Reliability of Beam Loss Monitors System for the Large Hadron Collider

LHC Superconductive Magnets

In LHC there are:

514 main quadrupoles (MQ),

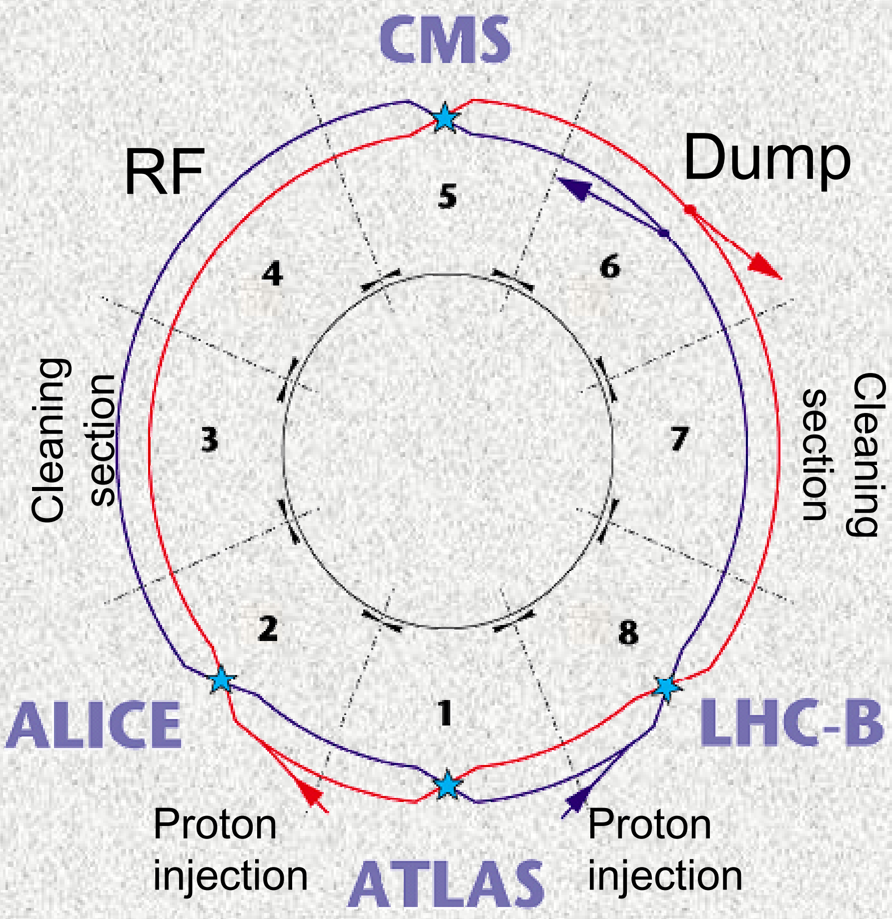
1232 main dipoles (MD).

Favorite loss location: quadrupole and transitions.

We will monitor only the MQ (and some other critical locations):

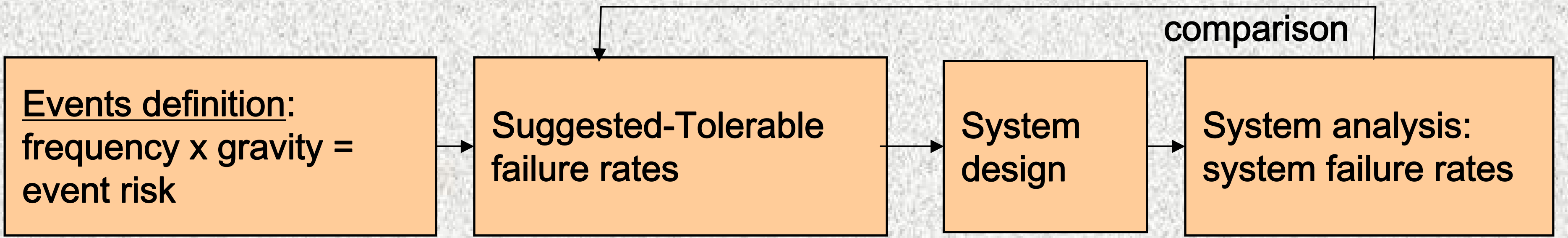
- aperture changes,
- larger beam size,
- most sensitive location to orbit changes.

If losses exceed a threshold, a dump signal is generated.



SIL approach

Safety Integrity Levels (IEC 61508): our guideline for LHC protection systems.



comparison

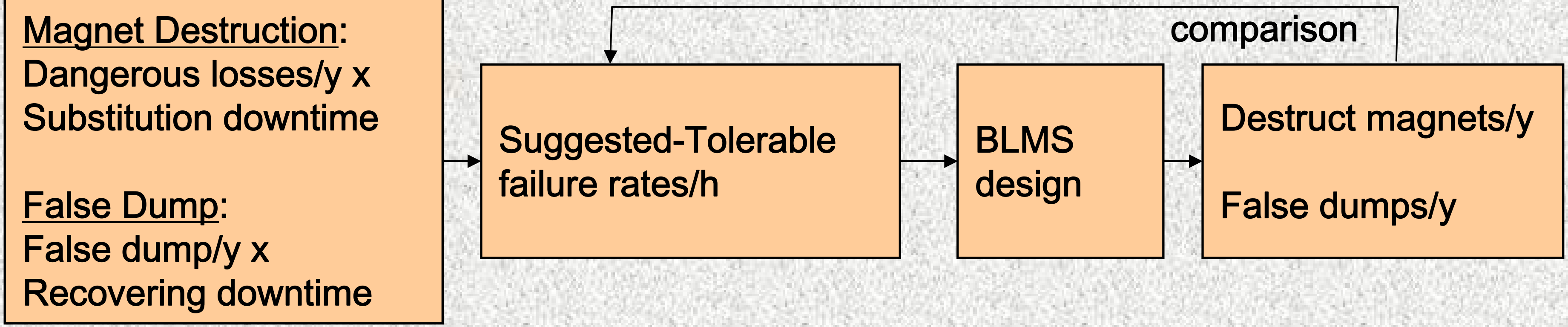
Events definition: frequency x gravity = event risk

Suggested-Tolerable failure rates

System design

System analysis: system failure rates

BLMS case



comparison

Magnet Destruction: Dangerous losses/y x Substitution downtime

False Dump: False dump/y x Recovering downtime

Suggested-Tolerable failure rates/h

BLMS design

Destruct magnets/y

False dumps/y

Events Definition

System fault events

Prevent superconductive magnet destruction (MaDe) due to an high loss (~30 downtime days for substitution).

Avoid false dumps (FaDu) (~3 downtime hours to recover previous beam status).

Frequency

TABLE 1). Frequency table used for LHC risk definition.

Category	**Description**	**Indicative frequency level (per year)**
Frequent	Events which are very likely to occur	> 1
Probable	Events that are likely to occur	10^{-1} - 1
Occasional	Events which are possible and expected to occur	$10^{-2} – 10^{-1}$
Remote	Events which are possible but not expected to occur	$10^{-3} – 10^{-2}$
Improbable	Events which are unlikely to occur	$10^{-4} – 10^{-3}$
Negligible / Not credible	Events which are extremely unlikely to occur	$< 10^{-4}$

Gravity

TABLE 1). Gravity table used for LHC risk definition.

Category	Injury to personnel		Damage to equipment	
	Criteria	N. fatalities (indicative)	CHF Loss	Downtime
Catastrophic	Events capable of resulting in multiple fatalities	≥ 1	$> 5*10^7$	> 6 months
Major	Events capable of resulting in a fatality	0.1 (or 1 over 10 accidents)	$10^6 – 5*10^7$	20 days to 6 months
Severe	Events which may lead to serious, but not fatal, injury	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

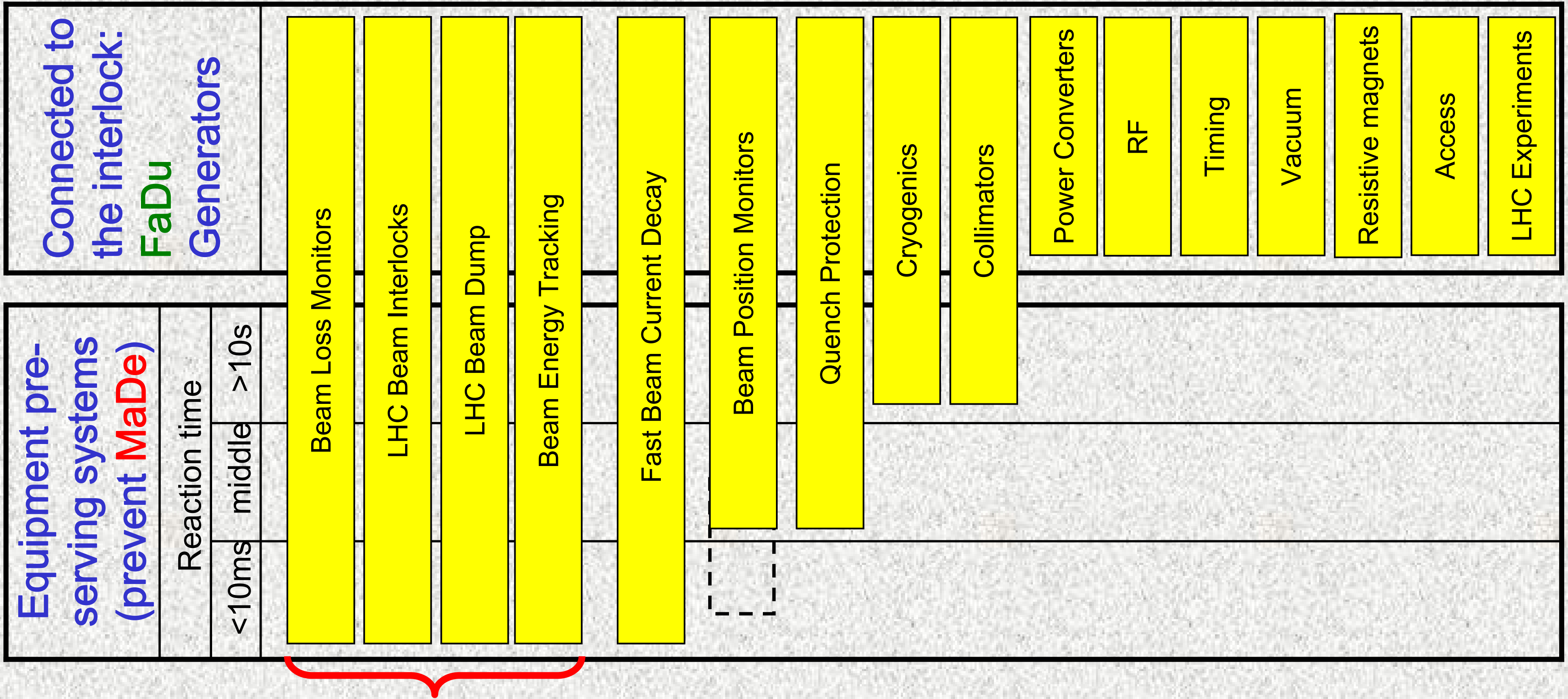
SIL levels and failure rates

Event Likelihood	Consequence			
	Catas-trophic	Major	Severe	Minor
Frequent	SIL 4	SIL 3	SIL 3	SIL 2
Probable	SIL 3	SIL 3	SIL 3	SIL 2
Occasional	SIL 3	SIL 3	SIL 2	SIL 1
Remote	SIL 3	SIL 2	SIL 2	SIL 1
Improbable	SIL 3	SIL 2	SIL 1	SIL 1
Negligible / Not Credible	SIL 2	SIL 1	SIL 1	SIL 1

For high demand / continuous mode of operation systems

SIL	Probability of a dangerous failure per hour
4	$10^{-9} < Pr < 10^{-8}$
3	$10^{-8} < Pr < 10^{-7}$
2	$10^{-7} < Pr < 10^{-6}$
1	$10^{-6} < Pr < 10^{-5}$

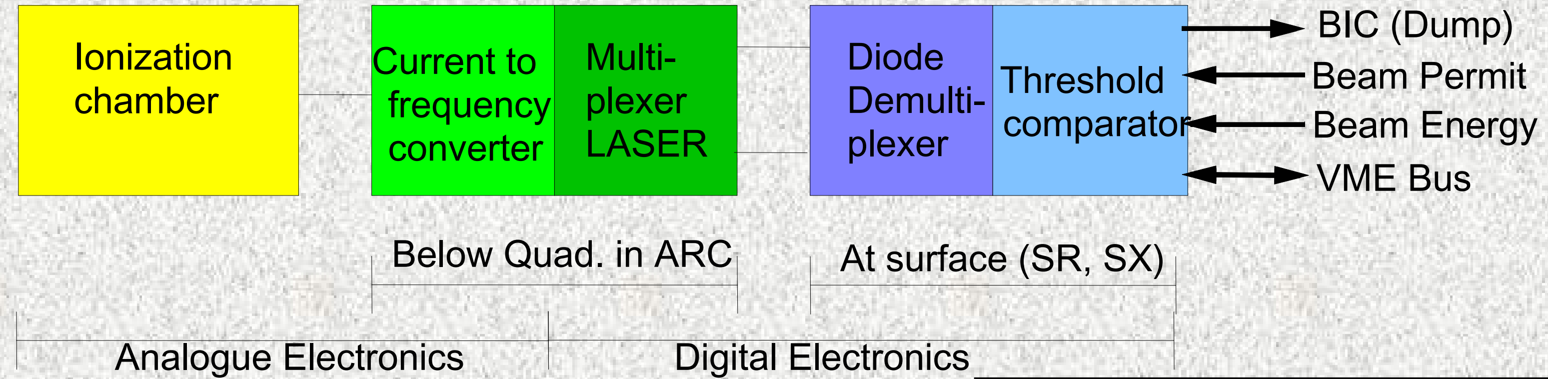
LHC Interlocked Systems



4 first line systems:
$\Sigma \lambda < 1E-7$ /h

~20 dump generator systems: $\Sigma \lambda < 1E-6$ /h

BLMS Overview



Ionization chamber

Current to frequency converter

Multi-plexer LASER

Diode Demulti-plexer

Threshold comparator

BIC (Dump)

Beam Permit

Beam Energy

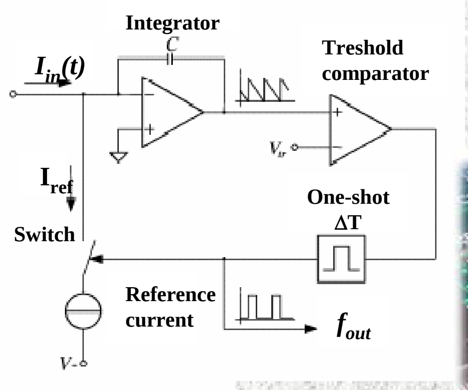
VME Bus

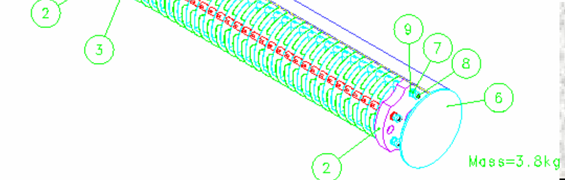
Below Quad. in ARC

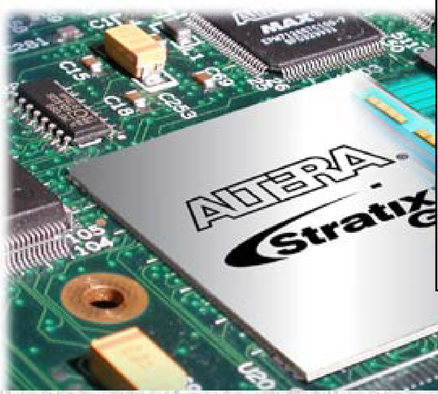
At surface (SR, SX)

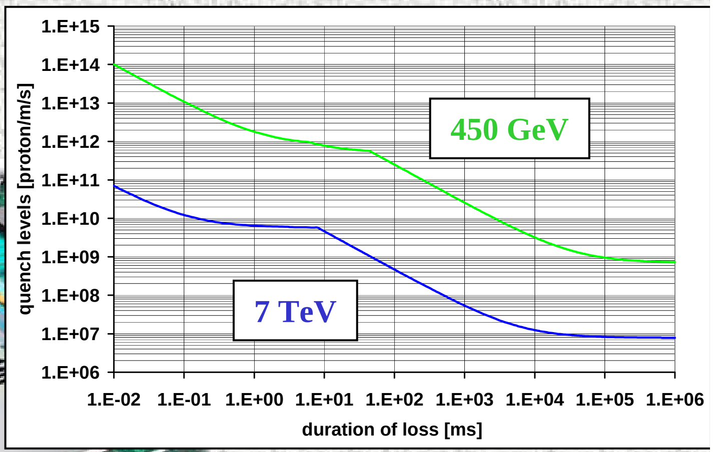
Analogue Electronics

Digital Electronics









Dependability improvements

Fail Safe Design

The design is conceived to generate a normal **status variation** following a fail.

Availability Improvements

Test (continuously, 20 hours and yearly) of detector and analog electronic, to face integral dose degradation; **voting** for digital part, to avoid single event effects.

Reliability Improvements

Actions against the weakest elements : **redundancy** (lasers, CRC, decisions table,…).

Failure Rates

Component	Failure rate λ [10^{-8} 1/h]			Notes	
	Single	Not redundant	Redundant	Inspection interval [h]	General
IC+cable+terminations	2.5	24		20	Experience SPS
Integrator	2.0			Continuous (40 µs)	Dose and fluence tested
Switch	8.7				
FPGA TX*	200	840	0.014		
Laser	510				
2 Optical connectors	20				
Optical fibre	20				
Photodiode	3.2				
FPGA RX*	70				

Reference:MIL-HDBK-217F

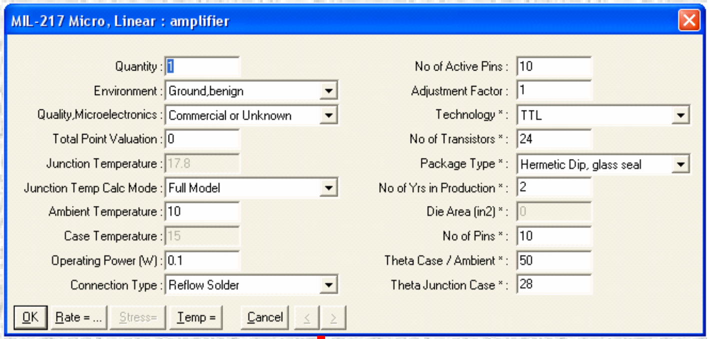
IC calculated with 60% confidence level of no fails over 140 IC in 30 years in SPS

Isograph Reliability Workbench

Component failure rate predictions.

References:

MIL-217 (electronic), Telcordia (telecommunication), IEC (electronic), NSWC (mechanical)



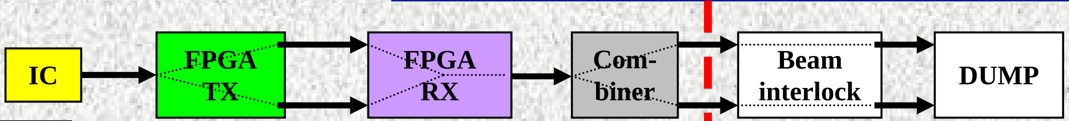
MIL-217 Micro, Linear : amplifier

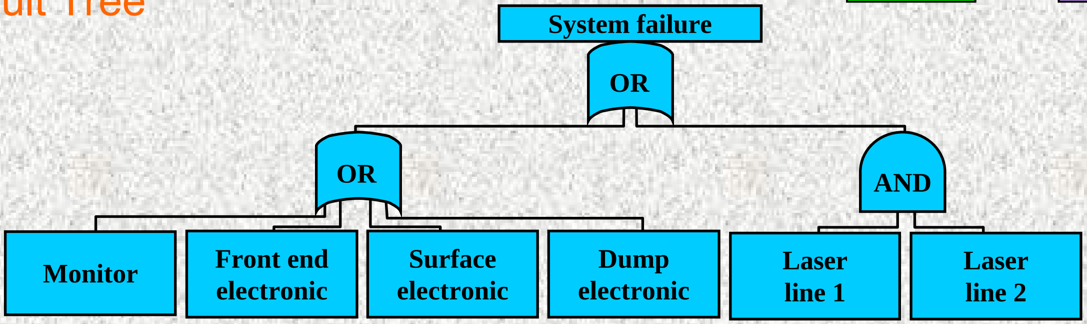
Quantity : 1
Environment : Ground,benign
Quality,Microelectronics : Commercial or Unknown
Total Point Valuation : 0
Junction Temperature : 17.8
Junction Temp Calc Mode : Full Model
Ambient Temperature : 10
Case Temperature : 15
Operating Power (W) : 0.1
Connection Type : Reflow Solder
No of Active Pins : 10
Adjustment Factor : 1
Technology * : TTL
No of Transistors * : 24
Package Type * : Hermetic Dip, glass seal
No of Yrs in Production * : 2
Die Area (in2) * : 0
No of Pins * : 10
Theta Case / Ambient * : 50
Theta Junction Case * : 28

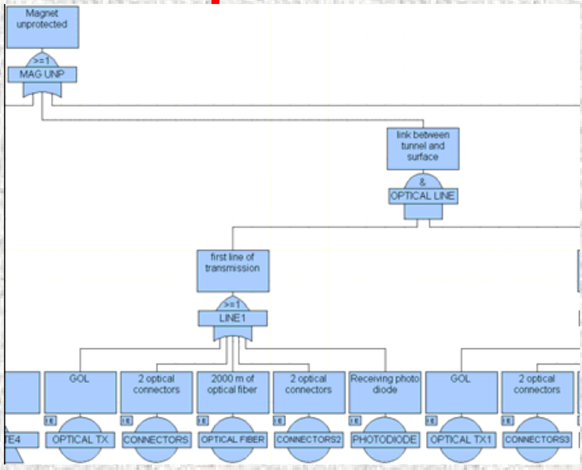
System dependability.

Reliability Block Diagram

Fault Tree







Assembly failure mode.

Failure Mode Effect and Criticality Analysis

FMECA analysis

Block : BLMS

Entry ID	Failure Mode	Contributors
1	Unsafe	1.3 no IC signa, 1.4 wrong IC signal

Block : 1
ID: tunnel installation
Level: 1

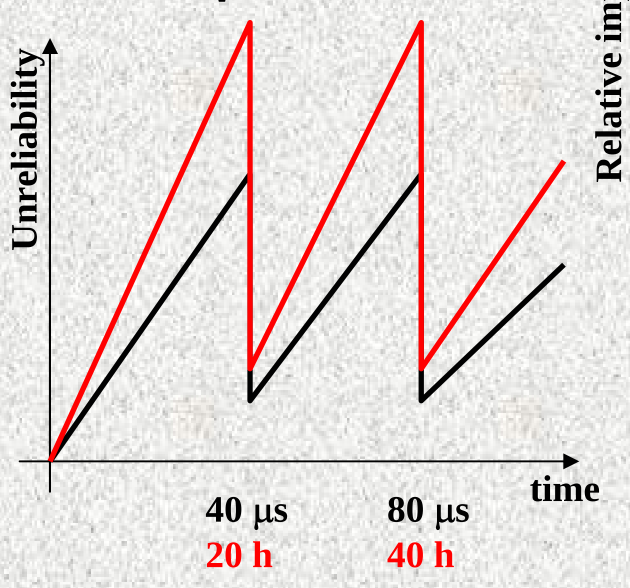
Entry ID	Failure Mode	Contributors		
1.2	wrong HT	1.1.3 Degradation of Insulatio Contact Resistance, 1.1.5 Mi Failure		
1.3	no IC signal	1.2.1 Signal Cable Shorts Mechanical Failure of C		
1.4	wrong IC signal	1.2.3 Degradation of Cable Ins Cable Miscellaneous Mechanical Failures, 1.2.11 IC gas pressure change	mission	more

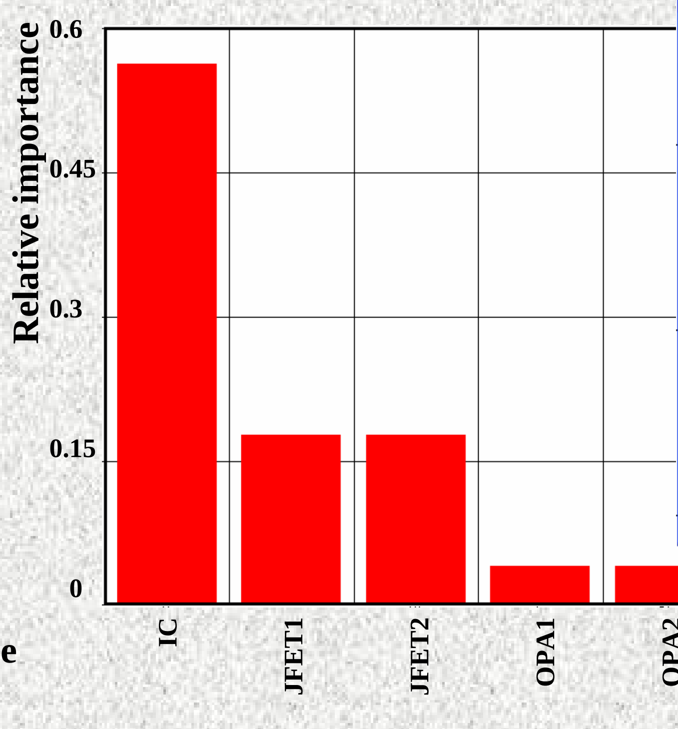
Block : 1.2
Function: Detect loss
ID: IC+cable

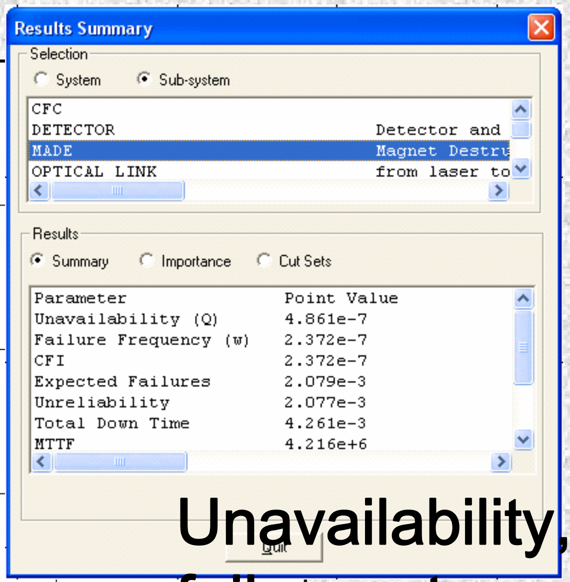
Entry ID	Failure Mode	Effects	End Effects	Detection Method
1.2.1	Signal Cable Shorts (Poor Sealing)	No IC signal	Unsafe mission	HV modulation
1.2.5	CIC Shorted (Electrical)	No HT	False dump	Surface HT status
1.2.11	IC gas pressure change	wrong signal from IC	Unsafe mission	Radiation Source

Importance analysis

Time profiles







```
CFC
DETECTOR                    Detector and
MADE                        Magnet Destru
OPTICAL LINK                from laser to
```

```
Parameter                   Point Value
Unavailability (Q)          4.861e-7
Failure Frequency (w)       2.372e-7
CFI                         2.372e-7
Expected Failures           2.079e-3
Unreliability               2.077e-3
Total Down Time             4.261e-3
MTTF                        4.216e+6
```

Unavailability, failure rate,…

Importance diagram

Results

Foreseen events frequency:

MaDe (single channel): $5.0\ 10^{-7}$/h * 4000 h/y * 100 = 0.2/y

SIL MaDe suggested rate: $2.5\ 10^{-8}$/h

Beam hours: 200 d*20 h/d

"Focused" dangerous losses per years: **pessimistic!**

FaDu (no Power Supply): $2.4\ 10^{-7}$/h * 4000 h/y * 3200 = 3/y

SIL FaDu suggested rate: $5.0\ 10^{-8}$/h

Number of channels

We are beyond the Functional limits, but tolerable for Malfunction approach: good confidence that in 20 year we will lose (less than) the 16 spares magnets and BLMS generate around 3 false dump per year.

Conclusions

1. Probable multi-detection per loss (further simulations on going): MaDe OK.
2. FaDu improving with better electronic components (and better power distribution).
3. The systematic reliability approach guide the BLMS design (redundancies, testing, sensitivity evaluations).