Will the Machine Protection System Let LHC Safely Operate?

Roberto Filippini

LHC Machine Protection System Review

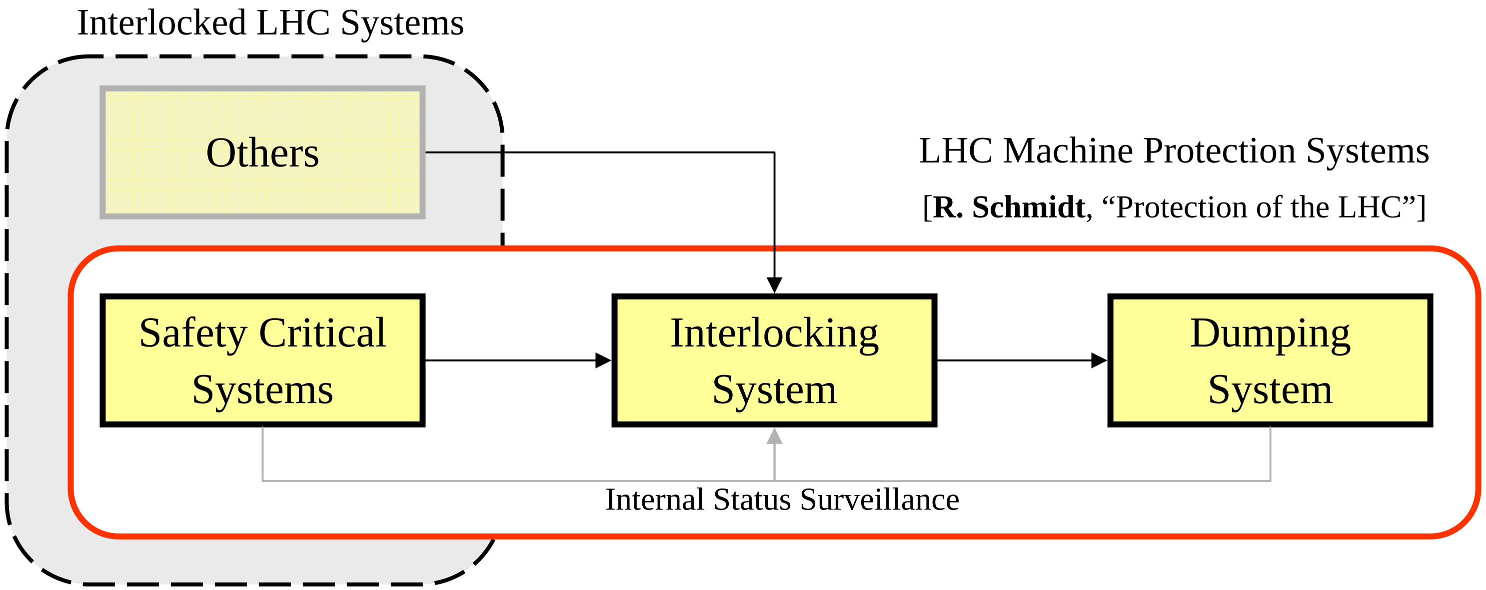
CERN, 11-13 April 2005

Introduction

- **Aims of the presentation**
  - **Safety** of the Machine Protection System (MPS)
    - Probability and equivalent failure rate of the system
  - **Unavailability** of the MPS
    - Number of machine fills aborted due to surveillance within the MPS
- **Topics of the presentation**
  - **MPS modeling aspects**
    - Functional architecture and the studied MPS
    - MPS attributes and design facilities
  - **System analysis**
    - Methodology
    - Results for safety and unavailability
    - Some sensitivity analyses
  - **Concluding remarks**

Modeling Aspects

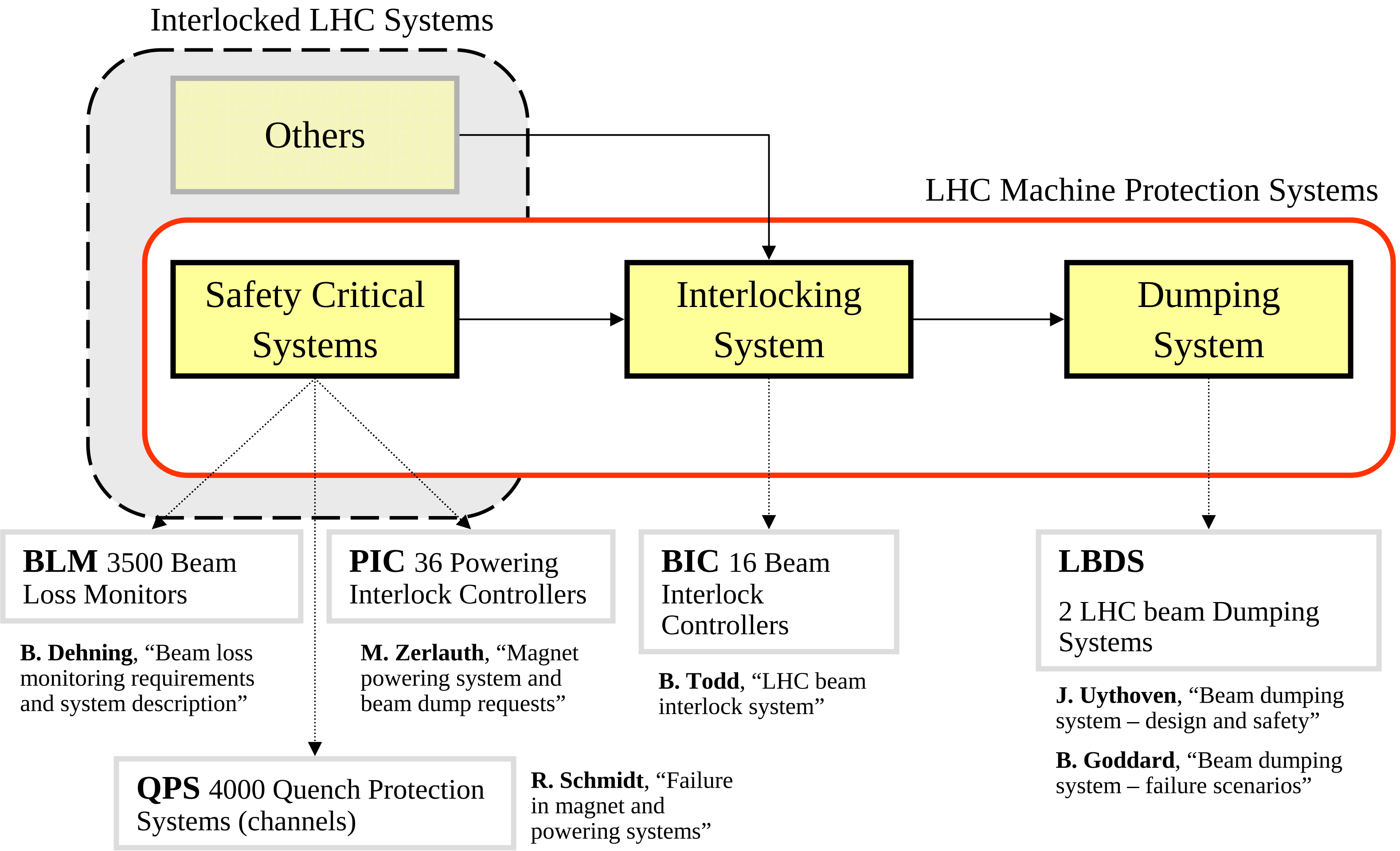
Functional Description of the MPS



- The MPS includes the **safety critical systems** of the LHC
- The other systems send their interlock directly to the interlocking system
- Internal **surveillance** also sends signals to the interlocking system

Modeling Aspects

Functional Description of the Simplified MPS



Modeling Aspects

MPS Tasks and Attributes

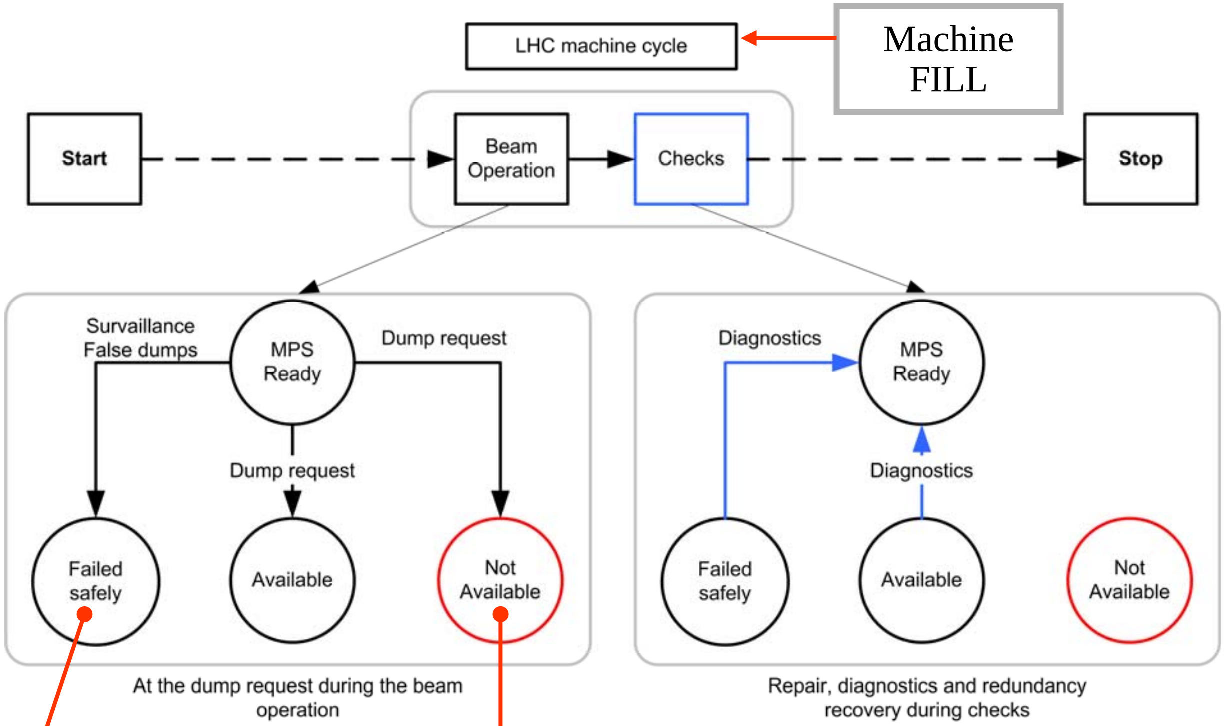
- **The MPS task is to receive and execute:**
  - Planned dump requests from the control room.
  - Unforeseen dump requests due to:
    - Detected beam losses in the LHC.
    - Detected failures in the MPS itself (FALSE DUMPS).
    - Other interlocked systems.
- **The MPS dependability attributes of interest are:**
  - **Safety:** the MPS must be available at request, resulting in a correct execution, and if fails it must fail safely with an operation abort.
  - **Unavailability** due to false dumps: it affects the LHC exploitation.

Safety and unavailability are a trade-off : The safer the system the higher the unavailability

Modeling Aspects

Machine Cycle and Attributes

Machine FILL



System UNAVAILABILITY due to false dumps

System UNSAFETY

Diagnostics and surveillance are **design facilities for safety**

Modeling Aspects

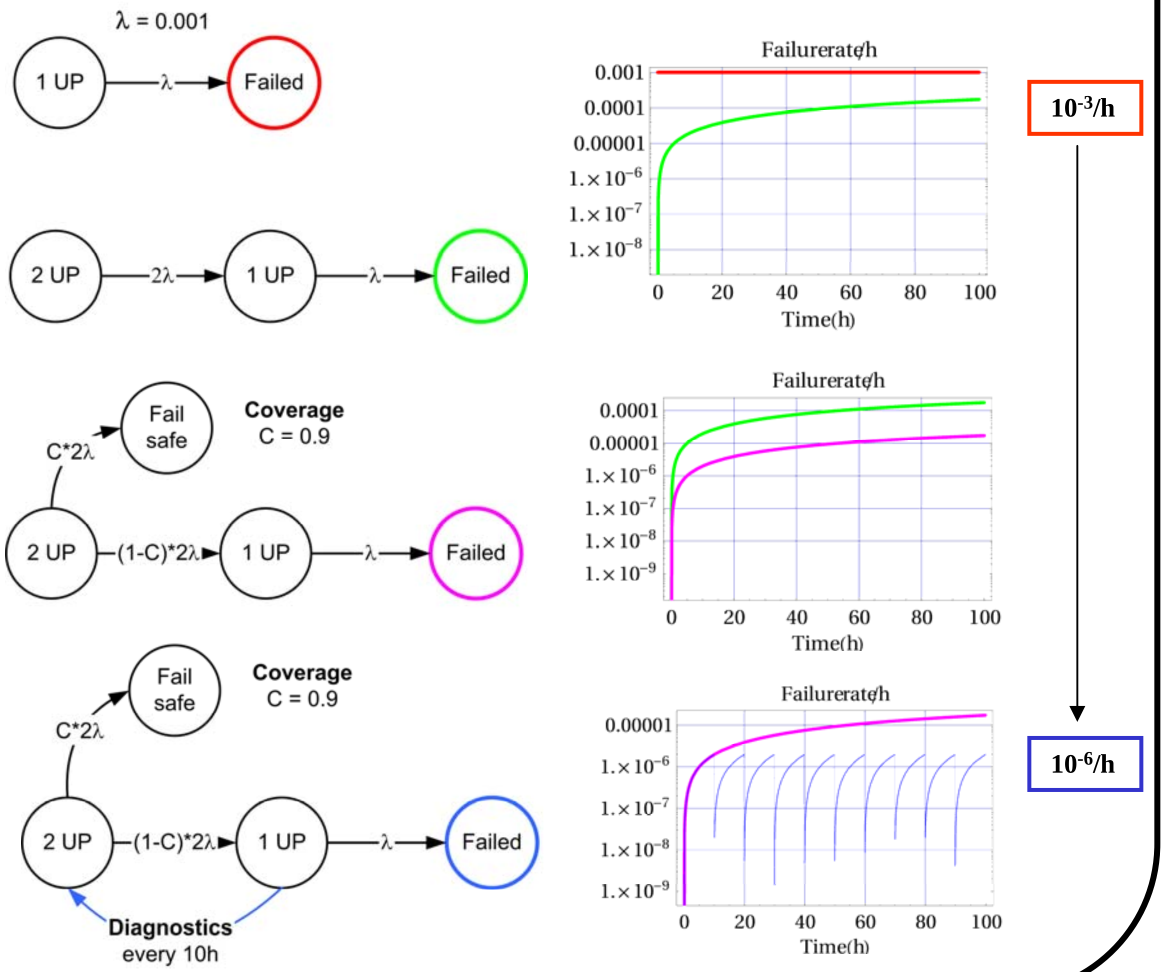
Design Facilities and Consequences

System with failure rate λ

Putting redundancy
“Fault tolerance”

Putting on-line surveillance
“Failsafe modes”

Putting off-line diagnostics
“As good as new”



System Analysis

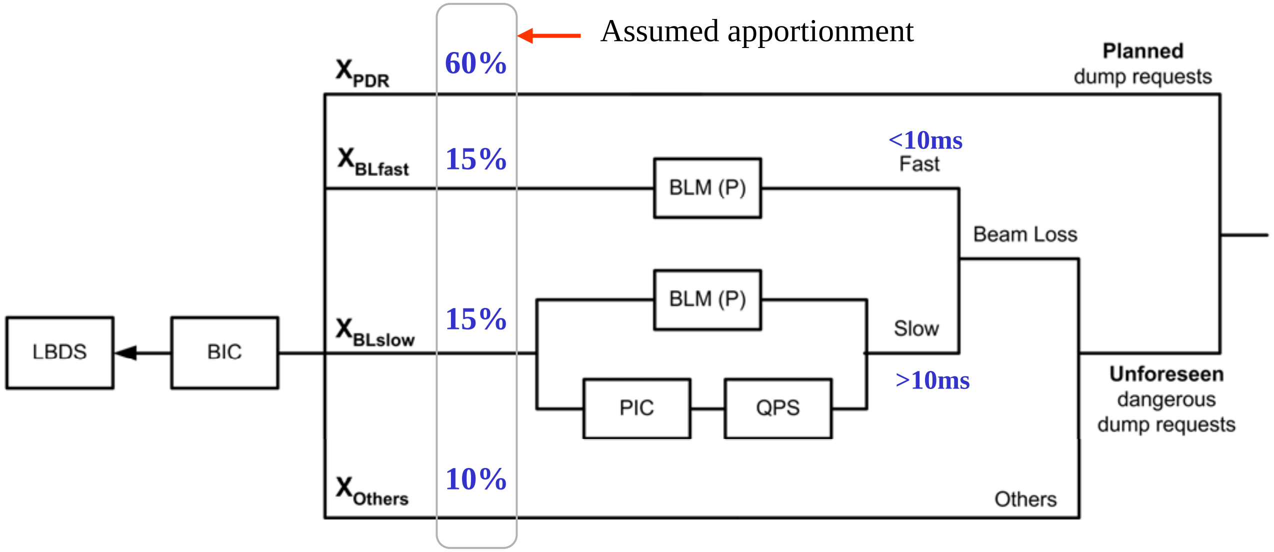
Followed Methodology

- **STEP 1: Separate analysis <u>of each system</u> in the MPS:**
  - Functional architecture and design facilities: redundancy, surveillance and diagnostics ("post mortem").
  - Reliability prediction at component level.
  - Failure Modes Effects and Criticalities Analysis (FMECA).
  - Calculations of unsafety and unavailability (due to false dumps) under identical assumptions.
- **STEP 2: Arrange results <u>in the MPS</u> model:**
  - Dump requests apportionment.
    - The systems demanded at a dump request depend on the type of dump request.
    - <u>Cross-redundancy</u> ⇒ possibility to cover the same event by means of two or more systems in the MPS.
  - Results ⇒ Unsafety and unavailability (due to false dumps) per year.

System Analysis

The MPS Model for Safety Calculation

- **Dump requests** are apportioned per year of operation
- **Cross-redundancy** exists for the beam losses
  - It is internal to the BLM and between the BLM and the QPS
- **Perfect coverage by BLM system** was assumed: All critical failures are assumed to lead to a beam loss [S. Redaelli, "Beam Losses versus BLM locations at the LHC"]



SOURCES of beam losses

User/operator
PC failures
Magnet failures
Collimators failures
RF failures
Obstacles
Vacuum
…

NOTE: False dumps are assumed safe thus they don't enter the model for safety

System Analysis

Assumptions and Results

Operational scenario

200 days/year of operations, 400 beam operations (10h each) followed by checks (2h each)

Diagnostics effectiveness

LBDS and BIC "as good as new" after checks (BLM, partially)

QPS and PIC "as good as new" after periodic inspection or power abort

Dump request apportionment

60% planned dumps

15% fast beam losses

15% slow beam losses

10% others

Cross-Redundancy

No within the Beam Loss Monitors (worst-case)

NOTE: Figures updated from J.Uythoven and R.Filippini, "Will we ever get the green light for beam operation?" Chamonix XIV LHC project workshop, CERN, Geneva 2005.

System	Unsafety/year	False dumps/year Average	Std. Dev.	Analysis including	Not included
LBDS [RF]	1.4×10^{-7} (2X)	2.6 (2X)	(+/-1.6)	(Re-)triggering system, MKD (MIL-217F) BET, BEM (assumptions)	MSD, Q4, MKB TDE
BIC [BT]	1.4×10^{-8}	0.5	(+/-0.5)	User Boxes only (MIL-217F)	BIC core, VME and permit loops
BLM [GG]	1.7×10^{-3}	4.8	(+/-2.1)	Single monitor plus VME electronics (MIL-217F, SPS data)	Design upgrades
PIC [MZ]	0.5×10^{-3}	1.5	(+/-1.2)	Complete system (MIL-217F)	PLC
QPS [AV]	0.4×10^{-3}	15.8	(+/-3.9)	Complete system (MIL-217F)	
OVERALL RESULTS for the MPS					
MPS	2.6×10^{-4}	27.8	(+/-11)		

Equivalent failure rate =

0.65×10^{-7} /h $\Rightarrow$ SIL3 is reached

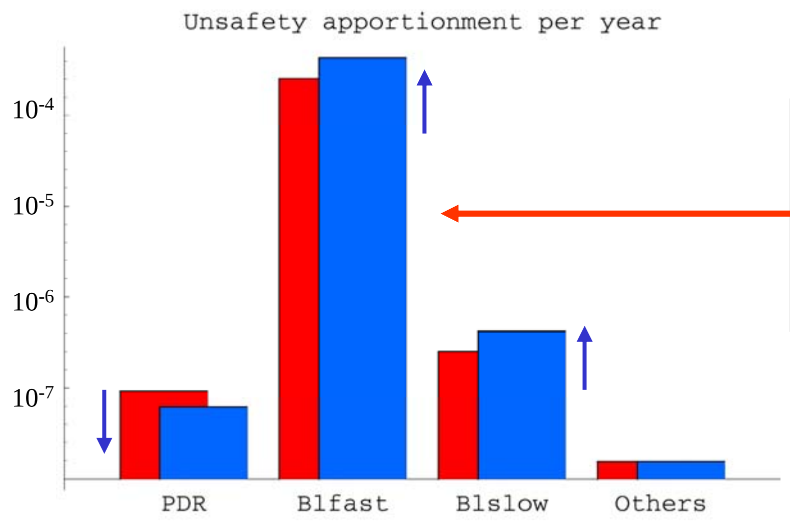
SIL3 = $[10^{-8}, 10^{-7}]$/h [IEC-61508]

Unavailability due to false dumps is **7%**

Sensitivity Analysis

Sensitivity to Dump Request Apportionment

X	(red)	(blue)
PDR	**60%**	**40%**
BL fast	**15%**	**25%**
BL slow	**15%**	**25%**
Others	**10%**	**10%**
UNSAFETY per year	**2.6×10^{-4}**	**4.2×10^{-4}**



Protection to fast beam losses takes the largest contribution to Unsafety

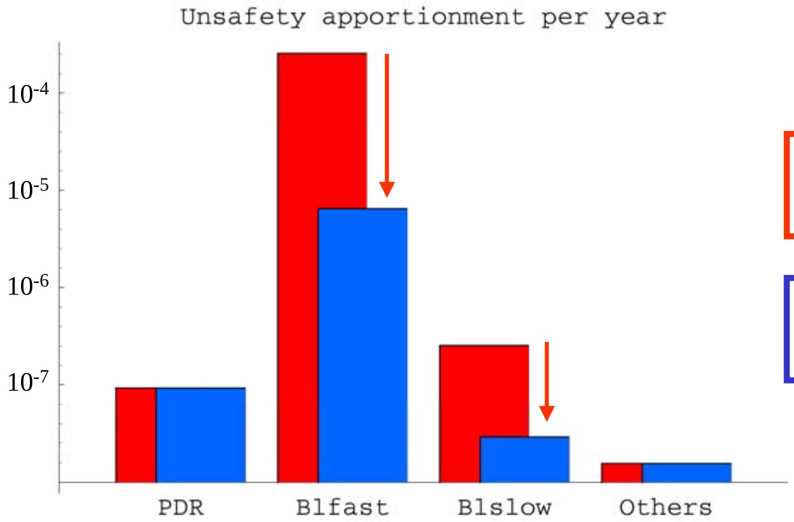
For certain dump requests apportionment and no cross redundancy within BL monitors, the MPS might not be SIL3 [> 4×10^{-4} per year]

Dump requests apportionment affects unsafety, not the false dumps

Sensitivity Analysis

Sensitivity to Cross-redundancy

- **The parameter P** stands for the probability a beam loss is detected with two monitors (connected to the same VME electronics). If we vary P then unsafety will change. Nothing happens for the false dumps.

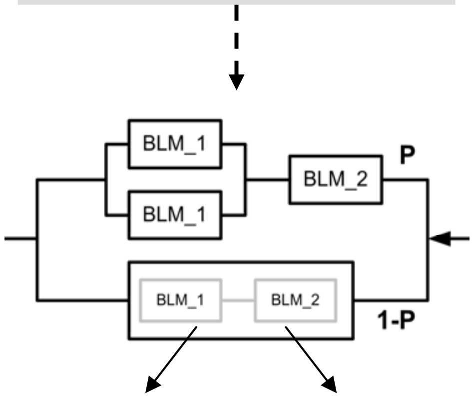


Unsafety = 2.6×10^{-4}
SIL3 is reached

Unsafety = 6.5×10^{-6}
SIL4 is reached

BLM cross-redundancy

P [0,1] is the probability the beam loss affected both monitors



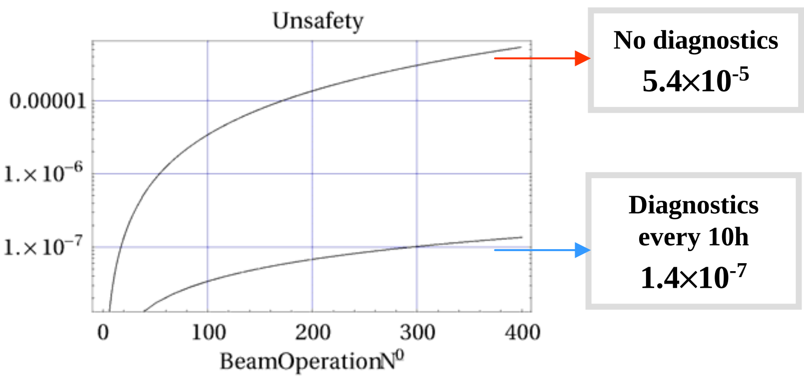
[**G. Guaglio**]

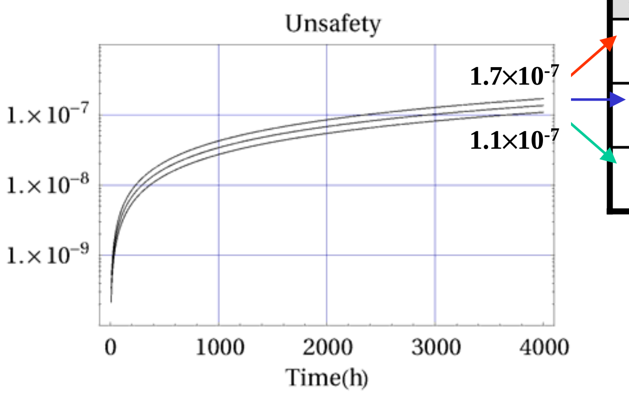
NOTE: The **BLUE** bar is for **P = 1**, while the **RED** bar is for **P = 0**

Sensitivity Analysis

Sensitivities to Other Parameters

- **Sensitivity to diagnostics effectiveness.**
  - Imperfect or no diagnostics means that the system is not recovered “as good as new” after the check.
- **Sensitivities to beam operation length.**
  - The longer runs delay checks and make the systems more prone to failure.
- **EXAMPLE**: The LHC Beam Dumping System.





RUNS /year	Length
320	12.5h
400	10h
500	8h

Concluding Remarks

Safety

- **The probability the MPS will let LHC safely operate depends on the apportionment of dump requests and cross-redundancy.**
  - For the assumed dump request apportionment the **unsafety per year** is:
    - **6.5×10^{-6}** with 100% cross-redundancy within BLM **which is SIL4.**
    - **2.6×10^{-4}** without cross-redundancy within BLM **which is SIL3.**
- **Calculations were based on:**
  - Simplified MPS with some systems needing further analysis.
  - Results refer only to safety with respect to beam losses and planned dump requests.
- **Fast beam Losses are the main concern for safety.**
  - Only beam loss monitors can cover a fast beam loss.
    - For an high rate of fast beam losses and lack of cross-redundancy the MPS is possible not anymore SIL3.
- **Other systems, presently not included, add cross-redundancy for many dump requests**:
  - Beam Current Transformer, Beam Position Monitors, Power converters, etc…

Concluding Remarks
Unavailability Due to False Dumps

- **The number of false dumps per year is 28 [+/-11] (on average).**
  - **7%** of all fills will be aborted due to a false dump.
  - Results are independent from dump requests apportionment and cross-redundancy.
- **Calculations were based on.**
  - About 3500 BLMs, 4000 channels for QPS, 36 PIC, 16 BIC and 2 LBDS.
  - Availability of the LHC also depends on systems outside the MPS.
- **Generally.**
  - Powering systems (power converters) cause the largest fraction of false dumps whose contribution might be overestimated.
    - More then 50% of the false dumps are expected to origin from the QPS. The effect of doubling the PC has been foreseen in the design of QPS: the expected number of false dumps would be halved.

Acknowledgements:

The Machine Protection Reliability Working Group