Bridging the gap between ICS/IoT and corporate IT security

The LHC: A One-Time Prototype

Revolution of ICS: The Problem 2.0

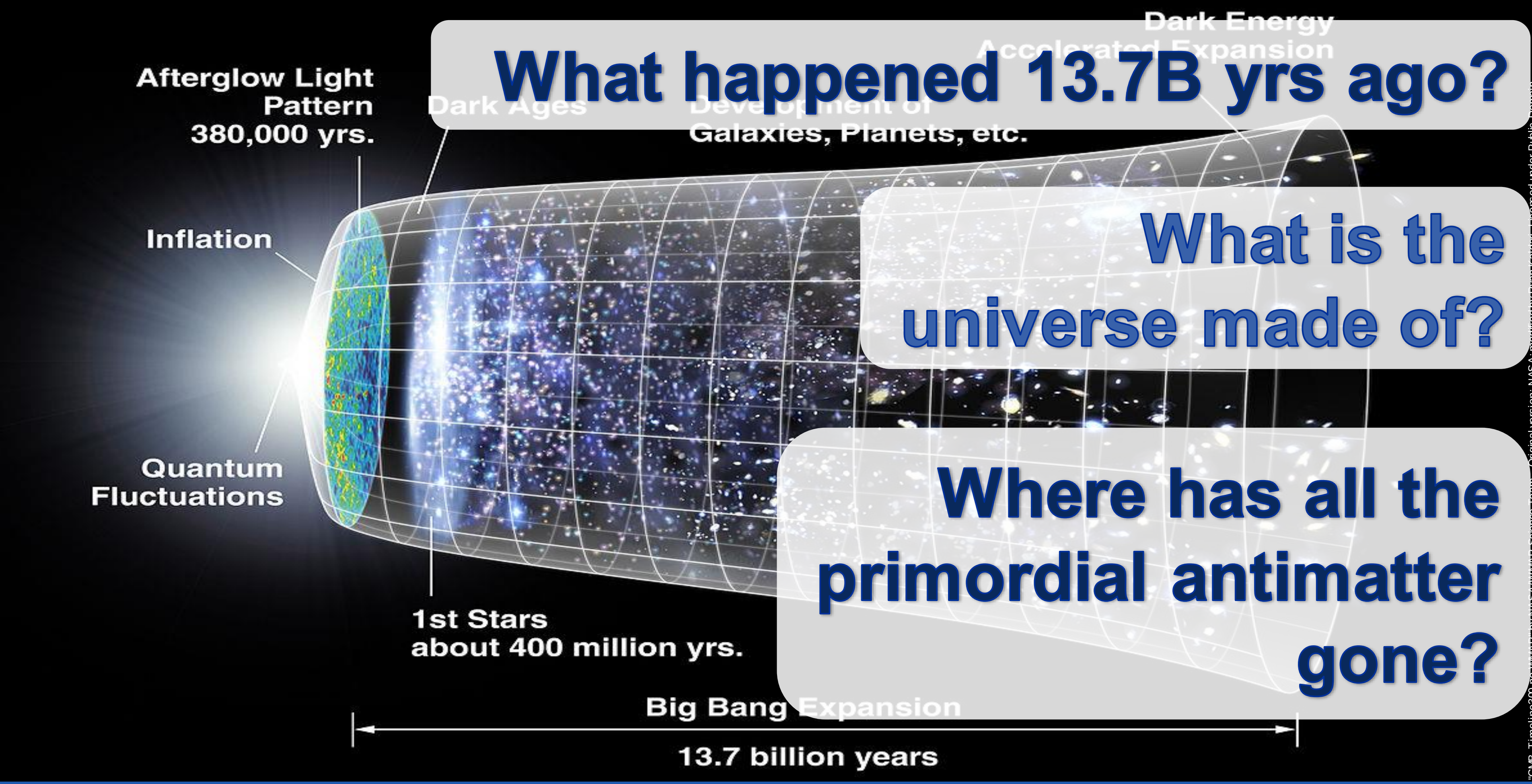
ICS & IT: Towards a joint future

Overview

CERN

European Organization for Particle Physics

Exploring the frontiers of knowledge



What happened 13.7B yrs ago?

What is the universe made of?

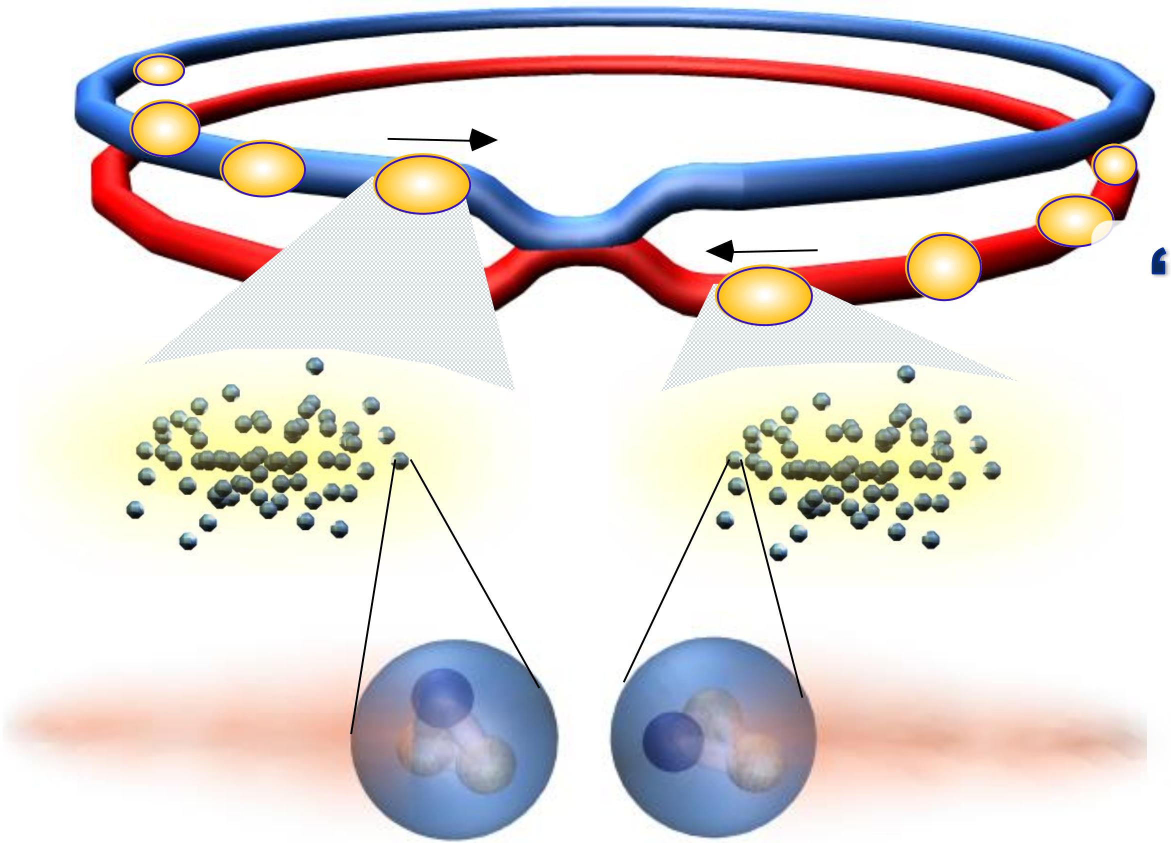
Where has all the primordial antimatter gone?

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

Mankind's Curiosity…

LIMATEUR
DE
OTECTION

Mankind. Literally.

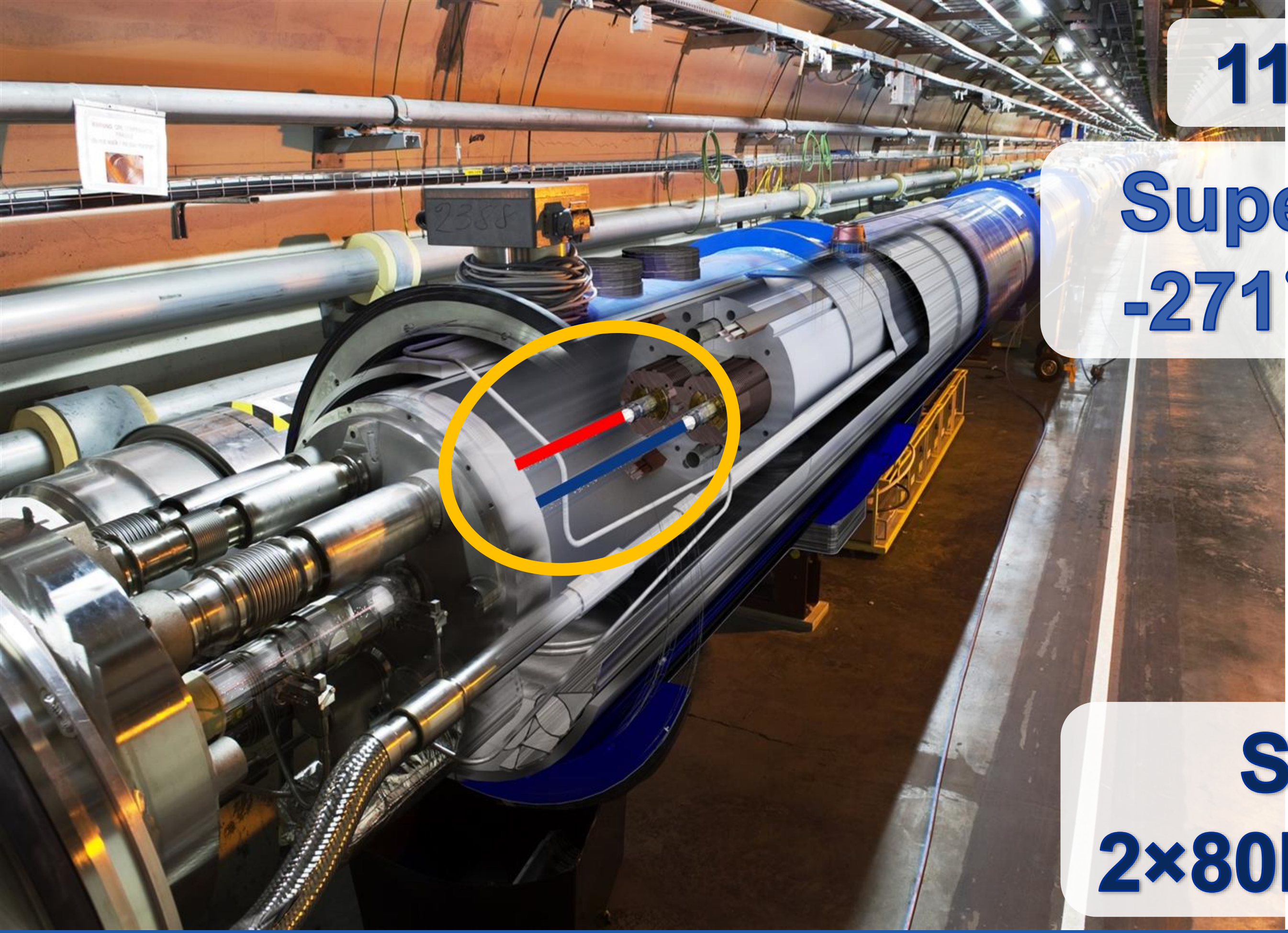


“Beam”: 2×2556b

“Bunch”: 10^{11}p

Protons/Quarks

Creating Big Bang Conditions

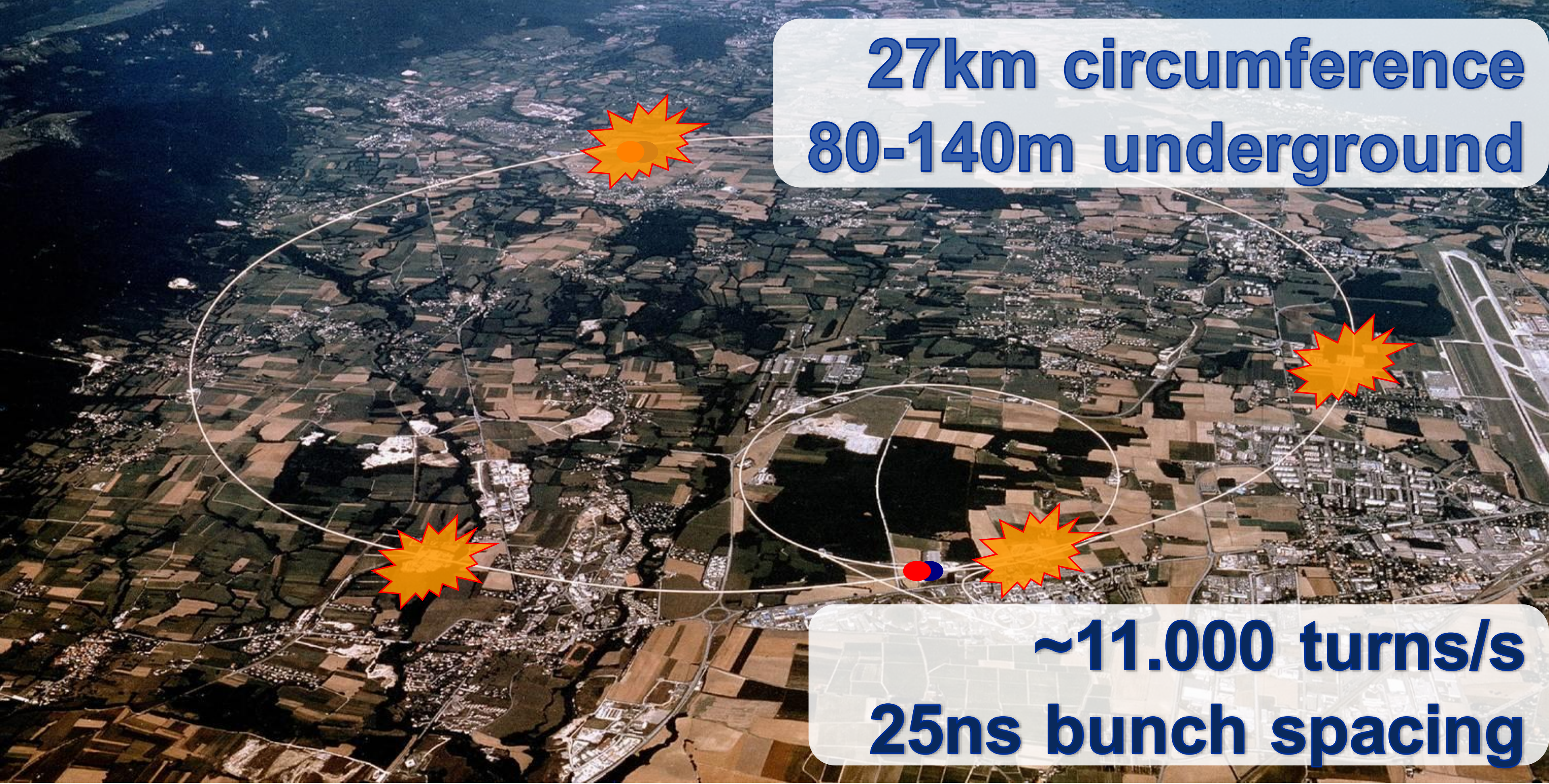


11.000A current

Superconducting: -271˚C (1.9K) cold

Stored energy: 2×80kg TNT equiv.

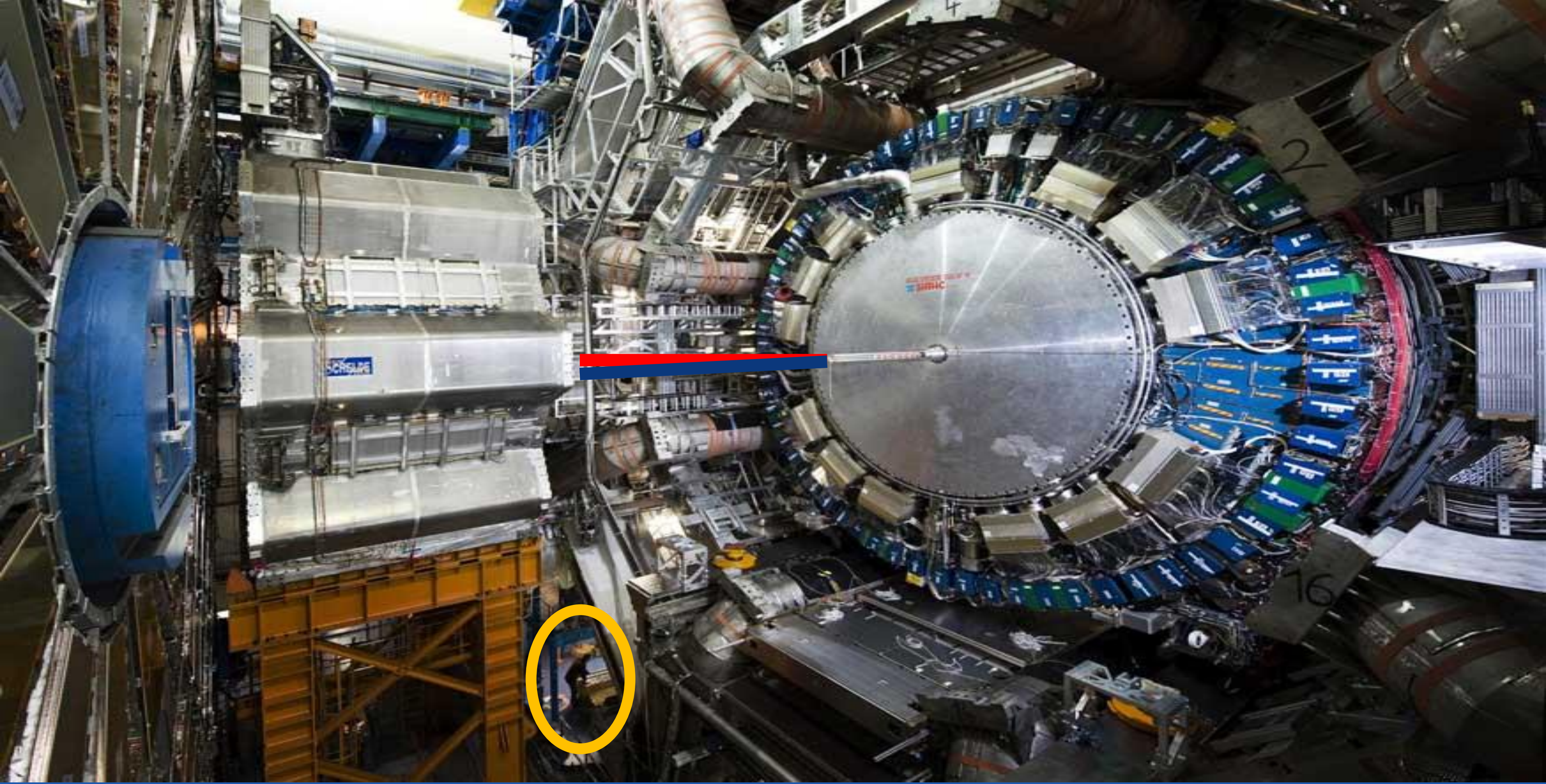
Controlling a Jedi™ Lightsaber



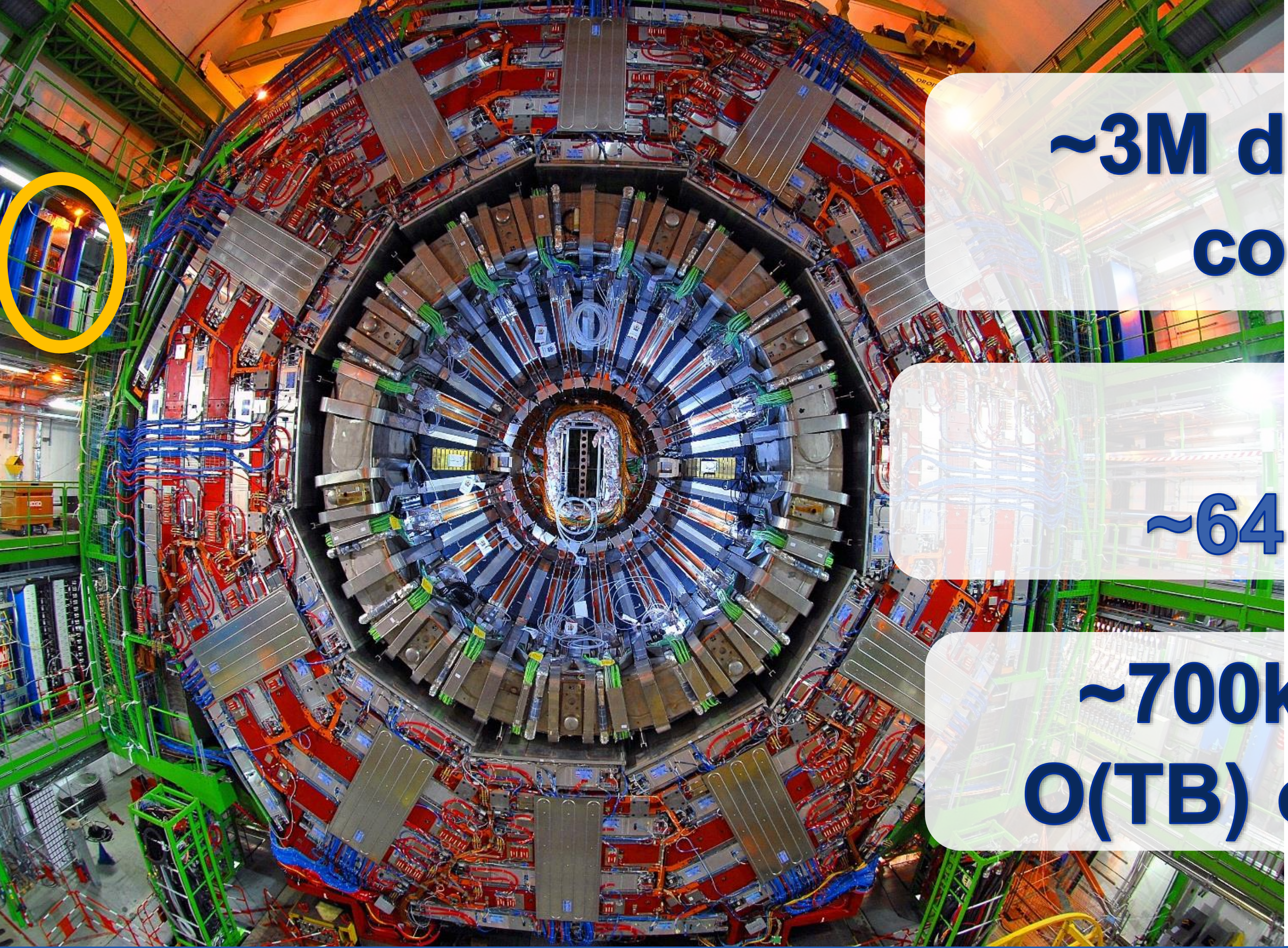
27km circumference
80-140m underground

~11.000 turns/s
25ns bunch spacing

The Large Hadron Collider (LHC)



The ATLAS “camera” (open)

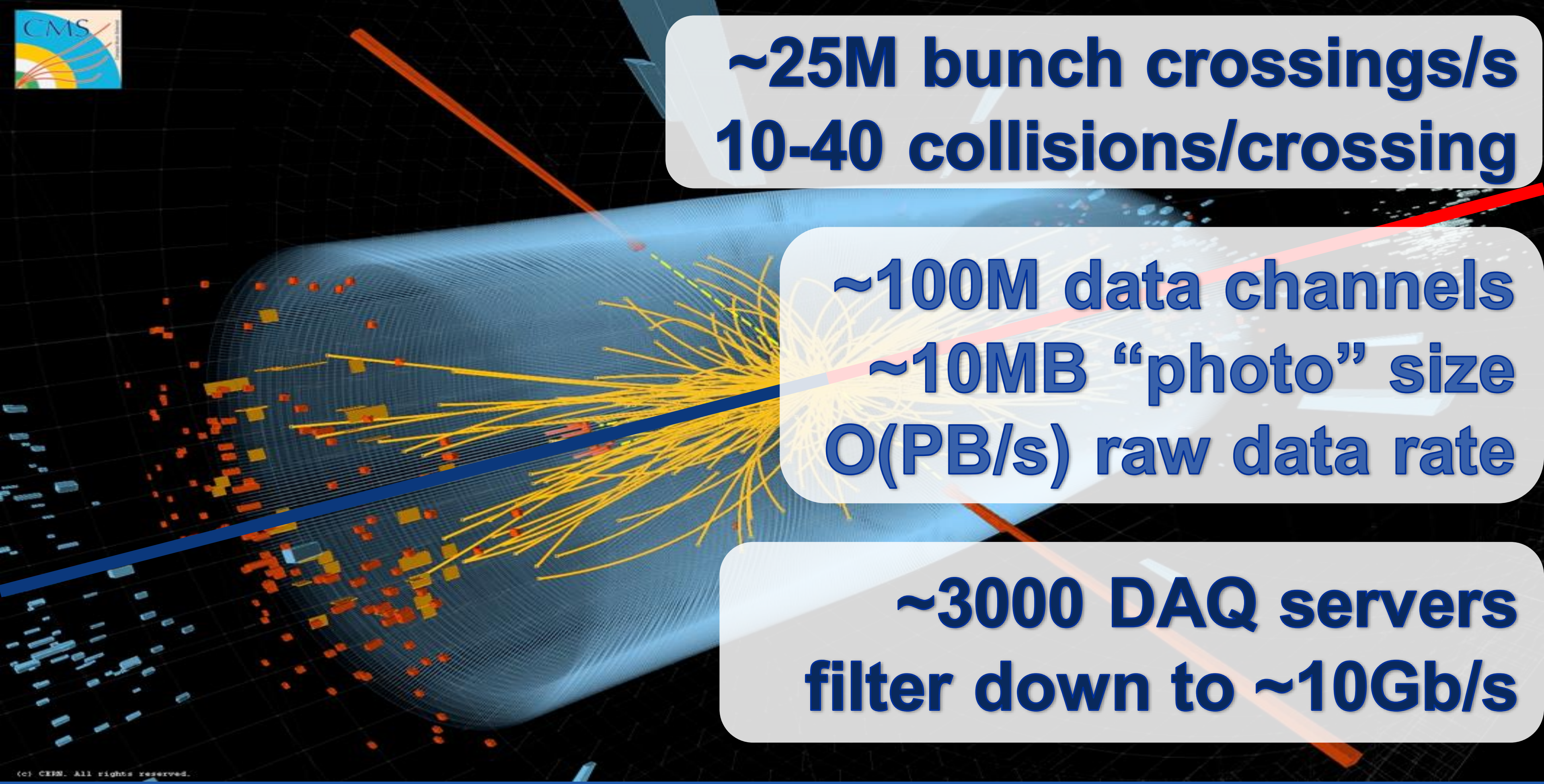


~3M digital & analog control channels

~34 ICS on ~64 blade servers

~700k lines of code O(TB) of config. data

The CMS “camera” (open)



~25M bunch crossings/s
10-40 collisions/crossing

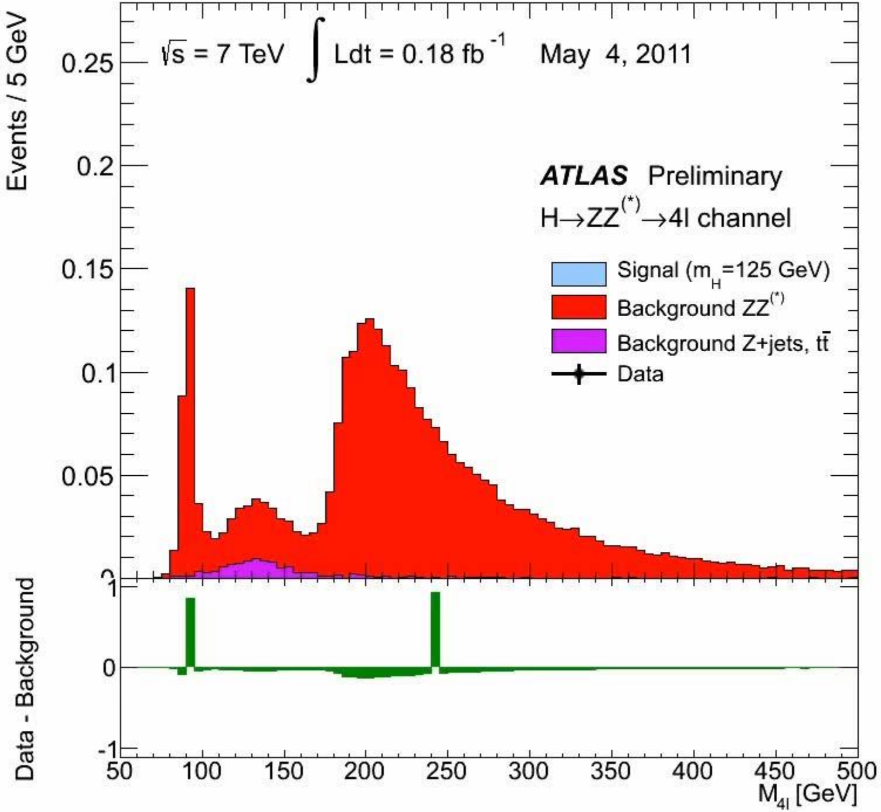
~100M data channels
~10MB “photo” size
O(PB/s) raw data rate

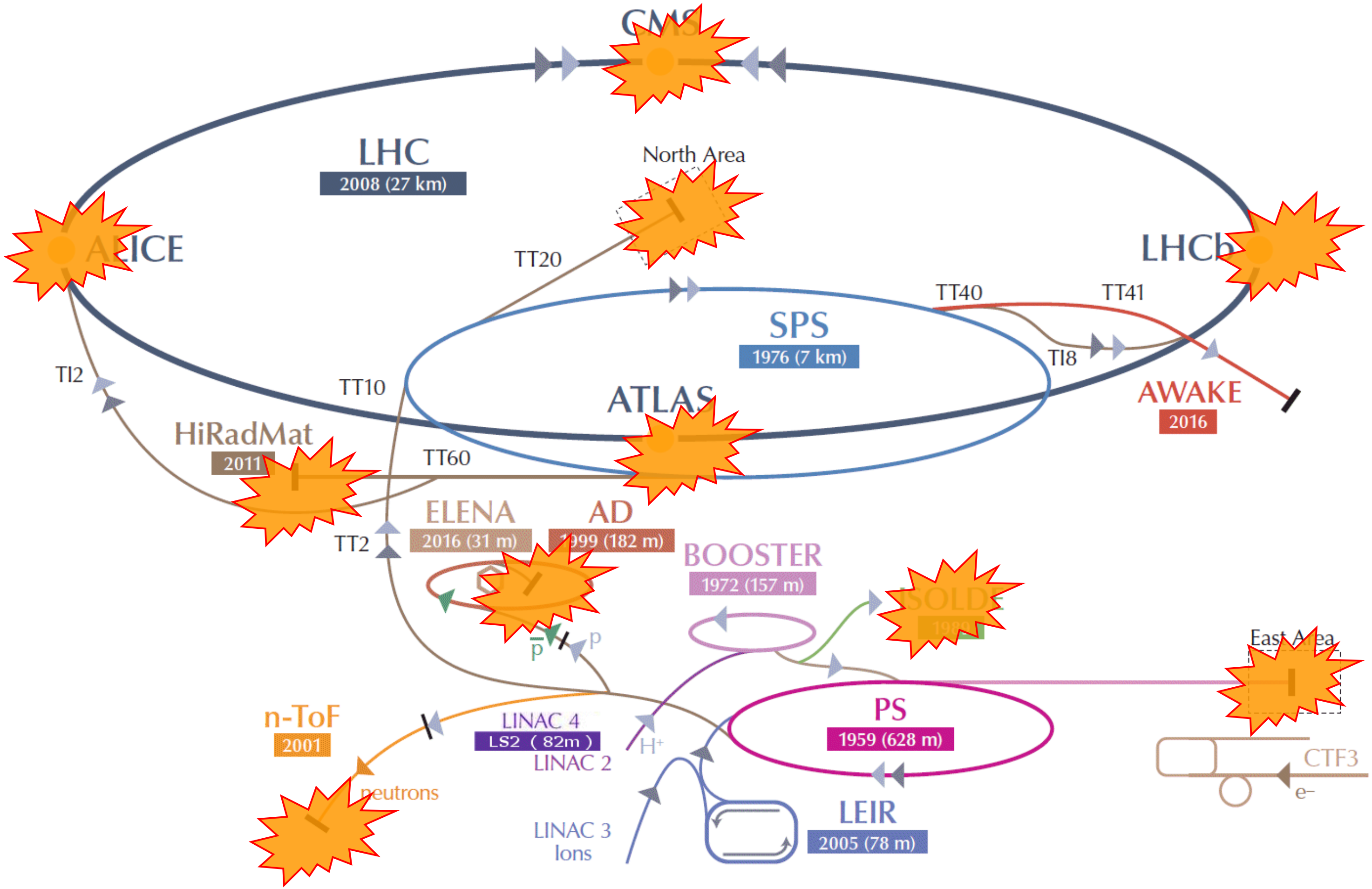
~3000 DAQ servers
filter down to ~10Gb/s

(c) CERN. All rights reserved.

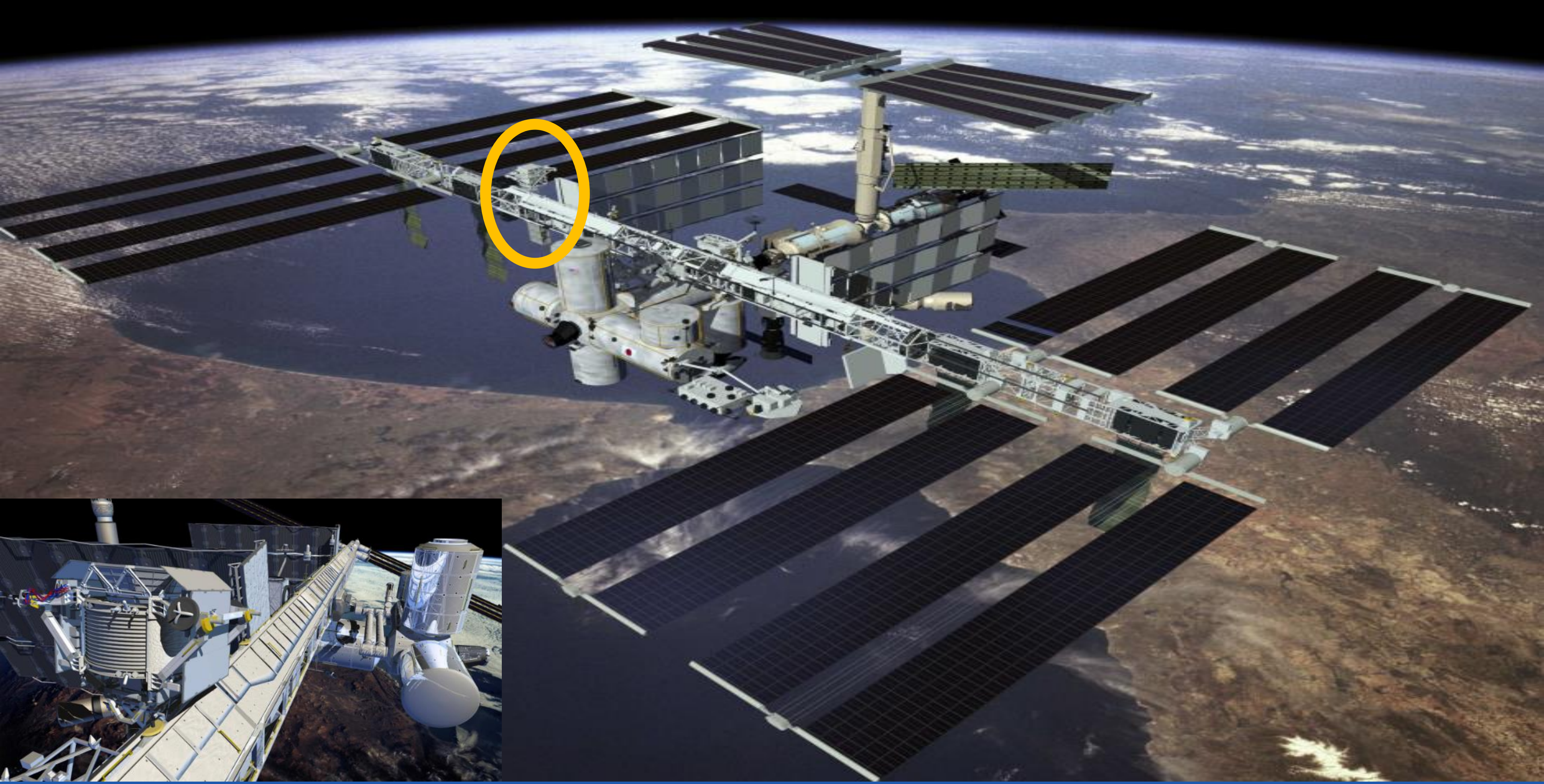
3D “Photo” of a LHC Collision

Return on Investment





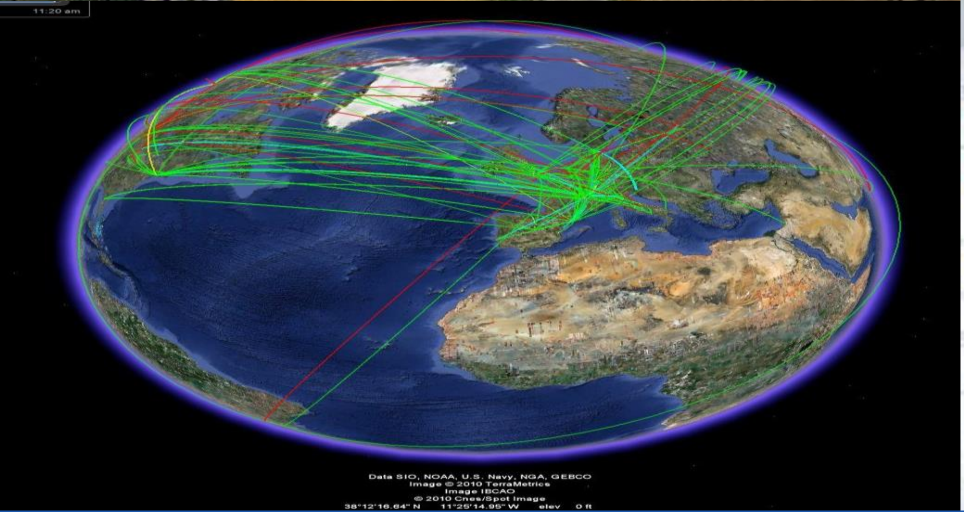
More than the LHC…



AMS: A Detector in Space

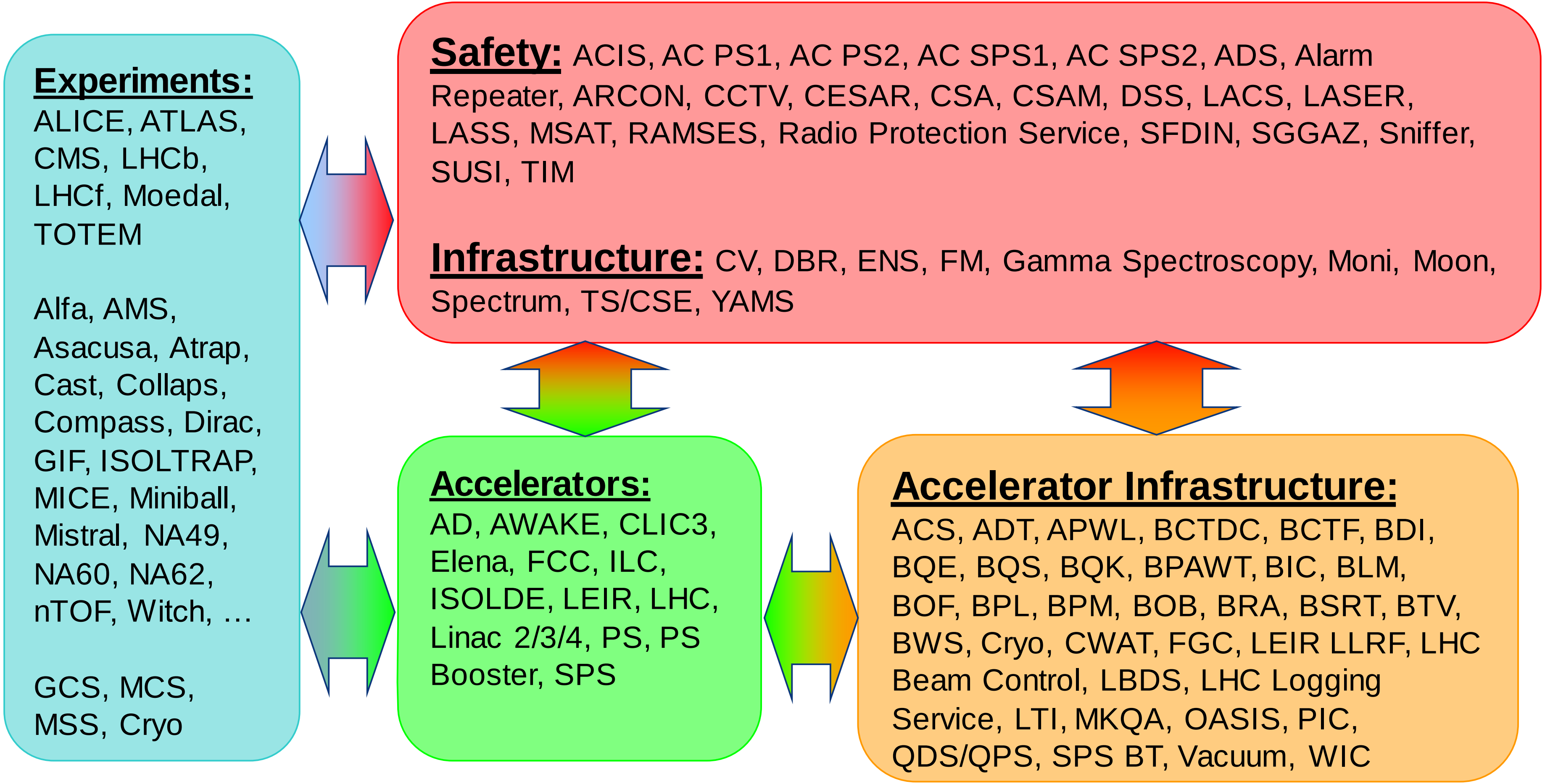
The LHC: A One-Time Prototype

Revolution of ICS: The Problem 2.0


11:20 am
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image © 2010 TerraMetrics
Image IBCAO
© 2010 Cnes/Spot Image
38°12'16.84" N 11°25'14.95" W elev 0 ft

Computer Security: Sectors of Operation

CERN: 100+ of (commercial) ICSes



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

CERN: Examples of ICS Devices

Bye, MS Win. Welcome RasPI & Arduino

Core-ICS apart, interconnections will grow

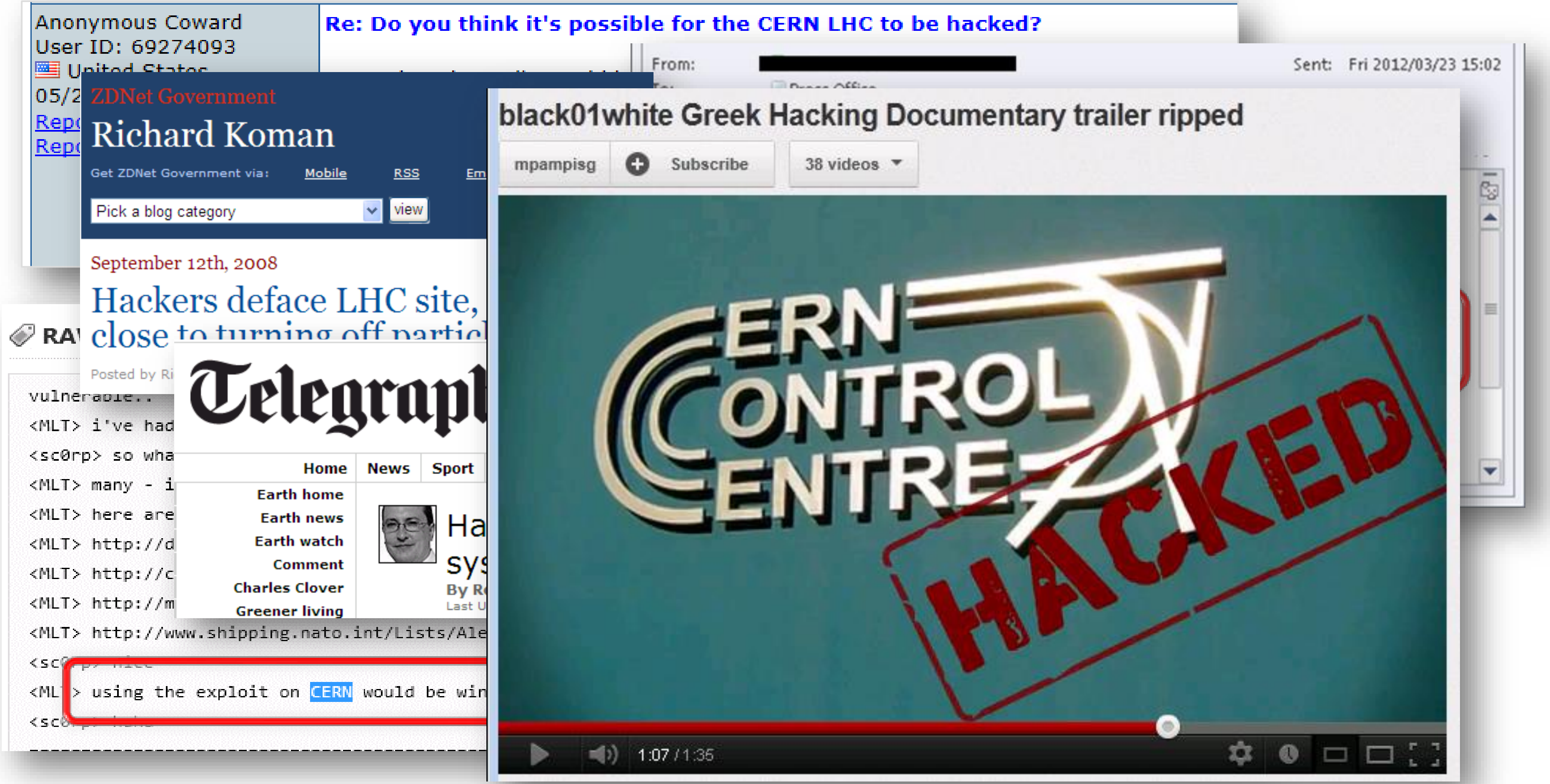
ICS and IoT will merge in some way

Wireless is already on the plant-floor

Internet & cloud access will become normal

Incentives for secure ICS lacks business case

The Problem 2.0



Anonymous Coward
User ID: 69274093
United States
05/2
Repo
Repo

Re: Do you think it's possible for the CERN LHC to be hacked?

From: [redacted] Sent: Fri 2012/03/23 15:02
To: Press Office

ZDNet Government
Richard Koman
Get ZDNet Government via: Mobile RSS Em
Pick a blog category view

September 12th, 2008

Hackers deface LHC site, close to turning off partic

Posted by Ri

RA

```
vulnerable..
<MLT> i've had
<sc0rp> so wha
<MLT> many - i
<MLT> here are
<MLT> http://d
<MLT> http://c
<MLT> http://m
<MLT> http://www.shipping.nato.int/Lists/Ale
<sc0rp> nice
<MLT> using the exploit on CERN would be win
<sc0rp> hehe
```

Telegraph
Home News Sport
Earth home
Earth news
Earth watch
Comment
Charles Clover
Greener living

Ha
sys
By R
Last U

black01white Greek Hacking Documentary trailer ripped
mpampisg Subscribe 38 videos

WE. ARE. TARGET.

The LHC: A One-Time Prototype

Revolution of ICS: The Problem 2.0

ICS & IT: Towards a joint future

Overview

Resilience & Robustness is key

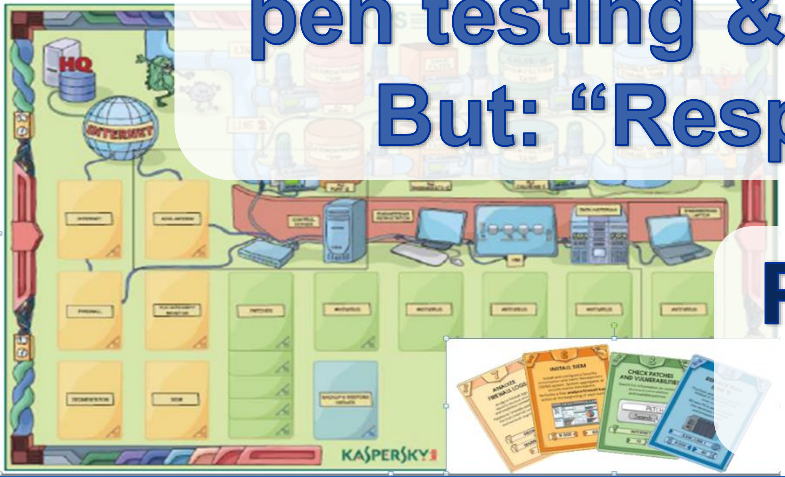
Impact & criticality analyses

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

No impact, no risk ☑☑☑

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?

Train Security at Plant Floor ☑☑☑

cs-srv-44@cern.ch
cs-ccr-dmm1.cern.ch
lxbst060m.cern.ch

Inventory of assets:

Connected devices (DC, ICS), VMs, DBs, accounts, websites, …

Ownership & automatic life-cycle

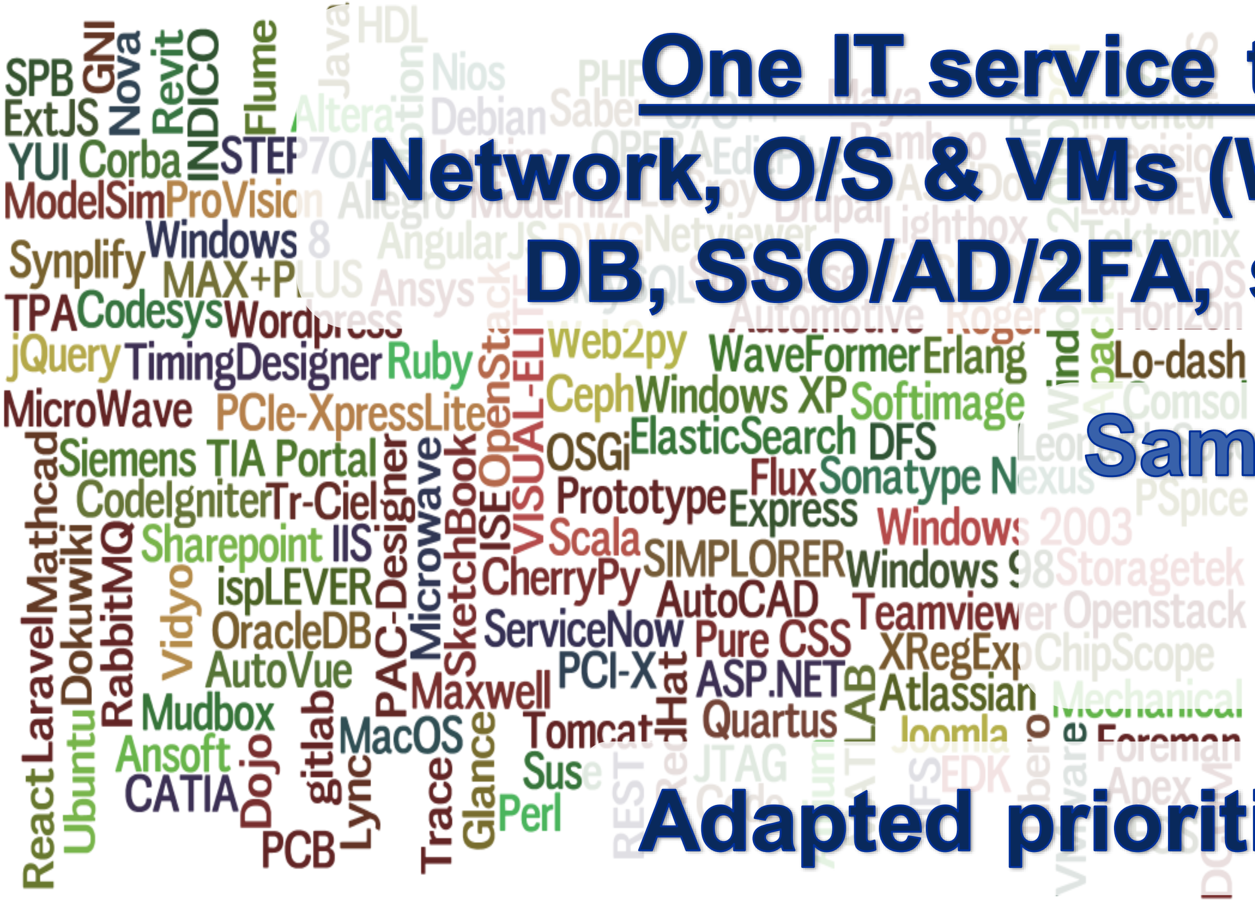
Analysis of identify (hidden) dependencies

One IT service to rule them all:

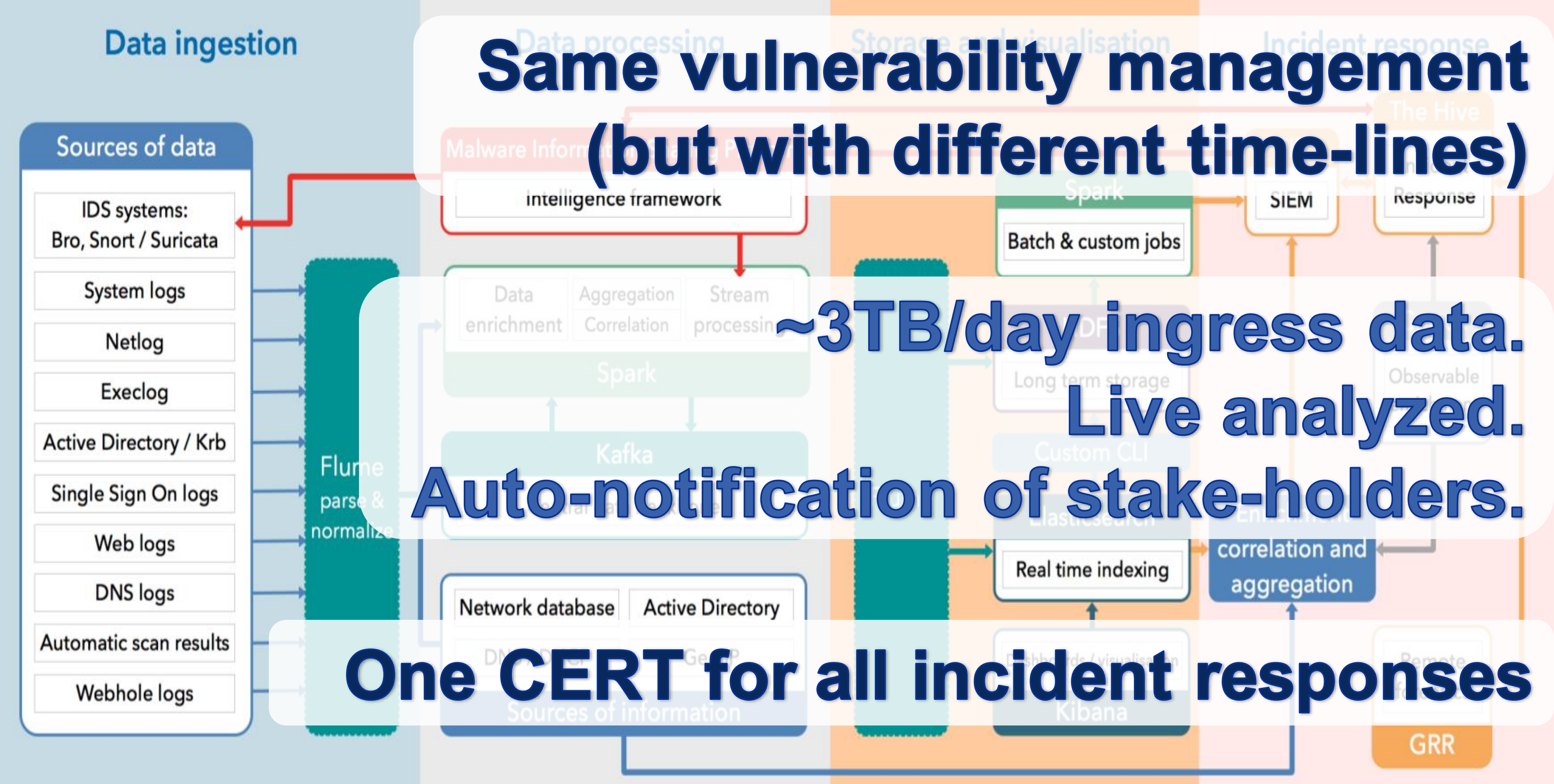
Network, O/S & VMs (WSUS, Puppet), DB, SSO/AD/2FA, storage, web,…

Same technologies.
Same support.
Same people.

Adapted priorities & schedules



Same vulnerability management (but with different time-lines)


Data ingestion

Data processing

Storage and visualisation

Incident response

Sources of data

IDS systems: Bro, Snort / Suricata

System logs

Netlog

Execlog

Active Directory / Krb

Single Sign On logs

Web logs

DNS logs

Automatic scan results

Webhole logs

Flume parse & normalize

Malware Information Sharing Platform

intelligence framework

Data enrichment

Aggregation Correlation

Stream processing

Spark

Kafka

Network database

Active Directory

DNS

GeoIP

Sources of information

Spark

Batch & custom jobs

HDFS

Long term storage

Custom CLI

Elasticsearch

Real time indexing

Dashboards / visualisation

Kibana

The Hive

SIEM

Response

Observable

correlation and aggregation

Remote forensics

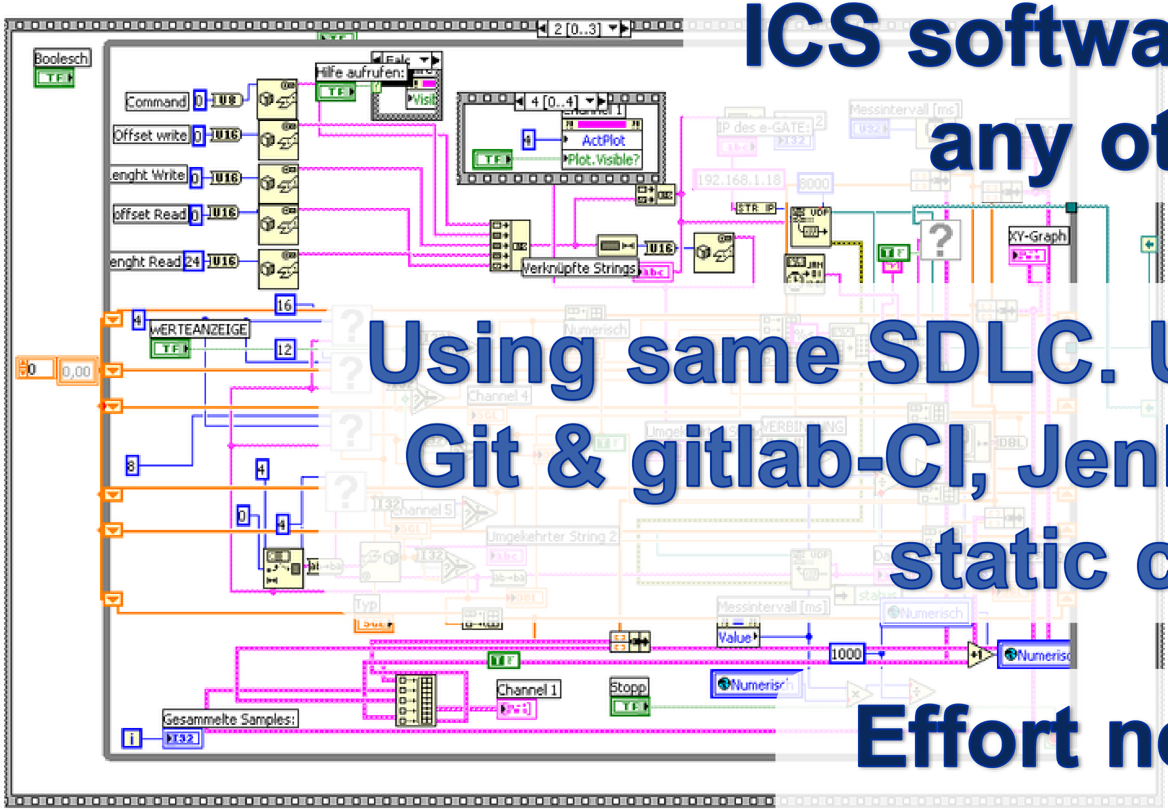
GRR

~3TB/day ingress data.

Live analyzed.

Auto-notification of stake-holders.

One CERT for all incident responses



ICS software not different to any other programming

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

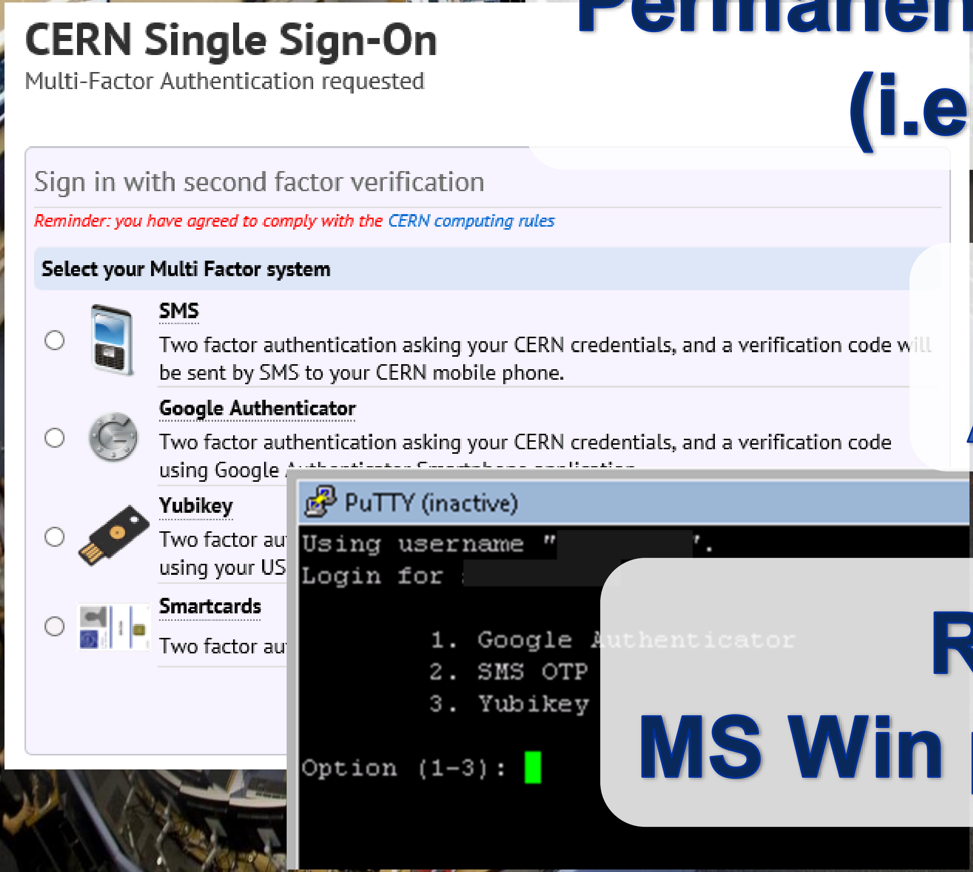
Effort needed to integrate commercial products…

Same S/W Development ☑

Permanent isolation impossible (i.e. economically costly)

Security vs Usability: Acceptance threshold

Rolling out 2FA AuthN: MS Win pain & no silver bullet



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

○ **Yubikey**
Two factor au
using your US

○ **Smartcards**
Two factor au

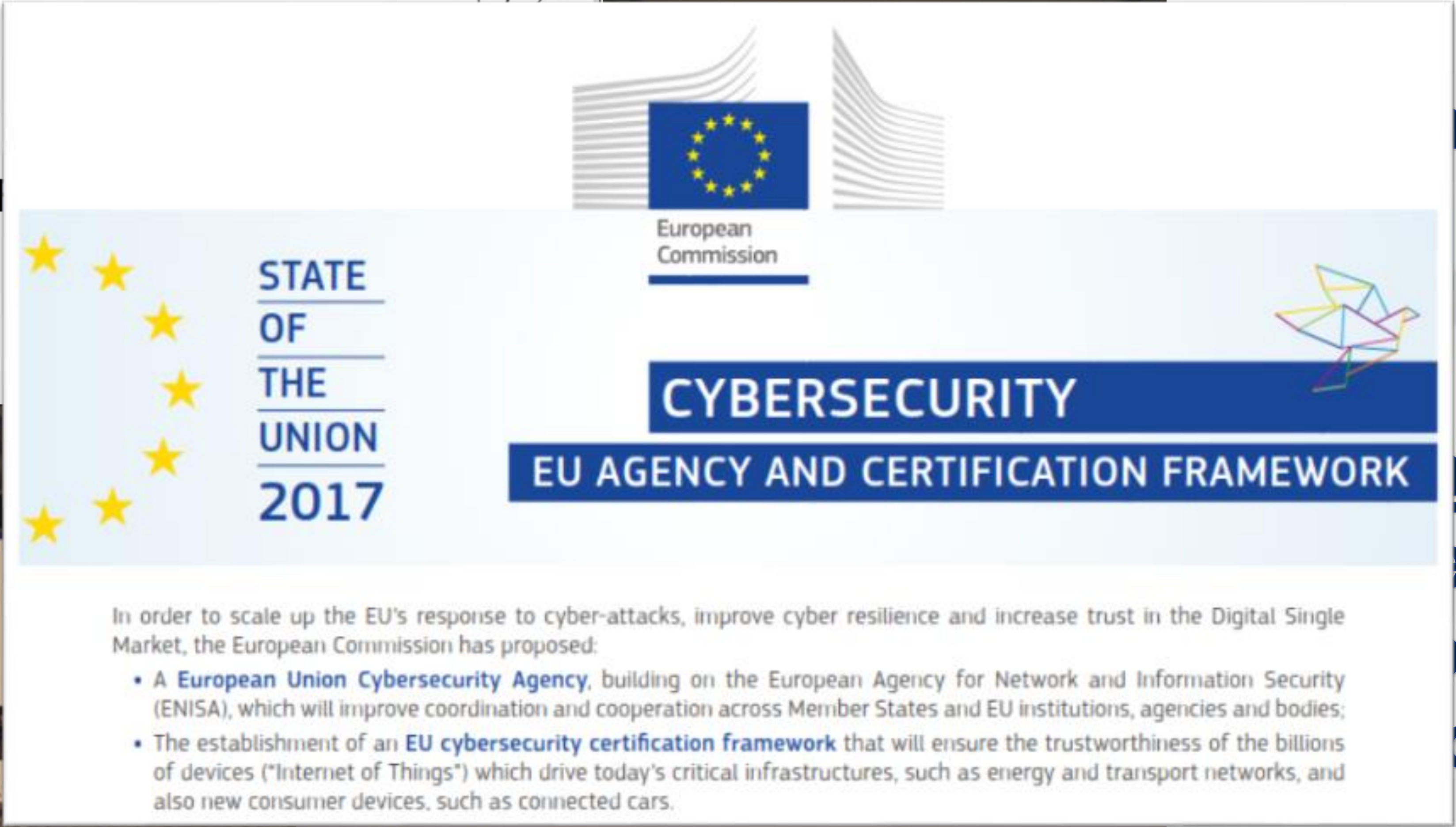
```
Using username "[redacted]".
Login for [redacted]

        1. Google Authenticator
        2. SMS OTP
        3. Yubikey

Option (1-3):
```

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

~600 VMs for developers

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

One-Time Prototype ☒ ☒


European
Commission

STATE OF THE UNION 2017

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.

…

e?

s!

es,

on.

ot.

We need Incentives! ☒ ☒ ☒

Central patching & provisioning

Adapted perimeter. 2FA access control. IDS.

Central services managed by CERN IT

Wifi on plant floor is professional fault

Staged hopping from Internet to plant floor

Involving vendors and complaining bitterly!

The Problem 2.0: CERNs Approach

Watch the new Angels and Demons trailer! In Theaters 5/15/09

THE MUPPETS - Full Trailer 2011

Thank you… Questions?

www.cern.ch