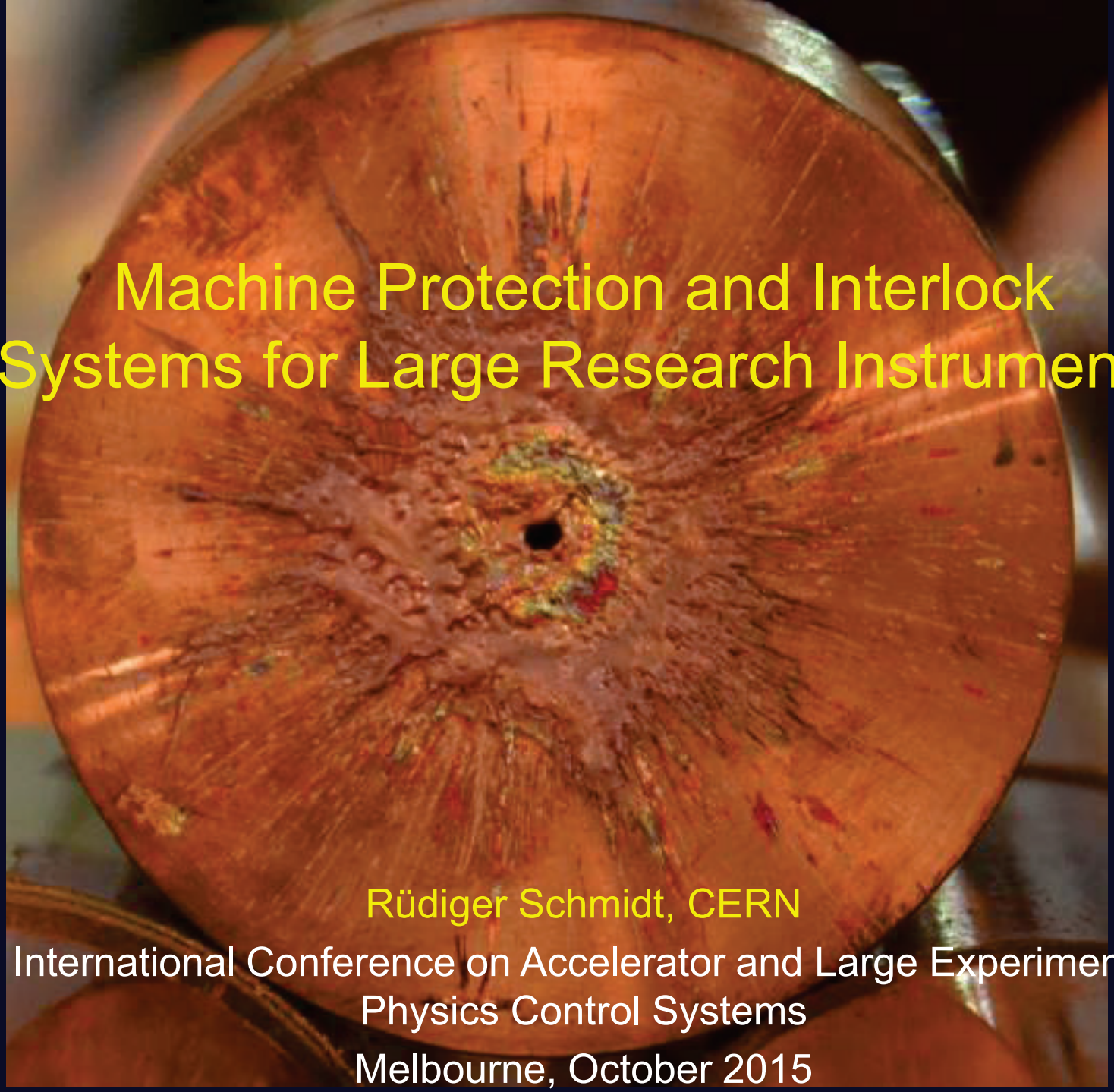
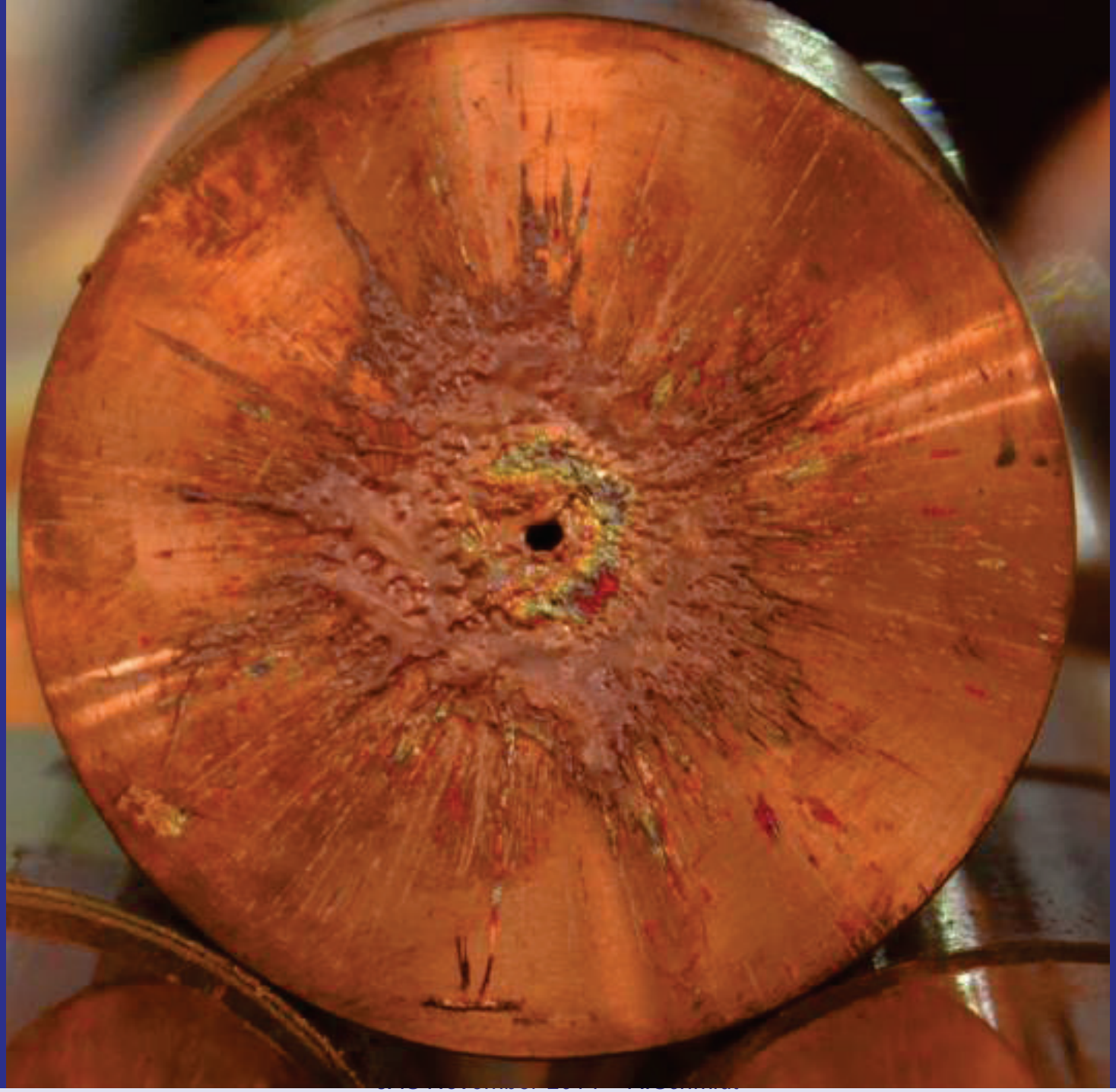


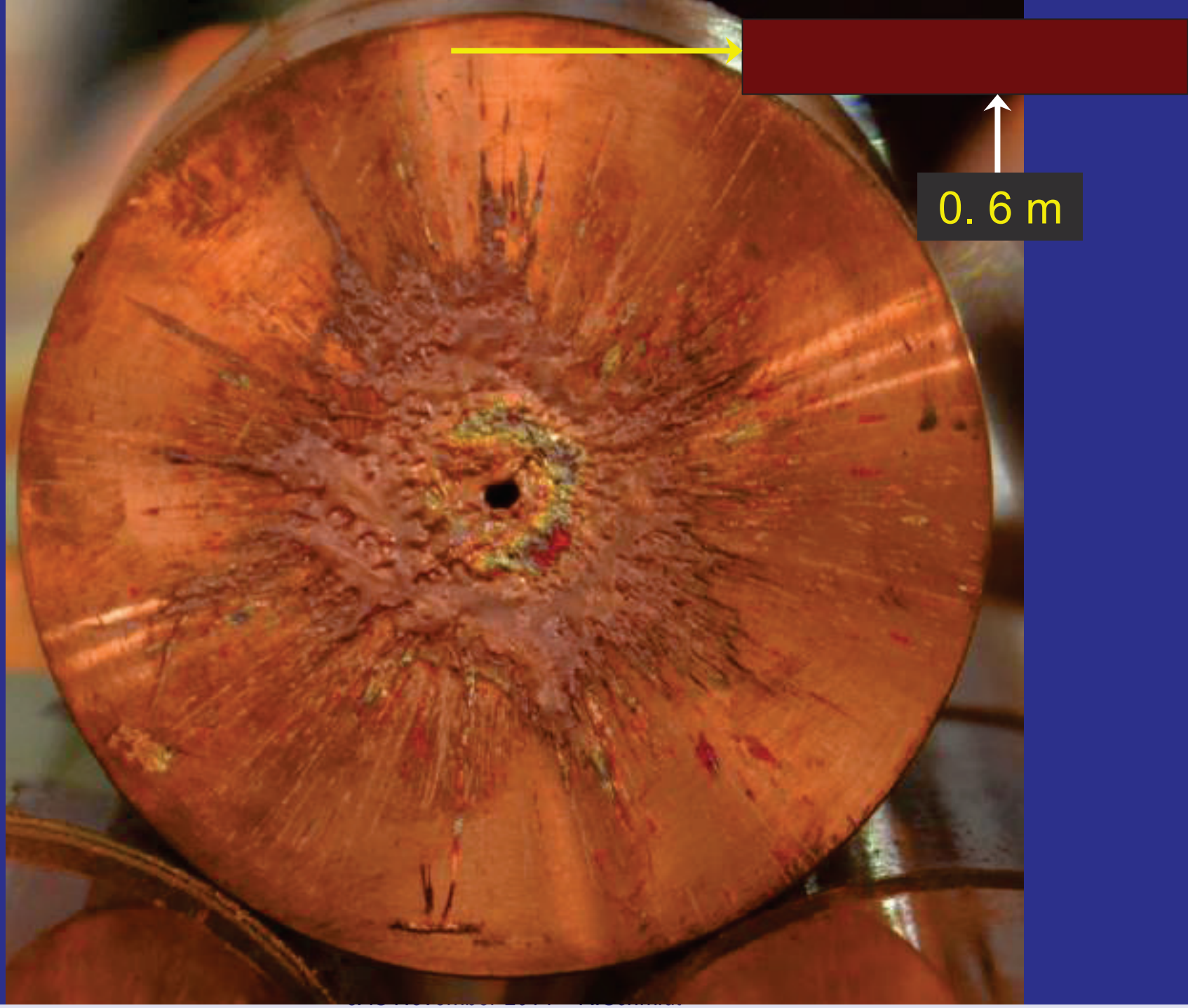
# Machine Protection and Interlock Systems for Large Research Instruments

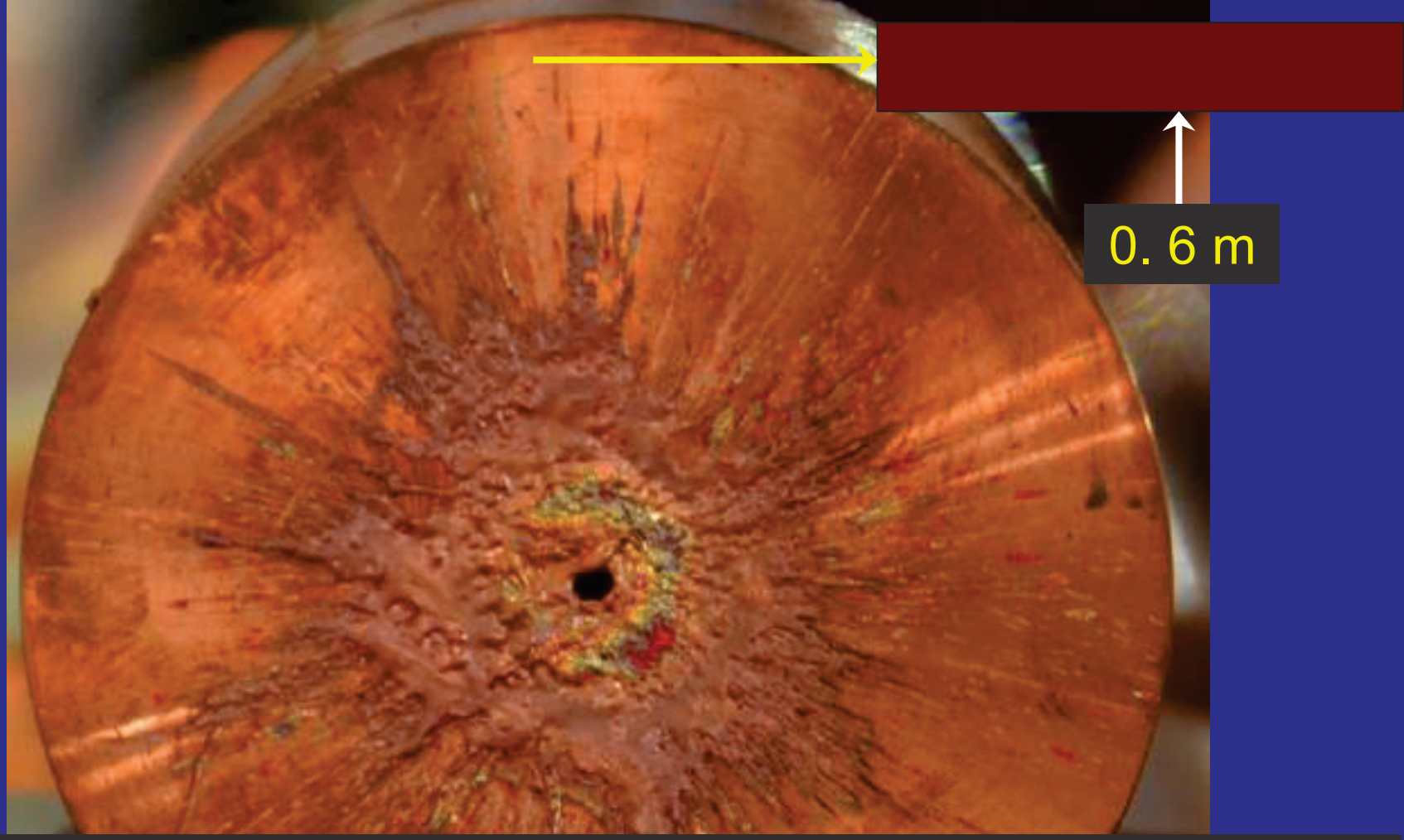
Rüdiger Schmidt, CERN

International Conference on Accelerator and Large Experimental Physics Control Systems

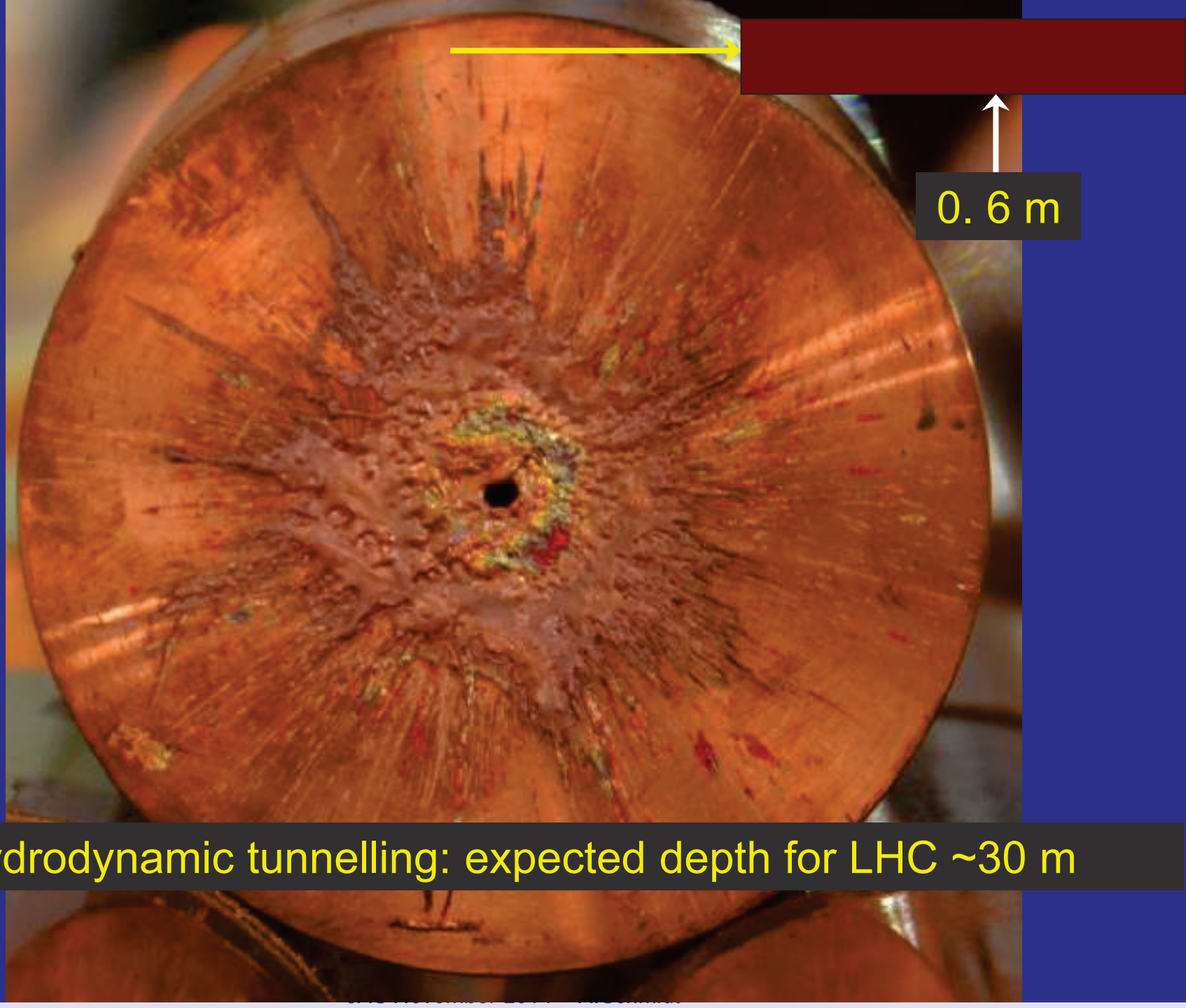
Melbourne, October 2015



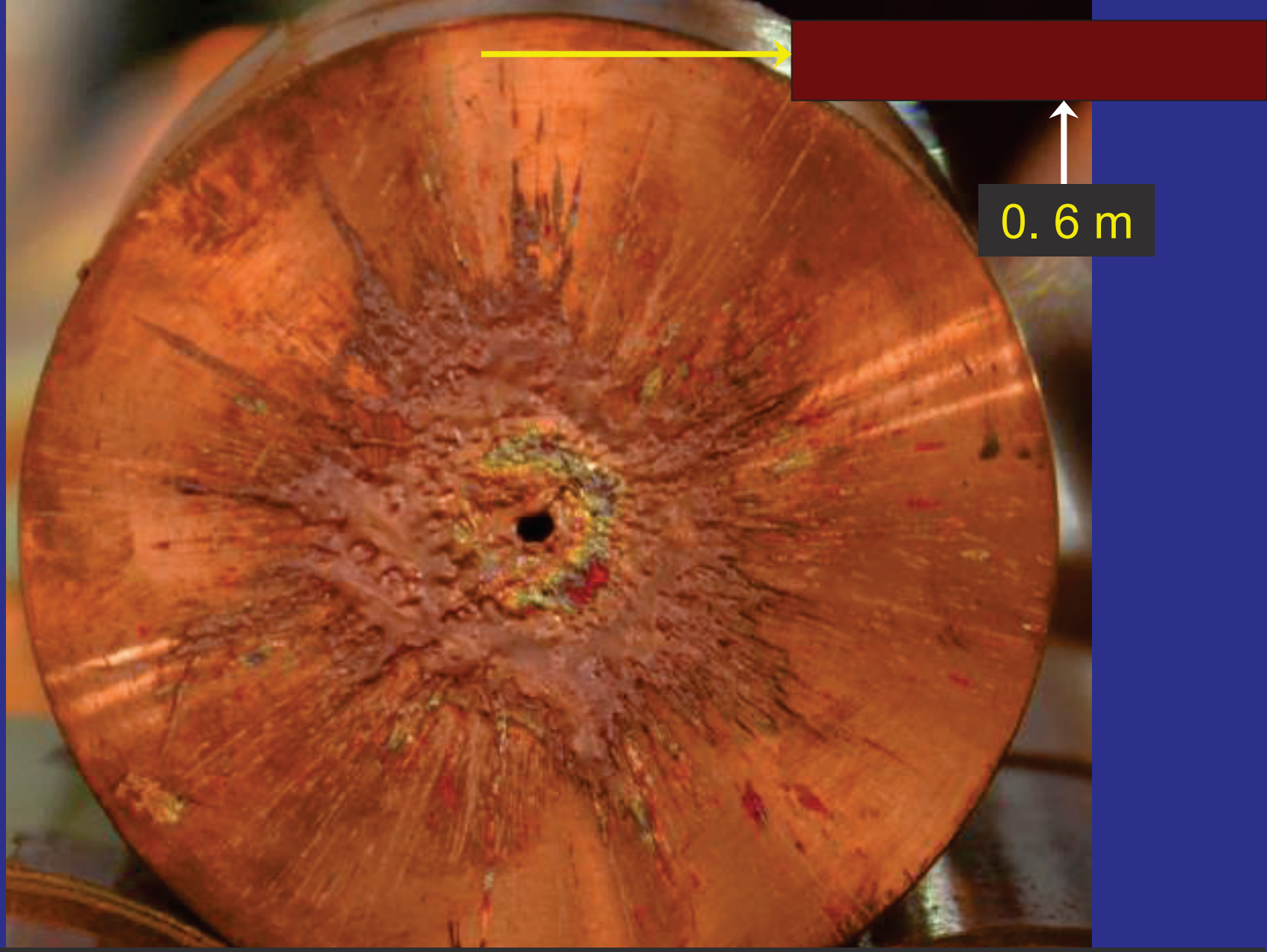

0. 6 m




Copper target at a depth of 0.6 m, irradiated with one SPS beam pulse (1.5 MJ, 7 μs, 450 GeV, 0.2 mm)




Hydrodynamic tunnelling: expected depth for LHC ~30 m




Hydrodynamic tunnelling: expected depth for FCC ~300 m
(FCC study for a proton collider with 100 TeV cm, 100 km length)

# Outline

- My understanding of Machine Protection
- Challenges for Machine Protection

- The role of Control Systems for Machine Protection

See also material in Joint International Accelerator School on "Beam Loss and Accelerator Protection"
http://uspas.fnal.gov/programs/JAS/JAS14.shtml Proceeding to be published by 2016

# What needs protection? From what?

- **Protection of people** – always highest priority
  - There are several hazards: beam, electrical, pressure, oxygen deficiency,..
  - Main strategy to personnel protection: keep them away from hazards (access system)
- **Protection of the environment**
- **This talk is focused on the protection of equipment (accelerators, experiments, targets, fusion reactors)**
  - Similar methods for protection of people and environment
  - Separate personnel protection from equipment protection (not always possible)
- Protection from what?
  - Particle beams and their effects
  - Electromagnetic energy in magnets and RF systems
  - Other sources of energy

# Protection from Energy and Power

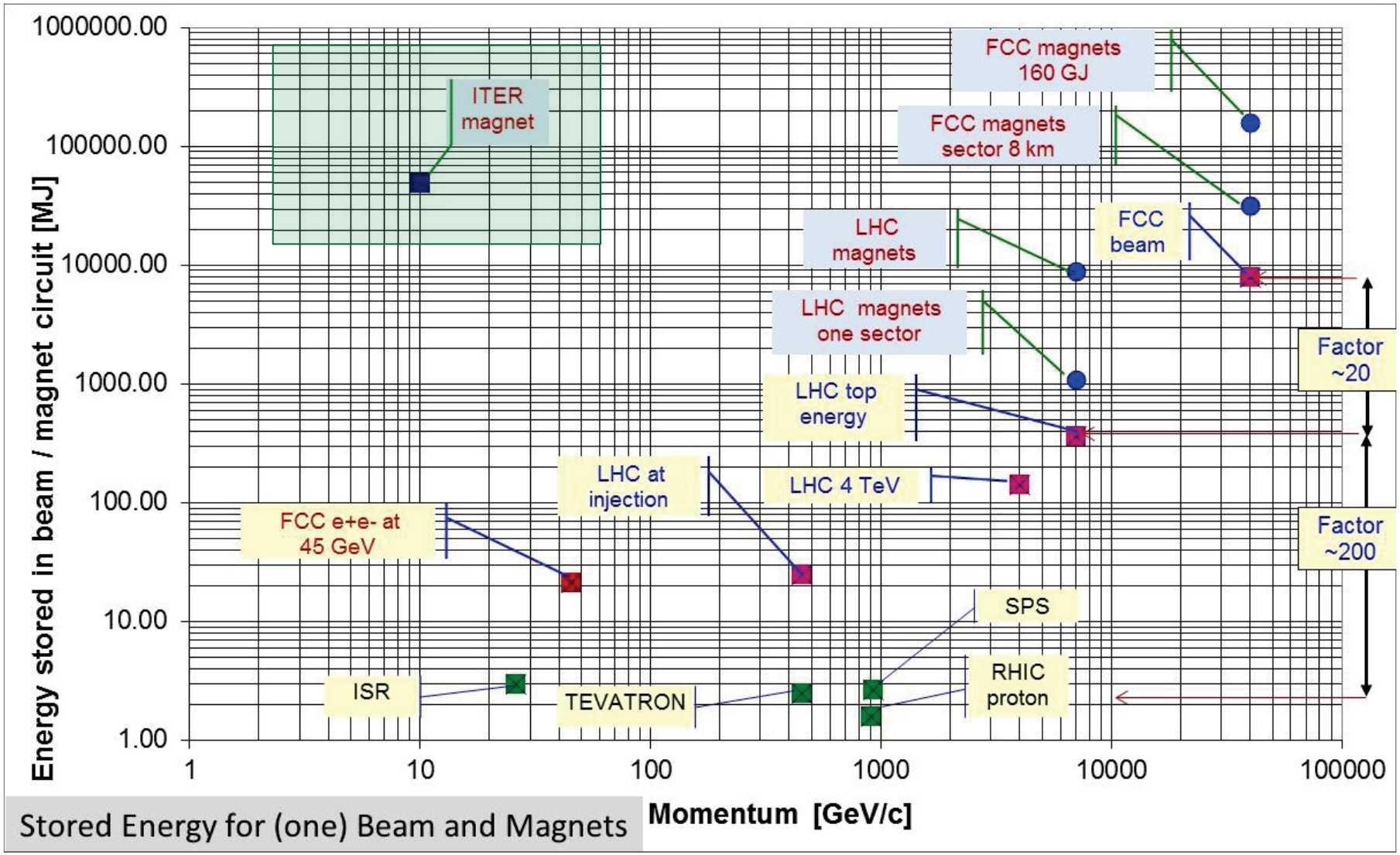
- Risks come from **Energy** stored **in a system** (Joule), and **Power** when **operating** a **system** (Watt)
  - "Very powerful accelerator" … the power flow needs to be controlled
- Particle accelerators and fusion reactors use **large amount of power** (few to many MW)
  - Where does the power go in case of failure?
- An **uncontrolled release** of energy or power flow can lead to **unwanted consequences**
  - Damage of equipment and loss of time for operation
  - Risk of activation of equipment when operating with particle beams

This is a particular **challenge** for complex systems such as **accelerators** and **fusion reactors**

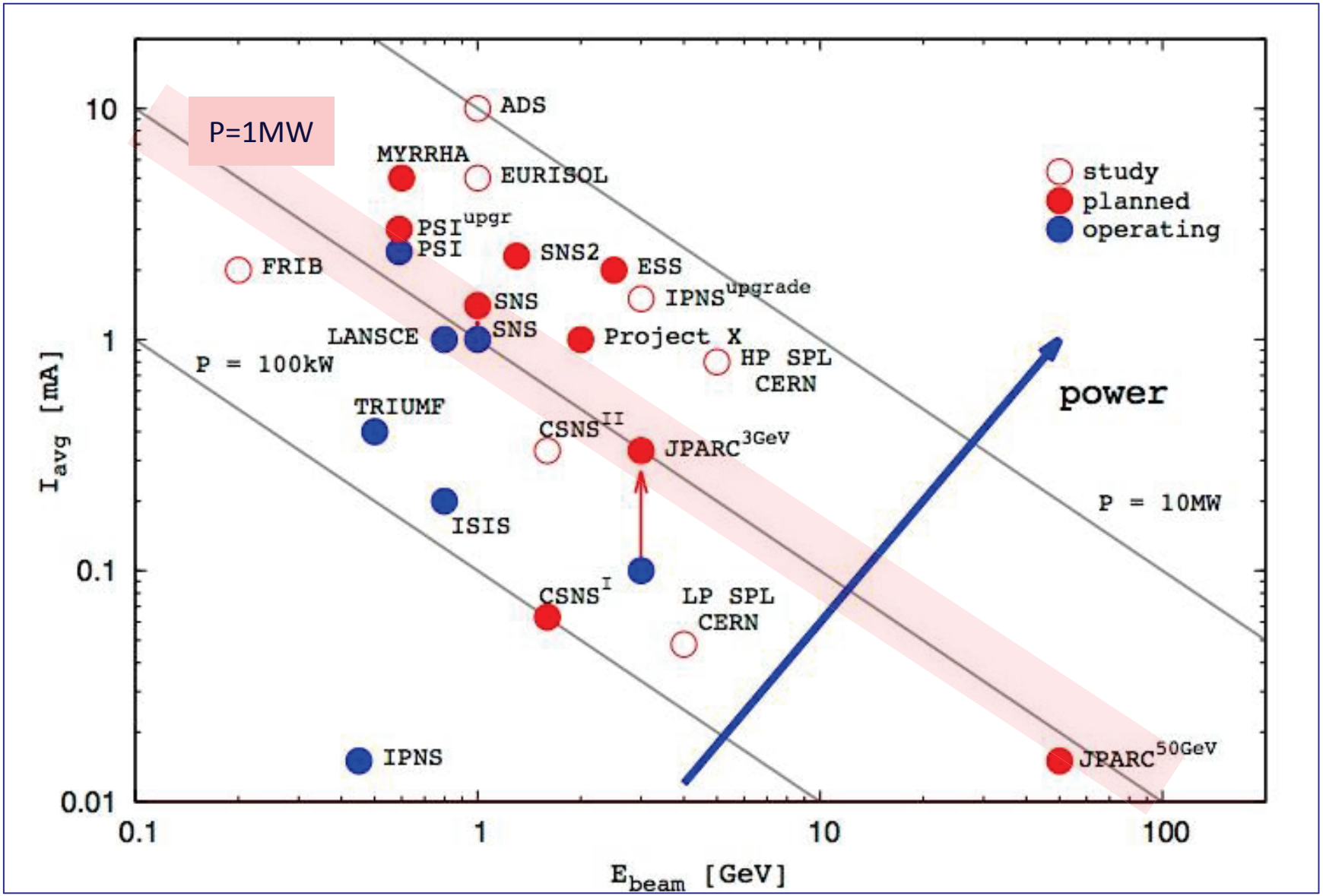
# Accelerators and Large Experimental Physics Systems

- **Synchrotrons and colliders** – energy stored in the beam and in the (superconducting) magnet system
  - Circular hadron synchrotrons and colliders: LHC, RHIC, SPS, FCC (100 km, 100 TeV cm energy), …
  - Stored energy: from MJ …. more than 100 GJ
- **High intensity proton accelerators**: PSI, SNS, JPARC, ESS (next 5 years), ADS (next decade)
- **Electron accelerators**: synchrotron light sources, free electron lasers, circular and linear e+e- colliders
  - High power, very small beam size, …..
  - Synchrotron light can also damage components….
- **Fusion reactors**
- **High power lasers** – 1 to 2 MJ per pulse (low rep rate) but with increasing average power in the future (e.g. ELI)

# Energy for accelerators and magnet systems



# High Intensity Proton Accelerators



# What does it mean …… Joule, kJ and MJ?

# What does it mean …… Joule, kJ and MJ?

The energy of pistol bullet:
about 500 J

# What does it mean …… Joule, kJ and MJ?

The energy of pistol bullet:
about 500 J

The energy of 1 kg TNT:
about 4 MJ

# What does it mean …… Joule, kJ and MJ?

The energy of pistol bullet:
about 500 J

The energy of 1 kg TNT:
about 4 MJ

To melt 1 kg of steel (copper is similar): about 800 KJ

# What does it mean …… Joule, kJ and MJ?

The energy of pistol bullet:
about 500 J

The energy of 1 kg TNT:
about 4 MJ

To melt 1 kg of steel (copper is similar): about 800 KJ

The energy stored in the ITER toroid magnet can melt 60 tons of copper

# Hazards and Risks

# Hazard and Risk

- **Hazard:** a situation that poses a level of threat to the machine. Hazards are dormant or potential, with only a theoretical risk of damage. Once a hazard becomes "active“: **incident / accident**.
- **Consequences** and **Probability** of an accident create **RISK**:

**RISK = Probability · Consequences**

Related to complex research instruments

- **Consequences** of a failure in a hardware systems or uncontrolled beam loss (in $$$, downtime, radiation dose to people, reputation)
- **Probability** of such event
- The higher the **RISK**, the more **Protection** is required

# Hazards related to magnet systems

- Accelerators and fusion reactors operate with **high field superconducting magnets**
- The **energy stored in the magnets increased** over the years (at TEVATRON, HERA, LHC, ITER, FCC, ….)
- **Superconducting magnets may quench** – and without a protection system superconducting magnets would in general be damaged
- There are **many mechanisms** that **can trigger a quench**, and a very small amount of energy is required to trigger a quench (few mJ)
  - Example: the loss of a fraction of $10^{-8}$ of the protons in one magnet in the LHC beams can lead to a quench, e.g. the interaction of a dust particle (UFO) with the circulating beam

# Hazards related to particle beams

- **Regular beam losses** during operation
  - To be considered since leads to activation of equipment and possibly quenches of superconducting magnets
  - Radiation induced effects in electronics (Single Event Effects)

- **Accidental beam losses** due to failures: understand hazards, e.g. mechanisms for accidental beam losses (**probability**)
  - Hazards become accidents due to a failure, machine protection systems prevent the failure or mitigate the consequences

- Understand **energy deposition** by particles and mechanisms for damage of components (**consequences**)

# Release of 600 MJ magnetic energy at LHC

**The 2008 LHC accident happened during test runs without beam.**

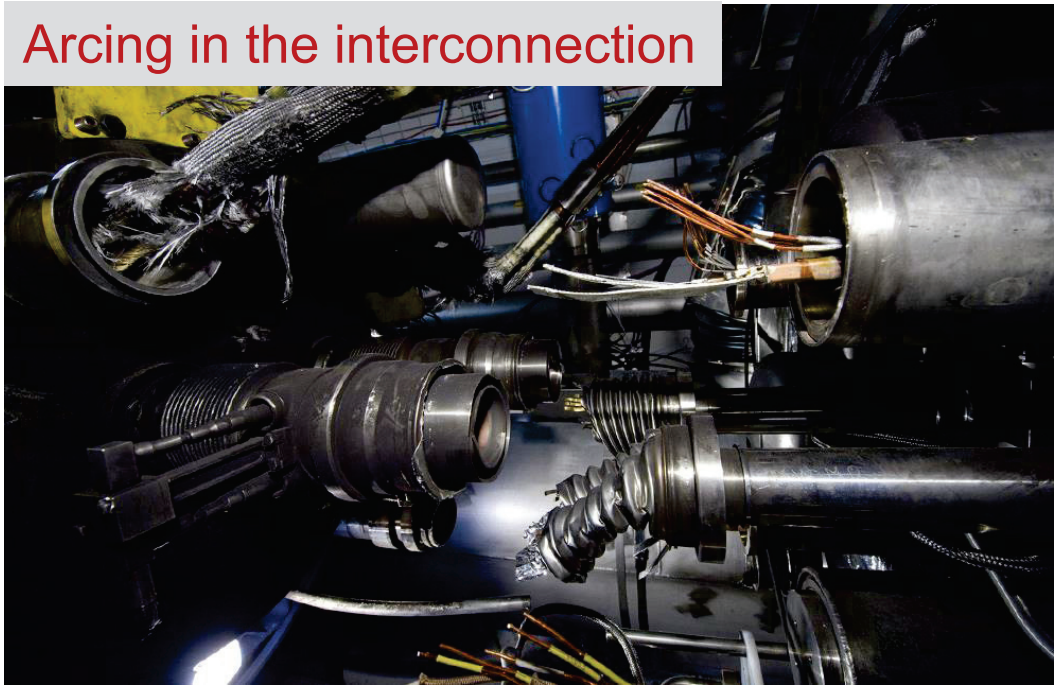
A magnet interconnect was defect and the circuit opened. An electrical arc provoked a He pressure wave damaging ~600 m of LHC, polluting the beam vacuum over more than 2 km.

# Release of 600 MJ magnetic energy at LHC

**The 2008 LHC accident happened during test runs without beam.**

A magnet interconnect was defect and the circuit opened. An electrical arc provoked a He pressure wave damaging ~600 m of LHC, polluting the beam vacuum over more than 2 km.

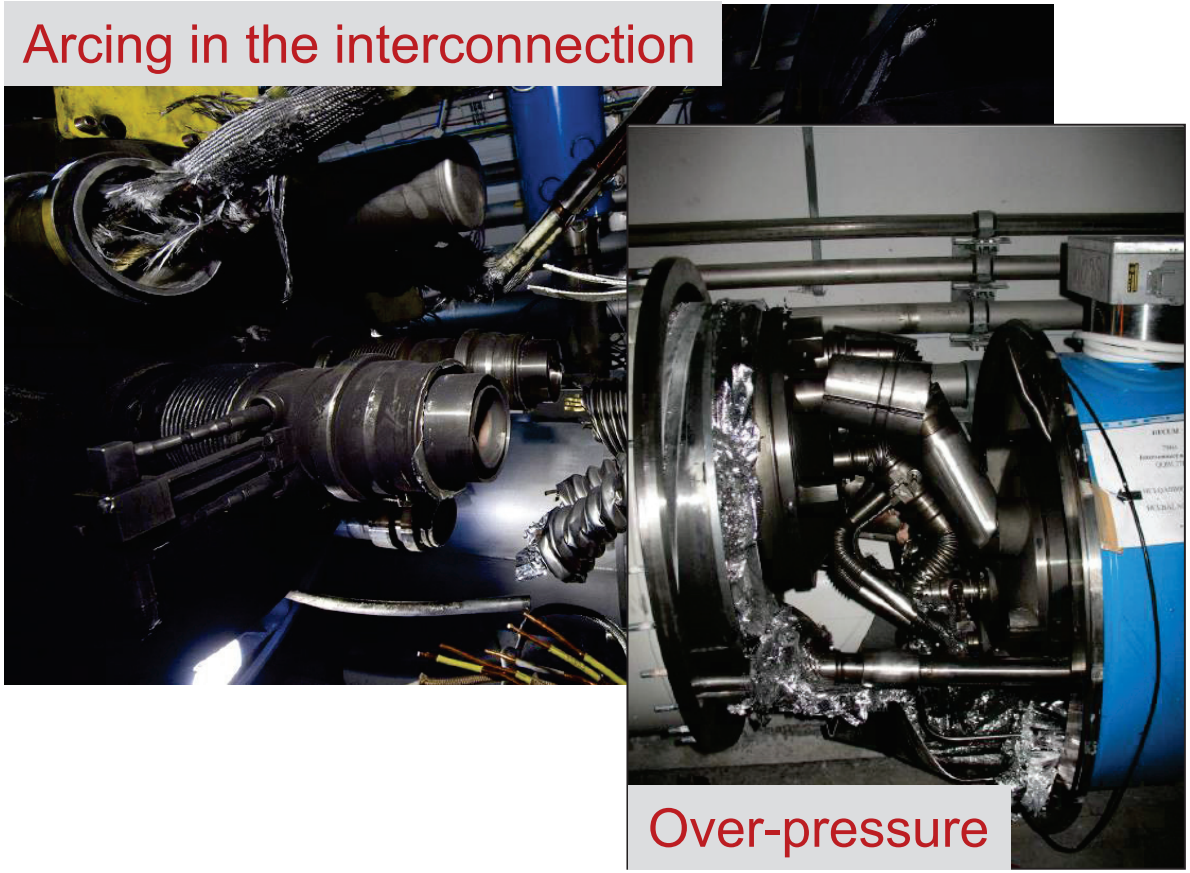
Arcing in the interconnection



# Release of 600 MJ magnetic energy at LHC

**The 2008 LHC accident happened during test runs without beam.**

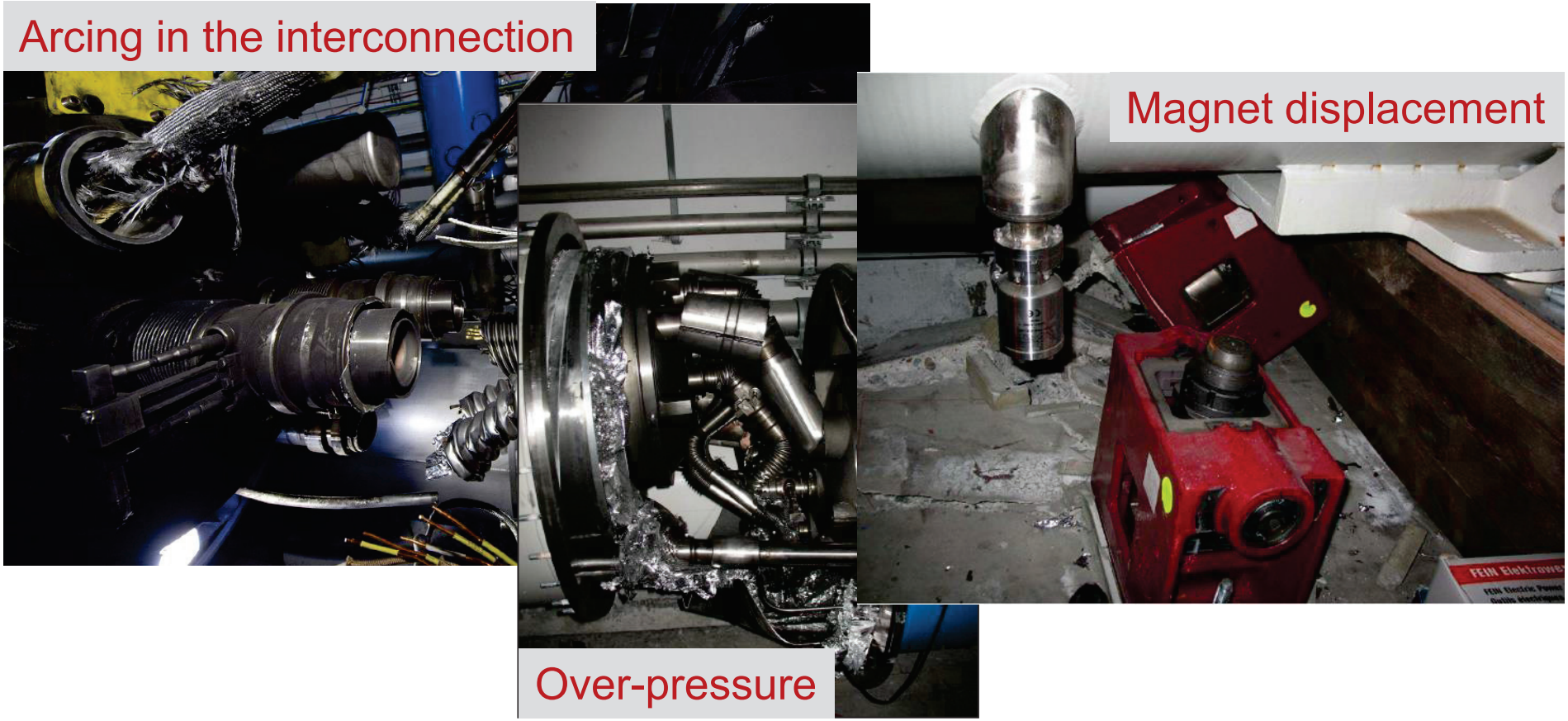
A magnet interconnect was defect and the circuit opened. An electrical arc provoked a He pressure wave damaging ~600 m of LHC, polluting the beam vacuum over more than 2 km.



# Release of 600 MJ magnetic energy at LHC

**The 2008 LHC accident happened during test runs without beam.**

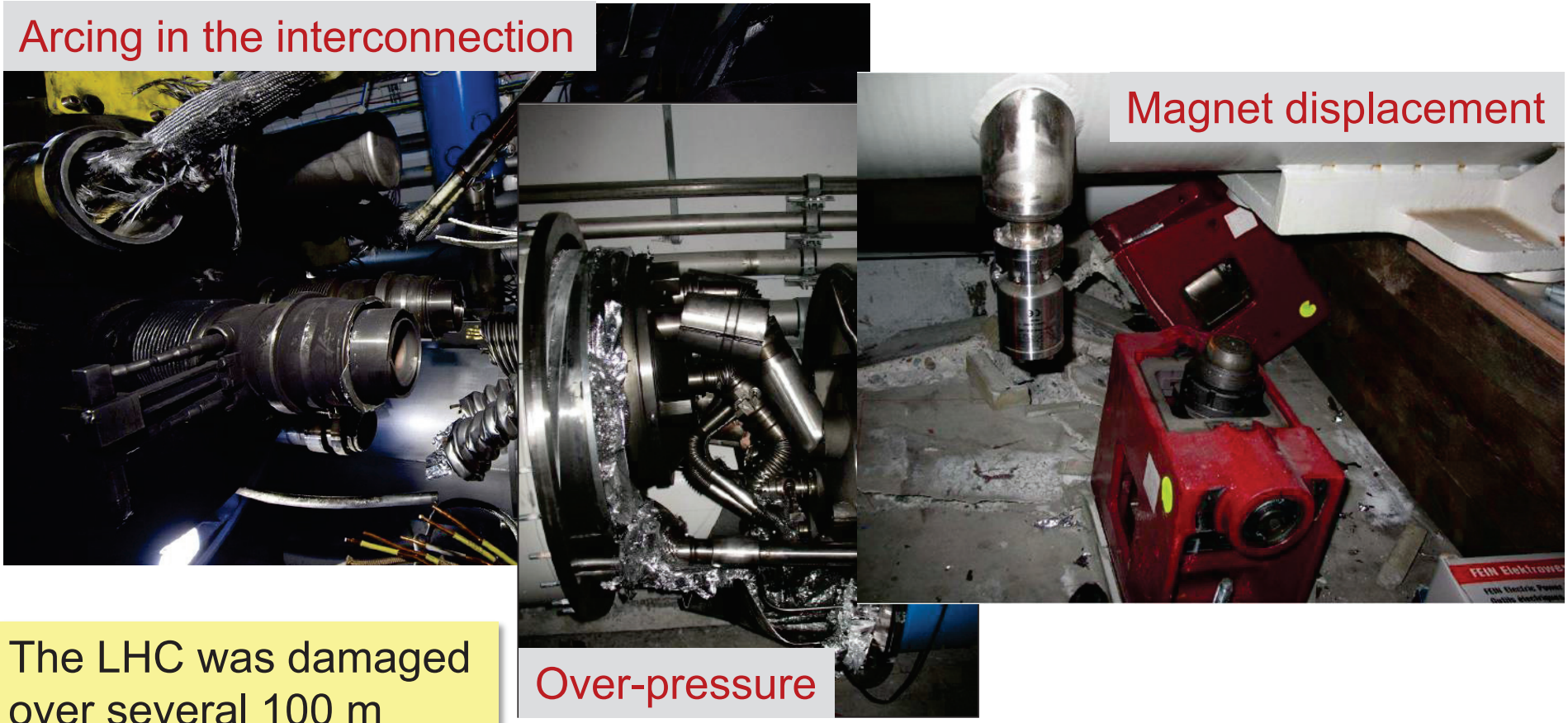
A magnet interconnect was defect and the circuit opened. An electrical arc provoked a He pressure wave damaging ~600 m of LHC, polluting the beam vacuum over more than 2 km.



# Release of 600 MJ magnetic energy at LHC

**The 2008 LHC accident happened during test runs without beam.**

A magnet interconnect was defect and the circuit opened. An electrical arc provoked a He pressure wave damaging ~600 m of LHC, polluting the beam vacuum over more than 2 km.

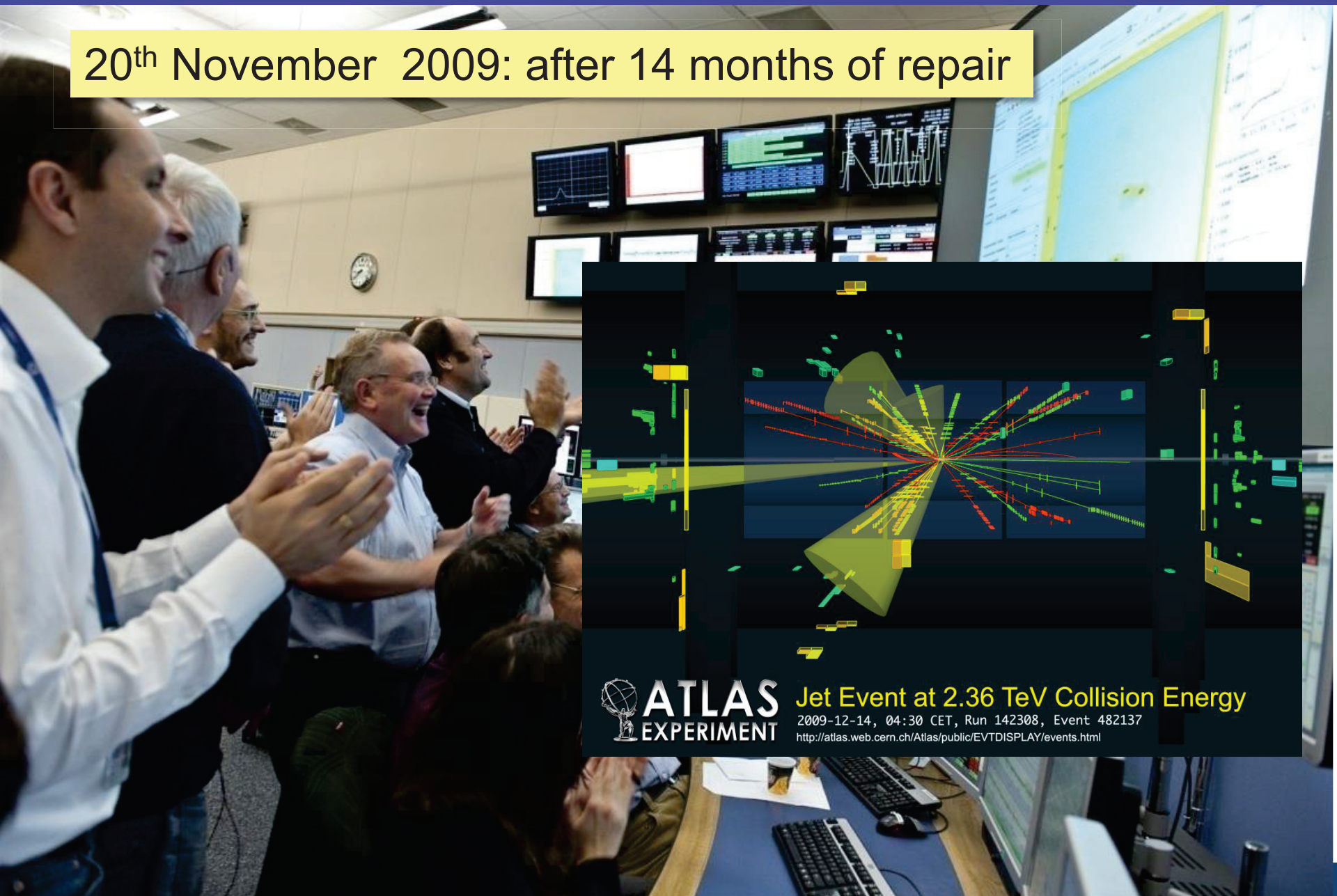



The LHC was damaged over several 100 m

# LHC is back !

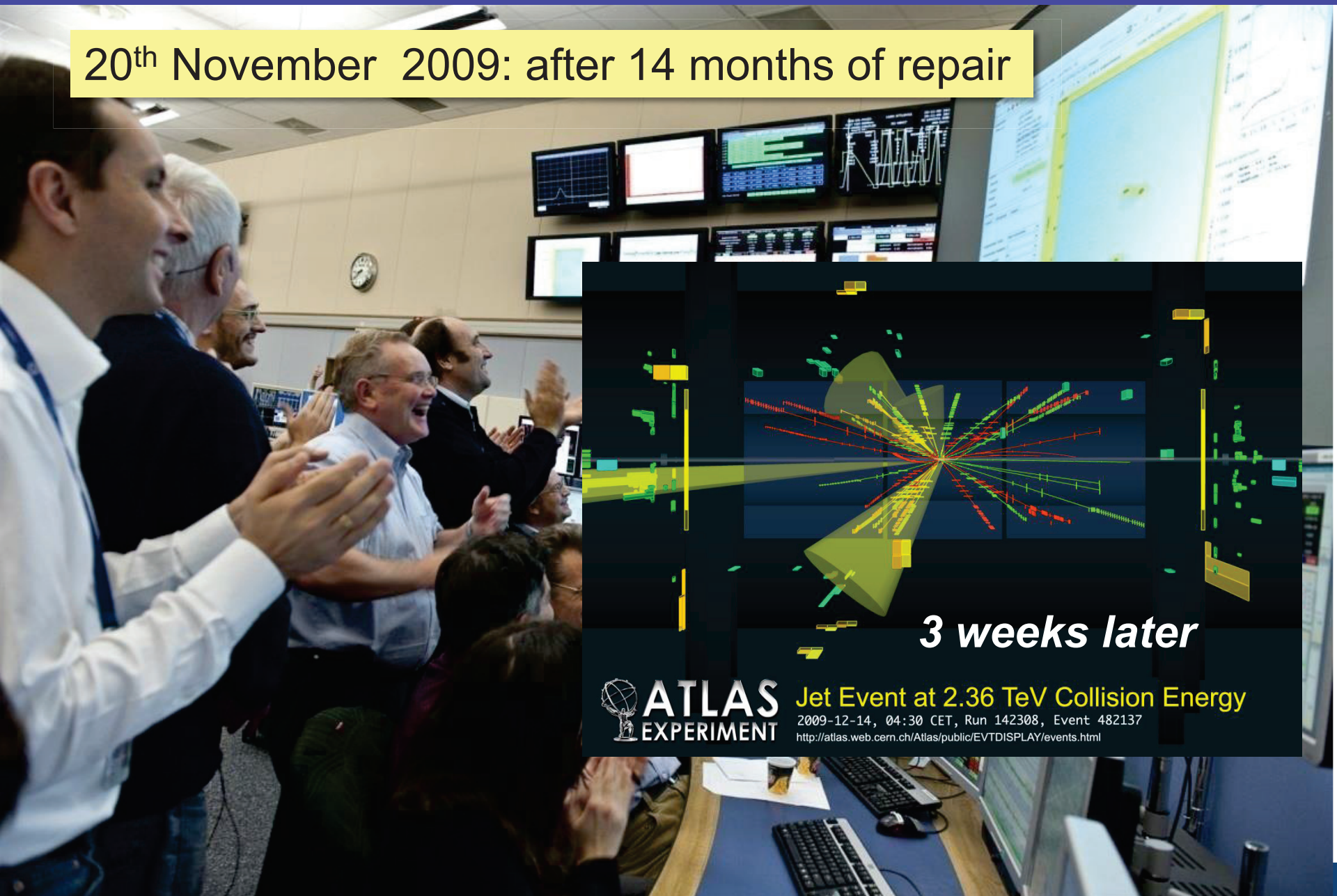
# LHC is back !

20th November 2009: after 14 months of repair



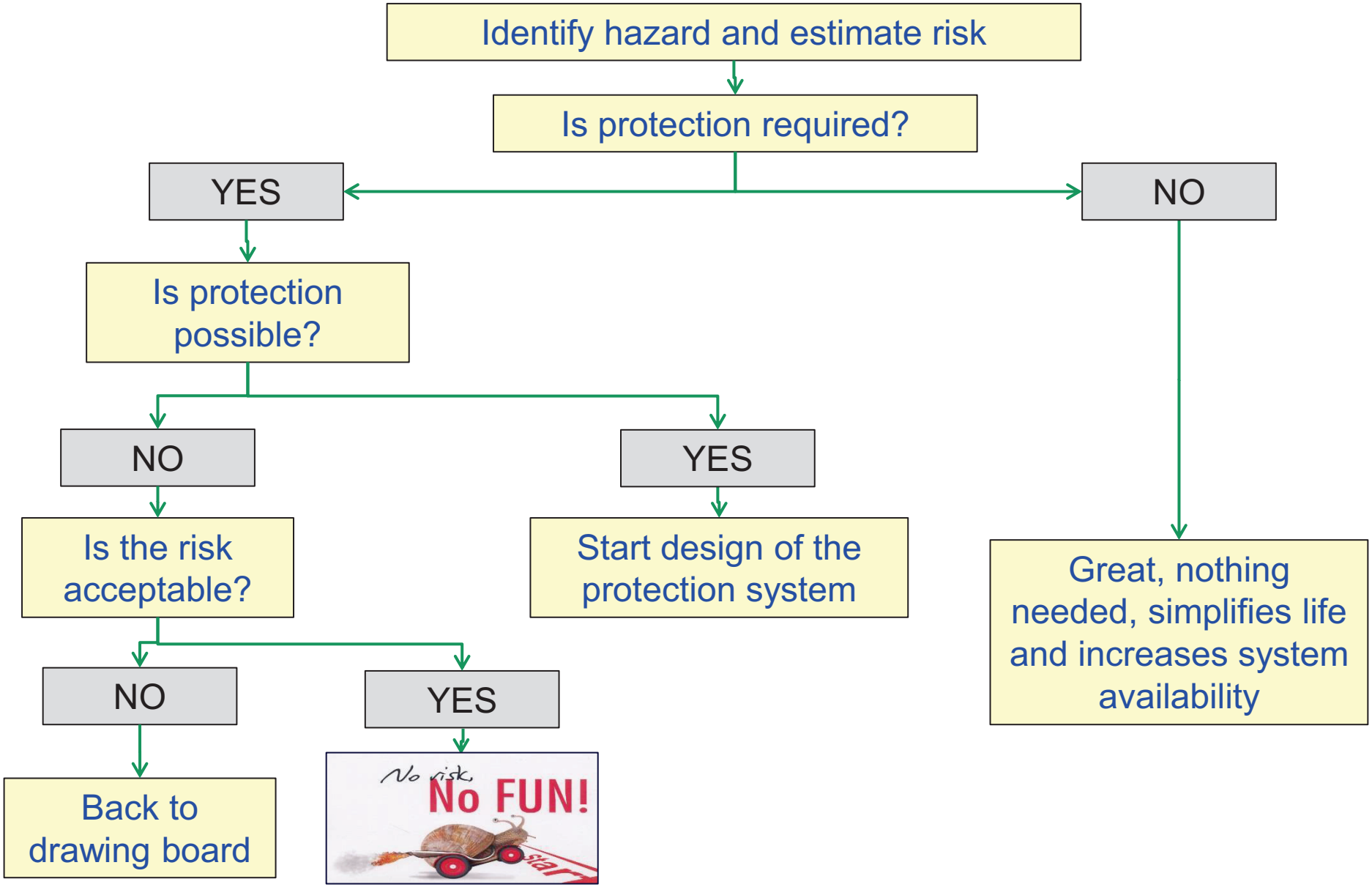
# LHC is back !

20th November 2009: after 14 months of repair



# Machine Protection

# Analysing need for machine protection



# Analysing need for machine protection

Identify hazard and estimate risk

Is protection required?

YES

NO

Is protection possible?

NO

YES

Great, nothing needed, simplifies life and increases system availability

- Magnets: if the magnet has large stored energy, and a too low ratio between copper and superconductor => magnet cannot be protected => magnet design not acceptable
- Beam: transverse deflecting devices in an accelerator that can deflect the beam by a large angle within about one turn

# Three Principles for Machine Protection

1. **Protect the equipment** (machine protection systems + interlock systems)

2. **Protect the process** (high availability systems)
   - Machine protection systems will always contribute to downtime
   - Protection action ONLY if a hazard becomes active (e.g. something went wrong threatening to damage equipment)

3. **Provide the evidence** (post mortem, logging of data)
   - Provide post mortem buffers in equipment (record data, and stop after protection action kicks in) – 70% of LHC luminosity fills dumped prematurely
   - Synchronisation of different systems is ultra – critical, to understand what happened
   - Post operational checks by the controls system

# Three Principles for Machine Protection

1. **Protect the equipment** (machine protection systems + interlock systems)

2. **Protect the process** (high availability systems)
   - Machine protection systems will always contribute to downtime
   - Protection action ONLY if a hazard becomes active (e.g. something went wrong threatening to damage equipment)

3. **Provide the evidence** (post mortem, logging of data)
   - Provide post mortem buffers in equipment (record data, and stop a protection action kicks in) – 70% of LHC luminosity fills dumped prematurely
   - Synchronisation of different systems is ultra – critical, to understand what happened
   - Post operational checks by the controls system

Forensic logger

# Active and Passive Protection

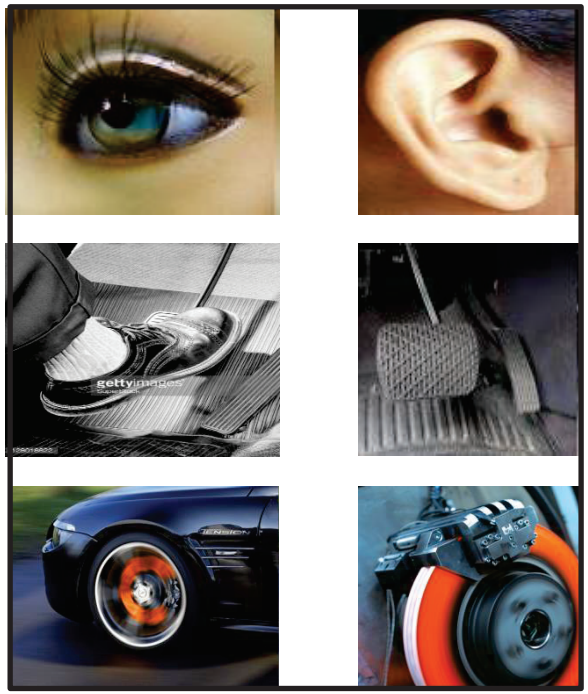
**Active protection**

- A sensor detects a dangerous situation
- An action is triggered by an actuator
- The energy stored in the system is safely dissipated

# Active and Passive Protection

**Active protection**

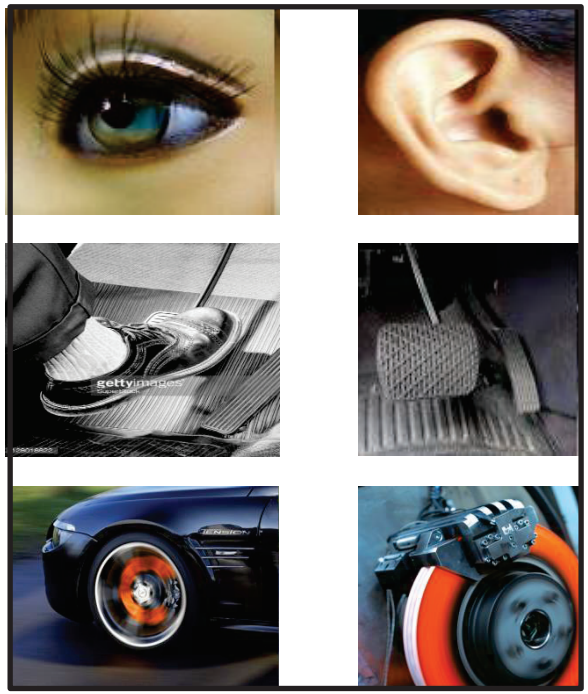
- A sensor detects a dangerous situation
- An action is triggered by an actuator
- The energy stored in the system is safely dissipated



# Active and Passive Protection

## Active protection

- A sensor detects a dangerous situation
- An action is triggered by an actuator
- The energy stored in the system is safely dissipated



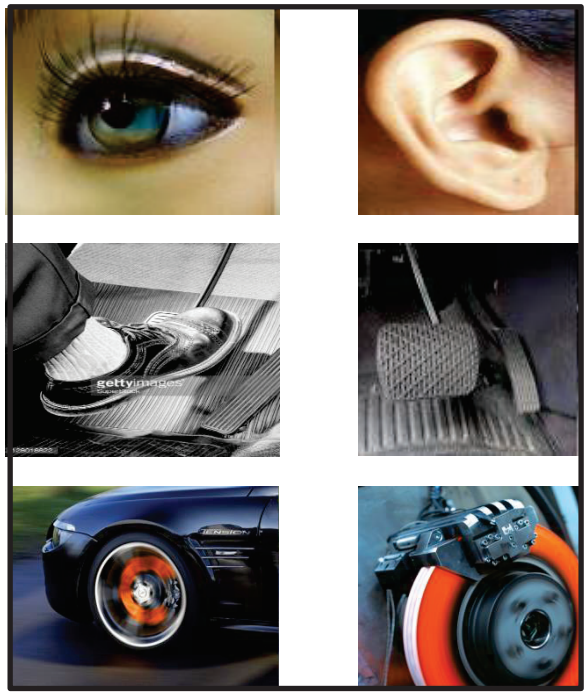
## Passive protection

- Preferred if possible to operate without active protection
- Active protection not possible, e.g. the reaction time is too short
- Monitors fail to detect a dangerous situation (redundancy)

# Active and Passive Protection

## Active protection

- A sensor detects a dangerous situation
- An action is triggered by an actuator
- The energy stored in the system is safely dissipated



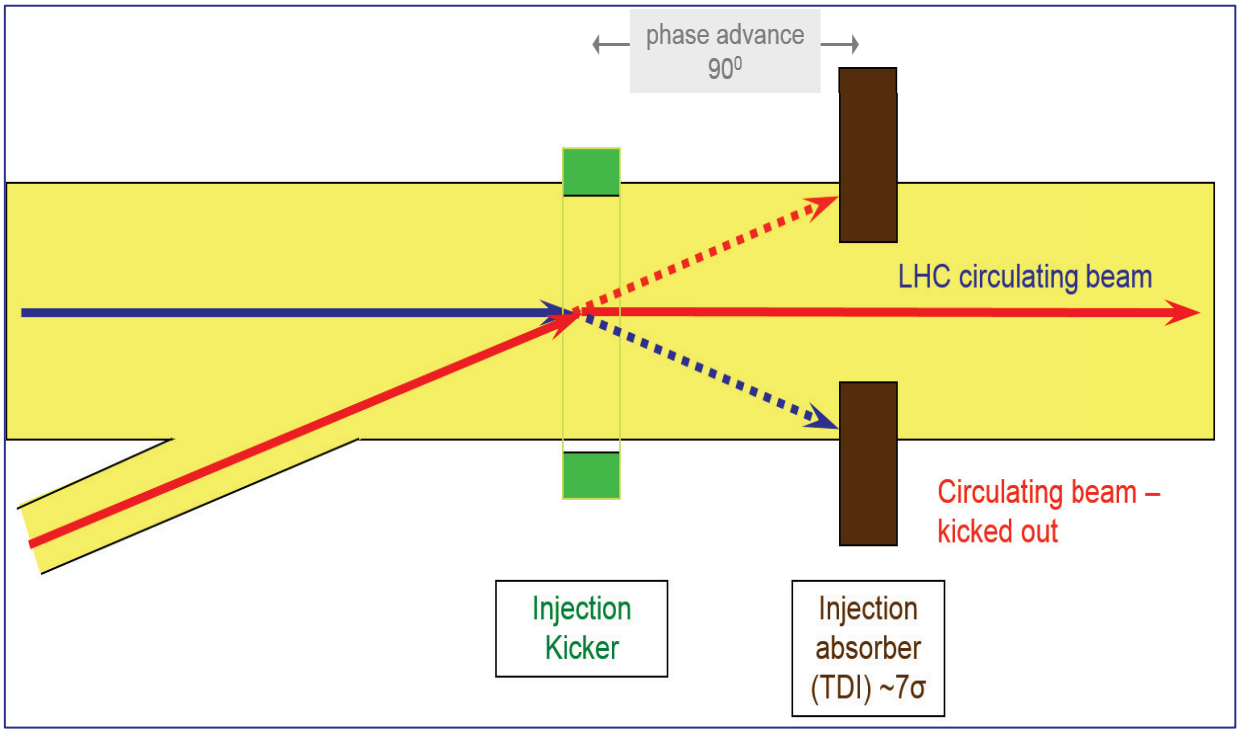
## Passive protection

- Preferred if possible to operate without active protection
- Active protection not possible, e.g. the reaction time is too short
- Monitors fail to detect a dangerous situation (redundancy)

## Passive protection

- Is always necessary when the time required for the response is too short (…remember the limitation of the speed of light)
- One example is the fast injection of a high intensity beam into a synchrotron with a fast kicker magnet

- If beam can damage hardware, **protection absorbers** are required
- For movable absorbers: need to be made sure that they are at the correct position during injection



# LHC strategy for machine protection

- Definition of aperture by collimators.

**Beam Cleaning System**

- Passive protection by beam absorbers and collimators for specific failure cases.

**Collimator and Beam Absorbers**

- Early detection of equipment failures generates dump request, possibly before beam is affected.

**Powering Interlocks**

**Fast Magnet Current change Monitor**

- Active monitoring of the beams detects abnormal beam conditions and generates beam dump requests down to a single machine turn.

**Beam Loss Monitors**

Other Beam Monitors

- Reliable operation of beam dumping system for dump requests or internal faults, safely extracting beams onto the external dump blocks.

**Beam Dumping System**

- Reliable transmission of beam dump requests to beam dumping system. Active signal required for operation, absence of signal is considered as beam dump request and injection inhibit.

**Beam Interlock System**

# Interlock Systems

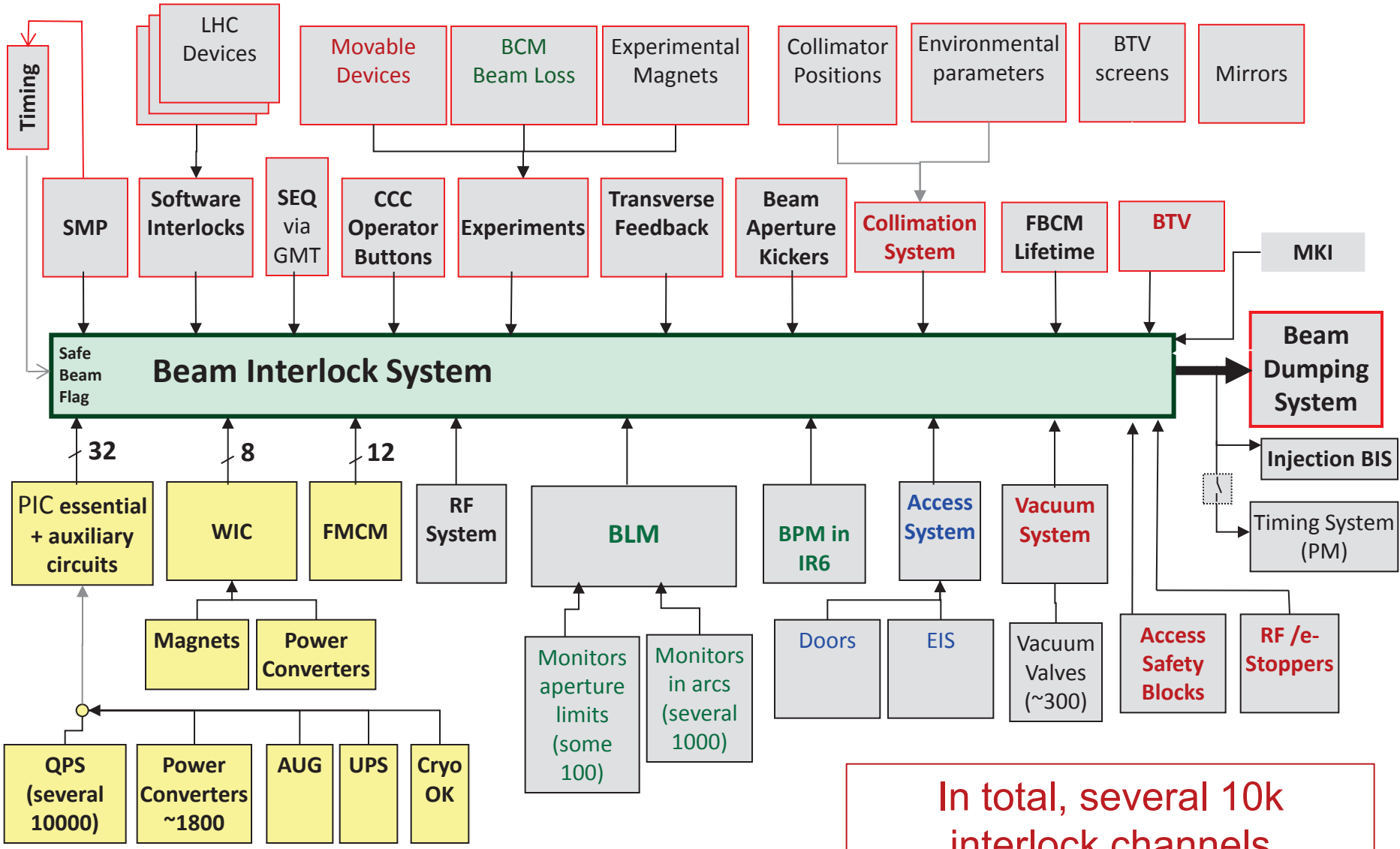
# Machine Interlock Systems at LHC

- **Beam Interlock System** (Fast FPGA based system, µs reaction time)
  - Ensures that the beams are extracted into the beam dump blocks when one of the connected systems detects a failure
- **Powering Interlock System** (PLC based system, much slower, ms reaction time)
  - Ensures communication between systems involved in the powering of the LHC superconducting magnets (magnet protection system, power converters, cryogenics, UPS, controls)
- **Software Interlock System** (SIS, order of one second)
  - Ensures redundant protection for many hazards, and early detection of failures
  - Ensures that the LHC operational parameters remain within well defined boundaries (e.g. closed orbit deviation within specs)

For LHC, **machine interlocks are strictly separated from** interlock for **personnel safety**

Poster B.Puccio MOPGF136

# LHC Interlock Systems and inputs




In total, several 10k interlock channels

# Reaction time for Interlock systems

- **Fast** interlock systems
  - Reaction time can be down to some ns (typically µs)
- **Slow** interlock systems
  - From seconds down to several milliseconds

- **Interlock systems** based on **hardware** (Electronics / Asics)
- Interlock systems including **intelligent controllers** (**FPGA** Field Programmable Gate Array)
  - Extremely fast, ns
- **PLCs** **P**rogrammable **L**ogic **C**ontrollers (standard and safety PLCs)
  - Milliseconds to hundred milliseconds (safety PLCs)
- **Software** interlock systems
  - In the order of one second

# Interlocks systems: other considerations

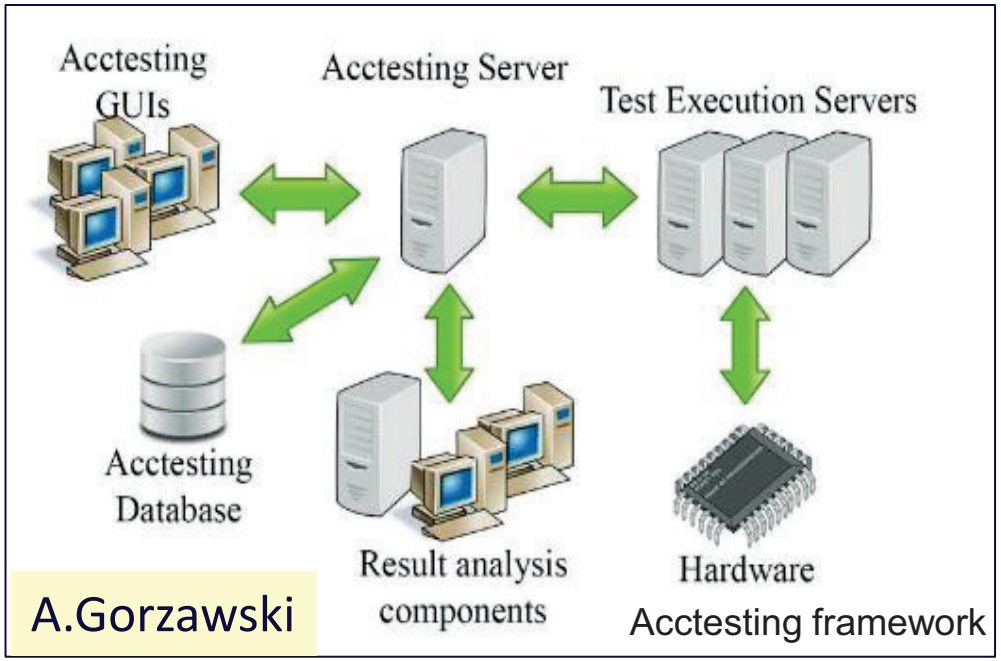
M. Kwiatkowski
B. Todd

- **P**rotection **I**ntegrity **L**evel (**PIL**)
  - Derived from **S**afety **I**ntegrity **L**evel (SIL) - IEC 61508
  - PIL1 to PIL4: PIL1…lowest risk, PIL4…highest risk
- **Radiation** environment (e.g. Single Event Effects)
- **Communication** layer
  - Current loops, frequency loops, use of intelligent network such as Profibus, Profisafe, Ethernet, …..
  - Electrical, optical, wireless in the future (?)
- **Time for development** (in-house design of electronics, buying and programming PLCs, ….)
- **Lab environment**
  - Lab standards
  - Competence in the lab and maintainability
- Cost

# Commissioning and Testing

- Design of the protection system: **testing to be considered**.
  - Correct commissioning and regular testing of protection system is vital to ensure reliable operation.
  - Repeated testing is very time consuming, can be extremely boring and prone to errors, in particular if done by humans.
  - Consider partial commissioning of accelerator (e.g. linacs)

- **Automatic test procedures** and automatic validation of the results via the controls system
- Framework for automatic testing used for LHC magnet system commissioning, about 10k tests performed.



# Machine Protection and Controls

# Other aspects

- **Several million parameters** for the protection systems
  - Many parameters can only be defined with operational experience
  - Management of critical parameters
  - Access to these parameters
  - Ensure that parameters in database are the same as in hardware
- (Cyber) security – **access to critical parameters**
  - Highest PIL: not possible to modify parameters via controls system
  - Medium PIL: parameter can be changed via the control system, but strict controls for parameter changes, e.g. two people role
  - Low PIL: parameter can be changed via the control system
- **Several 10k interlock channels** that can prevent operation
  - Nightmare for starting-up of a system, in particular, if the risk is (close to) zero
  - Option for bypassing of interlocks to be included in the design

# MP systems: design recommendations

- **Avoid** (unnecessary) **complexity** for protection systems
- **Failsafe** design
  - Detect internal faults
  - Possibility for remote testing, for example between two runs
- Critical equipment should be **redundant** (possibly diverse)
- Critical processes not by software and operating system
- No remote changes of most critical parameters
- **Calculate safety / availability / reliability**
  - Use methods to analyse critical systems and predict failure rate
- **Managing interlocks**
  - Bypassing of interlocks is common practice **(keep track!)**
  - LHC: bypassing of some interlocks possible for “setup beams”
- **Time stamping** for all system with adequate **synchronisation**

# Controls and Protection: not only Interlocks !

- **Logging and Post Mortem** recording of data + accurate and reliable time stamping
- Framework for **managing critical parameters**
- Framework to **relax interlock conditions** when risks are low (bypassing of interlocks)
- Framework for **automatic testing** of machine protection functionalities
- Framework to **respect operational boundaries** (sequencer, state machine, software interlocks, …)
- Feedback systems to **keep parameters within predefined limits** (e.g. closed orbit)
- Clear on-line **display of critical parameters** to operators (e.g. display of beam losses)

…….. **there is more**

# Summary

Machine protection and Interlocks for Accelerator and Large Experimental Physics Instruments……

- require **comprehensive understanding of all aspects of the instrument** (physics, operation, equipment, instrumentation, functional safety)
- require the **understanding** of **many different type of failures** that could lead to beam loss
- touch **many aspects** of **construction** and **operation**
- include **many systems**

**Controls plays an essential part in providing the environment for an efficient protection and operation**

# Acknowledgement


- Many colleagues at CERN, working on machine protection and interlocks
- Several colleagues from other labs – profiting from their experience and many discussions, in particular from DESY, BNL and ESS

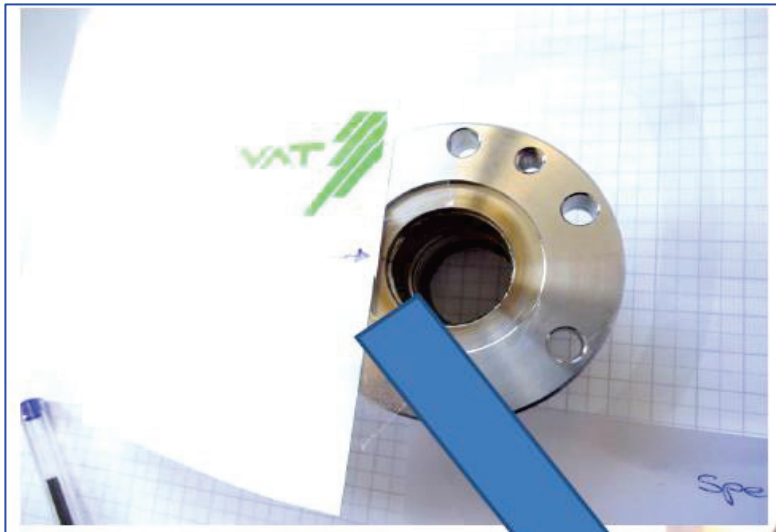
- A special thanks to Joerg Wenninger and Markus Zerlauth from CERN

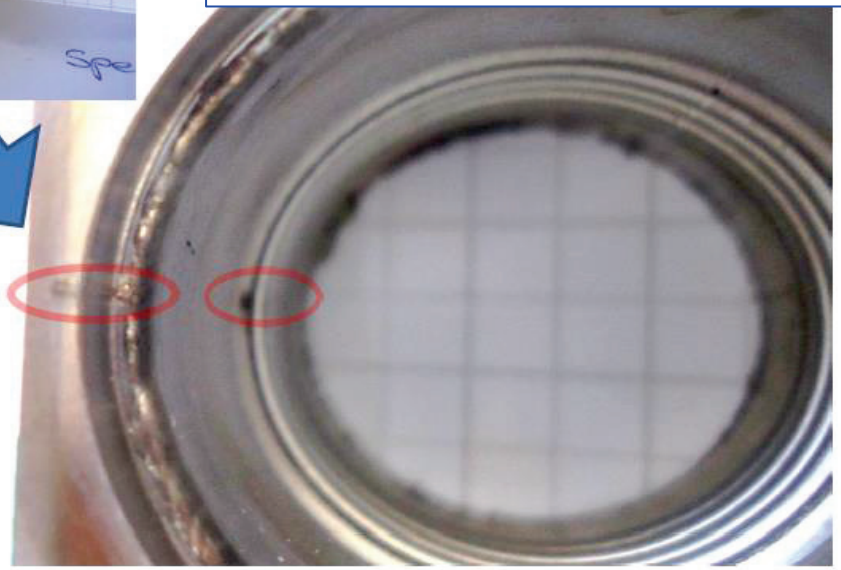
# Reserve

# CERN-LINAC 4 during commissioning at 3 MeV

December 2013 a vacuum leak on a below developed in the MEBT line.

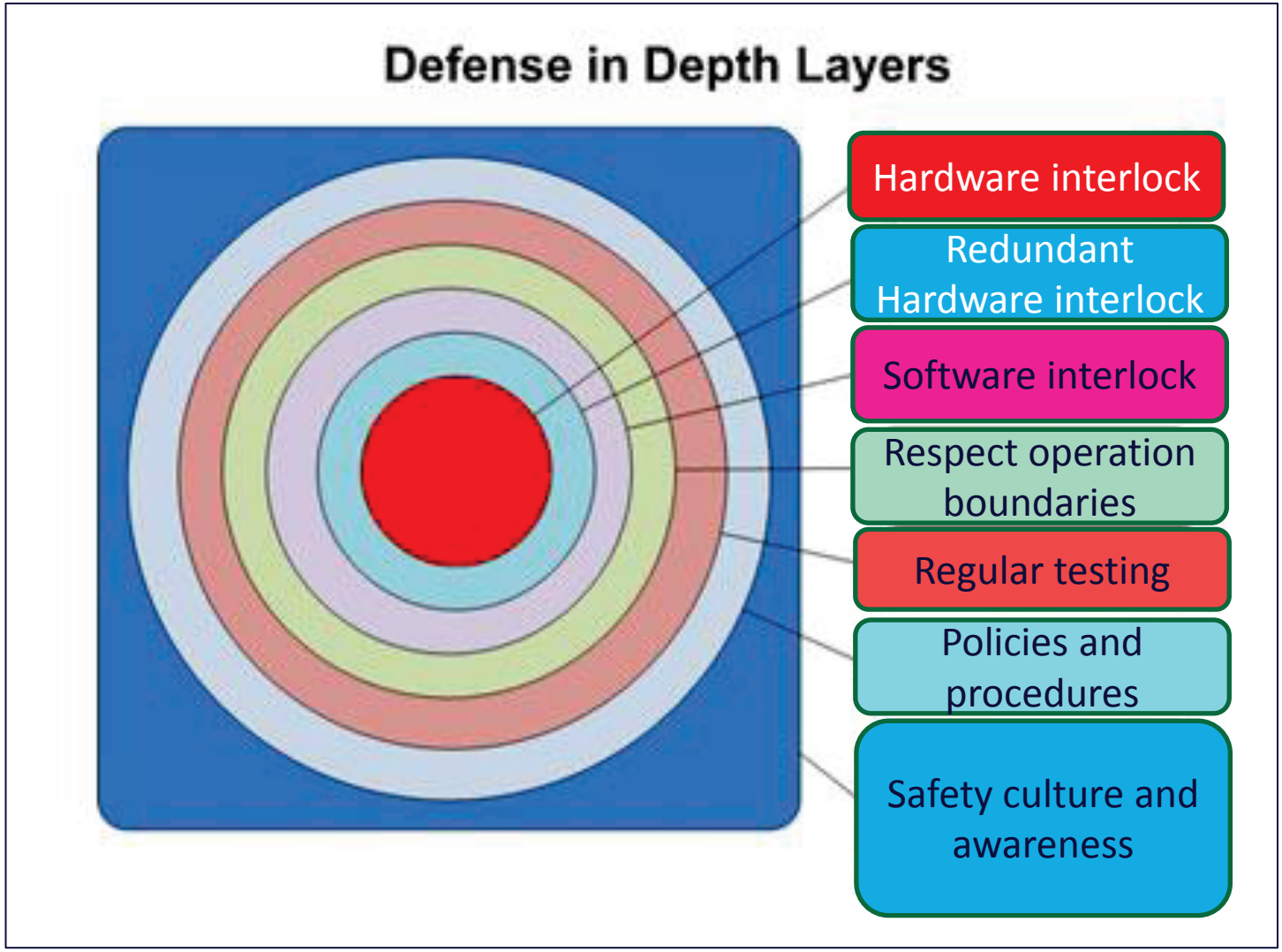
The analysis showed that the beam has been hitting the bellow during a special measurement (with very small beams in vertical but large in horizontal), ~16% of the beam were lost for about 14 minutes and damaged the bellow. The consequences were minor. Beam power – a few W.



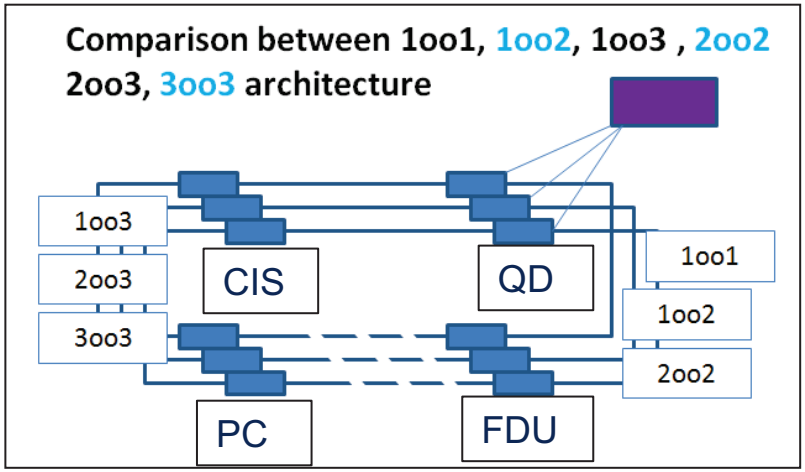
06/01/2014

A.Lombardi

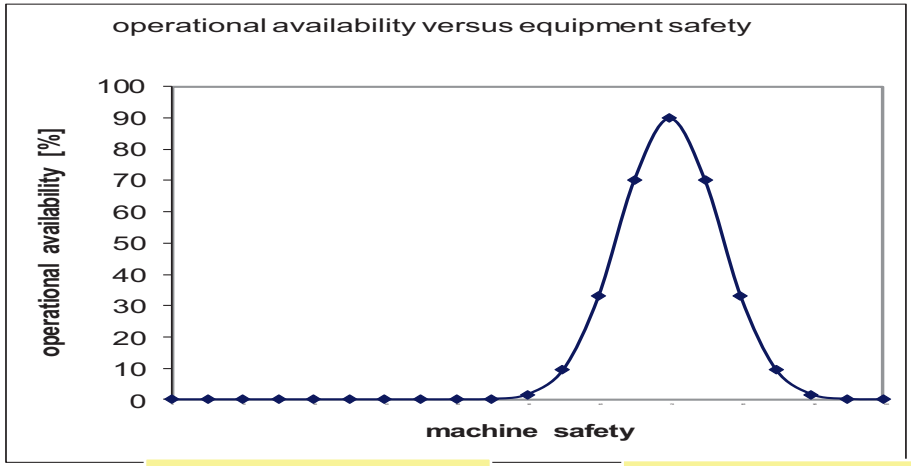

Defense in Depth Layers
Hardware interlock
Redundant Hardware interlock
Software interlock
Respect operation boundaries
Regular testing
Policies and procedures
Safety culture and awareness

# Machine Protection and Availability

- If the only objective is to maximising safety, this risks to reduce the overall availability – find a reasonable compromise
- For protection system: majority voting to be considered to increase failure tolerance
- Optimum has been found with 2oo3 voting systems
- Prototype powering interlock system developed for ITER




S. Wagner




Downtime for repairs due to insufficient protection systems

Downtime dominated by too complex Protection Systems

# Design guidelines for protection systems

- Having a vision to the operational phase of the system helps….
- Test benches for electronic systems should be part of the system development
  - Careful testing in conditions similar to real operation
- Reliable protection does not end with the development phase. Documentation for installation, maintenance and operation of the MPS
- The accurate execution of each protection function must be explicitly tested during commissioning
- Requirements are established for the test interval of each function
- Most failure are due to power supplies, mechanical parts and connectors

# The LHC machine need protection systems, but….

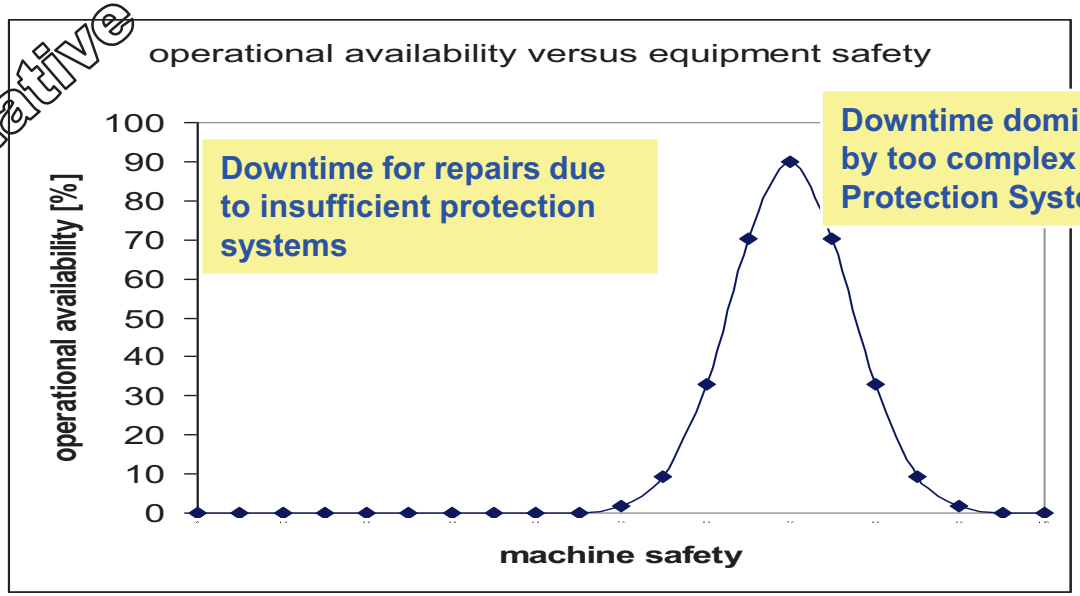
## Machine Protection is not an objective in itself, it is to

maximise operational availability by minimising down-time (quench, repairs)

avoid expensive repair of equipment and irreparable damage

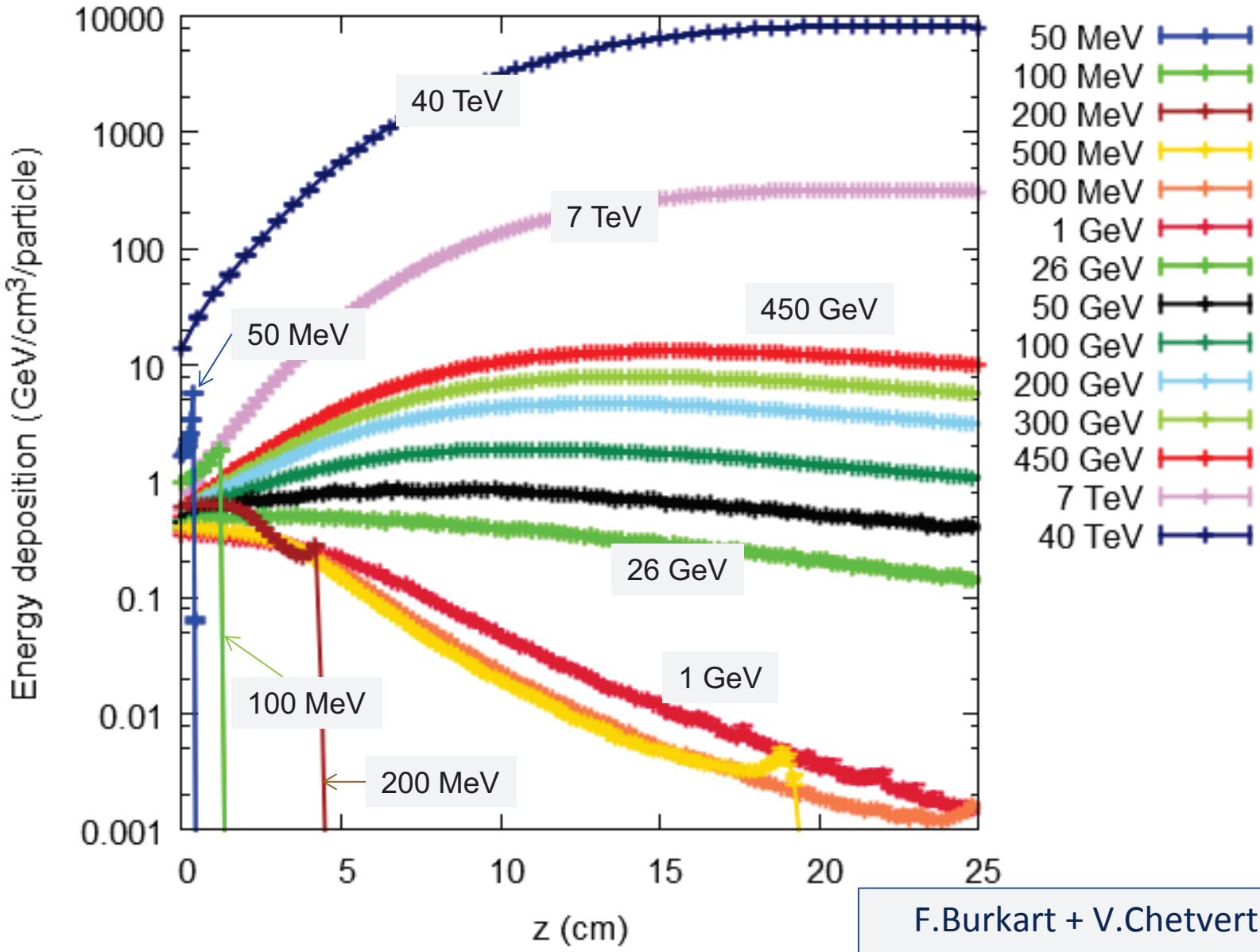
Operations workshop
R.Schmidt - Villars
30/01/2001

Qualitative




**Side effects from LHC Machine Protection System compromising operational efficiency must be minimised**

# Proton energy deposition for different energies




F.Burkart + V.Chetvertkova