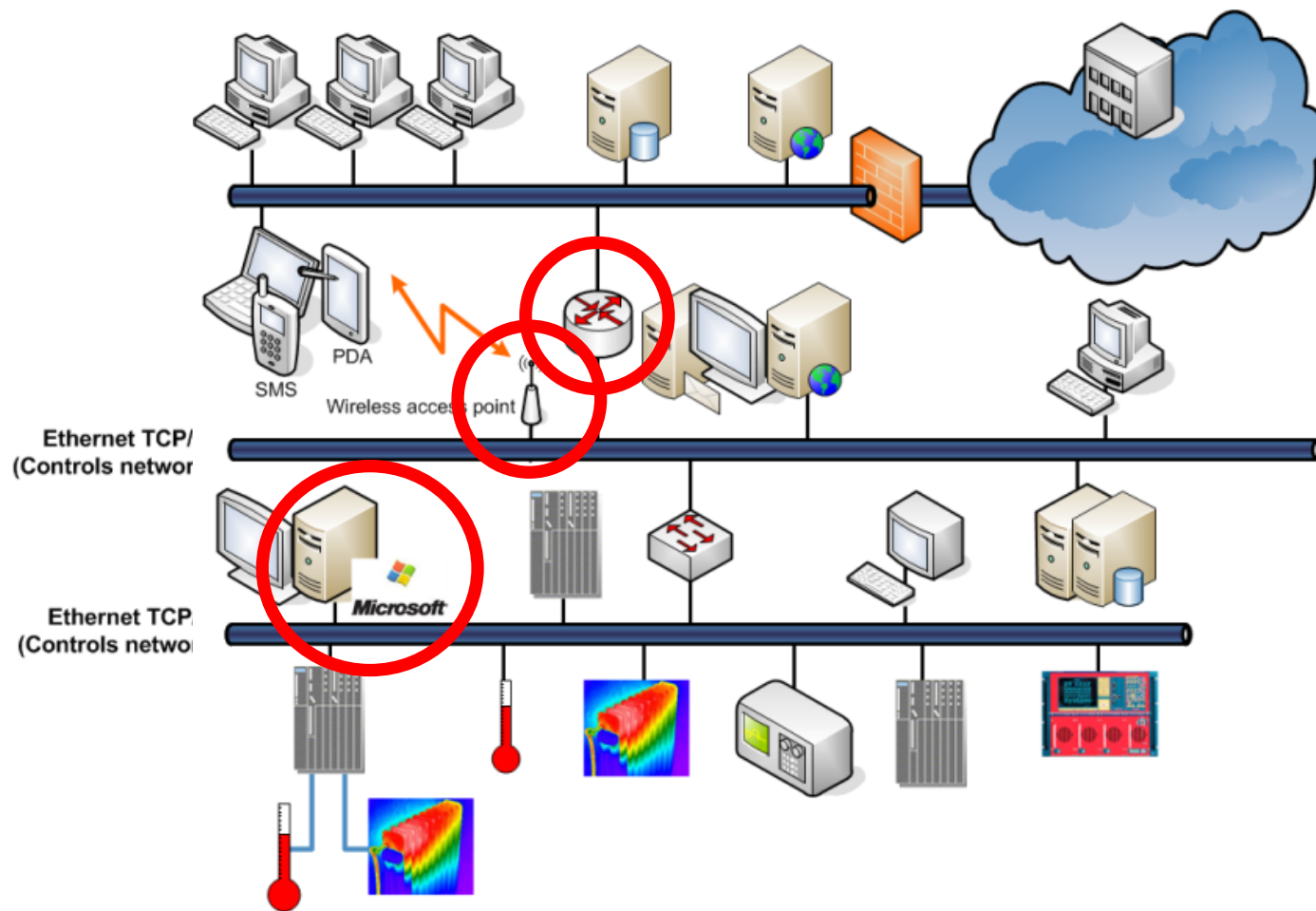


Industrial Control System (ICS)



Safety System





Experiments:

ALICE, ATLAS,
CMS, LHCb,
LHCf, Moedal,
TOTEM

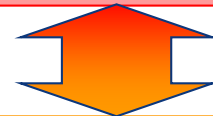
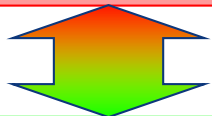
Alfa, AMS,
Asacusa, Atrap,
Cast, Collaps,
Compass, Dirac,
GIF, ISOLTRAP,
MICE, Miniball,
Mistral, NA49,
NA60, NA62,
nTOF, Witch, ...

GCS, MCS,
MSS, Cryo



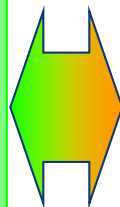
Safety: ACIS, AC PS1, AC PS2, AC SPS1, AC SPS2, ADS, Alarm Repeater, ARCON, CCTV, CESAR, CSA, CSAM, DSS, LACS, LASER, LASS, MSAT, RAMSES, Radio Protection Service, SFDIN, SGGAZ, Sniffer, SUSI, TIM

Infrastructure: CV, DBR, ENS, FM, Gamma Spectroscopy, Moni, Moon, Spectrum, TS/CSE, YAMS



Accelerators:

AD, AWAKE, CLIC3,
Elena, FCC, ILC,
ISOLDE, LEIR, LHC,
Linac 2/3/4, PS, PS
Booster, SPS



Accelerator Infrastructure:

ACS, ADT, APWL, BCTDC, BCTF, BDI,
BQE, BQS, BQK, BPAWT, BIC, BLM,
BOF, BPL, BPM, BOB, BRA, BSRT, BTV,
BWS, Cryo, CWAT, FGC, LEIR LLRF, LHC
Beam Control, LBDS, LHC Logging
Service, LTI, MKQA, OASIS, PIC,
QDS/QPS, SPS BT, Vacuum, WIC





Pain Points of Securing Modern ICSes
Dr. Stefan.Lueders@cern.ch
Swiss Cyber Storm, October 18th 2017, Lucerne (CH)

CERN: Examples of ICS Devices

Bye, Bill. Welcome RasPI & Arduino

Core-ICS apart, interconnections will grow

ICS and IoT will merge in some way

Wireless is already on the plant-floor

Internet & cloud access will become normal

Incentives for secure ICS lacks business case



**Exposure
Threats**

**Complexity
Vulnerabilities**

**Dependencies
Consequences**



The LHC: A One-Time Prototype

**The Revolution of ICS:
Old paradigms don't hold
anymore.**

ICS & IT: Towards a joint future



One IT service to rule them all:
Network, O/S & VMs (WSUS, Puppet),
DB, SSO/AD/2FA, storage, web,...

Adapted priorities & schedules

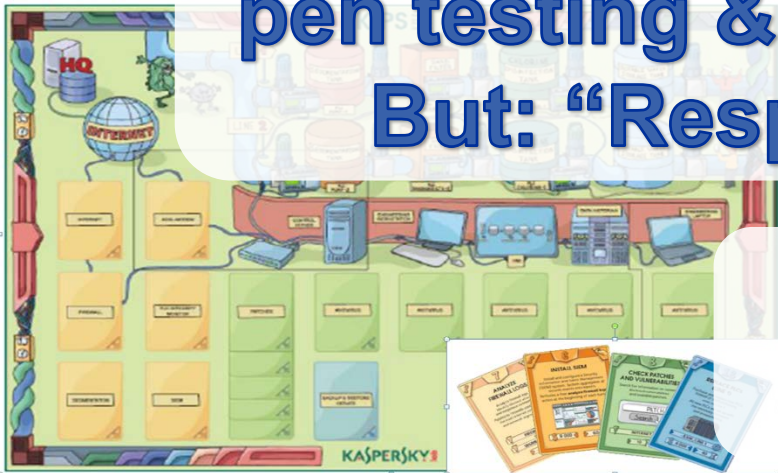
Same technologies.
Same support.
Same people.






Similar training for IT admins & control system experts

“WhiteHat” program to teach people pen testing & vulnerability assessments. But: “Responsible disclosure” fails...



P.S. Why do students come w/o security knowledge?





Know your assets:
Connected devices
(DC, ICS), VMs, DBs,
accounts, websites, ...

Ownership & automatic life-cycle

Analysis of identify (hidden) dependencies







CERN Single Sign-On

Multi-Factor Authentication requested

Sign in with second factor verification

Reminder: you have agreed to comply with the [CERN computing rules](#)

Select your Multi Factor system

- ☐  **SMS**
Two factor authentication asking your CERN credentials, and a verification code will be sent by SMS to your CERN mobile phone.
- ☐  **Google Authenticator**
Two factor authentication asking your CERN credentials, and a verification code using Google Authenticator Smartphone application.
- ☐  **Yubikey**
Two factor authentication using your USB Yubikey.
- ☐  **Smartcards**
Two factor authentication using your smartcard.

Putty (inactive)

Using username " ".
Login for [redacted]

1. Google Authenticator
2. SMS OTP
3. Yubikey

Option (1-3): █

Permanent isolation impossible (i.e. economically costly)

Security vs Usability: Acceptance threshold

Rolling out 2FA AuthN: CLI pain & no silver bullet



Pain Points of Securing Modern ICSES

Dr. Stefan.Lueders@cern.ch

Swiss Cyber Storm, October 18th 2017, Lucerne (CH)

Control Remote Access





**Independent test-stands
for initial dev't & roll-out
expensive & impossible...**

~600 VMs for developers



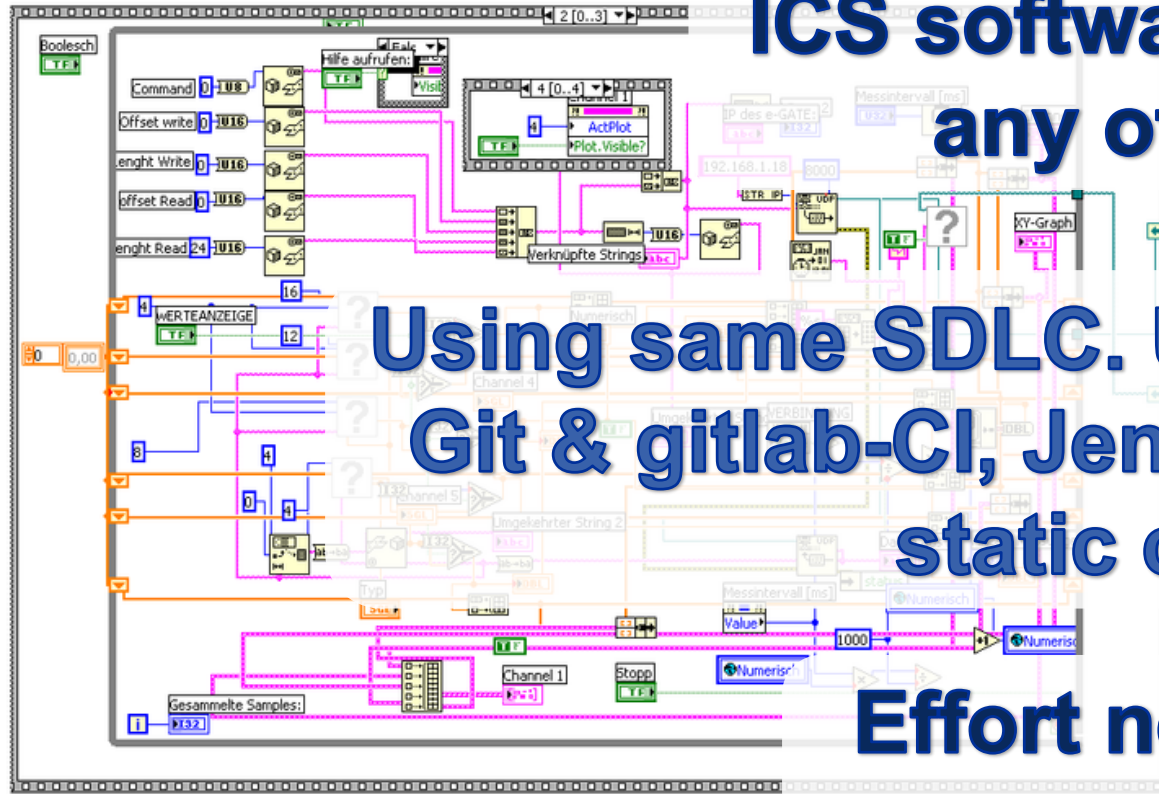
**Final dev't only
possible on real H/W...☹**



**ICS software not different to
any other programming**

**Using same SDLC. Using same tools:
Git & gitlab-CI, Jenkins, Koji, Maven,
static code analyzers, ...**

**Effort needed to integrate
commercial products...**



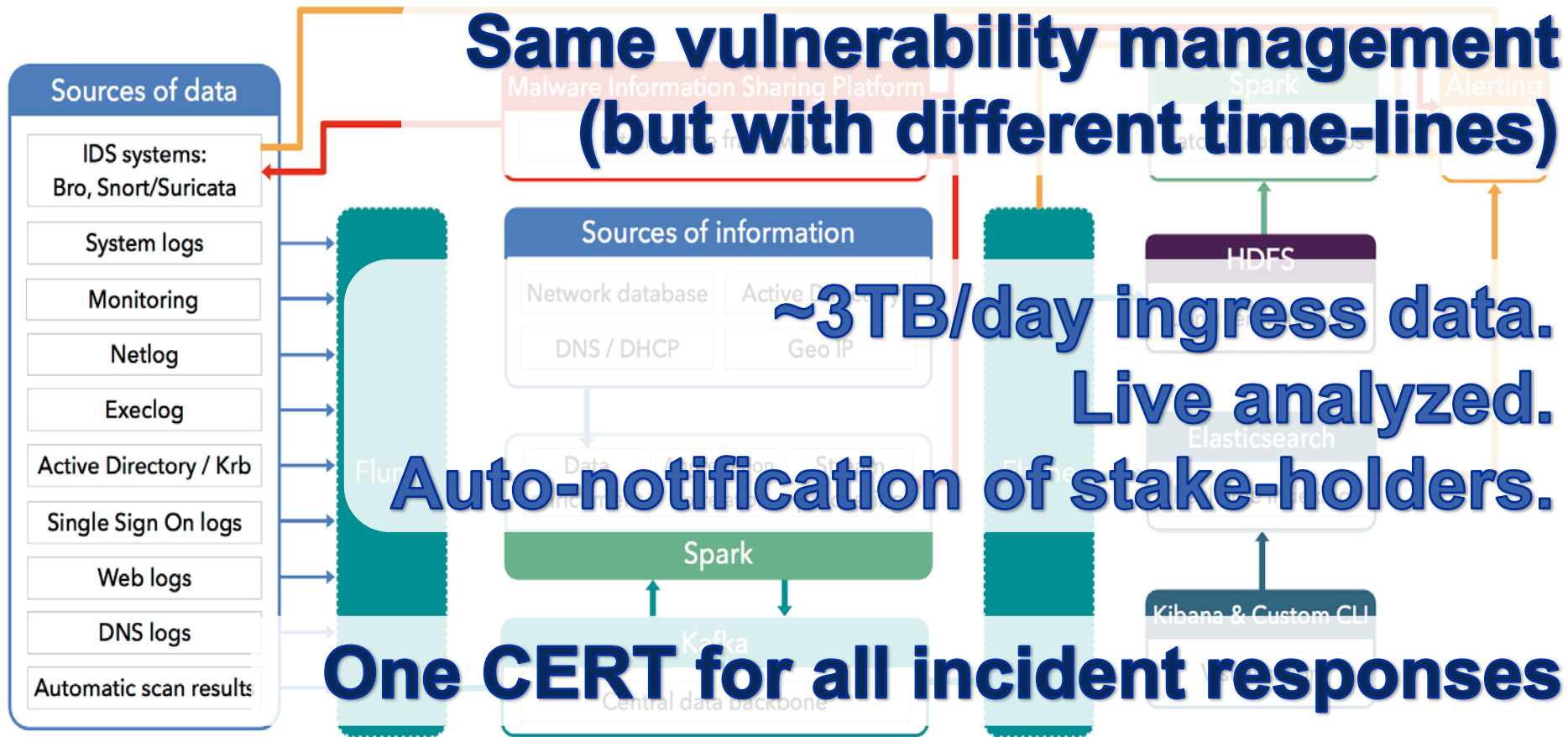


CYBERSECURITY EU AGENCY AND CERTIFICATION FRAMEWORK

In order to scale up the EU's response to cyber-attacks, improve cyber resilience and increase trust in the Digital Single Market, the European Commission has proposed:

- A **European Union Cybersecurity Agency**, building on the European Agency for Network and Information Security (ENISA), which will improve coordination and cooperation across Member States and EU institutions, agencies and bodies;
- The establishment of an **EU cybersecurity certification framework** that will ensure the trustworthiness of the billions of devices ("Internet of Things") which drive today's critical infrastructures, such as energy and transport networks, and also new consumer devices, such as connected cars.

Same vulnerability management (but with different time-lines)





**Resilience &
Robustness is key**

Impact & criticality analyses

**Rigorous safety systems
prevent (malicious) damage,
but reduce availabilities**

No impact, no risk   



We live in symbiosis with ICSes.

Their interconnections open up → IoT

Resilience through safety systems essential!

**Next: Apply same methods as for
Data Centre or office IT. Everywhere.**

**Still: Incentives for secure ICS/IoT lacking.
When are Bounty Programs enforced?**



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



Pain Points of Securing Modern ICSeS
Dr. Stefan.Lueders@cern.ch
Swiss Cyber Storm, October 18th 2017, Lucerne (CH)

Thank you... Questions?



www.cern.ch