Protection and Interlocks

CERN Accelerator School – May 2014

benjamin.todd@cern.ch

0v3

To Take Away Today

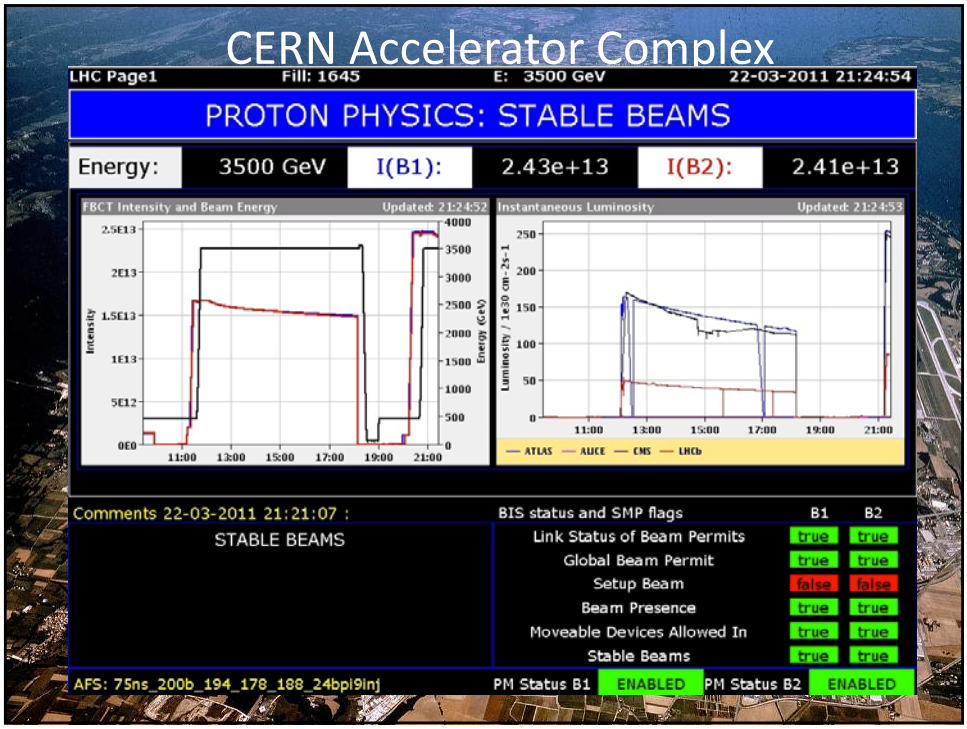
* the protection context is vital
  –need to consider system, machine and organisational level impact

* risk analysis is a core part of every engineer's toolbox
  – zero risk does not exist

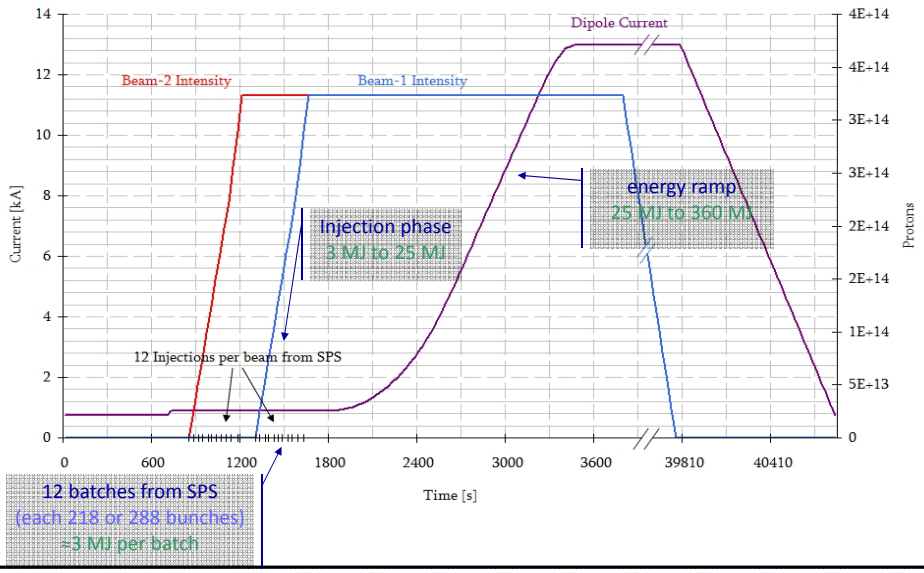
* specification of protection and interlocks is a compromise
  – they don't add to the function, but are an insurance for when things go wrong.
  – they do add to complexity, so will make the system less reliable.

Contents

CERN Accelerator Complex



LHC Magnetic Cycle



Technological Challenges

…To see the rarest events…
LHC needs high luminosity of 10^{34} [$cm^{-2}s^{-1}$]
→ 3 x 10^{14} p per beam

particle fluence near machine
= radiation-tolerant electronics

… to get 7 TeV operation…
LHC needs 8.3 Tesla dipole fields with circumference of 27 kms (16.5 miles)

… to get 8.3 Tesla …
LHC needs super-conducting magnets <2°K (-271°C)
with an operational current of ≈13kA
cooled in super fluid helium
maintained in a vacuum

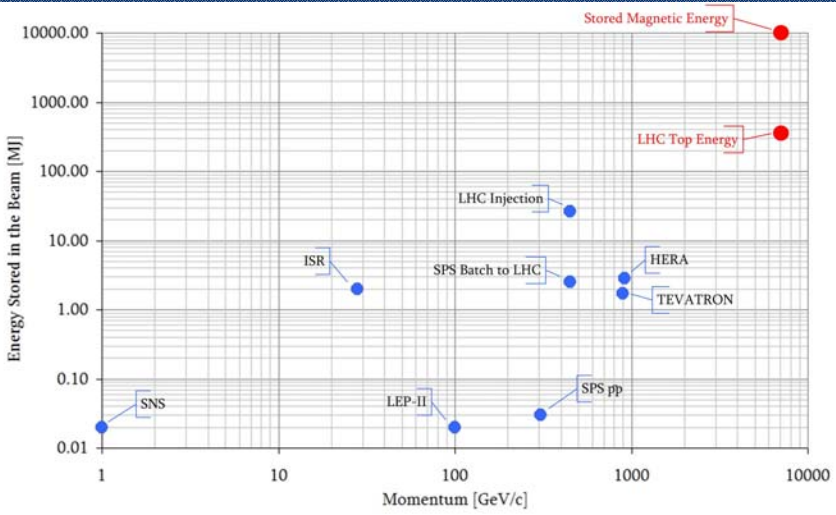
1 ppm

Stored energy per beam is 360 MJ
Stored energy in the magnet circuits is 9 GJ

two orders of magnitude higher than others

A magnet will QUENCH with millijoule deposited energy

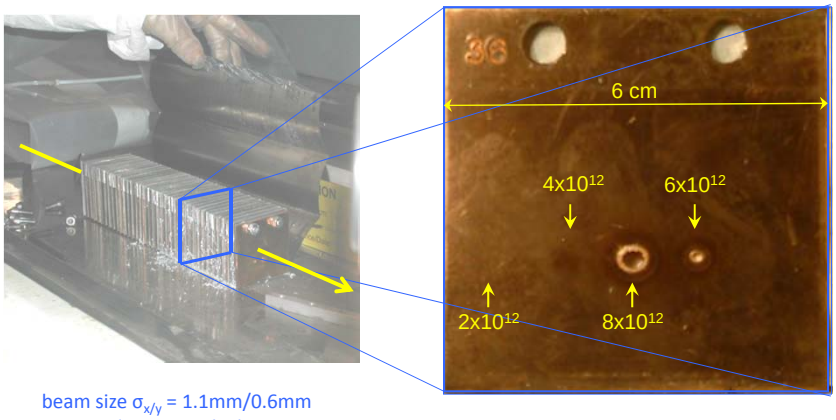
Comparison of LHC with others



powering is split into sub-sectors:
energy in each circuit manageable, allows for a staged commissioning

SPS Experiment at 450 GeV

Controlled SPS experiment to qualify simulations
At 450GeV … $8x10^{12}$ protons causes damage



beam size $\sigma_{x/y}$ = 1.1mm/0.6mm
Plate 2mm thick

0.1% LHC Full Beam Energy! Beam in LHC is 10x smaller!!

Technological Challenges

Kinetic Energy of 200m Train at 155 km/h ≈ 360 MJ

Stored energy per beam is 360 MJ

Stored energy in the magnet circuits is 9 GJ

Picture source: http://en.wikipedia.org/wiki/File:Alstom_AGV_Cerhenice_jmp_0265.jpg
Shared as: http://creativecommons.org/licenses/by-sa/3.0/deed.en

Technological Challenges

Kinetic Energy of 200m Train at 155 km/h ≈ 360 MJ

Stored energy per beam is 360 MJ

Stored energy in the magnet circuits is 9 GJ

Kinetic Energy of Aircraft Carrier at 50 km/h ≈ 9 GJ

Picture source: http://militarytimes.com/blogs/scoopdeck/2010/07/07/the-airstrike-that-never-happened/
Shared as: public domain

Protection Functions

Beam Protection:	Beam Energy	→	Beam Dump

100x energy of TEVATRON

0.000005% of beam lost into a magnet = quench
0.005% beam lost into magnet = damage

Failure in protection – complete loss of LHC is possible

Powering Protection:	Magnet Energy	→	Emergency Discharge

10-20x energy per magnet of TEVATRON

magnet quenched = hours downtime
many magnets quenched = days downtime

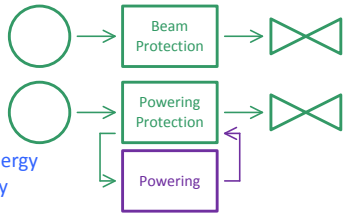
magnet damaged = $1 million, months downtime
many magnets damaged = many millions, many months downtime

Plants, Protection and Safety

Safety – Protection – Plant

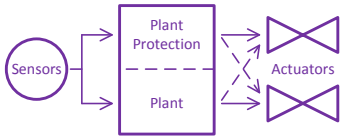
Personnel Safety System:

Machine Protection System:



danger will exist – prevent – extract energy
danger exists – protect – extract energy

Plant Systems:



So…

Each of these systems has a job to do…

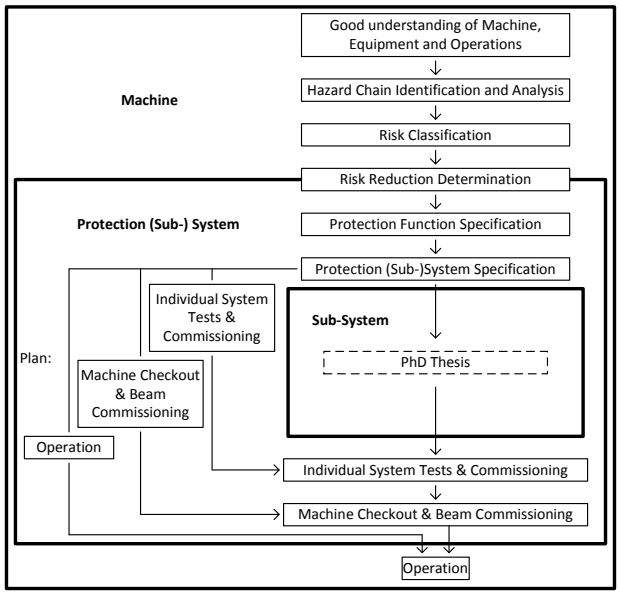
If they malfunction, we are in a tough situation

Everything that can malfunction, will eventually malfunction…
Prepare for and accept malfunction as “normal”.

Build the systems using a risk-based approach

e.g. Safety Systems – IEC 61508 inspired

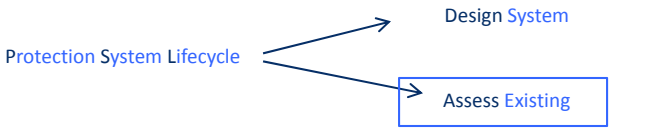
Protection System Lifecycle



Protection System Lifecycle

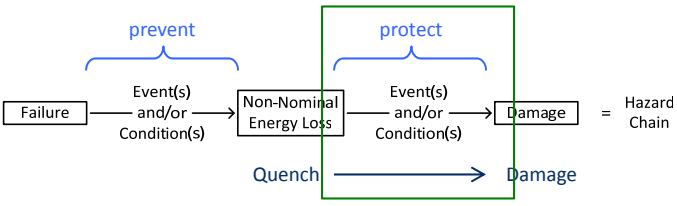
systems involved in protection are unique
certain technologies used have never been tried on this scale before
high cost of failure

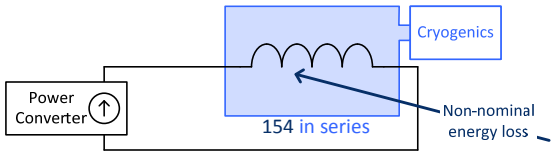
development and analysis of machine protection as if it were a safety system



worked example
Dipole Magnet Protection – **9GJ**

benjamin.todd@cern.ch





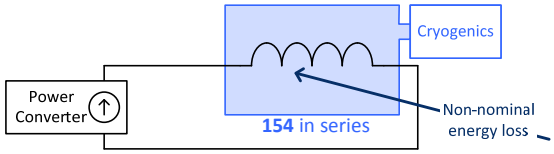
Equipment Under Control → Magnet, Cryogenics, Power Converter

Hazard Chain: from Quench to Damage…

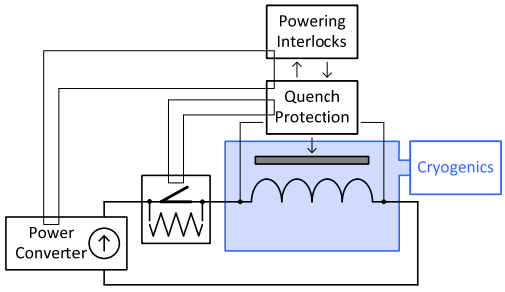
- Resistive zone appears in a magnet
- I^2R losses begin
- Zone heats up

(heat propagates to neighbouring magnets)

- Damage to magnets



What Protection Functions and Protection Systems are in place?

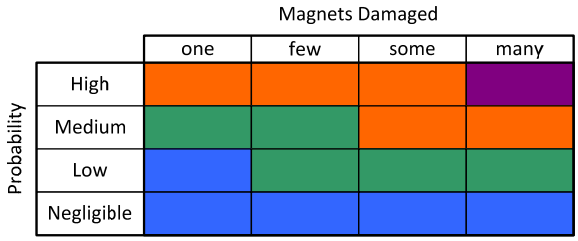


when quench occurs…

- Turn off Power Converter
- Propagate Quench
- Extract Energy
- Link Related Circuits

classify probability and consequence using risk matrix

Colour boundaries, probabilities, consequences intentionally vague = talking points



risk, if function didn't exist, according to system experts…

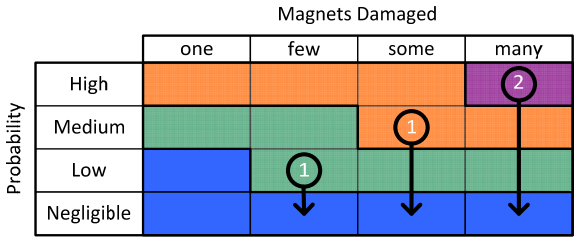
- Turn off Power Converter = **purple**
  - Propagate Quench = **orange**
    - Extract Energy = **purple**
  - Link Related Circuits = **green**

determine risk reduction level using matrix

original	desired	reduction
		3
		2
		1

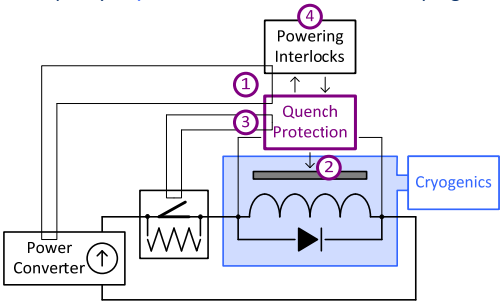
= dependability requirements

- Turn off Power Converter = **purple** = **3**
  - Propagate Quench = **orange** = **2**
    - Extract Energy = **purple** = **3**
  - Link Related Circuits = **green** = **1**



- Turn off Power Converter = **purple** = **3**
  - Propagate Quench = **orange** = **2**
    - Extract Energy = **purple** = **3**
  - Link Related Circuits = **green** = **1**

How do we qualify a system meets a level? How about programmable logic?



- Turn off Power Converter = **purple** = **3**
  - Propagate Quench = **orange** = **2**
    - Extract Energy = **purple** = **3**
  - Link Related Circuits = **green** = **1**

So…

Each of these systems has a job to do…

If they malfunction, we are in a tough situation = “risky”?

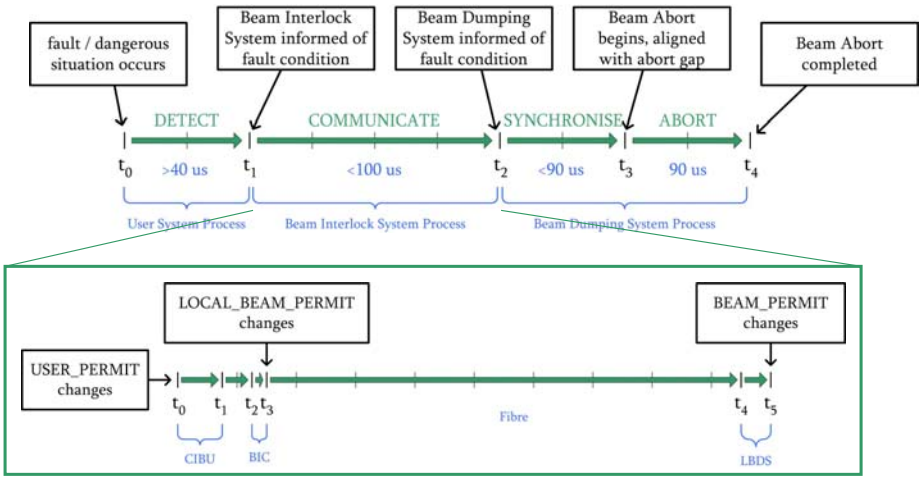
Everything that can malfunction, will eventually malfunction…
Prepare for and accept malfunction as “normal”.

Realise functions using a high-reliability approach, determine failure rates and modes

benjamin.todd@cern.ch

An Example System, Risk Reduction Level 3

The LHC Beam Interlock System



The LHC Beam Interlock System

BIS has a dependability specification

"…[BIS] must react to a single change in USER PERMIT by correctly actioning the relevant BEAM PERMIT with a safety better than or equal to Risk Reduction Level 3. Less than 1% of missions must be aborted due to failures in the Beam Interlock System..."

High Dependability → High Safety, High Reliability, High Availability, Maintainable

PIL3 or better?? = FMECA

Failure Modes, Effects and Criticality Analysis

In what way can something go wrong?…

…when it does go wrong, what happens to the system?…

…and just how much of a problem does this cause?

FMECA

MIL-STD-1629

FMECA starts at the Component Level of a system

Break a large system into blocks, defining smaller, manageable sub-systems

↓

get subsystem schematics, component list, and understand what it does

MIL-HDBK-338 ↓ MIL-HDBK-217

get MTBF of each component on the list, derive P_{FAIL}(mission)

MIL-HDBK-338 ↓ FMD-97

derive failure modes and failure mode ratios for each component

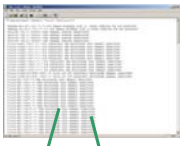
↓

explain the effect of each failure mode on both the subsystem and system

↓

determine the probability of each failure mode happening. Draw conclusions!

FMECA



Bill of Materials

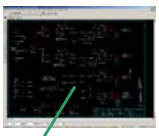
	A	B	C	D	E	F	G
1	**Failure Mode Effect and Criticality Analysis**						
2							
3	**CERN: European Organisation for Nuclear Research**						
4							
5	CRITICALITY WORK SHEET		System:	BEAM INTERLOCK SYSTEM			SubSystem:
6							
7	Part ID	Part Description	Base Failure Rate	Reference BFR	Failure Mode	Failure Mode Frequency Ratio	Reference FMFR
8							
9	(schematic Ref Des)		(/10^9h)		(FMD-97)	(FMD-97)	
10							
11	J1	Burndy FI12	3.9	MIL-HBDK-271F-15-(1-2-3)	Open BF	0.000	FMD-97-2-47/NE12 Cable FM
12			3.9		Open BD	0.060	
13			3.9		Open M	0.090	
14			3.9		Open NE	0.241	
15			3.9		Intermittant Operation	0.552	
16			3.9		Shorted BF	0.000	
17			3.9		Shorted BD	0.006	
18			3.9		Shorted M	0.008	
19			3.9		Shorted NE	0.043	

MIL-HDBK-217F or manufacturer

FMD-97

MIL-HDBK-338

FMECA



Schematic

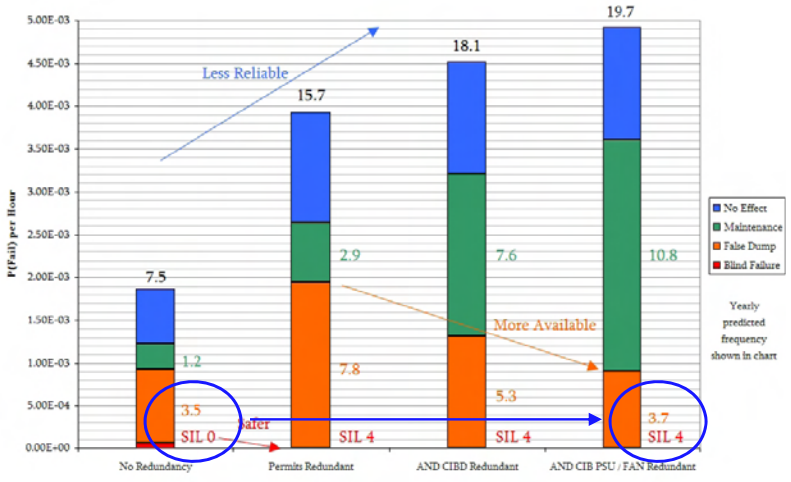
	H	I	J	K	L	M	N	O
				Criticality of system for: Blind Failures, Beam Dumps, Maintenance and No Effect				
						AB/CO/IN	Benjamin TODD	
	CIBU			Version:	1v0		Date:	28.1.05
	Failure Mode Effect Analysis (BF, BD, M, NE)	Failure Mode Effect Description	Detection Method (BD automatic)	P(Fail) During Mission (CIBU)	P(Blind Fail) Permit A (Permit Loop A)	P(Blind Fail) Permit B (Permit Loop B)	P(Fail) Beam Dump (CIBU)	P(Fail) Maintenance (CIBU)
	BF	Permit A/B Fail Blind	Monitoring/Test	0.00E+00	0	0	0	0
	BD	Permit A/B break	Monitoring/Test	2.35E-09	0	0	2.346E-09	0
	M	Command/Response Fail	Monitoring/Test	3.52E-09	0	0	0	3.519E-09
	NE	No Effect	None	9.38E-09	0	0	0	0
	BD	Permit A/B break	Monitoring/Test	2.15E-08	0	0	2.152E-08	0
	BF	Permit A/B Fail Blind	Monitoring/Test	0.00E+00	0	0	0	0
	BD	Permit A/B break	Monitoring/Test	2.28E-10	0	0	2.28E-10	0
	M	Command/Response Fail	Monitoring/Test	3.14E-10	0	0	0	3.139E-10
	NE	No Effect	None	1.68E-09	0	0	0	0

multiply through

Designer Knowledge

MIL-HDBK-338

Dependability vs. Configuration

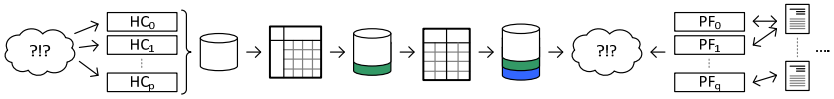


So…

It's clear that this is a huge amount of work

- Miminise the number of systems which need the highest levels
- Minimise the parts of the systems which need any level at all
  - Separate critical function from non-critical function

Failure Case 1: September 2008



not all circuits had been commissioned to 5 TeV - Final Main Dipole Circuit Commissioning

- Electrical Fault at 5.2 TeV in dipole bus bar, between quadrupole and dipole

Post-Analysis: R = 220 nΩ, nominal = 0.35nΩ

- Electrical Arc developed and punctured helium enclosure

Post-Analysis: 400 MJ dissipated in cold-mass and arcing

- Helium Release into the insulating vacuum

Post-Analysis: Pressure wave caused most damage

Hazard Chain had been identified in initial stages…

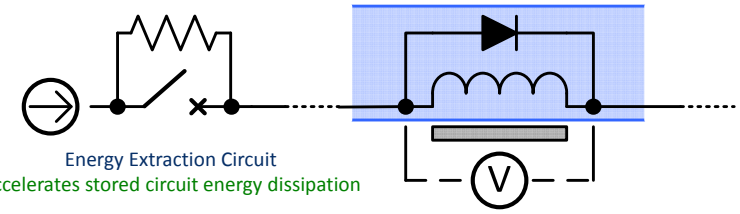
Probability classified as negligible
Risk Reduction Level was therefore minimum

Installation did not conform to simulations…

Case 1: September 2008

Magnet Protection Function

Escape Diode
If magnet quenches = path for current



Energy Extraction Circuit
Accelerates stored circuit energy dissipation

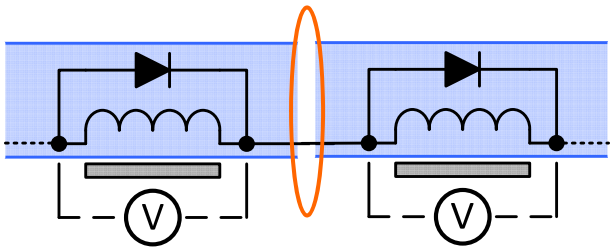
Quench Detector
detects magnet quench

triggers

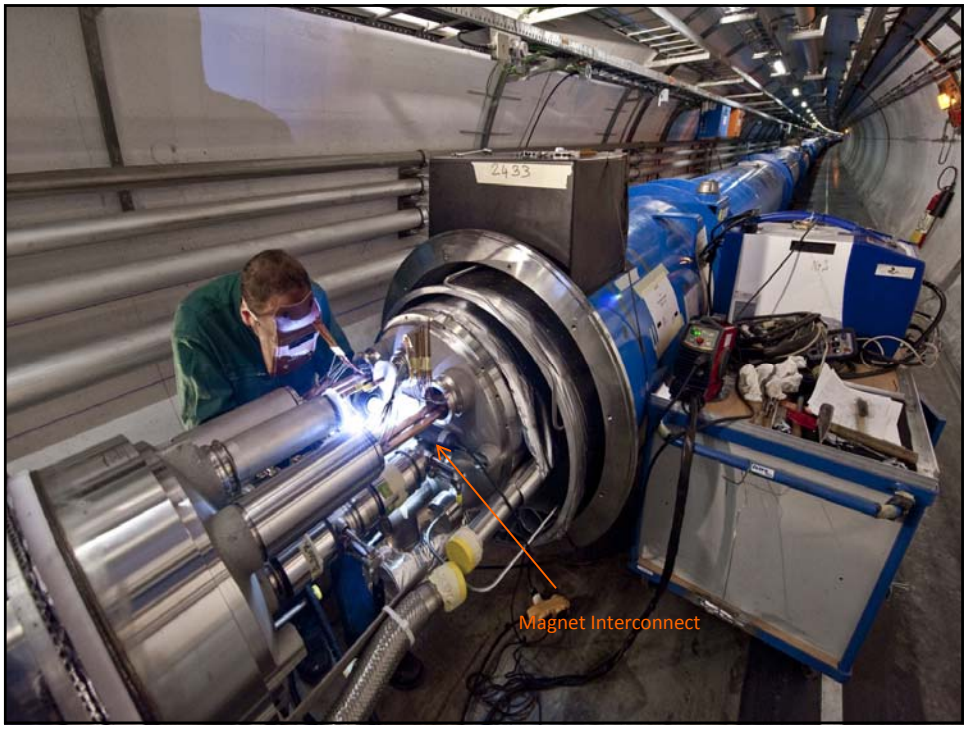
Quench Heater
spreads energy along magnet

Case 1: September 2008

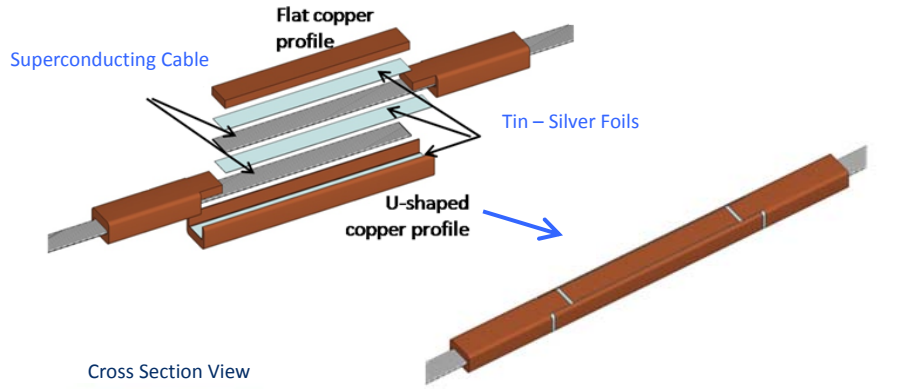
19th September – commissioning last circuit to 5 TeV = 9kA forward current



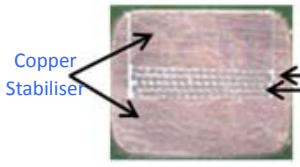
Magnet Interconnect



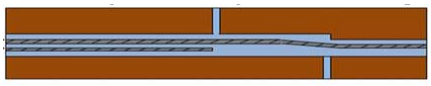
Ideal 13 kA Connection Scheme



Cross Section View

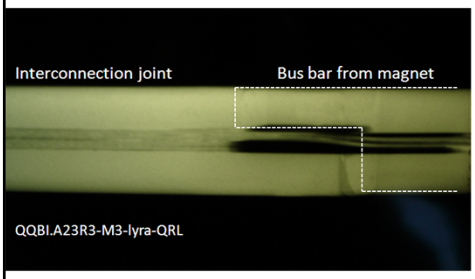


Longditudinal View – filled with Solder

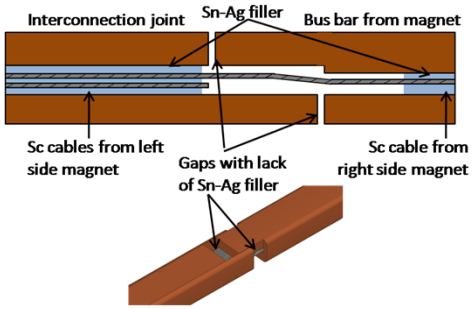


benjamin.todd@cern.ch

Observed Interconnections

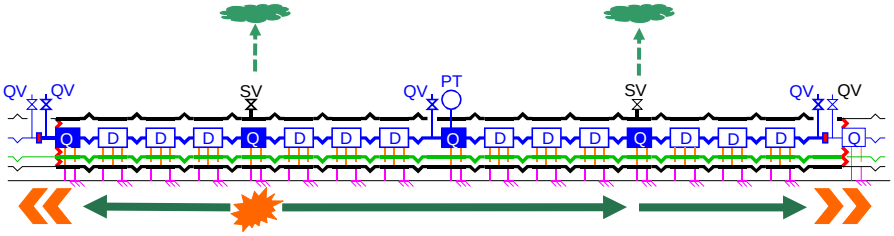


Defective interconnetion-bus bar transition γ-ray picture (left) and scheme (right)



benjamin.todd@cern.ch

Incident and Pressure Wave



1. Pressure Wave propagates inside insulation Vacuum enclosure

2. Rapid Pressure Rise

Self actuating relief valves could not handle pressure

Design: 2Kg He/s Incident: ~20 kg He/s

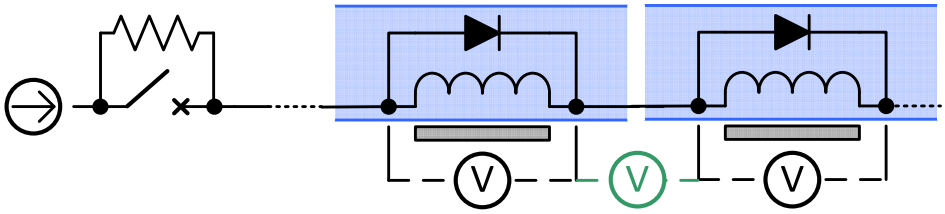
3. Forces on the vacuum barriers (every second cell)

Design: 1.5 bar Incident: ~8 bar

- Several Quadrupoles Displaced by ~50 cm
- Cryogenic line connections damaged
- Vacuum to atmospheric pressure

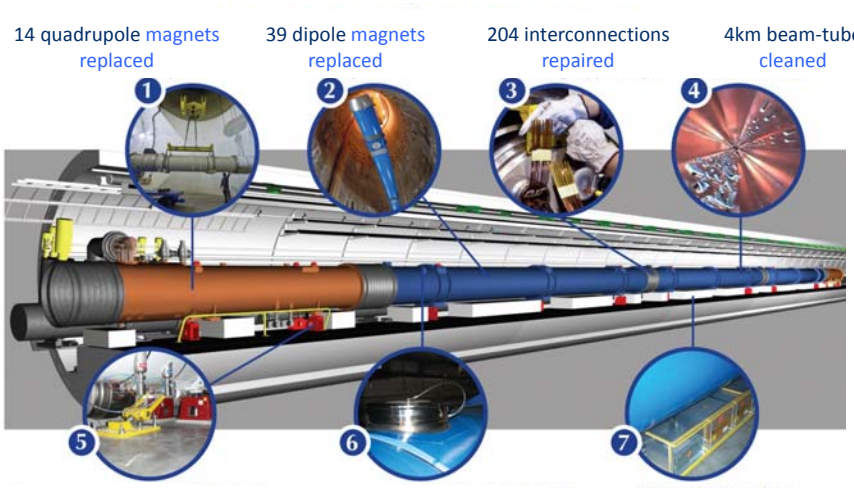
benjamin.todd@cern.ch

Magnet Protection

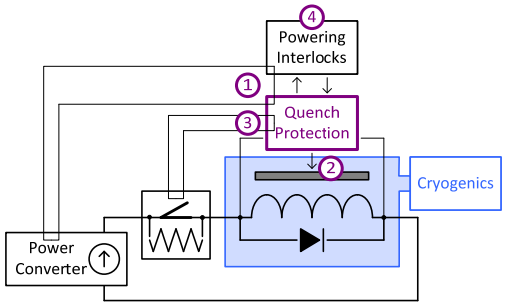


Interconnect impedance is measured
Energy Extracted if impedance unacceptable

2009: LHC repair and consolidation



Failure Case 2: January 2013



quench tests forced a quadrupole magnet quench, all four protection functions failed to activate

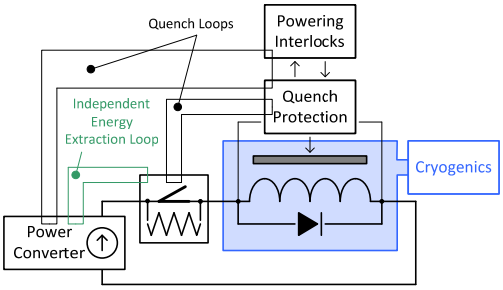
- Six months earlier a thunderstorm tripped several QPS detectors
- Piquet team needed to manually intervene to rearm

Post-Analysis: mitigation of this need by new firmware, piquet did not intervene

- Firmware update was not applied to this particular circuit

Post-Analysis: time and revalidation pressure

- Missing rearm does not prevent the circuit from being powered
- Circuit powered and unprotected for six months
- Event was repeated as failure of protection functions was not identified immediately
- Failure of this nature on dipole circuit represents most critical risk level for CERN.



QPS protection functions have too high a Risk Reduction Level

1. Qualification of QPS Functions

2. Addition of Independent Energy Extraction Loop Study

In Conclusion…

Coming Soon…

Year	Peak Energy [TeV]	Peak Intensity [p]	Peak Luminosity [cm^{-2} s^{-1}]
2010	3.5	4×10^{13}	2.0×10^{32}
2011	3.5	2.0×10^{14}	3.6×10^{33}
2012	4	2.2×10^{14}	7.7×10^{33}
LS_{1-2}	≈6.5	$\approx 3 \times 10^{14}$	$\approx 1 \times 10^{34}$

To Take Away Today

* the protection context is vital
  – need to consider system, machine and organisational level impact

As engineers building power systems, you need to understand how they will be used

* risk analysis is a core part of every engineer's toolbox
  – zero risk does not exist

Qualitatively and quantitatively determine how and how likely things are to go wrong

* specification of protection and interlocks is a compromise
  – they don't add to the function, but are an insurance for when things go wrong.
  – they do add to complexity, so will make the system less reliable.

In the academic – industrial world of HEP, you cannot trust only "it worked in the past"

Specifically If you ask "how reliable is this" and the reply is "great, it never broke down yet".

Take a closer look.

Fin!
Thank You!