HAL
open science

Reliability of the beam loss monitors system for the Large Hadron Collider at CERN

G. Guaglio

To cite this version:

G. Guaglio. Reliability of the beam loss monitors system for the Large Hadron Collider at CERN. High Energy Physics - Experiment [hep-ex]. Université Blaise Pascal - Clermont-Ferrand II, 2005. English. NNT : . tel-00128836

HAL Id: tel-00128836

https://theses.hal.science/tel-00128836v1

Submitted on 2 Feb 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Numéro d'ordre : DU 1631 PCCF T 0509
EDSF : 473

UNIVERSITÉ CLERMONT FERRAND II – BLAISE PASCAL

T H È S E

pour obtenir le grade de

DOCTEUR DE L'UBP

Discipline : Physique des Particules

préparée au CERN/BDI/BL

dans la cadre de l'**École Doctorale des Sciences Fondamentales**

présentée et soutenue publiquement

par

Gianluca GUAGLIO

le 16 Décembre 2005

Reliability of the Beam Loss Monitors System for the Large Hadron Collider at CERN

Directeurs de thèse :

Claudio SANTONI

Bernd DEHNING

JURY

M. Pierre HENRARD, Président

M. Alain BALDIT

M. Marcel LIEUVIN

M. Paolo PIERINI

M. Rüdiger SCHMIDT

To my
wonderful
wife

ACKNOWLEDGMENTS

My initial gratitude for completion of this thesis has to be dedicated to Federico, who made me aware about the opportunity to participate in this doctorate: with very many thanks for a great experience during the past three years.

Particular thanks to my two supervisors Bernd Dehning and Claudio Santoni: thank you for your patience in teaching me new subjects, for your support, friendship and encouragement during the “hard” times.

I would like to thank most sincerely the professors of the UBP for the opportunity they gave to me and to the members of the board for their availability during my early morning thesis discussion. If I ever have the opportunity to return the favour, I will do so without hesitation.

I also have to thank my English and French friends and colleagues who helped to considerably improve my language skills for this work: Andy, Ben, Chris, Joanne and Laurette. Thank you for your help and patience.

I cannot forget my section colleagues: Barbara, Christos, Claudine, Daniel, Edda, Ewald, Franco, Helge, Ion, Jan, Jonathan, Laurette, Markus, Michael, Raymond, Roman, Stian, Virginia. Apologies if I bothered you with my requests for more reliable components/designs… “LHC, il marchera, un jour”.

Finally, to all my friends at CERN. It is impossible to mention all 270 names in few lines, but I would like to thank each and every one of you. In particular, my Italo-Spanish friends for their welcome, my French course classmates for the laughs we had and the “international evenings”, the USPAS and ESREL mates for the long hours we spent together and the sincere friendship we developed, the colleagues of the RSWG for the hours we “wasted” together and the good teamwork and co-operation, the free-climbing mad guys for the nice evenings we spent together hanging by a rope, my housemates for the “dinners” we had “together”. My warmest and most sincere thanks to you all.

Last but definitely not least, thanks to Diletta (and Maria) for… everything.

CONTENTS

Acknowledgments *5*

Contents *7*

Glossary of the Acronyms *11*

Symbols *15*

Introduction *19*

LHC Project *21*

1.1 Accelerator Description **21**

1.1.1 Accelerators Chain 21

1.1.2 Luminosity 24

1.1.3 Comparison of High Energy Accelerators 25

1.2 LHC Protection System **26**

1.2.1 LHC Beam Dump System 30

1.2.2 LHC Beam Interlock System 32

1.2.3 Beam Loss Monitors System 34

Beam Loss Monitors System *35*

2.1 General Overview **35**

2.2 Threshold Levels **37**

2.2.1 Thresholds Levels Calculation Method 39

2.2.2 Criticalities of the Quench Level Estimates 41

2.3 Monitor Locations **42**

2.3.1 Particle Loss Simulations along the Ring 42

2.3.2 Proton Initiated Secondary Particle Shower 44

2.4 Monitor Properties **46**

2.5 Front-End Electronics **48**

2.5.1 Current to Frequency Converter 48

2.5.2 The CFC Radiation Behaviours 49

2.5.3 Digital Signal Transmission 52

2.6 FEE Alimentation and Ventilation 56

2.7 Back End Electronic 56

2.7.1 The DAB Mezzanine 57

2.7.2 The DAB 58

2.8 Combiner Card 60

2.8.1 Beam Permit Distribution 61

2.8.2 Energy Distribution 61

2.8.3 HT Tests 63

2.8.4 Power Supply Monitoring 64

2.8.5 Inhibition Tests for LBIS 64

2.9 BEE Power Supplies and Ventilations 64

2.9.1 VME Ventilation and Power Supplies 64

2.9.2 HT Power Supplies 65

Reliability Principles 67

3.1 Brief History 67

3.2 Definitions 69

3.2.1 Reliability 70

3.2.2 Maintainability 71

3.2.3 Availability 73

3.2.4 Risk 77

3.2.5 Safety 78

3.2.6 Dependability 78

3.3 Analysis Techniques 79

3.3.1 Hazard Rates Prediction 80

3.3.1.1 International Guidelines for Hazard Rate Prediction 80

3.3.1.2 Laboratory Test 80

3.3.1.3 Real Hazard Rates 84

3.3.2 Failure Modes, Effects and Criticalities Analysis 85

3.3.3 System Analysis 86

3.3.3.1 Combinational Techniques. 86

3.3.3.2 Stochastic Techniques. 89

3.3.3.3 Numeric Methods 90

3.3.4 Safety Evaluations 91
3.3.4.1 Safety Integrity Levels 91
3.3.4.2 As Low As Reasonably Achievable 94

Beam Loss Monitors System Dependability 97

4.1 Hazard Rate Prediction 97

4.2 Testing Processes 101

4.2.1 The BEE Bench Test 101
4.2.2 The FEE Bench Test 102
4.2.3 Combiner Bench Test 102
4.2.4 The 10 pA Test 102
4.2.5 The Barcode Check 102
4.2.6 Double Optical Line Comparison 103
4.2.6.1 Acceptable Bit Error Ratio 104
4.2.7 High Tension (HT) Tests 106
4.2.8 The PC Board (PCB) Test 109
4.2.9 Gain Test 109
4.2.10 Thresholds and Channel Assignment (TCA) Checks 110
4.2.11 Beam Inhibition Lines (BIL) Tests 112
4.2.12 Test Processes Conclusions 113

4.3 FMECA 114

4.4 The Fault Tree Analysis 118

4.4.1 Damage Risk 122
4.4.1.1 Damage Risk Fault Tree Construction 122
4.4.1.2 Damage Risk Results 124
4.4.2 False Alarm Generation 125
4.4.2.1 False Alarm Fault Tree Construction 125
4.4.2.2 False Alarm Results 128
4.4.3 Warnings Generation 130
4.4.3.1 Warning Fault Tree Construction 130
4.4.3.2 Warning Fault Tree Results 131

4.5 Sensitivity Analysis 132

4.6 Underlying Assumptions of Dependability Analysis 140

Conclusions 143

References 147

List of Figures 151

List of Tables 155

Appendix A Quench Levels Calculations 157

Appendix B FMECA 165

Appendix C Fault Tree Diagrams 213

GLOSSARY OF THE ACRONYMS

ADC Analogue to Digital Converter.

ALARA As Low As Reasonably Achievable.

ALICE A Large Ion Collider Experiment.

ATLAS A Thoroidal LHC ApparatuS.

AUG Arrêt d'Urgence General, i.e. emergency general stop.

BEE Back End Electronics. Surface electronics which receives signal from FEE and sends beam inhibition to the Combiner.

BER Bit Error Ratio (or Rate). The number of erroneous bits divided by the total number of bits transmitted, received, or processed.

BIL Beam Inhibition Lines tests.

BLMS Beam Loss Monitors System.

BP BackPlane lines, used for the beam permit transmission in the VME crate.

CERN Conseil Européen pour la Recherche Nucléaire (European Council for the Nuclear Research), former and consolidated denomination of the European Organization for Nuclear Research.

CFC Current to Frequency Converter. First part of the FEE.

CIC Capacitor of the Ionization Chamber.

CMOS Complementary Metal Oxide Semiconductor.

CMS Compact Muon Solenoid.

CPU Central Processor Unit. In the surface VME crate.

CRC Cyclic Redundancy Check. Extra bits added to the data frame to check the transmission correctness.

DAB Data Acquisition Board. Board in the surface, which elaborates the data and ask for a beam inhibition.

DAC Digital to Analogue Converter.

DOLC Double Optical Line Comparison. Testing process of the optical link.

FEE Front End Electronics. It digitises the current and sends it to the BEE.

FMECA Failure Modes, Effects and Criticalities Analysis.

FPGA Field Programmable Gates Array. Digital processor in both surface and tunnel electronics.

$FPPD_{ave}$ Average Failure Probability to Perform a design function on Demand.

FWHM	Full Width Half Maximum.
GeV	Giga-electron-Volt, energy corresponding to 10^9 eV.
GOH	GOL OptoHybrid. Chip for the digital transmission from the tunnel to the surface via optical fibre.
GOL	Gigabit Optical Link. Radiation hard component that serialises, encodes and drives an optical transmitter.
H	Historical data.
HT	High Tension. High tension source for the monitors, also used to generate testing signals.
HTAT	HT Activation Test.
HTLF	HT Low Frequency modulation test.
IC	Ionization Chamber. The monitor.
IP	Interaction Point.
LASER	Light Amplification by the Stimulated Emission of Radiation.
LBDS	LHC Beam Dump System.
LBIS	LHC Beam Interlock System.
LEIR	Low Energy Ions Ring.
LEP	Large Electron-Positron Collider.
LHC	Large Hadron Collider.
LHC-B	Large Hadron Collider Beauty experiment.
LINAC	LINear ACcelerator.
LVDS	Low Voltage Differential Signal.
MCS	Minimal Cut Set.
MIL	Military handbook data.
MIP	Minimum Ionizing Particle.
MO	Octupole Magnet.
PCB	Personal Computer Board. Interface board hosted in a laptop to test the BLMS electronics.
PIS	Power Interlock System.
PS	Proton Synchrotron.
PSB	Proton Synchrotron Booster.
QPS	Quench Protection System.
RF	Radio Frequency.
RIC	Resistor of the Ionization Chamber.

S	Supplier data.
SIL	Safety Integrity Level.
SPS	Super Proton Synchrotron.
SS	Straight Section.
SuSy	Supervising System. Generally indicates a centralized location.
SW	SoftWare.
TCA	Thresholds and Channel Assignment. Indicates tables in the BEE used to compare the signal with the limit and to orient the beam inhibition request for not active, maskable and unmaskable beam inhibition lines.
TCAC	TCA Check. Testing process to test the contents of the Thresholds and Channel Assignment tables.
TCAM	TCA Modification. Procedures to modify the contents of the Thresholds and Channel Assignment tables.
TeV	Tera electron Volt, energy corresponding to 10^{12} eV.
TLK	Input transceiver on the mezzanine card in the Back End Electronics.
TOTEM	TOTal cross section and Elastic scattering Measurement.
VME	VersaModular Eurocard. It is a standard for board and crate design.

SYMBOLS

α_i	FMECA apportionment of the ith element.
α_i^j	Apportionment of ith element for the effect j.
${}^t\alpha_i^{EE}$	Apportionment of ith element for the End Effect EE tested by the test t.
β^*	Betatron function at the interaction point.
γ	Relativistic factor.
$\chi^2_\alpha(\nu)$	100(1-α)th percentile of $\chi^2(\nu, x)$.
$\chi^2(\nu, x)$	Chi-Squared distribution.
ΔE_i	Energy variation between the QL i and i+1.
Δt	Reset period of the CFC.
ε_n	Normalized transverse emittance.
$\lambda(t)$	Conditional failure intensity.
$\hat{\lambda}$	Best constant hazard rate estimator.
λ^*	Equivalent hazard rate.
λ_i	Hazard rate of the ith element.
λ^{EF}	Hazard rate of the effect EF.
${}^t\lambda_i^{EE}$	Hazard rate of the ith element which generate the End Effect EE and is tested by the test t.
$\hat{\lambda}_{LL}$	Lower limit best estimator.
$\hat{\lambda}_{UL}$	Upper limit best estimator.
$\mu(t)$	Conditional repair intensity.
σ_x	Horizontal beam sizes of the Gaussian bunch.
σ_y	Vertical beam sizes of the Gaussian bunch.
τ	Testing period.
A	Accelerator factor.
A(t)	Availability.
c	Tolerance factor for the quench level definition.
C_i	Criticality of the ith element.
C_o	Safe factor in the thresholds level definition.
$C_{l,m}$	Threshold level factor depending on the location and on the magnet.
E_a	Activation energy.
F	Luminosity reduction factor.
f	Revolution frequency.

Symbols

f	Output frequency of the CFC.
f(t)	Failure density.
F(t)	Unreliability.
$f_E'(E_i)$	Finite derivative of the energy function of the quench level.
F_w	Probability that at least one bit in the frame is wrong.
G(t)	Maintainability.
g(t)	Repair density.
I_{in}	Input current in the CFC.
I_{res}	Resetting current in the CFC.
k	Boltzmann constant.
k_b	Number of bunches.
K	Multiplicity factor for redundant gates.
$\mathcal{L}$	Luminosity.
M	Mission time.
m	Number of minimum binomial failures.
MTBF	Mean Time Between Failure.
MTTF	Mean Time To Failure.
MTTR	Mean Time To Repair.
n	Number of elements.
N_i	Number of the ith component.
N_1	Number of particles per bunch in beam 1.
N_2	Number of particles per bunch in beam 2.
N_{bits}	Number of bits in a digital frame.
N_f	Number of frames in the mission.
N_r	Number of redundancies in a parallel branch.
P_F	Probability to generate a false alarm for BER in the BLMS.
O_c	Number of optical channels in BLMS.
$q(t)$	Unavailability of an element in a binomial ensemble.
Q(t)	Unavailability.
Q^{2oo3}	Unavailability of an 2oo3 gate.
Q^{AND}	Unavailability of an AND gate.
Q_{BIN}	Binomial unavailability.
Q_D^{MAX}	Maximum dormant unavailability.
$\overline{Q}_D$	Average dormant unavailability.
Q_{DR}	Probability that a dangerous loss is not detected.
Q^{EE}	Unavailability of the End Effect EE.
Q_i^{MCS}	Minimal Cut Set unavailability.

Q_{ij}^{*}	Mixed cut-set unavailability.
Q^{OR}	Unavailability of an OR gate.
Q^{s}	System unavailability.
Q^{XOR}	Unavailability of an XOR gate.
QL	Quench Level.
Q_{tol}	Tolerated unavailability.
r	Number of failures in a test.
r(t)	Hazard rate.
R(t)	Reliability.
r_E	Energy change rate.
R_w	Probability that N_r redundant system fails.
${}^{j}S^{EE}$	Severity of the End Effect of the jth failure mode.
S_i^{EE}	Sensitivity index of the ith components for the End Effect EE.
${}^{t}S^{EE}$	Sensitivity index of the tth test for the End Effect EE.
T	Test time.
t_i	Time to failure of the ith element.
T_o	Operative temperature.
T_t	Test temperature.
${}^{t}t$	Inspection period of the test t.
Th_i	Threshold level of the ith monitor.
$Th_m(E, d)$	Threshold level function depending on magnet class, the energy of the beam and the loss duration.
V(0,t)	Numbers of repairs.
v(t)	Unconditional repair intensity.
W(0,t)	Numbers of failures.
w(t)	Unconditional failure intensity.
w^{2oo3}	*w(t)* of an 2oo3 gate.
w^{AND}	*w(t)* of an AND gate.
$\overline{w}_D$	Average dormant *w(t).*
w^{OR}	*w(t)* of on OR gate.
w_{BIN}	Binomial *w(t).*
w_i^{MCS}	Minimal Cut Set *w(t).*
w^{s}	System *w(t).*
w^{XOR}	*w(t)* of on XOR gate.

INTRODUCTION

The LHC (Large Hadron Collider) is the next circular accelerator that is going to be constructed at CERN (Conseil Européen pour la Recherche Nucléaire) for high energy particle physics research. The accelerator is designed to accelerate and collide protons and heavy ions at energies of 7 TeV per charge. Such energies have never been reached in an accelerator before.

In order to achieve the required 8.4 T magnetic field strengths, superconducting magnets will be employed and they will be cooled down to a temperature of 1.8 K using superfluid helium.

The energy stored in the superconducting magnets is unprecedented: 10 GJ in the electrical circuits and 724 MJ in the circulating beams. It can potentially cause severe damage to the magnets, which cost around 350,000 € each, and necessitate a month's downtime to substitute a single one. Considering their large number, 502 quadrupoles and 1232 dipoles magnets, the importance of the reliability of the machine protection system becomes evident. The magnets could be damaged either by an uncontrolled dispersion of the stored magnetic energy or by the impact of the particles on the magnet structures.

The Beam Loss Monitors System (BLMS) detects the beam losses. In case of dangerous loss, the system initiates the extraction of the beam before any serious damage to the equipment could occur.

The aim of this thesis is to define the BLMS specifications in term of reliability. The main goal is the design of the system minimizing either the probability to not detect a dangerous loss or the number of false alarms generated.

In this thesis, methodical uncertainties have been investigated. Uncertainty sources are the evaluation of the thresholds levels and the location of the losses along the ring. The functional dependencies of the threshold values have been critically modelled and the order of the uncertainty has been evaluated. Interpreting the spatial loss patterns, further studies have been initiated to define the optimal coverage of the loss location by the BLMS.

The schematics and the prototypes of the BLMS have been analysed. Irradiation tests have been performed on the components of the front end electronics to evaluate their behaviour during the LHC operations. Critical components and subsystems have been identified. Improvements have been proposed, like the use

of a more reliable components or the introduction of redundancies in the system. Testing procedures have been defined to be applied during either the installation or operation phase. The reliability goals are only achievable with frequent testing procedures.

To evaluate the BLMS behaviour, reliability theory and state-of-the-art methods have been employed. The reliability figures of the system have been evaluated using a commercial software package (Isograph™). The probability of damage a magnet, the number of false alarms and the number of generated warnings have been derived with a fault tree analysis. The model has been implemented to be easily modified and updated. The weakest components in the BLMS have been pointed out. The effect of the variation of the parameters on the main figures of the system has been evaluated too.

The LHC's characteristics, main challenges and motivations are presented in chapter 1. Particular attention will be given to the systems in charge of the accelerator protection.

The resulting specifications and a detailed description of the BLMS components are set out in the chapter 2. Each subsystem is described in detail, focusing on the elements which are critical from the reliability point of view.

In chapter 3 the reliability theory and techniques used in this work are illustrated. A didactical approach has been used to introduce the terminology and the methodology utilized in the analysis.

The prediction of the hazard rates, the failure mode analysis, the fault tree analysis and the sensitivity analysis are illustrated in chapter 4. The effect of the proposed improvements is evaluated as well. A discussion about the assumed hypothesis is contained in the last section.

Finally, in chapter 5, the conclusions will be drawn.

Chapter 1

LHC PROJECT

1.1 Accelerator Description

1.1.1 Accelerators Chain

The Large Hadron Collider (LHC) will be the largest and most advanced particle accelerator, not only at CERN, but also in the world. A circular tunnel, almost 27 km in circumference and at an average of 100 m underground below the French and Swiss territories, will house the accelerator, which replaces the old Large Electron-Positron collider (LEP). The LHC consists of two concentric rings, as shown in figure 1.1, crossing at 4 Interaction Points (IP). ATLAS, ALICE, CMS and LHC-B are the detectors located at the IPs [1-5].

A long and complex chain of accelerators is used at CERN. A schematic view of

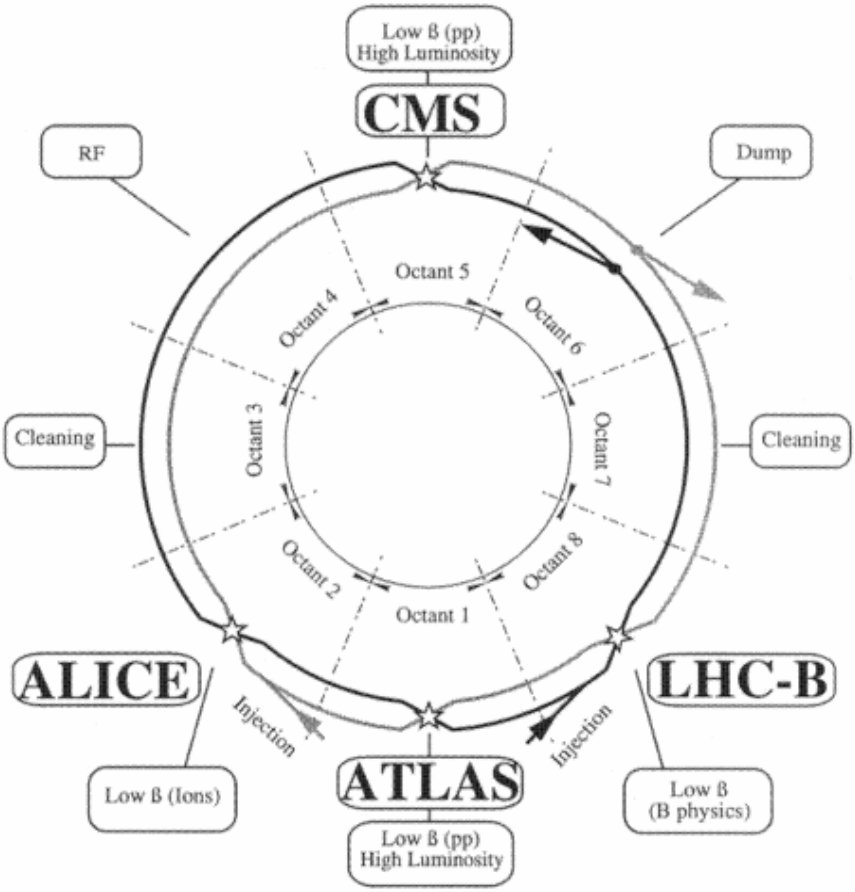


Figure 1.1: The LHC and octants destinations.

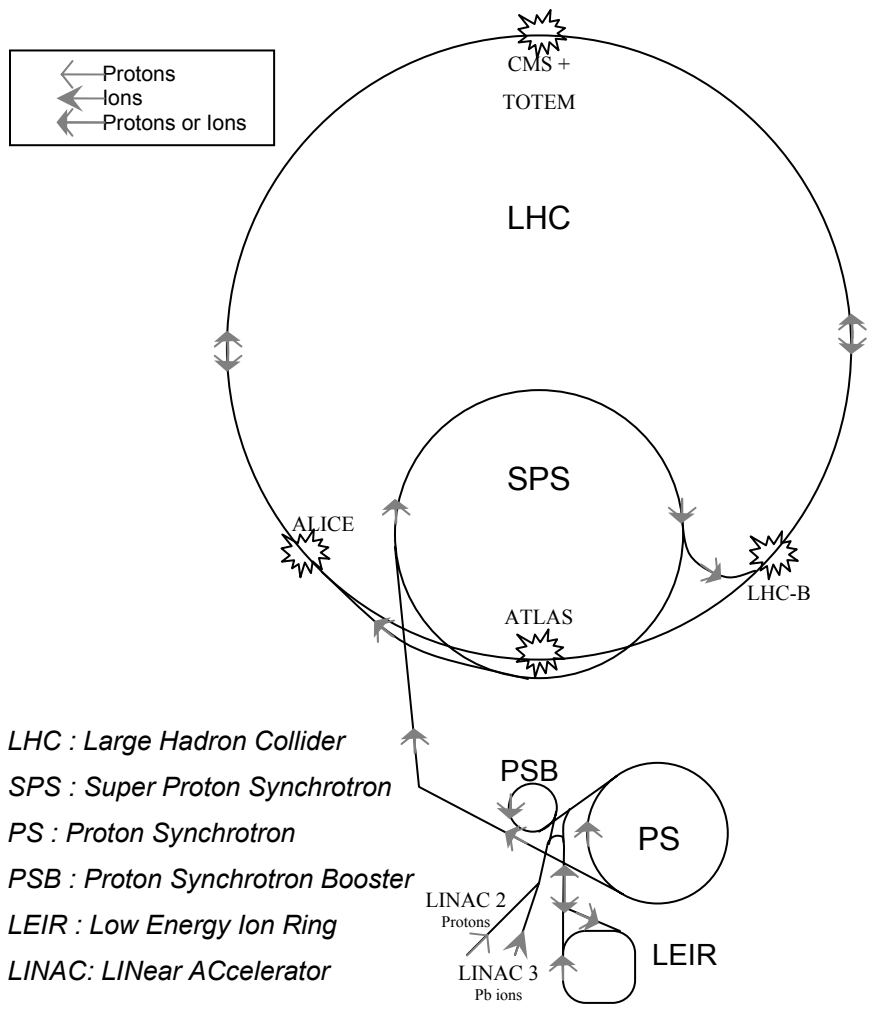


Figure 1.2: CERN accelerator complex, not in scale.

the whole system is given in figure 1.2.

The acceleration process for the bunches of hadrons follows different steps.

They are first accelerated in a LINAC (LINear ACcelerator): LINAC 2 is designed for protons and LINAC 3 for ions. The acceleration takes the energy up to 0.05 GeV per charge. Each LINAC is roughly 80 m long. Each pulse has a length that can last from 20 to 150 μs. This bunch could be sent either to the PSB or to the LEIR.

If the hadrons are accumulated in the PSB (Proton Synchrotron Booster), they are accelerated up to 1.4 GeV per charge. The diameter of the PSB is 160 m.

If not accumulated in the PSB, the hadrons are stored in the LEIR (Low Energy Ions Ring) where the beam a radial density is compacted by an electronic cooling system and accelerated up to 1.4 GeV per charge. LEIR is a ring of 25 m in diameter.

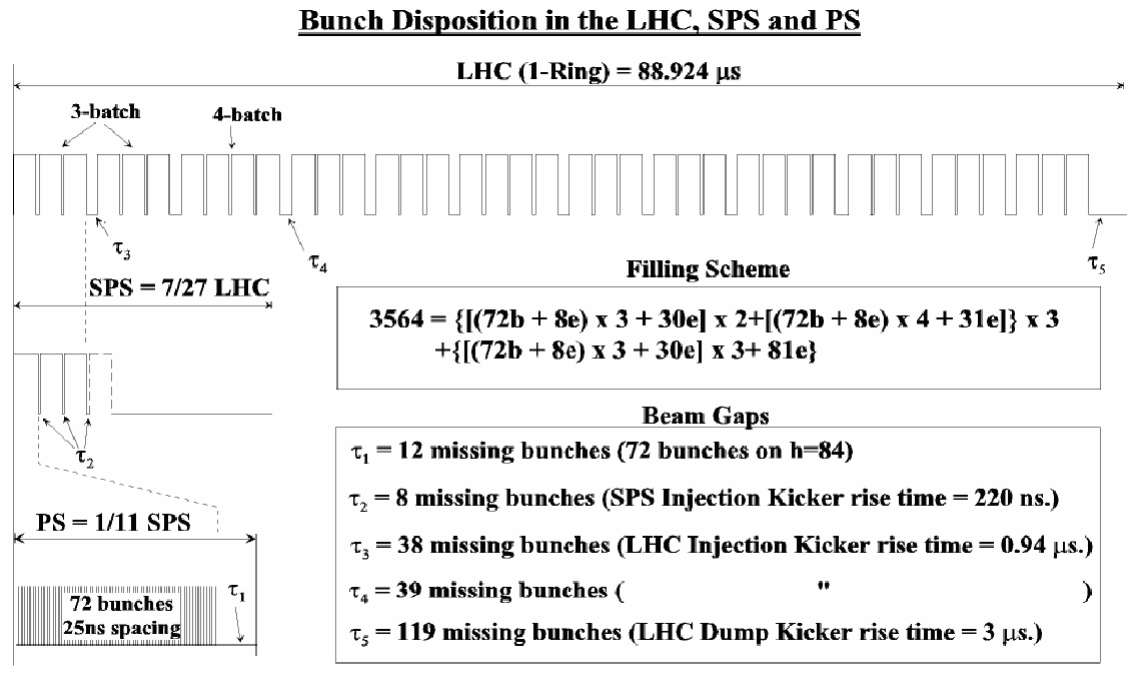


Figure 1.3: Reference filling pattern of the LHC.

The beam is then injected into the PS (Proton Synchrotron) and accelerated up to 25 GeV per charge. The diameter of PS is 200 m. Each bunch is split into 6 by the radiofrequency cavities modulation to create final bunches of 2.5 ns in length, every 25 ns. The PS can be filled by 84 bunches but only 72 are used and define the PS batch. The gap of 12 bunches, corresponding to 320 ns, is preserved for the rise time of the kicker magnet which permits the extraction from PS.

The PS batch is injected into the SPS (Super Proton Synchrotron) and accelerated up to 450 GeV per charge. The diameter of SPS is 2.2 km. It is filled with 3 or 4 PS batches separated by a space equivalent to 8 bunches and, at the end, an extra gap of 30-31 bunches to give a final gap of 38-39 bunches, i.e. 950-975 ns for the extraction magnet rising time.

Finally the hadrons are injected into the LHC and accelerated up to 7 TeV per charge. The diameter of the LHC is 9 km. The final beam structure is given by a pattern of 3 and 4 batches as shown in figure 1.3, with a final gap of 127 bunches for the 3.2 μs extraction kicker rising time.

At the end of the filling process the LHC will contain 39 PS batches giving a total of 2808 bunches of 1.2 10^{11} protons each. This structure is used for the particle beams of both LHC rings.

1.1.2 Luminosity

The discovering potential of a storage ring is proportional to the particle production rate. This rate $\dot{n}$ is expressed as the product of the particle cross section σ and the accelerator parameter luminosity $\mathcal{L}$:

$$\dot{n} = \mathcal{L} \cdot \sigma \ . \qquad (1.1)$$

The cross section is a measure of the probability of interaction of two particles, and the luminosity describes the particle beam characteristics:

$$\mathcal{L} = \frac{N_1 \cdot N_2 \cdot k_b \cdot f}{4\pi \cdot \sigma_x \cdot \sigma_y} F \ , \qquad (1.2)$$

where $\mathcal{L}$ is the luminosity; N_1 and N_2 are the number of hadrons per bunch in the beam 1 and 2; k_b is the number of bunches; f is the revolution frequency; σ_x and σ_y are the transversal beam sizes of the Gaussian bunch in the horizontal and vertical planes and F is a reduction factor caused by the crossing angle of the two beams.

The beam-beam interaction leads to an increase in transversal momentum of some particles. This effect increases at each turn the number particles that could impact on the vacuum chamber wall. Such particles are intercepted by collimators in order to avoid particle losses in the superconducting magnets. An efficient LHC operation is therefore limited to a beam lifetime of 18.4 hours. In the following, an average duration of the fill of 10 hours will be used. The mission time will be such period plus two hours for the refilling.

Table 1.1 summarises the values for the nominal operations at top energy.

		Nominal
Number of protons per bunch $N_1 \sim N_1$		$1.15\ 10^{11}$
Number of bunches k_b		2808
Revolution frequency f	[kHz]	11.2455
Transversal beam sizes $\sigma_x \sim \sigma_y$	[μm]	16.7
Reduction factor F		0.899
Luminosity $\mathcal{L}$	[$cm^{-2}\ s^{-1}$]	10^{34}
Beam current lifetime	[h]	18.4
Loss rate at collimator	[protons/s]	$4\ 10^{9}$

Table 1.1: Luminosity parameters at 7 TeV.

1.1.3 Comparison of High Energy Accelerators

If the LHC is compared with other existing accelerators, it can be seen that several parameters are increased by orders of magnitude.

As depicted in figure 1.4, the operative energy is almost 10 times than of other colliders and the stored beam energy is 200 times higher (see table 1.2 for the correct figures).

Proton Energy	[GeV]	450	7000
Number of protons per bunch N_b		$1.15\ 10^{11}$	
Number of bunches k_b		2808	
Circulating beam current	[A]	0.581	
Stored energy per beam	[MJ]	23.3	362

Table 1.2: Some LHC beam parameters.

To keep these high energy particles on a circular orbit with a given radius, strong magnetic fields are needed. To generate these fields, superconducting magnets are used. Although other accelerators using superconducting technology have been built and work well (e.g. Tevatron, HERA, RHIC), the LHC is a much more advanced accelerator. Its success will not only be defined by the two classic objectives in a high energy particle accelerator, high energy and high luminosity,

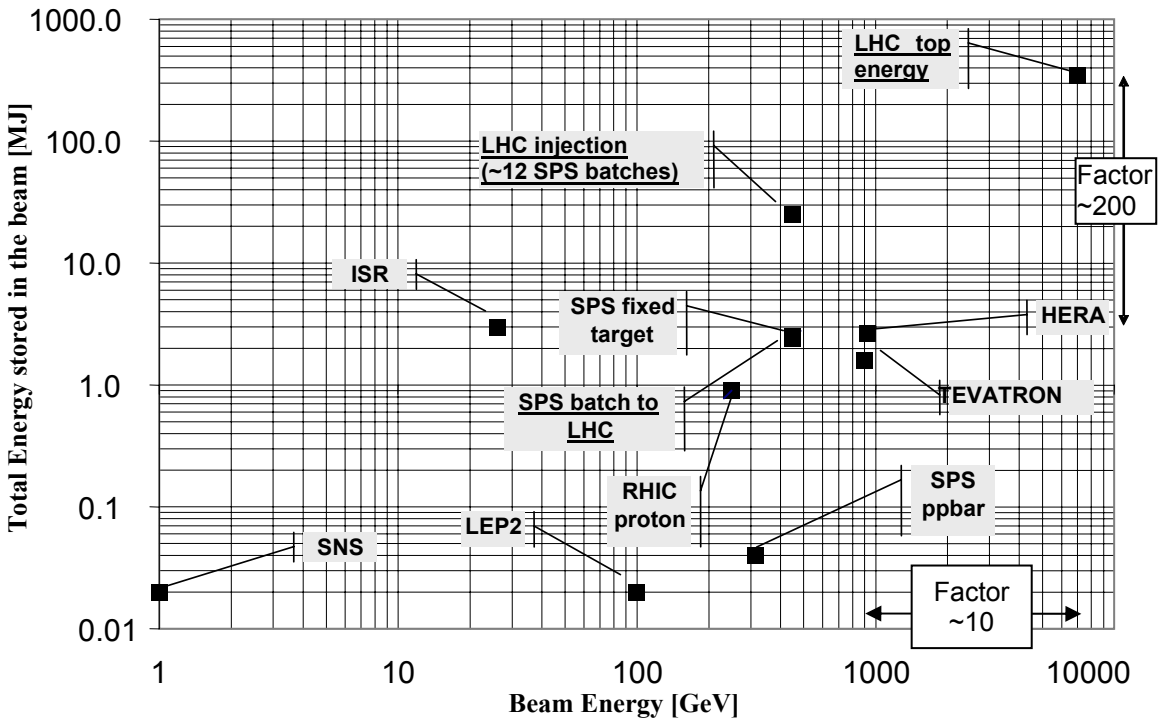


Figure 1.4: Accelerator Beam and total Energy comparison.
Courtesy of R. W. Assmann.

but also by its reliability and availability performance.

1.2 LHC Protection System

The energy stored in the electrical circuits during the LHC operation is over 10 GJ and the total energy of one beam is 362 MJ [6, page 3]. This stored beam energy could melt 589 kg of copper, corresponding to a cube that is 40 cm on a side, and if all the energy stored in the magnetic circuits of the LHC were released, it would be able to melt a copper cube 1.25 m on a side [7].

The most critical components in the accelerator are the superconducting magnets which also store the largest portion of the energy in the form of a magnetic field.

A critical failure of the superconducting magnets would be the transition to a normal resistive state.

The LHC superconducting magnets are made of NbTi coils that perform as shown in superconducting phase diagram in figure 1.5. NbTi is superconducting if it is in a state below the depicted surface, called the critical surface. The state is defined by

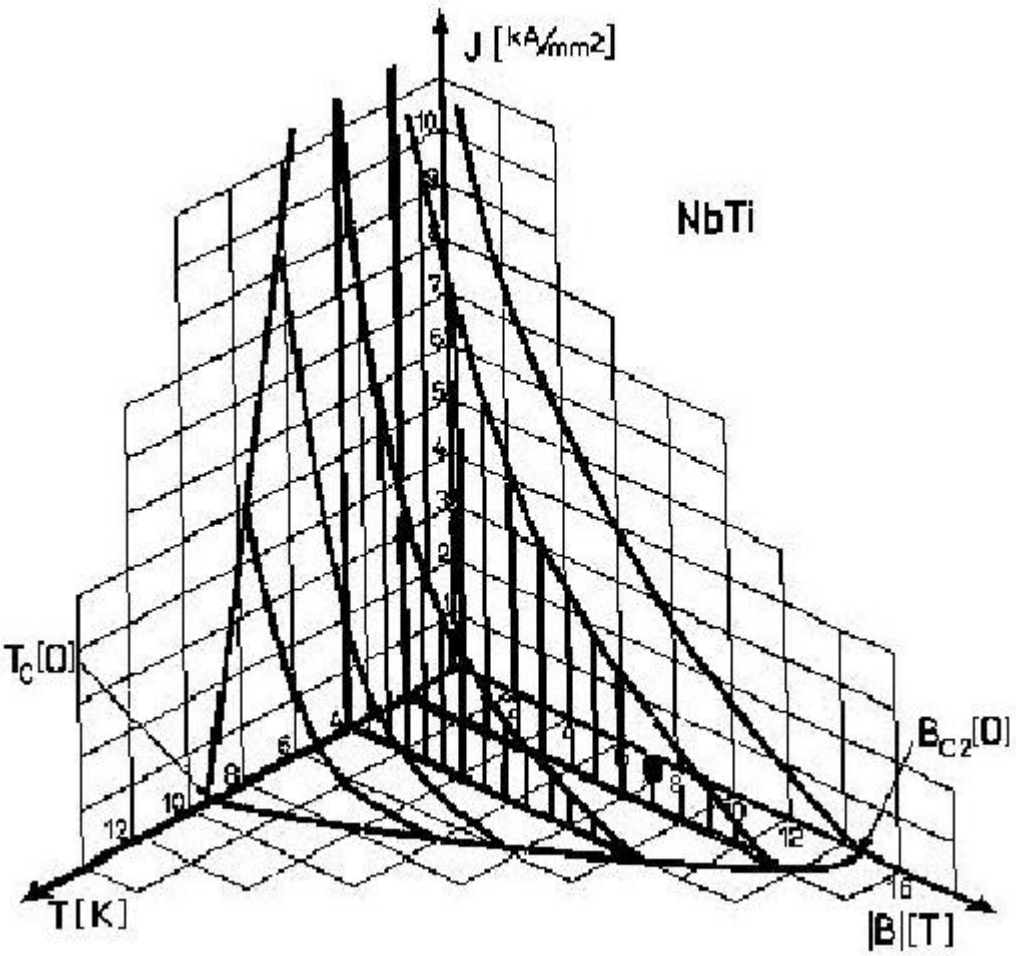


Figure 1.5: Superconducting phase diagram of the NbTi.

three coordinates: the absolute temperature *T*, the effective magnetic flux density *B* and the flowing current density *J*. During operation the magnet coil is in a liquid helium bath, typically at 1.9 K, and carries a current used to generate the intense magnetic field necessary to control the beam. This field is also felt by the NbTi itself.

If a portion of NbTi makes a transition from superconducting to normal state, it reacts to the huge amount of current flowing through it. Consequently it start to heat and could ultimately melt, destroying the superconductive coil. This event is called a “quench”. Such a transition could be initiated either by heat from the beam or by other non-beam processes, like the heating from cable friction, which deteriorate the NbTi coil, decreasing its superconducting ability. Deposited energy in the order of a few tens of mJ per gram is sufficient to generate a quench [8].

Safety systems have been designed to dissipate the stored magnetic energy in predefined safe processes in case of failure. The Quench Protection System (QPS) has also been studied for reliability [9]. This system detects the voltage change of the superconducting cable and, in case of dangerous variations, it interrupts the current alimentation and triggers heaters. The heaters are steel strips placed on the superconductive coils. When a current flows through the heater, the dissipated power generates a temperature increasing in the superconductive coils. Such a temperature increasing extends the normal state transition of the cable to distribute the energy release and avoid local melting of the coil. The QPS also triggers a beam extraction via the Power Interlock System (PIS) to prevent the beam heating because of beam loss. The QPS enables a safe dissipation of the magnetic energy for any non nominal behaviour of the superconducting magnets.

To prevent a quench caused by a beam loss, the beam must be extracted from the accelerator before such a quench can be generated by the heating of the secondary shower particles. To perform this action, any loss must be detected by the beam loss monitors, which inhibits the beam permit to extract the beam.

The extractions are performed by the LHC Beam Dump System (LBDS) triggered by the LHC Beam Interlock System (LBIS).

To illustrate the damage potential of the beam loss given by a nominal orbit perturbation, the damage and quench levels are shown in table 1.3.

	Number of protons	Number of bunches
Full beam protons	3E+14	2835
Damage level @ 450 GeV	1E+12	10
Damage level @ 7 TeV	1E+10	1E-1
Quench level @ 450 GeV	2E+09	2E-2
Quench level @ 7 TeV	1E+06	1E-5

Table 1.3: Approximated damage and quench levels for instantaneous losses.

It is sufficient for only a small fraction of the beam to be lost to a superconductor magnet to cause a serious damage, and even less to cause a quench. The dependency of the quench levels on energy and loss duration will be discussed later, in section 2.2.

A dangerous loss could be generated in a very short time, even less than a single LHC turn. Due to the inevitable delay before an active dump can be activated, only passive components can provide good protection for such very fast losses. The main actor in the prevention of such a loss is the Collimation System formed by several carbon or metal jaws that intercept the off orbit protons to decrease the amount of loss in the ring. These collimators will be installed, with different roles, in points 7 and 3 and they will be monitored by beam loss monitors both to prevent damage to the collimators themselves and to react in time against an evolving loss that could jeopardize the LHC equipment. Where fast triggering magnets, like the injection and extraction magnets, are located, passive components have been put in place to protect or at least to minimize the effect of a false firing which could shoot the beam all around the LHC.

The second type of loss is the fast one with a dynamic between 3 LHC turns (267 μs) and 10 ms. For this time scale, active protection based on the full extraction of the beam becomes effective. The lower limit of 3 turns is fixed by the reaction time of the whole chain of the protection system; the upper limit is essentially based on the reaction time of those systems that further assist the ones in the first line.

For losses with a duration longer than 10 ms, the Quench Protection System can also effectively generate a beam extraction and help in preventing the serious magnet damage.

Finally, for long losses of the order of seconds, the cryogenics temperature measuring system could trigger an extraction.

The main elements of the machine's protection system are the LHC Beam Dump System, see section 1.2.1, the LHC Beam Interlock System, section 1.2.2, the Safe LHC Parameters System and the BLMS, section 1.2.3. In addition to the BLMS there are other systems that could provide fast monitoring of the losses, such as the Fast Beam Current Decay Monitors and the Beam Position Monitors, but they will not be available for the protection of the system during the initial phase of the LHC life.

There are other systems connected to the LBIS that could also generate a dump request. A second aim of the machine protection systems is to guarantee the functionality of the LHC, by the minimization of false dump requests.

In a conservative approach the still undefined systems could be ignored and a simplified diagram of the distribution of requested dumps could be drawn: see figure 1.6. It is a conservative approach because the ignored systems will increase the reliability of the protection system. More reliability would be gained because these ignored systems allow for redundancy of the BLMS: they could detect the losses independently of the BLMS.

Around 400 fills per year are foreseen with an average duration of 12 hours each. This 12 hours fill will be called "mission" in the following. 60% of the annual missions will be intentionally terminated by the control room operators. 15% will be stopped by fast loss detection with the BLMS, where fast means lasting less then

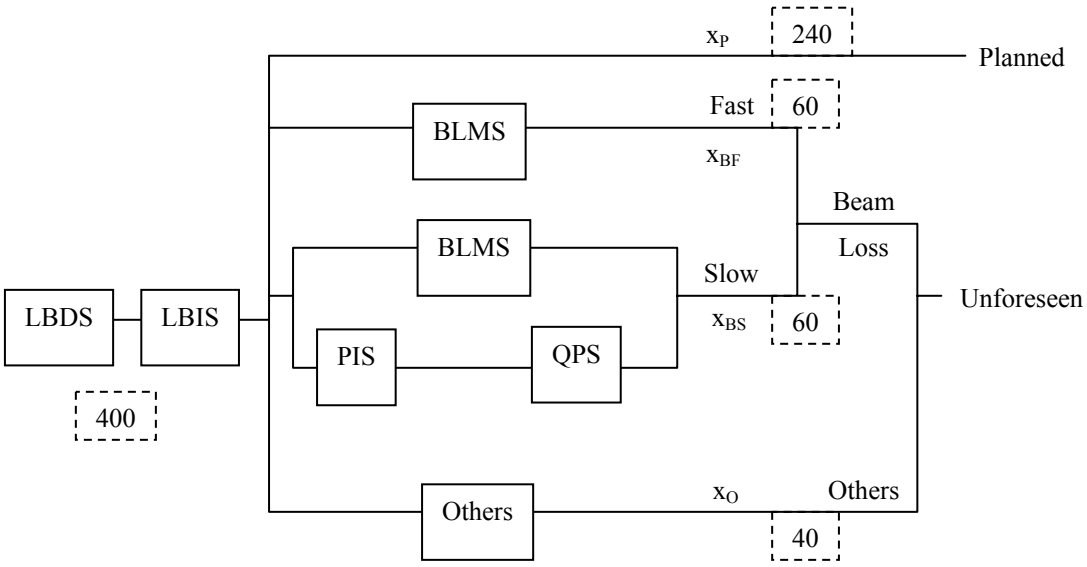


Figure 1.6: Simplified diagram of the source of dump requests.

100 turns. Another 15% of the interruptions would be caused by a slow beam loss detected either by BLMS or by the QPS. Finally the remaining 10% will be caused by other systems and false alarms. These estimates are based on previous experience at DESY [10].

A very high reliability is required for the LHC Beam Dump System and for the LHC Beam Interlock System because they have to handle 100% of the estimated 400 dump requests per year. Nevertheless, the Beam Loss Monitors System is currently the only system that could prevent superconductive magnet damage for all the possible sources of fast losses. It could also avoid the intervention of the QPS.

In the following section these three crucial systems will be briefly introduced.

1.2.1 LHC Beam Dump System

The purpose of a beam dump system, under normal conditions, is to remove the beam safely, on request, from the ring, for example when a refill is necessary due to the degradation of luminosity. It also becomes a crucial machine protection tool in case failures are detected in the LHC, like undesired beam loss or other potentially dangerous situations (magnet quench independent from the losses,

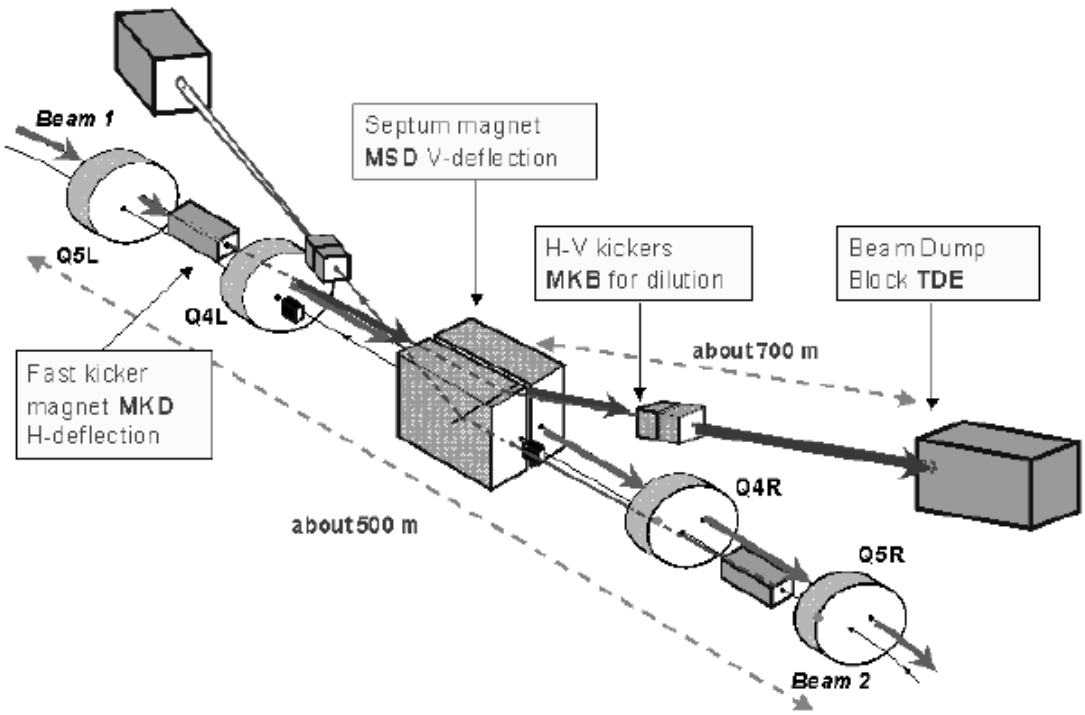


Figure 1.7: The LBDS schematic.
Courtesy of R. Filippini.

personal hazards, etc).

Figure 1.7 shows the schematic of the beam dump system for both LHC beams.

If the dump is activated, the beam is kicked out horizontally from the orbit by a kicker magnet (MKD), it is vertically bent by a septum magnet (MSD), and diluted by diluter magnets (MKB) before reaching the beam dump absorbing block (TDE). The role of diluter magnets (MKB) is to reduce the energy density on the graphite of the dump block.

The beam dump block is located in a cavern several hundred metres from the LHC ring tunnel. The core of the dump is made of a series of graphitic blocks, which have excellent thermo-mechanical properties up to temperatures of 2500 °C, surrounded by heavier materials like aluminium and iron in order to provide sufficient shielding against radiation.

The kicker magnet, made of 15 kicker modules, has a rise time of 3 μs, which is why the train of LHC bunches, section 1.1, has a gap of 3.2 μs.

If the extraction kickers are not fired in synchronization within this abort gap, several bunches will be deflected with a smaller amplitude and will be deviated onto a non-nominal orbit, with resulting damage of the collimation system or other aperture-limiting equipment. This failure scenario is called asynchronous beam dump.

Another possible failure scenario is a spontaneous firing of one of the 15 kicker modules. The internal protection system forces the other 14 modules to retrigger, 1.3 μs later. Certainly this trigger will also be out of synchronization with the abort gap, generating a failure similar to the asynchronous dump.

The criticality of the LBDS is easy to understand: it is unique. Great care has been taken in the design of the critical elements and in their surveillance system. For example: there are 15 fast kickers for the horizontal deflection but the system is designed to work if only 14 out of the 15 magnets fire; the dump signal from the Beam Interlock System is mirrored; many failures, like the failure of the magnets power converters, are surveyed and prevented with a safe beam dump.

Due to the necessary synchronization of beam and dump system, a maximum delay of one LHC turn (89 μs) could occur.

1.2.2 LHC Beam Interlock System

The LHC Beam Interlock System (LBIS) is responsible for transmitting to the dump requests, either the regular ones from the Control Room or the emergency ones from any of the protective systems. Figure 1.8 gives an idea of the amount of the systems connected to the LBIS that could generate a beam inhibition request.

The foreseeable criticalities of the system are the fast transmission of a beam inhibition request to point 6 and the 150 beam inhibition sources which could generate false alarms.

To create a reliable inhibition signal transmission, the LBIS has two identical loops, one per beam, transmitting a 10 MHz optical signal generated in point 6. Each loop has two central units at each LHC point; each unit receives the signal from the previous unit and sends it to the next. Depending on the clients' request, it could interrupt one, or both, loops. Each loop is actually comprised of by two optical lines, one clockwise and one anticlockwise (see figure 1.9). This configuration introduces a further redundancy and also reduces the time-delay from the request transmission to the dump. With this shrewdness the transmission

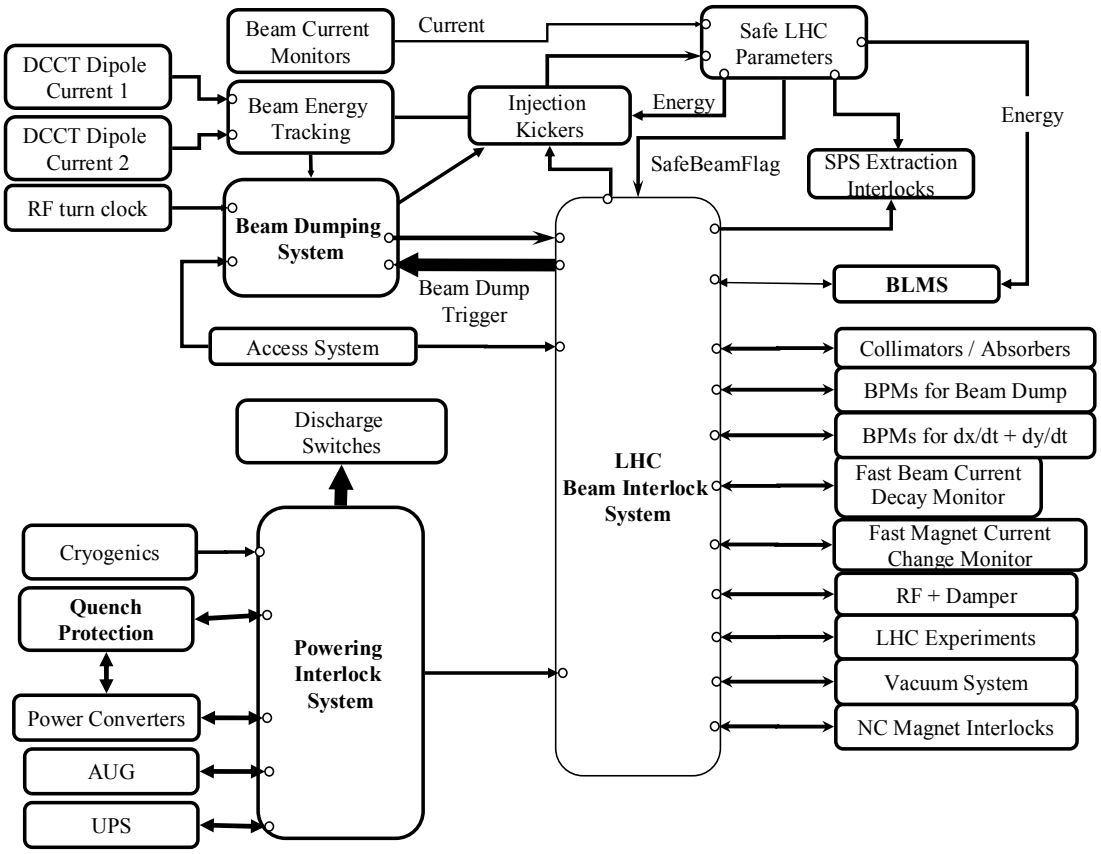


Figure 1.8: Dependency of the LBIS.
Courtesy of R. Schmidt.

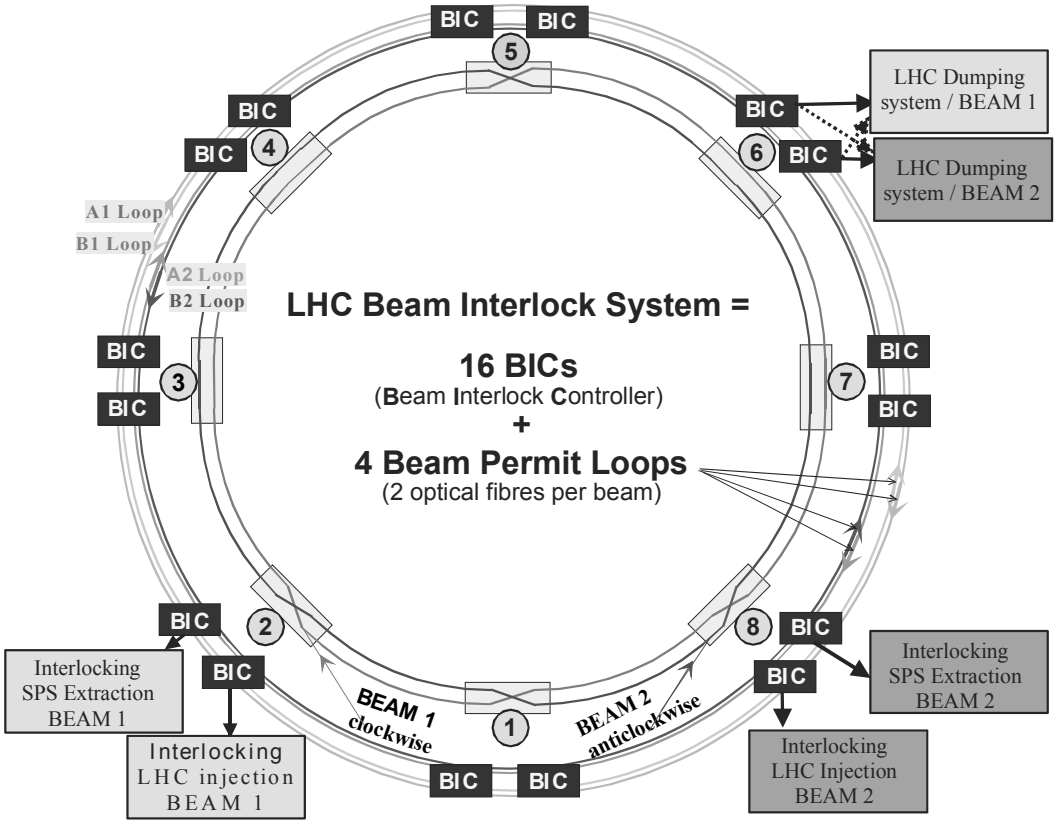


Figure 1.9: The LBIS backbone representation.
Courtesy of B. Puccio.

time delay of a redundant beam inhibition request, like the one from the BLMS, is a bit greater than half an LHC turn, almost 60 μs.

Four signals should arrive at the LBDS and if one of these signals is cut, the dump fires.

On every dump a test procedure is implemented to check if there are any blind channels from the clients so that at the beginning of the mission all the redundancies are active and ready to trigger the dump. This test procedure mainly consists of the generation of a beam inhibition request at the client level for beam 1 and later for beam 2. This sequence permits the verification of the functionality of the system and potential cross-talking or misconnections. These tests need to be implemented at the client system level, as shown for BLMS in section 2.8.5.

To prevent transmission of a false signal, several precautions have been taken with the electronics either to increase the reliability of the components or to reduce the failure modes that generate this event. For example, the VME crate power supplies have been duplicated, and it is possible to mask some input channels if

the energy and the intensity of the beam are known to be below a dangerous value.

1.2.3 Beam Loss Monitors System

The Beam Loss Monitors System (BLMS) is one of the main clients of the LBIS and it is the first-line system in charge of preventing superconductive magnet destruction caused by a beam loss.

The BLMS is the main focus of this thesis. A short description of the system is given here and a detailed description of the components follows in Chapter 2.

The main aim of the BLMS is to detect a dangerous loss and to generate a beam inhibition request which is transmitted by the LBIS to the dump. It must guarantee both the safety (no dangerous loss should be ignored) and the functionality (no false alarms must be generated). No beam should be injected into the LHC if the BLMS is not ready to protect the machine.

The system is composed of Ionization Chambers (IC) placed at the likely loss locations. The chamber current is proportional to the secondary particle shower intensity. This signal is digitized by the radiation tolerant electronics located in the LHC tunnel and then transmitted by a redundant optical link to the surface. A Data Acquisition Board (DAB) checks the signals, compares them with the threshold values depending on beam energy and, in case of losses exceeding such values, halts the beam permit-signal given to a Combiner card. This Combiner card forwards a beam inhibition request to the LBIS. It also drives the High Tension source for the Ionization Chambers.

The simplified layout of the system is given in figures 2.1 and 2.2.

The criticalities of the system in terms of reliability are linked to the number of channels (3500 IC), and to the imprecise knowledge about the behaviour of the dangerous losses. This first characteristic implies a high risk of generating a false alarm generation, whilst the second makes the statement of the system safety more arbitrary.

To avoid false alarms generation, several efforts have been made to increase the reliability of the components and to decrease the number of the devices in the chain.

For the safety consideration, all the calculations performed have been kept as conservative as reasonably possible, as illustrated in section 4.1.

Chapter 2

BEAM LOSS MONITORS SYSTEM

2.1 General Overview

Figures 2.1 and 2.2 show the signal flow of the Beam Loss Monitors System (BLMS).

In case of hadron loss into a superconducting magnet, the secondary particle shower causes a heating of the superconducting coil. The heating can induce a quench, depending on the loss intensity and duration, as introduced in section 2.2.

The secondary particles exit from the magnet and are detected by at least one monitor of the BLMS placed outside the magnet cryostat. The monitor locations and quantity are further discussed in section 2.3. The BLMS monitors are Ionization Chambers (IC) which provide a current signal proportional to the intensity of the secondary particle shower crossing the chamber.

The chamber current is digitalized by the Front End Electronics (FEE, section 2.5). In each FEE only 6 channels are generally in use and 2 are spares. The FEE also

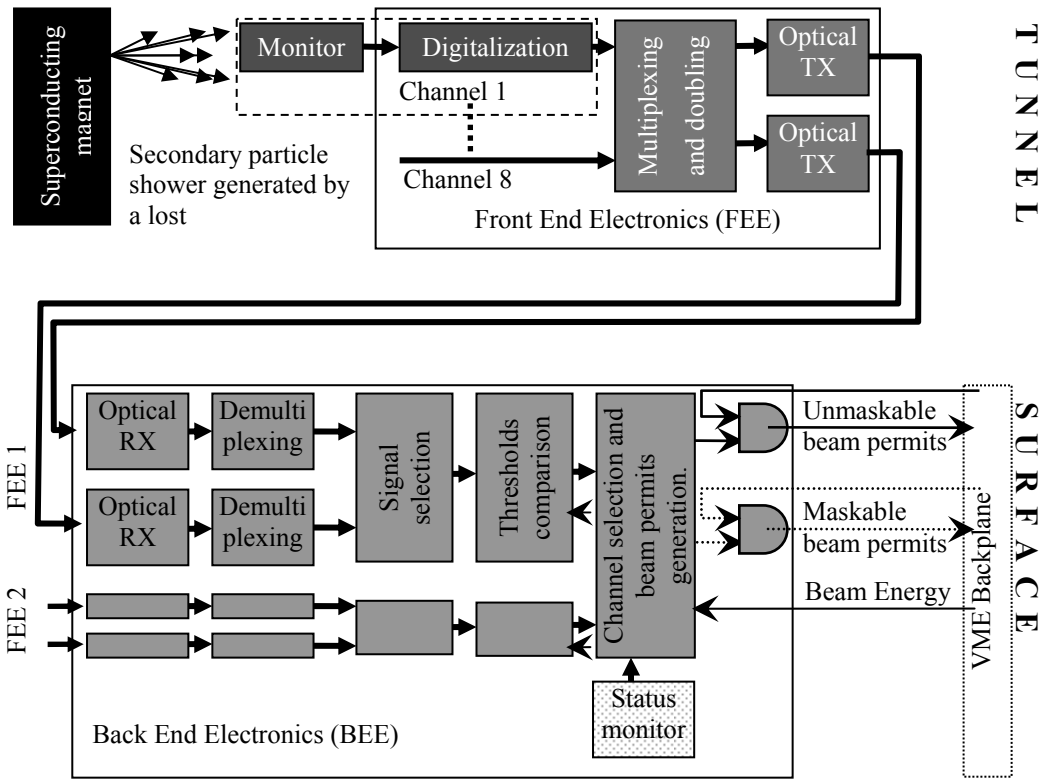


Figure 2.1: Schematic of the signal processing from the bam loss measurement to the beam permit generation.

contains the electronics to multiplex 8 channels and the transmission link of the digital frame to the surface point through two redundant optical fibres. The optical lines have been chosen to be able to transmit the 8 multiplexed signals from the tunnel electronic to the surface point 3 km away. Bandwidth, attenuation and cost have been the critical parameters for the choice. The doubling of the lines decreases the number of false alarms given by the low reliability of the lines (see section 4.2.6.1).

At the surface, the two optical signals are received, demultiplexed and checked by Back End Electronics (BEE, section 2.7). Each BEE can process the signals from two FEEs. After the checking, the signal is compared with energy and loss duration dependant thresholds. There are three kinds of channels: the inactive ones (the spares), the maskable and the unmaskable. The inactive channels do not have any effect on the output. The maskable and the unmaskable are connected to a beam permit signal link. If the particles loss has generated a signal higher than an acceptable value for the current energy, the beam permits corresponding to the channel type is inhibited.

The BEE is hosted by a VersaModular Eurocard (VME) crate, figure 2.2, and the two beam permits are sent via backplane connections to an interface card, the Combiner (section 2.8). One Combiner and, on average, 13 BEEs are present in each crate. The Combiner card receives the daisy chain beam permit signals from maximum 16 BEEs and it is interfaced with the redundant current loop signals of the LHC Beam Interlock System. The Combiner is also in charge of the beam

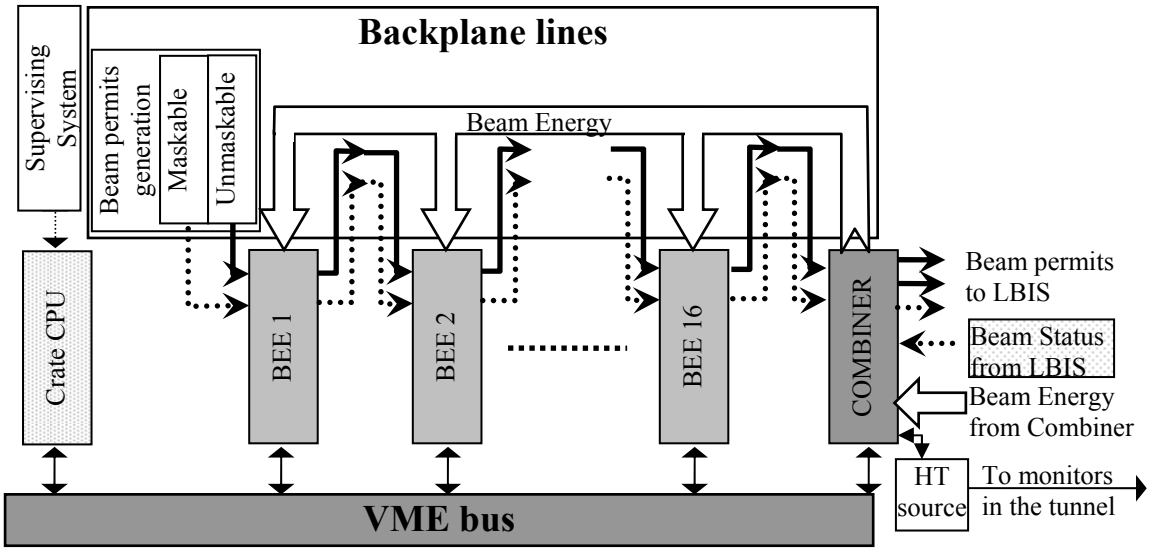


Figure 2.2: Simplified VME configuration for the BLMS.

energy distribution received from the Safe LHC Parameter system to the BEEs of the crate.

The BLMS is monitored on-line to assure the correct functionality and to react in case of malfunctions. In the BEE, the check of tunnel electronics status is done. The status can inhibit the beam permits as well. Each crate CPU is used to survey and to start testing procedures from the supervising system (section 4.2). These procedures are possible if there is no beam in the LHC as indicated by the beam status sent by the LBIS. Another function of the Combiner is the control of the redundant High Tension sources (HT, see section 2.9) for IC alimentation.

The current quantities of the different components to be installed in LHC are given in table 2.1.

Sub-systems	Quantity	Notes
VME crates	25	3 per points +1 in point 7 for collimators
Combiner card	25	1 per VME crate
HT	16	2 (redundant) per point
BEE	325	Up to 16 per VME crate
FEE	642	Up to 2 per BEE
IC	3864	Up to 8 per FEE

Table 2.1: Quantities of the BLMS components.

The layout, the chosen components and the working conditions have been studied to decrease the probability of failure in a dangerous situation. In this approach, the so called “fail safe philosophy”, it is accepted to fail with a minor consequence (false alarm: only 3 hours of downtime) rather then to fail in a catastrophic way (magnet damaged: 720 hours of downtime for the substitution). The BLMS treatment will be focused on the critical elements; the ones with hazard rate higher than 1E-9/h. Elements like resistors, normal capacitors and radiation hard connectors will marginally affect the global reliability, if not present in high quantity.

2.2 Threshold Levels

Threshold levels are compared with the measured loss signal. If the loss exceeds a threshold value, the beam permit is inhibited to extract the beam and avoid magnet damage.

Threshold levels depend on the energy of the beam. The thresholds change due to the increase in the superconducting coil current density and the increase of the

magnetic flux density resulting in a smaller temperature margin during the operation, see section 2.2.1. The energy change is also caused by the different ratio of energy deposited by secondary shower particles in the superconducting cable and in the loss monitor [11,12]. The threshold function is, consequently, a function of the beam energy, Th(E).

Another threshold level factor is the loss duration. The heat flow in the coil and in the magnet material have different time constants. For fast losses no dissipation path will be active. For long losses all the dissipation paths contribute to keeping the superconducting material below the critical temperature. Therefore, the thresholds are functions of the loss power or, better, of the duration of the loss, Th(d).

The variety of magnets used results in a variation of the thresholds, because current density, fields and heat flow are different for the different magnet types. For this reason, each set of monitors around a magnet has a threshold function Th_m which depends on the magnet type.

In addition the location of the loss along the magnet has a relevant influence to the thresholds settings. Heat dissipation varies along the magnet coil. For example, a heat deposition in the middle of the superconducting magnet could be dissipated upstream and downstream along the cable, end heating could be dissipated only in one direction. Furthermore, the ratio between the energy deposited in the coil and the one deposited in the detector varies with the amount of the interposed material. The different monitors located along the magnet will have different calibration factors $C_{l,m}$ given by the longitudinal location of the monitor along a given magnet type.

Finally, operative factors must be considered. Some margins will be applied to the quench levels of the magnets. In the current approach [13] magnet quenches are prevented by setting the threshold level below the quench levels. The safety factor C_o is between 0.3 and 0.4. In the table 2.2 the different levels are reported in relative number, given the quench level equal to 1.

The threshold levels of a monitor i is expressed as:

$$Th_i = C_o\, C_{l,m}\, Th_m(E, d), \qquad (2.1)$$

where C_o is a safe factor, $C_{l,m}$ depends on the location of the monitor and on the magnets dense material between the monitor and the beam lines, $Th_m(E, d)$

	Constant loss		10 ms loss	
	450 GeV	7 TeV	450 GeV	7 TeV
Damage to components	5	25	320	1000
Quench level	1	1	1	1
Beam inhibition threshold for quench prevention	**0.3**	**0.4**	**0.3**	**0.3**
Warning	0.1	0.25	0.1	0.1
Nominal losses	0.01	0.03		

Table 2.2: Characteristic loss levels relative to the quench level [13].

depends on the magnet coil, the heat flow trough the magnet, the energy of the beam and the loss duration.

In the following sections, a derivation of the function $Th_m(E, d)$ will be provided and, in the section 2.3, the dependency of the loss on the loss location will be discussed.

2.2.1 Thresholds Levels Calculation Method

The current calculation method of the thresholds levels is based on the treatment outlined in reference [8]. This study was done for the LHC bending magnets. It is expected that the thresholds for the majority of the quadrupole magnets are higher, due to the smaller current density and magnetic flux.

The steps for the quench level calculation are: simulation of the energy density deposited by the proton initiated secondary particle shower in the superconducting cable, calculation of the maximum allowed temperature of the superconducting strands and calculation of the maximum energy needed to reach the critical temperature for different loss duration ranges.

The deposited energy density varies both longitudinally and radially along the cable. The radial and longitudinal variations for a dipole are depicted in figure 2.3.

The longitudinal variation is quite smooth, with a maximum after 35 cm of the impact point. These distributions are normalized to the energy deposited by one proton. To estimate the deposited energy density by a distributed lost of protons, the longitudinal distribution should be convoluted with a rectangular distribution

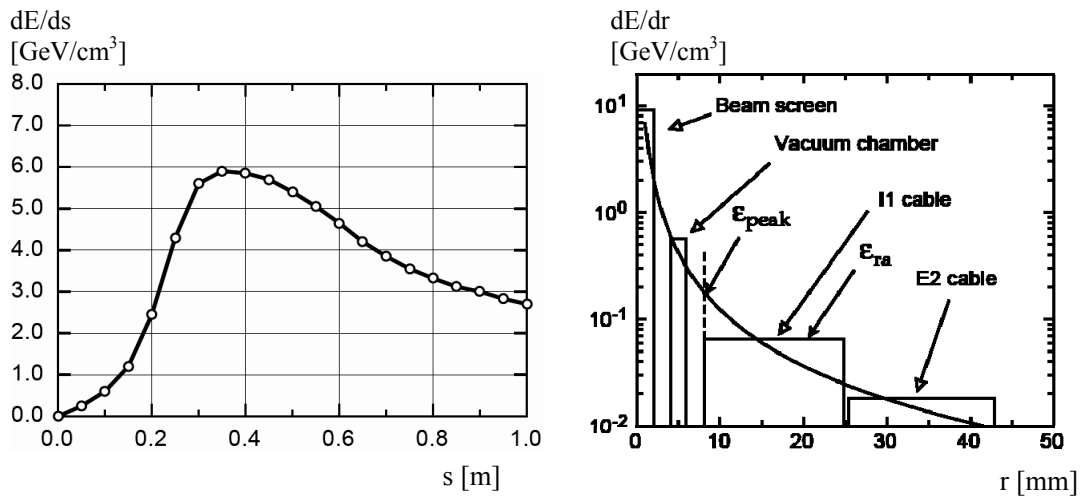


Figure 2.3: Left: the longitudinal energy deposition in the superconducting dipole at top energy. The impact point of the protons on the beam screen is at s = 0 m.
Right: the maximum radial energy density along the most exposed azimuth. [8].

representative of the loss spread. This convolution results in the energy per cubic centimetre deposited on the cable by a lost proton per meter.

The radial distribution follows a function of the type $E(r) = A\ r^{-n}$ with n in the range 1.15-1.76, depending on the beam energy. The power of r is determined by fitting the mean energy deposition in the different elements of the magnet.

As already discussed, the temperature margin has to be calculated in the whole beam energy range.

For instantaneous loss the deposited energy is not dissipated outside of the irradiated element. The deposited energy heats the element of the cable from the initial to the critical temperature. The heat capacity of the cable is the only relevant factor for these very fast losses. For the radial distribution the inner strands of the superconducting cable receive a higher energy than the outer ones. Since no heat flow in the cable is present during the short loss duration, the peak energy, marked as ε_{peak} in the figure 2.3 (right), is used.

For longer deposition time, of the order of milliseconds, the dissipation along the cable and into the helium bath has to be taken into account. The strands are plunged in a superfluid helium bath and the film boiling effect takes a limitation role in the heat transfer. This effect constrains the heat flux below certain values, introduces strong non linearity in the process and makes the calculation more critical in this loss duration range. The number of protons necessary to generate a quench increases due to this dissipation.

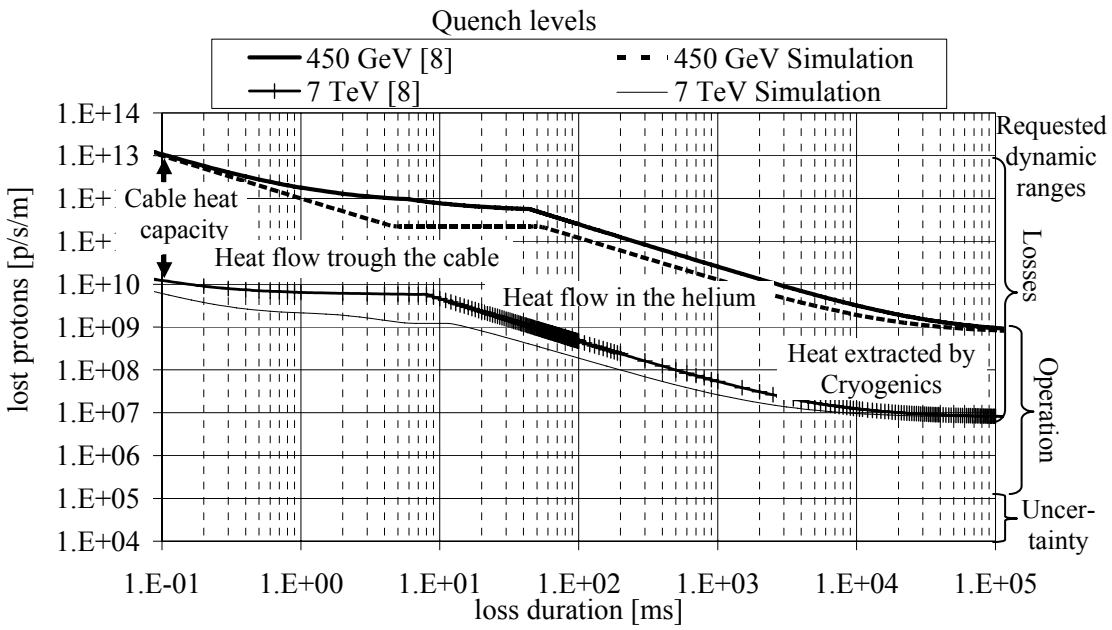


Figure 2.4: Quench levels for the LHC dipole magnet as a function of loss duration. Heat extraction regions and requested dynamic ranges are plotted too.

For very long loss duration, on the order of seconds, the limit is given by the cryogenics system, able to extract no more than 5-10 mW/cm^3.

All these considerations lead to the calculation of quench levels as a function of energy and loss duration. In figure 2.4 the proton density rate (protons per second per meter) is plotted as a function of loss duration. For the simulations, see section 2.2.2.

The quench level values cover a dynamic range of 6 orders of magnitude.

The monitors will not only be used for the machine protection but they will also be used to optimize the filling of the beam. In the case of high losses with a low intensity bunch, the filling procedure has to be either suspended or set properly to avoid dangerous situations during the following intensity and energy ramping. This protective-operational functionality requires a sensitivity 4 orders of magnitude smaller at the injection quench level (there will be 2808 bunches in LHC, see 1.1.1). This consideration leads to 8 orders of dynamic range of the monitor and their associated electronics.

2.2.2 Criticalities of the Quench Level Estimates

The quench level lines traced in the figure 2.4 have been estimated with a linear interpolation of the time constants for the different heat flow contributors [8]. This rough estimation takes only marginally into account the thermodynamics of the

heat flow. To provide a better estimation, a system of differential equations has been studied and the result has been plotted in figure 2.4. The model is outlined in appendix A.

The initial and the final values are identical in the two approaches. The instantaneous losses are fully dominated by the enthalpy of the irradiated superconductive cable: the heat flow has minimal effect. For long loss durations the dynamics is dominated by the heat flow extracted by the cooling system, therefore the quench levels are identical in the two cases. The simple improvements in the modelling already result in quench level differences which could be significant in terms of LHC operation time. Given the importance of the BLMS in the millisecond ranges (see section 1.2), further studies have been initiated on this subject to define the thresholds levels with less uncertainty in the intermediate loss duration region.

The comparison between the measured loss and the threshold values is done by allowing 20% of maximal error between the threshold curves and a step-like function approximation. This procedure results in 11 comparisons in time and 32 comparisons in energy. These 352 threshold values for each monitor will be further refined with the ongoing studies and during the first commissioning years of LHC.

2.3 Monitor Locations

2.3.1 Particle Loss Simulations along the Ring

An uncertainty on the magnitude of the particle loss is given by the determination of the loss location along the ring. Figure 2.5 shows the expected loss locations in the horizontal plane given by one beam, during nominal collimator operations. The highest losses are observed in the straight sections of the IPs, with the exception of the arc of the collimators in point 7.

The losses are localized in the aperture limitations, in the location where the transversal beam sizes are maxima and in the locations of the maximum excursions of the beam trajectory. These features lead to consideration that the losses are most likely located at the near end of the quadrupole magnets. Aperture limitations are caused by probable misalignment errors and the physical aperture

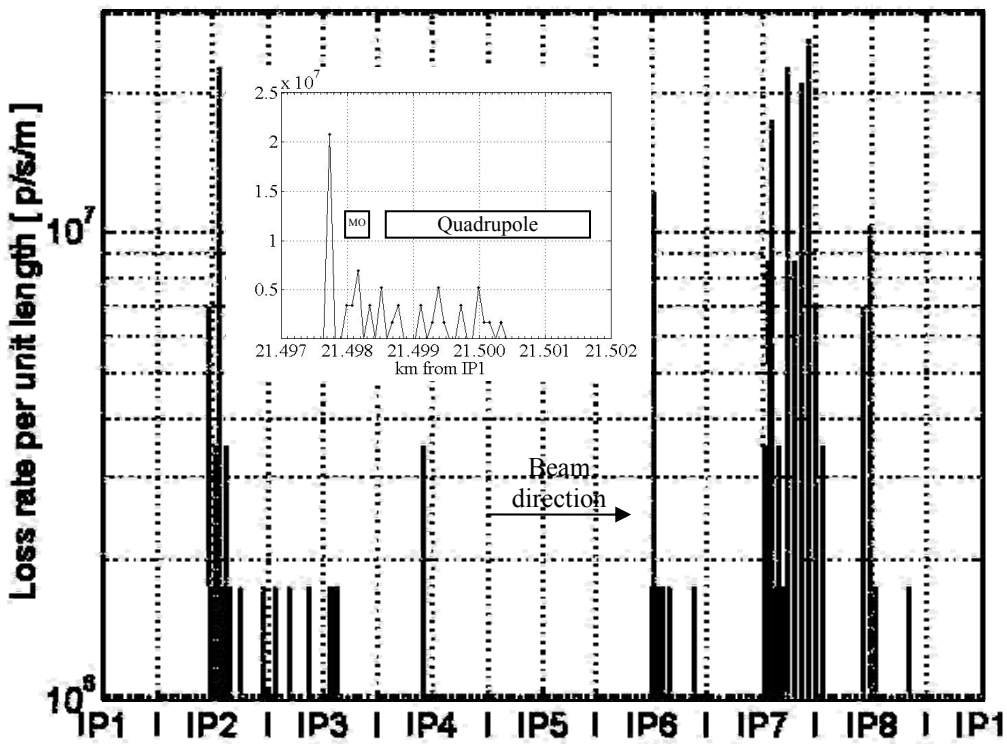


Figure 2.5: Simulation of the horizontal losses in the superconductive magnets during normal operation at 450 GeV. In the insert: magnification of the losses around the quadrupole region. Courtesy of S. Redaelli.

changes near the quadrupole. The beam size is largest at these locations and the orbit excursion too. If the orbit position is not centred within the coil, the quadrupole field creates a maximum excursion in the beam trajectory. Dipole corrector magnets are located just before the quadrupoles, and they are another location where kinks could be generated.

Several loss locations of comparable high intensity are occurring in the first tens of centimetres of the quadrupole region, due to an aperture decrease after a 70 cm long section with larger aperture. Such a loss pattern is also expected in case of dangerous losses.

For the determination of the beam loss monitor location a conservative approach has been followed. Monitors are placed where alignment errors could occur and where the transversal beam size is maximum. The losses are expected in the beginning, in the middle and at the end of the quadrupole region. This distribution of the monitors along the quadrupole assures the loss detection in case of non ideal magnet alignment and orbit perturbation.

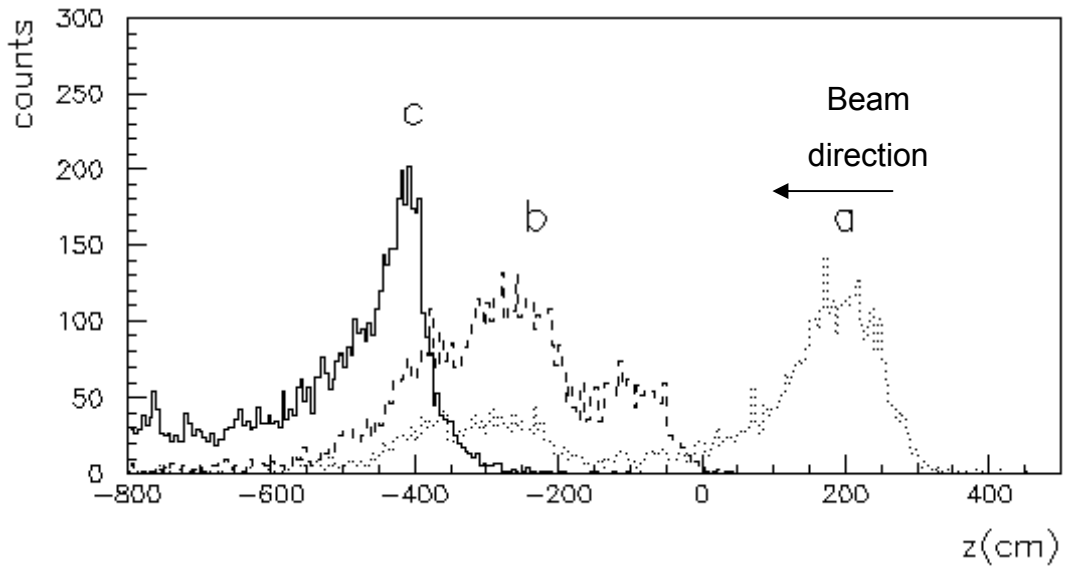


Figure 2.6: Longitudinal shower distribution for a point loss along quadrupole. Loss locations: a) 325 cm, b) 0 cm, c) -325 cm. The quadrupole region extends between point a and c [12].

2.3.2 Proton Initiated Secondary Particle Shower

The determination of the quench point and the detector placement has been determined by the shower simulator code Geant. The secondary particle showers are initiated by the lost proton impact. Their energy deposition in the coil and in the detector has been studied.

The simulations in the LHC arc and dispersion suppressor have been published [14-15] and the ones in the LHC straight section are in preparation.

Figure 2.6 shows the longitudinal shower distribution of the secondary particle outside the cryostat for a proton impact at the beginning, in the middle and at the end of a quadrupole region. The secondary particle shower peak is located between 1 and 2.5 meters from the impact point, depending on the

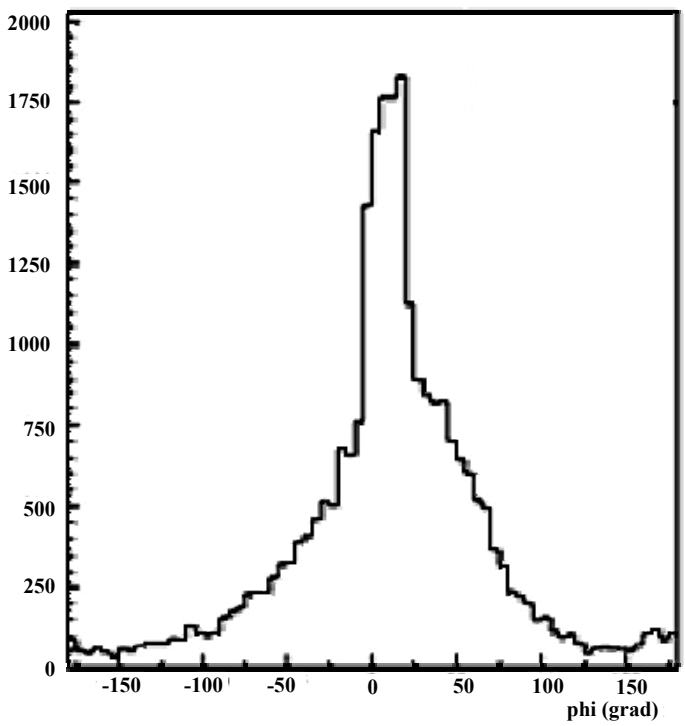


Figure 2.7: Radial distribution of secondary particle outside the magnet cryostat with respect the cryostat centre and the horizontal plane [15].

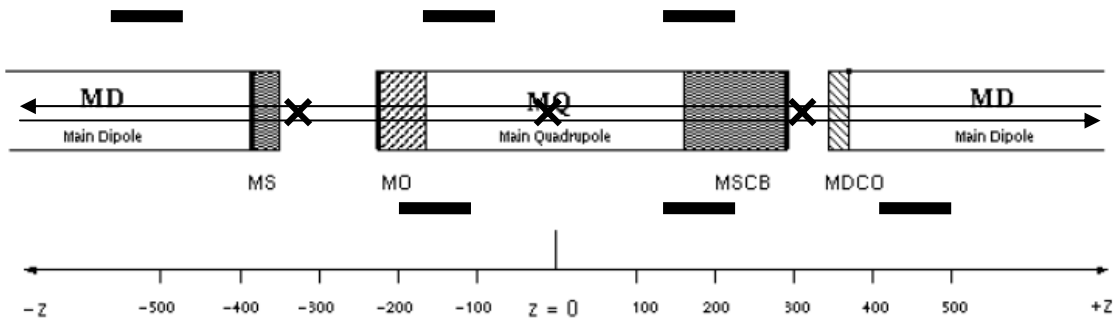


Figure 2.8: Loss monitor placements (bars) and most likely loss location (cross) around a quadrupole [11].

location of the proton loss and not on the beam energy [11]. The Full Width Half Maximum of the secondary shower is between 1 and 2 meters and this characteristic determines the location of the monitor around the magnet: the loss will generate a shower large enough to be detected by the monitors placed along the quadrupole.

The radial distribution of the loss is maximum in the horizontal plane given by the vacuum chambers, due to the minimum thickness of the iron yoke [15], see figure 2.7. The off zero position of the peak is caused by the shift of the plane of the vacuum chamber with respect to the origin of the figure, the centre of the cryostat.

Three loss locations can be distinguished: the losses at the bellows generated by misalignment; losses at the aperture reductions; losses at the centre of the quadrupole due to the largest beam size.

The thresholds will be set at a lower level to assure that just 3 monitors of 50 cm length will be sufficient to cover all the losses coming from a beam pipe of a quadrupole region of 6 m length. There are two beam pipes, clockwise and anticlockwise, so per each quadrupole 6 monitors will be installed in the locations sketched in figure 2.8, taking into account mechanical constrains and possible interferences.

The flux of ionizing particles reaching the monitor per lost proton varies from 5E-4 to 3E-3 charged particles/p/cm^2 at 450 GeV

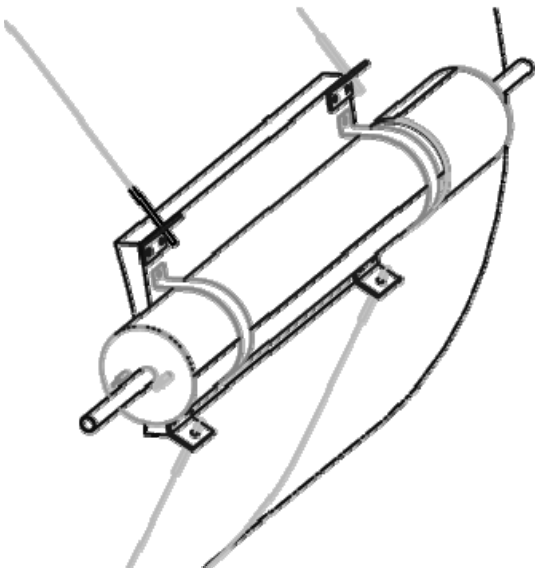


Figure 2.9: Fasten system of the ionization chamber on the quadrupole cryostat.

and from 8E-3 to 4E-2 charged particles/p/cm^2 at 7 TeV, always depending on the monitor position [11]. The spreads at each energy are given by the different amount of material that the particles have to pass through and also by the influence of the magnetic field on their trajectories.

The combination of these arguments leads to the definition of the coefficient $C_{l,m}$ defined in section 2.1: each monitor class will have a calibration factor depending on its location relative to the magnet type.

This additional source of variation adds another order of magnitude to the dynamic range of the ionization chamber and the acquisition electronics. The final dynamic range is 9 orders of magnitude (see figure 2.4).

The ionization chambers are mounted outside the cryostat at the location where maximum energy is deposited in the gas. It will be fastened with metal bands, figure 2.9, or on apposite trestles. These fixations leave certain flexibility in the monitor positioning and relocation of the monitor.

2.4 Monitor Properties

To cover 9 orders of magnitude of dynamic range, a Ionization Chamber (IC) has been designed to be capable to convert the particle energy deposition in a current between 1 pA and 1 mA

The baseline layout of the IC is shown in figure 2.10. It consists of a cylinder with a radius of 4.75 cm and a length of 49 cm. It is filled with 1.1 bar of nitrogen. The electrical field necessary to separate the electron and the ions is created between

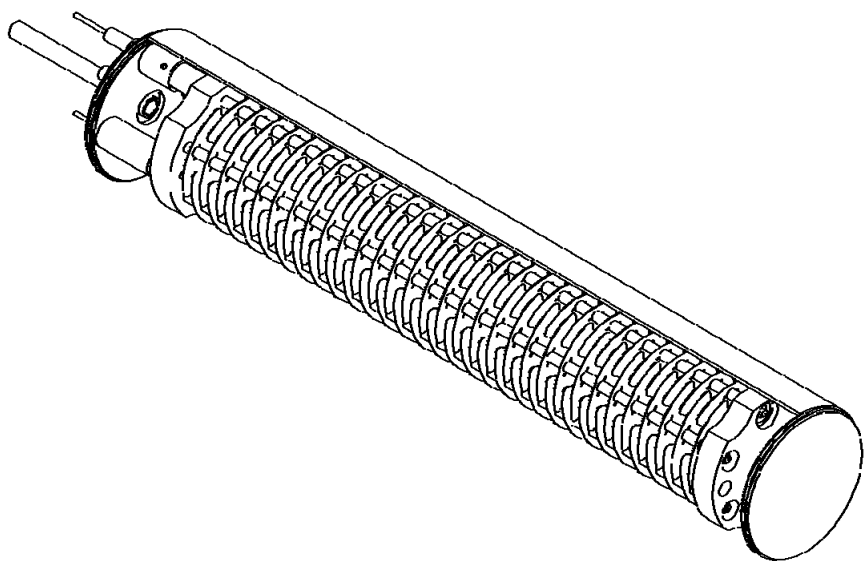


Figure 2.10: Design of the BLM with the external cylinder sectioned.

60 parallel plate electrodes separated by a distance of 0.5 cm. The total weight is less then 5 kg.

The parallel plates design has a constant electric field. Such a configuration allows a high intensity margin. The proportional gas gain region is not reached within the foreseen dynamic range [15]. Nitrogen filling has been chosen both for its charge pair creation property and for the possibility to work in case of a chamber leak with only 20% of reduction in the conversion factor between pairs and current. This event, working with leak, could be very dangerous in case of use of other filling gas with higher conversion factor because the gas gain is not tested during LHC operation. If there will be a leak, the detector would provide a signal lower than expected, failing in case of the hazard detection.

Similar ICs have been used since 1980s in the SPS with good performance both in term of functionality and reliability (see section 4.1).

The typical bias voltage is 1500 V and it will be provided by the High Tension (HT) source located at the surface and it will be in common for all the IC in the octant. In each quadrupole a HT branch is generated to feed the 6 ICs. 1 MΩ resistance is used to insulate the HT line in case of shortcut. The HT will be daisy chained between the 6 IC per quadrupole up to the Front End Electronics. The electrical capacitance of the whole chamber is 312 pF. On the HT line a resistor of 10 MΩ and a capacitor of 470 nF will be added in the configuration shown in figure 2.11. The resistance and the capacitor have a double functionality: to filter eventual noise in the HT line and to provide to the IC enough charge reserve to generate the 1 mA current for almost 0.5 ms.

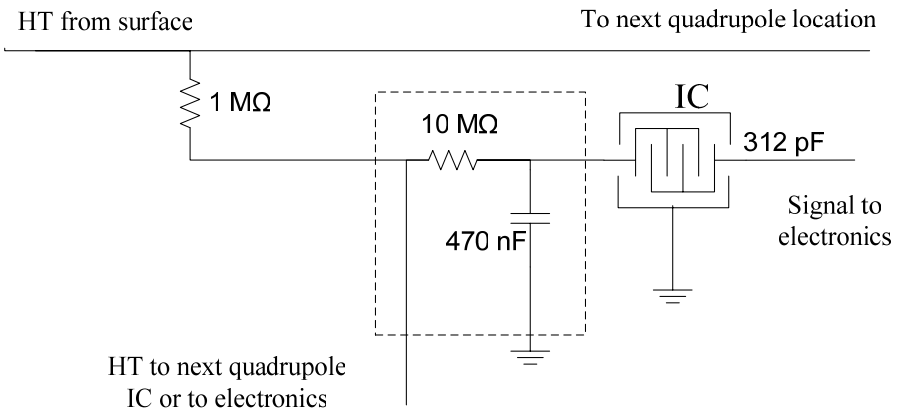


Figure 2.11: Electrical schematics of the Ionization chamber.

The assembly, the chosen materials, the check in and the installation procedures have been studied to minimize either the presence of dirt inside the chamber or the possibility to generate an internal damage. This approach permits either to have reproducible signal or to minimize the chamber aging.

2.5 Front-End Electronics

2.5.1 Current to Frequency Converter

In figure 2.12 a schematics view of the Current to Frequency Converter (CFC) circuits is given.

The main aim of the CFC is to convert the current signal coming from the Ionization Chamber (IC) to a series of pulses to send to the transmission FPGA. To perform this function [16], the IC signal is integrated by an integrator which provides a decreasing voltage signal proportional to the integral of the incoming current. A threshold comparator triggers a monostable when the voltage of the integrator reaches a threshold. The monostable receives the signal from the comparator and generates a voltage pulse, which is counted by the FPGA and triggers a JFET. The JFET discharges the integrator when a monostable signal is given, i.e. when the integrator voltage has reached the threshold. The output frequency has the following value:

$$f = \frac{I_{in}}{I_{res} \cdot \Delta t}, \qquad (2.2)$$

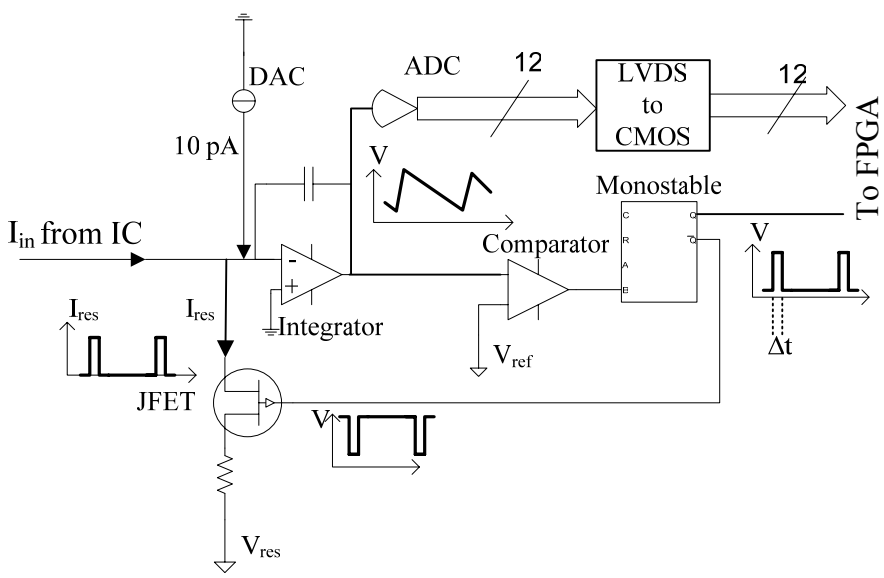


Figure 2.12: The CFC channel representation.

where *f* is the output frequency, I_{in} is the input current, I_{res} is the resetting current and Δt is the voltage pulse length generated by the monostable.

To increase the dynamic range of the detection, an ADC converts the analogue integrator voltage in a 12 bits digital signal. An LVDS to CMOS voltage level translator is necessary to interface the ADC output with the FPGA input.

These components are necessary to digitalize the signal. To increase the reliability a 10 pA current source has also been included. The 10pA current source is generated by a DAC, which constantly provides a current to test the functionalities of the signal chain. It is also driven by the FPGA during the High Tension Activation Test (see section 4.2.6.1).

In each front end electronics there are 8 CFC channels and generally only 6 are used to measure the loss around a quadrupole. The two left are spares used either for mobile monitors or just for a fast substitution of a damaged CFC channel.

2.5.2 The CFC Radiation Behaviours

During the design of the CFC electronics, some irradiation test have been performed at the Paul Scherrer Institut in Villigen, Switzerland, and at the Centre de Recherches du Cyclotron in Louvain La Neuve, Belgium. These facilities allowed the radiation testing of the electronics with 60 MeV proton beam with a

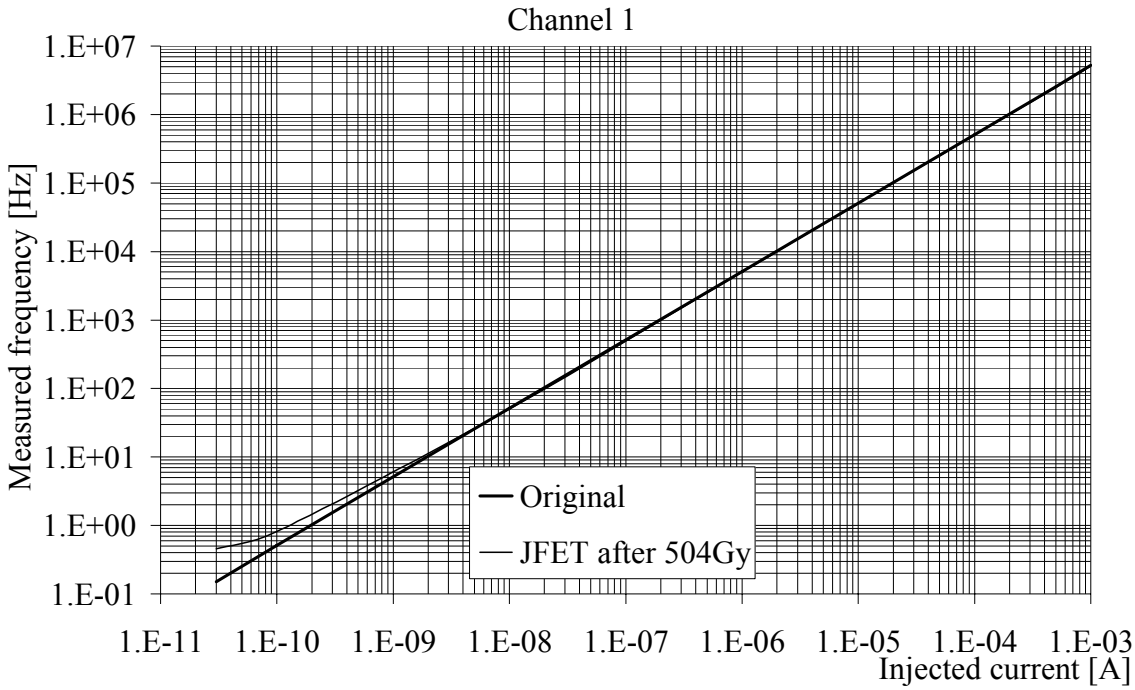


Figure 2.13 : Scan from 10 pA to 1 mA of an FEE, before and after irradiation of the CFC JFET.

maximum flux of 5E8 protons/s/cm^2.

The electronics have been tested irradiating the components one by one. The closer elements have been shielded with an 8 mm copper mask.

The test consists of the injection of a current of 1 nA into the CFC inputs and the measurement of the output frequency. The expected frequency is 5 Hz and its variations have been monitored during the irradiation. Several irradiation steps have been performed per each component. To monitor the degradations given by the integral dose effect, scans from 10 pA to 1 mA have been performed between the irradiation steps (see figure 2.13). The exposure dose is more than 500 Gy, even if the expected irradiation is lower then 10 Gy/y and a substitution after 10 year could be performed.

The measured variation of frequency is summarised in table 2.3 (1 Hz =200 pA).

Component	Name	Integral	Single event (5E8 p/s/cm^2)
JFET	J176	100 pA after 500 Gy	+700 pA (dark current)
Amplifier	OPA627	No	-800 pA (current signal lost into the component)
Comparator	NE521	No	+100 pA (threshold value is lower)
Monostable	74HCT123	No	Small

Table 2.3: Irradiation behaviours of the analogue CFC components.

There are no particular integral dose effects: only the JFET arrives at 100 pA after 500 Gy. This means that there is a dark current of 100 pA injected into the integrator. An extra current of 20 pA could be expected for the foreseen 100 Gy. This current adds to the signal current and could give wrong information during the low intensity bunch injection. This extra current problem has been easily solved using appropriated diodes in the circuit.

The single event behaviours during the irradiation reaches a saturation level between 5E6 and 1E7 p/s/cm^2 for a 60 MeV proton flux (see figure 2.14). To be conservative, an error of 1 nA at a flux of 5E6 p/s/cm^2 on the CFC card will be considered. This error current is in addition or in subtraction to the incoming signal current depending on the weakest element of the circuit.

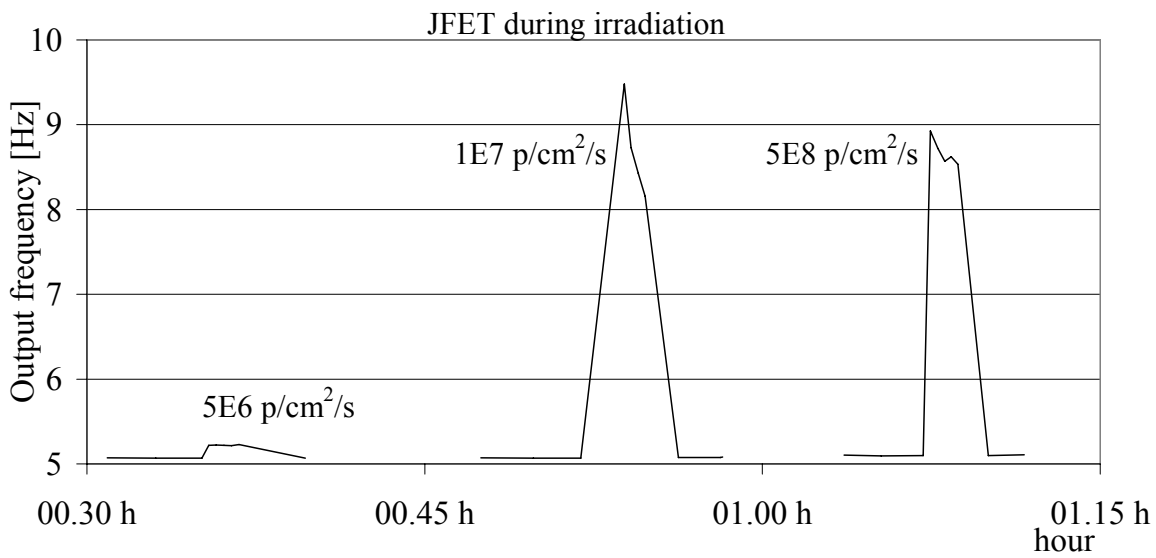


Figure 2.14: Signal variation during the JFET irradiation with different fluxes.

To define the maximum allowed flux on a CFC card in comparison to the quench levels, it is sufficient to summarise some data already exposed in the previous sections, (see table 2.4).

The minimum loss of protons per meter per second is given by the steady loss and it can be deducted from figure 2.4. Considering figure 2.6, the secondary particle longitudinal distribution can be approximated with a 3 meter long square function. The total numbers of loss protons per second in a location is the convolution of this square function with the loss locations along the magnet. This convolution results in the multiplication of the lost protons per meter per second by 3 meters.

	Steady state loss quench limits [p/m/s]	particles/p/cm^2	particles/s/cm^2 on the CFC at quench limits	Quench limits current on IC	Gy/y at 30% of the limits
450 GeV	7.00E+08	3.00E-03	6.30E+05	60 nA	155
		5.00E-04	1.05E+05	10 nA	26
7 TeV	7.00E+06	4.00E-02	8.40E+04	8 nA	21
		8.00E-03	1.68E+04	1.6 nA	4

Table 2.4: Estimated maximum electronics irradiation in the LHC.

The flux of secondary particles which leaves the magnet and reaches the detector is estimated with the ranges given in [11] and exposed in section 2.3.2.

Finally, following the secondary particle radial distribution of figure 2.7, it is necessary to decrease the number of particles by a factor 10 for the radial

intensity difference between the monitor location, beside the magnet at an angle of ~10°, and the electronic crate, below the magnet at an angle of -90°.

Table 2.4 contains the result of the flux on the CFC board at the quench limits. The thresholds are set to inhibit the beam when the lost is 30% of the limits. In the worst case there will be 1.89E+5 particles/s/cm^2 on the electronics. If a linear dependency between the flux and the error current up to the saturation is assumed, this flux will generate an extra current of 37.8 pA versus an incoming current of 18 nA (9.52E-15 A per particles/s/cm^2 for the IC): an error of ~0,2%.

In the table it is also reported the total integral dose (7.3E8 particles/cm^2/Gy in Silicon) in the case that the accelerator operates for 4000 hours with beam just below the thresholds limits (conservative hypothesis). If the accelerator will reasonably work 30% of the time at 450GeV and 70% at top energy, the maximum integral dose will be around 61 Gy/y. Likely LHC will work far below the inhibit limits, so the expected 10 Gy per year still remains a reasonable value.

2.5.3 Digital Signal Transmission

The next element in the signal chain is the transmission FPGA. See figure 2.15. This element performs several functions, both for the signal transmission and for the system surveillance.

First of all it has to multiplex 8 CFC channels, composed by a monostable train of pulses and 12 ADC bits each. The monostable signal is linked to a counter

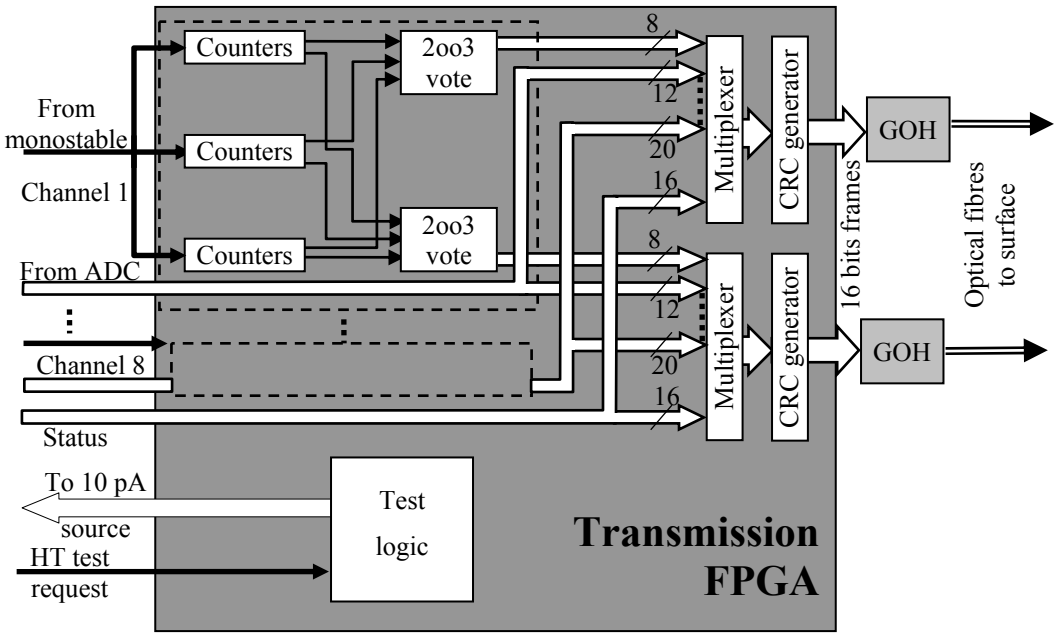


Figure 2.15: Transmission FPGA representation.

providing the final digitalization of the train of pulses. Actually in the transmission FPGA the counters are 3 to perform a 2-out-of-3 vote. The vote decreases the possibility to have a single event error generated by the radiation.

The FPGA collect also some status bits (see table 2.5). In the FEE, the status bits are:

a) 3 power supply statuses, detecting the alimentation failures into the tunnel electronics. These statuses provide maintenance requests, because the fail safe philosophy at the system level inhibits the beam in case of no working tunnel electronics. These statuses will be used to estimate if there is a possible degradation of the power supply to substitute it during the next service period.
b) 1 HT bit, measuring if the HT is present or not on the 6 ICs. In case of low tension on the chamber, the beam permit is inhibited at the surface level.
c) 2 signals from temperature sensors which provide a first and a second warning in case of ventilation failure. The electronics has been designed to function also without ventilation. To not increase the component aging, it is foreseen to have the FEE boards cooled. In a failure case, the fan tray will be substituted during the following access period. In case of warning, a simple maintenance request is formulated.
d) 2 bits linked to status of the two Giga optical link OptoHybrids (GOHs). They are useful in case of failure of one GOH. The working GOH will send the status to the surface electronics. A logical zero in this status means that the failure on the optical line is at the transmission level and not in the receiving part.
e) 2 test statuses. These statuses indicate if the FPGA is in test mode or operating. During the HT Activation Test, section 4.2.7, the first bit indicates that the FPGA has received the test request. The second bit means that the test is running and forces the inhibition of the beam permit at the surface level.
f) 4 bits statuses for the DAC control. They provide the possibility to reset the DAC and the feedback on possible high current from the DAC. These high currents can be generated either by failures on the analogue electronic of the channel or by DAC malfunction. Also slow degradation given by the irradiation can be monitored with these statuses. In case of DAC overflow, a

Bit	Name	Function	Operative status	BLMS action
1	P5V	Monitor 5V PS	1 if >4.75V	Beam inhibition if 0
2	M5V	Monitor -5V PS	1 if <-4.75V	Beam inhibition if 0
3	P2V5	Monitor 2.5V PS	1 if >2.3V	Warning if 0
4	HT	Monitor HT	1 if >1326V	Beam inhibition if 0
5	TEMP1	First temperature warning	1 if <50°C	Warning if 0
6	TEMP2	Second temperature warning	1 if <60°C	Warning if 0
7	GOH_ready_1	GOH status	1 if ready	Warning if 0
8	GOH_ready_2	GOH status	1 if ready	Warning if 0
9	HTAT	HTAT requested (HT>1584V)	1 if HTAT is requested	Beam inhibition if 1
10	HTAT_ON	HTAT running	1 if HTAT is running	Test mode
11	RST_DAC	DAC reset (HT>1700V)	1 when DAC reset is requested	Test mode
12	DAC_reset	DAC reset done	1 when DAC reset is done	Test mode
13	DAC_155	One DAC channel over 155 pA	1 if a DAC current is >155 pA	Warning if 1
14	DAC_FF	One DAC channel over 250 pA	1 if a DAC current is >250 pA	Beam inhibition if 1
15	Int_level	One integrator stuck high	1 if an integrator voltage is > 2.4 V	Warning if 1
16	-	-	1	

Table 2.5 : The FEE status bit table.

beam inhibition will be provided to avoid the risk of working with a blind channel (see section 4.2.4).

g) 1 bit is used to report the status of the integrators. The integrator voltage is monitored to provide fast maintenance in case of failure of the integrator.

After the multiplexing of the signal and of the statuses, the transmission FPGA calculates the Cyclic Redundancy Check (CRC) of 32 bits. This check is used to verify in the surface electronics the correctness of the transmission.

Another input is the HT Activation Test request. A step modulation of the HT activates the test procedure (see section 4.2.7).

During the test, the FPGA sets the HTAT_ON status to 1 and tunes the 10 pA source, a DAC, to provide high current into the CFC. Such a current injection

verifies the channels and DAC functionalities. After this step, the FPGA verifies the signal coming from the channel and eventually it tunes the 10 pA source to compensate CFC dark currents. This compensation guarantees the presence of a current which constantly monitor the channel. During operation, the absence of any current from a CFC channel means that a channel becomes blind to the loss signal. The reaction to this event is taken by the surface electronic and consists in a beam permit inhibition.

The outputs of the FPGA are two identical frames of 16 bits words sent to two different GOH. The frame has the following structure:

a) 16 bits of start of frame.
b) 16 bits of unique FPGA serial number, necessary to check the correct assignation of the threshold with the ICs (see section 4.2.5).
c) 16 bits of frame number, to detect missed frames.
d) 16 bits of statuses.
e) 20 bits (8 for the counter and 12 for the ADC) per each of the 8 CFC channels. The ADC value is used as fractional part of the counter.
f) 32 bits of CRC, to detect the correctness of the information.

In total, in the frame words, there will be 256 bits, transmitted every 40 μs.

The tunnel FPGA has a radiation hard architecture, with components in triple redundancy [17]. The hardware configuration has been build to decrease the integral dose effect while the redundancy is necessary to avoid Single Event Upset given by the radiation.

The transmission FPGA sends two identical signals to two Gigabit Optical Links (GOL) that serialise the signal and send it to a laser diode. The ensemble of GOL and laser diode is called GOH, GOL OptoHybrid. The component is radiation tolerant [18].

The data transmission frequency is at 800 Mbps into a Single Mode fibre at a wavelength of 1310 nm. The optical fibre connects the location in the tunnel up to the BLMS racks in the surface buildings. A maximum length of 3 km is reached. In the optical link analysis also 4 pairs of optical connectors per fibre have been considered. The GOH optical output power is -6 dBm and, in the worst case, the receiving photodiodes have a sensitivity of -21 dBm. The estimated loss for 4 pairs of connector is 4.8 dB maximum and for 3 km of fibre it is 1.2 dB. All the light

power losses add up to a total of 6 dB and give an optical power budget of 9 dB. This budget could be safely used for the fibre degradation given by the radiation.

2.6 FEE Alimentation and Ventilation

Each Front End Electronics (FEE) crate is powered by 3 Power Supply (PS) using the +2.5 V, +5 V and -5 V voltages. The first PS will be referred as Low Voltage PS, the last two as High Voltage PS.

The voltage of the PS will be monitored continuously by comparators on the FEE board and the status of the comparators will be sent to the surface every 40 μs in the data frame. The PS status could be OK or Warning.

To be conservative, the statuses will be not taken into account in the reliability analysis because a PS failure results in an immediate drop of the tension. If there is a failure, the fail safe philosophy of the BLMS system will react with a beam inhibition at the surface level.

This check has been introduced to generate a maintenance request, for a possible substitution during the next service time, in the cases of a constant degradation of the voltage. This argument will be further discussed in chapter 4.

In case ventilation failure, the FEE will continue to work properly. The power dissipation in the electronics will be small enough to allow reliable operations. Nevertheless, two temperature sensors have been inserted onto each FEE board to provide warnings in case of excessive electronics temperature. This event could be generated either by a failure in the fans tray of the CFC or by excessive temperature into the tunnel (wrong tunnel conditioning, other closer hot electronics,…). Repairing maintenance has to be performed when possible if a temperature warning is sent from the FEE.

2.7 Back End Electronic

The Back End Electronics (BEE, see figure 2.16) will be hosted at the surface in VME crates. There will be up to 16 BEE per crate. Each board is constituted by a mezzanine card with 4 optical receivers plus a memory and by a Digital Acquisition Board (DAB) with the analysis program. The DAB is a digital board technology based on the construction of a versatile motherboard connected to some mezzanines. The mezzanines host the components necessary to fulfil a dedicated function. The motherboard hosts a programmable unit (an FPGA in BLMS case),

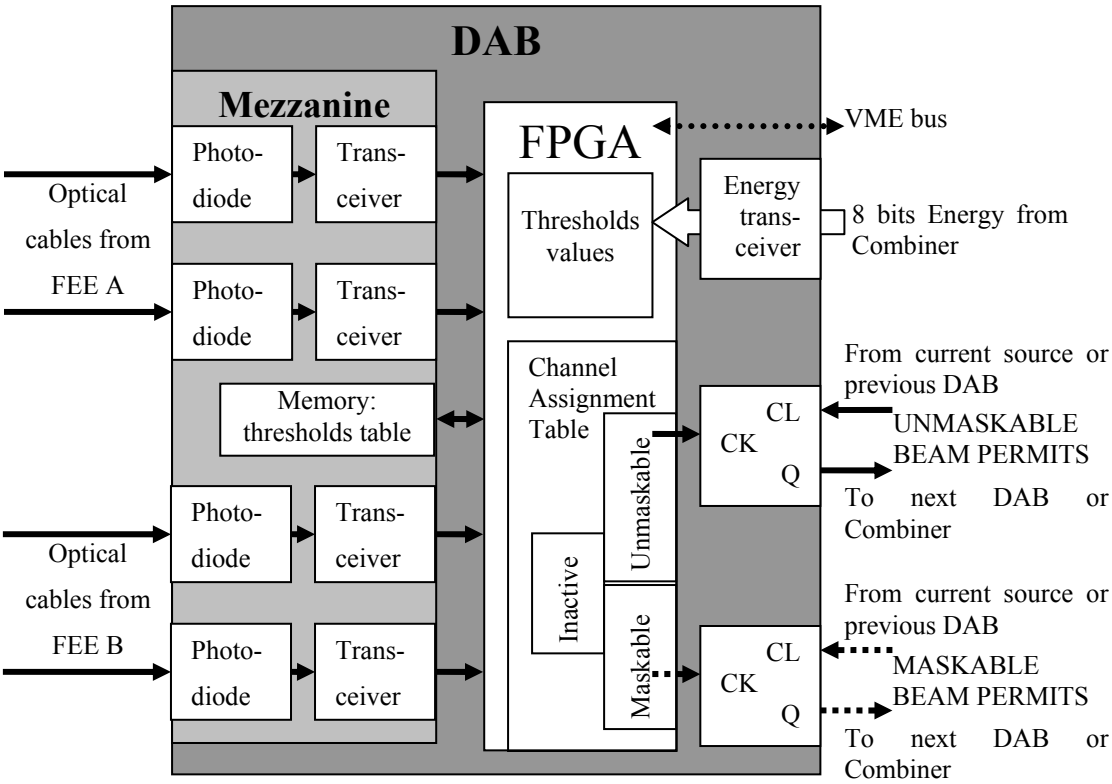


Figure 2.16: The BEE representation.

the components for the software managing and the components for the communications with backplane lines and buses.

Each BEE analyzes the signals coming from two FEE, for a total of 16 channels per DAB.

2.7.1 The DAB Mezzanine

Each optical fibre coming from the tunnel electronics is interfaced with a photodiode which converts the signal from optical to electrical. This signal is decoded and demultiplexed by an input transceiver (TLK) and then transmitted to the receiving FPGA. In the Back End Electronics four optical cables are arriving from two different FEE and all the receiving part is hosted onto a mezzanine card connected to the DAB. Regarding the need of a redundant optical line, see also section 4.2.6.1. The photodiodes are one of the weakest components in term of hazard rate and the DAB is the most expensive. With the mezzanine solution it is possible to substitute only the failed cheaper part saving the most expensive one.

In the mezzanine there is also a non-volatile memory placed to store the threshold values.

2.7.2 The DAB

In the design of the DAB it has been ensured that the beam permit inhibition was independent form the CPU of the VME crate during operation, to minimize the recurrence of false alarms given by its failure. There will be communication between the CPU and the DAB only during testing phase, for the HTLF and the BIL tests (see section 4.2).

The DAB processes the signal, it continuously sends two beam permit signals to the Combiner card, it receives the beam energy from the Combiner card and it communicates through the VME bus to the supervising system.

The Data Acquisition Board (DAB) used in the BLMS is based on the FPGA technology. The FPGA inputs are: the data coming from the transceivers, the beam energy value from the Combiner card trough the backplane lines, the thresholds values from the mezzanine memory.

The four series of data coming from two FEEs are demultiplexed by the TLK transceivers and are checked as described in section 4.2.6. The validated data is further elaborated with internal shift registers and accumulators to have the correct sum values for the 11 different duration windows. The calculated values are finally compared with the thresholds corresponding to the current energy value coming from the Combiner card.

The energy value is transmitted by the Combiner via an 8 lines data bus on the backplane and it is read through a transceiver.

These thresholds tables are downloaded and checked, with the energy value, from the supervising system as described in 4.2.10. In case of missing or out of range energy value, the 7 TeV value will be used to avoid such energy distribution failure (see section 2.8.2).

In case of ventilation malfunctions, a temperature sensor on the board will provide a warning. See chapter 4 for its role in the BLMS reliability.

The BEE FPGA checks the correctness of the ID number from the FEE, to be sure to use the threshold levels associated with the correct monitors. It checks also the statuses coming from the tunnel electronics.

In case of excessive losses or status fault, the beam permit signal is taken away. There are two beam permit lines coming from the DABs: the maskable and the unmaskable ones. At the DAB level, there is the possibility either to set a channel as inactive or to link it to a beam permit line. The inactive channels are spare

channels or channel connected to not critical monitor. The maskable channel can be masked during low energy or low intensity beam operation by the LHC Beam Interlock System. Only if the general hypothesis (see section 2.3.1) to have lower loss in the arcs rather than in the straight section will be confirmed, the masking philosophy could be used. This hypothesis, which could be verified during the first LHC years, will permit to mask several crates to reduce the number of false alarms. The masking is active only during certain phase of LHC life cycle, when the beam will be judged to be safe. At high energy and at full intensity beam, the masking will be not active. The unmaskable channels are channels in locations which are always critical, independently by the beam intensity or energy.

The beam permit lines are daisy chained between the DABs of the crates. The receiver of the combiner is located at the end of the chain.

The beam permit switches are monostables connected to an FPGA clocks, as show in figure 2.17. In the presence of the clock signal the beam permit is generated. The presence assures the nominal functioning of the FPGA. The FPGA clock continuously triggers the monostable, generating a continuous HIGH level signal on the Q line. This line is linked to the next switch via the backplane and it feeds the following monostable on the CLR input. Either no more clock transitions or no more CLR signal force the Q to stay LOW. This status generates the beam permit inhibition at the Combiner level.

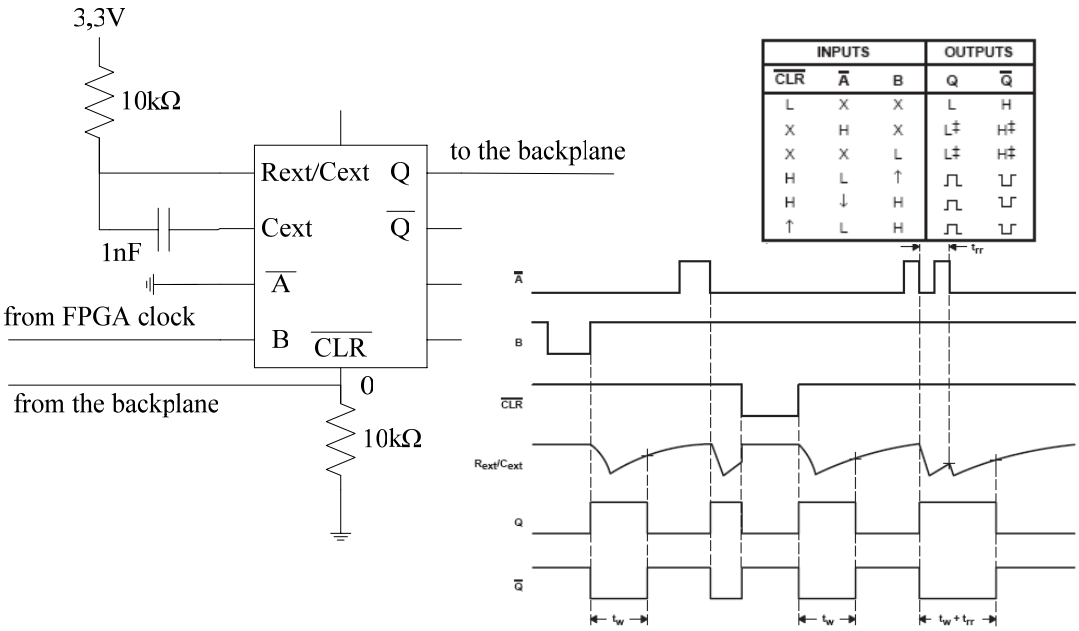


Figure 2.17 : Schematic circuit and functional schemes of the beam permits switch.

To analyze the loss developments, all the maximum values of each summation windows are written every second into a database. Also the current energy value and the current threshold setting are stored (see 2.8.2 for the reason).

2.8 Combiner Card

Next elements in the BLM chain is the Combiner card (see figure 2.18). It is a VME board, one per crates, at the end of the beam permits daisy chains (see figure 2.2). There will be 3 BLMS crates per LHC octant: one crate for the half right arc, one for the straight section and one for half left arc of each point. In point 7 there will be also en extra crate for the collimation control: there will be several ionization chambers around the collimator either to check the correct loss intensity created by the adjacent collimators or to inhibit the beam in case of dangerous loss. A dangerous orbit perturbation is expected to be “detected” either by the measurements of the collimators losses or by other high loss location due to the proximity of the beam to aperture limits.

Every rack will have redundant unmaskable connections to the LBIS, plus one maskable. All the Combiners in the rack will be interfaced by each other to transmit both the beam inhibition request and the energy data.

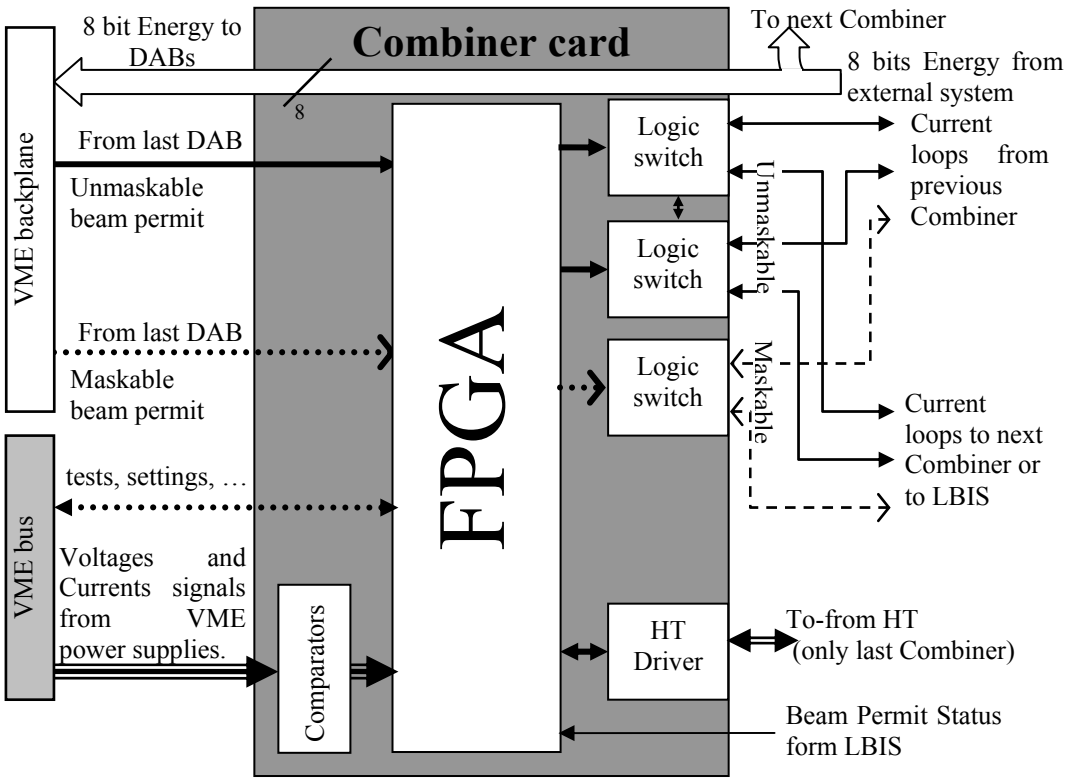


Figure 2.18: Combiner card representation.

Also the Combiner board will be based on a FPGA interfaced with the other subsystems (DAB, HT, LBIS, other Combiners) to provide the following functions.

2.8.1 Beam Permit Distribution

The beam permits are received by the Combiner and transmitted to the LBIS. The Combiner receives the signals from the DAB cards via the VME backplane (see figure 2.2). The incoming maskable and unmaskable voltage signals are transferred to a non redundant current loop in the first case and to redundant loops in the second case. The current loops are linked to the next Combiner or to the LBIS (see figure 2.19).

The beam inhibition could be also provided by the interruption of a current loop coming from another Combiner card. This inhibition of the beam permit is performed at the level of the logic switches.

In total there are 5 incoming beam permit signals and 3 outgoing. The 5 input beam permits are 2 from the crate DAB and 3, eventual, from a previous Combiner. The output signals are two redundant lines for the unmaskable requests and one for the maskable ones.

2.8.2 Energy Distribution

At the location of the BEEs rack there will be the distribution of the current beam energy received via external lines connected in parallel to all the Combiner cards (see figure 2.19).

Each Combiner will distribute this value to the DABs of the crate through the backplane connection (see figure 2.2).

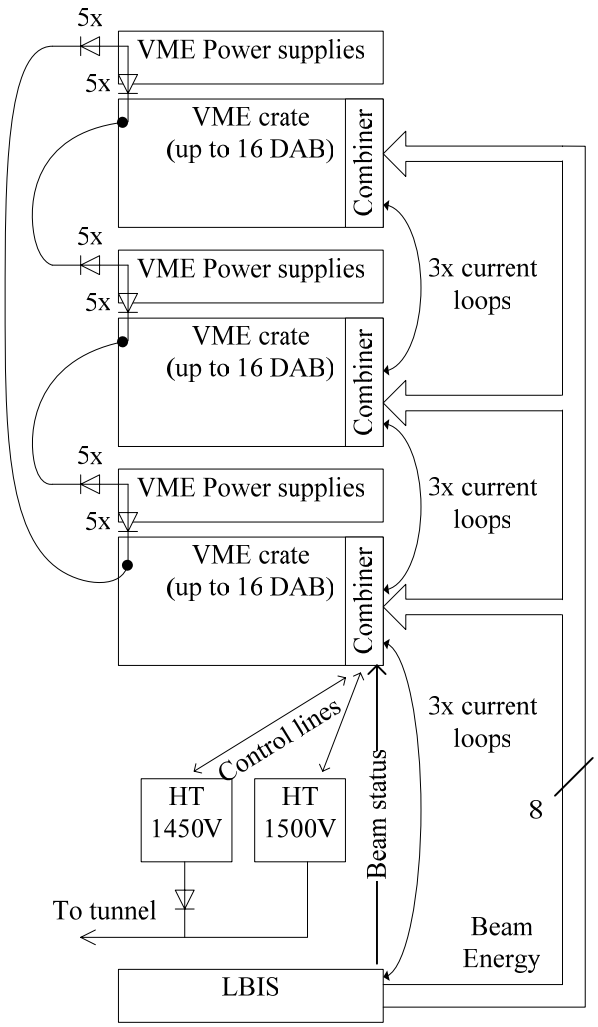


Figure 2.19: Standard rack representation. Optical fibres links are omitted.

It is not foreseen to treat this signal; but the energy distribution system is still in definition and a later supervision of the transmitted value could not be excluded.

To calculate the minimum time for updating the energy signal, some considerations are needed. Given that the energy range is 6550 GeV and the minimum ramping time is 25 minutes, the maximum change rate r_E of the energy is 262 GeV/min. The maximal approximation error of the quench levels *QL* should be less then 20% (see section 2.2). This requires that the difference between two ΔQL_i successive threshold levels should be equal to 0.2 times the high level QL_i, which reads:

$$\Delta QL_i \equiv QL_i - QL_{i+1} = c \cdot QL_i = 0.2 \cdot QL_i \,. \tag{2.3}$$

Referring to figure 2.20, the quench level varies as function of the beam energy, as well as with the finite increment:

$$QL = f(E) \rightarrow \Delta QL_i = \Delta f(E_i) = \frac{\Delta f(E_i)}{\Delta E_i} \cdot \Delta E_i = -f_E'(E_i) \cdot \Delta E_i \,, \tag{2.4}$$

where ΔE_i is the energy variation between the level i and i+1 while $f_E'(E_i)$ is the finite derivative of the quench level function *f(E)*.

The energy changes with the rate r_E which reads

$$r_E = \frac{\Delta E}{\Delta t} \rightarrow \Delta E = r_E \cdot \Delta t \,. \tag{2.5}$$

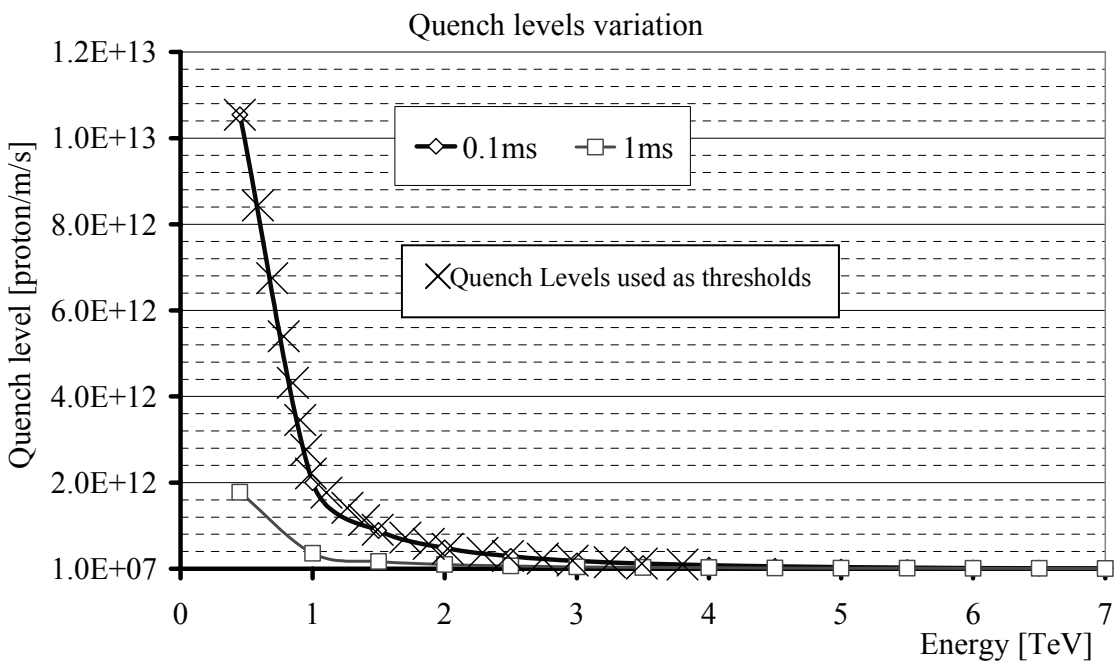


Figure 2.20: Variation of the quench levels with the beam energy and loss duration. The first quench levels for the 0.1 ms duration losses are marked too.

Substituting this equation in (2.4), result in:

$$\Delta QL_i = -f_E'(E_i) \cdot r_E \cdot \Delta t \ , \qquad (2.6)$$

with equation (2.3) it reads

$$\Delta t = \frac{c}{-f_E'(E_i) \cdot r_E} QL_i \ . \qquad (2.7)$$

The required update time of the quench level decreases with the decrease of the quench levels and with the increase of the absolute value of the derivative of the quench level curve.

Interpreting the quench level curves of figure 2.20, it is evident that the derivative is maximum during the first 550 GeV energy increase. Calculating the QL_i, the changing time has a minimum between the 7th and the 8th thresholds. Approximating the quench level function with a straight line the slope coefficient reads -1.55E10 lost proton/GeV, given r_E =262 GeV/min = 4.37 GeV/s, with c=0.2 and with 2.76E12 lost protons at the 7th level, a minimum update time or 8.15 s is required. Actually, as it will be shown in figure 4.8, the change rate r_E is lower for the first 500 GeV increasing. This would increase the minimum update time.

To be safe, the energy signal update is expected at least every 3 seconds. In case of no signal, the DAB reacts using the safer energy, 7 TeV. This action could only increase the number of false alarms, because a loss tens of time lower than the real thresholds could generate a beam inhibition.

The safety criticalities of the energy signal distribution are neither the transmission rate nor the absence of the data but only the freezing on a certain value. For this reason the energy arriving to the DAB is also stored by the logging processes, to allow at least a remote control of the energy value with relative warnings or beam inhibition.

2.8.3 HT Tests

The Combiner will also be used to generate the testing sequence to probe the functionality of the system, when no beam is present in LHC, as later described in section 4.2.7.

To do such operation in a safe way, the Combiner card has to know if there is no beam in the accelerator. If the testing would be done while beam is in the collider,

there will be a false alarm generated by the test procedure. In every Combiner card a beam status signal, coming from the LBIS, will be acquired. Only when the beam status reports that there is no beam in the accelerator, the supervising system can send the test signals to trigger the HT tests.

A failure mode of the HT driver could initiate a test when the beam is in LHC, generating a false alarm. All the other failure modes either will be immediately detected or require a double failure in both supervising system request and beam permit status.

Only one of the Combiners present in the point rack is connected to the HT power supply, to vary the HT voltage using a DAC driver.

2.8.4 Power Supply Monitoring

A series of comparators is used to check the statuses of the power supply at the surface. There will be maximum and minimum level for the two HT voltages and currents (8 statuses) as well as minimum levels for the four VME crate voltages (4 statuses). The eight HT statuses will only be significant for the crate connected to the two HT. The power supply characteristic is summarised in section 2.9.

In case of either under flowing or exceeding the limits by any of those statuses, a warning will be sent to the surveillance system, calling to a maintenance operation as soon as advisable.

2.8.5 Inhibition Tests for LBIS

To increase the LBIS reliability, a test of the beam permit lines has been introduced (see section 4.2.11). These tests could be activated, when the beam status indicates that there is no circulating beam, via the VME bus by the LBIS test procedure. The procedure inhibits the three beam permit lines consecutively. The 3 beam permit lines, two unmaskable and one maskable (see figure 2.18), are not activated at the same time. This constrain is requested by the LBIS to be able to check the functionality of the beam permit lines.

2.9 BEE Power Supplies and Ventilations

2.9.1 VME Ventilation and Power Supplies

Each crate electronics is cooled by a fan tray unit with three fans. In case of failure, the unit was set to switch off the VME power supply. The failure condition is a slow

down of the fans by 20% of their nominal speed, which is actually acceptable for the operation of the electronics. To reduce the number of false alarms, this functionality has been changed to a warning generation.

To further reduce the probability of false alarms, a chain connection with power diodes will permit to face the risk of losing one of the three power supply in the rack (see figure 2.19). Each VME crate is fed by power supplies of +3.3 V, +5 V, +15 V and -15 V. Each power supply is capable of providing a current of 100 A. The consumption of one crate is around 40 A. This allows to link the 3 crates in the same rack. In case of a failure of one power supply, a maintenance request will be generated. The other power supplies will provide the necessary current until the intervention. The intervention is even possible during the LHC operation, with beam in LHC.

2.9.2 HT Power Supplies

In the surface rack there are the High Tension (HT) modules. It consists of two power supplies capable of providing 3000 V which have been set to 1500 V and 1450 V. The 1500 V is actively connected to the 480 chambers in the octant, while the other provides a spare in case of a failure of the first. The two power supplies are connected with an insulation diode and are driven and checked by the last Combiner card (see figure 2.19). During the test phase, only the 1500 V module will be modulated. The voltage and the current of each module is checked by the Combiner card and, in case of not nominal voltages or currents, a warning is generated.

Chapter 3

RELIABILITY PRINCIPLES

3.1 Brief History

Reliability and risk concepts are very old. They have been appreciated since the ancient times: proverbs like “One cannot refuse to eat just because there is a chance of being choked” (Chinese proverb) or “Every noble acquisition is attended with its risks; he who fears to encounter the one must not expect to obtain the other.” (Metastasio, 1750) already underline the idea that risk is somewhat deleterious that could happen and something that in any case has to be faced on the way to reach a benefit.

However, as also reported in [9], the reliability concept was not applied to technology until the previous century. In the 20th century, the unprecedented technological growth pushed almost all the disciplines to their limits, highlighting the necessity of a further effort to guarantee the designed function.

After World War I, one of the first fields of application was the avionic technology which compared operational safety of airplanes with different number of engines. At that time reliability was just a measure of the number of accidents that the planes had per hour of flight time.

At the beginning of the 30’s, Walter Shewhart, Harold F. Dodge, and Harry G. Romig laid down the theoretical basis for using statistical methods in quality control of industrial products, formalising the *trial and error* approach. This method was essentially based on the identification of the best components trough a series of trials. Those methods were not brought into use until the beginning of Wold War II. At that time, products that were composed of a large number of parts, often did not work properly, despite the fact that they were constructed with high-quality components.

A German group, working under Wernher von Braun within the project to develop the V-1 missile, reported, after the conflict, that the first 10 missiles were all useless. Despite attempts to provide high-quality parts and careful attention taken during assembly, all of the first missiles either exploded in the launching pad or landed before reaching the target.

The mathematician Robert Lusser analysed the missile system and quickly derived the *product probability of series components* making the first step into the development of the Reliability Theory. This theorem concerns systems which function only if all the components are functioning and it is valid under certain assumptions. It states that the reliability of such a system is equal to the product of the individual component reliabilities. A system with a large number of components like the V-1 will reach a low reliability level even with very reliable components.

Also in the United States attempts were made to compensate low system reliability by improving the quality of the components. That improved the obtained reliability, but still extensive analyses of the problem were not carried out until the next decade.

Reliability studies for complex systems did not start until the end of the 50's and the beginning of the 60's when the research in the United States was concentrated on intercontinental ballistic missiles and space research mainly within the Mercury and Gemini programs. An association for engineers working with reliability issues was soon established. The first journal on the subject, *IEEE-Transactions on Reliability* [19], came out in 1963 and the first text books were published.

The extensive construction of nuclear power plants during the 70's marked an increase in the interest of engineers for comprehensive risk studies. The so called Rasmussen report [20] was, despite its weakness, the first serious safety analysis carried out in such a complicated system like a nuclear power plant.

Together with the nuclear energy industry, during the next decades the reliability theory was mainly developed at the request of space and offshore oil industries. In these fields the systems are expected to work under more hostile and inaccessible environments where low reliability cannot be compensated by extensive maintenance.

During the 90's reliability started being applied in industry management. Global risk management based on the sequence goal-assignment-proof, and risk informed decision-making techniques started being widely used by professionals in very disparate fields (like finances, project management, insurance, and marketing) and it was starting to deal with world scale problems.

Figure 3.1 summarises the milestones in the reliability history.

Although reliability is, at the beginning of the 21st century, a field used in very different domains of human knowledge, and in some of them, such as nuclear or

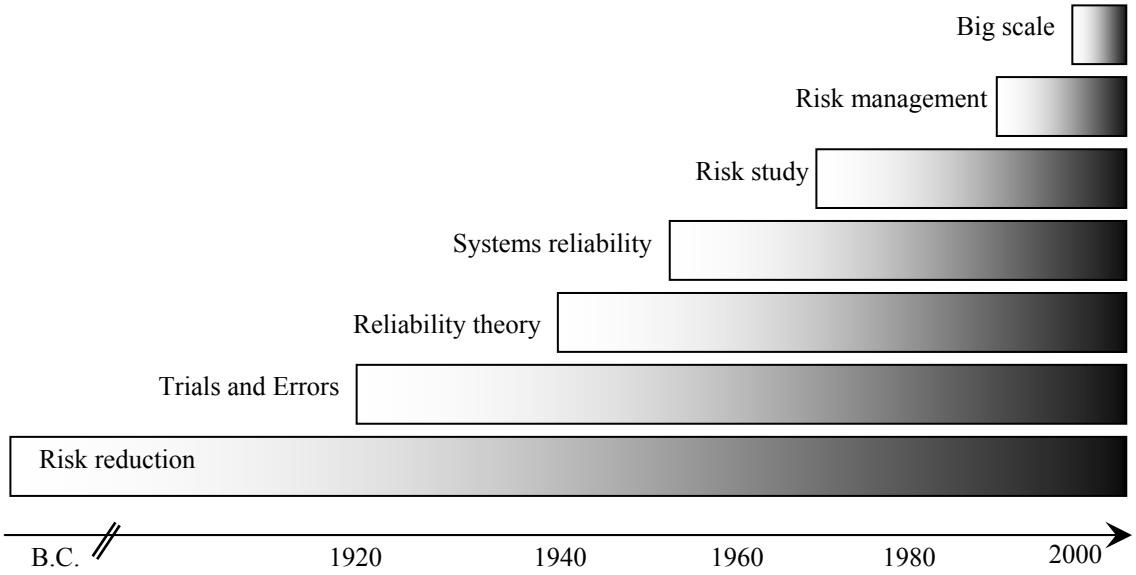


Figure 3.1: Historical development of the dependability.

space industry, of crucial importance, it is just taking its first steps into the world of high level research. Reliability studies for large scale test facilities such as high energy particle accelerators have not started until this century. Existing research accelerators are not optimised from the reliability point of view and all former studies show a lack of data and, above all, methodology.

This thesis is one of the first attempts to introduce such a methodology into the accelerators system design, and so, in the following, a didactical approach will be used to thoroughly explain the techniques used.

3.2 Definitions

To achieve a common language, some definitions are listed.

In the reliability field several definitions of the basic concepts are used, because each guideline introduces its own definitions. Each definition is compliant with others given elsewhere, it simply uses different words to underline peculiar and different aspects following the final aim and the subject of the guideline. In the following, definitions will be given in the frame of the purpose of the chapter. That will give rise to generic definitions, but it will permit to limits the numbers of entries, focusing on the most used and critical ones. For the most generic definitions, please refer to guidelines like ARMP-7 and IEEE 352 [21, 22].

In the next sections the conceptual definitions will be given followed by the mathematical ones when applicable.

In the definition the term "element" is used to indicate a component, a sub-system, a system, a software, a human activity or whatever could be the subject of the reliability study.

3.2.1 Reliability

Reliability is the probability of an element to operate under designated operating conditions up to a designated period of time or number of cycles.

In other words, reliability is the probability that an element works at the time t without any failure between time zero and t.

Unreliability is the complementary part of reliability and it is often used in the calculation, just for numerical reason and for simplicity: it is better to manage number of the form 1E-6 rather than 0.999999! Given that, *the unreliability at the time t could be defined like the probability that a component has failed to operate in an instant between the time zero and t.*

Mathematically speaking, two functions R(t), reliability, and F(t), unreliability, are defined with the following properties:

$$\begin{cases} R(t) + F(t) = 1 \\ 0 \le R(t) \le 1 \\ F(0) = 0 \\ F(\infty) = 1 \end{cases} \tag{3.1}$$

The reliability R(t) and unreliability F(t) are probabilities with the boundary conditions that the element works at time zero, R(0)=1 or complementarily F(0)=0, and it will be out of order in the indefinite future: it describes neither perfect or repairable elements.

Another used function is the failure density f(t):

$$f(t) \equiv \frac{dF(t)}{dt}. \tag{3.2}$$

f(t)dt is the probability that a component fails in the period between t and t+dt given that the component was working at time zero. Consequently

$$F(t) = \int_0^t f(u)du. \tag{3.3}$$

As the density functions in statistics, f(t) has a crucial importance because it is used to estimate the average parameters. The most used is the Mean Time To Failure (MTTF) defined as

$$MTTF \equiv \int_0^\infty t \cdot f(t)dt \,. \tag{3.4}$$

MTTF is the expected time to fail for an element.

The hazard rate, also called failure rate, definition is:

$$r(t) \equiv \frac{f(t)}{R(t)} = \frac{f(t)}{1-F(t)} \,. \tag{3.5}$$

The hazard rate r(t) is a function such as r(t)dt is the probability that an element fails in the period between t and t+dt given that it survived up to time t and it was working at time zero.

It is sufficient to know just one of the function F(t), f(t) or r(t) to calculate all the others. Refer to table 3.1 for a summary of the formulas.

3.2.2 Maintainability

Maintainability is the probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval or number of cycles when the maintenance is performed under stated conditions and using stated procedures and resources.

This is a generic definition that essentially states that maintainability is the probability that, after a period t, a failed element has been repaired. It is exactly the dual function of reliability, but with the accent on the repair rather than on the failure.

A formal difference is that there is no counter term “unmaintainability”. The mathematical expressions relevant for maintainability G(t) are:

$$\begin{cases} 0 \le G(t) \le 1 \\ G(0) = 0 \\ G(\infty) = 1 \end{cases} \tag{3.6}$$

In other words, maintainability G(t) is a probability with the boundary conditions that the element does not work at time zero, G(0)=0, and it will be repaired in the indefinite future.

Reliability	**Maintainability**	**Availability**
Reliability and Unreliability $R(t)+F(t)=1$		Availability and Unavailability $A(t)+Q(t)=1$
$\begin{cases} F(0)=0 \\ F(\infty)=1 \end{cases}$	$\begin{cases} G(0)=0 \\ G(\infty)=1 \end{cases}$	$\begin{cases} Q(0)=0 \\ Q(\infty)\le 1 \end{cases}$
Failure density $f(t)\equiv\dfrac{dF(t)}{dt}$	Repair density $g(t)\equiv\dfrac{dG(t)}{dt}$	Unconditional failure and repair intensities $\begin{cases} w(t)\equiv f(t)+\int_0^t f(t-u)v(u)du \\ v(t)\equiv\int_0^t g(t-u)w(u)du \end{cases}$
$F(t)=\int_0^t f(u)du$	$G(t)=\int_0^t g(u)du$	$Q(t)=\int_0^t [w(u)-v(u)]du$
Hazard rate $r(t)\equiv\dfrac{f(t)}{1-F(t)}$	Repair rate $m(t)\equiv\dfrac{g(t)}{1-G(t)}$	Conditional failure and repair intensities $\begin{cases} \lambda(t)\equiv\dfrac{w(t)}{1-Q(t)} \\ \mu(t)\equiv\dfrac{v(t)}{1-A(t)} \end{cases}$
Mean Time To Failure $MTTF\equiv\int_0^\infty t\cdot f(t)dt$	Mean Time To Repair $MTTR\equiv\int_0^\infty t\cdot g(t)dt$	Mean Time Between Failures $MTBF\equiv\int_0^\infty t\cdot[f(t)+g(t)]dt$
Other used relations		
$f(t)=r(t)\exp\left[-\int_0^t r(u)du\right]$	$g(t)=m(t)\exp\left[-\int_0^t m(u)du\right]$	Number of failures $W(t_1,t_2)\equiv\int_{t_1}^{t_2} w(u)du$
$F(t)=1-\exp\left[-\int_0^t r(u)du\right]$	$G(t)=1-\exp\left[-\int_0^t m(u)du\right]$	Number of repairs $V(t_1,t_2)\equiv\int_{t_1}^{t_2} v(u)du$

Table 3.1: Summary of the basic dependability functions.

Another used function is

$$g(t)\equiv\frac{dG(t)}{dt}. \tag{3.7}$$

The <u>repair density g(t)</u> is a function such as g(t)dt is the probability that a component repair is completed in the period between t and t+dt given that the component was failed at time zero. Consequently

$$G(t) = \int_0^t g(u)du \,. \tag{3.8}$$

As for f(t), g(t) has a crucial importance because it is used to estimate the average parameters. The most used one is the Mean Time To Repair (MTTR) defined as:

$$MTTR \equiv \int_0^\infty t \cdot g(t)dt \,. \tag{3.9}$$

MTTR is, for an element, the expected time to be repaired.

The repair rate is defined as:

$$m(t) \equiv \frac{g(t)}{1 - G(t)} \,. \tag{3.10}$$

The repair rate m(t)is a function such as m(t)dt is the probability that an element is repaired in the period between t and t+dt given that it has failed up to time t and it was failed at time zero.

As already noted for the reliability, it is sufficient to know one of the function G(t), g(t) or m(t) to calculate all the others. Refer to table 3.1 for a summary of the formulas.

It is worth noting that the reliability and maintainability formulas can be derived one from the other by simply applying the substitutions listed in table 3.2.

Reliability	F(t)	R(t)	f(t)	r(t)	MTTF
Maintainability	G(t)	1-G(t)	g(t)	m(t)	MTTR

Table 3.2: "Transformations" from reliability to maintainability and vice versa.

3.2.3 Availability

Availability is the probability of an element to operate under designated operating conditions at a designated time or cycle.

An important difference in the definitions of the availability is that the time, or cycle, is not anymore a period but a precise instant or cycle.

What is more, even if the definition is almost equivalent to the reliability ones, in the availability is hidden the concept of repairing the item in case of failure. It is not important that the item fails at a previous time or cycle but it is crucial that it works

at time t: it could have been failed before t, but it is available if it has been repaired, even if it is not strictly speaking reliable.

If the item is not repairable, reliability and availability are identical; but, if the item is repairable, availability is always higher than reliability.

The mathematical approach is similar to previous ones, with some complications given by the coexistence of failing and repairing effects.

The definitions of <u>availability A(t)</u> and <u>unavailability Q(t)</u> are:

$$\begin{cases} A(t) + Q(t) = 1 \\ 0 \le Q(t) \le 1 \\ Q(0) = 0 \\ Q(\infty) \le 1 \end{cases} \tag{3.11}$$

The last relation states that, due to the repairing processes, the *unavailability, the probability of an element to not operate under designated operating conditions at a designated time or cycle,* could be different from 1 in the steady-state. This means that the element could have been failed during its life but, if there is a repairing process, there is a finite probability to find the element working even after a long working time.

The crucial definitions of the availability theory are:

$$\begin{cases} w(t) \equiv f(t) + \int_0^t f(t-u)v(u)du & (3.12) \\ v(t) \equiv \int_0^t g(t-u)w(u)du & (3.13) \end{cases}$$

where w(t) (and analogously v(t)) is the <u>*unconditional failure (repair) intensity*</u> *defined as the probability that a component fails (is repaired) per unit time at time t, given that it was as good as new at time zero.*

The statement “unconditional” will be discussed later.

Analysing (3.12), it is possible to note that the probability to fail at time t is the sum of two terms: the probability to have failed and never been repaired, represented by the already defined failure density f(t), plus the probability to fail after the last repair. This second term is expressed by the convolution of f(t) and the unconditional repair intensity.

Also the repair intensity is a convolution of the repair density m(t) and the unconditional failure intensity, representing the probability to be repaired after the last failure.

The fact that the two definitions are in a system makes them recursive, and so they can represent the failing and repair of an element repaired and failed several times.

These intensities require the definitions of the failure and repair density f(t) and g(t). If the element is not repairable, g(t)=0, it results in v(t)=0 with the consequence w(t)= f(t) and Q(t) becomes equal to F(t), as it should be.

Q(t) is defined as

$$Q(t) \equiv \int_0^t [w(u) - v(u)]du \,, \tag{3.14}$$

so that the difference of the two unconditional intensities acts as an "unavailability density" function. The probability to find an element not working is essentially the difference between the *number of failures W(0,t)* between zero and t and the *number of repairs V(0,t)* that the elements had.

Those two latter functions are defined as:

$$W(t_1, t_2) \equiv \int_{t_1}^{t_2} w(u)du, \tag{3.15}$$

$$V(t_1, t_2) \equiv \int_{t_1}^{t_2} v(u)du. \tag{3.16}$$

Further used functions are the *conditional failure (repair) intensity $\lambda(t)$ ($\mu(t)$) defined as the probability that a component fails (is repaired) per unit time at time t, given that it was as good as new at time zero and it is working (is failed) at time t.*

These functions are defined as:

$$\lambda(t) \equiv \frac{w(t)}{A(t)}, \tag{3.17}$$

$$\mu(t) \equiv \frac{v(t)}{Q(t)}. \tag{3.18}$$

The previous unconditional intensities were not linked to the condition that the element should work up to the time t. That property essentially makes the conditional function greater than the unconditional ones. The mathematical reason is because A(t) and Q(t) are smaller than one. An example could help in

understanding the difference. Let us assume to have 100 working elements at time 0 and at time t only 80 work. A(t) is 80/100. After a period dt 4 components fail with no repairs take place (for simplicity). These events give an unconditional failure rate w(t)= 4/100= 0.04 while a conditional failure rate λ(t)= (4/100)/(80/100)= 4/80=0.05.

The fundamental problem of availability is to solve the system of equations (3.12) and (3.13)

The fastest way to solve such a system of equations is to use the Laplace method to transform convolutions in products. To obtain the solution it is sufficient to apply to the system the Laplace transformation, to solve the algebraic equations system and to apply the inverse transformation. Explicitly:

$$\begin{cases} w(t) \equiv f(t) + \int_0^t f(t-u)v(u)du \\ v(t) \equiv \int_0^t g(t-u)w(u)du \end{cases} \xrightarrow{\mathcal{L}} \begin{cases} \mathcal{L}[w(t)] \equiv \mathcal{L}[f(t)] + \mathcal{L}[f(t)]\mathcal{L}[v(t)] \\ \mathcal{L}[v(t)] \equiv \mathcal{L}[g(t)]\mathcal{L}[w(t)] \end{cases} \tag{3.19}$$

The final solutions are

$$\mathcal{L}[w(t)] \equiv \frac{\mathcal{L}[f(t)]}{1-\mathcal{L}[f(t)]\mathcal{L}[g(t)]}, \tag{3.20}$$

$$\mathcal{L}[v(t)] \equiv \frac{\mathcal{L}[g(t)]\mathcal{L}[f(t)]}{1-\mathcal{L}[f(t)]\mathcal{L}[g(t)]}. \tag{3.21}$$

Let's assume that both repair and failure density is an exponential function, so

$$\begin{cases} f(t) = \lambda e^{-\lambda t} \\ g(t) \equiv \mu e^{-\mu t} \end{cases} \xrightarrow{\mathcal{L}} \begin{cases} \mathcal{L}[f(t)] = \dfrac{\lambda}{s+\lambda} \\ \mathcal{L}[g(t)] = \dfrac{\mu}{s+\mu} \end{cases} \tag{3.22}$$

Substituting these equations into (3.20) and (3.21), after some algebraic manipulations, the solutions are given by:

$$\begin{cases} \mathcal{L}[w(t)] = \dfrac{\lambda\mu}{\lambda+\mu}\left(\dfrac{1}{s}\right) + \dfrac{\lambda^2}{\lambda+\mu}\left(\dfrac{1}{s+\lambda+\mu}\right) \\ \mathcal{L}[v(t)] = \dfrac{\lambda\mu}{\lambda+\mu}\left(\dfrac{1}{s}\right) - \dfrac{\lambda\mu}{\lambda+\mu}\left(\dfrac{1}{s+\lambda+\mu}\right) \end{cases} \xrightarrow{\mathcal{L}'} \begin{cases} w(t) = \dfrac{\lambda\mu}{\lambda+\mu} + \dfrac{\lambda^2}{\lambda+\mu}e^{-(\lambda+\mu)t} \\ v(t) = \dfrac{\lambda\mu}{\lambda+\mu} - \dfrac{\lambda\mu}{\lambda+\mu}e^{-(\lambda+\mu)t} \end{cases} \tag{3.23}$$

The unavailability is then calculated with equation (3.14) and reads:

$$Q(t) = \lambda \int_0^t e^{-(\lambda+\mu)u} du = \frac{\lambda}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right) \Rightarrow Q(\infty) = \frac{\lambda}{\lambda+\mu}. \tag{3.24}$$

The steady-state unavailability is less than 1 and it is 1 only if the conditional repair intensity function is null, i.e. μ=0. In this case, availability and reliability are coincident.

The Mean Time Between Failure (MTBF) is the expected value of time between two consecutive element failures and it is defined as:

$$MTBF \equiv MTTF + MTTR = \int_0^\infty t \cdot [f(t) + g(t)] dt. \tag{3.25}$$

Table 3.1 summarises the most important functions and properties of reliability, maintainability and availability.

3.2.4 Risk

The definition of risk is complex, because it changes depending on the different field of human knowledge. A common denominator is that the risk could be evaluated as a product of a consequence and likelihood:

Risk= Consequence · Probability of the Outcome

In economy, biology or common life the definition could be different, depending on the different aspects of the subject studied. This is reflected in the definition of the Consequence: money, time, lives and personal damages. What is more, the Consequence generally depends on the surrounding spatial location of the outcome and on the time in which the outcome is produced: the impact of a leak in a chemical plant is different if the plant is in the centre of a city rather than in a desert, or it is different if the wind has a certain direction and intensity rather than another one, or it is different if it happens during the day or the night due to the different number of people present in the surrounding habitations. In economy words like “economic situations”, “global trend”, “reserve margin” should be used, and so on for all the other scientific fields. All these parameters have to be evaluated to give the cost of the outcome.

The functions defined in section 3.2 are used to define the Probability of the Outcome, but further studies, in the different fields, have been done to define the Consequence. In the accelerator physic field, the consequence is generally given in terms of downtime and repairing cost.

3.2.5 Safety

When the risk associated with an event has been calculated, the answer to the question of whether this risk is acceptable or not has to be given.

Formally, *the safety is the likelihood of an element to maintain throughout its life cycle an acceptable level of risk that may cause a major damage to the product or its environment.*

It is a very generic definition, but the important thing is the definition of acceptability of a risk. What is the acceptable amount of money that could be lost per year in a financial operation? How many lives per year are accepted to be lost in car accidents?

Just from those two examples, it is clear that, in safety, also social, ethical and political aspects are involved in the definition of an acceptable level, that is, first of all, a trade-off between the calculated risk and the calculable benefits.

3.2.6 Dependability

Dependability is the modern term used to indicate the ensemble of all previously introduced disciplines, also abbreviated with the acronym RAMS for Reliability, Availability, Maintainability and Safety.

Figure 3.2 graphically summarises the relation between the different disciplines. In this sketch, the Reliability and the Maintainability are the basis to build the Availability theory. To make a Risk evaluation, the consequences have to be defined as well. With the consideration of the acceptable limits for the risk, in other words what is Safe or not, the Dependability is finally constructed.

This thesis should more correctly be titled “Dependability of…”, but due to the fact that it is not yet a consolidated term, up to now the use of the term “Dependability”

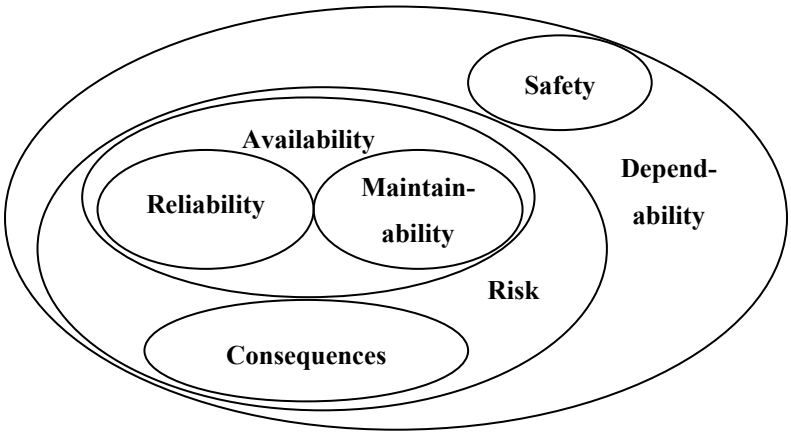


Figure 3.2: Graphical summary of the dependability disciplines.

has been avoided in this work.

3.3 Analysis Techniques

In the approach of a dependability study, several steps are needed. Here is a list that should be a simplified baseline for this investigation:

a) It is necessary to analyse the system and its functionalities to define the undesired consequences. The functionalities of BLMS are to inhibit the beam permit in case of dangerous loss and not to generate false alarms. The undesired consequences are to lose one or more magnets in the first case, and to reduce the operational time in the second case.

b) The system has to be investigated to locate the key elements which can cause those negative outcomes. In the BLMS analysis these elements have been described in Chapter 2.

c) For each key element, its hazard rate must be estimated, possibly with its failure modes.

d) The reaction of the system to the failure must be examined, to compute the probability of the appearance of the consequences. The system could react differently if redundancies or surveillance are present in the design.

e) At the same time, the cost of the consequences has to be evaluated, to calculate the risk. In the case of a missed loss there will be a lost magnet and a downtime of one month to substitute it. For the false alarms, 3 hours are needed to recover the previous operational scenario.

f) An acceptable risk has to be evaluated and then compared to the calculated risk. A year probability of missing a dangerous beam loss lower than 10^{-1} is acceptable. LHC will run for 20 years of 200 days each. The limit corresponds to 2 damaged magnets during the LHC lifetime, and to a downtime of 1.25%. This 1.25% downtime limit also results in a maximum number of 20 BLMS false alarms per year. In chapter 4 these limits will be further discussed.

g) If the risk is not acceptable, actions are required, such as better components, introduction of redundancies for the critical components, more frequent inspections or maintenance tasks.

In the following sections, the commonly used techniques of analysis are introduced starting from the element point of view and mainly focusing on the ones used later for the analysis of the BLMS.

3.3.1 Hazard Rates Prediction

Hazard rate has to be associated to the critical system components, according to their working point and their environment condition. Two possible ways are generally followed: either the determination of the hazard rate consulting international guidelines or laboratory test campaigns.

3.3.1.1 International Guidelines for Hazard Rate Prediction

Several guidelines for the estimation of the hazard rates exist [23 - 26]. There are guidelines mainly concentrated on electronics components or on mechanical parts and others dedicated to a specific field like naval installation or telecommunications.

A common feature in these databases is the evaluation of the hazard rate as a constant which is valid for the lifetime of the component. The hazard rate is dependent on temperature, mechanical or electrical stresses, fixed or mobile use or by specific features of the components.

The simplification of the constant hazard rate assumption is useful because, as will be shown in the section 3.3.1.3, it will permit easier calculation of the overall system dependability figures.

The guidelines are generally based on historical data and theoretical models. The military data handbooks are quite dated and do not take into account the technological improvement reached, in particular during the eighties and nineties [26]. They normally provide conservative figures: hazard rates are higher compared with the measured ones in the field.

3.3.1.2 Laboratory Test

The hazard rate evaluation done with laboratory test is made on an ensemble of components under accelerated condition. “Accelerated conditions” means that the components are put in operation under conditions which are more demanding than the defined working parameters. This stress is generated to accelerate the failures.

For example, an electronic component is fed with higher current or voltage and at a higher temperature.

Even if doubts exist concerning the fact that this harsh test could introduce failure sources which couldn't exist in normal operations, this conservative approach is generally accepted.

To calculate an accelerator factor, Arrhenius like formulas are used. For the temperature accelerated test the typical formula is:

$$A = e^{\frac{E_a}{k}\left(\frac{1}{T_o}-\frac{1}{T_t}\right)}. \qquad (3.26)$$

Where A is the accelerator factor of the components, E_a is the activation energy of the failure mode, generally in the range of 0.3-1 eV, *k* is the Boltzmann constant and the factor 1/*k* is commonly expressed as 11600 K/eV, T_o and T_t are respectively the operational and test temperature expressed in degree Kelvin.

In figure 3.3 an example of the Arrhenius accelerator factor is given. The operational temperature is 30°C, which is later used for the BLMS calculations.

Such tests are done with n elements. The time to failure of each component is recorded. Ordered by the times to failure, we can estimate the unreliability of the components with the median rank estimation. The estimation given by the ratio of the number of failed components over the total ones does not take into account

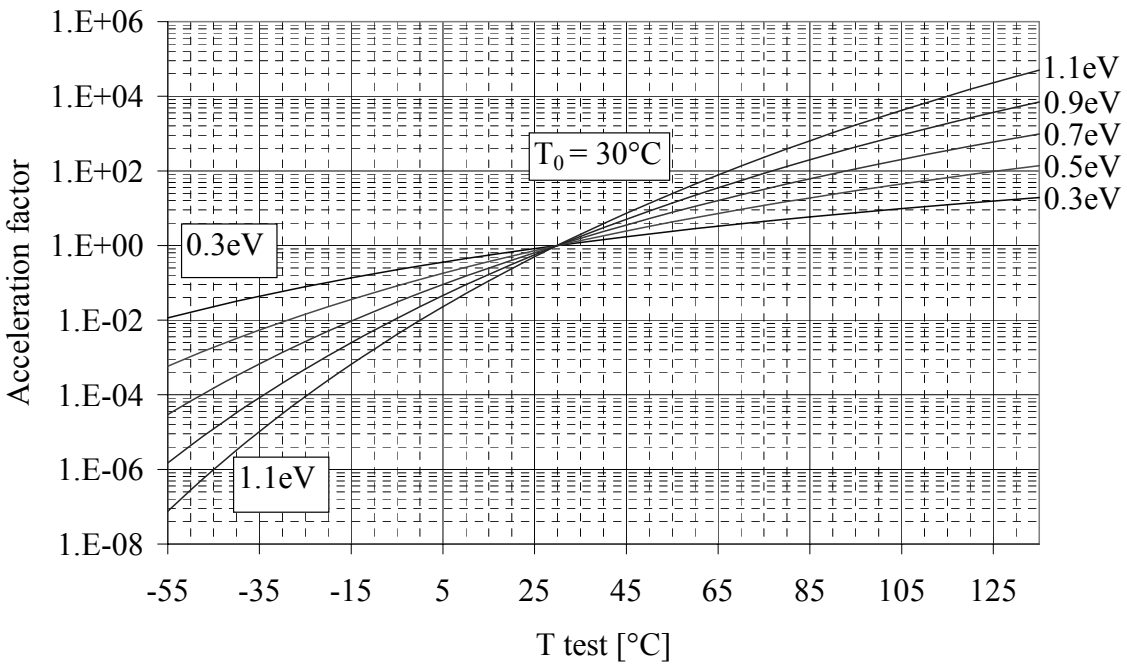


Figure 3.3: Acceleration factor calculated with the Arrhenius formula for an operational temperature of 30°C and activation energy range between 0.3 and 1.1 eV.

the fact that the time to failure is a random variable. The median rank estimator gives the unreliability values which have 50% of the probability to be overestimated by the recorded time to failure [27, p 334]. It is:

$$F_i = \frac{i-0.3}{n+0{,}4} \approx \frac{i-0{,}5}{n}, \tag{3.27}$$

where F_i is the unreliability after the ith failure.

Plotting F_i vs. time to failure for the different components, the time dependency of F(t) could be derived and a good interpolator function can be found. A generally "good" parameterization is given by the Weibull function, defined as:

$$F(t) = 1 - e^{-\left(\frac{t-\gamma}{\sigma}\right)^{\beta}}, \tag{3.28}$$

where the parameters σ, β and γ are derived by fitting the curve.

The failure density f(t) and the hazard rate r(t) are derived from (3.28) using equations (3.2) and (3.5):

$$f(t) = \frac{\beta}{\sigma}\left(\frac{t-\gamma}{\sigma}\right)^{\beta-1} e^{-\left(\frac{t-\gamma}{\sigma}\right)^{\beta}}, \tag{3.29}$$

$$r(t) = \frac{\beta}{\sigma}\left(\frac{t-\gamma}{\sigma}\right)^{\beta-1}. \tag{3.30}$$

The hazard rate could be decreasing, constant or increasing with time depending of the value of β which could be less than, equal to or greater than 1.

The hazard rate during a test is often not constant, but it is sometime possible to approximate the result with a constant hazard rate. Generally this estimator is given with its <u>confidence limits</u>.

For a constant hazard rate, the best estimator of its confidence limits after r failures are [28, 29]:

$$\hat{\lambda} = \frac{r}{(n-r)T + \sum_{i=1}^{r} t_i}, \tag{3.31}$$

$$\hat{\lambda}_{LL} = \frac{\chi^2_{1-\alpha}(2r+2\Delta)}{2((n-r)T + \sum_{i=1}^{r} t_i)}, \tag{3.32}$$

$$\hat{\lambda}_{UL} = \frac{\chi^2_{\alpha}(2r+2\Delta)}{2((n-r)T + \sum_{i=1}^{r} t_i)}, \tag{3.33}$$

where $\hat{\lambda}$, $\hat{\lambda}_{LL}$ and $\hat{\lambda}_{UL}$ are respectively the best estimator of the constant hazard rate with its lower and upper limits, r is the number of failures, n the number of tested elements, T the test time in time-terminated tests, t_i is the time to failure of the ith element, Δ is 0 for the component-terminated test and 1 for the time-terminated tests, $\chi^2_\alpha(\nu)$ is the abscissa value in a Chi-Squared distribution with ν degrees of freedom so that :

$$\int_{\chi^2_\alpha(\nu)}^{\infty} \chi^2(\nu, x) \cdot dx = \alpha \,. \tag{3.34}$$

The area α represents the probability that the abscissa of the Chi Squared distribution has a value higher then $\chi^2_\alpha(\nu)$ as shown in figure 3.4. An equivalent statements is: $\chi^2_\alpha(\nu)$ *is the 100 (1-α)th percentile of the Chi-Squared distribution with ν degrees of freedom.*

The Chi-Squared distribution is a particular gamma distribution defined as:

$$\chi^2(\nu, x) = \frac{1}{2^{\nu/2}\Gamma\left(\nu/2\right)} x^{\frac{\nu}{2}-1} e^{-\frac{x}{2}}, \tag{3.35}$$

with, finally, the usual gamma function

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt \,. \tag{3.36}$$

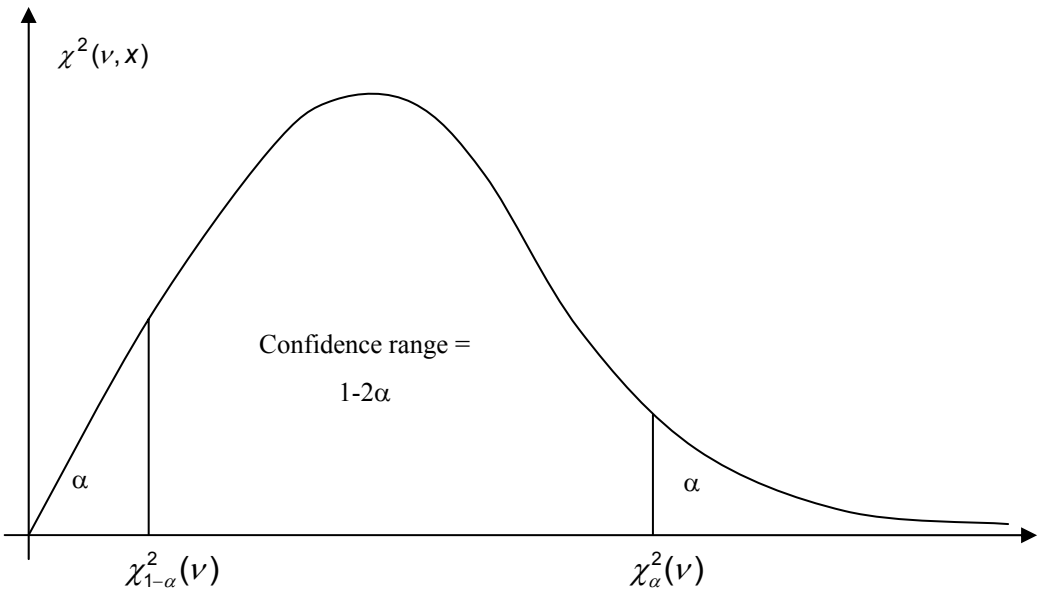


Figure 3.4: Confidence range example.

If it is desirable to calculate the 90% confidence range of the hazard rate estimator, α has to be (1-0.9)/2= 0.05. The values needed for the Chi-Squared have to be calculated with the $\chi^2_{0.95}(\nu)$ and $\chi^2_{0.05}(\nu)$ for the lower and upper limit formulas.

Other techniques are also used during the laboratory tests, to overcome missing data period, missing components, to analyze several failure modes and so on. However, the discussion of these techniques is beyond the aim of this work and we address the interested people to the bibliography [30].

3.3.1.3 Real Hazard Rates

A typical dependence of the hazard rate with time is given by the bathtub curve (see figure 3.5). The early failures are responsible for the high beginning of the curve, then the rate decreases to an almost constant rate given by the random failures of the elements and finally increases due to the wearout failures.

The constant hazard rate approximation generally underestimates the early failures and overestimates the random ones. This is generally accepted because the normal check-in procedure is a selection and rejection of the weakest components. The operation starts later, already within the random failures regime. The overestimation of the random failure during the mission time is generally accepted as a conservative approach.

If more accurate interpolations are needed, a combination of two Weibull functions

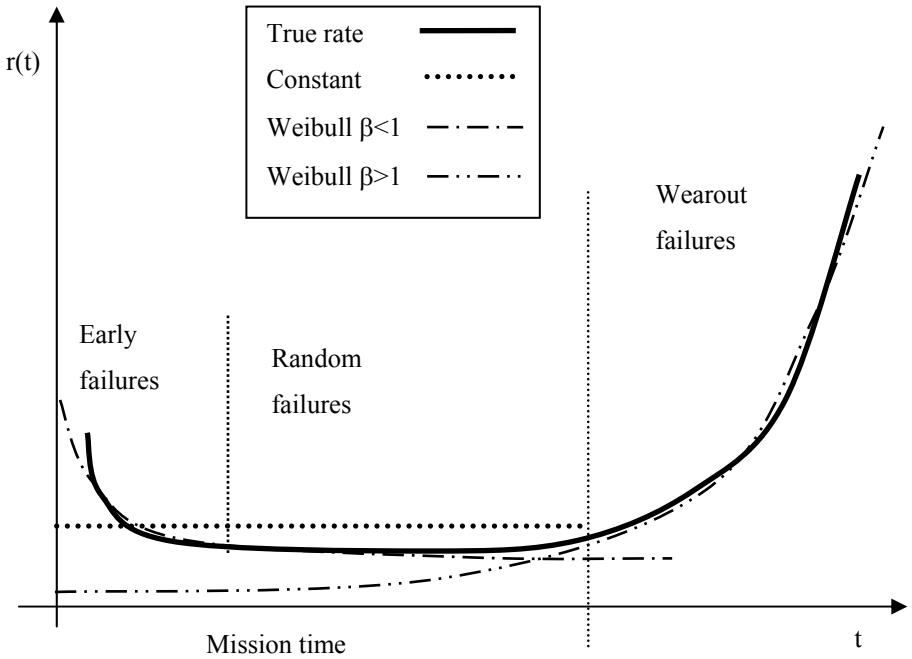


Figure 3.5: Bath tube curve.

are commonly used, one for the early failure plus another for the wearout state.
The pros and cons of using constant rather than time dependant hazard rate are:

a) Constant hazard rate: it is a rough estimation of the real rate, but it is easier to treat in the calculation for the system dependability.
b) Time dependant hazard rate: it is a better approximation of the reality, but it is not user-friendly for the system dependability computation.

The constant hazard rate is generally preferred, taking in mind that its validity is limited by the mission time and it is generally an overestimation of the real one in the random failure domain.

3.3.2 Failure Modes, Effects and Criticalities Analysis

An element could fail in several ways: a wire can have a shortcut to ground or an open contact, software can generate an infinite loop or a wrong assignment, an operator could do the wrong things or nothing.
Each failure mode has its probability to happen and it has a different effect on the sub-system in which it is placed.
Scope of the Failure Modes Effects and Criticalities (FMECA) is to enumerate all the failure modes of the elements with their effects and to propagate these effects through the different system levels up to the top one. It is a bottom-up approach.
FMECA is useful to:

a) analyze if all the element failures have been taken into account,
b) verify if there are possibilities to detect the failure,
c) define which are the largest contributors to the system failure,
d) estimate, in simple systems, the overall hazard rates and criticality levels per element.

To give quantitative evaluations, it is necessary to assign to each element its hazard rate, as already discussed in section 3.3.1, and to give an apportionment percentage α_i^j for the element failure modes. Several international reliability guidelines [31-33] propose their apportionments. The apportionment given by the military handbook FMD-97 [33] has been followed in this thesis.
Once the failure modes have been assigned, an effect for each failure mode is evaluated. The hazard rate of each effect reads:

$$\lambda^{EF} = \sum_i \alpha_i^{EF} N_i \lambda_i \,, \qquad (3.37)$$

where λ^{EF} is the hazard rate of the effect EF, λ_i is the hazard rate of the ith element, N_i is the quantity of the ith element, α_i^{EF} is the apportionment of the hazard rate of the ith element, which contributes to the effect EF. The sum is over all the failure modes which generate the same effect.

In an upper level, the previous low level effects become failure modes that could generate further effects on a higher level. The described calculations process is repeated at each level. At the top level, the hazard rate for the End Effects on the overall system is obtained. Each End Effect is associated with one or more Consequences to attain a representative ranking of the fault seriousness.

The seriousness could also be distributed to the original element failure modes to generate a ranking of the most critical element. The criticality of an element reads:

$$C_i = \sum_j {}^jS^{EE} \alpha_j^{EE} \lambda_i M \,, \qquad (3.38)$$

where C_i is the criticality of the ith element, ${}^jS^{EE}$ is the severity of the End Effect of the jth failure mode, M is the mission time. The sum is over all the failure modes of the element.

This method is mainly a check list of the elements failure modes rather than a quantitative evaluation of the system behaviours. With FMECA it is not possible to take into account all the possible system redundancies and the different maintenance options which could be performed on the subsystems to improve the general dependability.

3.3.3 System Analysis

During the last 50 years several techniques have been proposed to analyze the behaviours of a system in case of failure. Those techniques could be divided into three big families: combinational, stochastic and numerical techniques.

In Chapter 4 the combinatorial Fault tree Analysis will be widely used, therefore this technique will be discussed in this section.

3.3.3.1 Combinational Techniques.

These techniques describe the behaviour of the system by calculating the likelihood to have a certain system event using combinations of elementary failure probability. An event is a failure of a system component or the occurrence of an external input, like a dangerous beam loss. The Reliability Block Diagram, the

Success Tree, the Fault Tree and the Event Tree are the most known techniques of this family. During an analysis of this type, it is important to define the basic events and their availability because all the following analysis will be performed using their unavailability and their unconditional failure intensity.

These techniques are the oldest ones and until a few years ago were the only accepted at the institutional level. They are still widely used for they immediacy, even if they are limited to systems with simple phase dependency.

The base of the calculation in the Fault Tree Analysis approach, as well as in a Reliability Block Diagram and in the Success Tree, is the definition of the Minimal Cut Set. *A Cut Set is an ensemble of Basic Events that generate the Top Event, it is minimal when, subtracting any of its Basic Events, the Top Event is no longer generated.*

Any complex system can fail by several Minimal Cut Sets. The example in figure 3.6 has two Minimal Cut Sets: the failure of the Basic Events A, B and C is one and the other is the failure of the Basic Events A and D.

Three steps are needed to calculate the System Availability.

1. Calculation of the unavailability Q_i and unconditional failure density w_i for any Basic Event.
2. Calculation of the unavailability Q_i^{MCS} and unconditional failure density w_i^{MCS} for any Minimal Cut Set.
3. Calculation of the unavailability Q^s and unconditional failure density w^s and all the other parameters for the overall system.

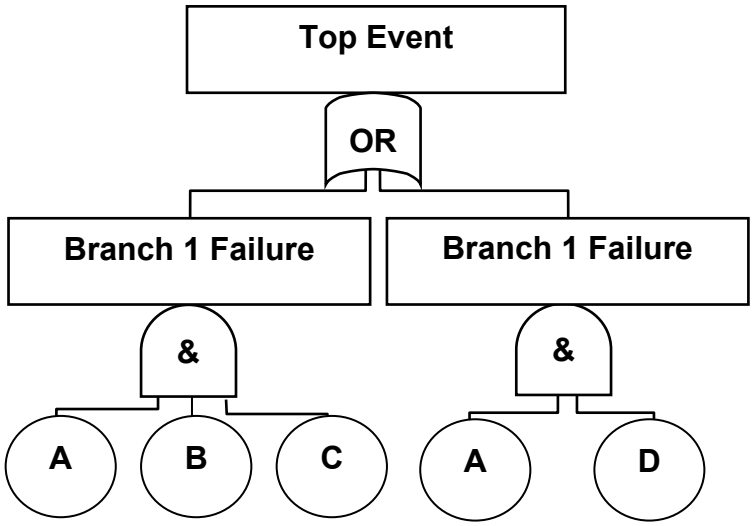


Figure 3.6: Example of Fault Tree diagram.

For the first step, it is sufficient to recall the formulas presented in section 3.2.3.
In the second step, the following formulas are used:

$$Q_i^{MCS} = \prod_{i=1}^{n} Q_i \ , \tag{3.39}$$

$$w_i^{MCS} = \sum_{i=1}^{n} w_i \prod_{\substack{j \neq i \\ j=1}}^{n} Q_j \ , \tag{3.40}$$

where n is the number of Minimal Cut Set Basic Event.
The results of the Fault Tree example of figure 3.6 are listed in table 3.3.

Minimal Cut Set:	**AD**	**ABC**
Q_i^{MCS}	$Q_a\, Q_d$	$Q_a\, Q_b\, Q_c$
w_i^{MCS}	$w_a Q_d + w_d Q_a$	$w_a Q_b Q_c + w_b Q_a Q_c + w_c Q_a Q_b$

Table 3.3: MCS of example in figure 3.6.

Finally, for the last step, the unavailability correct formula is:

$$Q^s = \sum_{i=1}^{n} Q_i^{MCS} - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} Q_{ij}^{*} + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=J+1}^{n} Q_{ijk}^{*} + \ldots + (-1)^{n-1} Q^{*}{}_{ijk\ldots n} \ , \tag{3.41}$$

where Q_{ij}^{*} is the cut set unavailability of a cut set made with the basic elements of the cut set i and j.
To calculate the unconditional failure density w^s the following formula is used:

$$w^s = w^{s1} - w^{s2}, \tag{3.42}$$

where w^{s1} is the probability that one or more MCS fail between the time t and t+dt, w^{s2} is the probability that one or more MCS fail between the time t and t+dt while one or more other MCS, already failed at time t, have still not been repaired. The analytical formulation of this problem is long (see [27, p 404]).
Due to the time dependence of the previous unavailability and unconditional failure intensities, some approximations are commonly used to boost the calculation of the system parameters. The two most used approximations are the rare event approximation and the Esary-Proschan approximation.
In the rare event approximation the unavailability and unconditional failure intensity are calculated with:

$$Q^s = \sum_{i=1}^{n} Q_i^{MCS} \ , \tag{3.43}$$

$$w^s = \sum_{i=1}^{n} w_i^{MCS} \,, \tag{3.44}$$

and they are an upper bound approximation of the exact calculation. This approximation is valid as long as the unavailability and unconditional failure intensity are small.

The Esary-Proschan formulas read:

$$Q^s = \prod_{i=1}^{m} Q_i^c \left(1 - \prod_{j=1}^{n} \left(1 - Q_j^{MCS} \right) \right), \tag{3.45}$$

$$w^s = \sum_{i=1}^{n} w_i^{MCS} \prod_{j=1 \neq i}^{n} \left(1 - Q_j^{MCS} \right), \tag{3.46}$$

where Q_i^c is the unavailability of basic event common to all Cut Sets, m the number of such basic elements, Q_j^{MCS} is the unavailability of Minimal Cut Set without the common basic event, n the number of Minimal Cut Set.

Q^s and w^s have been calculated for the example in figure 3.6 and they are listed in table 3.4.

Methods	$\mathbf{Q^s}$	$\mathbf{w^s}$
Rare event approximation	$Q_aQ_d+Q_aQ_bQ_c$	$w_aQ_d+w_dQ_a+ w_aQ_bQ_c+w_bQ_aQ_c+w_cQ_aQ_b$
Esary-Prochan approximation	$Q_a (1-(1-Q_d) (1-Q_bQ_c))$	$(w_aQ_d+w_dQ_a)(1-Q_aQ_bQ_c)+$ $(w_aQ_bQ_c+w_bQ_aQ_c+w_cQ_aQ_b)(1-Q_aQ_d)$
Exact calculation	$Q_aQ_d+Q_aQ_bQ_c-$ $Q_aQ_bQ_cQ_d$	$[(w_aQ_d+w_dQ_a+w_aQ_bQ_c+w_bQ_aQ_c+ w_cQ_aQ_b)-(w_aQ_bQ_cQ_d)]-$ $[w_dQ_aQ_bQ_c]$

Table 3.4: Q^s and w^s with the MCS methods.

3.3.3.2 <u>Stochastic Techniques.</u>

These techniques are also known as Markov chains, by the name of their Russian author, the mathematician Andrei Andreyevich Markov (1856-1922).

The basic procedure to build such models is illustrated in the following listing:

a) Definition of the system states. Naïvely an n elements system has 2^n states, number of each possible combination of working and failed elements. In reality it is often possible to make large simplifications.
b) Definition of the transition rates between the states. Generally they are sums or differences of repairing and hazard rates.

c) Construction of the transition matrix [$T_{i,j}$]. This matrix transforms the column vector of the probability that the system is found in the state i in its time derivative. The formula is P'_j=[$T_{i,j}$] P_i, given P_i the state probability vector and P'_j its derivative. If the matrix is constant with time, the technique used is the **Homogeneous Markov Graph**; if the matrix changes with system time, the technique used is the **Non-Homogeneous Markov Graph**; if the matrix changes with the arriving time into the states, the technique used is the **Semi-Markov Model**. Refer to the bibliography for further details [34].

These techniques are very powerful because they permit to model different phases of the process, simply changing the matrix during a certain period of the lifetime. The disadvantage of this approach is the explosion of the states in case of a complex system. Therefore this technique is generally used to model a complicated subsystem to subsequently use the unavailability result in other techniques.

3.3.3.3 Numeric Methods

To face the complexity of real operational systems which are, for example, limited in the number of repairing teams, other techniques have been introduced to better simulate the overall behaviour. The most used techniques are the Monte-Carlo simulations and the Petri Nets.

The **Monte-Carlo** simulation needs the definition of the basic events with their hazard rate, inspection philosophy, maintenance philosophy and the correlation of the element fault with other basic events. It is possible to treat the case of inspection of one element during the inspection of another one, or to maintain an element in case of failure of another one and only if there is a spare in a store or available repair teams.

The state of the element is simulated with the generation of random numbers that pick up the element state from the failure or repair distributions. Time step by time step, the status of the system is calculated depending on the status of the single element. Those calculations are performed for several missions or all the system lifetime to predict the system unavailability and its failure rates.

The **Petri Nets** [35] inherit their name by the German physicist Carl Adam Petri (1926). They are an evolution of the Markov Graphs with Monte Carlo simulations. In this technique the accent is placed on the transitions between the states. These

transitions could be triggered by a Monte Carlo evaluation. Such an evaluation depends either on the density functions in charge for that transition or on other definable conditions like repairing teams, spares, status of other part of the system, etc. The advantage of the Petri Net compared to the Monte Carlo is the more readable system dependencies which are not "hidden" in the basic event definitions.

A comparison of the different techniques is given in table 3.5.

	Advantages	**Disadvantage**	**Current use**
Combinatorial	Easy to read.	Maintenance not so realistic.	Complex system but with an easy maintenance.
Markov	Flexible.	States Explosion.	Models of complex sub-systems.
Monte-Carlo	Very flexible.	"Hidden" information. Computation time.	Complex systems.
Petri Net	Very flexible. Clear information.	Computation time.	Complex systems.

Table 3.5: Comparison of the techniques for the evaluation of the system dependability.

3.3.4 Safety Evaluations

Safety evaluation is necessary to estimate if the system is safe enough or any improvements are needed. To guide this estimation, the Safety Integrity Levels procedure and the As Low As Reasonably Achievable (or Possible) approach will be introduced in the next sections.

3.3.4.1 Safety Integrity Levels

The procedure is defined in the IEC 61508 standard [36].

The first step in the procedure is the estimation of the gravity, per each undesired event.

That could be done building a table like table 3.6, where the event gravity is associated with the entity of personnel damage or to the money or time lost for the accelerator.

Gravity Category	Injury to personnel		Damage to equipment	
	Criteria	**# 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

Table 3.6: Gravity tables used for LHC risk definition.

The second step is the evaluation of the event exposition.

This is how often the dangerous initiator event could occur, independent of the protection system built to minimize the impact.

Table of exposition frequency, like table 3.7, could be traced.

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}

Table 3.7: Frequency categories table.

Finally, a cross table indicating the suggested Safety Integrity Levels, called a “Risk Table”, has to be generated. Such a table has to combine the previously defined frequency and gravity to provide an indication of the requested probability to fail. A cross table like table 3.8 can be generated.

The Risk Table has to indicate the suggested SIL, the Arabian numerals, and the acceptable risk number, the Latin numerals.

SIL	Risk level	Consequences							
Event frequency		Catastrophic		Major		Severe		Minor	
Frequent		4	I	3	I	3	I	2	II
Probable		3	I	3	I	3	II	2	III
Occasional		3	I	3	II	2	III	1	III
Remote		3	II	2	II	2	III	1	IV
Improbable		3	II	2	III	1	IV	1	IV
Negligible / Not Credible		2	III	1	IV	1	IV	1	IV

Table 3.8: Risk Table.

The SIL values are defined in the standard and they are summarised in tables 3.9 and 3.10. The continuous operation mode figures are simply the probabilities of the first table divided by ten thousand, approximately the number of hours in a year (8766).

The SIL suggests the probability to fail of the system that has to prevent the consequence damage given by an initiator event with a certain frequency.

If a protection system is developed and a failure frequency is calculated, it is possible to again utilise the table 3.7 to classify the frequency and, later, use table 3.8 to obtain, with the Latin numerals, the risk levels defined in table 3.11. Those

SIL	Average probability of failure to perform its design function on demand ($FPPD_{ave}$)
4	$10^{-5} < FPPD_{ave} < 10^{-4}$
3	$10^{-4} < FPPD_{ave} < 10^{-3}$
2	$10^{-3} < FPPD_{ave} < 10^{-2}$
1	$10^{-2} < FPPD_{ave} < 10^{-1}$

Table 3.9: SIL values for Low demand mode of operation (< 1/ year or <2/ check time).

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	$10^{-6} < Pr < 10^{-5}$

Table 3.10: SIL values for high demand/continuous mode of operation.

RISK	DEFINITIONS
I	Intolerable risk
II	Undesirable risk, and tolerable only if reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
IV	Negligible risk

Table 3.11: Risk levels definitions.

levels are useful to evaluate whether to further improve the system or not.

In case of redundant protection systems, like parallel systems which perform the same functions, other tables in the form of table 3.8 are suggested.

As indicated in the IEC 61508 standard, all the tables are suggestion that should be adapted to the case of study.

Currently, SIL approach is widely used for the personnel safety and it is taking place also in the industrial area.

3.3.4.2 As Low As Reasonably Achievable

ALARA is a decision structure for the risk evaluation first introduced for the individual-related radiological protection (1987) [37] and subsequently adopted and developed in several fields. Three statements are the basis of this approach:

a) Practice Justification: no practice shall be adopted unless its introduction produces a positive net benefit.
b) Optimization of the protection: all the risks shall be kept As Low As Reasonably Achievable, economic and social factors being taken into account.
c) Upper and lower bound limit: in any case, the risk must be lower than the maximum acceptable and no actions shall be taken if the risk is already below a negligible value.

The first statement simply affirms that, if there is not a real positive effect, no activity has to be started. This is the crucial part of the trade-off between advantages and disadvantages: the benefit shall justify the risk taken.

The second statement is the core of the ALARA: if the risk is too high, protections have to be implemented until a good equilibrium between protection cost and risk reduction is reached.

The last statement avows that if the risk is still too high even after a reasonable reduction, the activity must be dropped. On the other hand, if the risk is lower than certain limits, it is not necessary to improve further the protection even if it would be still “economical”.

The ALARA approach is widely used for medical and nuclear power plants. A final remark: in the SIL approach, the table of the risks such as table 3.11 is actually already an ALARA approach.

Chapter 4

BEAM LOSS MONITORS SYSTEM DEPENDABILITY

The Beam Loss Monitors System, described in chapter 2, will be analysed with the methods exposed in chapter 3.

After the hazard rate predictions, a list of performed tests will be provided. The test descriptions are useful to understand the effect of a failure mode during the FMECA. The detectable failures will lead to a false alarm. The undetectable failures could result in a loss of protection for the LHC. The failure modes analysis will be the base for the construction of the fault tree. The dependability of the system is calculated and the weakest components are identified. The variation of the calculated unavailabilities with the system parameters is discussed. The effect of some system modifications are analysed as well. The final section contains general remarks about the adopted approximations.

4.1 Hazard Rate Prediction

The BLMS is mainly composed by non-standard and new components. The hazard rates for the different components have been collected with the priorities sorted below:

1. Supplier data (S). They are given by laboratory tests carried out by the suppliers. They are regarded as accurate enough as they are based on in-production components. The uncertainty of the data is caused by the unknown test procedures, in some case, and by the likelihood that test results are “filtered” by the suppliers. It is possible to have systematic difference between the different suppliers. Nevertheless, the supplier could also give conservative estimations for the new developed components or subsystem. Finally, some consolidated components on the market had already been used in other accelerator systems, showing no worsening of the hazard rate with the radiation. For such components no worsening factor has been used.
2. Historical data (H). Some components used in the field of the high energy physics and in the design of the accelerators are very particular. No supplier data is available for such components. Hazard rates have been calculated using the long term experience of these components in the accelerator. These

hazard rates already take into account the harsh environment with temperature and radiation effects.

3. International guidelines. When either no supplier data is available or no radiation effect has been studied, conservative international standards values have been selected. The Military Handbook MIL-HDBK 217F (MIL) [23] has been chosen to compare the results with other studies made or on going at CERN. The default parameters for the calculation are an environment temperature of 30°C and commercial quality of the components. For the surface installation a benign environment factor has been chosen, while for the tunnel a ground fixed factor has been taken to consider the possible radiation effect (a factor 4 worsen than the benign one).

For the study, the "Block failure rate" and "Part count failure rate" are not used.

Component	ID	Source	HR[1/h]
Arcs and Straight Section (72 chassis/octants)			
IC (6/chassis)	-	H	4.42E-8(1)
HT connectors (12/chassis)	-	MIL	5.20E-10
Integrator (8/chassis)	OPA627	MIL	7.50E-8
Comparator (4/chassis)(2)	NE521D	MIL	1.91E-7
Monostable (4/chassis)(2)	74LS123	MIL	1.15E-7
JFET (8/chassis)	J176	S	4.56E-10
ADC (8/chassis)	AD7492	S	1.00E-9
Translator (6/chassis)	LVDS_RX CMS	MIL	2.64E-9(3)
FPGA (1/chassis)	A54SX72ASX-A	S	8.70E-9
GOH (2/chassis)	-	MIL	5.15E-6(4)
3 Km optical fibre (2/chassis)	Corning SM	MIL	3.00E-7
Optical connectors (8 pairs/chassis)	E2000 Diamond	MIL	1.00E-7
DAC (1/chassis)	AD5346	S	8.93E-11
DAC alimentation (1/chassis)	LM4140	S	1.039E-9
Status comparators (4/chassis)(5)	LMV393	S	3.96E-9
HT activator (1/chassis)	TL072CD	S	1.82E-10
Arc (45 chassis/octants)			
Power Supplies (3/chassis)	LHC 4913 and 4791	S	1.93E-9(6)
Straight Section (27 chassis/octants)			
PS Low Voltage (1/chassis)	75SX5 DELTA	S	1.90E-6(6)
PS High Voltage (2/chassis)	USR515 Haltec	S	1.90E-6(6)

Table 4.1: Prediction of the hazard rates of components of the electronics located in the LHC tunnel.
H= form historical data MIL=from military handbook, S= form supplier.

Component	ID	Source	HR[1/h]
DAB (39/points)			
Photodiodes (4/DAB)	TXP00036 Afonics	MIL	1.59E-8
Input Transceiver (4/DAB)	TLK1501RCP	S	1.60E-9
FPGA (1/DAB)	EP1530F780C7	S	1.83E-8
Memory (1/DAB)	ST M25P10	S	1.39E-10
Energy Transceiver (1/DAB)	SN74LVT245B	S	1.02E-9
Crate (3/points)			
Inhibition Switch (13/Crate)	SN74LV123A	S	2.80E-10
Beam permits IN Combiner (1/ Crate)	LM339	S	1.82E-10
Combiner FPGA (1/Crate)	EP1530F780C7	S	1.83E-8
Beam permit OUT (3/ Crate)	SN75472P	S	1.82E-10
HT DAC (1/point)(7)	MAX038	S	2.27E-8
High Tension (2/points)			
HT for 1500V for IC	NCE 3000-20	S	1.90E-5
VME crate (3/points)			
PS for VME	6000 LHC	S	1.90-5
Fans tray for VME	Fan 6000 LHC	S	3.17E-5

Table 4.2: Prediction of the hazard rates of the components used in the surface electronics.
H= form historical data MIL=from military handbook, S= form supplier.

Such analyses are implemented to estimate the hazard rate for an ensemble of elements and are too generic and approximated when compared to the FMECA. In tables 4.1 and 4.2 the relevant hazard rates are summarised. In the tables, the hazard rates are sorted per locations in the system chain and average quantities are written in the brackets.

The comments to some components of the table are listed below.

(1) The hazard rate of the Ionization Chamber is the result of a calculation using formula (3.33) with a 60% confidence level of no failure over 20 years (of 4800 hours) on 216 SPS chambers under the LHC condition. In the SPS almost 300 chambers are installed. Some of them are in the injection and extraction lines where they have been irradiated with higher dose than the one expected in more than 90% of the monitors in the LHC. Variation of the gas gain has been below 30%, considering all the monitors [38]. These chambers had not been exchanged for over 20 years, whereas the LHC chambers will be tested and eventually substituted yearly. The hazard rate deduced from this observation is probably overestimated.

(2) The comparator and the monostable used in the CFC are dual models: one component is used for two channels.

(3) The translator LVDS_RX CMS has been developed for the CMS experiment. Extensive reliability reports do not exist, even if the component has been tested in radiation environment. The reported hazard rate has been estimated in analogy with similar commercial component (TI 74AVCA164) applying a factor 2 for the young component age, as suggested by [23].

(4) GOH is a radiation tolerant component developed at CERN for the CMS experiment [18]. It serialises a 16 bit parallel bus and drives a laser for the optical fibre transmission. No standard reliability tests have been performed on these components. The MIL has been used to calculate the hazard rate. Probably the electronic chip is more reliable than the reported figure but this figure seems to be compliant with the LASER chip reliability.

(5) Only 4 comparators of the 8 present on the CFC board will be considered. They are monitoring the HT status, the HT test activation, the +5V and the -5V power supplies. Only these comparators can either miss a dangerous failure or generate a false alarm, while the other 4 provide warnings without impact on the LHC operation.

(6) The reported hazard rate for the power supplies of the tunnel electronics are orders of magnitude different. The arc supplies seem to be very reliable; the straight section supplies have a low reliability. In the second case, the number provided looks to be a conservative number while, in the first case, even if the supplier provides the quality reports, the analysis seems to be limited only to some components, hence this figure looks to be too optimistic. This point will be further discussed in the analysis (section 4.5).

(7) The HT DACs for the test initiation are present in all the Combiner cards, but only one per rack is actively used and could generate a false alarm.

Comparing the hazard rate in the tables, the weakest components are the power supplies, followed by the GOH and the optical fibre. These observations brought to the decision to double the High Tension power supplies, the VME power supplies and the optical lines. For the tunnel power supplies, no action is foreseen for the moment. See section 4.4 for a further analysis.

4.2 Testing Processes

Before the evaluation of the effects of a failure on the system, at the basis of a Failure Modes and Effects Analysis, it is necessary to define and describe the testing process. The test process will influence the behaviour of the system and its global unavailability. A general definition of a testing process reads [21]:

The Testing Process is a series of test conducted to disclose deficiencies or to verify that corrective actions will prevent recurrence and to determine compliance with specified Reliability & Maintenance requirements.

Tests will be performed not only during the operation but also during installation and maintenance phases.

The test process proposed for the BLMS are summarised in table 4.3. See the glossary for the abbreviations.

	IC	FEE	BEE	COMBINER
INSTALLATION	**Gain test** with PC board; **Barcode check** data storage.	**FEE bench test; PCB test** in the tunnel with **HT test; Barcode check** data storage.	**BEE bench test;** BEE + Combiner test on the rack with **HT test; Barcode check** data storage; **TCA checks.**	**Combiner bench test;** BEE + Combiner test on the rack with **HT test; Barcode check** data storage.
OPERATION	**HT test** after every dump.	**10 pA test and DOLC** continuously; **HT test** after every dump.	**DOLC** continuously; **TCA checks; HT test** after every dump.	**HT test** and **BIL tests** after every dump.
MAINTENANCE	**Gain test** every year before start up; **Barcode check.**	Cable by cable check with **barcode check.**	**TCA checks;** Cable by cable check with **barcode check**.	**Barcode check.**

Table 4.3: Synoptic table of the testing processes.

4.2.1 The BEE Bench Test

The Back End Electronics is checked before its installation in the tunnel. With the proper instrumentation and procedures, the functionalities of the photodiodes, the FPGA and beam inhibition switches are tested. It will be advisable to keep at least two boards per location of the surface electronics already tested, ready to be installed in the VME crates.

4.2.2 The FEE Bench Test

This test checks the Front End Electronics before the installation in the tunnel. During the test, a calibration of the outgoing frequency is done, the 10 pA generation is tested and the FPGA and GOH functionalities verified.
After the test the FEE is ready to be installed in the tunnel. Two already tested boards per octant will be kept as spares.

4.2.3 Combiner Bench Test

During this test the functionality of the Combiner electronics is fully verified. The 2 beam permit lines from the DAB cards, the 3 beam permit lines from the other Combiners, the 3 beam permit lines to the LBIS, the energy signal from the energy distribution system and the power monitoring are controlled. At least two spares Combiner have to be kept in each point, for an immediate substitution of faulty boards.

4.2.4 The 10 pA Test

The aim of the test is to assure the functionality of the FEE analogue electronics and the presence of the connections to the surface.
The DAC in the FEE generates a current of 10 pA in each channel. This causes an ADC bit change every 5 ms or a CFC count every 20 seconds. If no count arrives in 22 seconds the FPGA increases by 1 pA the current in the channel. The channel is declared blind after 5 increase of current without any counts and a status bit will be send to the surface to inhibit the beam permit. Even if a bit change could occur after just 5 ms, the noise induced into the electronics requires a longer period to take an unambiguous decision. The sensitivity of the system to this waiting time is discussed in section 4.5.

4.2.5 The Barcode Check

This test detects possible maintenance errors of the whole system. It is performed during and after every maintenance action.
During installation, an association between IC position, the IC, the cables, the FEE, the crate, the optical fibres, the BEE, the surface rack and the Combiner is created. This association is based on barcodes present on the locations and on every BLMS component. It is stored into a database in the supervising system.

During maintenance, the position of elements is checked through the database to avoid wrong assignation to the channel.

The test assures the correct assignation of the threshold values to the correct BEE channel. The values of the thresholds change with the position of the chamber around the ring (section 2.3). A wrong link between the electronics will also generate false alarm, because each FEE sends a unique ID checked by the DAB. If the ID is wrong, the DAB inhibits the beam permit.

4.2.6 Double Optical Line Comparison

The Double Optical Line Comparison (DOLC) test continuously detects either possible optical transmission errors or optical line failures.

Possibilities of errors in the frame transmission with the BLMS optical link		Error in Transmission of either Data or CRC (1=OK, 0=error)				CRC comparison			Output (A= data A; B= data B; I= beam permit inhibition)
						In the same line		BEE CRCs	
		Data A	CRC A	Data B	CRC B	A	B		
a	No errors	1	1	1	1	1	1	1	A
		Single error							
b	Error in transmitted CRCB	1	1	1	0	1	0	1	A
c	Error in transmitted DataB	1	1	0	1	1	0	0	A
d	Error in transmitted CRCA	1	0	1	1	0	1	1	B
e	Error in transmitted DataA	0	1	1	1	0	1	0	B
		Double error							
f	Errors in DataB + CRCB	1	1	0	0	1	0	0	A (=c)
g	Errors in CRCA + CRCB	1	0	1	0	0	0	1	A
h	Errors in DataA + CRCB	0	1	1	0	0	0	0	I
i	Errors in DataB + CRCA	1	0	0	1	0	0	0	I (=h)
j	Errors in DataA + DataB	0	1	0	1	0	0	0	I (=h)
k	Errors in DataA + CRCA	0	0	1	1	0	1	0	B (=e)
		Triple or higher error							
p	4 (or 3) transmission errors	0	0	0	0	0	0	0	I (=h)
		Error in the Generation of either Data or CRC							
q	[(a)]CRC not corresponding to the data but equal to each other	1	0[(a)]	1	0[(a)]	0	0	1	A (=g)
r	[(b)]Data of line B different from data of line A: signal generation error	1	1	1[(b)]	1[(b)]	1	1	0	I

Table 4.4: Double Optical Line Comparison table.
In the first column the possible failure cases are listed. The second column lists the failure position with 0. The third column contains the result of the comparisons and the last shows the chosen line (A, B) or the inhibition request (I).

Two BLMS frames are generated in the tunnel electronics and transmitted with a CRC. Both signals are checked for errors by the surface FPGA (BEE) which regenerates a CRC and compares it with the one generated in the FEE. In addition the CRCs generated in the BEE are compared in order to check if they (as well as the data) are identical.

Following table 4.4, one of the two signals is selected or a beam permit inhibition is generated.

The data logging includes the number of the counted errors per line to estimate the Bit Error Ratio (BER) variation. This operation is important to monitor the fibre/component wearout due to several factors (radiation, temperature, aging…).

If the BER exceeds a certain level, as reported in section 4.2.6.1, maintenance on the transmission line shall be planned (transmission or receiving mezzanine replacement, optical fibre substitution).

4.2.6.1 Acceptable Bit Error Ratio

In the BLMS design, the check of the bit error is provided by the DOLC. The Bit Error Ratio (BER) increases, for example, following the degradation of the optical fibre. The receiving BEE FPGA counts the number of transmission errors and, in case of a high BER value, a maintenance action has to be planned. An acceptable probability of failure P_F of 1E-6 is derived by requiring a minor contribution of the optical link failures to the generation of False Alarm per year. This estimation generates less than one False Alarm per year taking 642 optical links and 400 missions into account.

The acceptable BER is estimated as follows.

For a frame of N_{bits} bits and a given BER, the probability F_w that at least one of the bits in the frame is wrong is binomially distributed and reads:

$$F_w = 1-(1-BER)^{N_{bits}} . \qquad (4.1)$$

In case of redundant frame, either double frame transmission or redundant lines, the probability R_w that N_r redundant frames in a systems fail is:

$$R_w = F_w^{\,N_r} . \qquad (4.2)$$

The acceptable probability P_F that there is at least one error in the transmission of N_f frames is:

$$P_F = 1-(1-R_w)^{N_f} \,. \qquad (4.3)$$

The probability of a transmission error P_F can be expressed as function of the BER using the above derived formulas:

$$P_F = 1-(1-(1-(1-BER)^{N_{bits}})^{N_r})^{N_f} \cong 1-(1-(N_{bits}\cdot BER)^{N_r})^{N_f} \cong N_f(N_{bits}\cdot BER)^{N_r} \qquad (4.4)$$

In the BLMS setup, the number of frames is calculated dividing the length of the mission (12 hours) by the transmission period (40 μs) which results in N_f= 1.08 E9. The current BLMS frames is made of 256 bits, see section 2.5.3, so N_{bits}=256.

For the cases of N_r equal to one or two, the probability P_F is plotted as function of the BER in figure 4.1. The BER plot limits have been chosen around its typical value for the evaluation of the performance of the optical components. A BER of 1E-11 results in a probability of failure of almost 1 for a single transmission. This value is unacceptable. To minimize the impact of the BER, the frame has to be transmitted at least twice. A double transmission guarantees an acceptable level of error up to a BER of 1E-10.

When the incoming optical power is higher, the BER is lower. The variation of the BER is of almost 2 orders of magnitude per optical dB. The optical power changes with the age of the optical component, either for the irradiation or the normal wear out. The initial optical power budget of the BLMS is 9 dB. After an attenuation of 9

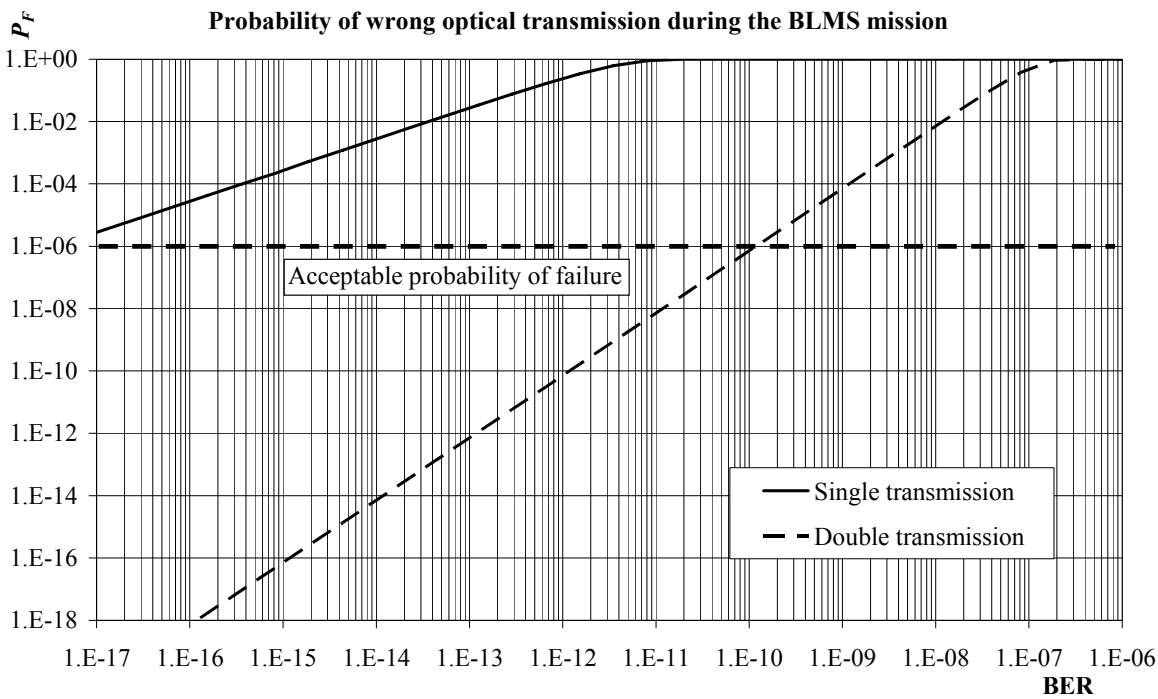


Figure 4.1: Probability of an erroneous digital transmission during a BLMS mission.

dB in the optical line the BER would be 1E-10. This degradation can be monitored by the BER, due to its high sensitivity to the value of the incoming power.

The final decision to double the optical lines, rather then simply double the transmission on a single line, is motivated by dependability considerations on the components of the optical line, see section 4.4.

In the BLMS setup, it is advisable to change an optical line when the recorded BER is around 1E-10.

4.2.7 High Tension (HT) Tests

During this test, possible malfunctions of the tunnel electronics and the electrical connections failures are detected.

The test will be performed during installation with a PC board and after every dump during operation.

The HT test could be generated by the Combiner card (during operation) or by the PC board. The test actually consists of two different tests.

HT Low Frequency modulation (HTLF): generation of an HT modulation with a frequency between 0.01 and 1 Hz. This oscillation tests the IC electronics degradation and detects if a channel is blind. Software of the supervising system and database should be used to detect variations and to plan maintenance. The

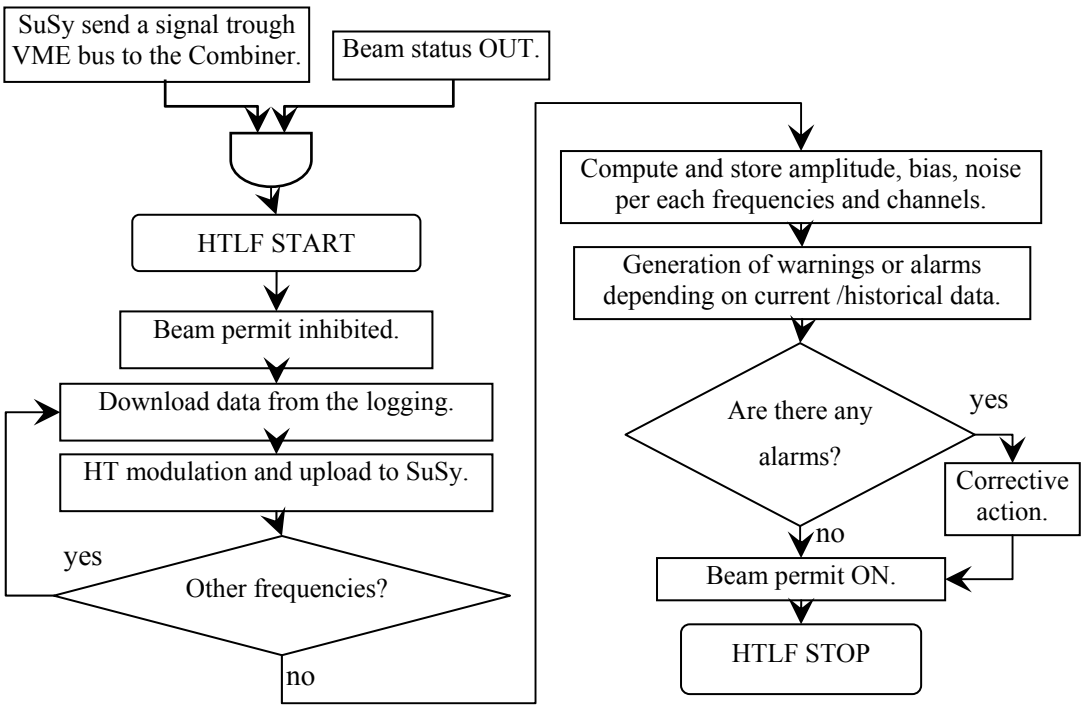


Figure 4.2: Simplified flowchart for HTLF test.

important steps of the procedure are (see also figure 4.2):

1. If the beam status received from the LBIS is OUT, the supervising system initiates the test sending a signal to the Combiner card trough the VME crate. The OUT status is essential to guarantee that the beam is out of the accelerator and no additional hazard has to be expected during the test. For the same reason, the Combiner inhibits the beam at the beginning of the test.
2. The Combiner downloads the modulation data from the VME bus. The data consists of the amplitude, frequency and number of periods of the modulation.
3. The Combiner drives the HT source generating a modulation with the desired characteristics. It uploads the values of the counting by using the data logging software, with a rate at least 20 times the modulation frequency. The supervision system reconstructs the sinusoidal signals for the test period.
4. Point 2 and 3 are repeated for all the desired frequencies.
5. The SuSy software has to extract per each channel the amplitude, the bias and the noise (standard deviation between the measurement and the expected sinusoidal).
6. The SuSy software has to compare this data with a database of previous data and generate warnings and/or alarms if there are variations in the values.
7. In case of an alarm, an action must be taken (FEE board substitution, channel masked, setting modification, external problem removed).
8. If there is no failure, the beam permit of the BLMS is set to ON.

Table 4.5 contains the proposed warning levels

Measurement	Warning	Alarms
Average amplitude	Variation of 5% w.r.t. history	Variation of 10% w.r.t. history
Bias	< 9 pA or big historical variation (also for wrong cable connection)	<7 pA
Noise	σ/ave > 5%	σ/ave > 10%

Table 4.5: Suggested alarms for the HTLF test.

HT Activation Test (HTAT): generation of steps on the HT line to trigger a test of the channels in the FEE. The DAC in the FEE generates higher current to initiate beam inhibitions in the 8 channels. The step by step procedure is described as follows (see figure 4.3):

1. If the beam status received from the LBIS is OUT, the supervision system initiates the test sending a signal to the Combiner card trough the VME crate.

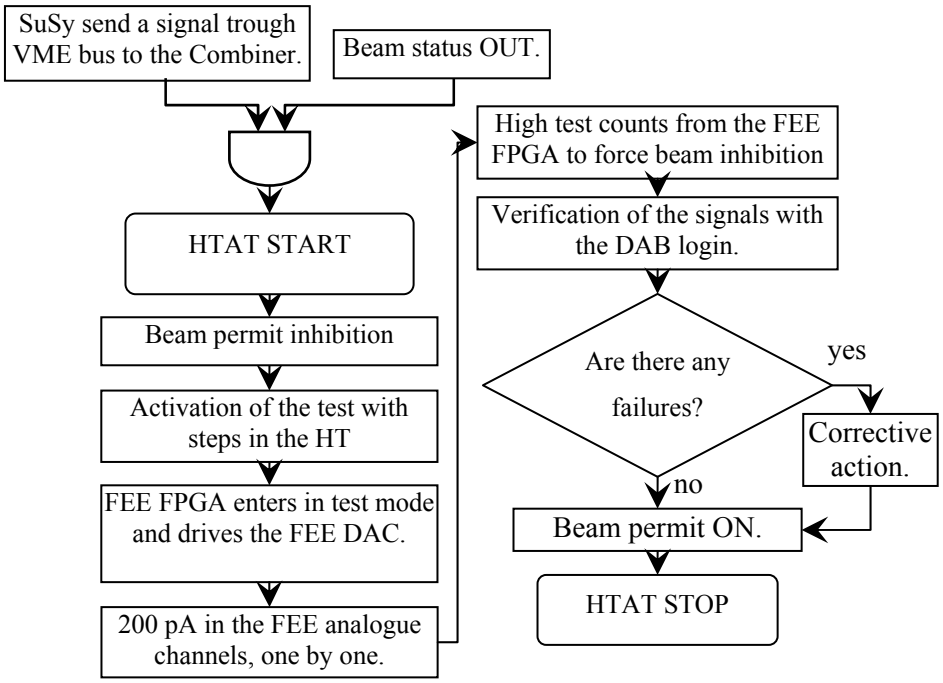


Figure 4.3: Simplified flowchart for HTAT.

The OUT status is essential to guarantee that the beam is out of the accelerator and so no additional hazard has to be expected during the test. For the same reason, the Combiner inhibits the beam at the beginning of the test.

2. The Combiner triggers the HT source to generate a step of 90 V in the high tension of the IC. This step is detected by a comparator in the FEE. The FPGA enters in test mode, modifying also the test mode status bit. Finally the combiner decreases the tension below the 1326 V to verify the functionality of the HT status.
3. The current source in the FEE is driven by the tunnel FPGA. The source generates a 200 pA current into the analogue electronics, channel by channel, to verify the proportional answer.
4. After the channel scan, the FEE FPGA transmits test data by setting high counter value, channel by channel, to simulate an intense loss. The BEE reacts at this high test values removing the beam permit and marking the dump request on the logging.
5. The SuSy software reads the values of the counting and verifies that the channels were at the highest level during the planned test time, trough the logging at the surface. If no beam permit inhibition request is registered channel by a channel, the threshold tables have to be verified or the FEE board has to be substituted.

The use of the two tests permits the discrimination if a failure is downstream the FEE, both tests detect it; or if the failure is upstream, only the HTAT registers the failure.

If there is a crucial channel which is out of the specification, it is advisable to substitute the electronics or the deteriorated IC as soon as possible. It would be better to perform the HTLF later after the dump, to minimize external irradiation influence.

4.2.8 The PC Board (PCB) Test

This test permits an easy check of the Front End Electronics and connections with a laptop. It is not an additional test but an alternative way to perform the HT tests (section 4.2.7). It can be performed in the tunnel or in the surface.

It consists of the use of an interfacing board [39] between the BLMS electronics and a laptop. The optical fibres can be connected to the PC interface. In this way it is possible to immediately visualize the signals from the FEE. An HT test can also be triggered either by the PC interface itself or by the supervision system.

Surface tests are useful to check the link from the tunnel to the surface. Verification of the FEE board ID, sent with the signals, can be used for this purpose.

In the tunnel, the test will be used for a fast check of the gain test (section 4.2.9) during maintenance and installation.

4.2.9 Gain Test

The aim of the test is the check of the IC inner gas and of the monitor connections by using a signal generated by a radioactive source. It will be performed every year before the LHC start-up. During the installation, the PCB will be used (section 4.2.8).

A radioactive source will be positioned on a marked position on the external IC cylindrical tube. The laptop, or the supervision system, records the signal from the chamber. The generated signal verifies if the monitor is assigned to the correct channel. This verification avoids misconnection failures. The signal and the result of the test are stored in a database. The chambers with an excessive variation of

the signal with respect to the DB could be affected either by a gas leak or insulation failure and they must be substituted.

4.2.10 Thresholds and Channel Assignment (TCA) Checks

The procedure to modify and check the Thresholds tables and Channel Assignment table in the BEE memory is described below. Such tests are performed to assure the integrity of the memory. The memory could be damaged by mechanical or electrical effects. Also the effect of the cosmic rays may not be negligible on the whole BLMS. As reported in [40], the cross section for the Single Event Upset to the cosmic ray of the used memory (ST M25P10) is lower than 1E-7 cm^2 per device. With a cosmic ray flux of 5.56E-3 s^{-1} cm^{-2} at Geneva [41], the hazard rate becomes 5.56E-10/s, i.e. 2E-6/h. Considering 4800 hours of LHC operation during one year and the 325 components, up to 3 induced errors per year could be expected in the BLMS. This calculation is probably overestimated for the high cross section, but it highlights that, for huge system and long working times, also these external factors can influence the electronics.

The threshold table contains the beam inhibition values which depend on the loss duration and the beam energy. The channel assignment table is used to define a channel as inactive or as linked to the maskable or unmaskable output. A threshold higher then foreseen could jeopardize the system. An unmaskable channel marked as either maskable or inactive lead to a dangerous situation too. For this reason, the modification and the checking of such tables requires particular attention.

The values in the tables could be changed during different phases of the LHC operation. During installation the values should be initialized. During the operation phase without the beam, the values could be refined. During the maintenance phase they could change following, for example, a relocation of the monitors. These operations require reliable software in the supervision system.

Two procedures are suggested to be safe against the accidental assignments: one for the table Modifications (TCAM), when there is no beam in LHC, and the other for the table Checking (TCAC) during the beam time.

For the <u>TCAM</u>, the software for the modification of the tables should be started on two different interfaces, A and B. The terminals download the tables which contain the values of for the BEE thresholds which have to be modified. The modifications

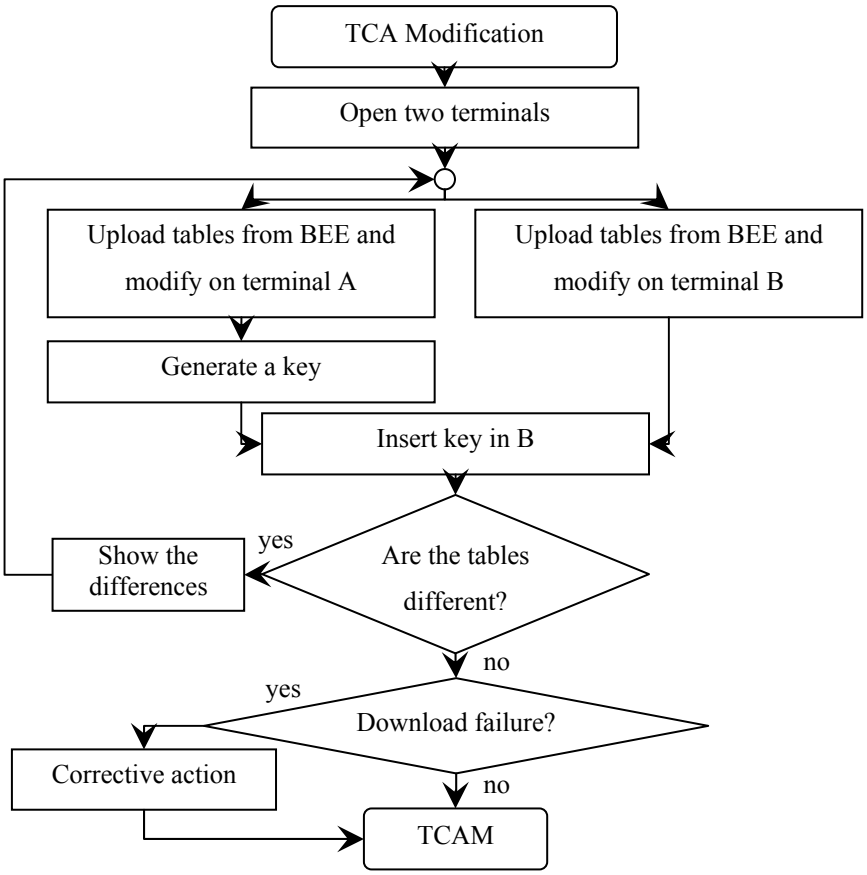


Figure 4.4: Simplified flowchart of TCAM during installation.

should be applied on both terminals. To upload the modifications, the request should be sent by the interface A. This action generates a software key that has to be inserted in 10 seconds in the interface B to confirm the upload. Then the software compares both tables. If they are different, the software does not load the tables to the BEE or database. The differences in the tables are highlighted and the process restarts from the insertion. If they are equal, the software uploads the tables to the BEE and to the database. Just after the upload, the software checks the correct transmission by downloading the data. If there is an error at this phase, a possible hardware/software failure should be solved.

Look at figure 4.4 for the simplified flowchart of the TCAM.

During the LHC operations, the TCAC checks the functionality of the memory and the values of the energy (see figure 4.5). The crate CPU continuously compares the tables in the BEE of its crate with the one in the database. It also reads and sends the energy value to the supervision system. If the tables do not match, the crate CPU does not send the OK to the supervision system. In this case, the SuSy software checks if there is an error either in the CPU memory or in the BEE ones. If the failure is in the CPU memory, the SuSy software tries to correct it. If it not

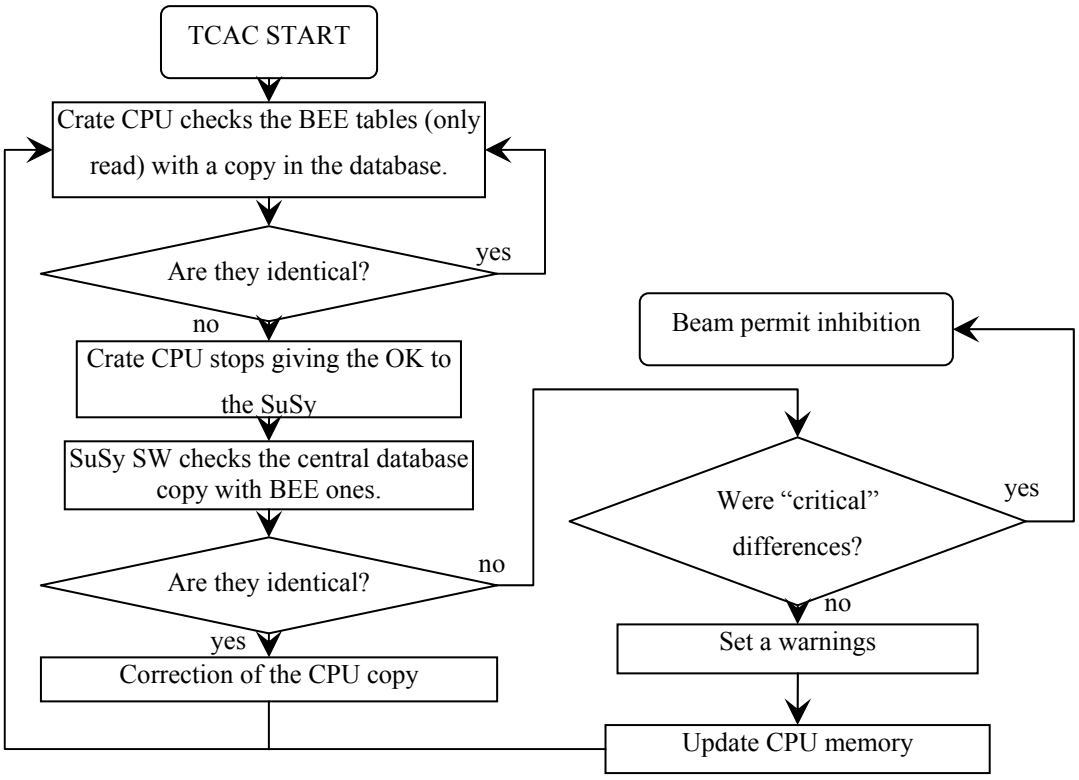


Figure 4.5: Flowchart oh TCAC during operation.

possible, the software excludes the CPU tables from the checking and asks for a maintenance action. If the failure is in the BEE memory two cases are possible. If it is a safe error (threshold limit lower then desired or safe channel assignment set to a safer status) it marks that the board should be substituted after the next dump; if it is an unsafe error, the software inhibits the beam permit.

During this check, the current energy value is checked too. In case of wrong lower energy, the beam permit is inhibited as well.

4.2.11 Beam Inhibition Lines (BIL) Tests

This test should assure that all the beam permit lines work properly before the injection of the beam in the LHC. The test is performed in two phases: one for the VME crate lines and the other for the LBIS lines (see section 2.8.5).

To test the VME crate lines, a request will be generated via the supervising system. A signal is consecutively sent to each DAB via the VME bus. The DAB forces the beam inhibition on the two channels, one by one, and the crate CPU reports the combiner status to the supervision system. The timing of the different steps has been tuned to assure the synchronization of the subsystems.

The LBIS test will be triggered by the LBIS system and it will force the combiner card of each crate to inhibit the 3 beam permit lines to the LBIS, one by one. The analysis of the test result is done by the LBIS system.

4.2.12 Test Processes Conclusions

The operative tests are eight: Barcode, Gain, HTLF, HTAT, 10pA, DOLC, TCA, BIL. The PCB test is a method, useful for the maintainers, to perform the HT tests and the bench tests are usual check-in electronic tests.

Figure 4.6 shows a flow chart diagram for the test usage. It starts with the installation of the instrumentation in the tunnel after the bench tests. During the installation the barcode database is created and checked. Later, the BEE at the

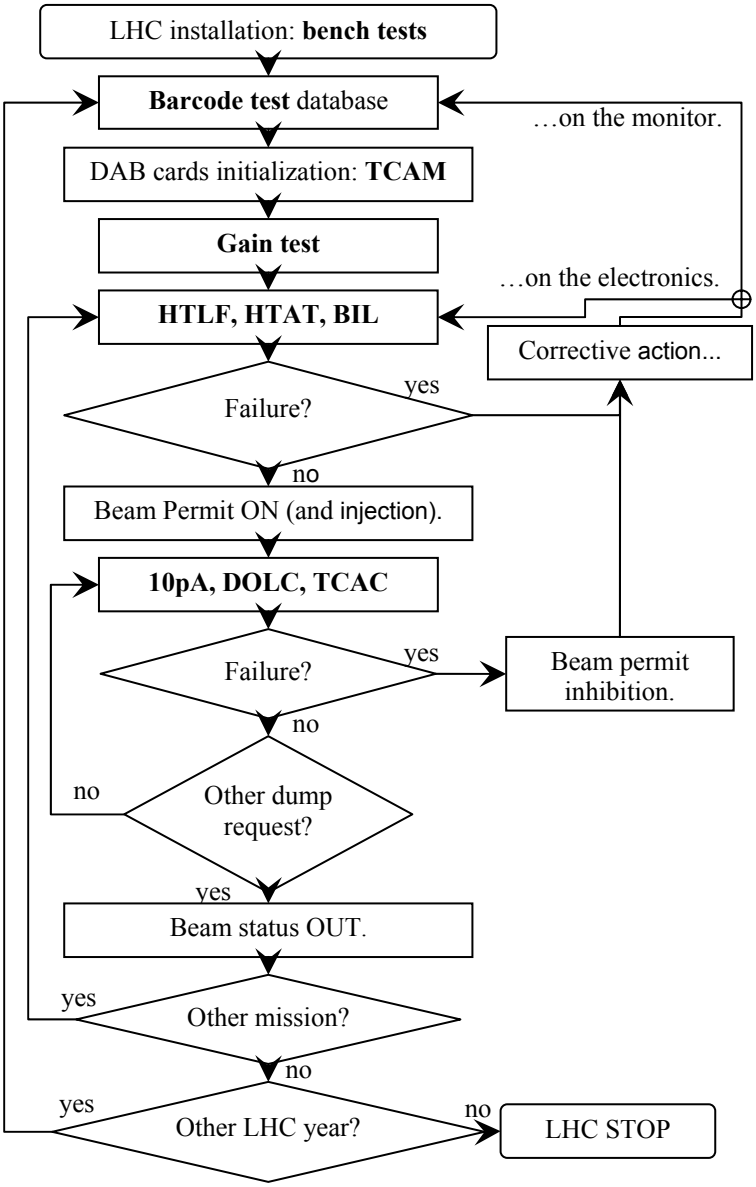


Figure 4.6: Synoptic flow chart of the BLMS tests.

surface is initialized with the proper TCA. The database for the monitoring of the IC is created with the gain test.

The mission tests (the HTLF, the HTAT and the BIL) are performed. If there is any failure, the proper corrective action can be performed.

If there are no failures, the beam permit is set to ON and the injection of the beam into LHC is allowed. Just after the beam permit ON, the three continuous tests commence. If they detect a failure, either in the FEE or in the optical link or in the BEE, a beam inhibition request is performed. The tests run continuously until another dump request is made either by BLMS or by another system. The beam status indicates that there is no beam in LHC.

If there is the need to start a new mission the cycle restart from the mission tests which check again that everything is ready to start.

Before another year of LHC operation, the barcode database has to be updated with the performed maintenance. Also the monitors have to be checked with the Gain test.

4.3 FMECA

The Failure Modes, Effects and Criticalities Analysis, as described in section 3.3.2, is a technique used to analyse the reaction of the system to a failure. It provides a check list of all the possible failure modes that could affect the functionality of the system.

The adopted guideline is the FMD-97 [33]. It has been chosen for its completeness and for the inclusion of more recent apportionment data. If the sum of the failure mode apportionment, due to the approximation used in the guideline, is not 100%, the failure mode with the highest percentage has been corrected. The introduced absolute error is never greater than ±0.1%.

The FMECA has been performed on the system layout described in chapter 2. Conservative hypotheses have also been taken:

1. Parametric variations of components have been assigned to the most critical effect, even if the components could drift toward a safer failure. For example, a wrong reading of the temperature sensor in the DAB card is assumed to be toward the high temperature, which generates a false dump, rather than toward a lower temperature, which generates a warning.

2. In case of monitored element, such as High Tension or power supplies, the failure has been modelled as instantaneous: no degradation will be monitored. With this assumption, the status monitor will not provide any improvement of maintenance. On the contrary, they will generate false warning requests.
3. The failures in the beam energy transmission are assumed to generate a false alarm. Actually, the procedure is to set the energy value at 7 TeV (see section 2.8.2), which does not necessary mean false alarm generation.
4. The maskable and unmaskable channels are treated in the same way, neglecting the possible false alarm reduction given by the masking.
5. The check-in tests, sections from 4.2.1 to 4.2.3, are assumed to be not effective in the detection of the early failures. No reduction of either the failure mode apportionment or of the hazard rate has been applied in the FMECA.

The full FMECA, following the model of the MIL-1629 [31] is reported in the appendix B. The FMECA has been performed on 5 levels. At the top level, level zero, the 3 End Effects of the BLMS are listed: damage risk, false alarm and warning. At the level 1 the failure modes are collected per location: in the tunnel or at the surface. At the level 2 the subsystems are analysed: 3 in the tunnel (common configuration, arc power supply, straight section power supply) and 4 at the surface (DAB, Combiner, HT power supply, VME crates). Level 3 is constituted by a first collection of the components failure modes. Level 4, the basic one, is the list of the components failure modes, as reported in the FMD-97 [33]. Figure 4.7 shows the structure of the first 4 levels. The quantities of the components are the same as listed in tables 4.1 and 4.2 for the prediction of the hazard rate.

The hazard rates are calculated bottom-up: they start from the base hazard rates of the prediction, they are subdivided to the failure mode with the apportionments and they are added up to the top, effect by effect, multiplied by the quantities (see equation (3.37)).

The BLMS will have a general failure rate of approximately 1.06E-2/h, i.e. one maintenance action every 4 days. The failure rates for the False Alarm and for the Warning generations are 2.73E-3/h and 7.37E-3/h respectively (see page 166). The fault tree analysis (see page 214 and 215) will show that these results are acceptable, even if they do not take into account the redundancies of the system. The hazard rate for the Damage Risk is widely overestimated with the FMECA. This difference in the estimated hazard rate is because the FMECA hazard rate is

constructed by summing up the failures of all the channels, and not only the failure of the one channel that has to detect the dangerous loss.

For the criticality analysis, three severities have been defined with their weighting expressed in induced downtime hours, as illustrated in table 4.6.

End Effect	Downtime [h]
Damage Risk	720
False Alarm	3
Warning	1

Table 4.6: Severity table for the BLMS.

Figure 4.7: Diagram of the FMECA from level 0 to 3. Block name, criticalities and failure rates are reported.

The 720 hours of downtime correspond to the 30 days necessary to substitute a damaged magnet. A maximum of 3 hours is required to recover after a false alarm generation. The time required to change a redundant or not crucial component is one hour. These severities are a pejorative hypothesis: a warning could be performed during the ramping down phase, leading to no downtime generation; a false alarm can be generated at the end of the mission, causing downtime to less than 3 hours; a channel can be blind but not subjected to any dangerous loss, resulting in no damaged magnet.

The ideal beam phases are summarised in figure 4.8. The downtime is generally taken as 3 hours to be more conservative and to consider eventual operative delays.

The criticalities are calculated multiplying the hazard rates of the failure mode times the mission time (12 hours) and the severity of the End Effect, see equation

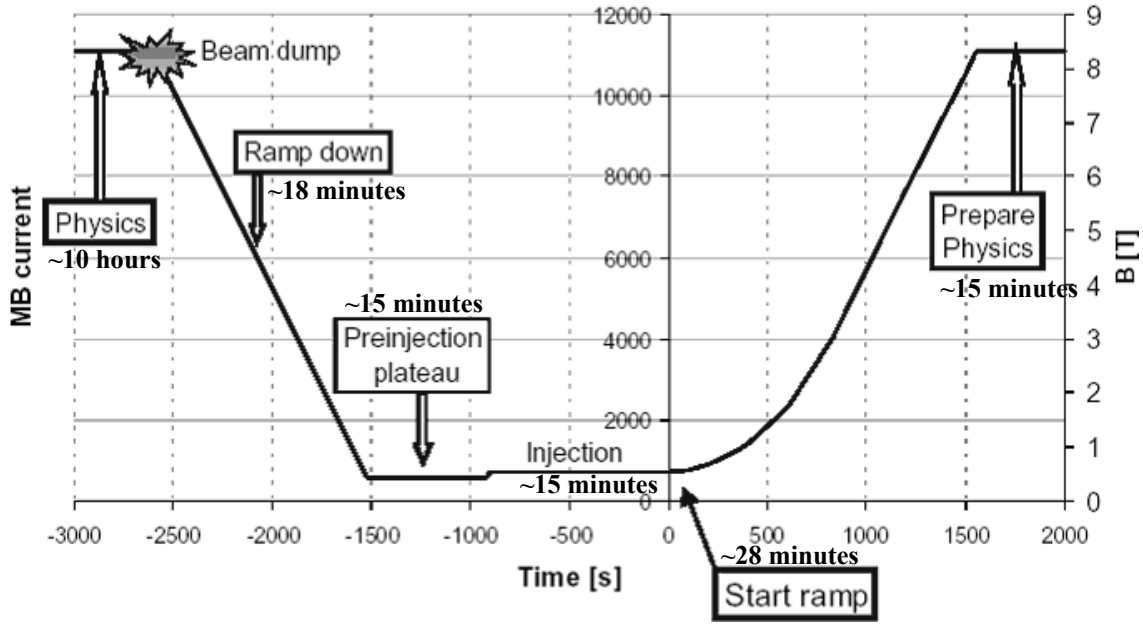


Figure 4.8: Dipole magnet current and field during one LHC mission. The different beam phases are indicated [6, p 524].

(3.38). Such a criticality expresses the number of hours lost during the mission generated by the failure mode.

The criticality figures are not significant for the Damage Risk at the top level, but only at the bottom ones, a cause of the construction of the hazard rates.

The BLMS components are ordered in table 4.7 with decreasing criticality. The VME fan tray and the VME power supply are between the most critical, thank to their high failure rates. The possibility that the VME crate could operate with a reduced cooling and the 2oo3 redundancy is not taken into account in the analysis. The components with the highest net criticality are the integrator, the IC and the monostable (the High Tension power supplies are redundant). The criticality of these components is given by their functions, which could generate a Damage Risk. In the fault tree analysis, it will be shown how the criticality of the amplifier and of the monostable has been reduced with the 10pA test, while the IC becomes more critical due to the Gain test executed only annually.

This criticality analysis is limited by not taking into account the quantity of the component in the system. In the BLMS this limitation is reflected by an underestimation of the criticality of the components which have a high probability to generate either a false alarms or a warning.

This limited validity of the results is one of the defects of the FMECA. In case of complex system, with redundancies or subsystem failures which do not propagate

Block Name	Description	Failure rate [1/h]	Criticality [h/mission]
#fantray	VME fan trays	3.17E-05	1.14E-03
#integrator	Integrators in the FEE	7.50E-08	6.15E-04
#IC	Ionization Chambers	4.41E-08	3.13E-04
#PSVME	VME PS	1.90E-05	2.28E-04
#PSHT	HT Power Supplies	1.90E-05	2.28E-04
#monostable	Monostables in the FEE	1.16E-07	1.28E-04
#PSSSLV	Low Voltage PS in the SS	1.90E-06	6.84E-05
#PSSSHV	High Voltage PS in the SS	1.90E-06	6.84E-05
#GOH	GOHs in the FEE	5.15E-06	6.18E-05
#Combiner FPGA	Combiner FPGA	1.83E-08	4.79E-05
#comp	Comparators in the FEE	1.91E-07	4.31E-05
#FPGATX	Transmission FPGA in FEE	8.70E-09	1.90E-05
#FPGARX	Receiving FPGA in the BEE	1.83E-08	1.64E-05
#translator	Translators in the FEE	2.64E-09	1.04E-05
#10pASource	10pA Sources in the FEE	1.13E-09	9.01E-06
#fibre	Fibres, 3 km	3.00E-07	3.60E-06
#ADC	ADCs in FEE	1.00E-09	3.43E-06
#OFcon	Optical connectors pairs	1.00E-07	1.20E-06
#BPswitch	Backplane switches	2.80E-10	6.12E-07
#status	Status monitors in the FEE	1.19E-08	4.26E-07
#HT DAC	HT DAC in the combiner	2.27E-08	2.91E-07
#transceiver	Transceivers in the BEE	1.02E-09	2.47E-07
#temperature	Temperature sensors in the BEE	1.14E-08	2.45E-07
#photodiode	Photodiodes in the BEE	1.59E-08	1.91E-07
#jfet	JFETs in the FEE	4.56E-10	1.50E-07
#memory	Memories in the BEE	1.39E-10	1.38E-07
#PSarc	Power supplies in the arc	1.93E-09	6.94E-08
#Com_BP_in	BP comparators in combiner	1.82E-10	4.09E-08
#TLK	TLK in the BEE	1.60E-09	1.92E-08
#HTcon	HT connectors	5.20E-10	1.87E-08
#LBIS switch	LBIS beam permit switches	1.82E-10	6.54E-09
#HT activator	HT activators in the FEE	1.82E-10	2.27E-09

Table 4.7: BLMS components sorted by criticality for a mission time of 12 hours.

to the zero level, its calculations are partial and approximated. Nevertheless, it provides a good source for both the basic events and the layout for the fault tree analysis.

4.4 The Fault Tree Analysis

Three top gates have been defined: one for the risk of damage, one for the risk of false alarms generation and the last for the warnings generation. The basic events

are the failure modes at the bottom level, level 4, of the FMECA (see previous section and appendix B). The Fault tree diagrams are collected in the appendix C. The system has been split in seven logic subsystems: in channels, digital FEE, tunnel Power Supplies, optical link, DAB, Crate electronics and the VME unit. Table 4.8 lists the subsystems with their components and the reference sections.

Logic Subsystem	Components	Sections
Channel	HT connectors, IC with its signal cable and the CFC	2.4 and 2.5.1
Digital FEE	FPGA, the 10pA source and the FEE statuses	2.5.3
Tunnel Power Supplies	Arc PS, Straight Session PS	2.6
Optical link	GOH, fibre, photodiode, TLK	2.5.3 and 2.7.1
BEE	Receiving FPGA, mezzanine memory, transceiver	2.7
Crate electronics	Beam permit daisy chain, Combiner, HT power supply	2.7.2 , 2.8 and 2.9
VME unit	VME PS and ventilation	2.9

Table 4.8: Subdivision of the BLMS in logic subsystems with section references.

The failure modes of the subsystems are further categorised with their testing frequency: Continuous testing (the fail safe failures, the status monitored failures and the DOLC), the Logging check (the TCA test), the 10pA test, the Mission tests (HT tests, BIL tests) and the Yearly test (Gain test).The fault tree levels are sorted by logic subsystem following the signal chain and by ascending testing period.

During the simulation no approximated methods have been used. Only the Optical Link construction has been approximated for the False Alarm and Warning top gates using the rare event approach. See sections 4.4.2 and 4.4.3 for details.

Nevertheless, the rare event approach is a flexible tool to easily estimate the impact of the different events on the system, with a negligible loss of precision in the case of probability, i.e. unavailability, lower then 1E-3. This approximation is widely used in section 4.5. In the case of constant hazard rates, the unavailability of the event i, $Q_i(t)$, and its unconditional failure intensity $w_i(t)$ read, in this approximation:

$$Q_i(t) = 1 - e^{-\lambda_i t} \approx \lambda_i t + o(\lambda_i t)^2 , \tag{4.5}$$

$$w_i(t) = \frac{dQ_i(t)/dt}{1 - Q_i(t)} \approx \frac{dQ_i(t)}{dt} \approx \lambda_i + o(\lambda_i t) , \tag{4.6}$$

where λ_i is the hazard rate of the event.

The basic events of the fault tree are associated with three main failure models: the rate model, the dormant model and binomial ones.

The rate model takes into account the possibility of repairing a component after a failure. It has been used in the modelling of the redundant VME power supplies. The dormant model is used to calculate the Damage Risk. It takes into account the inspection interval of the testing procedure. The binomial model is mainly used in the False Alarm evaluation, to consider the large amount of components in the system.

The rate model is a basic model and it is described by the time dependent equations (3.24). In the BLMS a constant repair rate of 1/h has been assumed.

The dormant model allows calculating the unavailability in case of tests which regenerate the component as good as new. The time dependence of the unavailability becomes as depicted in figure 4.9. In case of no repairing process, the maximum dormant unavailability Q_D^{MAX} is:

$$Q_D^{MAX} = 1 - e^{-\lambda\tau}, \qquad (4.7)$$

where λ is the hazard rate of the event and τ is its inspection interval. In the rare event case of $\lambda\tau<<1$, the maximum dormant unavailability is $\lambda\tau$ and the average ones is $\lambda\tau/2$. For not repairable events, the unconditional failure intensity *w(t)* is identical to the hazard rate.

The binomial model simulates the failure of one or more components out of a

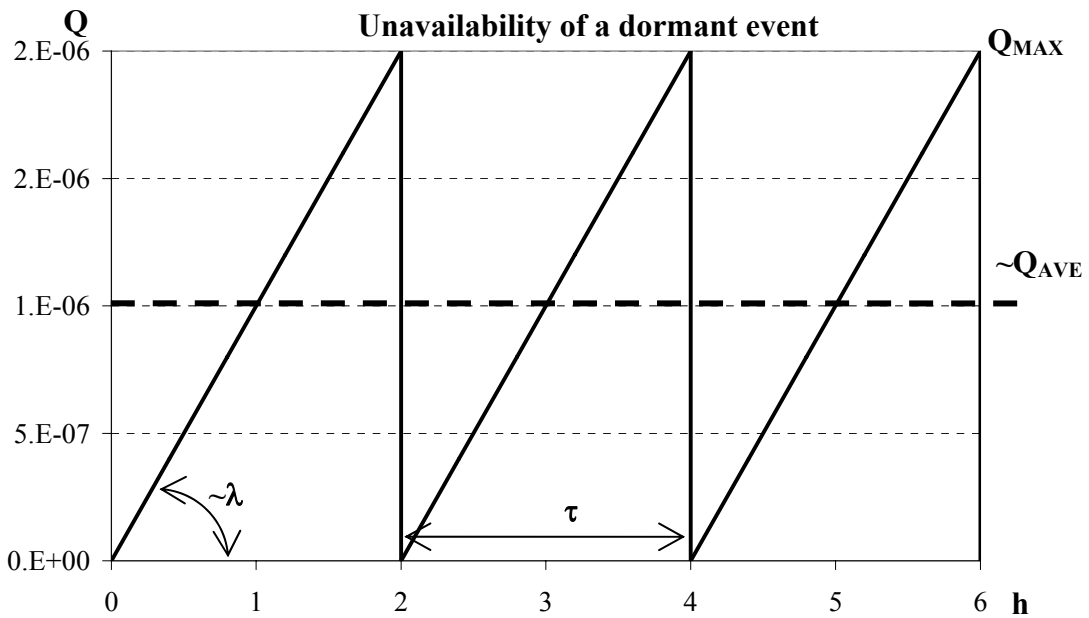


Figure 4.9: Dormant unavailability Q(t) in case of model with hazard rate λ and inspection period τ.

certain amount. The used formulas read:

$$q(t) = \frac{\lambda}{\lambda + \mu}\left(1 - e^{-(\lambda+\mu)t}\right), \tag{4.8}$$

$$Q_{BIN}(t) = \sum_{k=m}^{n} \frac{n!}{k!(n-k)!} \cdot q^{k}(t) \cdot (1 - q(t))^{n-k}, \tag{4.9}$$

$$w_{BIN}(t) = m\lambda \sum_{k=m}^{n} \frac{n!}{k!(n-k)!} \cdot q^{k-1}(t) \cdot (1 - q(t))^{n-k+1}, \tag{4.10}$$

where *q(t)*, following eq. (3.24), is the unavailability of an element in the ensemble, *n* is the number of components in the ensemble, *m* is the minimum number of units which have to fail to make the ensemble failed, $Q_{BIN}(t)$ is the unavailability of the ensemble and $w_{BIN}(t)$ is it unconditional failure density. In case of $\lambda t << 1$ and no repair the previous formulas read:

$$Q_{BIN}(t) = \frac{n!}{m!(n-m)!}(\lambda t)^{m}, \tag{4.11}$$

$$w_{BIN}(t) = m\lambda \frac{n!}{m!(n-m)!}(\lambda t)^{m-1}. \tag{4.12}$$

Four types of gates will be used in the calculation: the AND, OR, XOR and the 2oo3 gates.

The AND gate accepts two inputs, A and B, and returns the following Q^{AND} and w^{AND}:

$$Q^{AND}(t) = Q_1 Q_2 \approx (\lambda_1 \lambda_2) t^2, \tag{4.13}$$

$$w^{AND}(t) = w_1 Q_2 + w_2 Q_1 \approx 2(\lambda_1 \lambda_2) t. \tag{4.14}$$

In the case of an OR gate, most common case in the BLMS,

$$Q^{OR}(t) = Q_1 + Q_2 - Q_1 Q_2 \approx (\lambda_1 + \lambda_2) t, \tag{4.15}$$

$$w^{OR}(t) = w_1 + w_2 \approx (\lambda_1 + \lambda_2). \tag{4.16}$$

The OR gate can be generalised for a case of n inputs and becomes like the binomial model with m=1.

The exclusive OR, represented by the XOR gate, has the following unavailability and unconditional failure intensity:

$$Q^{XOR}(t) = Q_1 + Q_2 - 2Q_1 Q_2 \approx (\lambda_1 + \lambda_2) t, \tag{4.17}$$

$$w^{XOR}(t) = w_1 + w_2 \approx (\lambda_1 + \lambda_2). \tag{4.18}$$

It is identical with the OR in the rare event approximation.

The last case in the BLMS is the 2 out of 3 configuration, used for the VME power supplies:

$$Q^{2oo3}(t) = Q_1Q_2 + Q_1Q_3 + Q_2Q_3 - 2Q_1Q_2Q_3 \approx (\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3)t^2, \quad (4.19)$$

$$w^{2oo3}(t) = w_1(Q_2 + Q_3) + w_2(Q_1 + Q_3) + w_3(Q_1 + Q_2) \approx 2(\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3)t. \quad (4.20)$$

In table 4.9 a summary of the $Q_i(t)$ and the $w_i(t)$ for the different used methods is provided including the rare event approximations.

Method	Parameters and hypotheses	$Q_i(t)$		$w_i(t)$	
		Exact	Rare event	Exact	Rare event
Dormant Max	λ and τ (μ=0)	$Q_D^{MAX} = 1 - e^{-\lambda\tau}$	λτ	λ	λ
Dormant Ave	λ and τ (μ=0)	$Q_D^{AVE} = 1 - \frac{1 - e^{-\lambda\tau}}{\lambda\tau}$	λτ/2	λ	λ
Binonomial	λ, m=1, n (μ=0)	$Q_{BIN}(t) = 1 - (e^{-\lambda t})^n$	nλt	nλ	nλ
Gate OR	λ_i (n equal inputs)	$Q_{OR}(t) = 1 - (e^{-\lambda t})^n$	$n\lambda_i t$	$n\lambda_i$	$n\lambda_i$
Gate AND	$\lambda_1 = \lambda_2$	$Q^{AND}(t) = (1 - e^{-\lambda_1 t})^2$	$(\lambda_1 t)^2$	$\lambda_1\left(1 + \frac{1}{1 - 2e^{\lambda t}}\right)$	$2\lambda_1 t$

Table 4.9: Evaluation of the unavailability and of the unconditional failure intensity in simplified cases.

Each top gate constructions will be described and the obtained results will be presented in the following sections.

4.4.1 Damage Risk

4.4.1.1 Damage Risk Fault Tree Construction

The evaluation of the probability of not detecting a dangerous loss is based on the assumption that a dangerous beam loss can be detected only in one location.

The hazardous hypothesis of this assumption is that a full coverage of the loss location is assumed: the losses are not expected to happen outside of the quadrupole region or other monitored locations, section 2.3.1.

On the other hand, the possibility that a dangerous loss will generate a loss pattern along the LHC ring is neglected as simulation and experienced from other accelerators show (see section 2.3.1 and [10]). The possibility to detect the loss

with more than one channel would increase the availability of all the BLMS, as it will be discussed later during the sensitivity analysis in section 4.5.

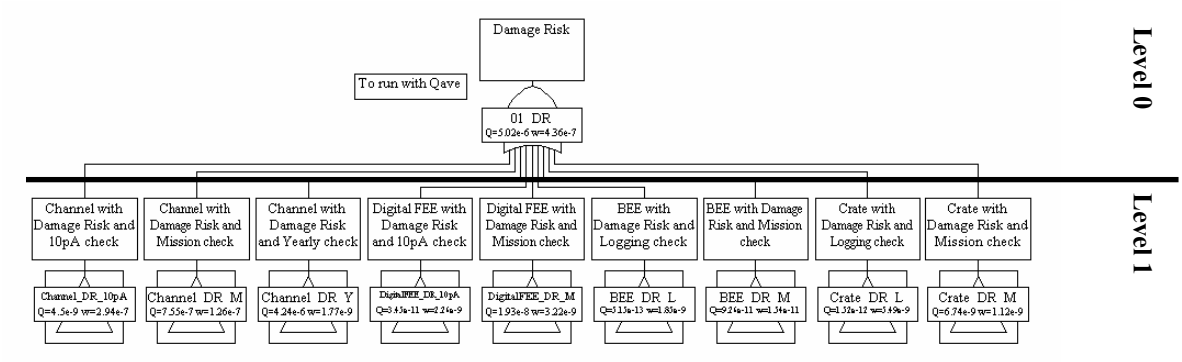


Figure 4.10: Top and first level of the Fault Tree diagram for the probability to not detect a dangerous loss.

Figure 4.10 represents the top and the first level of the Fault Tree diagram for the Damage Risk. The whole fault tree is organised into 4 levels. The first level includes the subdivision in the logic subsystems and checking periods. This initial subdivision has been chosen to highlight the importance of the checking period for the final unavailability calculation. The second level consists of the list of the component per each logic subsystems and period. Level 3 is a collection of causes that lead to the failure of the component and the basic event level contains the failure modes as collected in the FMECA.

In the Damage Risk fault tree, the HT connections are not present, because they are fully monitored by the statuses either in the tunnel or in the surface. Also the optical link is absent, due to its redundancy and checking which generate a false alarm in case of failures. The power supplies fail in a safe way, so they are not relevant for the Damage Risk.

The daisy chain in the backplane has been calculated with 16 beam permit switches. This is the maximum number available in the BLMS crates. This assumption is pejorative, because the average number of switches in the BLMS crate is 13 and the average unavailability of an element in a daisy chain of n

Test	Logging	10pA	Mission	Yearly
Periods [h]	5.56E-4 h (= 2s)	3.06E-2 h (= 110s)	12h	4800h

Table 4.10: Inspection intervals for the BLMS testing processes.

elements is, in a first approximation, (n+1)/2 times the unavailability of the single element.

During the mission time, no maintenance actions are possible, so the repair rate of the components is zero. All the events of the Damage Risk top gate are modelled with the dormant model and the used testing periods are listed in table 4.10.

The analysis is performed over one LHC year of 4800h and the average unavailability has been considered, as suggested by [36].

4.4.1.2 Damage Risk Results

In the BLMS, the probability Q_{DR} that a dangerous loss is not detected by the closest monitor is 5.02E-6. This number is an average over the year; the maximum unavailability during the last days of the year is 1.00E-5. The time dependence is given by the untested monitor during the year, as depicted in figure 4.11.

A reasonable order of magnitude for the expected number of dangerous losses per year is 100. The probability of a magnet suffering damage is given by a binomial sum, like in eq (4.9), with q equals 5.02E-6, n=100 and m=1: it reads 5.02E-4. This number is far below the tolerated figure for LHC, reported in section 3.3 and it is also below the SIL4 level, section 3.3.4.1. In twenty years the probability to lose a magnet is 9.99E-3. These figures are different from already published estimations [42-44] due to the optimised testing process and the design upgrades.

Figure 4.12 shows the relative importance of an event with respect to the whole system. It is the ratio between the sum of the unavailability of the cut sets containing the event and the whole system unavailability. It is generally addressed

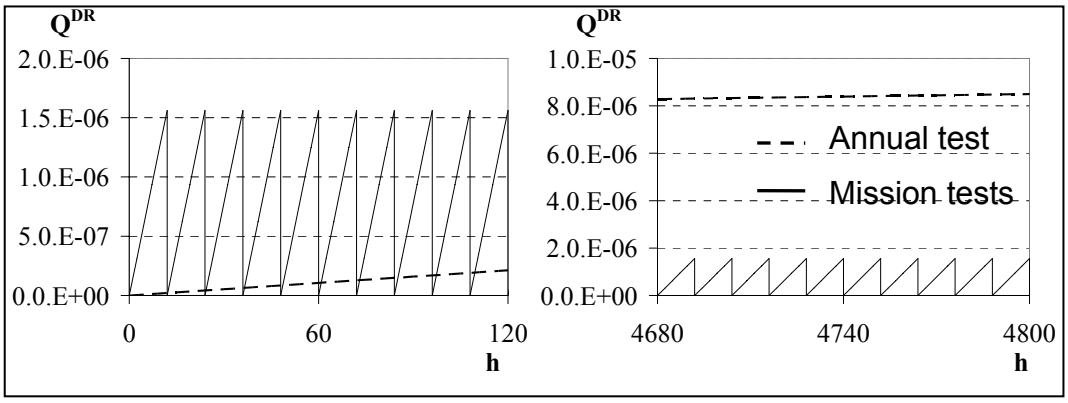


Figure 4.11: Unavailability variation of the BLMS components tested every mission or yearly.
Left: the first 10 missions. Right: the last 10 missions. Note the changing of scale.

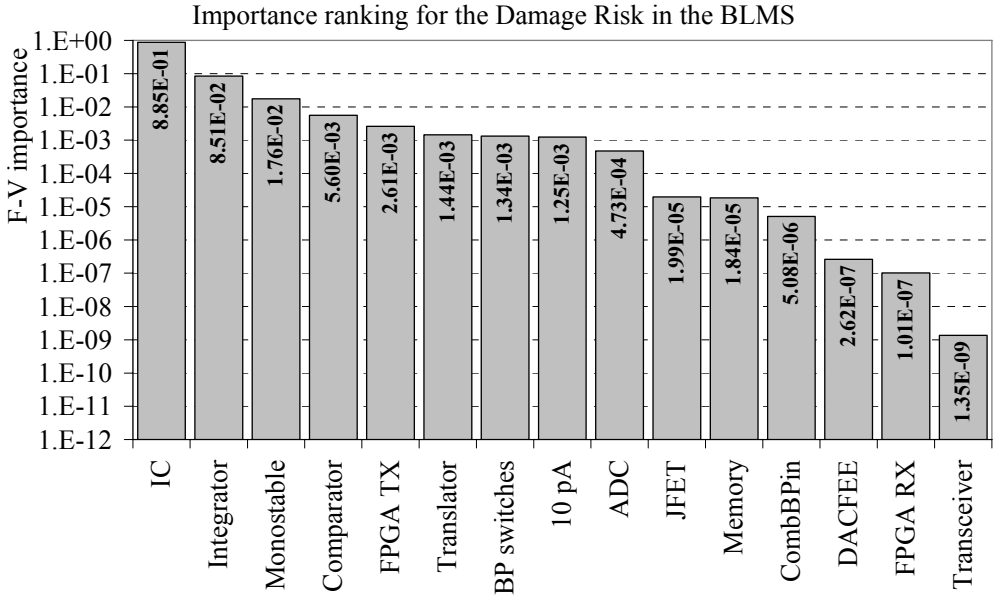


Figure 4.12: Relative importance of the event for the Damage Risk exposition.

as Fussell-Vesely importance. For the configuration of the system, with no redundancies in the diagram, it is coincident with the ratio between the event unavailability and the total unavailability.

The weakest element in the proposed configuration is the Ionization Chamber, responsible for 88.5% of the annual unavailability. This is mainly given by the gas leakage, checked yearly. This value could be overestimated, given the uncertainty on the IC hazard rate, see section 4.1. The second weakest component is the Integrator of the CFC, followed by the other CFC electronics components. These estimations could be affected by too conservative hazard rates assumption, but they are regarded as reasonable given the harsh environment of the tunnel electronics.

4.4.2 False Alarm Generation

4.4.2.1 False Alarm Fault Tree Construction

The False Alarm generation is given by the probability per mission to generate beam permit inhibition not linked to any dangerous loss. Only the failure modes checked with a period less than the mission time are relevant for this analysis. They could be either continuously checked (monitored by a status or fail-safe modes) or checked by tests with a period shorter than a mission (10pA or Logging test (TCAC)). For the False Alarm analysis, the checking period is not as important as for the Damage Risk. If $Q(\tau)$ is the probability to find the component failed after

a checking period τ, the probability that the component works at the end of the mission of duration M is $(1-Q(\tau))^{M/\tau}$. $Q(\tau)$ is in the form of (4.8) with zero repair rate. It is deduced that such a probability is $e^{-\lambda M}$. This is R(M): the reliability for the period M. For the False Alarm generation, the checking period τ does not decrease the probability to finish regularly the mission.

The fault tree spreads over 4 main levels. The first level is the subdivision in logic subsystems, followed by a subdivision in checking periods and components. The minor importance of the checking periods in the False Alarm generation allows this simplified layout. Level 3 is the collection of causes which lead to the failure of the component, as for the Damage Risk, and level 4 contains gates as listed in the FMECA. The binomial model, described in equations (4.8)-(4.10), with the parameter m=1 has been used to model in a compact way several hundreds of components. Such a setting allows that a failure of just one element out of *n* can generate the failure at higher level. The value of n is the number of the elements in the system. To bypass a limitation of the software, it has been necessary to introduce a fifth level in some situation. The software package limitation is given by n smaller than 1000 in the binomial model. The number of evens at levels 5 has been chosen so that they provide the correct estimation for the elements in the

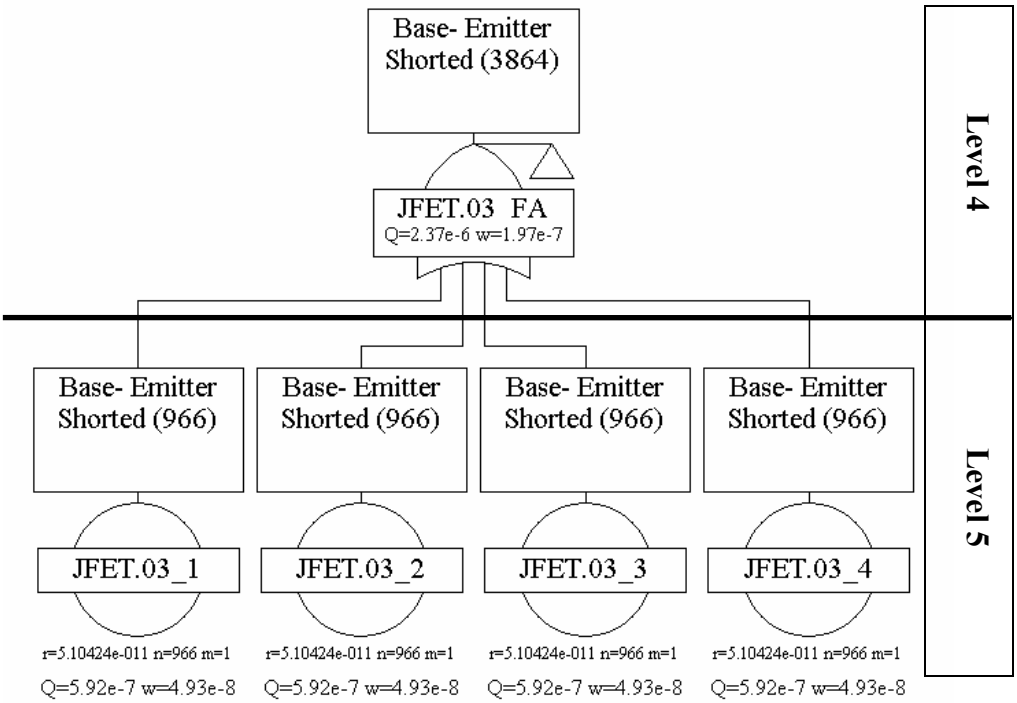


Figure 4.13: Schematic of some Level 5 events of the False Alarm fault tree.

system. Figure 4.13 shows the concept with the case of the failure mode “Base-Emitter Shorted” for the JFET.

Care has to be taken to model the redundant optical link. The optical link consists of two optical lines in parallel. One optical line consists of the GOH, the optical fibre with its connectors, the photodiode and the TLK, see sections 2.5.3 and 2.7.1. Due to the presence of two lines in parallel, the failure intensity is strongly time dependent. This is shown in the rare event approximation too, table 4.9. Generally it is not possible to use a binomial model with m=1 and n=642 for the optical links, because this model requires a constant hazard rate, not time dependant. The dependence on the unavailability Q(t) of the event is the reason why the term “hazard rate” as been introduced in place of the more generic term “failure rate”. The first indicates the number linked to a failure of a component while the second can indicates either the hazard rate or the unconditional failure intensity in a system of events.

This pragmatic approach will require a generation of 642 AND gates of 2 optical link each. This will make the fault tree quite large and less readable. A good approximation in the rare event hypothesis can be achieved with a manipulation of the unavailability and of the unconditional failure intensity for an optical link to introduce them in a dormant event. The approximations have been summarised in table 4.9.

If two elements of failure rate λ_i are linked to an AND gate, the unavailability and the failure rate of the gate at the mission time T are:

$$Q^{AND}(M) = (\lambda_i M)^2, \tag{4.21}$$

$$w^{AND}(M) = 2(\lambda_i)^2 M. \tag{4.22}$$

An OR of n of these gates reads:

$$Q^{OR}_{nAND}(M) = nQ^{AND}(M) = n(\lambda_i M)^2, \tag{4.23}$$

$$w^{AND}_{nAND}(M) = n \cdot w^{AND}(M) = 2 \cdot n \cdot (\lambda_i)^2 M. \tag{4.24}$$

On the other hand, a dormant event with failure rate λ^* and inspection interval τ has an average unavailability and a failure rate which are:

$$\overline{Q}_D(M) = \frac{\tau\lambda^*}{2}, \tag{4.25}$$

$$\overline{w}_D(M) = \lambda^*. \tag{4.26}$$

The parameter λ^* and τ which make the failure rate of eq (4.26) equal to (4.24) are:

$$\lambda^* = 2 \cdot n \cdot (\lambda_i)^2 M = n \cdot w^{AND}(M), \tag{4.27}$$

$$\tau = 2 \cdot \frac{Q_{nAND}^{OR}(M)}{\lambda^*} = 2 \cdot \frac{n(\lambda_i M)^2}{2 \cdot n \cdot (\lambda_i)^2 M} = M. \tag{4.28}$$

In conclusion, it is sufficient to model one AND gate of two optical lines and utilize its failure rate, multiplied by 642, into a dormant event with an inspection time equal to the mission. The calculation of the dormant unavailability must be set to the average method.

The error on the unavailability introduced in the approximation is proportional to $n(Q_{OL})^2$. In the case of the 642 optical links with an unavailability of 4.96E-9 the error is still negligible.

Two other redundant subsystems are present in the False Alarm fault tree: the redundancy of the High Tension power supplies and the 2oo3 configuration of the VME power supplies. Given the limited number of such components, their failure modes have been collected in 8 gates, one per each surface location. An AND gate has been used to model the HT power supplies, while a voting gate with m=2 represents the 2oo3 redundancy of the VME power supplies (see appendix C, page 237). The VME power supplies in point 7 have 4 input gates, given the extra combiner requested for the collimators.

4.4.2.2 <u>False Alarm Results</u>

The probability to have a False Alarm generated during a mission of 12 hours is 3.36E-2. This probability is in the range of the SIL1 (table 3.9 of section 3.3.4.1). Given its minor consequence, the risk is tolerable if the cost is disproportionate to the improvement gained (tables 3.8 and 3.11).

To evaluate the cost impact, the weakest components have to be identified. The Fussell-Vesely importance for each element is plotted in figure 4.14.

The components which generate more false alarms are the power supplies in the LHC straight section, both for the high and the low voltage. Together they are responsible for almost 57% of the foreseen false alarms. This high percentage is given by the quantity of the component (846 in total) and their relatively high hazard rate (1.90E-6/h). The cooling systems of the VME crates could generate another 28%, caused by their high hazard rate of 3.17E-5/h. The main component

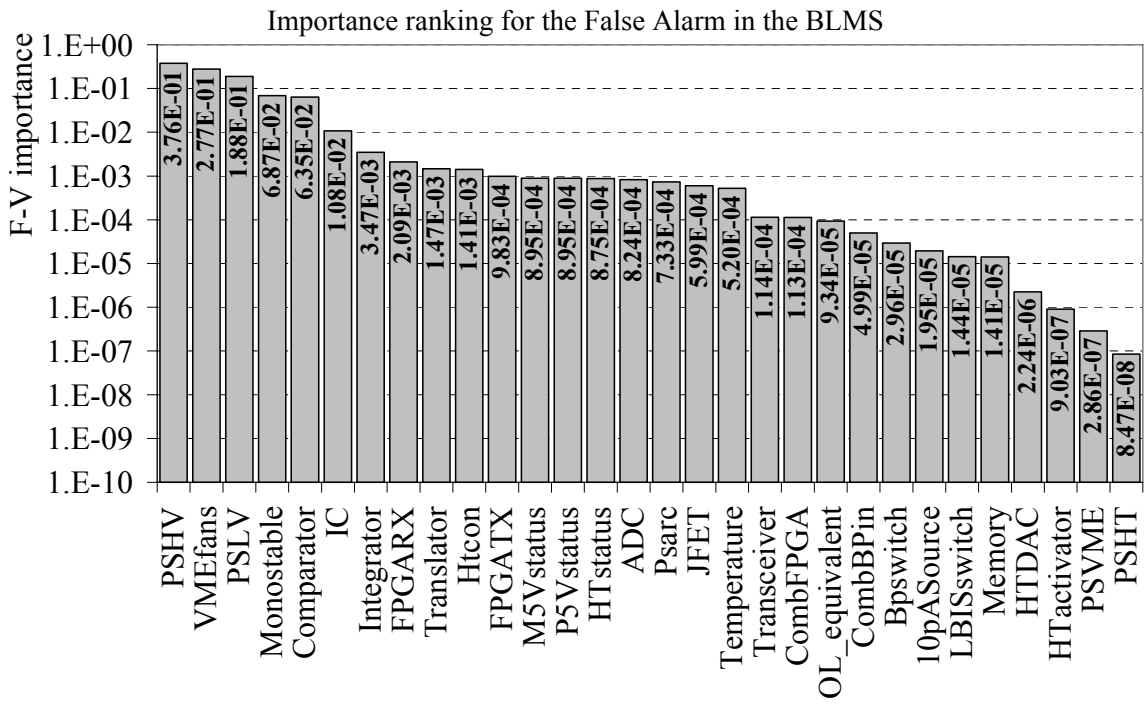


Figure 4.14: Fussell-Vesely importance for the False Alarm generation in the BLMS. Note the logarithmic scale.

of the FEE and the Ionization Chamber follows for their high quantity and middle rate. The other components will cause less then 1.5% of the false alarms. The optical link, the High Tension power supplies and the VME power supplies provide a negligible contribution, due to their redundant configuration.

If it is desired to improve the system availability, a more reliable power supply in the straight section or a redundancy should be introduced. The failures of the power supplies have been assumed to be sharp and not given by a slow degradation. If there will be a degradation, the status monitors in the tunnel electronics will generate warnings which will prevent the false alarm generation.

For a year of approximately 400 missions of 12 hours, the expected number of false alarms and their standard deviation are 13.4 ± 3.6. These figures have been calculated assuming the binomial distribution of the expected false alarms, where the average is nq and the standard deviation is $\sqrt{nq(1-q)}$ [27, p 306]. This number is below the tolerated 20 false alarms per year for LHC, reported in section 3.3.

4.4.3 Warnings Generation

4.4.3.1 Warning Fault Tree Construction

The last fault tree relevant for the BLMS analysis consists of the Warning generation. Such a fault tree provides the estimation of the expected maintenance request generated by the not crucial electronics. A not crucial item is a component whose failure does neither generate a False Alarm nor lead to a Damage Risk. This category include single failure of redundant units (optical line, VME power supplies, HT power supplies), test units (High Tension DAC), and status monitors used either for test (HT activator) or to monitor the degradation of components (Temperature monitor and HT level).

The fault tree is organised on 4 main levels. The first level consist of the subdivision in logic subsystems, the second contains the components, level 3 consist of the collection of causes which lead to the failure and level 4 contains events as listed in the FMECA.

From the Front End Electronic, only the High Tension activator for the HT test and the HT status monitor are relevant. The second is actually an enabler of the Damage Risk in case of the loss of the high tension. The unavailability of an Initiator-Enabler system (typically, a component and its monitor) is the product of the unconditional failure intensity of the Initiator times the unavailability of the enabler. Given the low unconditional failure intensity of one HT cable (see the value of *w* at page 222 and divide it by 642, the number of FEE boards) and the low unavailability of the status monitor, their contribution to the Damage Risk is negligible. Both the HT activator and the HT status are checked during the HT test.

The next component which provides a warning request is a loss of one of the two optical lines in the redundant optical link. Such a gate is presented by the repetition of 642 XOR gates like the OL_W (page 216). For simplicity, it has been preferred to model the link with a binomial distribution with the failure rate identical to the unconditional failure intensity of the OL_W. When an Optical line fails, the maintenance will be postponed to the time after the following dump.

In the surface electronics, either the failure of one of the HT power supply or the failure of the HT test generator can request for a maintenance action. The HT power supplies are modelled with extra levels to introduce XOR gate between the redundant power supplies. An hour is required to substitute the failed power

supply, therefore they are represented by a rate model with 1 hour of MTTR. An HT power supply failure is immediately detected by the combiner status, while a failure in the High Tension DAC will be discovered after the dump, when an HT test request is not executed.

Last elements in the warning generation analysis are the VME power supplies. These components also have an extra level with XOR gates to exclude the possibility that more than one event occurs and generate a False Alarm. These components are symbolised by rate models with 1 hour of MTTR. A failure of a VME power supply is immediately reported and maintenance action can be taken.

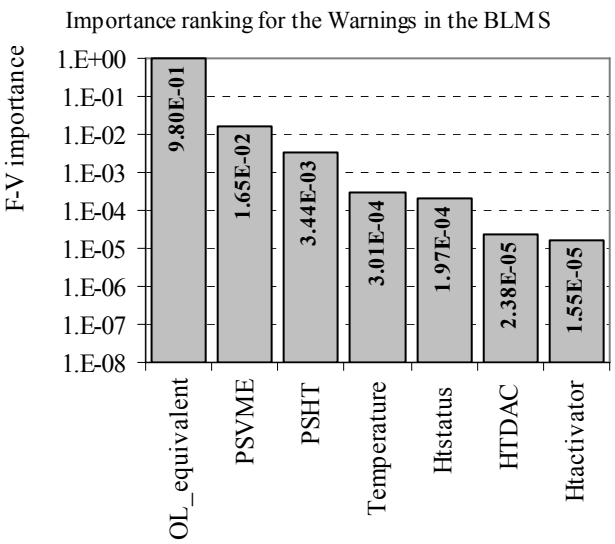


Figure 4.15: Fussell-Vesely importance ranking for the Warning generation in the BLMS. Note the logarithmic scale.

4.4.3.2 Warning Fault Tree Results

The probability to have a warning during a mission is 8.81E-2. The expected number of interventions per year is 35.2 ± 5.7. They are calculated with the binomial expression as for the False Alarm. These interventions do not cost anything in terms of downtime of the LHC. The importance diagram is sown in figure 4.15. Almost the totality of the interventions is given by an optical line failure. This result is expected, given the high quantity of optical lines in the system. Analysing the fault three of the optical line, figure 4.16, the GOH is identified as the weakest component which could generates almost 88% of the optical line failures. This is given by its high failure rate.

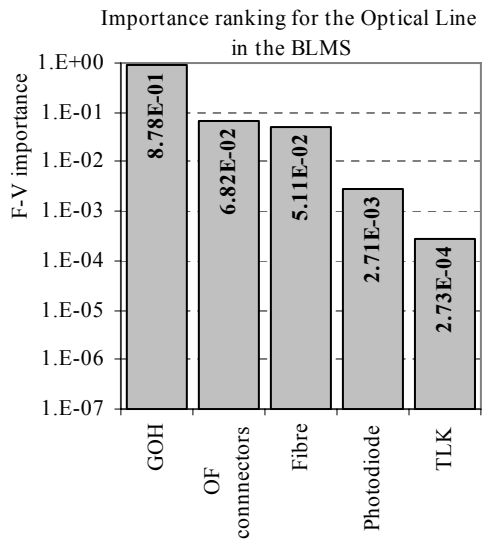


Figure 4.16: Fussell-Vesely importance ranking for the failure generation in the Optical line. Note the logarithmic scale.

As already discussed in section 4.1, this failure rate is probably overestimated. The first year of LHC commissioning will provide some confirmations on this estimation. The next weakest components which generate warnings are the power supplies, both the VME and the HT ones.

These results are a confirmation of the decision to double the optical lines and the power supplies: as will be shown in the next section. If there would be no redundancy, the generated warnings (divided by two for the minor quantity) would become a False Alarms, exceeding the acceptable total number of false alarms per year (around 31 false alarms per year).

4.5 Sensitivity Analysis

The sensitivity analysis permits an evaluation of the variation of the system figures with both the component parameters and the system configuration.

The parameter variations can be provided by the variation of either the hazard rates or the testing time. The variation of the hazard rates could mean a variation of the prediction hazard rate or a variation of the FMECA apportionments. The testing times can vary, for example, following the mission length variation or for maintenance reasons. They can be varied on purpose to allow a better testing of the component.

All the commercial software packets provide tools for the sensitivity analysis. But, in the BLMS case, it is worth analysing the system with the rare event approximation. This approach has the advantage of a direct explanation of the system sensitivity and its dependencies.

The basic assumption of the rare event approximation is the low value of the unreliability of the components. This allows exclusion of the double product from the calculations. For the BLMS this assumption is acceptable for the Damage Risk and can be tolerated with a relative error of the 4% for the False Alarm and also with 10% for the Warnings generation.

In the rare event approximation the unconditional failure intensities are equal to the hazard rate, because the difference 1-Q(t) is ~ 1 (3.17). For an OR gate the unavailability is equal to the sum of the input unavailability, as well as for the unconditional failure intensity. This can be generalised to an input of n equal events, as reported in the table 4.9. Particular care has to be taken for the redundant systems, where unavailability is depending with the second power of

the testing time and the unconditional failure intensity is proportional to such intensity (see table 4.9 and the equations (4.13) and (4.14)). In the following, the general name "failure rate" will be used to underline its dual use in the approximation: both as hazard rate and as unconditional failure intensity.

Given the small contribution to the Warning generation of the non redundant components, the analysis will be focused mainly on the Damage risk and on the False Alarm generation. The number of the components is important in the case of the False Alarm generation while the inspection periods will be relevant only for the Damage Risk.

The variation of the unavailability with a parameter could be extracted by the rare event approximation calculation of the system unavailability. For system with OR gates, the general formula of the unavailability is:

$$Q^{EE} = \sum_{i,t}^{OR} N_i \cdot {}^{t}\lambda_i^{EE} \cdot {}^{t}t \,, \qquad (4.29)$$

where the first sum runs over the OR inputs and over its testing periods, ${}^{t}\lambda_i^{EE}$ is the failure rate of the ith logic subsystem, which is checked by the test t and ${}^{t}t$ is the testing period, as reported in table 4.10.

For the dormant model, the time t has to be substituted with the inspection period, divided by two for the average unavailability evaluation. For the Damage Risk, collecting the term with the same inspection period, the equation reads:

$$\overline{Q}^{DR} = \frac{1}{2}({}^{10pA}\lambda_{CHANNEL}^{DR} \cdot {}^{10pA}\tau + {}^{M}\lambda_{CHANNEL}^{DR} \cdot {}^{M}\tau + {}^{y}\lambda_{CHANNEL}^{DR} \cdot {}^{Y}\tau + {}^{10pA}\lambda_{FEE}^{DR} \cdot {}^{10pA}\tau + \\ + {}^{M}\lambda_{FEE}^{DR} \cdot {}^{M}\tau + {}^{L}\lambda_{BEE}^{DR} \cdot {}^{L}\tau + {}^{M}\lambda_{BEE}^{DR} \cdot {}^{M}\tau + {}^{L}\lambda_{CRATE}^{DR} \cdot {}^{L}\tau + {}^{M}\lambda_{CRATE}^{DR} \cdot {}^{M}\tau), \qquad (4.30)$$

The values of the failure rate can be derived by the first level of the fault tree.

This logic of subdivision of the OR gates can be extended also at the lower levels. For the False Alarm, all the addenda have the mission time ${}^{M}\tau$ and the equation (4.29) becomes:

$$Q^{FA} = {}^{M}\tau \cdot ({}^{M}\lambda_{CHANNEL}^{FA} + {}^{M}\lambda_{DigFEE}^{FA} + {}^{M}\lambda_{OL}^{FA} + {}^{M}\lambda_{tunnelPS}^{FA} + {}^{M}\lambda_{BEE}^{FA} + {}^{M}\lambda_{CRATE}^{FA} + {}^{M}\lambda_{VME}^{FA}) \,. \qquad (4.31)$$

In the case of N_i AND gates, like for the optical link, in the False Alarm fault tree the calculation for the top unavailability is:

$$Q^{FA} = N_j \cdot K \cdot {}^{M}\tau^2 \cdot {}^{M}\lambda_1 \cdot {}^{M}\lambda_2 \,. \qquad (4.32)$$

The eventual multiplicity K of the AND configuration can be given by the 2oo3 or by the 2oo4 configuration (VME power supplies in point 7). In the first case K is equal to 3, in the second it is 6.

The value of the failure rates could be picking up from the fist level of the fault tree of either of the Damage risk or the False Alarm fault trees. Alternatively, the hazard rate can be extracted by the level 3 of the FMECA and add the failure rate of the failure mode corresponding to the desired end effect.

This estimation leads to the possibility to detect what is the impact on the unreliability of changing in the system configuration. Collecting the failure rates, see table 4.11, and calculating the unavailability with the eq (4.30) and (4.31), an unavailability table can be drawn, table 4.12.

From the two tables, the effect of the variation of the configuration can be already appreciated. Differentiating eq. (4.29), it is obtained:

$$\Delta Q^{EE} = \sum_{i,t} \Delta N_i \cdot {}^t\lambda_i^{EE} \cdot {}^t t + \sum_{i,t} N_i \cdot \Delta^t \lambda_i^{EE} \cdot {}^t t + \sum_{i,t} N_i \cdot {}^t\lambda_i^{EE} \cdot \Delta^t t \,. \qquad (4.33)$$

In case of $\Delta^t t$ variation, the sum $\sum_{i,t} N_i \cdot {}^t\lambda_i^{EE}$ is the reported logic subsystem failure rate in table 4.11.

Such formulas allow a first evaluation of the reconfiguration impact. The introduction of either the Mission test or the 10pA test moves the failure rate toward low unreliability value, due to the short inspection periods compared to the

Failure rates: $N_i \cdot {}^t\lambda_i^{EE}$	**Damage Risk**				**FA**
	TCAC (L)	**10pA**	**Mission (M)**	**Gain (Y)**	
Channel		2.94E-07	1.26E-07	1.77E-09	4.27E-04
Digital FEE		2.26E-09	3.22E-09		1.04E-05
Optical link					5.31E-07
(642 x OL)					*(3.77E-03)*
Tunnel PS					1.58E-03
BEE	1.85E-09		1.54E-11		7.79E-06
Crate electronics	5.49E-09		1.12E-09		5.99E-07
(8 x PS HT)					*(1.52E-04)*
VME unit*					7.84E-04
(25 x PS VME)					*(4.75E-09)*
Failure rates per period	7.34E-09	2.96E-07	1.30E-07	1.77E-09	2.81E-03

Table 4.11: Failure rate per inspection interval and logic subsystems of BLMS. They are also subdivided by final effects: DR for Damage Risk and FA for False Alarm.

LHC year. If only the 10 pA test would be performed with the frequency of the mission test, there would be an increase in unreliability of 2.94E-07/h times the difference between 12 hours and 3.06E-2 hours. This is the failure rate of the 10 pA test times the increment of the testing period. In this case there will be an increment of 3.52E-6 over a previous unreliability of 5.01E-6: an unavailability increase of the 70%.

In the table 4.12, the unreliability of the redundant component are also reported (in brackets) in the case of non implementation of the redundancy. With the redundancies, the situation of the False Alarm is improved. The redundancy of the optical line first followed by the VME power supplies and the HT power supplies, decrease the failure rate relative to the continuous checking from 7.21E-3/h to, respectively, 3.44E-3/h, 2,96E-3/h and 2.81E-2/h: almost a factor 3 of improving . Actually, such levels are already over the limits of the rare event approximation, but the qualitative evaluation is still valid.

The argumentation can be extended from the subsystem levels to the components

Q_i	Damage Risk					
%	TCAC (L)	10pA (10)	Mission (M)	Gain (Y)	DR per subsystems	FA
Channel		4.49E-09 0.0892%	7.56E-07 15.0%	4.25E-06 84.4%	5.01E-06 99.5%	5.12E-03 15.2%
Digital FEE		3.45E-11 0.000686%	1.93E-08 0.384%		1.94E-08 0.384%	1.25E-04 0.370%
Optical link						6.37E-06 0.0189%
(642 x OL)						*(4.52E-02)*
Tunnel PS						1.90E-02 56.2%
BEE	5.14E-13 0.0000102%		9.24E-11 0.00184%		9.29E-11 0.00185%	9.35E-05 0.277%
Crate electronics	1.53E-12 0.0000303%		6.72E-09 0.133%		6.72E-09 0.134%	7.19E-06 0.021%
(8 x HT Power supply)						*(1.82E-03)*
VME unit						9.41E-03 27.9%
(25 x PS VME)						*(5.70E-03)*
DR per inspection periods	2.04E-12 0.0000405%	4.53E-09 0.0899%	7.82E-07 15.5%	4.25E-06 84.4%	5.03E-06 100%	3.37E-02 100%

Table 4.12: Unreliability for the Damage Risk and the False Alarm generation per subsystem and inspection time. Percentages over the total are shown too.

to derive expression for sensitivity index for the components. A sensitivity index is the ratio $\Delta Q/\Delta p$, where p is the varied parameter. It expresses much of the unreliability change with respect to the variation of the parameter. For a non redundant component, this expression can be derived:

$$\frac{\Delta Q_{OR}^{EE}}{\Delta \lambda_i} = N_i \cdot \sum_t {}^t\alpha_i^{EE} \cdot {}^t t\,, \tag{4.34}$$

where λ_i is the hazard rate of a component, N_i is its quantity, ${}^t t$ is the inspection period and ${}^t\alpha_i^{EE}$ is the apportionment of the failure mode which gives the effect EE and it is tested by the test t.

In the case of the BLMS, for the End Event equal to Damage Risk every N_i is equal to one, with the exception of the 16 backplane switches for the beam inhibition. For the False Alarms, independent of the testing time, ${}^t t$ is equal to the mission time M and the sum coincide with the sum of the apportionment factors f the components which lead to a False Alarm. In the case of the Damage Risk, the variation of the testing time can have its sensitivity indexes:

In other words:

$$\frac{\Delta Q_{OR}^{DR}}{\Delta \lambda_i} = \sum_t {}^t\alpha_i^{DR} \cdot {}^t t = S_i^{DR}\,, \tag{4.35}$$

$$\frac{\Delta Q_{OR}^{FA}}{\Delta \lambda_i} = N_i \cdot M \cdot \sum_t {}^t\alpha_i^{FA} = S_i^{FA}\,, \tag{4.36}$$

$$\frac{\Delta Q_{OR}^{EE}}{\Delta {}^t t} = \sum_i N_i \cdot {}^t\alpha_i^{EE} \cdot \lambda_i = {}^t S^{EE}\,. \tag{4.37}$$

Sensitivity indexes of the BLMS component with the relevant parameters are listed in table 4.13, table 4.14 and table 4.15. In all the equations for the Damage Risk unavailability, the maximum unavailability has been considered. If the sensitivity indexes for the average unavailability are desired, the presented values have to be divided by 2.

If just one failure rate is varied, the impact on the unavailability variation for the Damage Risk is proportional to the inspection period duration. The variation of the failure rate of the DAC reference, fully tested by the HT test, is almost hundred times more important than the failure rate variation of a JFET. This component has only the 3.4% of its functionality tested with the HT test and the rest is checked by the faster 10pA test.

Entry ID	Hazard rate	End Effects	Detection Method	α%	^{t}t	S_i^{DR}
IC+cable	4.41E-08	Damage Risk	Yearly test	4.0%	4800	**2.01E+02**
			Mission	78.0%	12	
Integrator	7.50E-08	Damage Risk	Mission	94.9%	12	**1.14E+01**
		False Alarm	10 pA test	5.1%	3.06E-02	
Comparator	1.91E-07	Damage Risk	Mission	2.2%	12	**2.94E-01**
		False Alarm	10 pA test	97.8%	3.06E-02	
Monostable	1.15E-07	Damage Risk	Mission	12.5%	12	**1.53E+00**
		False Alarm	10 pA test	87.5%	3.06E-02	
JFET	4.56E-10	Damage Risk	Mission	3.4%	12	**4.38E-01**
		False Alarm	10 pA test	96.6%	3.06E-02	
ADC	1.00E-09	Damage Risk	Mission	39.4%	12	**4.75E+00**
		False Alarm	10 pA test	60.6%	3.06E-02	
Translator	2.64E-09	Damage Risk	Mission	45.5%	12	**5.48E+00**
		False Alarm	10 pA test	54.5%	3.06E-02	
FPGA TX	8.70E-09	Damage Risk	Mission	25.0%	12	**3.01E+00**
		False Alarm	10 pA test	25.0%	3.06E-02	
DAC FEE	8.93E-11	Damage Risk	Mission	3.5%	12	**4.49E-01**
		False Alarm	10 pA test	96.5%	3.06E-02	
DAC FEE ref	1.04E-09	Damage Risk	Mission	100.0%	12	**1.20E+01**
FPGARX	1.83E-08	Damage Risk	Logging	10.0%	5.56E-04	**5.56E-05**
Memory	1.39E-10	Damage Risk	Logging	11.1%	5.56E-04	**6.17E-05**
Transceiver	1.02E-09	Damage Risk	Logging	2.4%	5.56E-04	**1.33E-05**
BPswitch (16)	2.80E-10	Damage Risk	Mission	25.0%	12	**4.80E+01**
Com_BP_in	1.82E-10	Damage Risk	Mission	2.2%	12	**2.64E-01**
Combiner FPGA	1.83E-08	Damage Risk	Logging	30.0%	5.56E-04	**1.67E-04**

Table 4.13: Sensitivity index of the BLMS components for the Damage Risk event.

The higher is the sensitivity index, the higher is the variation of the unavailability. The variation could increase or decrease the unavailability. The most sensitive components for the Damage Risk is the Ionization Chamber, due to its dependency to the Gain test, with a long checking period. If a tolerable maximum unavailability of 2E-3 is assumed, the maximum value tolerable of the IC parameter is around 1E-5. In fact:

$$Q_{tol} = Q_0 + \Delta Q_{\max} = Q_0 + S_i \cdot \Delta\lambda_i^{\max} \Rightarrow \Delta\lambda_i^{\max} = \frac{Q_{tol} - Q_0}{S_i}, \qquad (4.38)$$

where Q_{tol} is the maximum tolerated and Q_o is the current unavailability, S_i is the sensitivity to the failure rate λ_i of the component i and $\Delta\lambda_i^{\max}$ is the maximum allowed parameter variation. The variation of the Ionization Chamber hazard rate extends over orders of magnitude compared to the foreseen one.

Entry ID	λ_i	End Effects	Detection	α%	Quantity	$\Sigma\alpha$%	S_i^{FA} [h]
IC+cable	4.41E-08	False Alarm	Continuous	18.0%	3864	18.0%	**8.35E+03**
HTcon	5.20E-10	False Alarm	Continuous	100.0%	7728	100.0%	**9.27E+04**
Integrator	7.50E-08	False Alarm	10 pA test	5.1%	3864	5.1%	**2.36E+03**
Comparator	1.91E-07	False Alarm	10 pA test	97.8%	1932	97.8%	**2.27E+04**
Monostable	1.15E-07	False Alarm	10 pA test	87.5%	1932	87.5%	**2.03E+04**
JFET	4.56E-10	False Alarm	10 pA test	96.6%	3864	96.6%	**4.48E+04**
ADC	1.00E-09	False Alarm	10 pA test	60.6%	3864	60.6%	**2.81E+04**
Translator	2.64E-09	False Alarm	10 pA test	54.5%	3864	54.5%	**2.53E+04**
FPGA TX	8.70E-09	False Alarm	10 pA test	25.0%	642	50.0%	**3.85E+03**
			Continuous	25.0%			
DACFEE	8.93E-11	False Alarm	10 pA test	96.5%	642	96.5%	**743E+3**
HT activator	1.82E-10	False Alarm	Continuous	2.2%	642	2.2%	**1.69E+02**
HTstatus	3.96E-09	False Alarm	Continuous	97.8%	642	97.8%	**7.53E+03**
M5V	3.96E-09	False Alarm	Continuous	100.0%	642	100.0%	**7.70E+03**
P5V	3.96E-09	False Alarm	Continuous	100.0%	642	100.0%	**7.70E+03**
PSarc	1.93E-09	False Alarm	Continuous	100.0%	1080	100.0%	**1.30E+04**
PSSSHV	1.90E-06	False Alarm	Continuous	100.0%	564	100.0%	**6.77E+03**
PSSSLV	1.90E-06	False Alarm	Continuous	100.0%	282	100.0%	**3.38E+03**
GOH	5.15E-06	Warning	Continuous	100.0%	1284	100.0%	**1.54E+04**
OFcon	1.00E-07	Warning	Continuous	100.0%	10272	100.0%	**1.23E+05**
Fibre	1.00E-10	Warning	Continuous	100.0%	1284	100.0%	**1.54E+04**
Photodiode	1.59E-08	Warning	Continuous	100.0%	1284	100.0%	**1.54E+04**
TLK	1.60E-09	Warning	Continuous	100.0%	1284	100.0%	**1.54E+04**
FPGARX	1.83E-08	Damage Risk	Logging	10.0%	325	100.0%	**3.90E+03**
		False Alarm	Continuous	90.0%			
Memory	1.39E-10	Damage Risk	Logging	11.1%	325	100.0%	**3.90E+03**
		False Alarm	Continuous	88.9%			
Transceiver	1.02E-09	Damage Risk	Logging	2.4%	325	100.0%	**3.90E+03**
		False Alarm	Continuous	97.6%			
BPswitch	2.80E-10	False Alarm	Continuous	75.0%	16	75%	**1.44E+2**
Temperature	1.14E-08	False Alarm	Continuous	40.0%	325	40.0%	**1.56E+03**
Com_BP_in	1.82E-10	False Alarm	Continuous	97.8%	25	97.8%	**2.93E+02**
Combiner FPGA	1.83E-08	Damage Risk	Logging	30.0%	25	100.0%	**3.00E+02**
		False Alarm	Continuous	70.0%			
LBIS switch	1.82E-10	False Alarm	Continuous	100.0%	225	100.0%	**2.70E+03**
HT DAC	2.27E-08	False Alarm	Continuous	3.5%	8	3.5%	**3.36E+00**
PSHT	1.90E-05	Warning	Continuous	100.0%	16	100.0%	**1.92E+02**
PSVME	1.90E-05	Warning	Continuous	100.0%	25	100.0%	**3.00E+02**
Fantray	3.17E-05	False Alarm	Continuous	100.0%	25	100.0%	**3.00E+02**

Table 4.14: Sensitivity index of the BLMS components for the False Alarm event in a not redundant configuration.

The second more sensitive component is the BackPlane switch in the VME crate. Its sensitivity is linked to the daisy chain of 16 elements.

In the False alarm case, the variation of Q^{FA} could be investigated by assuming that the arc power supplies have the same failure rate as the straight section one. The variation of the failure rate of the power supply is 1.90E-6/h. Its sensitivity index is 1.30E+4h and consequently the increment in the probability to generate a False Alarm is 2.47E-2. This leads to an increment of 9.9 expected False Alarms in 400 missions. With the number estimated in section 4.4.2.2, the expected number of False Alarms per year of the LHC would be in this case 23.3 ± 4.8, this is over the tolerate limit of 20, see section 3.3.

The values reported in table 4.14 are for non redundant systems. To evaluate the effect of the variation of a parameter of a redundant component to the system, expressions like equation (4.32) should be differentiated. However, the impact of this component is always negligible in the framework of the rare event approximation.

The effect of the variations of the inspection periods on the system unreliability can be evaluated with equation (4.37).

Table 4.15 contains the inspection periods with their sensitivity factors. It also shows the maximum time between two tests before reaching the maximum unavailability of 2E-3 over one year for the Damage Risk and 0.05 for the False Alarms, section 3.3 . The most sensitive inspection time for the Damage Risk is that for 10pA, which, in any case, it could be delayed over the LHC year before reaching the allowed unavailability. For the False Alarms generation, the mission time can be extended up to almost one month without passing the limit. Even if such results look reassuring, care is required in the evaluation inspection periods. Their sensitivity indexes are linearly modified by the failure rate of the components and a factor higher than 10 of variation in the sensitivity index for the inspection time can not be excluded a priori.

	${}^{t}t$	${}^{t}S^{DR}$	Max hours	Max days
Yearly test	4800	1.77E-09	1.13E+08	4.72E+06
Mission	12	1.29E-07	1.55E+06	6.45E+04
10 pA test	3.1E-02	2.97E-07	6.74E+05	2.81E+04
Logging	5.6E-04	7.36E-09	2.72E+07	1.13E+06
		${}^{t}S^{FA}$		
Mission	12	7.91E-05	6.44E+02	2.68E+01

Table 4.15: Sensitivity indexes for the inspection periods and maximum allowed before reaching the 2E-3 limits for the DR and 0.05 for FA.

4.6 Underlying Assumptions of Dependability Analysis

The underlying assumptions, listed in table 4.16, are in the follow collected and their effects on the BLMS are discussed.

The use of a constant hazard rate given by the standard is generally a conservative hypothesis, because it overestimates the hazard rate after the short period of the early failures (see figure 3.5). In addition, the check-in procedures (section from 4.2.1 to 4.2.3) reduces the hazard rates, eliminating some failure modes of the components. This reduction is has not been taken into account. Such failures have been assigned to a false alarm generation in the FMECA, leading to an increase of the expected number of the false alarms. These assumptions are partially counterbalanced by the “as good as new” checking, which neglects the possible worsening of the components during the LHC lifetime.

Another conservative hypothesis is the assumption that every undetected loss could lead to a magnet damage. As described in figure 1.6 and section 1.2, the assumption is false in case of slow losses, due to the redundancy provided by the QPS system. This assumption could also be false for the fast losses, if either the Fast Beam Current Decay Monitors or the Beam Position Monitors demonstrate reliability in the beam monitoring for machine protection. Still at the LHC level, it has been assumed prudently that only one BLMS channel could monitor a dangerous loss. If this conjecture is wrong, as indicated by simulation (figure 2.5) and experiences gained by other accelerators [10], at least the BLMS channel become redundant, because two monitors can inhibit the beam. Since a single

Conservative hypotheses.	**Consequences**
Constant failure rate	Unreliability overestimation.
No reduction of failures rate by Check-in procedures.	False Alarm overestimation.
Every undetected loss leads to a magnet damage.	Damage Risk overestimation.
No simultaneous detection of the multiple losses.	If multiple loss, DR becomes negligible.
16 beam permit switch and 3 LBIS lines daisy chained.	DR and FA overestimation.
No preventive detection by status monitor.	False Alarm overestimation.
Ambiguous failure assigned to the most critical effect.	DR and FA overestimation.
No masking philosophy	FA over estimation.
Hazardous hypotheses.	**Consequences**
Component “as good as new” after test.	Unreliability underestimation.
Loss only in quadrupole region	Full spatial coverage of the dangerous losses.

Table 4.16: Synoptic table of the assumed hypotheses during the BLMS analysis.

BLMS channel is responsible for 99.6% of the Damage Risk (section 4.4.1.2), this functional redundancy deeply decrease the risk of damage to magnet. Another hazardous hypothesis is the assumption that any dangerous loss will be detected at the quadrupole and a few other crucial locations. The superconducting dipoles are largely not covered by the BLMS. Simulation, experience and safe margins adopted against the damage risk (see table 2.2) support the assumption of the losses at the quadrupole magnet location.

In the calculation further hypotheses have been made. First, the Damage Risk and the False Alarm numbers have been calculated using the last module in the daisy chains of both the Backplane lines (16 cards daisy chained) and the BLMS rack (3 crate daisy chained) instead of smaller average values. Second, the status monitors of the power supplies have been taken as ineffective. They could detect the degradation of the power supplies in the tunnel. In the analysis this possibility has been negated, because it was complex to estimate the apportionment between the probability to have either a sharp failure or a smooth one. If the status monitor proves to be efficient in the detection of the degradation, the number of false alarms will strongly decrease. Finally, during the FMECA, all the “Parametric failure” modes have been assigned to the most critical final event, even if the “drift” of the component could be toward a safe direction. For example, the comparator in the FEE could be more sensitive to the voltage variation, generating a probable False Alarm, rather then less sensitive, leading to the Damage Risk. These three assumptions are conservative, because they increase both the Damage Risk and the number of False Alarms.

Neglecting the possibility of masking a channel at the BEE level, another conservative hypothesis has been made. The masking, see section 2.7.2, reduces the number of false alarms which improperly cause a dump of the beam.

Chapter 5

CONCLUSIONS

The Beam Loss Monitors System is crucial for machine protection. It measures the intensity of the losses along the LHC ring and must inhibit the beam permit signal in case of detection of dangerous losses. A high detection probability is demanded to avoid 30 days of downtime to substitute the damaged magnet. Following international guidelines, the probability of missing such losses should be less then 1E-3 (SIL3). This probability results in two lost magnets for missed detection in twenty years, assuming 100 dangerous losses per year. Such a probability has been decreased adopting a failsafe philosophy: if a dangerous system failure is detected, a beam permit inhibition is given to extract the beam form the accelerator. A trade off with the operational availability is then necessary, because the protection system could generate false alarms. The number of not necessary beam inhibitions must not deteriorate the operability of the accelerator. Up to three hours are required to restore the beam condition after a dump. It is tolerated that the BLMS generates a maximum of 20 false alarms per year, corresponding to a down time of 1.25% of the operational time.

The design of the system has to be compliant with several constrains. The monitors are located into the LHC tunnel in radioactive environment. The electronics have to be split: radiation tolerant front-end electronic is placed close to the monitors while the signal elaboration is made at the surface. The distance between the two electronics could reach 3 km. The signal covers over 9 orders of magnitude and the transmission rate is one frame every 40 μs.

The limitations given by both the distance and the bandwidth prompt the decision to use an optical link. Nevertheless, the optical component have high hazard rate. For example: 5E-6/h for optical transmitter and 3E-7/h for 3 km of fibre. This situation forced the decision to utilize two redundant optical lines from the tunnel to the surface. Checking algorithms have been implemented to select the error free signal and to inhibit the beam permit in case of ambiguous transmission.

The sources of the hazard rates have been compared and selected in order to provide appropriate rates. When data on the radiation behaviours were not available, the elements have been tested and safety factor have been used to

adapt them to the harsh environment. The effect of failure modes of each element on the system has been studied. The elements that could generate either an unsafe status or a false alarm have been pointed out. Particular attention has been given to the testing processes utilized to monitor the system status. Continuous testing with a bias signal provides good coverage against the risk that a channel is blind to a loss. Tests performed via the high tension alimentation after every dump check the functionality of the whole chains. The positive aspects of the testing processes are decreased the system unavailability and the possibility to plan maintenance actions. One negative aspect is the testing units generate false alarms either for the detection of a failed component or for their internal failure.

In the proposed configuration, the maximum probability that a channel will miss a dangerous loss is 5E-6, compliant with the SIL3 limit. The average probability per year to have severe beam damage, assuming 100 dangerous losses, is 5E-4. The number of false alarms given by system failures is 13 ± 4 per year. Both figures are below the tolerated limits. The expected weakest components are pointed out: the power supplies in the tunnel generate 57% of false alarms while the ionization chamber could be responsible for 88.5% of the probability to miss the dangerous loss.

The uncertainties present in the model are mainly linked to the number of simultaneously detectable dangerous losses and the correctness of the threshold levels. If frequently a loss scenario generates several comparable dangerous losses at different monitored locations, the probability to miss a loss could be neglected and also the consequence of the testing processes could be modified to transform some false alarms in warning requests. If the threshold levels are defined in a wrong manner, there is the risk not to take action against dangerous losses, in case of too high level, or to inhibit the beam without reasons, in case of too low level.

Some alternative system improvements have been studied. After the commissioning period, when more data are available both on the beam loss scenarios and on the system failure rate, reconfigurations of the system are from advantage. The effect of the variation of the hazard rate of the components and of the test frequency has been evaluated. Redesigns should reduce the amount of false alarms requests, without decreasing the overall protection level. To easily estimate the impact of the changes on the system, the model have been

implemented in a Fault Tree software and an approximated evaluation method has been described.

In the future a real failure analysis should be performed on the working system, either to improve the system capability or to provide reference numbers to other accelerators which will implement similar technologies.

REFERENCES

1. ATLAS: Technical Proposal for a General-Purpose pp Experiment at The Large Hadron Collider at CERN; Geneva: CERN, 1994. 272 p. (LHC Tech. Proposal; 2). CERN-LHCC-94-43. LHCC-P-2.
2. CMS Technical Proposal; Geneva: CERN, 1994. 254 p. (LHC Tech. Proposal; 1). CERN-LHCC-94-38. LHCC-P-1.
3. LHCb: Technical Proposal; Geneva: CERN, 1998. 170 p. (LHC Tech. Proposal; 4). CERN-LHCC-98-04. LHCC-P-4.
4. Total Cross Section, Elastic Scattering and Diffractive Dissociation at the LHC; Geneva: CERN, 1999. 38 p. (LHC Tech. Proposal; 7). CERN-LHCC-99-07. LHCC-P-7.
5. ALICE: Technical Proposal for a Large Ion Collider Experiment at the CERN LHC; Geneva: CERN, 1995. 237 p. (LHC Tech. Proposal; 3). CERN-LHCC-95-71.- LHCC-P-3.
6. Brüning, O. S.; Collier, P.; Lebrun, P. et al.; LHC Design Report v.1: the LHC Main Ring; Geneva: CERN, 2004. 548 p. CERN-2004-003-V1.
7. http://en.wikipedia.org/wiki/Copper .
8. Jeanneret, J. B.; Leroy, D.; Oberli, L.; et al.; Quench Levels and Transient Beam Losses in LHC Magnets; CERN-LHC-Project-Report-44. Geneva : CERN, 25 May 1996 . 16 p.
9. Vergara-Fernández, A.; Reliability of the Quench Protection System for the LHC Superconducting Elements. CERN-LHC-Project-Note-350. Geneva: CERN, 15 Jun 2004. 205 p.
10. Wittenburg, K.; Beam Loss & Machine Protection; 33rd ICFA Advanced Beam Dynamics Workshop on High Intensity & High Brightness Hadron Beams; Bensheim: 18-22 Oct 2004. p 65-69.
11. Arauzo Garcia, A.; Dehning, B.; Configuration of the Beam Loss Monitors for the LHC Arc, LHC-Project-Note-238; Geneva: CERN, 12 Oct 2000. 11 p.
12. Arauzo Garcia, A.; Bovet, C.; Computer Simulation of Beam Loss Detection in the Arcs of the LHC; SL-BI-LHC-Project-Note 213; Geneva: CERN, 30 Mar 2000. 22 p.
13. On the Measurement of the Beam Losses in the LHC Rings. Engineering Specification, LHC-BLM-ES-0001 Rev 2.0; Geneva: CERN, 13 Jan 2004. 30 p.

14. Arauzo Garcia, A.; Bovet, C.; Beam Loss Detection System in the Arcs of the LHC; CERN-SL-2000-052-BI; Geneva: CERN, 10 Jul 2000. 10 p.
15. Gschwendtner, E.; Assmann, R. W.; Dehning, B.; Ionization Chambers for the LHC Beam Loss Detection; CERN-AB-2003-068-BDI; Geneva: CERN, 19 Jun 2003. 4 p.
16. Friesenbichler W.; Development of the Readout Electronics for the Beam Loss Monitors of the LHC; Diploma thesis in Mechatronics Engineering, Fachhochschule Wr. Neustadt, Jun 2002.
17. http://www.actel.com/documents/RTSX_DS.pdf .
18. http://cms-ecal-optical-links.web.cern.ch/cms-ecal-optical-links/content/GOH_Specification.doc .
19. http://www.ieee.org/portal/site/relsoc/ : IEEE-Transactions on Reliability
20. Rasmussen, N.; NRC, WASH-1400: Reactor Safety Study, October 1975.
21. NATO R&M Terminology applicable to ARMPs, ARMP-7 (Edition1). 30 p.
22. IEEE 352™, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.
23. MIL 217-HDBK-217F, Reliability Prediction of Electronic Equipment, 2 December 1991.205p.
24. Telcordia Technologies Special Report SR-332, Issue 1, May 2001.
25. NSWC 98/LE1, Handbook of Reliability Prediction Procedures for Mechanical Equipment , 30-Sep-1998.
26. IEC/TR 62380- Ed. 1.0; Reliability data handbook, Universal model for reliability prediction of electronics components, PCBs and equipment, 2004-08-17. 88 p.
27. Kumamoto, H.; Henley, E. J.; Probabilistic Risk Assessment and Management for Engineers and Scientist; New York: IEEE PRESS, 1996. 598 p.
28. Kececioglu, D.; Reliability & Life Testing Handbook, Volume 1; Englewood Cliffs, NJ: Prentice Hall, 1993. 914 p.
29. Mann, N. R. R.; Schafer, R. E. and Singpurwalla, N. D.; Methods for Statistical Analysis of Reliability and Life Data; New York: John Wiley & Sons, 1974. 576 p.
30. JESD85, Methods for calculating Failure Rates in Units of FITs, July 2001, JEDEC Solid States Technology Association. 24p.

31. MIL-STD-1629A, Procedures for Performing a Failure Mode Effects and Criticality Analysis, 24 November 1980. 54 p.
32. IEEE standard reliability data for pumps and drivers, valve actuators, and valves, ANSI/IEEE Std 500-1984 P&V, 16 Sep 1986
33. FMD-97, Failure Mode/Mechanism Distribution 1997, RAC December 1997. 424 p
34. Markov, A. A.; Extension of the limit theorems of probability theory to a sum of variables connected in a chain; Reprinted in Appendix B of: R. Howard. *Dynamic Probabilistic Systems, volume 1: Markov Chains*. John Wiley and Sons, 1971.
35. Peterson, J. L.; Petri Net Theory and the Modelling of Systems, Prentice Hall, 1981.
36. IEC 61508 First edition 1998-11; Functional Safety Of Electrical/ Electronic/ Programmable Electronic Safety Related Systems. 838 p.
37. ICRP 26: Recommendations of the International Commission on Radiological Protection, January, 1977.
38. Dehning, B.; Ferioli, G.; Gonzalez, J. L., Guaglio, G. et al.; The Beam Loss Monitoring System; LHC Project Workshop; Chamonix XIII, 2004. p 256-262.
39. Leitner Roman; Realisation of a fast data storage and transfer system using a FPGA and an USB interface" Diploma thesis in Mechatronics Engineering, Fachhochschule Wr. Neustadt, Jun 2005.
40. Boscherinia, M.; Adriani O.; Bongi M.; et al.; Radiation damage of electronic components in space environment; Nuclear Instruments and Methods in Physics Research A 514 (2003). p 112–116.
41. http://www.research.ibm.com/journal/rd/421/ziegler.html .
42. Guaglio, G.; Dehning, B.; Santoni, C.; Reliability of Beam Loss Monitors System for the Large Hadron Collider; Beam Instrumentation Workshop 2004 Knoxville TN. p 141-149.
43. Guaglio, G.; Dehning, B.; Santoni, C.; Reliability considerations on LHC Beam Loss Monitors System; 33rd ICFA Advanced Beam Dynamics Workshop on High Intensity & High Brightness Hadron Beams; Bensheim: 18-22 Oct 2004. p 191-196.

44. Dehning, B.; Filippini, R.; Guaglio, G. et al.; Reliability Assessment of the LHC Machine Protection System; PAC 2005 Knoxville USA, CERN-LHC-Project-Report-812. Geneva: CERN, 14 Jun 2005. 4 p.

LIST OF FIGURES

Figure 1.1: The LHC and octants destinations. 21

Figure 1.2: CERN accelerator complex, not in scale. 22

Figure 1.3: Reference filling pattern of the LHC. 23

Figure 1.4: Accelerator Beam and total Energy comparison. 25

Figure 1.5: Superconducting phase diagram of the NbTi. 26

Figure 1.6: Simplified diagram of the source of dump requests. 29

Figure 1.7: The LBDS schematic. 30

Figure 1.8: Dependency of the LBIS. 32

Figure 1.9: The LBIS backbone representation. 33

Figure 2.1: Schematic of the signal processing from the bam loss measurement to the beam permit generation. 35

Figure 2.2: Simplified VME configuration for the BLMS. 36

Figure 2.3: Left: the longitudinal energy deposition in the superconducting dipole at top energy. The impact point of the protons on the beam screen is at s = 0 m. 40

Figure 2.4: Quench levels for the LHC dipole magnet as a function of loss duration. 41

Figure 2.5: Simulation of the horizontal losses in the superconductive magnets during normal operation at 450 GeV. In the insert: magnification of the losses around the quadrupole region. Courtesy of S. Redaelli. 43

Figure 2.6: Longitudinal shower distribution for a point loss along quadrupole. 44

Figure 2.7: Radial distribution of secondary particle outside the magnet cryostat with respect the cryostat centre and the horizontal plane [15]. 44

Figure 2.8: Loss monitor placements (bars) and most likely loss location (cross) around a quadrupole [11]. 45

Figure 2.9: Fasten system of the ionization chamber on the quadrupole cryostat. 45

Figure 2.10: Design of the BLM with the external cylinder sectioned. 46

Figure 2.11: Electrical schematics of the Ionization chamber. 47

Figure 2.12: The CFC channel representation. 48

Figure 2.13 : Scan from 10 pA to 1 mA of an FEE, before and after irradiation of the CFC JFET. 49

Figure 2.14: Signal variation during the JFET irradiation with different fluxes. 51

Figure 2.15: Transmission FPGA representation. 52

Figure 2.16: The BEE representation. 57

Figure 2.17 : Schematic circuit and functional schemes of the beam permits switch. 59

Figure 2.18: Combiner card representation. 60

Figure 2.19: Standard rack representation. Optical fibres links are omitted. 61

Figure 2.20: Variation of the quench levels with the beam energy and loss duration. 62

Figure 3.1: Historical development of the dependability. 69

Figure 3.2: Graphical summary of the dependability disciplines. 78

Figure 3.3: Acceleration factor calculated with the Arrhenius formula for an operational temperature of 30°C and activation energy range between 0.3 and 1.1 eV. 81

Figure 3.4: Confidence range example. 83

Figure 3.5: Bath tube curve. 84

Figure 3.6: Example of Fault Tree diagram. 87

Figure 4.1: Probability of an erroneous digital transmission during a BLMS mission. 105

Figure 4.2: Simplified flowchart for HTLF test. 106

Figure 4.3: Simplified flowchart for HTAT. 108

Figure 4.4: Simplified flowchart of TCAM during installation. 111

Figure 4.5: Flowchart oh TCAC during operation. 112

Figure 4.6: Synoptic flow chart of the BLMS tests. 113

Figure 4.7: Diagram of the FMECA from level 0 to 3. Block name, criticalities and failure rates are reported. 116

Figure 4.8: Dipole magnet current and field during one LHC mission. The different beam phases are indicated [6, p 524]. 117

Figure 4.9: Dormant unavailability Q(t) in case of model with hazard rate λ and inspection period τ. 120

Figure 4.10: Top and first level of the Fault Tree diagram for the probability to not detect a dangerous loss. 123

Figure 4.11: Unavailability variation of the BLMS components tested every mission or yearly. 124

Figure 4.12: Relative importance of the event for the Damage Risk exposition. 125

Figure 4.13: Schematic of some Level 5 events of the False Alarm fault tree. 126

Figure 4.14: Fussell-Vesely importance for the False Alarm generation in the BLMS. 129

Figure 4.15: Fussell-Vesely importance ranking for the Warning generation in the BLMS. 131

Figure 4.16: Fussell-Vesely importance ranking for the failure generation in the Optical line. 131

Figure B.5.1: Full diagram of the BLMS FMECA. 165

LIST OF TABLES

Table 1.1: Luminosity parameters at 7 TeV. 24

Table 1.2: Some LHC beam parameters. 25

Table 1.3: Approximated damage and quench levels for instantaneous losses. 28

Table 2.1: Quantities of the BLMS components. 37

Table 2.2: Characteristic loss levels relative to the quench level [13]. 39

Table 2.3: Irradiation behaviours of the analogue CFC components. 50

Table 2.4: Estimated maximum electronics irradiation in the LHC. 51

Table 2.5 : The FEE status bit table. 54

Table 3.1: Summary of the basic dependability functions. 72

Table 3.2: ”Transformations” from reliability to maintainability and vice versa. 73

Table 3.3: MCS of example in figure 3.6. 88

Table 3.4: Qs and ws with the MCS methods. 89

Table 3.5: Comparison of the techniques for the evaluation of the system dependability. 91

Table 3.6: Gravity tables used for LHC risk definition. 92

Table 3.7: Frequency categories table. 92

Table 3.8: Risk Table. 93

Table 3.9: SIL values for Low demand mode of operation (< 1/ year or <2/ check time). 93

Table 3.10: SIL values for high demand/continuous mode of operation. 93

Table 3.11: Risk levels definitions. 94

Table 4.1: Prediction of the hazard rates of components of the electronics located in the LHC tunnel. 98

Table 4.2: Prediction of the hazard rates of the components used in the surface electronics. 99

Table 4.3: Synoptic table of the testing processes. 101

Table 4.4: Double Optical Line Comparison table. 103

Table 4.5: Suggested alarms for the HTLF test. 107

Table 4.6: Severity table for the BLMS. 116

Table 4.7: BLMS components sorted by criticality for a mission time of 12 hours. 118

Table 4.8: Subdivision of the BLMS in logic subsystems with section references. 119

Table 4.9: Evaluation of the unavailability and of the unconditional failure intensity in simplified cases. 122

Table 4.10: Inspection intervals for the BLMS testing processes. 123

Table 4.11: Failure rate per inspection interval and logic subsystems of BLMS. They are also subdivided by final effects: DR for Damage Risk and FA for False Alarm. 134

Table 4.12: Unreliability for the Damage Risk and the False Alarm generation per subsystem and inspection time. Percentages over the total are shown too. 135

Table 4.13: Sensitivity index of the BLMS components for the Damage Risk event. 137

Table 4.14: Sensitivity index of the BLMS components for the False Alarm event in a not redundant configuration. 138

Table 4.15: Sensitivity indexes for the inspection periods and maximum allowed before reaching the 2E-3 limits for the DR and 0.05 for FA. 139

Table 4.16: Synoptic table of the assumed hypotheses during the BLMS analysis. 140

Appendix A Quench Levels Calculations

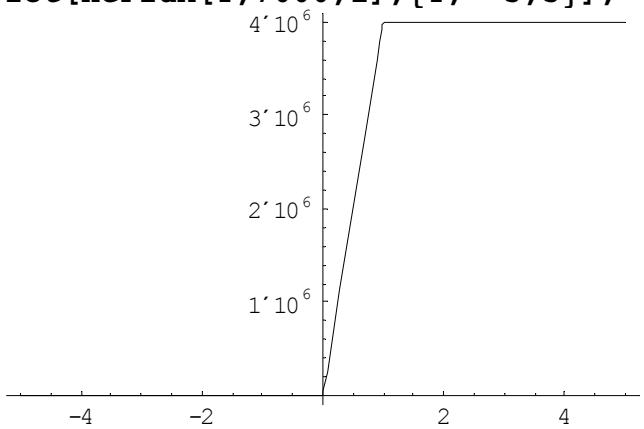
The Mathematica 5.1 notebook has been used for the estimation of the magnet quench limits. The main calculation is performed with a system of differential equation at page 163. The fitting with 20 MPa of helium pressure is calculated to test the variation with the helium property. Several properties (like energy deposition and effective length) have been, due to the lack of data, just linear interpolated with the energy.

Definition of the rectangular function, used for the Helium flux shape and for the proton loss shape.

```
Clear[UnitSquare];
UnitSquare[x_,init_,fin_]:=(UnitStep[x-init]-UnitStep[x-
fin]);
```

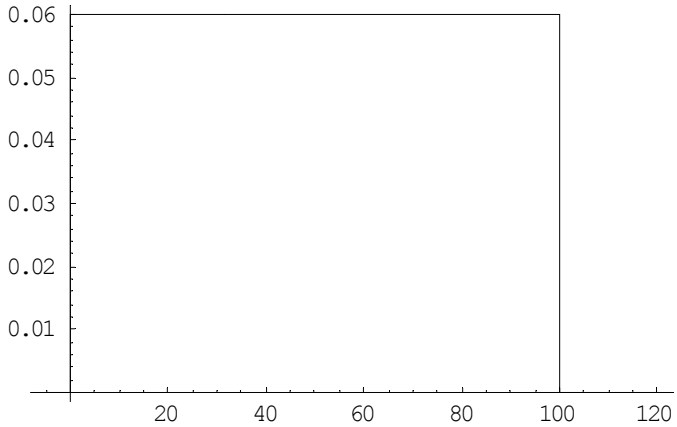
Helium thermal flux (in MKS:W/m3)

```
Clear[HeFlux,FluxMax,i,GeV];
Sv:=800
DTmax:=1
FluxMax[GeV_]:=Evaluate[Fit[{{450,10000},{7000,5000}},{1,GeV}
   , GeV]];
HeFlux[DT_,GeV_, flux_]:= Sv*FluxMax[GeV]*
   (DT/DTmax*UnitSquare[DT,0,DTmax]+flux *UnitStep[DT-
   DTmax]);
Plot[HeFlux[T,7000,1],{T, -5,5}];
```



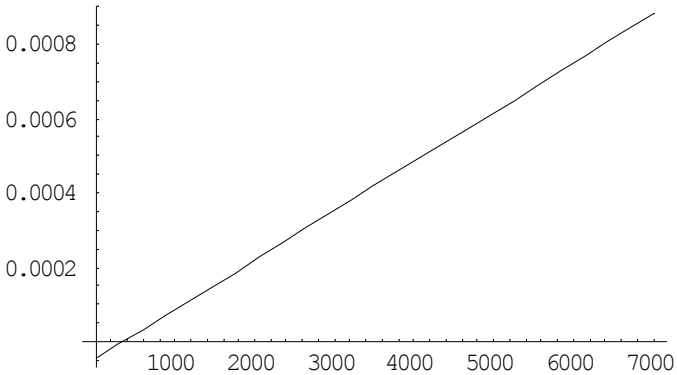
Loss rate in proton per second

```
LossRate[t_, tmax_,ptot_]:=ptot/tmax*UnitSquare[t,0,tmax];
Plot[LossRate[t, 100,6],{t, -5,120}];
```



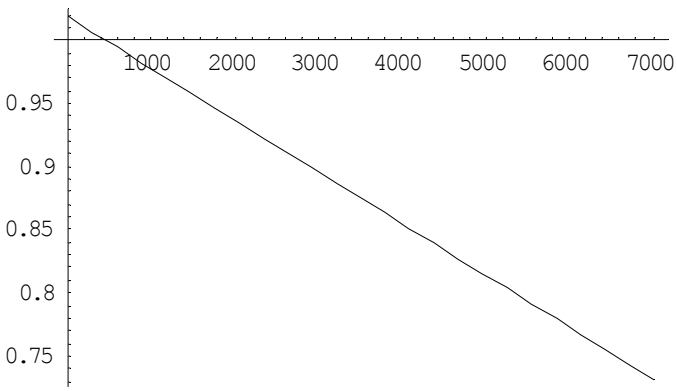
Energy deposition in J/m^3 (ε_{ra} on the paper)

```
EnDep7:=0.88 10^-9*10^6;
EnDep450:=1.4 10^-11*10^6;
EnDep[GeV_]:=(EnDep7-EnDep450)/(7000-450)*(GeV-450)+EnDep450;
Plot[EnDep[x],{x,0,7000}];
```



Effective Length in m

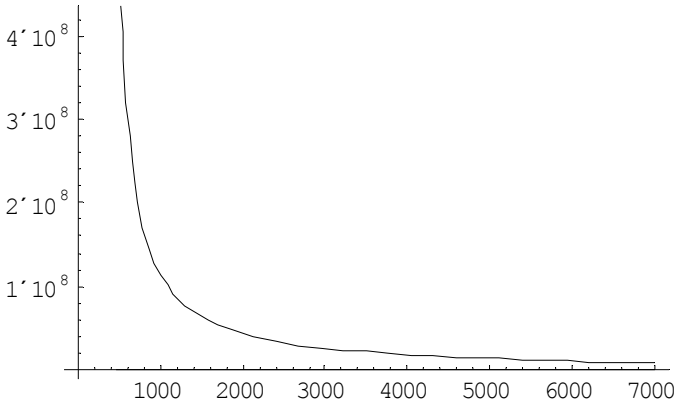
```
Leff7:=0.732;
Leff450:=1;
Leff[GeV_]:=(Leff7-Leff450)/(7000-450)*(GeV-450)+Leff450;
Plot[Leff[x],{x,0,7000}];
```



Steady rate of proton loss in p/s m, using the heat transmission capability in W/m^3 and the above defined Energy deposition and Effective Length.

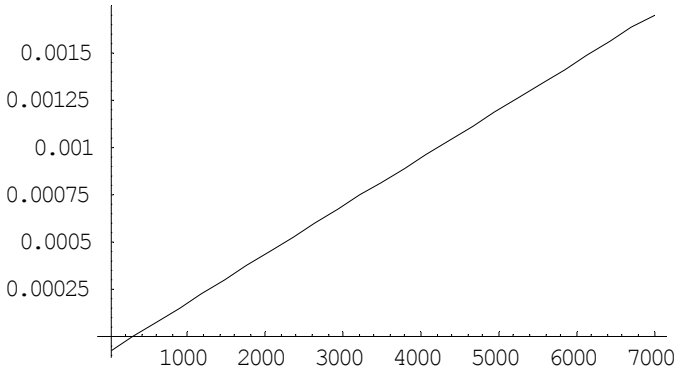
```
wq450:=10000;
wq7:=5000;
wq[GeV_]:=(wq7-wq450)/(7000-450)*(GeV-450)+wq450;
```

```
nsteady[GeV_]:=wq[GeV]/EnDep[GeV]/Leff[GeV];Plot[{wq[x],nstea
dy[x]},{x,450,7000}];
```



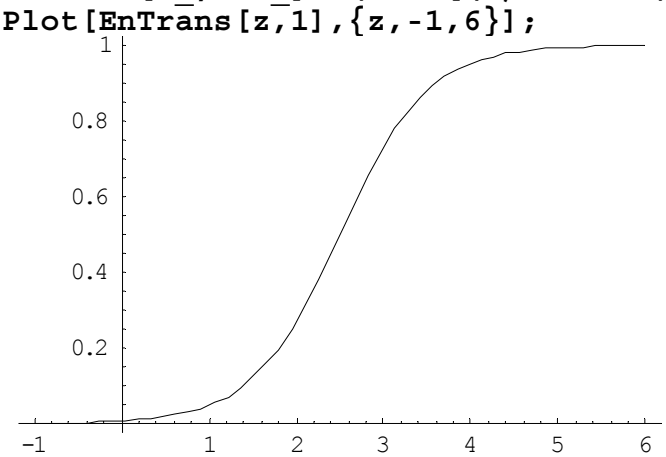
Peak Energy deposition in J/m^3 (ε_{peak} on the paper)

```
EnPeak7:=1.7 10^-9*10^6;
EnPeak450:=3.8 10^-11*10^6;
EnPeak[GeV_]:= (EnPeak7-EnPeak450)/(7000-450)*(GeV-450)+
   EnPeak450;
Plot[EnPeak[x],{x,0,7000}];
```



Energy Transition function: necessary to match the E_{peak} at fast losses with E_{ra} at slower ones. A 5-tau Sigma function has been used.

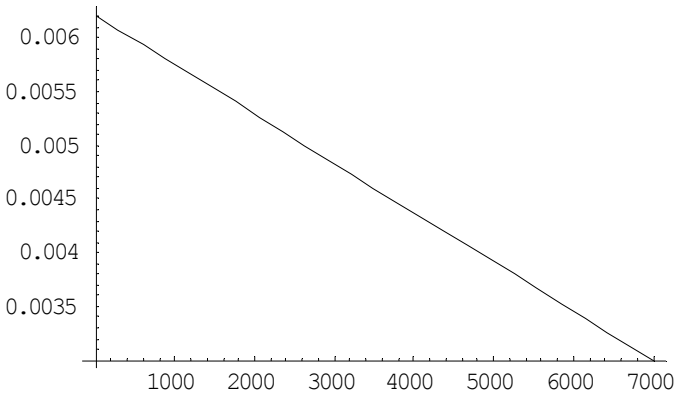
```
EnTrans[t_,tau_]:=(Tanh[(t/tau-2.5)]+1)/2;
Plot[EnTrans[z,1],{z,-1,6}];
```



Cable Time Constant, derived from the paper and used either in the equation or Transient Energy definition

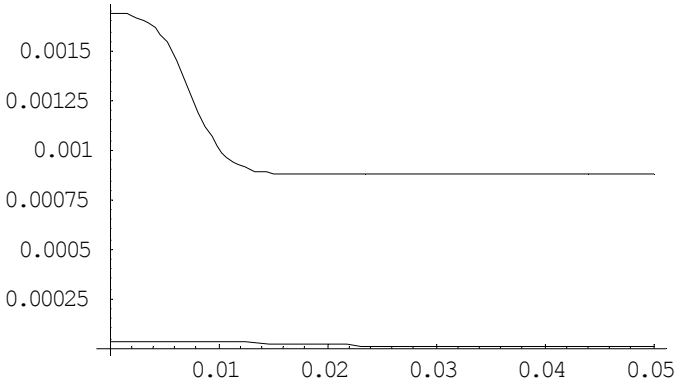
```
TimeCable7:=3 10^-3;
```

```
TimeCable450:=6 10^-3;
TimeCable[GeV_]:=(TimeCable7-TimeCable450)/(7000-450)*(GeV-
   450)+TimeCable450;
Plot[TimeCable[x],{x,0,7000}];
```



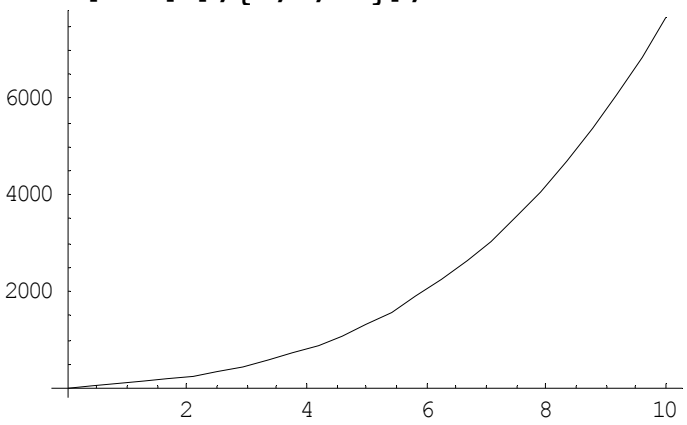
Transient Energy definition, used into equations, representing the deposited energy in function of loss duration

```
EnTransient[t_,GeV_]:=EnPeak[GeV]+EnTrans[t,TimeCable[GeV]]*(
   EnDep[GeV]-EnPeak[GeV]);
Plot[{EnTransient[t,7000],EnTransient[t,450]},{t,0,0.05}];
```



Copper thermal specific heat (in MKS: J/ m^3K)

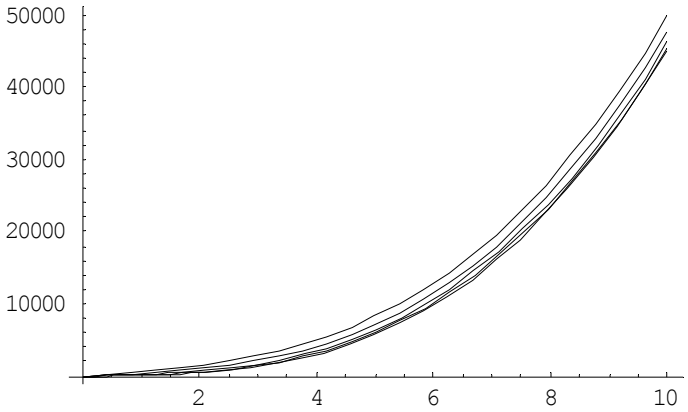
```
gamCu:=96.86 ;
alpCu:=6.684;
CCu[T_]=gamCu T+alpCu T^3;
Plot[CCu[T],{T,0,10}];
```



NbTi thermal specific heat (in MKS: J/m^3K)

Magnetic field estimation.

```
Bm[GeV_]:=8.65/7000 GeV;
Bm[450]
0.556071
gamNT:=870 ;
Bc:=14;
alpNT:=44.64;
CNT[T_,GeV_]=gamNT Bm[GeV]/Bc T+alpNT T^3;
Plot[{CNT[T,450],CNT[T,1000],CNT[T,2000],CNT[T,4000],CNT[T,70
   00]},{T,0,10}];
```

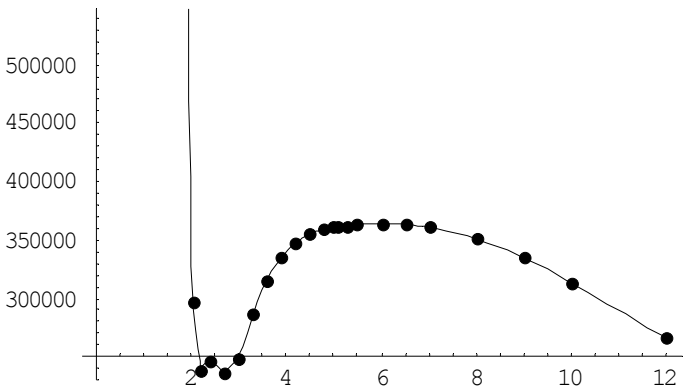


Wire thermal specific heat (in MKS: J/ m^3K)

```
fwire:=1.6;
Cw[T_,GeV_]=(fwire CCu[T]+CNT[T,GeV])/(1+fwire);
Hwire=Integrate[Cw[T,450],{T,1.9,9}]
37660.
```

Helium thermal specific heat (in MKS: J/ m^3K).
Fitting data from 1.9 to 9 K. @ 2MPa
Tlamba is 1.932: we consider only HeII.
Data from NIST 1998, point at 1,9 interpolated such as Qλ=233000 J/ m^3.

```
HeIICvpoints:={{1.9,2.1286221333333524`*^6},{1.933,171.7*5.21
   8 10^3},{1.942,171.7*3.260 10^3},{2.032,171.8*1.727
   10^3},{2.200,171.5*1.394 10^3},{2.400,171.0*1.447
   10^3},{2.700,170.2*1.393 10^3},{3.000,169.3*1.471
   10^3},{3.300,168.2*1.703 10^3},{3.600,166.9*1.895
   10^3},{3.900,165.5*2.030 10^3},{4.200,163.9*2.123
   10^3},{4.500,162.1*2.190 10^3},{4.800,160.2*2.242
   10^3},{5.000,158.9*2.273 10^3},{5.100,158.2*2.287
   10^3},{5.300,156.7*2.315 10^3},{5.500,155.3*2.342
   10^3},{6.000,151.3*2.408 10^3},{6.500,147.0*2.474
   10^3},{7.000,142.3*2.539 10^3},{8.000,132.1*2.662
   10^3},{9.000,120.9*2.773 10^3},{10.000,109.3*2.870
   10^3},{12.00,88.17*3.016 10^3}};
CvHeIIin=Interpolation[HeIICvpoints,InterpolationOrder •1];
Plot[CvHeIIin[T],{T,1.9,12},Epilog•Prepend[Point/@HeIICvpoint
s,PointSize[0.02]]];CvHe[T_]=CvHeIIin[T] ;
Vratio=(56.6+35.4)/5;
```



Main calculations.
Enter:
1-the directory and the name of the file, put **`savefile=True`** if you want to save the file,
2-the Energy of the beam,
3-the quench and steady temperature,
4-put **`withflux=0`** if you want 0 flux into He above Tgap=1
5-put **`withcable=0`** if you don't want to take into consideration the cable contribution to the dissipation,
6-define the initial and final loss duration and the number of points to be computed

The first For cycle runs over the time with logarithmic steps. It will use the last total lost protons (nlosst) for the following calculation. The second For cycle solves the differential equations changing the parameter nlossf (total protons in the loss) and stop only when the maximum temperature of the wire is Tquench or the instabilities for that loss are given by really closed number of protons. In the latter case the note "inst" will be added.
The output file contains the basic parameters and 5 columns: loss duration, protons in the loss, total protons, total protons rate and notes.

```
dir="C:\destination_directory";
filename="7TeV";
savefile=False;

EnGeV=450;

Tsteady=1.9;
Tquench=9;
DTquench=Tquench-Tsteady;

withflux=0;
withcable=0;

tlossinit=10^-2;
tlossfinal=10^-2;
numpoints=2;

toll=0.00001;
ntoll=0.00001;

SetDirectory[dir];
```

```
file=StringJoin[filename,"_",ToString[Round[FromDate[Date[]]]
   ],".dat"];
arr={{StringJoin["\"",dir,"\\",file,"\""]},{StringJoin["Energ
   y=",ToString[EnGeV]],StringJoin["withflux=",ToString[withf
   lux]],StringJoin["withcable=",ToString[withcable]]},{"
   "},{"Time[s]","Add_losses","Tot_loss[p]","Rate[p/s]","MaxH
   eFlux[W/m3]","HeFlux(Time)[w/m3]","Note"}};

nlosst=10^10;

For[k=0;nlossf=nlosst,k<numpoints,k++,
tloss=tlossinit*(tlossfinal/tlossinit)^(k/(numpoints-
1));test=True;
 For [tcalc=2*tloss;nlossf=nlosst; nmax=10^16;
 nmin=1;DTinf=0;DTsup=4000;DTMAX=0;i=1;note=" ",
   test,
   i++,

   (*Differential equations calculation*)
   solution=NDSolve[
    {DTw'[t]==
      (LossRate[t,tloss,nlossf]*EnTransient[tloss,EnGeV]-
      HeFlux[DTw[t]-DTh[t],EnGeV,withflux])
      /Cw[DTw[t]+Tsteady,EnGeV]-
      DTw[t]/TimeCable[EnGeV]*withcable,
    DTh'[t]==
      Vratio/CvHe[DTh[t]+Tsteady]* HeFlux[DTw[t]-DTh[t],EnGeV,
      withflux],
    DTw[0]==0, DTh[0] == 0},
    {DTw, DTh},
    {t, 0, tcalc}
    ]
    (*end Solution*);


   DTwire[t_]:=DTw[t]/.solution;
   DTHe[t_]:=DTh[t]/.solution;
   DTMAX=Part[DTwire[tloss],1];
   nnext=nlossf*DTquench/DTMAX;
   nlosst=nlossf;
   If[DTMAX>DTquench,
    (*If1 true*)
    nmax=nlossf;
    DTsup=DTMAX;
    If[nnext<nmin,
     (*If2a true*)
     nlossf=(nmax*DTinf+nmin*DTsup)/(DTinf+DTsup);note="inst"
     ,
     (*If2a false*)
     nlossf=nnext;note=" "
    ],
    (*If1 false*)
    nmin=nlossf;
    DTinf=DTMAX;
    If[nnext>nmax,
     (*If2b true*)
     nlossf=(nmax*DTinf+nmin*DTsup)/(DTinf+DTsup);note="inst"
     ,
```

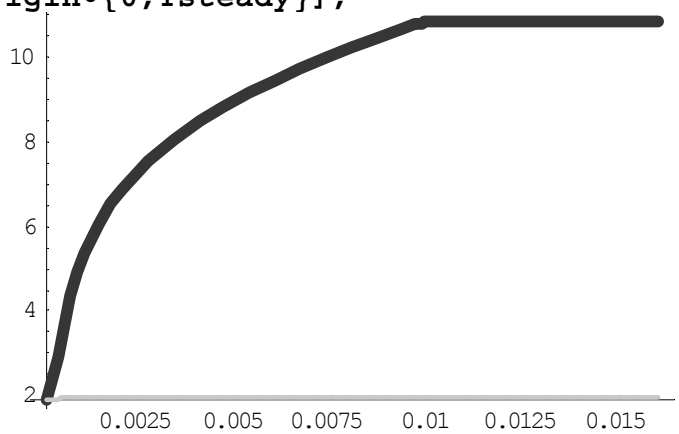
```
      (*If2b false*)
      nlossf=nnext;note= " "]
   ];(*end If 1*)

   test=And[Or[DTMAX>DTquench+toll,DTMAX<DTquench-
   toll],(nmax-nmin)/nmin>ntoll];
  ]; (*end For 2*)
time=EngineeringForm[N[tloss]];
ntotal=nlosst+nsteady[EnGeV]*tloss;
ratetotal=nlosst/tloss+nsteady[EnGeV];
maxHeflux=Part[NMaximize[{HeFlux[Part[DTwire[t]-
DTHe[t],1],EnGeV,withflux],t>0,t<tloss},t],1];
finalHeflux=HeFlux[Part[DTwire[tloss]-
DTHe[tloss],1],EnGeV,withflux];
Print[time," ",nlosst," ",ntotal," ",maxHeflux,"
",finalHeflux," ",note];
arr=Append[arr,{N[tloss],N[nlosst],N[ntotal],N[ratetotal],N[m
   axHeflux],N[finalHeflux],note}];
    ]; (*end For 1*)
If[savefile,Export[file,arr,"Table"]];
```

$10.\times 10^{-3}$ 2.38138×10^{9} 2.38853×10^{9} 7.99999×10^{6} 6.21914×10^{6} inst

$10.\times 10^{-3}$ 2.3814×10^{9} 2.38855×10^{9} $8.\times 10^{6}$ 0 inst

Evaluate the following plot to have the temperature profile of the last calculation of the previous cycle.

```
tgraph=tloss*1.6;
Plot[{DTwire[t]+Tsteady,DTHe[t]+Tsteady},{t,0,tgraph},PlotSty
le•{{Thickness[.02],Hue[0]},{Thickness[.01],Hue[0.5]}},AxesOr
igin•{0,Tsteady}];
```



Appendix B FMECA

The Failure Modes, Effects and Criticality Analysis of the BLMS is reported in this appendix, following the indication of the MIL-1629 [31].

The general diagram is reported in the figure below.

Figure B.5.1: Full diagram of the BLMS FMECA.

BLMS FMECA — Mission time: 12 h

Level: — Notes:

Block: BLMS — N: 1

FR [1/h]: 1.06E-2

Description :Beam Loss Monitors System — NxFR [1/h]: 1.06E-2

PN: — Block Criticality [h/mis]:

Function: Detect the losses and inhibit the LHC Beam Permit

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Damage Risk	4.76e+0	5.05e-04	Tunnel.01 Hidden channel failure, Surface.01 Hidden thresholds failure, Surface.02 Hidden combiner failure, Surface.03 Hidden backplane failure	None	N/A	Damage Risk	HT test, Logging, BIL test	4.36e+0	720h
02	False Alarm	2.57e+1	2.73e-03	Tunnel.02 Tunnel PS failure, Tunnel.03 CFC failure, Surface.04 VME fans failure, Surface.05 DAB failure, Surface.06 Thresholds failure, Surface.07 Crate failure	None	N/A	False Alarm	10 pA test, Surface and tunnel HT status, Fail safe, Tunnel status.	9.84e-2	3h
03	Warning	6.95e+1	7.37e-03	Tunnel.04 Tunnel Optical link failure, Tunnel.05 HT Test failure, Tunnel.06 HT status failure, Surface.08 VME PS failure, Surface.09 Surface HT failure, Surface.10 Surface Optical link failure, Surface.11 DAB temperature not checked, Surface.12 No test from combiner	None	N/A	Warning	DOLC, HT test, Fail safe, Surface status,	8.85e-2	1h

BLMS FMECA — Mission time: 12

hLevel: 1 — Notes:

Block: Tunnel (Parent: BLMS) — N: 8

FR [1/h]: 1.15e-3

Description: Tunnel electronic per sector — NxFR [1/h]: 9.21e-3

PN: Octants — Block Criticality [h/mis]: 5.63e-1

Function: Signal acquisition and digitalization

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Hidden channel failure	5.47e+0	6.30e-05	Common.01 Hidden CFC failure, Common.02 Hidden IC failure	Damage Risk	N/A	Damage Risk	HT test	5.44e-1	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 1 — Notes:

Block: Tunnel (Parent: BLMS) — N: 8

FR [1/h]: 1.15e-3

Description: Tunnel electronic per sector — NxFR [1/h]: 9.21e-3

PN: Octants — Block Criticality [h/mis]: 5.63e-1

Function: Signal acquisition and digitalization

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
02	Tunnel PS failure	1.34e+1	1.54e-04	Only arc.01 Wrong arc alimentation, Only arc.02 No arc alimentation, Only SS.01 Wrong SS alimentation, Only SS.02 No SS alimentation	False Alarm	N/A	False Alarm	Fail safe	5.55e-3	
03	CFC failure	7.94e+0	9.15e-05	Common.03 Channel failure, Common.04 Statuses failure, Common.05 No data, Common.06 No 10pA signal, Common.07 False HT test	False Alarm	N/A	False Alarm	10 pA test, Surface and tunnel HT status	3.29e-3	
04	Tunnel Optical link failure	7.32e+1	8.43e-04	Common.08 Optical line failure	Warning	N/A	Warning	DOLC	1.01e-2	
05	HT Test failure	1.11e-3	1.28e-08	Common.10 No HT test	Warning	N/A	Warning	HT test	1.53e-7	
06	HT status failure	1.41e-2	1.63e-07	Common.09 Hidden wrong HT status	Warning	N/A	Warning		1.95e-6	

BLMS FMECA — Mission time: 12 h

Level: 1 — Notes:

Block: Surface (Parent: BLMS) — N: 8

FR [1/h]: 1.75e-4

Description: Surface electronics per point — NxFR [1/h]: 1.40e-3

PN: Surface points — Block Criticality [h/mis]: 5.20e-3

Function: Threshold comparison and beam permit generation

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Hidden thresholds failure	4.17e-2	7.29e-08	DAB.01 Wrong energy, DAB.02 No right thresholds	Damage Risk	N/A	Damage Risk	Logging	6.30e-4	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 1 — Notes:

Block: Surface (Parent: BLMS) — N: 8

FR [1/h]: 1.75e-4

Description: Surface electronics per point — NxFR [1/h]: 1.40e-3

PN: Surface points — Block Criticality [h/mis]: 5.20e-3

Function: Threshold comparison and beam permit generation

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
02	Hidden combiner failure	9.42e-3	1.65e-08	Crate.01 Hidden combiner failure	Damage Risk	N/A	Damage Risk	Logging, BIL test	1.43e-4	
03	Hidden backplane failure	1.56e-3	2.73e-09	Crate.02 False closed backplane line	Damage Risk	N/A	Damage Risk	BIL test	2.36e-5	
04	VME fans failure	5.43e+1	9.50e-05	VME tray.01 VME Ventilation failure	False Alarm	N/A	False Alarm		3.42e-3	
05	DAB failure	4.68e-1	8.19e-07	DAB.03 FPGA dump request, DAB.04 Wrong temperature signal	False Alarm	N/A	False Alarm	Fail safe, Surface status	2.95e-5	
06	Thresholds failure	2.49e-2	4.36e-08	DAB.05 No Energy signal, DAB.06 No thresholds	False Alarm	N/A	False Alarm	Fail safe	1.57e-6	
07	Crate failure	2.95e-2	5.17e-08	Crate.03 Combiner failure, Crate.04 False open backplane line	False Alarm	N/A	False Alarm	Fail safe, Tunnel status	1.86e-6	
08	VME PS failure	3.26e+1	5.70e-05	VME tray.02 VME PS failure	Warning	N/A	Warning		6.84e-4	
09	Surface HT failure	1.09e+1	1.90e-05	HTPS.01 HT PS failure	Warning	N/A	Warning	Fail safe	2.28e-4	Redundancy
10	Surface Optical link failure	1.56e+0	2.73e-06	DAB.07 Wrong optical data, DAB.08 No optical data	Warning	N/A	Warning	DOLC	3.28e-5	Redundancy
11	DAB temperature not checked	1.52e-1	2.66e-07	DAB.09 No temperature signal	Warning	N/A	Warning	Surface status	3.19e-6	
CONTINUE										

BLMS FMECA — Mission time: 12 h

Level: 1 — Notes:

Block: Surface (Parent: BLMS) — N: 8

FR [1/h]: 1.75e-4

Description: Surface electronics per point — NxFR [1/h]: 1.40e-3

PN: Surface points — Block Criticality [h/mis]: 5.20e-3

Function: Threshold comparison and beam permit generation

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
12	No test from combiner	3.75e-2	6.57e-08	Crate.05 No HT test from combiner	Warning	N/A	Warning	HT test	7.88e-7	

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: Common (Parent: Tunnel) — N: 72

FR [1/h]: 1.39e-5

Description: Common tunnel electronic — NxFR [1/h]: 9.97e-4

PN: In all the octants — Block Criticality [h/mis]: 7.75e-3

Function: Signal acquisition and digitalization

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Hidden CFC failure	4.75e+0	6.58e-07	#integrator.01 Hidden wrong CFC signal, #comp.02 Hidden wrong CFC signal, #monostable.02 Hidden wrong CFC signal, #jfet.02 Wrong CFC signal, #ADC.01 Hidden Wrong ADC signal, #translator.02 Wrong ADC signal, #translator.03 Low ADC signal, #FPGATX.01 Wrong CFC signal, #10pASource.01 Wrong 10pA signal	Hidden channel failure	Damage Risk	Damage Risk	HT test	5.69e-3	
02	Hidden IC failure	1.57e+0	2.17e-07	#IC.01 Noise variation, #IC.02 No IC signal, #IC.03 Wrong signal, #IC.05 Noise increase	Hidden channel failure	Damage Risk	Damage Risk	HT test + gain test	1.88e-3	
03	Channel failure	9.05e+0	1.25e-06	#IC.04 No HT, #HTcon.1 No HT, #HTcon.2 Wrong HT, #integrator.02 No CFC signal, #comp.01 No CFC signal, #monostable.01 No CFC signal, #jfet.01 No CFC signal, #ADC.02 No ADC signal, #translator.01 No ADC signal, #translator.04 High ADC signal	CFC failure	False Alarm	False Alarm	10 pA test, surface and tunnel status	4.51e-5	
04	Statuses failure	8.51e-2	1.18e-08	#status.01 No PS status, #status.02 No HT status, #status.03 Wrong PS status	CFC failure	False Alarm	False Alarm	Tunnel status	4.25e-7	
05	No data	3.14e-2	4.35e-09	#FPGATX.02 No counter reading, #FPGATX.04 No FPGA data	CFC failure	False Alarm	False Alarm	Tunnel status + 10 pA test	1.57e-7	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: Common (Parent: Tunnel) — N: 72

FR [1/h]: 1.39e-5

Description: Common tunnel electronic — NxFR [1/h]: 9.97e-4

PN: In all the octants — Block Criticality [h/mis]: 7.75e-3

Function: Signal acquisition and digitalization

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
06	No 10pA signal	6.22e-4	8.62e-11	#10pASource.02 No 10pA signal	CFC failure	False Alarm	False Alarm	10 pA test	3.10e-9	
07	False HT test	2.88e-5	3.99e-12	#HT activator.02 Wrong test status	CFC failure	False Alarm	False Alarm	Tunnel status	1.44e-10	
08	Optical line failure	8.45e+1	1.17e-05	#GOH.01 No optical data, #GOH.02 Useless transmission, #GOH.03 Wrong optical data, #fibre.01 Higher BER, #fibre.02 No optical data, #OFcon.01 higher BER, #OFcon.02 No optical data	Tunnel Optical link failure	Warning	Warning	DOLC	1.40e-4	Redundancy
09	Hidden wrong HT status	1.63e-2	2.26e-09	#FPGATX.03 No HT reading, #status.04 Hidden wrong HT status	HT status failure	Warning	Warning		2.71e-8	
10	No HT test	1.28e-3	1.78e-10	#HT activator.01 No test status	HT Test failure	Warning	Warning	HT test	2.13e-9	

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: Only arc (Parent: Tunnel) — N: 45

FR [1/h]: 5.78e-9

Description: Arc Power Supplies — NxFR [1/h]: 2.60e-7

PN: Only in the arc — Block Criticality [h/mis]: 2.08e-7

Function: Provides power for the arc electronics

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong arc alimentation	5.72e+1	3.31e-09	#PSarc.01 Wrong alimentation	Tunnel PS failure	False Alarm	False Alarm	Fail safe	1.19e-7	
02	No arc alimentation	4.28e+1	2.47e-09	#PSarc.02 No alimentation	Tunnel PS failure	False Alarm	False Alarm	Fail safe	8.91e-8	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: Only SS (Parent: Tunnel) — N: 27 — FR [1/h]: 5.70e-6

Description: Straight Section Power supplies — NxFR [1/h]: 1.54e-4

PN: Only Straight Section — Block Criticality [h/mis]: 2.05e-4

Function: Provides power for the Straight Section electronics

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
01	Wrong SS alimentation	5.72e+1	3.26e-06	#PSSSHV.01 Wrong alimentation, #PSSSLV.01 Wrong alimentation	Tunnel PS failure	False Alarm	False Alarm	Fail safe	1.17e-4	
02	No SS alimentation	4.28e+1	2.44e-06	#PSSSHV.02 No alimentation, #PSSSLV.02 No alimentation	Tunnel PS failure	False Alarm	False Alarm	Fail safe	8.78e-5	

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: DAB (Parent: Surface) — N: 39 — FR [1/h]: 1.01e-7

Description: Data Acquisition Board — NxFR [1/h]: 3.94e-6

PN: DAB board — Block Criticality [h/mis]: 1.79e-5

Function: Data analysis and beam permit generation.

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong energy	1.84e+0	1.85e-09	#FPGARX.02 No energy updating, #transceiver.02 Wrong energy signal	Hidden thresholds failure	Damage Risk	Damage Risk	Logging	1.60e-5	
02	No right thresholds	1.53e-2	1.54e-11	#memory.02 No right thresholds	Hidden thresholds failure	Damage Risk	Damage Risk	Logging	1.33e-7	
03	FPGA dump request	1.63e+1	1.65e-08	#FPGARX.01 FPGA dump request	DAB failure	False Alarm	False Alarm	Fail safe	5.93e-7	
04	Wrong temperature signal	4.5e+0	4.54e-09	#temperature.02 Wrong temperature signal	DAB failure	False Alarm	False Alarm	Surface status	1.63e-7	
05	No Energy signal	9.86e-1	9.96e-10	#transceiver.01 No Energy signal	Thresholds failure	False Alarm	False Alarm	Fail safe	3.58e-8	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: DAB (Parent: Surface) — N: 39 — FR [1/h]: 1.01e-7

Description: Data Acquisition Board — NxFR [1/h]: 3.94e-6

PN: DAB board — Block Criticality [h/mis]: 1.79e-5

Function: Data analysis and beam permit generation.

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
06	No thresholds	1.22e-1	1.24e-10	#memory.01 No thresholds	Thresholds failure	False Alarm	False Alarm	Fail safe	4.45e-9	
07	Wrong optical data	3.62e+1	3.66e-08	#photodiode.01 Higher BER, #TLK.02 Wrong optical data	Surface Optical link failure	Warning	Warning	DOLC	4.39e-7	Redundancy
08	No optical data	3.32e+1	3.35e-08	#photodiode.02 No optical data, #TLK.01 No optical data	Surface Optical link failure	Warning	Warning	DOLC	4.02e-7	Redundancy
09	No temperature signal	6.75e+0	6.81e-09	#temperature.01 No temperature signal	DAB temperature not checked	Warning	Warning	Surface status	8.17e-8	

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: Crate (Parent: Surface) — N: 3 — FR [1/h]: 4.55e-8

Description: Electronics in the crates — NxFR [1/h]: 1.37e-7

PN: Combiners — Block Criticality [h/mis]: 5.62e-5

Function: Beam permit lines, LBIS interface, energy distribution, tests

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Hidden combiner failure	1.21e+1	5.50e-09	#Com_BP_in.02 False closed, #Combiner FPGA.02 Wrong combiner FPGA	Hidden combiner failure	Damage Risk	Damage Risk	Logging, BIL test	4.75e-5	
02	False closed backplane line	2.e+0	9.10e-10	#BPswitch.02 False closed	Hidden backplane failure	Damage Risk	Damage Risk	BIL test	7.86e-6	
03	Combiner failure	3.19e+1	1.45e-08	#Com_BP_in.01 False open, #Combiner FPGA.01 No combiner FPGA, #LBIS switch.01 No current loop, #HT DAC.02 False HT test from combiner	Crate failure	False Alarm	False Alarm	Fail safe, Tunnel status	5.22e-7	

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: Crate (Parent: Surface) — N: 3

FR [1/h]: 4.55e-8

Description: Electronics in the crates — NxFR [1/h]: 1.37e-7

PN: Combiners — Block Criticality [h/mis]: 5.62e-5

Function: Beam permit lines, LBIS interface, energy distribution, tests

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
04	False open backplane line	6.e+0	2.73e-09	#BPswitch.01 False open	Crate failure	False Alarm	False Alarm	Fail safe	9.83e-8	
05	No HT test from combiner	4.81e+1	2.19e-08	#HT DAC.01 No HT test from combiner	No test from combiner	Warning	Warning	HT test	2.63e-7	

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: HTPS (Parent: Surface) — N: 1

FR [1/h]: 1.90e-5

Description: Two redundant High Tension sources — NxFR [1/h]: 1.90e-5

PN: High Tension PS — Block Criticality [h/mis]: 2.28e-4

Function: Provide High Tension to the tunnel monitors

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	HT PS failure	1.00e+2	1.90e-05	#PSHT.01 Wrong HT, #PSHT.02 No HT	Surface HT failure	Warning	Warning	Fail safe	2.28e-4	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: VME crate (Parent: Surface) — N: 3

FR [1/h]: 5.07e-5

Description: VME Power Supplies and ventilation — NxFR [1/h]: 1.52e-4

PN: VME crate — Block Criticality [h/mis]: 1.37e-3

Function: Provide power and cooling to the surface electronic

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	VME Ventilation failure	6.25e+1	3.17e-05	#fantray.01 Low ventilation, #fantray.02 No ventilation	VME fans failure	False Alarm	False Alarm	DAB Temperature , Tray sensor	1.14e-3	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 2 — Notes:

Block: VME crate (Parent: Surface) — N: 3

FR [1/h]: 5.07e-5

Description: VME Power Supplies and ventilation — NxFR [1/h]: 1.52e-4

PN: VME crate — Block Criticality [h/mis]: 1.37e-3

Function: Provide power and cooling to the surface electronic

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
02	VME PS failure	3.75e+1	1.90e-05	#PSVME.01 Wrong alimentation, #PSVME.02 No alimentation	VME PS failure	Warning	Warning	Fail safe	2.28e-4	2oo3 connection

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #IC (Parent: Common) — N: 6

FR [1/h]: 4.41e-8

Description: Number of Ionization Chambers, the monitor — NxFR [1/h]: 2.65e-7

PN: ICs — Block Criticality [h/mis]: 3.13e-4

Function: Provide a current proportional to the lost particles

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Noise variation	2.8e+1	1.24e-08	IC+cable.06 CIC Change of Value, IC+cable.09 RIC Change of Value	Hidden IC failure	Hidden channel failure	Damage Risk	HT test	1.07e-4	
02	No IC signal	1.8e+1	7.94e-09	IC+cable.01 Signal Cable Shorts (Poor Sealing), IC+cable.02 Mechanical Failure of Cable Solder Joints	Hidden IC failure	Hidden channel failure	Damage Risk	HT test	6.86e-5	
03	Wrong signal	1.8e+1	7.94e-09	IC+cable.03 Cable Miscellaneous Mechanical Failures, IC+cable.04 Degradation of Cable Insulation Resistance, IC+cable.11 IC gas pressure change	Hidden IC failure	Hidden channel failure	Damage Risk	HT test + gain test	6.86e-5	
04	No HT	1.8e+1	7.94e-09	IC+cable.05 CIC Shorted (Electrical), IC+cable.10 RIC Open (Electrical)	Channel failure	CFC failure	False Alarm	Surface status	2.86e-7	
05	Noise increase	1.8e+1	7.94e-09	IC+cable.07 CIC Open (Electrical), IC+cable.08 RIC Shorted (Electrical)	Hidden IC failure	Hidden channel failure	Damage Risk	HT test	6.86e-5	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #HTcon (Parent: Common) — N: 12

FR [1/h]: 5.20e-10

Description: Number of HT connectors — NxFR [1/h]: 6.24e-9

PN: HT connectors — Block Criticality [h/mis]: 1.87e-8

Function: Provides High Tension from the surface to 6 monitors

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
1	No HT	5.52e+1	2.87e-10	HTcon.02 Shorts, HTcon.03 Broken, HTcon.04 Opened	Channel failure	CFC failure	False Alarm	Surface and tunnel HT status	1.03e-8	
2	Wrong HT	4.48e+1	2.33e-10	HTcon.01 Improper output, HTcon.05 Intermittent, HTcon.06 Loose	Channel failure	CFC failure	False Alarm	Tunnel status	8.39e-9	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #integrator (Parent: Common) — N: 8

FR [1/h]: 7.50e-8

Description: Number of integrator in the FEE — NxFR [1/h]: 6.00e-7

PN: Amplifiers — Block Criticality [h/mis]: 6.15e-4

Function: Integrate the current from the monitors

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Hidden wrong CFC signal	9.49e+1	7.12e-08	Integrator.01 Parametric Failure	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	6.15e-4	
02	No CFC signal	5.1e+0	3.83e-09	Integrator.02 Shorted, Integrator.03 Functional Failure	Channel failure	CFC failure	False Alarm	10 pA test	1.38e-7	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #comp (Parent: Common) — N: 4

FR [1/h]: 1.91e-7

Description: Number of comparators in the FEE — NxFR [1/h]: 7.65e-7

PN: Comparators (dual) — Block Criticality [h/mis]: 4.31e-5

Function: Trigger the monostable with the integrated value

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No CFC signal	9.78e+1	1.87e-07	Comparator.01 Not parametric failure	Channel failure	CFC failure	False Alarm	10 pA test	6.73e-6	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #comp (Parent: Common) — N: 4

FR [1/h]: 1.91e-7

Description: Number of comparators in the FEE — NxFR [1/h]: 7.65e-7

PN: Comparators (dual) — Block Criticality [h/mis]: 4.31e-5

Function: Trigger the monostable with the integrated value

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
02	Hidden wrong CFC signal	2.2e+0	4.21e-09	Comparator.02 Parametric failure	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	3.64e-5	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #monostable (Parent: Common) — N: 4

FR [1/h]: 1.15e-7

Description: Number of monostables in the FEE — NxFR [1/h]: 4.62e-7

PN: Monostables (dual) — Block Criticality [h/mis]: 1.28e-4

Function: Generate a pulses train

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No CFC signal	8.75e+1	1.01e-07	Monostable.01 Electrical overstressed, Monostable.02 No Output, Monostable.03 Opened, Monostable.04 Shorted High	Channel failure	CFC failure	False Alarm	10 pA test	3.64e-6	
02	Hidden wrong CFC signal	1.25e+1	1.44e-08	Monostable.05 Timing Error	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	1.25e-4	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #jfet (Parent: Common) — N: 8

FR [1/h]: 4.56e-10

Description: Number of JFETs in the FEE — NxFR [1/h]: 3.65e-9

PN: JFETs — Block Criticality [h/mis]: 1.50e-7

Function: Discharge the integrator

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No CFC signal	9.66e+1	4.40e-10	JFET.01 Shorted, JFET.02 Opened, JFET.03 Base- Emitter Shorted, JFET.04 Electrical Overstressed, JFET.05 Bond Failure	Channel failure	CFC failure	False Alarm	10 pA test	1.58e-8	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #jfet (Parent: Common) — N: 8

FR [1/h]: 4.56e-10

Description: Number of JFETs in the FEE — NxFR [1/h]: 3.65e-9

PN: JFETs — Block Criticality [h/mis]: 1.50e-7

Function: Discharge the integrator

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
02	Wrong CFC signal	3.4e+0	1.55e-11	JFET.06 Contamination	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	1.34e-7	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #ADC (Parent: Common) — N: 8

FR [1/h]: 1.00e-9

Description: Number of ADCs in FEE — NxFR [1/h]: 8.00e-9

PN: ADCs — Block Criticality [h/mis]: 3.43e-6

Function: Increase the dynamic range of the integration

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Hidden Wrong ADC signal	3.94e+1	3.94e-10	ADC.01 Parametric failure, ADC.05 Leakage	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	3.40e-6	
02	No ADC signal	6.06e+1	6.06e-10	ADC.02 Electrical failure, ADC.03 Fabrication defect, ADC.04 Stacking faults, ADC.06 Electrical overstresses	Channel failure	CFC failure	False Alarm	10 pA test	2.18e-8	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #translator (Parent: Common) — N: 6

FR [1/h]: 2.64e-9

Description: Number of translators in the FEE — NxFR [1/h]: 1.58e-8

PN: Translators — Block Criticality [h/mis]: 1.04e-5

Function: Translate the voltage levels from the ADC to the FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No ADC signal	4.54e+1	1.20e-09	Translator.01 Short Low, Translator.05 No Output	Channel failure	CFC failure	False Alarm	10 pA test	4.31e-8	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #translator (Parent: Common) — N: 6

FR [1/h]: 2.64e-9

Description: Number of translators in the FEE — NxFR [1/h]: 1.58e-8

PN: Translators — Block Criticality [h/mis]: 1.04e-5

Function: Translate the voltage levels from the ADC to the FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
02	Wrong ADC signal	2.73e+1	7.21e-10	Translator.03 Voltage Improper, Translator.06 Unstable	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	6.23e-6	
03	Low ADC signal	1.82e+1	4.80e-10	Translator.02 Low Output	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	4.15e-6	
04	High ADC signal	9.1e+0	2.40e-10	Translator.04 High Output	Channel failure	CFC failure	False Alarm	10 pA test	8.65e-9	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #FPGATX (Parent: Common) — N: 1

FR [1/h]: 8.70e-9

Description: Number of transmission FPGA in FEE — NxFR [1/h]: 8.70e-9

PN: FPGA TX — Block Criticality [h/mis]: 1.90e-5

Function: Serialize and double the signal, status check, tests

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong CFC signal	2.5e+1	2.17e-09	FPGA TX.01 No ADC reading	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	1.88e-5	
02	No counter reading	2.5e+1	2.17e-09	FPGA TX.02 No counter reading	No data	CFC failure	False Alarm	10 pA test	7.83e-8	
03	No HT reading	2.5e+1	2.17e-09	FPGA TX.03 Blind HT reading	Hidden wrong HT status	HT status failure	Warning	HT test	2.61e-8	
04	No FPGA data	2.5e+1	2.17e-09	FPGA TX.04 General failure	No data	CFC failure	False Alarm	Tunnel status	7.83e-8	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #GOH (Parent: Common) — N: 2

FR [1/h]: 5.15e-6

Description: Number of GOHs in the FEE — NxFR [1/h]: 1.03e-5

PN: GOHs — Block Criticality [h/mis]: 6.18e-5

Function: Serialize and transmit the FPGA signal into the optical fibers

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No optical data	5.0e+1	2.58e-06	GOH.03 No transmission, GOH.04 General failure	Optical line failure	Tunnel Optical link failure	Warning	DOLC	3.09e-5	Redundancy
02	Useless transmission	2.5e+1	1.29e-06	GOH.01 Lost of data	Optical line failure	Tunnel Optical link failure	Warning	DOLC	1.55e-5	Redundancy
03	Wrong optical data	2.5e+1	1.29e-06	GOH.02 Wrong transmission	Optical line failure	Tunnel Optical link failure	Warning	DOLC	1.55e-5	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #fibre (Parent: Common) — N: 2

FR [1/h]: 3.00e-7

Description: Number of fibres, 3 km — NxFR [1/h]: 6.00e-7

PN: SM fibres — Block Criticality [h/mis]: 3.60e-6

Function: Carry the signal from the tunnel to the surface

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Higher BER	7.5e+1	2.25e-07	Fibre.01 Attenuation increase	Optical line failure	Tunnel Optical link failure	Warning	DOLC	2.70e-6	Redundancy
02	No optical data	2.5e+1	7.50e-08	Fibre.02 All failures	Optical line failure	Tunnel Optical link failure	Warning	DOLC	9.00e-7	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #OFcon (Parent: Common) — N: 8

FR [1/h]: 1.00e-7

Description: Number of optical connectors pairs — NxFR [1/h]: 8.00e-7

PN: Optical connectors — Block Criticality [h/mis]: 1.20e-6

Function: Connection of the fibre from the tunnel to the surface

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	higher BER	7.5e+1	7.50e-08	OFcon.01 Attenuation increase	Optical line failure	Tunnel Optical link failure	Warning	DOLC	9.00e-7	Redundancy
02	No optical data	2.5e+1	2.50e-08	OFcon.02 All failures	Optical line failure	Tunnel Optical link failure	Warning	DOLC	3.00e-7	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #10pASource (Parent: Common) — N: 1

FR [1/h]: 1.13e-9

Description: Number of 10pA Sources in the FEE — NxFR [1/h]: 1.13e-9

PN: 10pA Sources — Block Criticality [h/mis]: 9.01e-6

Function: Generate a continuous test current

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong 10pA signal	9.24e+1	1.04e-09	DACFEE.04 Parametric failure, DACFEE ref.01 Electrical Failure, DACFEE ref.02 Oxide defect, DACFEE ref.03 Mechanical failure	Hidden CFC failure	Hidden channel failure	Damage Risk	HT test	9.00e-6	
02	No 10pA signal	7.64e+0	8.62e-11	DACFEE.01 Electrical overstress, DACFEE.02 Corrosion, DACFEE.03 Package failure, DACFEE.05 Low Output, DACFEE.06 Electrical Failure	No 10pA signal	CFC failure	False Alarm	10 pA test	3.10e-9	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes: 2 status for the tunnel PS can give false dumps, status of HT can be unsafe

Block: #status (Parent: Common) — N: 1

FR [1/h]: 1.19e-8

Description: Number of status monitors in the FEE — NxFR [1/h]: 1.19e-8

PN: Statuses — Block Criticality [h/mis]: 4.26e-7

Function: Monitor the analogue power supplies and the HT

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No PS status	6.52e+1	7.75e-09	P5V.01 Not parametric failure, M5V.01 Not parametric failure	Statuses failure	CFC failure	False Alarm	HT test	2.79e-7	
02	No HT status	3.26e+1	3.87e-09	HTstatus.01 Not parametric failure	Statuses failure	CFC failure	False Alarm	Tunnel status	1.39e-7	
03	Wrong PS status	1.47e+0	1.74e-10	P5V.02 Parametric failure, M5V.02 Parametric failure	Statuses failure	CFC failure	False Alarm	Tunnel status	6.27e-9	
04	Hidden wrong HT status	7.33e-1	8.71e-11	HTstatus.02 Parametric failure	Hidden wrong HT status	HT status failure	Warning	HT test	1.05e-9	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #HT activator (Parent: Common) — N: 1

FR [1/h]: 1.82e-10

Description: Number of HT activators in the FEE — NxFR [1/h]: 1.82e-10

PN: HT activators — Block Criticality [h/mis]: 2.27e-9

Function: Activate the HT test

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No test status	9.78e+1	1.78e-10	HT activator.01 Not Parametric Failure	No HT test	HT Test failure	Warning	HT test	2.13e-9	
02	Wrong test status	2.2e+0	3.99e-12	HT activator.02 Parametric Failure	False HT test	CFC failure	False Alarm	Tunnel status	1.44e-10	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #PSarc (Parent: Only arc) — N: 3

FR [1/h]: 1.93e-9

Description: Number of Power Supplies in the arc — NxFR [1/h]: 5.78e-9

PN: PSarc — Block Criticality [h/mis]: 6.94e-8

Function: Feed the arc FEE

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong alimentation	5.72e+1	1.10e-09	PSarc.02 Improper Output, PSarc.03 Improper Voltage, PSarc.04 Intermittent, PSarc.06 Subsystem Failure	Wrong arc alimentation	Tunnel PS failure	False Alarm	Fail safe	3.97e-8	
02	No alimentation	4.28e+1	8.25e-10	PSarc.01 No output, PSarc.05 Shorted	No arc alimentation	Tunnel PS failure	False Alarm	Fail safe	2.97e-8	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #PSSSHV (Parent: Only SS) — N: 2

FR [1/h]: 1.90e-6

Description: Number of High Voltage PS in the Straight Section — NxFR [1/h]: 3.80e-6

PN: PS SS HV — Block Criticality [h/mis]: 6.84e-5

Function: Feed the analogue electronics in the SS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong alimentation	5.72e+1	1.09e-06	PSSSHV.02 Improper Output, PSSSHV.03 Improper Voltage, PSSSHV.04 Intermittent, PSSSHV.06 Subsystem Failure	Wrong SS alimentation	Tunnel PS failure	False Alarm	Fail safe	3.91e-5	
02	No alimentation	4.28e+1	8.13e-07	PSSSHV.01 No output, PSSSHV.05 Shorted	No SS alimentation	Tunnel PS failure	False Alarm	Fail safe	2.93e-5	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #PSSSLV (Parent: Only SS) — N: 1

FR [1/h]: 1.90e-6

Description: Number of Low Voltage PS in the Straight Section — NxFR [1/h]: 1.90e-6

PN: PS SS LV — Block Criticality [h/mis]: 6.84e-5

Function: Feed the digital electronics in the SS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong alimentation	5.72e+1	1.09e-06	PSSSLV.02 Improper Output, PSSSLV.03 Improper Voltage, PSSSLV.04 Intermittent, PSSSLV.06 Subsystem Failure	Wrong SS alimentation	Tunnel PS failure	False Alarm	Fail safe	3.91e-5	
02	No alimentation	4.28e+1	8.13e-07	PSSSLV.01 No output, PSSSLV.05 Shorted	No SS alimentation	Tunnel PS failure	False Alarm	Fail safe	2.93e-5	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #photodiode (Parent: DAB) — N: 4

FR [1/h]: 1.59e-8

Description: Number of photodiodes in the BEE — NxFR [1/h]: 6.37e-8

PN: Photodiodes — Block Criticality [h/mis]: 1.91e-7

Function: Optical-electric data conversion

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Higher BER	5.58e+1	8.89e-09	Photodiode.01 Contamination, Photodiode.04 Seal Failure, Photodiode.05 Leakage, Photodiode.06 Metallization	Wrong optical data	Surface Optical link failure	Warning	DOLC	1.07e-7	Redundancy
02	No optical data	4.42e+1	7.03e-09	Photodiode.02 Die Shear Failure, Photodiode.03 Bond Failure	No optical data	Surface Optical link failure	Warning	DOLC	8.44e-8	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #TLK (Parent: DAB) — N: 4

FR [1/h]: 1.60e-9

Description: Number of TLK in the BEE — NxFR [1/h]: 6.40e-9

PN: TLKs — Block Criticality [h/mis]: 1.92e-8

Function: Deserialization of the data

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No optical data	8.43e+1	1.35e-09	TLK.01 Shorted, TLK.02 Bond Failure, TLK.04 Microcrack, TLK.06 Leakage	No optical data	Surface Optical link failure	Warning	DOLC	1.62e-8	Redundancy
02	Wrong optical data	1.57e+1	2.51e-10	TLK.03 Functional failure, TLK.05 Parametric failure	Wrong optical data	Surface Optical link failure	Warning	DOLC	3.01e-9	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #FPGARX (Parent: DAB) — N: 1

FR [1/h]: 1.83e-8

Description: Number of receiving FPGA in the BEE — NxFR [1/h]: 1.83e-8

PN: FPGA RX — Block Criticality [h/mis]: 1.64e-5

Function: Check the signals, manipulate the data, beam permit inhibition

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	FPGA dump request	9.e+1	1.65e-08	FPGARX.01 General failure, FPGARX.02 Internal error	FPGA dump request	DAB failure	False Alarm	Fail safe	5.93e-7	
02	No energy updating	1.0e+1	1.83e-09	FPGARX.03 Wrong energy from backplane	Wrong energy	Hidden thresholds failure	Damage Risk	Logging	1.58e-5	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #memory (Parent: DAB) — N: 1

FR [1/h]: 1.39e-10

Description: Number of memories in the BEE — NxFR [1/h]: 1.39e-10

PN: Memories — Block Criticality [h/mis]: 1.38e-7

Function: Threshold values storing

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No thresholds	8.89e+1	1.24e-10	Memory.01 Mechanical Failure, Memory.02 Electrical Failure	No thresholds	Thresholds failure	False Alarm	Fail safe	4.45e-9	
02	No right thresholds	1.11e+1	1.54e-11	Memory.03 Functional Failure	No right thresholds	Hidden thresholds failure	Damage Risk	Logging	1.33e-7	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #transceiver (Parent: DAB) — N: 1

FR [1/h]: 1.02e-9

Description: Number of transceivers in the BEE — NxFR [1/h]: 1.02e-9

PN: Tranceivers — Block Criticality [h/mis]: 2.47e-7

Function: Carry the energy signal to the FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No Energy signal	9.76e+1	9.96e-10	Transceiver.01 Electrical Failure, Transceiver.02 Mechanical Failure, Transceiver.03 Opened, Transceiver.04 Electrical Overstressed, Transceiver.05 Shorted	No Energy signal	Thresholds failure	False Alarm	Fail safe	3.58e-8	
02	Wrong energy signal	2.4e+0	2.45e-11	Transceiver.06 Data Bit Error	Wrong energy	Hidden thresholds failure	Damage Risk	Logging	2.12e-7	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #temperature (Parent: DAB) — N: 1

FR [1/h]: 1.14e-8

Description: Number of temperature sensors in the BEE — NxFR [1/h]: 1.14e-8

PN: Temperatures — Block Criticality [h/mis]: 2.45e-7

Function: Monitor VME fan failures

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No temperature signal	6.e+1	6.81e-09	Temperature.01 Cracked Glassivation, Temperature.02 Bonding Faulty	No temperature signal	DAB temperature not checked	Warning	Surface status	8.17e-8	
02	Wrong temperature signal	4.0e+1	4.54e-09	Temperature.03 Contamination, Temperature.04 Failure Not Verified	Wrong temperature signal	DAB failure	False Alarm	Surface status	1.63e-7	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #BPswitch (Parent: Crate) — N: 13 — FR [1/h]: 2.80e-10

Description: Number of backplane switches — NxFR [1/h]: 3.64e-9

PN: BP switches (dual) — Block Criticality [h/mis]: 6.12e-7

Function: Beam permit and FPGA working to the BackPlane

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	False open	7.5e+1	2.10e-10	BPswitch.01 Electrical overstressed, BPswitch.02 No Output, BPswitch.03 Opened	False open backplane line	Crate failure	False Alarm	Fail safe	7.56e-9	
02	False closed	2.5e+1	7.00e-11	BPswitch.04 Shorted High, BPswitch.05 Timing Error	False closed backplane line	Hidden backplane failure	Damage Risk	BIL test	6.05e-7	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #Com_BP_in (Parent: Crate) — N: 2 — FR [1/h]: 1.82e-10

Description: Number of BP comparators in combiner — NxFR [1/h]: 3.63e-10

PN: BP_comb comparator dumps — Block Criticality [h/mis]: 4.09e-8

Function: Carry backplane beam permit lines to Combiner FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	False open	9.78e+1	1.78e-10	Com_BP_in.01 Not parametric failure	Combiner failure	Crate failure	False Alarm	Fail safe	6.39e-9	
02	False closed	2.2e+0	3.99e-12	Com_BP_in.02 Parametric failure	Hidden combiner failure	Hidden combiner failure	Damage Risk	BIL test	3.45e-8	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #Combiner FPGA (Parent: Crate) — N: 1

FR [1/h]: 1.83e-8

Description: Number of combiner FPGA — NxFR [1/h]: 1.83e-8

PN: Comb FPGA — Block Criticality [h/mis]: 4.79e-5

Function: Beam inhibition distribution

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No combiner FPGA	7.0e+1	1.28e-08	Combiner FPGA.01 General failure	Combiner failure	Crate failure	False Alarm	Fail safe	4.61e-7	
02	Wrong combiner FPGA	3.0e+1	5.49e-09	Combiner FPGA.02 Internal error	Hidden combiner failure	Hidden combiner failure	Damage Risk	Logging	4.74e-5	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #LBIS switch (Parent: Crate) — N: 3

FR [1/h]: 1.82e-10

Description: Number of LBIS beam permit switches — NxFR [1/h]: 5.45e-10

PN: LBIS switches — Block Criticality [h/mis]: 6.54e-9

Function: Inhibit the beam permit to the LBIS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No current loop	1.00e+2	1.82e-10	LBIS switch.01 No output, LBIS switch.02 Opened, LBIS switch.03 Aluminum Corrosion, LBIS switch.04 Burned Out	Combiner failure	Crate failure	False Alarm	Fail safe	6.54e-9	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes: Only one of the 3 DAC in the rack will be used

Block: #HT DAC (Parent: Crate) — N: 1

FR [1/h]: 2.27e-8

Description: Number of HT DAC in the combiner — NxFR [1/h]: 2.27e-8

PN: HT DACs — Block Criticality [h/mis]: 2.91e-7

Function: Drive the HT test

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No HT test from combiner	9.65e+1	2.19e-08	HT DAC.01 Electrical overstress, HT DAC.02 Corrosion, HT DAC.03 Package failure, HT DAC.05 Low Output, HT DAC.06 Electrical Failure	No HT test from combiner	No test from combiner	Warning	HT test	2.63e-7	
02	False HT test from combiner	3.5e+0	7.94e-10	HT DAC.04 Parametric failure	Combiner failure	Crate failure	False Alarm	Tunnel status	2.86e-8	

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #PSHT (Parent: HTPS) — N: 1

FR [1/h]: 1.90e-5

Description: Number of HT Power Supplies — NxFR [1/h]: 1.90e-5

PN: HT PSs — Block Criticality [h/mis]: 2.28e-4

Function: Feed the monitors, trigger the HT tests

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong HT	5.72e+1	1.09e-05	PSHT.02 Improper Output, PSHT.03 Improper Voltage, PSHT.04 Intermittent, PSHT.06 Subsystem Failure	HT PS failure	Surface HT failure	Warning	Fail safe	1.30e-4	Redundancy
02	No HT	4.28e+1	8.13e-06	PSHT.01 No output, PSHT.05 Shorted	HT PS failure	Surface HT failure	Warning	Fail safe	9.76e-5	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #PSVME (Parent: VME tray) — N: 1

FR [1/h]: 1.90e-5

Description: Number of VME PS — NxFR [1/h]: 1.90e-5

PN: VME PS — Block Criticality [h/mis]: 2.28e-4

Function: Feed the VME crate cards

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Wrong alimentation	5.72e+1	1.09e-05	PSVME.02 Improper Output, PSVME.03 Improper Voltage, PSVME.04 Intermittent, PSVME.06 Subsystem Failure	VME PS failure	VME PS failure	Warning	Fail safe	1.30e-4	2oo3 connection
02	No alimentation	4.28e+1	8.13e-06	PSVME.01 No output, PSVME.05 Shorted	VME PS failure	VME PS failure	Warning	Fail safe	9.76e-5	2oo3 connection

BLMS FMECA — Mission time: 12 h

Level: 3 — Notes:

Block: #fantray (Parent: VME tray) — N: 1

FR [1/h]: 3.17e-5

Description: Number of VME fan trays — NxFR [1/h]: 3.17e-5

PN: VME fan trays — Block Criticality [h/mis]: 1.14e-3

Function: Cooling the VME cards

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Low ventilation	5.01e+1	1.59e-05	Fantray.01 Bearing Failure, Fantray.03 Sensor failure	VME Ventilation failure	VME fans failure	False Alarm	Tray sensor	5.71e-4	
02	No ventilation	4.99e+1	1.58e-05	Fantray.02 Mechanical Failure, Fantray.04 Blade erosion, Fantray.05 Out of Balance, Fantray.06 Switch failure	VME Ventilation failure	VME fans failure	False Alarm	DAB Temperature	5.69e-4	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes: The FM are shorted by components: Cable, Capacitor, Resistor and IC

Block: IC+cable (Parent: #IC) — N: 1

FR [1/h]: 4.41e-8

Description: Historical data — NxFR [1/h]: 4.41e-8

PN: IC+cable — Block Criticality [h/mis]: 3.13e-4

Function: Provide a current proportional to the lost particles

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Signal Cable Shorts (Poor Sealing)	1.0e+1	4.41e-09		No IC signal	Hidden IC failure	Damage Risk	HT test	3.81e-5	
02	Mechanical Failure of Cable Solder Joints	8.e+0	3.53e-09		No IC signal	Hidden IC failure	Damage Risk	HT test	3.05e-5	
03	Cable Miscellaneous Mechanical Failures	8.e+0	3.53e-09		Wrong signal	Hidden IC failure	Damage Risk	HT test	3.05e-5	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes: The FM are shorted by components: Cable, Capacitor, Resistor and IC

Block: IC+cable (Parent: #IC) — N: 1

FR [1/h]: 4.41e-8

Description: Historical data — NxFR [1/h]: 4.41e-8

PN: IC+cable — Block Criticality [h/mis]: 3.13e-4

Function: Provide a current proportional to the lost particles

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
04	Degradation of Cable Insulation Resistance	6.e+0	2.65e-09		Wrong signal	Hidden IC failure	Damage Risk	HT test	2.29e-5	
05	CIC Shorted (Electrical)	1.6e+1	7.06e-09		No HT	Channel failure	False Alarm	Surface HT status	2.54e-7	
06	CIC Change of Value	1.4e+1	6.18e-09		Noise variation	Hidden IC failure	Damage Risk	HT test	5.34e-5	
07	CIC Open (Electrical)	2.e+0	8.83e-10		Noise increase	Hidden IC failure	Damage Risk	HT test	7.63e-6	
08	RIC Shorted (Electrical)	1.6e+1	7.06e-09		Noise increase	Hidden IC failure	Damage Risk	HT test	6.10e-5	
09	RIC Change of Value	1.4e+1	6.18e-09		Noise variation	Hidden IC failure	Damage Risk	HT test	5.34e-5	
11	IC gas pressure change	4.e+0	1.77e-09		Wrong signal	Hidden IC failure	Damage Risk	Yearly test	1.53e-5	
10	RIC Open (Electrical)	2.e+0	8.83e-10		No HT	Channel failure	False Alarm	Surface HT status	3.18e-8	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: HTcon (Parent: #HTcon) — N: 1

FR [1/h]: 5.20e-10

Description: Historical data — NxFR [1/h]: 5.20e-10

PN: HT connector — Block Criticality [h/mis]: 1.87e-8

Function: Provides High Tension from the surface to 6 monitors

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Improper output	2.71e+1	1.41e-10		Wrong HT	Channel failure	False Alarm	Tunnel HT status	5.07e-9	
02	Shorts	2.27e+1	1.18e-10		No HT	Channel failure	False Alarm	Tunnel HT status	4.25e-9	
03	Broken	1.75e+1	9.10e-11		No HT	Channel failure	False Alarm	Surface HT status	3.28e-9	
04	Opened	1.5e+1	7.80e-11		No HT	Channel failure	False Alarm	Tunnel HT status	2.81e-9	
05	Intermittent	9.e+0	4.68e-11		Wrong HT	Channel failure	False Alarm	Tunnel HT status	1.68e-9	
06	Loose	8.7e+0	4.52e-11		Wrong HT	Channel failure	False Alarm	Tunnel HT status	1.63e-9	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Integrator (Parent: #integrator) — N: 1

FR [1/h]: 7.50e-8

Description: IC, plastic, Op. Amplifier — NxFR [1/h]: 7.50e-8

PN: OPA627 — Block Criticality [h/mis]: 6.15e-4

Function: Integrate the current from the monitors

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Parametric Failure	9.49e+1	7.12e-08		Hidden wrong CFC signal	Hidden CFC failure	Damage Risk	HT test	6.15e-4	
02	Shorted	3.4e+0	2.55e-09		No CFC signal	Channel failure	False Alarm	10 pA test	9.19e-8	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Integrator (Parent: #integrator) — N: 1

FR [1/h]: 7.50e-8

Description: IC, plastic, Op. Amplifier — NxFR [1/h]: 7.50e-8

PN: OPA627 — Block Criticality [h/mis]: 6.15e-4

Function: Integrate the current from the monitors

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
03	Functional Failure	1.7e+0	1.28e-09		No CFC signal	Channel failure	False Alarm	10 pA test	4.59e-8	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Comparator (Parent: #comp) — N: 1

FR [1/h]: 1.91e-7

Description: IC, Unknown, Comparator — NxFR [1/h]: 1.91e-7

PN: NE521D — Block Criticality [h/mis]: 4.31e-5

Function: Trigger the monostable with the integrated value

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Not parametric failure	9.78e+1	1.87e-07		No CFC signal	Channel failure	False Alarm	10 pA test	6.73e-6	
02	Parametric failure	2.2e+0	4.21e-09		Hidden wrong CFC signal	Hidden CFC failure	Damage Risk	HT test	3.64e-5	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Monostable (Parent: #monostable) — N: 1

FR [1/h]: 1.15e-7

Description: IC,Unknown,Multivibrator, Monostable,Unknown — NxFR [1/h]: 1.15e-7

PN: 74LS123 — Block Criticality [h/mis]: 1.28e-4

Function: Generate a pulses train

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Electrical overstressed	5.0e+1	5.77e-08		No CFC signal	Channel failure	False Alarm	10 pA test	2.08e-6	
CONTINUE										

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Monostable (Parent: #monostable) — N: 1

FR [1/h]: 1.15e-7

Description: IC,Unknown,Multivibrator, Monostable,Unknown — NxFR [1/h]: 1.15e-7

PN: 74LS123 — Block Criticality [h/mis]: 1.28e-4

Function: Generate a pulses train

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
02	No Output	1.25e+1	1.44e-08		No CFC signal	Channel failure	False Alarm	10 pA test	5.20e-7	
03	Opened	1.25e+1	1.44e-08		No CFC signal	Channel failure	False Alarm	10 pA test	5.20e-7	
04	Shorted High	1.25e+1	1.44e-08		No CFC signal	Channel failure	False Alarm	10 pA test	5.20e-7	
05	Timing Error	1.25e+1	1.44e-08		Hidden wrong CFC signal	Hidden CFC failure	Damage Risk	HT test	1.25e-4	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: JFET (Parent: #jfet) — N: 1

FR [1/h]: 4.56e-10

Description: Transistor, Bipolar — NxFR [1/h]: 4.56e-10

PN: MBVFJ176 — Block Criticality [h/mis]: 1.50e-7

Function: Discharge the integrator

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Shorted	6.26e+1	2.85e-10		No CFC signal	Channel failure	False Alarm	10 pA test	1.03e-8	
02	Opened	1.27e+1	5.79e-11		No CFC signal	Channel failure	False Alarm	10 pA test	2.08e-9	
03	Base-Emitter Shorted	1.12e+1	5.10e-11		No CFC signal	Channel failure	False Alarm	10 pA test	1.84e-9	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: JFET (Parent: #jfet) — N: 1

FR [1/h]: 4.56e-10

Description: Transistor, Bipolar — NxFR [1/h]: 4.56e-10

PN: MBVFJ176 — Block Criticality [h/mis]: 1.50e-7

Function: Discharge the integrator

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
04	Electrical Overstressed	5.2e+0	2.37e-11		No CFC signal	Channel failure	False Alarm	10 pA test	8.53e-10	
05	Bond Failure	4.9e+0	2.23e-11		No CFC signal	Channel failure	False Alarm	10 pA test	8.04e-10	
06	Contaminati on	3.4e+0	1.55e-11		Wrong CFC signal	Hidden CFC failure	Damage Risk	HT test	1.34e-7	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: ADC (Parent: #ADC) — N: 1

FR [1/h]: 1.00e-9

Description: IC, Unknown, Converter, A/D — NxFR [1/h]: 1.00e-9

PN: AD7492 — Block Criticality [h/mis]: 3.43e-6

Function: Increase the dynamic range of the integration

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Parametric failure	2.91e+1	2.91e-10		Hidden Wrong ADC signal	Hidden CFC failure	Damage Risk	HT test	2.51e-6	
02	Electrical failure	2.16e+1	2.16e-10		No ADC signal	Channel failure	False Alarm	10 pA test	7.78e-9	
03	Fabrication defect	1.84e+1	1.84e-10		No ADC signal	Channel failure	False Alarm	10 pA test	6.62e-9	
04	Stacking faults	1.41e+1	1.41e-10		No ADC signal	Channel failure	False Alarm	10 pA test	5.08e-9	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: ADC (Parent: #ADC) — N: 1

FR [1/h]: 1.00e-9

Description: IC, Unknown, Converter, A/D — NxFR [1/h]: 1.00e-9

PN: AD7492 — Block Criticality [h/mis]: 3.43e-6

Function: Increase the dynamic range of the integration

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
05	Leakage	1.03e+1	1.03e-10		Hidden Wrong ADC signal	Hidden CFC failure	Damage Risk	HT test	8.90e-7	
06	Electrical overstresses	6.5e+0	6.50e-11		No ADC signal	Channel failure	False Alarm	10 pA test	2.34e-9	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Translator (Parent: #translator) — N: 1

FR [1/h]: 2.64e-9

Description: LVDS to CMOS — NxFR [1/h]: 2.64e-9

PN: LVDS_RX CMS — Block Criticality [h/mis]: 1.04e-5

Function: Translate the voltage levels from the ADC to the FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Short Low	3.63e+1	9.58e-10		No ADC signal	Channel failure	False Alarm	10 pA test	3.45e-8	
02	Low Output	1.82e+1	4.80e-10		Low ADC signal	Hidden CFC failure	Damage Risk	HT test	4.15e-6	
03	Voltage Improper	1.82e+1	4.80e-10		Wrong ADC signal	Hidden CFC failure	Damage Risk	HT test	4.15e-6	
04	High Output	9.1e+0	2.40e-10		High ADC signal	Channel failure	False Alarm	10 pA test	8.65e-9	
05	No Output	9.1e+0	2.40e-10		No ADC signal	Channel failure	False Alarm	10 pA test	8.65e-9	
06	Unstable	9.1e+0	2.40e-10		Wrong ADC signal	Hidden CFC failure	Damage Risk	HT test	2.08e-6	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: FPGA TX (Parent: #FPGATX) — N: 1

FR [1/h]: 8.70e-9

Description: Not available — NxFR [1/h]: 8.70e-9

PN: ACTEL 0.25 SX-A — Block Criticality [h/mis]: 1.90e-5

Function: Serialize and double the signal, status check, tests

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No ADC reading	2.5e+1	2.17e-09		Wrong CFC signal	Hidden CFC failure	Damage Risk	HT test	1.88e-5	
02	No counter reading	2.5e+1	2.17e-09		No counter reading	No data	False Alarm	10 pA test	7.83e-8	
03	Blind HT reading	2.5e+1	2.17e-09		No HT reading	Hidden wrong HT status	Warning	HT test	2.61e-8	
04	General failure	2.5e+1	2.17e-09		No FPGA data	No data	False Alarm	Tunnel status	7.83e-8	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: GOH (Parent: #GOH) — N: 1

FR [1/h]: 5.15e-6

Description: Not available — NxFR [1/h]: 5.15e-6

PN: GOH — Block Criticality [h/mis]: 6.18e-5

Function: Serialize and transmit the FPGA signal into the optical fibers

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Lost of data	2.5e+1	1.29e-06		Useless transmission	Optical line failure	Warning	DOLC	1.55e-5	redundancy
02	Wrong transmission	2.5e+1	1.29e-06		Wrong optical data	Optical line failure	Warning	DOLC	1.55e-5	redundancy
03	No transmission	2.5e+1	1.29e-06		No optical data	Optical line failure	Warning	DOLC	1.55e-5	redundancy
04	General failure	2.5e+1	1.29e-06		No optical data	Optical line failure	Warning	DOLC	1.55e-5	redundancy

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Fibre (Parent: #fibre) — N: 3000

FR [1/h]: 1.00e-10

Description: Not Available — NxFR [1/h]: 3.00e-7

PN: Corning — Block Criticality [h/mis]: 1.20e-9

Function: Carry the signal from the tunnel to the surface

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Attenuation increase	7.5e+1	7.50e-11		Higher BER	Optical line failure	Warning	DOLC	9.00e-10	Redundancy
02	All failures	2.5e+1	2.50e-11		No optical data	Optical line failure	Warning	DOLC	3.00e-10	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: OFcon (Parent: #OFcon) — N: 1

FR [1/h]: 1.00e-7

Description: Not Available — NxFR [1/h]: 1.00e-7

PN: E2000 — Block Criticality [h/mis]: 1.20e-6

Function: Connection of the fibre from the tunnel to the surface

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Attenuation increase	7.5e+1	7.50e-08		higher BER	Optical line failure	Warning	DOLC	9.00e-7	Redundancy
02	All failures	2.5e+1	2.50e-08		No optical data	Optical line failure	Warning	DOLC	3.00e-7	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: DACFEE (Parent: #10pASource) — N: 1

FR [1/h]: 8.93e-11

Description: IC, Unknown, Converter, D/A — NxFR [1/h]: 8.93e-11

PN: AD5346 — Block Criticality [h/mis]: 3.01e-8

Function: Generate a continuos test current in the 8 channels of the CFC

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Electrical overstress	5.17e+1	4.62e-11		No 10pA signal	No 10pA signal	False Alarm	10 pA test	1.66e-9	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: DACFEE (Parent: #10pASource) — N: 1

FR [1/h]: 8.93e-11

Description: IC, Unknown, Converter, D/A — NxFR [1/h]: 8.93e-11

PN: AD5346 — Block Criticality [h/mis]: 3.01e-8

Function: Generate a continuos test current in the 8 channels of the CFC

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUE										
02	Corrosion	3.61e+1	3.22e-11		No 10pA signal	No 10pA signal	False Alarm	10 pA test	1.16e-9	
03	Package failure	3.5e+0	3.13e-12		No 10pA signal	No 10pA signal	False Alarm	10 pA test	1.13e-10	
04	Parametric failure	3.5e+0	3.13e-12		Wrong 10pA signal	Hidden CFC failure	Damage Risk	HT test	2.70e-8	
05	Low Output	2.9e+0	2.59e-12		No 10pA signal	No 10pA signal	False Alarm	10 pA test	9.32e-11	
06	Electrical Failure	2.3e+0	2.05e-12		No 10pA signal	No 10pA signal	False Alarm	10 pA test	7.39e-11	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: DACFEE ref (Parent: #10pASource) — N: 1

FR [1/h]: 1.04e-9

Description: IC, Unknown, Voltage Reference, Precision, Unknown — NxFR [1/h]: 1.04e-9

PN: LM4140 — Block Criticality [h/mis]: 8.98e-6

Function: Gives the reference to the DAC for the 10 pA test

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Electrical Failure	4.76e+1	4.95e-10		Wrong 10pA signal	Hidden CFC failure	Damage Risk	HT test	4.27e-6	
02	Oxide defect	4.76e+1	4.95e-10		Wrong 10pA signal	Hidden CFC failure	Damage Risk	HT test	4.27e-6	
03	Mechanical failure	4.8e+0	4.99e-11		Wrong 10pA signal	Hidden CFC failure	Damage Risk	HT test	4.31e-7	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: HTstatus (Parent: #status) — N: 1

FR [1/h]: 3.96e-9

Description: IC, Unknown, Comparator — NxFR [1/h]: 3.96e-9

PN: LMV393 — Block Criticality [h/mis]: 1.40e-7

Function: Monitor if the HT is not low

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Not parametric failure	9.78e+1	3.87e-09		No HT status	Statuses failure	False Alarm	Tunnel HT status	1.39e-7	
02	Parametric failure	2.2e+0	8.71e-11		Hidden wrong HT status	Hidden wrong HT status	Warning	HT test	1.05e-9	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: P5V (Parent: #status) — N: 1

FR [1/h]: 3.96e-9

Description: IC, Unknown, Comparator — NxFR [1/h]: 3.96e-9

PN: LMV393 — Block Criticality [h/mis]: 1.43e-7

Function: Monitor the +5V PS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Not parametric failure	9.78e+1	3.87e-09		No PS status	Statuses failure	False Alarm	Tunnel status	1.39e-7	
02	Parametric failure	2.2e+0	8.71e-11		Wrong PS status	Statuses failure	False Alarm	Tunnel status	3.14e-9	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: M5V (Parent: #status) — N: 1

FR [1/h]: 3.96e-9

Description: IC, Unknown, Comparator — NxFR [1/h]: 3.96e-9

PN: LMV393 — Block Criticality [h/mis]: 1.43e-7

Function: Monitor the -5V PS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Not parametric failure	9.78e+1	3.87e-09		No PS status	Statuses failure	False Alarm	Tunnel status	1.39e-7	
02	Parametric failure	2.2e+0	8.71e-11		Wrong PS status	Statuses failure	False Alarm	Tunnel status	3.14e-9	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: HT activator (Parent: #HT activator) — N: 1

FR [1/h]: 1.82e-10

Description: IC, Unknown, Comparator — NxFR [1/h]: 1.82e-10

PN: TL072CD — Block Criticality [h/mis]: 2.27e-9

Function: Trigger the HT test into the tunnel FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Not Parametric Failure	9.78e+1	1.78e-10		No test status	No HT test	Warning	HT test	2.13e-9	
02	Parametric Failure	2.2e+0	3.99e-12		Wrong test status	False HT test	False Alarm	Tunnel status	1.44e-10	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSarc (Parent: #PSarc) — N: 1

FR [1/h]: 1.93e-9

Description: Power supply in the arc — NxFR [1/h]: 1.93e-9

PN: LHC4913&791 — Block Criticality [h/mis]: 6.94e-8

Function: Feed the arc FEE

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No output	3.44e+1	6.63e-10		No alimentation	No arc alimentation	False Alarm	Fail safe	2.39e-8	
02	Improper Output	2.43e+1	4.68e-10		Wrong alimentation	Wrong arc alimentation	False Alarm	Fail safe	1.69e-8	
03	Improper Voltage	1.4e+1	2.70e-10		Wrong alimentation	Wrong arc alimentation	False Alarm	Fail safe	9.71e-9	
04	Intermittent	1.25e+1	2.41e-10		Wrong alimentation	Wrong arc alimentation	False Alarm	Fail safe	8.67e-9	
05	Shorted	8.4e+0	1.62e-10		No alimentation	No arc alimentation	False Alarm	Fail safe	5.83e-9	
06	Subsystem Failure	6.4e+0	1.23e-10		Wrong alimentation	Wrong arc alimentation	False Alarm	Fail safe	4.44e-9	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSSSHV (Parent: #PSSSHV) — N: 1

FR [1/h]: 1.90e-6

Description: High Voltage PS in the Straight Section — NxFR [1/h]: 1.90e-6

PN: 75SX5 DELTA — Block Criticality [h/mis]: 6.84e-5

Function: Feed the analogue electronic in the SS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No output	3.44e+1	6.54e-07		No alimentation	No SS alimentation	False Alarm	Fail safe	2.35e-5	
02	Improper Output	2.43e+1	4.62e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	1.66e-5	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSSSHV (Parent: #PSSSHV) — N: 1

FR [1/h]: 1.90e-6

Description: High Voltage PS in the Straight Section — NxFR [1/h]: 1.90e-6

PN: 75SX5 DELTA — Block Criticality [h/mis]: 6.84e-5

Function: Feed the analogue electronic in the SS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
03	Improper Voltage	1.4e+1	2.66e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	9.58e-6	
04	Intermittent	1.25e+1	2.38e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	8.55e-6	
05	Shorted	8.4e+0	1.60e-07		No alimentation	No SS alimentation	False Alarm	Fail safe	5.75e-6	
06	Subsystem Failure	6.4e+0	1.22e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	4.38e-6	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSSSLV (Parent: #PSSSLV) — N: 1

FR [1/h]: 1.90e-6

Description: Low Voltage PS in the Straight Section — NxFR [1/h]: 1.90e-6

PN: USR515 Haltec — Block Criticality [h/mis]: 6.84e-5

Function: Feed the digital electronics in the SS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No output	3.44e+1	6.54e-07		No alimentation	No SS alimentation	False Alarm	Fail safe	2.35e-5	
02	Improper Output	2.43e+1	4.62e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	1.66e-5	
03	Improper Voltage	1.4e+1	2.66e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	9.58e-6	
04	Intermittent	1.25e+1	2.38e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	8.55e-6	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSSSLV (Parent: #PSSSLV) — N: 1

FR [1/h]: 1.90e-6

Description: Low Voltage PS in the Straight Section — NxFR [1/h]: 1.90e-6

PN: USR515 Haltec — Block Criticality [h/mis]: 6.84e-5

Function: Feed the digital electronics in the SS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
05	Shorted	8.4e+0	1.60e-07		No alimentation	No SS alimentation	False Alarm	Fail safe	5.75e-6	
06	Subsystem Failure	6.4e+0	1.22e-07		Wrong alimentation	Wrong SS alimentation	False Alarm	Fail safe	4.38e-6	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Photodiode (Parent: #photodiode) — N: 1

FR [1/h]: 1.59e-8

Description: Optoelectronics Device, Sensor, Photodiode — NxFR [1/h]: 1.59e-8

PN: TXP0036 Afonics — Block Criticality [h/mis]: 1.91e-7

Function: Optical-electric data conversion

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Contami-nation	4.19e+1	6.67e-09		Higher BER	Wrong optical data	Warning	DOLC	8.00e-8	Redundancy
02	Die Shear Failure	2.33e+1	3.71e-09		No optical data	No optical data	Warning	DOLC	4.45e-8	Redundancy
03	Bond Failure	2.09e+1	3.33e-09		No optical data	No optical data	Warning	DOLC	3.99e-8	Redundancy
04	Seal Failure	7.e+0	1.11e-09		Higher BER	Wrong optical data	Warning	DOLC	1.34e-8	Redundancy
05	Leakage	4.7e+0	7.48e-10		Higher BER	Wrong optical data	Warning	DOLC	8.97e-9	Redundancy
06	Metalli-zation	2.3e+0	3.66e-10		Higher BER	Wrong optical data	Warning	DOLC	4.39e-9	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: TLK (Parent: #TLK) — N: 1

FR [1/h]: 1.60e-9

Description: IC, Unknown, Receiver/Transmitter — NxFR [1/h]: 1.60e-9

PN: TLK1501RCP — Block Criticality [h/mis]: 1.92e-8

Function: Deserialization of the data

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Shorted	5.86e+1	9.38e-10		No optical data	No optical data	Warning	DOLC	1.13e-8	Redundancy
02	Bond Failure	1.71e+1	2.74e-10		No optical data	No optical data	Warning	DOLC	3.28e-9	Redundancy
03	Functional failure	1.0e+1	1.60e-10		Wrong optical data	Wrong optical data	Warning	DOLC	1.92e-9	Redundancy
04	Microcrack	5.7e+0	9.12e-11		No optical data	No optical data	Warning	DOLC	1.09e-9	Redundancy
05	Parametric failure	5.7e+0	9.12e-11		Wrong optical data	Wrong optical data	Warning	DOLC	1.09e-9	Redundancy
06	Leakage	2.9e+0	4.64e-11		No optical data	No optical data	Warning	DOLC	5.57e-10	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: FPGARX (Parent: #FPGARX) — N: 1

FR [1/h]: 1.83e-8

Description: Not available — NxFR [1/h]: 1.83e-8

PN: EP1530F780C7 — Block Criticality [h/mis]: 1.64e-5

Function: Check the signals, manipulate the data, beam permit inhibition

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	General failure	7.0e+1	1.28e-08		FPGA dump request	FPGA dump request	False Alarm	Fail safe	4.61e-7	
02	Internal error	2.0e+1	3.66e-09		FPGA dump request	FPGA dump request	False Alarm	Fail safe	1.32e-7	
03	Wrong energy from backplane	1.0e+1	1.83e-09		No energy updating	Wrong energy	Damage Risk	Logging	1.58e-5	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Memory (Parent: #memory) — N: 1

FR [1/h]: 1.39e-10

Description: IC, Unknown, Memory, CMOS, Flash, CMOS — NxFR [1/h]: 1.39e-10

PN: ST M25P10 FLASH — Block Criticality [h/mis]: 1.38e-7

Function: Threshold values storing

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Mechanical Failure	6.67e+1	9.27e-11		No thresholds	No thresholds	False Alarm	Fail safe	3.34e-9	
02	Electrical Failure	2.22e+1	3.09e-11		No thresholds	No thresholds	False Alarm	Fail safe	1.11e-9	
03	Functional Failure	1.11e+1	1.54e-11		No right thresholds	No right thresholds	Damage Risk	Logging	1.33e-7	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Transceiver (Parent: #transceiver) — N: 1

FR [1/h]: 1.02e-9

Description: IC, Unknown, Bidirectional, Octal, Unknown — NxFR [1/h]: 1.02e-9

PN: SN74LVT245B — Block Criticality [h/mis]: 2.47e-7

Function: Carry the energy signal to the FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Electrical Failure	4.9e+1	5.00e-10		No Energy signal	No Energy signal	False Alarm	Fail safe	1.80e-8	
02	Mechanical Failure	3.16e+1	3.22e-10		No Energy signal	No Energy signal	False Alarm	Fail safe	1.16e-8	
03	Opened	8.3e+0	8.47e-11		No Energy signal	No Energy signal	False Alarm	Fail safe	3.05e-9	
04	Electrical Overstressed	5.8e+0	5.92e-11		No Energy signal	No Energy signal	False Alarm	Fail safe	2.13e-9	
05	Shorted	2.9e+0	2.96e-11		No Energy signal	No Energy signal	False Alarm	Fail safe	1.06e-9	
06	Data Bit Error	2.4e+0	2.45e-11		Wrong energy signal	Wrong energy	Damage Risk	Logging	2.12e-7	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Temperature (Parent: #temperature) — N: 1

FR [1/h]: 1.14e-8

Description: IC, Unknown, Transducer, Temperature, Unknown — NxFR [1/h]: 1.14e-8

PN: MAX6627MKA-T — Block Criticality [h/mis]: 2.45e-7

Function: Monitor VME fan failures

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Cracked Glassivation	4.0e+1	4.54e-09		No temperature signal	No temperature signal	Warning	Continuous	5.45e-8	
02	Bonding Faulty	2.0e+1	2.27e-09		No temperature signal	No temperature signal	Warning	Continuous	2.72e-8	
03	Contaminati on	2.0e+1	2.27e-09		Wrong temperature signal	Wrong temperature signal	False Alarm	Continuous	8.17e-8	
04	Failure Not Verified	2.0e+1	2.27e-09		Wrong temperature signal	Wrong temperature signal	False Alarm	Continuous	8.17e-8	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: BPswitch (Parent: #BPswitch) — N: 1

FR [1/h]: 2.80e-10

Description: IC, Unknown, Multivibrator, Monostable, Unknown — NxFR [1/h]: 2.80e-10

PN: SN74LV123A — Block Criticality [h/mis]: 6.12e-7

Function: Beam permit and FPGA working to the BackPlane

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Electrical overstressed	5.0e+1	1.40e-10		False open	False open backplane line	False Alarm	Fail safe	5.04e-9	
02	No Output	1.25e+1	3.50e-11		False open	False open backplane line	False Alarm	Fail safe	1.26e-9	

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: BPswitch (Parent: #BPswitch) — N: 1

FR [1/h]: 2.80e-10

Description: IC, Unknown, Multivibrator, Monostable, Unknown — NxFR [1/h]: 2.80e-10

PN: SN74LV123A — Block Criticality [h/mis]: 6.12e-7

Function: Beam permit and FPGA working to the BackPlane

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
03	Opened	1.25e+1	3.50e-11		False open	False open backplane line	False Alarm	Fail safe	1.26e-9	
04	Shorted High	1.25e+1	3.50e-11		False closed	False closed backplane line	Damage Risk	BIL test	3.02e-7	
05	Timing Error	1.25e+1	3.50e-11		False closed	False closed backplane line	Damage Risk	BIL test	3.02e-7	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Com_BP_in (Parent: #Com_BP_in) — N: 1

FR [1/h]: 1.82e-10

Description: IC, Unknown, Comparator — NxFR [1/h]: 1.82e-10

PN: LM339 — Block Criticality [h/mis]: 4.09e-8

Function: Carry backplane beam permit lines to Combiner FPGA

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Not parametric failure	9.78e+1	1.78e-10		False open	Combiner failure	False Alarm	Fail safe	6.39e-9	
02	Parametric failure	2.2e+0	3.99e-12		False closed	Hidden combiner failure	Damage Risk	BIL test	3.45e-8	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Combiner FPGA (Parent: #Combiner FPGA) — N: 1

FR [1/h]: 1.83e-8

Description: Not available — NxFR [1/h]: 1.83e-8

PN: EP1530F780C7 — Block Criticality [h/mis]: 4.79e-5

Function: Beam inhibition distribution

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	General failure	7.0e+1	1.28e-08		No combiner FPGA	Combiner failure	False Alarm	Fail safe	4.61e-7	
02	Internal error	3.0e+1	5.49e-09		Wrong combiner FPGA	Hidden combiner failure	Damage Risk	Logging	4.74e-5	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: LBIS switch (Parent: #LBIS switch) — N: 1

FR [1/h]: 1.82e-10

Description: IC, Unknown,Peripheral Driver,Unknown — NxFR [1/h]: 1.82e-10

PN: SN75472P — Block Criticality [h/mis]: 6.54e-9

Function: Inhibit the beam permit to the LBIS

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No output	4.0e+1	7.26e-11		No current loop	Combiner failure	False Alarm	Fail safe	2.61e-9	
02	Opened	4.0e+1	7.26e-11		No current loop	Combiner failure	False Alarm	Fail safe	2.61e-9	
03	Aluminum Corrosion	1.0e+1	1.82e-11		No current loop	Combiner failure	False Alarm	Fail safe	6.54e-10	
04	Burned Out	1.0e+1	1.82e-11		No current loop	Combiner failure	False Alarm	Fail safe	6.54e-10	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: HT DAC (Parent: #HT DAC) — N: 1

FR [1/h]: 2.27e-8

Description: IC, Unknown, Converter, D/A — NxFR [1/h]: 2.27e-8

PN: MAX038 — Block Criticality [h/mis]: 2.91e-7

Function: Drive the HT test

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Electrical overstress	5.17e+1	1.17e-08		No HT test from combiner	No HT test from combiner	Warning	HT test	1.41e-7	
02	Corrosion	3.61e+1	8.19e-09		No HT test from combiner	No HT test from combiner	Warning	HT test	9.83e-8	
03	Package failure	3.5e+0	7.94e-10		No HT test from combiner	No HT test from combiner	Warning	HT test	9.53e-9	
04	Parametric failure	3.5e+0	7.94e-10		False HT test from combiner	Combiner failure	False Alarm	Tunnel status	2.86e-8	
05	Low Output	2.9e+0	6.58e-10		No HT test from combiner	No HT test from combiner	Warning	HT test	7.89e-9	
06	Electrical Failure	2.3e+0	5.22e-10		No HT test from combiner	No HT test from combiner	Warning	HT test	6.26e-9	

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSHT (Parent: #PSHT) — N: 1

FR [1/h]: 1.90e-5

Description: Power supply — NxFR [1/h]: 1.90e-5

PN: NCE 3000-20 — Block Criticality [h/mis]: 2.28e-4

Function: Feed the monitors, trigger the HT tests

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No output	3.44e+1	6.54e-06		No HT	HT PS failure	Warning	Fail safe	7.84e-5	Redundancy
02	Improper Output	2.43e+1	4.62e-06		Wrong HT	HT PS failure	Warning	Fail safe	5.54e-5	Redundancy
03	Improper Voltage	1.4e+1	2.66e-06		Wrong HT	HT PS failure	Warning	Fail safe	3.19e-5	Redundancy
04	Intermittent	1.25e+1	2.37e-06		Wrong HT	HT PS failure	Warning	Fail safe	2.85e-5	Redundancy
05	Shorted	8.4e+0	1.60e-06		No HT	HT PS failure	Warning	Fail safe	1.92e-5	Redundancy
06	Subsystem Failure	6.4e+0	1.22e-06		Wrong HT	HT PS failure	Warning	Fail safe	1.46e-5	Redundancy

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSVME (Parent: #PSVME) — N: 1

FR [1/h]: 1.90e-5

Description: Power supply in the VME crate — NxFR [1/h]: 1.90e-5

PN: 6000 LHC — Block Criticality [h/mis]: 2.28e-4

Function: Feed the VME crate cards

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	No output	3.44e+1	6.54e-06		No alimentation	VME PS failure	Warning	Fail safe	7.84e-5	2oo3 redundancy
02	Improper Output	2.43e+1	4.62e-06		Wrong alimentation	VME PS failure	Warning	Fail safe	5.54e-5	2oo3 redundancy

CONTINUE

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: PSVME (Parent: #PSVME) — N: 1

FR [1/h]: 1.90e-5

Description: Power supply in the VME crate — NxFR [1/h]: 1.90e-5

PN: 6000 LHC — Block Criticality [h/mis]: 2.28e-4

Function: Feed the VME crate cards

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
03	Improper Voltage	1.4e+1	2.66e-06		Wrong alimentation	VME PS failure	Warning	Fail safe	3.19e-5	2oo3 redundancy
04	Intermittent	1.25e+1	2.37e-06		Wrong alimentation	VME PS failure	Warning	Fail safe	2.85e-5	2oo3 redundancy
05	Shorted	8.4e+0	1.60e-06		No alimentation	VME PS failure	Warning	Fail safe	1.92e-5	2oo3 redundancy
06	Subsystem Failure	6.4e+0	1.22e-06		Wrong alimentation	VME PS failure	Warning	Fail safe	1.46e-5	2oo3 redundancy

BLMS FMECA — Mission time: 12 h

Level: 4 — Notes:

Block: Fantray (Parent: #fantray) — N: 1

FR [1/h]: 3.17e-5

Description: Blower, Fan Assembly — NxFR [1/h]: 3.17e-5

PN: fan 6000LHC — Block Criticality [h/mis]: 1.14e-3

Function: Cooling the VME cards

ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
01	Bearing Failure	3.34e+1	1.06e-05		Low ventilation	VME Ventilation failure	False Alarm	Tray sensor	3.81e-4	
02	Mechanical Failure	2.62e+1	8.30e-06		No ventilation	VME Ventilation failure	False Alarm	DAB Temperature	2.99e-4	
03	Sensor failure	1.67e+1	5.29e-06		Low ventilation	VME Ventilation failure	False Alarm	Tray sensor	1.90e-4	
CONTINUE										

BLMS FMECA

Mission time: 12 h

Level: 4

Notes:

Block: Fantray (Parent: #fantray)

N: 1

FR [1/h]: 3.17e-5

Description: Blower, Fan Assembly

NxFR [1/h]: 3.17e-5

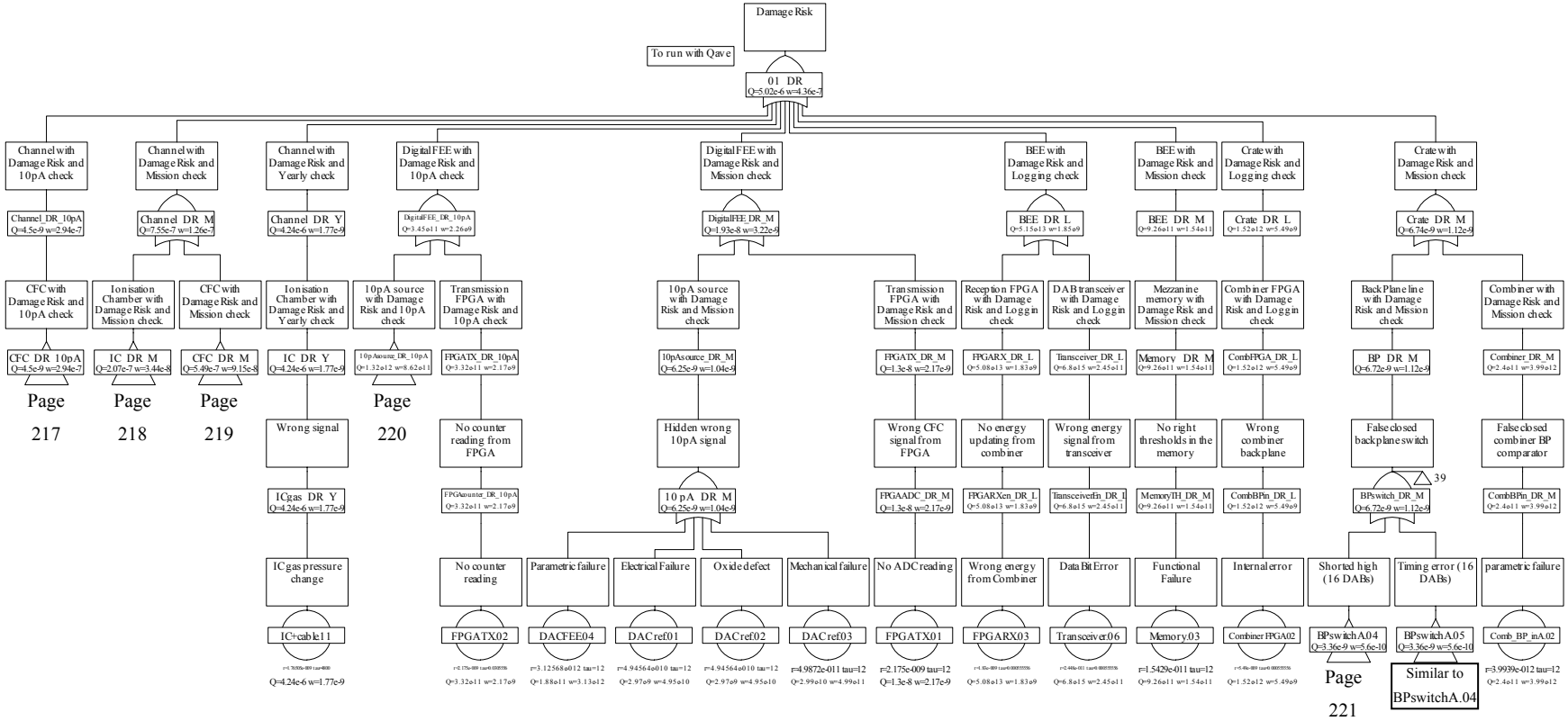
PN: fan 6000LHC

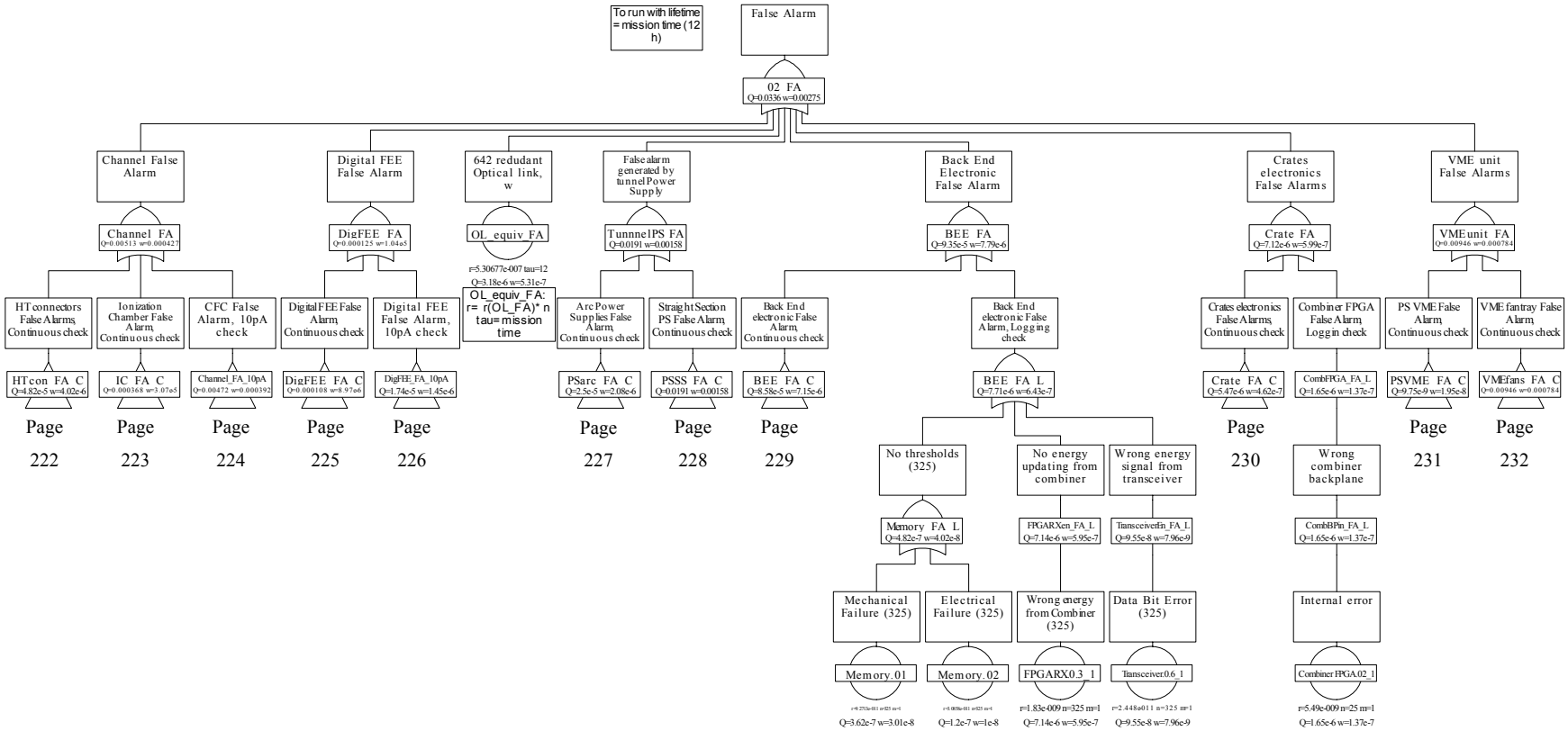
Block Criticality [h/mis]: 1.14e-3

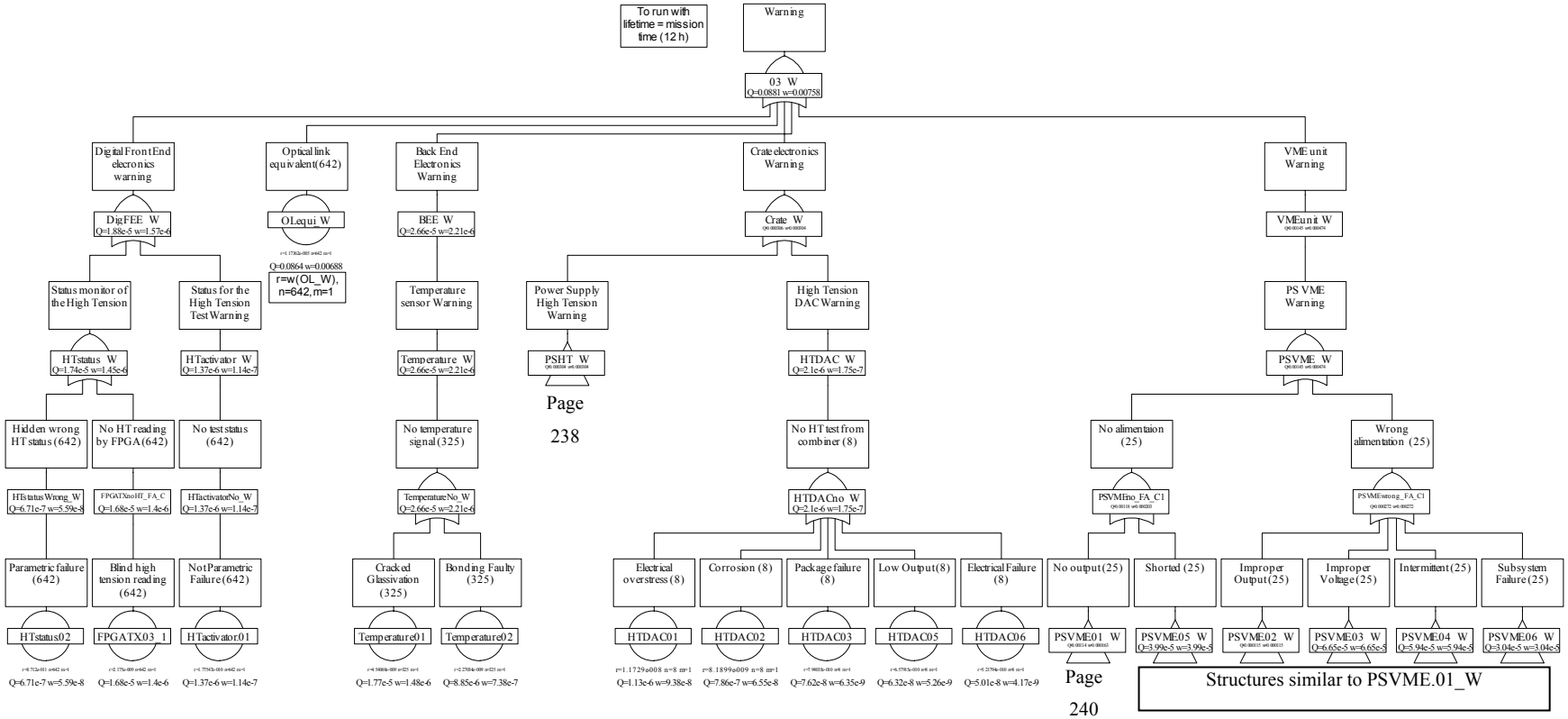
Function: Cooling the VME cards

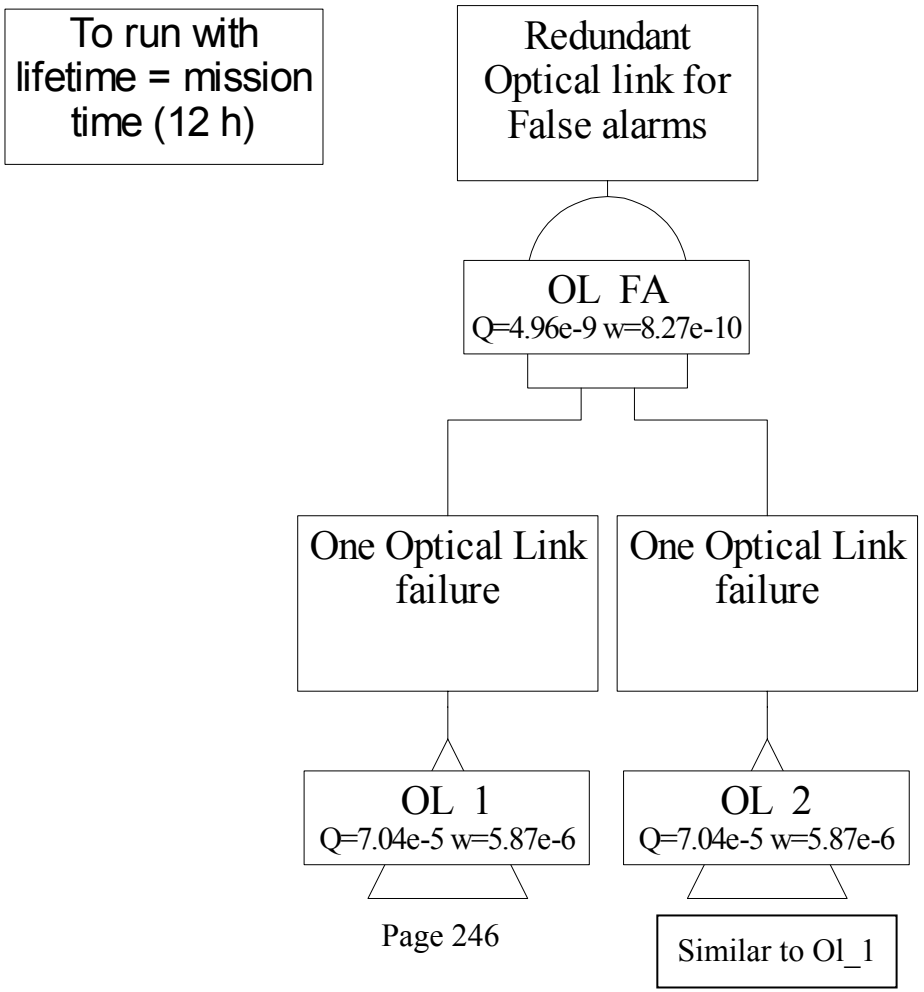
ID	Failure Mode	Alpha	Failure rate	Contributors	Effects	Next Level Effects	End Effects	Detection Method	Criticality [h/mis]	Compensating Provisions
CONTINUED										
04	Blade erosion	9.5e+0	3.01e-06		No ventilation	VME Ventilation failure	False Alarm	DAB Temperature	1.08e-4	
05	Out of Balance	7.1e+0	2.25e-06		No ventilation	VME Ventilation failure	False Alarm	DAB Temperature	8.09e-5	
06	Switch failure	7.1e+0	2.25e-06		No ventilation	VME Ventilation failure	False Alarm	DAB Temperature	8.09e-5	

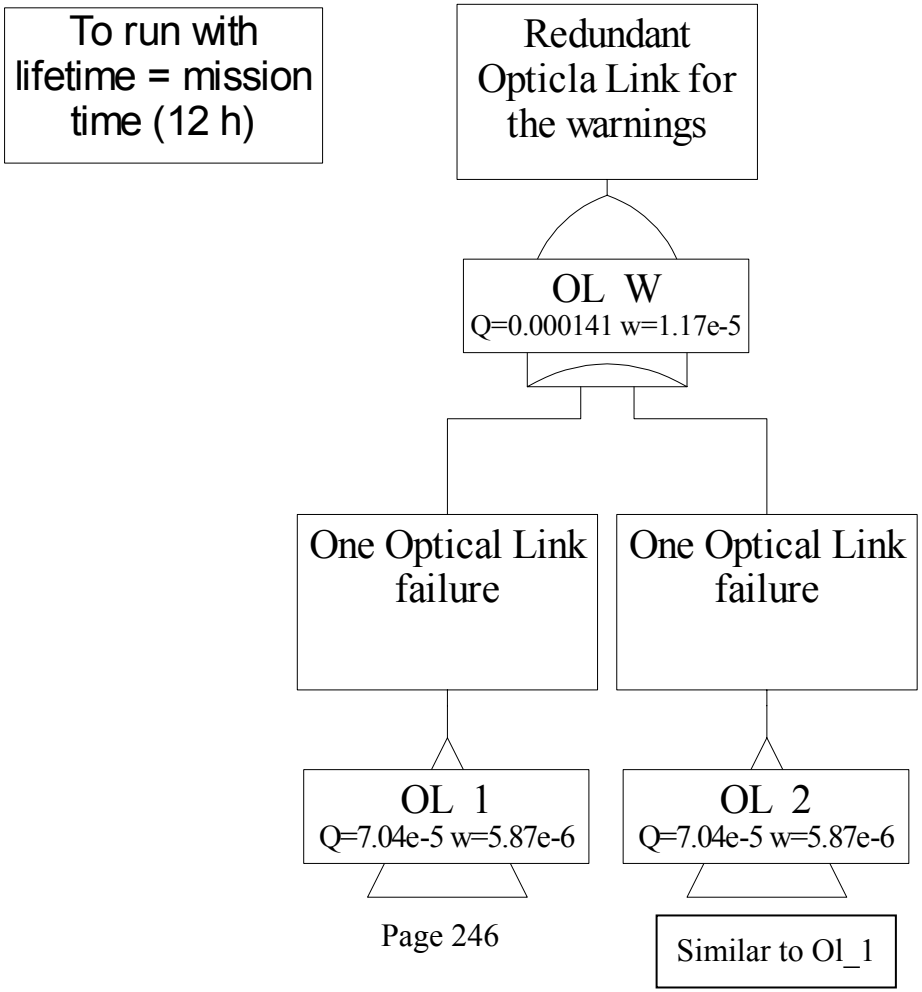
Appendix C Fault Tree Diagrams

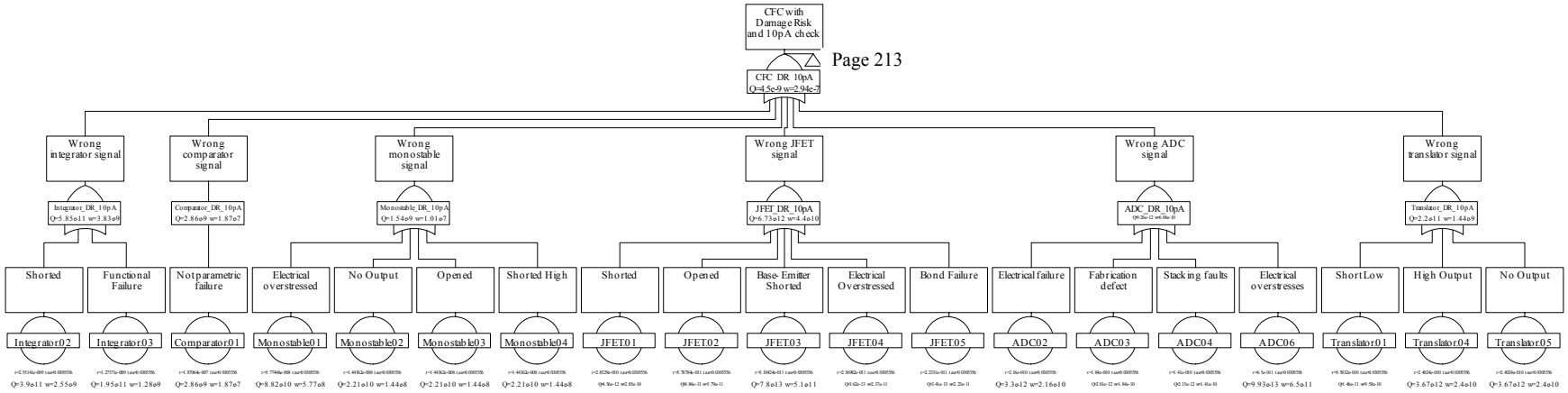


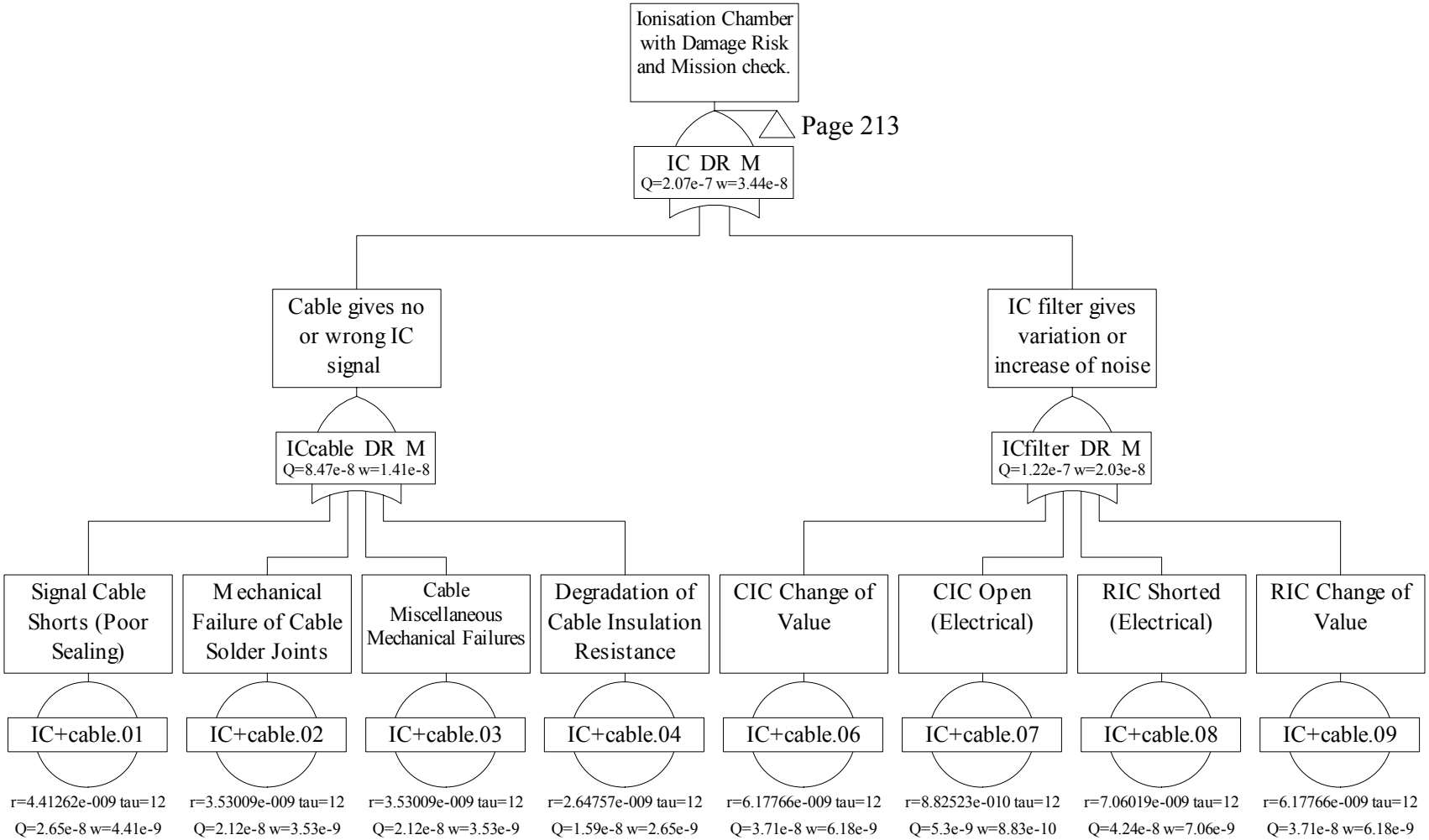

To run with lifetime = mission time (12 h)
False Alarm
02 FA
Q=0.0336 w=0.00275
Channel False Alarm
Digital FEE False Alarm
642 redudant Optical link, w
False alarm generated by tunnel Power Supply
Back End Electronic False Alarm
Crates electronics False Alarms
VME unit False Alarms
Channel FA
Q=0.00513 w=0.000427
DigFEE FA
Q=0.000125 w=1.04e5
OL_equiv_FA
r=5.30677e-007 tau=12
Q=3.18e-6 w=5.31e-7
OL_equiv_FA: r= r(OL_FA)* n tau= mission time
Tunnnel PS FA
Q=0.0191 w=0.00158
BEE FA
Q=9.35e-5 w=7.79e-6
Crate FA
Q=7.12e-6 w=5.99e-7
VMEunit FA
Q=0.00946 w=0.000784
HTconnectors False Alarms, Continuous check
Ionization Chamber False Alarm, Continuous check
CFC False Alarm, 10pA check
Digital FEE False Alarm, Continuous check
Digital FEE False Alarm, 10pA check
Arc Power Supplies False Alarm, Continuous check
Straight Section PS False Alarm, Continuous check
Back End electronic False Alarm, Continuous check
Back End electronic False Alarm, Logging check
Crates electronics False Alarms, Continuous check
Combiner FPGA False Alarm, Loggin check
PS VME False Alarm, Continuous check
VME fan tray False Alarm, Continuous check
HTcon FA C
Q=4.82e-5 w=4.02e-6
IC FA C
Q=0.000368 w=3.07e5
Channel_FA_10pA
Q=0.00472 w=0.000392
DigFEE FA C
Q=0.000108 w=8.97e6
DigFEE_FA_10pA
Q=1.74e-5 w=1.45e-6
PSarc FA C
Q=2.5e-5 w=2.08e-6
PSSS FA C
Q=0.0191 w=0.00158
BEE FA C
Q=8.58e-5 w=7.15e-6
BEE FA L
Q=7.71e-6 w=6.43e-7
Crate FA C
Q=5.47e-6 w=4.62e-7
CombFPGA_FA_L
Q=1.65e-6 w=1.37e-7
PSVME FA C
Q=9.75e-9 w=1.95e-8
VMEfans FA C
Q=0.00946 w=0.000784
Page 222
Page 223
Page 224
Page 225
Page 226
Page 227
Page 228
Page 229
Page 230
Page 231
Page 232
No thresholds (325)
No energy updating from combiner
Wrong energy signal from transceiver
Wrong combiner backplane
Memory FA L
Q=4.82e-7 w=4.02e-8
FPGARXen_FA_L
Q=7.14e-6 w=5.95e-7
Transceiverfn_FA_L
Q=9.55e-8 w=7.96e-9
CombBPin_FA_L
Q=1.65e-6 w=1.37e-7
Mechanical Failure (325)
Electrical Failure (325)
Wrong energy from Combiner (325)
Data Bit Error (325)
Internal error
Memory.01
Memory.02
FPGARX0.3_1
Transceiver.0.6_1
Combiner FPGA.02_1
r=1.83e-009 n=325 m=1
r=2.448e011 n=325 m=1
r=5.49e-009 n=25 m=1
Q=3.62e-7 w=3.01e-8
Q=1.2e-7 w=1e-8
Q=7.14e-6 w=5.95e-7
Q=9.55e-8 w=7.96e-9
Q=1.65e-6 w=1.37e-7

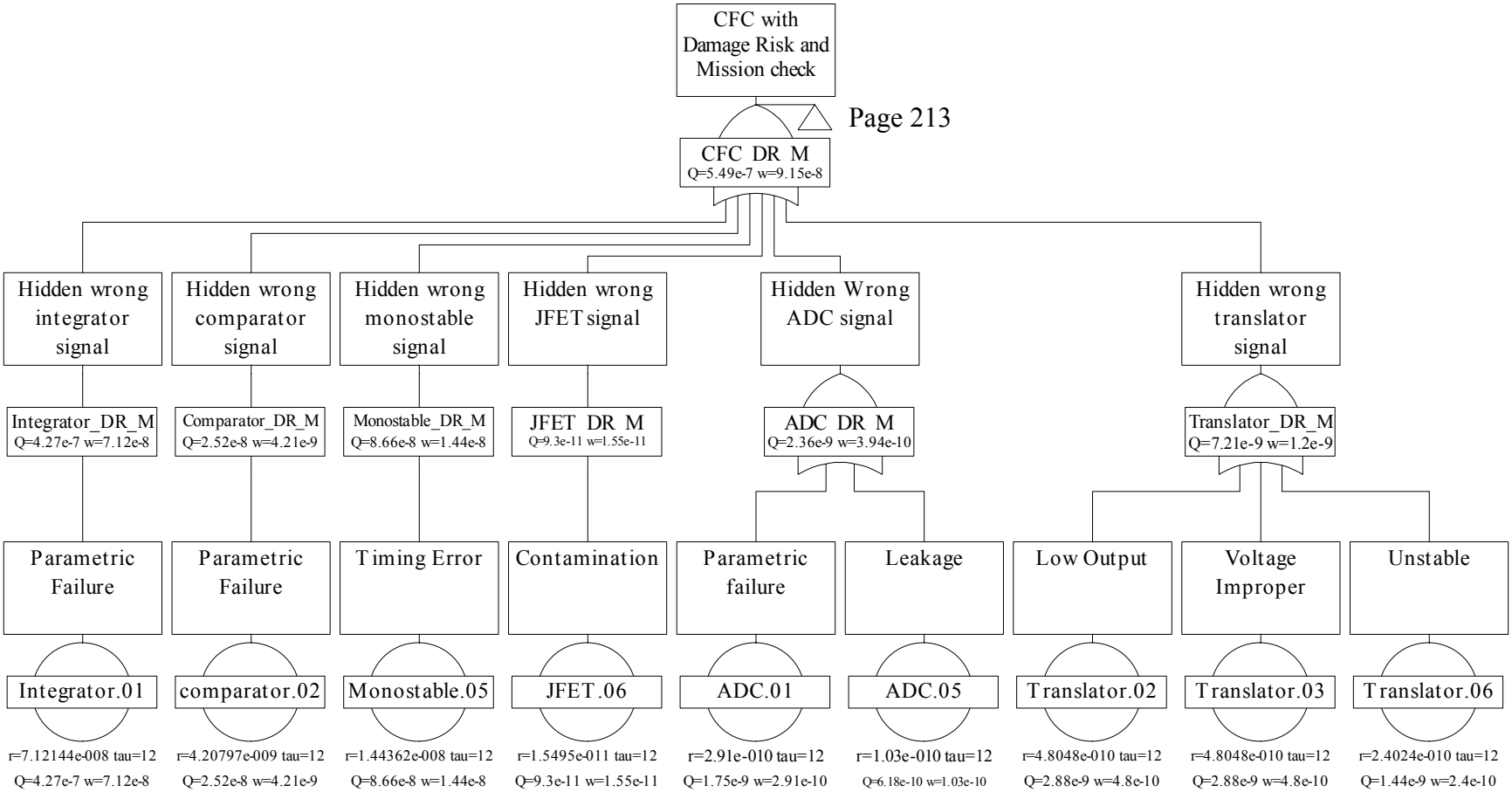

To run with lifetime = mission time (12 h)
Warning
03_W
Q=0.0881 w=0.00758
Digital Front End elecronics warning
Optical link equivalent(642)
Back End Electronics Warning
Crate electronics Warning
VME unit Warning
DigFEE_W
Q=1.88e-5 w=1.57e-6
OLequi_W
Q=0.0864 w=0.00688
r=w(OL_W), n=642, m=1
BEE_W
Q=2.66e-5 w=2.21e-6
Crate_W
VMEunit_W
Status monitor of the High Tension
Status for the High Tension Test Warning
Temperature sensor Warning
Power Supply High Tension Warning
High Tension DAC Warning
PS VME Warning
HTstatus_W
Q=1.74e-5 w=1.45e-6
HTactivator_W
Q=1.37e-6 w=1.14e-7
Temperature_W
Q=2.66e-5 w=2.21e-6
PSHT_W
Page 238
HTDAC_W
Q=2.1e-6 w=1.75e-7
PSVME_W
Hidden wrong HT status (642)
No HT reading by FPGA (642)
No test status (642)
No temperature signal (325)
No HT test from combiner (8)
No alimentaion (25)
Wrong alimentation (25)
HTstatusWrong_W
Q=6.71e-7 w=5.59e-8
FPGATXnoHT_FA_C
Q=1.68e-5 w=1.4e-6
HTactivatorNo_W
Q=1.37e-6 w=1.14e-7
TemperatureNo_W
Q=2.66e-5 w=2.21e-6
HTDACno_W
Q=2.1e-6 w=1.75e-7
PSVMEno_FA_C1
PSVMEwrong_FA_C1
Parametric failure (642)
Blind high tension reading (642)
Not Parametric Failure (642)
Cracked Glassivation (325)
Bonding Faulty (325)
Electrical overstress (8)
Corrosion (8)
Package failure (8)
Low Output (8)
Electrical Failure (8)
No output (25)
Shorted (25)
Improper Output (25)
Improper Voltage (25)
Intermittent (25)
Subsystem Failure (25)
HTstatus02
Q=6.71e-7 w=5.59e-8
FPGATX03_1
Q=1.68e-5 w=1.4e-6
HTactivator01
Q=1.37e-6 w=1.14e-7
Temperature01
Q=1.77e-5 w=1.48e-6
Temperature02
Q=8.85e-6 w=7.38e-7
HTDAC01
Q=1.13e-6 w=9.38e-8
HTDAC02
Q=7.86e-7 w=6.55e-8
HTDAC03
Q=7.62e-8 w=6.35e-9
HTDAC05
Q=6.32e-8 w=5.26e-9
HTDAC06
Q=5.01e-8 w=4.17e-9
PSVME01_W
Page 240
PSVME05_W
Q=3.99e-5 w=3.99e-5
PSVME02_W
PSVME03_W
Q=6.65e-5 w=6.65e-5
PSVME04_W
Q=5.94e-5 w=5.94e-5
PSVME06_W
Q=3.04e-5 w=3.04e-5
Structures similar to PSVME.01_W

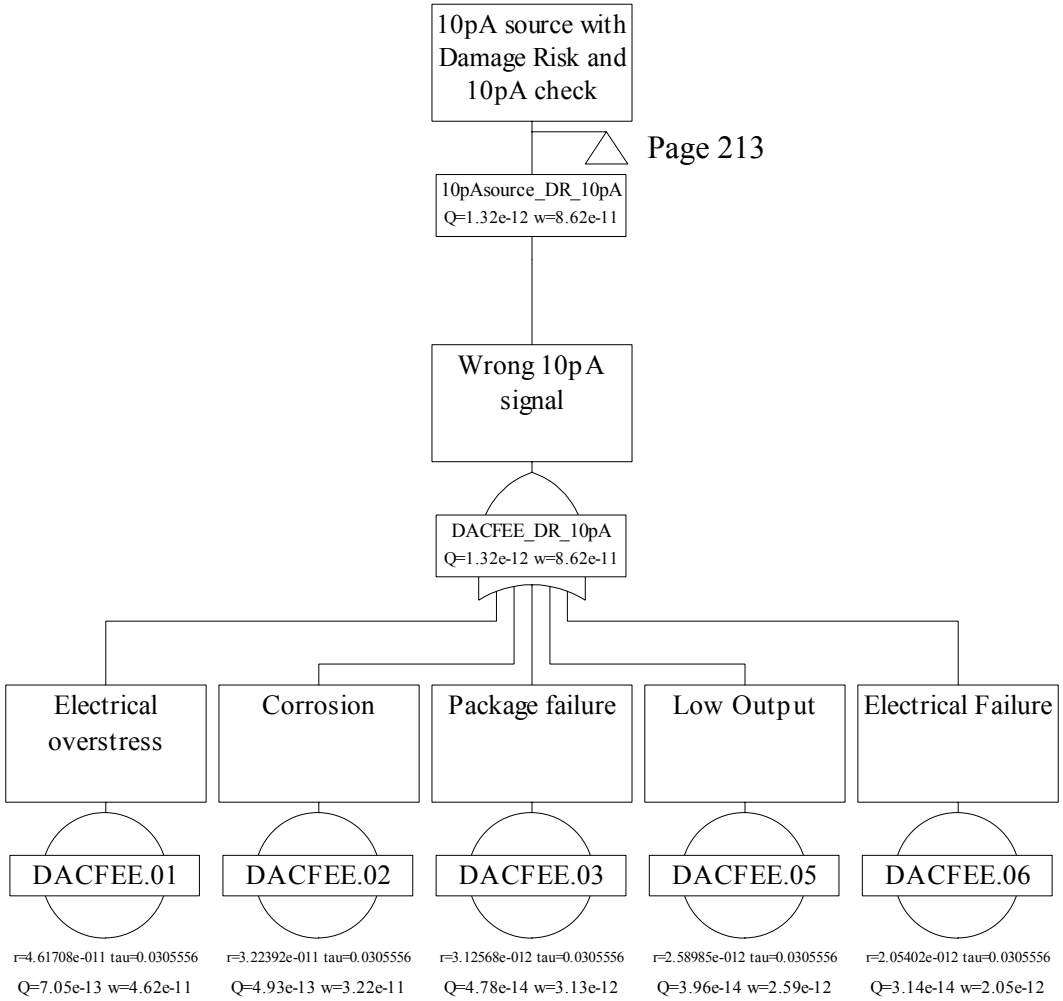

To run with lifetime = mission time (12 h)
Redundant Optical link for False alarms
OL FA
Q=4.96e-9 w=8.27e-10
One Optical Link failure
One Optical Link failure
OL 1
Q=7.04e-5 w=5.87e-6
OL 2
Q=7.04e-5 w=5.87e-6
Page 246
Similar to Ol_1

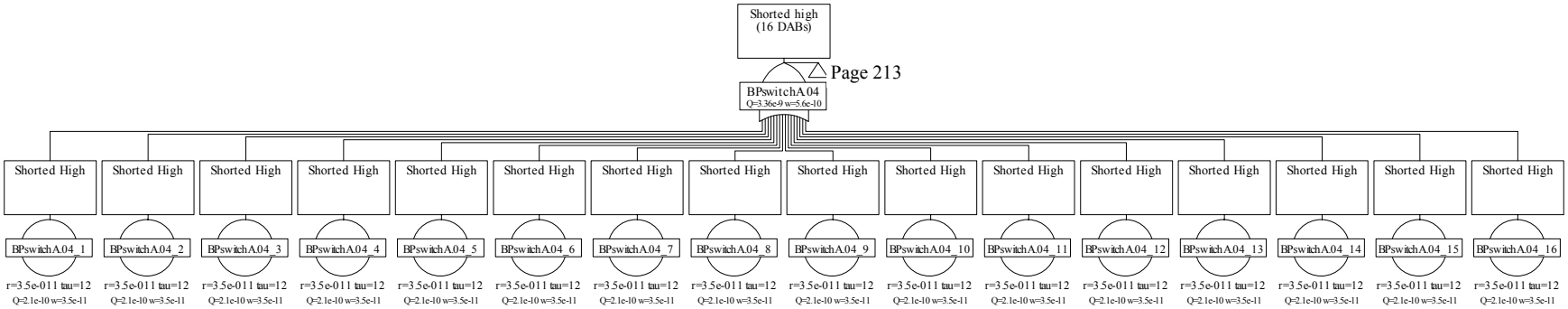

To run with lifetime = mission time (12 h)
Redundant Opticla Link for the warnings
OL W
Q=0.000141 w=1.17e-5
One Optical Link failure
One Optical Link failure
OL 1
Q=7.04e-5 w=5.87e-6
OL 2
Q=7.04e-5 w=5.87e-6
Page 246
Similar to Ol_1

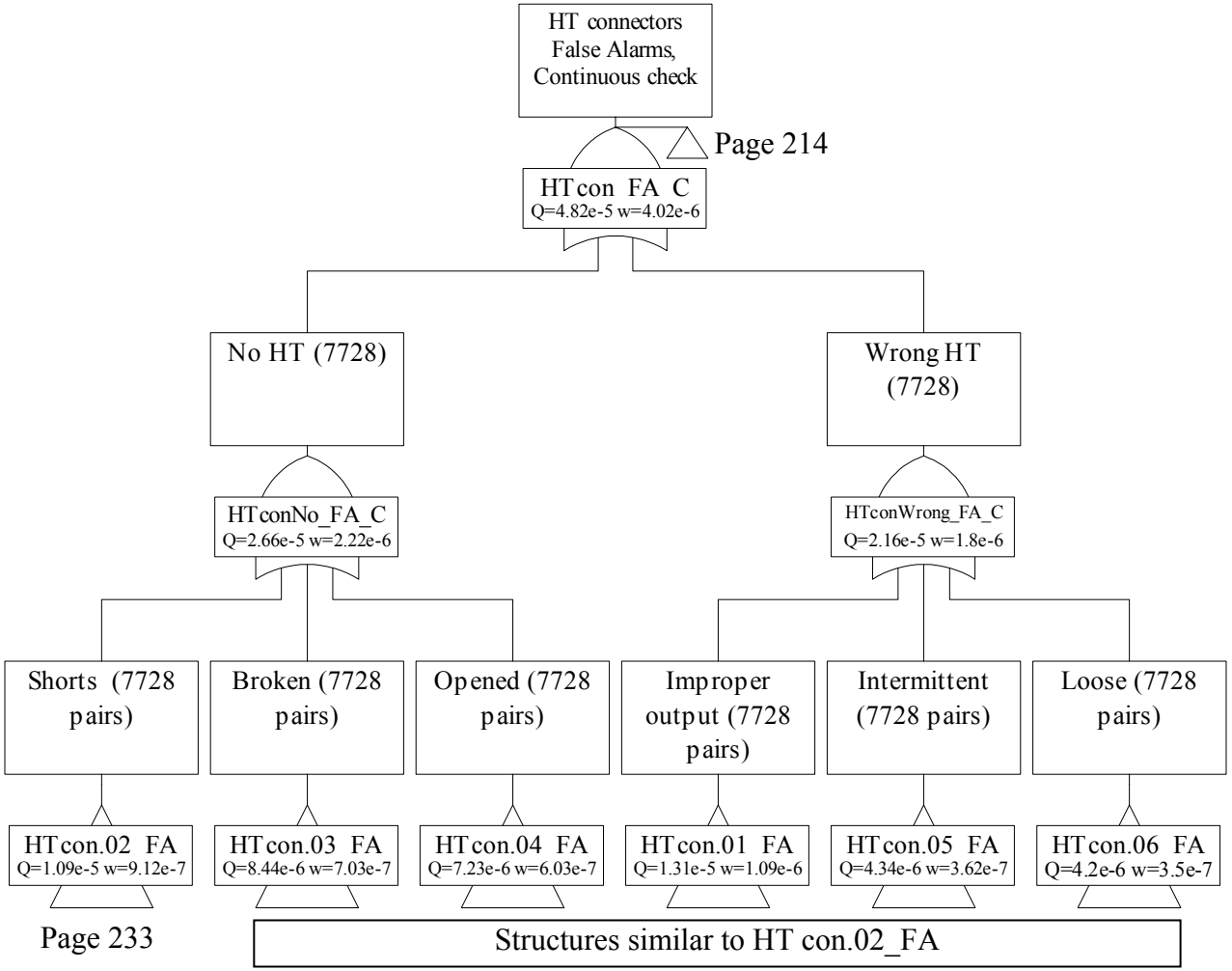

CFC with Damage Risk and 10pA check
Page 213
CFC_DR_10pA
Q=4.5e-9 w=2.94e-7
Wrong integrator signal
Wrong comparator signal
Wrong monostable signal
Wrong JFET signal
Wrong ADC signal
Wrong translator signal
Integrator_DR_10pA
Q=5.85e11 w=3.83e9
Comparator_DR_10pA
Q=2.86e9 w=1.87e7
Monostable_DR_10pA
Q=1.54e9 w=1.01e7
JFET_DR_10pA
Q=6.73e12 w=4.4e10
ADC_DR_10pA
Translator_DR_10pA
Q=2.2e11 w=1.44e9
Shorted
Functional Failure
Not parametric failure
Electrical overstressed
No Output
Opened
Shorted High
Shorted
Opened
Base-Emitter Shorted
Electrical Overstressed
Bond Failure
Electrical failure
Fabrication defect
Stacking faults
Electrical overstresses
Short Low
High Output
No Output
Integrator02
Integrator03
Comparator01
Monostable01
Monostable02
Monostable03
Monostable04
JFET01
JFET02
JFET03
JFET04
JFET05
ADC02
ADC03
ADC04
ADC06
Translator01
Translator04
Translator05
Q=3.9e11 w=2.55e9
Q=1.95e11 w=1.28e9
Q=2.86e9 w=1.87e7
Q=8.82e10 w=5.77e8
Q=2.21e10 w=1.44e8
Q=2.21e10 w=1.44e8
Q=2.21e10 w=1.44e8
Q=7.8e13 w=5.1e11
Q=3.3e12 w=2.16e10
Q=9.93e13 w=6.5e11
Q=3.67e12 w=2.4e10
Q=3.67e12 w=2.4e10

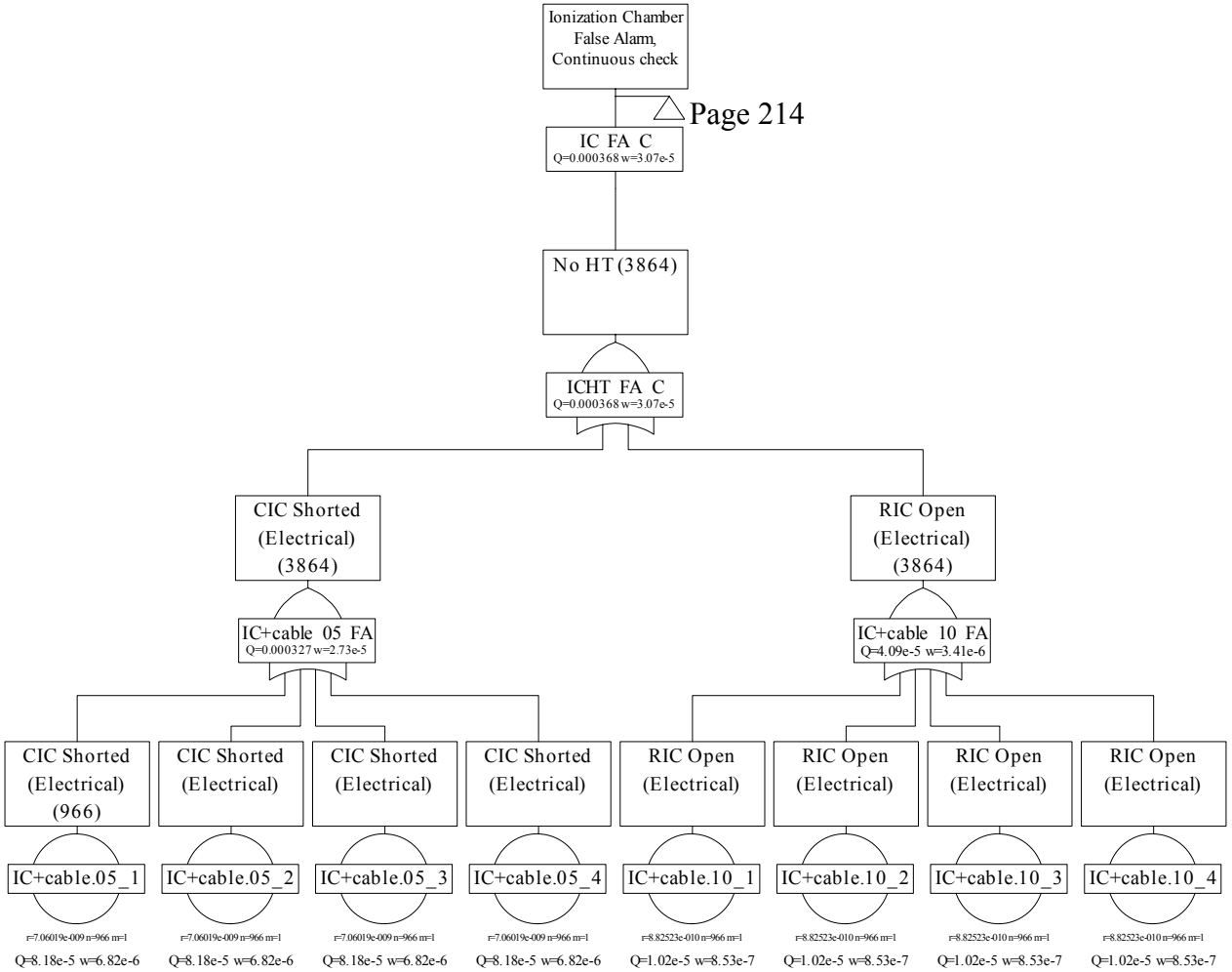

Ionisation Chamber with Damage Risk and Mission check.
Page 213
IC DR M
Q=2.07e-7 w=3.44e-8
Cable gives no or wrong IC signal
IC filter gives variation or increase of noise
ICcable DR M
Q=8.47e-8 w=1.41e-8
ICfilter DR M
Q=1.22e-7 w=2.03e-8
Signal Cable Shorts (Poor Sealing)
Mechanical Failure of Cable Solder Joints
Cable Miscellaneous Mechanical Failures
Degradation of Cable Insulation Resistance
CIC Change of Value
CIC Open (Electrical)
RIC Shorted (Electrical)
RIC Change of Value
IC+cable.01
IC+cable.02
IC+cable.03
IC+cable.04
IC+cable.06
IC+cable.07
IC+cable.08
IC+cable.09
r=4.41262e-009 tau=12
Q=2.65e-8 w=4.41e-9
r=3.53009e-009 tau=12
Q=2.12e-8 w=3.53e-9
r=3.53009e-009 tau=12
Q=2.12e-8 w=3.53e-9
r=2.64757e-009 tau=12
Q=1.59e-8 w=2.65e-9
r=6.17766e-009 tau=12
Q=3.71e-8 w=6.18e-9
r=8.82523e-010 tau=12
Q=5.3e-9 w=8.83e-10
r=7.06019e-009 tau=12
Q=4.24e-8 w=7.06e-9
r=6.17766e-009 tau=12
Q=3.71e-8 w=6.18e-9

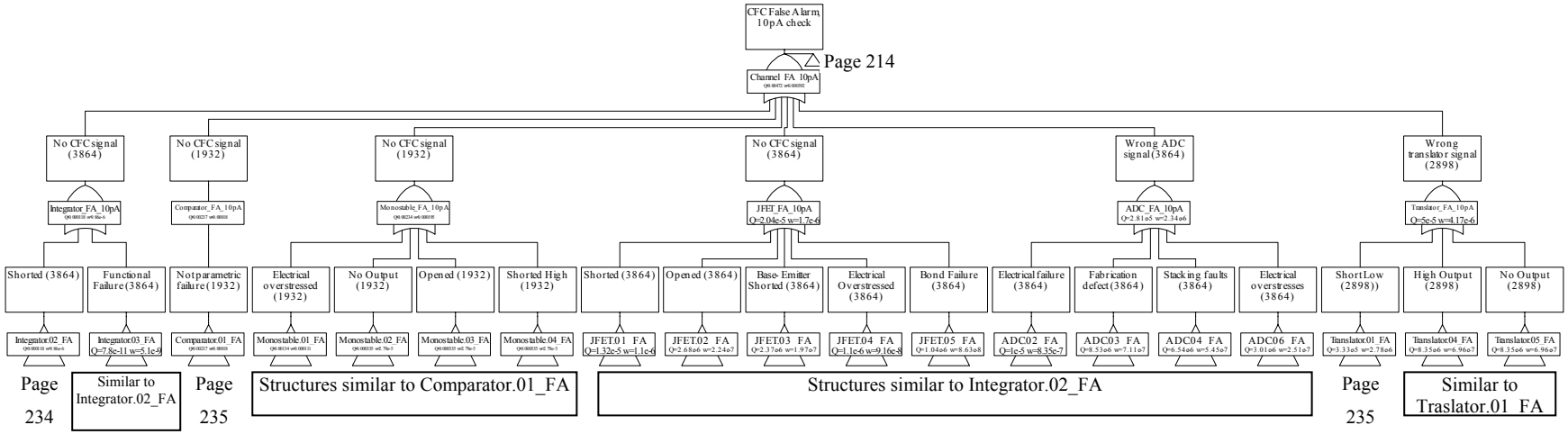

CFC with Damage Risk and Mission check
Page 213
CFC DR M
Q=5.49e-7 w=9.15e-8
Hidden wrong integrator signal
Hidden wrong comparator signal
Hidden wrong monostable signal
Hidden wrong JFET signal
Hidden Wrong ADC signal
Hidden wrong translator signal
Integrator_DR_M
Q=4.27e-7 w=7.12e-8
Comparator_DR_M
Q=2.52e-8 w=4.21e-9
Monostable_DR_M
Q=8.66e-8 w=1.44e-8
JFET DR M
Q=9.3e-11 w=1.55e-11
ADC DR M
Q=2.36e-9 w=3.94e-10
Translator_DR_M
Q=7.21e-9 w=1.2e-9
Parametric Failure
Parametric Failure
Timing Error
Contamination
Parametric failure
Leakage
Low Output
Voltage Improper
Unstable
Integrator.01
comparator.02
Monostable.05
JFET.06
ADC.01
ADC.05
Translator.02
Translator.03
Translator.06
r=7.12144e-008 tau=12
Q=4.27e-7 w=7.12e-8
r=4.20797e-009 tau=12
Q=2.52e-8 w=4.21e-9
r=1.44362e-008 tau=12
Q=8.66e-8 w=1.44e-8
r=1.5495e-011 tau=12
Q=9.3e-11 w=1.55e-11
r=2.91e-010 tau=12
Q=1.75e-9 w=2.91e-10
r=1.03e-010 tau=12
Q=6.18e-10 w=1.03e-10
r=4.8048e-010 tau=12
Q=2.88e-9 w=4.8e-10
r=4.8048e-010 tau=12
Q=2.88e-9 w=4.8e-10
r=2.4024e-010 tau=12
Q=1.44e-9 w=2.4e-10

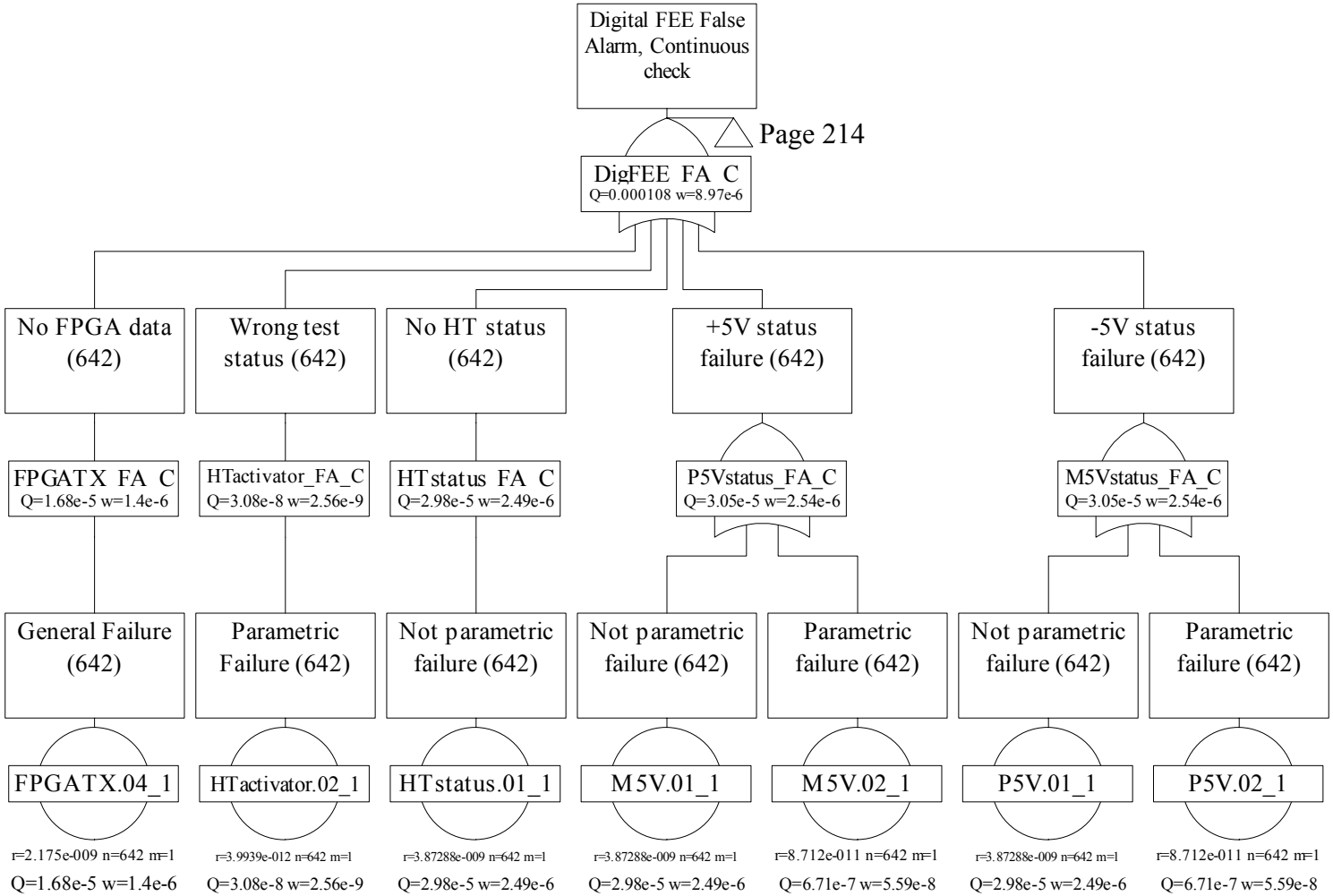

10pA source with Damage Risk and 10pA check
Page 213
10pAsource_DR_10pA
Q=1.32e-12 w=8.62e-11
Wrong 10pA signal
DACFEE_DR_10pA
Q=1.32e-12 w=8.62e-11
Electrical overstress
Corrosion
Package failure
Low Output
Electrical Failure
DACFEE.01
DACFEE.02
DACFEE.03
DACFEE.05
DACFEE.06
r=4.61708e-011 tau=0.0305556
Q=7.05e-13 w=4.62e-11
r=3.22392e-011 tau=0.0305556
Q=4.93e-13 w=3.22e-11
r=3.12568e-012 tau=0.0305556
Q=4.78e-14 w=3.13e-12
r=2.58985e-012 tau=0.0305556
Q=3.96e-14 w=2.59e-12
r=2.05402e-012 tau=0.0305556
Q=3.14e-14 w=2.05e-12

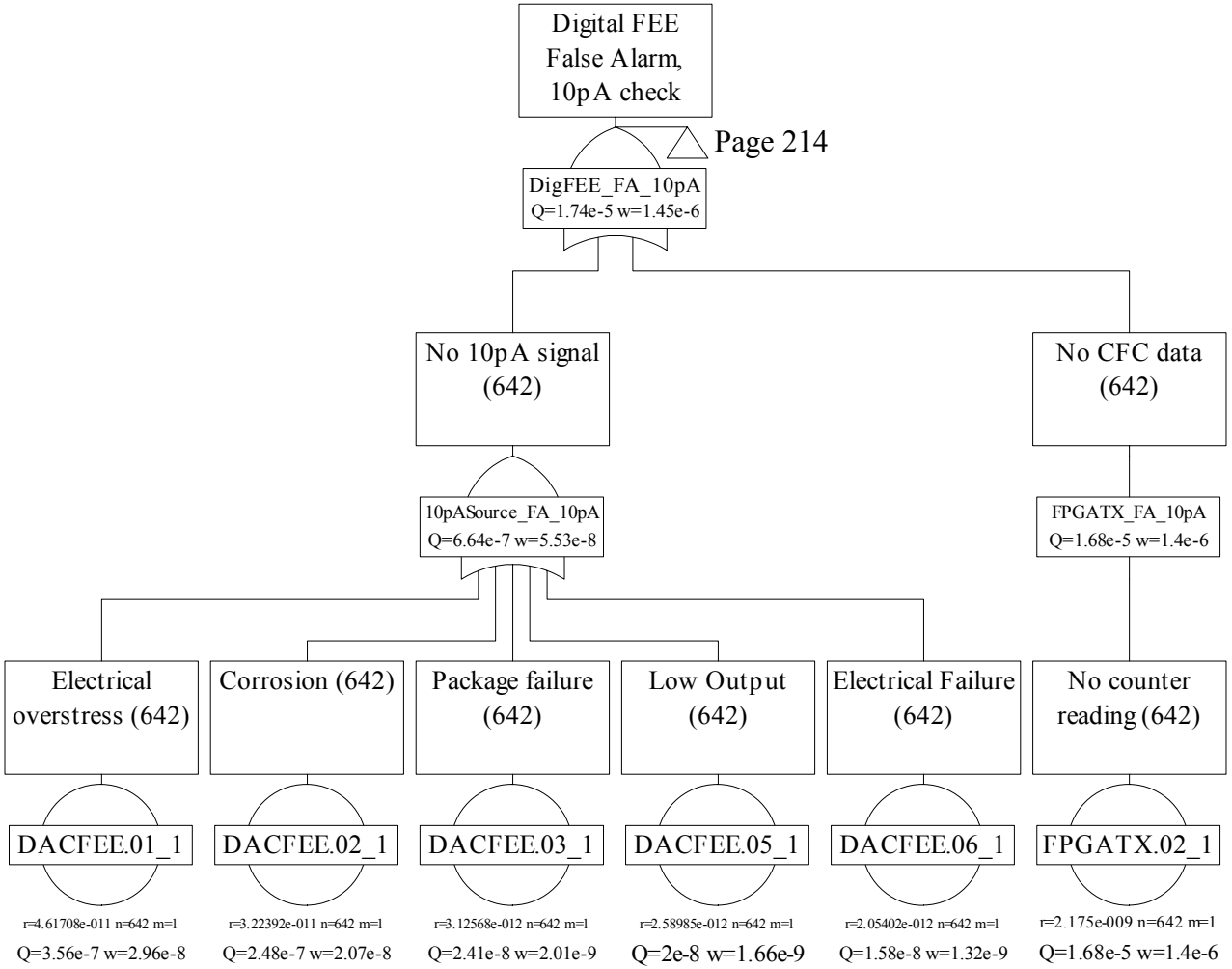

Shorted high
(16 DABs)
Page 213
BPswitchA.04
Q=3.36e-9 w=5.6e-10
Shorted High
BPswitchA.04_1
BPswitchA.04_2
BPswitchA.04_3
BPswitchA.04_4
BPswitchA.04_5
BPswitchA.04_6
BPswitchA.04_7
BPswitchA.04_8
BPswitchA.04_9
BPswitchA.04_10
BPswitchA.04_11
BPswitchA.04_12
BPswitchA.04_13
BPswitchA.04_14
BPswitchA.04_15
BPswitchA.04_16
r=3.5e-011 tau=12
Q=2.1e-10 w=3.5e-11

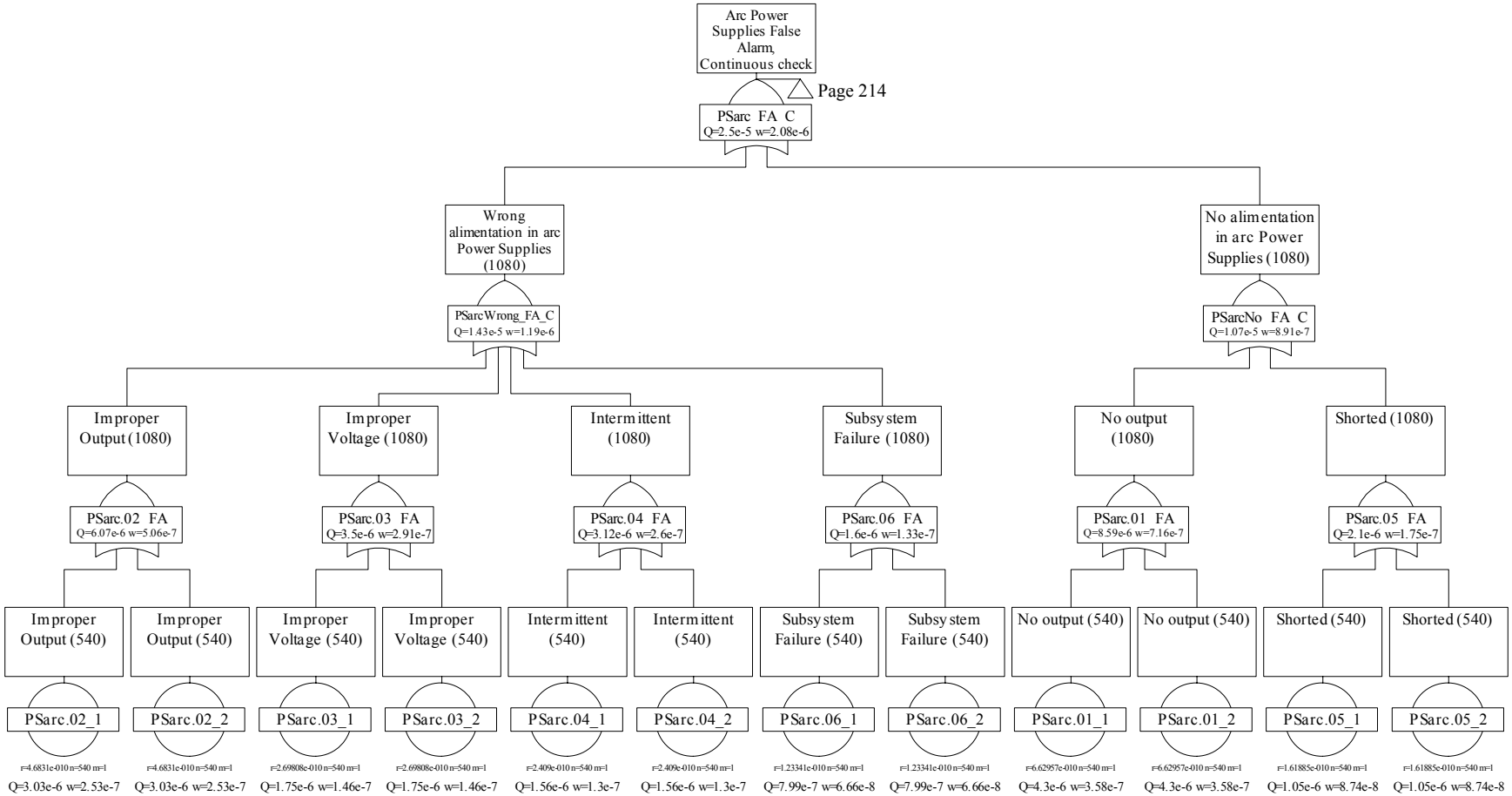

HT connectors
False Alarms,
Continuous check
Page 214
HTcon FA C
Q=4.82e-5 w=4.02e-6
No HT (7728)
Wrong HT
(7728)
HTconNo_FA_C
Q=2.66e-5 w=2.22e-6
HTconWrong_FA_C
Q=2.16e-5 w=1.8e-6
Shorts (7728
pairs)
Broken (7728
pairs)
Opened (7728
pairs)
Improper
output (7728
pairs)
Intermittent
(7728 pairs)
Loose (7728
pairs)
HTcon.02 FA
Q=1.09e-5 w=9.12e-7
HTcon.03 FA
Q=8.44e-6 w=7.03e-7
HTcon.04 FA
Q=7.23e-6 w=6.03e-7
HTcon.01 FA
Q=1.31e-5 w=1.09e-6
HTcon.05 FA
Q=4.34e-6 w=3.62e-7
HTcon.06 FA
Q=4.2e-6 w=3.5e-7
Page 233
Structures similar to HT con.02_FA

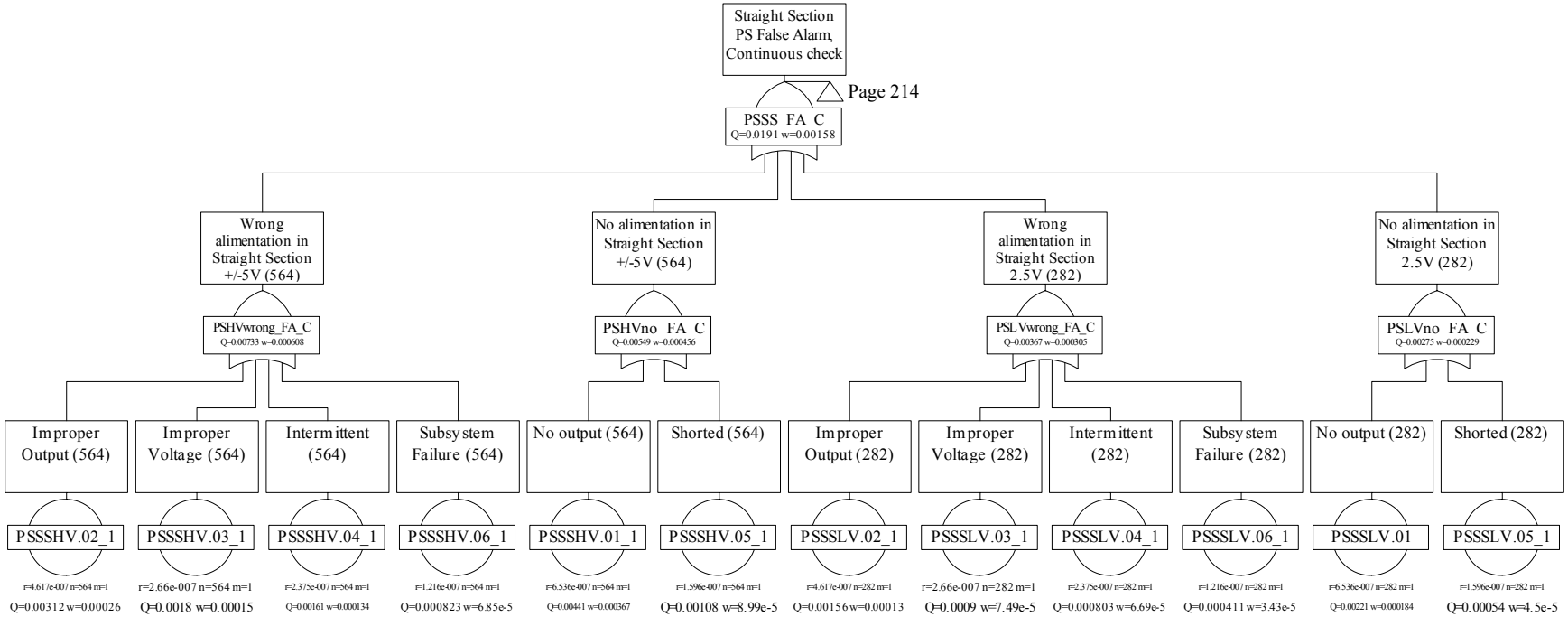

Ionization Chamber False Alarm, Continuous check
Page 214
IC FA C
Q=0.000368 w=3.07e-5
No HT (3864)
ICHT FA C
Q=0.000368 w=3.07e-5
CIC Shorted (Electrical) (3864)
RIC Open (Electrical) (3864)
IC+cable 05 FA
Q=0.000327 w=2.73e-5
IC+cable 10 FA
Q=4.09e-5 w=3.41e-6
CIC Shorted (Electrical) (966)
CIC Shorted (Electrical)
CIC Shorted (Electrical)
CIC Shorted (Electrical)
RIC Open (Electrical)
RIC Open (Electrical)
RIC Open (Electrical)
RIC Open (Electrical)
IC+cable.05_1
IC+cable.05_2
IC+cable.05_3
IC+cable.05_4
IC+cable.10_1
IC+cable.10_2
IC+cable.10_3
IC+cable.10_4
r=7.06019e-009 n=966 m=1
Q=8.18e-5 w=6.82e-6
r=7.06019e-009 n=966 m=1
Q=8.18e-5 w=6.82e-6
r=7.06019e-009 n=966 m=1
Q=8.18e-5 w=6.82e-6
r=7.06019e-009 n=966 m=1
Q=8.18e-5 w=6.82e-6
r=8.82523e-010 n=966 m=1
Q=1.02e-5 w=8.53e-7
r=8.82523e-010 n=966 m=1
Q=1.02e-5 w=8.53e-7
r=8.82523e-010 n=966 m=1
Q=1.02e-5 w=8.53e-7
r=8.82523e-010 n=966 m=1
Q=1.02e-5 w=8.53e-7

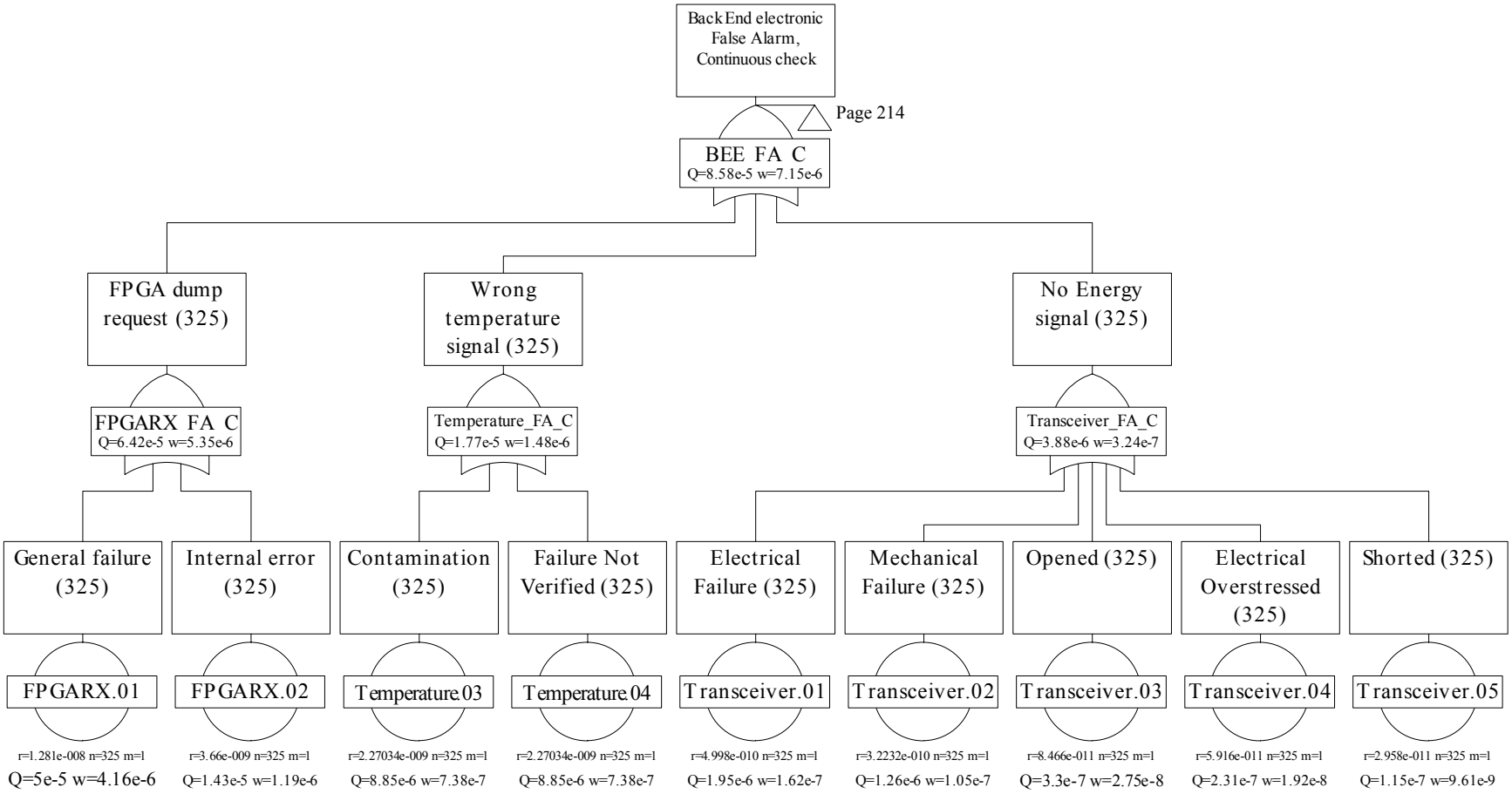

CFC False Alarm, 10pA check
Page 214
Channel_FA_10pA
No CFC signal (3864)
No CFC signal (1932)
No CFC signal (1932)
No CFC signal (3864)
Wrong ADC signal (3864)
Wrong translator signal (2898)
Integrator_FA_10pA
Comparator_FA_10pA
Monostable_FA_10pA
JFET_FA_10pA
Q=2.04e-5 w=1.7e-6
ADC_FA_10pA
Q=2.81e5 w=2.34e6
Translator_FA_10pA
Q=5e-5 w=4.17e-6
Shorted (3864)
Functional Failure (3864)
Not parametric failure (1932)
Electrical overstressed (1932)
No Output (1932)
Opened (1932)
Shorted High (1932)
Shorted (3864)
Opened (3864)
Base- Emitter Shorted (3864)
Electrical Overstressed (3864)
Bond Failure (3864)
Electrical failure (3864)
Fabrication defect (3864)
Stacking faults (3864)
Electrical overstresses (3864)
Short Low (2898))
High Output (2898)
No Output (2898)
Integrator.02_FA
Integrator.03_FA
Q=7.8e-11 w=5.1e-9
Comparator.01_FA
Monostable.01_FA
Monostable.02_FA
Monostable.03_FA
Monostable.04_FA
JFET.01_FA
Q=1.32e-5 w=1.1e-6
JFET.02_FA
Q=2.68e6 w=2.24e7
JFET.03_FA
Q=2.37e6 w=1.97e7
JFET.04_FA
Q=1.1e-6 w=9.16e-8
JFET.05_FA
Q=1.04e6 w=8.63e8
ADC.02_FA
Q=1e-5 w=8.35e-7
ADC.03_FA
Q=8.53e6 w=7.11e7
ADC.04_FA
Q=6.54e6 w=5.45e7
ADC.06_FA
Q=3.01e6 w=2.51e7
Translator.01_FA
Q=3.33e5 w=2.78e6
Translator.04_FA
Q=8.35e6 w=6.96e7
Translator.05_FA
Q=8.35e6 w=6.96e7
Page 234
Similar to Integrator.02_FA
Page 235
Structures similar to Comparator.01_FA
Structures similar to Integrator.02_FA
Page 235
Similar to Traslator.01_FA

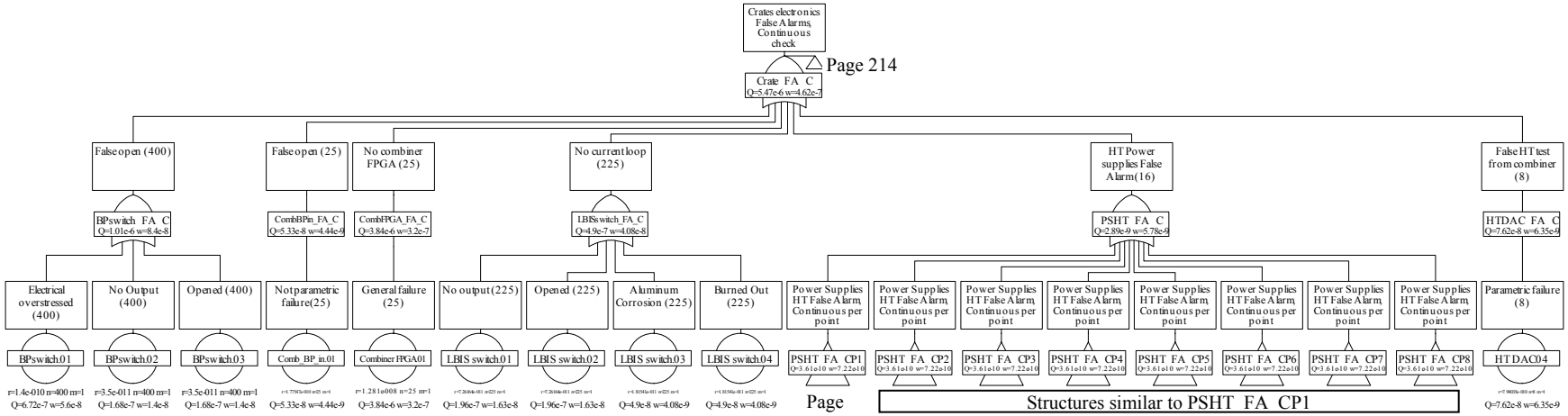

Digital FEE False Alarm, Continuous check
Page 214
DigFEE_FA_C
Q=0.000108 w=8.97e-6
No FPGA data (642)
Wrong test status (642)
No HT status (642)
+5V status failure (642)
-5V status failure (642)
FPGATX_FA_C
Q=1.68e-5 w=1.4e-6
HTactivator_FA_C
Q=3.08e-8 w=2.56e-9
HTstatus_FA_C
Q=2.98e-5 w=2.49e-6
P5Vstatus_FA_C
Q=3.05e-5 w=2.54e-6
M5Vstatus_FA_C
Q=3.05e-5 w=2.54e-6
General Failure (642)
Parametric Failure (642)
Not parametric failure (642)
Not parametric failure (642)
Parametric failure (642)
Not parametric failure (642)
Parametric failure (642)
FPGATX.04_1
HTactivator.02_1
HTstatus.01_1
M5V.01_1
M5V.02_1
P5V.01_1
P5V.02_1
r=2.175e-009 n=642 m=1
Q=1.68e-5 w=1.4e-6
r=3.9939e-012 n=642 m=1
Q=3.08e-8 w=2.56e-9
r=3.87288e-009 n=642 m=1
Q=2.98e-5 w=2.49e-6
r=3.87288e-009 n=642 m=1
Q=2.98e-5 w=2.49e-6
r=8.712e-011 n=642 m=1
Q=6.71e-7 w=5.59e-8
r=3.87288e-009 n=642 m=1
Q=2.98e-5 w=2.49e-6
r=8.712e-011 n=642 m=1
Q=6.71e-7 w=5.59e-8

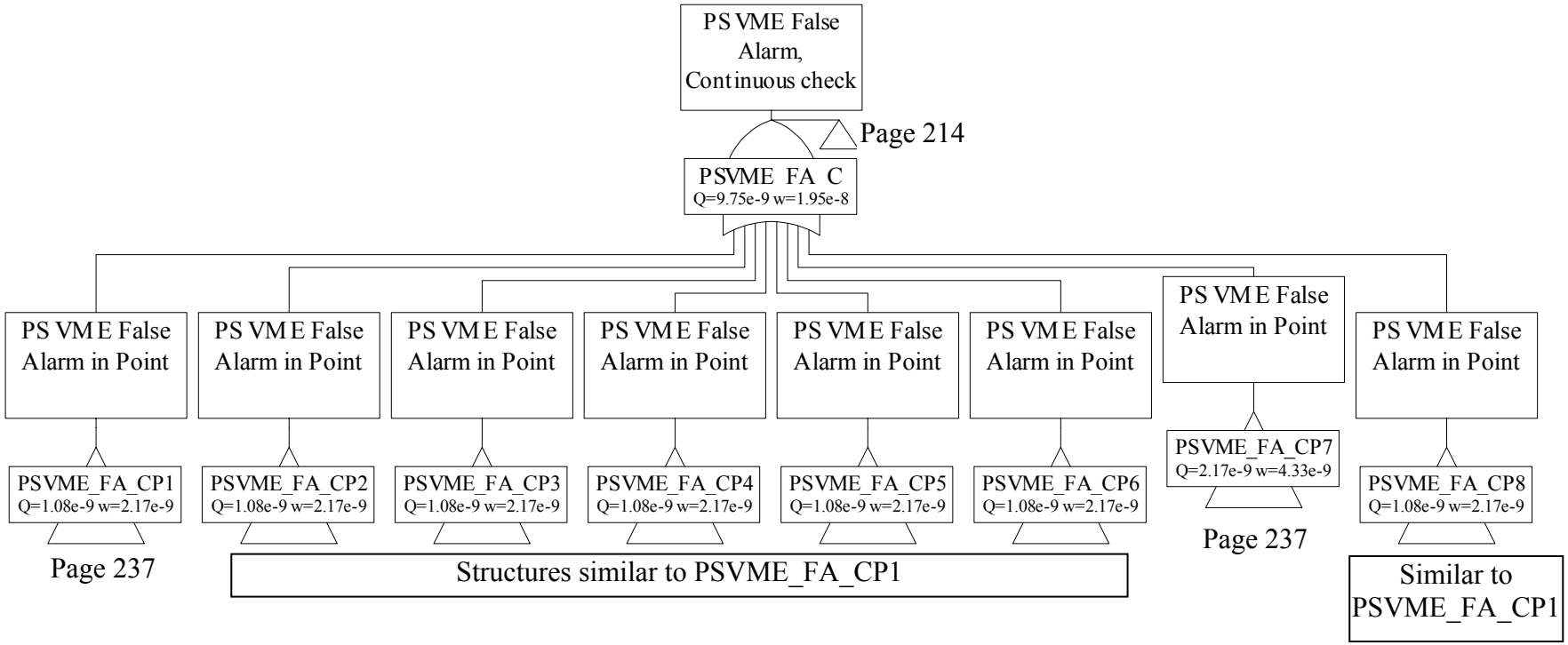

Digital FEE
False Alarm,
10pA check
Page 214
DigFEE_FA_10pA
Q=1.74e-5 w=1.45e-6
No 10pA signal
(642)
No CFC data
(642)
10pASource_FA_10pA
Q=6.64e-7 w=5.53e-8
FPGATX_FA_10pA
Q=1.68e-5 w=1.4e-6
Electrical
overstress (642)
Corrosion (642)
Package failure
(642)
Low Output
(642)
Electrical Failure
(642)
No counter
reading (642)
DACFEE.01_1
DACFEE.02_1
DACFEE.03_1
DACFEE.05_1
DACFEE.06_1
FPGATX.02_1
r=4.61708e-011 n=642 m=1
Q=3.56e-7 w=2.96e-8
r=3.22392e-011 n=642 m=1
Q=2.48e-7 w=2.07e-8
r=3.12568e-012 n=642 m=1
Q=2.41e-8 w=2.01e-9
r=2.58985e-012 n=642 m=1
Q=2e-8 w=1.66e-9
r=2.05402e-012 n=642 m=1
Q=1.58e-8 w=1.32e-9
r=2.175e-009 n=642 m=1
Q=1.68e-5 w=1.4e-6

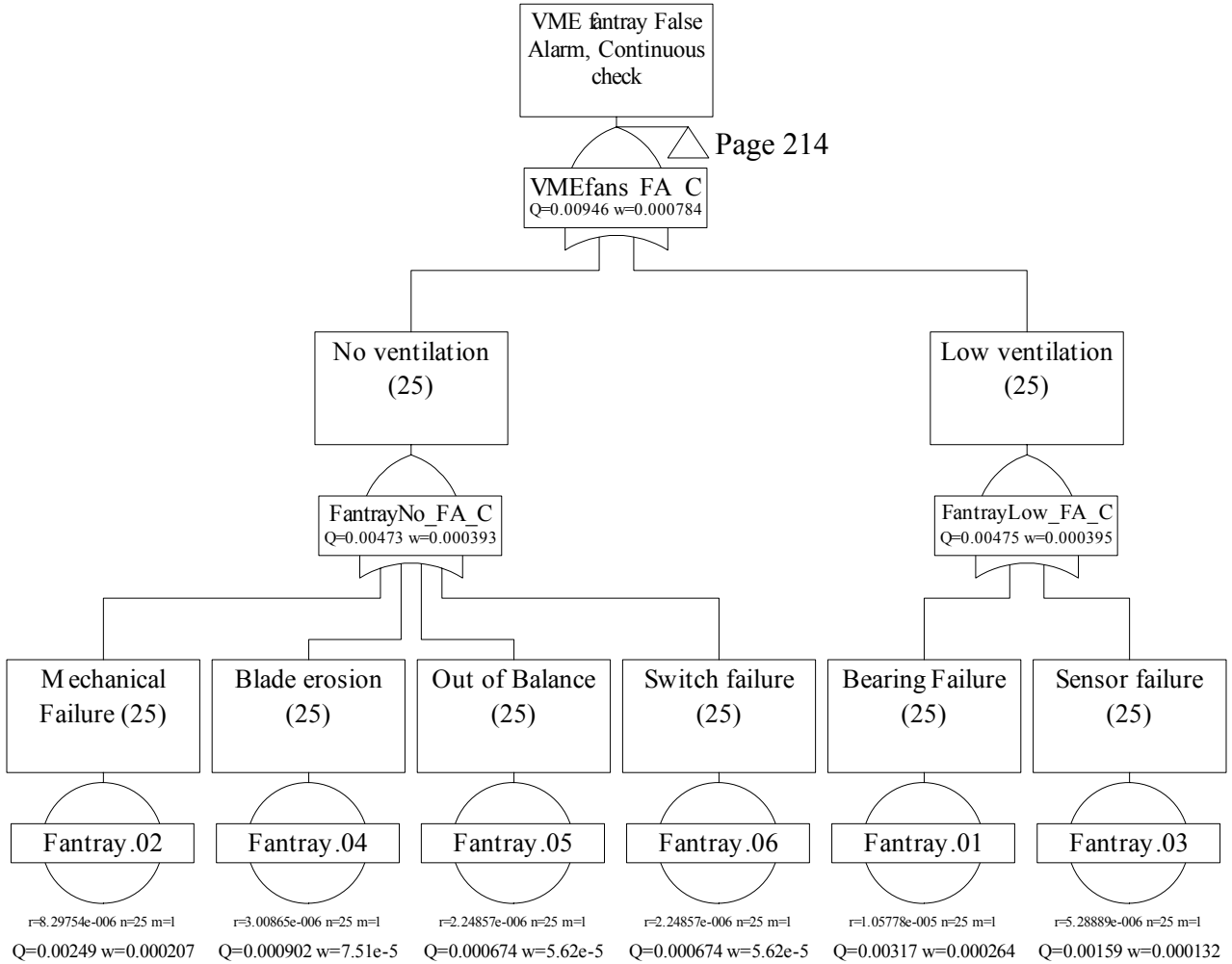

Arc Power Supplies False Alarm, Continuous check
Page 214
PSarc FA C
Q=2.5e-5 w=2.08e-6
Wrong alimentation in arc Power Supplies (1080)
PSarcWrong_FA_C
Q=1.43e-5 w=1.19e-6
No alimentation in arc Power Supplies (1080)
PSarcNo FA C
Q=1.07e-5 w=8.91e-7
Improper Output (1080)
PSarc.02 FA
Q=6.07e-6 w=5.06e-7
Improper Voltage (1080)
PSarc.03 FA
Q=3.5e-6 w=2.91e-7
Intermittent (1080)
PSarc.04 FA
Q=3.12e-6 w=2.6e-7
Subsystem Failure (1080)
PSarc.06 FA
Q=1.6e-6 w=1.33e-7
No output (1080)
PSarc.01 FA
Q=8.59e-6 w=7.16e-7
Shorted (1080)
PSarc.05 FA
Q=2.1e-6 w=1.75e-7
Improper Output (540)
Improper Output (540)
Improper Voltage (540)
Improper Voltage (540)
Intermittent (540)
Intermittent (540)
Subsystem Failure (540)
Subsystem Failure (540)
No output (540)
No output (540)
Shorted (540)
Shorted (540)
PSarc.02_1
PSarc.02_2
PSarc.03_1
PSarc.03_2
PSarc.04_1
PSarc.04_2
PSarc.06_1
PSarc.06_2
PSarc.01_1
PSarc.01_2
PSarc.05_1
PSarc.05_2
r=4.6831e-010 n=540 m=1
Q=3.03e-6 w=2.53e-7
r=4.6831e-010 n=540 m=1
Q=3.03e-6 w=2.53e-7
r=2.69808e-010 n=540 m=1
Q=1.75e-6 w=1.46e-7
r=2.69808e-010 n=540 m=1
Q=1.75e-6 w=1.46e-7
r=2.409e-010 n=540 m=1
Q=1.56e-6 w=1.3e-7
r=2.409e-010 n=540 m=1
Q=1.56e-6 w=1.3e-7
r=1.23341e-010 n=540 m=1
Q=7.99e-7 w=6.66e-8
r=1.23341e-010 n=540 m=1
Q=7.99e-7 w=6.66e-8
r=6.62957e-010 n=540 m=1
Q=4.3e-6 w=3.58e-7
r=6.62957e-010 n=540 m=1
Q=4.3e-6 w=3.58e-7
r=1.61885e-010 n=540 m=1
Q=1.05e-6 w=8.74e-8
r=1.61885e-010 n=540 m=1
Q=1.05e-6 w=8.74e-8

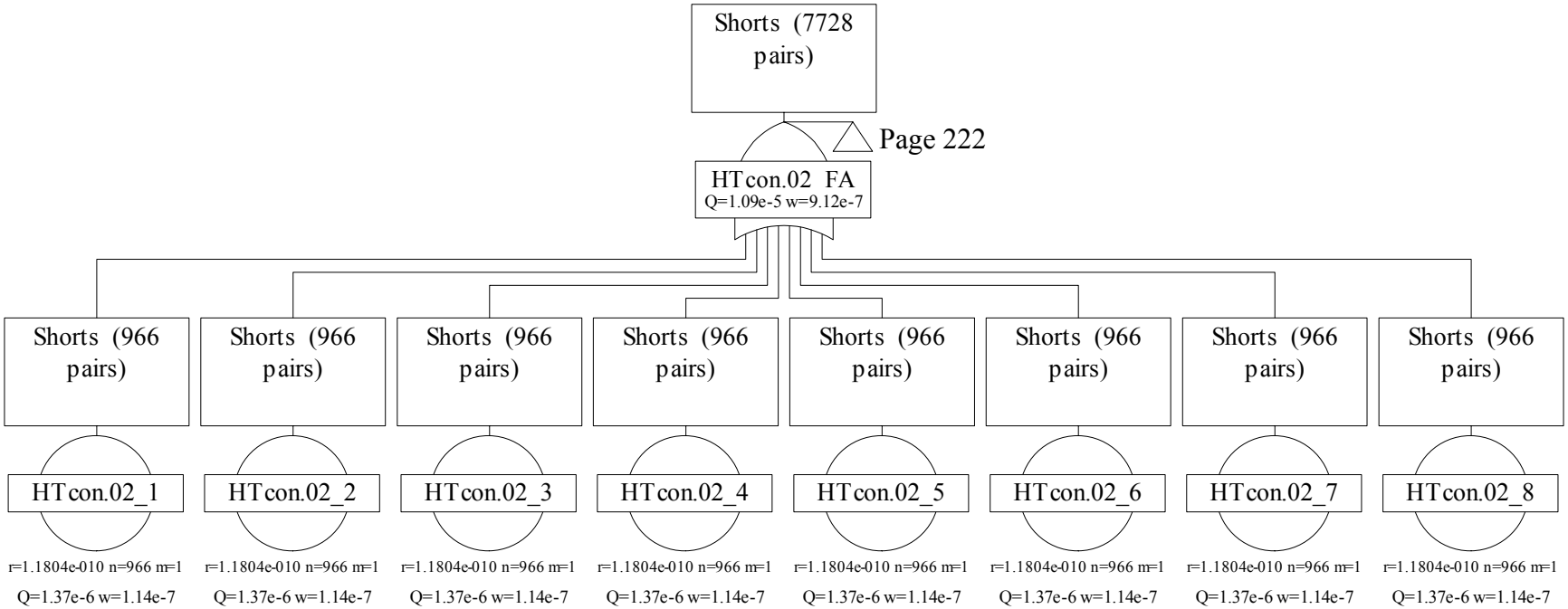

Straight Section PS False Alarm, Continuous check
Page 214
PSSS_FA_C
Q=0.0191 w=0.00158
Wrong alimentation in Straight Section +/-5V (564)
No alimentation in Straight Section +/-5V (564)
Wrong alimentation in Straight Section 2.5V (282)
No alimentation in Straight Section 2.5V (282)
PSHVwrong_FA_C
Q=0.00733 w=0.000608
PSHVno_FA_C
Q=0.00549 w=0.000456
PSLVwrong_FA_C
Q=0.00367 w=0.000305
PSLVno_FA_C
Q=0.00275 w=0.000229
Improper Output (564)
Improper Voltage (564)
Intermittent (564)
Subsystem Failure (564)
No output (564)
Shorted (564)
Improper Output (282)
Improper Voltage (282)
Intermittent (282)
Subsystem Failure (282)
No output (282)
Shorted (282)
PSSSHV.02_1
PSSSHV.03_1
PSSSHV.04_1
PSSSHV.06_1
PSSSHV.01_1
PSSSHV.05_1
PSSSLV.02_1
PSSSLV.03_1
PSSSLV.04_1
PSSSLV.06_1
PSSSLV.01
PSSSLV.05_1
r=4.617e-007 n=564 m=1
Q=0.00312 w=0.00026
r=2.66e-007 n=564 m=1
Q=0.0018 w=0.00015
r=2.375e-007 n=564 m=1
Q=0.00161 w=0.000134
r=1.216e-007 n=564 m=1
Q=0.000823 w=6.85e-5
r=6.536e-007 n=564 m=1
Q=0.00441 w=0.000367
r=1.596e-007 n=564 m=1
Q=0.00108 w=8.99e-5
r=4.617e-007 n=282 m=1
Q=0.00156 w=0.00013
r=2.66e-007 n=282 m=1
Q=0.0009 w=7.49e-5
r=2.375e-007 n=282 m=1
Q=0.000803 w=6.69e-5
r=1.216e-007 n=282 m=1
Q=0.000411 w=3.43e-5
r=6.536e-007 n=282 m=1
Q=0.00221 w=0.000184
r=1.596e-007 n=282 m=1
Q=0.00054 w=4.5e-5

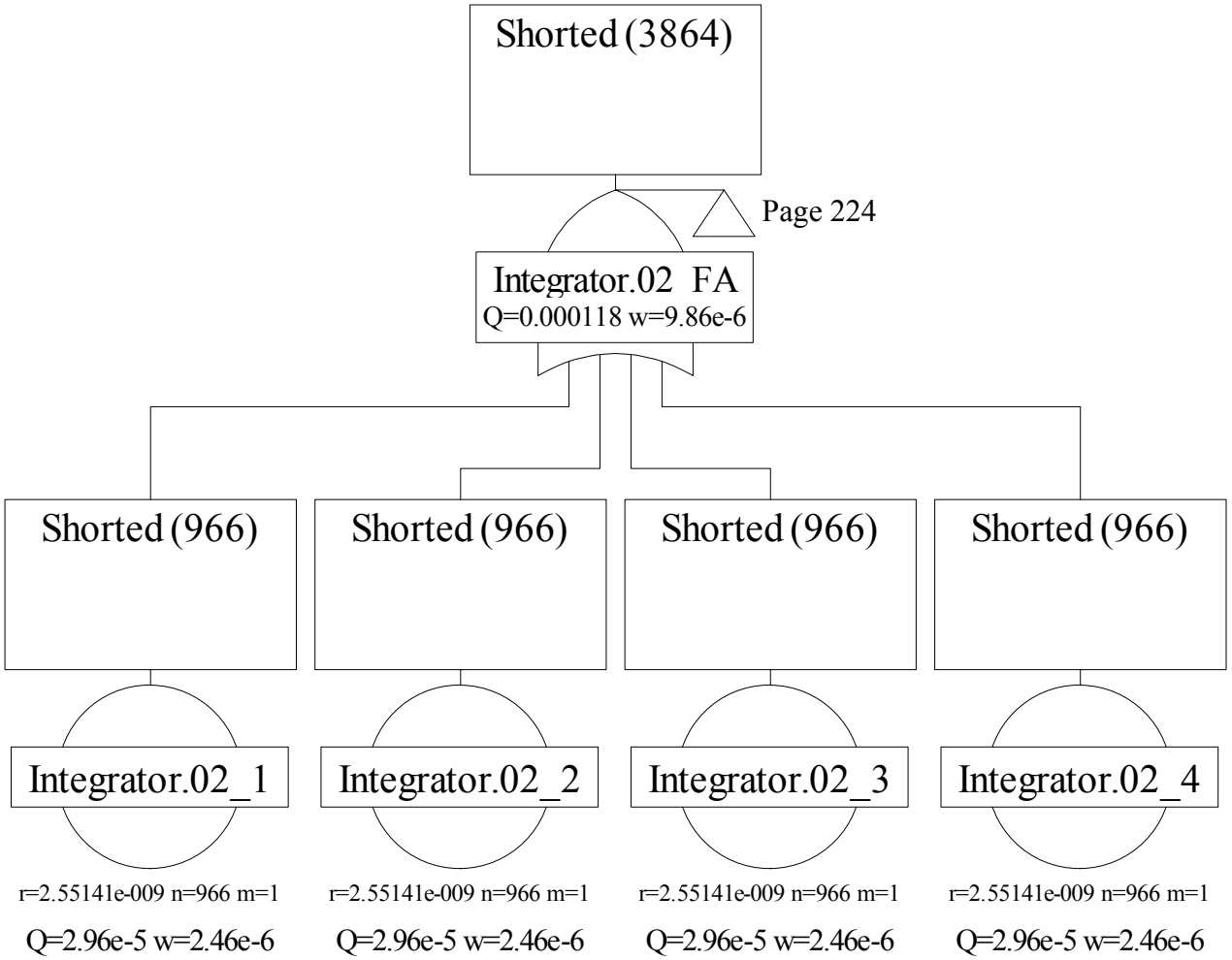

BackEnd electronic
False Alarm,
Continuous check
Page 214
BEE FA C
Q=8.58e-5 w=7.15e-6
FPGA dump
request (325)
Wrong
temperature
signal (325)
No Energy
signal (325)
FPGARX FA C
Q=6.42e-5 w=5.35e-6
Temperature_FA_C
Q=1.77e-5 w=1.48e-6
Transceiver_FA_C
Q=3.88e-6 w=3.24e-7
General failure
(325)
Internal error
(325)
Contamination
(325)
Failure Not
Verified (325)
Electrical
Failure (325)
Mechanical
Failure (325)
Opened (325)
Electrical
Overstressed
(325)
Shorted (325)
FPGARX.01
FPGARX.02
Temperature.03
Temperature.04
Transceiver.01
Transceiver.02
Transceiver.03
Transceiver.04
Transceiver.05
r=1.281e-008 n=325 m=1
Q=5e-5 w=4.16e-6
r=3.66e-009 n=325 m=1
Q=1.43e-5 w=1.19e-6
r=2.27034e-009 n=325 m=1
Q=8.85e-6 w=7.38e-7
r=2.27034e-009 n=325 m=1
Q=8.85e-6 w=7.38e-7
r=4.998e-010 n=325 m=1
Q=1.95e-6 w=1.62e-7
r=3.2232e-010 n=325 m=1
Q=1.26e-6 w=1.05e-7
r=8.466e-011 n=325 m=1
Q=3.3e-7 w=2.75e-8
r=5.916e-011 n=325 m=1
Q=2.31e-7 w=1.92e-8
r=2.958e-011 n=325 m=1
Q=1.15e-7 w=9.61e-9

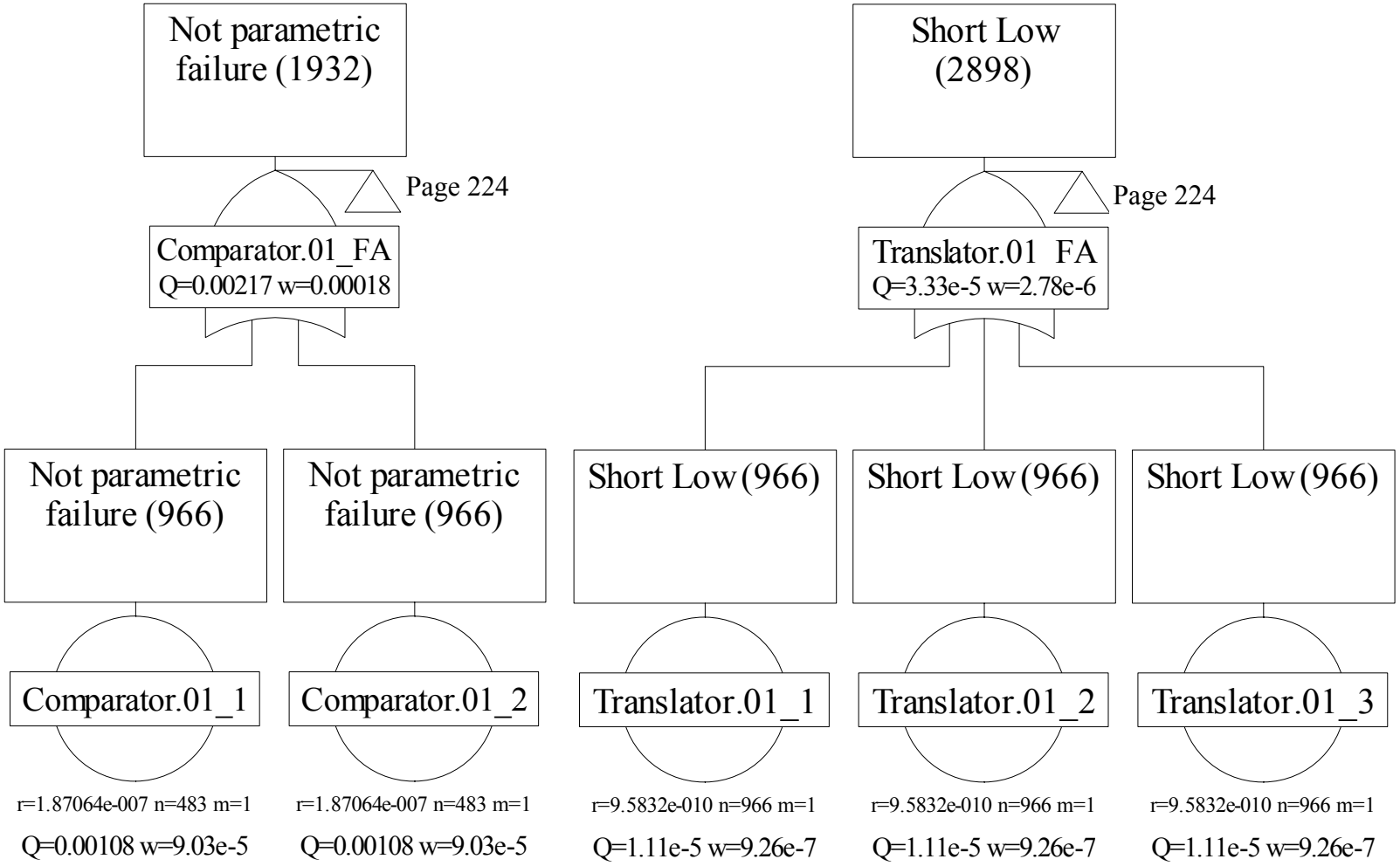

Crates electronics False Alarms, Continuous check
Page 214
Crate FA C
Q=5.47e-6 w=4.62e-7
False open (400)
False open (25)
No combiner FPGA (25)
No current loop (225)
HT Power supplies False Alarm(16)
False HT test from combiner (8)
BPswitch FA C
Q=1.01e-6 w=8.4e-8
CombBPin_FA_C
Q=5.33e-8 w=4.44e-9
CombFPGA_FA_C
Q=3.84e-6 w=3.2e-7
LBISswitch_FA_C
Q=4.9e-7 w=4.08e-8
PSHT FA C
Q=2.89e-9 w=5.78e-9
HTDAC FA C
Q=7.62e-8 w=6.35e-9
Electrical overstressed (400)
No Output (400)
Opened (400)
Not parametric failure(25)
General failure (25)
No output (225)
Opened (225)
Aluminum Corrosion (225)
Burned Out (225)
Power Supplies HT False Alarm, Continuous per point
Parametric failure (8)
BPswitch.01
BPswitch.02
BPswitch.03
Comb_BP_in.01
Combiner FPGA01
LBIS switch.01
LBIS switch.02
LBIS switch.03
LBIS switch.04
PSHT FA CP1
Q=3.61e10 w=7.22e10
PSHT FA CP2
PSHT FA CP3
PSHT FA CP4
PSHT FA CP5
PSHT FA CP6
PSHT FA CP7
PSHT FA CP8
HTDAC04
r=1.4e-010 n=400 m=1
Q=6.72e-7 w=5.6e-8
r=3.5e-011 n=400 m=1
Q=1.68e-7 w=1.4e-8
r=3.5e-011 n=400 m=1
Q=1.68e-7 w=1.4e-8
r=1.779e-010 n=25 m=1
Q=5.33e-8 w=4.44e-9
r=1.281e008 n=25 m=1
Q=3.84e-6 w=3.2e-7
r=2.304e-011 n=225 m=1
Q=1.96e-7 w=1.63e-8
r=2.304e-011 n=225 m=1
Q=1.96e-7 w=1.63e-8
r=4.835e-011 n=225 m=1
Q=4.9e-8 w=4.08e-9
r=4.835e-011 n=225 m=1
Q=4.9e-8 w=4.08e-9
r=7.940e-010 n=8 m=1
Q=7.62e-8 w=6.35e-9
Page
Structures similar to PSHT FA CP1

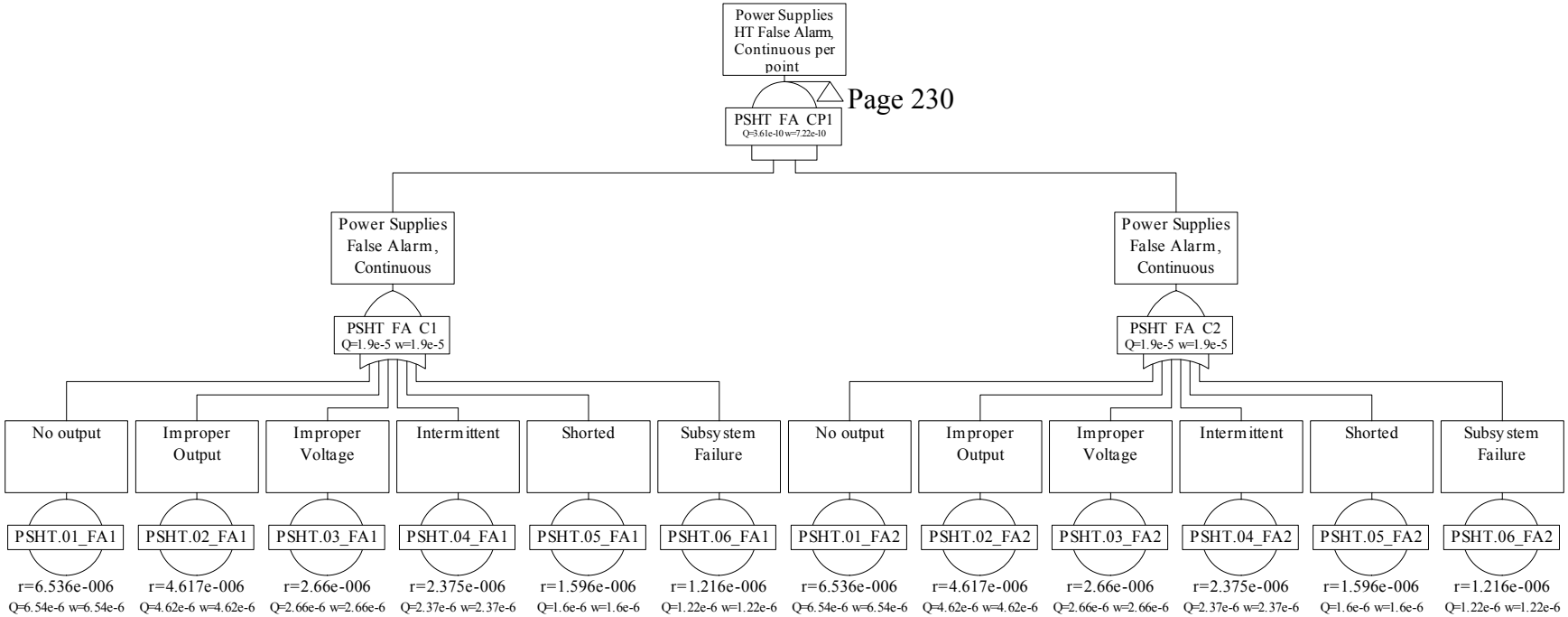

PS VME False Alarm, Continuous check
Page 214
PSVME_FA_C
Q=9.75e-9 w=1.95e-8
PS VME False Alarm in Point
PS VME False Alarm in Point
PS VME False Alarm in Point
PS VME False Alarm in Point
PS VME False Alarm in Point
PS VME False Alarm in Point
PS VME False Alarm in Point
PS VME False Alarm in Point
PSVME_FA_CP1
Q=1.08e-9 w=2.17e-9
PSVME_FA_CP2
Q=1.08e-9 w=2.17e-9
PSVME_FA_CP3
Q=1.08e-9 w=2.17e-9
PSVME_FA_CP4
Q=1.08e-9 w=2.17e-9
PSVME_FA_CP5
Q=1.08e-9 w=2.17e-9
PSVME_FA_CP6
Q=1.08e-9 w=2.17e-9
PSVME_FA_CP7
Q=2.17e-9 w=4.33e-9
PSVME_FA_CP8
Q=1.08e-9 w=2.17e-9
Page 237
Page 237
Structures similar to PSVME_FA_CP1
Similar to PSVME_FA_CP1

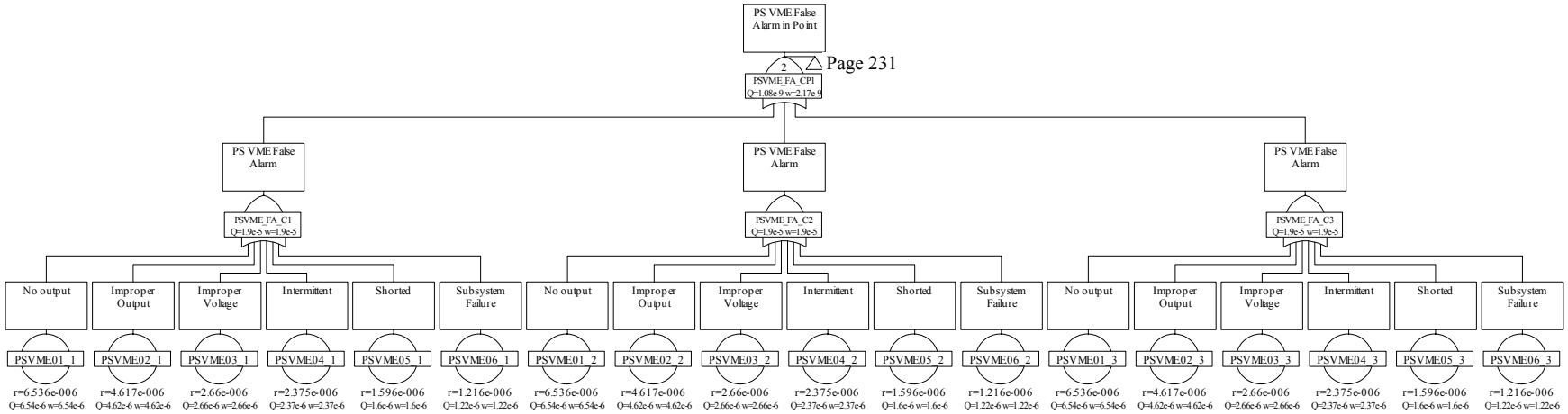

VME fantray False Alarm, Continuous check
Page 214
VMEfans FA_C
Q=0.00946 w=0.000784
No ventilation (25)
Low ventilation (25)
FantrayNo_FA_C
Q=0.00473 w=0.000393
FantrayLow_FA_C
Q=0.00475 w=0.000395
Mechanical Failure (25)
Blade erosion (25)
Out of Balance (25)
Switch failure (25)
Bearing Failure (25)
Sensor failure (25)
Fantray.02
Fantray.04
Fantray.05
Fantray.06
Fantray.01
Fantray.03
r=8.29754e-006 n=25 m=1
Q=0.00249 w=0.000207
r=3.00865e-006 n=25 m=1
Q=0.000902 w=7.51e-5
r=2.24857e-006 n=25 m=1
Q=0.000674 w=5.62e-5
r=2.24857e-006 n=25 m=1
Q=0.000674 w=5.62e-5
r=1.05778e-005 n=25 m=1
Q=0.00317 w=0.000264
r=5.28889e-006 n=25 m=1
Q=0.00159 w=0.000132

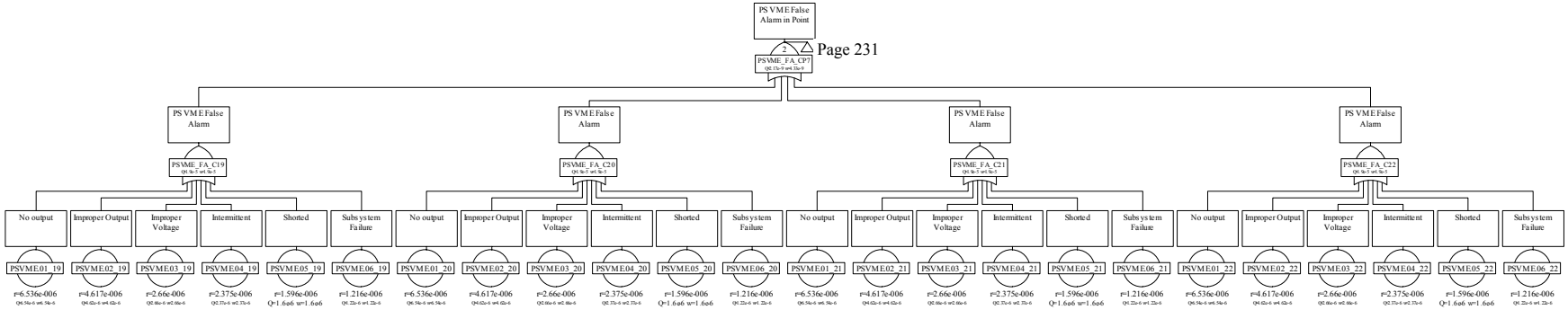

Shorts (7728 pairs)
Page 222
HTcon.02 FA
Q=1.09e-5 w=9.12e-7
Shorts (966 pairs)
Shorts (966 pairs)
Shorts (966 pairs)
Shorts (966 pairs)
Shorts (966 pairs)
Shorts (966 pairs)
Shorts (966 pairs)
Shorts (966 pairs)
HTcon.02_1
HTcon.02_2
HTcon.02_3
HTcon.02_4
HTcon.02_5
HTcon.02_6
HTcon.02_7
HTcon.02_8
r=1.1804e-010 n=966 m=1
Q=1.37e-6 w=1.14e-7

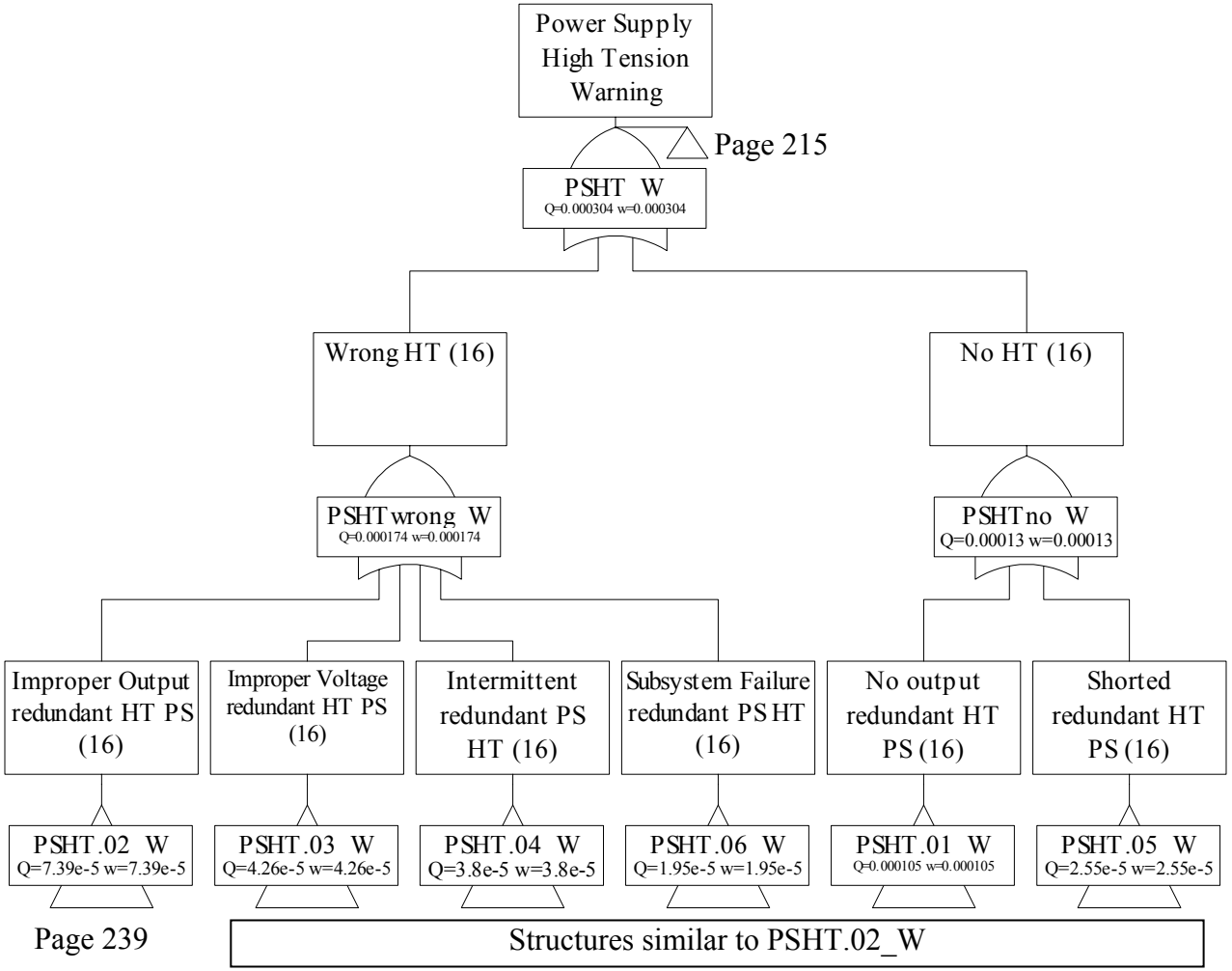

Shorted (3864)
Page 224
Integrator.02 FA
Q=0.000118 w=9.86e-6
Shorted (966)
Shorted (966)
Shorted (966)
Shorted (966)
Integrator.02_1
Integrator.02_2
Integrator.02_3
Integrator.02_4
r=2.55141e-009 n=966 m=1
Q=2.96e-5 w=2.46e-6
r=2.55141e-009 n=966 m=1
Q=2.96e-5 w=2.46e-6
r=2.55141e-009 n=966 m=1
Q=2.96e-5 w=2.46e-6
r=2.55141e-009 n=966 m=1
Q=2.96e-5 w=2.46e-6

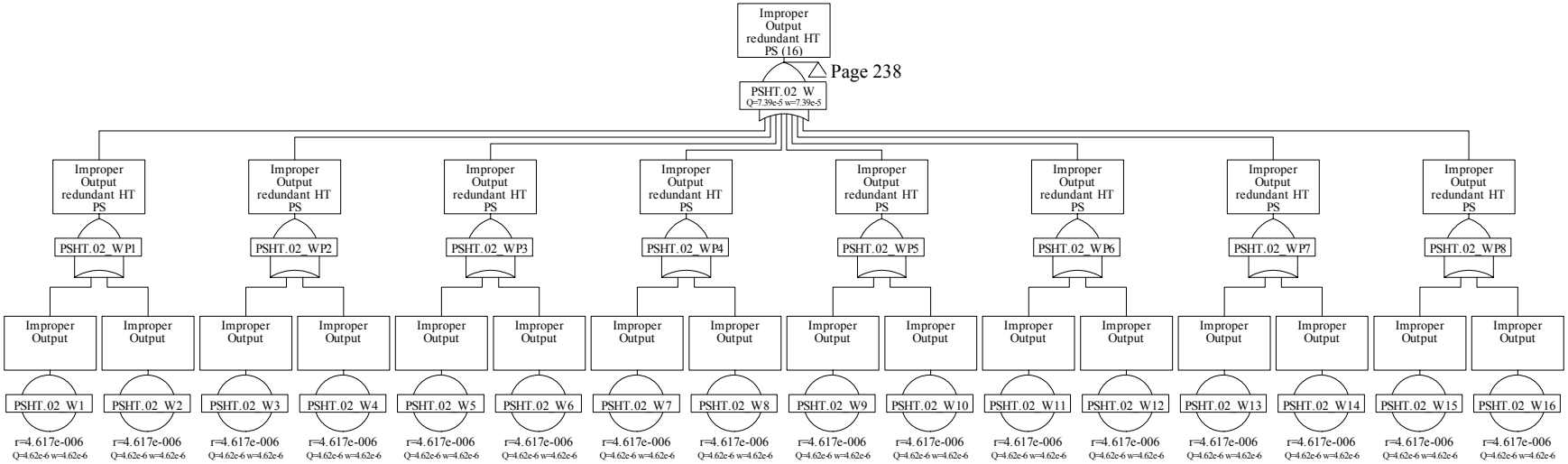

Not parametric failure (1932)
Page 224
Comparator.01_FA
Q=0.00217 w=0.00018
Not parametric failure (966)
Not parametric failure (966)
Comparator.01_1
Comparator.01_2
r=1.87064e-007 n=483 m=1
Q=0.00108 w=9.03e-5
r=1.87064e-007 n=483 m=1
Q=0.00108 w=9.03e-5
Short Low (2898)
Page 224
Translator.01 FA
Q=3.33e-5 w=2.78e-6
Short Low (966)
Short Low (966)
Short Low (966)
Translator.01_1
Translator.01_2
Translator.01_3
r=9.5832e-010 n=966 m=1
Q=1.11e-5 w=9.26e-7
r=9.5832e-010 n=966 m=1
Q=1.11e-5 w=9.26e-7
r=9.5832e-010 n=966 m=1
Q=1.11e-5 w=9.26e-7

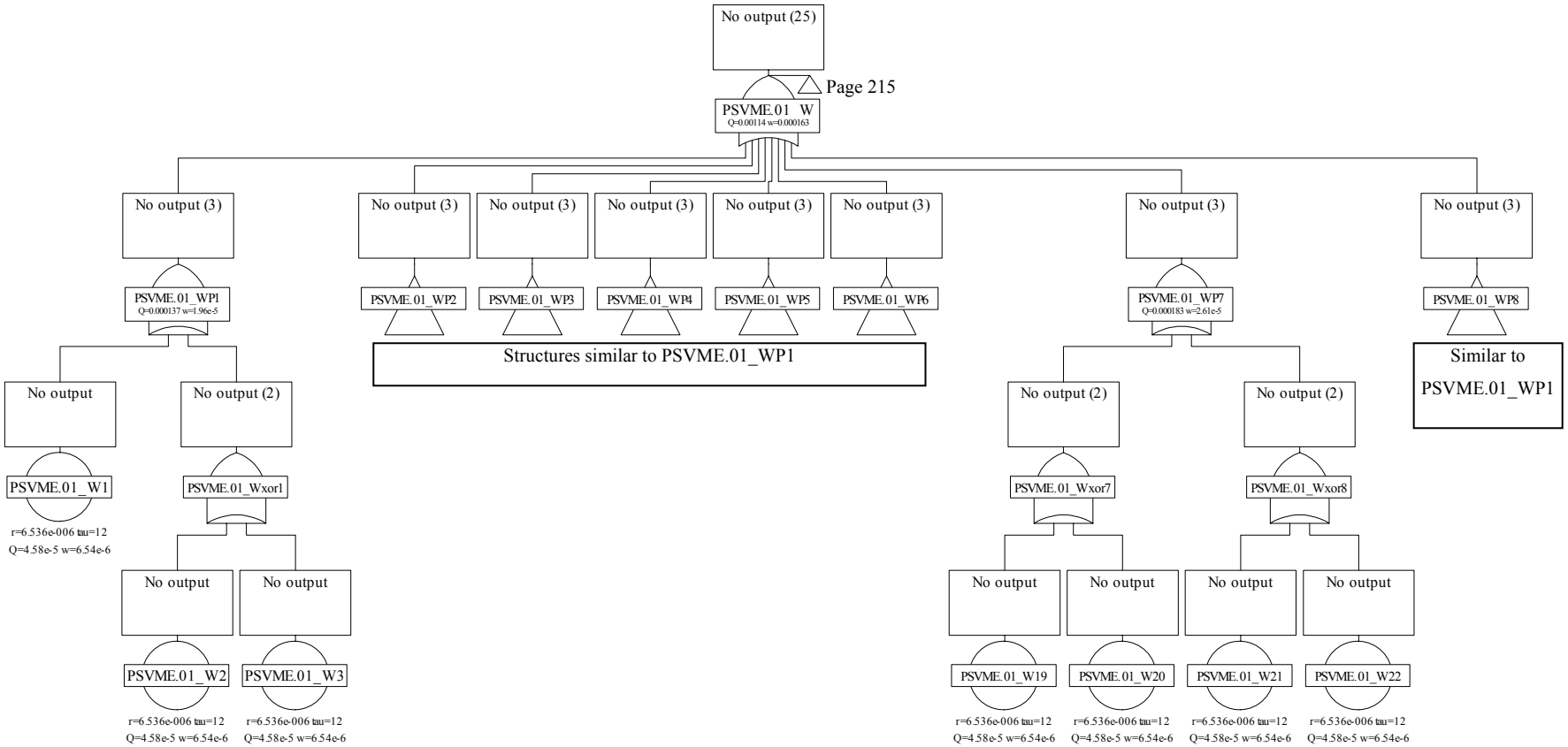

Power Supplies HT False Alarm, Continuous per point
Page 230
PSHT_FA_CP1
Q=3.61e-10 w=7.22e-10
Power Supplies False Alarm, Continuous
PSHT_FA_C1
Q=1.9e-5 w=1.9e-5
Power Supplies False Alarm, Continuous
PSHT_FA_C2
Q=1.9e-5 w=1.9e-5
No output
Improper Output
Improper Voltage
Intermittent
Shorted
Subsystem Failure
No output
Improper Output
Improper Voltage
Intermittent
Shorted
Subsystem Failure
PSHT.01_FA1
PSHT.02_FA1
PSHT.03_FA1
PSHT.04_FA1
PSHT.05_FA1
PSHT.06_FA1
PSHT.01_FA2
PSHT.02_FA2
PSHT.03_FA2
PSHT.04_FA2
PSHT.05_FA2
PSHT.06_FA2
r=6.536e-006
Q=6.54e-6 w=6.54e-6
r=4.617e-006
Q=4.62e-6 w=4.62e-6
r=2.66e-006
Q=2.66e-6 w=2.66e-6
r=2.375e-006
Q=2.37e-6 w=2.37e-6
r=1.596e-006
Q=1.6e-6 w=1.6e-6
r=1.216e-006
Q=1.22e-6 w=1.22e-6
r=6.536e-006
Q=6.54e-6 w=6.54e-6
r=4.617e-006
Q=4.62e-6 w=4.62e-6
r=2.66e-006
Q=2.66e-6 w=2.66e-6
r=2.375e-006
Q=2.37e-6 w=2.37e-6
r=1.596e-006
Q=1.6e-6 w=1.6e-6
r=1.216e-006
Q=1.22e-6 w=1.22e-6

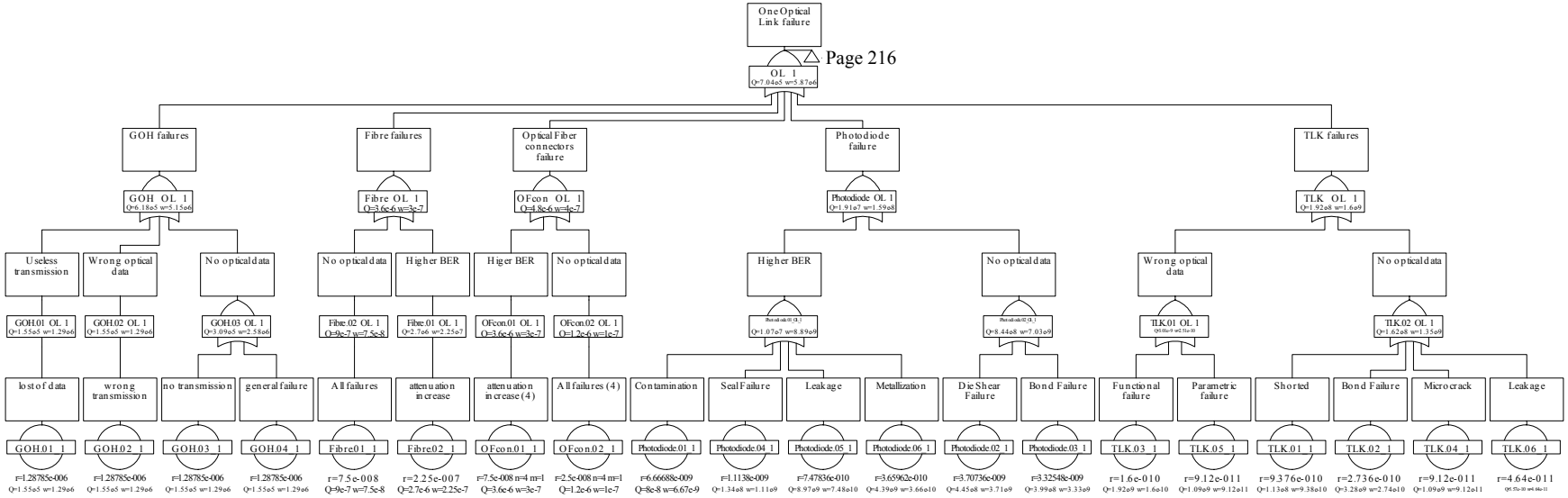

PS VME False Alarm in Point
2
Page 231
PSVME_FA_CP1
Q=1.08e-9 w=2.17e-9
PS VME False Alarm
PSVME_FA_C1
Q=1.9e-5 w=1.9e-5
PS VME False Alarm
PSVME_FA_C2
Q=1.9e-5 w=1.9e-5
PS VME False Alarm
PSVME_FA_C3
Q=1.9e-5 w=1.9e-5
No output
Improper Output
Improper Voltage
Intermittent
Shorted
Subsystem Failure
PSVME01_1
r=6.536e-006
Q=6.54e-6 w=6.54e-6
PSVME02_1
r=4.617e-006
Q=4.62e-6 w=4.62e-6
PSVME03_1
r=2.66e-006
Q=2.66e-6 w=2.66e-6
PSVME04_1
r=2.375e-006
Q=2.37e-6 w=2.37e-6
PSVME05_1
r=1.596e-006
Q=1.6e-6 w=1.6e-6
PSVME06_1
r=1.216e-006
Q=1.22e-6 w=1.22e-6
PSVME01_2
r=6.536e-006
Q=6.54e-6 w=6.54e-6
PSVME02_2
r=4.617e-006
Q=4.62e-6 w=4.62e-6
PSVME03_2
r=2.66e-006
Q=2.66e-6 w=2.66e-6
PSVME04_2
r=2.375e-006
Q=2.37e-6 w=2.37e-6
PSVME05_2
r=1.596e-006
Q=1.6e-6 w=1.6e-6
PSVME06_2
r=1.216e-006
Q=1.22e-6 w=1.22e-6
PSVME01_3
r=6.536e-006
Q=6.54e-6 w=6.54e-6
PSVME02_3
r=4.617e-006
Q=4.62e-6 w=4.62e-6
PSVME03_3
r=2.66e-006
Q=2.66e-6 w=2.66e-6
PSVME04_3
r=2.375e-006
Q=2.37e-6 w=2.37e-6
PSVME05_3
r=1.596e-006
Q=1.6e-6 w=1.6e-6
PSVME06_3
r=1.216e-006
Q=1.22e-6 w=1.22e-6


PS VME False Alarm in Point
2
Page 231
PSVME_FA_CP7
PS VME False Alarm
PSVME_FA_C19
PS VME False Alarm
PSVME_FA_C20
PS VME False Alarm
PSVME_FA_C21
PS VME False Alarm
PSVME_FA_C22
No output
Improper Output
Improper Voltage
Intermittent
Shorted
Subsystem Failure
PSVME01_19
PSVME02_19
PSVME03_19
PSVME04_19
PSVME05_19
PSVME06_19
PSVME01_20
PSVME02_20
PSVME03_20
PSVME04_20
PSVME05_20
PSVME06_20
PSVME01_21
PSVME02_21
PSVME03_21
PSVME04_21
PSVME05_21
PSVME06_21
PSVME01_22
PSVME02_22
PSVME03_22
PSVME04_22
PSVME05_22
PSVME06_22
r=6.536e-006
r=4.617e-006
r=2.66e-006
r=2.375e-006
r=1.596e-006
r=1.216e-006


Power Supply High Tension Warning
Page 215
PSHT W
Q=0.000304 w=0.000304
Wrong HT (16)
No HT (16)
PSHTwrong W
Q=0.000174 w=0.000174
PSHTno W
Q=0.00013 w=0.00013
Improper Output redundant HT PS (16)
Improper Voltage redundant HT PS (16)
Intermittent redundant PS HT (16)
Subsystem Failure redundant PS HT (16)
No output redundant HT PS (16)
Shorted redundant HT PS (16)
PSHT.02 W
Q=7.39e-5 w=7.39e-5
PSHT.03 W
Q=4.26e-5 w=4.26e-5
PSHT.04 W
Q=3.8e-5 w=3.8e-5
PSHT.06 W
Q=1.95e-5 w=1.95e-5
PSHT.01 W
Q=0.000105 w=0.000105
PSHT.05 W
Q=2.55e-5 w=2.55e-5
Page 239
Structures similar to PSHT.02_W


Improper Output redundant HT PS (16)
Page 238
PSHT.02_W
Q=7.39e-5 w=7.39e-5
Improper Output redundant HT PS
PSHT.02_WP1
PSHT.02_WP2
PSHT.02_WP3
PSHT.02_WP4
PSHT.02_WP5
PSHT.02_WP6
PSHT.02_WP7
PSHT.02_WP8
Improper Output
PSHT.02_W1
PSHT.02_W2
PSHT.02_W3
PSHT.02_W4
PSHT.02_W5
PSHT.02_W6
PSHT.02_W7
PSHT.02_W8
PSHT.02_W9
PSHT.02_W10
PSHT.02_W11
PSHT.02_W12
PSHT.02_W13
PSHT.02_W14
PSHT.02_W15
PSHT.02_W16
r=4.617e-006
Q=4.62e-6 w=4.62e-6


No output (25)
Page 215
PSVME.01_W
Q=0.00114 w=0.000163
No output (3)
No output (3)
No output (3)
No output (3)
No output (3)
No output (3)
No output (3)
No output (3)
PSVME.01_WP1
Q=0.000137 w=1.96e-5
PSVME.01_WP2
PSVME.01_WP3
PSVME.01_WP4
PSVME.01_WP5
PSVME.01_WP6
PSVME.01_WP7
Q=0.000183 w=2.61e-5
PSVME.01_WP8
Structures similar to PSVME.01_WP1
Similar to PSVME.01_WP1
No output
No output (2)
No output (2)
No output (2)
PSVME.01_W1
r=6.536e-006 tau=12
Q=4.58e-5 w=6.54e-6
PSVME.01_Wxor1
PSVME.01_Wxor7
PSVME.01_Wxor8
No output
No output
No output
No output
No output
No output
PSVME.01_W2
r=6.536e-006 tau=12
Q=4.58e-5 w=6.54e-6
PSVME.01_W3
r=6.536e-006 tau=12
Q=4.58e-5 w=6.54e-6
PSVME.01_W19
r=6.536e-006 tau=12
Q=4.58e-5 w=6.54e-6
PSVME.01_W20
r=6.536e-006 tau=12
Q=4.58e-5 w=6.54e-6
PSVME.01_W21
r=6.536e-006 tau=12
Q=4.58e-5 w=6.54e-6
PSVME.01_W22
r=6.536e-006 tau=12
Q=4.58e-5 w=6.54e-6


One Optical Link failure
Page 216
OL 1
Q=7.04e5 w=5.87e6
GOH failures
Fibre failures
Optical Fiber connectors failure
Photodiode failure
TLK failures
GOH OL 1
Q=6.18e5 w=5.15e6
Fibre OL 1
Q=3.6e-6 w=3e-7
OFcon OL 1
Q=4.8e-6 w=4e-7
Photodiode OL 1
Q=1.91e7 w=1.59e8
TLK OL 1
Q=1.92e8 w=1.6e9
Useless transmission
Wrong optical data
No optical data
No optical data
Higher BER
Higer BER
No optical data
Higher BER
No optical data
Wrong optical data
No optical data
GOH.01 OL 1
Q=1.55e5 w=1.29e6
GOH.02 OL 1
Q=1.55e5 w=1.29e6
GOH.03 OL 1
Q=3.09e5 w=2.58e6
Fibre.02 OL 1
Q=9e-7 w=7.5e-8
Fibre.01 OL 1
Q=2.7e6 w=2.25e7
OFcon.01 OL 1
Q=3.6e-6 w=3e-7
OFcon.02 OL 1
Q=1.2e-6 w=1e-7
Photodiode.01 OL 1
Q=1.07e7 w=8.89e9
Photodiode.02 OL 1
Q=8.44e8 w=7.03e9
TLK.01 OL 1
Q=1.6e-9 w=1.5e-10
TLK.02 OL 1
Q=1.62e8 w=1.35e9
lost of data
wrong transmission
no transmission
general failure
All failures
attenuation increase
attenuation increase (4)
All failures (4)
Contamination
Seal Failure
Leakage
Metallization
Die Shear Failure
Bond Failure
Functional failure
Parametric failure
Shorted
Bond Failure
Microcrack
Leakage
GOH.01_1
GOH.02_1
GOH.03_1
GOH.04_1
Fibre01_1
Fibre02_1
OFcon.01_1
OFcon.02_1
Photodiode.01_1
Photodiode.04_1
Photodiode.05_1
Photodiode.06_1
Photodiode.02_1
Photodiode.03_1
TLK.03_1
TLK.05_1
TLK.01_1
TLK.02_1
TLK.04_1
TLK.06_1
r=1.28785e-006
Q=1.55e5 w=1.29e6
r=1.28785e-006
Q=1.55e5 w=1.29e6
r=1.28785e-006
Q=1.55e5 w=1.29e6
r=1.28785e-006
Q=1.55e5 w=1.29e6
r=7.5e-008
Q=9e-7 w=7.5e-8
r=2.25e-007
Q=2.7e-6 w=2.25e-7
r=7.5e-008 n=4 m=1
Q=3.6e-6 w=3e-7
r=2.5e-008 n=4 m=1
Q=1.2e-6 w=1e-7
r=6.66688e-009
Q=8e-8 w=6.67e-9
r=1.1138e-009
Q=1.34e8 w=1.11e9
r=7.47836e-010
Q=8.97e9 w=7.48e10
r=3.65962e-010
Q=4.39e9 w=3.66e10
r=3.70736e-009
Q=4.45e8 w=3.71e9
r=3.32548e-009
Q=3.99e8 w=3.33e9
r=1.6e-010
Q=1.92e9 w=1.6e10
r=9.12e-011
Q=1.09e9 w=9.12e11
r=9.376e-010
Q=1.13e8 w=9.38e10
r=2.736e-010
Q=3.28e9 w=2.74e10
r=9.12e-011
Q=1.09e9 w=9.12e11
r=4.64e-011
Q=5.57e-10 w=4.64e-11

Numéro d'ordre : DU 1631 PCCF T 0509
EDSF : 473

UNIVERSITÉ CLERMONT FERRAND II – BLAISE PASCAL

T H È S E

pour obtenir le grade de

DOCTEUR DE L'UBP

Discipline : Physique des Particules

préparée au CERN/BDI/BL

dans la cadre de l'**École Doctorale des Sciences Fondamentales**

présentée et soutenue publiquement

par

Gianluca GUAGLIO

le 16 Décembre 2005

Reliability of the Beam Loss Monitors System for the Large Hadron Collider at CERN

Directeurs de thèse :

Claudio SANTONI

Bernd DEHNING

JURY

M. Pierre HENRARD, Président

M. Alain BALDIT

M. Marcel LIEUVIN

M. Paolo PIERINI

M. Rüdiger SCHMIDT

SUMMARY

The energy stored in the Large Hadron Collider is unprecedented. The impact of the beam particles can cause severe damage on the superconductive magnets, resulting in significant downtime for repairing. The Beam Loss Monitors System (BLMS) detects the secondary particles shower of the lost beam particles and initiates the extraction of the beam before any serious damage to the equipment can occur. This thesis defines the BLMS specifications in term of reliability. The main goal is the design of a system minimizing both the probability to not detect a dangerous loss and the number of false alarms generated. The reliability theory and techniques utilized are described. The prediction of the hazard rates, the testing procedures, the Failure Modes Effects and Criticalities Analysis and the Fault Tree Analysis have been used to provide an estimation of the probability to damage a magnet, of the number of false alarms and of the number of generated warnings. The weakest components in the BLMS have been pointed out. The reliability figures of the BLMS have been calculated using a commercial software package (Isograph™). The effect of the variation of the parameters on the obtained results has been evaluated with a sensitivity analysis. The reliability model has been extended by the results of radiation tests. Design improvements, like redundant optical transmission, have been implemented in an iterative process. The proposed system is compliant with the reliability requirements. The model uncertainties are given by the limited knowledge of the thresholds levels of the superconductive magnets and of the locations of the losses along the ring. The implemented model allows modifications of the system, following the measuring of the hazard rates during the LHC life. It can also provide reference numbers to other accelerators which will implement similar technologies.

RÉSUMÉ

L'énergie stockée dans le Large Hadron Collider est sans précédent. La perte des particules du faisceau peut endommager gravement les aimants supraconducteurs, ayant pour résultat des temps significatifs d'arrêt pour la réparation. Le système des moniteurs de pertes du faisceau (en anglais: BLMS) détecte les gerbes de particules secondaires créées par les pertes faisceau et provoque l'extraction du faisceau avant que des dommages sérieux de l'équipement ne puissent se produire. Cette thèse définit les caractéristiques du BLMS en termes de la fiabilité. Le but principal est la conception d'un système réduisant au minimum soit la probabilité de ne pas détecter une perte dangereuse, soit le nombre de fausses alarmes produites. La théorie et les techniques de fiabilité utilisées sont décrites. La Prédiction de fiabilité, Analyse des Modes de Défaillance de leurs Effets et de leur Criticité (en anglais: FMECA), et l'Analyse par Arbre de Défaillance ont été employées pour fournir une évaluation de la probabilité d'endommager un aimant, du nombre de fausses alarmes et du nombre d'avertissements produits. Les composants les plus faibles dans le BLMS ont été précisés. Les chiffres de fiabilité du BLMS ont été calculés en utilisant un logiciel commercial (Isograph™). L'effet de la variation des paramètres sur les résultats obtenus a été évalué avec une Analyse de Sensibilité. Le modèle de fiabilité a été complété par les résultats des tests d'irradiation. Des améliorations de la conception du système, comme la transmission optique redondante, ont été mises en application grâce à un processus itératif. Le système proposé est conforme aux requêtes de fiabilité. Les incertitudes du modèle proviennent de la connaissance limitée des niveaux de seuils des aimants supraconducteurs et de la localisation des pertes autour de l'anneau. Le modèle mis en œuvre permet des modifications du système, suivant la mesure des taux de risque pendant la durée de vie du LHC. Il peut également fournir des valeurs de référence à d'autres accélérateurs qui mettront en application des technologies semblables.

MOTS-CLÉS

LHC	Faisceau de particules	Moniteurs des pertes de faisceau
Prédiction de fiabilité	Arbre de Défaillance	Analyse de Sensibilité
AMDEC	FMECA	Maintenabilité
Disponibilité	Risque	Sûreté de fonctionnement
Sécurité	Diagnostique	Aimants supraconducteurs

SPECIALITÉ

Physique des Particules

INTITULES ET ADRESSES DES LABORATOIRES

Université Blaise Pascal- Clermont Ferrand II
34 Avenue Carnot- 63000 Clermont-Ferrand
France

CERN AB/BDI/BL
Genève 23 CH-1211
Suisse