

Machine Protection and Interlock System for the LHC

R.Schmidt, A.Vergara - Grenoble

5/02/2002

Accelerator Reliability Workshop

The LHC Challenges

LHC equipment

LHC protection systems

LHC and Reliability

Remarks to case studies

Conclusions

Energy at collision / beam	7	TeV
Energy at injection	450	GeV
Dipole field at 7 TeV	8.33	Tesla
Circumference	26658	m

Superconducting magnets at 1.9 K

Luminosity	10^{34}	$\text{cm}^{-2} \text{s}^{-1}$
Luminosity lifetime	10	h
Particles per bunch	$1.1 \cdot 10^{11}$	
DC beam current	0.56	A
Stored energy per beam	350	MJ

Very high beam power

Normalised emittance	3.75	μm
Beam size at IP / 7 TeV	15.9	μm
Beam size in arcs (rms)	300	μm

Beam power concentrated across tiny area

Two counter-rotating proton beams		
Magnet coil inner diameter	56	mm
Distance between beams	194	mm

Limited aperture for beam

**LHC
proton-proton
collider**

**7 TeV in LEP
Tunnel**

**Circumference
26.8 km**

**Injection
from SPS at
450 GeV**



Complexity of the LHC equipment: Main hardware systems

Magnet system

1232 superconducting main dipole magnets, about 400 superconducting main quadrupole magnets

5000 - 6000 superconducting corrector magnets

Cryogenic system

cool down 26 km long accelerator to a temperature of about 1.9 K
helium supply by a 26 km long cryo-line, separated from the magnets

Cold electrical engineering

2000 power diodes at cold inside cryo-magnets

6 sc bus bars for 13 kA for dipole, QF and QD electrical circuits

18 sc bus bars for 6 kA for matching quadrupoles

about 60 sc bus bars for 600 A for corrector magnets

about 60000 joints between superconductors

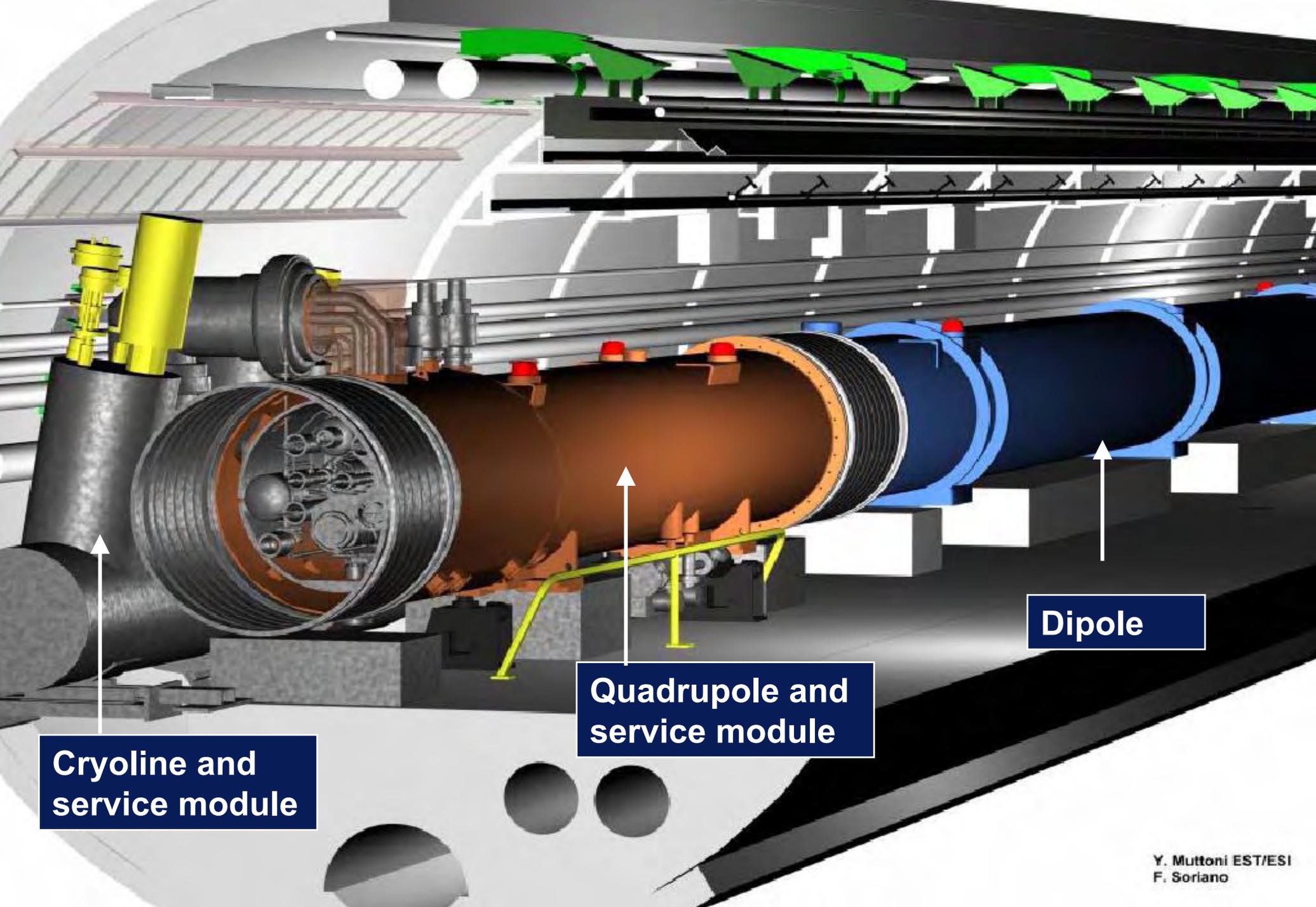
HTS current leads for 900 electrical circuits (600A 13 kA)

Vacuum system

insulation vacuum for external cryogenic distribution line

insulation vacuum for machine cryostat

vacuum for both beam tubes



**Cryoline and
service module**

**Quadrupole and
service module**

Dipole

Interconnect between two superconducting magnets



The reliability of my systems is entirely sufficient, we do as best as we can !

includes 68 superconducting cables, 600 A - 13 kA

Quality of equipment to be installed

Reliability relies on quality - Quality assurance for the LHC equipment is well advanced, and widely used for the LHC

A team is in charge of defining the policy for Quality Assurance, summarised by the quality assurance categories and defined in the QAP in the LHC hardware baseline.

This includes:

- Naming conventions
- Approval of Engineering Specifications by everyone concerned
- Engineering Change Requests for approval, in case of modifications
- Coherent description of equipment in a database
- Engineering and Design standards, Document standards, Procedures, ...

Reliability of equipment:

- Responsibility of the Engineer in charge of this equipment
- MTBF to be defined in the Technical Specification of that equipment as input for design

Reliability of the entire system starts to be considered, together with first operation scenarios

Systems directly linked with operation and protection

Powering system

Power converters for magnets in about 1700 electrical circuits

Beam systems

Injection

RF system

Beam instrumentation

Protection systems

Protection of superconducting elements (magnets, bus bars and HTS current leads) - ensure protection of the sc elements in case of quench, with approximately 5000 channels

Beam dump system

Beam loss monitor system (more than 1000 beam loss monitors)

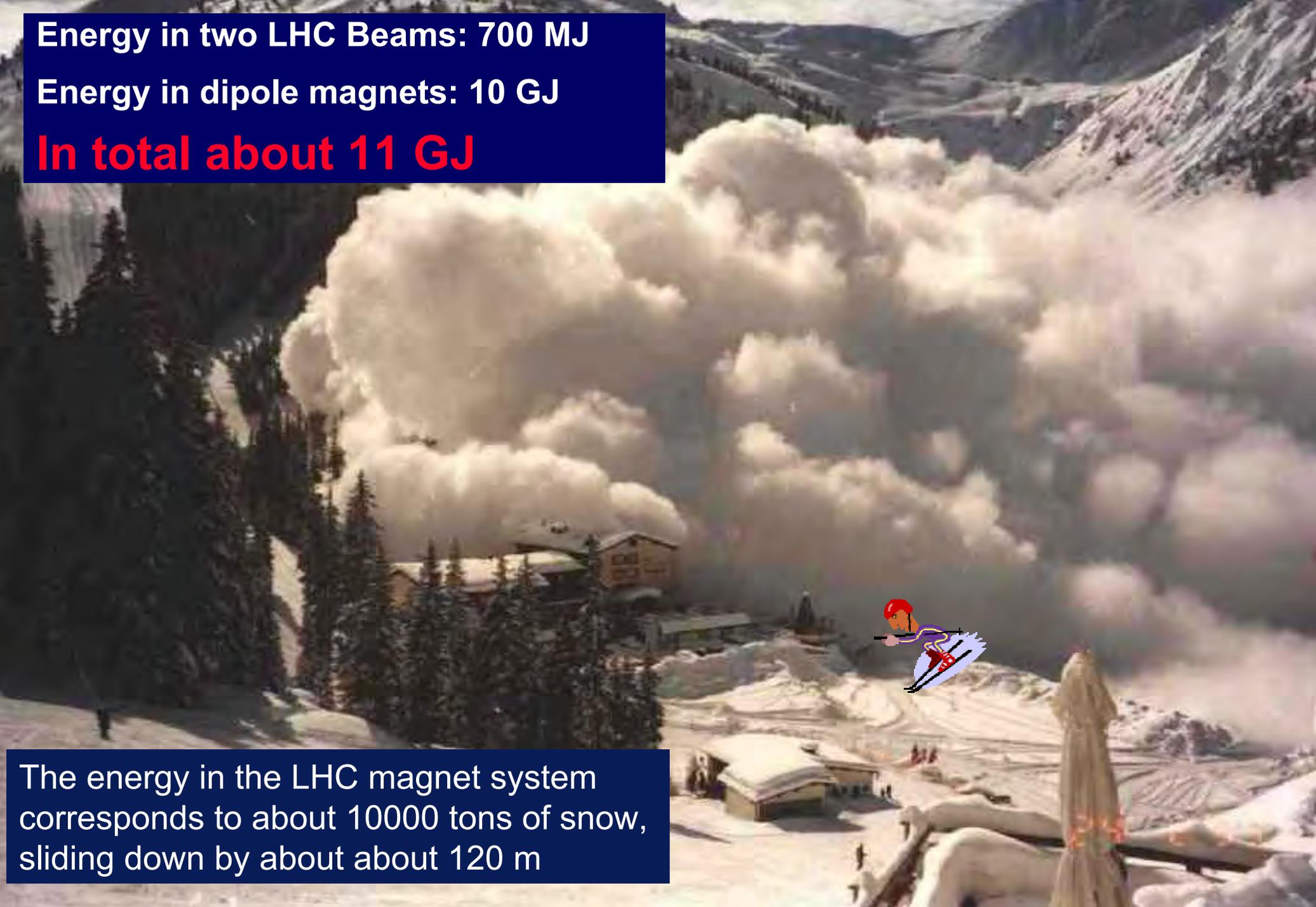
Beam cleaning system: Collimators / Beam absorbers

Energy in two LHC Beams: 700 MJ

Energy in dipole magnets: 10 GJ

In total about 11 GJ

The energy in the LHC magnet system corresponds to about 10000 tons of snow, sliding down by about about 120 m



Energy to quench a superconducting dipole magnet is very small

**LHC magnets operate at 1.9 K - little enthalpy - temperature margin about 1.4 K
- 0.6 J/cm³**

Nominal beam intensity : $3 \cdot 10^{14}$ protons / beam

Energy at 7 TeV to quench a dipole magnet is 0.6 J/cm³ - this energy density would be generated by about 10^7 protons

- less than 10^{-7} of the beam would quench a dipole magnet => efficient beam cleaning system required - for a lifetime of 1h about 10^{11} protons would leave the machine, to be captured by collimators

Energy at 450 GeV to quench a dipole magnet corresponds to about 10^9 protons

The energy stored in magnets and beam can....

- quench magnets
- destroy equipment

LHC Machine Protection is to.....

Prevent an uncontrolled release of stored energy, thus avoiding:

- damage of equipment
- unnecessary down-time - for example: we intend to **DUMP the beam** in case of beam loss that could lead to a magnet quench

The Machine Protection Systems includes

- Systems to protect the LHC in case of a quench, of others failures in the powering system
- Systems that protects the LHC in case of beam losses that become unacceptable
- tools for consistent error and fault tracing POST MORTEM

BEAM ABORT

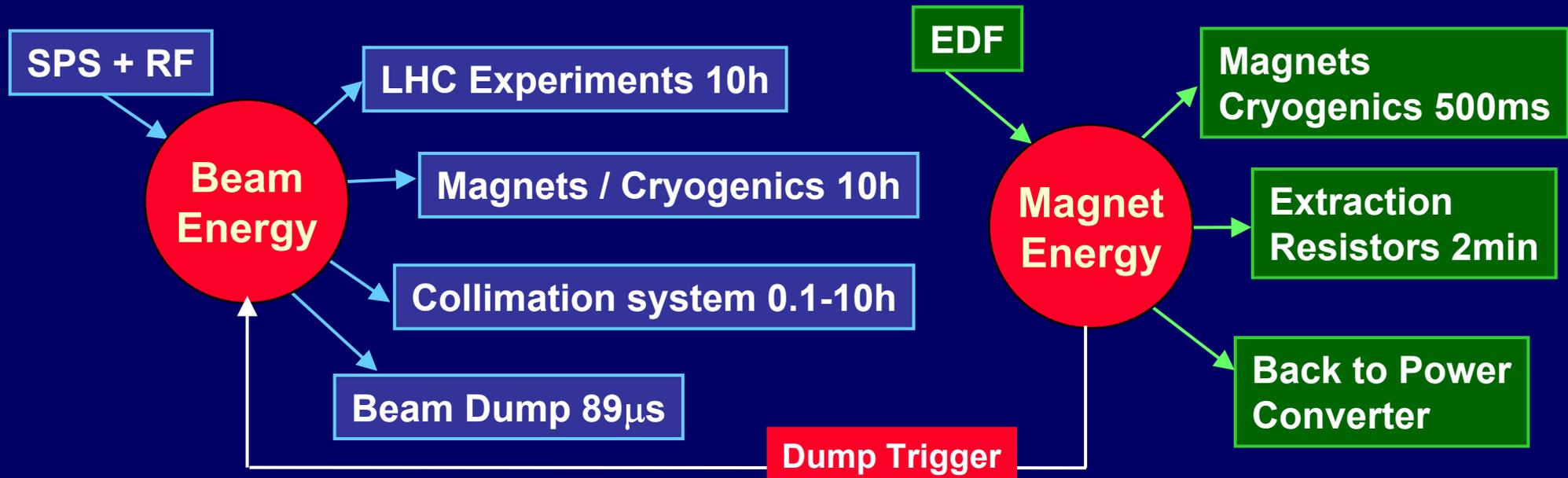
With respect to BEAM OPERATION

- Detect dangerous failures or beam losses
- Energy stored in beams to be safely deposited with BEAM DUMP SYSTEM

POWERING ABORT

With respect to POWERING

- Detect quenches
- Energy stored in magnets to be safely deposited with POWER DUMP SYSTEM



Both systems are largely independent

- No signals from BEAM DUMP SYSTEM to POWER DUMP SYSTEM
- Signal from POWER DUMP SYSTEM to BEAM DUMP SYSTEM in case of power fault

Why “reliability engineering” is discussed here?

- LHC produces **integrated luminosity** that depends on the machine parameters and the time with colliding beams (**reliability**)
- The LHC has **large stored energy** in magnet system and beams
 - potential hardware damage leading to down-time
 - many interlock channels leading to down-time (interlocks that are not strictly required are detrimental to the operation)

=> Reliability of components of the machine protection systems - for critical elements
- The number of critical components (required for operation) in the LHC is larger than for other (CERN) accelerators

=> Reliability for the technical systems of the accelerator
- Repair in the cold part takes long (10...30 days), therefore MTTR (**Mean Time To Repair**) about factor 10 higher than for other accelerators
- After a beam dump, say, at 7 TeV it takes several hours to re-establish colliding beam conditions

CERN and reliability engineering

- Many colleagues at CERN are working on issues related to reliability, safety, quality assurance,
- There is a lot of experience in **reliability engineering** at CERN, for example...
 - for safety systems such as access systems, alarm systems
 - in teams working on equipment protection
- Still, **reliability engineering** is not considered as a general tool for the construction and operation of complex accelerators. Often **reliability engineering** comes with new people with previous experience in the field
- Is **reliability engineering** just a set of hand-waving arguments?
- My understanding:
Reliability engineering = **quantifying common sense** with established scientific tools (using mathematical probability and statistics - at an advanced level) **together with a clear definition of “fuzzy” terms**

Quantifying reliability for the LHC

- **Reliability can be quantified** - with accepted mathematical tools. Such tools are challenging since mathematics involved can be rather advanced
- **Reliability** of different systems **can be compared**
- To **estimate the reliability** of the entire accelerator, the **reliability of all subsystems** need to be estimated
- **Strictly required** for all systems for the **safety of personnel** (INB, legal obligation)
- **Required for all systems to avoid equipment damage**
 - Beam Abort System
 - Beam Interlock System
 - Powering Interlock System
 - Quench Protection System
 - Beam Loss Monitor System
- **Required** for other systems in order **to optimise the efficiency** of LHC operation

Examples of studies on reliability

- **Interconnects between magnets**
- **Quench Protection System**
- **Access System**
- **Beam Dump System**
- **Safety systems**

- L.Scibile, P.Ninin, S.Grau, Functional Safety, A total quality approach, CERN-ST-2001-055 (2001)
- C.Garion, B.Skoczen, Reliability oriented optimum design of the LHC interconnections - Part I: Mechanical compensation system LHC, PROJECT-NOTE-245 (2000)
- W.Hees, R.Trant, Evaluation of Electro Pneumatic Valve Positioners for LHC Cryogenics, LHC-PROJECT-NOTE-190 (1999)
- M.Rampl, Study for a failsafe trigger generation system for the LHC beam dump kicker magnets, CERN-THESIS-99-056, 29 Apr 1999
- J.H.Dieperink et al. Design aspects related to the reliability of the LHC beam dump kicker system, PAC 1997, Vancouver
- A.Vergara et al.: Risk analysis for the quench detection in the LHC machine, EPAC 2002, in preparation, and future CERN-THESIS
- Conceptual design of the LHC Post Mortem Recording System, J.Wenninger et al, being prepared

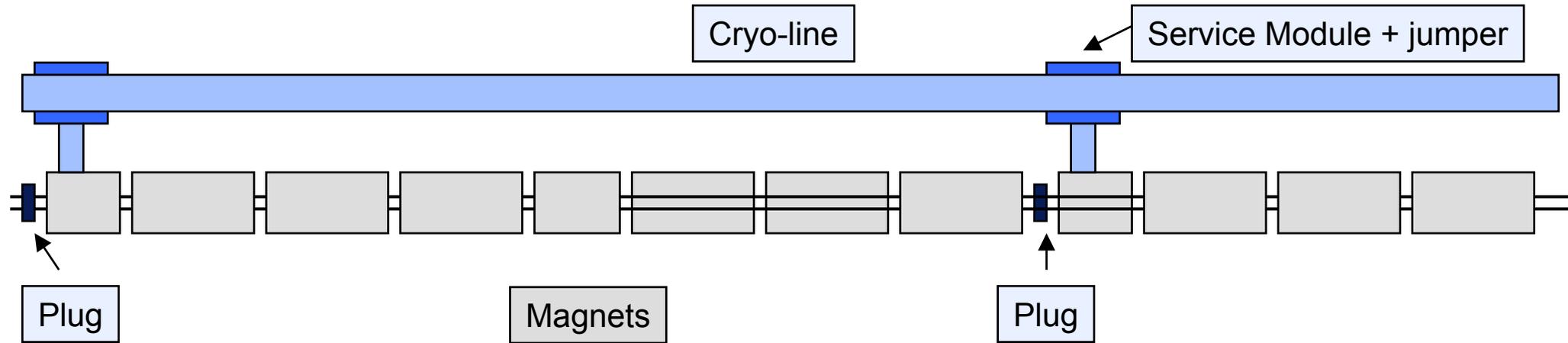
Extending Reliability Engineering for the LHC

- Training of people, outside and inside CERN, for example, this week a series of lectures by P.Kafka
- Use of common software for all CERN users, and courses to use the software: IsographDirect's RAMS tools package
- Quantifying Reliability and Safety
 - SIL (**S**afety **I**ntegrity **L**evels) for protection of personnel and equipment protection
- Using standards: IEC 61508 gives guidance for system design and exploitation
- Discussions and information exchange in Working Groups across systems
 - Machine Protection WG
 - Access and Interlock WG
 - others

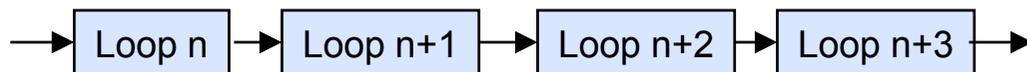
Agree upon Safety Integrity Level

Category	Injury to personnel		Damage to equipment	
	Criteria	N. fatalities (indicative)	CHF Loss	Downtime
Catastrophic	Events capable of resulting in one or more fatalities	≥ 1	$> 5 \cdot 10^7$	> 6 months
Major	Events capable of resulting in very serious injuries	0.1 (or 1 over 10 accidents)	$10^6 - 5 \cdot 10^7$	20 days to 6 months
Severe	Events which may lead to serious injuries	0.01 (or 1 over 100 accidents)	$10^5 - 10^6$	3 to 20 days
Minor	Events which may lead to minor injuries	0.001 (or 1 over 1000 accidents)	$0 - 10^5$	< 3 days

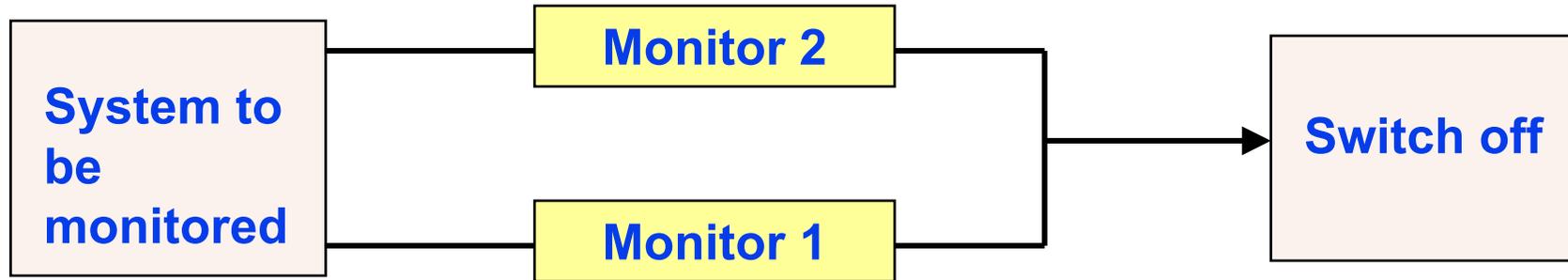
Example of systems in parallel / in series: Cryogenics



- Cooling in general for one cell - this allows to separate one cell from the adjacent cell (Cooling loops in parallel)
- For considering the reliability: Every cooling loop needs to work without failure, therefore “**reliabilitywise**” the **cooling loops are in series** for a mission that requires operation at 1.9 K of the entire 8 arc cryostats
- To estimate the reliability of a complex system, **Reliability Block Diagrams** are required



Example for monitors of a protection system



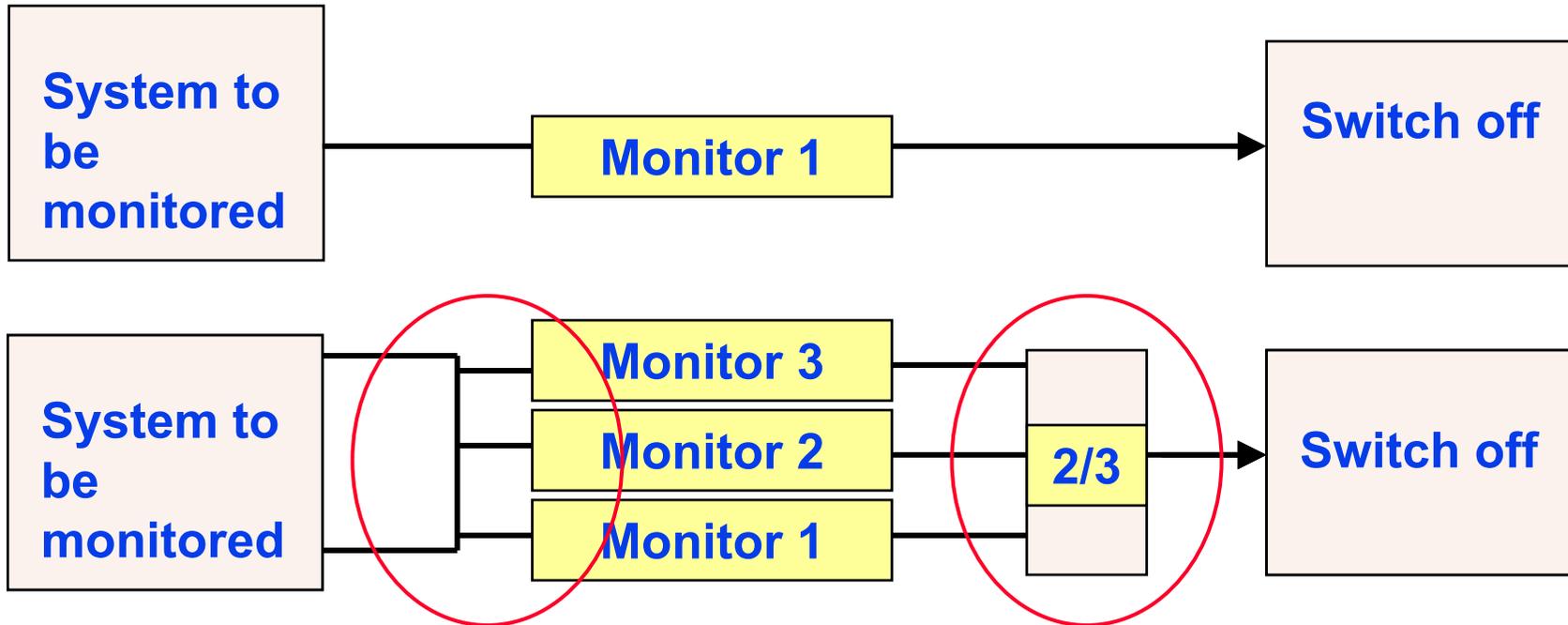
- Two monitors are measuring the status of a system parameter. In case of failure each (working) monitor would switch the system off
- It is sufficient that only ONE monitor is working to switch off
- Assume a constant failure rate that is the same for each of the monitors (chance failure)

CASE I: Only one monitor is used for 20 years. What is the reliability (probability for correct operation of the system) ?

CASE II: Two monitors are operating in parallel of a time of 20 years.

CASE III: The correct functioning of both monitors is verified, for example, once per month. What is the reliability ?

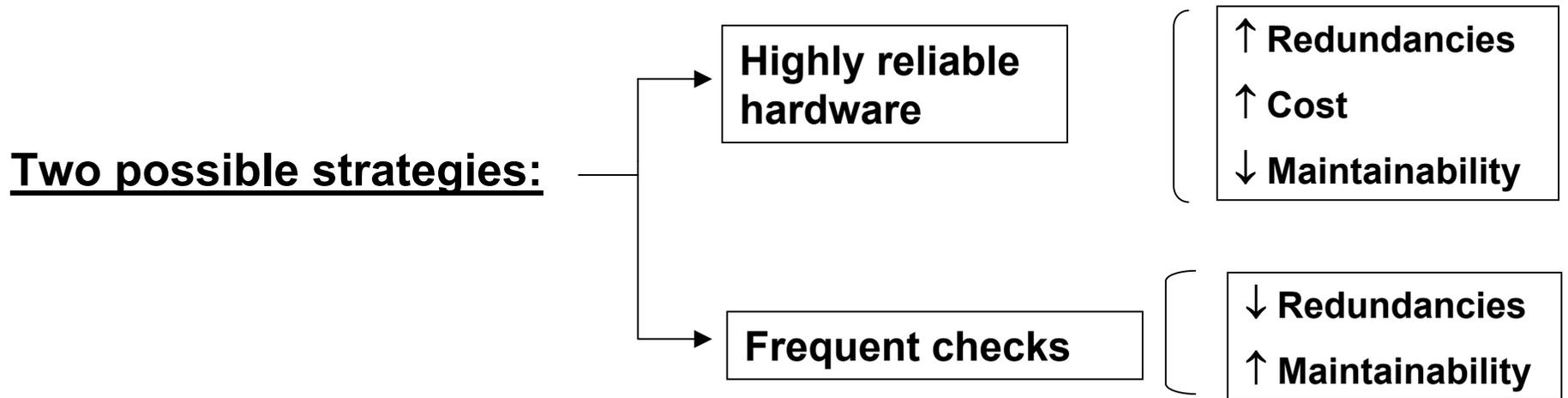
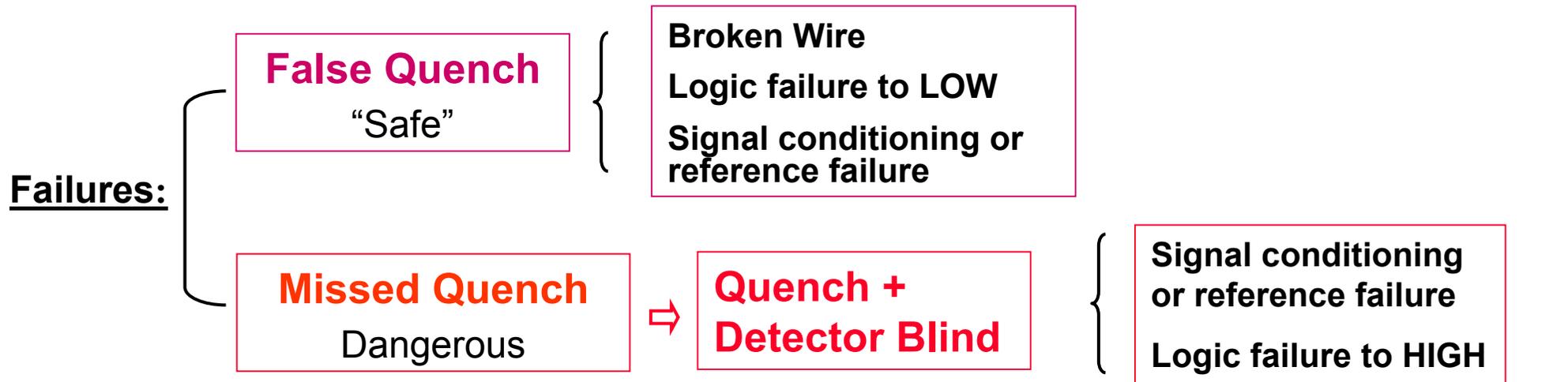
Very careful study is required.....



Example from Quench Detection studies by A.Vergara et al.

What is the optimum system?

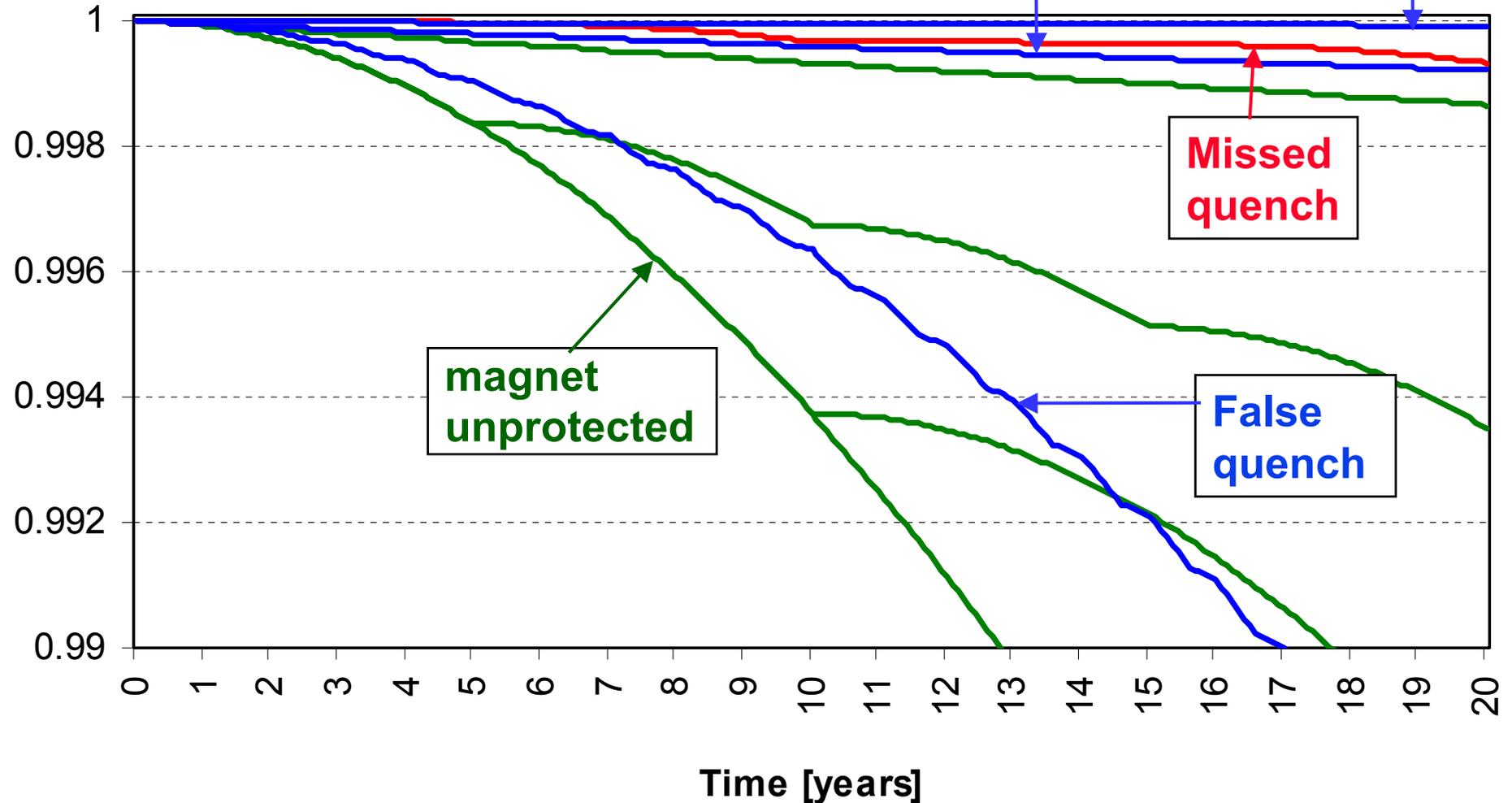
Reliability of Quench Detectors: Minimise accelerator downtime due to quench detection failures



Reliability as a function of time depending on test strategy

Test every year

Test every month

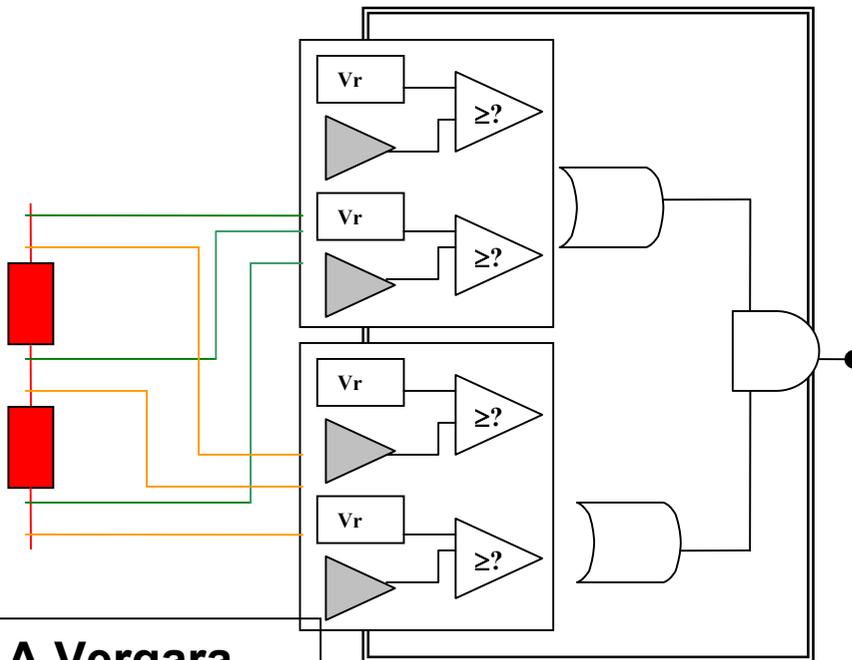
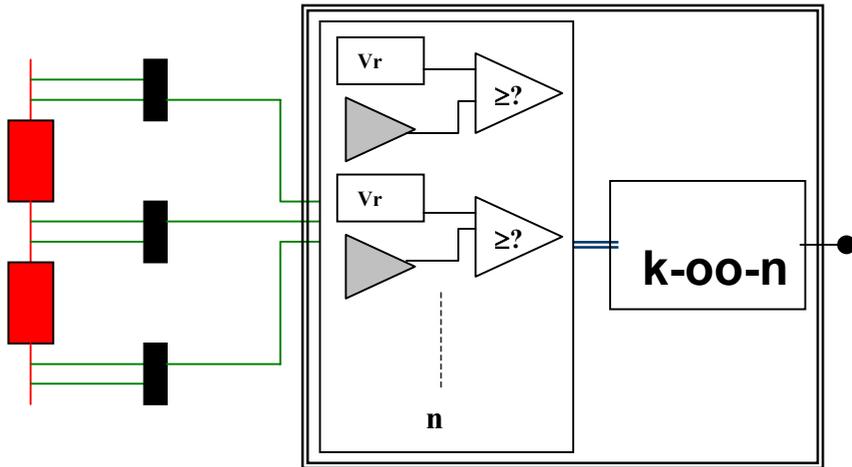


Missed quench

magnet unprotected

False quench

Quench Detectors: 2 solutions

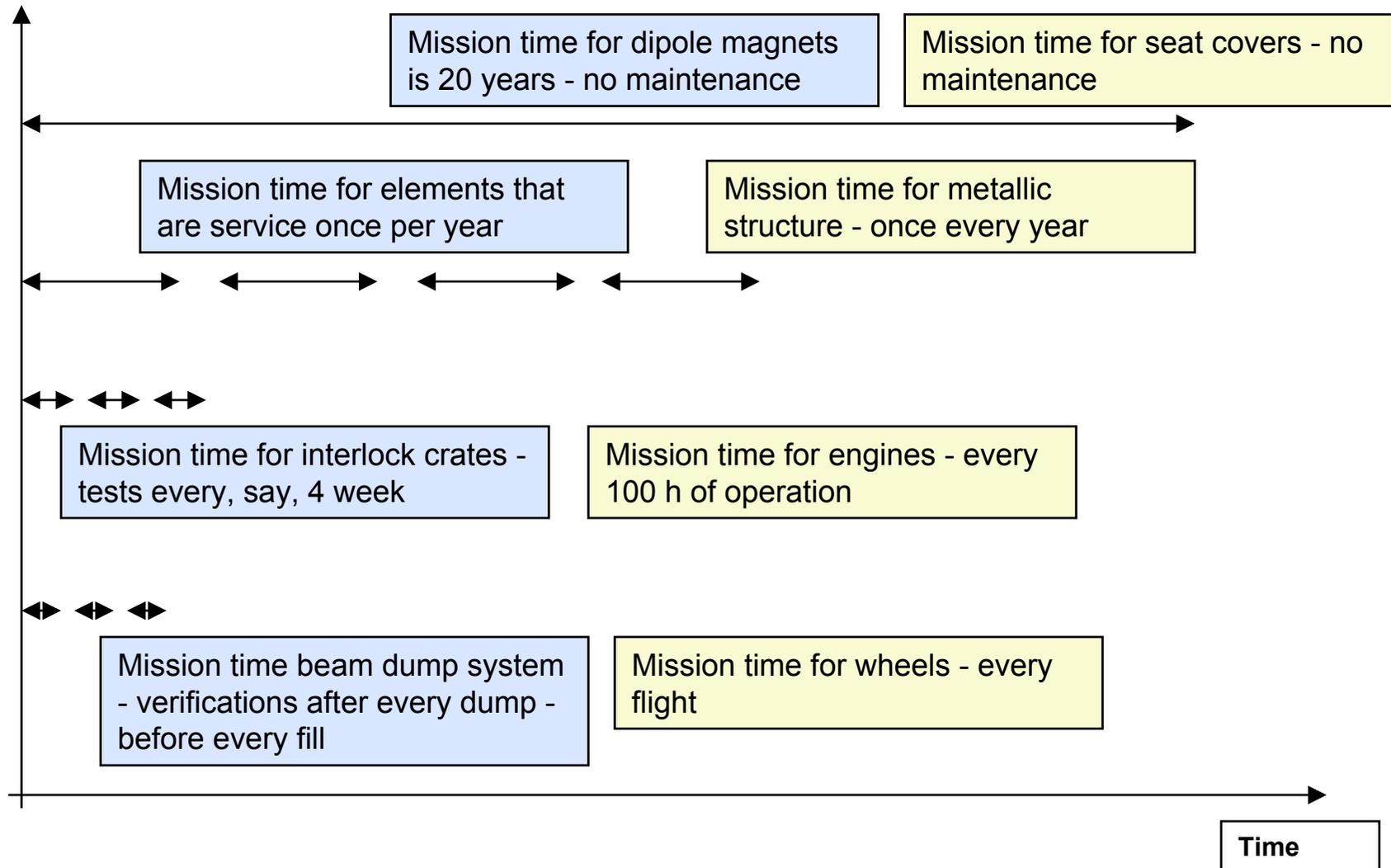


A.Vergara

- ✓ Simplicity: Only one board.
- ✓ Acceptable performance for 4 channels or more
- ✗ FQ very reliable schemes \Rightarrow MQ low reliability
- ✗ MQ very reliable schemes \Rightarrow FQ low reliability
- ✗ \uparrow Channels \Rightarrow \uparrow Logic complexity \Rightarrow \downarrow Logic Rel.
- ✗ Broken wires not detectable.

- ✓ Two independent QD \Rightarrow Simple maintainability.
- ✓ Very good performance against FQ and MQ.
- ✓ Very simple logics \Rightarrow Reliable.
- ✓ Broken wires detectable.
- ✓ Possibility of independent powering \Rightarrow \uparrow Cost ✗
- ✗ More space required

Mission time for different systems - LHC and Airbus*



* numbers for illustration only

Reliability is essential for the success of the LHC Mission

- Many people are aware that reliability is required
- In many teams, work is on-going on the reliability of sub-systems

There is no “Reliability Engineering for Accelerators”

There is no usage of common tools, neither much communication among the players

Many of us (e.g. myself) are not educated in the formalism's to describe “Reliability” (Terms, and mathematical models)

It is difficult to identify systems where improvements are most efficient

It is today not possible to have a number for the overall LHC reliability

Training, Communication (Working Groups)

Use of common software tools

Training and communication, successful examples

Difficult - but not impossible, comes with time

Should be possibly at a later date

The end

The role of the LHC Collimation System in Machine Protection

At 7 TeV and nominal intensity, energy in each LHC Beam: 350 MJ

Energy in one beam could melt about 550 kg of copper

- A small fraction of the beam could damage equipment
- The entire beam would cause massive damage of equipment

Collimators for operating the machine

- Absorb the beam halo to avoid quenches of the superconducting magnets
- Collimator adjustment is critical - need to be close to the beam

Collimators for machine protection in case of failure

- Protect the accelerator elements and experiments from beam loss after a failure
- Absorbers need to limit the aperture - adjustment is less critical

Failures of machine equipment to be anticipated

The LHC is the most complex accelerator that has ever been constructed

- There are about 7000 magnets (most of them superconducting), powered in 1700 electrical circuits, each circuit powered with one power converter
- The protection of the sc elements (magnets, busbars and current leads) requires more than 5000 detectors
- A quench in a superconducting magnet would lead to beam loss
- A failure of a power converter is likely to lead to beam loss

Examples:

- at 7 TeV, one orbit corrector magnet fails that operates at 40% of its strength: beam deflection by about 4 sigma
- quench of one dipole magnet: beam deflection by about 4 sigma after about 60 ms - and 45 sigma after 0.4 s

The beams will (MUST**) always touch the collimators first!**

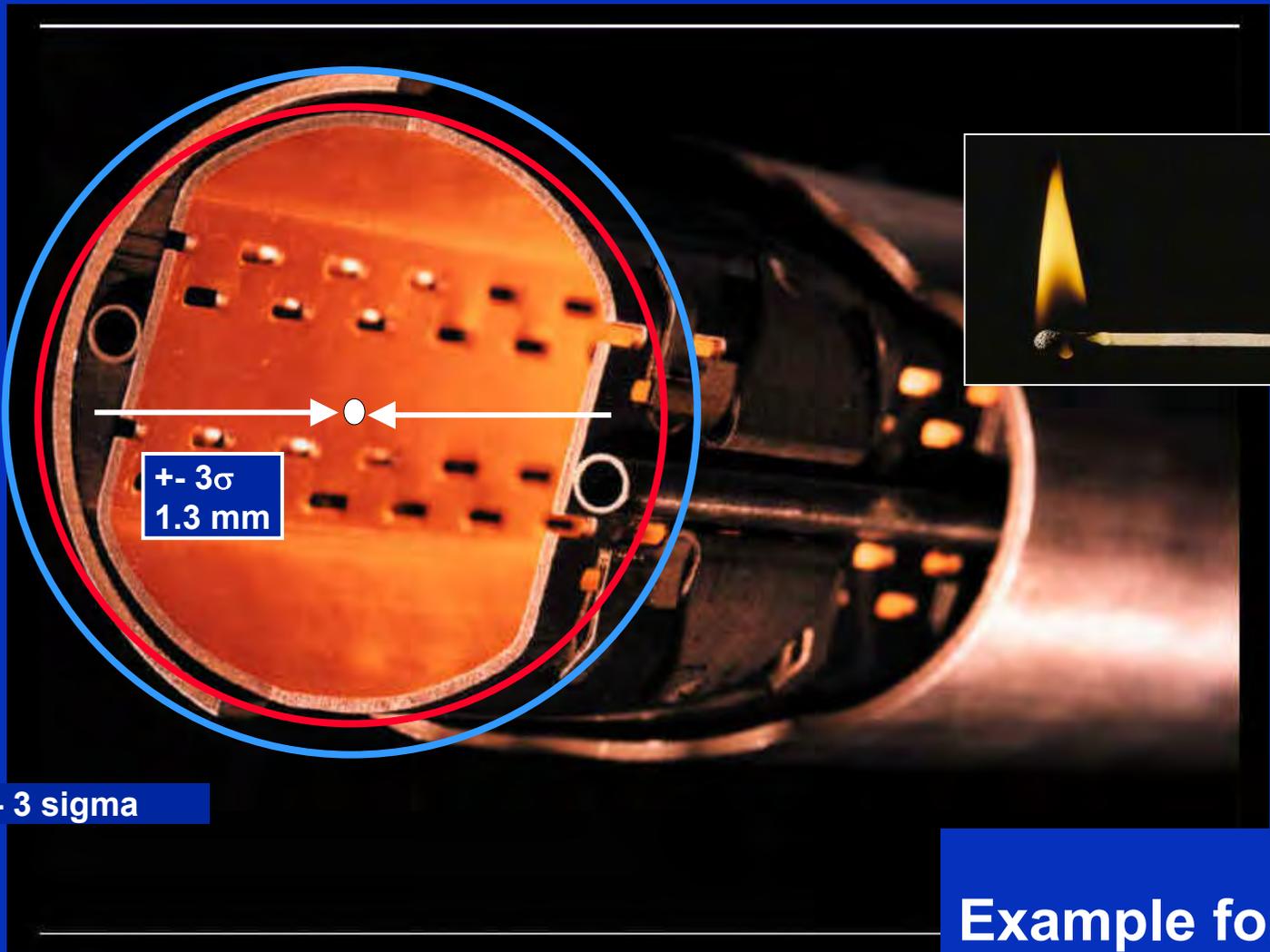
Tasks of the collimation system in machine protection

Task 1: Capture beam losses that could damage LHC equipment in case of a failure before the beam dump fires

Task 2: Together with the Beam Loss Monitors produce a fast and reliable signal to dump the beam if beam losses become unacceptable

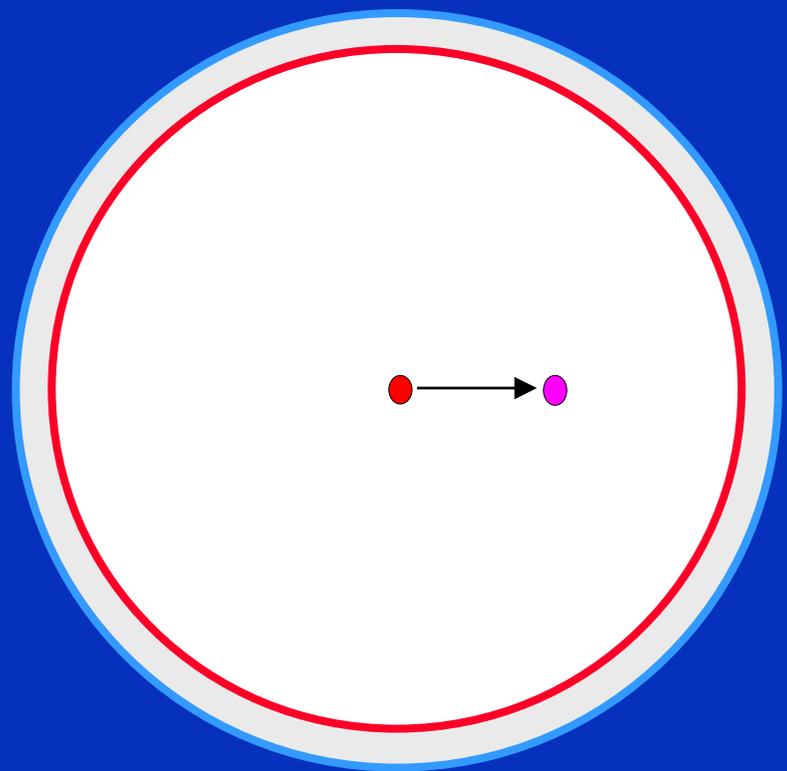
The beam dump block is the only systems that can stand the full 7 TeV beam

- The beam dump is an **active system** - it requires **a trigger** to dump the beam
- The collimators must be the elements that limit the aperture when operating with “high” intensity - high intensity is already in the order of 10^{-3} of the total beam intensity
- The threshold of the monitors to dump the beam should be below the destruction level of the collimators
- Quality and reliability of the beam dump system can not be better than the quality of the trigger



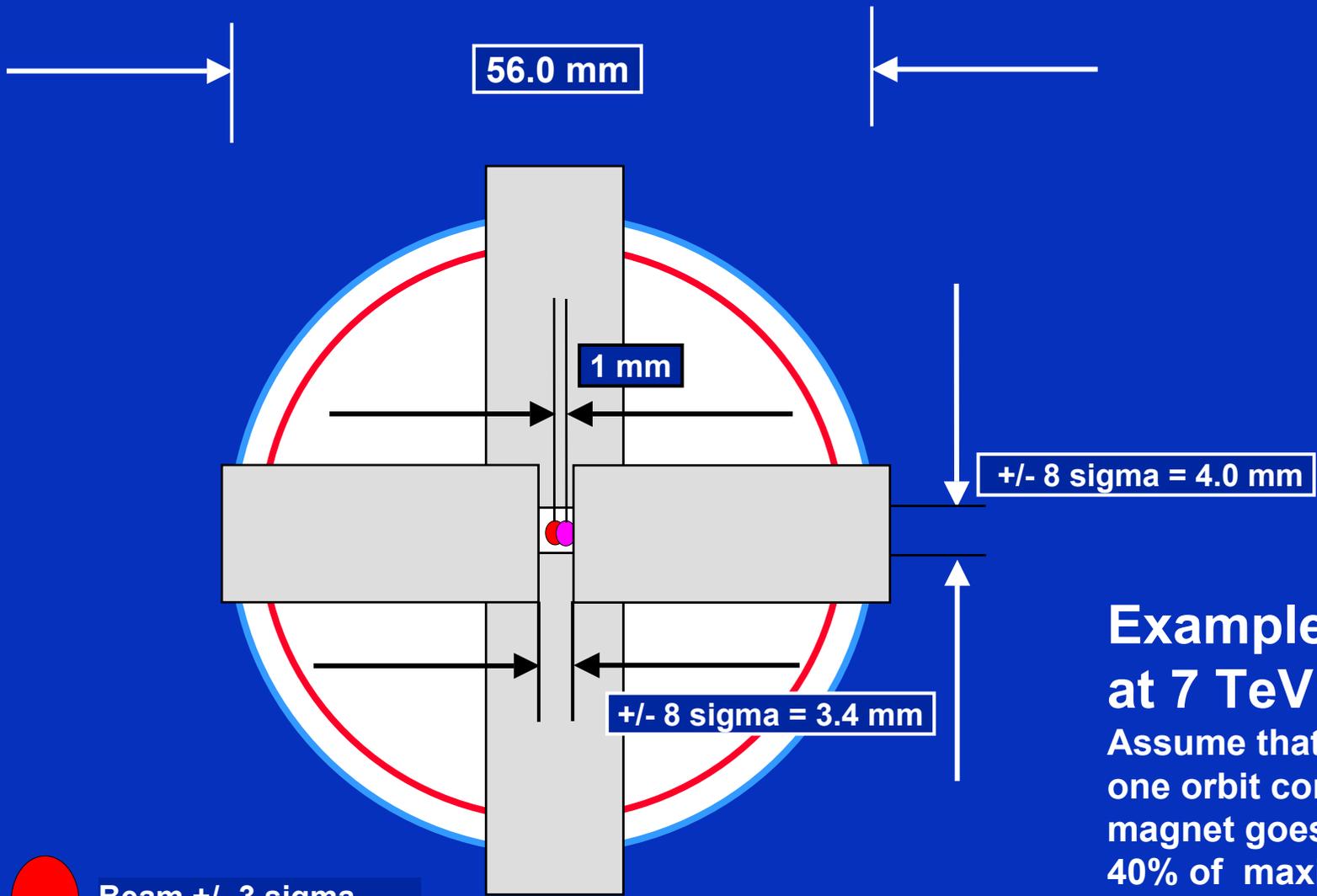
Beam +/- 3 sigma

Example for failure at 7 TeV energy



-  Beam +/- 3 sigma
-  Beam +/- 3 sigma and dipole magnet quench

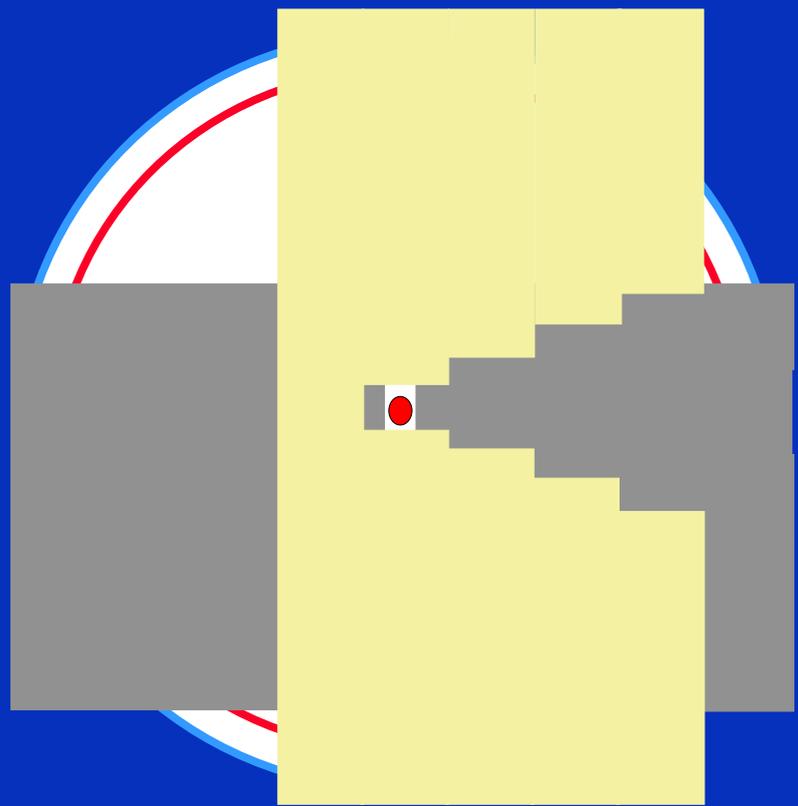
**Example for failure
at 7 TeV energy**
Assume that a dipole magnet
quenches



- Beam +/- 3 sigma
- Beam +/- 3 sigma and orbit corrector at 40% of I_{max}

Example for failure at 7 TeV energy

Assume that the current in one orbit corrector magnet goes off to 0 from 40% of maximum current (I_{max} = 60 A)



 Beam +/- 3 sigma

No preconception
for the collimator
design

Equipment failure with circulating beam: BLMC

Primary strategy for protection: Beam loss monitors at collimators continuously measure beam losses

Example for failure:

- Power converter fault induces orbit distortion
- Beam approaches collimators
- Beam loss monitors (BLMC) indicate increased losses
- Beam loss measured with monitor exceeds predefined threshold
- Beam loss monitors break Beam Permit Loop
- Beam dump sees “No Beam Permit” => dump beams

In case of failure of [most / all ?] equipment, enough time is available to dump the beam before damage of equipment - including all magnets and power converters

Failure scenarios of operation with circulating beam were studied by O.Brüning (time constants for failures) - the studies continue

Conclusions and Suggestions

- **Reliability is essential for the success of the LHC Mission**
 - Many people are aware that reliability is required
 - In many groups, work is on-going on the reliability of sub-systems
- There is no “Reliability Engineering for Accelerators”
- There is no usage of common tools, neither much communication among the players
- Many of us (e.g. myself) are not educated in the formalism's to describe “Reliability” (Terms, and mathematical models)
- It is difficult to identify systems where improvements are most efficient
- It is not possible to have a number for the overall LHC reliability
- Use of common software tools
- Training
- Communication - such as presentation in the MPWG on the reliability predictions for sub-systems - to be scheduled

Remarks

- Reliability Engineering very much used for space missions
- Reliability relies on quality - and quality control assures that parts are being made within specific tolerance limits, and the number of defectives is at a level that is determined by the required reliability.
- The cost of a product needs to consider the reliability during the mission (life-cycle cost).
- Hardware commissioning as method of burning-in - does this concept make sense for LHC equipment?
- *“If you need an accident to know there is a problem, then you are part of the problem”* (Joe Barton)

Summary of architecture for the machine protection

General

- Separation of **BEAM PERMIT** and **POWER PERMIT**
- Separation of POWER PERMITS for cryostats - **one (two for arcs) PPC** per cryostat
- **Diagnostics** after fault is integral part of the system

Classification of Electrical Circuits

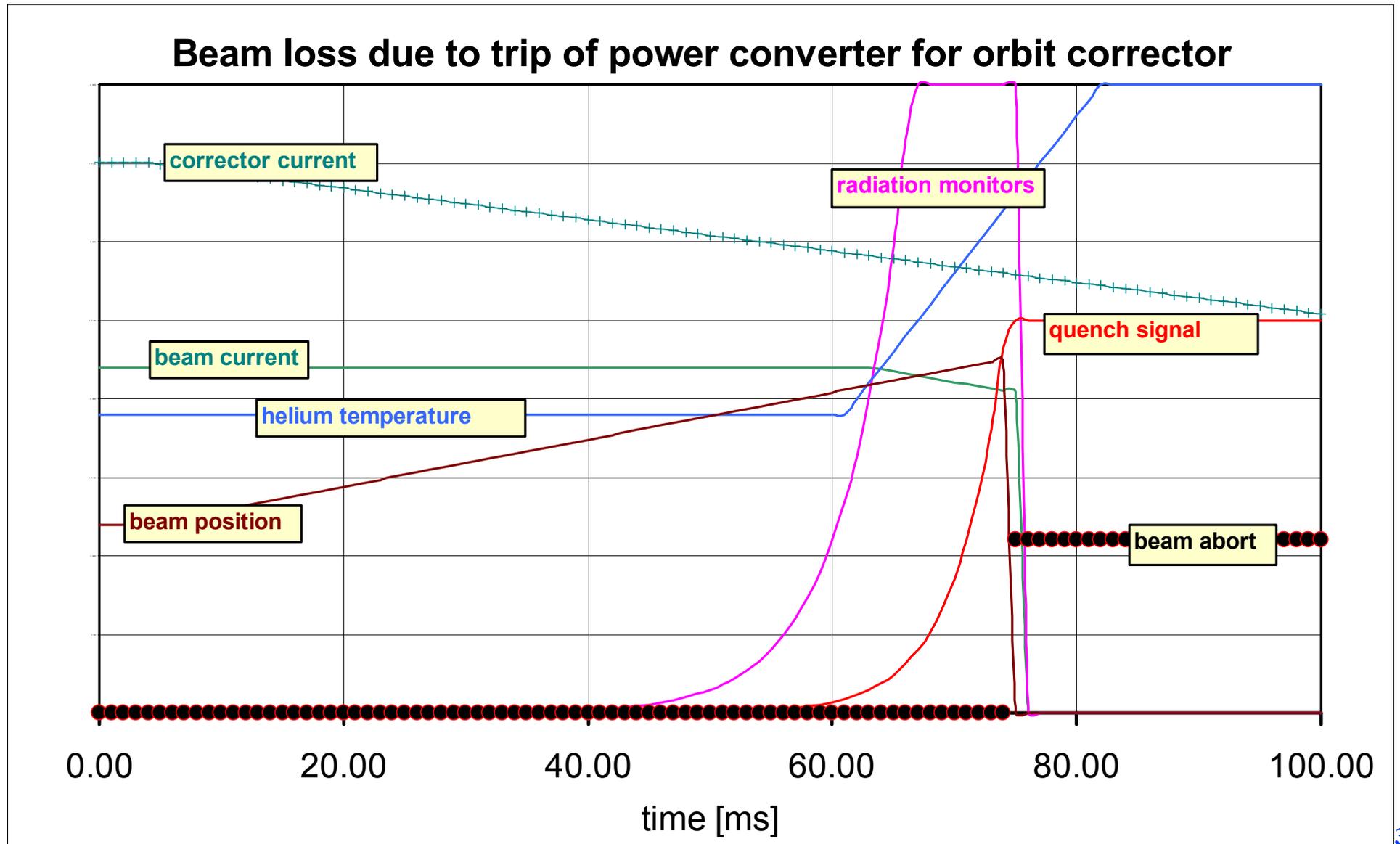
- **Powering:** Main circuits (**CRYOSTAT POWER ABORT**) and auxiliary circuits (**CRYOSTAT POWER FAULT**)
- **Beam Operation:** **CRITICAL** CIRCUITS and **LESS CRITICAL** CIRCUITS

Inventory

- About 60 electronics crates
- **Two fast links** for **BEAM ABORT** with **optical fibres** (plus some reserve fibres)
- Several **slower links** for **POWER ABORT**, possibly using **current loops**
- Fail-safe links, and input signals to electronics

Post Mortem Diagnostics MUST be a part of the system

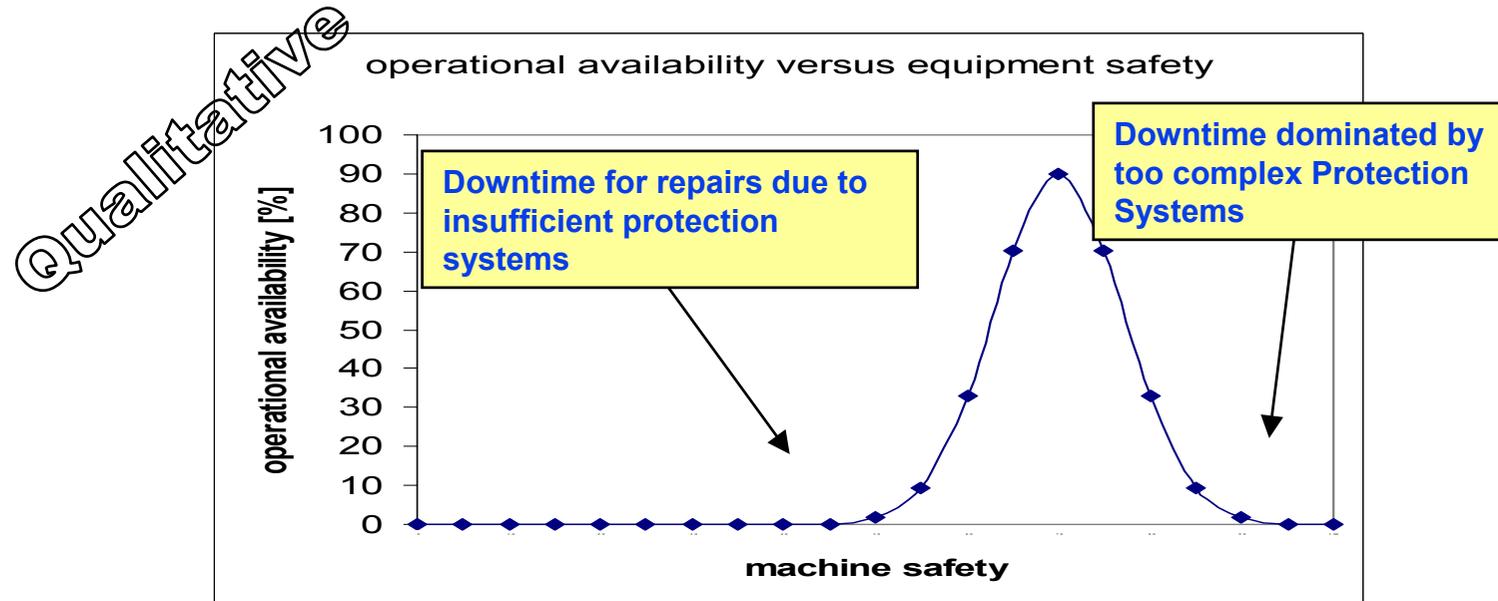
- Artist view of the requirement



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



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

Three-Fold Functionality

- **Enable: A system that allows to switch on (equipment interlock system)**

- power converters
- beam injection enable
- other systems and test modes - to be defined

this is in general not time critical and includes many systems (eg. Cryogenics)

- **A system that stops beam - BEAM ABORT**

- beam dumps (as fast as technical possible - see Oliver)

this is VERY time critical and must be fail safe, and includes less systems

- **A system that stops power - POWER ABORT**

- fire quench protection heaters (local action)
- act on power converter (10ms - 1s)
- open energy extraction switches (10ms - 1s)
- discharge circuits (time constants between 1 and 104 seconds)

this is time critical and must be fail-safe (failure could lead to heavy equipment damage)

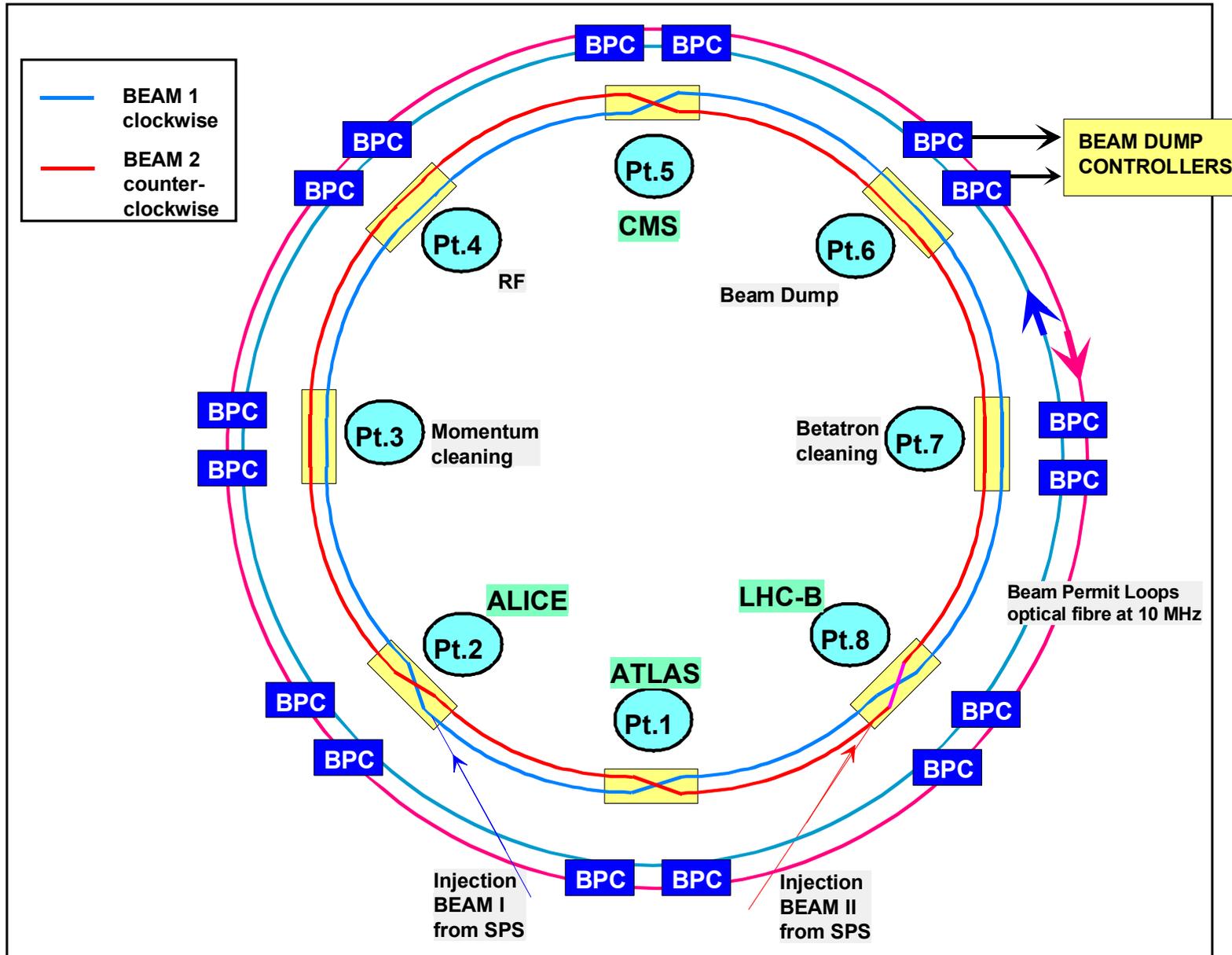
- **A system recording the data for post-mortem analysis of any ABORT**

- Clear diagnostics (example - get info MB 112 in sector 5 quenched)

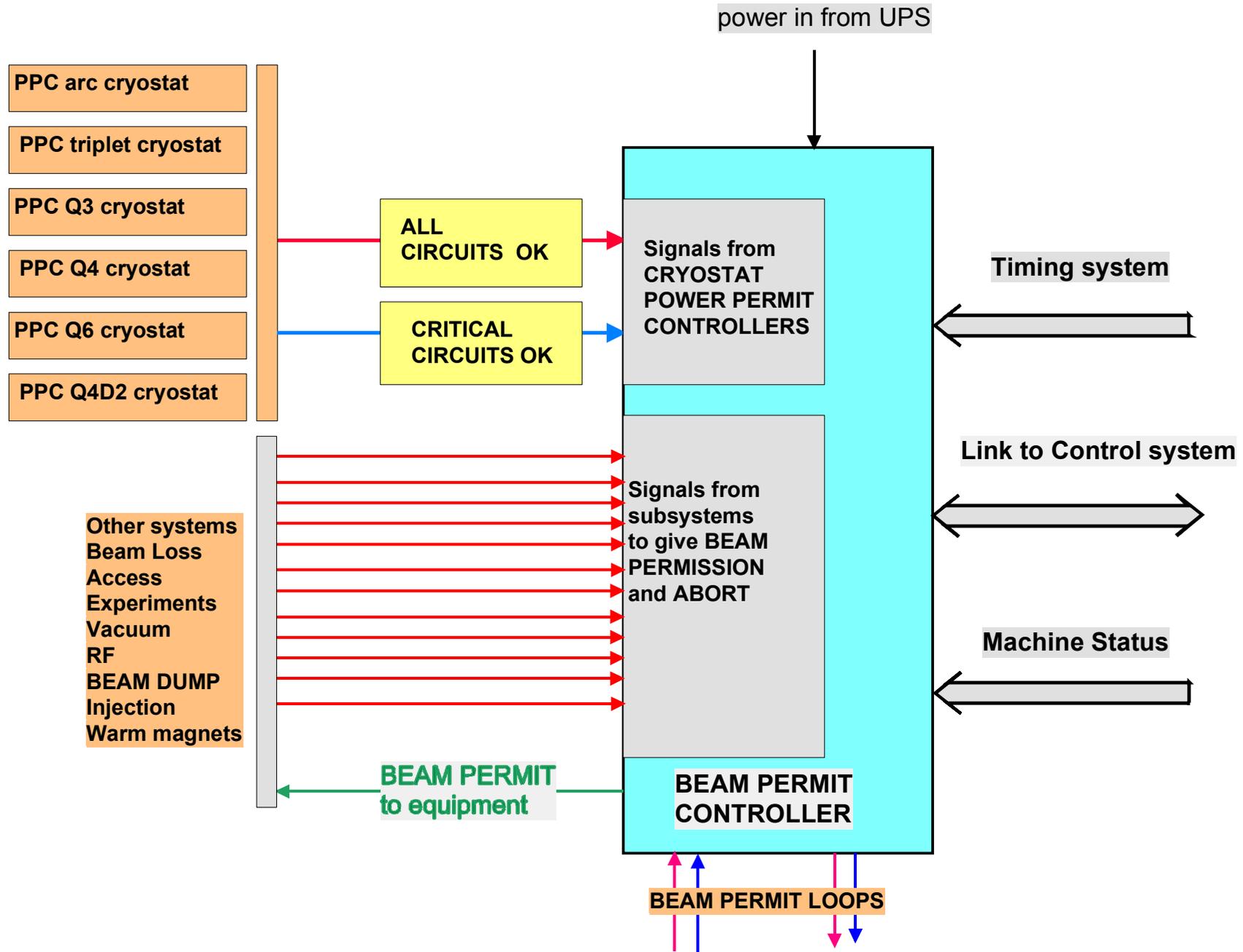
LHC General Parameters

Energy at collision	7	TeV
Energy at injection	450	GeV
Dipole field at 7 TeV	8.33	Tesla
Luminosity	10^{34}	$\text{cm}^{-2} \text{s}^{-1}$
Luminosity lifetime	10	h
Beam beam parameter	0.0036	
Particles per bunch	$1.1 \cdot 10^{11}$	
DC beam current	0.56	A
Stored energy per beam	350	MJ
Bunch spacing	7.48	m
Bunch separation	24.95	ns
Normalised emittance	3.75	μm
Total crossing angle	300	μrad
Energy loss per turn	7	keV
Critical photon energy	44.1	eV
Total SR power per beam	3.8	kW
Filling time per ring	4.3	min
Magnet coil inner diameter	56	mm
Distance between beams	194	mm

Architecture of BEAM PERMIT in the LHC



BEAM PERMIT CONTROLLER



Some Parameters of the Protection Systems

BEAM PERMIT / ABORT for the entire LHC accelerator

- Fast system - the beam can be dumped in a few turns
- BEAM PERMIT CONTROLLERS (BPC) linked via optical fibres with 10 MHz signal (fast data transmission)
- Absence of BEAM PERMIT triggers BEAM DUMP
- 16 BEAM PERMIT CONTROLLERS are required
- Input from variety of systems, such as powering and protection, access, BLM, vacuum, and others

POWER PERMIT / ABORT for each continuous cryostat

- System is less fast, the power is extracted in several seconds
- Impact beams after some 10 ms - therefore more time to react
- About 48 POWER PERMIT CONTROLLERS (PPC) are required, one per cryostat (two for long arc cryostat)
- Links in tunnel could be via current loop and non-critical communication between controllers via control system