UNI STUTTGART

Berichte aus dem
Institut für Maschinenelemente
Antriebs-, Dichtungs-, Schienenfahrzeug- u. Zuverlässigkeitstechnik

Volker Schramm

Dependable System Development Methodology and Case Study for the LHC Beam Loss Monitoring System at CERN

Bericht Nr. 197

D 93
ISBN 978-3-936100-98-3

Institut für Maschinenelemente
Antriebs-, Dichtungs-, Schienenfahrzeug- u. Zuverlässigkeitstechnik

Universität Stuttgart
Pfaffenwaldring 9
70569 Stuttgart
Tel. (0711) 685 – 66170

Prof. Dr.-Ing. B. Bertsche, Ordinarius und Direktor

Dependable System Development Methodology and Case Study for the LHC Beam Loss Monitoring System at CERN

Von der Fakultät Konstruktions-, Produktions- und Fahrzeugtechnik
der Universität Stuttgart
zur Erlangung der Würde eines Doktor-Ingenieurs (Dr.-Ing.) genehmigte Abhandlung

Vorgelegt von

Volker Schramm M.Sc.

aus Welzheim

Hauptberichter:	Prof. Dr.-Ing. Bernd Bertsche
Mitberichter:	Hon.-Prof. Dr. rer. nat. Rüdiger Schmidt
Tag der mündlichen Prüfung:	23.02.2021

Institut für Maschinenelemente der Universität Stuttgart

2021

Para Tenar 

Por supuesto !

Abstract

The Beam Loss Monitoring system acts as a protection system of the Large Hadron Collider at CERN. Its primarily ionisation detectors measure potential off-orbit particles escaping from their trajectory. Its dependable performance is of utmost interest for the operation of the collider. This primarily involves constantly protecting the machine by initiating a safe beam extraction in case of dangerous particle losses. Secondary, the system has been designed in a fail-safe architecture to always favour the safe beam extraction in order to avoid any situation comprising the risk of missing dangerous loss. Therefore, the system comprises the potential to optimise its performance, *i.e.* minimise its impact on the collider performance, by reducing the number of false beam extractions whilst maintaining its protection function.

This work analyses the system architecture and protection strategy of the Beam Loss Monitoring system by reviewing a dependability model previously created during its design phase. Furthermore, the thesis investigates newly available performance data, remodels the current hardware configuration comprehensively bottom-up, and, based on this model, performs a Failure Mode, Effects, and Criticality Analysis in order to evaluate the dependable hardware design and review the protection function of the system.

Making use of the applied methodology, in particular of the retrospectively performed analysis and the available performance data of the system operating since a decade, a methodology for dependable development and operation during the entire life cycle of systems is presented. Based on the experience gathered with a beam instrumentation system, the methodology is tailored to such accelerator systems characterised by their high functional as well as dependability requirements, large modularity and critical operation during long lifetimes in harsh environments. In five defined life cycle phases and several iterative sub-phases, dependability requirements are derived and specified, designed into the system, reviewed by according analysis methods, and validated by tests. Furthermore, the methodology covers the system installation, commissioning and dependability support during operation up to the decommissioning and potential upgrade and refurbishment to reuse the system or parts of it. The entire methodology is designed as a continuous cycle within these phases to be applied to different development projects, profiting from previous projects and operational systems. In this way, it steadily grows and enhances the dependability capability of an organisation. Therefore, a comprehensive

and holistic framework for dependability application during all these phases is provided, enabling the methodology to be adjusted to the specific design project. The steady improvement of the dependability capability is established by an ever growing base of dependability data from tests, operation and decommissioning of previous systems. Furthermore, this base comprises experience gathered whilst applying and enhancing the presented design analyses, improving production and handling procedures, as well as from the operational and maintenance support of the operational systems.

In a subsequently performed case study of a Beam Loss Monitoring system processing board upgrade the methodology was applied. The study entirely covers the planning and design, production and testing phases of the life cycle, as well as makes use of operational, failure and repair data of the predecessor module, hence the two remaining life cycle phases. Furthermore, considerations for the upcoming system installation and operation are described. Initially defined dependability specifications for the system influenced the design and the execution of associated dependability analysis methods, which led to defining specifications for the production and accompanying it by several tests and inspections. The output of the analyses during the planning and design phase also led to the integration and following execution of according functional and environmental validation tests for the later system application and its operational environment. Furthermore, the entire production was screened for early life failures and the reliability requirements were demonstrated by tests. Hence, the application of the developed methodology within the case study was successful in meeting the study's objective to provide feedback to the overall procedure. This enabled to adjust the methodology and to validate it as it is presented in this work.

Kurzfassung

Methodik zur zuverlässigen Systementwicklung und Fallstudie für das LHC Beam Loss Monitoring System am CERN

Das Beam Loss Monitoring System fungiert als Schutzsystem des Large Hadron Colliders. Primär durch Ionisationsdetektoren erfasst es potentiell verlorene Teilchen des Speicherrings, die ihre Sollumlaufbahn innerhalb ihres vorgegebenen Orbits verlassen. Das zuverlässige Funktionieren des Schutzsystems ist von höchstem Interesse, um den Betrieb des Speicherrings zu gewährleisten. In erster Linie betrifft das den ständigen Schutz der Maschine, indem im Falle von gefährlichen Strahlverlustwerten eine sichere Extraktion der Teilchen aus den beiden Ringen initiiert wird. Zusätzlich wurde das System in einer "Fail-Safe"-Architektur entworfen, um im Falle eines bestehenden Risikos gefährlichen Strahlverlust nicht zu erfassen, immer die sichere Strahlextraktion zu bevorzugen. Aus diesen Gründen beherbergt das System das Optimierungspotential, seinen Einfluss auf den Speicherringbetrieb zu minimieren, indem die Anzahl fälschlicherweise durchgeführter Strahlextraktionen reduziert wird, währenddessen es seine Schutzfunktion erhält.

Die vorliegende Arbeit analysiert die Systemarchitektur und Schutzstrategie des Beam Loss Monitoring Systems, indem es ein bisheriges Zuverlässigkeitsmodell untersucht, welches während seiner Entwicklungsphase erstellt wurde. Außerdem untersucht die Thesis nun verfügbare Betriebsdaten, remodelliert die aktuelle Hardwarekonfiguration umfassend "bottom-up" und führt auf der Grundlage dieses Modells eine "Failure Mode, Effects, and Criticality Analysis" durch um die Zuverlässigkeit des Hardwaredesigns zu bewerten und die Schutzfunktion des Systems zu überprüfen.

Unter Zuhilfenahme der angewandten Methodik, insbesondere durch die rückwirkend durchgeführte Analyse und die Auswertung der verfügbaren Betriebsdaten des seit einer Dekade betriebenen Systems, wird eine Methodik zur zuverlässigen Entwicklung und zum Betrieb von Systemen während des gesamten Lebenszyklus präsentiert. Durch die gesammelte Erfahrung mit einem Strahlinstrumentierungssystem ist die Methodik auf solche Beschleunigersysteme zugeschnitten, die durch ihre hohen funktionalen, sowie Zuverlässigkeitsanforderungen, ebenso wie durch hohe Modularität und den kritischen Betrieb während langer Lebensdauern in rauen Umgebungen charakterisiert sind. In fünf definierten Lebenszyklusphasen und mehreren iterativen Unterphasen werden

Zuverlässigkeitsanforderungen hergeleitet und festgelegt, in das System hineinentwickelt, durch entsprechende Methoden analysiert und durch Erprobungen validiert. Außerdem wird die Systeminstallation, Inbetriebnahme und die zuverlässigkeitstechnische Systembetreuung während des Betriebs bis hin zur Außerbetriebnahme abgedeckt, welche mit potentiellen Upgrades oder einer Instandsetzung des Systems, oder Teilen davon, zur Wiederverwendung verbunden ist. Die gesamte Methodik ist als kontinuierlicher Zyklus innerhalb dieser Phasen konzipiert und anwendbar für verschiedene Entwicklungsprojekte, die jeweils von vorherigen Projekten und dem Betrieb anderer Systeme profitieren. Auf diese Weise wächst die Methodik ständig und steigert so das Zuverlässigkeitspotential einer Organisation. Aus diesem Grund wird ein umfangreicher und ganzheitlicher Rahmen für die Zuverlässigkeitsanwendung während aller Lebenszyklusphasen bereitgestellt, der es ermöglicht die Methodik für das konkrete Entwicklungsprojekt anzupassen. Die Steigerung des Zuverlässigkeitspotentials wird durch eine sich ständig erweiternde Datenbasis aus Zuverlässigkeitsdaten von Tests, dem Betrieb und der Außerbetriebnahme voriger Systeme erreicht. Außerdem beinhaltet diese Basis gesammelte Erfahrungen aus der Anwendung und Weiterentwicklung der präsentierten Analysemethoden, der Verbesserung von Produktionsverfahren und Handhabung, sowie aus der Betriebs- und Wartungsbetreuung.

In einer im Anschluss durchgeführten Fallstudie eines Verarbeitungsmodulupgrades des Beam Loss Monitoring Systems wurde die Methodik angewandt. Die Studie deckt die Planungs- und Design-, Produktions- und Testphasen vollständig ab und bezieht außerdem Betriebs-, Ausfall- und Reparaturdaten des Vorgängermoduls und dementsprechend die verbleibenden Lebenszyklusphasen mit ein. Des Weiteren werden Aspekte für die bevorstehende Systeminstallation und den Betrieb beschrieben. Zu Beginn definierte Zuverlässigkeitsanforderungen beeinflussten das Design und die Durchführung damit verbundener Analysemethoden, woraus Produktionsanforderungen und begleitende Tests und Inspektionen abgeleitet wurden. Das Ergebnis der Analysen während der Planungs- und Designphase führte außerdem zu der Definition und darauffolgenden Durchführung dementsprechender Funktions- und Umweltvalidierungstests für die spätere Systemanwendung in der Betriebsumgebung. Außerdem wurde die gesamte Produktion einem Frühausfallscreening unterzogen und die Zuverlässigkeitsanforderungen wurden durch Tests nachgewiesen. Infolgedessen wurde die entwickelte Methodik erfolgreich innerhalb der Fallstudie angewandt und das erlangte Feedback für die Vorgehensweise erfüllte die Zielsetzung. Dies ermöglichte es die in dieser Arbeit präsentierte Methodik anzupassen und zu validieren.

Table of Contents

Acknowledgements

This thesis was written during my time at CERN supported by the Wolfgang Gentner scholarship and as scientific staff at the Institute of Machine Components (IMA) of the University of Stuttgart.

I would like to start expressing my gratitude to a very special person I met only once before starting to work at CERN. Sadly, Dr. Bernd Dehning passed away before the completion of this work. In his obituary, CERN refers to him as "'the expert' on beam loss monitoring". Having had the opportunity to meet him personally and to prepare my PhD project at CERN together, the results of his work constantly came across my daily work on the LHC Beam Loss Monitoring system, a dependably working system based on an impressive design he and his team developed.

I would like to express the same gratitude to Dr. Christos Zamantzas, Prof. Dr.-Ing. Bernd Bertsche and William Viganò. From my first day in the section, Christos agreed to supervise my work at CERN although he was very busy taking over the section leadership. Being gifted with an impressive knowledge about accelerator technology and electronics, in particular about beam loss monitoring, he was always available literally next doors to answer the many questions I had. I would like to emphasise his support beyond his excellent technological and academic assistance. He would spend time with me reviewing my presentations and giving me practical advice on how to present our work in front of the accelerator community. He would also remind me countlessly to leave the office at late hours and to continue the next day, even if he would then stay himself many extra hours discussing my questions.

I would like to thank Prof. Dr.-Ing. Bernd Bertsche for my now ten-year-long experience at the IMA starting off with his lecture on "Konstruktionslehre I" in 2010. It tells its own story that I never thought about changing to any other institute during the entire period, bit by bit discovering my passion for dependability engineering. First meeting in person during my Bachelor thesis in 2013 I wrote a research project in 2015 already at CERN as well as my Master thesis in 2016, all supervised by him in a very professional and fair atmosphere. This collaboration continued whilst supervising my doctorate and during its final six months I had the opportunity to, again, work literally next door at the IMA.

William was one of the first people I met when starting at CERN in 2014. My section back then in the power converters group contacted him straight after I begun in order to consult CERN's dependability expert. He was also the one I first got in

touch before starting my doctoral studentship in the BL section. Then, during these three years he has been the one constantly being there for me, showing me the installations and working together in the laboratories. I profited incredibly from his practical experience on electronics' dependability which he gathered during his career in the automotive industry, working on-site for NASA and for many other projects. And yes, he is even gifted with biological knowledge, having sent scorpions into space (more correctly being involved in such a project). Thank you very much for your support and your time, professionally, as well as privately.

In addition, I would like to thank Prof. Dr. Rüdiger Schmidt for agreeing to be the co-examiner of my thesis and for the critical review of it.

Because there haven't only been Christos and William, I would like to thank all my colleagues in the BL section for forming the greatest team to work with. Each one contributed a lot to this thesis, and everyone has always been helpful, creating this pleasant work atmosphere I enjoyed working in. Unfortunately, I cannot mention all personally, but I name a few. Thanks a lot to Simon Eitelbuß and Lorenzo Stefanini, who contributed a lot to this work performing the entire VFC-HD test campaign solving all arising difficulties. Equally, my acknowledgements to Mathieu Saccani, who did an exceptional job writing the test firmware and debugging the test bench besides always being available to help us when we faced problems. And since a test bench does not only consist of the electronics, I want to express the same appreciation to Magdalena A. Stachon, James O. Robinson and Manuel Gonzalez Berges for configuring the software and doing an incredible job to provide us with a test application. This is also to be extended for the support received from Manoel Barros Marin, Andrea Boccardi and Tom Levens about the End-of-Line test bench and the VFC-HD design. At last but not the least, I would like to thank Ewald Effinger for always helping out and for keeping me in shape during our lunch-break sports.

Within the collaboration of CERN and the IMA, I was fortunate to also have colleagues in Stuttgart. I really enjoyed meeting all once per year at the Söllerhaus seminar and then working those six months together. Thanks for the fruitful discussions we had and the support I received from all of you. In particular I would like to thank Thomas Herzig for his support of the collaboration, Andreas Ostertag for the support in our common office and both Tamer Tevetoglu and Martin Dazer for the continuous support and for reviewing my thesis. Thanks to all "IMAner" for finding many new friends.

Finally, I would like to thank my family for always having been there for me. Mama, Papa, Franzi and Timo thank you for all you have done for me. And for its currency, thanks to Tati and Timo for enlarging the family, soon making me a first-time uncle. Of course, I cannot forget mentioning Tenar, the most special person in my life and my rock during all these times together with my Spanish family. Belén, Asia, all aunts and uncles, and the myriad of cousins, I love you all.

List of Figures

List of Tables

List of Symbols and Indices

Latin Symbols

A	Cross section of the particle beams
$A(t)$	Availability function
AF	Acceleration Factor
b	Weibull/Gamma distribution shape parameter; Fatigue exponent
B	Voltage acceleration parameter
c	Speed of light
C	Confidence level
D	Detection probability of a failure cause
e	Electron
E	Energy
f	Frequency
$f(t)$	Failure density function (Probability density function)
$F(t)$	Probability of failure function
G	Acceleration
$h(t)$	Hazard function
I	Electric current
k	Boltzmann constant
$\mathcal{L}$	Luminosity
L	Stress level
m	Mass; Humidity power constant
$MTBF$	Mean Time Between Failure
$MTTF$	Mean Time To Failure
$MTTR$	Mean Time To Repair
n_x	number of index x
N_x	Number of index x

r	Number of failures
O	Occurrence probability of a failure mode
P	Electric power
$Q(t)$	Unavailability function
R	Temperature range
$R(t)$	Reliability function
RH	Relative Humidity
RPN	Risk Priority Number
S	Severity of a failure effect
SS	Screening Strength
t	Time
T	Temperature; Characteristic life
V	Voltage
$Var(x)$	Variance
$\bar{x}$	Mean value

Greek Symbols

α	Acceptable risk of error (Chi-Square distribution)
β	Weibull/Gamma distribution shape parameter
γ	Relativistic factor; Failure-free time
$\Gamma( )$	Gamma function
Δ	Difference
η	Characteristic life
θ	Exponential mean
$\lambda(t)$	Failure rate function
μ	Repair rate
ν	Degrees of freedom
π_x	Pi-factor (Reliability prediction methods)
ν	Number of degrees of freedom (Chi-Square distribution)
σ	Standard deviation

χ	Chi-Square distribution (χ^2)

Indices

0	Rest energy; Failure-free time; Basic failure rate
A	Activation
acc	Accumulated
amb	Ambient
b	Base failure rate; Bunch
c	Cycling
cc	Common collector
cy	Cycles
diss	Dissipation
i	i^{th} term; induced
int	Integrated
j	Junction
kin	Kinetic
max	Maximal
n	n^{th} term
o	Operational
p	Part
P	System failure rate
r	Run
rev	Revolution
RMS	Root mean square
S	System
sj	Solder joint
SS	Steady state
T	Temperature; Transition frequency
ta	Turnaround
TC	Temperature cycling

Glossary of Terms, Acronyms and Abbreviations

ADC	Analog-to-Digital Converter
AFT	Accelerator Fault Tracking
ALICE	A Large Ion Collider Experiment
ALT	Accelerated Life Testing
APP	APPlication
ASIC	Application-Specific Integrated Circuit
ASIL	Automotive Safety Integrity Level
ATLAS	A Large Toroidal LHC ApparatuS
BE	Back End
BET	Beam Energy Tracker
BGA	Ball Grid Array
BI	Beam Instrumentation
BIC	Beam Interlock Controller
BIS	Beam Interlock System
BIT	Built-In Test
BLE	Beam Loss Electronics
BLECF	Beam Loss Electronics Current-to-Frequency converter module
BLECS	Beam Loss Electronics Combiner and Survey module
BLETC	Beam Loss Electronics Threshold Comparator module
BLM	Beam Loss Monitoring
BOBR	Beam OBservation Receiver
BoM	Bill of Materials
BPM	Beam Position Monitor
BST	Beam Synchronous Timing
C	Capacitor

CA	Criticality Analysis
CALCE	Center for Advanced Life Cycle Engineering
CERN	Conseil Européenne pour la Recherche Nucléaire (European Organization for Nuclear Research)
CFC	Current-to-Frequency Conversion
CHF	Confoederatio Helvetica Franc (swiss currency)
CIBUS	Controls Interlocks Beam User Single
CISV	Safe Machine Parameters VME Receiver
CMS	Compact Muon Solenoid
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CTRV	Controls Timing Receiver VME
DAB64x	Digital Acquisition Board (Versa Module Eurocard 64x)
DAC	Digital-to-Analog Converter
DC	Direct Current
DDR3	Double Data Rate 3
DFMEA	Design Failure Mode and Effects Analysis
DfR	Design for Reliability
DUT	Device Under Test
E/E	Electrical/Electronic
EAM	Enterprise Asset Management
EDMS	Engineering Data Management System (CERN)
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMI	ElectroMagnetic Interference
EN	European Norm
EPCQ	Quad-Serial Configuration (In-system programmable NOR flash memory)
ESD	ElectroStatic Discharge
ESS	Environmental Stress Screening

ETH	Ethernet
FE	Front End
FID	Frame IDentifier
FIT	Failure In Time
FMC	FPGA Mezzanine Card
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FPGA	Field-Programmable Gate Array
fp(m)h	failures per (million) hour(s)
FRACAS	Failure Reporting, Analysis and Corrective Action System
FTA	Fault Tree Analysis
GOH	GOL Opto-Hybrid
GOL	Gigabit Optical Link
GPIO	General Purpose Input/Output
GUI	Graphical User Interface
HL-LHC	High-Luminosity Large Hadron Collider
HPC	High Pin Count
HSSL	High Speed Serial Link
HTOL	High Temperature Operating Life
HV PSU	High Voltage Power Supply Unit
I^2C	Inter-Integrated Circuit (serial data bus on VFC-HD board)
IC	Integrated Circuit
ID	IDentifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPC	Association Connecting Electronics Industries (former Institute of Printed Circuits)
ISO	International Organization for Standardization
JTAG	Joint Test Action Group (standard connector on VFC-HD board)

LB	LoopBack
LBDS	LHC Beam Dumping System
LE	Logic Element
LED	Light-Emitting Diode
LEIR	Low Energy Ion Ring
LEP	Large Electron-Positron Collider
LHC	Large Hadron Collider
LHCb	Large Hadron Collider beauty
LINAC	LINear ACcelerator
LIC	Little Ionisation Chamber
LS	Long Shutdown
LSA	LHC Software Architecture
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MPS	LHC Machine Protection System
MTF	Manufacturing and Test Folder (CERN)
NASA	National Aeronautics and Space Administration
OSC	Oscillator
Pb	*Plumbum* (latin)
PB	Push-Button circuit (VFC-HD board)
PCB	Printed Circuit Board
PFMEA	Process Failure Mode and Effects Analysis
PIC	Powering Interlock Controller
PHM	Prognostics and Health Management
PoF	Physics-of-Failure
PS	Proton Synchrotron
PSB	Proton Synchrotron Booster
PSU	Power Supply Unit
PTH	Plated Through-Hole

QFN	Quad Flat No-leads
QPS	Quench Protection System
QR	Quick Response
Qty	Quantity
R	Resistor
RAMS	Reliability, Availability, Maintainability, and Safety
RF	Radiofrequency
RH	Relative Humidity
SEM	Secondary Emission Monitor
SFP	Small Form-factor Pluggable
SIL	Safety Integrity Level
SPS	Super Proton Synchrotron
SS	Straight Section (*SS* = Screening Strength, see Symbols)
TID	Total Ionizing Dose
TM	Trademark
US DoD	United States Department of Defense
V_ADC	Analog-to-Digital Converter Voltage
V2	Version two
VFC-HD	VME FMC Carrier - HPC DDR3
VME	Versa Module Eurocard
WS	Wire Scanner

1 Introduction

To investigate the fundamentals of our universe, physicists, engineers and many more perform experiments by operating particle accelerators and other machines at CERN: the European Organisation for Nuclear Research. Founded in 1954, with the first accelerator built in 1957, the organisation nowadays carries out research in a variety of fields and operates a total of eight accelerators and two decelerators along with their associated experiments. This includes the 27 km in circumference Large Hadron Collider (LHC), the largest machine in the world.

The LHC accelerates and collides protons and heavy ions currently at centre-of-mass energies up to 13 TeV, storing an energy of up to 362 MJ in each of its circulating beams. To achieve such high energies, the LHC uses superconducting electromagnets, which store a total magnetic energy of up to 11 GJ producing an 8.3 T strong magnetic field. The field is produced by currents of up to 11 kA in niobium-titanium coils, which are cooled down to 1.9 K in order to reach the superconducting state.

Such high energies imply the risk to seriously damage the machine leading to significant costs and downtime, as demonstrated by an incident on the 19th September 2008, which caused more than a year of operational delay [1]. For this reason, it is fundamental to control the circulating particle beams, and to protect the machine and the equipment from uncontrolled release of both the beam and magnet energy.

Thus, to operate the LHC safely a variety of systems form the LHC Machine Protection System (MPS). The LHC Beam Loss Monitoring (BLM) system, which measures secondary particle showers created by off-orbit particles lost from the beams, is part of the LHC MPS. If beam losses above predefined thresholds are measured, the LHC BLM system initiates the process of a safe beam extraction in order to protect the machine.

In order to provide and maintain its protection function, the LHC BLM system needs to meet high dependability requirements involving system reliability, as well as system availability to avoid downtime of the LHC. In the particular case of LHC downtime, this also comprises a low number of false alarms. Thus, a comprehensive dependability analysis was already executed during the system design phase [2]. Afterwards, steady efforts were carried out such as an external audit in 2010 [3], tracking and analysis of system failures, or implemented upgrades.

1.1 Motivation and Objective

To carry out research in the field of particle physics, CERN operates the above described accelerators and their associated experiments. To achieve the necessary statistical significance for the collected data, many of the experiments require a great number of repetitions. Thus, the underlying machines and their instrumentation are dependent on precise, well-functioning and dependable technology. This involves two substantial parts of dependability engineering: first, the concerned systems have to operate at high reliability to fulfil their intended functions without failures for the given time at given conditions; and secondly, as the probability to provide the function for the required time period, high system availability is crucial.

To address dependability already during the system development and onwards continue its application until the end of the life cycle, the objective of this work is to develop a generic methodology for dependable electronic system development. More precisely, the methodology aims to adopt dependability engineering during the system development, installation, operation and decommissioning, thus integrating a common procedure to enhance the dependability within an organisation. This is to continuously enhance the dependability of the operated systems and to integrate dependability management as a part of the organisational culture.

For the LHC BLM system dealt within this work, the above described reflects precise fulfilment of its machine protection function at high availability during the intended mission time with reliably working equipment. Thus, the herein presented dependability analysis and related improvement measures of the LHC BLM system has served as motivation to develop the presented methodology.

1.2 Structure of the Thesis

The described objective of this work aims to provide a methodology for dependability coverage during the full product life cycle as well as to update the existing dependability model and strategy of the LHC BLM system at CERN. As illustrated in Figure 1.1, the thesis is divided into six distinct chapters.

In chapter 1, a short introduction to CERN and the LHC is provided. Chapter 2 describes the LHC BLM system, which is further examined within this work. The third chapter investigates the state of the art for methodological approaches on dependability engineering and outlines the necessary dependability engineering basics.

Chapter 4 presents the elaborated LHC BLM system dependability model by updating and expanding an existing model, which has been prepared prior to the system becoming operational [2]. Furthermore, the model uses available operational data of the system and takes, as well as suggests, actions to improve the current strategies of operation, maintenance and upgrades.

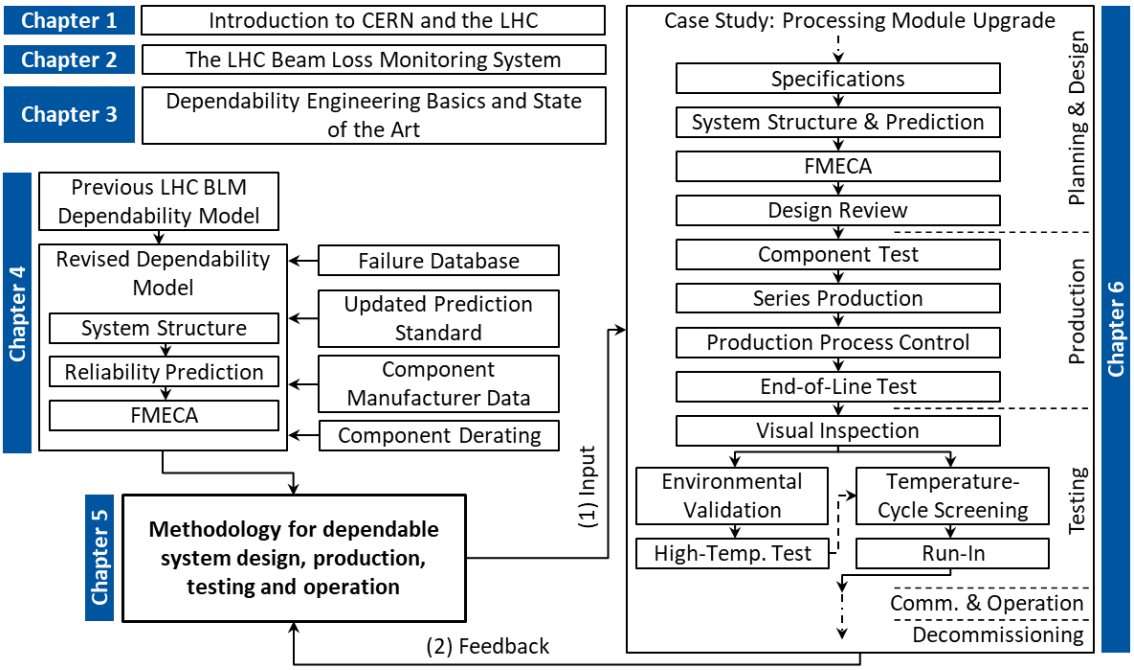


Figure 1.1: Structure of the thesis and interconnection of the individual chapters.

Based on the examined dependability analysis of a beam instrumentation system in chapter 4, the subsequent chapter 5 comprises a developed methodology to accompany the entire system life cycle by employing various dependability methods and, in this way, enhance its performance and dependability. This involves specifying the requirements in the planning phase and applying appropriate methods and analyses during the design phase. With the different functionalities of the system being essential parts of the dependability, the subsequent prototyping, and parallel testing up to the final validation is covered hand in hand with the pre-production. This continues with the properly planned production, conducting appropriate actions to achieve the required quality for a dependable performance, and is to be confirmed by following functionality tests, early failure screening and reliability tests. Furthermore, the methodology also comprises the system installation or the respective integration into a primary system. During operation or field use, potentially necessary actions are displayed, such as implementing a previously developed maintenance strategy or the implementation of a tracking system to monitor the performance in order to improve dependability in the long term.

The final chapter 6 applies the elaborated methodology within a case study of a newly developed processing board as an upgrade for the LHC BLM system. The planning phase up to production and various testing of all produced boards is covered. The dependability model and optimisations along the design process, as well as data of validation, screening and reliability testing are presented. A strategy for the upcoming installation and the henceforth operation during the next years are also a part of the study.

1.3 CERN

The *Conseil Européen pour la Recherché Nucléaire*, CERN [4], which nowadays is referred to as the European Organization for Nuclear Research, was founded in the year 1954 in the French-Swiss border region close to the city of Geneva.

With the main objective to study fundamental particle physics, the organisation grew in the following years to become the largest particle physics laboratory in the world. This led to currently more than 2 500 employees and additional 17 500 people across collaborations all around the world contributing their individual share to the research and experiments executed at CERN. [4]

Figure 1.2: Higgs boson discovery announcement at CERN in 2012 [5]. Rolf Heuer (center), CERN Director-General in 2012 with Joseph Incandela (right), spokesperson of the CMS experiment and Fabiola Gianotti (left), project leader of the ATLAS experiment, nowadays CERN Director-General.

Outcomes of this ongoing process have been two won Nobel prices by C. Rubbia and S. van der Meer for the discovery of the W and Z bosons [6] in 1984 and by F. Englert and P. W. Higgs for the discovery of the Higgs boson [7] in 2013. In 1989, T. Berners Lee published a proposal for information management at CERN, which led to the World Wide Web [8]. On another level, further achievements of CERN comprise bringing international people together with different expertises and cultures working in a peaceful and creative environment following CERN's 60th anniversary slogan "Science for Peace".

1.4 Particle Accelerators in Brief

Since the year 1927, when R. Widerøe built the first linear particle accelerator [9], the world now comprises a vast amount of different accelerators and technologies for a variety of applications. Such applications range from big accelerators to collide

particles for nuclear or high energy physics, up to a use in industry and medicine, for instance for X-ray scans, sterilisation or in radiotherapy [10].

As basic principles to accelerate and control charged particles, either static or dynamic electromagnetic fields are used. Depending on the used particles, different sources form the first stage of an accelerator. To generate electrons for example, one method is to heat a cathode in a vacuum environment emitting electrons through thermionic emission. For protons, a method is to inject hydrogen gas into an electric field, stripping of its two electrons. After creation, the particles pass on to the according accelerator, which can be linear, primarily using accelerating structures, or circular machines, in addition using beam-bending elements. [10]

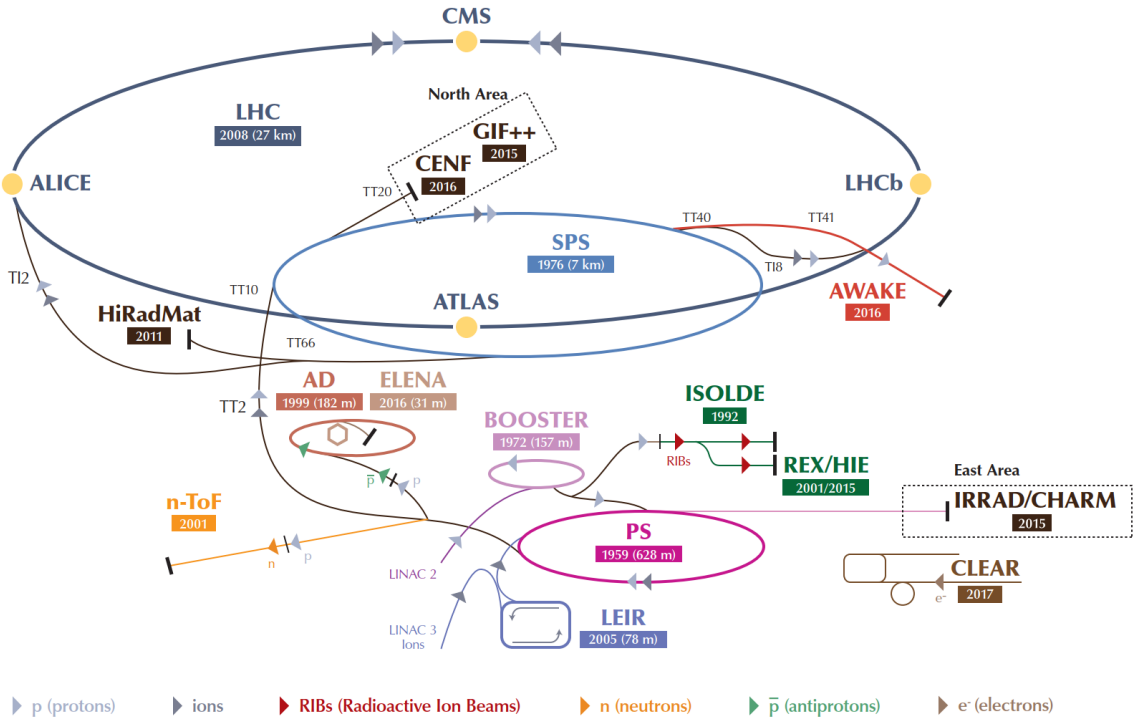


Figure 1.3: The CERN accelerator complex [11]. Depending on the operation mode, the LHC can be filled through four distinct pre-accelerators with either protons or ions. In addition, the complex comprises various peripheral experiments.

Regarding the physics involved, different parameters are used to classify the performance of accelerators. Of course, the characteristics depend on the accelerator technology and the used particles, but commonly energy, the emittance of the beams or beam intensity distinguish different machines. More specifically for particle colliders, luminosity is an important performance measure, see subchapter 1.6. To quantify the energy of accelerated particles the unit electron Volt (eV) is used. 1 eV is defined as the kinetic energy an electron e gains from acceleration through a potential difference of 1 V, thus 1 eV = $1.602*10^{-19}$ J [10].

Based on the CERN accelerator complex in Figure 1.3, the following two subchapters describe different accelerator technologies and physics involved more in detail.

1.5 CERN Accelerator Chains

Figure 1.3 displays particle accelerators and decelerators as well as experimental areas at CERN. The central machine of this complex is the LHC with its associated experiments and the injecting accelerators to gradually increase the energy level. This subchapter illustrates these previous injectors, which build two distinct accelerator chains to either inject protons or heavy ions into the LHC.

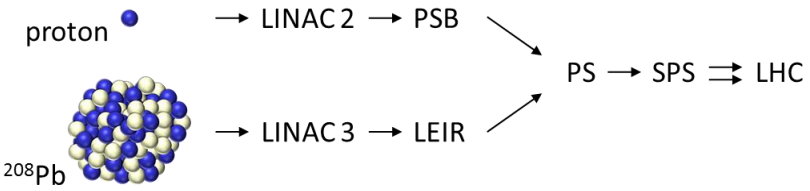


Figure 1.4: Different accelerator chains feeding the two beam pipes of the LHC. Depending on proton or heavy ion operation, different LINACs and, for the second stage, circular accelerators are used.

LINACs

After creation, the journey of particles begins in dedicated linear accelerators (LINAC). Protons are generated from hydrogen gas which is released into the electrical field of the Duoplasmatron, until they are injected into the vacuum of the LINAC 2. Heavy ions, for instance lead, are generated during a process which heats up ^{208}Pb until it evaporates. The vapour is ionised in a plasma chamber to then be accelerated by the LINAC 3. [12]

The operating principles of LINAC 2 and LINAC 3 are very similar. Both accelerate particles in a straight line using radiofrequency (RF) cavities equipped with a series of drift tubes. An oscillating electric field is generated in gaps between the tubes. When passing a gap, the bunched particles feel an accelerating force while the polarisation of the field is alternated when inside the drift tube. Progressively increasing lengths of the gaps and drift tubes ensure the correct tuning of the field change while the particles gain velocity. [10]

At extraction, heavy ions in LINAC 3 reach an output kinetic energy of 4.2 MeV. In LINAC 2, the protons reach 50 MeV, see Table 1.1. This energy is to be increased by a factor of more than three to 160 MeV once the new LINAC 4 starts to operate in 2020, in the framework of the LHC Injectors Upgrade [13].

PSB

Fed by LINAC 2, the Proton Synchrotron Booster (PSB) is built up by a spiral of four rings to accelerate protons up to energies in the GeV-range. In contrary to linear accelerators, the PSB supplementary uses beam bending elements to keep the particles on a circular path. While not being a perfect circle, the PSB uses a mix of accelerating structures as a LINAC, alternated by beam bending dipole magnets. In addition, several sets of quadrupole magnets focus the proton bunches. Over the

course of the accelerator, the magnetic dipole fields are raised proportionally to the acceleration to keep the foreseen trajectory.

LEIR

The Low Energy Ion Ring (LEIR) receives its ion beam via a LINAC 3 transfer line. It is set up with four beam bending and four straight sections in between to accelerate and condition the beam for extraction.

PS

The Proton Synchrotron (PS) is the oldest accelerator in the current complex. Since starting operation in 1959, the 628 m in circumference PS nowadays accelerates protons or ions from either the PSB or LEIR up to 26 GeV.

SPS

The last link in the LHC injector chain is the Super Proton Synchrotron (SPS). Accommodated underground in a tunnel of roughly 7 km in circumference, the SPS raises the energy level up to 450 GeV. The injected protons already move at a velocity of 99.93% the speed of light, which the SPS increases to 99.999 8% [14]. At this energy level, the SPS injects into the LHC beam pipes via two separate transfer lines.

Table 1.1: Maximum kinetic energies for LHC pre-accelerators [15, 16]. Kinetic energies of a proton or the concerned ion (*). For protons, the relativistic factor γ is given, see Eq. (1.3).

	LINAC 2	LINAC 3	LINAC 4	PSB	LEIR	PS	SPS	LHC
Maximum energy [GeV]	0.05	0.0042*	0.16	1.4	0.072*	26	450	7 000
Relativistic factor γ [-]	1.05		1.17	2.5		28	481	7 464

1.6 The Large Hadron Collider

Being the largest in the world, the LHC is naturally the most important machine at CERN. It has been constructed to perform experiments at collision energies, which have never been reached before in order to answer fundamental questions in physics and to find new discoveries, possibly beyond the standard model of particle physics. In 2012 the LHC already answered such question when discovering the long-searched Higgs boson [7].

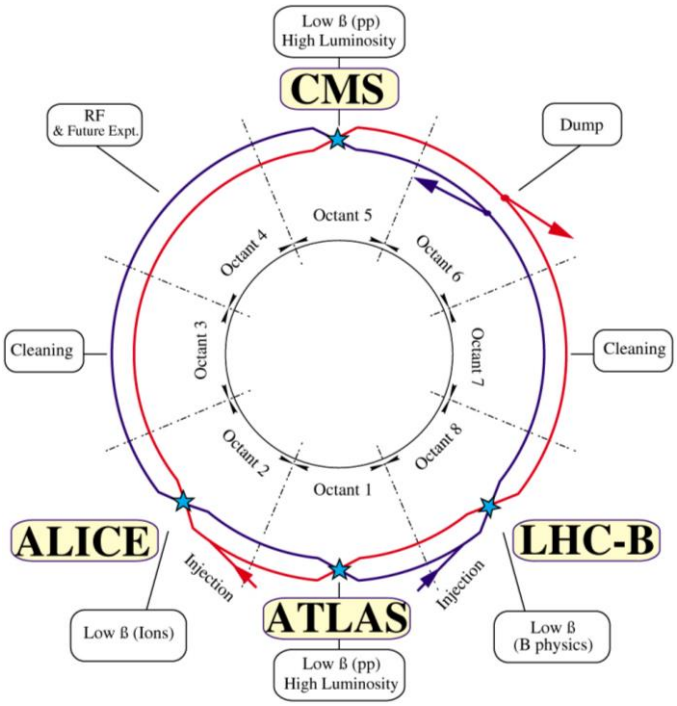


Figure 1.5: LHC layout [17]. Two counter-circulating beams (red, blue) collide at four interaction points. The beams are injected at point 2 (ALICE) and 8 (LHC-B) and get extracted at point 6 (Dump).

1.6.1 Design and Technology

Planning of the LHC project begun in the early 1980's to become the successor of the Large Electron-Positron Collider (LEP) which was operating in the same 27 km tunnel as is nowadays the LHC. Approved in 1994, construction of the LHC started in the following years to inject the first beam on 10th September 2008 [14].

The design of the LHC accommodates two counter-circulating beam pipes including the magnets inside a single cryostat structure, see Figure 1.6. The ring is located between 50 and 175 m underground and divided into eight octants with individual access points on the surface. Not forming a perfect circle, each octant is established as two times half an arc with a Straight Section (SS) in the middle. Thus, eight arcs in total each consisting of 154 main dipole magnets as well as different focussing magnets, *e.g.* quadrupoles. The eight SS are more diverse, each fulfilling its individual purpose. Four house the major experiments, see subchapter 1.6.3. Two in the opposite octants 3 and 7 comprise the collimation systems to clean off-orbit particles of the beams. The RF cavities are in octant 4, and the extraction system to dump the beams is accommodated in octant 6, see Figure 1.5. [18]

The LHC magnets are located inside the cryostat, which sets the temperature to 1.9 K above the absolute minimum of -273.15°C by using superfluid helium. At this temperature, the niobium-titanium coils reach the superconducting state. With no

measurable resistance in that state, it is possible to create magnetic main dipole fields of up to 8.3 T using currents close to 12 kA. [14]

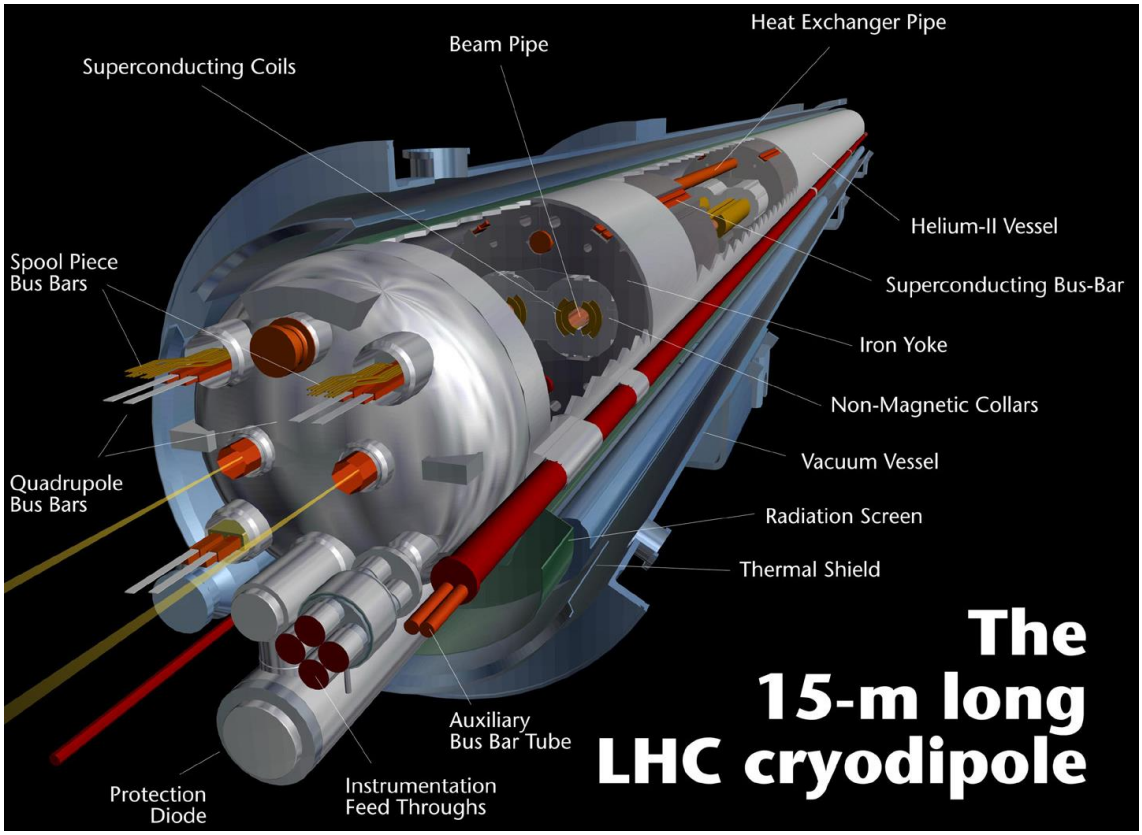


Figure 1.6: Cross section of an LHC dipole [19]. The two beam pipes and their magnet structures are surrounded by the cryostat to establish superconductivity conditions.

1.6.2 LHC Physics

To put the properties of the LHC into perspective the mass-energy equivalence of the special relativity theory, first proposed by A. Einstein [20], can be consulted:

$$E = mc^2. \tag{1.1}$$

The speed of light c is a constant, hence the relativistic mass m of a particle is proportional to its energy E. For protons in the LHC accelerated up to 6.5 TeV, this kinetic energy E_{kin} is expressed together with the rest energy E_0 as a part of E:

$$E_{kin} = E - E_0 = (\gamma - 1)mc^2 \tag{1.2}$$

The relativistic factor γ introduced in Table 1.1 is applied to establish the energy-mass relationship for moving objects. It is defined as

$$\gamma = \frac{E}{E_0} = \frac{mc^2}{m_0 c^2}\ , \tag{1.3}$$

the ratio of the total energy and the rest energy, which is a factor of c and the rest mass m_0. For a particle at rest, with no kinetic energy, γ is equal to 1. [10]

The LHC increases the relativistic factor up to 7 464, which is equal to the relativistic mass being 7 464 times the rest mass of a proton. The velocity in contrast reaches 99.999 999 1% of c from 99.999 8% at injection. In absolute terms, it is hence more consistent to refer to the LHC as a storage ring, rather than an accelerator. Especially, because it only increases the energy during a small fraction at the beginning of its cycle, maintaining the top energy during most of it, see Figure 1.8.

Once this top energy is reached, collisions are recorded at the LHC experiments. At the beginning of a fill, up to 40 collisions occur per bunch crossing, resulting in about 10^9 collisions per second [14]. Hence, it seems that during a typical year of currently around 6 000 h (Table 1.4) of operation, large amounts of data are available. Nevertheless, certain events only occur at low rates and require sufficient confidence to be proven, which is one reason why the LHC is intended to operate until the year 2038. This includes the High-Luminosity LHC (HL-LHC) upgrade starting in 2024 [21]. To quantify the performance in this regard, the luminosity $\mathcal{L}$, rather the integrated luminosity $\mathcal{L}_{int}$ with respect to time, is used, according to [10], defined as

$$\mathcal{L} = \frac{N_1 N_2}{A} n_b f_{rev} \text{ , with } \mathcal{L}_{int} = \int \mathcal{L}\, dt \,. \tag{1.4}$$

Luminosity is a measure of how many collisions occur per time interval and interaction area typically given in $cm^{-2}\,s^{-1}$. It is characterised by the total number of particles in each of the two beams N_1, N_2. The luminosity increases for a small interaction area A of the beams at the colliding point as well as for a high revolution frequency f_{rev} and a high number of circulating particle bunches n_b.

To increase the collision energy in comparison to a stationary target accelerator, the LHC collides two beams with each other at energies up to 6.5 TeV, resulting in a centre-of-mass energy of 13 TeV.

1.6.3 The LHC Experiments

The collisions take place at four interaction points, where the two LHC beam pipes cross each other. At each of them, one of four major experiments is located:

1. ATLAS - A Toroidal Lhc ApparatuS [22]
2. ALICE - A Large Ion Collider Experiment [23]
3. CMS - Compact Muon Solenoid [24]
4. LHCb - LHC beauty [25]

The opposite located ATLAS and CMS detectors (Figure 1.7) are the largest with ATLAS being 46 m long at a diameter of 25 m and CMS smaller but heavier, weighing 14 000 t. Both measure data, such as speed, mass or charge of particles produced in the collisions. They have been designed using different technologies, yet to study similar phenomena. This redundancy is needed to independently confirm new discoveries, excluding any measurement error, design flaw or other sources of error.

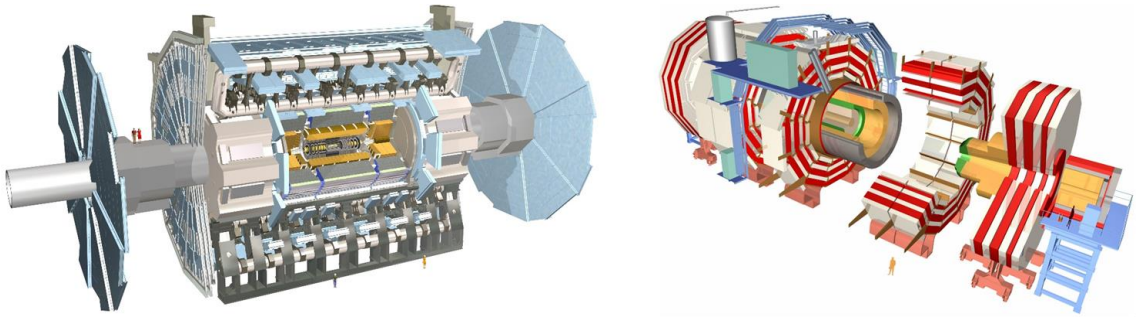


Figure 1.7: ATLAS (left) and CMS (right) detector drawings [26, 27]. The inner parts are composed of the inner detector and calorimeters (*i.a.* yellow) measuring the energy loss of passing particles. The outer structures comprise the magnet systems and muon detectors.

The other two detectors are smaller and pursue other goals. The design of ALICE has been adjusted for the heavy ion runs of the LHC. The detector intends to study physics of strongly interacting matter at high energy densities. At such conditions a quark-gluon plasma forms, the state the universe is believed to have been in pico-seconds after the big bang [14]. In a similar manner, LHCb is a detector dedicated to explore the "beauty quark", a fast decaying particle. In doing so, physicists try to recreate the conditions shortly after the big bang to answer the question why nature is formed out of matter instead of antimatter.

1.6.4 LHC Operation and Figures

After particle beams are injected into the LHC, the energy is ramped up and the experiments start taking data. At this point, the number of circulating particles, referred to as beam intensity, is the highest with around $120*10^9$ protons per bunch. For the maximum of 2 808 bunches inside one beam, this leads to particle intensities of more than $3*10^{14}$ per beam [14]. Afterwards, the storage ring is continuously loosing particles during collisions, at the collimators or due to other effects such as beam-gas interactions, see subchapter 2.1. As a consequence, it is at a certain point favourable to extract, or "dump" the beams and prepare the machine for a new fill in order to optimise the luminosity. Using data of the 2012 LHC run, an optimum run time to take physics data of 14.2 h has been computed [28]. This parameter however depends on many factors and can vary, *e.g.* for an improved turnaround time between fills. Nevertheless, it can serve well to align the dependability design of the LHC and its accompanying systems, as the LHC BLM system.

During regular operation, an LHC cycle separates into different phases, as shown in Figure 1.8. The actual run time t_r as introduced in [28] is referred to as the time of stable physics operation (phase 1). The turnaround time t_{ta} is the period between a beam dump and the re-establishment of stable physics conditions (phases 2 - 5).

$$t_{cycle} = t_r + t_{ta} \tag{1.5}$$

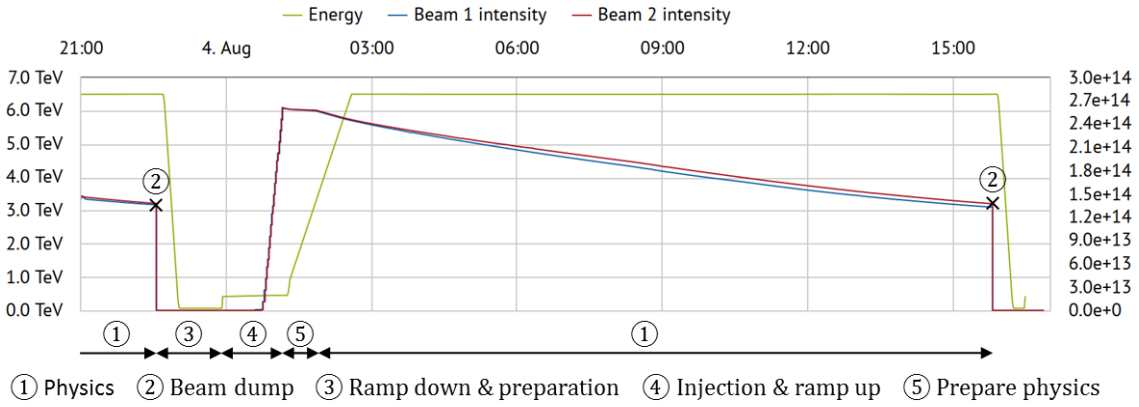


Figure 1.8: LHC cycle (04.08.2018), extracted from [29]. The energy (green) is ramped up to 6.5 TeV and kept for 13.5 hours during which the beam intensities (red, blue) constantly decrease from a maximum of around 2.7*10^{14} protons per beam.

Having a nominal LHC mission established, the LHC also undergoes greater cycles on the scale of weeks and years. On the top level, the current mandate of the LHC and HL-LHC is scheduled into six Runs, which are interrupted by Long Shutdowns (LS), see Figure 1.9. The shutdowns serve to repair, maintain and upgrade the machine. On a yearly basis, during runs, the schedule foresees a year-end technical stop, a commissioning phase afterwards, as well as machine development phases and other stops, which grant access to the machine during the year.

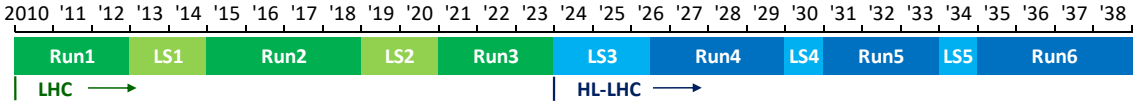


Figure 1.9: LHC and HL-LHC project schedule, according to [30]. In the year 2024, at the end of Run 3, the LHC mandate finishes and it is foreseen to construct and exploit the HL-LHC until 2038.

In accordance with the operational schedule, the LHC systems have to subordinate their individual strategies for maintenance, repair and upgrade. This condition influences the designs of these strategies, especially with regard to dependable design. As described more in detail in chapter 3, availability is a crucial factor of dependability. For the LHC, availability, and in this manner also luminosity, respectively its integral over time, can directly be correlated to the various cost factors of the project. Table 1.2 gives an overview of different costs involved in the LHC project.

Table 1.2: Current costs of the LHC project [31]. For detectors and computing only the share which CERN has paid is given (*). Costs for Run 2 are not yet published.

	Machine & areas	Detectors*	Computing*	Run1	LS1	Run2	**Total**
Personnel [MCHF]	1 224	869	85				
Material [MCHF]	3 756	493	83				
Total [MCHF]	4 980	1 362	168	1 100	150	?	**>7 760**

In order to quantify the impact of failure-caused downtime, the hourly costs of LHC operation up to the current date are computed. Eq. (1.6) only takes into account the costs paid by CERN and furthermore neglects other costs as for example already available infrastructure, primarily the 27 km LEP tunnel. Operational costs include the runs and shutdowns, while for the four-year-long Run 2 the same costs as of Run 1 are assumed. Furthermore, only operational days as displayed in Table 1.3 are considered assuming 24 h of daily planned operation.

$$Cost(t) = \frac{\sum costs}{\sum op.hours} t = \frac{8.86*10^9 CHF}{1\,774*24h} t = 208\,098 \frac{CHF}{h} t \qquad (1.6)$$

This present figure is likely to decrease during Run 3 and eleven following years of HL-LHC, which yet also involves 950 million CHF of investment [32]. Furthermore, other cost estimates exist, *e.g.* [33] conducts an analysis yielding the total LHC costs between 1993 and 2025 at 13.5*10^9 €. For ten operational years in that timeframe, assuming for each roughly 6 000 operational hours, this equals around 240 000 CHF hourly costs, based on nowadays exchange rate[1].

Table 1.3: Operational LHC days since 2010, extracted from [29]. An operational day is defined as a fill day of the LHC, in other words with intensity measurements of both beams greater than zero.

Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	**Total**
No. of fill days	245	260	270	43	0	255	237	225	239	**1 774**

To sum up, obtaining precise hourly operational costs is complex dependent upon a variety of factors involved and the applied run time. As a lower benchmark it can be referred to a minimum of 200 kCHF per hour. Table 1.4 finally summarises figures of the LHC relevant for the scope of this thesis.

Table 1.4: General LHC figures for proton operation.

Parameter	**Value**	**Dimension**	**Source**
Maximum beam energy	6.5	[TeV]	[14]
Maximum number of bunches	2 808	[-]	[14]
Bunch intensity (at injection)	1.2*10^{11}	[-]	[14]
Number of collisions per second	1*10^9	[/s]	[14]
Revolution frequency f_{rev} (1 revolution = 89 µs)	11 245	[Hz]	[18]
Maximum stored beam energy	2 × 362	[MJ]	[34]
Maximum stored main dipole magnet energy	11	[GJ]	[34]
Optimum run time t_r	14.2	[h]	[28]
Average turnaround time t_{ta} in 2018	6.0	[h]	[35]
Average yearly operational hours during Runs	6 000	[h]	Table 1.3
Current operational costs per time	>200 000	[CHF/h]	Table 1.2

[1] 1 CHF = 0.94 € (European Central Bank average exchange rate on 04.07.2020)

1.7 The LHC Machine Protection System

Table 1.4 shows that the two circulating particle beams of the LHC each can store an energy of up to 362 MJ. If released in an uncontrolled manner, this implies the risk to seriously damage the LHC and its equipment. To mitigate the risk of such events occurring, which can lead to significant costs and downtime [1], the LHC Machine Protection System (MPS) [36] has been designed, see Figure 1.10.

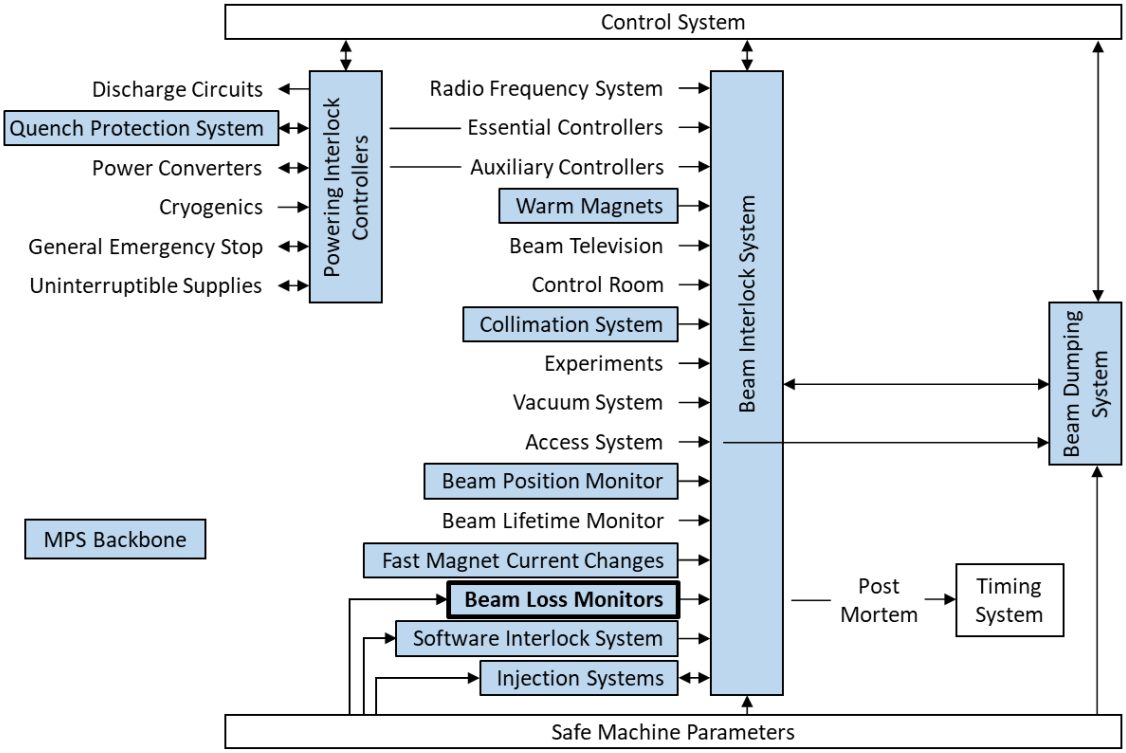


Figure 1.10: Architecture of LHC machine protection systems according to [37]. Various subsystems are linked together, which in case of potential danger, transmit a beam dump request via the BIS to the LBDS which extracts the beams.

As a protection system, the MPS design fulfils high reliability requirements using practices such as the Safety Integrity Level (SIL) according to the IEC 61508 standard [38] of the International Electrotechnical Commission (IEC), a fail-safe approach or redundancies [36]. It unites a variety of subsystems from injection systems, to systems monitoring the LHC, its equipment and beam parameters up to extraction systems of which only the relevant ones for the scope of this thesis are covered in here. Numerous parameters are constantly surveyed to take mitigating actions in case of critical values or potential danger. Together with their connected systems, three central elements establish the MPS:

- The Powering Interlock Controllers (PIC) [39]
- The Beam Interlock System (BIS) [40]
- The LHC Beam Dumping System (LBDS) [41]

The PICs interact with the power converters and the Quench Protection System (QPS) [42, 43] stopping the magnet powering and initiating a beam dump request in case of critical parameters. The QPS is designed to detect when the superconducting magnets reach a resistive state, referred to as a quench. A quench can be caused by energy deposition of lost beam particles and leads above a certain threshold to a sudden release of the stored magnet energy. To prevent magnet damage requiring months of repair, the QPS fires resistive heaters to distribute the released energy and initiates a safe discharge of the magnet energy via the power converters when the resistive voltage across the magnet surpasses a threshold for a certain time.

To avoid energy deposition above the quench level in the first place, the MPS comprises additional systems to prematurely act. The collimation system [44], for instance, moves robust blocks from the sides into the beams to remove off-orbit particles. Another vital system to prevent energy deposition in the magnets is the LHC BLM system, see chapter 2. Both these systems connect to the BIS.

In total about 20 subsystems are connected to the BIS which establishes the MPS backbone. Using redundancy, the BIS is formed by two communication loops per each beam along the LHC connecting to the LBDS. The loops carry the “Beam Permit” signal allowing injection or operation with beams. To interface with the MPS subsystems, 16 Beam Interlock Controllers (BIC) are distributed around the loops. The subsystems constantly feed the BICs with their individual status information and send a beam dump request if a potentially dangerous event is monitored. The Beam Permit is then removed from the loops triggering the LBDS to initiate a safe beam extraction by firing the extraction kicker magnets at the LHC dump lines.

The LBDS is responsible to safely extract the beams for such an event or at the end of an LHC fill. An LBDS failure mode, which results into not being able to extract the particle beams, is one of the worst possible scenarios. Hence, the LBDS has been designed according to the highest SIL 4 level [45]. It is composed of fast pulsed extraction kicker magnets and septum magnets to deflect the beams, diluter elements and at the end of the 750 m long extraction tunnels graphite blocks to absorb the beam energy. Already at injection into the LHC, a 3 μs abort gap is established between two bunches to allow the kicker magnets to build up their field. This means, that once the LBDS receives a beam dump request, a maximum time of 2*89 μs, or two LHC revolutions, passes to synchronise with the abort gap and extract the beams.

On a larger scope, a worst-case response time of 100 μs of the BIS has to be added, as well as the individual response times of the subsystems [40]. Depending on the individual criticality, these response times range between half an LHC revolution in the μs-range to some hundreds of milliseconds and several seconds for actions taken by human operators. Using worst-case assumptions, an extraction in less than four LHC turns is provided by the fastest reacting subsystems. The LHC BLM system has one of the fastest response times, described more in detail in the following chapter.

2 The LHC Beam Loss Monitoring System

A crucial and critical part of the LHC MPS is the LHC BLM system. It is designed to detect potentially dangerous beam losses early in time in order to prevent causing any damage. To do so, the system constantly measures the level of beam losses all around the LHC and processes the data in order to decide whether a safe extraction of the particle beams should be initiated via the BIS. In addition to its machine protection functionality, the LHC BLM system is also used to provide beam diagnostics data to tune the LHC in operation, or as a source of data to reduce irradiation of the LHC tunnel equipment.

2.1 Beam Loss

During nominal LHC operation a certain particle loss cannot be completely avoided. Different effects such as interactions between beam particles or with residual gas, instabilities or misalignment of the LHC cause beam loss and lead to particles leaving the dynamic aperture, which is the maximum oscillation amplitude for stable moving particles [18], *i.e.* they remain inside the LHC. A majority of these particles is caught by the collimators designed for that purpose. Yet, a few remaining particles escape from the stable trajectories and impact into the vacuum pipes interacting with the material. These interactions create secondary particle showers, which propagate by impacting into the LHC and its equipment, ionising and activating the respective, depositing energy and, in case of electronics, damaging and disrupting the functionality. Depending on the loss duration and intensity, the LHC and its equipment can tolerate such losses up to certain thresholds. With respect to time, four main categories of losses are distinguished: ultra-fast losses within one LHC turn ($< 89\ \mu s$), very fast losses (< 5 ms), fast losses (< 1 s) and steady losses (≥ 1 s) [36]. Ultra-fast losses can be caused by injection or extraction faults and can only be passively protected by the collimators. For other loss intervals, the MPS is able to protect actively. Thus, to monitor the beam losses and to enforce the location specific loss thresholds, the LHC BLM system acts as a first-in-line protection system.

2.2 LHC BLM System Overview

The LHC BLM system is a highly distributed system, which spans around the complete LHC tunnel, and from there connects in modular slices to its eight surface

installation points, compare Figure 2.1. Functionally, it can be divided into four principal main parts, which the following subchapters describe more in detail:

1) Beam loss detectors and supply
2) Front End (FE) acquisition electronics
3) Optical fibre link
4) Back End (BE) processing electronics and interfaces

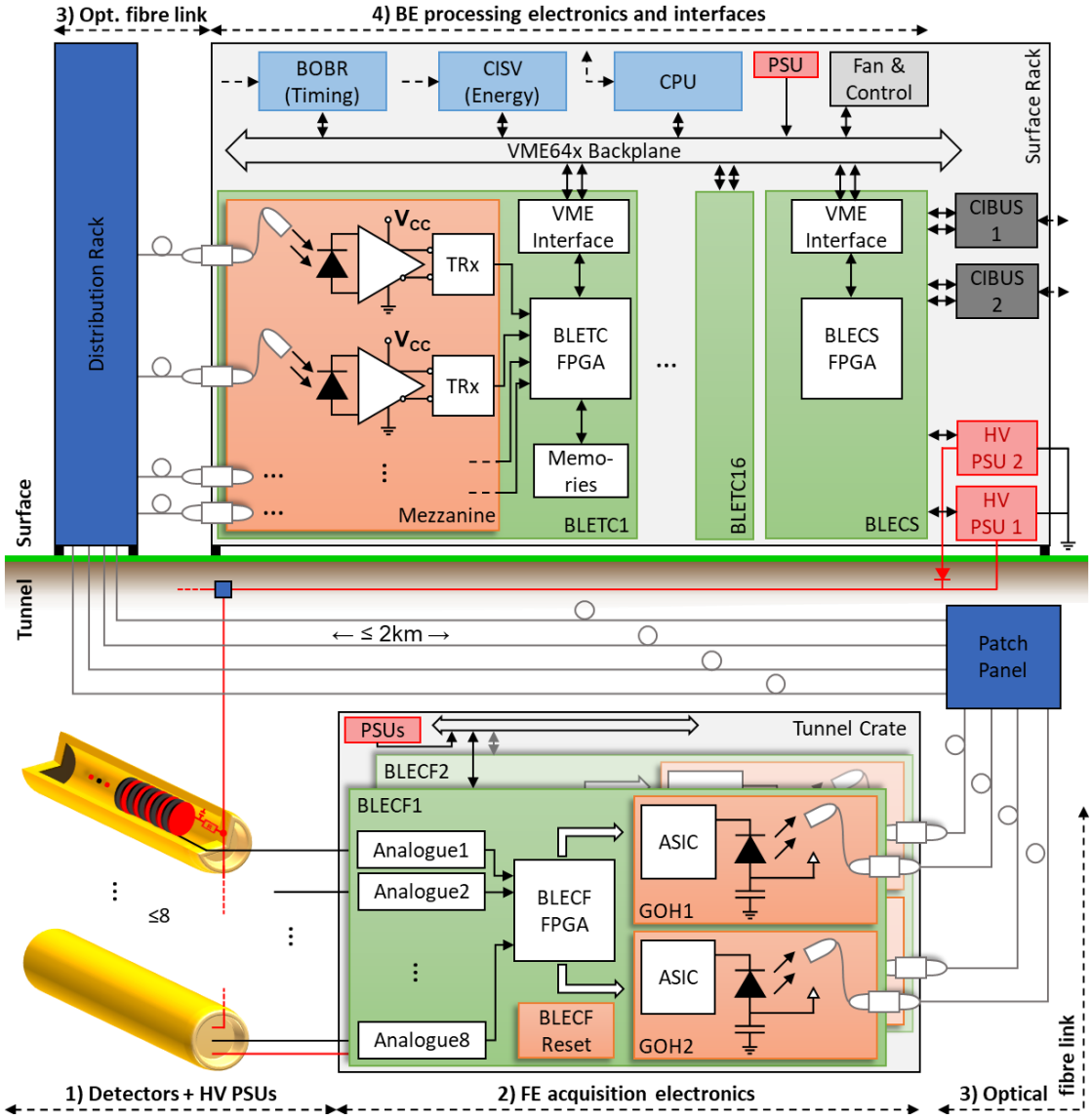


Figure 2.1 : Vertical slice of the current LHC BLM system (SS configuration). Ionisation Chambers (yellow) measure a current signal proportional to the beam loss. The FE tunnel board (BLECF) acquires, digitises and transmits the signal via optical fibres to the BE surface electronics, which process the loss signal and connect to the BIS via the CIBUS interfaces.

As loss detection sensors, primarily Ionisation Chambers are mounted outside the LHC cryostat (see Figure 2.3) connected to the various Beam Loss Electronics (BLE). At the beginning of the chain, up to eight chambers connect to the FE electronics, the Current-to-Frequency converter board BLECF, which acquires the beam loss signals

in its analogue part, see subchapter 2.4.1. The board digitises the signals and sends them using two “GOH” transmitter mezzanines via a redundant optical fibre link of up to 2 km in length to the corresponding BE electronics at the surface installations.

Two redundant links, in total four optical fibre inputs, are received by the mezzanine board of the Threshold Comparator module (BLETC), see subchapter 2.6. Up to 16 loss signals are processed and compared to predefined thresholds depending on the specific detector location and different integration time windows of the losses. If a threshold is surpassed, the BLETC initiates a beam dump request via the Versa Module Eurocard (VME64x; VME in the following) bus on the backplane. Potential beam dump requests of up to 16 BLETC per VME crate are transmitted via two parallel daisy chains and are handled by the Combiner and Survey module (BLECS) in the last crate slot. Finally, the BLECS modules of up to four VME crates per surface point forward their Beam Permit until the last module in this chain connects to the BIS via the Controls Interlocks Beam User Single (CIBUS) interface, see Figure 2.2.

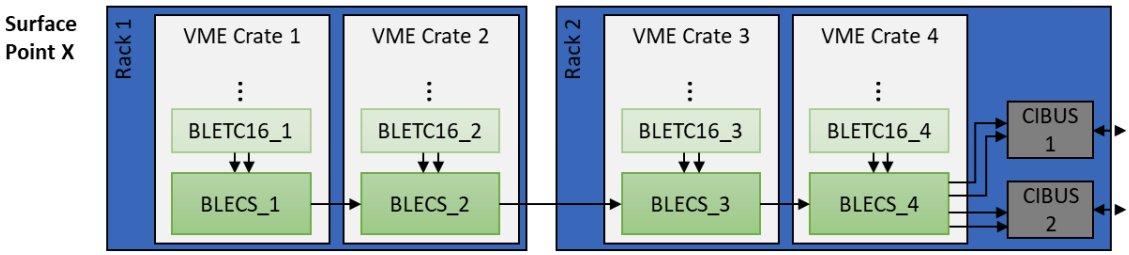


Figure 2.2: BLECS Beam Permit signal path. On each surface point, up to four BLECS receive the BLETC daisy chain signals and forward them in another daisy chain to the last module, which transmits the Beam Permit to the BIS.

In order to define the system boundaries for the later dependability analysis inside the MPS (see subchapter 4.4), the LHC BLM system is specified as displayed in Figure 2.1 from the ionisation detectors up to the CIBUS connection, which forms the BIS interface. This comprises the entire installation displayed and does only exclude the CIBUS modules and the physical surface racks.

Table 2.1: LHC BLM system component numbers. Only fibre connections are listed. Electrical connections, *i.e.* cables and connectors are not displayed.

Qty	Component (surface)	Qty	Component (tunnel)	Qty	Fibre link
27	VME crate (+PSU, Fan&Control):	3635	Ionisation Chamber	4014	Fibre cable
27	CPU (Access, Logging etc.)	191	Secondary Emission Monitor	2676	Pigtail fibre
348	DAB64x (BLETC processing)	108	Little Ionisation Chamber	5352	Connector
348	Mezzanine (BLETC receiver)	329	Arc rack (+PSU) and		
27	BLECS (Combiner)	37	SS crate (+PSU):		
27	BOBR (Timing)	669	BLECF (Acquisition)		
8	CISV (Beam energy)	1338	GOH (Transmitter, redundant)		
84	Daisy Chain Jumper	669	BLECF Reset		
16	HV PSU (redundant)				

In total, the LHC BLM system comprises more than 3 500 Ionisation Chambers, as well as particular other detectors, which form the beginning of the complex read-out chains. These individual chains conclude at 27 VME crates and the associated connections to the BIS at the surface points. An overview of the major component numbers of the LHC BLM system is provided in Table 2.1. The following subchapters 2.3 up to 2.6 describe the most essential system parts more in detail.

2.3 Ionisation Detectors

Different kinds of detectors measure losses of the particle beams at CERN's accelerators. A variety of gas, vacuum-filled, solid state or scintillating sensors is used for different purposes, *e.g.* beam diagnostics, equipment protection or beam measurements in order to optimise beam parameters and luminosity [46].

Figure 2.3: LHC BLM system Ionisation Chamber. Installed chamber on the LHC cryostat (left) and the inner multilayer capacitor with insulation (right).

To protect the LHC, the LHC BLM system uses two main kinds of detectors. With more than 3 500 installed, by far the most used type is the Ionisation Chamber [47, 48]: an 80 cm long steel tube filled with nitrogen gas at 1.1 bar, see Figure 2.3. Inside, it consists of a multilayer capacitor with 61 electrodes, each separated by 0.5 cm. The anode is supplied by a high voltage of 1 500 V. In the event of a particle passing through the detector, the chamber gas gets ionised. The ionised particles move towards the cathode, which enables the acquisition electronics to measure a change in current, compare Figure 2.4. This current change is proportional to the deposited energy, respectively the beam loss. With the Ionisation Chamber, the LHC BLM system is able to detect beam losses, expressed as the proton density rate in protons*$s^{-1}m^{-1}$ and measured as a current signal, with a dynamic range of eight orders of magnitude [49].

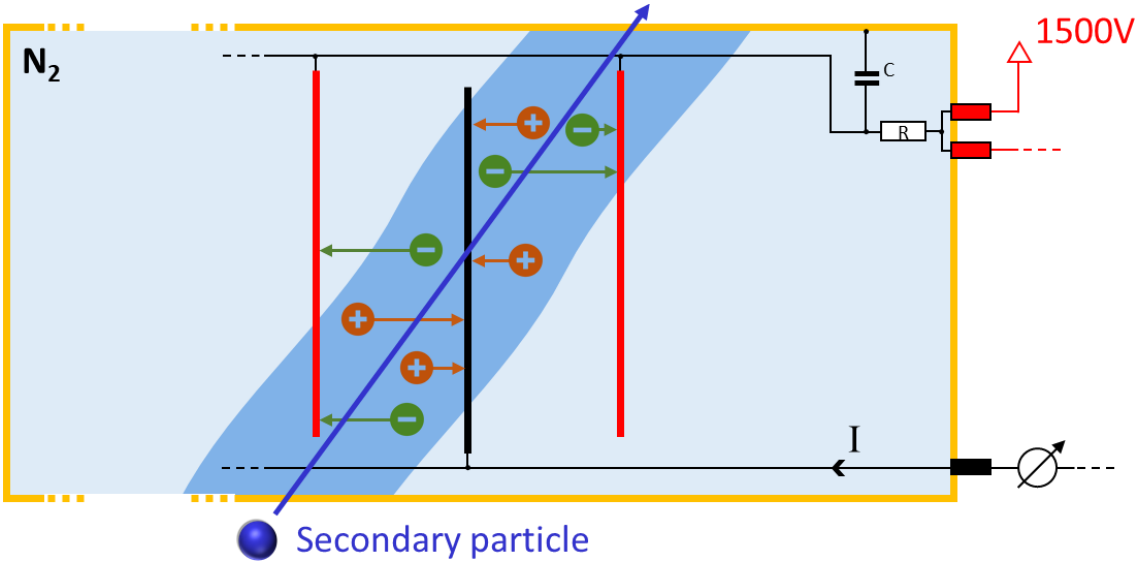


Figure 2.4: Functional principle of the LHC BLM system Ionisation Chamber. Particles of secondary showers ionise the contained gas. Electrons move to the anode of the multilayer capacitor under high voltage which leads to a current being measured at the cathode.

To extend the combined dynamic range up to 13 orders of magnitude, a second detector type is used to cover specific LHC locations with higher loss rates. The Secondary Emission Monitor (SEM) [50] is a similar steel tube as the Ionisation Chamber, which uses a different functional principle. Three metallic electrodes are under a vacuum inside the detector to exclude ionised gas significantly contributing to the measured signal. The current signal is created between the bias electrodes and the single signal electrode by secondary electron emission in its metallic surface layer. Impacting secondary particles excite conduction band and inner shell electrons creating electron-ion pairs, and thus a signal proportional to the particle's energy loss.

As displayed in Table 2.1 also other detectors, such as the Little Ionisation Chamber (LIC) [51] to measure high losses or the Diamond BLM [52] providing nanosecond time resolution are installed at the LHC, but are not further treated in here. The essential detectors for the MPS are the Ionisation Chambers.

2.4 Front End Electronics

On the FE of the LHC BLM system, the detectors connect to the BLECF board, with cables of up to 600 m in length depending on their location either in the LHC SS or in the arcs. Either supplied by a single-board-chassis or with up to 10 BLECF inside the SS chassis the boards are located in the LHC tunnel under the quadrupole magnets or inside different side alcoves, thus exposed to different levels of ionising radiation. For this reason, the BLECF as well as its two optical transmitter mezzanines (GOH) for the redundant optical link have been qualified for such an environment [53, 54].

2.4.1 The Current-to-Frequency Converter Board (BLECF)

The BLECF board [53, 55], is the main FE board. It uses Current-to-Frequency Conversion (CFC) to acquire the beam loss signals of up to eight channels within a measuring range between 2.5 pA and 1 mA. The analogue CFC parts each embed an integrator circuit at the current input, which connects to a comparator circuit at its output, compare Figure 2.5. There, the integrated signal is compared to a threshold voltage, triggering a monostable multivibrator (one-shot) at its output. The monostable multivibrator generates an output frequency, which is proportional to the current input, respectively the beam loss signal. These output frequencies of the up to eight connected CFC circuits are measured by the on-board Field-Programmable Gate Array (FPGA). In parallel, two Analogue-to-Digital Converters (ADC) connect to the FPGA. The 12 bit ADCs measure the integrator output voltages and have been added to cover low input currents below the one shot trigger level. Furthermore, a Digital-to-Analog Converter (DAC) acts as a current source generating a 10 pA current during a test mode to check the functionality of the channels, see subchapter 4.2. This current should trigger a CFC count supposedly every 20 s, being increased in steps of 1 pA if it does not. After five such increases the channel is declared blind.

Input Current	Output frequency
1 mA	5 MHz
1 µA	5 kHz
1 nA	5 Hz
1 pA	5 mHz

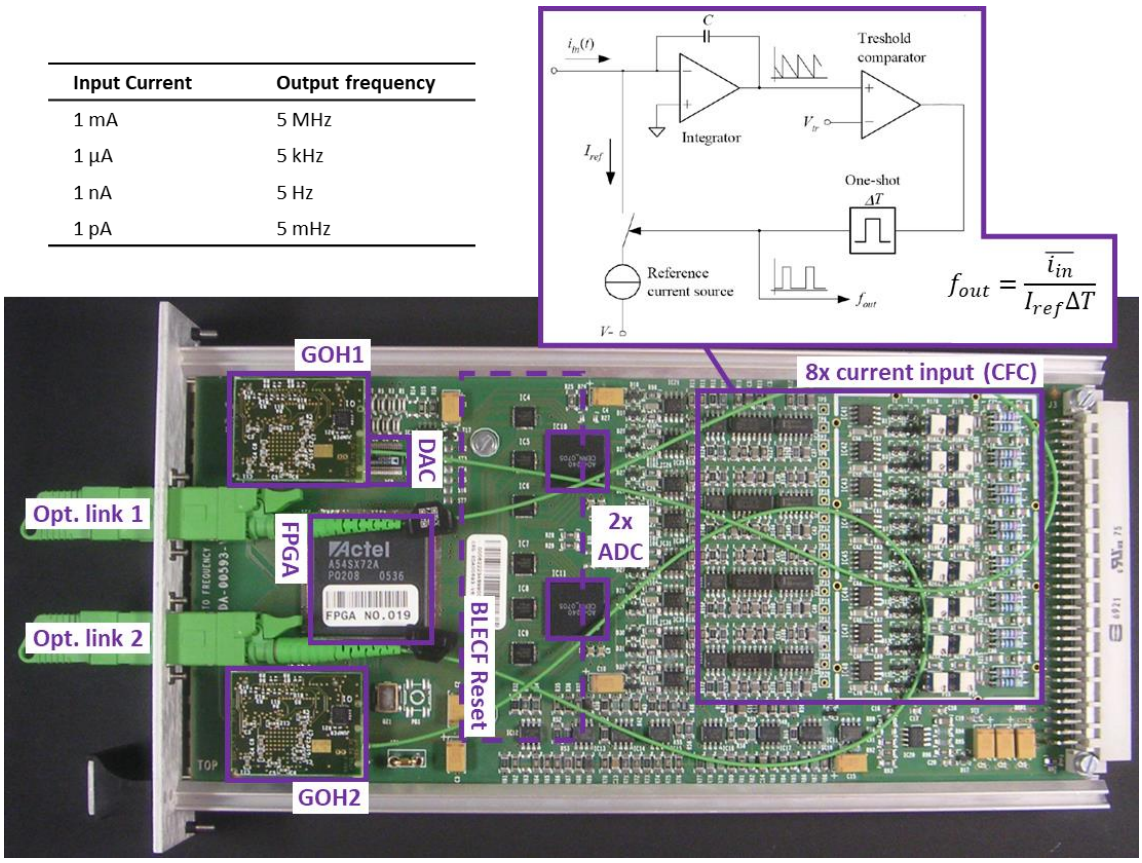


Figure 2.5 : BLECF board with two GOH mezzanines and optical fibre connectors according to [53, 56]. The current input signals are received by the BLECF connector (right). The CFC part measures these signals and generates the according output frequencies, which are measured and digitised by the FPGA. Via the two redundant GOH mezzanines the FPGA sends the data onto the optical link.

The FPGA sends the combined data every 40 µs in two identical 256-bit packets via the optical transmitter modules onto the optical link. To mitigate the risk of internal errors, in particular of such caused by the radiation environment, *e.g.* Single Event Effects, the FPGA uses on the one hand Triple Modular Redundancy for its most critical parts, primarily the CFC counters. On the other hand, it calculates a checksum to add a Cyclic Redundancy Check (CRC) to the transmission packets.

To further address the dependability on the board level, the BLECF has been designed in accordance with the SIL 3 level. Amongst different tests for its radiation [2], temperature and magnetic field tolerances, and during burn-in (see subchapter 3.4.2), this has also involved the design of protection circuits and a variety of diagnostic checks performed by the board. These diagnostics involve different test modes and status information, such as temperature or voltage statuses. [53]

The following subchapter describes the plugged optical transmitter modules more in detail. In addition, the complete module comprises a third mezzanine on the indicated spot in Figure 2.5. This "BLECF Reset" board is added to perform a general power reset of the module and is connected to the BLECF by soldered wires.

2.4.2 The Optical Data Link Transmitter (GOH)

To transmit the generated packets onto the optical fibre link, two GOL Opto-Hybrid (GOH) transmitter mezzanines plug into the BLECF. This GOH comprises the custom designed radiation tolerant Gigabit Optical Link (GOL) Application-Specific Integrated Circuit (ASIC) [54, 57, 58]. The GOL ASIC serialises and encodes the data received from the BLECF FPGA and in addition employs 8b/10b encoding to increase the transmission reliability [59]. Furthermore, it drives the laser diode, which transmits the data via the attached optical pigtail fibre onto the link, see Figure 2.5.

In terms of dependability, the manufactured GOH boards have been required to pass an extensive quality assurance comprising a variety of inspections, stress tests and burn-in [58]. Since then, it has proved its dependability as a part of the LHC BLM system as well as being installed within the harsh environment of the CMS Electromagnetic Calorimeter, compare subchapter 4.3.

2.5 Optical Fibre Link

The optical fibre link between the tunnel and the surface electronics is a fully passive, yet crucial part of the LHC BLM system connecting the FE and the BE. During the system design phase, the performed dependability analysis [2] has resulted in the implementation of a fully redundant link. From the redundant GOH modules on the BLECF, up to the receiver modules on the BLETC mezzanine (subchapter 2.6.1), the up to 2 km long link is entirely duplicated.

A single slice of the complete optical fibre link comprises the two pigtail fibres of the GOH and the BLETC mezzanine, three supplementary fibre cables as well as four fibre connectors on the FE and BE boards, the tunnel patch panel and the surface distribution rack, as displayed in Figure 2.1. The total number of fibre cables and connectors is displayed in Table 2.1.

The tunnel configuration of the optical link enables to pursue a replacement strategy of damaged fibres due to the radiation exposure. To implement this strategy, the link performance is continuously monitored and analysed, see subchapter 4.2.

2.6 Back End Electronics

The LHC BLM system's BE electronics are located inside temperature-controlled racks, compare Figure 2.1. The optical fibres coming from the tunnel connect to these racks, which accommodate up to two VME crates containing the surface electronics. In addition, the racks comprise the interfaces to receive LHC timing and beam energy information, the CPU connection to the network and databases, the CIBUS interface to the BIS, as well as the High Voltage (HV) distribution which can be interpreted as closing the loop to the FE by supplying the Ionisation Chambers.

2.6.1 The Versa Module Eurocard (VME) Crate

The main body of the BE processing is the VME crate [60], which accommodates on its customised backplane [61] the Beam Permit lines. An additional *P0* connector per slot complements the two 160 pin standard backplane connectors facilitating two daisy chains for potential beam dump requests. Together with other in the following described boards, up to 16 BLETC processing modules can be plugged into each crate. This equals a maximum of 256 ionisation detectors connected per crate. To supply the VME crate with four different voltages (±15 V, +5 V, +3.3 V), it is equipped with an according Power Supply Unit (PSU) and an additional fan and control unit to cool the electronics [62].

2.6.2 The Threshold Comparator Module (BLETC)

This subchapter describes the currently used version of the BLE Threshold Comparator (BLETC) module [63, 64]. It is to be upgraded by the new developed VFC-HD, compare subchapter 6.1.

The BLETC consists of two boards, the main processing Digital Acquisition Board (DAB64x) [65] and a plugged mezzanine card [66] receiving the tunnel data of two redundant optical links, *i.e.* four fibre connections in total, compare Figure 2.6. The module forms the digital processing unit within the beam loss read-out chain. Embedding the four photodiodes and receiver parts, the mezzanine de-serialises as well

as decodes the optical link data. Then, the DAB64x merges the individual CFC and ADC data of up to 16 detectors and compares the redundant packets to select the error-free data. These combined data get integrated in parallel and in real-time by the on-board FPGA within twelve different moving sum windows spanning between 40 µs up to 84 s, which are defined for protection against all kind of expected losses [64]. For each Ionisation Chamber unique loss thresholds are defined depending on its location and 32 different LHC beam energy levels [67].

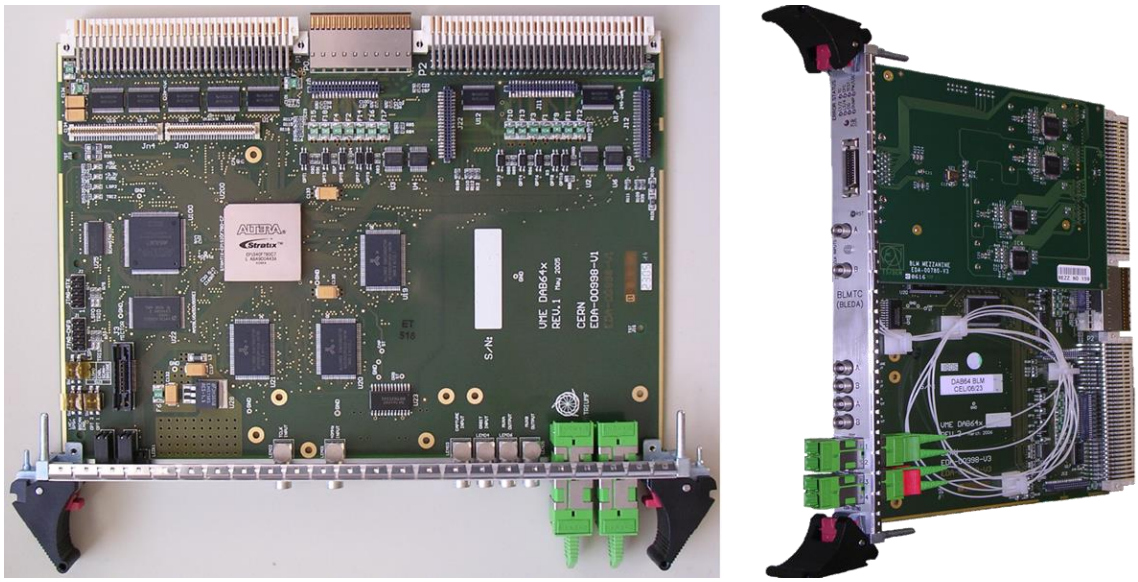


Figure 2.6: BLETC threshold comparator module composed of the DAB64x motherboard (left) [56] and the plugged mezzanine (right) receiving four optical fibre cables of two BLECF.

In the next processing step, the FPGA compares the moving sums and initiates a beam dump request if a threshold is surpassed. Subsequently, potential beam dump requests of the up to 16 BLETC per VME crate are transmitted via the daisy chains on the VME backplane and are handled by the BLECS in the last slot. This is implemented using a frequency signal to protect against board failures, but also against sudden reset or disconnection of the BLETC.

In order to always ensure the LHC protection, the BLETC is capable of autonomously performing the described threshold comparison to protect against failures of the CPU board. Apart from the described protection function, the module also comprises other functionalities, such as data recording for analysis, *e.g.* logging of transmission errors and reporting of tunnel statuses, provision of beam loss data for automatic collimator setup, or data to be analysed by LHC operators and for logging.

2.6.3 The Combiner and Survey Board (BLECS)

Situated in the last VME crate slot, the BLECS board [68] receives the two daisy chains of the BLETC modules establishing the link between the threshold comparison and the BIS. It forwards a potential beam dump request to the BIS using twice

two lines connecting to separate CIBUS interfaces inside the rack, compare Figure 2.1.

At each of the eight LHC surface points, the BIS connections are only established for the BLECS of the last VME crate, within a daisy chain comprised of the previous crates' BLECS boards, see Figure 2.2. Besides providing this link between the LHC BLM system read-out chain and the BIS, the BLECS is further responsible to receive the current beam energy value from the in the following described CISV module and to distribute this info to the 16 BLETC modules using dedicated VME lines.

These VME lines are also used to initiate certain BLETC test procedures on the modules, as described more in detail in subchapter 4.2. The checks involve for instance the test procedure of various regular checks prior to particle beam injection into the LHC, referred to as "Sanity Checks", compare subchapter 4.2. The BLECS is responsible to initiate such checks, *e.g.* by generating a modulation signal to be added to the Ionisation Chamber high voltage supply. Moreover for this particular check, it processes and analyses the read back results of the individual BLETC modules and provides these results to the external logging system. In case a certain test does not pass, the BLECS is able to remove the Beam Permit, which either leads to a beam dump request or inhibits injection into the LHC. This is also the case for different status information received by the previous read-out electronics.

2.6.4 Timing and Beam Energy Boards (BOBR and CISV)

To be able to compare the beam loss data to the varying thresholds which depend on the current LHC operation, two boards provide the corresponding values to the VME crate, compare Figure 2.1.

The Beam Observation Receiver (BOBR) board [69, 70] receives the Beam Synchronous Timing information from the Timing, Trigger and Control network [71]. Located in the central slot of the VME crates, the BOBR board distributes this information each time to eight BLETCs on its right and left slots [59]. In the event of a beam dump occurring, the BOBR forwards a trigger with the current time stamp to the BLETCs in order to freeze their collected post mortem data for the logging.

The reception of the present beam energy value is done by the Safe Machine Parameters VME Receiver (CISV) board [72], which is a development based on the Controls Timing Receiver VME (CTRV) [73] board. The present beam energy is determined by means of measuring the beam bending dipole magnet current and sent to the CISV from the LHC Safe Machine Parameters system via the LHC General Machine Timing system [74]. Per LHC surface point, one CISV board is located in the crate of the last BLECS board within their daisy chain (BLECS_4 in Figure 2.2). This BLECS board receives the beam energy information and distributes this info to the

other BLECS' of the surface point racks, as well as distributes it to the BLETC modules of the according crate for the threshold adaption.

2.6.5 The CPU board

The first slot of each VME crate is equipped with a board, referred to as Central Processing Unit (CPU) board. For this crate CPU, the LHC BLM system uses a commercial solution with available reliability report data provided by the manufacturer, the *A25* by "MEN Mikro Elektronik" [75]. The CPU enables to access the crate for development and technical support purposes through a gigabit Ethernet link. As previously outlined, for purposes of protection, the CPU board possesses no function which can cause any interruption of ongoing LHC operation. During operation, it establishes a link between the crate and the logging and post mortem systems. This includes the sending of potential warnings related to the beam loss data to the logging system and the LHC control room.

In order to feed the logging and post mortem systems, the CPU communicates with the up to 16 BLETC modules periodically (1/s) accessing their processed data. These data include for instance the beam loss data and applied thresholds, in particular the beam loss data of the straight sections for adjustment of the collimators or the recorded transmission errors and statuses of the optical link for offline analysis. The CPU reads all the data, calculates the warning level alerts, and normalises the data for display in the control room.

2.6.6 The High Voltage Power Supply (HV PSU)

Besides the powering of the surface electronic modules via the VME crate, the BE installation also comprises the High Voltage Power Supply Unit (HV PSU) to supply the FE Ionisation Chambers. In fact, two redundant HV PSUs are installed at each LHC surface point with cables connecting to the Ionisation Chambers inside the tunnel. Designed to deliver up to 3 000 V, the primary HV PSU is configured to deliver a nominal voltage of 1 500 V, with the secondary installed in hot redundancy, *i.e.* as spare unit immediately supplying the voltage in case of the primary unit failing. This is being implemented using an isolation diode with the spare HV PSU delivering 1 450 V, compare Figure 2.1.

As previously outlined, the HV PSUs are driven by the last BLECS board of their daisy chain. Connections are established to control the voltages as well as to re-check these values and to send warnings for the case of variations. This involves limiting the maximum voltage to 2 000 V in order to avoid internal discharges of the Ionisation Chambers. As described more in detail in the subchapter 4.2, the BLECS also generates the HV modulation signal to check the connectivity of the Ionisation Chambers.

3 Dependability Engineering Basics and State of the Art

Chapter 1 has outlined the importance of integrated luminosity for the successful operation of the LHC. This luminosity is directly connected to the performance of the LHC, regarding its reliability and high availability. For instance, one hour of availability loss, *i.e.* LHC downtime, can be linked to the calculated around 200 000 CHF hourly cost estimate in Eq. (1.6). To quantify these terms, this chapter provides the definitions, introduces the necessary mathematical and statistical basics, as well as existing analysis and test methods of dependability engineering. Furthermore, the last subchapter herein investigates the current state of the art regarding a methodological approach on dependability engineering during the life cycle of systems.

3.1 Definitions

The necessary terms and definitions for the scope of this work are specified in the following. The associated mathematical descriptions are outlined in subchapter 3.2.

3.1.1 Dependability and Associated Terms

The term dependability of an item is defined as the [76]:

"Ability to perform as and when required."

Dependability is often used interchangeably with the term reliability. In fact, according to [76], reliability is a part of dependability, which incorporates "availability, reliability, recoverability, maintainability, and maintenance support performance", as well as "durability, safety and security" in specific cases, see Figure 3.1.

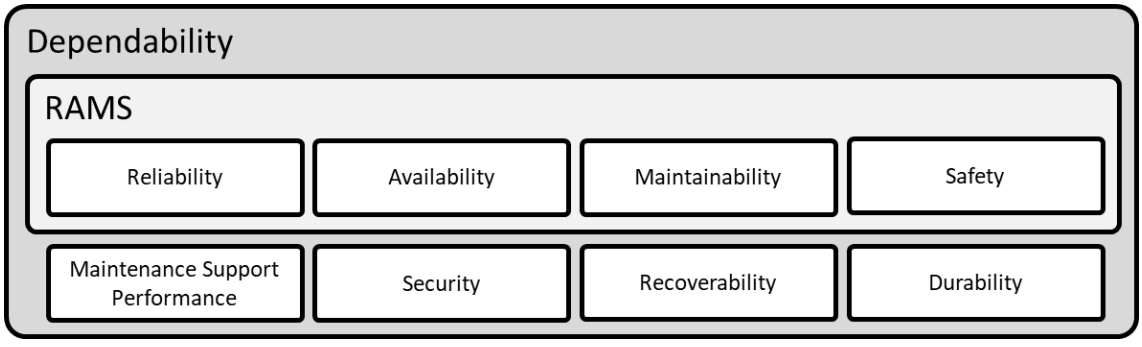


Figure 3.1: Areas of dependability according to [76] and the RAMS disciplines according to [77].

Covering the operating LHC BLM system with its machine protection function, performance requirements, available past experience, or continuous maintenance and upgrades, the scope of this work overcomes the extent of reliability engineering as it is often referred to in literature. In the same way, the presented methodology in chapter 5 of this work spans over several distinct areas of dependability.

Similarly, the collective term RAMS [77] is commonly used to compile Reliability, Availability, Maintainability and Safety. As illustrated in Figure 3.1, RAMS is considered a part of dependability. Thus, in the framework of this work dependability is used as an umbrella term, while reliability is referred to as the following.

Reliability

According to the above referenced IEC 60050-192 standard [76], reliability is defined as the "ability to perform as required, without failure for a given time interval, under given conditions". This definition is valid for the scope of this work, however for a system like the LHC BLM system with its vital main function of protecting the LHC, a slightly different definition is more suitable. In [78], B. Bertsche et al. define reliability rather in the later presented mathematical sense as a probability, and emphasise the intended function of the concerned system:

> *"The probability that a product does not fail during a defined period of time under given functional and surrounding conditions."*

Availability

Availability is a measure for the probability that a system is in an operable state. It is connected to reliability in the sense that on the one hand, 100% of reliability relates to 100% of availability, but on the other hand poor reliability does not necessarily relate to poor availability. According to [78], availability is defined as:

> *"The probability that a system is in a functional condition at the time t or during a defined time span, under the condition that it is operated and maintained correctly."*

To illustrate the relationship between reliability and availability, Figure 3.2 shows a system with rather high availability because of short maintenance intervals, but poor reliability due to a high rate of failure.

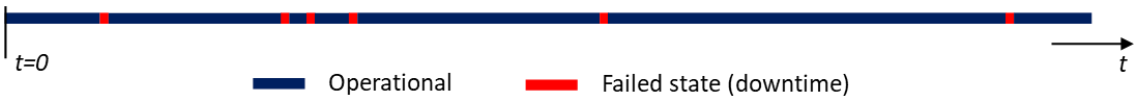


Figure 3.2: Relationship between reliability and availability. The high availability of 95% of the example does not reflect its reliability, characterised by six failures during the regarded time interval.

Maintainability

The definition of availability includes already maintenance. Maintainability refers to the time needed to bring a system back into operation after a failure, defined as [76]:

> *[The] "probability that a given maintenance action, performed under stated conditions and using stated procedures and resources, can be carried out within a stated time interval."*

In this manner, high maintainability is characterised by an efficient maintenance system, for example trained personnel or good spare parts availability, as well as by design solutions which allow interventions to be executed fast and efficient. The example in Figure 3.2 can be regarded as a system with a high degree of maintainability, because the time period to return to an operable state is fairly short.

Safety, Security and Protection

In the framework of RAMS in [77] and in IEC 61508-0 [38], safety is the *"freedom from unacceptable risk"*, with the annotation that risk refers to human health or the environment. Following this paradigm, safety is only of concern for certain access or supervision systems of the LHC as a closed machine. Nevertheless, in the closed LHC environment, machine protection can be interpreted in a similar way to replace safety within the RAMS disciplines. In fact, the IEC 60050:351 [79] standard which is related to [76] defines safety and security interchangeably, which is also owed to the fact that many languages do not differentiate between these terms. For all these reasons, this definition is used herein, referred to as protection in order to describe the protected state of the LHC aimed to be achieved by the LHC MPS systems [79]:

> *"Freedom from unacceptable risk to the physical units considered from the outside."*

Recoverability, Maintenance Support and Durability

The three remaining fields of dependability are summarised in Table 3.1:

Table 3.1: Definitions of Recoverability, Maintenance Support and Durability, according to [76].

Term	Definition
Recoverability	*"Ability to recover from a failure without corrective maintenance"*
Maintenance Support Performance	*"Effectiveness of an organization in respect of maintenance support"* *[Maintenance support: "Provision of resources to maintain an item"]*
Durability	*"Ability to perform as required, under given conditions of use and maintenance, until the end of useful life"*

3.1.2 Other Terms

To complement the previous subchapter, Table 3.2 displays terms already comprised in the above definitions and other terms necessary for the scope of this work.

Table 3.2: Other definitions related to dependability, according to [76, 80].

Term	Definition	Ref.
Criticality	*"Severity of effect with respect to specified evaluation criteria"*	[76]
Fault	*"Inability to perform as required, due to an internal state"*	[76]
Failure:	*"Loss of ability to perform as required"*	[76]
- Cause	*"Set of circumstances that leads to failure"*	[76]
- Effect	*"Consequence of a failure, within or beyond the boundary of the failed item"*	[76]
- Mechanism	*"Process that leads to failure"*	[76]
- Mode	*"Manner in which failure occurs"*	[76]
Risk	*"Combination of the probability of occurrence of harm and the severity of that harm"*	[80]
Validation	*"Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled"*	[76]

3.2 Mathematical Basics

In the mathematical sense, many of the terms described in the previous subchapter are quantifiable as statistical probabilities based on individual failure behaviour of technical components and systems. In order to quantify dependability parameters, this subchapter introduces these mathematical fundamentals, on the basis of the literature of B. Bertsche [78], W. Q. Meeker and L. A. Escobar [81], W. B. Nelson [82], P. O'Connor and A. Kleyner [83] and the United States (US) Department of Defense (DoD) Military Handbook (MIL-HDBK) 338B [84].

The term dependability is not mathematically defined, yet its constituent elements. To derive to a mathematical definition of these elements, the necessary statistics and probability theory are commonly referred to as "reliability theory".

3.2.1 Mathematical Description of Reliability

The reliability, or probability of survival, of a system comprises its failure behaviour and is defined as *R(t)*. To derive to the mathematical definition of *R(t)*, the failure density function *f(t)* has to be introduced first. It describes the frequency of failure times as a function of the time *t* or other variables for *t*, *e.g.* number of cycles, with

$$f(t) = \frac{dF(t)}{dt}. \tag{3.1}$$

f(t) is the derivation of the unreliability function or probability of failure *F(t)*, which describes the probability, that a system has already failed at a certain time *t*.

Analogue to Eq. (3.1), *F(t)* is the integral of the density function, characterised as

$$F(t) = \int_0^t f(t)dt\,. \tag{3.2}$$

For $t \to \infty$, *F(t)* equals 1, corresponding to the certainty that all systems within a population will eventually fail.

Finally, the reliability *R(t)* describes the probability of survival at a certain time *t*, as the complement of *F(t)* with

$$R(t) = 1 - F(t)\,. \tag{3.3}$$

Reversely to *F(t)*, *R(t)* is the probability that a system will survive up until *t*.

To determine the rate at which failures occur in time, the failure rate $\lambda(t)$ and the hazard rate *h(t)* are used. The failure rate $\lambda(t)$ describes the "ratio of probability that failure occurs in the [considered time] interval" [84], defined as

$$\lambda(t) = \frac{R(t) - R(t+\Delta t)}{\Delta t * R(t)}\,. \tag{3.4}$$

In other words, $\lambda(t)$ can be interpreted as the ratio of the sum of failures occurred and the total of operational hours during the time interval Δt. To describe the failure rate for $\Delta t \to 0$, the instantaneous failure rate or hazard rate *h(t)* is defined as

$$h(t) = \lim_{\Delta t \to 0} \frac{R(t) - R(t+\Delta t)}{\Delta t * R(t)} = \frac{f(t)}{R(t)}\,. \tag{3.5}$$

For the interval approaching zero, this instantaneous failure rate *h(t)* corresponds to the fraction of the failure density function *f(t)* and the reliability function *R(t)*.

Mathematically correct, the correlation between failure rate and hazard rate is defined as $\lambda(t) = \int_0^t h(t)dt$. However, the instantaneous failure rate *h(t)* is in many literature often erroneously referred to as $\lambda(t)$. Taking this fact into account, this work follows the convention set in [84], which mathematically accurate distinguishes between failure rate and hazard rate, but points out the fact, that both $\lambda(t)$ and *h(t)* are "usually used synonymously in conventional reliability engineering practice". As a conclusion, the failure rate is referred to as $\lambda(t)$, which is done in the same way within this work.

3.2.2 Statistical Values and Other Reliability Parameters

Apart from the failure rate $\lambda(t)$, additional parameters are used to describe reliability data. In particular for electrical and electronic systems, datasheets often present reliability data as Mean Time To Failure (*MTTF*) and Mean Time Between Failure (*MTBF*) or as failure rates in units of failures per million hours (fpmh) or Failure In Time (FIT).

Such reliability parameters are often determined using statistical values, for example the mean $\bar{x}$, which is defined for a sample of *n* values $x_1, x_2, \ldots, x_n$ as

$$\bar{x} = \frac{1}{n}(x_1 + x_2 + \cdots + x_n) = \frac{1}{n}\sum_{i=1}^{n} x_i\,. \tag{3.6}$$

The mean describes the average of the considered values, for instance failure times. It can be considered as the "centre of mass" of a distribution. For a symmetric bell curve, or normal distribution, $\bar{x}$ is located at the peak value, compare Figure 3.4 (1) for b = 3.5. For asymmetrical distributions, however, the mean can be sensitive to outliers, *i.e.* very low and very high values. Less sensitive to outliers is the median, which is located in the centre of all values x_n. For failure times, it is defined by

$$F(t_{median}) = 0.5\,. \tag{3.7}$$

To assess the dispersion, *i.e.* how much the values of a distribution vary from the mean, the variance *Var(x)* is given as the squared standard deviation σ,

$$Var(x) = \sigma^2 = \frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n}\text{, with} \tag{3.8}$$

$$\sigma = \sqrt{Var(x)}\,. \tag{3.9}$$

To obtain a better estimate when sample data is taken instead of population data, the *Var(x)* in Eq. (3.8) is often calculated with $n - 1$ in the denominator instead of n.

Based on the described statistical values, the *MTTF* is defined for a non-repairable system as the mean, or the expected value of the time to failure in hours, by

$$MTTF = \int_0^\infty t * f(t)dt = \int_0^\infty R(t)dt\,. \tag{3.10}$$

For a constant failure rate λ, the *MTTF* becomes

$$MTTF = \frac{1}{\lambda}. \tag{3.11}$$

If the system is considered repairable, the designation *MTBF* characterises the mean uptime between repair interventions, as illustrated in Figure 3.3.

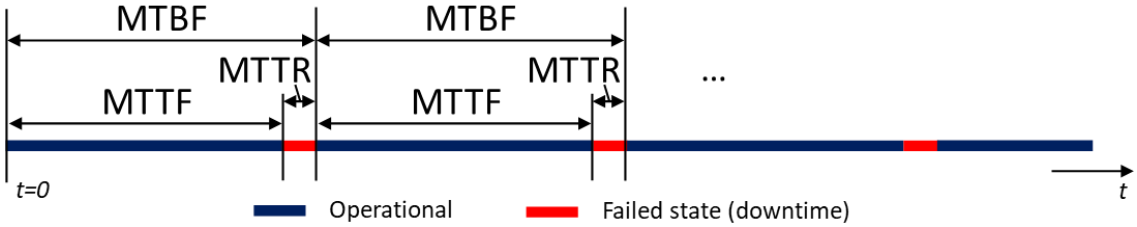


Figure 3.3: Illustration of the *MTBF*. For repairable systems, the *MTTF* is the mean time in operation until a failure occurs. The *MTBF* is comprised of the *MTTF* and the mean time to bring the system back into an operational state, the Mean Time To Repair (*MTTR*).

Hence, the aforementioned datasheet values present the reliability data either in hours as *MTTF* or *MTBF* for repairable systems, or alternatively as a constant failure rate λ in the frequently used units fpmh, which is failures per 10^6 hours and the for electronics more commonly used FIT, which refers to failures per 10^9 hours. For electronics, these values generally refer to the later described "useful life"-period, which is characterised by a constant failure rate.

3.2.3 Continuous Distributions

The functions *f(t)*, *F(t)*, *R(t)* and *λ(t)* describe the failure behaviour of a system. If the exact progression of these functions is of interest, specific lifetime distributions can be applied representing the behaviour in a continuous sense.

For the scope of this work, two distributions commonly used in dependability engineering are of interest. The one-parameter and mathematically fairly simple exponential distribution and the two- or three-parameter Weibull distribution, which is more flexible and thus able to fit a variety of different lifetime distributions.

Furthermore, the gamma- and its related chi-square distribution are also of interest to determine statistical confidence, as outlined later in subchapter 3.2.5. For other distributions, further literature can be consulted [78, 81-84].

The Exponential Distribution

The exponential distribution is commonly used to model the failure behaviour of systems, which are characterised by a constant failure rate $\lambda(t) = \lambda = \text{const}$. This often applies to electronic systems during their intended life, or "useful life" period, as described in the next subchapter.

The according equations for the exponential distribution are the following:

$$f(t) = \lambda e^{-\lambda t} \tag{3.12}$$

$$F(t) = 1 - e^{-\lambda t} \tag{3.13}$$

$$R(t) = e^{-\lambda t} \tag{3.14}$$

$$\lambda(t) = const. \tag{3.15}$$

For the special case of a constant failure rate, it is possible to assess the *MTTF* as shown in Eq. (3.11). Moreover, this circumstance enables to sum up individual component failure rates in order to determine the system failure rate λ_S for a system of n components:

$$\lambda_S = \lambda_1 + \lambda_2 + \cdots + \lambda_n = \sum_{i=1}^{n} \lambda_i \tag{3.16}$$

The Weibull Distribution

Developed in the year 1951, the distribution named after its creator Waloddi Weibull [85], evolved to be one of the most common lifetime distributions in the field of dependability engineering. The advantage of the Weibull distribution is its flexibility in fitting a wide range of distributions by introducing a shape and a scale parameter.

The according equations for the two-parameter Weibull distribution are the following, with β as the shape parameter and η the scale parameter, or characteristic life, for $\beta, \eta > 0$. Their various progressions are displayed in Figure 3.4.

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{3.17}$$

$$F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{3.18}$$

$$f(t) = \frac{dF(t)}{dt} = \frac{\beta}{\eta^{\beta}} t^{\beta-1} e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{3.19}$$

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\beta}{\eta^{\beta}} t^{\beta-1} \tag{3.20}$$

The three-parameter Weibull distribution is characterised by a failure-free time γ at the beginning of the product life, sometimes also referred to as t_0. This failure-free time γ defines the starting point of the density function. To obtain the according equations, the t variable of the above equations is to be replaced by t - γ.

As the scale parameter, the characteristic life η influences the location of the distribution on the abscissa as well as the abscissa scale, *i.e.* an increasing η value widens the function of *f(t)*, while keeping the shape parameter β constant. For the probability of failure *F(t)*, the characteristic life is the point on the ordinate where 1 - e^{-1} = 0.632, or 63.2% of the population have failed, compare Figure 3.4 (2).

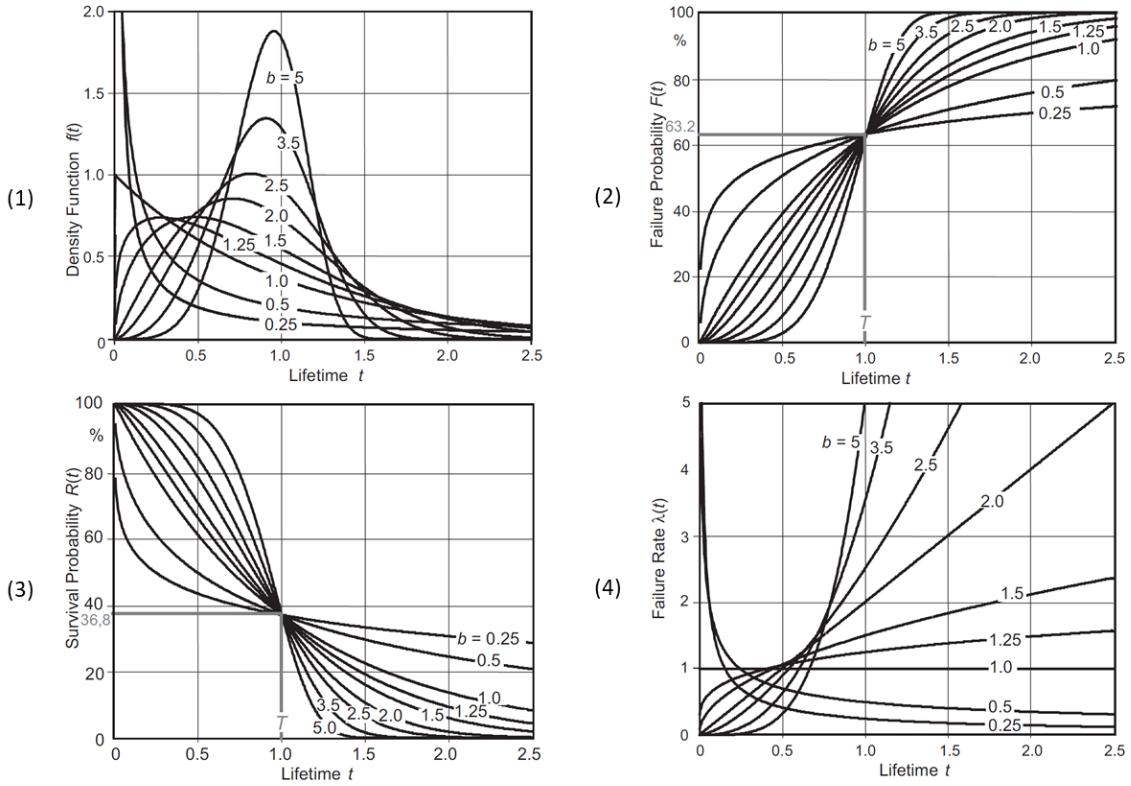


Figure 3.4: Weibull distributions for different shape parameters $\beta = b$ and the characteristic life of $T = \eta = 1$ [78]. The failure-free time is set to $\gamma = 0$.

Other designations used for η in literature are the distribution mean θ, which is equal to $1/\lambda$, analogous to the *MTTF* of the exponential distribution in Eq. (3.11), and

T [78], which for the three-parameter Weibull distribution further involves an adjustment of the characteristic life η - γ with $T = \eta$ in the above equations. This transformation results into a straight line on the logarithmic x-axis and double-logarithmic y-axis scaled "Weibull probability paper", compare Figure 3.6 (1) and [78], instead of a curved line without adjustment of η.

In Figure 3.4 (4), it can be seen that the failure rate is constant for a shape parameter of 1. In fact, the flexibility gained with β can be summarised as follows:

- $\beta < 1$: The failure rate decreases with time, a characteristic of failures occurring during the early phase of a product life.
- $\beta = 1$: The failure rate is constant, a characteristic of failures occurring random in time.
- $\beta > 1$: The failure rate increases with time, a characteristic of failures occurring at the end of a product life.

The previously mentioned normal distribution is represented by the Weibull with approximately $\beta \approx 3.5$. For the exponential distribution, this is the case for $\beta = 1$.

The Gamma and the Chi-Square Distribution

The gamma distribution can also be described by the Weibull distribution for a shape parameter of $\beta < 1$. Similar to the Weibull distribution, it is capable of describing various failure behaviours. The gamma distribution itself makes use of the gamma function $\Gamma(b)$ with the shape parameter b, as in [78]. In the context of this work however, not the gamma distribution itself is of interest, rather than a special case of it, the Chi-Square (χ^2) distribution. For a more detailed description of the gamma distribution further literature can be consulted [78, 81-84].

In the herein framework, the Chi-Square distribution $\chi^2_{(\alpha,\nu)}$ is used to determine statistical confidence, as dealt with in subchapter 3.2.5. It is a type of gamma distribution with in this context the acceptable risk of error $\alpha = 1 - C$, the quantile of the applied confidence level C, and ν the number of degrees of freedom, see Table 3.3. In practice, associated values for α and ν are contained in according tables, *e.g.* in [86].

3.2.4 The Bathtub Curve

To describe the failure behaviour of technical systems, as well as components during their lifetime, the bathtub curve describes a fundamental relationship in dependability engineering. As displayed in Figure 3.5, it is called bathtub curve because of its similar shape, which divides the curve into three sections.

Its left section, the early failures period, is characterised by an initially high followed by a monotone decreasing failure rate. This is caused by early, or infant mortality failures which occur by a variety of causes, such as manufacturing faults, design flaws or material defects.

The middle section is referred to as the "useful life" period. It shows an approximately constant, slightly decreasing failure rate. No category of failures is dominating, but the occurrence of random failures at a generally low rate. As stated, these failures occur randomly in time and are difficult to predict. Potential failure causes can be poor maintenance, environmental impact or of operational nature.

On the right of the bathtub curve, the section of wear out failures is situated. In this region, material wears out leading to failures. This can be caused by various material aging effects, fatigue or wear.

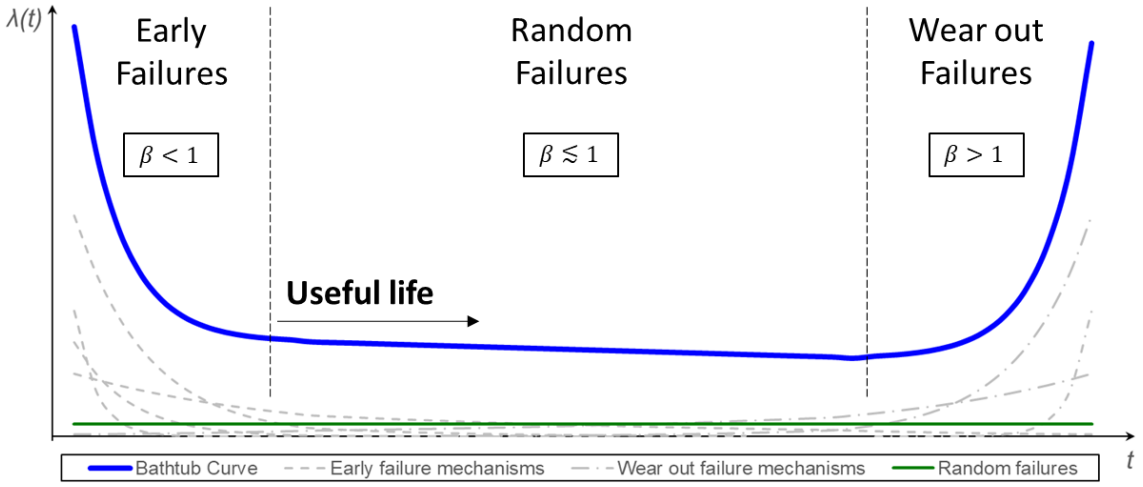


Figure 3.5: Bathtub curve illustrated for a system of various components. The first section is mainly influenced by a decreasing failure rate of early failures occurring (grey dashed progressions), the second region is characterised by an approximately constant failure rate, and in its third region, dominating wear out failures (grey dashed and dotted progressions) lead to an increasing failure rate. The green line represents random failures, which occur at a constant rate during the entire lifetime.

As shown in the previous subchapter 3.2.3, the individual sections of the bathtub curve can be described with the Weibull distribution. Shape parameters β smaller than, about equal to and higher than one separate the distinct sections.

As previously mentioned, the failure behaviour illustrated by the bathtub curve applies on the one hand to a single component with only two different failure mechanisms, one introduced at the beginning of its lifetime causing early failures of a few components, and the other mechanism leading to wear out at the end of its lifetime. An example can be a liquid electrolytic capacitor, with a small amount of badly manufactured components which induces cracks in their package, causing an early loss of the electrolyte, and thus a continuous decrease in capacitance up to an open circuit failure. A second failure mechanism can be caused by a poor design of the sealing, which very slowly but constantly leads to the electrolyte drying out and at the end of its lifetime to failures with the same failure mode. On the other hand, the bathtub curve also represents the failure characteristics of complete systems with several components and their individual failure mechanisms combined and summing up, as illustrated in grey colour in Figure 3.5.

An example on how to determine the first section of the bathtub curve based on actual failure data from tests is shown in Figure 6.17 of subchapter 6.5.6. Furthermore, the introduced methodology in chapter 5 covers how to make use of this failure behaviour to accomplish high reliability of an operating system. In general, high reliability can be determined from the bathtub curve by a low position of the bathtub on the ordinate, as well as a far right position, or late start of the wear out period.

3.2.5 Statistical Confidence

The previously described mathematical basics of reliability theory are based on statistics and probabilities. Therefore, complete certainty for the above parameters is not achievable. Specified values always include some uncertainty, respectively are to be specified with a certain confidence. This same confidence, or significance applied to dependability parameters is also required to obtained physics data at the experiments of CERN, *e.g.* the discovery of the Higgs boson required to surpass a significance of 5 σ (standard deviations), translating to a certainty of 99.999 9%, in addition recorded twice by the two independent detectors ATLAS and CMS [87, 88].

In dependability engineering, the application of statistical confidence includes for instance analysis of field failure data, reliability testing data in terms of sample size and testing time (compare Table 3.3), approximation of the constant failure rate during the useful life, or the risk assessment of an operating system.

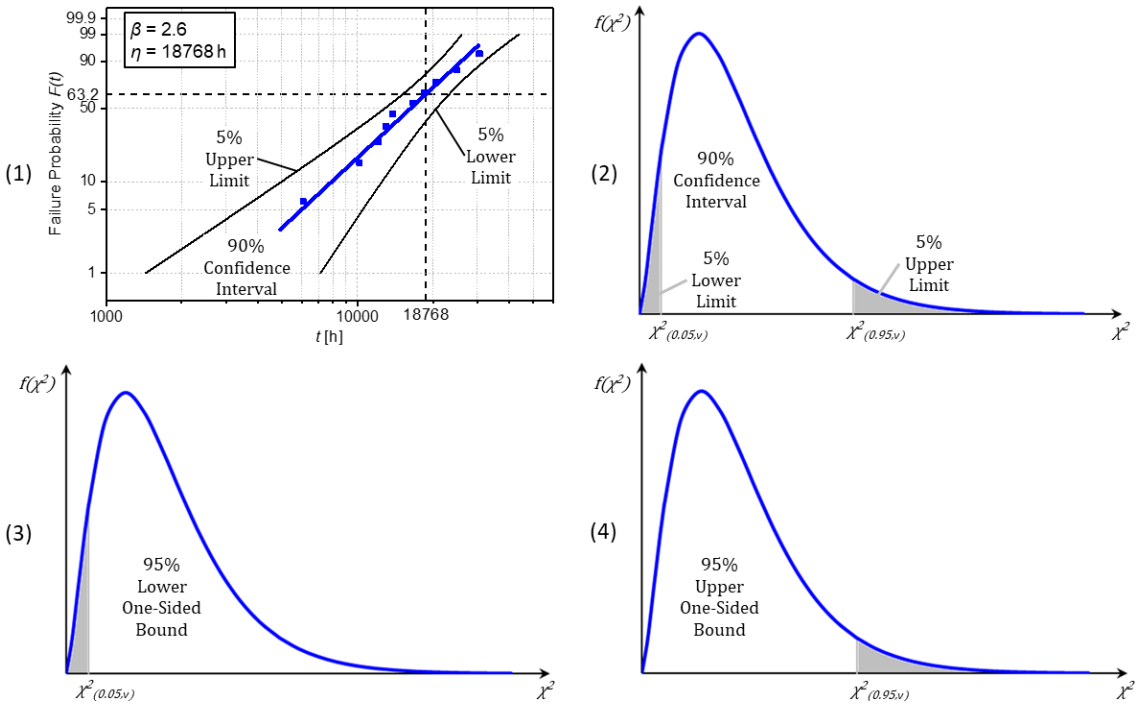


Figure 3.6: Various confidence intervals. Closed 90% confidence interval for the Weibull straight line (1, blue) and the Chi-Square probability density function with $\nu = 5$ (2). Left sided (3) and right sided (4) 5% confidence interval for the Chi-Square probability density function.

As displayed in Figure 3.6, a confidence interval is a certain range situated inside the full range of possible values, for example around the true value of the mean. It is an estimate that the observed data is within that range. The associated confidence level *C* quantifies the confidence that the data is inside the range of the interval as a percentage. A confidence level of 50% implies the precision of the estimate, that in 50% of cases, the observed value is located inside the confidence interval. For instance, the Weibull straight line in Figure 3.6 (1) uses the median rank method to determine $F(t_i)$, hence represents the boundary for which 50% of values are located above (lower bound), and the other 50% below the line (upper bound). A higher confidence level relates to a higher probability to cover the true value as in Figure 3.6 (1), or a higher coverage of the possible values as for Figure 3.6 (2, 3, 4).

The first two graphs of Figure 3.6 display closed, two-sided confidence intervals at a confidence level of 90%. If only a single limit of one side is of interest, *e.g.* to assess the lower reliability limit, a one-sided confidence interval as in the bottom two graphs can be used. Under the assumption of λ = const., the shown Chi-Square distribution $\chi^2_{(\alpha,\nu)}$ can be used to calculate the lower *MTTF* limit at a given confidence level for a reliability test or to prior determine the required test time for a maximum number of failures allowed. The degrees of freedom ν are represented by the corresponding mathematical term for the number of observed failures *r*, compare Table 3.3. In subchapter 6.5 this is applied to evaluate a Run In reliability test.

Table 3.3: *MTTF* calculation for time and failure truncated tests as well as different confidence intervals according to [83, 84]. t_{acc} is the accumulated test time, or the accumulated equivalent test time when additionally multiplied with an Acceleration Factor *AF*, compare subchapter 3.4.1.

Confidence Interval	Time Truncated	Failure Truncated
One-sided (Lower limit)	$MTTF \geq \frac{2t_{acc}}{\chi^2_{(\alpha,2r+2)}}$	$MTTF \geq \frac{2t_{acc}}{\chi^2_{(\alpha,2r)}}$
Two-sided (Lower and upper limit)	$\frac{2t_{acc}}{\chi^2_{(\alpha/2,2r+2)}} \leq MTTF \leq \frac{2t_{acc}}{\chi^2_{(1-\alpha/2,2r+2)}}$	$\frac{2t_{acc}}{\chi^2_{(\alpha/2,2r)}} \leq MTTF \leq \frac{2t_{acc}}{\chi^2_{(1-\alpha/2,2r)}}$

3.2.6 Availability and Maintenance Parameters

The definitions of availability and maintainability have been given in subchapter 3.1.1. In the mathematical context, availability involves the concept of repairable systems, specifying the two states “operational” and “repair”. To derive to a definition, the constant mean repair rate μ has to be introduced, defined using the *MTTR,* analogous to the failure rate λ as

$$\mu = \frac{1}{MTTR}\,. \tag{3.21}$$

As a general metric, availability is a probability between [0, 100]%. Following the definition in subchapter 3.1.1, a straightforward definition is the fraction of uptime and the total time supposedly in operation, the steady state availability A_{SS}:

$$A_{SS} = \frac{Uptime}{Uptime+Downtime} = \frac{MTTF}{MTTF+MTTR} = \frac{\mu}{\lambda+\mu} \tag{3.22}$$

This presumes constant values of the associated repair and failure rates, compare Figure 3.3. Furthermore, it assumes full restoration of the system state "as good as new" after a repair intervention.

Apart from this, literature distinguishes various other definitions, depending on the considered time interval or for other system states in between "up" and "down", *e.g.* [78, 84]. In here, the approach of [83] is followed differentiating between the steady state and instantaneous availability. Hence, the instantaneous availability *A(t)* is the probability that a system is in an operational state at time *t*, expressed as:

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \tag{3.23}$$

3.3 Analysis Methods

Based on the mathematical basics, different methods to not only analyse, but to also actively influence and improve the dependability of a system are presented in here.

3.3.1 Reliability Prediction and Alternatives

The early history of reliability prediction started in the 1950s. At that time, the electronic tube had been one of the most failing electronic components. This led to the study of the potential causes, concluding with the following needs: better reliability data; development of better components; establishment of reliability requirements, and reliability verification prior to production. Another conclusion was to install a permanent committee for reliability guidance, which later on led to the creation of the "Reliability Stress Analysis for Electronic Equipment TR 1100" standard work [89], a predecessor of the in 1962 by the US DoD introduced MIL-HDBK-217. [90]

In the following decades, the MIL-HDBK-217 developed to be a standard reference for requirements in specifications. Several versions in the meantime have led to its nowadays latest version MIL-HDBK-217F "Reliability Prediction of Electronic Equipment" [91] with its last revision in 1995 [92].

In addition, many other approaches to reliability prediction have been established. A brief overview is provided in the following subchapter. The second subchapter critically reviews the practice of predicting reliability based on mathematical models which rely on empirical failure data, as well as presents proposed

alternatives to the practice. The herein framework uses the term "reliability prediction" for such a quantitative bottom-up method. The third subchapter outlines alternatives, such as Physics-of-Failure (PoF), which are often also referred to as a reliability prediction method in literature [93]. The use and application of reliability prediction within the scope of this work is discussed in subchapters 4.5.1 and 5.2.1.

Different Approaches to Reliability Prediction

The already outlined variety of reliability prediction standards comprises generalised as well as tailored data collections and guidelines for different component categories and applications, compare Table 3.4. Their common approach is to estimate component failure rates using mathematical models based on historical failure data, while a few further include PoF models. Because of this variety and a certain similarity, only three concepts are described in here: the MIL-HDBK-217F and its potential successor, the Quanterion 217Plus™ [94], as well as the FIDES [95] approach.

The **MIL-HDBK-217F** (217F in the following) provides a reliability prediction guideline which uses historical failure data to quantitatively predict component and system failure rates. It uses two different methods to estimate the system failure rate. The fairly simple Parts Count Method estimates the reliability at early stages of the design, with the insufficient information available at that stage. It only takes into account the generic part types, their quantities, quality levels and the environment trying to estimate the reliability. The more elaborated Part Stress Analysis Method makes use of more available data in later design stages. Under the assumption of constant failure rates, it estimates individual part failure rates λ_p, for example as

$$\lambda_p = \lambda_b \pi_T \pi_A \pi_R \pi_S \pi_C \pi_Q \pi_E \text{ [96].} \tag{3.24}$$

A given constant base failure rate λ_b for the specific component category and type is multiplied, and in that way modified, by a variety of π-factors determined and adjusted for the specific component category, operational conditions and other parameters. These are for instance the operating temperature, the used quality level, applied electrical stress factors, or the category of environmental application.

The entire concept of the 217F is based on the assumption of a constant failure rate and the relationship shown in Eq. (3.16), which enables to sum up individual component failure rates to a system failure rate.

The **217Plus™** handbook was initially funded by the US DoD after the cancellation of the 217F in the 1990s, and can therefore be considered its successor. To assess the component (λ_p) and system failure rates (λ_P), 217Plus™ uses a similar approach than the 217F, but extends this by applying a combination of multiplication and summation of individual factors. Overall, the model is more complex than the 217F, which can be observed by Eq. (3.25) [94]:

$$\lambda_P = \lambda_{IA}(\pi_P \pi_{IM} \pi_E + \pi_D \pi_G + \pi_M \pi_{IM} \pi_E \pi_G + \pi_S \pi_G + \pi_I + \pi_N + \pi_W) + \lambda_{SW} \tag{3.25}$$

$$\lambda_p = \lambda_o \pi_o + \lambda_e \pi_e + \lambda_c \pi_c + \lambda_i + \lambda_{sj} \pi_{sj} \tag{3.26}$$

Both equations are established by several multiplicative terms which are summed up. The general form of the component failure rate λ_p in Eq. (3.26) separates operational- (index *o*), environmental- (index *e*), temperature cycling- (index *c*) and induced (index *i*) stresses and adds an additive term considering solder joint (index *sj*) failures. These individual terms are separated by generic classes of failure mechanisms intending to overcome the potentially strong influence of extreme values in Eq. (3.24). For the variety of π-factors indices in Eq. (3.25) refer to [94].

The **FIDES** methodology also takes a more complex approach using a similar combination of multiplication and addition. To estimate the failure rate λ of an item it considers physical, technological, manufacturing and process influences [95]:

$$\lambda = \lambda_{Physical} * \prod_{PM} * \prod_{Process} \text{ , with} \tag{3.27}$$

$$\lambda_{Physical} = \left[\sum_{Physical\ Contributions} (\lambda_0 * \prod_{acceleration}\ )\right] * \prod_{induced} . \tag{3.28}$$

$\lambda_{Physical}$ sums up physical contributions of applied stresses during operation with the individual basic failure rate λ_0 multiplied by the acceleration factor for the specific stress, compare subchapter 3.4.1. The multiplier $\prod_{induced}$ considers the contribution of different overstress, *e.g.* the influence of the geographical or functional placement in the system, the usage environment or the overstress consideration during development. To evaluate this factor, questionnaires which weigh different criteria are to be completed. The $\prod_{PM}$-factor similarly evaluates the manufacturing quality, and the $\prod_{Process}$-factor the development, manufacturing and usage process.

It has already been pointed out, that the complete variety of reliability prediction methods cannot be explained in this framework. For a more detailed overview, [97] can be consulted. Major standards are briefly summarised in Table 3.4.

Table 3.4: Overview of major reliability prediction standards for electronic components. Note that a few are either outdated or cancelled.

Standard	Publisher	Year	Comment
MIL-HDBK-217F	US DoD	1995	Generally obsolete models
217Plus™	Quanterion Solutions Inc.	2015	Comprehensive and complex
FIDES	FIDES group	2010	Very comprehensive and complex
IEC 62380	IEC	2004	Very comprehensive and complex; Cancelled, but pursued in IEC 61709
SN 29500	Siemens	2004 - 2016	IEC 62380 related; Several documents
SR-332	Telcordia Technologies	2016	Strong similarity to MIL-HDBK-217F

Critical Review of Reliability Prediction

Already in the year 1960, before the publication of the first MIL-HDBK-217, R. A. Davis and W. Wahrhaftig start their paper with [98]:

"The process of predicting reliability is usually treated like the weather; but we found that due to contractual requirements we had to do something about it."

Since then, the practice of reliability prediction of electronic systems has been discussed and criticised in a large number of publications, *e.g.* [83, 97, 99-106], yet continued to be widely applied [107]. Still nowadays, values determined from reliability prediction standards are found in device datasheets. The following paragraph summarises major aspects of the criticism, well considering, that the criticism may not apply on all existing standards, and without claiming full comprehensiveness.

Major points of the criticism are the general approach of intending to cover a comprehensive range of component categories [101], which comprises a great variety of individual failure mechanisms, based on sometimes very limited field failure data [107] potentially determined without knowledge, or correct assignment, of the exact failure causes [97, 99, 102]. Only component internal failure causes may be addressed [83], or only hardware failures sometimes accounting for just a small fraction of the overall failure rate [83, 102, 106], down to less than 10% [107]. Usually, this data has been acquired over a long period of time for different systems, operating in different applications, and at different and varying environmental conditions, for which potential statistical spread is not considered [107]. The same applies to not taking into account different design solutions, manufacturers and manufacturing processes [103]. Furthermore, the data is often outdated since it cannot keep pace with recent developments. This is especially the case for the rapidly evolving and highly innovative modern Integrated Circuit (IC) technologies with their life cycles becoming ever shorter [96, 97, 101, 106]. In a negative way, this can lead to misguiding design decisions or penalising the use of new technologies only for the reason that their reliability cannot be accurately predicted by outdated models with limited recent data [99, 102]. The same applies to design solutions aiming to improve the reliability, such as a circuit input protection, or redundancies, which owed to more components being summed up results in a higher failure rate [105]. Many standards also consider the predicted failure rate as an intrinsic characteristic, while real failures often have external causes such as design flaws, electrostatic discharge (ESD), mishandling, or other human factors [97, 101, 102, 105]. Although a few standards, *e.g.* 217Plus™ or FIDES, consider such aspects, it is nonetheless implemented in a qualitative way based on questionnaires, while other standards do not contain a method to determine the failure causes, and thus are unable to implement corrective actions. Associated to this, certain assumptions of the standards are viewed critical, such as the default constant failure rate for all component categories, for which possible statistical variation is not taken into consideration and which is generally true for big series systems with many components summed up, but in that way potentially concealing single failure mechanisms, which may still experience increasing failure rates [97, 101, 102, 106]. Another point of criticism is certain

model sensitivities, as previously discussed for extreme values [102, 108], *e.g.* quality factors, but also for small changes in certain model factors, *e.g.* the activation energy E_A of temperature models [104], compare Table 3.5. It is also criticised that steady conditions are often overrepresented in the models not considering temperature and humidity cycling, vibration or mechanical shock [104, 107, 108]; or addressing thermal interaction between mounted components [100]. Many studies have moreover shown large deviations between predicted values and the actual field reliability, as well as large deviations for predicted values of the same system determined by different standards [99, 102, 107-110]. In fact, operational experience of the US DoD has shown that out of 52 investigated defence systems between 2006 and 2011, 50% did not meet their predicted reliability goals [97].

Aside of the criticism, another aspect of performing reliability predictions is that it is a very time consuming practice, requiring a certain degree of detailed knowledge, tying up resources and creating costs.

To overcome the shortcomings of reliability predictions, executing dependability analyses is often suggested as outlined in the subchapters 3.3.2 and 3.3.3, as well as reliability testing, described in subchapter 3.4. One of the main critics based on the number of publications on that topic, is the Center for Advanced Life Cycle Engineering (CALCE) of the University of Maryland, frequently represented by Prof. M. Pecht. To address certain of the criticised aspects of reliability prediction practice, as mentioned, design analyses are proposed embedded in a "reliability assessment methodology", including practices such as Design for Reliability (DfR) and criteria to determine the need of testing [107]. DfR is a process uniting different tools during the design phase, for manufacturing and beyond that, to enhance the system reliability, see [97, 111]. M. Pecht et al. furthermore emphasise replacing reliability predictions by "physics-of-failure methods and with estimates based on validated models" and to pursue "holistic design methods" to address the diverse aspects of system reliability [97]. PoF itself is considered a DfR sub-area, see next subchapter.

M. Pecht is also an author of the "IEEE standards on reliability program and reliability prediction methods for electronic equipment" [112], describing efforts of the Institute of Electrical and Electronics Engineers (IEEE) on reliability prediction and proposed alternatives. The mentioned standards are the IEEE 1332 [113], yielding guidance in planning a reliability program for electronic system development and production, and the IEEE 1413 [114] providing a methodology for reliability prediction and assessment. A more detailed description follows in subchapter 3.5.

To summarise essential aspects of this subchapter for the context of this work: despite the negative points, the execution of a reliability prediction yet can be beneficial during the design process of electronic systems, as further elaborated in subchapter 5.2.1. By doing so however, it needs to be stressed that the determined reliability values should not be used to fulfil any kind of dependability requirement.

Design for Reliability (DfR) and Physics-of-Failure (PoF)

The proposed alternative to reliability prediction, **DfR**, is a process comprising a variety of techniques and practices to already enhance the system dependability from the initial design phases onward. Such techniques are for example the FMECA and FTA analyses (subchapters 3.3.2 and 3.3.3), PoF methods, root-cause analysis, and other techniques suitable for the concerned system. A principal objective of DfR is to minimise the required efforts in terms of resources and costs by successfully applying the necessary techniques early in the development process to avoid or reduce corrective measures, testing expenses, or, even more severe, to prevent expensive field failures and recalls. More details on DfR can be found in [83, 97, 111, 115, 116].

Amongst the DfR techniques, **PoF** is a deterministic method [117] which intends to determine potential failure mechanisms and their root-causes occurring during the product life, and to predict their propagation up to the point of failure with an appropriate model. PoF requires detailed knowledge of the design - including component characteristics, geometries and materials used; manufacturing process, application, and both operational and environmental parameters and stresses. Furthermore, knowledge about potential failure mechanisms and the structural, mechanical, thermal, electrical or chemical processes leading to failure at specified sites is necessary. This all enables PoF to adapt to changing factors like new designs, materials, processes, and other technological advancements.

While it can be a complex method requiring resources and a high degree of expertise, PoF comprises the advantages of obtaining a detailed analysis of potential failure causes instead of considering the component or system as a black box, as being done by reliability prediction, and, in that way, predicting a more accurate time to failure. The detailed knowledge of the failure physics also enables PoF to be applied within Prognostics and Health Management (PHM) [118, 119]. PHM is a method, which monitors performance or physical degradation during system operation, *e.g.* using sensor data, in order to determine the remaining life, *i.e.* the reliability, based on PoF models, and in that way aligning necessary actions such as maintenance. For more information on PHM, refer to [120, 121]. More detailed information on PoF can be found in [117, 122-126], corresponding models are presented in Table 3.5.

3.3.2 Failure Mode, Effects, and Criticality Analysis (FMECA)

Dependability design analyses provide a tool to overcome shortcomings of reliability prediction by enlarging the extent of the analysis from the level of individually considered components to the higher functional level and the system level. One of the most popular and most applied method is the FMECA, also referred to as FMEA.

The Failure Mode and Effects Analysis (FMEA) was first introduced in 1949 by the US Military and developed in the following, on its pathway of being used for the

NASA (National Aeronautics and Space Administration) Apollo project, in the avionics industry and widely in the automotive industry, to be a common practice of dependability analysis. The analysis is performed in five steps: first analysing the system, second determining potential failure modes and their effects, then assessing the risk and lastly taking actions and optimising the design, see Figure 3.7. Its execution starts during the early design process as a dynamic method, accompanying the full design cycle whilst being constantly adapted and modified. [78]

Figure 3.7: The five steps of the System FMEA, according to [78].

The first two steps perform the system analysis of the current design solution. In the first step, the structure of the system is created by means of collecting all its constituent subsystems and single elements and organising them on hierarchical levels in a structure tree. The second step assigns the individual functions to the elements creating a function structure, or network if more suitable. In the electronics design process this is often available as a functional block diagram. [78]

The last three steps comprise the risk analysis and consequential optimisation actions. The risk analysis performed at this point is part of the FMEA [78], often also referred to as Criticality Analysis (CA) [84, 127], separately addressed by the abbreviation FMECA used hereafter. The third step is connected to the second making use of the determined functions to identify the potential failure functions in order to assign all potential failure modes to the individual elements. On the component level of electronics this is usually straightforward, for example is a resistor characterised by three potential failure modes: a short or open circuit, and a change in its resistance value. Corresponding collections provide summaries for different component categories [128, 129]. On higher system levels, failure modes might be determined by negating the block functions. Also failure statistics, internal experience or checklists may be consulted. In fact, failure modes on the component level lead to the potential failure effects to be determined on the next higher level. This is done up the hierarchy, until the “end effects” on the system level are identified. [78]

The subsequent fourth step performs the risk assessment, or CA. Figure 3.8 illustrates two methods to assess the risk: the Risk Priority Number (*RPN*) and the risk matrix, also called criticality matrix. This is because its axes scale the two factors defining criticality: the Severity (*S*) of the in the FMECA determined effect and the Occurrence probability (*O*) of the failure mode [127]. The *RPN* further takes a Detection (*D*) ranking into account characterised by the probability of detecting the

concerned failure cause during the development or production [78]. In another context, *D* may also be used as the probability of detecting potential failures or their causes during operation in order to prevent further potential failure effects [78], for instance to evaluate the efficiency of system checks. The individual rankings of *S*, *O* and *D* are commonly defined between 1 for a very low severity and occurrence probability, and a high detection probability, up to 10 for opposite rankings. The lower the rankings are, the lower the corresponding risk. Tables for the determination of these rankings can be accessed in [78, 84].

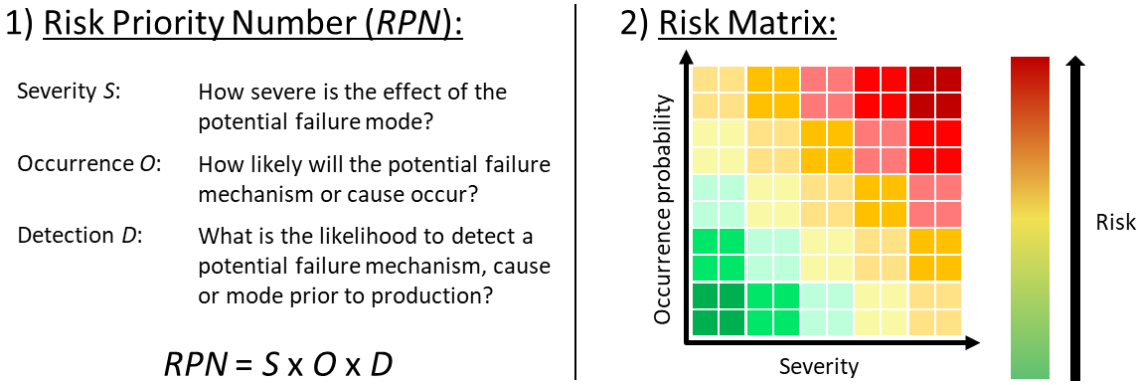


Figure 3.8: Risk assessment methods using the *RPN* and the risk matrix. The three *RPN* factors *S*, *O* and *D* are defined according to [84]. The risk matrix illustrates the risk on a colour scale.

The final fifth step uses the output of the risk assessment and realises optimisation actions if necessary. The necessity of these actions follows the priority established by the *RPN* or the colour scale of the risk matrix. An individual maximum risk limit can be defined in accordance with the dependability goals.

To conclude, this subchapter has presented the steps of an FMECA to analyse and optimise a system design, also referred to as DFMEA. The method however, may also be applied beyond system design as a Process FMEA (PFMEA) to identify and mitigate potential errors of a manufacturing process, see [78]. Two examples of system design FMECAs can be found in subchapters 4.5.2 and 6.3.3.

3.3.3 Fault Tree Analysis (FTA)

The FTA is a deductive method which creates a tree structure of potential system and lower level faults and their dependencies. In contrary to the FMECA analysing the system “bottom-up”, the FTA is performed “top-down”. In this opposite manner, the fault tree starts by determining undesired events, or potential failure effects on the top system level. These “top events” are equal to the end effects of an FMECA. Starting from these top events, the remainder of the tree is created by assigning potential failures of the next lower level, which may cause these higher level events. This is pursued until the lowest system level is reached, or can be terminated if the reached level meets the required resolution for the analysis. [78]

The logical connection of the different levels is established using Boolean algebra. A variety of event blocks and connecting gates can be used, see Figure 3.9. For example, an OR gate implies the higher level event is caused if any of the inputs fails (series structure), an AND gate if all inputs fail (parallel structure; redundancy). [78]

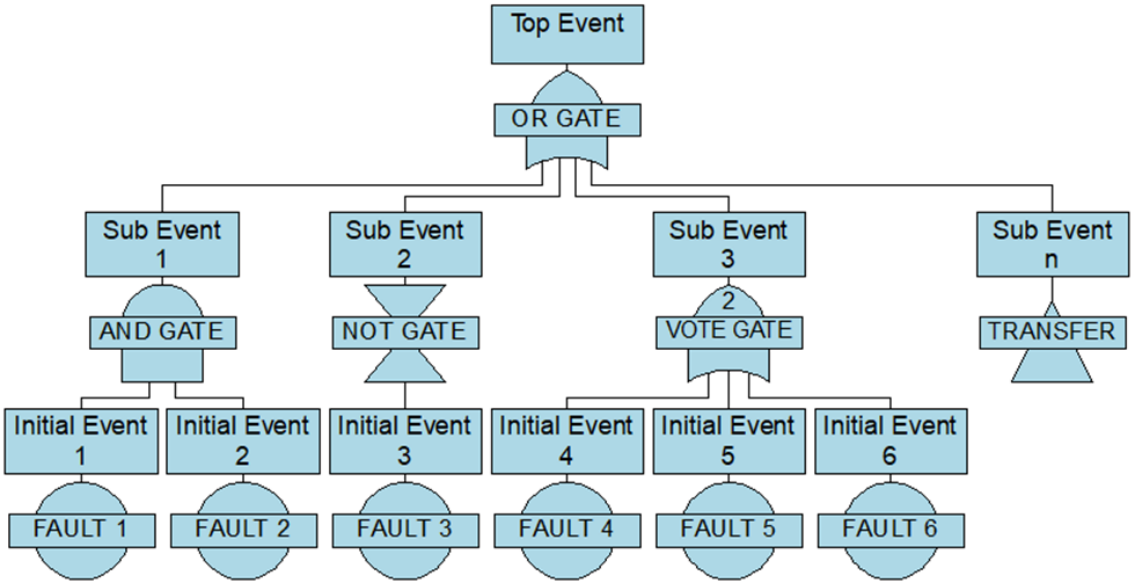


Figure 3.9: Three level fault tree. The top event is caused by any of the *n* sub events (OR gate). Sub event 1 represents a redundancy, caused if both initial events occur (AND gate). The NOT gate of sub event 2 negates its input. It is triggered if initial event 3 changes its state. The VOTE gate represents a two-out-of-three redundancy. It causes sub event 3 if two of the connected initial events occur.

An FTA can be used during the design phase of a system in order to identify potential system failures, compare different solutions and facilitate design decisions. For instance, applying the "minimum cut set" method, the smallest combination of failure modes which leads to a specific top event can be evaluated, see [83]. Taking the LHC BLM system as an example, this can be applied to review its protection function. The FTA is performed qualitatively by deductively assigning potential failures top-down to the component level, but may also be performed quantitatively if available component failure rates are assigned to the blocks.

In practice, an FTA is often executed with the aid of dedicated software. In fact, certain software packages allow to convert an FMECA into an FTA, as well as already to convert a determined system structure within a reliability prediction into an FMECA. A comprehensive dependability analysis previously performed that way allows at the stage of the FTA to implement system redundancies, foreseen system checks (online and offline) and maintenance interventions to be executed. Such a detailed dependability model enables to accurately simulate the system availability and to develop a strategy for diagnostic checks and maintenance. It is pointed out, that such an FTA model does not serve to identify potential system faults, already done bottom-up within the FMECA, it rather serves to simulate the operational performance.

3.4 Reliability Testing

Previously, reliability has been defined as the probability that a product does not fail under given functional, environmental and time conditions. At the point in time where the applied stress exceeds the strength of the design, *R(t)* equals zero leading to an immediate failure. This stress-strength relationship does not only apply to an instantaneous point in time, but also to a period of time during which the product suffers degradation. Furthermore, the applied stress and the strength of the design are characterised by distributions, as illustrated in Figure 3.10.

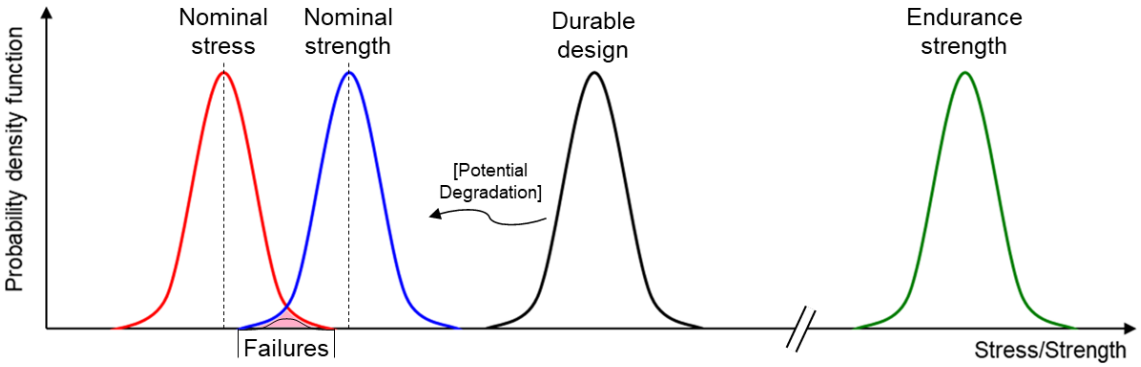


Figure 3.10: Stress-Strength Interference, also referred to as "Load-Strength Interference". Products with a low strength fail if operated in the overlapping area at high applied stresses. Durable designs do not immediately lead to failures, but may over time as a result of degrading strength. Designs for endurance strength generally do not show failures during their foreseen lifetime.

This Stress-Strength Interference involves every designed product exposed to stresses. Unless a product is designed enduring, it reaches at a certain point during its lifetime the wear out region of the bathtub curve as a consequence of degradation. This is represented by the black distribution of Figure 3.10 over time approaching towards the red distribution of exposed stresses. The point in time when these distributions overlap can be predicted by performing tests exposing the product to higher stresses than in operation, in that way “accelerating” degradation and time. The normal distributions illustrated in Figure 3.10 represent scattering product parameters induced by deviating quality. They can be characterised by a variety of other shapes (compare [83]), which is why an interference with the stress distribution is already possible at the beginning of a product life resulting in early failures.

The following two subchapters present corresponding tests to identify and screen such weaker products before the start of operation and tests to determine the margin for degradation in order to predict the lifetime.

3.4.1 Accelerated Life Testing (ALT)

In the framework of PoF, it has been illustrated previously how models can be applied to describe propagating failure mechanisms. The models and their underlying

stresses, for example voltage, power or temperature, but also cycling conditions of these parameters, can be used to perform ALT. The models are generally determined as displayed in Figure 3.11. Strength distributions at different stress levels are determined for the tested failure mechanism(s). Based on the obtained data a mathematical model is computed which represents the correlation of the strength and the stress level, scaled by lifetime or number of applied cycles for instance. In general this correlation is expressed by an Acceleration Factor AF as a ratio of the product life at the field stress level L_{Field} and the accelerated stress level during the test L_{Test} [83]. Hence, these models serve to predict the failure behaviour of a system during operation at low stress conditions based on ALT data obtained at high stress.

$$AF = \frac{L_{Field}}{L_{Test}} \tag{3.29}$$

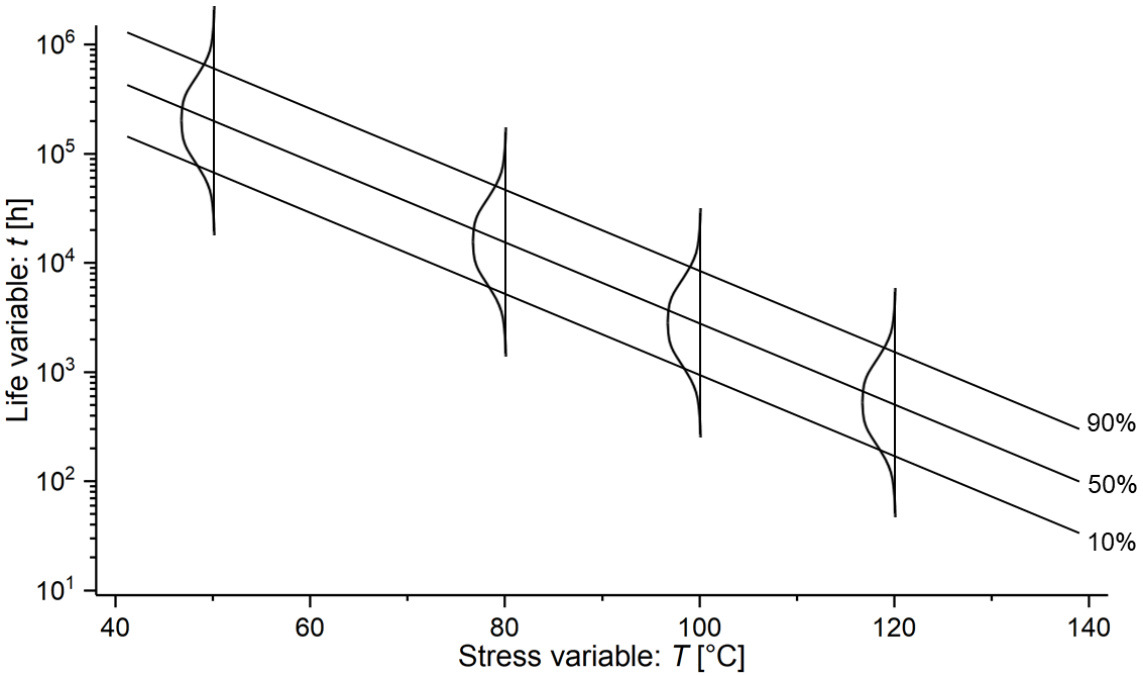


Figure 3.11: Example of the Arrhenius-lognormal life model, according to [81]. The life-stress relationship is represented by straight lines in the logarithmic plot based on four stress levels.

Table 3.5 presents an overview of existing life-stress models. For more information on the models, their application as well as other existing models please refer to [83, 86, 123, 126, 130, 131]. For electronics, a widely applied model is based on the Arrhenius temperature relationship illustrated in Figure 3.11. For instance, amongst other qualification tests IC components are commonly qualified performing High Temperature Operating Life (HTOL) [132, 133]. HTOL operates the components statically or dynamically at high temperature and voltage, *e.g.* $T_j \geq 125°C$ and $V_{cc} \geq V_{cc,max}$ [133], for a specified time in order to provoke potential failures.

Table 3.5: Selection of Acceleration Factors *AF* for different life-stress models, see [83].

Model	**Acceleration Factor *AF***
Arrhenius (Temperature)	$AF_T = e^{\left[\frac{E_A}{k}\left(\frac{1}{T_{Field}} - \frac{1}{T_{Test}}\right)\right]}$
Peck (Temperature-Humidity)	$AF_{TH} = \left(\frac{RH_{Test}}{RH_{Field}}\right)^m e^{\left[\frac{E_A}{k}\left(\frac{1}{T_{Field}} - \frac{1}{T_{Test}}\right)\right]}$
Inverse power law (Voltage)	$AF_V = \left(\frac{V_{Test}}{V_{Field}}\right)^B$
Mechanical fatigue (Sinusoidal/Random vibration)	$AF_{sin} = \left(\frac{G_{Peak\text{-}Test}}{G_{Peak\text{-}Field}}\right)^b \quad ; \quad AF_{random} = \left(\frac{G_{RMS\text{-}Test}}{G_{RMS\text{-}Field}}\right)^b$
E_A: Activation energy [eV]	V: Voltage [V]
k: Boltzmann constant (8.62E-05 eV/K)	B: Voltage acceleration parameter [-]
T: Temperature [K]	G: Acceleration [m/s^2]
m: Humidity power constant, typically [2.0, 4.0]	b: Fatigue exponent, commonly [4.0, 6.0] for electronics related failures
RH: Relative humidity [%]	

3.4.2 Screening of Electronics

To avoid a high failure rate during the early product life as shown in Figure 3.5, the products can be operated prior to starting their intended use while screening failed devices. In the same way as ALT, this screening can be performed at accelerated conditions. In fact, in [132] it is outlined that tests such as HTOL performed for "a short duration […] may be used to screen". Such stress screening based on either temperature, voltage or current stress is commonly known as burn-in. A broader term is Environmental Stress Screening (ESS) which encompasses procedures applying different stresses in order to provoke defective products to fail while not inducing defects, activating other failure mechanisms, or significantly affecting the useful life of "healthy" products.

The variety of ESS stresses applied should be tailored to the specific product design and its later application, while different stresses may be combined. Screening may be performed on the component or assembly level, while it is more complex for assemblies which generally comprise a variety of different component categories and technologies as well as a more extensive manufacturing process. The definition of screening stresses, their intensity and time of exposure requires knowledge of potential early failure mechanisms. Their origin may stem from the design or manufacturing. Furthermore, it is important to take potential environmental stresses during operation into account. For the assembly level it has particularly been shown, that temperature cycling is the most effective stress [84, 130]. This is followed by random vibration, high temperature and electrical stress [84].

For the particularity of each system the definition of ESS conditions is generally very specific. Some general guidelines can be found in [134, 135].

3.5 State of the Art: Methodological Approach on Dependability Engineering

A variety of different methodological approaches, procedures and other methods to apply, analyse, improve, track or support dependability during the life cycle of technological systems, in particular of electronic systems, exist. Some of these treat tailored methods for specific use cases whilst others provide fundamental basics of dependability engineering. This subchapter investigates the state of the art of methodological approaches to dependability application during the entire life cycle of electronic systems with special focus on the methodology introduced in chapter 5. Please note that some of the below described literature, *e.g.* of the US DoD or IEEE, do not follow the used IEC definition of dependability [76], instead referring to dependability by the term reliability.

The **MIL-HDBK-338B** [84] of the US DoD is one major source of literature. Originated in the year 1984 as MIL-HDBK-338, the superseding version 338B of 1998 is the nowadays latest version, which was last reviewed and found to be valid in 2012 [136]. It is one of the most exhaustive reference guides on the topic comprehensively covering basics of dependability engineering, *i.e.* the underlying theory of the RAMS disciplines, and a wide range of methods as the previously described FMEA or FTA. Furthermore, it provides design guidelines, for example for component derating, reliable circuit or fault tolerant design, and introduces methods such as design for reliability (a structured part selection and design process including analytical techniques [84], similar to DfR), design for manufacturability, or design for testability. In this context, it also gives guidance for production and use, including quality control measures, ESS or reliability data collection and analysis, as well as for shipment and storage. To only name a few more, the 338B also encompasses topics such as design reviews, software reliability or accelerated testing. Its ultimate chapter covers reliability management considerations, which comprises a methodological approach in the form of a reliability program outlining reliability management and engineering tasks during the life cycle phases: 1) Planning and control, 2) Analysis, 3) Testing, 4) Production and 5) Other. Furthermore, citing the variety of associated US Military specifications, standards and handbooks, the 338B includes powerful reference sources, which are all aligned with each other.

The earlier mentioned **IEEE 1332** [113] and the interrelated **IEEE 1624** standard [137], both from reliability working groups chaired by M. Pecht, provide a set of standards to develop a reliability program covering the life cycle of electrical/electronic (E/E) components or products and by these means to assess the organisational reliability capability.

The IEEE 1332 “Reliability Program for the Development and Production of Electronic Products” defines a set of three reliability program objectives established in

a supplier/customer relationship: 1) Requirements, 2) Engineering, and 3) Feedback. The objectives cover the (1) determination of reliability requirements in the early planning phase including the provision of appropriate resources comprising training to improve employees' skills and knowledge; (2) performing tasks, such as the DfR process, reliability analyses and testing during the engineering phase, or verification and validation of these efforts; and (3) tracking and analysis of all kinds of available failure data, and corrective actions within reliability improvement efforts during the engineering phase and especially during the following field use. This includes lessons learned for future projects. [113]

Expanding the IEEE 1332, the IEEE 1624 "Organizational Reliability Capability" provides a measure of the effectiveness of the reliability program comprised of its reliability practices and reliability activities of an organisation. In five distinct levels, eight key practices comprised in IEEE 1332 may be assessed qualitatively or quantitatively to determine an organisation's reliability capability. The lowest level 1 is characterised by a lack of consistency in reliability procedures with no clear such effort on the organisational level, while the top level 5 requires reliability to be "an integral part of strategic business planning" [137]. This means that reliability, respectively dependability, is a continuous and wide-spanning improvement effort of an organisation encompassing the full product life cycle. This involves taking a proactive perspective on present and future dependability challenges. [137]

Within the comprehensive IEC standard collection, the **IEC 61508** [38] deals in its eight parts with functional safety introducing the SIL classification, which has been used to design the LHC MPS. Having its focus on safety, its second part (Part 1) describes an "overall safety lifecycle" for E/E and programmable electronic systems and outlines corresponding activities from the early concept phase through 14 other phases comprising for instance risk analysis, validation or maintenance tasks, to the final decommissioning phase. Based on four defined Safety Integrity Levels, each classified by the frequency of a dangerous failure per hour of which the failure rate λ is a major factor, the standard allows to specify and accomplish a target level of safety integrity for a function of the concerned system.

A similar relevant IEC standard is the **IEC 60300** "Dependability Management" [138], defining in its first two parts six life cycle phases from the concept and definition to the last disposal phase. In these phases, a sequence of six activities is outlined beginning with the definition of dependability objectives and ending with an evaluation step of the achieved dependability results, providing the possibility to return to an earlier step and iterate the sequence. Intermediate steps comprise analysis, strategy planning to the implementation of dependability activities, and the analysis of the activities' results. The other parts of the IEC 60300 provide a comprehensive collection of dependability analysis methods, field data collection and analysis, dependability specification, testing, risk assessment, maintenance aspects

including measurement of maintenance performance, and system dependability aspects, reaching a level of comprehensiveness similar to that of the MIL-HDBK-338B.

In context to the IEC standards, two more standards remain to be mentioned. The automotive **ISO 26262** [139] is a recent and nowadays widely applied standard pursuing the concept of the IEC 61508, introducing four Automotive Safety Integrity Levels (ASIL) similar to the SIL. The **IEC 61513** [140] is tailored for nuclear power plant instrumentation and control for systems, showing large similarities to accelerator systems, in particular beam instrumentation systems such as the LHC BLM system. Also focusing on safety, it provides guidance on dependability activities within the safety life cycle of these systems from requirements definition up to operation and maintenance. Another similarity is the presence of a radiation environment at the nuclear power plant.

Besides standard works, a variety of book literature also comprise methodologies for dependability application. The most relevant are mentioned in the following paragraphs. A list of other publications on methodological approaches for dependability during the life cycle is provided in [111, 115, 116, 124, 141, 142].

B. Bertsche et al.'s books [78, 143] present fundamental dependability basics, analysis and test methods for mechanic and mechatronic systems. An introduced "reliability assurance program" focusses on the entire product life cycle, giving guidance during the product definition, design, production and use steps. Addressing mechatronic systems, the **V-model** [144], a "design methodology for mechatronic systems" is described. On the two arms of the V-shaped model, this methodology comprises the different process steps of system design starting from requirements within the three domains of mechatronics on its left arm. On its right arm, dependability assuring steps, *i.e.* verification and validation, are performed during various integration steps vice versa to the other arm creating the final product. The full process is accompanied by modelling and model analysis.

G. Yang [145] distinguishes in "Life Cycle Reliability Engineering" six phases during which he outlines a series of reliability tasks within a reliability program: first setting up the program suitable for the individual product, then to "design-in" the reliability using different techniques, thereafter verifying the design and validating the production process using tests, as well as assuring stable processes, and finally pointing out, that the program reaches even beyond the field deployment phase by means of analysis and processing of field data.

K. C. Kapur and M. Pecht [146] define ten reliability and quality management related activities during the system life cycle. The steps are interconnected forming a loop with the last two steps evaluating and continuously providing feedback to the first and other previous steps. Similar to the IEEE 1332, the concept can be regarded as an ever-improving reliability program.

A. Birolini [130] defines 20 "main tasks for quality and reliability (RAMS) assurance" to be performed throughout five basic life cycle phases of complex equipment and systems. This includes a variety of engineering tasks, but also management tasks, such as a motivation and training program for involved engineers.

D. N. Prabhakar Murthy et al. propose a model for "making decisions relating to performance and specification" [147] in development linked to five product life cycle phases. Furthermore, the three stages (I) pre-development, (II) development and (III) post-development, as well as eight further sub-phases are defined within the life cycle, in which either business, product or component related activities are outlined. An overall process in the form of a flow diagram links the eight sub-phases integrating "Yes/No" decisions and step iterations.

Taking a more practical approach, **A. Kleyner and P. D. T. O'Connor** [83] cover a wide variety of dependability disciplines during the life cycle. Putting the importance of a reliability program in relation to the associated risk of failure, they propose a "Reliability Programme Flow", which ranges from the specification of a product up to its service life. The methodology is based on continuous feedback of information between steps for potential design iterations and uses DfR as a central element within the design phase. Besides outlining activities during the different life cycle phases, the book also deals with other associated topics, such as organisation for reliability, reliability training or supplier management.

Concluding the above, a variety of different methodological approaches on dependability during the life cycle of electronic, as well as other systems exists. The MIL-HDBK-338B is one of the most comprehensive sources covering different life cycle phases, but nevertheless it is rather an integral reference guide for dependability engineering than a methodological procedure to be followed during different life cycle phases. The two IEEE standards themselves provide a clear guideline to address and assess dependability during the life cycle, but other than the 338B the contained information is in principal restricted to instructions, while necessary dependability engineering knowledge is either presumed or referenced in associated IEEE standard works and other sources, in particular US Military standards. The IEC 60300 provides a comprehensive overview of many methods, but lacks a clear procedure providing guidance on which method to apply when. Of the different books and publications mentioned, each follow the individual approaches described, but none suits the specific characteristics of accelerator systems without constraints.

Overall, none of the above referenced tailors dependability application to the specific area of accelerator systems, which is generally characterised by largely distributed, customised systems with high functional requirements being designed for high reliability and availability requirements and long lifetimes, operating in often hardly accessible and harsh radiation environments.

4 LHC BLM System Dependability Model

Before putting the LHC BLM system into operation in the year 2008, dependability engineering methods have been employed during its design phase preparing a dependability model [2]. This chapter projects the predicted outcome of the model to now available operational data of more than a decade. The results and lessons learnt serve to update and further develop the existing model. The following chapters 5 and 6 use experience from creating the updated model to introduce and apply a methodology for dependable system development and support during operation.

4.1 Previous Dependability Model

The initial design of the LHC BLM system has been strongly influenced by results of the previously performed dependability assessment, in particular the applied "fail-safe" philosophy trading off availability for protection. The dependability model prepared in 2005 comprises a reliability prediction, an FMECA and an FTA [2].

The reliability prediction was performed using three distinct failure rate data sources prioritised according to: 1) test data of component and subsystem suppliers, *e.g.* for entire PSUs; 2) available historical failure data, in principle for the custom Ionisation Chamber; and 3) the MIL-HDBK-217F at boundary conditions of 30°C environmental temperature and a "ground fixed" environmental factor for the FE, respectively "benign" for the BE [96]. A total of 33 component level blocks was distinguished forming 32 higher level blocks. It is pointed out that for subsystem failure rates determined using either the MIL-HDBK-217F or component supplier test data - in principle the custom designed electronics, the prediction was not executed entirely bottom-up at that early point in time during the design phase. Only the most fundamental components were taken into account, omitting other components and associated failure modes such as the great quantity of passive components, and entire modules like the BOBR, CISV or CPU boards.

Within the FMECA, the 32 determined reliability prediction blocks were used as input. The according failure modes were assigned to the blocks and to those their immediate failure effects, carrying on to effects on the next level up to the three defined end effects. These are the most severe "Damage Risk" with a downtime of 720 h required to repair major damage on a quenched superconducting magnet, a "False Alarm" erroneously generating a beam dump request causing 3 h of operational delay to refill the LHC, and the generation of a "Warning" equivalent to 1 h of

delay - for example the time required to replace a redundant component. Executing a quantitative analysis, the in total 157 lowest block level failure modes were additionally apportioned to the block failure rates, in most cases using the data collection of the FMD-97 [148]. This allowed to assess the individual criticalities of the failure modes and components, as a product of the failure rates and the determined end effect severities. All underlying assumptions of the FMECA were estimated conservative, for example always assigning the most critical effect to a failure mode, or the resulting downtime always caused during operation and not during other LHC modes.

The determined failure mode and effect blocks served as input for the performed FTA, which formed the central analysis of the model. Using the three FMECA end effects as equivalent top events and assigning the other FMECA blocks top-down until the failure mode blocks representing basic events, the three main branches were established. Integrating the redundancies into the fault tree and assigning to the basic events the variety of established system checks, presented in the following subchapter, enabled to simulate the system availability during specific LHC missions, more precisely its complement the unavailability $Q(t) = 1 - A(t)$ given the nature of a fault tree. The unavailability was simulated using three different failure models. The rate model for repairable components based on the exponential distribution with constant rates λ and μ, *e.g.* for redundant BE PSUs. To simulate the Damage Risk during LHC missions the dormant model which considers the effect of the implemented system checks performed at individual frequencies to ensure the state of certain subsystem functionalities to be "as good as new" and in this way increasing the average availability during missions. And the binomial model for the generation of either Warnings or False Alarms, which models voting arrangements for *m* out of *n* failures causing a higher-level failure. However, this model was exclusively used in order to summarise blocks with a single failure leading to the subsystem failure. For a more detailed description of the models refer to [2].

Table 4.1: Results of the previous LHC BLM system dependability model (2005) [2]. Underlying assumptions comprise an LHC mission time of 12 h and 4 800 h of yearly LHC operation.

Parameter	Result
System failure rate	$\lambda = 0.0106\ fph$ } 1 failure every 4 days
Unavailability Warning generation	$Q(12h) = 0.0881$ } or 35.2 ± 5.7 /year
Unavailability False Alarm generation	$Q(12h) = 0.0336$ } or 13.4 ± 3.6 /year
Unavailability Damage Risk	$Q_{average}(1a) = 5.02E-06$ $Q_{max}(1a) = 1.0E-05$ } or 1% in 20 years

The overall results of the FTA and the other performed analyses are summarised in Table 4.1. Immediate consequences of the model were the implementation of the in chapter 2 described redundancies on the optical link, the VME backplane and the

HV PSUs. Another major output was the implementation of the mentioned various system checks to improve the system availability. The established frequencies of these checks were evaluated within the sensitivity analysis.

4.2 Dependability Efforts and System Checks

The implemented system checks of the initial LHC BLM system design have been revised and expanded during a variety of system upgrades in the meantime [149-151]. Having a clear influence on availability, such checks also serve to improve the maintainability by facilitating maintenance tasks, the reliability by providing valuable data for upgrades as shown in chapter 6, or enhance the protection function initiating a beam dump instead of risking energy deposition above the quench level as shown in the previous subchapter. In fact, such checks enhance the overall dependability. The previously mentioned PHM method particularly deals with such a topic.

Table 4.2: LHC BLM system checks per subsystem. The check intervals are aligned with operational LHC parameters and the system design. Offline routines are run periodically to inform and in case of critical parameters warn the system support by electronic mail (✉).

Subsystem	System Check	Frequency	Subsystem	System Check	Frequency
Detector	Radioactive source test	/1a	BLECS	VME voltages (5V, 3.3V, ±12V)	</80µs
BLECF	Temperatures (>35°C, >60°C)	/40µs		*P0* voltages (5V, ±15V)	</80µs
	Voltages (HV, ±5V, 2.5V)	/40µs		HV PSU voltage	</80µs
	GOH1/GOH2 ready	/40µs		CRC beam energy reception	/0.1s
	DAC >155 bit	/40µs		Internal Beam Permit check	/24h
	DAC overflow	/40µs		Connectivity (HV modulation)	/24h
	CFC integrator level	/40µs	External	Beam energy comparison	/3s
	10pA test (error bit)	/120s		External Beam Permit check	/24h
BLETC	CRC BLECF signal	/40µs		✉ High DAC values	/1d
	CRC comparison link A+B	/40µs		✉ Rapid DAC increase	/1d
	8b/10b error detection	/40µs		✉ VME crates temperatures	/1d
	Lost frame check	/40µs		✉ CRC errors & comparison	/1d
	Frame ID (FID) comparison	/40µs		✉ Lost frame, FID comparison	/1d
	Card/Channel assignment	/40µs		✉ VME crates temp. summary	/7d
	CRC beam energy reception	/1ms		✉ CFC/HV voltage statuses	/1d
	On-board temperature	/1.2s		✉ LSA threshold changes	/1d
CPU	Thresholds & settings integrity	/60s			

For the present LHC BLM system design, Table 4.2 gives an overview of the currently implemented checks. These involve continuous checks at a frequency of 40 µs, less than half an LHC revolution, up to yearly performed manual checks. Some checks only supply information, others trigger individual actions depending on the result. These range from the generation of a warning to LHC operation or system

support up to an immediate beam dump request sent to the BIS, *e.g.* by detecting an error of the BLETC boards daisy chain by the internal Beam Permit check. In here, the variety of individual checks and their effects is not elaborated in complete detail. This also involves the variety of implemented fail-safe mechanisms and redundancies, for instance the doubled VME daisy chains using a frequency signal to recognise the disconnection of a BLETC, initiating a beam dump request. For more information, refer to [2, 53, 56, 59, 149-153].

On a higher level, some of the checks in Table 4.2 are combined to entire procedures to be performed regularly. A major procedure comprises the Sanity Checks [149, 150] together with the Management of Critical Settings check [152] required to be performed at least every 24 h by LHC operators to avoid beam injection being blocked. The procedure combines different checks ensuring the operational state of the LHC BLM system hardware. These are the internal and external Beam Permit checks testing the daisy chain connections of the BLETC modules as well as the BIS connections, the HV modulation to assure the integrity of the cabling and detectors identifying detector channels that are blind or out of specifications [153], and a beam threshold table check comparing the threshold tables on the BLETC memories with the reference database (LSA) [152].

4.3 Operational Failure Data

Up until now, more than a decade of LHC operation has generated a large amount of operational data. It can be noted, that after the incident in 2008 causing major damage to the LHC [1], the LHC MPS including the LHC BLM system fulfilled its protection function with no such event occurring anymore. The comprehensiveness and data quality of several available databases varies greatly. The next subchapters outline these constraints and describe two data sources chosen to be the most comprehensive and suitable for LHC BLM system performance data.

4.3.1 Sources and Quality of Available Failure Data

Several applications have been used to log the occurred failures and other issues of the LHC BLM system after becoming operational in the year 2008. This variety of sources exists for the different constraints to log such data, *e.g.* the individual tool usability, the system hierarchy level regarded or the required resolution of the logged failure data, and, at last, the availability of the specific tool during the past LHC operation.

For the LHC BLM system, the most consistent as well as detailed source is the section internal logging using the JIRA software tool by Atlassian [154]. The tool allows to log, edit and track the history of any issue by the different people working directly

on the system, compare Figure 4.1. The JIRA data reaches back until the 30.03.2012, therefore misses the first two operational years of Run 1, see Figure 1.9.

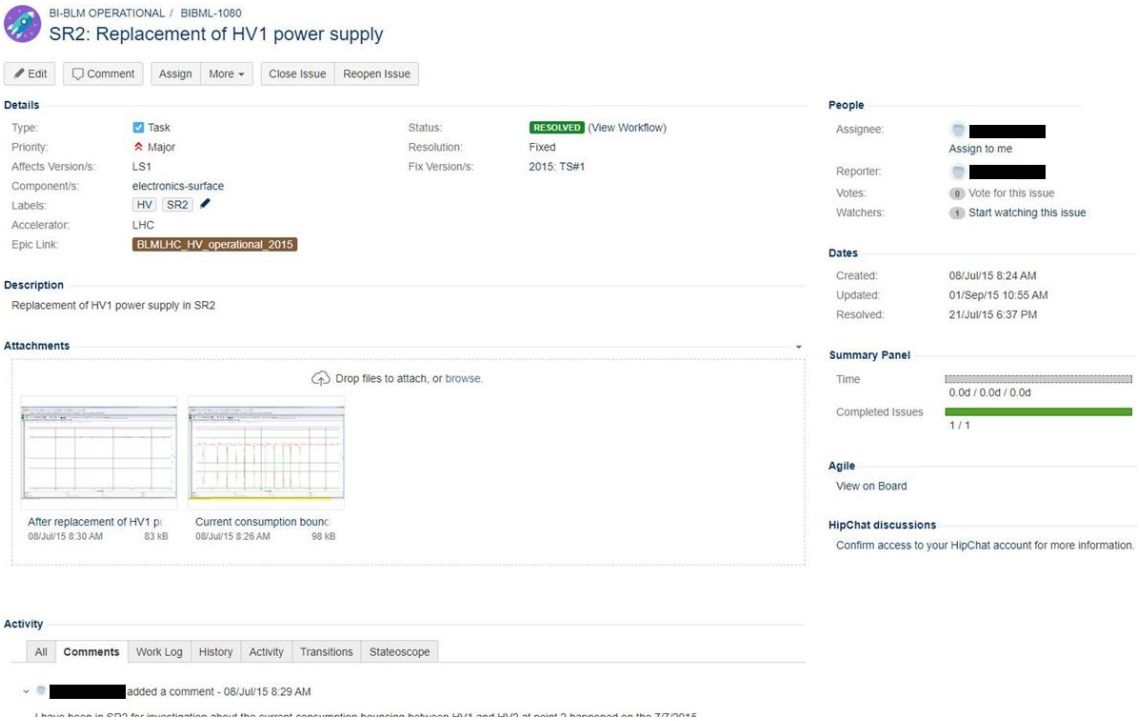


Figure 4.1: Screenshot of the JIRA tool[154]. The tool tracks and logs the workflow of entered issues. Titles are assigned to issues and can be described in detail. Additional functionalities comprise a variety of different tags, linking of issues, attaching files or adding comments.

Another tool which provides data for the LHC BLM system is the Accelerator Fault Tracking (AFT) [29, 155]. The AFT was launched in the year 2015 to capture LHC faults and provide a tool to analyse and extract the data. It tracks faults directly on the LHC machine level. In a first step, LHC machine operators create a basic entry describing the fault and assign it to a suspected subsystem. The second step involves the designated expert of the specific subsystem to review the fault and complete details, if necessary. In addition, experts of CERN's Availability Working Group review the faults and add information such as relations between faults. Since 2015, the AFT provides consistent data, however data is available back until July 2010. Prior to 2015 the AFT uses retrospectively added LHC Operations ELogbook data.

4.3.2 Failure Data Classification and Summary

The comprehensive LHC BLM system-level JIRA data comprises a great variety of capabilities to process, categorise and link logged failure data. After launching the tool in 2012, these capabilities - *e.g.* to create subsystem categories or operational mode tags, have been applied gradually. Unfortunately, however with the variety of different personnel supporting the system, each in an individual manner, such categorisation has not been applied consistently. For this and other reasons regarding

consistency, the in total 1 418 JIRA entries until the end of Run 2, which also comprise non-failure issues, have been reviewed and re-categorised in order to achieve the most consistent data possible.

Table 4.3: JIRA logging failure data between 03/2012 and 06/2019. For the VME Fan&Control module failures have been present, but no precise number could be determined (*).

Subsystem	No. of failures		Percentage [%]	Quantity installed	Failure Rate; *C*=90% [/a]	
	"Hard"	"Soft"			$\lambda_{Component}$	$\lambda_{\Sigma Component}$
Ionisation Chamber:	2+15	2	3.81	3635	9.83E-04	3.57
Connector	(4)					
Soldering	(1)					
Cable	(4)					
BJBAP filter	(6)					
LIC/SEM		4	0.80	299	3.69E-03	1.10
BLECF:	43+6	14+1	12.83	669	1.56E-02	10.42
GOH	(5)			1338	9.56E-04	1.28
BLECF Reset	(1)	(1)		669	1.10E-03	0.73
SS crate	5		1.00	37	3.46E-02	1.28
Tunnel PSU (Arc/SS)	2		0.40	396	1.85E-03	0.73
Optical fibre link	11	57	13.63	1338	8.23E-03	11.01
BLETC:	71+13	12	19.24	348	4.35E-02	15.15
Mezzanine	(9)			348	5.63E-03	1.96
DAB64x	(4)			348	3.17E-03	1.10
BLECS	6	2	1.60	27	6.64E-02	1.79
CISV	2	5	1.40	8	2.03E-01	1.62
CPU	3	3	1.20	27	5.38E-02	1.45
BOBR	1	3	0.80	27	4.08E-02	1.10
VME crate	2	9	2.20	27	8.48E-02	2.29
VME PSU	18		3.61	27	1.26E-01	3.41
VME Fan&Control	Multiple	1	/*	(27)		
HV PSU	7	5	2.40	16	1.53E-01	2.45
BLM system level	1	2	0.60			0.54
Sanity Check		71				11.46
Software		46				7.72
Firmware		9				1.96
External:	2+2	0+4	26.45%			1.79
Surface Rack	(2)					
BIS interface		(1)				
Software		(3)				
Non assignable	7	33	8.02			6.81
Total:	**>217**	**283**	**(100)***			>85.44
	>500					

The result of the in this way processed data is displayed in Table 4.3. The categorisation involves the distinction between a “hard” failure, defined as a failure requiring a hardware replacement, and a “soft” failure, which may have been an intermittent failure disturbing LHC operation, or a permanent one, which however has been solvable by performing a reset or similar. The resolution of the data is unfortunately limited to the subsystem level as displayed in the first column. No component level failure modes and causes were identifiable in a statistical relevant extent. Furthermore, it was not possible to determine the exact times of failure, especially regarding the current LHC operation. Only the times of the JIRA issue creation were available, which in general were created after restoration of the operational state.

In total, 500 system failures were identified which break down into 69 failures per year on average. A quantity of eight are of “external” systems, not part of the LHC BLM system as defined in subchapter 4.4, 40 failures, or 8% could not be assigned to a subsystem and three failures occurred on the LHC BLM system level, *e.g.* wrong loss threshold limits entered. Only for the VME crate Fan&Control modules with a datasheet *MTBF* of 85 000 h, at 25°C, no precise number of performed replacements could be determined. As one of the few mechanical system components a preventive maintenance strategy has been in place to replace these fans, but the data nevertheless showed that failures had been present.

Furthermore, Table 4.3 comprises the subsystem failure rates per year computed according to Table 3.3 assuming an exponential failure behaviour at 90% confidence. The failure rate is displayed per operational year since the regarded time period of 7.25 years comprises the entire LS1 and Run 2, collectively being representative for nominal LHC operation in the longer term.

For 329 out of the 500 entries, it was possible to determine the failure effect on LHC operation. For this data set, Table 4.4 displays that 16% of the failures caused a beam dump during operation, while 21% created a Warning and around two thirds had no operational effect. To distinguish between actual protection beam dumps and false alarms, the data is missing detail. It is pointed out, that these statistics cannot claim full comprehensiveness, thus can only be compared with limitations to the results of Table 4.1.

Table 4.4: LHC operational effect of LHC BLM system failures based on JIRA failure logging data.

Effect on operation:	**Beam Dump**	**Warning**	**No effect**	**Total:**
Number of failures (Percentage):	52 (16%)	70 (21%)	207 (63%)	329

It has already been pointed out that the time of failure is not precisely available. Nevertheless, by dividing the time axis of the 7.25 years of data into month-long classes, a progression can be determined. Figure 4.2 displays the progression for the 500 determined failures. The long shutdown periods are marked. It is however

pointed out that there are months which included week-long technical stops, in particular between the years. Not operating during all these periods it is unlikely that failures occurred, but likely that they were used to perform foreseen maintenance tasks, in that way creating many JIRA logs.

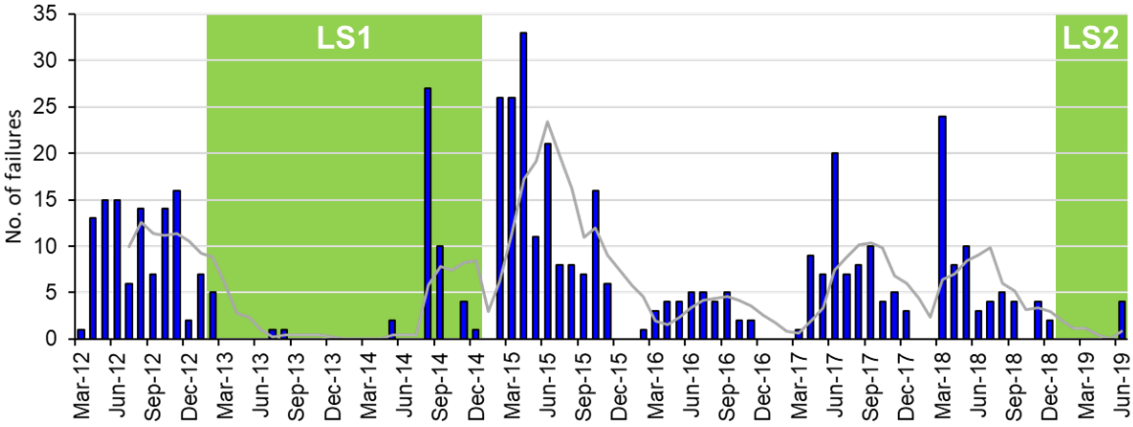


Figure 4.2: Logged LHC BLM system failures per month. The year-end technical stops are identifiable and the Long Shutdown periods are marked. After 2015 the failure rate has decreased during the following three years.

For the three years after 2015, a trend can be observed of less failures occurring at a relatively constant failure rate. This trend, as well as the LHC operational effect data of Table 4.4, can be rendered more precise by looking at LHC system level availability data of the AFT, more exactly by looking at the LHC downtime impact of the LHC BLM system, see Figure 4.3.

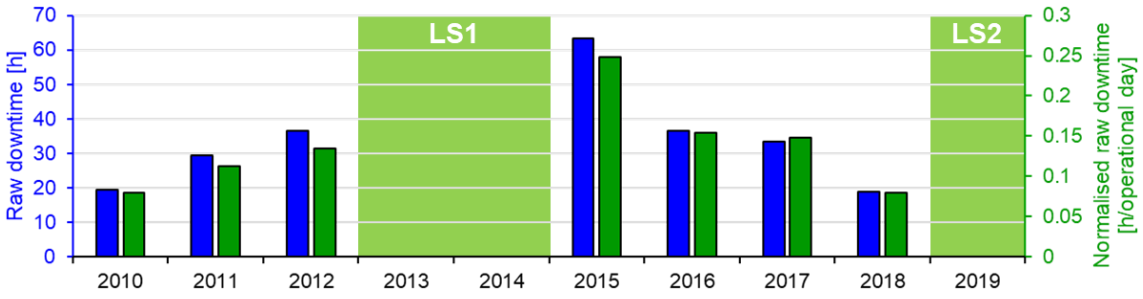


Figure 4.3: Yearly LHC downtime impact of the LHC BLM system, extracted from [29]. The normalised raw downtime per operational LHC day, *i.e.* days where data showed that the LHC was filled (see [156]), correlates well with the absolute raw downtime, indicating consistent support performance.

4.4 System and Environment Definition

In order to update the LHC BLM system dependability model, the hardware to be modelled had to be defined inside its system borders interfacing to other systems and with regard to the boundary conditions in its operational environment, compare Figure 5.4.

According to the quantities specified in Table 2.1, the system hardware was defined. As outlined in subchapter 2.2, the system border is defined around the hardware illustrated in Figure 2.1, with the BLECS, BOBR, CISV, CPU and the PSUs establishing the interfaces to external systems or supplies. Furthermore, the temperature-controlled racks are not considered a part of the system, presumed to be operating at hypothetical 100% reliability.

The operational environment divides into three locations: the radiation environment of the LHC tunnel kept at a temperature below 25°C, the optical fibre cables establishing the surface installation connection inside ducts and the surface racks as well set to control the temperature below 25°C. At the surface, external temperature and humidity data loggers were installed inside the racks at the eight points, as well as at two points directly outside the racks, to verify the reliable performance of the rack temperature control and to assess potential humidity variations over the year, see Figure 4.4.

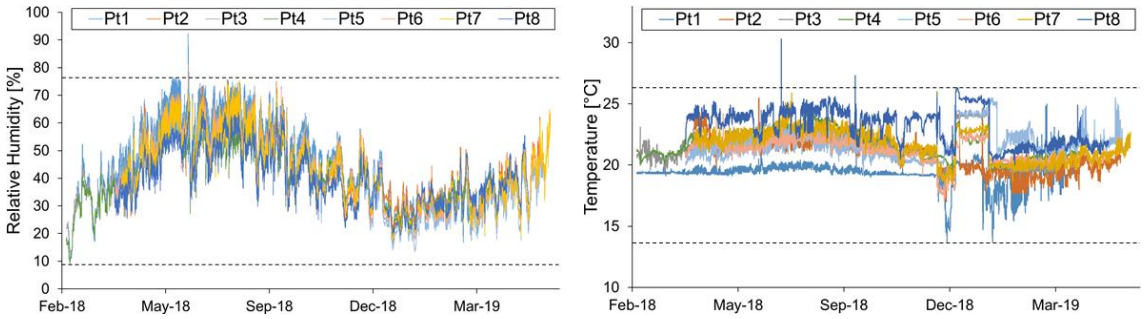


Figure 4.4: Temperature and humidity measurements inside the surface racks of the LHC BLM system over 1.25 years. A relative humidity variation between 8 and 77% with its peak in summer and an upper temperature threshold closely above 25°C can be determined. Data from outside the racks showed that the humidity conditions inside the rack follow the ones from outside with a small time delay. Intermediate strong parameter increases were caused by the rack doors being opened.

Regarding the radiation environment inside the LHC tunnel, no specific considerations were taken into account for the model update of the next subchapter, because the tunnel electronics were designed to be radiation tolerant [53] and operate since then without significant radiation failures monitored. If radiation failures occurred, they are taken into consideration by the failure rates presented in Table 4.3. Nevertheless, cumulative degradation effects, *e.g.* Total Ionizing Dose (TID) inducing semiconductor lattice damage, are to be monitored during operation (see "Weibull Analysis" in subchapter 5.2.4), potentially reaching the third section of the bathtub curve at some point in the future. The same applies to the other tunnel electronics and the optical fibre cables in the tunnel. The BLECF was designed to withstand a radiation dose equivalent to 20 years of operation [53].

Design methods and operation strategies considering operation inside a radiation environment, are dealt with in subchapters 5.2.1 and 5.2.3.

4.5 Model Update

The objective to update the existing LHC BLM system model has been to create a model of the final system design integrating the intermediate system changes and upgrades. Because the previous model only took 33 components into account, it cannot be used to compare its results to the presented performance data in subchapter 4.3. As described in the next subchapter, the current system comprises a much greater variety of components. Furthermore, the shortcomings of failure data from such reliability predictions has been outlined in subchapter 3.3.1.

For all these reasons, an updated dependability model has been prepared in order to establish the system structure comprehensively bottom-up, to reversely determine and evaluate the robustness of the design by applying stress analysis and derating techniques from reliability prediction as well as to reversely execute a study on an existing system profiting from the available performance data to tailor a modelling procedure for the methodology introduced in chapter 5. The entire study comprises the creation of the complete system structure, a quantitative failure rate assignment to the created components based on data of a recently updated reliability prediction standard, test reports or the available failure statistics and an FMECA using this input. The approach taken and modifications with respect to the previous model are displayed in Table 4.5.

Table 4.5: Boundary conditions of the updated LHC BLM system dependability model and modifications with respect to the previous model [2].

#	General conditions	Description
1	Environment	Ambient temperature (tunnel + surface): < 30°C Ambient humidity: < 80% RH
2	System structure	The entire hardware is comprehensively modelled bottom-up creating a hierarchy upwards from the component level of the custom designed boards
3	Failure rate data and	Passive components: 217Plus™ standard [94]; Semiconductors and ICs: Primarily test reports, if not available 217Plus™; Entire modules (*e.g.* PSUs): Test reports; Custom modules/No other data available: Operational data (Table 4.3)
4	stress analysis	Individual component stresses (*e.g. T*, *P*, *V*) are computed and considered for the failure rate models. Applied derating is reviewed.
5	Confidence	A more conservative 90% confidence level is applied instead of the previously used 60%
6	FMECA	Based on functional blocks created from the bottom-up system structure; Worst-case failure effect assessment, see Eq. (4.1)

4.5.1 Creation of the System Structure and Reliability Prediction

The shortcomings of reliability predictions have been described in subchapter 3.3.1. Nevertheless, as it is pointed out in subchapter 5.2.1, the procedure of performing a reliability prediction is a beneficial tool to model the system structure and, to a certain degree, evaluate the dependability of a system during its design phase. In the same subchapter it is outlined, but already emphasised at this point here, that the obtained failure rate shall not be used to fulfil any reliability requirement. Furthermore, chapter 5 shows the importance of this step to create a fundament providing input for subsequent analyses, as done in the following subchapter.

As outlined in Table 4.5 for being a recently updated and maintained standard as well as encompassing the component categories present in the LHC BLM system, the 217Plus™ reliability prediction standard was chosen to predict the failure rates of passive components of the custom designed boards of the LHC BLM system according to the component failure rate model of Eq. (3.26). For ICs, test report data of these components from the year of installation was adapted to the environmental conditions, the applied stresses and a 90% confidence level. In addition, the 217Plus™ standard was used to model the failure rates of the soldered IC pin connections. For more than 90% of the ICs, test reports were available. The remaining were modelled with the according 217Plus™ models. For commercial subsystems, such as PSUs, test report data of the entire modules were used. As in the previous model, the custom designed Ionisation Chamber module was modelled based on the available updated failure data comprised in Table 4.3. Since in the meantime they have been disconnected from the BIS, SEM detectors are not part of the model. A small fraction of other subsystems without available schematics or test reports were also modelled based on failure data of Table 4.3.

The determined system structure is organised on up to six hierarchical levels, distinguishing three top blocks according to Table 2.1, the surface installation, the optical fibre link and the tunnel installation, see Figure 4.5. The lowest level is the component level either as components on electronic boards, *e.g.* a resistor, or as entire modules such as a PSU.

The system model is composed of 856 distinct hierarchical blocks, *i.e.* one slice as displayed in Figure 2.1. For the entire modular LHC BLM system, this multiplies to more than half a million blocks in total.

Concluding the analysis, the entire LHC BLM system design has been reviewed bottom-up. All components of custom electronic designs have been verified to be correctly derated, thus the observed failures in Table 4.3 should not have been caused by design internal overstress. For passive components, no peculiarities have been found. The same applies to ICs and other semiconductors including power components such as voltage regulators. The component operating at the highest

stress level is a voltage regulator both on the DAB64x and the similar BLECS board, operating at a ratio of $T_j/T_{j,max}$ = (81/150)°C = 0.54, compare Table 5.1. For these components, the manufacturer failure rates from tests were adjusted to the maximum internal junction temperature T_j calculated.

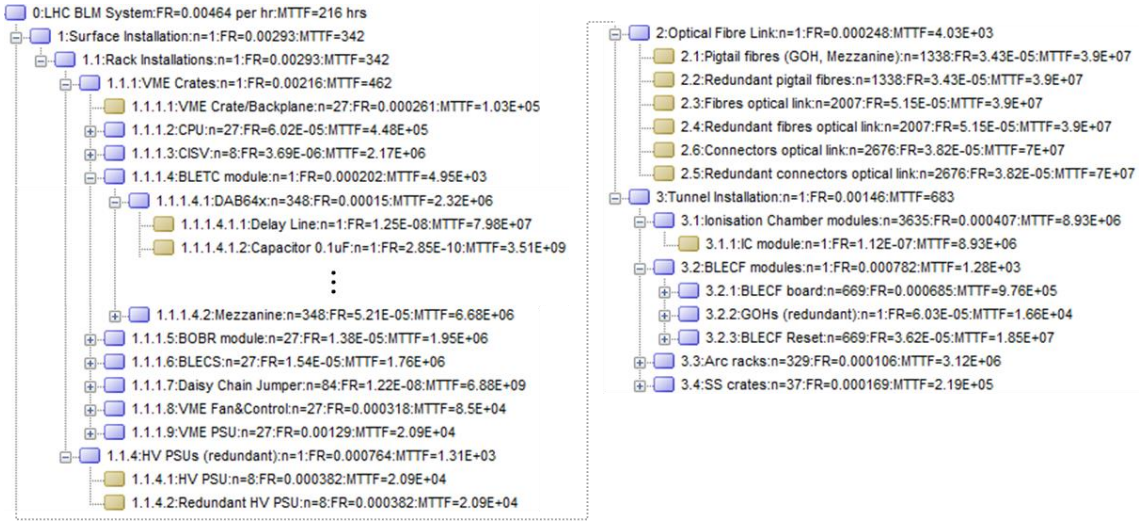


Figure 4.5: Hierarchical system structure of the LHC BLM system. The predicted failure rates of the component level (yellow blocks) are totalled up to the hierarchical levels, compare Eq. (3.16).

While the overall predicted failure rate of 40 “hard” failures per full calendar year (30 were observed, see Table 4.3) remains a side note, this value can be apportioned to different component categories. Table 4.6 displays the apportionment, which for mechanical and power electronic components is primarily composed of the datasheet *MTBF* values, *i.e.* assuming corrective maintenance for these components wearing out. This does not involve on-board components such as switches or voltage regulators. For other categories, the small semiconductor apportionment based on test reports data compared to the quantity of components, and related to that, a high 26% share for passive components, can be observed. However, regarding the in Table 4.3 observed “hard” failures, for the few where causes were determined none could be traced back to semiconductors, a certain amount to power electronic modules and the majority to environmental and human factors, *e.g.* dust on optical fibre connectors.

Table 4.6: Apportioned failure rates for different component categories. The detector failure rate is the determined value from operational data of the Ionisation Chamber modules, see Table 4.3 (*).

	Detectors*	Mechanical	Optical	Power	Electronics		
					Passive	Semiconductor	Modules
Failure rate [fph]	4.07E-04	3.24E-04	2.85E-04	2.21E-03	1.22E-03	1.14E-04	6.02E-05
Percentage [%]	8.8	7.0	6.2	47.8	26.4	2.5	1.3
Component qty [-]	3635	1877	15870	13523	632338	95070	27

4.5.2 FMECA

Provided the comprehensive bottom-up system structure, it is possible to review in a next step the protection function of the LHC BLM system, as well as effects of system failures on the availability performance of the system.

Using software, the modelled system structure was converted into an FMECA by assigning potential failure modes and corresponding effects to the determined system blocks. Given the large quantity of the blocks, this was not done entirely bottom-up, *i.e.* assigning failure modes on the schematic component level. Moreover, from the available system structure, functional blocks were determined to which the according failure modes were assigned pursuing a worst-case approach, see Eq. (4.1). This means that of the entirety of component blocks and their potential failure modes the higher functional block is composed of, the potentially worst-case failure effect was determined and assigned. Given the previous input and the knowledge of all potential component level failure modes, a comprehensive bottom-up approach was still followed, only involving an adverse loss of resolution assessing the system conservatively, *i.e.* overestimating the effect of the more severe failure modes.

$$Block\ Effect \coloneqq Worst\text{-}Case\ Effect(\sum Block\ Failure\ Modes) \tag{4.1}$$

Table 4.7: Determined FMECA severity rankings for the LHC BLM system. The analysis showed that the system architecture is designed to prevent the most severe "catastrophic" failure effect from occurring.

#	Severity Rank	Effect
1	Negligible	No Effect
2	Moderate	Warning (Maintenance required)
3	High	False Beam Dump
4	Critical	Blind Failure (1 detector)
[5]	[Catastrophic]	[Blind Failure (several detectors)]

Table 4.7 displays the severity rankings of the four determined end effects on the system, respectively the LHC level. Similar to the previous model, these are on the lower two levels failure modes having "No Effect" on the top system level, or a generation of a "Warning" not interrupting the current LHC mission but requiring a maintenance intervention either after finishing the current LHC fill or during the next technical stop. At higher severities, these are the generation of a "False Beam Dump" request not by fulfilling the protection function, but as a false alarm, and the "Blind Failure" end effect only applicable to the very FE with the rest of the system designed fail-safe regarding this effect. Two potential Ionisation Chamber module failure modes can yet cause this critical, but not catastrophic, LHC BLM system failure which would miss to detect dangerous beam loss, compare Figure 4.6. However,

the HV modulation test verifies at maximum every 24 h that no BIS-connected channel is blind. Furthermore, the layout of the detectors around the LHC with the individually defined loss thresholds prevents such a failure causing losses above the critical quench level, because even ultra-fast beam losses occur alongside a certain circumference of the LHC, thus several Ionisation Chamber modules would need to suffer such failure modes in parallel.

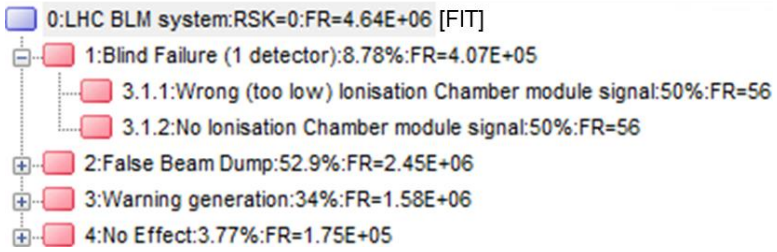


Figure 4.6: Top level FMECA end effects with apportioned failure rates in FIT from the reliability prediction model. Note the conservative approach taken resulting in an overestimation of more severe effects. In particular the apportionment for a potential "Blind Failure (1 detector)" reflects the entire observed failure rate of the Ionisation Chamber module for the sum of all potential failure modes.

To summarise, the protection function of the LHC BLM system and its impact on LHC operation has been reviewed by assessing the criticality of each determined functional block as the multiplication of the severity rank and the occurrence probability of the failure mode(s), analogue to Eq. (4.1). Furthermore, the detection of potential failures or failure causes to prevent severe effects from happening have been reviewed to particularly verify the protection function. This examination has been the primary outcome of performing the FMECA. The analysed system architecture as defined in Figure 2.1 prevents the possibility of a catastrophic failure effect occurring. To do so, the generation of false beam dump requests is intended. From the hardware point of view assessed by the FMECA, only little potential exists to reduce such false alarms. Upgrades to enhance the reliability and maintainability of certain modules are one possibility, while the system already encompasses a high number of redundancies and diagnostics, compare subchapter 4.2. One such development in the framework of an entire upgrade strategy is presented in chapter 6. Other optimisation potential involves the system checks to reduce their negative impact on the LHC availability not compromising their role in protecting the accelerator. This involves, in particular, the optimisation of the Sanity Checks procedure which is already ongoing, see [156]. The constant availability increase over the past years displayed in Figure 4.3 shows that such similar optimisations have already been performed in the past.

A potential next step to pursue the review of the LHC BLM system is to perform an FTA on the basis of the FMECA. This is not performed in here because the FMECA already showed that the occurrence of catastrophic system failures is highly unlikely as it is prevented by the system architecture. This conclusion is supported by no

such catastrophic blind failure occurring since the system start-up. As the performed system checks have already been reviewed by the FMECA, their application, together with the implemented redundancies got validated by the system successfully operating since 2008. In fact, to review operating systems, the bottom-up approach of an FMECA with the previously determined hierarchical system structure proved to be a powerful analysis technique. The performance of an FTA is rather beneficial during the system design, especially during early phases, or if the system is to be upgraded to enhance its availability performance, as well as to perform top-down failure analyses during operation to identify failure causes of on the top-level visible failures.

5 Methodology for Dependable System Development and Operation

The scope of this chapter is to present a methodology for dependable electronic system development from early planning and design to production and testing, up until dependability monitoring and support during operation, and acquiring know-how for future developments after decommissioning. Subchapter 3.5 presented the state of the art on existing methodological approaches for dependability engineering with no approach addressing the specific area and requirements of accelerator systems, in particular modular beam instrumentation systems. The presented methodology here addresses dependability during the full life cycle of a system with an emphasis on electronics for accelerator systems.

The methodology makes use of the dependability practices profoundly presented in chapter 3 establishing a step-by-step procedure to be followed one after the other, whilst being adjustable to the present system focussing on highly distributed accelerator subsystems and systems. The objective is to provide a holistic framework for dependability application during all life cycle phases. Furthermore, the methodology shall serve in its completeness to be applicable to several development projects, in order to continuously enhance the dependability capability of an organisation for all systems being developed, *i.e.* to continuously enhance the superordinate system, in general being the top level accelerator. The methodology has been developed based on experiences made during the development of the LHC BLM system dependability model and the feedback given from the existing model, as well as from the operational failure data analysis of the previous chapter 4. Furthermore, in the subsequent chapter 6, the methodology has been applied and reviewed within a case study encompassing the planning, design, production and testing phases, as well as operational considerations of an LHC BLM system upgrade. Experiences made within the case study have been fed back to adapt and improve the methodology, as it is presented in here.

5.1 The Product Life Cycle

The life of technical systems or products can be divided into different phases. This starts with the preliminary planning phase and closes at the end of the service life or after decommissioning with the potential reuse of parts during recycling. The different phases together are commonly referred to as the “product life cycle”.

In [78], B. Bertsche et al. define seven distinct phases of the product life cycle, displayed in Figure 5.1. Associated dependability methods and actions during different phases as a part of an entire dependability management are assigned on the bottom.

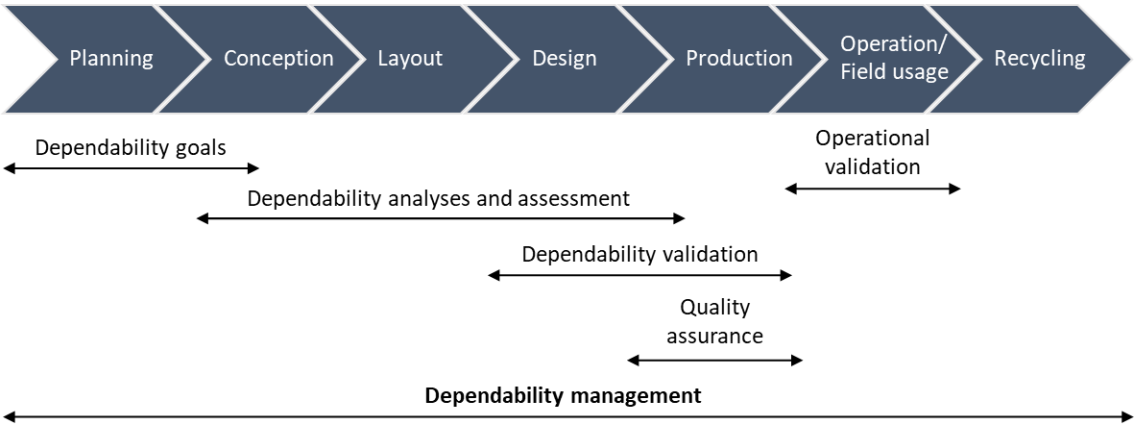


Figure 5.1: Dependability management during the product life cycle phases, according to [78].

Accelerator systems, such as the various beam instrumentation systems of the LHC undergo a similar life cycle. New developments, upgrades or modifications of entire systems, subsystems and components begin by defining specifications, developing concepts and first prototypes, and end with decommissioning and potential refurbishment or partial upgrades after operation, being then reused. Particularities of accelerator systems compared to consumer products are their high dependability requirements, especially RAMS, but also functional requirements of high precision and reproducibility. Furthermore, production numbers are usually low and the production is generally terminated before the start of operation, which also involves considerations for spare device management. The high requirements often result in complex systems developed at high expenses, thoroughly qualified and tested, and well monitored and maintained during operation. A good example are the yearly and long term LHC schedules, comprising a high number of technical stops and long shutdowns in order to repair, maintain and upgrade the machine and its subsystems, compare Figure 1.9.

For such accelerator systems, Figure 5.2 slightly adapts the product life cycle into five phases being used by the methodology in the next subchapter. The phases are defined paying special attention to dependability.

The first four phases of Figure 5.1 are merged into a planning and design phase. Together with the design specifications, the dependability specifications are defined at first, based on which the system is then designed. This design is accompanied by dependability analyses and methods, as well as production considerations and the development of test and operational strategies in parallel, all considering potentially associated design adaptions.

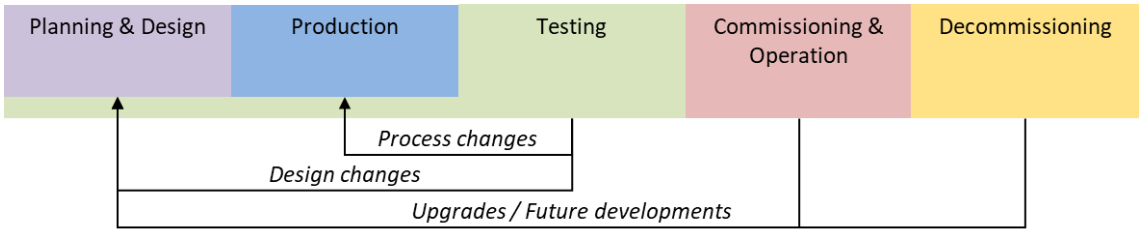


Figure 5.2: Life cycle phases for accelerator systems, grouped with emphasis on distinct dependability steps further elaborated in subchapter 5.2. Later phases can provide feedback leading to immediate changes during iterations of earlier phases, or feedback in a continuous sense for upgrades or future systems, in this way enhancing the organisational dependability in the long term.

The next production phase comprises dependability considerations during Printed Circuit Board (PCB) manufacturing, board assembly and soldering processes. This includes associated steps such as cleaning processes, quality controls, or potential functionality tests. Furthermore, the phase comprises the packaging and transport during and after production.

The third phase of Figure 5.2 starts with the reception of the boards from internal manufacturing or after shipment. This phase is not included in the product life cycle of Figure 5.1, being particularly added to perform a variety of necessary validation and reliability tests accompanied by potentially necessary inspections. As illustrated in Figure 5.2, it is pointed out, that tests of this phase may be already performed alongside the design and production phases.

The actual system operation takes place in the fourth phase. It further comprises the installation and commissioning of the system and operational strategies, for instance maintenance strategies, system monitoring and data analysis.

The last phase is similar to the seventh phase of the product life cycle [78]. The decommissioning of the system after its service life comprises the potential to analyse the decommissioned system and provide feedback to previous phases of future developments within the entire cycle.

The following methodology makes use of the phases shown in Figure 5.2. Individual steps within the phases are presented more in detail to address dependability engineering during the complete life cycle of systems.

5.2 Dependability Methodology during the System Life Cycle

To achieve reliable system operation at high availability, the full spectre of the underlying dependability engineering needs to be present and consequently applied, not only during design, but during all phases of a system's life cycle. In fact, a well-structured organisational dependability program should constantly have the objec-

tive to maintain, or even better improve, the current status quo and in this way become an essential part of the organisational culture. Being valid across all kinds of fields, this is especially important for accelerator technology with generally highly precise, custom-designed instruments for dependable operation in severe environments, primarily radiation, often hardly or not accessible during their therefore long required lifetimes.

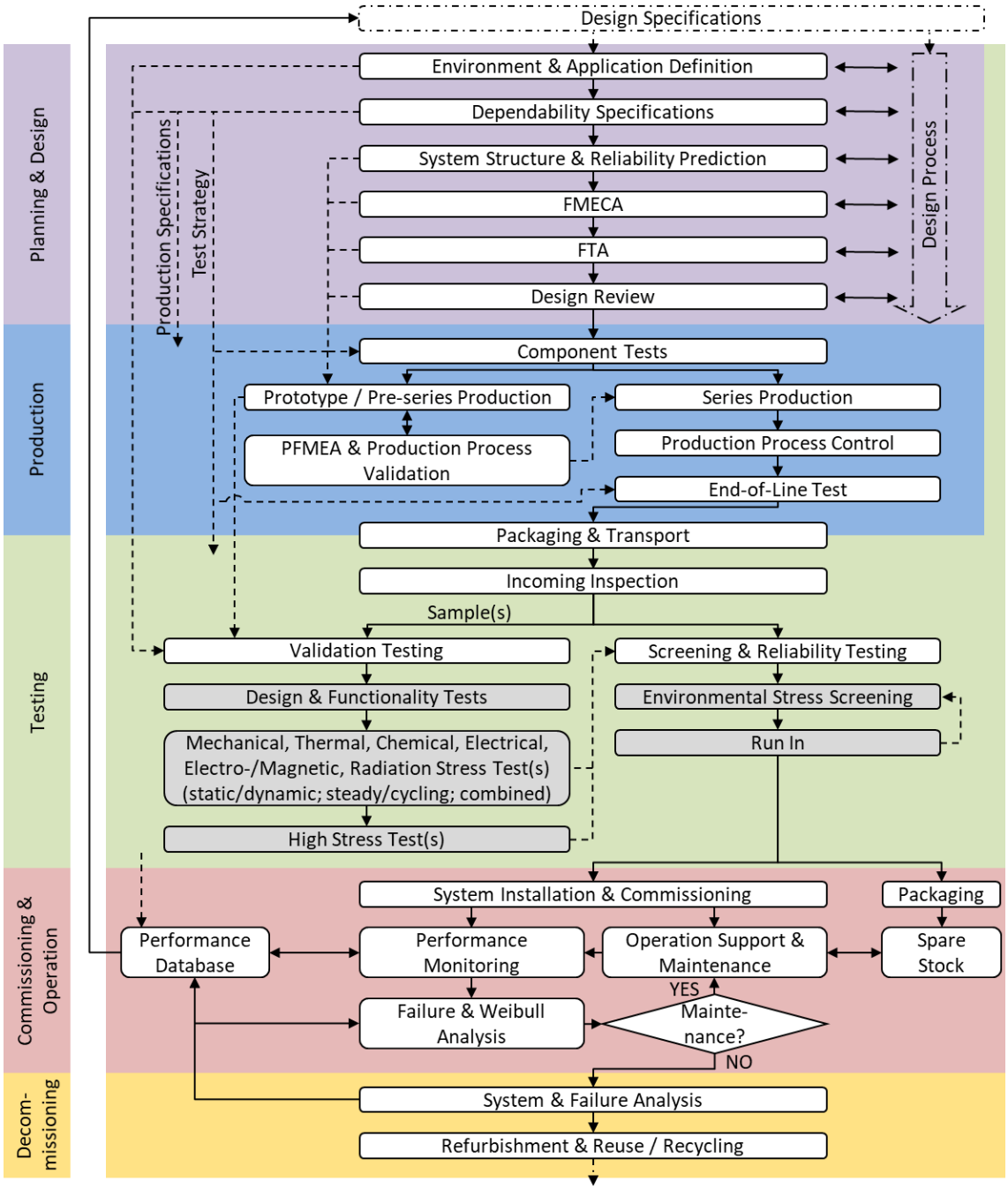


Figure 5.3: Dependable electronic system development methodology during the different life cycle phases. The figure displays the main steps during the different phases, which are further subdivided. It is pointed out, that a variety of intermediate results may trigger iterations of previous steps which is not comprised in the figure, compare Figure 5.2.

The herein introduced methodology has been developed to address dependability during all these phases: planning, system design, production, testing, installation, commissioning, operation and decommissioning, also comprising a constant improvement process learning from experiences of previous systems, compare Figure 5.2. The individual steps of the methodology during the different life cycle phases are presented in Figure 5.3.

The individual steps displayed attempt to cover a broad range of electronic systems, with special focus on the development and operation of electronics for accelerators. Nevertheless, each system is individual with different specifications, which is why the objective of the methodology is to provide generic guidance whilst being adjustable for the individual use case. Therefore, it should each time be tailored to the specific system in question.

The following subchapters present the five phases with their individual intermediate steps more in detail. Each subchapter provides a comprehensive collection of steps, comprising methods, guidelines, applicable standards and other considerations to be followed one after another for an entirely established dependability program. Furthermore, correlations between steps, for instance to provide input for other steps, are being described. Once again, the objective is to make use of these steps by selecting the ones matching the specific development project as well as to integrate the methodology within an organisation in order to enhance the dependability capability in a broader sense. The case study in chapter 6 provides an example for such a system development.

5.2.1 The Planning and Design Phase

Addressing dependability during the life cycle begins already at the early phases of a new development project. The methodological procedure in Figure 5.3 starts by using the existing design specifications as an input, which should already be defined with the dependability goals of the system in mind. Having the design project preliminary established and specified, the design process is conducted in parallel to the methodology steps of this phase. This involves a regular exchange and alignment of the two processes.

Taking notice of the functional design specifications, the operational environment is to be defined. This comprises the assessment of all potentially present environmental stresses, essentially of mechanical, thermal, chemical, radiation, electrical or electromagnetic origin. Furthermore, this also involves potential stresses induced by the future application, on the one hand internally induced by the operating system, and on the other hand from connected systems for the case of a subsystem development. Furthermore, all steps of the life cycle need to be considered, for instance temperature exposure during the soldering process or potential stresses during

transport and handling, *e.g.* vibrations or ESD. In order to determine these potential influences, the system can be regarded as a black box defining its interfaces to the environment and application as displayed in Figure 5.4.

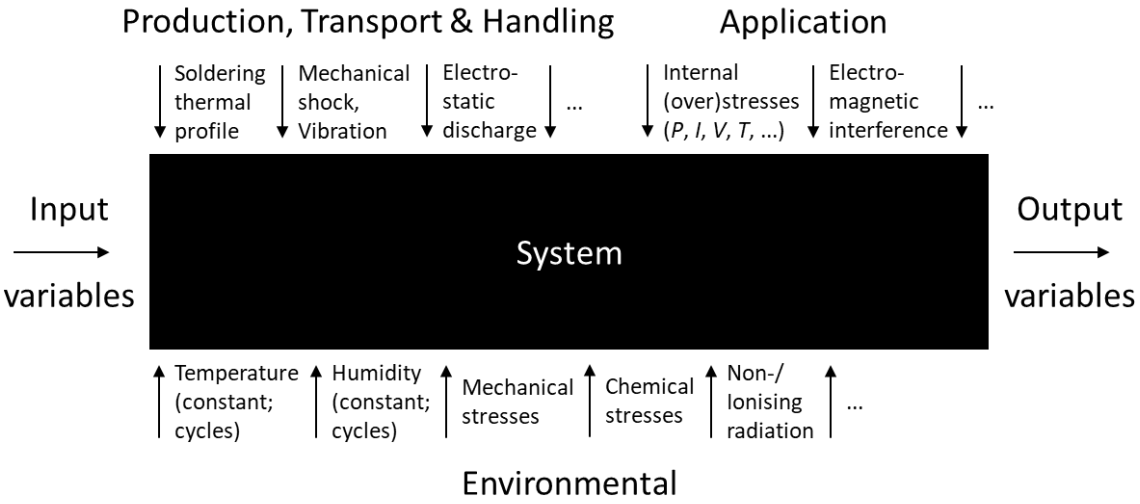


Figure 5.4: Definition of internal and external influences on the system using a Black Box approach.

On the basis of the design, environment and application specifications, together with the knowledge of potential failure mechanisms, the dependability specifications are derived. Dependability goals are defined quantitatively using the parameters outlined in subchapter 3.2, but may also be defined qualitatively. Examples are a minimum *MTTF* demonstrated at a certain confidence level by tests including an early failure screening, a required minimum lifetime to be demonstrated, an availability requirement for specific missions, or a defined maximum risk or criticality to be demonstrated by an FMECA. The dependability specifications shall be defined based on an organisational guideline addressing all life cycle phases defining applicable methods during the design, production standards and process control, transport and handling instructions, validation and reliability testing as well as operational support and performance monitoring. Guidance to define dependability specifications is given in [157].

Already at this stage of having potential influences on the system defined according to Figure 5.4, the parallel design process shall consider the preliminary outcome by implementing solutions to prevent or mitigate the influence of such effects. These can be for example ESD input protection for all connector and contact pins, heat sinks, protection against humidity or radiation of structural nature, electromagnetic compatibility considerations, but also considerations for the later production process or the testing strategy. Applicable techniques comprise the previously outlined DfR and the related Design for Manufacturability as well as Design for Testability, furthermore expanding such techniques to Design for Maintainability, Storage, Handling, Packaging or Transportation, see [83, 84]. To consider internal stresses, the

design should apply derating techniques to an adequate extent. Table 5.1 summarises reference values [130], while it is pointed out, that these minimum values should be further derated whenever possible in order to increase the stress-strength margin, compare Figure 3.10. Such over-dimensioning also involves the PCB design.

Table 5.1: Recommended derating values for electronic components at ambient temperature 20°C ≤ T_{amb} ≤ 40°C, according to [130]. The given values are determined as the ratio of the applied load and the rated load at 40°C. For other and more detailed component categories see [83, 130].

Component	Power	Voltage	Current	Internal temperature	Frequency
Resistors	≤0.4 - 0.6			≤0.7 - 0.8	
Capacitors		≤0.5 - 0.8		≤0.5	
Diodes	≤0.6	≤0.5*	≤0.6	≤0.7	
Transistors		≤0.5*	≤0.7	≤0.7	≤0.1f_T
ICs		≤0.7	≤0.7 - 0.8**	≤0.7***	≤0.9

* breakdown voltage; ** sink current; *** T_j ≤ 100°C; f_T: gain bandwidth [Hz]

In the persisting manner of parallel functional and dependable design, the system structure is at first created top-down and already analysed during the early stages and subsequently bottom-up once first schematics are available. Techniques such as an FTA or a Reliability Block Diagram can be applied to be eventually transformed into a comprehensively bottom-up performed FMECA.

This bottom-up system structure grows together with the evolving design. It can be advantageous to perform such analyses along with a reliability prediction. The quantitative failure rate allocation should be prioritised following internally available test or field data of components or modules, manufacturer test reports and lastly prediction models. The predicted outcome shall not be used to fulfil any set requirements, but may well serve to compare different design solutions, to identify potential weaknesses early, to assess the feasibility of the requirements and to provide input for a CA based on which the strategy for the upcoming production and testing can be defined. Furthermore, the execution of the bottom-up methodology allows to review the correct circuit design, component selection in terms of specifications, qualifications and quality level, as well as the correctly applied derating.

In the framework of the entire methodology, the comprehensive bottom-up analysis also comprises further reaching effects to enhance the organisational dependability. A knowledge base is established which facilitates later steps such as production, testing and operation, in particular regarding a potential failure analysis. In addition, future projects profit from such a knowledge base, for example through the integration of dependable proven standard circuits, designed, tested and operating for several projects.

The in parallel performed FMECA enlarges this knowledge base by determining the effects of potential system failure modes. Based on the severity of the top-level faults or end effects, the FMECA may be performed entirely bottom-up determining component failure modes. As shown in chapter 4 and 6, it may also be done in functional blocks summarising the components the functionality is composed of, according to Eq. (4.1). It is pointed out, that the conservative worst-case assessment resulting in a loss of resolution is to be applied which does require the knowledge of the comprised component failure modes.

In a next step of the FMECA, the assessed risk either by *RPN* or CA ranks the system blocks accordingly. Based on this output, blocks above a defined threshold should be optimised either by performing actions on the design, *e.g.* design changes or additional diagnostic checks, or by implementing additional testing to demonstrate the required reliability. This may also involve actions for the production process as shown in chapter 6.

With the substantial database of the FMECA it is possible to link the determined blocks top-down using the Boolean logic of an FTA. Potentially already performed earlier, the FTA at this point is no longer useful to identify critical cut sets resulting in a top-level failure because these events should have been excluded by the FMECA. Moreover, the FTA may serve to assess the availability during later operation, as done in [2]. The effect of redundancies and implemented diagnostics can be assessed and the design can be optimised for specific missions. Furthermore, it can serve to define a maintenance strategy, for which however more sophisticated analyses exist such as the Markov analysis or Petri Nets, compare [83, 130].

As presented in chapter 4, the analysis of operational failures of the LHC BLM system has shown that only around 43% of occurred system failures were identified as hardware failures with the remaining “soft” failures not needing interventions to exchange modules. Given this fact that more than half of the failures are due to soft errors, the importance of design analyses such as an FMECA, but primarily an FTA, is pointed out in order to detect and mitigate such potential error states. To detect such potential errors the negation of system functions determined during the second step of an FMECA may be performed, or experience with operating systems and available failure statistics may be consulted. Output of such analyses furthermore involves the maintenance planning, employing techniques such as PHM, together with facilitating the remote access and reset of the subsystems for instance, to increase the maintainability.

As failure data has furthermore shown the future system user and support in its operational environment should be considered in such analyses to address the human factor causing failures. The identification of potential failure modes and their optimisation should address topics such as environmental protection, simplified

handling or modularity, but also deal with operation, for instance the spare management of a maintenance strategy. An example is given in chapter 6 facilitating the exchange of the BLETC optical receiver by replacing the mezzanine board by a commercial transceiver module.

Already after intermediate milestones in the design process, design reviews should be implemented. Even more importantly, once the preliminary final design exists a design review or external audit should be performed. Such reviews should be organised by a project internal designer who nominates experts of different disciplines external to the project and distributes the necessary documents. In a next step the designer introduces the system to the experts pointing out potential problems. Issues found and elaborated solutions are documented together with future actions to be implemented in a third step. These implementations shall be verified in an additional control step. To facilitate the entire process, document templates and a checklist providing questions to be asked in different thematic areas can be elaborated within the organisation. Guidelines for design reviews can be found in [83, 84, 130, 158]. A checklist elaborated for CERN specific designs also comprising a scorecard can be accessed in [159], other checklists can be found in [84, 130, 158]. The process of a design review is illustrated in Figure 5.5.

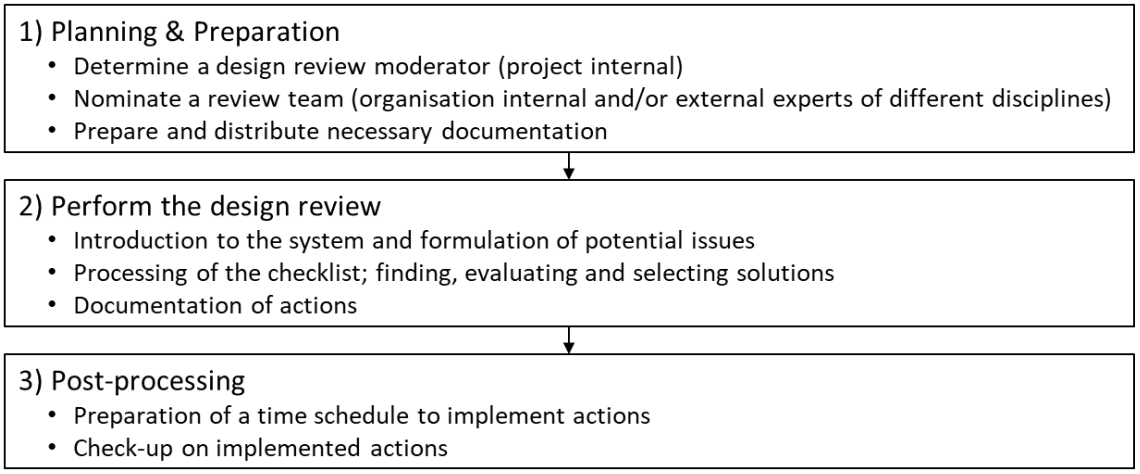


Figure 5.5: Steps in performing a design review, according to [160].

To conclude the planning and design phase, the parallel execution of the design process accompanied by the different methods of the dependability process profiting from continuous exchange and alignment is emphasised. As displayed in Figure 5.3, this does not only concern the present phase, but also specifications and actions for following phases. Furthermore, the general design process involves the production of different versions and prototypes. Besides the development and functional testing purposes comprised in the design process, these devices should also perform the described validation tests of subchapter 5.2.3 to assess, already during this phase, potential shortcomings in order to adapt the dependable design and to mitigate the risk of discovering such design flaws at later phases.

For the long-term perspective, the application of the methodology shall also serve to be adapted to the specific organisation and projects, by developing customised design criteria, analyses' guidelines, checklists and a constantly evolving methodology to be applied. This is to be enlarged by maintaining a performance database to profit from during future projects.

5.2.2 The Production Phase

During the production of pre-versions within the design phase, the production process should be already defined and reviewed to establish a well-functioning process for the series production mitigating potential complications and delays. Figure 5.6 displays the main process steps, during and in between each the process should be validated and constantly controlled.

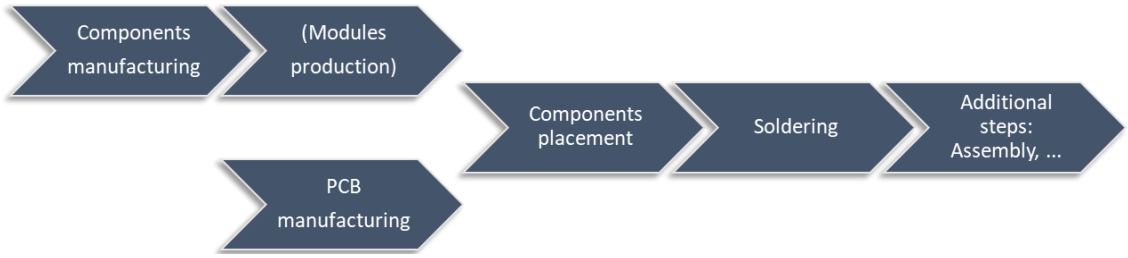


Figure 5.6: Main process steps during the production of a PCB assembly.

To set the boundary conditions, it is recommended to refer to a standard defining general criteria for the entire process, in particular for the case of external production. Common standards are the IPC-A-600 [161] defining acceptability criteria for PCBs and the IPC-A-610 [162] for electronic assemblies, which are also described in the case study of chapter 6. To select the manufacturer, attention should also be paid for according certifications, in principal the ISO 9001 certification for quality management systems [163].

The chosen standard should define applicable criteria for acceptance of the produced PCB and the entire assembly, *i.e.* defect and anomaly criteria. To achieve these, it should give instructions for the individual processes, define necessary inspections during these processes to survey the PCB production by trace impedance measurements or micro-sectioning for instance, assure correct component placement and soldering, provide instructions on handling of the components and the final assembly in between steps, as well as define cleanliness criteria during the entire process and for the final acceptance. Different inspection technologies comprise optical camera inspection for components placement, X-ray to inspect PCB layers and bottom termination components such as Ball Grid Array (BGA) and Quad Flat No-leads (QFN), or destructive methods such as micro-sectioning for a metallographic analysis of the PCB laminate and Plated-Through Holes (PTH). To analyse and validate the process, a PFMEA assists in determining potential process failure

modes and in optimising the process. For internal production, the execution of a PFMEA should be mandatory.

Next to a production standard covering the entire process and acceptance of the final assembly, the implementation of potential intermediate tests and inspections in between the main process steps of Figure 5.6 should be assessed. An output of performed design analyses may be the integration of additional tests at intermediate process steps. Such tests can be necessary for custom designed components or modules, while for commercial components it should be referred to qualifications performed by the component manufacturer. Component qualifications such as high reliability [164] or automotive, *e.g.* for ICs [165], assure a certain level of quality and should be favoured. Such qualifications themselves rely on a variety of individual standards of which a majority is from the US DoD or JEDEC organisation, for example outlined in [124, 164]. To test and qualify custom designed components the corresponding standards should be consulted. An example provides the GOH module with its custom designed GOL ASIC primarily designed for the harsh environment inside the CMS detector. For the ASIC and the module, a comprehensive campaign comprised a large variety of tests for environmental qualification, burn-in and lifetime testing, as well as component-specific tests such as "wire-bond pull strength" for instance, see [58]. The according inspections and tests are to be integrated into the process shown in Figure 5.6. The following case study outlines such tests for a custom designed DC/DC converter module on a custom designed test bench.

Then, for the entire PCB assembly it is likely beneficial to design a test bench executing an End-of-Line test to check the functionality of the produced final assembly, in addition to fulfilling the acceptance criteria. Such a test is also comprised in the case study. In fact, the End-of-Line test is a first filtering, or screening, before the actual testing phase. Issues found at that stage reduce the effort required to detect them later in the life cycle, thus reducing expenses.

Finally, between steps and phases of the methodology, devices are handled and moved, which should always be done in a manner to prevent inducing defects. A main transition is the transport from the manufacturing site to the testing or installation site. To not induce defects, the devices should be packaged in a way to prevent any environmental influence. Humidity and ESD protective packaging should be used. To prevent mechanical influence from shocks and vibrations a stress profile during the transport can be assessed (see [166]) and adequate actions taken using shock absorbing material, compare Figure 6.14. It is advantageous to use shock or humidity indicators monitoring such influences during the transport and indicating a too high exposure at reception.

5.2.3 The Testing Phase

Figure 5.3 displays that the necessity of testing is already defined, as well as partly performed during the design phase. The methodology distinguishes between two categories of tests, on the one hand tests under the term validation to be performed with a sample of the production and, on the other hand, tests to screen the entire production for early failures as well as tests to determine the reliability. Prior to performing any of the tests, fail criteria are to be defined based on the design and dependability specifications.

Validation Testing

Validation as defined in Table 3.2 provides "objective evidence, that the requirements for a specific intended use or application have been fulfilled" [76]. The tests outlined in Figure 5.3 are performed to validate the design and its functionalities as well as its individual operational environment. Furthermore, this involves high stress tests to determine and validate specific stress-strength margins.

The first step represents tests to perform a functional validation of the design by identifying potential design weaknesses. Besides pure functionality tests, this may also comprise tests at nominal operation conditions, for instance, to test signal quality, Electromagnetic Interference (EMI) or infrared temperature measurements reviewing the calculated thermal characteristics of components.

The second step encompasses a variety of tests applying stresses which can be referred to as environmental validation. Based on the specifications formulated in the planning phase, according tests are to be performed. From these specifications the stress categories are derived, either mechanical, thermal, chemical, electrical, electromagnetic, magnetic or radiation, as well as how the stress is applied, *i.e.* at constant or varying conditions. Despite these stresses also other potential impacts on the devices during operation such as different contamination or human interaction may be taken into account. Different occurring stresses during operation may be separated or combined increasing the overall stress level. The stress levels should be determined conservatively above the maximum levels reached during the life cycle. This does not only encompass operation, but also non-operational or maintenance periods. In addition, potential degradation may be taken into account. More information on how to define the variety of stresses as well as other particular stresses can be found in [166]. To perform the tests, equipment such as climatic chambers, vibration shakers or irradiation facilities are to be consulted.

Having the design and its operation validated at nominal conditions, it is beneficial to test higher stress levels up to the maxima the device can withstand, hence performing destructive tests. Such testing has the objective of triggering potential failure mechanisms to determine the stress-strength margin and to derive a benchmark for potential degradation, *i.e.* for the expected lifetime. Furthermore, such tests

provide feedback on the design revealing potential weaknesses, hence and as the first two steps, they should already be performed with first prototypes to enhance the design robustness. A very common stress for such tests is temperature, characterised by an exponential stress increase according to the Arrhenius relationship, compare Table 3.5. Other stresses are strong vibration or high dose irradiation testing of cumulative effects such as Displacement Damage or the TID limit for the intended system lifetime, see [167, 168]. Other irradiation tests to determine the effect of transient radiation errors [168, 169] are part of the previous step.

Screening and Reliability Testing

Having the design in its operational environment validated and the series production running, the produced devices should undergo a screening for early life failures. Because completing the first period of the bathtub curve at nominal conditions takes a long time, the application of accelerating conditions is favourable. The definition of the applicable stresses for this ESS has already been done within the validation tests. Also, the results of the various validation tests, in particular the high stress tests, serve as input to define the stress levels.

The precise definition of the stress level, which amongst several parameters involves its amplitude as well as its time of exposure, is a difficult task. On the one hand it bears the risk of being set too high, potentially inducing defects or significantly reducing the useful life of the devices. On the other hand, it bears the risk of being set too low resulting in not screening reliably all defective devices or requiring long testing times. The initial level should be set conservatively low consulting all data available and potentially performing additional tests at different stress levels. During the entire screening campaign, the obtained data, especially the evolution of the failure rate, should be monitored while reviewing these set parameters. An example of an evolving failure rate during a screening campaign is displayed in Figure 6.17 of the following chapter. While doing so, it is important to thoroughly perform a failure root cause analysis and to strictly separate the occurring failure mechanisms. Furthermore, it is important to verify that the level is sufficiently high to screen all relevant failure mechanisms present in earlier tests. This is a similar difficult task comprising the possibility that certain mechanisms are only triggered at very high stress levels. To overcome this, it is possible to extend the test duration for a sample of devices and monitor the potential occurrence of such failure mechanisms, as being done in the case study of the following chapter. Despite this, the possibility to raise the initially set low stress level while obtaining more data during the campaign should also be considered.

The stresses are always to be defined according to the present failure mechanisms, however as pointed out in subchapter 3.4.2, effective stress categories are temperature cycling and random vibration followed by high temperature and elec-

trical stress [84]. It is mentioned that certain failure mechanisms resulting from failure causes, for instance weak solder joints, may be triggered by a variety of stresses. To accelerate the crack propagation in solder joints both temperature shocks or vibration may be used.

Once the screening data is sufficient to assure that the useful life region is reached represented by a Weibull shape parameter $\beta \lesssim 1$, *i.e.* no or very few failures in the late phases of the screening, this data from a certain point in time onwards may already be taken into account to assess the failure rate during the useful life period. The application of an according confidence level is to be considered.

To increase the data basis of this failure rate assessment, the devices may perform a "Run In" at operational conditions. The objective is to accumulate supposedly failure-free testing time in order to demonstrate a specified reliability requirement. A second objective can be to assure a successful screening, for which a collective strategy for ESS and Run In may be determined reducing the screening effort or risk by reducing either the time or stress level. The resulting failure rate, respectively *MTTF*, can be determined using Table 3.3.

Lastly, the execution of thorough inspections and tests during the production phase, such as the described End-of-Line test, is emphasised. Such a pre-filtering of defective devices may significantly reduce the screening effort, especially regarding the identification and potential misinterpretation of occurring failure mechanisms.

5.2.4 Installation, Commissioning and Operational Phase

The main period of this fourth phase is the long operational phase. However, the prior performed installation and system commissioning may strongly influence the operational dependability in the positive as well as in a negative way. The system installation involves a high risk of inducing defects, hence it should be thoroughly planned and documented ahead along with instructions and training of the executing personnel. The subsequent commissioning phase may be regarded a final validation or integration test of the system into its operational environment. The possibility provided by this phase of evaluating the performance and to enlarge the reliability assessment should be exploited. Certainly however, it should be strictly separated from the testing phase and not be used as an extension of the respective.

Consequentially, the initial operational period should also be well monitored to assure the success of all previous phases fulfilling the requirements. With the start of operation previously planned actions, such as performance monitoring, operational and maintenance support become active.

The maintenance strategy should be defined following the results of the FMECA, moreover of FTA, Petri Nets or Markov analyses. Different types of maintenance ex-

ist, compare [78, 170]. Corrective maintenance is carried out after detection of a failure and should apply to components characterised by random failures not expected to experience any wear out mechanisms, *i.e.* electronics operating at low stresses. Preventive maintenance should apply to components wearing out, such as entire PSUs for example. Prior to the specified *MTBF*, the devices should be refurbished or exchanged at a predetermined point in time during operation. Other more sophisticated types to preventively maintain encompass the proactive condition-based and predictive maintenance types. Both should be implemented based on the dependability specifications and analyses' results during the design phase. Condition-based maintenance relies on performance data measurements to perform maintenance when measured parameters surpass a predefined threshold, while the more elaborated predictive maintenance furthermore processes such data using appropriate formulae or neural networks [171] to precisely predict the time of failure in the future and prepare according actions. The previously outlined PHM deals with this subject [118, 119].

Apart from all that, the maintenance strategy should also involve the logistics planning by providing high availability and fast access of spares, as well as ensuring their functionality, all together enhancing the maintainability. Experience showed that this allegedly trivial task often involves a variety of problems. To overcome potential problems, the maintenance support should be well trained and perform reliably, as well as spares should be readily accessible which also involves corresponding documented instructions. Furthermore, spares should be regularly inspected for their availability and tested for their functionality. According protective packaging and benign storage environment apply, as well as parameters such as shelf lives of components need to be taken into account. Provided the hourly LHC cost estimate in Eq. (1.6), the importance of in this paragraph described tasks is highlighted.

The performance monitoring during operation involves the establishment of a failure tracking system, for example as shown in Figure 4.1. The tracking system should provide data acquisition, allocation, processing and analysis capabilities and the supporting engineers should be trained to perform the according. As shown in Figure 5.3, it should not only comprise operational data, but also data of the three previous life cycle phases. Regarding the parallel operation, it is crucial to achieve the tracing of all occurring system faults and failures with their time of occurrence and perform the analysis in a timely manner. This further involves an in-depth failure analysis of exchanged or repaired modules to determine different failure mechanisms, and thus be able to distinguish between them. Using this data, a Weibull Analysis (see [172, 173]) should be constantly performed in order to be able to identify potential wear out failure mechanisms characterised by a Weibull shape parameter $\beta > 1$, and to take immediate actions. Such actions may involve upgrades or maintenance up until replacement and decommissioning of the system.

A method implementing the tracking of failures is the Failure Reporting, Analysis and Corrective Action System (FRACAS), see [84]. FRACAS does not only encompass operational data, it should already be applied during the design, production and testing phase. Subchapter 6.6 of the case study presents operational considerations for an LHC BLM system upgrade.

5.2.5 Decommissioning

By entering the decommissioning phase, the service life of the present system reaches its end. Nevertheless, being a cycle, the application of dependability continues in order to continuously improve the overall dependability within an organisation. In particular for accelerator machines, such as the LHC characterised by very long lifetimes with constant replacements and upgrades of subsystems adopting to ever increasing performance requirements, this is a crucial phase.

Therefore, the decommissioning of systems provides an extensive source of data to enhance future developments and to improve the accuracy and efficiency of dependability application during the life cycle phases, in other words to improve the entire methodology. This involves performing in-depth failure analyses with the decommissioned systems to provide input for the development process of upgrades and new systems, as shown in the following chapter 6. Such analyses, *e.g.* of destructive nature, may have not been possible during operation. This also comprises potential additional testing to assess the accuracy of previously modelled dependability parameters. For the case of decommissioning only a part of the entire system population installed, this opportunity should be exploited to perform stress tests in order to assess the end of lifetime for still installed systems. The same applies to a potential refurbishment and reuse of systems or parts of systems in other machines.

6 Case Study for the Processing Board Upgrade

The following case study applies the introduced methodology to a major upgrade of the LHC BLM system. The analysis of operational failure data in subchapter 4.3 characterised the optical fibre link between the transmitting BLECF tunnel module up to the receiving BLETC surface module as a weak part for the system dependability. As a result, an upgrade strategy was established to first upgrade the surface processing module and later towards LS3 the tunnel acquisition module [174]. This chapter outlines the development and dependability assurance of the new VFC-HD module as an upgrade for the BLETC, see Figure 2.6. The study entirely covers the methodology from the early planning phase up to the board production and the following reliability tests.

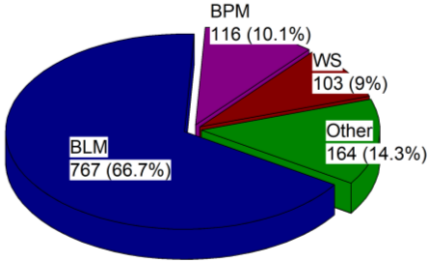
6.1 The VFC-HD Processing Module

After the LHC restart in 2010 at the beginning of the Run 1, the Beam Instrumentation (BI) group of CERN started the development of a new general purpose digital acquisition carrier board for beam instrumentation back end systems. This VME FMC Carrier (VFC) board [175] has been designed for compatibility with the VME standard and the according crates, widely used at CERN. In addition, the board comprises an FPGA Mezzanine Card (FMC) slot for potential extensions of the various user systems.

Table 6.1: VFC-HD main characteristics and distribution to BI systems. The distribution share of the BLM systems includes other accelerator beam loss monitoring systems apart from the LHC (*).

#	VFC-HD main characteristics
1	Intel *Arria V* FPGA
2	HPC FMC slot
3	6x SFP+ transceiver slot
4	2x DDR3 memories
5	6x custom designed DC/DC converter
6	Flexible clocking resources
7	VME64x standard with a custom *P0* connector

BI system distribution	Qty
Beam Loss Monitoring (BLM)*	767
Beam Position Monitors (BPM)	116
Wirescanner (WS)	103
Other systems	164



Over the course of its development, the VFC has become in its third version the VFC-HPC DDR3 (VFC-HD) [176, 177], see Figure 6.1, which has gone into mass production. The FMC slot of that version is a High Pin Count (HPC) connector with 400 pins. Two Double Data Rate 3 (DDR3) memories with each a capacity of 8 gigabits are also mounted. Table 6.1 summarises other main characteristics of the VFC-HD.

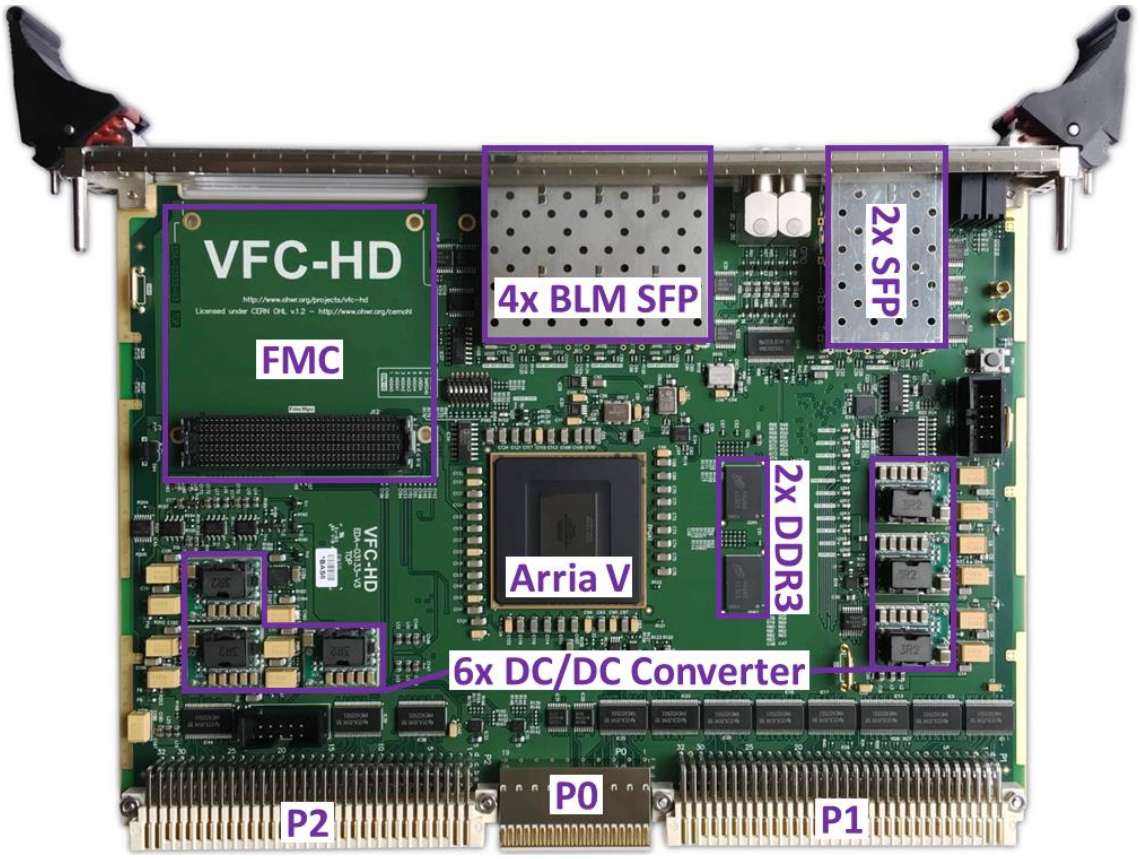


Figure 6.1: Picture of the VFC-HD version 3. The front panel on top of the picture comprises six SFP+ slots, various Light-Emitting Diodes (LED) and electronic connectors (LEMO). The three opposite backplane connectors supply the board with power and communicate via the VME crate backplane.

The series production of the VFC-HD, with a volume of around 1 150 boards in total, was launched in autumn 2018 until in summer 2019 the final boards were received at CERN from an external manufacturer. Two thirds of this production are foreseen for beam loss monitoring systems at CERN. Around 600 of those boards are planned to be used for the LHC BLM system, to replace the BLETC modules, supply other associated systems such as the Diamond BLM or to provide sufficient spare modules. Concerning the costs, the final production price per VFC-HD sums up to 1 200 CHF, which equals 1.38 million CHF for the complete series production.

In particular for the LHC BLM system, the change from the currently used BLETC to the VFC-HD enables additional resources and possibilities. For instance, the increase from 41 000 logic elements of the DAB64x FPGA to 300 000 logic elements for the *Arria V* [178] provides new opportunities for the LHC BLM system protection

strategy as well as to improve its dependability, *e.g.* by implementation of additional or faster diagnostics and related failure mitigation actions. The same applies to the slots for commercially available Small Form-factor Pluggable+ (SFP+) optical transceiver modules and the option to add an FMC for possible future extensions.

6.2 Adjusted Methodology for the VFC-HD

In chapter 5 it is stated, that the introduced methodology is to be adjusted to the specific use case for the individual constraints and boundary conditions. For the VFC-HD project this was done as displayed in Figure 6.2.

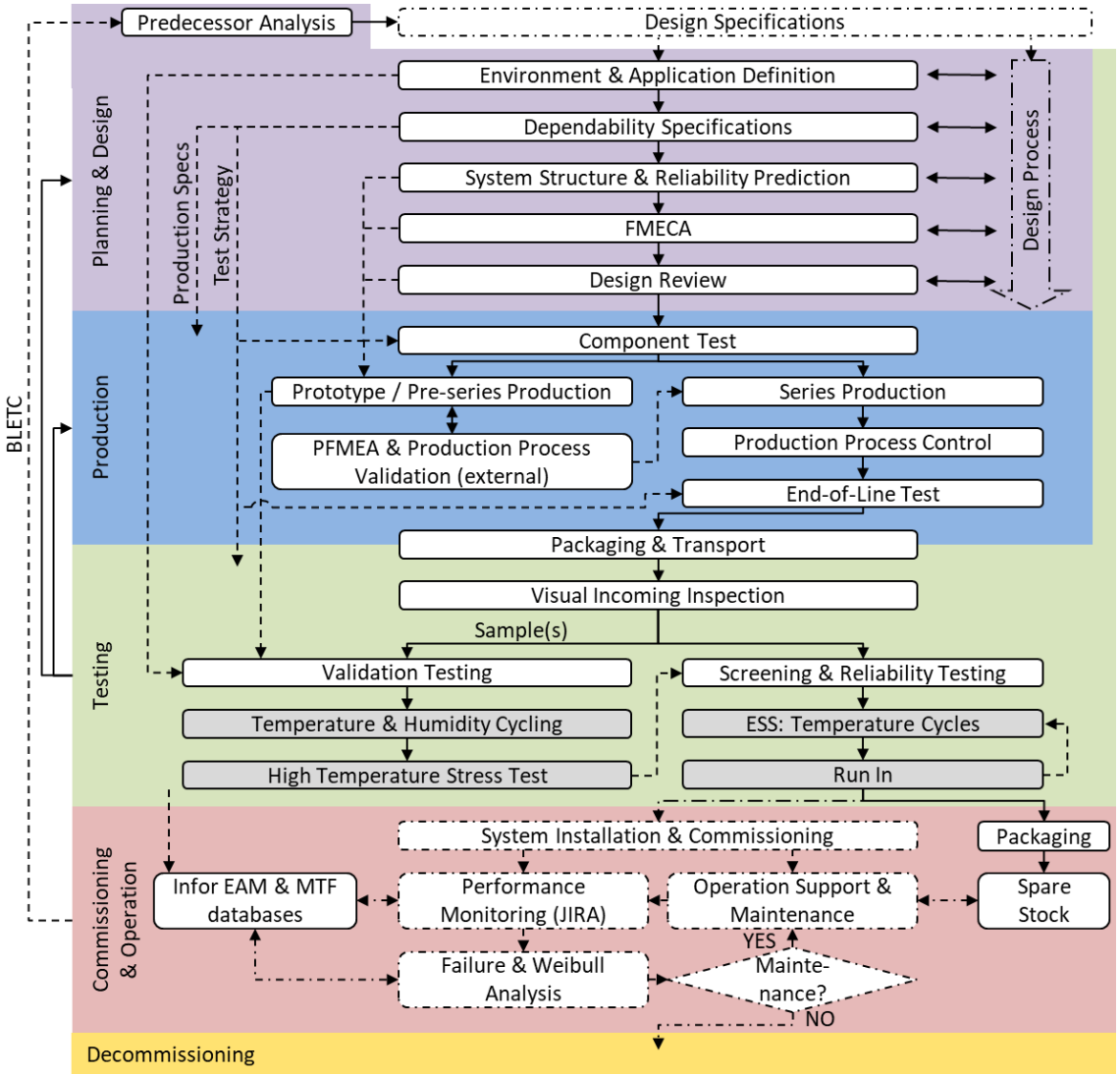


Figure 6.2: Dependability methodology adjusted to the VFC-HD case study [179]. The case study entirely covers the phases from the early planning and board design over the production with according tests and inspections to validation, screening and reliability tests with the produced boards.

The adjustment was influenced by the individual dependability requirements, production volume, specific use environment, and performance data available from the predecessor module BLETC. The following subchapters present the different phases of the case study more in detail.

6.3 Planning and Design Phase

As a part of the LHC BLM system, the dependability requirement of a minimum *MTTF* of 175 000 h during the VFC-HD's useful life period was defined. This failure rate requirement was to be demonstrated by according tests at a high 95% upper one-sided confidence bound, *i.e.* lower *MTTF* (compare Figure 3.6), and includes the execution of a successful screening for early life failures. For the around 350 surface processing modules currently installed, this equals a maximum of 10 accepted failures per LHC operational year of around 5 000 h, which is a lower failure rate as currently recorded for the used BLETC module, compare Table 4.3.

As an output of the BLETC predecessor analysis [180] described in the next subchapter and environmental measurements displayed in Figure 4.4, requirements were derived such as the environmental validation of the module including its optical link for changing temperature and humidity environments [181]. The presence of other environmental stresses was excluded based on the controlled rack environment. Other requirements involving dependability as well as the functionality of the VFC-HD were a simplified maintenance of the optical transceiver modules, as well as additional diagnostic features of these to predict and facilitate maintenance. Furthermore, the outlined increase in FPGA processing resources to implement such features was a requirement.

The VFC-HD then was designed according to its given functional specifications as well as in alignment with the additional dependability requirements. This involved the creation and continuous update of the system structure together with performing a reliability prediction and FMECA. This led to the design changes outlined in Table 6.7.

6.3.1 Predecessor Analysis

The available failure data of the BLETC from subchapter 4.3 triggered a detailed analysis for possible weaknesses of the module [180]. The major identified issues were found on the receiver mezzanine board, which is confirmed by the failure data, as far as the available resolution allows conclusions, compare Table 4.3.

A wide range of different weaknesses was found which most probably in a combined manner led to the occurred failures, in particular to the transmission errors,

referred to as “soft” failures. Table 6.2 presents an overview of the identified issues, major ones are outlined in the following.

Table 6.2: Identified potential weaknesses of the BLETC mezzanine [180].

No.	Category	Potential weakness
1	Environmental strength	1) Temperature/error rate dependence above ~30°C 2) Suspected additional humidity dependence at high humidity
2	Ground plane	Two bottlenecks on the ground plane can lead to a higher current density, thus a concentrated field and thermal heating
3	Power plane	Potential noise influence of redundant A1/A2 link due to A1 transceiver power lines routed underneath A2 transceiver
4	Line routing	Discontinuity of A1 transceiver pinout line layout can lead to errors at 40 MHz transmission speed
5	Oscillator	Potential drift of the quartz oscillator due to aging can lead to inaccuracies
6	Mezzanine solution	Potential shortcomings of the mezzanine solution which adds two additional PCB connectors
7	Manufacturing	Poor manufacturing quality of the installed version 3 mezzanine, *i.e.* soldering and packaging issues

Especially the temperature vulnerability of certain produced boards at rather low temperatures of around 30°C was identified as a major failure cause, which led to an intolerable failure rate, compare Figure 6.3. To address such a potential issue for the upgrade, temperature, as well as humidity validation tests were set up with the new system. In addition, it was decided to use commercial optical transceiver modules instead of the mezzanine solution. The chosen SFP+ transceivers are designed according to the SFF-8431 standard [182].

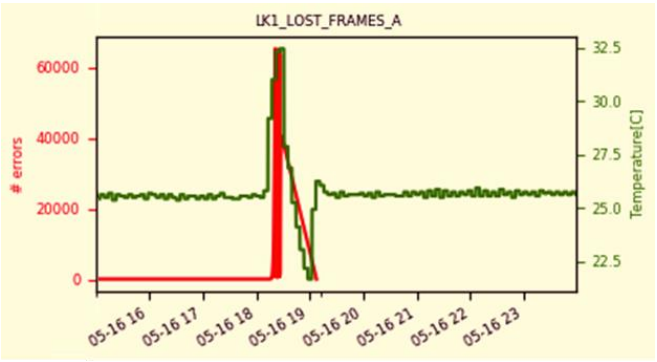


Figure 6.3: Automatically generated report for optical link transmission errors on the 16.05.2017 [180]. For an increasing rack temperature (green), transmission errors (red) start occurring between 27.5 and 30°C and stop at the same temperature when the temperature decreases.

Looking further at the hardware failures of the mezzanine, many can be assigned to issues with the manufacturing quality. One example is the soldering of the transceiver chip pins. For the LHC start-up, the version 3 of the mezzanine was installed.

Afterwards, within a fourth version the design and manufacturing quality was improved while mezzanines were continuously being replaced when failures occur. Nevertheless, still a large number of the third version remains installed.

The issue with the soldering of version 3 is illustrated in Figure 6.4. For the transceiver chip, the solder pads were designed too long, which increases the risk of short circuits induced during manufacturing as well as in operation. In addition, the pads were misplaced which led to a bad coating of the pin during the soldering process.

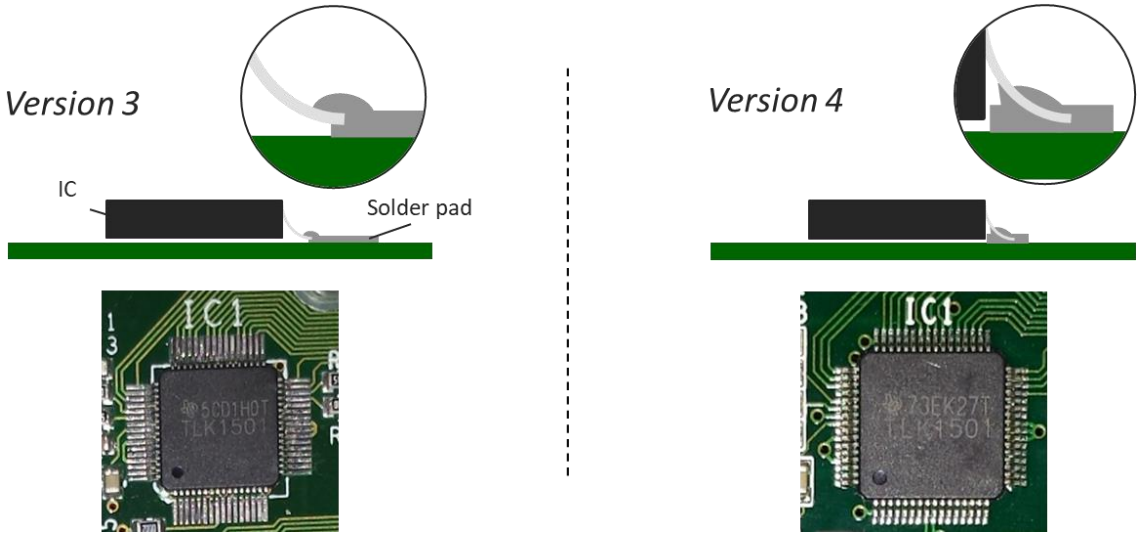


Figure 6.4: Identified solder weakness of the BLETC mezzanine transceiver chip (IC1). The solder pad of version 3 (left) is too large and misplaced, which was corrected in version 4 (right).

Comprehensive conclusions for the dependability process based on this predecessor analysis are presented in Table 6.7 and in the subchapters 6.4 and 6.5.

6.3.2 System Structure and Reliability Prediction

The system structure of the VFC-HD was created together with performing a reliability prediction during the design phase to review the chosen components and the applied derating, estimating and comparing the output for individual system parts and components. The same underlying conditions as for the LHC BLM system dependability model, as displayed in Table 4.5, were applied.

Generated outputs of the prediction to enhance the dependability were implemented in a continuous manner during the VFC-HD design process. Table 6.7 of the following subchapter summarises the outcome. For the final board design, a classification according to the predicted failure rates of the individual board components, moreover for the functional circuits was compiled, see Figure 6.5. For the soldered pins of ICs, which cannot be fully represented by the manufacturer data, a separate block was created to predict their failure rate for the full VFC-HD according to the 217Plus™ model. Based on the block classification it was possible to identify those

system parts which were predicted to be less reliable and further enhance the reliable design of the board. Furthermore, it served to assess the individual risks within the pursuing FMECA. A total of 32 functional blocks were determined, of which Figure 6.5 ranks those with the highest predicted failure rates.

The *Arria V* FPGA is the only component which is part of several functional blocks. Its predicted failure rate is 54.09 FIT which involves a conservative assessment of the internal power dissipation resulting to a constant temperature increase of ΔT = 31°C, see Eq. (6.1). This failure rate was divided into 18 equal parts according to the schematics. In that respect, the failure rate was distributed accordingly to the functional blocks.

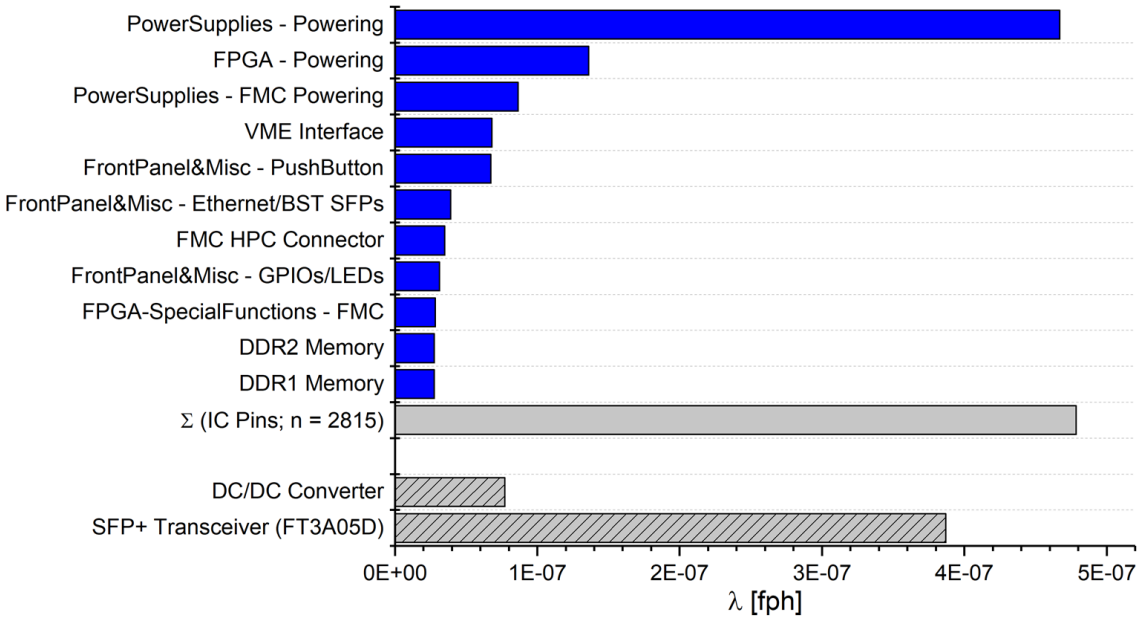


Figure 6.5: Ranking of the VFC-HD highest failure rate functional blocks. For the "PowerSupplies – Powering" block, the model predicts the highest failure rate. This circuit comprises five DC/DC converter modules of which the module failure rate is displayed at the bottom bar. The summarised predicted failure rate of 479 FIT for all IC pin connections is shown in a separate bar. In addition, the manufacturer test data of the chosen *FT3A05D* SFP+ transceiver model is displayed.

Taking into account the fact that the blocks were defined based on their functionality and the necessary hardware to implement that functionality, the ranking is to be considered with care because the total block failure rate does not represent the quantity and categories of the included components. This is a drawback of the loss in resolution when summarising the components to functional blocks. Nevertheless, the initial application of a bottom-up analysis allows to access this information if necessary.

The highest block failure rate of 467 FIT is assigned to the main powering circuit, which represents 29% of the total VFC-HD predicted failure rate. This block is composed of five DC/DC converter modules (Figure 6.6), which contribute the major share to the predicted circuit failure rate. As a single block, one DC/DC converter

would represent the fourth highest predicted block failure rate. The second highest predicted failure rate of the FPGA powering circuit is due to a large number of used decoupling capacitors. The remaining sixth DC/DC converter is part of the separated FMC powering circuit, which is only used when an FMC is plugged in.

As already outlined in subchapter 4.5.1, the resulting *MTTF* for the complete VFC-HD board of close to 600 000 h (1 614 FIT) remains a side note. The implemented improvements as a result of the prediction are paramount.

As a part of the complete module, but as no direct component of the designed VFC-HD, the interfacing SFP+ transceivers and the FMC are considered separately to the prediction of the board as entire components themselves. Especially regarding the module use in the LHC BLM system, no FMC is foreseen for the near future and four SFP+ transceivers are to be used to receive the front end beam loss data from the optical fibre link, compare Figure 2.1. Different constraints have influenced the choice of the corresponding SFP+ transceivers, not at least the cost factor of the for the current system configuration around 1 400 needed. Eventually, the model *FT3A05D* by FTTX Technology was preselected, of which HTOL tests performed by the manufacturer specify 387 FIT for the set environmental temperature of 30°C at an applied confidence level of 90%. Taking into account the use of four transceivers, this is a rather high failure rate, which however is due to a low executed testing time. The test data shows that no failures occurred during the accumulated test time of 95 000 h at the applied environmental temperature of 85°C. The preselection of the *FT3A05D*, was thus made based on the implementation of additional environmental validation tests (subchapter 6.5.2), as well as based on good internal experience of the model already operational in LHC injector BLM systems during the past years.

6.3.3 FMECA

The component blocks and the assigned predicted failure rates of the previous subchapter continuously provided input for the VFC-HD FMECA, which was executed on a higher level as the component level. Several components were summarised to appropriate circuits representing individual functional blocks.

The FMECA was specifically prepared for its integration into the LHC BLM system. As such, circuits not used by the system were reviewed for their possible effect on the system level and for the case they have no effect disregarded. As in Eq. (4.1), for each functional block a worst-case assessment was presumed for the potential effect caused by the sum of all failure modes. The potential end effects were determined for the integrated system on the LHC BLM system level, as in subchapter 4.5.2. The LHC BLM system is designed in a way that the catastrophic effect “Blind Failure” can be neglected for the VFC-HD. The effect “Warning” was further subdivided to distinguish between maintenance to be scheduled during upcoming technical stops and

maintenance which allows to complete the LHC fill, but requires an immediate intervention thereafter. Table 6.3 ranks the effects according to their severity.

Table 6.3: Determined VFC-HD FMECA severity rankings.

#	Severity Rank	Effect
1	Negligible	No Effect
2	Marginal	Scheduled Maintenance
3	Moderate	Immediate Maintenance
4	High	False Beam Dump

Based on this, the FMECA was able to elaborate the prediction results by assigning to each block the determined severity ranking as well as the occurrence probability. This probability was ranked taking into account the dependability requirement of the VFC-HD. As displayed in Table 6.4, the lowest ranking was defined below 300 FIT which is less than one failure during a full year, or around one failure per two years of typical LHC operation for 350 installed modules. Keeping in mind the requirement of maximum 10 failures per year for the full module, this can be tolerated on the functional block level. On the other hand, a failure rate of more than 1 000 FIT can hardly be tolerated for the functional block level.

Table 6.4: Determined VFC-HD FMECA occurrence rankings for the functional block level.

#	Occurrence Rank	Failure Rate [fph]	Failure Rate [FIT]
1	Remote	< 3E-07	< 300
2	Low	< 6E-07	< 600
3	Moderate	< 1E-06	< 1000
4	High	> 1E-06	> 1000

The results of the analysis are displayed in Table 6.5 which shows failure modes of the functional blocks distributed to the four potential end effects. For the LHC BLM system, more than 20% of the total failure rate, or 350 FIT, are assigned to cause no effect on the system level, thus can be neglected for a strict reliability assessment. Yet, these system parts can be vital for the dependability, for instance front panel LEDs, which indicate an error, and, in this way, can contribute to efficient maintenance. Around 4% of the assigned block failure rates furthermore cause a maintenance intervention, while 75%, or 1 254 FIT, lead to a false beam dump request. This distribution can be interpreted in two distinct ways. On the one hand, it is a high proportion which causes the, for this module, worst-case end effect. On the other hand, it also demonstrates that the system was designed in an efficient way, avoiding unnecessary circuits, which themselves can impact the performance. In addition, it is mentioned that the resolution loss of the functional blocks approach is reflected by this data.

Table 6.5: Failure rate distribution for assigned failure modes to end effects.

End Effect	Failure Rate [FIT]	Percentage of Failure Rate [%]
False beam dump	1254	75
Immediate maintenance	55	3.3
Scheduled maintenance	9	0.6
No effect	350	21
Total: VFC-HD	**1668**	**100**

In a second step, the generated risk matrix for the 32 functional blocks of the VFC-HD provided a more precise overview of the tolerated risks as a factor of the failure mode severity and occurrence probability. The added colour scale shows, which risk can be tolerated from green to red.

Table 6.6: Risk matrix for the VFC-HD analysis. The 32 functional blocks are distributed according to their failure severity and occurrence probability ranking on a colour scale for the level of the risk. The summarising block of general IC pin failures was added to the highest severity rank keeping a conservative approach (*).

			Severity (Effect)			
			No effect	Scheduled Maintenance	Immediate Maintenance	False Beam Dump
Occurrence Probability	Remote	< 300 FIT	13	2	5	11 (+1*)
	Low	< 600 FIT				1
	Moderate	< 1000 FIT				
	High	> 1000 FIT				

As it can be seen, the worst-case failure mode of 12 functional blocks leads to the highest severity rank, a false beam dump request. The “PowerSupplies - Powering” block, has the second occurrence probability rank (light red). In order to be able to accept this classification, optimisation actions were taken to mitigate the risk. As the main contributor to the high failure rate are the five DC/DC converters in the circuit, it had already been decided to design these components internally. Nevertheless, the predicted failure rate remained high, which such component category is generally characterised for, especially due to the voltage conversion and therefore the temperature increase. Thus, it was decided to additionally test these components for their functionality during manufacturing (subchapter 6.4.1) and to monitor their behaviour during a high temperature test throughout the VFC-HD board validation, see subchapter 6.5.2.

To ultimately point out the benefit of the VFC-HD dependability analysis building upon the analysis of the predecessor module, the reliability prediction and the FMECA, implemented improvements or mitigation actions as output of the analysis are summarised in Table 6.7. Based on the negligible catastrophic end effect, the execution of an FTA was not foreseen.

Table 6.7: Identified issues and performed actions of the VFC-HD analysis.

No.	Category	Identified/Suspected Issue(s)	Improvement / Mitigation Action
1	Components	Low capacitor voltage ratings	Higher component ratings to increase stress-strength margin
2	Powering (DC/DC converter)	High predicted failure rate & critical component category	1) Internal component design 2) High temperature validation test 3) Component test during manufacturing
3	Optical SFP+ transceiver	Temperature and suspected humidity vulnerability of the predecessor module	1) Temperature and humidity rack measurements for a full year (Figure 4.4) 2) Temperature and humidity validation tests
		Manufacturer data shows low HTOL testing time (*FT3A05D*)	In addition to tests failure rate monitoring during operation
4	Assembled PCB	Manufacturing quality problem of predecessor module	Manufacturing inspections for components and solder joints (IPC-A-610J)

6.3.4 Design Review

A vital step during the VFC-HD design process was the organisation of design reviews involving engineers from other teams and disciplines. This step did not followed a strict course of action rather it was performed in a continuous manner during the board design, executed in regular meetings - in particular for the digital design, as well as electronically. While doing so, a guideline for design reviews of electronic systems comprising a checklist was developed, see [159]. This development also involved reviews of other CERN systems.

Results produced while reviewing the design were continuously integrated, of which dependability related output is comprised in Table 6.7. A lot of other output was of functional nature represented by the different versions evolving from the VFC to the VFC-HD. A summary of this process can be accessed in [183, 184], whilst it is continuing with the new VFC-HS [185].

6.4 Production Phase

Based on a technical specification, the conditions for the supply of 1 150 series produced VFC-HD were established with an external manufacturer. This specification included component and material procurement for the VFC-HD and DC/DC converter modules, PCB manufacturing and assembly, execution of the component and End-of-Line tests by CERN supplied test benches described in the following, packaging, and shipping. Furthermore, various corresponding requirements were specified including a variety of 19 applicable PCB manufacturing and assembly standards, in

particular the IPC-A-600J [161] and IPC-A-610G [162] for PCB and assembly acceptability requiring the highest “performance class 3” for high reliability. Material, tolerances, inspection and test procedures, PFMEA preparation, handling, storage, a Quality Assurance program, and other requirements, described more in detail in the following subchapters were also defined. This had to be accompanied by the according documentation, *e.g.* thermal profile data of the soldering process, potential non-conformity reports, or also PCB substrate quality, impedance of lines and PCB micro-sectioning reports in the form of test coupons. The eventual manufacturer was selected in accordance with the tender procedure of CERN, providing a quality management certification according to EN 9100 and ISO 9001 [163].

After several prototype boards were already produced during the design phase for various purposes, *e.g.* to test functionalities or to debug the board and digital design, as well as a final pre-series of ten boards for similar development purposes and the validation tests described in subchapter 6.5.2, the series production of 1 150 was launched. Focussing on the dependability related activities, the following subchapters describe the entire process up to the delivery at CERN.

6.4.1 Component Test

The previously determined component test of the DC/DC converter module [186, 187] was established with the start of the series production prior to the board assembly of around 7 000 modules, compare Figure 6.6. For the other standard components mounted, no further testing was performed, relying on the specific datasheet qualifications of the chosen components.

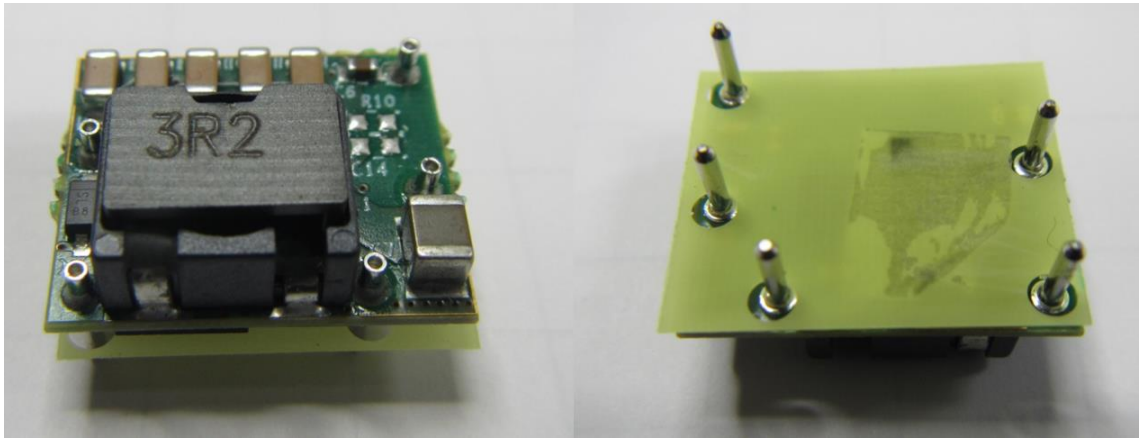


Figure 6.6: VFC-HD DC/DC converter module.

An automated test bench ensuring reproducibility and traceability was designed at CERN, able to test 16 modules produced on a single panel at once [188], compare Figure 6.7. Setting the DC/DC converters to deliver 3.3 V, the test bench also executed a short pre-screening sequence, applying a stress of 3 A sinking at the output.

The corresponding output voltage of 2.7 V was checked between defined thresholds of lower 2.4 and upper 3.2 V.

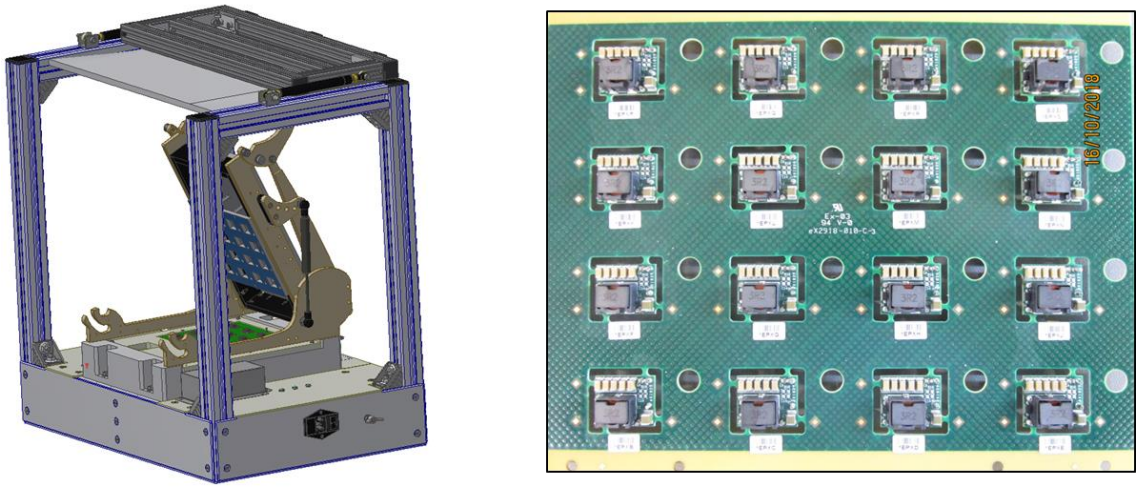


Figure 6.7: Automated DC/DC converter test bench and produced panel [188]. The test bench (3D drawing, left) is able to test 16 modules at once. By closing the handle, spring-loaded pins connect to the modules on the inserted panel (right) enabling the test to be executed. Each module is traceable by an individual barcode sticker put onto the module during VFC-HD assembly.

The test assured that only fully functional DC/DC converter modules inside defined tolerances are mounted onto the VFC-HD, and in this way minimised potential delays and costs arising from later on detection and correction. Together with additional inspections established during the module production, it provided failure data as a design and production feedback. This had primarily been production defects with around 85 defects related to soldering, 25 to misaligned or damaged components and four to the PCB. A single actual failure detected was a shorted capacitor, repaired by replacement. [188]

In the framework of the complete test strategy for the DC/DC converter module, the afterwards performed functionality, screening and Run In tests on the system level were also taken into consideration, potentially detecting additional defects, as well as the results of the validation, especially the high temperature stress test.

6.4.2 PCB Production and Assembly

Following the production of the 12-layer PCB in compliance with IPC-A-600J, the DC/DC converters and all other components were assembled and soldered to the final VFC-HD module following IPC-A-610G. The full process complying with a variety of other required standards encompassed a total of 54 process steps, which involved 23 distinct intermediate inspection and three washing steps, compare [189]. Inspections comprised optical camera inspection, X-ray scans, *e.g.* for the PTH and BGA components, or ionic contamination tests.

6.4.3 Functional End-of-Line Test

As for the DC/DC converter modules on the component level, a second test bench was designed at CERN to perform testing on the VFC-HD system level, see Figure 6.8. The goal of this End-of-Line test to be performed with the fully produced boards was of pure functional nature, assuring a set of basic functionalities working before shipment to CERN, *i.e.* pre-filtering the production before further testing at CERN, hence mitigating costs and delays.

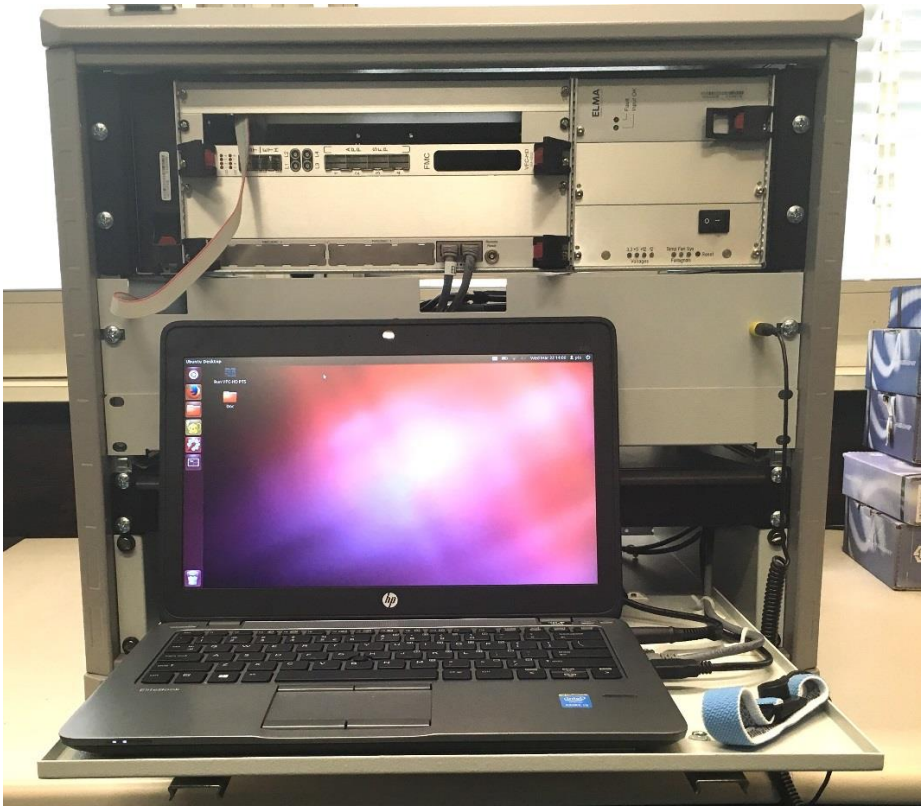


Figure 6.8: Test bench for the VFC-HD End-of-Line test. Each DUT had to be tested at once running the custom Production Test Suite.

The test bench was designed for testing a single board at once. Executing the test, the test bench writes the specific test program onto the VFC-HD FPGA, which checks a total of 16 basic functionalities, compare [189]. The results are accessed and saved on the connected computer, on which a software tool automatically saves a file for each performed test.

To test the SFP slots, the test was performed plugging electrical loopback modules with an attenuation of 5 dB, significantly above the estimated attenuation during later operation. If not passing, a second attenuation level of 3.5 dB was also accepted. This was decided whilst pre-assigning the 5 dB boards with the higher strength margin (compare Figure 3.10) to the LHC BLM system, the most critical amongst the user systems. Final results showed more than 85% of produced boards passed the 5 dB test.

6.4.4 Packaging and Transport

In order to deliver the produced boards to CERN, the VFC-HD modules were individually packaged in ESD protective bags inside a cardboard box with shock absorbing material, compare Figure 6.14. This had the objective to mitigate the risk of inducing defects during the shipment. To ensure that no transport damages were induced, an additional inspection step was added on reception at CERN, see subchapter 6.5.3.

6.5 Testing

This subchapter encompasses tests performed on the system level after delivery of the VFC-HD at CERN. As illustrated in Figure 6.2, these tests comprised validation during the design and pre-series-production phase as well as inspections, screening and reliability tests performed on the full series production.

6.5.1 Test Setups and Configuration

In order to execute the various tests, a test bench including a dedicated FPGA configuration was developed to test the various internal functionalities as well as the interfaces of the VFC-HD. Furthermore, different test setups were prepared to perform the different tests and to create the specific conditions.

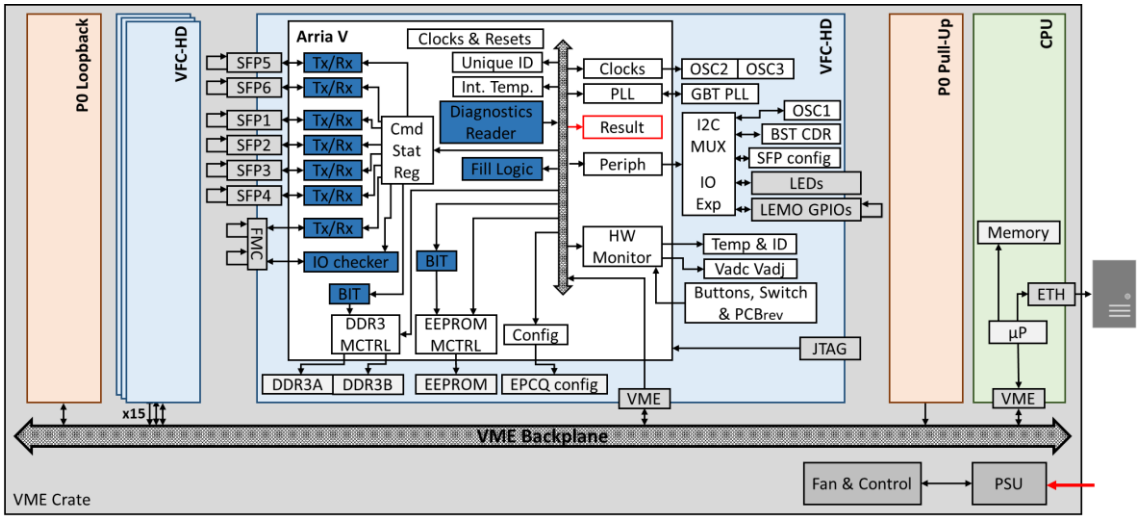


Figure 6.9: VME crate test setup with *Arria V* Built-In Test (BIT) configuration [181]. The crate can be equipped with up to 16 DUTs, independently running the BIT on their *Arria V* FPGA. The individual test results are constantly updated into a result register (red), which can be queried every second by the CPU module over the VME bus and further logged onto a database.

To constantly test and monitor the various board functionalities and to log the results, the VFC-HD FPGA was configured with a Built-In Test (BIT). As displayed in

Figure 6.9, the FPGA configuration allows to access and test the different board functionalities. To give two examples, this is done by sending a pattern to the plugged SFP+ transceivers, which loop back the signal to be read back by the FPGA checking its correctness, or by first writing to the DDR3 memories, then reading back. The tests are performed in parallel and constantly, *i.e.* the distinct 220 tested parameters are written to a dedicated results-register inside the FPGA, updated at a frequency of 100 MHz. Furthermore, the FPGA was configured in accordance with a worst-case operational scenario in terms of potential noise, power consumption and in this context internal temperature increase.

Figure 6.10: Fully setup VME crate inside the climatic chamber. The displayed configuration allows testing of 16 DUTs in parallel, all equipped with FMCs, LEMO connectors and SFP loopback modules.

The FPGA configuration allows to perform all tests described in the following. During the tests, the VFC-HD boards are plugged into the VME crate, see Figure 6.10. Up to 16 Devices Under Test (DUT) can be tested at once, which is the same configuration used for the LHC installation, compare Figure 2.1. The crate configuration comprises three additional custom boards designed to test the *P0* backplane lines, a pull up board for the two daisy chain backplane signals, a board to loop back these signals and a jumper board available from the LHC configuration to forward the lines for the central BOBR board slot, compare Figure 6.10. Over the VME bus, the DUTs

communicate with the standard CPU board, for which a real-time software was written to access the test status and results at a modifiable rate between once per second up to every 60 s. [190]

The CPU board moreover establishes an Ethernet link to the database to log and save the results as well as feeds a test application providing a Graphical User Interface (GUI). The GUI enables to select the different test modes and to configure the test, compare Figure 6.15. In addition, the GUI provides a real-time monitoring tool during test execution. This especially turned out to be helpful during test preparations and start-up. [190]

Finally, the complete crate can be placed inside a climatic chamber to create the environmental test conditions, as displayed in Figure 6.10. Specific configurations for the individual tests are described more in detail in the according subchapters. The boundary conditions of the design, setup and operation environment are displayed in Table 6.8.

Table 6.8: Boundary conditions for the VFC-HD tests.

Limits	Parameter	Value	Data source
Board Design	Temperature	0 - 54°C	T_{min}(component datasheets); T_{ArriaV} (P_{diss_max}) from Eq. (6.1)
Operational Environment	Yearly temperature (failure state)	<25°C (≥ 29°C)	Data loggers, see Figure 4.4 (DAB64x sensor, see Figure 6.3)
	Yearly humidity	8 - 77% RH	Data loggers, see Figure 4.4
Climatic Chamber	Temperature control	-40 - 180°C	Datasheet
	Temperature rate of change	≤ 5 K/min	Datasheet
	Humidity control	10 - 98% RH	Datasheet (theoretical)

In summary, the developed test bench is configurable for the four distinct tests described in the following subchapters and able to test all VFC-HD functionalities, with a single exception of not testing 40 lines of the *P2* rear transition modules. This compromise was made due to the required expenditure and only accepted having the lines already tested during the End-of-Line test at the manufacturer. In addition, these are for the current BI system implementations, in particular the LHC BLM system, only spare lines not being used.

6.5.2 Validation Tests

To validate the design and successful production process of the VFC-HD on the one hand and its operation in the installation environment on the other hand, the according tests performed are described in this subchapter. Subchapter 6.4.3 has already outlined a post-production test of the main functionalities, which was carried on by validating the functionality at the limits of the operational environment in the

following subchapter. A second high temperature stress test intends to determine the upper temperature limits, moreover to validate the reliability requirements and the associated design margin (compare Figure 3.10) for temperature induced failure mechanisms, providing specifications for the temperature cycling test described in subchapter 6.5.4.

Temperature- and Humidity Environmental Validation

Environmental influences affecting the successful operation of the VFC-HD are limited regarding the later installation environment inside stationary temperature-controlled closed racks. This led to the exclusion of several stressors to be tested, such as vibration for example. However, the failure analysis of the predecessor module led to testing potential temperature and humidity influences. The analysis showed transmission errors for certain modules of the surface optical link with a dependency to increasing temperatures, caused for example by cooling failures or opened rack doors resulting from interventions, already starting at rack temperatures down to 29°C, as well as a suspected humidity dependency [180], compare Figure 6.3.

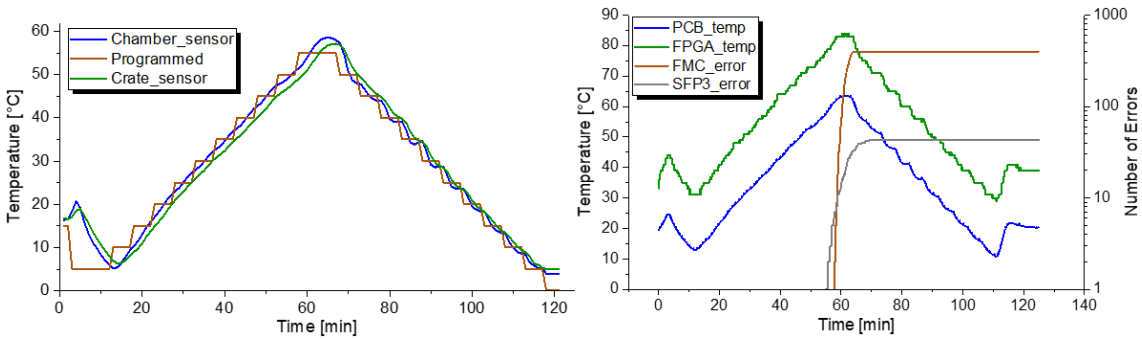


Figure 6.11: VFC-HD validation test temperature cycle [181]. The left graph displays a programmed (brown) temperature cycle between 5 and 55°C inside the climatic chamber with the following temperature curves of the chamber sensor (blue) and an additional sensor inside the VME crate (green). The right graph shows the fourth test of Table 6.9 with two temperature curves of a separate on-PCB chip sensor (blue) and the FPGA internal sensor (green). Around the temperature peaks incrementing FMC (brown) and SFP (grey) errors can be observed.

In addition to the predecessor experience, data from temperature and humidity sensors installed inside and outside the surface racks for a complete year (see Figure 4.4) was taken into account to define a test strategy in order to determine the required design margins, in other words the operational window. The test strategy determined in this manner gradually increases and decreases the temperature and humidity conditions whilst providing the flexibility to monitor the resulting optical link communication error rate and adapt the conditions in order to determine the design margins more precisely. Having the immediate response, the climatic chamber conditions were varied in a pyramid shape with dwell times at intermediate steps to ensure the temperature propagation inside the components, see Figure

6.11. According to Table 6.8, the test was performed inside the design temperature window with the lower 0°C limit for certain components' datasheet restrictions and the upper limit for the maximum junction temperature of the *Arria V* FPGA, determined at peak performance [181]:

$$T_{test\_max} = T_{j\_max} - \Delta T = 85°C - 31°C = 54°C\ , \tag{6.1}$$

with the maximum recommended junction temperature T_{j_max} given in the datasheet and the conservatively assessed internal temperature increase ΔT from internal power dissipation. In order to prevent condensation, the humidity was varied up to 90% RH.

With the conditions set for the temperature and humidity characterisation, a second goal was to test different configurations on the SFP+ transceiver slots and to equip the boards with FMC loopback mezzanines. The full operational setup with the LHC tunnel module sending data over the up to 2 km optical fibre link could not be reproduced, which is why three different SFP setups aimed to investigate potential failure mechanisms and draw conclusions for the operational setups. The SFP+ transceiver function was used to transmit and receive the test signal both from the VFC-HD.

An SFP electrical loopback module (LB) with 3.5 dB attenuation was used for reference purposes and to exclude the VFC-HD as potential failure cause. The other two configurations used the foreseen *FT3A05D* SFP+ transceiver from "FTTX Technology" [191]. One looped back the signal with a 1 m long fibre cable (LC), the other (Mix) used output and input patch cords converting the two different connector systems, "LC" of the SFP+ transceiver and "E2000" currently and continued to be used in the LHC BLM system. Between the patch cords, two E2000/E2000 adapters were connected, such as in the operating system, compare Figure 2.1.

Once the final board design was available, the environmental validation was executed with two boards of the pre-series each having all six SFP slots occupied. The results are summarised in Table 6.9.

With the objective to dynamically adapt the strategy, eleven tests were performed in total. The first two tests were executed with the purpose of functional validation at the temperature extreme values with all SFP slots equipped with electrical loopback modules, the third at a high humidity of 80% with one DUT equipped with the LC configuration. No SFP failures occurred during these tests. Based on this first validation, five temperature cycling tests (4 to 8) were performed varying all SFP configurations. Test 4, displayed in the right diagram of Figure 6.11, shows the incrementing SFP errors for the LC-configured DUT A around the temperature peak. This result led to investigating this region more in detail during three more tests (6 to 8) at reduced temperature steps of 2.5°C, represented by the red curve in Figure 6.12.

Table 6.9: Environmental validation cycling tests summary [181]. Temperature steps of at first 5°C (1), then 2.5°C (2) were used. The humidity was raised at steps of 10% (3). Tests 8 to 11 were performed with six new SFP+ transceivers on DUT B (4).

Test	Temp. range	RH range	SFP configuration		SFP errors		FMC errors	
No.	[°C]	[%]	DUT A	DUT B	DUT A	DUT B	DUT A	DUT B
1	5	< 35	LB	LB	/	/	/	Yes
2	55	< 50	LB	LB	/	/	Yes	Yes
3	25	80	LC	LB	/	/	Yes	/
4	5 - 55[1)]	50	LC	LB	Yes	/	Yes	/
5	5 - 55[1)]	70	LB	LC	/	Yes	/	/
6	35 - 55[2)]	50	LB	LC	/	Yes	/	/
7	35 - 55[2)]	50	Mix	LB	Yes	/	/	Yes
8	35 - 55[2)]	50	Mix	LC[4)]	Yes	Yes	/	/
9	30	50 - 90[3)]	Mix	LC[4)]	/	/	/	/
10	30	80	Mix	LC[4)]	/	/	/	/
11	40	80	Mix	LC[4)]	Yes	Yes	/	/

The correlation of an increasing error rate with increasing temperature was confirmed. It was found that the upper temperature limit for error-free operation is at 40°C, see Figure 6.12. A wide spread between different SFP+ transceivers was found, for example did the transceivers in slots 2 and 4 show no errors, reaching a Bit Error Rate above 6E-15, while the one in the third slot showed errors during all tests. Furthermore, show temperature values of the first and last error occurring at increasing and later decreasing temperatures a degradation path. This effect was especially caused by the transceiver in slot 5.

Test No.	4	5	6	7	8	8
VFC-HD DUT	A	B	B	A	A	B
SFP+ config.	LC	LC	LC	Mix	Mix	LC
T(1st error) [°C]	57	53	46	44	42	46
T(last error) [°C]	54	45	45	40	40	45
SFP slot 1		3	8			
SFP slot 2						
SFP slot 3	40	200	700	1	1	1300
SFP slot 4						130
SFP slot 5			1300	500	350	
SFP slot 6		30	90	30	16	

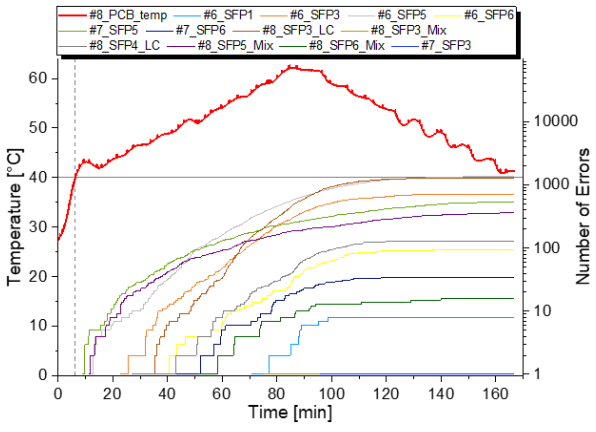


Figure 6.12: Summary of SFP+ transceiver errors during temperature cycling tests (left) and combined graph of incrementing errors during tests 6 to 8 (right) [181]. Please note that the first five tests were performed with the same SFP+ transceivers; for DUT B in test 8 additional transceivers were used.

To test for humidity, two more tests were performed after the third test had already validated the used configuration at 25°C and 80% RH. Unfortunately test 9

showed condensation inside the climatic chamber, likely caused by interference of the crate, occupying most of the chamber volume (see Figure 6.10), with the humidity regulation. This led to only being able to raise the humidity and the execution of two more tests at constant humidity.

Based on the outcomes, it was concluded that the upper temperature limit of 40°C, for high humidity of 30°C, is low, but accepted for later operation in at 25°C controlled racks. Resulting consequences were to continue monitoring the observed degradation, if it is observed for the lower and constant temperature conditions in operation. The decision to use the *FT3A05D* transceiver was made based on cost considerations having to purchase more than 1 500 transceivers, performance considerations and the five diagnostic parameters provided by the chosen model, *e.g.* supply voltage, received optical power or temperature. Furthermore, the decision was based on 5 years of operational experience with around 100 devices of the chosen model in BLM systems of the LHC injector chain. The modular integration with its hot-swappable function supported the decision facilitating a fast exchange by another model in case of poor performance in operation.

Regarding only the VFC-HD, the board was validated for the applied conditions since no hardware failures, neither communication errors were observed during the complete test campaign. For the two different fibre connection setups LC and Mix, no negative effect of the additional adapters was observed, in fact, the LC setup showed more errors. Making use of the transceiver diagnostic parameters, additional tests showed that the higher LC setup failure rate was likely caused by a saturation at the receiver end as a result of the short fibre length.

It remains to be mentioned the test results of the FMC. An analysis identified the FPGA test firmware used at that time as cause of failure. With a later version resolving timing issues no further FMC errors were observed during additional tests. In any case, it is not foreseen to use the FMC extension for the LHC BLM system.

High Temperature Stress Tests

The strategy of the high temperature stress tests was to raise the environmental temperature in steps aiming to determine the margin between operational temperature and actual design strength, compare Figure 3.10. In addition, the acquired data should provide input to tailor the later screening conditions.

In total, four tests were performed with boards of three different productions, one prototype, two pre-series boards and one final design board of the series production. Tests were performed after completed milestones in the development with the test bench being developed in parallel. Table 6.10 summarises the tests.

Table 6.10: High temperature stress tests summary.

Date	Production batch	$T_{max\_chamber}$	SFP	FMC	Errors	HW failures
26.07.18	Pre-series	70°C	LC	Yes	SFP+, FMC	/
26.07.18	Pre-series	70°C	LB	Yes	EEPROM	/
31.08.18	Prototype (V2)	100°C	LB	Yes	/	/
27.11.18	1st series batch	115°C	LB	Yes	Multiple	/

The two pre-series boards were tested with the VME crate inside the climatic chamber, which restricted the maximum achievable temperature to 70°C [181]. The analysis of the occurred FMC and Electrically Erasable Programmable Read-Only Memory (EEPROM) errors also identified the test firmware as failure cause as outlined in the previous subchapter. The third test should have already been performed during the development after production of the Version 2 (V2) prototype, however, it could not be executed without the test bench being available. Performed once the final test bench was available, with only the DUT inside the climatic chamber connected via three backplane connector cables to the VME crate outside, no errors occurred up to a temperature of 100°C.

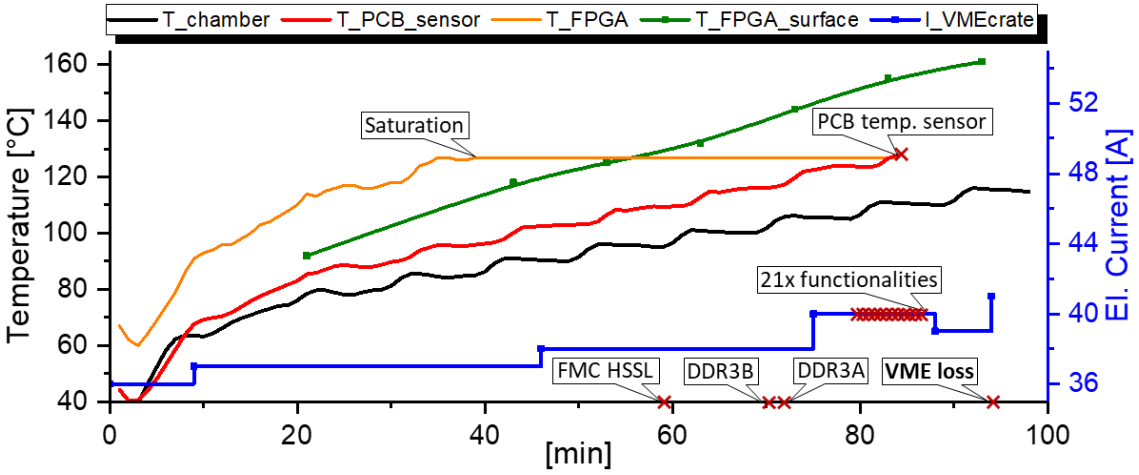


Figure 6.13: Series production high temperature stress test (27.11.2018). The four top curves represent measured temperatures of the chamber sensor (black), the on-PCB temperature chip (red), the internal FPGA sensor (yellow) and manually taken infrared measurements on the FPGA surface while opening the chamber door. The current consumption measured by the VME crate outside of the chamber is shown on the bottom. The red crosses represent lost functionalities. [192]

The fourth test validated the series production up to a temperature of 95°C ("FMC HSSL" failure), moreover above 100°C if the first failure affecting the LHC BLM system is taken into account (DDR3B). Figure 6.13 displays the test results during which the temperature was increased in small steps of 5°C with sufficient dwell time up to 115°C. The majority of functionalities was lost between 105 and 110°C, until the VME communication with the CPU failed at 115°C. When the on-board LEDs

which indicate an operating FPGA went off after around five more minutes, the test was terminated.

It can be seen that the current consumption of the crate increased by 5 A, with a drop around 110°C, most probably due to the loss of several functionalities. The increase can be explained by the effect of an exponentially increasing subthreshold power leakage of transistors, not fully turning off anymore at increasing temperatures [193]. This effect can explain the steeper temperature slopes of the *Arria V* FPGA (yellow and green), with its 300 000 Logic Elements (LE) [178] equal to approximately $1 – 2*10^9$ transistors depending on the LE design, in relation to the chamber (black) and PCB chip sensor (red) temperatures. Unfortunately, the readout value of the internal FPGA temperature sensor saturated at 127°C, but as examined in the Appendix, using a conservative linear extrapolation an internal FPGA temperature of 197°C was determined at the time the VME communication was lost.

After termination of the test, the chamber temperature was decreased slowly, during which all board functionalities recovered. Analysis and further operation showed no hardware failures caused by the test. This was the case for all four tests performed, resulting in a successful high temperature stress validation of the VFC-HD hardware design, providing feedback to a successful application of the corresponding derating. Evaluating the stress-strength relationship, a high 90°C margin, *i.e.* design strength, between the tested temperature of 115°C and the operational temperature of 25°C was validated.

6.5.3 Visual Inspection after Reception

As presented at the end of subchapter 6.4, the End-of-Line test assured that only fully functional boards leave the manufacturer. Yet, the possibility exists to induce defects during the shipment. To mitigate this risk, an additional visual inspection step after board reception at CERN was added, see Figure 6.14. Using a digital microscope, the complete first batch of 141 VFC-HDs was inspected showing anomalies for more than half of the batch, such as cleanliness and tolerance issues, or surface and component damages, see [189]. Moreover 10 boards had to be sorted out for repair or further investigations.

As a result, manufacturing process steps as well as the packaging were reviewed and improved in collaboration with the manufacturer. This increased the quality and led to a reduction of necessary inspections for the following batches.

In conclusion, this additional inspection step turned out to be necessary in order to check the production and transport with the correct implementation of the agreed conditions. Another important objective was the exclusion of potentially induced failure causes for the following tests, thus assuring their integrity.

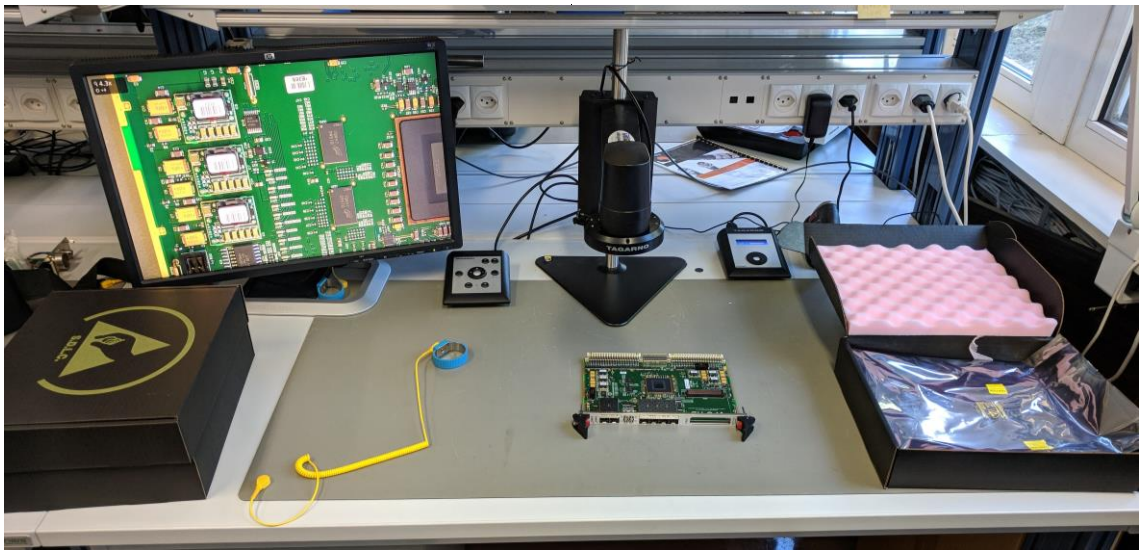


Figure 6.14: Visual income inspection of the VFC-HD. The boards arrive inside ESD and shock protected cardboard boxes (left and right). At an ESD workstation, the inspection is performed first by the naked eye and in case of suspicious findings using a digital microscope.

6.5.4 Environmental Stress Screening (ESS)

As Figure 6.2 displays, ESS was performed with the full production. Subchapter 3.4.2 outlined that amongst various stresses, temperature cycles and random vibration are regarded as the potentially most effective methods [84, 130]. Expecting no vibration in operation, temperature cycles were chosen as accelerating stress.

Table 6.11: Temperature cycling ESS conditions [179].

Parameter	Symbol	Value	Unit	Comment
Temperature range	R	[5, 50]	°C	Defined within BoM specifications [0, 54]°C
Thermal rate of change	dT	5	°C/min	Maximum specification climatic chamber
Number of cycles	N_{cy}	31	-	Preliminary aligned for t_{Screen} < 1 day
Screening Strength	$\boldsymbol{SS_{TC}}$	**98.65**	**%**	See Eq. (6.2)
Relative Humidity	RH	[10, 90]	%	Set to minimum, but varied, see Figure 6.16
Dwell time	t_{Dwell}	12	min	Defined for dT < 1°C/min, see Figure 6.16
Total screening time	t_{Screen}	21.7	h	$t_{Screen} = N_{cy}(R/dT + t_{Dwell})$

The cycling conditions were defined based on components' datasheet specifications given the high confidence of not inducing defects because of the wide temperature margin previously tested. To evaluate the screening efficiency, the number of cycles was first set to 31 to be able to perform five screenings per workweek but kept adaptable to potentially increase the stress if the registered β shape parameter does not sufficiently approach towards a constant failure rate. To approximately set conditions before first tests were performed the Screening Strength (SS) as the "probability that a specific screen will precipitate a latent defect to failure", with

$$SS_{TC} = 1 - e^{\left[-0.0017*(R+0.6)^{0.6}*(\ln(e+dT))^{3}*N_{cy}\right]} \quad (6.2)$$

was used as a point of reference [194]. The determined parameters are summarised in Table 6.11, for which Eq. (6.2) gives a SS_{TC} of 98.65%.

The last column of the table presents the given constraints to define the conditions. Setting screening conditions on the system level can be a difficult task with a variety of restrictions given by the high number and diversity of components. In comparison to screening guidelines [130, 194], the defined temperature range R and thermal rate of change dT were defined on the lower recommended limits, for which the number of cycles N_{cy} was increased in order to compensate. Figure 6.15 displays a temperature cycling sequence during test setup.

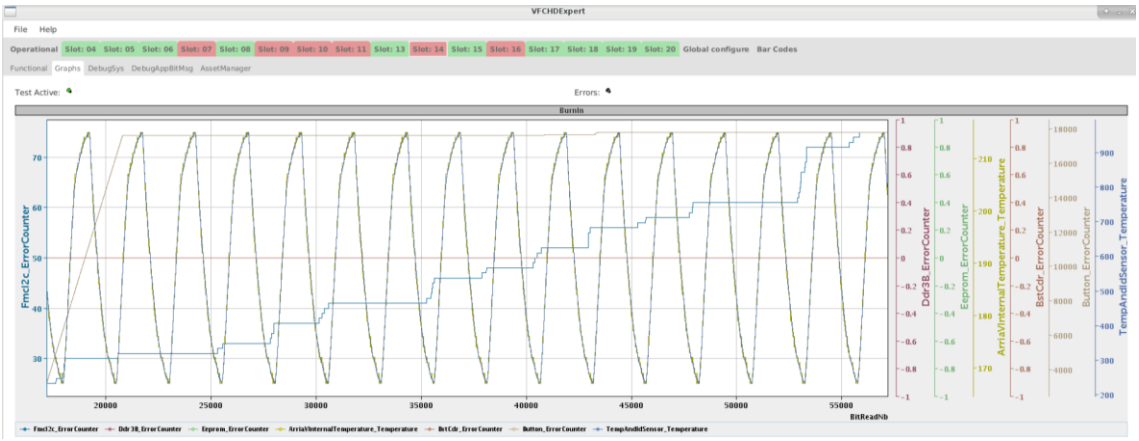


Figure 6.15: Screenshot of the user application GUI during temperature cycles [190]. The screenshot was captured during debugging of the test bench. The top row tabs allow to select and configure the specific test mode including 16 tabs selectable for the DUTs, colour-coded to highlight potential errors. Each DUT tab comprises a functional subtab, illustrating statuses of the tested parameters, the selected configurable graphs subtab and three additional for debugging and asset management.

With the baseline set, first screenings started and demonstrated that the conditions had not induced any immediate failures. Moreover, occurring failures of a small number of boards indicated and later on demonstrated, that the conditions were sufficient to trigger certain failure mechanisms. During the following campaign, the conditions were kept.

In total, 1 129 VFC-HD performed the ESS. The 13 missing boards out of the received production volume of 1 142 divide into five used for development purposes without being tested, one for the high temperature stress test, and seven boards which have not yet performed the ESS because they showed the issues listed in rows 20 - 26 of Table 6.12, *e.g.* an FPGA configuration memory (EPCQ) failure inhibiting to program the BIT. Taking these seven boards into account, a total of 23 - or 2%, of the tested boards showed hardware failures.

Table 6.12: VFC-HD failures during ESS [179]. For three failures occurring on the 12.12.2018, the time of failure could not be determined because of a logging problem (*). Rows 18 and 19 summarise SFP slot failures. The last seven rows show failures which were identified prior to starting ESS.

#	Date	Board ID	Batch No.	$t_{Failure}$ [h]	$T_{Failure}$ [°C]	Component/ Circuit	Failure Cause
1	06.11.18	10124	1	1.96	25.69	PB	Contamination
2	06.11.18	10139	1	2.63	19.25	PB	Contamination
3	06.11.18	10098	1	3.45	48.06	I^2C: IC2,IC35,C236	Contamination
4	09.11.18	10089	1	1.25	23.81	I^2C: IC2	Contamination
5	14.11.18	10014	1	7.56	27.13	PB	Contamination
6	15.11.18	10104	1	4.91	55	PB	Contamination
7	17.11.18	10170	2	0	24.25	R158	Missing component (R)
8	12.12.18	10077	1	/*	/*	PB	Contamination
9	12.12.18	10043	1	/*	/*	PB	Contamination
10	12.12.18	10115	1	/*	/*	R155	Unsolved (Contamination)
11	10.01.19	10405	3	1.43	56.25	SFP_ETH	Design weakness, see row 18
12	05.04.19	10601	4	0.49	26.56	DDR3A	Unsolved (Component?)
13	13.04.19	10704	5	0	24.25	EPCQ	Unsolved
14	18.04.19	10832	6	21.61	39.56	PB	Contamination
15	27.08.19	10444	3	9.78	52.81	DDR3A, DDR3B	Unsolved (Component(s)?)
16	08.10.19	10890	6	0	24.25	DDR3A, DDR3B	Unsolved (Component(s)?)
17	10.10.19	10792	6	0	24.25	V_ADC	Component (ADC)
18	**49x** VFC-HD		All	/	/	SFP_ETH	Design weakness
19	**13x** VFC-HD		All	/	/	SFP_APP1,2,3,4,BST	Intermittent caused by cycles
20	/	10165	2	0	/	JTAG or DC/DC	Unsolved
21	/	10357	3	0	/	VME	Unsolved
22	/	10601	4	0	/	DDR3A, DDR3B	Unsolved (Component?)
23	/	10672	5	0	/	OSC1	Unsolved (Component?)
24	/	10704	5	0	/	EPCQ	Unsolved (Component?)
25	/	10725	5	0	/	DDR3A, DDR3B	Unsolved (Component?)
26	/	11141	8	0	/	EPCQ	Component

Furthermore, the screening revealed failures related to the Ethernet SFP (SFP_ETH) slot. The problem was only identified after sufficient data of the first batches was available. The first eleven rows in Table 6.12 present data of mainly the first production batch [179], after which the implemented production process improvements led to a significant reduction of screened failures for the following batches. This data includes one SFP_ETH failure (row 11), however misses many other VFC-HDs with such a failure characteristic filtered out by the End-of-Line test and not being delivered. The later performed failure analysis identified the failure cause as a potential design problem leading to randomly occurring intermittent communication errors, which occurred for 49 boards of the total production, as summarized in row 18 of Table 6.12. Nevertheless, it was decided to accept these boards for installation after passing ESS and Run In tests without any other failures

because the LHC BLM system fortunately does not make use of the SFP_ETH slot. For all five other SFP slots intermittent transmission errors were also registered for 13 boards in total (row 19). However, in complete contrast to the SFP_ETH errors, they are caused by the cycling conditions with all 13 boards passing the following Run In at constant conditions. Nevertheless, showing low tolerances, the boards were sorted out for the use in the LHC BLM system.

Four different failure causes - contamination, design weakness, manufacturing (*e.g.* missing components), and component internal causes were identified for at least 19 different components or circuits involved. The dominating failure cause was contamination by remaining solder flux and other dirt, mainly within the Push Button (PB) circuit. This component is one of the few components which are mounted manually implying the risk of contamination. During the screening, this led to various short circuits probably caused by varying humidity conditions, compare Figure 6.16 left. The issue mainly concerned the first production batch and got resolved by the previously mentioned process changes.

Next to PB and SFP_ETH failures, the other screened boards comprise a wide variety of failures and associated causes without dominating failure modes or causes. The identified failures were considered as random, successfully screened and bearing a low operational risk. No further analyses and actions were performed.

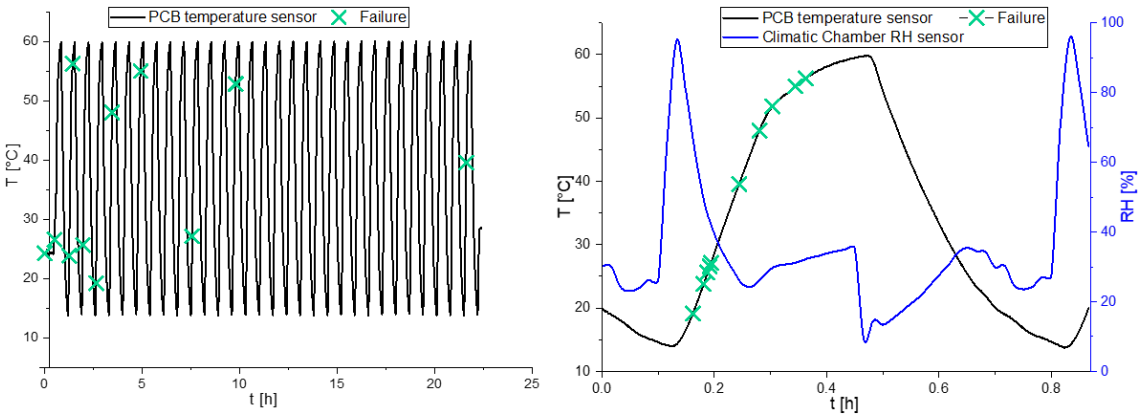


Figure 6.16: ESS failures during temperature cycles (Rows 1 - 7 and 11 - 17 of Table 6.12). On the left during a complete screen comprised of 31 cycles, on the right those failures with $t_{Failure} \neq 0$ summarised within a nominal cycle.

To assess the efficiency of the screening campaign, Figure 6.16 displays on the left graph the occurrence of failures during the 31 temperature cycles performed, as well as on the right graph their time of failure represented on a single nominal temperature cycle. It can be seen that the majority of failures occurred during the first third of the temperature cycles leading to the conclusion of a successful definition of the stress conditions in order to screen the identified failure mechanisms.

The occurrence of failures only at increasing temperature and shortly after the humidity peak can explain the short circuit failures caused by contamination. Remaining solder flux and dirt may contain salts, which step by step absorbed humidity (distilled water), creating a conductive paste which may have caused a short circuit. In this context, the effect of exposing electronics to humidity in order to screen for contamination can be emphasised.

6.5.5 Extended Screening and Reliability Test (Run In)

Adding a Run In at low stress and constant conditions pursued two goals: to firstly ensure the screening success of the previously performed ESS and, secondly, to assess the reliability during operation by means of a lower *MTTF* within the useful life period. All VFC-HD passing ESS performed the subsequent Run In inside eight VME crates during test times, which were first set to around 4 weeks, then taken the fact that no failures occurred reduced to two weeks. A single crate of 16 DUTs was tested for 144 days in order to explore longer time periods.

The VME crates were operated in a separated room at a surrounding air temperature of at least 30°C maintained by the constant power dissipation of the crates. This is above the yearly maximum temperature inside the LHC BLM system racks, compare Figure 4.4. Because eight crates were tested in parallel, no SFP, FMC and LEMO loopbacks were available for use, compare Figure 6.9. Hence, the Run In was not able to discover such periphery failures. Table 6.13 summarises the accumulated test time.

Table 6.13: Run In testing times. Some DUTs were tested more than once, being used to top up not fully equipped crates in order to adjust to the delivery schedule.

Crate No.	Tested days [d]	No. of DUTs [-]	No. of failures [-]	Accumulated test time [h]
1	144	16	0	55 280
2 - 76	≥ 14	75 * 16	0	627 764
76	**1 774**	**1 216**	**0**	**683 044**

All the previously screened VFC-HD passed the Run In with no single failure occurring, accumulating a total test time of 683 044 h. Together with the ESS results, the following subchapter analyses the data to determine the demonstrated reliability.

6.5.6 ESS and Run In Results Summary

To summarise the results of the ESS and the Run In, Figure 6.17 displays the evolution of the demonstrated failure rate for an upper confidence bound of 95% according to Table 3.3, hence a higher degree of confidence than the 90% of the dependability model.

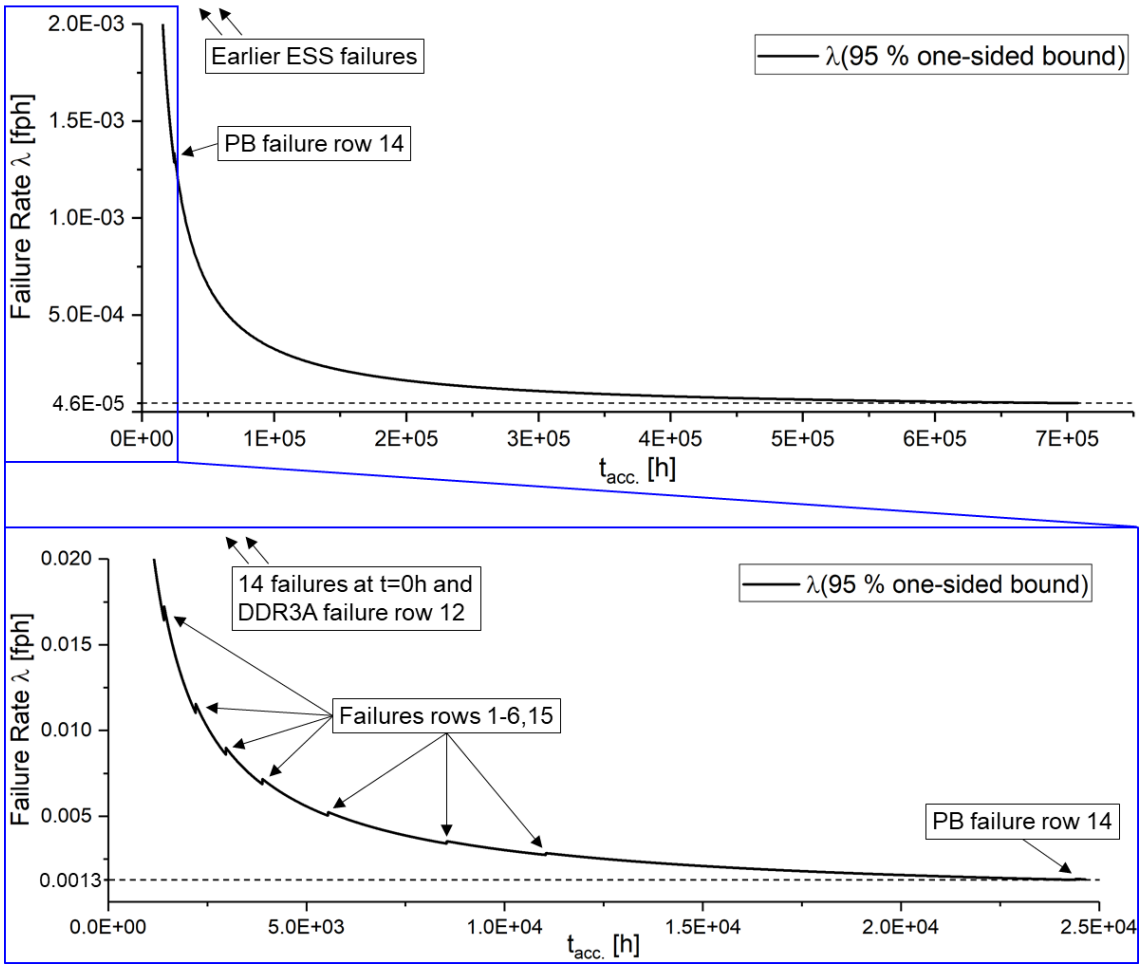


Figure 6.17: Failure rate progression during ESS and Run In, represented for all crates accumulating time in parallel. The top graph combines the accumulated test time during ESS and Run In, not displaying 23 earlier ESS failures on the limited y-axis. The bottom graph only displays the ESS, without 14 failures, accounted for at $t = 0$ and one at $t = 0.49$ *h*. The SFP slot failures of Table 6.12 (rows 11, 18, 19) either an intermittent failure or caused by the design fault, are not taken into account.

The continuously decreasing failure rate, approximating towards a low, constant rate ($\beta \lesssim 1$) can be observed. The lower graph displays the failures occurring during ESS, similar to Figure 6.16 left, for 1 129 DUTs each accumulating 21.7 h of test time, or together 24 500 h. The demonstrated upper failure rate at this point equals 0.0013 fph, corresponding to a lower *MTTF* of 750 h at the specified confidence. The initially high and continuously decreasing failure rate ($\beta > 1$) shows the typical characteristic of the early life period of the bathtub curve. Additionally, taking into account the subsequent Run In, the lower *MTTF* equals a preliminary calculated value of 21 700 h.

Both these preliminary calculated *MTTF* values comprise the failures occurring in the first two sections of the bathtub curve, including failures of the first production batch with associated failure causes corrected by production process changes. Ful-

filling its goal to extend and assure the screening success, the Run In showed no failure during more than half a million device hours, operating some >5°C above the later operational temperature. In order to determine a more precise *MTTF* during the useful life period, the successfully screened failures during ESS are censored resulting in a value of more than 235 000 h, fulfilling the set requirement. This value takes into account the accumulated time during ESS on the assumption that all induced failures were successfully screened.

Having achieved the *MTTF* requirement, the theoretical temperature acceleration factor of $AF_T > 1.5$ according to Table 3.5 ($E_A = 0.7$ eV) would yield an *MTTF* > 350 000 h, but is only considered as an additional confidence margin. This is especially important because the *MTTF* does not include potential failures of the commercial SFP+ transceivers. A risk remains for these components, but being a redundant part of the VFC-HD module the operational effect is low. Furthermore, this is accepted provided the outlined characteristic of being hot-swappable. Additional considerations are outlined in the following subchapter.

6.6 Installation and Operation Considerations

Already at the reception at CERN and during the testing phase, a tracking system was established to trace all VFC-HDs during their life cycle [190]. Making use of the device individual bar and Quick Response (QR) codes placed on the board as well as on the front panel, two distinct yet linked data management systems are used.

CERN's Asset and Maintenance Management platform "Infor EAM" [195] enabled to register the board at reception and track it during following tests and operation through a web service. The linked CERN Manufacturing and Test Folder (MTF) system [196] allowed to define the different life cycle phases as statuses and to enter the results of the different tests. This includes potential test iterations and the possibility to comment and describe the iterations and potential repairs. Amongst a variety of other properties, the SFP slots attenuation performance, the PCB lot code and production batch number is comprised. In addition, a responsible "owner" is assigned to each module.

During operation it is planned to continue using these platforms to track eventual maintenance tasks, repairs and while doing so make use of the information contained. The front panel QR codes allow to use a cell phone application to further facilitate maintenance tasks. In particular the comprised testing data shall facilitate and enhance failure analyses which include the continued assessment of the evolving failure rate and the Weibull shape parameter. Next to these tools, the JIRA application is continued to be used for the VFC-HD boards installed in BLM systems.

To organise the future maintenance, sufficient VFC-HD spare modules were produced, compare Table 6.1. These spares are centrally stored in a closed environment and were vacuumed in two steps inside ESD protective bags. This involved the extraction of the inside air before adding a nitrogen atmosphere, which then got again extracted to assure that no oxygen is present. In addition, the bags were filled with a humidity absorbing silica gel bag and a humidity indicator for fast detection of irregular storage. The bags were then packed inside the shock absorbing cardboard boxes from shipment, compare Figure 6.14.

In order to further improve the maintenance in the future, the additional SFP+ transceiver diagnostic features, as well as other potential offered by the increased FPGA resources, should be considered.

7 Conclusion and Outlook

The protection function and dependability of the LHC BLM system has been reviewed concluding that the system is capable of fulfilling its role as a part of the LHC MPS. The review comprised the update of a dependability model prepared during the initial system design. Since then available performance data of the operating system enabled to review the predicted dependability results and provided input for the updated model. Creating a comprehensive bottom-up system structure, in particular for custom designed electronics, the current extent of the system has been modelled reviewing the individual component dimensioning, *i.e.* their stress-strength ratio based on applied and rated stresses. Using this structure, a subsequent FMECA determined the failure modes of functional system blocks by applying a worst-case approach.

It has been verified that the most severe catastrophic failure effect to miss the detection of potential dangerous loss containing the energy to seriously damage the LHC is prevented by the system design architecture. Furthermore, the maintenance strategy of the LHC BLM system has been reviewed based on the model output and the operational failure data. The existing effort to preventively exchange mechanical, but mainly PSU modules, should be intensified. Under the assumption of only corrective maintenance being performed, the updated model assigned more than 50% of the predicted failures to such component categories, while the actual failure data showed a smaller apportionment above 6%, or 27 PSU failures, as well as a high, yet not exactly traceable number of cooling fan failures potentially contributing to PSU failures. This is still a significant number of failures which should be further reduced, especially as the effect of such failures in most cases leads to a false LHC beam dump request and long maintenance periods. To give just one example, an executed replacement of a tunnel PSU transformer created an LHC availability loss of close to 8 h. If one would put the success of the LHC in contrast to its time in operation, this is equivalent to costs of more than 1.6 million CHF as it has been estimated for hourly LHC costs based on overall LHC project expenses.

Other optimisation actions based on the available failure data analysis have been to improve the dependability of the optical fibre link identified to be the bottleneck of the system for its high failure rate. The actions involved the described surface module upgrade as well as currently ongoing developments to upgrade the tunnel module. Furthermore, the data analysis showed the importance of the implemented

exhaustive system diagnostics. For the future operation, it is recommended to further enlarge these existing diagnostics, in particular with the additional features provided by the chosen SFP+ optical transceiver module for the new surface processing board. For both the optical fibre hardware and PSUs characterised by degradation, techniques such as PHM should be considered.

The applied methodology to update the LHC BLM system dependability model served as an input to develop a generic methodology for dependability application during the complete life cycle of electronic systems. The elaborated methodology made use of experiences from all the three sources - the existing and the updated dependability model, as well as the failure statistics providing a feedback tool. Encompassing the entire system life in a cycle, the methodology is moreover designed as a continuous procedure to be applied on a variety of projects within an organisation, hence continuously increasing the dependability capability of the organisation. The objective has been to be universally applicable and adjustable to several electronic system development projects depending on the individual design and dependability specifications. In each phase the methodology defines a variety of steps to be followed consecutively defining iterations between steps and actions or necessary input for following steps, keeping in mind the overall cycle. For each step, practical aspects have been presented and guidance provided to implement the outlined.

To underline the practical aspect, a case study was performed applying the methodology during the planning, design, production, and testing phases of the LHC BLM system surface module upgrade, a board which receives signals of four optical fibre links using commercial transceiver modules and processes the corresponding data to protect the LHC. A thoroughly planned as well as executed dependability qualification was done. Experience of the predecessor module provided input to establish the design and dependability specifications, *i.e.* to establish the extent of the adjusted methodology.

During the design phase actions were already taken to achieve a more robust design, which was expanded by defining strategies for control and tests during production as well as validation, screening and reliability testing of the produced modules. The results of these prior considerations led to a robust production process which was only fully established after implementing feedback given from introduced incoming inspections at CERN for the first production batch.

The following testing phase performed validation tests which were partly already executed during earlier phases in order to increase the efficiency of the entire process by providing immediate feedback. The environmental validation for potential temperature and humidity effects showed a low temperature robustness of the VFC-HD module, more precisely for its communication via the plugged SFP+ trans-

ceiver modules. Nevertheless, it was possible to profit from the comprehensive performance data available from other installations and environmental data taken inside the surface rack, as well as from the integration into the already redundant optical link of the LHC BLM system. The assessed risk was evaluated as sufficiently low enabling to proceed the development with the chosen transceiver models. However, this led to implementing actions to monitor the future performance and a plan to quickly react if requirements are not met.

The validated and series produced modules entirely underwent a screening for early life failures to prevent such failures occurring after installation. Applying temperature cycles within ESS in a rather small temperature window compared to standards' guidelines with an additional humidity peak during each cycle, enabled to successfully screen around 2% defective modules. Furthermore, the screening identified a design weakness of a single SFP transceiver slot affecting less than 5% of the total production. Not yet entirely being investigated, established signal attenuation measurements during an End-of-Line test at the manufacturer enabled to screen devices affected for the use in the LHC BLM system.

Following the ESS, an additional Run In at nominal operation conditions was performed with all devices. As initially planned, the Run In assured the success of the ESS with no further failure occurring during a total of 680 000 device hours accumulated. This led to fulfilling the previously set dependability requirement of demonstrating a lower failure rate than the currently operating module. The determined *MTTF* during the useful life period is at least 235 000 h at a high confidence of 95%, furthermore disregarding potential temperature acceleration. For the upcoming commissioning and operation phase, provisions for the dependable operation have been made using the existing infrastructure.

8 Bibliography

[1] L. Rossi, "Superconductivity: its role, its success and its setbacks in the Large Hadron Collider of CERN," *Superconductivity Science and Technology,* vol. 23, no. 3, p. 17, 2010.

[2] G. Guaglio, Reliability of the Beam Loss Monitors System for the Large Hadron Collider at CERN, CERN-THESIS-2006-012, Geneva, CH: CERN/Université Clermont Ferrand II - Blaise Pascal, 2005, p. 246.

[3] C. Zamantzas, "Information on the external LHC BLM audit," CERN Web Services, 12 03 2003. [Online]. Available: https://ab-div-bdi-bl-blm.web.cern.ch/Audit_External/audit_external.htm. [Accessed 04 05 2020].

[4] "CERN Accelerating science," CERN, 2020. [Online]. Available: https://home.cern/about. [Accessed 04 05 2020].

[5] M. Brice, L. Egli, "CERN Document Server," 04 07 2012. [Online]. Available: https://cds.cern.ch/record/1459503. [Accessed 04 05 2020].

[6] The Royal Swedish Academy of Sciences, "Press release: The Nobel Prize in Physics 1984," Stockholm, SE, 17/10/1984.

[7] The Royal Swedish Academy of Sciences, "Press release: The Nobel Prize in Physics 2013," Stockholm, SE, 08/10/2013.

[8] T. Berners-Lee, "Information Management: A Proposal," CERN, Geneva, CH, 1989.

[9] P. Waloschek, The Infancy of Particle Accelerators - Life and Work of Rolf Wideröe, Braunschweig/Wiesbaden, DE: Vieweg & DESY, 2002.

[10] H. Wiedemann, Particle Accelerator Physics, Stanford, CA, US: Springer, 2015.

[11] E. Mobs, "CERN Document Server," 28 08 2018. [Online]. Available: https://cds.cern.ch/record/2636343. [Accessed 04 05 2020].

[12] R. Scrivens et al., "Overview of the Status and Developments on Primary Ion Sources at CERN," in *2nd International Particle Accelerator Conference (IPAC 2011)*, San Sebastian, ES, 2011.

[13] E. Shaposhnikova et al., "LHC Injectors Upgrade (LIU) Project at CERN," in *7th International Particle Accelerator Conference*, Busan, KR, 2016.

[14] Communications and Outreach Group, "LHC faq the guide," CERN, Geneva, CH, 2017.

[15] S. Gilardoni et al., "Fifty years of the CERN Proton Synchrotron," CERN Yellow Reports, Geneva, CH, 2013.

[16] M. Benedikt et al., "Design Optimization of PS2," in *23rd Particle Accelerator Conference (PAC09)*, Vancouver, CA, 2009.

[17] J.-L. Caron, "CERN Document Server," 1997. [Online]. Available: https://cds.cern.ch/record/841573. [Accessed 04 05 2020].

[18] O. Brüning et al., "LHC Design Report Volume I - The LHC Main Ring," CERN, Geneva, CH, 2004.

[19] AC Team, "CERN Document Server," 11 09 1998. [Online]. Available: https://cds.cern.ch/record/39731. [Accessed 04 05 2020].

[20] A. Einstein, "Ist die Trägheit eines Körpers von seinem Energieinhalt abhängig?," *Annalen der Physik,* vol. 323, no. 13, pp. 639-641, 1905.

[21] "HL-LHC Project Website," CERN, 2020. [Online]. Available: http://hilumilhc.web.cern.ch/. [Accessed 04 05 2020].

[22] "ATLAS Experiment," CERN, 2020. [Online]. Available: https://atlas.cern. [Accessed 04 05 2020].

[23] "ALICE Collaboration," CERN, 2020. [Online]. Available: http://alice-collaboration.web.cern.ch/. [Accessed 04 05 2020].

[24] "CMS," CERN, 2020. [Online]. Available: https://cms.cern/. [Accessed 04 05 2020].

[25] "LHCb - Large Hadron Collider beauty experiment," CERN, 2020. [Online]. Available: http://lhcb-public.web.cern.ch. [Accessed 04 05 2020].

[26] J. Pequenao, "CERN Document Server," 27 03 2008. [Online]. Available: https://cds.cern.ch/record/1095924. [Accessed 04 05 2020].

[27] CMS Collaboration, "CERN Document Server," 21 03 2012. [Online]. Available: https://cds.cern.ch/record/1433717. [Accessed 04 05 2020].

[28] M. Benedikt et al., "Optimizing integrated luminosity of future hadron colliders," *Physical Review Special Topics - Accelerators and Beams,* vol. 18, no. 10, p. 18, 2015.

[29] "Accelerator Fault Tracking," CERN, v3.29.0. [Online]. Available: https://aft.cern.ch. [Accessed 04 05 2020].

[30] I. Béjar Alonso et al., "High-Luminosity Large Hadron Collider (HL-LHC) - Technical Design Report V. 0.1," CERN, Geneva, CH, 2017.

[31] "LHC Season 2 - facts & figures," CERN, Geneva, CH, 2014.

[32] CERN Management, "The High-Luminosity LHC Project," in *181st Session of Council*, CERN, Geneva, CH, 2016.

[33] M. Florio et al., "Forecasting the socio-economic impact of the Large Hadron Collider: A cost-benefit analysis to 2025 and beyond," *Technological Forecasting and Social Change,* vol. 112, no. 38, pp. 38-53, 2016.

[34] "LHC Machine Outreach," CERN, [Online]. Available: https://lhc-machine-outreach.web.cern.ch. [Accessed 04 05 2020].

[35] B. Todd et al., "LHC and Injector Availability: Run 2," in *9th LHC Operations Evian Workshop*, Evian, FR, 2019.

[36] R. Schmidt et al., "Protection of the CERN Large Hadron Collider," *New Journal of Physics,* vol. 8, no. 290, p. 31, 2006.

[37] R. Assmann et al., "First operational experience with the LHC machine protection system when operating with beam energies beyond the 100MJ range," in *3rd International Particle Accelerator Conference (IPAC 2012)*, New Orleans, LA, US, 2012.

[38] International Electrotechnical Commission (IEC), "IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems," Geneva, CH, 2010.

[39] R. Harrison et al., "Powering Interlock Systems at CERN with Industrial Controllers," in *10th International Conference on Accelerator and Large Experimental Physics Control Systems (ICALEPCS)*, Geneva, CH, 2005.

[40] B. Todd, A Beam Interlock System for CERN High Energy Accelerators, Geneva, CH: CERN, 2006.

[41] O. Brüning et al., "LHC Design Report Volume 1: Beam Dumping System," CERN, Geneva, CH, 2004.

[42] R. Denz, "Electronic Systems for the Protection of Superconducting Elements in the LHC," in *19th International Conference on Magnet Technology*, Genova, IT, 2005.

[43] R. Denz et al., "Upgrade of the Protection System for Superconducting Circuits in the LHC," in *23rd Particle Accelerator Conference (PAC)*, Vancouver, CA, 2009.

[44] R. Assmann et al., "The Final Collimation System for the LHC," in *10th European Particle Accelerator Conference (EPAC)*, Edinburgh, UK, 2006.

[45] R. Filippini, Dependability Analysis of a Safety Critical System: The LHC Beam Dumping System at CERN, Pisa, IT: University of Pisa, 2006.

[46] P. Forck, "Beam Diagnostics and Instrumentation," in *Joint Universities Accelerator School*, Archamps, FR, 2017.

[47] M. Stockner et al., "Classification of the LHC BLM Ionization Chamber," in *8th European Workshop on Beam Diagnostics and Instrumentation for Particle Accelerators (DIPAC)*, Venice, IT, 2007.

[48] B. Dehning et al., "The LHC Beam Loss Measurement System," in *22nd Particle Accelerator Conference (PAC)*, Albuquerque, NM, US, 2007.

[49] M. Stockner et al., "Measurements and Simulations of Ionization Chamber Signals in Mixed Radiation Fields for the LHC BLM System," in *IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC)*, San Diego, CA, US, 2006.

[50] D. Kramer et al., "Very High Radiation Detector for the LHC BLM System Based on Secondary Electron Emission," in *IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC)*, Honolulu, HI, US, 2007.

[51] M. Kalliokoski et al., "Performance Study of Little Ionization Chambers at the Large Hadron Collider," in *IEEE Nuclear Science Symposium, Medical Imaging Conference and Room-Temperature Semiconductor Detector Workshop (NSS/MIC/RTSD)*, Strasbourg, FR, 2016.

[52] C. Xu et al., "Diamond Monitor Based Beam Loss Measurements in the LHC," in *International Beam Instrumentation Conference (IBIC)*, Barcelona, ES, 2016.

[53] E. Effinger et al., "The LHC Beam Loss Monitoring System's Data Acquisition Card," in *12th Workshop on Electronics For LHC and Future Experiments*, Valencia, ES, 2006.

[54] P. Moreira et al., "A Radiation Tolerant Gigabit Serializer for LHC Data Transmission," in *7th Workshop on Electronics for LHC Experiments*, Stockholm, SE, 2001.

[55] E. Effinger, "EDA-00593-V8-0 v.0 (CERN EDMS)," 04 10 2013. [Online]. Available: https://edms.cern.ch/item/EDA-00593-V8-0/0. [Accessed 04 05 2020].

[56] C. Zamantzas, The Real-Time Data Analysis and Decision System for Particle Flux Detection in the LHC Accelerator at CERN, CERN-THESIS-2006-037, Geneva, CH: CERN/Brunel University West London, 2006.

[57] C. Sigaud, "EDA-353869 v.1 (CERN EDMS)," 09 10 2002. [Online]. Available: https://edms.cern.ch/document/353869/1. [Accessed 04 05 2020].

[58] "ab-div-bdi-bl-blm: GOL Opto-Hybrid Manufacturing Specifications: Version 3.30," 21 03 2006. [Online]. Available: https://ab-div-bdi-bl-blm.web.cern.ch/Electronics/GOH/. [Accessed 04 05 2020].

[59] C. Zamantzas et al., "The LHC Beam Loss Monitoring System's Surface Building Installation," in *12th Workshop on Electronics for LHC and Future Experiments (LECC)*, Valencia, ES, 2006.

[60] VMEbus International Trade Association, "American National Standard for VME64 Extensions," VMEbus INTERNATIONAL TRADE ASSOCIATION (VITA), Scottsdale, AZ, US, 1997.

[61] "Technical Specification of LHC instrumentation VME crates Back plane, power supplies and transition modules (CERN EDMS)," 31 07 2009. [Online]. Available: https://edms.cern.ch/document/1013521/1. [Accessed 04 05 2020].

[62] W-IE-NE-R Plein & Baus GmbH, "Series 6000 LHC VME64x-Crate - User Manual," Burscheid-Hilgen, DE, 2006.

[63] TRIUMF, Vancouver, CA, "EDA-572033 v.4 (CERN EDMS)," 04 05 2006. [Online]. Available: https://edms.cern.ch/document/572033/4. [Accessed 04 05 2020].

[64] C. Zamantzas et al., "An FPGA Based Implementation for Real-Time Processing of the LHC Beam Loss Monitoring System's Data," in *IEEE Nuclear Science Symposium*, San Diego, CA, US, 2006.

[65] TRIUMF, "EDA-00998-V3 (CERN EDMS)," 05 04 2006. [Online]. Available: https://edms.cern.ch/document/572033/3. [Accessed 04 05 2020].

[66] C. Zamantzas, "EDA-00780-V4 (CERN EDMS)," 06 12 2007. [Online]. Available: https://edms.cern.ch/item/EDA-00780/0. [Accessed 04 05 2020].

[67] E. Nebot del Busto et al., "Beam Losses and Thresholds," in *MPP Workshop March 2013*, Annecy, FR, 2013.

[68] J. Emery, "EDA-01660-V3-1 (CERN EDMS)," 18 12 2017. [Online]. Available: https://edms.cern.ch/document/1878606/1. [Accessed 04 05 2019].

[69] E. Murer, "EDA-00111-V5 (CERN EDMS)," 30 11 2004. [Online]. Available: https://edms.cern.ch/item/EDA-00111/0. [Accessed 04 05 2020].

[70] J.-J. Savioz, "The Beam Synchronous Timing Receiver Interface for the Beam Observation System (LHC-BOBR-ES-0001)," CERN, Geneva, CH, 2003.

[71] M. Joos, S. Baron, "Timing, Trigger and Control (TTC) Systems for the LHC," [Online]. Available: http://ttc.web.cern.ch/TTC/intro.html. [Accessed 04 05 2020].

[72] P. Alvarez, B. Puccio, "The CISV GMT Receiver Module LHC Version," CERN, Geneva, CH, 2009.

[73] P. Alvarez, "EDA-00531-V1 (CERN EDMS)," 05 05 2004. [Online]. Available: https://edms.cern.ch/item/AB-000495/0. [Accessed 04 05 2020].

[74] B. Todd et al., "Safe Machine Parameter System: SMP in Operation," CERN, Geneva, CH, 2011.

[75] MEN Holding, "Embedded Single Board Computer with Intel Xeon D - 6U VMEBus for Industrial Applications," 28 06 2017. [Online]. Available: https://www.dpie.com/datasheets/vme/a25-data-sheet.pdf. [Accessed 09 02 2020].

[76] International Electrotechnical Commission (IEC), "IEC 60050-192: International electrotechnical vocabulary - Part 192: Dependability," Geneva, CH, 2015.

[77] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, "DIN EN 50126-1: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process; German version EN 50126-1 :2017," VDE VERLAG GMBH, Berlin, DE, 2018.

[78] B. Bertsche et al., Reliability in Automotive and Mechanical Engineering, Heidelberg, DE: Springer, 2008.

[79] International Electrotechnical Commission (IEC), "IEC 60050-351: International electrotechnical vocabulary - Part 351: Control technology," Geneva, CH, 2013.

[80] International Electrotechnical Commission (IEC), "IEC 60050-903: International Electrotechnical Vocabulary - Part 903: Risk assessment," Geneva, CH, 2013.

[81] W. Q. Meeker, L. A. Escobar, Statistical Methods for Reliability Data, New York, NY, US: John Wiley and Sons, Inc., 1998.

[82] W. B. Nelson, Applied Life Data Analysis, Hoboken, NJ, US: John Wiley & Sons, Inc., 2004.

[83] P. D. T. O'Connor, A. Kleyner, Practical Reliability Engineering - Fifth Edition, West Sussex, UK: John Wiley & Sons, Ltd., 2012.

[84] US Department of Defense (DoD), "MIL-HDBK-338B: Military Handbook - Electronic Reliability Design Handbook," United States of America - DoD, Arlington, VA, US, 1998.

[85] W. Weibull, "A Statistical Distribution Function of Wide Applicability," *ASME Journal of Applied Mechanics,* vol. 18, pp. 293-297, 1951.

[86] "JEDEC Standard - JESD74A: Early Life Failure Rate Calculation Procedure for Semiconductor Components," JEDEC Solid State Technology Association, Arlington, VA, US, 2014.

[87] ATLAS Collaboration, "Observation of a new particle in the search for the Standard Model Higgs boson with the ATLAS detector at the LHC," *Physics Letters B,* vol. 716, no. 1, pp. 1-29, 2012.

[88] CMS Collaboration, "Observation of a new boson at a mass of 125 GeV with the CMS experiment at the LHC," *Physics Letters B,* vol. 716, no. 1, pp. 30-61, 2012.

[89] Radio Corporation of America, Reliability Stress Analysis for Electronic Equipment - TR 1100, Washington DC, US: Department of the Navy - Bureau of Ships, 1956.

[90] W. Denson, "The History of Reliability Prediction," *IEEE Transactions on Reliability,* vol. 47, no. 3, pp. 321-328, 1998.

[91] "MIL-HDBK-217F: Military Handbook - Reliability Prediction of Electronic Equipment," US Department of Defense, Washington DC, USA, 1991.

[92] "MIL-HDBK-217F Notice 2: Military Handbook - Reliability Prediction of Electronic Equipment," US Department of Defense, Washington DC, US, 1995.

[93] A. Goel, R. J. Graves, "Electronic System Reliability: Collating Prediction Models," *IEEE Transactions on Device and Materials Reliability,* vol. 6, no. 2, pp. 258-265, 2006.

[94] "Handbook of 217Plus Reliability Prediction Models 2015," Quanterion Solutions Incorporated, Utica, NY, US, 2014.

[95] "FIDES guide 2009 Edition A - Reliability Methodology for Electronic Systems," FIDES Group, 2010.

[96] US Department of Defense (DoD), "MIL-HDBK-217F: Military Handbook - Reliability Prediction of Electronic Equipment," United States of America DoD, Arlington, VA, US, 1991.

[97] Panel on Reliability Growth Methods for Defense Systems, Reliability Growth: Enhancing Defense System Reliability, Washington DC, US: The National Academies Press, 2015.

[98] R. A. Davis, W. Wahrhaftig, "Reliability Predictions, a Case History," *IRE Transactions on Reliability and Control,* vol. 9, no. 1, pp. 87-90, 1960.

[99] M. J. Cushing et al., "Comparison of Electronics-Reliability Assessment Approaches," *IEEE Transactions on Reliability,* vol. 42, no. 4, pp. 542-546, 1993.

[100] M. Pecht, W.-C. Kang, "A Critique of Mil-Hdbk-217E Reliability Prediction Methods," *IEEE Transactions on Reliability,* vol. 37, no. 5, pp. 453-457, 1988.

[101] N. Sinnadurai, M. Pecht et al., "A Critique of the Reliability-Analysis-Center Failure-Rate-Model for Plastic Encapsulated Microcircuits," *IEEE Transactions on Reliability,* vol. 47, no. 2, pp. 110-113, 1998.

[102] M. Pecht, F. R. Nash, "Predicting the Reliability of Electronic Equipment," *Proceedings of the IEEE,* vol. 82, no. 7, pp. 992-1004, 1994.

[103] M. Pecht, "Why the traditional reliability prediction models do not work - is there an alternative?," *Electronics Cooling,* 01 01 1996.

[104] G. P. Pandian et al., "A critique of reliability prediction techniques for avionics applications," *Chinese Journal of Aeronautics,* vol. 31, no. 1, pp. 10-20, 2018.

[105] V. Loll, "From Reliability-Prediction To a Reliability-Budget," in *Annual Reliability and Maintainability Symposium (RAMS)*, Anaheim, CA, US, 1998.

[106] J. G. McLeish, "Enhancing MIL-HDBK-217 Reliability Predictions with Physics of Failure Methods," in *Annual Reliability and Maintainability Symposium (RAMS)*, San Jose, CA, US, 2010.

[107] C. Jais et al., "Reliability Predictions - Continued Reliance on a Misleading Approach," in *59th Reliability and Maintainability Symposium (RAMS)*, Orlando, FL, US, 2013.

[108] J. Jones, J. Hayes, "A Comparison of Electronic-Reliability Prediction Models," *IEEE Transactions on Reliability,* vol. 48, no. 2, pp. 127-134, 1999.

[109] M. Held, K. Fritz, "Comparison and evaluation of newest failure rate prediction models: FIDES and RIAC 217Plus," *Microelectronics Reliability,* vol. 49, no. 9, pp. 967-971, 2009.

[110] A. P. Wood, J. G. Elerath, "A Comparison of Predicted MTBFs to Field and Test Data," in *Annual Reliability and Maintainability Symposium (RAMS)*, Anaheim, CA, US, 1994.

[111] D. Crowe, A. Feinberg, Design for Reliability, Boca Raton, FL, US: CRC Press, 2001.

[112] M. Pecht et al., "IEEE standards on reliability program and reliability prediction methods for electronic equipment," *Microelectronics Reliability,* vol. 42, no. 9, pp. 1259-1266, 2002.

[113] IEEE Reliability Society, "IEEE Standard Reliability Program for the Development and Production of Electronic Products," IEEE, NY, US, 2012.

[114] IEEE Reliability Society, "IEEE Standard Framework for Reliability Prediction of Hardware," IEEE, NY, US, 2010.

[115] M. Silverman, A. Kleyner, "What Is Design for Reliability and What Is Not?," in *Annual Reliability and Maintainability Symposium (RAMS)*, Reno, NV, US, 2012.

[116] A. Mettas, "Design for Reliability: Overview of the Process and Applicable Techniques," *International Journal of Performability Engineering,* vol. 6, no. 6, pp. 577-586, 2010.

[117] M. Pecht et al., "The Reliability Physics Approach to Failure Prediction Modelling," *Quality and Reliability Engineering International,* vol. 6, pp. 267-273, 1990.

[118] J. Gu, M. Pecht, "Prognostics and Health Management Using Physics-of-Failure," in *Annual Reliability and Maintainability Symposium (RAMS)*, Las Vegas, NV, US, 2008.

[119] M. Pecht, J. Gu, "Physics-of-failure-based prognostics for electronic products," *Transactions of the Institute of Measurement and Control,* vol. 31, no. 3, pp. 309-322, 2009.

[120] N.-H. Kim, D. An, J.-H. Choi, Prognostics and Health Management of Engineering Systems - An Introduction, Cham, CH: Springer International Publishing, 2017.

[121] M. G. Pecht, M. Kang, Prognostics and Health Management of Electronics, Hoboken, NJ, US: John Wiley & Sons, 2018.

[122] M. Pecht, A. Dasgupta, "Physics-of-failure: An approach to reliable product development," in *Integrated Reliability Workshop*, Lake Tahoe, CA, US, 1995.

[123] J. W. McPherson, Reliability Physics and Engineering - Time-To-Failure Modeling - Third Edition, Plano, TX, US: Springer Nature Switzerland AG, 2019.

[124] "JEDEC Standard - JEP148A: Reliability Qualification of Semiconductor Devices Based on Physics of Failure Risk and Opportunity Assessment," JEDEC Solid State Technology Association, Arlington, VA, US, 2008.

[125] I. Snook, J. M. Marshall, R. M. Newman, "Physics of Failure As an Integrated Part of Design for Reliability," in *Annual Reliability and Maintainability Symposium (RAMS)*, Tampa, FL, US, 2003.

[126] M. White, J. B. Bernstein, "Microelectronics Reliability: Physics-of-Failure Based Modeling and Lifetime Evaluation," National Aeronautics and Space Administration NASA, Pasadena, CA, US, 2008.

[127] US Department of Defense (DoD), "MIL-STD-1629A: Procedures for Performing a Failure Mode, Effects and Criticality Analysis," United States of America - DoD, Washington DC, US, 1980.

[128] "FMD-2016: Failure Mode Mechanism Distributions," Quanterion Solutions Incorporated, Utica, NY, US, 2016.

[129] Reliability Analysis Center, "FMD-91: Failure Mode/Mechanism Distributions," United States Department of Commerce, Rome, NY, US, 1991.

[130] A. Birolini, Reliability Engineering - Theory and Practice, Berlin, DE: Springer, 2017.

[131] "JEDEC Standard - JEP122F: Failure Mechanisms and Models for Semiconductor Devices," JEDEC Solid State Technology Association, Arlington, VA, US, 2010.

[132] "JEDEC Standard - JESD22-A108F: Temperature, Bias, and Operating Life," JEDEC Solid State Technology Association, Arlington, VA, US, 2017.

[133] "JEDEC Standard - JESD47I: Stress-Test-Driven Qualification of Integrated Circuits," JEDEC Solid State Technology Association, Arlington, VA, US, 2012.

[134] International Electrotechnical Commission (IEC), "IEC 61163-1 Ed 2.0: Reliability stress screening - Part 1: Repairable assemblies manufactured in lots," Geneva, CH, 2006.

[135] US Department of Defense (DoD), "MIL-HDBK-344A: Military Handbook - Environmental Stress Screening (ESS) of Electronic Equipment," United States of America - DoD, Washington DC, US, 1993.

[136] US Department of Defense (DoD), "MIL-HDBK-338B Notice 2," United States of America - DoD, Arlington, VA, US, 2012.

[137] IEEE Reliability Standards Committee, *IEEE Std 1624-2008: IEEE Standard for Organizational Reliability Capability,* New York, NY, US: Institute of Electrical and Electronics Engineers, Inc., 2009.

[138] International Electrotechnical Commission (IEC), "IEC 60300, Ed.2: Dependability management," Geneva, CH, 2003.

[139] "ISO 26262: Road vehicles - Functional safety (First edition)," International Organization for Standardization, Geneva, CH, 2011.

[140] International Electrotechnical Commission (IEC), "IEC 61513: Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems (First edition)," Geneva, CH, 2001.

[141] C. Laplante, "Improving Reliability Throughout the Product Life Cycle," in *Annual Reliability and Maintainability Symposium (RAMS)*, Reno, NV, US, 2018.

[142] M. H. Shepler, N. Welliver, "New Army and DoD Reliability Scorecard," in *Annual Reliability and Maintainability Symposium (RAMS)*, San Jose, CA, US, 2010.

[143] B. Bertsche et al., Zuverlässigkeit mechatronischer Systeme - Grundlagen und Bewertung in frühen Entwicklungsphasen, Berlin/Heidelberg, DE: Springer, 2009.

[144] "VDI 2206: Design methodology for mechatronic systems," Verein Deutscher Ingenieure (VDI), Düsseldorf, DE, 2004.

[145] G. Yang, Life Cycle Reliability Engineering, Hoboken, NJ, US: John Wiley & Sons, Inc., 2007.

[146] K. C. Kapur, M. Pecht, Reliability Engineering, Hoboken, NJ, US: John Wiley & Sons, Inc., 2014.

[147] D. N. Prabhakar Murthy, M. Rausand, T. Østerås, Product Reliability - Specification and Performance, London, UK: Springer-Verlag London Limited, 2008.

[148] "FMD-97: Failure Mode/Mechanism Distributions," Reliability Analysis Center (RAC), Rome, NY, US, 1997.

[149] J. Emery et al., "First experiences with the LHC BLM sanity checks," in *Topical Workshop on Electronics for Particle Physics*, Aachen, DE, 2010.

[150] B. Dehning et al., "Self Testing Functionality of the LHC BLM System," in *10th European Workshop on Beam Diagnostics and Instrumentation for Particle Accelerators (DIPAC)*, Hamburg, DE, 2011.

[151] C. Zamantzas et al., "Real-Time System Supervision for the LHC Beam Loss Monitoring System at CERN," in *14th International Conference on Accelerator & Large Experimental Physics Control Systems (ICALEPCS)*, San Francisco, CA, US, 2013.

[152] C. Zamantzas et al., "Configuration and Validation of the LHC Beam Loss Monitoring System," in *9th European Workshop on Beam Diagnostics and Instrumentation for Particle Accelerators (DIPAC)*, Basel, CH, 2009.

[153] J. Emery et al., "LHC BLM Single Channel Connectivity Test using the Standard Installation," in *9th European Workshop on Beam Diagnostics and Instrumentation for Particle Accelerators (DIPAC)*, Basel, CH, 2009.

[154] Atlassian, "Atlassian - Jira software," 2019. [Online]. Available: https://www.atlassian.com/software/jira. [Accessed 04 05 2020].

[155] C. Roderick et al., "Accelerator Fault Tracking at CERN," in *16th International Conference on Accelerator and Large Experimental Physics Control Systems (ICALEPCS)*, Barcelona, ES, 2017.

[156] V. Schramm et al., "System's Performances in BI," in *8th LHC Operations Evian Workshop*, Evian, FR, 2017.

[157] International Electrotechnical Commission (IEC), "IEC 62347 Ed. 1.0: Guidance on system dependability specifications," Geneva, CH, 2006.

[158] International Electrotechnical Commission (IEC), "IEC 61160 Ed. 2.0: Design Review," Geneva, CH, 2005.

[159] B. Todd et al., "2002392 v. 12: Reliable Electronics Design - Worksheet & Checklist (CERN EDMS)," 18 06 2019. [Online]. Available: https://edms.cern.ch/document/2002392/12. [Accessed 04 05 2020].

[160] "Zuverlässigkeitssicherung bei Automobilherstellern und Lieferanten - Zuverlässigkeits-Methoden und -Hilfsmittel," Verband der Automobilindustrie e.V. (VDA), Berlin, DE, 2016.

[161] "IPC-A-600J: Acceptability of Printed Boards," IPC Association Connecting Electronics Industries, Bannockburn, IL, US, 2016.

[162] "IPC-A-610G: Acceptability of Electronic Assemblies," IPC Association Connecting Electronics Industries, Bannockburn, IL, US, 2017.

[163] DIN Deutsches Institut für Normung e. V., "ISO 9001:2015: Quality management systems - Requirements," Beuth Verlag GmbH, Berlin, DE, 2015.

[164] US Department of Defense (DoD), "MIL-PRF-38535K: Performance Specification - Integrated Circuits (Microcircuits) Manufacturing, General Specification for," United States of America - DoD, West Conshohocken, PA, US, 2013.

[165] "AEC - Q100 - Rev-H: Failure Mechanism based Stress Test Qualification for Integrated Circuits," Automotive Electronics Council - Component Technical Committee, US, 2014.

[166] US Department of Defense (DoD), "MIL-STD-810H: Department of Defense Test Method Standard - Environmental Engineering Considerations and Laboratory Tests," United States of America - DoD, 2019.

[167] European Space Components Coordination (ESCC), "Total Dose Steady-State Irradiation Test Method (ESCC 22900, Issue 5)," European Space Agency (ESA), 2016.

[168] US Department of Defense (DoD), "MIL-STD-883K 2/CHANGE 3: Test Method Standard Microcircuits," United States of America - DoD, Columbus, OH, US, 2018.

[169] European Space Components Coordination (ESCC), "Single Event Effects Test Method and Guidelines (ESCC 25100, Issue 2)," European Space Agency (ESA), 2014.

[170] International Electrotechnical Commission (IEC), "IEC 60050-191 Ed 2.0: International Electrotechnical Vocabulary - Part 191: Dependability," Geneva, CH, 2007.

[171] J. Krenek et al., "Application of Artificial Neural Networks in Condition Based Predictive Maintenance," in *Studies in Computational Intelligence*, Cham, CH, Springer International Publishing, 2016, pp. 75-86.

[172] R. B. Abernethy, The New Weibull Handbook - Reliability & Statistical Analysis for Predicting Life, Safety, Survivability, Risk, Cost and Warranty Claims (Fifth Edition), North Palm Beach, FL, US: Robert B. Abernethy, 2004.

[173] International Electrotechnical Commission (IEC), "IEC 61649 Ed. 2.0: Weibull analysis - Goodness-of-fit tests and confidence intervals for Weibull distributed data," UK, 2007.

[174] F. Martina, "New Radiation tolerant Acquisition System for the Beam Loss Monitoring at HL-LHC (CERN)," PGR First Annual Report at University of Liverpool (PhD Progress Report), Geneva, CH, 2019.

[175] A. Boccardi, "Ongoing electronic development in the CERN Beam Instrumentation Group: challenges and solutions for the measurement of particle accelerator beam parameters," *Journal of Instrumentation,* vol. 8, no. 03, p. 11, 2013.

[176] A. Boccardi et al., "A Modular Approach to Acquisition Systems for Future CERN Beam Instrumentation Developments," in *15th International Conference on Accelerator and Large Experimental Control Systems (ICALEPCS)*, Melbourne, AU, 2015.

[177] A. Boccardi, "EDA-03133-V3-1 v.0 (CERN EDMS)," 18 10 2017. [Online]. Available: https://edms.cern.ch/item/EDA-03133-V3-1/0. [Accessed 04 05 2020].

[178] "Arria V Device Overview (Model 5AGXMB1G4F40C4N)," Altera now part of Intel, San Jose, CA, US, 2018.

[179] V. Schramm et al., "Screening and Run-In of complex electronics for the new LHC BLM processing module," in *29. VDI-Fachtagung Technische Zuverlässigkeit*, Nürtingen, DE, 2019.

[180] V. Schramm et al., "Dependability Study of the LHC BLM Optical Link and Comparison to the Next Generation under Development," in *6th Accelerator Reliability Workshop (ARW)*, Poster presentation, Versailles, FR, 2017.

[181] V. Schramm et al., "Combined Testing and Validation Strategy for the new LHC BLM Processing Module," in *65th Annual Reliability and Maintainability Symposium (RAMS)*, Orlando, FL, US, 2019.

[182] A. Ghiasi, I. Dal Allan et al., "SFF-8431 Rev 4.1 + Addendum: Specification for SFP+ High Speed Electrical Interface," SFF Committee, San Jose, CA, US, 2013.

[183] A. Boccardi, "VME FMC Carrier VFC," Open Hardware Repository, 11 08 2011. [Online]. Available: https://www.ohwr.org/project/fmc-vme-carrier. [Accessed 04 05 2020].

[184] A. Boccardi, E. van der Bij, "VME FMC Carrier (VFC-HD)," Open Hardware Repository, 15 11 2019. [Online]. Available: https://ohwr.org/project/vfc-hd/wikis/home. [Accessed 04 05 2020].

[185] A. Boccardi, "VME FMC+ Carrier (VFC-HS)," Open Hardware Repository, 08 04 2019. [Online]. Available: https://ohwr.org/project/vfc-hs/wikis/home. [Accessed 04 05 2020].

[186] W. Viganò, "EDA-02878-V3-1 v.0 (CERN EDMS)," 09 02 2017. [Online]. Available: https://edms.cern.ch/item/EDA-02878-V3-1/0. [Accessed 04 05 2020].

[187] W. Viganò, A. Boccardi, C. Zamantzas, "High Reliability DC/DC converter module for electronic boards equipped with FPGAs," *Journal of Instrumentation (JINST),* vol. 10, no. 1, 2015.

[188] W. Viganò, V. Schramm, "CERN Indico - BI Seminars," 14 06 2019. [Online]. Available: https://indico.cern.ch/event/822827/. [Accessed 04 05 2020].

[189] S. Eitelbuß, Screening and Reliability Testing of Beam Loss Monitor Electronics at CERN, CERN-THESIS-2019-050, Geneva, CH: CERN/University of Stuttgart, 2019.

[190] M. Gonzalez-Berges et al., "Test-Bench Design for New Beam Instrumentation Electronics at CERN," in *17th Biennial International Conference on Accelerator and Large Experimental Physics Control Systems (ICALEPCS)*, New York, NY, US, 2019.

[191] "Product Datasheet: SFP 3.072Gb/s CPRI&OBSAI Transceiver (FT3A05D)," FTTx Technology, Nanshan, SZ, CN, 2011.

[192] V. Schramm et al., "Validation and Reliability Tests for the new VFC-HD (Presentation)," 11 01 2019. [Online]. Available: https://indico.cern.ch/event/769070/.

[193] J. Jose et al., "Study of Temperature Dependency on MOSFET Parameter using MATLAB," *International Research Journal of Engineering and Technology (IRJET),* vol. 3, no. 7, pp. 1530-1533, 2016.

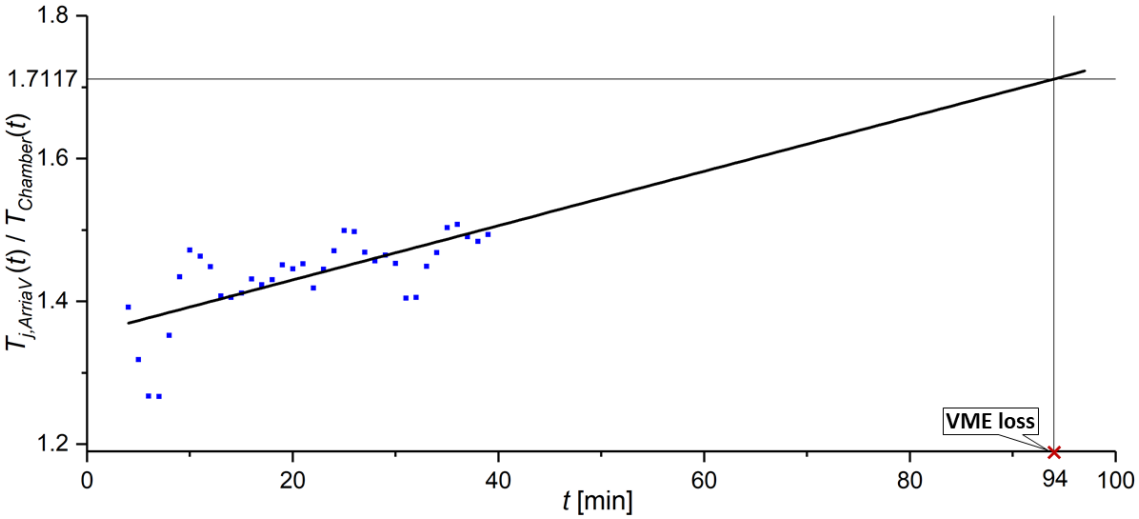
[194] W. H. Horner, "Technical Report: Report 2477 - Environmental Stress Screening (ESS) Guide," United States Army, Fort Belvoir, VA, US, 1989.

[195] "Infor EAM - CERN Asset & Maintenance Management platform," CERN Collaboration Workspaces, 2020. [Online]. Available: https://espace.cern.ch/cmms-service/default.aspx. [Accessed 04 05 2020].

[196] C. Delamare, "Manufacturing and Test Folder: MTF," in *8th European Particle Accelerator Conference (EPAC)*, Paris, FR, 2002.

9 Appendix

Linear extrapolation of the Arria V FPGA sensor temperature during the high temperature stress test (27.11.2018):



$T_{j,ArriaV}(94min) = 1{,}7117 * T(94min) = 1.7117 * 115.59°C = 197.86°C$

Biography

Personal Data

Name	Volker Schramm
Date/Place of Birth	01.04.1990 in Schwäbisch Gmünd

Professional Experience

06/20 – present	Senior Fellowship CERN, Geneva, CH
09/19 – 02/20	Academic staff Institute of Machine Components, University of Stuttgart
09/16 – 08/19	Doctoral student CERN, Geneva, CH
09/15 – 12/15	Master studies intern ZF TRW Automotive Holdings, Alfdorf, GER
10/14 – 07/15 & 01/16 – 04/16	Technical student CERN, Geneva, CH

Education

09/16 – 07/20	Doctorate University of Stuttgart
10/13 – 05/16	Master studies Vehicle and Engine Engineering University of Stuttgart
10/10 – 10/13	Bachelor studies Mechanical Engineering University of Stuttgart
09/00 – 07/09	Limes Gymnasium Welzheim

Liste der bisher erschienenen Berichte aus dem IMA:

Nr.	Verfasser	Titel
1	H.K. Müller	Beitrag zur Berechnung und Konstruktion von Hochdruckdichtungen an schnellaufenden Wellen
2	W. Passera	Konzentrisch laufende Gewinde-Wellen-Dichtung im laminaren Bereich
	K. Karow	Konzentrische Doppelgewindewellendichtung im laminaren Bereich
3	F.E. Breit	Die Kreiszylinderschalendichtung: Eine Axialspaltdichtung mit druckabhängiger Spaltweite
	W. Sommer	Dichtungen an Mehrphasensystemen: Berührungsfreie Wellendichtungen mit hochviskosen Sperrflüssigkeiten
4	K. Heitel	Beitrag zur Berechnung und Konstruktion konzentrisch und exzentrisch betriebener Gewindewellendichtungen im laminaren Bereich
5	K.-H. Hirschmann	Beitrag zur Berechnung der Geometrie von Evolventenverzahnungen
6	H. Däuble	Durchfluß und Druckverlauf im radial durchströmten Dichtspalt bei pulsierendem Druck
7	J. Rybak	Einheitliche Berechnung von Schneidrädern für Außen- und Innenverzahnungen. Beitrag zu Eingriffsstörungen beim Hohlrad-Verzahnen mittels Schneidräder
8	D. Franz	Rechnergestütztes Entwerfen von Varianten auf der Grundlage gesammelter Erfahrungswerte
9	E. Lauster	Untersuchungen und Berechnungen zum Wärmehaushalt mechanischer Schaltgetriebe
10		Festschrift zum 70. Geburtstag von Prof. Dr.-Ing. K. Talke
11	G. Ott	Untersuchungen zum dynamischen Leckage- und Reibverhalten von Radialwellendichtringen
12	E. Fuchs	Untersuchung des elastohydrodynamischen Verhaltens von berührungsfreien Hochdruckdichtungen
13	G. Sedlak	Rechnerunterstütztes Aufnehmen und Auswerten spannungsoptischer Bilder
14	W. Wolf	Programmsystem zur Analyse und Optimierung von Fahrzeuggetrieben
15	H. v. Eiff	Einfluß der Verzahnungsgeometrie auf die Zahnfußbeanspruchung innen- und außenverzahnter Geradstirnräder
16	N. Messner	Untersuchung von Hydraulikstangendichtungen aus Polytetrafluoräthylen
17	V. Schade	Entwicklung eines Verfahrens zur Einflanken-Wälzprüfung und einer rechnergestützten Auswertemethode für Stirnräder
18	A. Gührer	Beitrag zur Optimierung von Antriebssträngen bei Fahrzeugen
19	R. Nill	Das Schwingungsverhalten loser Bauteile in Fahrzeuggetrieben
20	M. Kammüller	Zum Abdichtverhalten von Radial-Wellendichtringen
21	H. Truong	Strukturorientiertes Modellieren, Optimieren und Identifizieren von Mehrkörpersystemen
22	H. Liu	Rechnergestützte Bilderfassung, -verarbeitung und -auswertung in der Spannungsoptik
23	W. Haas	Berührungsfreie Wellendichtungen für flüssigkeitsbespritzte Dichtstellen
24	M. Plank	Das Betriebsverhalten von Wälzlagern im Drehzahlbereich bis 100.000/min bei Kleinstmengenschmierung
25	A. Wolf	Untersuchungen zum Abdichtverhalten von druckbelastbaren Elastomer- und PTFE-Wellendichtungen
26	P. Waidner	Vorgänge im Dichtspalt wasserabdichtender Gleitringdichtungen
27	Hirschmann u.a.	Veröffentlichungen aus Anlaß des 75. Geburtstags von Prof. Dr.-Ing. Kurt Talke
28	B. Bertsche	Zur Berechnung der Systemzuverlässigkeit von Maschinenbau-Produkten
29	G. Lechner; K.-H.Hirschmann; B. Bertsche	Forschungsarbeiten zur Zuverlässigkeit im Maschinenbau
30	H.-J. Prokop	Zum Abdicht- und Reibungsverhalten von Hydraulikstangendichtungen aus Polytetrafluoräthylen
31	K. Kleinbach	Qualitätsbeurteilung von Kegelradsätzen durch integrierte Prüfung von Tragbild, Einflankenwälzabweichung und Spielverlauf
32	E. Zürn	Beitrag zur Erhöhung der Meßgenauigkeit und -geschwindigkeit eines Mehrkoordinatentasters
33	F. Jauch	Optimierung des Antriebsstranges von Kraftfahrzeugen durch Fahrsimulation
34	J. Grabscheid	Entwicklung einer Kegelrad-Laufprüfmaschine mit thermografischer Tragbilderfassung
35	A. Hölderlin	Verknüpfung von rechnerunterstützter Konstruktion und Koordinatenmeßtechnik
36	J. Kurfess	Abdichten von Flüssigkeiten mit Magnetflüssigkeitsdichtungen
37	G. Borenius	Zur rechnerischen Schädigungsakkumulation in der Erprobung von Kraftfahrzeugteilen bei stochastischer Belastung mit variabler Mittellast
38	E. Fritz	Abdichtung von Maschinenspindeln
39	E. Fritz; W. Haas; H.K. Müller	Berührungsfreie Spindelabdichtungen im Werkzeugmaschinenbau. Konstruktionskatalog

Nr.	Verfasser	Titel
40	B. Jenisch	Abdichten mit Radial-Wellendichtringen aus Elastomer und Polytetrafluorethylen
41	G. Weidner	Klappern und Rasseln von Fahrzeuggetrieben
42	A. Herzog	Erweiterung des Datenmodells eines 2D CAD-Systems zur Programmierung von Mehrkoordinatenmeßgeräten
43	T. Roser	Wissensbasiertes Konstruieren am Beispiel von Getrieben
44	P. Wäschle	Entlastete Wellendichtringe
45	Z. Wu	Vergleich und Entwicklung von Methoden zur Zuverlässigkeitsanalyse von Systemen
46	W. Richter	Nichtwiederholbarer Schlag von Wälzlagereinheiten für Festplattenlaufwerke
47	R. Durst	Rechnerunterstützte Nutprofilentwicklung und clusteranalytische Methoden zur Optimierung von Gewindewerkzeugen
48	G.S. Müller	Das Abdichtverhalten von Gleitringdichtungen aus Siliziumkarbid
49	W.-E. Krieg	Untersuchungen an Gehäuseabdichtungen von hochbelasteten Getrieben
50	J. Grill	Zur Krümmungstheorie von Hüllflächen und ihrer Anwendung bei Werkzeugen und Verzahnungen
51	M. Jäckle	Entlüftung von Getrieben
52	M. Köchling	Beitrag zur Auslegung von geradverzahnten Stirnrädern mit beliebiger Flankenform
53	M. Hildebrandt	Schadensfrüherkennung an Wälzkontakten mit Körperschall-Referenzsignalen
54	H. Kaiser	Konstruieren im Verbund von Expertensystem, CAD-System, Datenbank und Wiederholteilsuchsystem
55	N. Stanger	Berührungsfrei abdichten bei kleinem Bauraum
56	R. Lenk	Zuverlässigkeitsanalyse von komplexen Systemen am Beispiel PKW-Automatikgetriebe
57	H. Naunheimer	Beitrag zur Entwicklung von Stufenlosgetrieben mittels Fahrsimulation
58	G. Neumann	Thermografische Tragbilderfassung an rotierenden Zahnrädern
59	G. Wüstenhagen	Beitrag zur Optimierung des Entlasteten Wellendichtrings
60	P. Brodbeck	Experimentelle und theoretische Untersuchungen zur Bauteilzuverlässigkeit und zur Systemberechnung nach dem Booleschen Modell
61	Ch. Hoffmann	Untersuchungen an PTFE-Wellendichtungen
62	V. Hettich	Identifikation und Modellierung des Materialverhaltens dynamisch beanspruchter Flächendichtungen
63	K. Riedl	Pulsationsoptimierte Außenzahnradpumpen mit ungleichförmig übersetzenden Radpaaren
64	D. Schwuchow	Sonderverzahnungen für Zahnradpumpen mit minimaler Volumenstrompulsation
65	T. Spörl	Modulares Fahrsimulationsprogramm für beliebig aufgebaute Fahrzeugtriebstränge und Anwendung auf Hybridantriebe
66	K. Zhao	Entwicklung eines räumlichen Toleranzmodells zur Optimierung der Produktqualität
67	K. Heusel	Qualitätssteigerung von Planetengetrieben durch Selektive Montage
68	T. Wagner	Entwicklung eines Qualitätsinformationssystems für die Konstruktion
69	H. Zelßmann	Optimierung des Betriebsverhaltens von Getriebeentlüftungen
70	E. Bock	Schwimmende Wellendichtringe
71	S. Ring	Anwendung der Verzahnungstheorie auf die Modellierung und Simulation des Werkzeugschleifens
72	M. Klöpfer	Dynamisch beanspruchte Dichtverbindungen von Getriebegehäusen
73	C.-H. Lang	Losteilgeräusche von Fahrzeuggetrieben
74	W. Haas	Berührungsfreies Abdichten im Maschinenbau unter besonderer Berücksichtigung der Fanglabyrinthe
75	P. Schiberna	Geschwindigkeitsvorgabe für Fahrsimulationen mittels Verkehrssimulation
76	W. Elser	Beitrag zur Optimierung von Wälzgetrieben
77	P. Marx	Durchgängige, bauteilübergreifende Auslegung von Maschinenelementen mit unscharfen Vorgaben
78	J. Kopsch	Unterstützung der Konstruktionstätigkeiten mit einem Aktiven Semantischen Netz
79	J. Rach	Beitrag zur Minimierung von Klapper- und Rasselgeräuschen von Fahrzeuggetrieben
80	U. Häussler	Generalisierte Berechnung räumlicher Verzahnungen und ihre Anwendung auf Wälzfräserherstellung und Wälzfräsen
81	M. Hüsges	Steigerung der Tolerierungsfähigkeit unter fertigungstechnischen Gesichtspunkten
82	X. Nastos	Ein räumliches Toleranzbewertungssystem für die Konstruktion
83	A. Seifried	Eine neue Methode zur Berechnung von Rollenlagern über lagerinterne Kontakt-Beanspruchungen
84	Ch. Dörr	Ermittlung von Getriebelastkollektiven mittels Winkelbeschleunigungen
85	A. Veil	Integration der Berechnung von Systemzuverlässigkeiten in den CAD-Konstruktionsprozeß
86	U. Frenzel	Rückenstrukturierte Hydraulikstangendichtungen aus Polyurethan
87	U. Braun	Optimierung von Außenzahnradpumpen mit pulsationsarmer Sonderverzahnung
88	M. Lambert	Abdichtung von Werkzeugmaschinen-Flachführungen
89	R. Kubalczyk	Gehäusegestaltung von Fahrzeuggetrieben im Abdichtbereich

Nr.	Verfasser	Titel
90	M. Oberle	Spielbeeinflussende Toleranzparameter bei Planetengetrieben
91	S. N. Dogan	Zur Minimierung der Losteilgeräusche von Fahrzeuggetrieben
92	M. Bast	Beitrag zur werkstückorientierten Konstruktion von Zerspanwerkzeugen
93	M. Ebenhoch	Eignung von additiv generierten Prototypen zur frühzeitigen Spannungsanalyse im Produktentwicklungsprozeß
94	A. Fritz	Berechnung und Monte-Carlo Simulation der Zuverlässigkeit und Verfügbarkeit technischer Systeme
95	O. Schrems	Die Fertigung als Versuchsfeld für die qualitätsgerechte Produktoptimierung
96	M. Jäckle	Untersuchungen zur elastischen Verformung von Fahrzeuggetrieben
97	H. Haiser	PTFE-Compounds im dynamischen Dichtkontakt bei druckbelastbaren Radial-Wellendichtungen
98	M. Rettenmaier	Entwicklung eines Modellierungs-Hilfssystems für Rapid Prototyping gerechte Bauteile
99	M. Przybilla	Methodisches Konstruieren von Leichtbauelementen für hochdynamische Werkzeugmaschinen
100	M. Olbrich	Werkstoffmodelle zur Finiten-Elemente-Analyse von PTFE-Wellendichtungen
101	M. Kunz	Ermittlung des Einflusses fahrzeug-, fahrer- und verkehrsspezifischer Parameter auf die Getriebelastkollektive mittels Fahrsimulation
102	H. Ruppert	CAD-integrierte Zuverlässigkeitsanalyse und -optimierung
103	S. Kilian	Entwicklung hochdynamisch beanspruchter Flächendichtverbindungen
104	A. Flaig	Untersuchung von umweltschonenden Antriebskonzepten für Kraftfahrzeuge mittels Simulation
105	B. Luo	Überprüfung und Weiterentwicklung der Zuverlässigkeitsmodelle im Maschinenbau mittels Mono-Bauteil-Systemen
106	L. Schüppenhauer	Erhöhung der Verfügbarkeit von Daten für die Gestaltung und Berechnung der Zuverlässigkeit von Systemen
107	J. Ryborz	Klapper - und Rasselgeräuschverhalten von Pkw- und Nkw- Getrieben
108	M. Würthner	Rotierende Wellen gegen Kühlschmierstoff und Partikel berührungsfrei abdichten
109	C. Gitt	Analyse und Synthese leistungsverzweigter Stufenlosgetriebe
110	A. Krolo	Planung von Zuverlässigkeitstests mit weitreichender Berücksichtigung von Vorkenntnissen
111	G. Schöllhammer	Entwicklung und Untersuchung inverser Wellendichtsysteme
112	K. Fronius	Gehäusegestaltung im Abdichtbereich unter pulsierendem Innendruck
113	A. Weidler	Ermittlung von Raffungsfaktoren für die Getriebeerprobung
114	B. Stiegler	Berührungsfreie Dichtsysteme für Anwendungen im Fahrzeug- und Maschinenbau
115	T. Kunstfeld	Einfluss der Wellenoberfläche auf das Dichtverhalten von Radial-Wellendichtungen
116	M. Janssen	Abstreifer für Werkzeugmaschinenführungen
117	S. Buhl	Wechselbeziehungen im Dichtsystem von Radial-Wellendichtring, Gegenlauffläche und Fluid
118	P. Pozsgai	Realitätsnahe Modellierung und Analyse der operativen Zuverlässigkeitskennwerte technischer Systeme
119	H. Li	Untersuchungen zum realen Bewegungsverhalten von Losteilen in Fahrzeuggetrieben
120	B. Otte	Strukturierung und Bewertung von Eingangsdaten für Zuverlässigkeitsanalysen
121	P. Jäger	Zuverlässigkeitsbewertung mechatronischer Systeme in frühen Entwicklungsphasen
122	T. Hitziger	Übertragbarkeit von Vorkenntnissen bei der Zuverlässigkeitstestplanung
123	M. Delonga	Zuverlässigkeitsmanagementsystem auf Basis von Felddaten
124	M. Maisch	Zuverlässigkeitsorientiertes Erprobungskonzept für Nutzfahrzeuggetriebe unter Berücksichtigung von Betriebsdaten
125	J. Orso	Berührungsfreies Abdichten schnelllaufender Spindeln gegen feine Stäube
126	F. Bauer	PTFE-Manschettendichtungen mit Spiralrille - Analyse, Funktionsweise und Erweiterung der Einsatzgrenzen
127	M. Stockmeier	Entwicklung von Klapper- und rasselgeräuschfreien Fahrzeuggetrieben
128	M. Trost	Gesamtheitliche Anlagenmodellierung und -analyse auf Basis stochastischer Netzverfahren
129	P. Lambeck	Unterstützung der Kreativität von verteilten Konstrukteuren mit einem Aktiven Semantischen Netz
130	K. Pickard	Erweiterte qualitative Zuverlässigkeitsanalyse mit Ausfallprognose von Systemen
131	W. Novak	Geräusch- und Wirkungsgradoptimierung bei Fahrzeuggetrieben durch Festradentkopplung
132	M. Henzler	Radialdichtungen unter hoher Druckbelastung in Drehübertragern von Werkzeugmaschinen
133	B. Rzepka	Konzeption eines aktiven semantischen Zuverlässigkeitsinformationssystems
134	C.G. Pflüger	Abdichtung schnelllaufender Hochdruck-Drehübertrager mittels Rechteckring und hocheffizient strukturierter Gleitfläche
135	G. Baitinger	Multiskalenansatz mit Mikrostrukturanalyse zur Drallbeurteilung von Dichtungsgegenlaufflächen

Nr.	Verfasser	Titel
136	J. Gäng	Berücksichtigung von Wechselwirkungen bei Zuverlässigkeitsanalysen
137	Ch. Maisch	Berücksichtigung der Ölalterung bei der Lebensdauer- und Zuverlässigkeitsprognose von Getrieben
138	D. Kirschmann	Ermittlung erweiterter Zuverlässigkeitsziele in der Produktentwicklung
139	D. Weber	Numerische Verschleißsimulation auf Basis tribologischer Untersuchungen am Beispiel von PTFE-Manschettendichtungen
140	T. Leopold	Ganzheitliche Datenerfassung für verbesserte Zuverlässigkeitsanalysen
141	St. Jung	Beitrag zum Einfluss der Oberflächencharakteristik von Gegenlaufflächen auf das tribologische System Radial-Wellendichtung
142	T. Prill	Beitrag zur Gestaltung von Leichtbau-Getriebegehäusen und deren Abdichtung
143	D. Hofmann	Verknüpfungsmodell zuverlässigkeitsrelevanter Informationen in der Produktentwicklung mechatronischer Systeme
144	M. Wacker	Einfluss von Drehungleichförmigkeiten auf die Zahnradlebensdauer in Fahrzeuggetrieben
145	B. Jakobi	Dichtungsgeräusche am Beispiel von Pkw-Lenkungen – Analyse und Abhilfemaßnahmen
146	S. Kiefer	Bewegungsverhalten von singulären Zahnradstufen mit schaltbaren Koppelungseinrichtungen
147	P. Fietkau	Transiente Kontaktberechnung bei Fahrzeuggetrieben
148	B. Klein	Numerische Analyse von gemischten Ausfallverteilungen in der Zuverlässigkeitstechnik
149	M. Klaiber	Betriebs- und Benetzungseigenschaften im Dichtsystem Radial-Wellendichtung am Beispiel von additivierten synthetischen Schmierölen
150	A. Baumann	Rasselgeräuschminimierung von Fahrzeuggetrieben durch Getriebeöle
151	M. Kopp	Modularisierung und Synthese von Zuverlässigkeitsmethoden
152	M. Narten	Abdichten von fließfettgeschmierten Getrieben mit Radialwellendichtungen – Reibungsminderung durch Makrostsrukturierung der Dichtungsgegenlauffläche
153	P. Schuler	Einfluss von Grenzflächeneffekten auf den Dichtmechanismus der Radial-Wellendichtung
154	A. Romer	Anwendungsspezifischer Zuverlässigkeitsnachweis auf Basis von Lastkollektiven und Vorwissen
155	A. Daubner	Analyse, Modellierung und Simulation von Verschleiß auf mehreren Skalen zur Betriebsdauervorhersage von Wellendichtringen aus PTFE-Compound
156	J. Rowas	Ökologischer Einsatz der Traktionsarten im System Bahn
157	D. J. Maier	Sensorlose online Zustandserfassung von Vorschubantriebskomponenten in Werkzeugmaschinen
158	J.-P. Reibert	Statisches Abdichten auf nicht idealen Dichtflächen in der Antriebstechnik
159	M. Sommer	Einfluss des Schmierfetts auf das tribologische System Radial-Wellendichtung – Betriebsverhalten und Funktionsmodell
160	W. Haas	Basics der Dichtungstechnik
161	U. Nißler	Dichtheit von Hydraulikstangendichtringen aus Polyurethan
162	S. M. Neuberger	Entwicklung einer gasgeschmierten Gleitringdichtung für den Einsatz im Verbrennungsmotor
163	W. Goujavin	Strömungsmechanische Untersuchungen zur Funktionsweise von Manschettendichtungen aus PTFE-Compounds mit Rückförderstrukturen
164	K. Mutter	Simulation der Zuverlässigkeit von Gesamtfahrzeugfunktionen am Beispiel Fahrkomfort
165	S. Sanzenbacher	Reduzierung von Getriebegeräuschen durch Körperschallminderungsmaßnahmen
166	O. Koller	Zuverlässigkeit von Leistungsmodulen im elektrischen Antriebsstrang
167	M. Remppis	Untersuchungen zum Förderverhalten von Dichtsystemen mit Radial-Wellendichtringen aus Elastomer
168	M. Baumann	Abdichtung drallbehafteter Dichtungsgegenlaufflächen – Messung, Analyse, Bewertung und Grenzen
169	M. Schenk	Adaptives Prüfstandsverhalten in der PKW-Antriebstrangerprobung
170	J. Gölz	Manschettendichtringe aus PTFE-Compounds, Funktionsmechanismus von PTFE-Manschettendichtungen und Entwicklung von Rückförderstrukturen für beidseitig drehende Wellen
171	J. Kümmel	Schmutzabdichtung mittels Fettgefüllter Berührungsfreier Wellendichtungen
172	S. Bader	Gehäusedichtungen unter korrosiver Last
173	J. Juskowiak	Beanspruchungsgerechte Bestimmung des Weibull-Formparameters für Zuverlässigkeitsprognosen
174	F. Jakob	Nutzung von Vorkenntnissen und Raffungsmodellen für die Zuverlässigkeitsbestimmung
175	N. P. Tonius	Klauenschaltelemente in Stufenautomatgetrieben
176	V. Schweizer	Berücksichtigung und Bewertung streuender Einflussgrößen in der Zuverlässigkeitssimulation
177	F. Bosch	Abdichtung trockener Stäube mit fettgefüllten berührungsfreien Wellendichtungen
178	M. Botzler	Präventive Diagnose abnutzungsabhängiger Komponentenausfälle
179	C. Fehrenbacher	Förderverhalten im Dichtsystem Radial-Wellendichtung

Nr.	Verfasser	Titel
180	B. Heumesser	Optimierung des Klapper- und Rasselgeräuschverhaltens bei Doppelkupplungsgetrieben
181	A. Eipper	Einfluss transienter Betriebsbedingungen auf den RWDR im System Radial-Wellendichtung
182	Alexander Buck	Einfluss der Oberflächenrauheit auf den Verschleiß an Hydraulikstangendichtungen
183	Andrea Buck	Simulation und Optimierung der Instandhaltung unter Berücksichtigung sich ändernder Belastungen mittels Petrinetzen
184	St. Kemmler	Integrale Methodik zur Entwicklung von robusten, zuverlässigen Produkten
185	T. Rieker	Modellierung der Zuverlässigkeit technischer Systeme mit stochastischen Netzverfahren
186	M. Bartholdt	Kunden- und kostenorientierte Zuverlässigkeitszielermittlung
187	V.Warth	Systematische Synthese und Bewertung von Stufenlosgetrieben
188	N. Nowizki	Funktionale Sicherheit und Zuverlässigkeit in frühen Phasen der Produktentwicklung
189	F. Schiefer	Additive Fertigung von Radial-Wellendichtringen
190	M. Dazer	Zuverlässigkeitstestplanung mit Berücksichtigung von Vorwissen aus stochastischen Lebensdauerberechnungen
191	J. Totz	Funktionsuntersuchungen an Dichtsystemen mit weichgeschliffenen Dichtungsgegenlaufflächen und Radial-Wellendichtringen aus NBR
192	M. Stoll	Entwicklung und Funktionsanalyse rückenstrukturierter Manschettendichtringe aus PTFE-Compound
193	N. Dakov	Elastohydrodynamische Simulation von Wellendichtungen am Beispiel der PTFE-Manschettendichtung mit Rückförderstrukturen
194	Z. Beslic	Modellierung der Schadensdegradation Zahnradgrübchen bei Fahrzeuggetrieben
195	St. Jetter	Zuverlässigkeitsprognose mechanischer Komponenten auf Basis simulierter Betriebsfestigkeit
196	O. R. Orozco	Availability of Particle Accelerators: requirements, prediction methods and optimization