

A
Machine Protection
Risk Management Method
for Complex Systems

Riccard Andersson

October 2, 2017

© **Riccard Andersson, 2017**

*Series of dissertations submitted to the
Faculty of Mathematics and Natural Sciences, University of Oslo
No. 1903*

ISSN 1501-7710

All rights reserved. No part of this publication may be
reproduced or transmitted, in any form or by any means, without permission.

Cover: Hanne Baadsgaard Utigard.
Print production: Reprintsentralen, University of Oslo.

Abstract

Particle accelerators play a key role in modern research, and their ability to enable the study of objects on the smallest of scales has been fundamental for the development of today's society. Modern accelerators not only push the limits of beam energies and intensities, but also aim at competing with industrial facilities and nuclear research reactors in metrics such as reliability and availability. This combination requires state-of-the-art equipment, strategic thinking, and robust risk management methods to deal with all challenges. The work behind this thesis has been focused on the latter of the three - to develop a technical risk management method that is integrated into the design and early commissioning phases of an accelerator facility to enhance its operational availability. The implementation of the method is ongoing at the European Spallation Source (ESS), currently under construction in Lund, Sweden.

The method is executed through the usage of customized protection functions, which can be argued to be a non-negotiable feature for complex machines. As opposed to the field of safety, the field of protection, concerned with equipment rather than people and the environment, does not have any standardized risk management methods to apply. However, safety (and more so functional safety) has plenty of such standards that are, at least partially, found suitable for protection as well. In addition to the functional safety standards IEC 61508 and 61511, the ISO standards 31000 and 16085, targeting risk management in a generic way, are also useful in the development of a functional protection method. This thesis combines the four into a unique and applicable risk management method for complex systems in general, and particle accelerators in particular.

The structure of this thesis initially highlights the four main components for the application of the method: a study of the usage and best practices of particle accelerators within modern research; a motivation for and technical challenges with developing the method; a review of current safety and standards, available risk management methods, and their usability within complex systems; and the structure and process of the method itself. These components are briefly discussed in Chapters 1-4, respectively. Chapter 5 shows how the method is applied to some of the most critical systems within ESS. Finally, Chapter 6 briefly discusses and concludes the outcome of the thesis.

Acknowledgements

To start, I want to sincerely thank my academic supervisor, Erik Adli, for taking on the role as supervisor, obtaining the NFR project grant, and above all showing great interest in the topic of machine protection and giving valuable comments on all aspects of my work. Erik has done continuous hard work in the background and has not shown any discouragement despite me doing most of the work in a neighboring country.

Annika Nordt has carried the heavy load of acting as both on-site supervisor and group leader of the protection and safety systems group (PSG). She has managed to give plenty of (in)valuable inputs when necessary and built a very supporting and enjoyable group spirit. This sure has been important in the development of this thesis. Annika has been forced to put up with many of my (often unorthodox) ideas on my work, her work, other's work, and the philosophy of work in general.

Enric Bargalló, my third supervisor, has done at least as much work as I have in putting the functional protection method together. His sometimes surprising enthusiasm is a main driver for the reliability, availability, and protection work at ESS and without his contribution, this thesis would have been of no use. Enric has stood strong through hours, days, weeks, months, and years of workshops, meetings, discussions, agreements, disagreements, and visions, despite being approximately four months younger than I am.

Christian Hilbes at ZHAW has already reached rock star status at ESS for his groundbreaking ideas, brilliant expertise, ease of understanding, and tireless work drive. His passion for functional safety and documentation is shocking, in a good way. Christian has been an invaluable support to ESS, machine protection, and this thesis.

Martin Rejzek, also at ZHAW, has contributed immensely to much of the work that has been put together, directly or indirectly, in this thesis. His understanding of most/all complex things and useful clarifications make the most complex of tasks seem like a stroll in Winterthur Stadtgarten.

Aurélien Ponton is a bearing pillar in the discussions about how to implement vague theoretical ideas into actual implementations and agreements for the ESS accelerator. He is pulling the heavy load in the communication with a vast variety of scientists and engineers, which is a job that most people would not even come close to managing.

I am grateful for all of the friends and colleagues in the PSG at ESS for the support, laughs, jokes, and fruitful discussions. The many colleagues in the ICS, Accelerator, and Target divisions at ESS have been generally supportive and cooperative when I have bothered and bombarded them with questions - some of them relevant, most of them not.

Finally, I want to thank all of my close friends and family for the support and conversations that have kept me connected to the outside world where necessary - beyond safety standards,

flowcharts, and in-kind contributions. Not to forget anyone, whoever feels they have contributed to this can consider themselves mentioned in this acknowledgement.

Contents

Abstract	iii
Acknowledgements	v
Contents	vii
Preface	xi
Acronyms and Abbreviations	xiii
List of Figures	xvi
List of Tables	xx
1 Particle Accelerators in Research	1
1.1 User Facilities	2
1.2 Linacs and Synchrotrons	2
1.3 Neutron Spallation Sources	2
1.4 Existing Particle Accelerators	3
1.4.1 Large Hadron Collider (LHC)	3
1.4.2 Spallation Neutron Source (SNS)	5
1.4.3 Japan Proton Accelerator Research Complex (J-PARC)	6
1.4.4 ISIS	8
1.5 Future Particle Accelerators	9
1.5.1 European Spallation Source (ESS)	9
1.5.2 International Fusion Material Irradiation Facility (IFMIF)	11
1.5.3 International Linear Collider (ILC)	11
1.5.4 Compact Linear Collider (CLIC)	13
1.6 Beam Physics and Propagation Along a Linac	14
1.6.1 Beam Bunching	14
1.6.2 Beam Acceleration	15
1.6.3 Beam Steering	16
1.6.4 Beam Focusing	16
1.6.5 Beam Monitoring	18
1.6.6 Beam Energy and Damage Potential	20
1.6.7 Beam Power and Damage Potential	22

1.7	Preventing Damage and Downtime of Particle Accelerators	22
1.7.1	Machine Protection "Systems"	23
1.7.2	Reliability, Availability, and RAMI	24
1.7.3	Risk Management	25
2	Motivation of This Thesis - Technical Challenges and Boundaries	27
3	Systematic Approaches to Safety, Protection, and Risk Management	29
3.1	Functional Safety Standards	29
3.1.1	IEC 61508	30
3.1.2	IEC 61511	31
3.2	Risk Management Standards	32
3.2.1	ISO 31000	32
3.2.2	ISO 16085	33
3.3	Quantitative System Analysis Techniques	34
3.3.1	Reliability Block Diagram (RBD)	35
3.3.2	Fault Tree Analysis (FTA)	35
3.3.3	Event Tree Analysis (ETA)	35
3.3.4	Failure Modes and Effects Analysis (FMEA)	35
3.4	Qualitative System Analysis Techniques	37
3.4.1	Systems Theoretic Process Analysis (STPA)	37
3.4.2	Functional Resonance Analysis Method (FRAM)	38
3.4.3	Hazard and Operability Analysis (HAZOP)	39
3.5	Discussion on Standards and Methods	39
4	The Functional Protection Method and Its Lifecycle	41
4.1	Rationale Behind the Method	41
4.2	Key Concepts and Processes	42
4.2.1	The Lifecycle Process	42
4.2.2	The Risk Management Process	43
4.2.3	Balancing Protection and Reliability	43
4.3	Framework and Scope	43
4.3.1	Organizational Context of the Functional Protection Method	44
4.3.2	Objectives and Requirements	45
4.4	The Functional Protection Lifecycle	45
4.5	The Functional Protection Analysis Technique	45
4.5.1	Hazard and Risk Analysis	47
4.5.2	Overall Protection Requirements	50
4.5.3	Overall Protection Requirements Allocation	51
4.5.4	Protection Function Specification	52
4.5.5	Discussion on the Functional Protection Analysis Technique	54
4.6	The Functional System Interaction Process	57
4.7	The Functional Protection Implementation and Adjustments	59
4.8	Summary of the Functional Protection Method	60

5	Applying the Functional Protection Method - Proof of Concept	63
5.1	Machine Protection at ESS	63
5.1.1	System of Systems	64
5.1.2	The ESS MP-SoS Layout	65
5.1.3	Reliability and Availability Requirements for ESS	65
5.1.4	Fast Beam Interlock System	66
5.1.5	ESS Timing System	67
5.1.6	Beam Stop Actuation Systems	68
5.1.7	Beam Monitoring Systems	68
5.1.8	Post-Mortem System	68
5.1.9	Protection Integrity Levels at ESS	69
5.2	Concept and Scope	70
5.2.1	Normal Conducting Linac Systems	70
5.2.2	Target Station Systems	70
5.3	The Functional Protection Analysis at ESS	70
5.3.1	Hazard and Risk Analysis, Overall Protection Requirements, and Overall Protection Requirements Allocation	71
5.3.2	Protection Function Specification	88
5.3.3	Risk Register and Traceability	89
5.4	The Functional System Interaction Process at ESS	90
5.5	Functional Protection Implementation and Adjustments at ESS	90
5.6	Estimation of the Availability and Cost Impact of Functional Protection at ESS	90
5.6.1	Simulation Assumptions	91
5.6.2	Simulation Setup	91
5.6.3	Simulation Results	91
5.6.4	Discussion	92
6	Discussion and Conclusions	93
6.1	The Functional Protection Method	93
6.2	Differences Between Safety and Protection Systems	93
6.3	Application to ESS	94
6.4	Live Process and Future Work	95
	Bibliography	97
	Appendix A - Core Scientific Papers	107
	Appendix B - Steps of the Functional Protection Analysis Technique	131
	Appendix C - Graphical Functional Protection Analyses	135

Preface

This thesis is submitted for the degree of Philosophiæ Doctor at the Department of Physics, Faculty of Mathematics and Natural Sciences, University of Oslo, Norway. It has been funded by the the Norwegian Research Council (Project 234239/F50)¹ and the European Spallation Source ERIC². The thesis is written around four scientific core papers, listed below and appended at the end of this thesis. When referred to in the thesis text, the papers are indicated by their roman numeral.

- I R. Andersson, E. Bargalló, A. Nordt, E. Adli. **Machine Protection Systems and Their Impact on Beam Availability and Accelerator Reliability**, paper MOPTY044, *Proceedings of IPAC2015*, Richmond, VA, USA, 2015. [1]
- II R. Andersson, E. Bargalló, A. Nordt, **A Functional Protection Method for Availability and Cost Risk Management of Complex Research Facilities**, *Submitted to ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*, 2017. [2]
- III R. Andersson, E. Bargalló, S. Kövecses, A. Nordt, M. Zaera-Sanz, C. Hilbes, M. Rejzek, **Development and Status of Protection Functions for the Normal Conducting Linac at ESS**, paper TUPIK079, *Proceedings of IPAC2017*, Copenhagen, Denmark, 2017. [3]
- IV R. Andersson, E. Bargalló, L. Emås, J. Harborn, A. Lundgren, U. Odén, J. Ringnér, K. Sjögreen, **Machine Protection Risk Management of the ESS Target System**, paper TUPIK078, *Proceedings of IPAC2017*, Copenhagen, Denmark, 2017. [4]

The following papers, documents, and presentations have been developed throughout the PhD contract but are not considered a core part of the thesis.

- 1. R. Andersson, S. Kövecses, E. Bargalló, **Challenges in Technical Risk Management for High-Power Accelerators**, paper P1-03, *Proceedings of ICANS XXII*, Oxford, UK, 2017.
- 2. R. Andersson, C. Hilbes, A. Nordt, **ESS Machine Protection Risk Management Process**, ESS Internal Document (ESS-0095000), 2017.
- 3. H. Carling, R. Andersson, S. Birch, J. Cereijo, T. Friedrich, T. Korhonen, E. Laface, M. Mansouri-Sharifabad, A. Monera-Martinez, A. Nordt, D. Paulic, D. Piso, S. Regnell, M.

¹Norwegian tax money

²European tax money

Zaera-Sanz, **The European Spallation Source Design - Controls Chapter**, IOP Ref: PHYSSCR-105817, *Submitted to Physica Scripta*, 2017.

4. R. Andersson, E. Bargalló, A. Nordt, **Development of an Analysis Framework for the Beam Instrumentation Interface to the Beam Interlock System at ESS**, paper TH-POY039, *Proceedings of IPAC2016*, Busan, South Korea, 2016.
5. R. Andersson, A. Monera Martinez, M. Zaera-Sanz, A. Nordt, **Beam Interlock Systems - Proposed Architecture and Physical Deployment**, ESS Internal Document (ESS-0110715), 2016.
6. R. Andersson, E. Bargalló, A. Monera Martinez, A. Nordt, **A Modified Functional Safety Method for Predicting False Beam Trips and Blind Failures in the Design of the ESS Beam Interlock System**, paper MOPGF126, *Proceedings of ICALEPCS2016*, Melbourne, Australia, 2015.
7. A. Monera Martinez, R. Andersson, A. Nordt, M. Zaera-Sanz, C. Hilbes, **Overview and Design Status of the Fast Beam Interlock System at ESS**, paper MOPGF138, *Proceedings of ICALEPCS2016*, Melbourne, Australia, 2015.
8. A. Nordt, R. Andersson, T. Korhonen, A. Monera Martinez, M. Zaera-Sanz, A. Apollo-
nio, R. Schmidt, C. Hilbes, **Development and Realisation of the ESS Machine Protection Concept**, paper TUC3O03, *Proceedings of ICALEPCS2016*, Melbourne, Australia, 2015.
9. E. Bargalló, K.H. Andersen, R. Andersson, A. De Isusi, A. Nordt, E.J. Pitcher, **ESS Availability and Reliability Approach**, paper MOPTY045, *Proceedings of IPAC2015*, Richmond, VA, USA, 2015.
10. R. Andersson, **The Impact of Machine Protection on Accelerator Reliability and Beam Availability**, *Presentation at ARW2015*, Knoxville, TN, USA, 2015.
11. E. Bargalló et al., **ESS Reliability and Availability Requirements**, ESS Internal Document (ESS-0008886), 2015.
12. R. Andersson, A. Monera Martinez, **Failure Mode, Effect, and Diagnostics Analysis of the ESS Beam Interlock System**, ESS Internal Document (ESS-0110714), 2015.
13. R. Andersson, **Relying on ESS**, *Presentation at ICPS2014*, Heidelberg, Germany, 2014.

Acronyms and Abbreviations

A2T	Accelerator to Target
ACS	Annular Coupled Structure
ALARA	As Low As Reasonably Achievable
BC	Buncher Cavity
BCM	Beam Current Monitor
BIS	Beam Interlock System
BLM	Beam Loss Monitor
BPM	Beam Position Monitor
CCL	Coupled Cavity Linac
CERN	European Organization for Nuclear Research
CLIC	Compact Linear Collider
CMS	Cryogenic Moderator System
CTF3	CLIC Test Facility 3
CW	Continuous Wave
DE	Damage Event
DESY	Deutsches Elektronen-Synchrotron
DoE	Department of Energy (US)
DTL	Drift Tube Linac
DR	Damping Rings
E/E/PE	Electric, Electronic, Programmable Electronic
ENSA	European Neutron Scattering Association
EO	Expected Occurrence
ESS	European Spallation Source
ETA	Event Tree Analysis
FACET	Facility for Advanced Accelerator Experimental Tests
FC	Faraday Cup
FEL	Free Electron Laser
FIM	Functional Integrity Magnitude
FPGA	Field-Programmable Gate Array
FMEA	Failure Mode and Effect Analysis
FRAM	Functional Resonance Analysis Method
FTA	Fault Tree Analysis
GeV	Giga Electron Volt
HAZOP	Hazard and Operability Analysis
HEP	High Energy Physics

HFT	Hardware Fault Tolerance
IC	Ionization Chamber
ICFA	International Committee for Future Accelerators
ID	Interceptive Device
IDT	Implementation and Design Team
IEC	International Electrotechnical Commission
IFMIF	International Fusion Material Irradiation Facility
ILC	International Linear Collider
IPT	Integrated Protection Team
ISO	International Organization for Standardization
J-PARC	Japan Proton Accelerator Research Complex
KEK	High Energy Accelerator Research Organization (Japan)
keV	Kilo Electron Volt
LEBT	Low Energy Beam Transport
LEP	Large Electron-Positron
LH ₂	Liquid Hydrogen
LHC	Large Hadron Collider
Linac	Linear Accelerator
LOPA	Layer Of Protection Analysis
LWU	Linac Warm Unit
MAG	Linac Magnet System
MDT	Mean Downtime
MEBT	Medium Energy Beam Transport
MeV	Mega Electron Volt
MLF	Materials and Life Science Experimental Facility
MP	Machine Protection
MPS	Machine Protection System
MP-SoS	Machine Protection System of Systems
MR	Main Ring
MTBF	Mean Time Between Failures
MTBO	Mean Time Between Occurrences
MTTR	Mean Time To Repair
NC	Normal Conducting
OECD	Organization for Economic Cooperation and Development
OPF	Overall Protection Function
OR	Occurrence Rate
ORNL	Oak Ridge National Laboratory
ORRM	Other Risk Reduction Measure
PAT	Protection Analysis Team
PF	Protection Function
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PIL	Protection Integrity Level
PLC	Programmable Logic Controller

PS	Proton Synchrotron
PWCS	Primary Water Cooling System
RAMI	Reliability, Availability, Maintainability, Inspectability
RBD	Reliability Block Diagram
RCS	Rapid-Cycle Synchrotron
RF	Radio Frequency
RFQ	Radio Frequency Quadrupole
RMS	Root Mean Square
RR	Risk Reduction
SC	Superconducting
SC	Systematic Capability
SC-HWR	Superconducting Half-Wave Resonators
SCL	Superconducting Linac
SDTL	Separated-Type DTL
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLAC	Stanford Linear Accelerator Complex
SNS	Spallation Neutron Source
SoS	System of Systems
SPS	Super Proton Synchrotron
STPA	Systems Theoretic Process Analysis
T2K	Tokai to Kamioka
TEF	Transmutation Experimental Facility
TeV	Tera Electron Volt
TMCP	Target Moderator Cryogenic Plant
ToF	Time of Flight
TOM	Tolerable Occurrence Magnitude
TPCS	Target Primary Cooling System
TW	Target Wheel
VAC	Vacuum System
WS	Wire Scanner
XFEL	X-ray Free Electron Laser

List of Figures

1.1	The CERN accelerator complex with LHC being the largest ring [17].	4
1.2	The Spallation Neutron Source at Oak Ridge National Laboratory, displaying the contributors for the different sections [22].	6
1.3	The Japan Proton Accelerator Research Complex, J-PARC, displaying the linac, RCS, MR, and the experimental facilities [25].	7
1.4	The ISIS neutron source with its two target stations [31].	8
1.5	The European Spallation Source looking from northwest [35].	10
1.6	The ESS linac layout [36].	11
1.7	The IFMIF linac layout [40].	12
1.8	The International Linear Collider [44].	13
1.9	The Compact Linear Collider [50].	14
1.10	The phase-space ellipse with some parameters (left) [61] and a Gaussian distribution of particles in and around the ellipse (right) [62].	18
1.11	Bragg peaks for protons of energies between 30 MeV and 70 MeV [74].	21
3.1	The IEC 61508 lifecycle [86].	31
3.2	The ISO 31000 risk management process [99].	33
3.3	The ISO 16085 risk management process model [101].	34
3.4	Reliability Block Diagram.	35
3.5	Fault Tree Analysis.	36
3.6	Event Tree Analysis.	36
3.7	Example FMEA, including criticality and diagnostics, of a MOSFET transistor for an early ESS beam interlock system version [106].	37
3.8	The STPA process flow from controller, through actuators acting on the controlled process, monitored by sensors and then back to the controller.	38
3.9	Example of four resonating functions, from a FRAM perspective, that lead to a traffic accident [113].	39
4.1	The organizational triangle for carrying out the functional protection lifecycle. The figure is taken from Paper II [2].	44
4.2	The functional protection lifecycle, as found in Paper II [2]. The colored rectangles circling the boxes correspond to the responsibilities of the matching-colored teams in the organizational triangle in Figure 4.1. The processes within the same-colored rectangles are described in Sections 4.5, 4.6, and 4.7. The non-circled boxes are carried out in collaboration between all of the teams.	46

4.3	The functional protection analysis technique is applied inside the purple rectangle. The figure also contains the concept and overall scope definition above and the protection function specification below. Extracted from Figure 4.2.	47
4.4	The functional protection analysis technique for a <i>continuous mode</i> hazard setup, where the hazards have been assigned an expected occurrence of EO0 (normal operation).	56
4.5	The functional protection analysis technique for a <i>discrete mode</i> hazard setup, where the hazards have been assigned an expected occurrence of EO1 (facility lifetime) and EO2 (unexpected).	56
4.6	The functional protection analysis technique for a damage event with subhazards, displaying both continuous and discrete mode hazards.	57
4.7	The functional system interaction process inside the green rectangle, as well as the concept and overall scope definition above and the protection function specification below. Extracted from Figure 4.2.	58
4.8	The functional protection implementation and adjustments within the orange rectangle. Extracted from Figure 4.2.	59
4.9	Summary of the functional protection method.	60
5.1	The functional protection lifecycle with the boundary for this chapter's application in orange.	64
5.2	The ESS MP-SoS layout including the protection-related, proton beam monitoring, beam interlock, beam stop actuation, MP management, control, safety, and timing systems.	65
5.3	The allocation of protection function PFH or PFD for the sensors, logic systems, and actuator systems at ESS.	69
5.4	The target station systems and their locations in the target monolith [136]. . . .	71
5.5	The location and connection of the gate valves along the normal conducting linac.	72
5.6	Example of the graphical derivation of the functional protection analysis technique for the vacuum (gate valve) system. The graphical derivations are all found in Appendix C.	72
5.7	The aperture change from 38 to 30 mm in the MEBT when entering a buncher cavity, where an unfocused or mis-steered beam (coming from the left) could cause damage [138].	78
5.8	The target primary cooling system and its immediate interfaces [139].	80
5.9	The target wheel system setup.	81
5.10	The target wheel, drive and shaft system setup [144].	82
5.11	The cryogenic moderator system and its interfaces [145].	83
5.12	The tuning beam dump path, as selected by the bending dipole magnets in the A2T area [152].	86
5.13	An example view of a damage event in the Insight risk register: the gate valve after DTL tank 1 is hit by beam [153].	89

6.1 The functional ownership is typically shared among several system owners. The figure also displays the difference between a local protection function (managed by the system owner) and a global protection function (managed by facility-wide functional protection). 94

List of Tables

1.1	Comparison of particle type, beam energy, peak beam current, and average beam power for five particle accelerators [11, 12, 13]. *For an experimental length of 10 hours.	3
4.1	The first risk matrix, combining downtime and cost to generate a consequence category. Taken from Paper II [2].	48
4.2	The second risk matrix, displaying tolerable occurrence magnitudes based on the consequence category. Taken from Paper II [2].	48
4.3	The underlying correspondence between tolerable occurrence magnitude (TOM), mean time between occurrences (MTBO), and occurrence rates (OR) for functional protection analysis at ESS.	49
4.4	Expected occurrence rates for hazards, including their description and awarded reduction level.	50
4.5	Examples of how two protection functions fulfill the FIM through addition of PILs and adding the number one.	53
4.6	Available protection integrity levels (PIL) in the functional protection method, and their corresponding requirements. The SFF and HFT numbers appear with a matrix relation (see Table 3 in [96]) and either the top row numbers or the bottom row numbers can be selected for PIL1 and PIL4. PIL2 and PIL3 have three options for SFF and HFT.	54
4.7	Overview of the damage events, hazards, overall protection functions, and protection functions for the example analysis of a closed or closing vacuum gate valve.	55
5.1	ESS requirements for the maximum number of beam stops, and their no-beam duration [123].	66
5.2	Available protection integrity levels (PIL) for the ESS MP-SoS, and their corresponding requirements. For the SFF and HFT, either top row or the bottom row numbers can be selected for PIL1. For PIL2, the same holds but with three options.	69
5.3	Damage events, hazards, overall protection functions, and protection functions for the vacuum system (gate valves) at ESS.	73
5.4	Damage events, hazards, overall protection functions, and protection functions for the linac magnets (focusing quadrupoles and steering dipoles) at ESS. . . .	75

5.5	Damage events, hazards, overall protection functions, other risk reduction measures, and protection functions for the interceptive devices at ESS, including beam stops (Faraday cups), emittance measurement units, beam scrapers, and the iris collimator. Wire scanners are excluded from the functional protection analysis in the normal conducting linac.	77
5.6	Damage events, hazards, overall protection functions, and protection functions for the MEBT buncher cavities at ESS.	79
5.7	Damage events, hazards, overall protection functions, and protection functions for the target primary cooling system at ESS. The target wheel-related analysis and its numbering of damage events etc. continue in Table 5.8.	81
5.8	Damage events, hazards, overall protection functions, and protection functions for the target wheel movement and rotation at ESS. Note that the target wheel analysis is made for both cooling and movement together. This makes the damage events in this table start at number 2 rather than 1, which is located in the previous table. The same holds for hazards, OPFs, and PFs as well.	83
5.9	Damage events, hazards, overall protection functions, and protection functions for the cryogenic moderator system at ESS.	84
5.10	Damage events, hazards, overall protection functions, and protection functions for the water moderator and reflector systems at ESS.	86
5.11	Damage events, hazards, overall protection functions, and protection functions for the tuning beam dump at ESS.	88
5.12	Simulated availability and downtime for the normal conducting linac and target station systems at ESS, with and without the MP protection functions in place [155].	92

Chapter 1

Particle Accelerators in Research

Particle accelerators as seen today have their origin in the late 1920s when John Cockcroft and Ernest Walton, encouraged by Ernest Rutherford, started designing a "generator" that could produce a voltage of up to 800 kV. This generator was used to e.g. split the lithium atom, which rewarded them the Nobel prize in 1951. Another researcher, named Robert van de Graaff, designed a static generator that could reach 1.5 MV and was used in research during the 30s. These two early versions of particle accelerators cleared the path for a new type of research, but were limited by their static voltage. The emerging field of high-energy physics required higher accelerating voltages, and this could only be reached by finding another technology. Luckily, and in parallel with the development of static particle acceleration, so-called drift tubes with alternating fields were first proposed by Gustav Ising in 1924 and demonstrated by Rolf Widerøe in 1928. This oscillator applied 25 kV to two accelerating gaps, reaching a total of 50 keV kinetic energy - thus clearly pointing the direction of future particle accelerators [5].

Nowadays, particle accelerators vary in both their application and design. There are over 30000 particle accelerators in operation around the world, and the applications are spread throughout medical radiation therapy and the production of low-energy beams, high-energy physics applications using colliding beams, the production of synchrotron light through circulating electron beams, and nuclear research accelerators that are used for the study of material samples. While radiation therapy is the quantitatively largest group of accelerators, the high-energy physics applications have received most attention. Also material research and the study of molecular structure are areas that keep expanding their usage of particle accelerators [6].

The first two sections of this chapter (Sections 1.1 and 1.2) bring up the idea of user facilities and how they affect requirements and design, together with making the distinction between linear accelerators and synchrotrons - the two types of particle accelerators in large-scale facilities. In Section 1.3, the process of neutron spallation and the usage related research facilities is briefly introduced. Section 1.4 describes a few of the existing particle accelerators and their usage within research. Following the success of these, even more sophisticated accelerators are discussed around the world and some of these are presented in Section 1.5, including the European Spallation Source, which has been the center of attention for the risk management method described in this thesis. Section 1.6 describes the different functions of an accelerator and how a particle beam is generated to achieve its end goal. Finally, Section 1.7 points out the inherent risks of accelerator-driven facilities and existing means to deal with those. This will then be the focus for the remainder of the thesis (Chapters 3 through 6), culminating in a suggested method

to manage these risks.

1.1 User Facilities

Up until the 1970s, the users of accelerator facilities were mainly the accelerator developers and physicists themselves. This meant that a machine failure only affected a limited and specialized group. As some accelerators later became so-called *user facilities*, where the researchers were other people than the accelerator physicists and engineers themselves, the requirements on operational reliability and availability increased [7].

Nowadays, most accelerator facilities are considered to be user facilities. To target the higher demands that this brings - demands beyond the particle beam parameters - reliability and availability studies of the accelerator need to be accounted for in the design phase. As the case is with modern accelerator facilities, *other people's research* (much of it quite beneficial to mankind) is dependent on close to continuous operation of the facility. Many of these demands can be incorporated in an integrated *machine protection* (MP) strategy, whose primary goal is not to disappoint the thousands of guest researchers that visit a typical user facility each year.

1.2 Linacs and Synchrotrons

There are two distinctly different kinds of accelerators. One is the linear accelerator (linac), where the beam is transported in a straight line and only passes the equipment once. Such accelerators can reach a high intensity particle beam and pulse repetition rate. In addition, they allow for a better upgradeability and due to the possibility of restarting the beam operation quickly after an error, the availability (see Section 1.7.2) can be high. Linacs appear in the beginning of accelerator complexes and are suitable where high availabilities are required. In the high energy physics field, linacs are useful for precision measurements with light, elementary particles such as electrons and positrons. By using linacs for the acceleration of these, where the particles are accelerated in a straight line rather than circulated, energy losses are minimized.

Synchrotrons are instead suitable when size is of importance, as the accelerating equipment is "re-used" each turn. The typical synchrotron also acts as a *storage ring*, where particles are first injected and accumulated, and then have their energy increased to very high levels. The energy that is lost in the circular bending process is called *synchrotron radiation*, and is inversely proportional to m^4 , where m is the particle mass [8]. It is therefore not suitable to use synchrotrons for light particles at high energies unless the synchrotron radiation is exactly what one wants to achieve. In high energy physics, storage rings appear in the search for new discoveries by colliding heavier hadrons, such as protons.

1.3 Neutron Spallation Sources

The process of neutron spallation was first discovered in 1937 by Glenn Seaborg. The process is performed by accelerating protons and colliding them with a neutron-rich target material, such as mercury for SNS (Section 1.4.2) or tungsten for ESS (Section 1.5.1). Upon being hit, the

target nuclei become unstable and consequentially scatter a number of neutrons per incoming proton. The released neutrons are tuned to the desired energies and guided to their respective experiments using so-called moderators and reflectors. As neutrons do not carry any charge, they do not interact with the electron clouds surrounding the atoms. Instead, they only interact through the strong nuclear force with the atomic nuclei, which makes it possible to study bulky materials without ionizing (and damaging) the samples.

Research with neutrons complements the use of x-rays, where x-rays resolve heavy and hard materials such as metals and teeth, and neutrons resolve light and soft materials such as hydrogen, carbon, and oxygen. This allows for research to be carried out within a multitude of disciplines spanning over life science, energy, environmental technology, culture and archeology, plastics, pharmaceuticals, molecular science, fundamental physics, engine technology, and more [9, 10].

1.4 Existing Particle Accelerators

There is a vast number of large particle accelerator facilities that deserve attention from both a technical and a usage point of view. This section describes four of these and briefly go through their design, application, and context for the field. Some of the aspects related to their machine protection can be found in Paper I [1].

The particle accelerators in this section have different purposes and are aimed at various scientific fields. Their particle types and beam energies vary, as well as their beam powers. Some of their inherent parameters are summarized and compared in Table 1.1, where also ESS, discussed in Section 1.5.1, is included in addition to the accelerators in this section.

	LHC	SNS	J-PARC	ISIS	ESS
Particle Type	p	H ⁻	H ⁻	H ⁻	p
Beam Energy	7 TeV	1 GeV	50 GeV	800 MeV	2 GeV
Beam Current	580 mA	33 mA	11.1 A	0.25 mA	62.5 mA
Beam Power	10 kW*	1.4 MW	133 kW	200 kW	5 MW

Table 1.1: Comparison of particle type, beam energy, peak beam current, and average beam power for five particle accelerators [11, 12, 13]. *For an experimental length of 10 hours.

1.4.1 Large Hadron Collider (LHC)

The LHC, located at the European Organization for Nuclear Research (CERN) in Switzerland, is perhaps the most famous particle accelerator and has been in the frontline of high-energy physics for the past seven years. CERN is a global collaboration consisting of 21 member countries and 7 observer countries, and its collaborative governing model is now used at other laboratories as well. LHC is a superconducting proton synchrotron that accelerates two colliding proton beams to a center of mass collision energy of 14 TeV. The LHC is currently the largest machine in the world, and the circumference of its underground tunnel is 27 km. The collisions take place in four different experiments that are spread around the accelerator: ATLAS, CMS, ALICE, and LHCb [14].

The idea behind LHC dates back to the early 1980s and a concept for the accelerator was first proposed in 1984. The development of the Standard Model for particles required higher energies in order to collect data that would verify the existence of previously undetected particles. When it was decided to build LHC, it was placed in the tunnel that used to house the Large Electron-Positron (LEP) collider. The construction of LHC faced many technological challenges that spawned new groundbreaking developments. Some of these are the superconducting dipole magnets that reach a magnetic field of over 8 Tesla and the rigorous machine protection system to ensure steady operation [15, 16].

CERN is an accelerator complex that houses a number of machines, of which four are used to prepare the proton beams for entering into the LHC. First, the beam is pre-accelerated in Linac 2 up to 50 MeV, before it enters the Booster. The Booster then accelerates and delivers the 1.4 GeV beam to the Proton Synchrotron (PS), which increases the energy to 26 GeV, and injects it to the Super PS (SPS). Finally, the SPS delivers a beam of 450 GeV, which is high enough to inject it into the LHC where it reaches its nominal energy of 7 TeV per beam. Figure 1.1 shows an overview of the accelerators within the CERN complex. While most of the operational year for LHC is dedicated to proton-proton collisions, one part is also used for proton-ion and ion-ion collisions using lead ions.

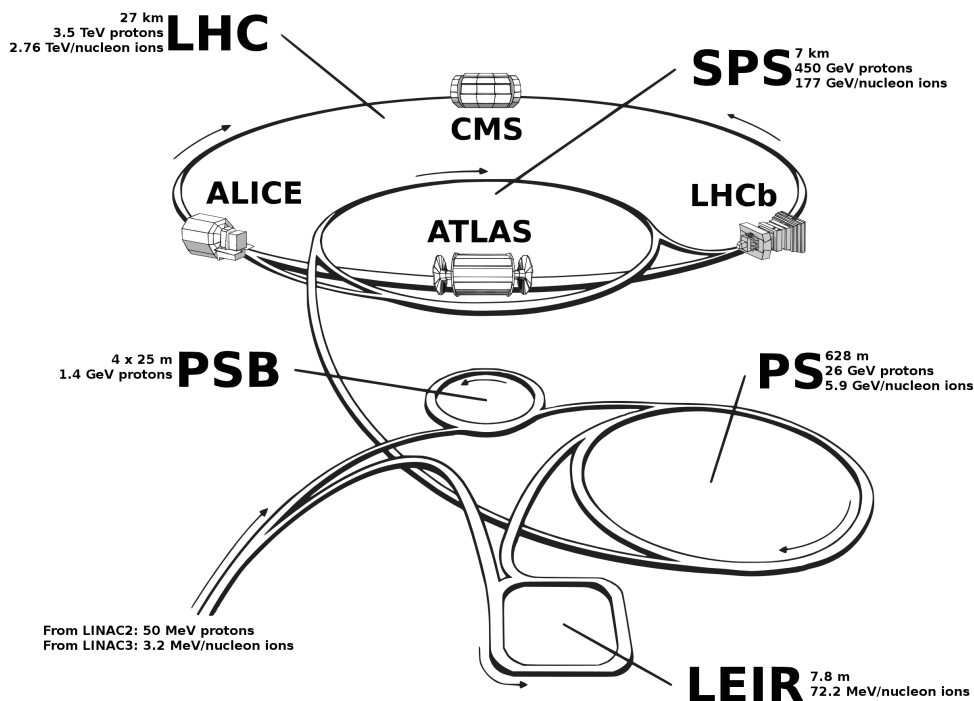


Figure 1.1: The CERN accelerator complex with LHC being the largest ring [17].

The most significant discovery of LHC, on top of the technological advancements to construct the accelerator, is the discovery of the Brout-Englert-Higgs boson. This particle resembles the last piece of the Standard Model.

Already in 2008, the initial year of operation for LHC, its vulnerability to damage became apparent. A faulty connection in the electrical bus between two superconducting magnets led to excess resistance and a quench of the superconducting bus. The quench was not detected as the bus quench detectors were not sensitive enough, leading to a local heating and an opening of

the bus connection. The damage due to the accident led to one year of downtime and enforced the design of new and appropriate electronics to handle the failure mode [18, 19]. Machine protection has been an important aspect of the design of LHC, and the balance between protection and machine availability is a key challenge for the system design. The top-level system architecture is split between safety, beam related machine protection, and magnet powering machine protection. While the safety part is dedicated to the safety of personnel, the beam related part makes use of a vast amount of beam loss monitors for the detection of accidental beam energy release. The powering part targets the accidental release of energy stored in the highly powerful magnet powering circuits, where quenching (loss of superconductivity) is a large challenge [15, 16]. LHC has a dedicated beam dumping system that, in the case of an unwanted scenario, makes sure that the beam is extracted from the synchrotron, transported through a dump line, and safely dumped into the dedicated beam dump.

1.4.2 Spallation Neutron Source (SNS)

SNS is a neutron source with the highest intensity pulsed neutron beam as of today [20]. It is located at the Oak Ridge National Laboratory (ORNL) in Tennessee, USA and managed by the US Department of Energy (DoE). SNS uses negative hydrogen ions (H^-) that are accelerated to 1 GeV through a linac and injected into an accumulator ring. As the ions enter the ring, they go through a so-called charge exchange injection, which means that the electrons are removed by passing the beam through a thin foil. Thus, only the protons remain to enter the ring. The ring compresses and bunches the proton beam before it is delivered in 695 ns pulses at 60 Hz repetition rate to the liquid mercury target. The average proton beam power delivered to the target is currently around 1.4 MW. However, SNS is looking for a future upgrade to reach twice that and to install a second target station. Once the proton beam hits the mercury target, roughly 25 neutrons are released per incoming proton [13, 21].

SNS is built as a partnership of six different US national laboratories: Argonne, Brookhaven, Lawrence Berkeley, Los Alamos, Oak Ridge, and Jefferson. Each lab was responsible for the delivery of a different section of the accelerator, as is seen in Figure 1.2. At that time, the collaboration was one of the largest in the scientific history of the US. SNS was completed in 2006 and started its scientific program in 2007. When it stood ready, after seven years of construction, it was the first MW hadron linac in the world using superconducting radiofrequency technology. The technological success of SNS has influenced the design of the European Spallation Source, described in Section 1.5.1.

The beginning of the SNS linac consists of a front-end with an ion source and low energy beam transport (LEBT), including beam choppers, for creating the correct beam pulse length of 945 ns. This is followed by a radio-frequency quadrupole (RFQ), producing 2.5 MeV beam, a medium energy beam transport (MEBT), and a six-tank drift-tube linac (DTL), generating 86.8 MeV. The last part of the normal conducting (room temperature) linac is the coupled cavity linac (CCL) of 186 MeV, which then leads into the superconducting part delivering 1.0 GeV H^- ions to the entrance to the accumulator ring [13].

Due to its usage of H^- ions as accelerated particles, SNS has faced challenges in their linac that are typically not seen in proton accelerators, such as the LHC. One such challenge is the intra-beam stripping that occurs when an H^- ion loses one or two of its electrons, which

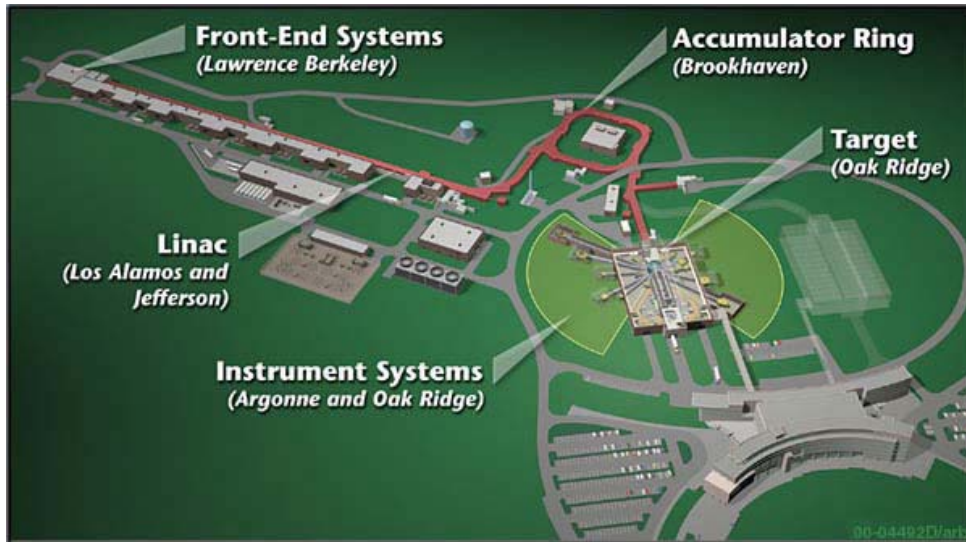


Figure 1.2: The Spallation Neutron Source at Oak Ridge National Laboratory, displaying the contributors for the different sections [22].

makes the ion either not react to the electric fields (if one electron is lost), or go in the opposite direction of the beam (if losing two electrons). This inevitably creates beam losses that need to be considered, as too much of it tends to degrade the superconducting accelerating cavities in the linac. To clean the cavity surface from these beam loss-created impurities, SNS has developed a novel technique of using hot plasma to "burn off" impurities from the surface. This technique makes it possible to avoid dismounting of complex equipment, such as the superconducting cavities, and instead treat the impurities directly as mounted on site [21].

SNS has had a number of studies made in relation to machine protection, such as necessary response times in case of beam losses [23] and reliability analyses [24]. This, along with continuous system improvements during the ten years of scientific operation, has created a stable machine protection system that fits the needs of the facility. SNS uses two types of beam interlocks¹ - one related to hardware and immediate stops of the beam, and one implemented in the software that considers slower beam loss scenarios to trigger a beam stop in case of too high integrated losses.

1.4.3 Japan Proton Accelerator Research Complex (J-PARC)

J-PARC consists of three particle accelerators - one linac and two synchrotrons. While the 400 MeV H^- linac is used to generate a steady beam to the Rapid-Cycle Synchrotron (RCS), the RCS itself either delivers the 3.0 GeV proton beam to the Materials and Life Science Experimental Facility (MLF) or into the Main Ring (MR) that then accelerates the beam up to 30 GeV and sends it either to the neutrino beamline Tokai to Kamioka (T2K) or to the hadron experiment hall. Just as at SNS described above, J-PARC utilizes charge-exchange injection through a copper foil where the H^- ions lose their electrons and enter the RCS. The linac and SCR were finalized in 2007, and the complete facility, including the MR, stood ready two years

¹An interlock is a feature that "locks" two functions together, so that the state of one is dependent on the state of the other. In particle accelerators, a *beam* interlock prevents beam operation if one of the required functions is in an undesired state.

later. The purpose of J-PARC is to generate a variety of particles, such as neutrons, kaons, and pions decaying into muons and neutrinos for a suite of experiments [25, 26].

The performance goal of J-PARC has been to reach a beam power of 1 MW in the RCS, which was achieved in the beginning of 2015. The devastating earthquake in Japan in 2011 delayed the technical projects, but J-PARC has since then stepped up towards its design parameters. The RCS delivers most of its beam (approximately 95%) to the MLF, while four pulses every few seconds are injected to the MR. The entire complex setup with accelerators and experimental facilities is seen in Figure 1.3.

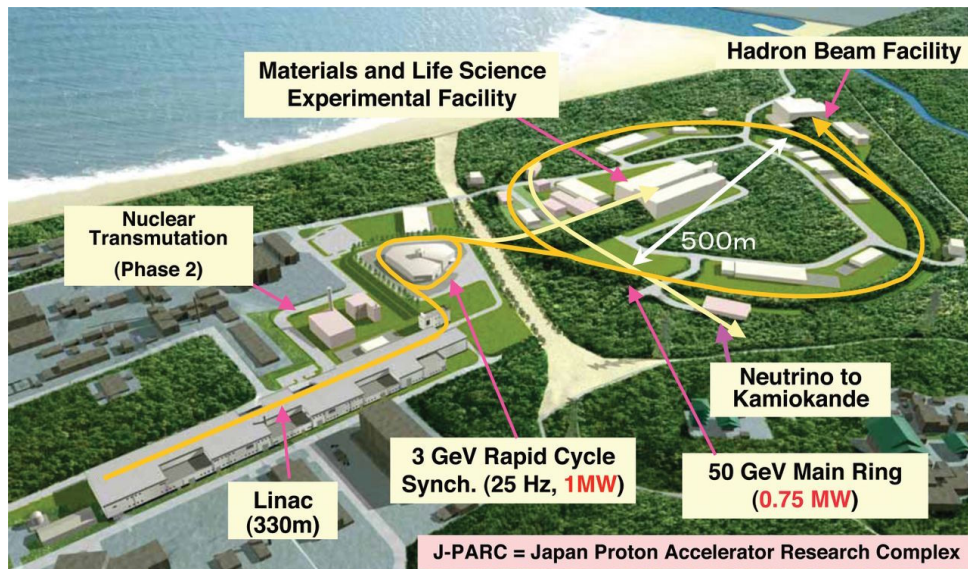


Figure 1.3: The Japan Proton Accelerator Research Complex, J-PARC, displaying the linac, RCS, MR, and the experimental facilities [25].

The H^- linac at J-PARC is designed to generate a 0.5 ms pulse of 25 Hz repetition rate, that it feeds into the RCL. It consists of a multicusp ion source, followed by a radio frequency quadrupole (RFQ) that bunches the ions and accelerates them to 3.0 MeV. After this, there is a drift-tube linac (DTL) of 50 MeV and a Separated-type DTL (SDTL), which generates 191 MeV. To reach the required 400 MeV, an Annular Coupled Structure (ACS) is the last part before the RCL. In the case of delivering beam to the Transmutation Experimental Facility (TEF, noted as "phase 2" in Figure 1.3), an additional 600 MeV superconducting linac (SCL) is used as a final step after the ACS [27, 28].

J-PARC has, just as similar high-power facilities, identified beam losses as an important metric to keep as low as possible in order to reach a satisfactory availability. This is due to that high beam losses prevent quick hands-on maintenance, which on its part causes longer downtimes than necessary [29]. J-PARC uses a hierarchical architecture of their machine protection system, where the control system has the possibility to prevent unwanted scenarios before the beam interlock system takes over. This is implemented to avoid excessive use of the interlock system and balancing protection with reliability [1].

1.4.4 ISIS

ISIS² is a neutron source in Oxfordshire, UK, that has been in operation since 1985. Besides neutrons, ISIS also uses muon spectroscopy for its material research, and since 2009 it operates two target stations. An overview of the facility is seen in Figure 1.4. Despite having a planned lifetime of twenty years, the success of ISIS has provided it with upgrades and investments to make it an operational neutron scattering facility to date [30, 31].

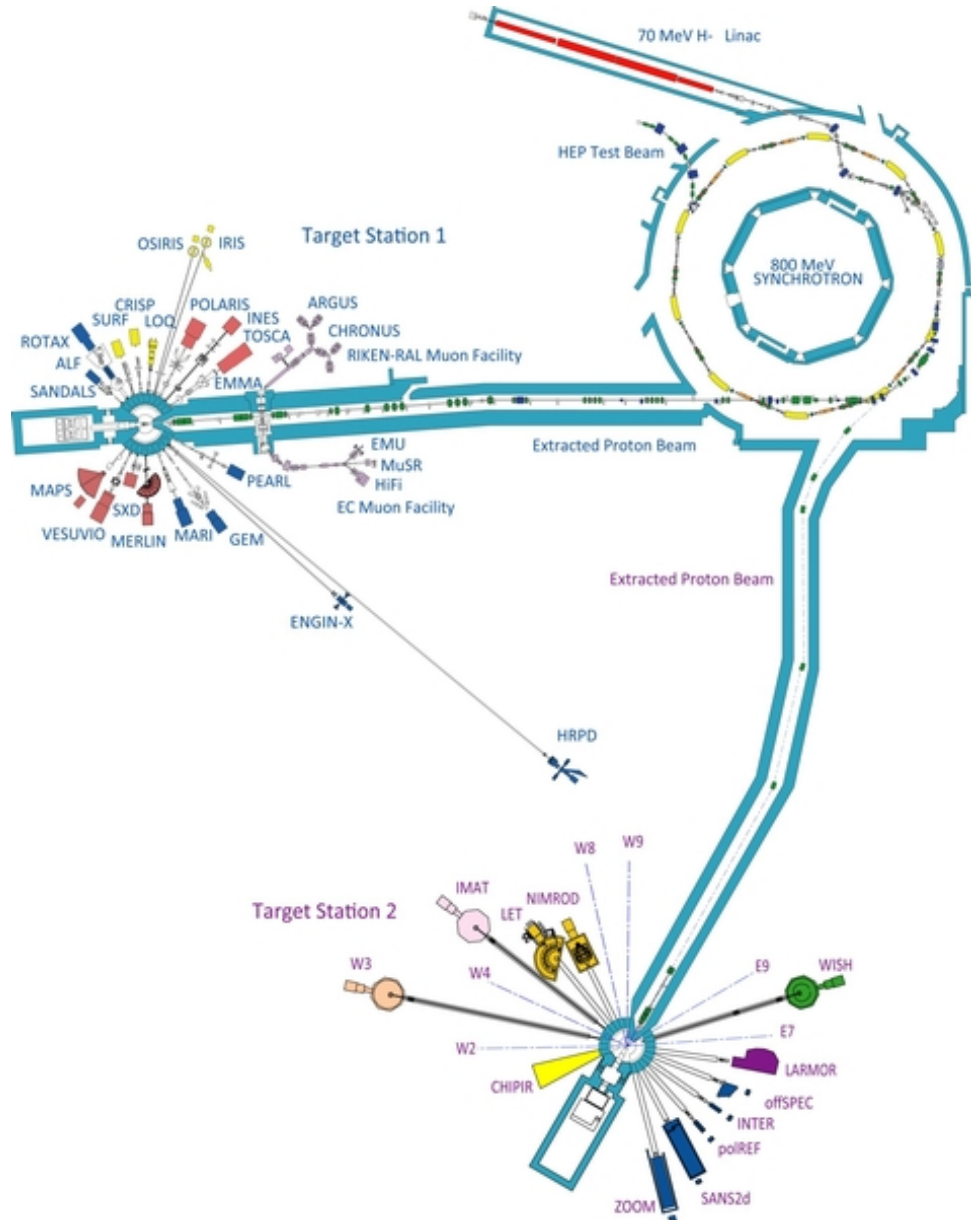


Figure 1.4: The ISIS neutron source with its two target stations [31].

Just as the two previously mentioned facilities, ISIS uses an H^- linac. The linac starts with an ion source followed by a low energy beam transport (LEBT) and an RFQ. After the RFQ, four drift-tube tanks generate the correct beam energy to exit the linac into the 52 m diameter synchrotron, where the final acceleration to 800 MeV takes place. The H^- ions enter

²The name ISIS is not an acronym, but simply refers to both the local name for the Thames river and the Egyptian goddess with the same name.

the synchrotron through a charge-exchange injection using a stripper foil of aluminum oxide, converting the negative ions to protons. The spallation targets consist of thick tungsten (W) plates inside a pressurized vessel. To remove most of the heat that is generated by the 200 kW proton beam in the process, the tungsten plates are water cooled. For the production of muons, for which about 2-3% of the beam is used, the protons are collided with a carbon target. This produces pions that rapidly decay into muons (and neutrinos) [31].

Every year, some 2000 scientists visit ISIS to perform their experiments within a vast number of scientific fields. It is important that the facility is performing as designed in order to succeed in its mission to the scientific community. Upgrades and a long operational lifetime (over three decades) allows ISIS to typically reach 90% availability for its neutron production. In order to keep availability high, it is found critical to keep beam losses low. This allows for quick-access hands-on maintenance and reduces stress on the equipment. ISIS continuously tracks the beam losses and their mechanisms in order to optimize the equipment for this and similar features [31, 32].

1.5 Future Particle Accelerators

Building on much of the technology described in the previous section, a new set of accelerators is studied and designed to enable future research. As the understanding and focus of natural sciences go towards smaller scales, the need for new facilities arises in parallel. Future accelerators are concerned with delivering more powerful, more energetic, but also more intense, particle beams. As intensity is increased, data collection for the scientific experiments can reach a higher yield in a shorter time, hence increasing the efficiency of the experiments. This section describes four such facilities, where the first one, ESS, is used for the proof of concept for the risk management method that is developed in this thesis. The second facility, IFMIF, is taking form in Japan, while the last two facilities, ILC and CLIC, are in their study phases and have not yet been approved.

1.5.1 European Spallation Source (ESS)

The European Spallation Source (ESS) is a high-power neutron spallation source that is currently being built in Lund, Sweden. It is a stand-alone European project involving 16 countries, of which Sweden and Denmark are the host countries. The neutron facility itself is built in northern Lund, while the data management center is located at the Niels Bohr Institute in Copenhagen. The first neutrons are planned to be produced by the end of 2020. Delivery of full beam power and complete installation of 15 instruments is planned for 2025 [33, 34]. As the proof of concept for the method developed in this thesis is done for ESS in Chapter 5, this section and facility will receive slightly more attention than the other facilities.

Neutron Spallation at ESS

Since the construction of ISIS in 1985 (Section 1.4.4), there has been a defined need for an even stronger neutron source to perform experiments in the front line of science. In 1999, the European Neutron Scattering Association (ENSA) convinced the Organization for Economic

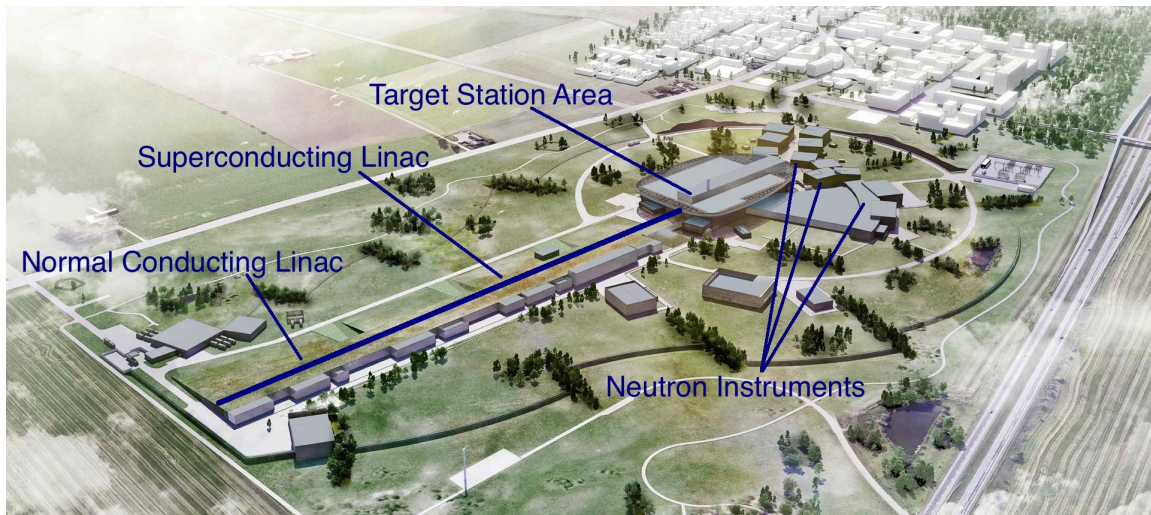


Figure 1.5: The European Spallation Source looking from northwest [35].

Cooperation and Development (OECD) that powerful neutron sources were important research tools for the future. Therefore, one high-power neutron scattering facility should be placed in each of the continents of Europe, Asia, and America. The latter two already had such high-end neutron sources (SNS and J-PARC), and the turn had come to Europe. In 2009, it was decided that Lund will be its location [1].

Within the partner countries, there are over 100 associated partner labs that are involved in the construction and research at ESS. In addition to the partner lab visits to the neutron source, external researchers will be invited and in total some 3000 guest researchers are expected to come to ESS each year. The ESS proton beam power will reach 5 MW and, as the first neutron facility ever, use a long-pulsed proton beam with a nominal pulse length of 2.86 ms. Objects of sizes 10^{-11} to 10^{-6} m can be resolved in time frames between 10^{-9} to 10^{-3} s, allowing for studying smaller and more complex objects than before [33].

ESS Technology

The production of spallation neutrons at ESS is done through a series of steps. The first step is to heat a hydrogen gas to produce a plasma of free protons and electrons. The protons and electrons are separated by an electromagnetic field, and the protons are collected and accelerated through 48 m of normal conducting linac. The normal conducting linac is operated at 352.21 MHz and includes a LEBT, RFQ, MEBT, and five DTL tanks. This gives the protons an energy of 90 MeV. This is followed by the superconducting part of the accelerator, containing 26 spoke cavities at 352.21 MHz and 36 medium β and 84 high β elliptical cavities at 704.42 MHz. All of the superconducting cavities are placed in cryomodules, where they are immersed in liquid helium baths and cooled to 2 K. After the 312 m of superconducting linac, the protons have a nominal energy of 2.0 GeV, corresponding to a velocity of 96% of the speed of light at the point of hitting the spallation target. A schematic view of the linac and its parts is seen in Figure 1.6.

The proton beam current is 62.5 mA with a pulse repetition rate of 14 Hz at full power. A pulse length of 2.86 ms then gives a 4% duty factor. In total, the whole linac is 603 m long, where the last 241 m are dedicated for contingency space and possible future upgrades [37].

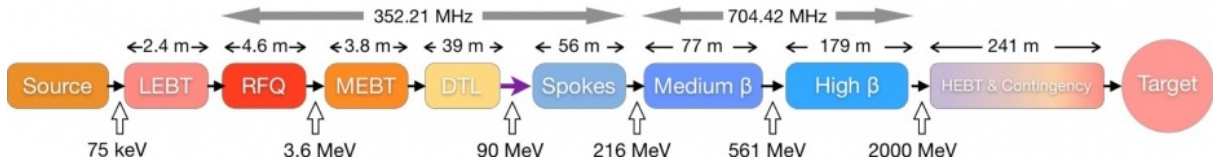


Figure 1.6: The ESS linac layout [36].

The target consists of neutron-rich tungsten ($^{110}_{74}\text{W}$) divided into 36 radial sections, which is rotating at a frequency of 0.39 revolutions per second. The produced neutrons initially have a very high energy, and a velocity of about 10% of the speed of light. This is too high for usage within most experiments, and the neutrons have to be slowed down to about the speed of sound using water and hydrogen moderators, and then guided to the experimental stations. There, they scatter off the nuclei of the samples in various directions yielding large amounts of data, which is used for e.g. 3D image production and further analysis [37].

1.5.2 International Fusion Material Irradiation Facility (IFMIF)

With the development of nuclear test reactors for energy production through fusion, such as ITER [38] and DEMO [39], there is a need for test facilities that can help in the development and verification of new material solutions to be used in close proximity of the fusion plasma. These materials will be irradiated beyond current standards and it has been found that accelerator-driven systems (ADS) are a perfect tool for these experiments. The International Fusion Material Irradiation Facility (IFMIF) is such a project that has started, and the facility is to be located in Japan. IFMIF will try to mimic the environment inside the fusion reactor [40].

To achieve its end goal, IFMIF will consist of two identical advanced linacs and a final lithium target, producing the particles that will irradiate the experimental materials. The linacs follow, to a large extent, that of current high-power linacs as described in Section 1.4 and ESS as described above. After the ion source (100 keV), LEBT, RFQ (5 MeV), and MEBT, there are four superconducting half-wave resonator (SC-HWR) cryomodules (of 9, 14.5, 26, 40 MeV) [40]. These SC-HWR were selected instead of the "traditional" DTL due to the continuous wave (CW) beam, and were found to save both ten meters of length and around 6 MW of power compared to the copper DTL choice of pulsed linacs [41]. A schematic of the IFMIF linac layout is seen in Figure 1.7.

Each accelerator will generate a 125 mA 5 MW deuteron beam in CW. The beam with a final energy of 40 MeV is impinged on a steady 15 m/s flow of lithium, which reacts with the deuterons to generate a steady neutron flux onto the materials. The facility will provide high, medium, and low neutron flux regions, where the high flux region can house 1000 individual and temperature controlled specimens to simulate long-term effects in the materials. To generate the anticipated outcome, IFMIF has to run continuously for very long periods of time and its reliability and availability are critical parameters for its success [40, 41, 42].

1.5.3 International Linear Collider (ILC)

ILC is a study for a linear electron-positron collider, first outlined already in 2003. While hadron colliders, such as the LHC, are useful in making new discoveries within high energy physics

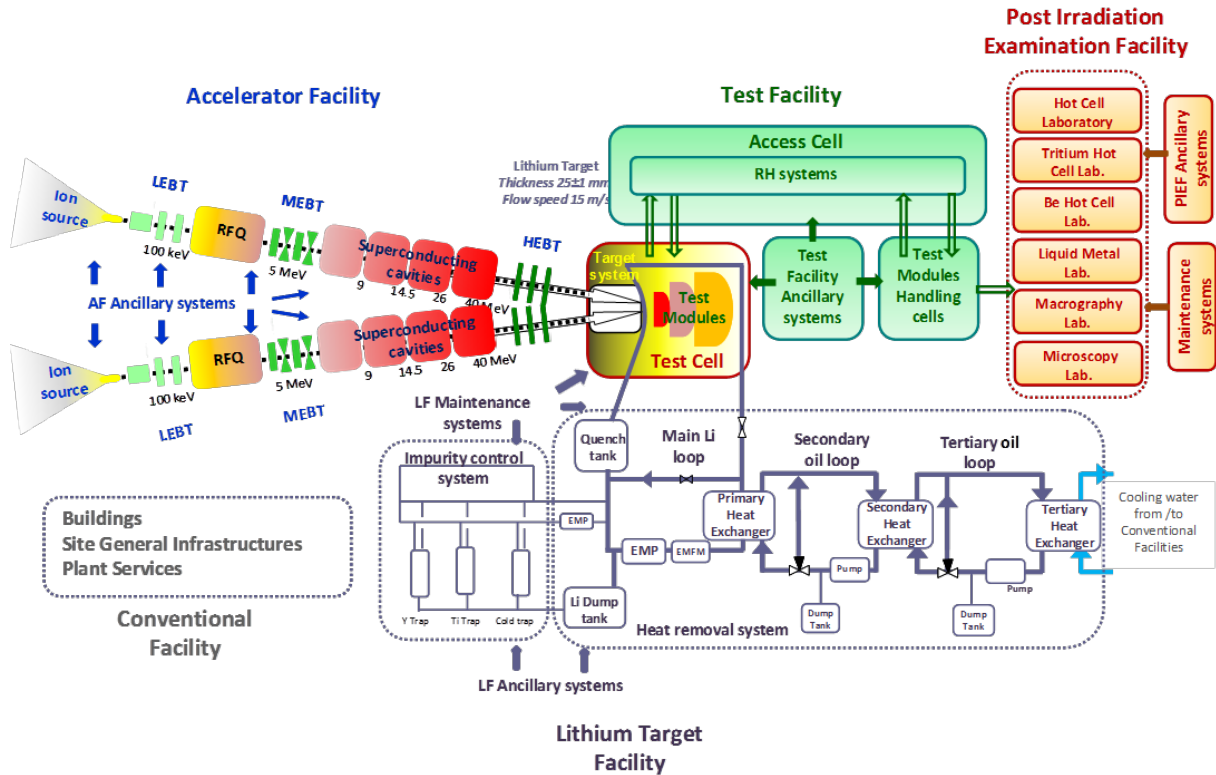


Figure 1.7: The IFMIF linac layout [40].

(HEP), precision measurements require more precisely defined particles, such as leptons. In addition, there are still several questions within HEP that cannot be answered by the Standard Model as it stands today, such as the connection between gravity and the other forces or the imbalance between matter and antimatter. The ILC design, as presented in the Technical Design Report of 2013 [43], is a result of two decades of accelerator research within the physics community and under the mandate of the International Committee for Future Accelerators (ICFA).

The main technology behind ILC is superconducting radio frequency acceleration. The design specifies a center of mass collision energy of 200-500 GeV. The linear collider consists of one electron and one positron source, 5 GeV damping rings (DR) with a circumference of 3.2 km and a transport to the linacs, which are 11 km long and reaching an average accelerating gradient of 31.5 MV/m. Finally, there are two 2.2 km beam-delivery systems bringing the two beams into collision. An overview of ILC is seen in Figure 1.8, where the vast scales of the facility are seen, totaling a length of some 31 km. A curious technological piece is the positron source, which makes use of undulated electrons, producing high-energy photons that are converted to electron-positron pairs [43].

The technical parameters for ILC call for careful design and planning, and also have to consider foreseen emergent phenomena and cost-performance balancing for the accelerator. Such phenomena are e.g. electron cloud formation in the positron ring, cryogenic heat loads, RF power, and beam instabilities. The linacs consist of around 7400 nine-cell superconducting cavities located in approximately 850 cryomodules, with an unloaded Q factor of more than 10^{10} [45]. Needless to say, this scaling of a factor 9 in physical footprint from existing electron linacs, such as the European XFEL [46], require robust and reliable design and controls.

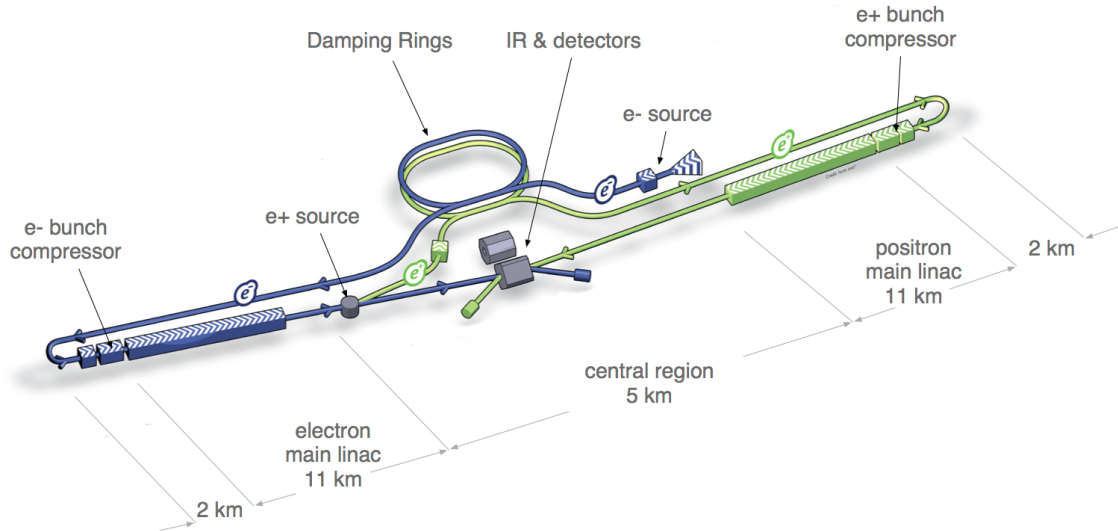


Figure 1.8: The International Linear Collider [44].

1.5.4 Compact Linear Collider (CLIC)

CLIC is yet another international collaboration for the study of a possible future accelerator, including over 70 institutes in 30 countries. Just as ILC, its goal is to collide electrons and positrons for precision measurements. However, the aim is a multi-TeV center of mass beam energy and accelerating fields up to 100 MV/m are attempted. CLIC was initially initiated by CERN, but has now grown to encompass a much broader interest [47]. The design of CLIC allows for a staged construction, where the initial collision energy could be 380 GeV, followed by 1.4 TeV and finally 3.0 TeV. A schematic overview of the CLIC facility is seen in Figure 1.9

The main difference between CLIC and other modern particle accelerators is the usage of a drive beam, rather than RF power, to accelerate the main beams through a two-beam acceleration scheme. In traditional RF structures, the accelerating gradient reaches somewhere in the order of a few tens of MV/m, as the 31.5 MV/m in ILC (Section 1.5.3). This makes a high-energy linac very long, and CLIC is aiming to reduce this (hence the "compact" in its name) by having an unprecedented accelerating gradient.

Such high gradient is achieved in CLIC by using very short RF pulses generated at high efficiency through a compressed electron drive beam. The accelerated drive beam electrons are guided along the main linac and are then decelerated in separate structures, which leaves a trailing wake field behind them. This field is built up through many bunched particles following each other, and is then transferred through waveguides into the main beam [47, 48, 49].

In the past few years, key concepts and technology for CLIC have been demonstrated and validated at CTF3 at CERN [47], at SLAC through the FACET experiment [51], at Elettra [52], and at KEK [53]. CLIC technology has also spread to other related fields, such as medical facilities [54] and free electron lasers (FEL) [55], showing how the field of accelerator physics is expanding and developing beyond the immediate facilities themselves.

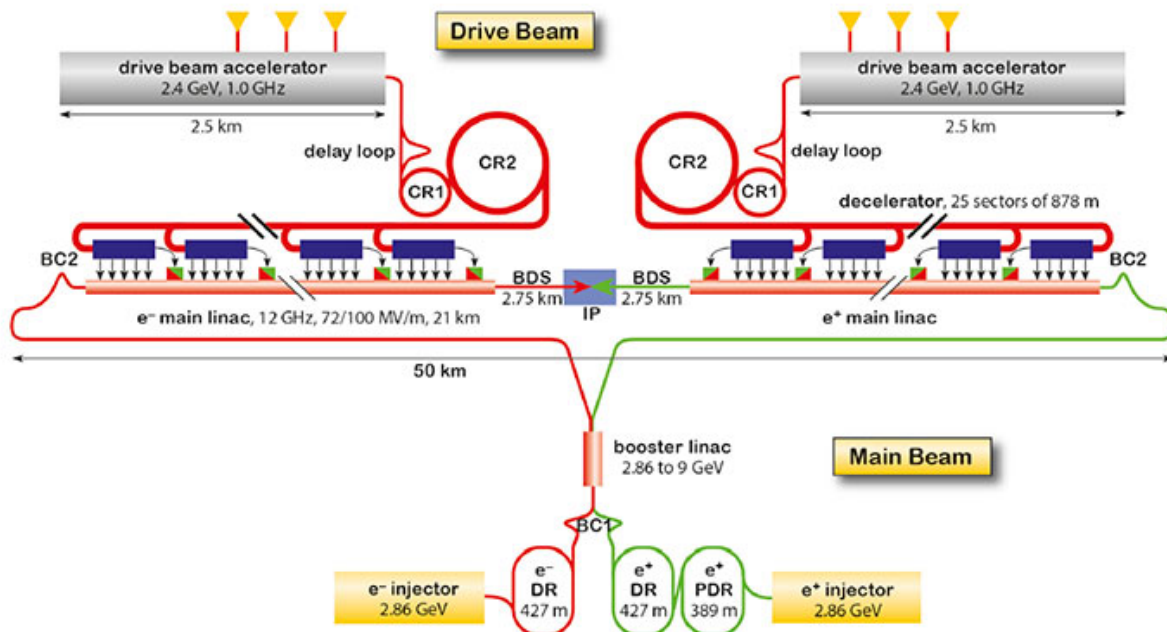


Figure 1.9: The Compact Linear Collider [50].

1.6 Beam Physics and Propagation Along a Linac

To propagate a particle beam through an accelerator for its final use, either in the collision with a target to produce other particles (as in a neutron spallation source) or to collide with another beam for fundamental physics experiments (as in a particle collider), there are several mechanisms that have to work in a collaborative fashion. One could say that an accelerator needs to perform five main functions to the particle beam:

- Bunch
- Accelerate
- Steer (bend or correct)
- Focus (shape)
- Monitor

Specialized accelerator equipment has been developed over the past century to perform these functions. This section will very briefly describe this equipment and their main functionality, taking ESS as an example where this is due. Figure 1.6 in the previous section then displays the details of the ESS linac. In the last two subsections, the correlation between beam energy, beam power, and damage potential of the beam is described.

1.6.1 Beam Bunching

In order to allow for efficient acceleration, the particle beam has to be *bunched*. This means that the steady flow of particles is chopped up into shorter pieces to match the resonant frequencies of the accelerating structures. This should not be confused with the beam *pulse*, which is a

macro-scale time structure of the beam. The bunch is instead a micro-scale entity, typically in the range of nanoseconds [56].

By adjusting the accelerating phase to slightly reduce the energy of the early particles in the bunch and increase the energy of the later particles, the bunch becomes more compressed and separated from the other bunches. At ESS, the beam bunching is done in the RFQ and in specialized buncher cavities that are located in the MEBT section of the linac.

1.6.2 Beam Acceleration

Due to the change of beam energy along the linac, different accelerating structures are used at different locations to produce the required electric fields. In current state of the art proton and ion machines, such as SNS and J-PARC, as well as for ESS, the low energy, normal conducting section uses the RFQ and DTL to accelerate the beam, while the superconducting section uses electromagnetic resonators, or cavities, for the same purpose. As mentioned in the beam bunching description, the bunches are created to match the resonant frequency of these accelerating structures in a linac.

It is not possible to produce stable electric fields above a few tens of MV per meter using DC fields, since this would lead to e.g. vacuum arcing and (electron) field emissions from the metallic walls of the accelerating structures. Instead, modern accelerators use alternating fields, usually at a frequency of hundreds of MHz. These fields alternate direction to match the particle beam bunches, so that the field is along the acceleration direction when the bunch passes, and the opposite direction when the bunch is out of reach [8, 57].

Drift Tube Acceleration

In a DTL, each separate tank has an alternating accelerating field and a number of drift tubes in them. While inside the drift tubes, the particles are shielded from the field, and while outside, they are affected by it. The structure is thus, by physically matching the frequency of the field, set up so that the bunches are accelerated during the length L between the drift tubes when the field is in the right direction (generally called the positive z direction). While the field makes its "flip", the bunches are inside the drift tubes. If the center between two consecutive drift tubes is considered zero, the alternating electric field, $E_z(t) = E_0 \cos(\omega t + \phi)$, gives a power increase to each particle, being

$$\Delta W = qE_0 \int_{-L/2}^{L/2} \cos(\omega t + \phi) dz \quad (1.1)$$

for each accelerating gap. Using the trigonometric addition rule for cosine, performing the integral, and keeping in mind that sine is an odd function, the power increase becomes

$$\Delta W = qV_0 T \cos(\phi), \quad (1.2)$$

where T is the so-called transit time factor, written as

$$T = \frac{\sin(\pi L / \beta \lambda)}{\pi L / \beta \lambda}. \quad (1.3)$$

In the above expression, ϕ is called the *synchronous phase* and should be minimized to achieve the highest accelerating gradient and energy gain. The above expressions are simplifications for "infinite" plates and a particle that is exactly on the main trajectory axis. For completeness, the E_0 term needs to consider the particle position in longitudinal z direction and radial r direction [8, 57, 58].

Cavity Acceleration

Metallic electromagnetic resonators - called cavities and often being superconducting - carry a standing wave of accelerating radio frequency (RF) fields. These cavities are powered through electromagnetic wave guides that transport a modulated and amplified RF wave from the RF system to the cavities. For an efficient linac acceleration, it is important that the beam receives a large amount of energy from the cavity RF field. The energy that is delivered to the beam in the cavity needs to be compensated for, which is done by the RF system [8].

Each cavity typically contains a number of cells, in between which the field is coupled. This means that the RF field flows between the different cells and feed each other. It is inevitable that some energy also dissipates into the cavity walls, which is aimed to be reduced as much as possible. The fraction of the energy that is stored in the cavity to the amount that is dissipated through the walls per RF cycle is called the *quality factor*, or Q factor, of the cavity. Mathematically, it is written as $Q = \omega U/P$. A lower surface resistance yields a higher Q factor, and a superconducting cavity has a Q factor of $10^8 - 10^{10}$, while a normal conducting copper cavity has around $10^3 - 10^4$. Just as in the drift tube case, the cavities achieve phase stability through setting the field phase so that particles arriving early receive less accelerating gradient than late particles so the bunch stays longitudinally compact [58].

1.6.3 Beam Steering

In order to steer, bend, and correct the path of the particle beam, dipole magnets are used. These produce a magnetic field from two opposite poles on each side of the beam. Depending on the energy of the particles, the magnetic field is adjusted accordingly. Synchrotrons use magnetic fields that are synchronized to the beam energy to keep an increasingly energetic beam in a circular motion with constant radius [59].

1.6.4 Beam Focusing

Accelerators are designed around a reference particle trajectory, followed by an "ideal particle", which is in the middle of the beam pipe. However, particles in a beam will be distributed around this reference trajectory and thus experience slightly different fields depending on their position and momentum. This combination is referred to as the 6D *phase-space*, written as $\psi(x, x', y, y', z, E)$, where the prime signifies the first derivative with respect to z [60].

Quadrupole Magnets and Accelerator Lattice

The particle beam needs to be focused towards the center trajectory not to disperse and be lost. This is typically done by quadrupole magnets, which have four coils that focus in one

direction (x or y) and defocus in the other. By setting up a structure that alternates between focus and defocus (and vice versa for the other direction), one achieves a focusing effect in total called alternating gradient focusing. One set of a focus and a defocus quadrupole magnet is called a FODO doublet, which is a common way to focus particles beams in an accelerator. The accelerator structure, consisting of dipoles, quadrupoles, and sextupoles, is often called the *accelerator lattice*.

Emittance and the Beta Function

When applying the FODO structure, the stability of the focusing needs to be observed. Stability is ensured by having a focal length of $f > L/4$ for each quadrupole, where L is the length of the FODO doublet. The beam motion can be calculated using the so-called Courant-Snyder framework, where one first has a look at Hill's equation (note the similarity with the harmonic oscillator if $K(s) = K$):

$$x'' + K(s)x = 0. \quad (1.4)$$

By introducing the *beta function*, which varies along the lattice, the solution to the above equation is

$$x(s) = \sqrt{\varepsilon\beta(s)}\sin(\phi(s) + \phi_0), \quad (1.5)$$

with the following constraint on the beta function

$$\frac{1}{2}\beta(s)\beta'' - \frac{1}{4}\beta'^2 + K(s)\beta^2(s) = 1. \quad (1.6)$$

The constraint above is called the *betatron equation* and plays a major role in beam stability and potential beam losses [57].

Coming back to the phase-space mentioned above and looking at Eq. (1.5) as the expression for the particle position (in x or y), the momenta can be obtained through derivation with respect to s :

$$x'(s) = \sqrt{\frac{\varepsilon}{\beta(s)}} \left(\cos(\phi(s) + \phi_0) + \frac{\beta(s)}{2} \sin(\phi(s) + \phi_0) \right). \quad (1.7)$$

Now all parameters are in place to actually describe the beam shape in the transverse phase-space, which in turn includes the beam size and distribution that is required to be monitored, as described in Section 1.6.5, and kept under control by the focusing magnets. The transversal phase-space of a single particle could be described as an ellipse (of area $\pi\varepsilon$) by introducing the Twiss parameters:

$$\alpha(s) = -\frac{1}{2}\beta'(s) \quad (1.8)$$

$$\gamma(s) = \frac{1 + \alpha^2(s)}{\beta(s)}. \quad (1.9)$$

Also $\beta(s)$ is a Twiss parameter, as solved from either of $\alpha(s)$ or $\gamma(s)$ above, or Eq. (1.6). The single particle *emittance* can then be expressed as [58]

$$\varepsilon = \gamma x^2 + 2\alpha x x' + \beta x'^2. \quad (1.10)$$

Particle Distribution in a Beam

The beam consists of many particles corresponding to different ellipses. It is often a good approximation to use a Gaussian distribution to describe all of the particles in the beam, and to derive a single parameter for the emittance of the collection of particles in the beam, the root mean square (RMS) emittance. Using this, the transversal beam size becomes

$$\varepsilon_{RMS} = \gamma x_{RMS}^2 + 2\alpha x x' + \beta x'^2 \quad (1.11)$$

at one standard deviation from the beam center. Typically, the beam size is given as a pre-defined number of standard deviations from the beam center, which needs to fit into the vacuum chamber aperture. The accelerator lattice then ensures that the beam particles stay within the physical limitations in the transverse planes [57].

It is clear that if the emittance of the particles grows, the area of the phase-space ellipse increases. If the area increases too much, particles will be lost in the surrounding equipment of the accelerator. Therefore, it is very useful to minimize the emittance growth, which is done through beam focusing. The beam ellipse, with some of the relevant parameters, is seen in Figure 1.10. Particles far outside the ellipse core may become unstable and form beam halos that lead to losses as they drift outside of the physical aperture. In addition to beam focusing, the beam halo is handled through *collimators* in the beam pipe, that "scrape off" the particles that are outside the desired transversal aperture of the beam.

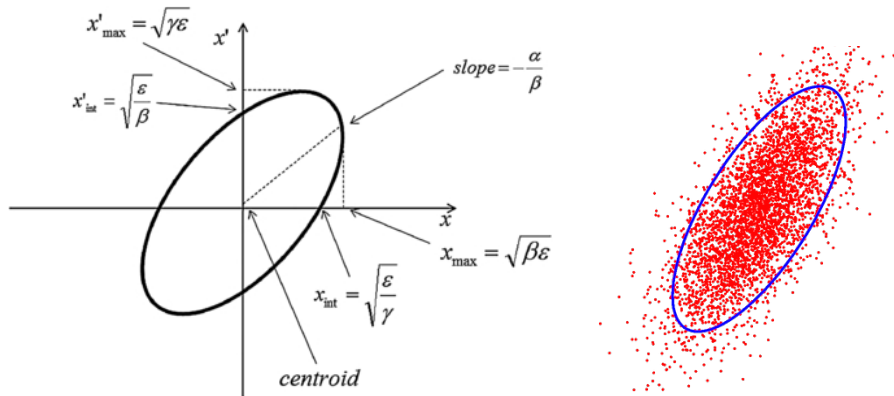


Figure 1.10: The phase-space ellipse with some parameters (left) [61] and a Gaussian distribution of particles in and around the ellipse (right) [62].

1.6.5 Beam Monitoring

In order to correct for errors and ensure the beam-related protection of accelerator equipment, as discussed in Sections 1.6.6 and 1.6.7, the particle beam is continuously monitored. As seen above, several phenomena can lead to beam losses, and this needs to be taken care of through constant adjustments and tuning of the accelerator. Typically, one measures the beam position, shape, and phase; its pulse length, current, and repetition rate; and contingent beam losses. At ESS, this can be done by beam position monitors (BPM), beam current monitors (BCM), and beam loss monitors (BLM), respectively. In addition to these monitors, the beam profile, energy, and current can be measured with wire scanners and Faraday cups.

Beam Position Monitors

ESS has two kinds of BPMs to measure the beam position and shape - stripline and electrostatic button - for a total of about 100 BPMs. The stripline monitors are used in the normal conducting linac and appear in the MEBT and DTL. The electrostatic button monitors are located in the linac warm units (LWU) in between cryomodules in the cold linac, and are of similar type to those used in e.g. the European XFEL at DESY in Germany. In order to allow for time of flight (ToF) measurements of the beam, which are used to derive phase differences and beam energy, the BPMs in the cold linac are alternately located close to the upstream and downstream cryomodules (staggered locations), so that the distance difference between two consecutive monitor pairs is approximately 0.5 m. The BPMs at ESS have an accuracy of $200\ \mu\text{m}$ and a resolution of $20\ \mu\text{m}$ [63].

Beam Current Monitors

BCMs are sometimes also referred to as beam current transformers, which points out that they are of AC current transformer type (ACCT). At ESS, there is a total of 15 ACCTs and the majority of those are found in the normal conducting linac. This makes it possible to detect potential beam losses through the differential measurements between monitors, where the difference between beam current in one monitor to the next corresponds to the current (or number of particles) that has been lost. BCMs also measure the actual current of the beam, to make sure that this corresponds to the requested beam current. In addition to the 15 ACCTs, there will be one fast current transformer (FCT) in the MEBT to detect whether or not the beam has been accurately chopped in the LEBT and MEBT choppers and is ready for entering higher energy acceleration [64].

Beam Loss Monitors

BLMs monitor both prompt and integrated beam losses. This means that there needs to be a dynamic range that is wide enough to encompass both large, instantaneous losses as well small losses over time. The related BLM electronics has to be able to quickly process fast losses and in addition integrate over a certain period of time to identify small but relevant losses that could lead to unwanted activation of the beamline equipment. ESS will contain over 300 BLMs of two different types. The most common is the parallel plate ionization chamber (IC), which measures the lost particles and their particle showers through an ionized N_2 gas at just above atmospheric pressure. This monitor is the same as that used in the LHC at CERN [65]. There are also neutron detectors (ND), based on MicroMegas technology [66], to measure secondary neutrons. The NDs can operate at lower particle energies than the ICs and are therefore useful for beam loss measurements in the normal conducting linac [67, 68].

Wire Scanners

Wire scanners (WS) are used especially in the commissioning and accelerator restart phases to characterize the transverse beam profile. The WSs operate by inserting a wire that moves across the beam profile and creates secondary emissions at lower energies (up to around 200 MeV) and hadronic showers at higher energies. These emissions and showers are proportional

to the number of particles, and one is thus able to get a picture of the beam profile. The WSs use scintillators and PMTs to detect the particles, located around 4 m downstream of the wire. The ESS design contains eight WS stations along the linac [69].

Faraday Cups

Faraday cups (FC) are used to measure the beam current and completely absorb the beam at different locations along the linac. The FCs are also able to measure the beam energy and are used in the accelerator during the commissioning and tuning stages, with the purpose to absorb the beam and help in optimizing the beam parameters up until the FC location. They move in and out of the beam pipe through a pneumatic actuator system and due to the high energy deposit, they need to be water cooled [70].

Proton Beam Imaging System

The proton beam imaging system, located in the target station of ESS, monitors the beam profile and current at the end of the linac, as it hits the target. It ensures that the beam is consistent with the requested beam shape and that the intensity is within intended limits. The imaging system consists of a luminescent coating that is sprayed onto the target and proton beam window, a mirror-based optical system, and readout electronics with associated software. The optical system needs to accurately transfer the optical image of the beam out of the target station environment into a camera. As the luminescent coating is placed in a highly radioactive environment and receives unprecedented integrated beam power over the 5-year lifetime of the target, it is critical that the correct chemical is used and accurate spraying measures are taken for the imaging system to be successful [71].

1.6.6 Beam Energy and Damage Potential

The damage potential of a particle beam depends on a variety of parameters, such as energy, power, particle type, beam size, energy density, current, and the cooling conditions of the surrounding equipment. A detailed discussion on all of these is outside the scope of this section, but they are all indirectly considered in the definition of protection functions in Chapter 5. This section and the next will quickly touch upon the two former parameters - beam energy and beam power.

The increase in beam energy along a linac, or with every turn in a synchrotron, generates different phenomena related to particle interaction with the surrounding equipment at different locations, which needs to be considered when designing an accelerator and its protection functionality. The Bethe-Bloch equation describes the stopping power of a certain material for impinging charged particles (above a few MeV) - or, put differently, the energy loss of the charged particle during interaction with matter. Most of this energy loss is transferred to the atomic electrons, thus ionizing the atoms in the material. For a particle with charge z and energy E that travels with speed v into a material with atomic number Z and relative atomic mass

A , the energy loss per traveled distance, $-dE/dx$, is written as

$$-\frac{dE}{dx} = 4\pi N_A r_e^2 m_e c^2 \cdot \frac{Z}{A} \cdot \frac{z^2}{\beta^2} \cdot \left[\frac{1}{2} \ln \frac{2m_e c^2 \gamma^2 \beta^2}{I^2} \cdot T_{max} - \beta^2 - \frac{\delta}{2} \right], \quad (1.12)$$

where N_A is Avogadro's number, r_e the electron radius, m_e the electron mass, γ the Lorentz factor, c the speed of light, and $\beta = v/c$ [72]. For practical purposes, the tabulated value for dE/dx can be found in e.g. [73] for different particles and materials. This formula shows that the energy loss of a particle is higher the lower its energy. Thus, a highly energetic particle results in different kinds of losses in the material without depositing damaging energy at its surface, while a particle of lower energy will cause quicker damage if lost in the surrounding equipment. This is also seen in the shift of the so-called Bragg peak Figure 1.11, where the relative dose of energy deposit from a particle is closer to the material surface for lower energies [58].

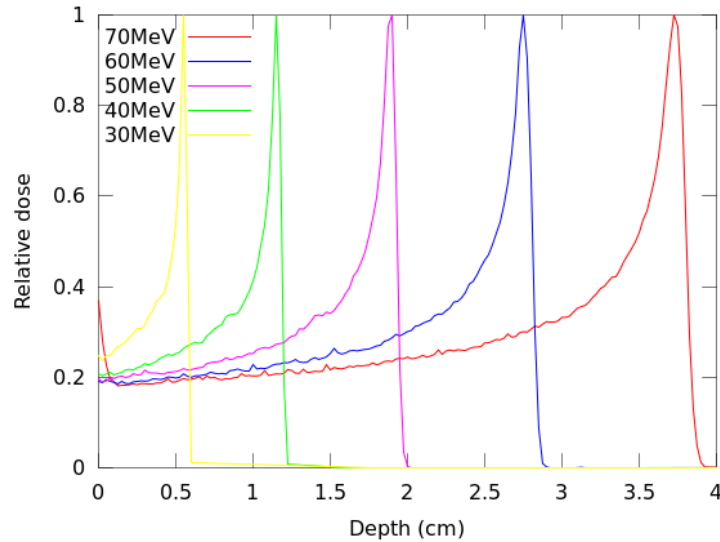


Figure 1.11: Bragg peaks for protons of energies between 30 MeV and 70 MeV [74].

Therefore, the beam losses in the early sections of the linac have a different damage potential than the later sections, being that they deposit energy quicker and closer to the surface. Referring again to Eq. (1.12), for a beam hitting a piece of equipment perpendicularly, the time before permanent damage is

$$t = \frac{2\pi\sigma_x\sigma_y j}{I \cdot dE/dx}, \quad (1.13)$$

where $2\pi\sigma_x\sigma_y$ is the beam size, I the beam current, and j the energy deposition [23]. For a copper structure ($j = 62$ J/g) at ESS, with a beam current of $I = 62.5$ mA and beam size $\sigma_z = \sigma_y = 1$ mm, the melting time could be as low as $t = 1.5$ μ s at $E = 2.5$ MeV [75]. One should keep in mind though, that since this is based on the entire beam hitting perpendicularly on copper beamline equipment, there are only very few cases where this scenario is possible and relevant.

1.6.7 Beam Power and Damage Potential

For a pulsed linac, the average beam power is defined as

$$P = I_{peak} \cdot E_{beam} \cdot f_{rep} \cdot \tau_{pulse}, \quad (1.14)$$

where I_{peak} is the peak beam current within a pulse, E_{beam} is the energy, f_{rep} the pulse repetition rate, and τ_{pulse} is the pulse length. The achievement of a high beam power is thus linearly proportional to the achievement of the beam mode parameters above. ESS aims at delivering a 125 MW peak-power (5 MW average power) proton beam to the tungsten target, which is both a world record and the cause behind most of the ESS challenges. As seen in Section 1.6.6, the increase in beam energy is actually relaxing the reaction time requirements on the protection systems, while the other parameters increase them. However, a higher beam power naturally means that only a smaller *fraction* of the beam can be lost along the linac without causing critical and possibly damaging losses.

Beam losses can be divided into prompt (or immediate) losses that occur quickly and continuous losses over time. While the prompt losses are typically caused by failures in equipment and are treated by stopping the beam, the continuous losses require careful monitoring as a very small portion of the beam that is lost over an extended period of time can lead to equipment degradation and unwanted activation. As stated above, the higher the beam power, the smaller portion of the beam can be lost. As an example, a continuous loss of 1% of a 5 MW beam corresponds to 50 kW. If this is lost in the HEBT and contingency at ESS, being 241 meters (Section 1.5.1), the average loss is 207 W/m. It is often claimed [11, 76, 77, 78, 79, 80] that 1 W/m of beam losses can be allowed for hands-on maintenance, something that in this example would be largely exceeded. This allowable loss ratio, depending on the beam power, then plays a key role in the design of the accelerator and the procedures for maintenance by directly affecting the maintainability (Section 1.7.2) and in extension the availability of the facility.

1.7 Preventing Damage and Downtime of Particle Accelerators

All of the machines that are discussed in Sections 1.4 and 1.5 are very complex and expensive. As their purpose is to serve external users, they need to fulfill the demands of the users, both in terms of performance and availability. It goes without saying that there are numerous operational risks to account for. Two of the most imminent are *damage to equipment* and the associated *downtime of the facility*. The increasing beam powers yield an increase in damage potential, both from the particle beam and through the increased stress on the equipment. In addition to the unwanted downtime related to damage, there is also a certain cost to consider as well. It is therefore necessary for accelerator facilities to have a strategy and systems that consider these risks. Such systems are generally referred to as machine protection systems (MPS), even though the "S" has become more of a *strategy*, or *system of systems* (SoS, see Chapter 5), than a single system.

In order to assess whether machine protection is necessary, a large set of criteria are considered. These are, among many other things, the damage potential of the beam, the expected beam

loss levels at different locations of the accelerator, the delicacy (susceptibility for damage) of the equipment, the beam injection and extraction mechanisms, beam stop procedures, and requirements on availability. On top of this, there is a tendency for unexpected events to occur as unbeaten paths are taken by modern accelerators. An overview of some MPS strategies and damages to particle accelerators, including unexpected events, is found in Paper I [1], where LHC, SNS, and J-PARC from Section 1.4 appear.

1.7.1 Machine Protection "Systems"

The purpose of *machine protection* (MP) is to reduce the scientific and economic losses as much as possible. The underlying task is, arguably, to optimize the happiness of the users and facility employees, meaning that machine damages that cause the users to receive failed experiments and too little data need to be kept *as low as reasonably achievable* (ALARA). On the one hand, this can be done by stopping the particle beam and adjust relevant equipment to avoid damage and downtime. On the other hand, simply stopping everything in case of *any* errant situation in such a complex facility would lead to very little operational time. Instead, MP needs to be able to handle "minor" problems while still continuing operation.

In addition to protecting equipment and avoiding unnecessary downtime, information on the *cause of the stop* can be collected for further analysis, to allow for continuous operational improvements. The "tasks" of MP for an accelerator facility can then be summarized as to [81, 82, 83]

- Protect the equipment (by taking action...)
- Protect the beam (... but not too much action)
- Provide the evidence (of what caused the stop)

Protecting the equipment means avoiding damage due to wrong behavior or configurations. Protecting the beam means that the number of *false stops* should be kept at a minimum. To provide the evidence, a so-called post-mortem system is implemented. This is a system that, in case of a beam stop, collects data on the current machine configuration, time stamps of when the event occurred, and what part of the system that sent the beam stop signal. MP uses sensors, some of them described in Section 1.6.5, to measure beam losses, current, position etc. to be able to act accordingly.

For any particle accelerator user facility, the beam is protected by ensuring it is produced, bunched, accelerated, steered, focused, and monitored (Section 1.6) to meet the goals of the facility. A repeated loss of beam would decrease the facility's reliability, availability, and user happiness. On the other side, the equipment also needs protection and a failure in meeting this could result in drastic damage and long shutdowns. These two need to be balanced to keep the machine operational as much as possible while not jeopardizing any of the delicate equipment. Thus, a facility-wide reliability and availability strategy should be complemented with a MP strategy, as a key component for the outcome.

1.7.2 Reliability, Availability, and RAMI

In addition to the demands on the equipment and the devastating beam power (as well as other beam parameters) modern accelerator-driven user facilities take on experimental availability numbers previously only seen in nuclear research reactors [84]. Long and uninterrupted operation of the equipment and systems need optimized procedures.

A specialized term for this interplay of various demands is found to be quite suitable: RAMI. The term RAMI abbreviates reliability, availability, maintainability, and inspectability. This particular grouping of concepts not only includes standard reliability and availability measures, but also pays attention to strategies for maintenance and inspection, or monitoring. By approaching the facility, or system, from all of these aspects, RAMI has become an increasingly popular concept and has been applied to state of the art facilities, such as SNS, IFMIF, and Linac4 [18, 24, 84]. The four RAMI terms are briefly described individually below.

Reliability

Reliability refers to the *probability of having continuous and correct operation within a set time interval* [85]. This time interval can vary depending on the purpose of the machine operation. Typically, one hour or one year is used, but in the case of experimental research facilities, it is just as common to use the time for one measurement, experiment, or run period. Mathematically, reliability is written as

$$R(t) = e^{-\lambda(t)t}, \quad (1.15)$$

where $\lambda(t)$ is the (constant or time-dependent) failure rate of a component or system and t is the time interval of the calculation. Another way of expressing the constant failure rate is by using the inversion

$$\lambda = \frac{1}{MTBF}, \quad (1.16)$$

where *MTBF* stands for mean time between failures. However, caution must be applied to this formulation, as the term is often confused with the actual *mean life time* of the component, which is *not* the case.

Availability

Availability is the *probability that a specific component or system (or accelerator) is operating correctly at a specific moment in time* [85]. The formula for its calculation is given by

$$A(t) = 1 - \frac{\lambda}{\lambda + \frac{1}{MTTR}} \cdot \left(1 - e^{-(\lambda + \frac{1}{MTTR})t}\right). \quad (1.17)$$

Here, *MTTR* is the Mean Time To Repair and Restore and λ is, as above, the failure rate of the system or component. After some time of operation, when the system under study has undergone appropriate adjustments and operation has become stable, the mean availability is simply defined as

$$A(t) = \frac{MTBF}{MTBF + MDT} = \frac{\text{uptime}}{\text{uptime} + \text{downtime}}, \quad (1.18)$$

where *MDT* stands for mean downtime.

Maintainability

Maintainability is a measure of the ability of a system or piece of equipment to be repaired or replaced. This means that not only the performance needs to be considered in the design phase, but also how easily accessible the equipment is and how quickly it can be replaced or repaired. Increasing maintainability keeps the downtime shorter where maintenance is required for recovery. By reducing the downtime, this yields a higher availability of the equipment and system.

Inspectability

Inspectability is related to the ability of testing, monitoring, and inspecting the equipment and systems. By allowing good inspectability, one can get a clear picture on the behavior and status of equipment and thus make appropriate judgements on how to take, or not take, action. At the same time, there is a balance between taking action when necessary to avoid downtime and testing or monitoring too much, which increases complexity that could also lead to downtime. This balance is also considered within inspectability, which provides the means required to make relevant maintenance.

Reliability and Availability for Linacs and Synchrotrons

Typically, a linac has less of a connection between reliability and availability than a synchrotron, as it has the possibility to "restart" as soon as the fault is fixed. Synchrotrons, and specifically storage rings, need to go through a ramp-up procedure where other synchrotrons and linacs have to boost the beam energy to the right level before filling the storage ring. As this thesis is mostly concerned with linac operation, this separation of reliability and availability should be kept in mind. Paper I [1] has a section where it discusses the difference in downtime between linacs and storage ring synchrotrons, and how reliability and availability are connected for these.

1.7.3 Risk Management

This chapter has described some of the challenges for modern accelerator facilities, and some of the main concepts that are associated with these challenges. Clearly, there is a demand for a systematic and robust approach that can account for the different success measures and the complexity of such modern research facilities. Beam power, beam energy, complexity, facility size, investments, and demands are ramping up. Thus, developing a holistic risk management method to deal with this has become the essential goal of this thesis.

The risk management method benefits from something of a "pre-mortem", as the counterpart of post-mortem in Section 1.7.1. This would be something that can envision unwanted events already during the facility design, take measures to reduce these, and implement them before operation starts. In the following, the ideas spawned in this introduction chapter will be put into practice in such a risk management method and later applied to ESS.

Chapter 2

Motivation of This Thesis - Technical Challenges and Boundaries

This thesis has been developed as an influential part in the MP work at ESS. It has directed the ongoing technical risk management analyses towards a cost-efficient and availability-driven design where the substantial technical risks of operating such a high beam power facility as ESS have been considered and managed. Its main contribution is the functional protection method, its lifecycle process, and the functional protection analysis technique. These are described in Chapter 4 and their application to ESS is seen in Chapter 5.

Already at an early stage in the planning of ESS, MP was identified to be a key part in the success of the facility. The amount of custom-made equipment, system complexity, and unprecedented performance output call for a necessary but challenging process that goes beyond the current standards of risk management. The technical challenges motivate a system of systems approach, as opposed to a conventional and segregated system-by-system approach, where MP makes use of *several* systems to achieve its end goal. The systems thus work together to ensure that ESS stays protected, and one system alone does not carry all of the functionality required to reach the desired level of protection. Stepping away from *one* machine protection *system* towards a strategic process that affects many systems is unique in the field of accelerator-driven facilities and the motivation for this thesis.

At the same time as MP for ESS is a facility-wide system of systems, it is important to confine the efforts within reasonable boundaries. For this thesis, these boundaries only include *global* protection. As examples, a magnet overheating due to too high supplied current or collision protection for movable devices are considered *local* protection and are thus not within the scope of MP, as addressed in the method in this thesis. This distinction is further discussed in Chapter 6, where Figure 6.1 exemplifies a local and a global protection function. A failing accelerator cavity or an inserted wire scanner during full-power beam operation are highly affecting beam losses and further damage to other equipment and are within the scope of MP. On the other side of the spectrum, completely external events outside the technical operation of the facility, such as outages in the conventional power grid or intentional (malevolent or benevolent) damage by people, are not included. By putting these statements together, and by performing the analysis for ESS presented in Chapter 5, it is found that this global protection is concerned with beam-related damages and the protection thereof. Consequently, the central node as confined within MP for ESS is the beam interlock system (BIS).

Chapter 3

Systematic Approaches to Safety, Protection, and Risk Management

Robust and reliable protection systems are necessary to successfully handle the protection-related issues described in Section 1.7. However, as they are associated with protection (of equipment) rather than safety (of humans), they are not legally required to follow a certain method or standard. Instead, their development and application is done on a case-by-case basis and vary, if at all present, between different facilities. A deeper discussion on this issue is found in Paper II [2].

Despite that the topic of this thesis is not functional safety, many approaches and features from that field are highly relevant for equipment protection. It is therefore quite useful to look into some of those standards for inspiration and guidance. Additionally, there is a set of internationally renowned risk management standards that can be applied as they stand. Finally, there are some (generally older) quantitative approaches for calculating system performance, which, combined with some (generally newer) qualitative approaches for systematic performance analysis, are well suited for the topic of protection management. This chapter will describe some of these safety and risk management standards together with a few quantitative and qualitative analysis techniques.

3.1 Functional Safety Standards

The International Electrotechnical Committee (IEC) has developed several safety standards related to electric, electronic, and programmable electronic (E/E/PE) devices and systems. The central node in this suite of standards is IEC 61508 [86], which has been the foundation for other industry-specific standards. Some of these include the IEC 61511 for process industry [87], IEC 61513 for nuclear power industry [88], IEC 62061 for machinery sector [89], and IEC 62304 for medical applications [90]. In addition to IEC 61508, the 61511 standard includes aspects that can be applied to a research facility such as a particle accelerator, where the "process" encompasses the production of particles for experimental purposes. Hence, these two standards, that are also a source of inspiration for the functional protection method and its lifecycle discussed in Chapter 4, will be discussed briefly in this section.

Functional safety, as targeted by the standards, depends on equipment or a system operating

as designed and in correct response to its inputs. The term *safety* signifies a "freedom from acceptable risk" [91], where the word *acceptable* is key. It is typically not possible to be completely free from risk, and it should not be the aim either as risk itself also generates operational benefits. However, it needs to be managed properly and needs to be kept at an acceptable level.

3.1.1 IEC 61508

IEC 61508 is a generic functional safety standard that applies to a broad range of safety systems and their design. It is used by manufacturers, designers, and suppliers that develop E/E/PE systems. The initial release of the standard was made in 1998, and the updated (and current) version came out 2010. It consists of seven parts, where the initial three are normative and the following four are informative. The standard applies to the entire lifecycle of the system, and its 16 steps, distributed throughout the system lifecycle, are seen in Figure 3.1. Steps 1 to 5 cover the concept and scope, analysis, and requirement allocation. Steps 6 to 13 implement the realization of the standard into the system design and operation. Steps 14 to 16 address the operational adjustments and decommissioning of the complete system [86].

The standard guides in how to set up a system that detects hazardous situations and activates a protective or corrective procedure, in order to eliminate or mitigate the following consequences. Any safety relying on passive systems, such as shielding or a parameter limitation, is not included in the term functional safety [91]. The functional safety system achieves its purpose through so-called *safety functions*, specifying the *sensor* that detects the hazardous situation, the *logic* that does the decision-making on what action to take, as well as the *actuator* (sometimes called final element) that performs the functionality. Additionally, the safety function often needs to fulfill a predefined timing requirement, from detection to execution, as well as a *safety integrity level* (SIL).

The applicability of the lifecycle and the clear definition of analysis steps has made parts of the standard attractive for MPS applications at accelerator facilities such as CERN and SLAC, as seen in e.g. [92, 93, 94]. Its generic approach thus makes it suitable within a broad range of analysis and functionality.

Hazard and Risk Analysis

The IEC 61508 standard accepts both quantitative and qualitative techniques for risk and hazard analyses, and also guides on a number of these in part 7 of the standard [95]. Some of these appear further down in this chapter, in Sections 3.3 and 3.4. IEC 61508 also proposes a risk ranking, in order to determine the likelihood and severity of the risks under analysis, where their combination generates a two-dimensional *risk matrix*. Such a risk matrix is expanded to encompass the method described in this thesis in Chapters 4 and 5.

Safety Integrity Levels

The outcome of the risk assessment is, through a series of steps that are described but slightly modified in Chapter 4, safety functions with targeted SILs. These SILs appear in four levels, where SIL1 is the lowest and SIL4 the highest. Depending on the SIL, the standard enforces certain processes and validation techniques to be compliant with, as well as failure rates and

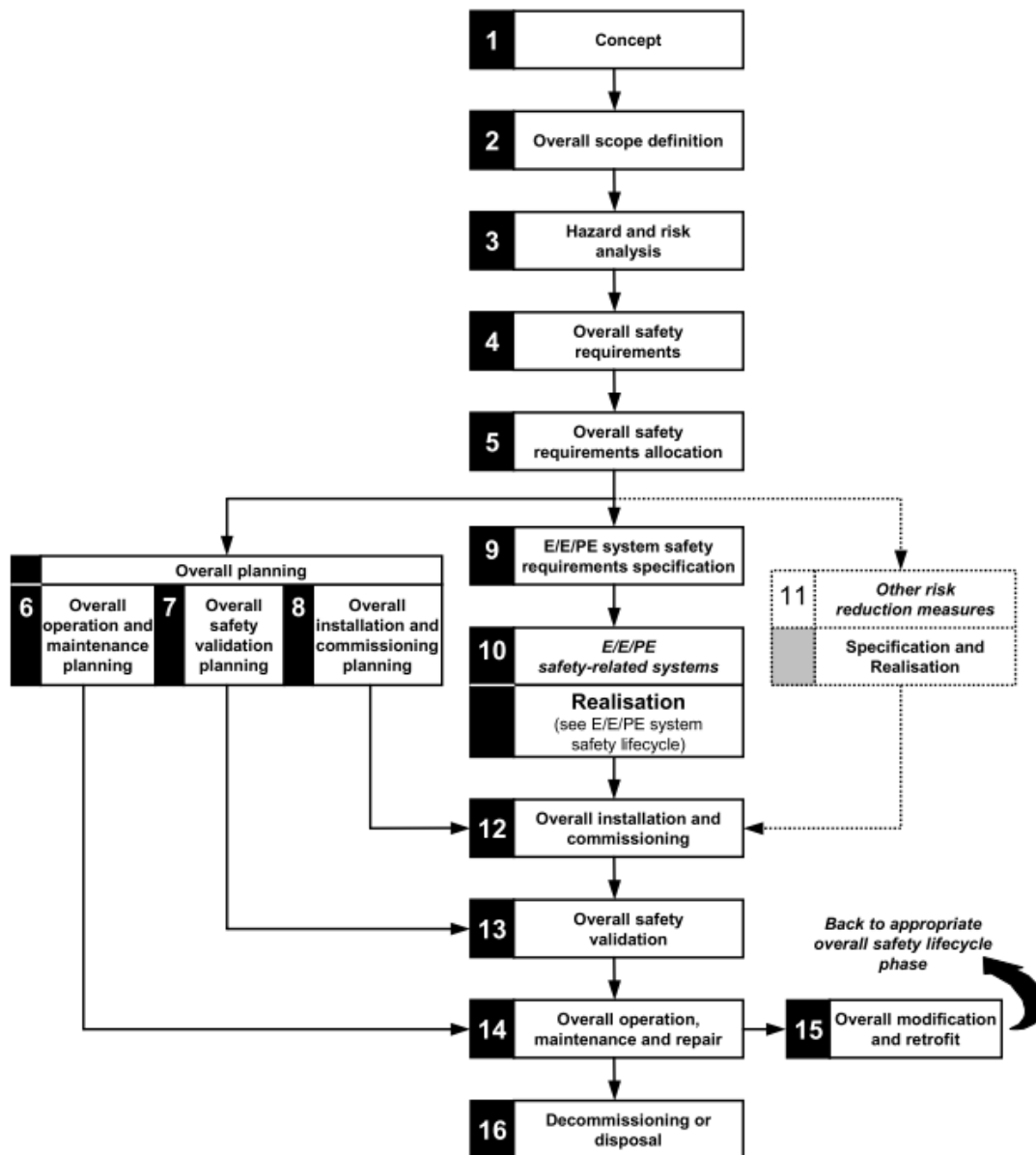


Figure 3.1: The IEC 61508 lifecycle [86].

architectural capabilities of the safety systems. These requirements, necessary for the fulfillment of a certain SIL, are described in parts 2 (for hardware) and 3 (for software) of IEC 61508 [96, 97].

3.1.2 IEC 61511

As a development based on IEC 61508, IEC 61511 deals with functional safety for the *process industry*, where the terminology and specific applications are adjusted to fit that specific industry. It initially appeared in 1996 as the ISA S84 standard, and was adapted into the IEC family in 2003. The latest updated version is from 2016. As opposed to IEC 61508, it only considers safety instrumented systems (SIS), and targets designers, integrators, and users of such safety systems [98]. For the device manufacturers and suppliers, the IEC 61508 standard still applies alone. IEC 61511 has three parts, where the first one is normative and the following two act as

informative [87].

As the IEC 61511 standard is an extension of the IEC 61508 standard, many of the key aspects are shared. The process industry, however, tends to place emphasis on *layers of protection* and their analysis (LOPA) as well as operational availability, which is recognized in the standard. IEC 61511 gives guidelines for the development of safety systems, and describes issues such as (physical and functional) separation, common cause failures, hardware reliability, and the concept of proven in use [87, 98].

IEC 61511 together with IEC 61508 emphasize that a safe (process) design is essential, and that this is the main approach to safety. Therefore, the safety mentality and its implications on the design need to be targeted at an early stage. The SIS should then reduce the remaining risks to acceptable levels, but not be the sole enforcer of this end goal. Since the process for an accelerator facility resembles that of process industries, at least on a global systematic scale, IEC 61511 is in many aspects an appropriate guideline for accelerator facilities.

3.2 Risk Management Standards

The scope of this thesis is the development and conceptual application of a risk management method. It is therefore useful to look into the generic standards that exist for risk management, especially from the International Organization for Standardization (ISO). ISO carries out the development of standards through technical committees, where each member body of interest has the right to be represented. The work is also supported by governmental and non-governmental organizations, and for electrotechnical standardization, much of the work is done in collaboration with IEC, mentioned above. Two relevant ISO standards are the ISO 31000 that contains principles and guidelines for (general) risk management and ISO 16085 that handles risk management of lifecycle processes.

3.2.1 ISO 31000

ISO 31000 is, by its scope, not specific to any industry or sector. It therefore provides generic guidelines and highlights the main aspects of risk management. Unlike the IEC standards in the previous section, the ISO 31000 is not intended for any type of certification process. Chapter 1 provides the scope and Chapter 2 is dedicated to terms and definitions, to align the risk manager with the language used in the standard. These terms, where applicable, are used within the functional protection method, as described in Chapter 4 of this thesis. More specifically, the term *risk*, as stated in Note 2 of Chapter 2.1 in ISO 31000 as a "reference to potential events (2.17) and consequences (2.18)" [99] is the key concept in the functional protection method.

Chapter 3 of ISO 31000 provides a set of principles that need to be considered when managing risk, while Chapter 4 gives the framework of risk management for different levels and contexts in an organization. Finally, Chapter 5 outlines the risk management process of communication and consultation, context, risk identification, analysis, evaluation, its treatment, and monitoring and reviewing the outcomes [99]. The process of functional protection is directly following the process defined in this standard [100], which is seen in Figure 3.2.

An important aspect in the ISO 31000 standard is that establishing a context of the risk management is critical in order to be able to target the appropriate risks. This varies between

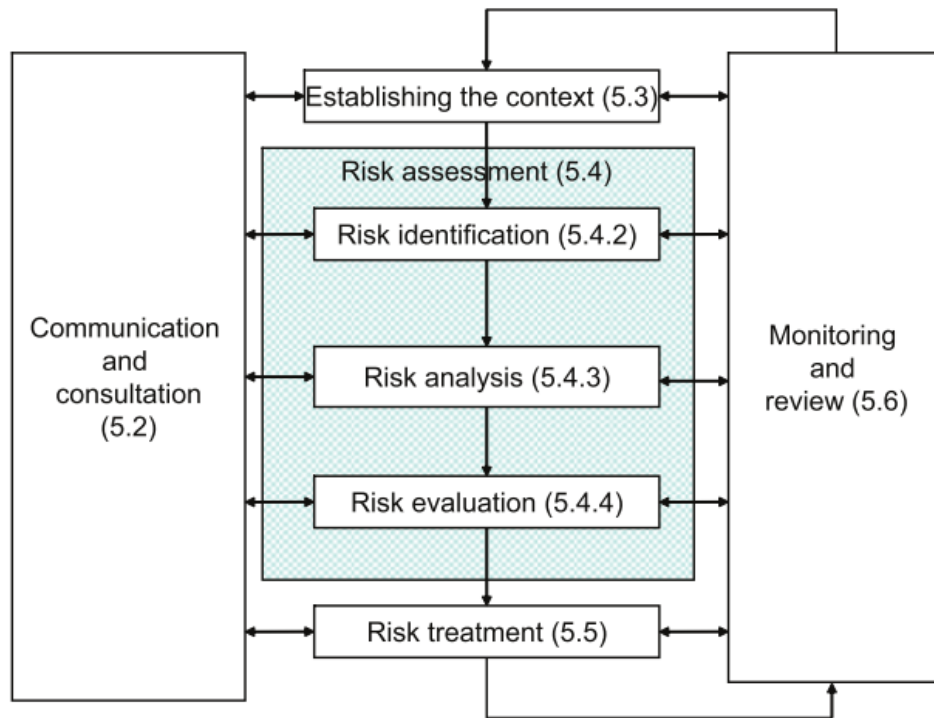


Figure 3.2: The ISO 31000 risk management process [99].

industries and facilities and cannot be generically applied to different processes. Further, risk management needs to be part of the organization, its culture, and its decision making, and cannot be a standalone process done on the side. For it to have the correct effect, it needs to be done in a "systematic, structured, and timely" manner and tailored to the context where it is applied [99]. Finally, it needs to be dynamic and iterative, and respond to the changes that are applied in the organization or system. It is therefore not something that can be done once and not re-evaluated, which ties back to the lifecycle approach found in the functional safety standards in Section 3.1.

3.2.2 ISO 16085

The ISO 16085 is a standard specified for risks within lifecycle processes. It is part of the series of standards for systems and software engineering, but can be used as standalone as found appropriate. Similar to ISO 31000, it has five chapters, however different in their appearance. The first chapter gives an overview, including the scope and purpose of the standard. Chapter 2 contains normative references, Chapter 3 definitions as they appear in the standard, and Chapter 4 is a guide on how to apply the ISO 16085 standard. Chapter 5 is describing the actual risk management process in the lifecycle, where the goal is, just as in ISO 31000 above, to identify, analyze, treat, and monitor the risks [101].

The ISO 16085 risk management process is seen in Figure 3.3, where the iterative nature of the process is shown. The standard explicitly states that the process "is not a 'waterfall' process" and Chapter 5 specifies the content of the different boxes in detail. First, the information requirements to make decisions on risk need to be specified (1), which are passed onto the

planning and implementation of the risk management (2). The project risk profile (3) includes the sum of all risk profiles and their risk states, and this information is continuously updated as needed through the risk analysis (4) and the risk monitoring (6). The outcomes for these are sent to the risk management for treatment (5). As often as required, there is a periodic evaluation of the risk management process (7), which includes all relevant feedback for improvements of the process [101].

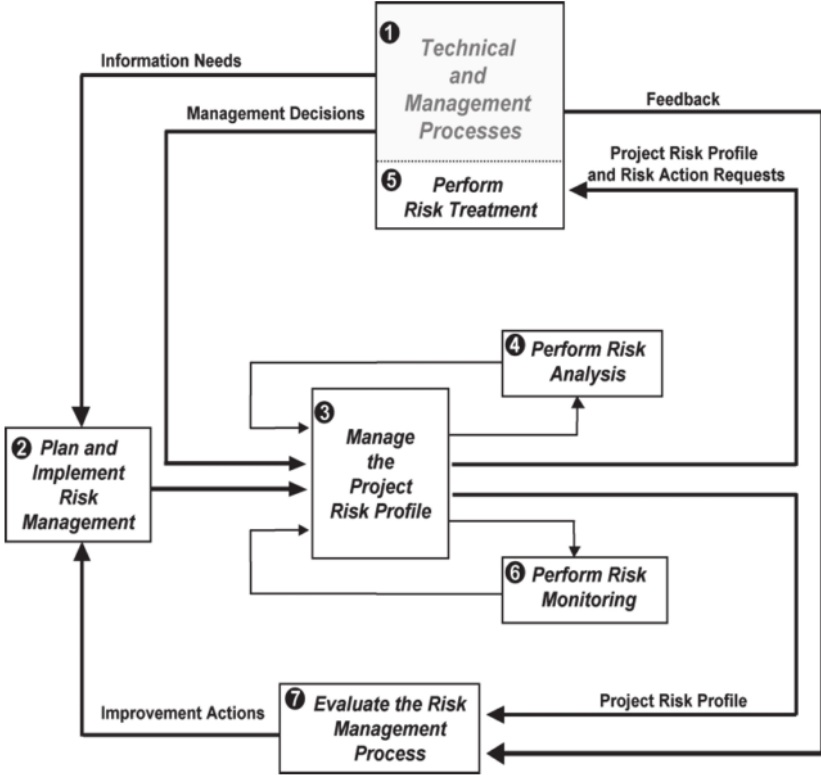


Figure 3.3: The ISO 16085 risk management process model [101].

ISO 16085 is also applied in the functional protection method, and its iterative process is found very useful in a changing organization with varying technical demands over time. Clearly, risk is analyzed and evaluated differently throughout the lifecycle of a research facility, and this needs to be honored for efficient and successful risk management.

3.3 Quantitative System Analysis Techniques

To verify whether a system design or a piece of equipment fulfills its intended quantitative requirements, several useful tools can be applied. These tools generally date back to the 50s, 60s, and 70s, and thus come with certain limitations when they are applied to modern, complex, electronic systems. Despite this, they are found to be handy for quantitative purposes and are applied at different stages during the verification of isolated system designs in the functional protection method. This section will quickly elaborate on four of the most commonly used methods. All of the quantitative techniques in this section are proposed as options within the safety standards presented above.

3.3.1 Reliability Block Diagram (RBD)

A reliability block diagram (RBD) consists of a set of blocks connected in series or parallel. A series configuration requires all of the components to function, while a parallel configuration implies redundancy and all of the blocks in parallel need to fail for the system to fail. The diagram is used to determine the reliability of a chain of components or systems depending on the individual component or system reliabilities. An example RBD, for a combination of series and parallel configuration, is seen in Figure 3.4.

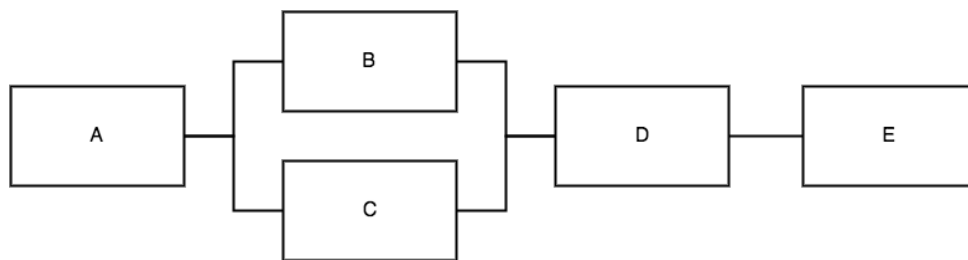


Figure 3.4: Reliability Block Diagram.

3.3.2 Fault Tree Analysis (FTA)

A fault tree analysis (FTA) looks, opposite to an RBD, on what has faulted or failed in order to determine an outcome. It is a top-down method, meaning that one first looks at a so-called *top event* and then tries to find intermediate and basic events that would lead to this top event. By building up the fault tree using these different types of events and boolean logic, one can deductively calculate how and with what probability a system can fail through the top event, based on the individual probabilities of the other events. FTA first appeared in 1962, in order to evaluate control system for ballistic missiles within the US Air Force [102]. An example of an FTA is seen in Figure 3.5, including one top, two intermediate, and five basic events.

3.3.3 Event Tree Analysis (ETA)

Contrary to FTA, event tree analysis (ETA) is a bottom-up method that aims at modeling both successes and failures. Its *forward* modeling, as opposed to the *backward* modeling of FTA, makes it suitable as the right hand side in a so-called "bowtie analysis" [103], where the FTA generates a top event and the ETA generates the possible outcomes in case of such an event. Thus, the assumption for an ETA is that the event has occurred, and one wants to find out what that might lead to. ETA has its origin in analysis of nuclear power plants, and was first introduced in 1967, however under a different name. The actual name *event tree* rather appeared in the mid 70s [104]. A simple ETA is seen in Figure 3.6.

3.3.4 Failure Modes and Effects Analysis (FMEA)

Failure modes and effects analysis (FMEA) was one of the very first structured and systematic methods for the analysis of failures. Its origin dates back as long as 1949, where it was described in the US Department of Defense document MIL-P-1629 [105]. The method has since then

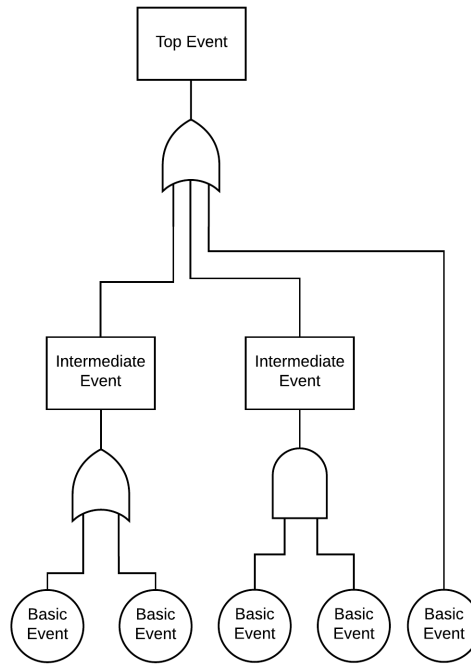


Figure 3.5: Fault Tree Analysis.

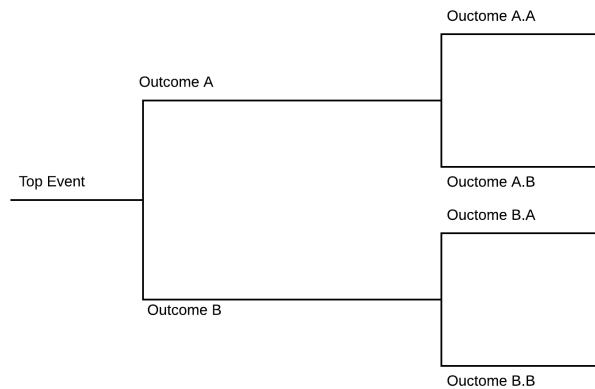


Figure 3.6: Event Tree Analysis.

developed and been applied in fields such as aerospace, automotive, and process industries. On top of the failure modes and effects, the method often includes criticality or diagnostics, or a combination. By doing this, the abbreviation sometimes includes a C for criticality, as in FMECA, or a D for diagnostics, making an FMEDA.

Despite its many versions, it is generally accepted that the abbreviation FMEA can include any variation or adjustment to it. The purpose is to analyze as many parts and components of a system as is possible and reasonable, in order to make judgements on whether there are changes that need to be made or not. The *failure mode* (a short circuit, open switch, drifting value etc.) is matched with its *effect* on the system level in an FMEA worksheet. The worksheet does not follow any specific design but can be altered for the intended purpose. Despite locating this method under quantitative methods in this thesis, which it is generally used for, it can also be a qualitative method by simply excluding the failure rates and allocation of failure mode probabilities. An example of this method is shown in Figure 3.7, where the analysis of a transistor in the ESS beam interlock system is seen.

Name	Location	Component	Supplier	Supplier ID	Component Failure Rate	References	Failure Mode	Ratio	Mode Failure Rate	Module Effect	Detection
					[1/1E9 hours]	MIL-HDBK-217F	MIL-HDBK-338B	MIL-HDBK-338B	[1/1E9 hours]	Blind, Trip	Test, Diagnostics
					Sheet-Calculator					Maintain, Negligible	Inspection, Hidden
		MOSFET Transistor			1213.83		Open Circuit	0.61	740.4	Trip	Diagnostics
Q1_P	Permit	P Channel, -4 A	Farnell	1864586RL	1213.83	6.4	Value Drift	0.13	157.8	Trip	Diagnostics
		-20 V, 0.045 ohm, -4.5 V, -600			1213.83		Short Circuit	0.26	315.6	Negligible	Hidden

Figure 3.7: Example FMEA, including criticality and diagnostics, of a MOSFET transistor for an early ESS beam interlock system version [106].

3.4 Qualitative System Analysis Techniques

As mentioned in Section 3.3, the quantitative analysis tools that are applied are typically several decades old and cannot completely cope with modern systems and their many features. Due to this, there are a few newer techniques that have been developed, mainly within an academic environment, that well suit the challenges and emergent properties of contemporary systems-of-systems and alike. Research facilities in particular often include newly developed equipment within untested systems and benefit from qualitative and systematic analyses. These techniques are not yet implemented within proven safety standards, but still tend to give a robust and systematic framework to identify weak links and unwanted system behaviors. Two of these, which have served as inspiration to the development of the functional protection method in Chapter 4, are described in this section. Additionally, the HAZOP technique, still frequently used within various genres of engineering, is described as well.

3.4.1 Systems Theoretic Process Analysis (STPA)

STPA [107] builds on systems thinking rather than component-based analysis. It takes the standpoint that a purely reliability-based theory does not cover all of the possible scenarios in complex and modern systems, typically referred to as emergent properties of the systems. Instead, one needs to apply systems theory, recognizing the whole system, in order to perform an accurate analysis. With consideration of systems theory, accidents are seen as *control problems* instead of *failure problems*. The prevention of accidents is then done through constraining behaviors and interactions for components and subsystems.

STPA consists of two steps, applied after the *control structure* has been constructed by drawing the flow of information. A simplified and generic control structure is seen in Figure 3.8. Step 1 is to identify a set of unsafe control actions (UCA) by using four specific guide words, similar to those in a HAZOP in Section 3.4.3. The guide words are

- Not providing causes hazard
- Providing causes hazard
- Incorrect timing or order
- Stopped too soon or applied too long

This is stepped through for each signal path in the control structure and for each guide word. Step 2 is to identify causal factors, meaning that the reasons for each UCA to occur are documented [85, 107].

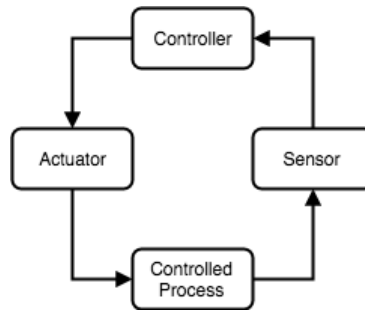


Figure 3.8: The STPA process flow from controller, through actuators acting on the controlled process, monitored by sensors and then back to the controller.

STPA has been applied in the aerospace, automotive, chemical, and medical industries, as well as for cyber-physical systems and the new Linac 4 at CERN [107, 108, 109, 110]. Its broad areas of application has made it an increasingly popular method in the past years and the method is now the topic of several conferences and workshops per year. There are also efforts to try to make it appear in some of the functional safety standards [111].

3.4.2 Functional Resonance Analysis Method (FRAM)

The functional resonance analysis method (FRAM) was developed with focus on the role of humans within technical systems, but can be applied just as well to purely technical systems. FRAM is closely related to the area of *resilience engineering* [112], and identifies that the sources of failure may in some cases be the same as the sources of success. They are claimed to be, at least metaphorically, "two sides of the same coin" [113]. The name points at the idea of resonance in the sense that everyday performance of systems fluctuate with a natural variability, and that failures are a combination of "resonating" system flaws. Hence, FRAM aims at identifying and dampening these resonances and thus provide a system design that is less prone to failures [113].

Besides the resonance concept above, FRAM has three more basic principles. One is that, at least when people are involved, but also for software and controls, things will not always be done exactly according to specifications. Depending on e.g. manpower, conflicts, resources, or information, tasks might be adjusted or fluctuating - called *performance variability*. Another principle is that one performance variability alone might not be the pure cause of an accident, but the *combination* of several of them might create emergent, rather than resultant, failures. Finally, the combination, or resonance, of some variable functions can sometimes *enforce* each other, so that the effect is larger than what would be anticipated through traditional cause and effect analyses. An example of several resonating functions, being the foundation for FRAM, is seen in Figure 3.9.

The process in using the FRAM is to follow breadth first, meaning that it is more important to understand the situation or system as a whole rather than going into details. From another viewpoint, the agenda is to rather *understand* what did *not go right* than making a claim on what went wrong. Therefore, it is important to first understand what happens in a situation where nothing goes wrong, to be able to tell that from an unwanted or unexpected scenario [113, 114].

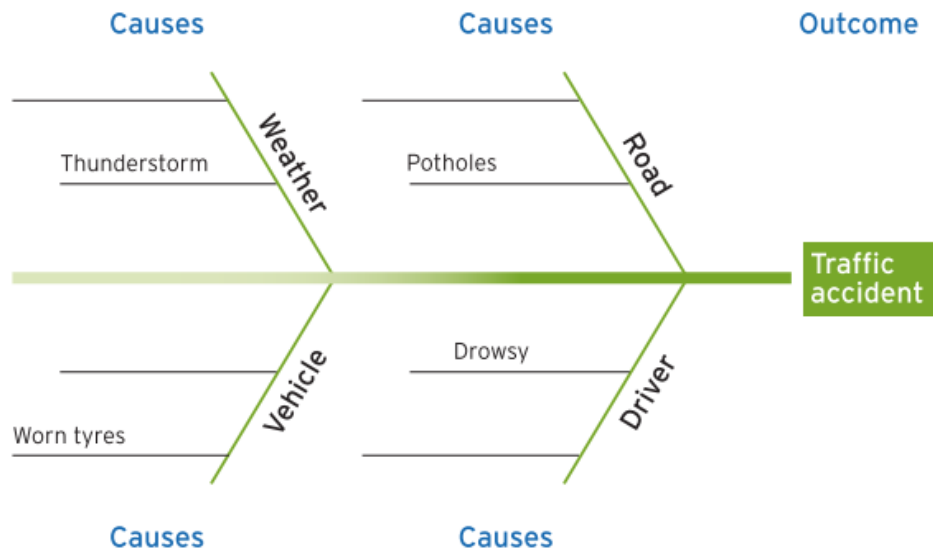


Figure 3.9: Example of four resonating functions, from a FRAM perspective, that lead to a traffic accident [113].

3.4.3 Hazard and Operability Analysis (HAZOP)

The hazard and operability analysis (HAZOP) aims at identifying and evaluating problems and hazards that are associated with a certain process or operational system. It has its background in the chemical process industry in the 1960s, but has since been implemented in all types of industry. The main focus is not to solve the problems, but rather to point them out and check them against existing safeguards and design choices. The method is applied in a workshop setting with a multi-disciplinary team and uses a set of predefined *guide words* to apply on the system and its processes.

In order to carry out a successful HAZOP, the system design needs to be mature enough to be evaluated, but should not be finalized, as the application of HAZOP might reveal flaws that need to be corrected. Each guide word, which represents a deviation from the design intent, is paired up with a system parameter and evaluated individually to find its causes and consequences on the system. While the guide words are of the form *more, less, reverse, early, before* etc., the parameters are related to *flow, pressure, temperature* and so on [115].

3.5 Discussion on Standards and Methods

The standards, approaches, lifecycles, and methods described in this chapter all construct a solid foundation for developing something like a functional protection method for complex systems. Many of the ideas and concepts within safety standards have already been seen within academic research accelerators [92, 93], and it would be beneficial to expand on these applications. Additionally, ISO has created two generic but useful risk management standards that are successfully applied in numerous areas, and implementing these in a concept for protection is both robust and direct. The functional safety standards describe a set of quantitative methods for analyzing system reliability and the consequences of failures. Those methods are typically straightforward and their applications are seen in both reliability and systems engineering. However, systems

have grown increasingly complex, and modern research facilities and particle accelerators are good proofs of this development. With this, the task of accurately analyzing the system reliabilities with all interactions and emergent properties in quantitative detail is found impossible. By approaching complex systems from both traditional device-by-device methods and newer systems-as-wholes concepts, the necessary quantitative numbers can be gathered at the same time as a holistic approach is recognized for the analysis of overall behaviors.

Chapter 4

The Functional Protection Method and Its Lifecycle

This chapter describes the functional protection method and its lifecycle for complex systems, as developed in this thesis. A description of the method and its fundamental aspects are found in Paper II [2] and its specific application at ESS is described in the ESS Machine Protection Risk Management Document [100]. The method is largely based on the standards and methods described in Chapter 3 of this thesis, and the applicability, motivation, and sources of inspiration are the many facilities and their associated risks seen in Chapter 1.

The structure of this chapter contains first a section on the rationale behind the method, its intended usage, and incentives. This is followed by a brief description on how the method was developed and which key concepts and processes that were adapted from other methods, frameworks, and standards. Next, there is a section describing the framework of the method itself, and its current scope. The fourth section outlines the lifecycle process, while the last three sections describe the different parts of this lifecycle. One of these sections (4.5) goes into more details on the functional protection analysis technique, which is used for the derivation of protection functions and their requirements.

4.1 Rationale Behind the Method

As seen in Chapter 1 and Paper I [1], modern particle accelerators are increasingly complex and require robust strategies for them to be operated without damage and with the desired availability. Due to their complexity and vast number of systems and subsystems, it is argued that these facilities cannot be analyzed and treated accurately by applying traditional reliability approaches alone. Instead, they need a system of systems (SoS) mentality as well as a recognition of the emergent and often incomplete descriptions of its complex properties [116].

The functional protection method aims at being the link between *complex systems* and *acceptable damage risk*. Following functional safety standards (Section 3.1) for protection purposes and connecting the lifecycle steps to proven-in-use risk management (Section 3.2) and analysis (Section 3.3) methods would give partial confidence in this link. Looking at qualitative analysis methods for modern systems, as seen in Section 3.4, adds yet another layer of confidence. Finally, the functional protection method is not complete without recognizing the work

done at other particle accelerator facilities [18, 20], to incorporate the best practices and lessons learned from the field.

A large portion of the background work for this thesis and the functional protection method has been done through the study of accidents at accelerator facilities and the application of functional safety standards. An important remark is that the early conceptualization and mentality of protection are important factors in order to reach success several years later, when the operational phase of the facility starts. The functional protection method has therefore placed emphasis on the *early* risk management and *continuous* interaction with system owners and stakeholders, which is described in Section 4.3. The lifecycle approach ensures that risk management is not lost at a later stage when all the design phase analyses are complete, but stays as a significant and decisive part during the whole facility lifetime.

4.2 Key Concepts and Processes

This section describes the key concepts taken from the functional safety and risk management standards, as described in Sections 3.1 and 3.2. These lay the foundation for the development of the method and are tools that help achieving fewer long operational downtimes.

4.2.1 The Lifecycle Process

The first layer of the functional protection method is the *lifecycle*, closely resembling that found in the IEC 61508 [86] and IEC 61511 [87] standards for functional safety, described in Section 3.1. For functional protection, the lifecycle is merged with the risk management process described in Section 4.2.2. The complete lifecycle is described in Section 4.4. As opposed to the safety lifecycle, the final decommissioning step is left out here, as the concern of operational availability is not affected by the method in which the facility is decommissioned. The lifecycle process ensures that all the necessary steps are followed to derive the functional behavior and to verify its implementation and follow-up. Applying the proven in use IEC standards generates an advantage in that it has been successfully applied in many different fields and industries.

The application of a lifecycle process for an actual particle accelerator is also described in [92], in this case for the LHC, which further confirms its applicability in the field. Just as in the lifecycle process for LHC, carrying out *protection* is not legally binding and can therefore omit the external certification process. The adaptation of *safety* integrity levels (SIL) into the language of protection, by calling it *protection* integrity levels (PIL) [92], is used also in this method. When matching the functional safety concept for the protection of LHC, the usage of SIL and PIL (Section 4.5.4) is somewhat dubious and typically only refers to the random failure rate aspect of the term [82, 92, 94], leaving out the systematic failures with the concepts of safe failure fraction (SFF) and hardware fault tolerance (HFT). This is adjusted for in the functional protection method, and the systematic capabilities (SC) of the protection-related systems are acknowledged as well.

4.2.2 The Risk Management Process

The second layer of functional protection is the risk management process from the ISO 31000 [99] and ISO 16085 [101] standards for risk management, described in Section 3.2. The setup for the functional protection risk management method is therefore standard compliant, with the following structural key concept from the ISO standards:

- **Establishing the (external and internal) context** describes the facility and its purpose for the users, which gives an understanding of the overall requirements and global framework for the risk analysis. It also places the risk management process into the organizational and functional context of the facility.
- **Risk assessment** is the main focus of the functional protection analysis technique, where the risks are broken down into components and matched with their respective impact on the facility. The assessment contains identification, analysis, and evaluation of risks as key steps. The work involves not only the assessment personnel but all of the relevant system owners and experts.
- **Risk treatment** applies the findings of the risk assessment into practice by documenting necessary functionality and distributing the implementation to the correct systems.
- **Monitoring and review** is fundamental in establishing confidence that the intended purposes of the risk management are fulfilled, by continuously reviewing principal aspects of the management process.
- **Recording the risk management process** highlights the traceability approach of the method and is vital to a continued development of risk management. This step should describe how and where such a recording and relevant documentation takes place.

4.2.3 Balancing Protection and Reliability

As described below, the reason for applying functional protection to an accelerator facility is to achieve a higher operational *availability*. This can be achieved through avoiding long downtimes by stopping a hazardous process before damage is caused. It is also achieved by not stopping operation unnecessarily, which is closely related to the reliability concept described in Section 1.7.2. Unnecessary stops cause less operational time in itself, but might also have the outcome of frustration and bypassing of important protection features through human intervention. Therefore, it is important to keep the balance between protection and reliability in mind.

4.3 Framework and Scope

The main intended purpose with the development and application of the functional protection method is to achieve a high *availability*, as described in Section 1.7.2. Since there is no *legal* obligation to protect equipment and facility operation, one can sometimes improve availability through slightly *relaxing* the constraints from protection. Many accelerator facilities apply the

"as low as reasonably achievable" (ALARA) approach [81, 117, 118, 119], which is a good foundation for judging whether a certain function should be implemented or whether its cost (in a broad sense) is too high. This is reflected in the risk matrix categorization in Section 4.5.1.

The functional protection method highlights the organization and the top-level objectives and requirements, seen in in the next sections, in order to tailor the method for increased availability and performance.

4.3.1 Organizational Context of the Functional Protection Method

The functional protection method and its lifecycle need to be understood by the organization that implements the requirements, operates the facility, and creates the necessary culture. Paper II [2] outlines the different organizational teams and their roles within the analysis, design, and implementation, where the three main teams are seen in Figure 4.1.

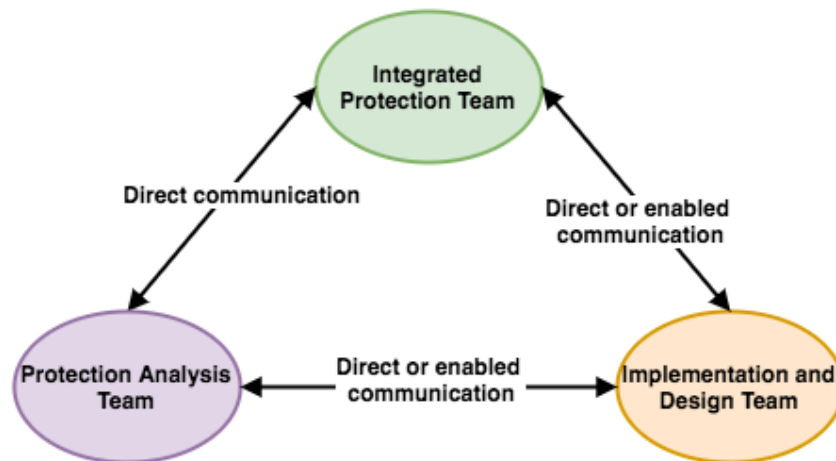


Figure 4.1: The organizational triangle for carrying out the functional protection lifecycle. The figure is taken from Paper II [2].

One needs to be aware that quantitative analyses alone, such as those seen in [3, 4, 120, 121], cannot include all of the risks associated with running a complex accelerator facility, which is discussed in [122]. Thus, the approach needs to be tuned and adjusted to recognize the role of the organization and its ability to implement the analysis findings, and also operate within the associated system limits.

Additionally, the time and resources are limited for a particle accelerator project, and carrying out tedious analyses for *all* components and subsystems is not possible. Therefore, an appropriate method should account for this and ensure that the "incomplete" analyses still make as much of an impact for protection as necessary and desired. The method should therefore allow for continuous adjustments as well as the ability to quickly identify the most pressing issues, so that those can be handled with priority. This requires good communication and understanding between the different stakeholders and analysts, and the functional protection organization (Figure 4.1) needs to be set up in a way that facilitates this interaction.

4.3.2 Objectives and Requirements

The functional protection method takes its *starting point* in the overall facility objectives and requirements. Often, these overall objectives are on a high and abstract level and need to be concretized for usability. In a particle accelerator, the performance requirements (such as beam power, accelerating gradient, magnetic fields etc.) can be distributed across the facility for each system, which is done outside the scope of functional protection and generally in a facility-wide systems engineering setting. However, the top-level performance is dependent on a reliable and available operation, which presents the objectives for a holistic machine protection approach where failures and damages need to be considered. This then becomes the objectives and requirements for the functional protection method.

The overall availability goal can be allocated to the facility subsystems, where each subsystem receives a certain unique requirement [123, 124]. As these subsystems interact with each other, it is not possible to carry out the appropriate analyses in isolation. Therefore, the functional protection analysis technique as seen below takes its starting point in the *final outcome* rather than individual failures.

4.4 The Functional Protection Lifecycle

The functional protection lifecycle is described in Paper II [2] and is seen in Figure 4.2. It includes the concept and overall scope definition followed by two parallel analysis paths. The left path in Figure 4.2 is performed by the protection analysis team (PAT) in Figure 4.1 and is described in Section 4.5, while the right path is carried out by the integrated protection team (IPT) and described in Section 4.6. The paths merge in the specification of protection functions, whose purpose, definitions, and derivations are adjusted from the safety functions described in [86] and described in detail in Paper II [2] and in [100]. The protection functions are developed and agreed upon collaboratively by the PAT and IPT together with the implementation and design teams (IDT). Once the protection function is specified, it is completely handed over to the IDT for them to implement, install, and test the functionality and quality (Section 4.7). It should be noted that several systems are often involved in implementing a protection function, highlighting the system of systems approach and stressing that the IDT in Figure 4.1 often corresponds to several system owners. During facility operation, continuous monitoring and appropriate adjustments are made in order to ensure that the functionality and quality is in place.

4.5 The Functional Protection Analysis Technique

The functional protection analysis technique is applied to the left analysis path (in purple) in Figure 4.2 and follows a detailed, top-down, and deductive analysis process. As the functional protection analysis technique has been the part of focus in the development of this thesis and the functional protection method and lifecycle, this section is more developed and detailed than the following two sections, describing the rest of the lifecycle. This section will describe and argue for the steps, assumptions, and outcomes of this functional protection analysis technique. Figure

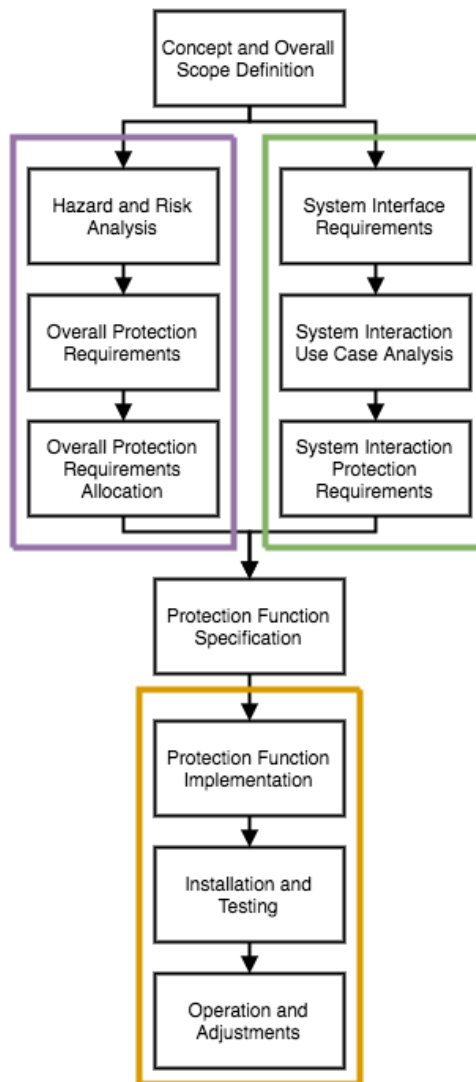


Figure 4.2: The functional protection lifecycle, as found in Paper II [2]. The colored rectangles circling the boxes correspond to the responsibilities of the matching-colored teams in the organizational triangle in Figure 4.1. The processes within the same-colored rectangles are described in Sections 4.5, 4.6, and 4.7. The non-circled boxes are carried out in collaboration between all of the teams.

4.3 displays an extraction from Figure 4.2 containing the functional protection analysis together with the concept and overall scope definition and protection function specification surrounding the left analysis path. The hazard and risk analysis and overall protection requirements are *generic* and follow a straightforward *order of magnitude mentality* through all steps. As the design, technology, and behavior of the constituent systems and equipment are difficult to verify beforehand and often lack being proven in use, this generic approach is found suitable in the protection analysis stages of the facility.

It is important to note that the process is to be carried out in an open-minded and iterative manner. The first iteration will be suitable for initiating discussions and implementations of protective measures, but is rarely the final version. It is useful to involve system experts and engineers to verify the assumptions and analyses in order to ensure that the necessary protection can actually be implemented and contains solid understanding of the systems and their behav-

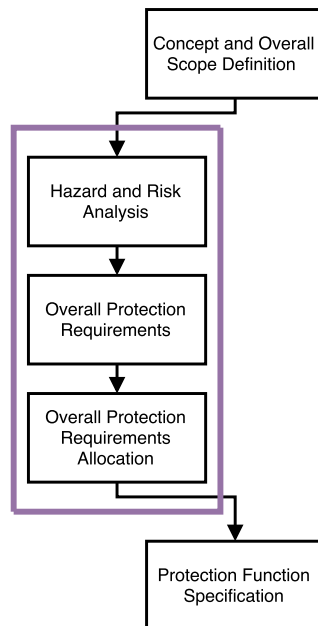


Figure 4.3: The functional protection analysis technique is applied inside the purple rectangle. The figure also contains the concept and overall scope definition above and the protection function specification below. Extracted from Figure 4.2.

ior. Common sense, good engineering judgement, and continuous communication are required throughout the analysis, as the complexity and diversity of systems within the facility differ and the appropriate approaches and measures will not be identical. Appendix B shows the 23 detailed steps of the functional protection analysis process as well as their link to the IEC 61508 and ISO 31000 standards, and a simplified overview is found in Figure 4.9 in this chapter. The process and steps of the technique are described in this section.

4.5.1 Hazard and Risk Analysis

The hazard and risk analysis is the first of the functional protection analysis technique boxes in Figure 4.3 and contains two components: the identification and analysis of *damage events* ("risks") and the following identification and analysis of *hazards* that would lead to the damage events. The damage events are evaluated depending on their consequence category, as a combination of downtime (loss of availability) and cost (loss of operational budget). This evaluation is done through two linked risk matrices. The identification and analysis of damage events and hazards are then described under the respective headlines below.

For clarity and to help guiding the reader, an example including the "thinking steps" of the functional protection analysis technique will follow the steps below. This example is located as the last paragraph of each step and is written in italics, just as this description. The example here is for a vacuum gate valve (the device itself is described in Section 5.3.1) in the normal conducting linac at ESS, that is damaged by beam if it is closed during beam operation. After the final protection function definition step in Section 4.5.4, all of the steps are summed up for an overview in Table 4.7.

The Risk Matrices

The risk matrices represent the allowed risks per damage event, as allocated from the overall facility availability requirements [85, 100]. The matrices are associated with the risk assessment bullet point in Section 4.2.2, and apply to all damage events. By combining the associated downtime and cost for a specific event, one is able to deduct a tolerable occurrence magnitude (TOM) for the event. The two risk matrices for ESS are seen in Tables 4.1 and 4.2, where the first generates a consequence (risk) category, and the second translates that category into a TOM.

In Table 4.2, the red color means that the risk is unacceptable. Measures are then required to be taken to make the risk acceptable. The green color means acceptable. If the risk is kept here, the protection is satisfactory. The orange color means undesirable, and the risk should ideally be moved to a green box. However, if the risk assessment indicates that the required measures are *not* possible or extremely costly, there is the option to decide to keep the risk in an orange box and still comply with the risk management method and system availability goals [124] as part of the ALARA concept.

		Downtime				
		< 1 h	1 h – 1 d	1 d – 14 d	14 d – 3 m	> 3 m
Cost	< 0.1 M€	Minor	Moderate	Significant	Significant	Severe
	0.1 M€ – 1 M€	Moderate	Moderate	Significant	Significant	Severe
	1 M€ – 5 M€	Significant	Significant	Significant	Severe	Severe
	> 5 M€	Severe	Severe	Severe	Severe	Severe

Table 4.1: The first risk matrix, combining downtime and cost to generate a consequence category. Taken from Paper II [2].

		Consequence			
		Minor	Moderate	Significant	Severe
Tolerable Occurrence Magnitude	TOM3				
	TOM2				
	TOM1				
	TOM0				

Table 4.2: The second risk matrix, displaying tolerable occurrence magnitudes based on the consequence category. Taken from Paper II [2].

It should be noted that these matrices are examples from ESS and need to be modified for each individual facility or system [125, 126]. The derivation of the matrices and their numbers can be quite a tedious process, and needs to be done in a collaborative effort between the facility management, the risk assessors, and the facility users [124].

Damage Event Identification and Analysis

Initially, a set of damage events are selected for each *damage device* (system or equipment) under analysis. These damage events clearly state what happens to the device as well as when or in which operational modes the damage event is relevant. Additionally, an analysis is required to specify the *cost* and *downtime* that are associated with the damage event, as given by the categories in Table 4.1. For the sake of traceability, these cost and downtime estimations require a reference to back up their categorization. These two parameters then yield a *consequence* category (see Table 4.1), which is transferred to Table 4.2 to produce a *tolerable occurrence magnitude* (TOM). The TOM is a number between zero and three and the quantitative value to be traced through the functional protection analysis technique below.

The introduction of the TOM is a helpful and straightforward tool, that both *simplifies* the analysis and creates an obvious *traceability* throughout. The simplicity in having four discrete numbers (0, 1, 2, 3) makes the rest of the quantitative analysis less error-prone and more direct. Table 4.3 matches the TOM levels with the mean time between occurrences (MTBO) and occurrence rates (OR), as they are derived for the example of ESS.

TOM	MTBO (y)	OR (y^{-1})
TOM0	5	$2 \cdot 10^{-1}$
TOM1	50	$2 \cdot 10^{-2}$
TOM2	500	$2 \cdot 10^{-3}$
TOM3	5000	$2 \cdot 10^{-4}$

Table 4.3: The underlying correspondence between tolerable occurrence magnitude (TOM), mean time between occurrences (MTBO), and occurrence rates (OR) for functional protection analysis at ESS.

The (closed) vacuum gate valve is damaged if it is hit by beam. This is then our damage event: "Gate valve is damaged by beam". The cost of a gate valve is somewhere around 15 k€, which is within the category "< 0.1 M€" in Table 4.1. The downtime associated with a damaged gate valve in the normal conducting linac (it is much longer in the superconducting linac!) is around two days. This ends up in the "1 day - 14 days" category in Table 4.1. We can then extract the consequence category "Significant" from Table 4.1. Placing this in Table 4.2 gives us a TOM3 level for this specific damage event.

Hazard Identification and Analysis

When the fully analyzed damage event is in place, the next step is to identify the *hazards*. A hazard is here defined as a situation or state that would lead to the damage event if not properly managed. In the first round, all hazards that *immediately* lead to the damage event (top-level hazards) are identified and given an *expected occurrence* (EO) rate, as they are expected to occur without any protection functionality included, but considering the basic control system and operational procedures. The EO rate is selected from three levels, as given and described in Table 4.4. The choice of EO levels is by definition qualitative, which intends to avoid a dependency on "enforced" quantitative expert estimations for hazard occurrence rates. The

choices of EO levels therefore contain *normal operation* (EO0), *facility lifetime* (EO1), and *unexpected* (EO2) as keywords. These levels are used as described in the next step and for the mode definition of a protection function in Section 4.5.4.

Expected Occurrence Level	Description	Reduction Level
EO0	Normal operation	0
EO1	Facility lifetime	1
EO2	Unexpected	2

Table 4.4: Expected occurrence rates for hazards, including their description and awarded reduction level.

The hazard identification step *might* be re-visited after the first functional protection analysis iteration, in the cases where appropriate or satisfactory protective measures *cannot* be found or implemented for the top-level hazards alone, and where *sub-hazards* are required. Note that if there is no reason to go into sub-hazards, this should be left out. If re-visiting is needed, the identification goes one level down to find sub-hazards that lead to the top-level hazards, with the intent to identify more protection functionality, targeted at these second-level hazards. For this second iteration, the analysis process follows the same steps as below also for the sub-hazards.

We identify that the damage event from above can happen due to two hazards. Either (1) we start beam operation when the gate valve is already closed (upstream of the beam destination), or (2) we operate with beam and all of a sudden the gate valve starts closing (upstream of the beam destination). These hazards are then qualitatively given an EO level. Do we expect these things to happen during "normal operation"? For the first hazard, there are plenty of starts and stops of the beam during a normal year, and gate valves are closed each time there is maintenance. Therefore, hazard 1 receives an E00 level. From the function and robustness of the gate valve system, we do not expect this for hazard 2. How about during the facility lifetime? This is quite likely as the valves would be automatically triggered to close if we have bad vacuum conditions (or due to a controller failure), and this is expected a few times during the facility lifetime. Hazard 1 then receives E00 (normal operation) and hazard 2 receives E01 (facility lifetime).

4.5.2 Overall Protection Requirements

Each hazard is assigned one overall protection function (OPF). The OPF specifies, in a *generic* way, a certain function to be implemented in order to prevent or mitigate the hazard. However, it does *not* specify the technology to be used. An example of how to phrase the OPF is given in 7.5.2.1 in IEC 61508 Part 1 [86]. Nevertheless, other phrasings might be useful depending on the purpose of the OPF. The generic feature of the OPF is important as it will prevent the analyst to be biased towards a certain solution, especially if the system is familiar to her or him. The OPF receives a FIM (functional integrity magnitude), which is calculated as the TOM of the damage event minus the EO of the hazard:

$$\text{FIM} = \text{TOM} - \text{EO} . \quad (4.1)$$

While it can now be tempting to directly translate EO levels 1 and 2 into "once every 10 years" (one order of magnitude) or "once every 100 years" (two orders of magnitude), which is sensible from the order of magnitude mentality in the analysis process, it needs to be kept in mind that detailed quantitative estimations have not been made at this stage and that the order of magnitude approach is fundamental so far.

This approach is not very different from what is described in IEC 61508 Part 5 [127], Annex F, where Section F.1.2 states that "all relevant parameters are rounded to the higher decade range". It is important to note though, that this order of magnitude approach is appropriate in the case of *few to several hazards* per damage event, but needs to be re-considered if the number of top-level hazards for a damage event approaches ten or so, as this becomes yet *another* order of magnitude and the analysis outcome would be too relaxed.

Looking at the above referenced section (7.5.2.1) of the IEC 61508 Part 1 standard, it is suggested to phrase the OPF as to prevent something. Our OPFs for the hazards above are then (1) "prevent starting beam operation when the gate valve is closed upstream of the beam destination" as well as (2) "prevent closing the gate valve during beam operation if it is located upstream of the beam destination". They should be kept as generic as that, not going into what type of technology we can use for these functions. For OPF 1, we get $FIM = TOM - EO = 3 - 0 = 3$, and for OPF 2 we get $FIM = 3 - 1 = 2$. These are the values we transfer to the following, more technology-specific, steps.

4.5.3 Overall Protection Requirements Allocation

Once a set of OPFs are defined for a certain damage event, the FIM is allocated to a set of technology-specific protection functions (PFs) and other risk reduction measures (ORRM). Depending on the analysis outcome, it is not necessary to include *both* PFs and ORRMs in the allocation of the OPF. If found appropriate, only PFs alone or in some cases ORRMs alone can be used to achieve the FIM. In the first iteration of this functional protection analysis technique, the PFs can be suggested by the analyst. However, before any further analysis proceeds or implementations are discussed, it is important to initiate continuous communication with the relevant system owners, whose systems will be either protected by the PFs or are directly involved in implementing the PFs. The allocation of OPFs to PFs and ORRMs is discussed in details in Section 7.6.2 of IEC 61508 Part 1 [86].

Other Risk Reduction Measures

An ORRM is any non-protection-related functionality that still helps in protecting the damage device. This could for example be a shielding wall, a protection-oriented control system, dedicated procedures, or sensors not directly connected to the E/E/PE protection-related system. An ORRM can be credited with a maximum risk reduction (RR) of one order of magnitude (10^{-1}) for its use to fulfill an OPF¹. This is due to that the ORRM does not undergo the same quality assurance by the PAT, IPT, and IDT (Figure 4.1) for its use, and therefore it is not possible to award it a PIL requirement (see Section 4.5.4). It is necessary to identify the available ORRMs

¹Comparable to or less than the risk reduction of a PIL0 function, see Section 4.5.4.

for each OPF before moving on to the the PF specification, discussed in the next section. This way, any functionality that is already in place to aid in the protection of the damage device is included in the analysis, which avoids unnecessary conservatism and cost.

The vacuum system gate valves do not have any other risk reduction measures associated with them. Therefore, the FIMs will be transferred as they are to the next step below.

4.5.4 Protection Function Specification

A PF is a function carried out by one or more E/E/PE protection-related systems that achieve or maintain a protected state for the damage device, referred to as equipment under control (EUC) in Section 3.5 of IEC 61508 Part 4 [128]. Most PFs require five features, or criteria, as stated in Section 3.1.1: 1) Sensor, 2) Logic, 3) Actuator, 4) Timing², and 5) Protection Integrity Level (PIL). These criteria can be identified in the first iteration of the protection analysis, or in direct discussion with the relevant system experts. While the functional protection analysis technique provides a framework for the derivation of the PFs, it is important that also system or equipment limitations are considered, as well as the proposed design architecture of the systems. As the PFs are *integrated into* the system designs, rather than standalone functions (which is typically the case for safety functions), it is necessary to apply certain pragmatism in the development of PFs and their implementation.

Protection Integrity Levels

The order of magnitude approach stays up until the allocation of PIL for the PFs. The IEC 61508 standard includes four PILs (read: SILs), named PIL1-4. As machine protection is not required to follow a stringent safety standard, an "expansion" of the PIL set is both possible and also seen in other applications of the IEC 61508 standard, such the EN 50128 standard for the railway industry [129]. Therefore, a PIL0 (zero) is useful and implemented, where the probability of failure per hour (PFH) is set to 10^{-4} to 10^{-5} , being one order of magnitude below a PIL1.

Including the PIL0 level, there are now five available PILs in the functional protection method. However, as is further discussed in Section 5.1.9 for the case of ESS, it is sometimes practical to leave out a few of the higher levels from the analysis to match the actual design and performance of protection functions. Once a PIL is allocated to a PF, an estimation is required whether the PF can reach the allocated PIL or not. If it is reachable, the included hardware is analyzed in detail to confirm this. If not, yet another analysis iteration might be necessary in order to define sub-hazards to help fulfilling the necessary protection.

The allocation of PIL follows the same order of magnitude approach as the previous functional protection analysis technique steps. This way, the remaining FIM after the ORRM risk reduction becomes the required PIL for the technology-specific PF if only *one* PF is used. Naturally, it is possible to include and combine more PFs per OPF to reach the FIM. In this case,

²The timing requirement is sometimes left out, for example where the protection function is associated with preventing something or keeping a system in a specific state. All of the other four requirements are necessary for any protection function.

the PILs of the functions are added and then the number one (1) is added on top of that³. For example, two PIL0 functions achieve a FIM1 (0+0+1=1), a PIL1 and a PIL2 function reach FIM4 (1+2+1=4), and so on. Table 4.5 gives some examples of PIL combinations and the FIM they fulfill together.

PF1	PF2	FIM
PIL0	PIL0	1
PIL0	PIL1	2
PIL0	PIL2	3
PIL0	PIL3	4
PIL1	PIL1	3
PIL1	PIL2	4

Table 4.5: Examples of how two protection functions fulfill the FIM through addition of PILs and adding the number one.

Protection Function Requirements

For the *detailed* analysis concerning probability of failure per hour (PFH) or demand (PFD) of the equipment included in carrying out the protection functions, the discrete order of magnitude levels are left aside and exact numbers are used. The difference being that the process from damage event to PF is done in a generic way, where exact hardware failure rates are typically not possible to estimate since the underlying equipment, functions, or software have not been identified. By allowing exact PFH or PFD numbers (associated with continuous or discrete modes in Section 4.5.5) for the PFs once they have received a PIL, one is able to consider and adjust for the *actual* technology to be used and can apply estimated, calculated, or proven in use numbers for the fulfillment of the function.

In addition to the failure probabilities, the protection functions have requirements on safe failure fractions (SFF) and hardware fault tolerances (HFT), as defined in Section 7.4.4.2 in IEC 61508 Part 2 [96]. All of the protection functions are regarded to contain equipment of "Type B", based on the definition of this being that "the failure mode of at least one constituent component is not well defined; or the behaviour of the element under fault conditions cannot be completely determined; or there is insufficient dependable failure data to support claims for detected and undetected dangerous failures" [96], which is applicable here. The determination of a fulfilled PIL based on the SFF and HFT appear in a matrix relation in the safety standard, seen in Table 3 of [96]. The combination of PFH, PFD, corresponding mean times between occurrences (MTBO), SFF, and HFT for the five PILs within the scope of the functional protection method is summarized in Table 4.6 below.

We now have a remaining FIM = 3 for OPF 1 and FIM = 2 for OPF 2. OPF 1 can be achieved by connecting the gate valve position switches (sensor) to a protection-verified interlock system (logic) outside of the control system. In case a gate valve upstream of the beam

³This stems from the *multiplication* of powers of ten (orders of magnitude), where the exponents are *added*. Example: 10^{-3} (PIL1) \cdot 10^{-4} (PIL2) = 10^{-7} (PIL4).

PIL	PFH (10^{-x} h^{-1})	PFD (10^{-x})	MTBO (kh)	SFF	HFT
0	4 - 5	1	10-100	< 60%	0
1	5 - 6	1 - 2	100-1000	60 - 90% < 60%	0 1
2	6 - 7	2 - 3	10^3 - 10^4	90 - 99% 60 - 90% < 60%	0 1 2
3	7 - 8	3 - 4	10^4 - 10^5	> 99% 90 - 99% 60 - 90%	0 1 2
4	8 - 9	4 - 5	10^5 - 10^6	> 99% 90 - 99%	1 2

Table 4.6: Available protection integrity levels (PIL) in the functional protection method, and their corresponding requirements. The SFF and HFT numbers appear with a matrix relation (see Table 3 in [96]) and either the top row numbers or the bottom row numbers can be selected for PIL1 and PIL4. PIL2 and PIL3 have three options for SFF and HFT.

destination that is not fully open (position switch = "NOT OPEN"), the interlock system prevents beam extraction from the ion source (actuator). In addition, there can be a PF including a position switch that reads if the gate valve is actually closed (position switch = "CLOSED"). The PIL for these PFs have to combine to reach a FIM3 or more. By following the combination of PFs in Table 4.5, we find that these two PFs can be PIL1, adding up to the desired FIM. The PFs do not require any timing requirement as they prevent beam extraction rather than change a system state. OPF 2 requires a PIL2 function, or splitting between more functions (see the section above on protection integrity levels). The latter can be achieved by having a first PF that monitors the gate valve position switches (sensor), and as soon as the valve closes, the electronics (logic) sends a "stop beam" signal through the BIS that activates the beam stop actuators (actuator). This PF receives a PIL1 requirement and a timing requirement of 500 ms, which is an approximate time before the gate valve is closed enough for possible beam impact. The last PF receives the "close" signal from the vacuum pressure monitor (sensor) into the beam interlock system (logic), and stops the beam (actuator) before the gate valve has time to close. We give this PF a PIL0 requirement and a timing of 500 ms. From above, we then achieve the FIM2 through $PIL1 + PIL0 + 1 = 2$. This step concludes the functional protection analysis technique. The collection of the damage event, hazards, OPFs, ORRM, and PFs for this example case is summarized in Table 4.7.

4.5.5 Discussion on the Functional Protection Analysis Technique

The protection analysis is done slightly differently depending on whether one considers a continuous or discrete mode, as discussed in Tables 2 and 3 in IEC 61508 Part 1 [86], for the definition of protection functions. In the functional protection analysis technique, this choice is determined based on the EO of the hazard. If the hazard is estimated as EO0, the continuous mode is selected, while for EO1 and EO2, the discrete mode is selected for the PIL. The motivation behind this is to separate the probability of failure per hour (PFH) from the probability

Damage Event	Description	Risk Category	TOM
EX-DE-1	Vacuum gate valve is damaged by beam	Significant	3
Hazard	Description	Linked Damage Event	Expected Occurrence
EX-HAZ-1	Beam operation starts when gate valve upstream of beam destination is closed	EX-DE-1	EO0
EX-HAZ-2	Gate valve upstream of beam destination closes during beam operation	EX-DE-1	EO1
OPF	Description	Linked Hazard	FIM
EX-OPF-1	Prevent beam operation if gate valve upstream of beam destination is closed	EX-HAZ-1	3
EX-OPF-2	Stop beam operation before gate valve upstream of beam destination closes	EX-HAZ-2	2
PF	Description	Linked OPF	PIL
EX-PF-1	Prevent beam operation when the gate valve position switch transmits NOT OPEN	EX-OPF-1	1
EX-PF-2	Prevent beam operation when the gate valve position switch transmits CLOSED	EX-OPF-1	1
EX-PF-3	Stop beam operation when a gate valve position switch transitions from OPEN to NOT OPEN	VAC-OPF-2	1
EX-PF-4	Stop beam operation when the vacuum pressure interlock signal transmits a CLOSE signal to the gate valve	VAC-OPF-2	0

Table 4.7: Overview of the damage events, hazards, overall protection functions, and protection functions for the example analysis of a closed or closing vacuum gate valve.

of failure per demand (PFD) for the two modes [86]. Figure 4.4 shows the analysis process for a continuous mode, where the FIM receives no reduction from the hazard EO (since it is EO0). Figure 4.5 on the other hand, shows the same process for a discrete mode, where the EO of the hazard gives a FIM reduction of 2 and 1 for the two OPFs.

In Figure 4.6, the process is shown for a damage event that includes *subhazards*. While this makes the process look a little bit more tedious, it follows exactly the same process for the subhazards and the consecutive sub-OPFs as for top-level hazards and OPFs. For overview, Figure 4.6 includes two EO1 hazards, one EO2, and one EO0.

The IEC 61508 standard emphasizes the use of independent systems for the fulfillment of the safety functions. As the PFs and protection-related systems are integrated into the existing system design, complete system independence can often not be claimed. An applied discussion of this is found in Section 5.1.1 as well as in Paper II [2]. Different PFs might use the same interlock system or actuation method, or some of the systems involved in a PF are also used for the control system or operator information, organizationally and physically outside the power of protection personnel. Therefore, the assumption of "Type B" equipment in the PF requirements, as previously discussed in Table 4.6, is accurate.

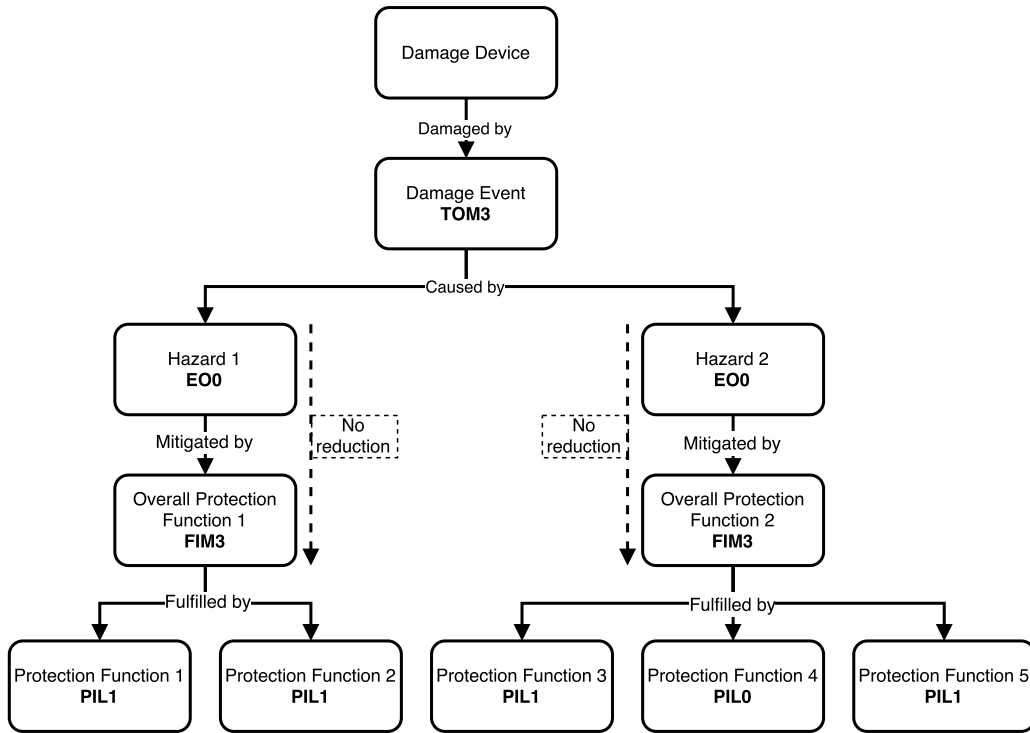


Figure 4.4: The functional protection analysis technique for a *continuous mode* hazard setup, where the hazards have been assigned an expected occurrence of EO0 (normal operation).

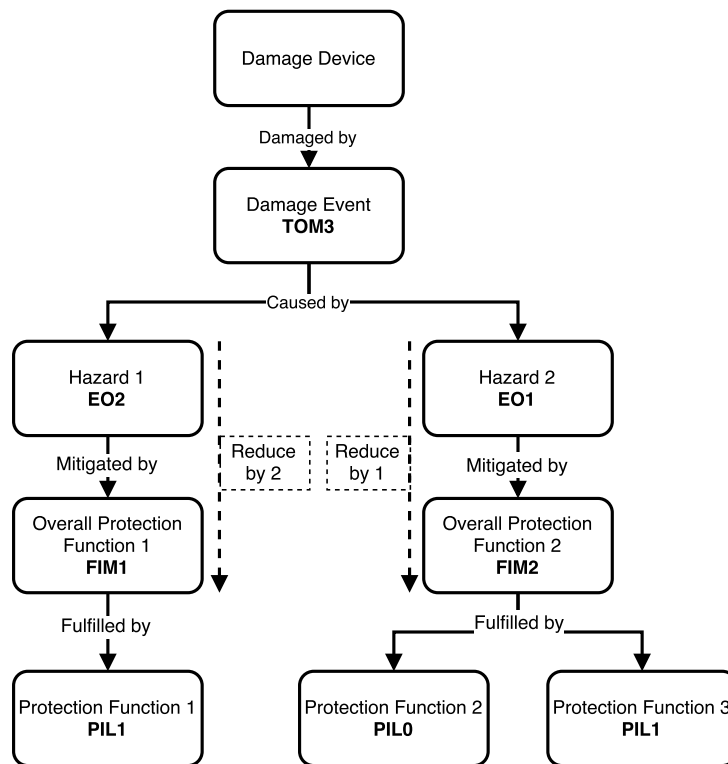


Figure 4.5: The functional protection analysis technique for a *discrete mode* hazard setup, where the hazards have been assigned an expected occurrence of EO1 (facility lifetime) and EO2 (unexpected).

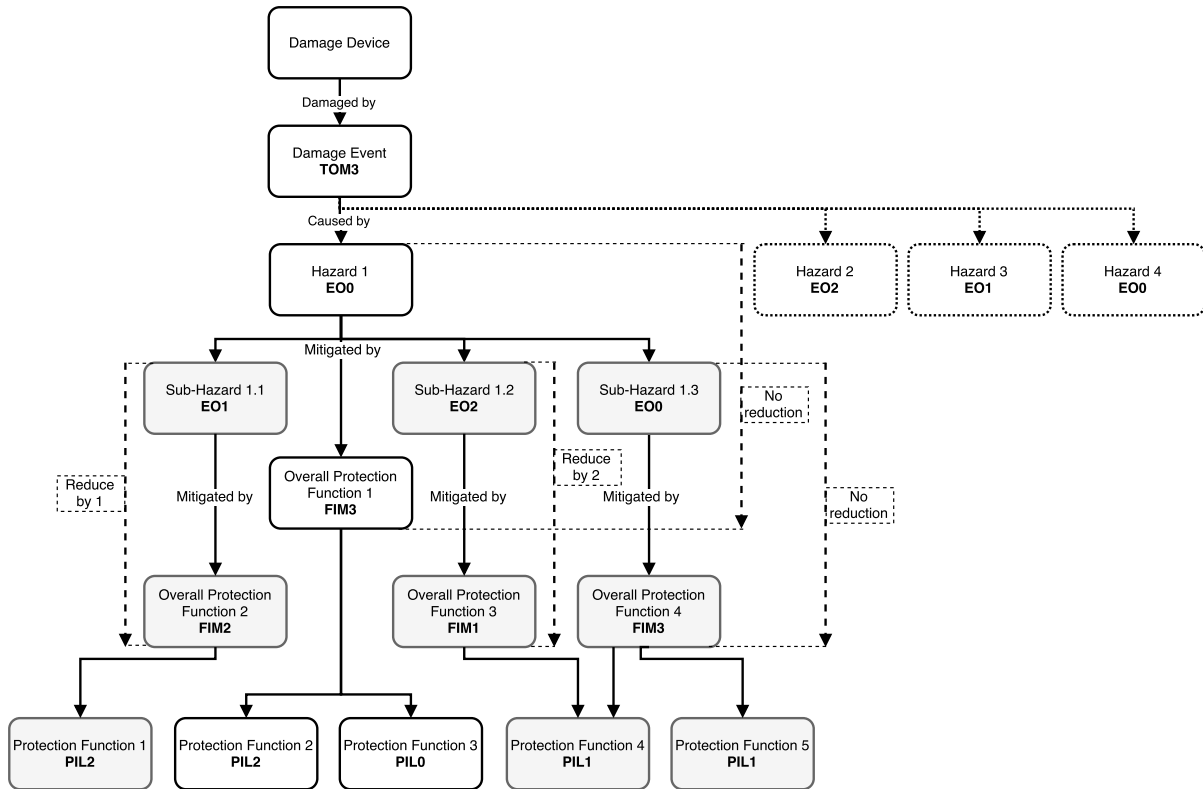


Figure 4.6: The functional protection analysis technique for a damage event with subhazards, displaying both continuous and discrete mode hazards.

The analysts need to be aware of these limitations, regardless of it being positive or negative for a certain situation. It is therefore useful to apply the order of magnitude approach where exact numbers are omitted in the favor of finite estimations, but still aiming at not "overprotecting" the system.

Further, the IEC 61508 standard deals with clear and independent chains, from accident to overall safety function and safety function. The safety engineers own all of the constituent systems and equipment, and the systems are often few and robust (in comparison to the equipment required to operate complex research facilities). This is the main difference that separates functional *protection* from functional *safety*, even though the approach is the same. However, the note in Section 7.5.1 of IEC 61508 Part 1 [86] still claims that "in application areas where valid assumptions can be made about the risks, likely hazards, harmful events and their consequences, the analysis required ... may be carried out by the developers of application sector versions of this standard", which is an indication that also the safety sector is aware of the necessity to use pragmatic "common sense" and relevant adjustments in the analyses. By keeping this discussion in mind, it is accentuated that transparency and continuous discussions are beneficial for the actual implementation of functional protection.

4.6 The Functional System Interaction Process

The functional system interaction process corresponds to the right analysis path (within the green rectangle) in Figure 4.2 and extracted into Figure 4.7. It is carried out by the integrated

protection team (IPT) in the green bubble in Figure 4.1. The process contains three main entities, being the definition of system interface requirements, the system interaction and use case analysis⁴, and obtaining the system interaction protection requirements.

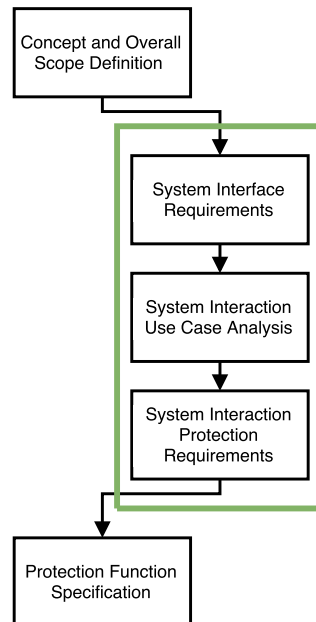


Figure 4.7: The functional system interaction process inside the green rectangle, as well as the concept and overall scope definition above and the protection function specification below. Extracted from Figure 4.2.

The system interface requirements are defined from the concept and overall scope definition (top box in Figure 4.7) for the functional protection. The key is to identify the protection-relevant systems and list the necessary interfaces for these systems.

These interfaces are then transferred to a set of system interaction use case analyses, typically in the format of dedicated workshops, where the IPT (often with the help of the IDT) go through signal paths and interactions between the systems under study in order to derive appropriate and robust solutions for the signal types and interfaces. During the use case studies, it may be identified that systems perform well as stand alone but that the signal exchange with other systems is flawed or causes a different action than expected. This analysis may also derive additional interfaces that are necessary, that are then added to the requirements in the system interface requirements box above.

The system interaction protection requirements will, similar to the functional protection analysis technique above, propose a set of protection functions. But these are defined on the system level and based on the interfaces and interactions between protection-related and other systems. This analysis path completes the picture of the protection requirements in a way that is not possible through the damage-based analysis in Section 4.5 alone.

⁴A use case analysis is a way to identify behaviors and communication links for a system, in order to derive and specify associated system requirements.

4.7 The Functional Protection Implementation and Adjustments

The last path in the functional protection analysis lifecycle is the bottom functional protection implementation and adjustments part (in the orange rectangle) in Figure 4.2. This part is carried out through the implementation and design team (IDT) in the orange bubble in Figure 4.1. As a reminder, this part of the lifecycle is extracted in Figure 4.8.

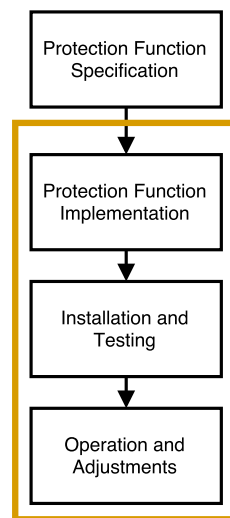


Figure 4.8: The functional protection implementation and adjustments within the orange rectangle. Extracted from Figure 4.2.

Once a set of protection functions are defined and analyzed in Sections 4.5 and 4.6 above, they need to be implemented into the protection-related designs. The design of system architectures, electronics, and firmware are naturally done by the system owners, based on the protection-related requirements given together with the protection function specifications. Before the systems are built, there should be one or more system design reviews where the IPT is present as a reviewer to ensure that the architecture and its functionality is appropriate and accepted for protection purposes.

The systems are then installed, tested, verified, and validated (through both factory and site acceptance tests) by the IDT, to verify that the systems behave as expected and that the protection-related functionality reaches the desired levels. This requires proper traceability of requirements and appropriate storage of information.

Finally, it is critical that the actual operation with the protection-related equipment and systems contains a portion of adjustments and improvements where necessary. As seen in Chapter 1, there are typically plenty of adjustments and tuning to incorporate into the early operational phases of a complex facility, and this needs to be recognized as part of the functional protection lifecycle.

4.8 Summary of the Functional Protection Method

The method described in this chapter contains a number of key steps. While these steps are seen in both standardized and less formal risk management processes, they arguably favor from a summarized outline for the work to be done in the next chapter and in future applications. Figure 4.9 displays a simplified version of the method, while the extended and detailed process is found in Appendix B.

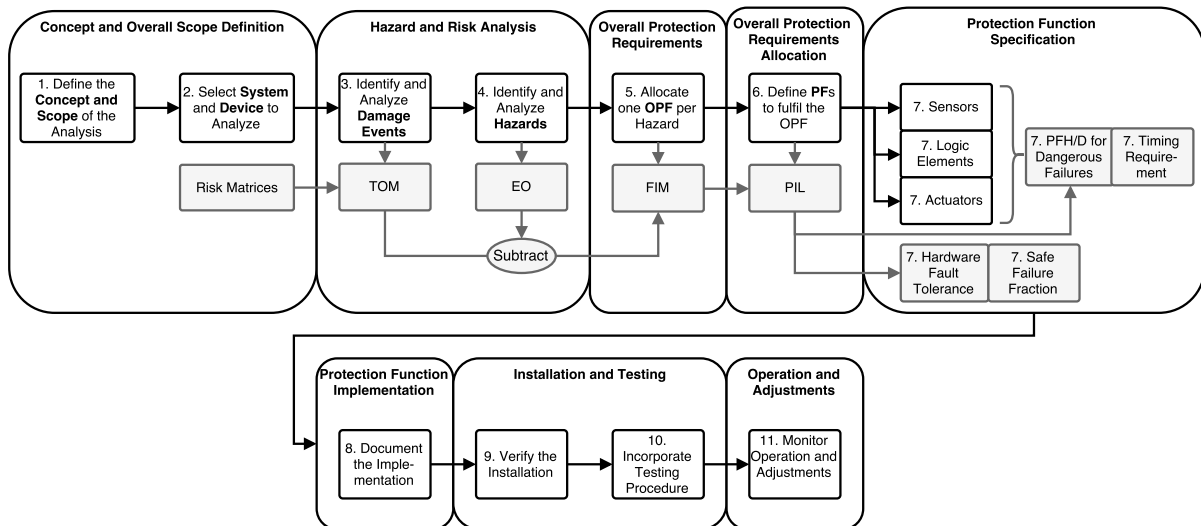


Figure 4.9: Summary of the functional protection method.

It is essential to begin by clarifying the concept and scope of the systems to be analyzed, as well as defining their end protection goal. The risk matrices are straightforward tools to apply in order to check whether something is ok (green) or not (red). After selecting a scope and system to analyze, the FPAT is applied as it is seen in Figure 4.9. Once a set of PFs are identified, they need to be detailed, implemented, installed, tested, and operational. Evidently, this is performed through an integrated organization and one person or group alone cannot carry out all of the steps for a complex research facility. The key steps are summarized in the numbered list below, which can be used for reference when reading Chapter 5 or applying the method to another complex system.

1. Define the concept and scope of the analysis, by establishing the
 - Context
 - Objectives
 - Requirements
2. Select a system and a damage device from the system to analyze
3. Identify and analyze the damage events (DE), by finding the associated
 - Cost
 - Downtime

4. Identify and analyze all immediate hazards for the DE
5. Allocate one overall protection function (OPF) per hazard
6. Define a set of protection functions (PF) to fulfill the OPF
 - If required, add more PFs to reach the FIM
 - If required, re-iterate the hazards and add sub-hazards
 - If required, re-iterate the DEs and start over with a more distributed analysis
7. Allocate the sensors, logic elements, and actuators for the PF and verify that the PIL can be achieved. Specify the required hardware fault tolerance (HFT), safe failure fraction (SFF), probability of failure per hour (PFH) or demand (PFD), and (possibly) timing requirement.
8. Document the implementation of the PF in agreement with the system owners
9. Verify the installation of the PF
10. Incorporate a testing procedure of the PF, through e.g. a dedicated verification and validation (V&V) plan
11. Monitor the operation and adjust the functionality of the PF

Chapter 5

Applying the Functional Protection Method - Proof of Concept

This chapter describes how the functional protection method and its lifecycle, described in Chapter 4, are applied to ESS. As ESS is currently under design and construction, it has not been possible to completely follow the lifecycle through to the last steps. This thesis therefore displays a proof of concept for the *first five boxes* in Figure 4.2, following the details in the functional protection analysis technique from Section 4.5. This boundary is seen in Figure 5.1. As ESS design is ongoing, the scope of this thesis contains a demonstration of how the method has been applied to the protection-relevant systems in the *normal conducting linac* as well as the *target station systems* of ESS.

Functional protection has been incorporated into the machine protection (MP) strategy at ESS, which means that the scope definition and analyses are carried out, organizationally, by the MP team. The development of the functional protection method has thus been running in parallel with the development of the MP team, both in terms of technical responsibilities and staffing. This has been successful and the method is now applied and completely integrated into the design of the ESS machine protection system of systems (MP-SoS).

To put the application and proof of concept into context, the chapter starts with outlining MP at ESS and its role at the facility. Some concepts are taken from other facilities, seen in Section 1.4, while some concepts are new. This is followed by the application of the functional protection method for the normal conducting linac and target station systems at ESS, where the analyzed systems are briefly described in the respective sections. The functional protection analysis process, up until the protection function specification, as well as the usage of the MP-SoS risk register tool are portrayed in the next section. The two following sections describe the functional system interaction process and functional protection implementation and adjustments for ESS. Finally, the last section shows on the availability and cost impact that functional protection has at ESS.

5.1 Machine Protection at ESS

ESS identified the need for a robust MP strategy early in the design phase. The unprecedented beam power, high investment costs, and stringent availability requirements were main drivers

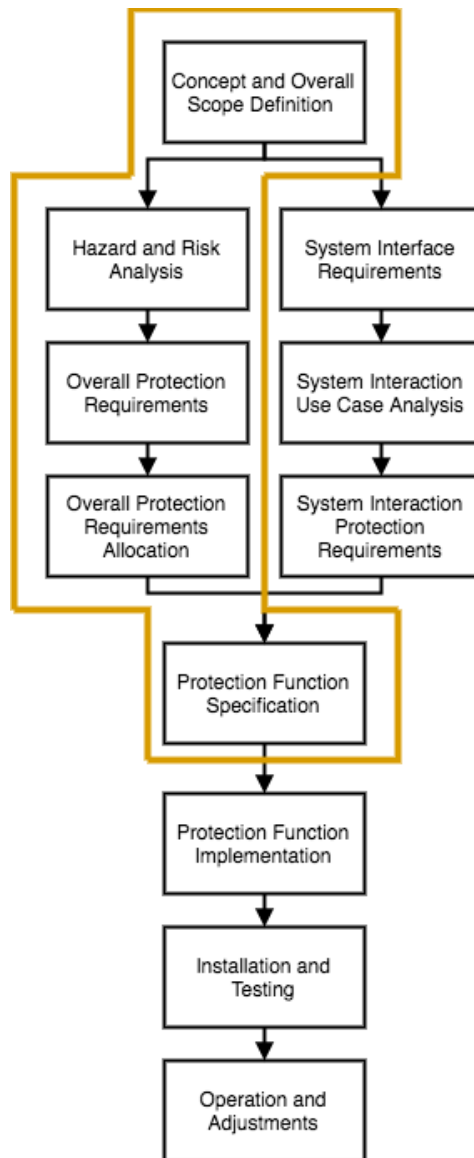


Figure 5.1: The functional protection lifecycle with the boundary for this chapter’s application in orange.

for this need. MP at ESS therefore considers these features by keeping close discussions and recurring meetings with the different system owners.

The key concept for ESS MP is the system of systems (SoS) approach [130], as required from the physical layout and diverse systems. The central system of the ESS MP is the beam interlock system (BIS) [131, 132], which is a fast and distributed logic solver system that takes sensor inputs from the protection-relevant systems as well as the ESS timing system, and generates outputs for the actuation systems and the same timing system [133]. These concepts and behaviors are described in this section and seen in Figure 5.2.

5.1.1 System of Systems

The ESS MP consists of five identified system classes, being the (local) protection-related systems throughout the facility, the proton beam monitoring systems, the beam interlock system

(BIS), the beam stop actuation systems, and the MP management systems [130]. Referring to the requirements of a system of systems (SoS), discussed in Paper II [2] and [116], the ESS MP-SoS complies with this category. This means that the system classes operate together to carry out more complex tasks and achieve the two main goals of the MP-SoS [130]:

- Prevent and mitigate damage to the machine in any operating condition and lifecycle phase in accordance with beam and facility related availability requirements.
- Protect the machine from unnecessary beam-induced activation having a potential to cause long-term damage to the machine or increase maintenance times in any operating condition and lifecycle phase in accordance with beam and facility related availability requirements.

5.1.2 The ESS MP-SoS Layout

The MP-SoS is spread geographically over more than 600 m of accelerator, target station, and neutron science instruments. An overview of the constituent systems, as mentioned in Section 5.1.1, is seen in Figure 5.2. It should be noted that the protection-related systems for accelerator, target, and neutron science are in fact multiple systems in themselves, as can be seen on e.g. page 15 of [130].

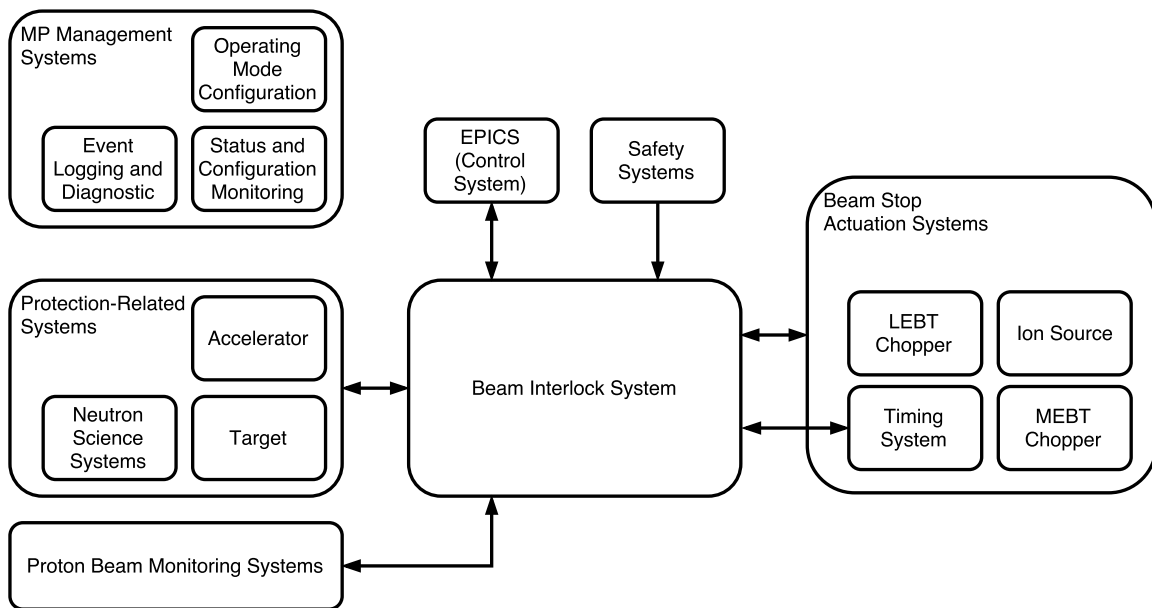


Figure 5.2: The ESS MP-SoS layout including the protection-related, proton beam monitoring, beam interlock, beam stop actuation, MP management, control, safety, and timing systems.

5.1.3 Reliability and Availability Requirements for ESS

To reach the ESS availability requirements, the system reliability plays a role, as defined in Section 1.7.2. The ESS goal is to reach 95% operational availability during the steady-state operation of the facility, and MP needs to be a significant player in avoiding too long and too many unplanned stops. Table 5.1 is taken from [123] to show an example of the number and

length of operational stops in respect to neutron production at ESS. These numbers are then translated into the risk matrices in Tables 4.1 and 4.2 to generate one of the two (cost is the other one) factors for the consequence level of the risk.

No-beam Duration	Maximum Occurrence
1 second - 6 seconds	24000 per year
6 seconds - 1 minute	8000 per year
1 minute - 6 minutes	1000 per year
6 minutes - 20 minutes	350 per year
20 minutes - 1 hour	100 per year
1 hour - 3 hours	33 per year
3 hours - 8 hours	17 per year
8 hours - 1 day	6 per year
1 day - 3 days	2 per year
3 days - 14 days	1 per year
14 days - 3 months	1 in 5 years
3 months - 10 months	1 in 100 years
more than 10 months	1 in 500 years

Table 5.1: ESS requirements for the maximum number of beam stops, and their no-beam duration [123].

5.1.4 Fast Beam Interlock System

The beam interlock system (BIS) at ESS is designed from customized electronics to meet the stringent response time requirements on the scale of microseconds (see Section 1.6.6). In addition to the response time requirements, the BIS needs to have a high reliability, both in terms of *blind failures* (missing to stop when requested) and *false trips* (stopping when not requested). The main purpose of the BIS is to verify whether or not all relevant systems are ready for beam operation. If they are, the BIS allows beam operation. If they are not, beam operation is inhibited or prevented. These requirements, as well as the results for an early design of the BIS, are discussed in [120]. To meet the BIS requirements, field programmable gate arrays (FPGA) are used to combine the input signals and produce a binary output signal to the actuation systems, described in Section 5.1.6.

The BIS is thus a *logic solver* element for all protection functions at ESS that are related to *stopping the beam*. It is the only system that is completely owned by the MP team and it has a central role in the MP-SoS. As is seen in Figure 5.2, the BIS receives a large number of inputs from the different proton beam monitoring and other central systems, and sends outputs to the beam stop actuation systems. These inputs and outputs are briefly described below.

Input Signals

The input signals for the BIS consist of beam permit, operational status, and health information signals from the MP-related systems required for beam operation, such as the systems analyzed in Section 5.3.1. This category also includes the safety systems as seen in Figure 5.2, as well

as the software control system EPICS¹. As the timing system is the system that broadcasts the different modes of the machine, it is a critical input to the BIS as well. There might also be other relevant signals as inputs to the BIS that will be defined at a later stage. In addition, the MP-related systems will send their mode configuration, to be matched with the (requested) mode sent to the BIS through the timing system. The MP-related beam monitoring systems in Section 5.1.7 send signals about beam losses, beam parameters, and whether the beam reaches its intended destination or not. Finally, the interceptive devices and vacuum gate valves provide information about their (open or closed) positions [131, 132].

Output Signals

The output signals of the BIS have the purpose to inhibit or stop the proton beam when necessary. There are three different "types" of beam stop mechanisms, being the beam inhibit, regular beam interlock, and emergency beam interlock. The beam inhibit occurs if a beam stop is requested (input signal changes to "not ok") in between beam pulses. The BIS then sends a signal to the timing system to prevent its delivery of beam pulses, and as a precaution stops the ion source and activates the LEBT and MEBT choppers. The BIS initiates the regular beam interlock if a beam stop is requested when there is a beam pulse already injected in the accelerator, that needs to be stopped immediately. The regular beam interlock mechanism contains the same procedures as the the beam inhibit, with one signal being sent to the timing system and one to activate the choppers, but in addition also interlocks the ion source proton beam extraction. Finally, as is described in Section 5.1.6 below, the emergency beam interlock takes place if the two former beam stops are unsuccessful. This interlock interrupts the power to the ion source plasma generator and proton extraction systems [132].

5.1.5 ESS Timing System

The ESS timing system is the "heartbeat" of the facility that delivers information to all of the equipment related to the beam. The timing system makes sure that the facility equipment is synchronized and generates time-stamped signals to define when and how a beam pulse is to be produced. It is the system to trigger beam injection for the ion source, as well as the signal that indicates that beam is coming for the linac magnets and RF system to ramp up and produce the required magnetic and electric fields, respectively. The timing system also distributes the different operational modes, setting the requirements on beam parameters and beam destination for the accelerator equipment.

The MP-SoS naturally needs to interface with this timing system. This is done as an *input* for the BIS to verify that the equipment is configured as expected, such as for mode consistency checks, and as an *output* (actuator) for the BIS to prevent the extraction and acceleration of beam (pulse inhibit) in a hazardous situation.

¹EPICS stands for Experimental Physics and Industrial Control System and is the facility-wide control system framework at ESS and many other research facilities [134].

5.1.6 Beam Stop Actuation Systems

To stop the proton beam in case of a non-nominal situation, ESS MP will implement a set of beam stop actuators, as briefly discussed in Paper III [3] and Section ???. These include inhibiting the timing system signal that produces the beam pulse, interlocking the ion source beam extraction, activating the MEBT chopper to deflect the proton beam into an absorber, and activating the LEBT chopper, which also deflects the beam into an absorber. The additional emergency beam stop actuation mechanism completely cuts the power to the ion source plasma generation and proton beam extraction mechanism. The emergency beam stop is only used in case the (regular) ion source actuation process is unsuccessful.

The timing system, described in Section 5.1.5, is the system that produces the signal to extract beam from the ion source. By inhibiting this signal, the extraction of the next beam pulse(s) will be interrupted.

Interlocking the ion source beam extraction is done through a dedicated beam interlock input, which interrupts the extraction of protons from the ion source.

By activating the MEBT chopper, the proton beam is steered towards a titanium-zirconium-molybdenum (TZM) absorber which can withstand about 0.2 ms of full-current beam. The reaction time of this deflection is a mere 10 ns, which allows for stopping the beam quickly.

Activating the LEBT chopper permanently deflects all of the inserted beam towards its copper absorber, which can take all of the beam at maximum current. The reaction time of the LEBT chopper is some 300 ns.

5.1.7 Beam Monitoring Systems

To be able to tell if the machine runs as it should and that the beam follows its correct path, a sophisticated beam monitoring system is needed. Within the scope of MP, the monitors include beam loss monitors (BLM), beam current monitors (BCM), and beam position monitors (BPM), as described in Section 1.6.5. There are also other *monitors* present throughout the accelerator facility that monitor the different system process variables and the equipment status, but these belong to the respective systems and are therefore managed by the MP stakeholders.

The BLMs detect beam losses along the linac and send a corresponding signal to the BIS to stop the beam in case the losses exceed the pre-defined limits. The BCMs are used for two purposes: one is to perform differential measurements by comparing the beam current at two different locations, in order to detect if any particles have been lost in the section between the two monitors; the other is to detect whether there is beam or not at the location of the monitor, to ensure that the beam reaches its intended beam destination and is not transported further (or is lost earlier). The BPMs are used to monitor whether the particle beam has the correct shape, position, and size, to allow for the BIS to take appropriate action in case the beam is incorrect.

5.1.8 Post-Mortem System

MP also contains a post-mortem system that collects information on the machine states at the time before and during a beam stop. It is thus possible to continuously identify non-nominal conditions and improve the performance of the machine over time. The usage of a post-mortem system has proven extremely useful in recent accelerator facilities [78, 82, 135].

5.1.9 Protection Integrity Levels at ESS

As the work has proceeded with the application of the functional protection method to derive protection functions (see Section 4.5.4) at ESS, the demand to integrate equipment that would not achieve the PIL1 requirements, but still contribute to the protection of the facility, is apparent. This equipment, which could encompass e.g. non-certified logic solvers and generic COTS² equipment, have then been included in PIL0 functions.

The tough and costly demands on the equipment and systems necessary to achieve the two highest PILs, PIL3 and PIL4, have caused the ESS MP-SoS to avoid these two levels, either through *re-design* or *multiple risk treatments*. This makes it possible to avoid e.g. safety PLCs as necessary logic elements of protection functions, avoid impractical redundancies (such as safe failure fractions above 99% and hardware fault tolerances above 2), and make use of non-safety classified sensors. In addition, the required pragmatism also grasps that the beam stop actuation systems and BIS at ESS would not be able to cope with a PIL higher than 2. Table 5.2 summarizes the available PILs at ESS and their inherent PFH, PFD, MTBO, SFF, and HFT requirements.

PIL	PFH (10^{-x} h^{-1})	PFD (10^{-x})	MTBO (kh)	SFF	HFT
0	4 - 5	1	10-100	< 60%	0
1	5 - 6	1 - 2	100-1000	60 - 90%	0
				< 60%	1
2	6 - 7	2 - 3	1000-10 000	90 - 99%	0
				60 - 90%	1
				< 60%	2

Table 5.2: Available protection integrity levels (PIL) for the ESS MP-SoS, and their corresponding requirements. For the SFF and HFT, either top row or the bottom row numbers can be selected for PIL1. For PIL2, the same holds but with three options.

The numbers seen in Table 5.2 then need to be allocated to the different constituent systems within a PF. While the SFF and HFT applies to all parts of the PF, the PFH (or PFD) needs to be accurately distributed among the sensors, logic, and actuators. From the layout of the MP at ESS described in this section, this allocation is done as seen in Figure 5.3, being that 70% is given to the sensors, 10% to the logic systems, and 20% to the actuator systems.

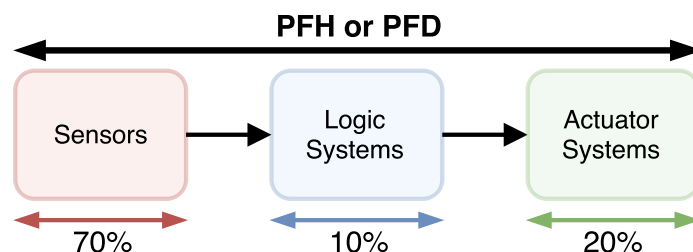


Figure 5.3: The allocation of protection function PFH or PFD for the sensors, logic systems, and actuator systems at ESS.

²"Commercial Off The Shelf", as opposed to custom-made equipment.

5.2 Concept and Scope

This section considers the first box in Figure 5.1 and defines the boundaries for the functional protection method for ESS. The concept is, as described in Section 5.1 above, concerned with MP of the facility.

Within the scope of this thesis, each system in the *normal conducting linac* and *target station systems* related to MP has been analyzed. These systems are briefly described under the respective headline below in this section. The superconducting linac and the neutron science systems at ESS have *not* yet had this method applied to them and are therefore not considered in this chapter.

The identification of damage events, as part of the hazard and risk analysis described in the next section, has been done on a system by system basis. The relevant damage events are related to the following damage sources: the proton beam, radiation, electrical, or thermal. All of these damage sources are concerned with how the systems are affected by *external* sources. Internal failures due to e.g. failing components are not treated in this analysis and are delegated to the system-specific RAMI analyses. Only damages that fit accurately within the risk matrix in Table 4.1 are analyzed. This means that very small damages and degradations that are confined within the everyday operation of the facility are omitted as well.

5.2.1 Normal Conducting Linac Systems

The normal conducting linac corresponds to the first 48 m of the ESS linac and consists of an ion source, LEBT, RFQ, MEBT, and DTL. The purpose is to create a high quality proton beam that is ready for further acceleration in the superconducting linac, by carrying out the five main functions listed in Section 1.6. For this, the vacuum system, linac magnets (focusing and steering), interceptive devices (that enter the beam pipe and intercept the beam), and buncher cavities are identified as protection-related. These systems are described in the introduction to their analyses in Section 5.3.

5.2.2 Target Station Systems

The target station systems support the production and moderation of neutrons for the experimental stations by keeping the tungsten target wheel cooled and in the correct position (XYZ alignment directions and rotation), as well as ensuring sufficient cooling of the neutron moderators and reflectors. The target wheel is cooled by a helium system, the moderators have one hydrogen and one water circuit, and the reflectors have a water circuit similar to that of the moderators. The setup of the target station systems within the so-called target monolith vessel can be seen in Figure 5.4. Just as above, these systems are described in the introduction to their analyses in Section 5.3.

5.3 The Functional Protection Analysis at ESS

The functional protection analysis technique that is applied in this section is described in Section 4.5 and corresponds to the purple rectangle in Figure 4.2. It involves a hazard and risk

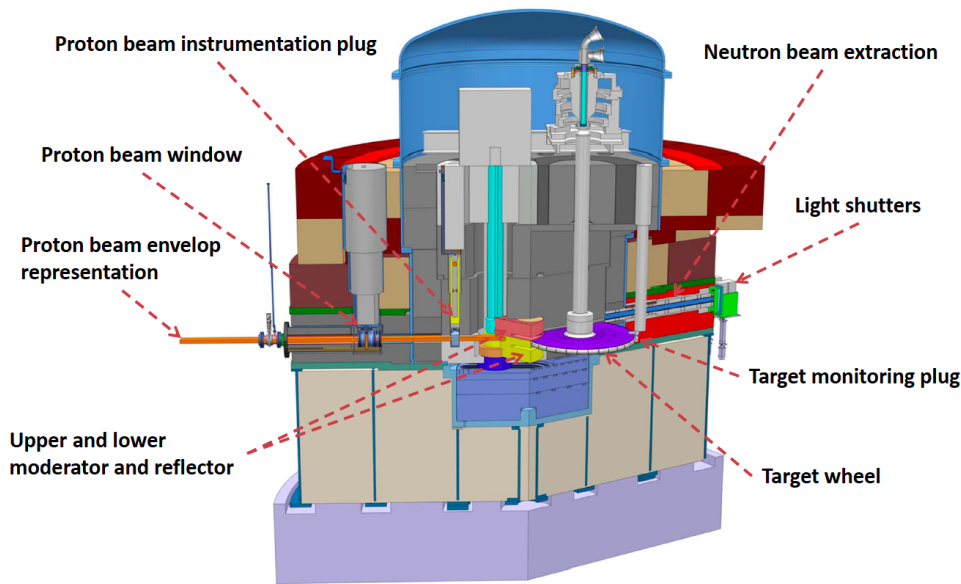


Figure 5.4: The target station systems and their locations in the target monolith [136].

analysis, overall protection requirements, and overall protection requirements allocation, and is managed by the PAT (purple bubble) in Figure 4.1. Additionally, the analysis is concluded with a definition of a set of protection functions that are traceable back to the initial damage events for the system.

5.3.1 Hazard and Risk Analysis, Overall Protection Requirements, and Overall Protection Requirements Allocation

As the functional protection analysis technique is carried out in an iterative manner, the first analysis was done by the PAT (see Section 4.3.1) alone, followed by a discussion with the system owner(s) for a second analysis iteration. This is then what is presented in this and the following section of the chapter.

The analyses and results in this section are presented in Paper III [3] and Paper IV [4], and their corresponding graphical analysis flowcharts are found in Appendix C. An example of such a graphical flowchart for the vacuum system is given in Figure 5.6 and the rest are placed in the appendix. This section will identify and analyze the damage events, hazards, OPFs, and ORRMs of the systems. These are listed, together with the derived PFs (Section 5.3.2) for overview and completeness, in Tables 5.3 to 5.11. All of the target station systems have been analyzed internally by target personnel through dedicated HAZOP workshops (see Section 3.4.3), and the MP analysis is thus based on the outcome of these workshops. Figures 4.4, 4.5, and 4.6 in the previous chapter display the overview of the functional protection analysis technique and its allocation process.

Vacuum System

The vacuum system has the role to provide satisfactory vacuum conditions for the beam transportation, as well as vacuum shielding for cryogenic purposes in the target station and superconducting linac (which is not discussed in this thesis). In addition to vacuum pumps, it contains a

set of gate valves along the linac beam pipe in order to separate sections from each other when necessary. This could be in case of a loss of vacuum in some section or due to maintenance on parts of the linac. The locations of the vacuum gate valves in the normal conducting linac are seen in Figure 5.5. Additionally, there are two fast vacuum valves, one on each side of the superconducting linac. These close in case of poor vacuum conditions that could harm and damage the sensitive niobium cavities, and are much faster (closing in around 20 ms) than the normal gate valves (closing in around 1 s). The outcome of the functional protection analysis for the gate valves, which encompass all the damage events for the vacuum system, is presented in Table 5.3 and Appendix C. The graphical derivation of the vacuum system analysis for the normal conducting linac, as presented in Appendix C, is also seen in Figure 5.6 for this system.

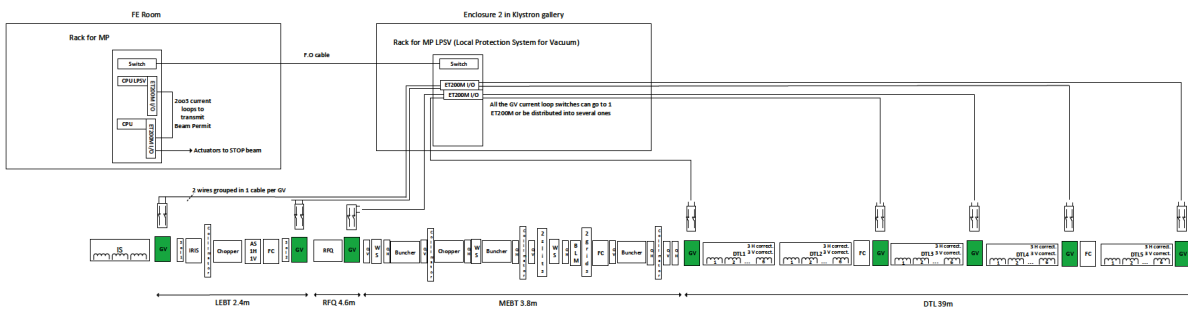


Figure 5.5: The location and connection of the gate valves along the normal conducting linac.

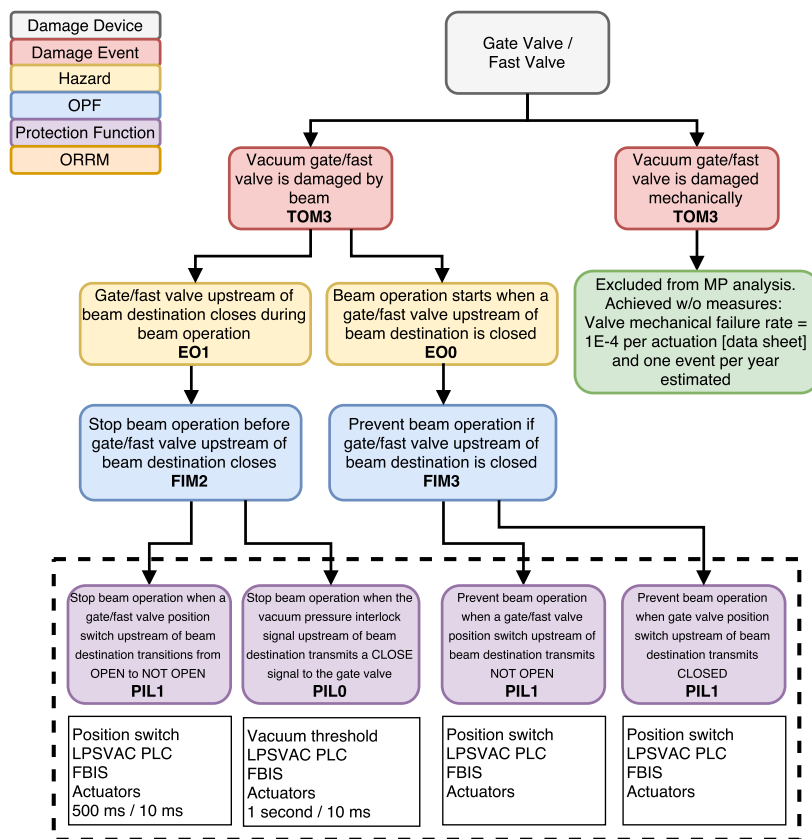


Figure 5.6: Example of the graphical derivation of the functional protection analysis technique for the vacuum (gate valve) system. The graphical derivations are all found in Appendix C.

Damage Event	Description	Risk Category	TOM		
VAC-DE-1	Vacuum gate valve is damaged by beam	Significant	3		
Hazard	Description	Linked Damage Event	Expected Occurrence		
VAC-HAZ-1	Beam operation starts when a gate valve upstream of beam destination is closed	VAC-DE-1	EO0		
VAC-HAZ-2	Gate valve upstream of beam destination closes during beam operation	VAC-DE-1	EO1		
OPF	Description	Linked Hazard	FIM		
VAC-OPF-1	Prevent beam operation if gate valve upstream of beam destination is closed	VAC-HAZ-1	3		
VAC-OPF-2	Stop beam operation if gate valve upstream of beam destination starts closing	VAC-HAZ-2	2		
PF	Description	Linked OPF	Sensor	Timing	PIL
VAC-PF-1	Prevent beam operation when a gate valve position switch upstream of beam destination transmits NOT OPEN	VAC-OPF-1	Position switch	N/A	1
VAC-PF-2	Prevent beam operation when gate valve position switch upstream of beam destination transmits CLOSED	VAC-OPF-1	Position switch	N/A	1
VAC-PF-3	Stop beam operation when a gate valve position switch upstream of beam destination transitions from OPEN to NOT OPEN	VAC-OPF-2	Position switch	500 ms	1
VAC-PF-4	Stop beam operation when the vacuum pressure interlock signal upstream of beam destination transmits a CLOSE signal to the gate valve	VAC-OPF-2	Vacuum pressure monitor	500 ms	0

Table 5.3: Damage events, hazards, overall protection functions, and protection functions for the vacuum system (gate valves) at ESS.

Linac Magnets

The linac magnets in the normal conducting linac, as analyzed in this thesis, consist of eleven focusing quadrupole magnets, combined with dipole steerer magnets located inside of the quadrupoles. All of them are located in the MEBT and are water cooled. For completeness, there is also a set of permanent magnet quadrupoles (PMQs) and corrector magnets in the DTL. But, as these are not water cooled, nor do the PMQs have power supplied to them, they are excluded from this analysis. Table 5.4 and Appendix C outline the outcome of the analysis of the MEBT linac magnets, showing that they are susceptible to both prompt beam losses as well as slow integrated beam losses causing radiation damage. Also the water cooling system is critical as the magnets are permanently supplied with current from the power supplies.

Damage Event	Description	Risk Category	TOM		
MAG-DE-1	Magnet coil is damaged from overheating	Significant	3		
MAG-DE-2	Magnet is deformed or degraded by radiation from beam losses	Significant	3		
Hazard	Description	Linked Damage Event	Expected Occurrence		
MAG-HAZ-1	Magnet receives prompt beam losses beyond maximum limits	MAG-DE-1	EO1		
MAG-HAZ-2	Cooling water flow for magnet is below acceptable limits	MAG-DE-1	EO1		
MAG-HAZ-3	The total beam losses in the magnet are above acceptable limits	MAG-DE-2	EO0		
OPF	Description	Linked Hazard	FIM		
MAG-OPF-1	Prevent magnet temperature to increase above acceptable limits	MAG-HAZ-1	2		
MAG-OPF-2	Prevent cooling water flow in magnet below acceptable limits	MAG-HAZ-2	2		
MAG-OPF-3	Prevent beam losses above acceptable limits in the magnet	MAG-HAZ-3	3		
PF	Description	Linked OPF	Sensor	Timing	PIL
MAG-PF-1	Stop beam operation if thermostats detect temperature above acceptable limits	MAG-OPF-1 MAG-OPF-2	Thermostat	100 ms	2
MAG-PF-2	Stop beam operation and magnet power supply if cooling water flow meters detect a flow below acceptable limits	MAG-OPF-2	Current monitor	1 s	0
MAG-PF-3	Stop beam operation if differential BCM measurements detect critical beam losses ³ above acceptable limits	MAG-OPF-3	BCM	30 μ s	2

MAG-PF-4	Stop beam operation if nBLMs detect critical beam losses above acceptable limits	MAG-OPF-3	nBLM	N/A	0
----------	--	-----------	------	-----	---

Table 5.4: Damage events, hazards, overall protection functions, and protection functions for the linac magnets (focusing quadrupoles and steering dipoles) at ESS.

Interceptive Devices

Interceptive devices is a collective term at ESS for all the devices that, *on purpose*, intercept the beam in the beam pipe. Therefore, the vacuum gate valves mentioned above do not belong to this category, as they are not intended to interact with the beam. The interceptive devices are mostly used for beam parameter measurements, such as the wire scanners, Faraday cups, and emittance measurement units (EMU). The category also includes the beam stops (BS), of which some are Faraday cups, the iris for beam current adjustment, as well as the MEBT scrapers, which act as movable collimators for beam halo removal.

All the interceptive devices (except the LEBT Faraday cup, discussed in Section 5.1.6) have restrictions on the beam parameters (beam current, repetition rate, beam power) they can withstand without damage, as well as that they require proper water cooling (except the wire scanners). Due to the differences in purpose between the interceptive devices, however, the number hazards and OPFs are slightly larger than for the other systems. The wire scanners are left out from this analysis, as it was judged that their damage in the *normal conducting linac* do not require immediate mitigation, but could be replaced during a longer shutdown period. The functional protection analysis results are seen in Table 5.5 and in Appendix C.

Damage Event	Description	Risk Category	TOM
ID-DE-1	Interceptive device is damaged by beam	Significant	3
ID-DE-2	Interceptive device (EMU, BS, iris, scraper) is damaged from lack of cooling	Significant	3
Hazard	Description	Linked Damage Event	Expected Occurrence
ID-HAZ-1	Beam stop or EMU upstream of beam destination moves into the beam pipe during beam operation	ID-DE-1	EO1
ID-HAZ-2	Beam exceeds acceptable beam parameters when interceptive device is interacting with beam	ID-DE-1	EO0
ID-HAZ-2.1	Scraper blades are inserted into the beam pipe beyond acceptable limits	ID-DE-1	EO1
ID-HAZ-2.2	Beam is not correctly focused	ID-DE-1	EO0
ID-HAZ-2.3	Beam is not correctly steered	ID-DE-1	EO0

ID-HAZ-3	The interceptive device (EMU, BS, iris, scraper) cooling water flow is below acceptable limits	ID-DE-2	EO1		
ID-HAZ-4	The interceptive device (EMU, BS, iris, scraper) cooling water temperature is above acceptable limits	ID-DE-2	EO1		
OPF	Description	Linked Hazard	FIM		
ID-OPF-1	Prevent beam stop or EMU upstream of beam destination to move in during beam operation	ID-HAZ-1	2		
ID-OPF-2	Prevent beam above acceptable beam parameters if interceptive device is interacting with beam	ID-HAZ-2	3		
ID-OPF-3	Prevent scraper blades to be inserted into beam pipe beyond acceptable limits	ID-HAZ-2.1	2		
ID-OPF-4	Prevent beam focusing outside of accepted limits	ID-HAZ-2.2	3		
ID-OPF-5	Prevent beam position to be more off center than acceptable limits	ID-HAZ-2.3	3		
ID-OPF-6	Prevent interceptive device cooling water flow to be below acceptable limits	ID-HAZ-3	2		
ID-OPF-7	Prevent interceptive device cooling water temperature to be above acceptable limits	ID-HAZ-4	2		
ORRM	Description	Linked OPF	RR		
ID-ORRM-1	Do not allow unused interceptive devices upstream of beam destination to go in during beam operation	ID-OPF-1	1		
ID-ORRM-2	Restrictive scraper position-limits prevent scraper from moving past accepted limits into the beam pipe	ID-OPF-3	1		
PF	Description	Linked OPF	Sensor	Timing	PIL
ID-PF-1	Stop beam operation if beam stop or EMU position switch upstream of beam destination changes from OUT to NOT OUT	ID-OPF-1	Position switch	500 ms	1
ID-PF-2	Stop beam operation if wire scanner position switch upstream of beam destination changes from OUT to NOT OUT during beam operation above acceptable limits	ID-OPF-2	Position switch	100 ms	1
ID-PF-3	Stop beam operation if BCM detects beam above beam mode limits	ID-OPF-2	BCM	30 μ s	1
ID-PF-4	Stop beam operation if scraper charge deposition monitor detects beam charge above acceptable limits	ID-OPF-2 ID-OPF-3 ID-OPF-4 ID-OPF-5	Charge monitor	30 μ s	1

ID-PF-5	Stop beam operation if quadrupole magnets are operating outside of acceptable limits	ID-OPF-4	Current monitor	100 ms	0
ID-PF-6	Stop beam operation if BPMs detect that the beam is not correctly steered	ID-OPF-5	BPM	30 μ s	0
ID-PF-7	Stop beam operation if differential BCMs detect beam losses above acceptable limits	ID-OPF-5 ID-OPF-6	BCM	30 μ s	0
ID-PF-8	Stop beam operation if interceptive device cooling water flow sensor detects flow below acceptable limits	ID-OPF-6	Flow sensor	1 s	1
ID-PF-9	Stop beam operation if interceptive device cooling water temperature sensor detects temperature above acceptable limits	ID-OPF-7	Temperature sensor	1 s	1
ID-PF-10	Stop beam operation if EMU or iris temperature sensor detects temperature above acceptable limits	ID-OPF-6 ID-OPF-7	Temperature sensor	1 s	0

Table 5.5: Damage events, hazards, overall protection functions, other risk reduction measures, and protection functions for the interceptive devices at ESS, including beam stops (Faraday cups), emittance measurement units, beam scrapers, and the iris collimator. Wire scanners are excluded from the functional protection analysis in the normal conducting linac.

MEBT Buncher Cavities

The MEBT contains three buncher cavities that bunch the beam for optimized acceleration through the DTL and later the superconducting linac. Beam physics simulations show that only the second and third buncher cavities can be hit due to a mis-steered or unfocused beam [137], while all of them are water cooled and can experience poor cooling conditions. Due to the abrupt aperture transition when entering the buncher cavities, as seen in Figure 5.7, careful beam steering and focusing is necessary to avoid beam losses. The analysis of the bunchers is shown in Table 5.6 and Appendix C.

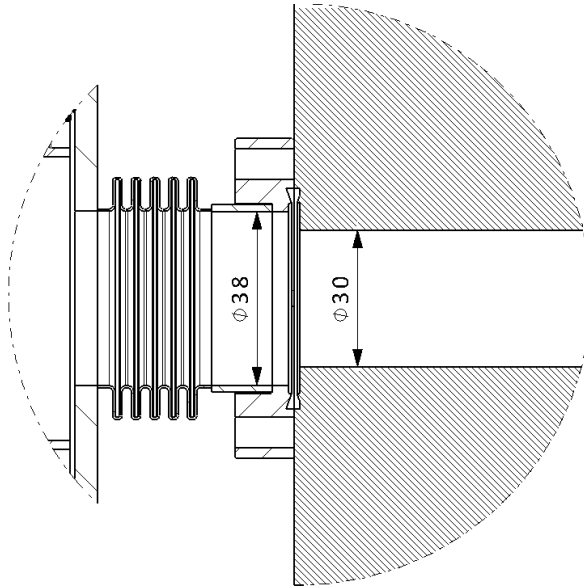


Figure 5.7: The aperture change from 38 to 30 mm in the MEBT when entering a buncher cavity, where an unfocused or mis-steered beam (coming from the left) could cause damage [138].

Damage Event	Description	Risk Category	TOM
BC-DE-1	Buncher cavity is damaged from over-heating	Significant	3
BC-DE-2	Buncher cavity (2 or 3) is deformed by critical beam losses	Significant	3
Hazard	Description	Linked Damage Event	Expected Occurrence
BC-HAZ-1	Buncher cavity cooling water flow is below acceptable limits	BC-DE-1	EO1
BC-HAZ-2	Buncher cavity cooling water temperature is above acceptable limits	BC-DE-1	EO1
BC-HAZ-3	Beam losses in the buncher cavities are above acceptable limits	BC-DE-2	EO0
BC-HAZ-3.1	Beam is not correctly steered in the MEBT	BC-DE-2	EO0
OPF	Description	Linked Hazard	FIM
BC-OPF-1	Prevent buncher cavity cooling water flow below acceptable limits	BC-HAZ-1	2
BC-OPF-2	Prevent buncher cavity cooling water temperature is above acceptable limits	BC-HAZ-2	2
BC-OPF-3	Prevent beam losses above acceptable limits in the buncher cavity	BC-HAZ-3	3
BC-OPF-4	Prevent beam position to be more off center than acceptable limits	BC-HAZ-3.1	3

PF	Description	Linked OPF	Sensor	Timing	PIL
BC-PF-1	Stop beam operation if buncher cavity cooling water flow sensor detects flow below acceptable limits	BC-OPF-1	Flow sensor	1 s	0
BC-PF-2	Stop beam operation if buncher cavity cooling water temperature sensor detects temperature above acceptable limits	BC-OPF-2	Temperature sensor	3 s	1
BC-PF-3	Stop beam operation if differential BCM measurements detect critical beam losses above acceptable limits	BC-OPF-3 BC-OPF-4	BCM	30 μ s	2
BC-PF-4	Stop beam operation if BPMs detect that the beam is not correctly steered	BC-OPF-3	BPM	30 μ s	1
BC-PF-5	Stop beam operation if nBLMs detect detect critical beam losses above acceptable limits	BC-OPF-3 BC-OPF-4	nBLM	30 μ s	0

Table 5.6: Damage events, hazards, overall protection functions, and protection functions for the MEBT buncher cavities at ESS.

Target Primary Cooling (He)

The target primary cooling system (TPCS) is a helium system that has the primary purpose to cool the target wheel through continuous heat removal during beam operation, as well as keeping activated or contaminated fluid enclosed within the system. Its secondary tasks are also to collect radiated particles in filters and separate particles from the fluid. The system operates at a maximum pressure of 1.3 MPa and the helium keeps a temperature below 60°C in the target wheel inlet and 270°C at the outlet. The heat within the TPCS is removed through heat exchangers in the target intermediate (water) cooling systems [139].

An overview of the TPCS is seen in Figure 5.8, where the heat exchange, filters (for contamination and particles), purification system, and target wheel interfaces are identified. The MP analysis of this system is based on the HAZOP reports in [139] and [140] as well as discussions with the system owner. The identified and analyzed damage events, hazards, OPFs, and PFs are listed in Table 5.7, while their detailed graphical derivation is found in Appendix C.

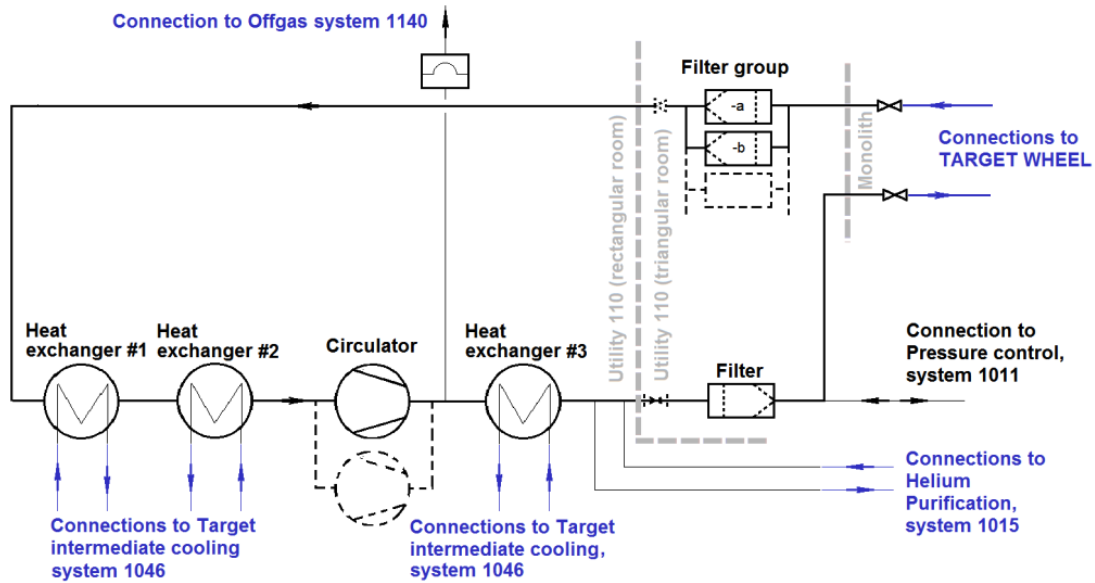


Figure 5.8: The target primary cooling system and its immediate interfaces [139].

Damage Event	Description	Risk Category	TOM		
TW-DE-1	Target wheel overheats due to lack of cooling	Severe	3		
Hazard	Description	Linked Damage Event	Expected Occurrence		
TW-HAZ-1	Helium flow in cooling system is below acceptable limits	TW-DE-1	EO1		
TW-HAZ-2	Helium temperature in cooling system is above acceptable limits	TW-DE-1	EO1		
OPF	Description	Linked Hazard	FIM		
TW-OPF-1	Prevent helium flow in system below acceptable limits	TW-HAZ-1	2		
TW-OPF-2	Prevent helium temperature in cooling system above acceptable limit	TW-HAZ-2	2		
PF	Description	Linked OPF	Sensor	Timing	PIL
TW-PF-1	Stop beam operation if the differential pressure measurements in the helium outflow from the target wheel is above or below acceptable limits	TW-OPF-1	Pressure sensor	1 s	1
TW-PF-2	Stop beam operation if the helium mass flow out of the target wheel is below acceptable limits	TW-OPF-1	Flow sensor	5 s	0
TW-PF-3	Stop beam operation if the helium temperature in the outflow from the target wheel is above acceptable limits	TW-OPF-2	Temperature sensor	2 s	1

TW-PF-4	Stop beam operation if the target wheel monitoring plug infrared monitor shows temperature above acceptable limits	TW-OPF-2	IR monitor	1 s	0
---------	--	----------	------------	-----	---

Table 5.7: Damage events, hazards, overall protection functions, and protection functions for the target primary cooling system at ESS. The target wheel-related analysis and its numbering of damage events etc. continue in Table 5.8.

Target Wheel Movement and Rotation

The target wheel movement and rotation is carried out by the target wheel, drive and shaft system. The system functions are to rotate and control the speed of the wheel, monitor friction, position, alignment, and suspension of the setup, and connect to the TPCS, as described above [141]. An overview of the target wheel setup, with the helium cooling inlet and outlet and the target drive unit for XYZ movement and wheel rotation, is seen in Figure 5.9.

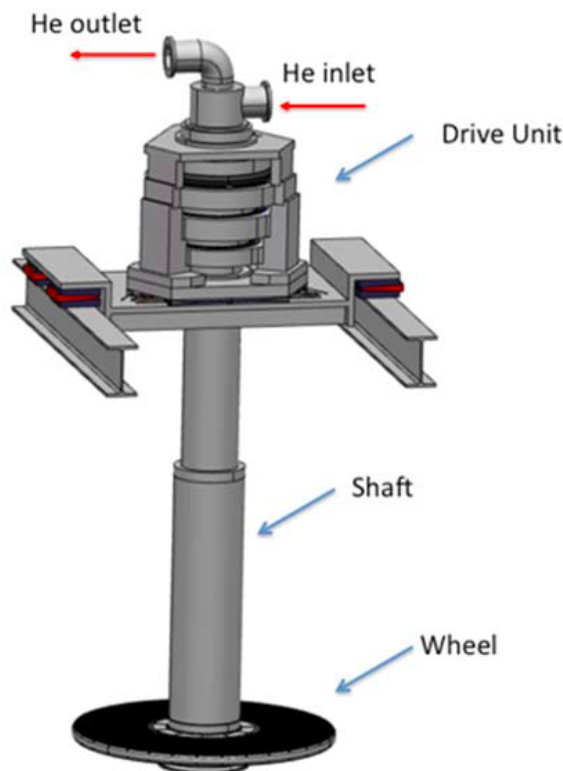


Figure 5.9: The target wheel system setup.

The analysis of the target wheel as the one entity to be protected by MP⁴ has been done in collaboration with the system owner and is based on the HAZOP reports in [142] and [143]. A more detailed view of the system and its interfaces, as analyzed in these HAZOPs, is displayed in Figure 5.10. The damage events, hazards, OPFs, and PFs are found in Table 5.8 and the graphical derivation in Appendix C.

⁴The surrounding equipment is viewed to have the function of *supporting* the target wheel function.

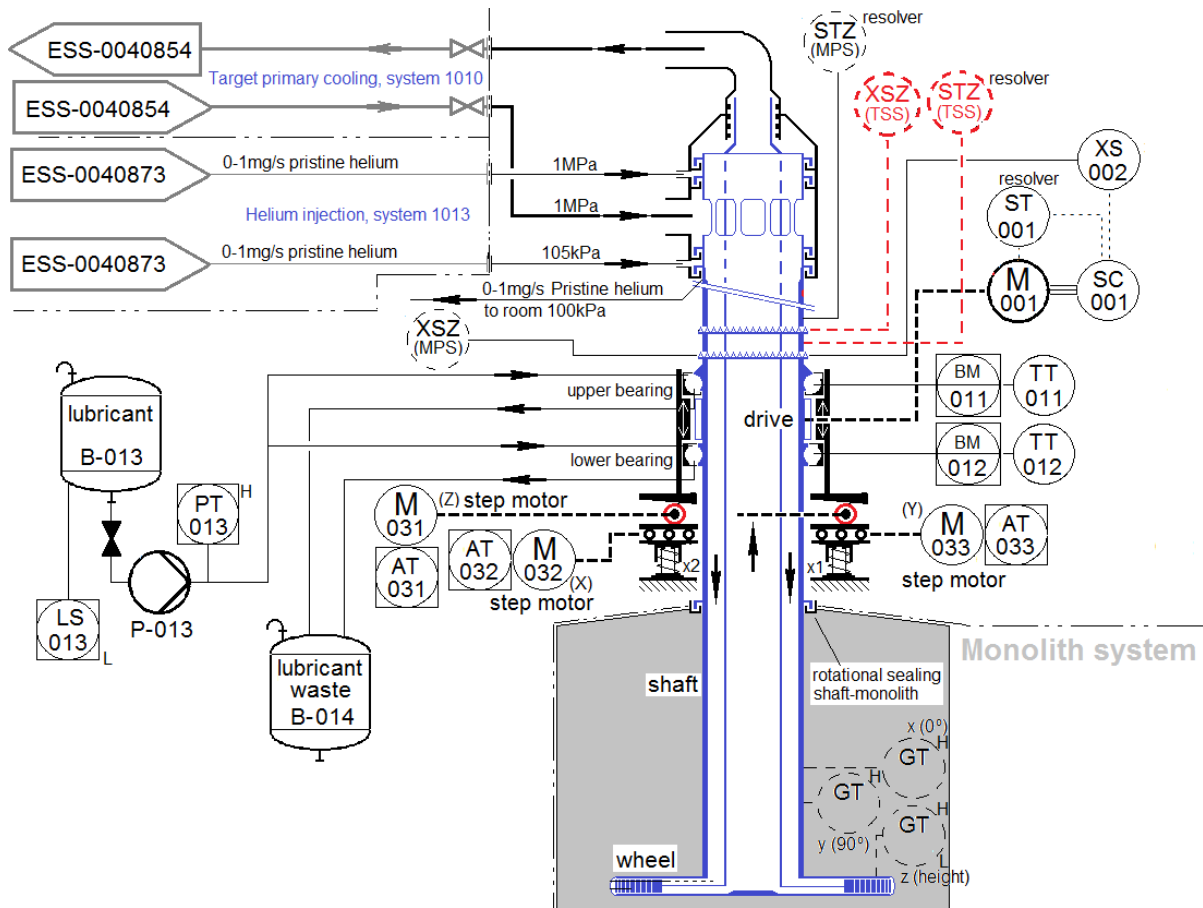


Figure 5.10: The target wheel, drive and shaft system setup [144].

Damage Event	Description	Risk Category	TOM
TW-DE-2	Target wheel is damaged from the proton beam hitting the wrong wheel position	Severe	3
Hazard	Description	Linked Damage Event	Expected Occurrence
TW-HAZ-3	Wheel rotation is out of phase with the proton beam pulse	TW-DE-2	EO0
OPF	Description	Linked Hazard	FIM
TW-OPF-3	Prevent wheel rotation out of phase with the proton beam pulse	TW-HAZ-4	3
ORRM	Description	Linked OPF	RR
TW-ORRM-1	Continuous checks of the motor rotation and bearing friction	TW-OPF-3	1

PF	Description	Linked OPF	Sensor	Timing	PIL
TW-PF-5	Stop beam operation if the rotational encoder transmits that the rotational speed of the target wheel is below minimum or exceeds maximum value	TW-OPF-3	Magnetic rotational encoder	100 ms	1
TW-PF-6	Stop beam operation if the target wheel rotation phase is not consistent with the phase reference value	TW-OPF-3	Optical phase monitor	2.57 s	1

Table 5.8: Damage events, hazards, overall protection functions, and protection functions for the target wheel movement and rotation at ESS. Note that the target wheel analysis is made for both cooling and movement together. This makes the damage events in this table start at number 2 rather than 1, which is located in the previous table. The same holds for hazards, OPFs, and PFs as well.

Cryogenic (LH₂) Moderator System

The cryogenic moderator system (CMS) provides the moderating medium, being liquid hydrogen, for the production of *cold neutrons*. The same medium also removes the resulting heat load from the moderator structures. The hydrogen is circulated at 1 kg/s at a working temperature of 17-20 K. At full capacity, the system is able to remove 28 kW of heat load. The CMS has an interface with the intermediate cooling water system for cooling the two pumps, and the target moderator cryogenic plant (TMCP), which provides the cooled hydrogen [145]. The system itself contains plenty of subsystems and is beyond the scope of this short section, but the overview including the interfaces is seen in Figure 5.11.

The MP analysis is based on the HAZOP in [146], and the resulting damage events, hazards, OPFs, and PFs are listed in Table 5.9. The detailed and graphical derivation is found in Appendix C.

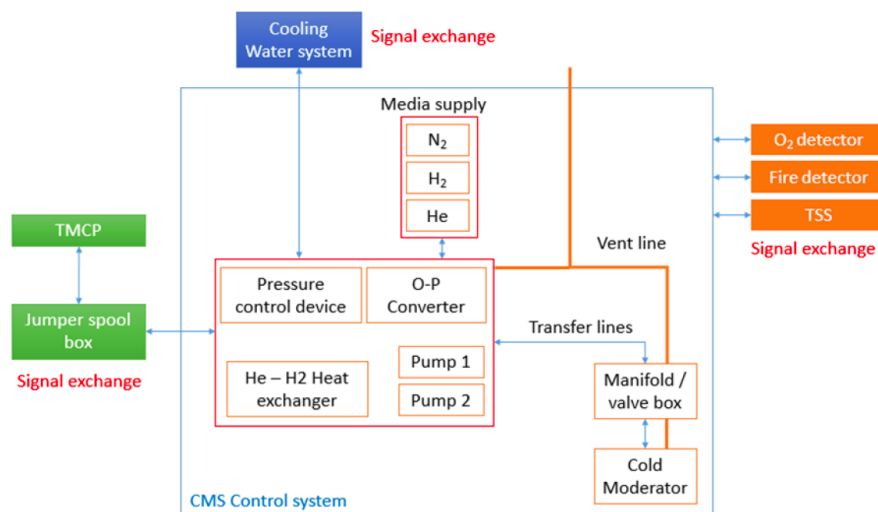


Figure 5.11: The cryogenic moderator system and its interfaces [145].

Damage Event	Description	Risk Category	TOM		
CMS-DE-1	Cryogenic moderators are damaged by lack of LH ₂ cooling	Significant	3		
CMS-DE-2	The CMS is damaged from pressure above acceptable limits in the system	Significant	3		
Hazard	Description	Linked Damage Event	Expected Occurrence		
CMS-HAZ-1	LH ₂ flow is below acceptable limit	CMS-DE-1	EO1		
CMS-HAZ-2	LH ₂ pressure is above or below acceptable limit	CMS-DE-1	EO1		
CMS-HAZ-3	LH ₂ temperature is above acceptable limits	CMS-DE-1	EO1		
CMS-HAZ-4	Vacuum pipe leakage (air) into vacuum shielding	CMS-DE-2	EO2		
CMS-HAZ-5	LH ₂ leakage into vacuum shielding	CMS-DE-2	EO2		
OPF	Description	Linked Hazard	FIM		
CMS-OPF-1	Stop beam operation if LH ₂ flow is below acceptable limits	CMS-HAZ-1	2		
CMS-OPF-2	Stop beam operation if LH ₂ pressure is above or below acceptable limits	CMS-HAZ-2	2		
CMS-OPF-3	Stop beam operation if LH ₂ temperature is above acceptable limits	CMS-HAZ-3	2		
CMS-OPF-4	Stop beam operation if vacuum shielding pressure is above acceptable limits	CMS-HAZ-4 CMS-HAZ-5	1		
PF	Description	Linked OPF	Sensor	Timing	PIL
CMS-PF-1	Stop beam operation if LH ₂ flow in the moderator inlet is below acceptable limits	CMS-OPF-1	Flow sensor	1 s	1
CMS-PF-2	Stop beam operation if LH ₂ pressure is above or below acceptable limits	CMS-OPF-2	Pressure sensor (hydrogen)	1 s	1
CMS-PF-3	Stop beam operation if LH ₂ temperature in the moderator inlet is above acceptable limits	CMS-OPF-3	Temperature sensor	5 s	0
CMS-PF-4	Stop beam operation if LH ₂ temperature in the moderator outlet is above acceptable limits	CMS-OPF-3	Temperature sensor	5 s	1
CMS-PF-5	Stop beam operation if the CMS vacuum system pressure is above acceptable limits	CMS-OPF-4	Pressure sensor (vacuum)	5 s	1

Table 5.9: Damage events, hazards, overall protection functions, and protection functions for the cryogenic moderator system at ESS.

Water Moderator and Reflector Systems

Organizationally and physically, the primary water cooling systems (PWCS) for the water moderators and reflectors are designed as two separate and independent systems, but their identical setup (from an analysis point of view) allows for a collected functional protection analysis to be carried out and all of the damage events, hazards, OPFs, and PFs are the same for both systems. The MP analyses for these systems are based on a number of discussions with the system owners and experts, as well as the HAZOP in [147]. Table 5.10 provides the identified and analyzed damage events, hazards, OPFs, and PFs for these two systems, as graphically derived in Appendix C.

The PWCS for the water moderators and reflectors cool the respective system during beam operation through a steady flow of water. The two systems interface with the intermediate cooling system through a heat exchanger that cools the PWCS to an operating temperature of 20°C. The systems contain a delay tank where the water stays for 300 seconds in order to let short-lived radioactive isotopes decay [148, 149]. There are currently no simplified figures of the PWCS, and as the piping and instrumentation diagrams (P&ID) are too complex to include here, the interested reader is directed to [150] for the moderators and [151] for the reflectors.

Damage Event	Description	Risk Category	TOM		
PWCS-DE-1	Moderators or reflectors overheat due to lack of water cooling	Significant	3		
Hazard	Description	Linked Damage Event	Expected Occurrence		
PWCS-HAZ-1	Cooling water flow is below acceptable limit	PWCS-DE-1	EO1		
PWCS-HAZ-2	Cooling water temperature is above acceptable limit	PWCS-DE-1	EO1		
PWCS-HAZ-3	Cooling water system pressure is below acceptable limit	PWCS-DE-1	EO1		
OPF	Description	Linked Hazard	FIM		
PWCS-OPF-1	Prevent cooling water flow in moderator or reflector below acceptable limit	PWCS-HAZ-1	2		
PWCS-OPF-2	Prevent temperature in moderator or reflector above acceptable limit	PWCS-HAZ-2	2		
PWCS-OPF-3	Prevent cooling water pressure below acceptable limit	PWCS-HAZ-3	2		
PF	Description	Linked OPF	Sensor	Timing	PIL
PWCS-PF-1	Stop beam operation if the cooling water mass flow in the moderator or reflector INLET is below acceptable limits	PWCS-OPF-1	Flow sensor	1 s	1

PWCS-PF-2	Stop beam operation if the cooling water mass flow in the moderator or reflector OUTLET is below acceptable limits	PWCS-OPF-1	Flow sensor	0 s	1
PWCS-PF-3	Stop beam operation if the cooling water temperature in the moderator or reflector OUTLET is above acceptable limits	PWCS-OPF-2	Temperature sensor	10 s	2
PWCS-PF-4	Stop beam operation if the cooling water pressure in the moderator or reflector INLET is above acceptable limits	PWCS-OPF-3	Pressure sensor	1 s	2

Table 5.10: Damage events, hazards, overall protection functions, and protection functions for the water moderator and reflector systems at ESS.

Tuning Beam Dump

The tuning beam dump (TBD) is located outside of the target area, but belongs to the target station systems. Its location underneath the target station, as well as the role of the A2T bending magnets to guide the beam to either the target or the tuning beam dump, is seen in Figure 5.12. The tuning beam dump is in place to receive proton beam during accelerator tuning phases and when the tungsten target is not ready for it. This allows for more effective beam tuning and maintenance as the target station does not have to be vacated before beam can be propagated along the entire ESS linac. However, the dump can only take up to 12.5 kW of average beam power, corresponding to 4 nominal beam pulses before a stop is required [152]. This generates restrictions on the beam parameters and requires monitoring of the beam that goes to the dump. To be able to handle continuous and prolonged beam operation to the TBD (more than 10 hours), its radiation shielding houses a small water cooling circuit located about 1.5 m above the TBD itself. Table 5.11 and Appendix C show the straightforward results from the analysis.

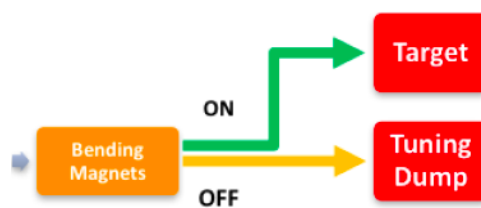


Figure 5.12: The tuning beam dump path, as selected by the bending dipole magnets in the A2T area [152].

Damage Event	Description	Risk Category	TOM		
TBD-DE-1	The tuning beam dump damaged by beam	Significant	3		
TBD-DE-2	The tuning beam dump damaged by heat	Significant	3		
Hazard	Description	Linked Damage Event	Expected Occurrence		
TBD-HAZ-1	High power beam (hundreds of kW-MW) is delivered to tuning beam dump	TBD-DE-1	EO1		
TBD-HAZ-2	Low power beam (tens of kW, slightly above acceptable limits) is delivered to tuning beam dump	TBD-DE-2	EO1		
TBD-HAZ-3	Extended beam operation to the tuning beam dump is carried out without water cooling	TBD-DE-2	EO1		
OPF	Description	Linked Hazard	FIM		
TBD-OPF-1	Prevent high power beam to be delivered to tuning beam dump	TBD-HAZ-1	2		
TBD-OPF-2	Prevent low power beam above acceptable parameters to be delivered to tuning beam dump for an extended period of time	TBD-HAZ-2	2		
TBD-OPF-3	Prevent extended beam operation to the tuning beam dump without water cooling	TBD-HAZ-3	2		
ORRM	Description	Linked OPF	RR		
TBD-ORRM-1	If tuning beam dump water cooling is not functioning correctly, an alarm is sent to the operators to restrict (in time) continuous beam to the dump	TBD-OPF-3	1		
PF	Description	Linked OPF	Sensor	Timing	PIL
TBD-PF-1	Prevent beam operation above acceptable repetition rates and beam energies when bending magnets are not deflecting	TBD-OPF-1	Timing system	N/A	0
TBD-PF-2	Prevent beam operation if proton beam mode is inconsistent with tuning beam dump as destination	TBD-OPF-1 TBD-OPF-2	Timing system	N/A	0
TBD-PF-3	Stop beam operation if the dump beamline BCMs detect beam above acceptable beam parameters	TBD-OPF-1 TBD-OPF-2	BCM	280 ms	0
TBD-PF-4	Stop beam operation if tuning dump temperature sensors notice a dump temperature above acceptable limits	TBD-OPF-2 TBD-OPF-3	Temperature sensor	3 s	1

TBD-PF-5	Prevent beam operation above acceptable beam parameters when beam destination is set to tuning beam dump	TBD-OPF-1	Dipole power supply	N/A	0
----------	--	-----------	---------------------	-----	---

Table 5.11: Damage events, hazards, overall protection functions, and protection functions for the tuning beam dump at ESS.

5.3.2 Protection Function Specification

The specification of protection functions at ESS is performed in close collaboration between the PAT, IPT, and IDT teams (Figure 4.1). This is essential in order to meet requirements that a) fulfill the protection needs and b) are implementable. All of the specified protection functions have been iterated with the system experts, and are found suitable for the goals of MP and the system design. As ESS is still under development and design, some of the analyses will likely continue to be iterated, but their current status gives a clear indication on the direction of the functional protection analysis efforts.

The protection functions at ESS that are associated with *stopping beam*⁵ go through the same logic element (the BIS) as well as the same actuation systems. Following the IEC 61508 standard (e.g. part 2, Figure 6 [96]), this should mean that these are *the same* protection function, but with several sensors. Due to this architecture at ESS, and most other modern accelerator facilities that stop the beam as a protection measure, the analysis has been carried out by looking at the specific *function* itself. And then, through the detailed specification of *protection functions*, foreseen the same logic and actuators. This does not, however, affect the validity or outcome of the analysis itself, due to that the BIS and actuators are all given requirements on the *continuous* spectrum, or mode, requiring appropriate probabilities of *failure per hour* (PFH), given in Table 5.2. Since the dangerous failure rates of the BIS and actuators are stated in units of time, they are able to cope with the inherent demands no matter if there is one or a thousand *uses* of the function per year, despite being included in separate protection functions.

The protection functions for the systems mentioned in Section 5.2 are presented in Paper III [3] for the normal conducting linac and Paper IV [4] for the target station systems. Their derivation is found in the graphical form in Appendix C, where they are included as the last step of the functional protection analysis presented in Section 5.3.1. Tables 5.3 through 5.11 display the associated protection functions as well as their linked OPF, sensor, timing requirements, and PIL.

⁵This goes for all of the protection functions derived in this thesis (Tables 5.3-5.11). The role of the BIS and the sequence of actuators for these protection functions are as described in Section 5.1.


5.3.3 Risk Register and Traceability

Traceability is a key feature during the whole risk management process described in this thesis. This holds for the referencing of information that is used in the analyses as well as for tracking the definition of PFs from a damage event. This ensures that the method and the analyses can be anchored in the organization so that the protection requirements that are derived by the PAT and IPT teams are relevant to the system owners.

The functional protection method at ESS uses the Insight add-on to the Atlassian JIRA tool [153] as risk register during the design phase. The tool is collaborative and allows versioning, which fits the needs of a flexible and user-friendly risk register as the analyses are iterative procedures. An example of the view of a damage event in Insight is seen in Figure 5.13, and a more detailed description of the tool and its usage is found in [100]. Once the PFs are defined and agreed, they are modeled in detail in the UML tool Enterprise Architect [154] by the IPT, and then documented, reviewed, and approved through the ESS document management tool (CHESS).

Machine Protection / 4.1 Damage Events / MP-645

Gate Valve - DTL 1 : Beam : GV damaged by beam

[Edit](#)
[Comment](#)
[More](#)
[Object Graph](#)

[Watch](#)

Details

Name	Gate Valve - DTL 1 : Beam : GV damaged by beam
Affects	Gate Valve - DTL 1
Damage Source	Beam
Operational Mode	Operation
Operational Impact	Not possible to operate
Description	All of the gate valves are pneumatic and fail-closed. In case there is any kind of problem, the beam permit is withdrawn and the GV will be closed.
Unmitigated Expected Cost	2) 10 - 100 k€
Rationale for UEC	Gate valve cost is 8-20 k€ [Simone Scolari, Hilko Spoelstra]
Unmitigated Expected Downtime	e) 1 day - 3 days
Rationale for UED	DTL to be opened, valve replaced. Spares are available, but undecided how many [Simone Scolari, Hilko Spoelstra]
Unmitigated Risk Category	Significant
Unmitigated Tolerable Mean Time Between Occurrences	f) > 5000 years
TMTBO Achieved without Measures	No
Status	ANALYZED

Dates

Created	28/Feb/17 3:30 PM
Updated	27/Apr/17 4:44 PM

Attachments

Drop files to attach

Maximum file upload size: 50.0 MB

[Attach Files](#)

File name	Size	Created
GV_cost.png	193.1 kB	06/Mar/17 7:11 PM

Inbound References

Object	Reference Type	Object Type
Gate valve upstream of beam destination closes during beam operation	Affects	5. Hazards
MP-Haz-Vac-01 Beam is injected while gate valve/fast vacuum valve is closed upstream of beam destination	Affects	5. Hazards

Figure 5.13: An example view of a damage event in the Insight risk register: the gate valve after DTL tank 1 is hit by beam [153].

5.4 The Functional System Interaction Process at ESS

The functional system interaction process corresponds to the purple rectangle in Figure 4.2 and is consequently carried out by the purple IPT bubble in Figure 4.1. Its application at ESS has not been the focus of this thesis, but it is still performed in parallel with the analysis in Section 5.3. The IPT at ESS has set up a framework for the use case workshops to be able to document and model the protection-related system interface requirements (first box in the lifecycle in Figure 4.2) and interactions (second box in the same figure).

Besides the definition of system interaction protection requirements (third box in Figure 4.2), the interface definitions and workshops help in the communication of MP at ESS and its role for the facility. This is an important aspect and the consensus in interface agreements are critical for the success of the functional protection method.

One example of a protection requirement that has been defined through the system interaction use case analyses is the interface with vacuum pressure monitors in the ESS linac. The increase in vacuum pressure was not found in the first iteration of the functional protection analysis technique in Section 5.3, as it does not immediately cause a damage event. However, as increased pressure means an increase in beam losses and is a cause for an eventual closing of the vacuum gate valves, the functional system interaction process found that vacuum pressure monitoring within the scope of MP at ESS is beneficial and that this functionality should be implemented.

5.5 Functional Protection Implementation and Adjustments at ESS

Once the protection functions are in place and agreed, the following step is to implement them into the design of the protection-related systems. This implementation is based on the outcome of the functional protection analysis and functional system interaction process, and thus have full traceability to motivate their role. As described in Section 4.7, the system owners take over the responsibility to implement and test the protection-related systems to ensure that they fulfill the required behavior and quality. However, the PAT and IPT still remain active in discussions and as reviewers once the system designs are finished and installation is taking place.

The IDT (system owners) will, together with the IPT, develop a verification and validation (V&V) plan for each system that takes part in a PF. The plan is reviewed during one of the critical system reviews and is followed up during the site and facility acceptance tests. Finally, the commissioning and initial operation phases require proper adjustments and tuning to ensure that the PFs and protection-related systems behave as expected.

5.6 Estimation of the Availability and Cost Impact of Functional Protection at ESS

The functional protection method in this chapter has specified a set of protection functions that reduce both downtime and cost at ESS. Despite the fact that a *detailed* quantitative estimation is

currently not possible, due to the early stage and undefined concept of operation for the facility, it is still possible to give an indication on the impact that MP has for the analyzed systems in this thesis [155]. This has been simulated using the ReliaSoft BlockSim 10 software [156] and the results are described in this section.

It should also be pointed out that the application of MP at ESS in this chapter is relevant for the normal conducting linac and the target station systems, and any availability estimation does therefore not give a number that is relevant for the facility as a whole. The functional protection method has been applied to the systems as they are expected to appear for nominal operation, where the EOs and TOMs are applicable. By making an estimation of the quantitative aspect of the EO, and using the numbers given in Table 4.3 for the TOM, it is possible to simulate the associated operational availabilities for the NCL and target station systems a) without any PFs applied to them and b) with the PFs defined in Tables 5.3-5.11. As the cost associated with each DE was estimated during the analysis to derive the specific TOM, it too can be simulated to obtain the annual impact on the operational budget.

5.6.1 Simulation Assumptions

To be able to assess the qualitative aspects of the method, three assumptions need to be made. The EO (expected occurrence) rates were estimated to correspond to twice per year for an EO0, once every ten years for EO1, and once every hundred years for EO2. The average downtime associated with a PF beam stop, whether to protect against an actual hazard or as a spurious trip, is assumed to be one hour per trip. Further, the impact from the added complexity and additional spurious trips of the PFs are assumed to generate ten times more trips with MP in place than without. The downtime and cost of each DE were analyzed and inserted into the risk matrices (Tables 4.1 and 4.2), as a part of the analysis described in this chapter, to obtain a TOM for each event. These numbers are logged in the Insight risk register (described in Section 5.3.3) and the ones used in this simulation [155].

5.6.2 Simulation Setup

The simulation was performed using ReliaSoft BlockSim 10 [156] and included all of the damage events in this chapter. The simulation length was taken to be 200 days (corresponding to one operational year for ESS), and the simulation was run until convergence, which corresponded to 10000 simulations. The simulation considered all events to be independent and they were modeled as series blocks [155].

5.6.3 Simulation Results

The results of the simulation as described in this section yields the availability numbers seen in Table 5.12. As seen, the availability of the normal conducting linac and target station systems is increased from 53.1% to 97.3% by implementing the PFs described in this thesis. This corresponds to a downtime reduction by a factor 17.4, or from 2252 hours to 130 hours per year. The cost saving per operational year for having the PFs in place is found to be 2.2 M€.

	Availability	Downtime (hours/year)
Without PFs	53.1%	2252
With PFs	97.3%	130

Table 5.12: Simulated availability and downtime for the normal conducting linac and target station systems at ESS, with and without the MP protection functions in place [155].

5.6.4 Discussion

As stressed above, a *detailed* quantitative estimation is not possible at this stage, and is also not within the scope of the functional protection method, which has accentuated the order of magnitude approach and lack of detailed estimations. Despite this, the availability and cost simulation is still able to give a hint on the way that MP can be beneficial for ESS during the operational phase and it indicates a significant operational improvement.

Chapter 6

Discussion and Conclusions

6.1 The Functional Protection Method

Many accelerator-driven facilities, some of which discussed in Chapter 1 in this thesis, have started to implement more and more sophisticated systems and procedures for the protection of their facility. As also new generations of accelerator facilities are planned and designed, with even higher performance demands in terms of beam power, beam energy, and availability, the protection analysis methods and protection system designs need to *keep up* with this technological development. The system of systems approach is a good way forward to fully describe how a modern protection system is intertwined with the rest of the equipment in the facility.

The functional protection method for machine protection has considered the use of protection systems in other facilities to highlight and implement the best practices. A systematic approach is then necessary due to the vast complexity of modern accelerator facilities. Looking at the functional safety standards, IEC 61508 and IEC 61511 present a complete lifecycle that covers all phases in the life of a safety system. This gives a solid foundation at the same time as it gives room for purposeful freedom in the analyses and design of systems. The ISO 31000 and ISO 16085 risk management standards give a systematic approach to the identification, analysis, and evaluation of risks, which is a perfect fit to the initial steps in the functional safety standards. Combining these four has resulted in a method that is straightforward to apply and has distinct results.

6.2 Differences Between Safety and Protection Systems

The main difference between machine protection as described in this thesis and a typical safety system is the functional ownership. While safety functions are often completely owned and implemented by the safety team, protection functions are spread over several systems with different owners. As is displayed in Figure 6.1, the full chain is consequently not controlled by one team or group. This requires the approach to be flexible enough to implement external sensors, logic, and actuators to achieve the end goal of machine protection. Therefore, a system of systems approach is necessary in combination with well-defined protection function requirement specifications and follow-ups, such as for the compliance of protection integrity levels.

Additionally, a safety system typically has legal restrictions and requirements and therefore

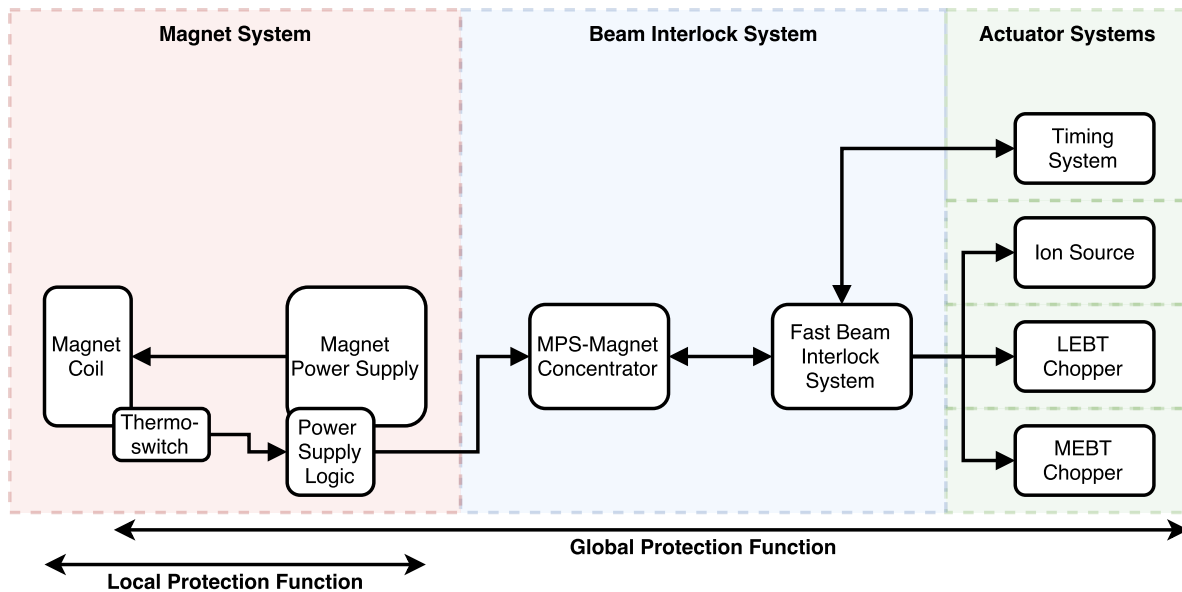


Figure 6.1: The functional ownership is typically shared among several system owners. The figure also displays the difference between a local protection function (managed by the system owner) and a global protection function (managed by facility-wide functional protection).

goes through an external certification process, which is not necessary for a protection system. This allows the protection methodology to be more flexible and it is possible, and arguably important, to adjust the method towards the needs of the facility where it is applied.

6.3 Application to ESS

While there have been careful analyses associated with the functionality of ESS machine protection and its related components in this thesis, there are other, perhaps as important, factors involved in the successful construction and operation of an advanced facility such as ESS. One such factor is the interaction between engineers, designers, and researchers, where constructive discussions and mutual understanding is key. Effectiveness in protection and achieving a desired availability requires decisions and appropriate project management, and a technical risk management method alone cannot foresee the effects of such aspects.

So far, the functional protection method has been applied during the design phase of ESS. Despite that the sources of inspiration have been other accelerator facilities and their machine protection systems, the exact analysis steps and definition of the three protection teams at ESS are not seen elsewhere. The same goes for the standard-compliant usage of protection integrity levels, where systematic and architectural requirements are implemented in addition to the probabilities of function failure.

Throughout the application of the functional protection method at ESS, a relatively small amount of the analyzed events turned out to require *additional measures* to be taken by the system designers. This means that for the vast majority of systems, the analysis was able to identify the appropriate protection functions and decrease the damage risk to an acceptable level purely through protection functions. This is desired as the protection functions need to be *integrated* into the ongoing, and sometimes finalized, design work. Despite this, there are a few

cases where additional protection-related functionality has been added at ESS, as an outcome of the functional protection method. Two of these are the usage of BCMs to verify the proton beam mode and destination as given in ID-PF-3 and the necessity to install beam scraper charge deposition monitors as defined in ID-PF-4 in Table 5.5. While the former arose due to the need for an additional protection layer, the latter was based on the strict time constraints to avoid damage and required a means to quickly take action in case of beam losses above limits. The stringent time constraints for some protection functions has also defined the requirement to implement a fast shutdown unit for the ion source, in order to quickly prevent the extraction of protons in the case of a prompt beam loss. In addition, identified protection functions have driven requirements on e.g. redundancy, logic setups, and connector types. The definition of protection functions for the target station systems created a clear indication on which sensors that require an interface with the beam interlock system. These sensors are already included in the target station system designs and can, after the protection function specification, be verified to comply with the facility-wide MP strategy.

The practical implication of the method described in this thesis, and in extension MP at ESS, is to enhance operational availability. Subsequently, it is possible to trace this back throughout the analyses. Nonetheless, the effect of including additional functionality also typically implies a *reduced reliability*, as more operational stops are expected from both the increased complexity due to more equipment and because the functionality of this equipment is to stop operation when required. The task of MP can be seen as "transferring" long downtimes due to significant damage into shorter downtimes, if still more frequently, and thus *increasing the overall availability* of the facility. As a comparison, the availability and cost simulation in Section 5.6 results in a total downtime of approximately 2252 hours per year for the damage events listed in this thesis. By introducing the protection functions to handle these damage events, this is instead estimated to be reduced to 130 hours with a cost saving of around 2.2 M€ per year, and a corresponding decrease in unavailability by a factor 17.

The functional protection method has based its analysis on the steady-state operation, or neutron production, phase of ESS. This means that the protection functions are implemented to cope with operational modes and variations during normal operation, and are not customized for the commissioning and initial operation phases. This does not mean that they will not be used in these earlier stages, but rather that their availability-driven approach cannot be extrapolated to tuning and staged commissioning of equipment. As these phases of the facility do not have specified protection goals, the concept and scope is not accurately established and the method rather becomes one of the tools for successful initial operation, but not the only one.

6.4 Live Process and Future Work

It should be noted that risk management is a live process, and that continuous review is necessary to achieve the desired performance. Therefore, the method in this thesis presents a direction of analysis and protection integration rather than a final stop. Much in the same way as this thesis somewhat expands on what has been developed for LHC in [92] on the machine protection system lifecycle. A substantial portion of work remains in iterating the protection function requirements that are presented in Chapter 5 as well as applying the method to e.g. the super-

conducting linac and neutron science systems at ESS. However, as the method developed in this thesis rests on a stable foundation of proven in use standards, its application to accelerator protection is merely a natural step towards more advanced applications.

As ESS develops and moves into installation and initial operation, the last boxes of the life-cycle (orange rectangle in Figure 4.2) will become more developed and involved in the everyday work. Work is currently ongoing in defining e.g. installation procedures and verification and validation processes for the MP-related systems, and their outcome will affect the final results of the protection functionality. This thesis has been successful in initiating and advancing discussions between system owners and analysts, and in directing the ongoing MP work. However, it is dependent on further (risk and project) management, as well as systematic engineering processes, to be able to complete the application of this method. This work is now launched and the functional protection method will be useful in defining the focal points of the protection efforts.

Bibliography

- [1] Riccard Andersson, Annika Nordt, and Erik Adli. Machine Protection Systems and Their Impact on Beam Availability and Accelerator Reliability, paper MOPTY044. *Proceedings of IPAC2015*, 2015.
- [2] Riccard Andersson, Enric Bargalló, and Annika Nordt. A Functional Protection Method for Availability and Cost Risk Management of Complex Research Facilities. *Submitted to ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*, 2017.
- [3] Riccard Andersson, Enric Bargalló, Szandra Kövecses, Annika Nordt, Christian Hilbes, and Martin Rejzek. Development and Status of Protection Functions for the Normal Conducting Linac at ESS, paper TUPIK079. *Proceedings of IPAC2017*, 2017.
- [4] Riccard Andersson, Enric Bargalló, Leif Emås, Jens Harborn, Allan Lundgren, Ulf Odén, Jesper Ringnér, and Kristoffer Sjögreen. Machine Protection Risk Management of the ESS Target System, paper TUPIK078. *Proceedings of IPAC2017*, 2017.
- [5] Philip Bryant. A Brief History and Review of Accelerators. *CERN Accelerator School: Course on General Accelerator Physics*, 1992.
- [6] National Research Council. *Nuclear Physics: Exploring the Heart of Matter*. The National Academic Press, Washington, DC, 2012.
- [7] Lucien Hardy. Accelerator Reliability-Availability, paper WEXLA001. *Proceedings of EPAC2002*, 2002.
- [8] Stanley Humphries. *Principles of Charged Particle Acceleration*. John Wiley and Sons, Albuquerque, NM, USA, 1999.
- [9] Riccard Andersson. *Cool-down and Warm-up of the Cryogenic Distribution Line at ESS*. MSc Thesis, Lund University, Sweden, 2014.
- [10] The European Technical Working Group on ADS. *A European Roadmap for Developing Accelerator Driven Systems (ADS) for Nuclear Waste Incineration*. 2001.
- [11] Masanori Ikegami. Machine and Personnel Protection for High Power Hadron Linacs, paper WEXC1. *Proceedings of IPAC2015*, 2015.
- [12] Alexander Wu Chao and Weiren Chou. *Reviews of Accelerator Science and Technology - Volume 6: Accelerators for High Intensity Beams*. World Scientific, Singapore, 2014.

- [13] Robert L. Kustom. An Overview of the Spallation Neutron Source Project, paper TU101. *Proceedings of Linac2000*, 2000.
- [14] CERN. *LHC Design Report - Chapter 10: Experimental Areas*. 2004.
- [15] Frederick Bordry, Reiner Denz, Karl-Hubert Mess, Bruno Puccio, Felix Rodriguez-Mateos, and Rüdiger Schmidt. Machine Protection for the LHC: Architecture of the Beam and Powering Interlock Systems (LHC Project Report 521). 2001.
- [16] Benjamin Todd, Maciej Kwiatkowski, Bruno Puccio, Rüdiger Schmidt, Sigrid Wagner, and Markus Zerlauth. Machine Protection of the Large Hadron Collider. *IET International Conference on System Safety 2011*, 2011.
- [17] Jet Goodson. Search for Supersymmetry in States with Large Missing Transverse Momentum and Three Leptons including a Z-Boson. 2012.
- [18] Andrea Apollonio. *Machine Protection: Availability for Particle Accelerators*. PhD Thesis (CERN-THESIS-2015-023), Vienna University of Technology, 2015.
- [19] CERN Press. CERN releases analysis of LHC incident, <https://press.cern/press-releases/2008/10/cern-releases-analysis-lhc-incident>, 2008.
- [20] John Galambos. SNS Performance and the Next Generation of High Power Accelerators, paper FRYAA1. *Proceedings of PAC2013*, 2013.
- [21] Jeremy Rumsey. SNS accelerator celebrates 10 years of leading the way, <https://phys.org/news/2016-10-sns-celebrates-years.html>, 2016.
- [22] Wikimedia Commons. SNS Facility Design, <https://en.wikipedia.org/wiki/File:Sns-facility-design.jpg>, 2011.
- [23] R. Shafer. How Long a SNS Beam Pulse would Damage a Copper Accelerating Structure? Technical report, 2001.
- [24] Adrian Eugen Pitigoi and Pedro Fernandez Ramos. Reliability model of an existing accelerator (SNS linac). *European Commission Report*, (269565), 2012.
- [25] Shoji Nagamiya. Introduction to J-PARC. *Prog. Theor. Exp. Phys.*, 2(2012):02B001, 2012.
- [26] Tadashi Koseki. Beam commissioning and operation of the J-PARC main ring synchrotron. *Prog. Theor. Exp. Phys.*, 2(2012):02B004, 2012.
- [27] Ouchi Nobuo. Status Report of J-PARC. *J. Korean Phys. Soc.*, 56 (6), 2010.
- [28] Masanori Ikegami. Transition from Commissioning to Operation in J-PARC Linac, paper WGD02. *Proceedings of Hadron Beam 2008*, 2014.

- [29] H Hotchi, H Harada, S Kato, M Kinsho, K Okabe, P K Saha, Y Shobuda, F Tamura, N Tani, Y Watanabe, K Yamamoto, M Yamamoto, and M Yoshimoto. The Path to 1 MW: Beam Loss Control in the J-PARC 3-GeV RCS, paper THAM6X01. *Proceedings of HB2016*, 2016.
- [30] Paul Simmonds, Erika Kraemer-Mbula, Andrej Horvath, James Stroyan, and Frank Zujdam. *Big Science and Innovation*. Technopolis Group, 2013.
- [31] STFC. About ISIS, <http://www.isis.stfc.ac.uk/>, 2017.
- [32] D. Adams, C. Warsop, B. Jones, B. Pine, H. Smith, R. Williamson, A. Seville, R. Mathieson, I. Gardner, D Wright, A H Kershaw, A Pertica, and A Letchford. Operational Experience and Future Plans at ISIS, paper TUPM3Y01. *Proceedings of HB2016*, 2016.
- [33] European Spallation Source. www.esss.se, 2017.
- [34] Roland Garoby. Progress on the ESS Project Construction, paper MOXBA1. *Proceedings of IPAC2017*, 2017.
- [35] Henning Larsen Architects. European Spallation Source, <http://www.henninglarsen.com/media/1173321/HenningLarsenArchitects.ESS.5.jpg>, 2015.
- [36] The ESS Linac, <http://esss.se/accelerator>, 2016.
- [37] Steve Peggs (ed.). *ESS Technical Design Report*. 2013.
- [38] ITER Organization. www.iter.org, 2017.
- [39] DEMO. <http://fusionforenergy.europa.eu/understandingfusion/demo.aspx>, 2017.
- [40] IFMIF. www.ifmif.org, 2017.
- [41] J. Knaster. The accomplishment of the Engineering Design Activities of IFMIF/EVEDA: The European and Japanese project towards a Li (d,xn) fusion relevant neutron source. *Nucl. Fusion*, 55(2015):086003, 2015.
- [42] Enric Bargalló. *IFMIF Accelerator Facility RAMI Analyses in the Engineering Design Phase*. PhD Thesis (10803/144657), Universitat Politècnica de Catalunya, 2014.
- [43] T. Behnke, J. E. Brau, B. Foster, J. Fuster, M. Harrison, J. P. Paterson, M. Peskin, M. Stanitzki, N. Walker, and H. Yamamoto. *ILC Technical Design Report*. 2013.
- [44] International Linear Collider. ILC Facts and Figures, <http://www.linearcollider.org/ILC/What-is-the-ILC/Facts-and-figures>, 2013.
- [45] R Appleby, L Keller, and T Markiewicz. ILC Technical Design Report Volume 3.2: Accelerator Baseline Design. 2013.
- [46] European XFEL. www.xfel.eu/. 2017.

- [47] CLIC. <http://clic-study.web.cern.ch/>, 2017.
- [48] P. Rowson and Dong Su. A Multi-TeV Linear Collider Based on CLIC Technology - CLIC Conceptual Design Report (CERN-2012-007). 2012.
- [49] Reidar Lunde Lillestøl. CLIC - The Compact Linear Collider High-energy particle colliders, <https://indico.cern.ch/event/140993/sessions/121324/attachments/124667/176978/agder-clic.pdf>. *Presentation at Visit from the University of Agder to CERN*, 2011.
- [50] Cern. Summary of Session 1 - CLIC MP.
- [51] FACET. facet.slac.stanford.edu, 2016.
- [52] Elettra. <https://www.elettra.trieste.it>, 2017.
- [53] KEK. <https://www.kek.jp/en/index.html>, 2017.
- [54] Henrik Bjerke. *Application of Novel Accelerator Research for Particle Therapy*. MSc Thesis, Norwegian University of Science and Technology, Trondheim, 2014.
- [55] M. Boland, T. Charles, R. Dowd, G. Leblanc, Y. Tan, K. Wootton, D. Zhu, R. Corsini, A. Grudiev, A. Latina, D. Schulte, S. Stapnes, I. Syratchev, and W. Wuensch. Plans for an Australian XFEL Using a CLIC X-Band Linac, paper THPME081. *Proceedings of IPAC14*, 2014.
- [56] Peter Forck. Lecture Notes on Beam Instrumentation and Diagnostics. *Joint University Accelerator School*, 2011.
- [57] Klaus Wille. *The Physics of Particle Accelerators*. Oxford University Press, 2000.
- [58] Volker Ziemann. *Accelerator Physics and Technology*. Lecture Notes, Uppsala University, Sweden, 2011.
- [59] G. Stupakov. Lecture notes on Classical Mechanics and Electromagnetism in Accelerator Physics. *US Particle Accelerator School*, 2011.
- [60] Alexander Wu Chao. *Physics of Collective Beam Instabilities in High Energy Accelerators*. John Wiley & Sons, Dallas, Texas, 1993.
- [61] IOP Science. Phase-Space Ellipse, <http://iopscience.iop.org/>, 2016.
- [62] Comsol. Phase-Space Ellipse, <https://www.comsol.com/blogs/sampling-from-phase-space-distributions-in-3d-charged-particle-beams/>. 2016.
- [63] Hooman Hassanzadegan. Beam Position Monitor Design Overview Document, ESS Internal Document (under review). 2015.
- [64] Hooman Hassanzadegan. Beam Current Monitor Design Overview Document, ESS Internal Document (under review). 2015.

- [65] M. Stockner, B. Dehning, C. Fabjan, E.B. Holzer, C. Fabjan, and D. Kramer. Classification of the LHC BLM Ionization Chamber, paper WEPC09. *Proceedings of DIPAC2007*, 2007.
- [66] Thomas Papaevangelou. MicroMegas detector applications for beam diagnostics, <https://indico.cern.ch/event/540799/>, 2016.
- [67] Lali Tchelidze. Current Status and Open Issues Associated with the ESS Beam Loss Monitoring System, ESS Internal Document (ESS-0009093). 2014.
- [68] Irena Dolenc Kittelmann and Thomas Shea. Simulations and Detector Technologies for the Beam Loss Monitoring System at the ESS Linac, paper THAM6Y01. *Proceedings of HB2016*, 2016.
- [69] Benjamin Cheymol. Wire scanner scintillator, ESS Internal Document (ESS-0068702). 2016.
- [70] Benjamin Cheymol. Faraday cup design specifications for the ESS MEBT, ESS Internal Document (ESS-0036676). 2015.
- [71] Erik Adli, Håvard Gjersdal, Ole Rohne, Ole Dorholt, David Bang, Cyrille Thomas, Ricard Andersson, Thomas Shea, Mark Ibison, and Shrikant Joshi. The ESS Target Proton Beam Imaging System as In-Kind Contribution, paper WEPVA066. *Proceedings of IPAC2017*, 2017.
- [72] Peter Sigmund. *Particle Penetration and Radiation Effects*. Springer-Verlag, Berlin, Germany, 2006.
- [73] NIST. Physical Reference Data, <http://www.physics.nist.gov/PhysRefData/contents.html>. 2016.
- [74] SLAC HyperNews, <http://hypernews.slac.stanford.edu/>, 2013.
- [75] Lali Tchelidze. In How Long the ESS Beam Pulse Would Start Melting Steel/Copper Accelerating Components?, ESS Internal Document (ESS/AD/0031). 2012.
- [76] I. Strasik, E. Mustafin, M. Pavlovi, N. Sobolevskiy, and V. Chetvertkova. Activation and "Hands-On" Maintenance Criteria for Heavy-Ion Accelerators. *Presentation at SATIF10*, 2010.
- [77] Lali Tchelidze, Thomas Hansson, and Peter Jacobsson. Hands on maintenance conditions for ESS accelerator, ESS Internal Document (ESS-0008351). 2014.
- [78] JAS2014. *Proceedings of JAS2014 on Beam Loss and Accelerator Protection*. CERN Document (CERN-2016-002), 2016.
- [79] Peter Forck. Lecture Notes on Beam Instrumentation and Diagnostics. *Joint University Accelerator School*, 2011.
- [80] Marc Ross. Machine Protection and Interlock Systems: Linear Machines, 2014.

- [81] Coles Sibley. Machine protection strategies for high power accelerators. *Proceedings of the 2003 Bipolar/BiCMOS Circuits and Technology Meeting*, 2003.
- [82] Rüdiger Schmidt, R. Assmann, E. Carlier, B. Dehning, R. Denz, B. Goddard, E. Holzer, Verena Kain, Bruno Puccio, Benjamin Todd, Jan Uythoven, Jörg Wenninger, and Markus Zerlauth. Protection of the CERN Large Hadron Collider. *New J. Phys.*, 8 (2006) 2, 2006.
- [83] Rüdiger Schmidt, Andrea Apollonio, Doug Curry, and Annika Nordt. Architecture of the ESS Machine Protection System, ESS Internal Document (unpublished). 2013.
- [84] Enric Bargalló. Tailoring the ESS Reliability and Availability needs to satisfy the users. *Presentation at WAO2014*, 2014.
- [85] David J. Smith. *Reliability, Maintainability and Risk, 7th ed.* Elsevier, 2011.
- [86] International Electrotechnical Committee. IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010.
- [87] International Electrotechnical Committee. IEC 61511:2004 Functional safety - Safety instrumented systems for the process industry sector. 2004.
- [88] International Electrotechnical Committee. IEC 61513:2013 Nuclear power plants - Instrumentation and control important to safety. 2013.
- [89] International Electrotechnical Committee. IEC 62061:2016 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems. 2016.
- [90] David J. Smith and Kenneth Simpson. *Functional Safety. A straightforward guide to applying IEC 61508 and related standards.* Butterworth-Heinemann, 2004.
- [91] International Electrotechnical Committee. <http://www.iec.ch/>, 2016.
- [92] Maciej Kwiatkowski. *Methods for the Application of Programmable Logic Devices in Electronic Protection Systems for High Energy Particle Accelerators.* PhD Thesis (CERN-THESIS-2013-216), Warsaw University of Technology, 2013.
- [93] Enzo Carrone. Controls and Machine Protection Systems. *Proceedings of JAS2014*, 2016.
- [94] R. Filippini, B. Dehning, G. Guaglio, F. Rodriguez-Mateos, R. Schmidt, B. Todd, J. Uythoven, A. Vergara-Fernandez, and M. Zerlauth. Reliability Assessment of the LHC Machine Protection System. *Proceedings of PAC2005*, 2005.
- [95] International Electrotechnical Committee. IEC 61508 Part 7 - Overview of techniques and measures. 2010.
- [96] International Electrotechnical Committee. IEC 61508 Part 2 - Requirements for electrical/electronic/programmable electronic safety-related systems (hardware). 2010.

- [97] International Electrotechnical Committee. IEC 61508 Part 3 - Software requirements. 2010.
- [98] ARC Advisory Group. *Reduce Risk with a State-of-the-Art Safety Instrumented System*. ARCweb.com, 2004.
- [99] International Organization for Standardization. ISO 31000: Risk management - Principles and guidelines. 2009.
- [100] Riccard Andersson, Enric Bargalló, Christian Hilbes, and Annika Nordt. Machine Protection Risk Management Process, ESS Internal Document (ESS-0095000). 2017.
- [101] International Organization for Standardization. ISO 16085: Systems and software engineering - Life cycle processes - Risk management. 2006.
- [102] Claudia Klüppelberg, Daniel Straub, and Isabell Welpé. *Risk - A Multidisciplinary Introduction*. Springer, 2014.
- [103] CGE Risk Management Solutions. The Bowtie Method, <http://www.cgerisk.com/knowledge-base/risk-assessment/thebowtiemethod>, 2016.
- [104] P.L. Clemens and Rodney J. Simmons. *System Safety and Risk Management*. National Institute for Occupational Safety and Health, Cincinnati, OH, 1998.
- [105] US Department of Defense. MIL-P-1629 - Procedures for performing a failure mode effect and critical analysis. Technical report, 1949.
- [106] Riccard Andersson. Failure Mode, Effect, and Diagnostics Analysis of the ESS Beam Interlock System, ESS Internal Document (ESS-00110714). 2015.
- [107] Nancy Leveson. *An STPA Primer*. 2013.
- [108] Blandine Antoine. *Systems Theoretic Hazard Analysis (STPA) Applied to the Risk Review of Complex Systems: An Example from the Medical Device Industry*. PhD thesis, Massachusetts Institute of Technology, 2013.
- [109] Philip Asare, John Lach, and John A. Stankovic. FSTPA-I: A formal approach to hazard identification via system theoretic process analysis. *ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2013*, 2013.
- [110] John Thomas. Systems Theoretic Process Analysis (STPA). *MIT Presentation*, 2015.
- [111] Asim Abdulkhaleq, Stefan Wagner, Daniel Lammering, Hagen Boehmert, and Pierre Blueher. Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles. *Lecture Notes in Informatics, Gesellschaft für Informatik, Bonn 2016*, 2017.
- [112] The Resilience Engineering Association. <http://www.resilience-engineering-association.org/>, 2017.

- [113] Erik Hollnagel. *FRAM - The Functional Resonance Analysis Method Centre for Quality*. Centre for Quality, Region of Southern Denmark, 2014.
- [114] Erik Hollnagel. The Functional Resonance Analysis Method, <http://functionalresonance.com/>, 2016.
- [115] International Electrotechnical Committee. IEC 61882:2002 Hazard and operability studies (HAZOP studies) - Application Guide. 2002.
- [116] Thilo Friedrich, Christian Hilbes, and Annika Nordt. Systems of Systems Engineering for Particle Accelerator based Research Facilities - A case study on engineering Machine Protection. *Proceedings of 11th Annual IEEE International Systems Conference*, 2017.
- [117] Dave Gurd. SNS Machine Protection System Final Design Review. *Presentation at SNS Machine Protection System Final Design Review*, 2001.
- [118] E Blanco, S Karstensen, T Ladzinski, J Lindkvist, T Lensch, A Marqueta, D Mcginnis, A Nordt, D Piso Fernandez, F Plewinski, I Romera, R Schmidt, A Vergara, M Werner, F Valentini, M Zaera Sanz, and M Zerlauth. Summary of Discussions. *Workshop on PLC Based Interlock Systems for Accelerators and Other Large Research Installations*, 2013.
- [119] Rüdiger Schmidt. Machine Protection. *CAS Update*, 2013.
- [120] Riccard Andersson, Angel Monera-Martinez, Annika Nordt, and Enric Bargalló. A Modified Functional Safety Method for Predicting False Beam Trips and Blind Failures in the Design of the Ess Beam Interlock System, paper MOPGF126. *Proceedings of ICALEPCS2015*, 2015.
- [121] R Andersson, E Bargalló, and A Nordt. Development of an Analysis Framework for the Beam Instrumentation Interface to the Beam Interlock System at ESS, paper THPOY039. *Proceedings of IPAC2016*, 2016.
- [122] Riccard Andersson, Szandra Kövecses, and Enric Bargalló. Challenges in Technical Risk Management for High-Power Accelerators, paper P1-03. *Proceedings of ICANS XXII*, 2017.
- [123] Enric Bargalló, John Haines, and Roland Garoby. ESS Neutron Source Reliability and Availability Requirements, ESS Internal Document (ESS-0064499). 2016.
- [124] E. Bargalló, R. Andersson, A. Nordt, A. De Isusi, E. Pitcher, B. Yndemark, P. Sångberg, and A. Pettersson. ESS reliability and availability requirements, ESS Internal Document (ESS-0008886). 2015.
- [125] International Electrotechnical Committee. IEC 61511 Part 2 - Guidelines for the application of IEC 61511 Part 1. 2004.
- [126] International Organization for Standardization. ISO 31010: Risk management - Risk assessment techniques. 2016.

- [127] International Electrotechnical Committee. IEC 61508 Part 5 - Examples of methods for the determination of safety integrity levels. 2010.
- [128] International Electrotechnical Committee. IEC 61508 Part 4 - Definitions and Abbreviations. 2010.
- [129] European Standard EN 50128: Railway applications - Communication, signalling and processing systems. 2011.
- [130] Christian Hilbes and Annika Nordt. Machine Protection - Systems Requirements and Architectural Framework, ESS Internal Document (ESS-0057251). 2015.
- [131] Christian Hilbes and Annika Nordt. MP Beam Interlock System - System Requirements Specification, ESS Internal Document (unpublished). 2015.
- [132] Martin Rejzek and Christian Hilbes. Fast Beam Interlock System (FBIS) Concept of Operations, ESS Internal Document (under review). 2017.
- [133] Timo Korhonen and Javier Garcia Cereijo. ESS Timing System, ESS Internal Document (ESS-0088633). 2017.
- [134] EPICS Community. <http://www.aps.anl.gov/epics/>, 2017.
- [135] C Sibley. Machine Protection Strategies for High Power Accelerators. *Proceedings of PAC2003*, 2003.
- [136] Naja de la Cour. Target Station Systems at ESS (image). 2015.
- [137] Ryoichi Miyamoto and Mohammad Eshraqi. How to estimate the possible max angle for studies of BLM and MPS, <https://jira.esss.lu.se/browse/BPWP-328> (access required), 2016.
- [138] Daniel Lundgren. MEBT Buncher Entrance Aperture (image). 2016.
- [139] Jens Harborn. Target Helium Cooling Systems Requirements, ESS Internal Document (ESS-0012524). 2016.
- [140] Leif Emås. HAZOP - Target Primary Cooling System, ESS Internal Document (ESS-0045961). 2016.
- [141] Kristoffer Sjögreen and Jens Harborn. System Description Document - Requirements for Target Wheel, Drive and Shaft, ESS Internal Document (ESS-0020435). 2017.
- [142] Leif Emås. HAZOP - Target Wheel X-Y-Z movement, ESS Internal Document (ESS-0084807). 2016.
- [143] Leif Emås. HAZOP - Target Wheel Rotational speed, ESS Internal Document (ESS-0081414). 2016.
- [144] Jens Harborn. P&ID System 1000 - Target Wheel, Drive and Shaft, ESS Internal Document (ESS-0023965). 2016.

- [145] Benedetto Gallese, Daniel Lyngh, Daniel Piso Fernandez, Eric Pitcher, and Timo Korhonen. ICD between ICS and Target Liquid Hydrogen System, ESS Internal Document (ESS-0084977). 2017.
- [146] Leif Emås. HAZOP - System 1100 - Cryogenic Moderator System, ESS Internal Document (ESS-0092008). 2017.
- [147] Leif Emås. HAZOP - Water Moderators Primary Cooling System, ESS Internal Document (ESS-0043423). 2015.
- [148] Allan Lundgren. Water Moderator Primary Cooling System, ESS Internal Document (ESS-0018268). 2016.
- [149] Allan Lundgren. Reflector Primary Cooling System, ESS Internal Document (ESS-0018280). 2016.
- [150] Allan Lundgren. P&ID - Water Moderators Primary Cooling System, ESS Internal Document (ESS-0040857). 2016.
- [151] Allan Lundgren. P&ID - Reflectors Primary Water Cooling System, ESS Internal Document (ESS-0040861). 2016.
- [152] Y Lee, A Olsson, M Eshraqi, R Miyamoto, M Möller, T Shea, C Thomas, M Wilborgsson, S Ghatnekar Nilsson, S Molloy, Y Levinsen, and F Sordo. Working Concept of 12.5 kW Tuning Dump at ESS, paper THPVA065. *Proceedings of IPAC2017*, 2017.
- [153] ESS Insight/JIRA Risk Tracker. <https://jira.ess.lu.se/secure/ObjectSchema.jspx?id=5> (access required), 2017.
- [154] Sparx Systems. Enterprise Architect, <http://www.sparxsystems.eu/start/home/>, 2017.
- [155] Riccard Andersson and Enric Bargalló. Simulation of Availability and Cost Impact of Machine Protection, ESS Internal Document (ESS-0149489). 2017.
- [156] ReliaSoft. BlockSim, <http://www.reliasoft.com/BlockSim>. 2015.

Appendix A - Core Scientific Papers

This appendix contains the four core scientific papers listed in the thesis Preface and referred to as Paper I, II, III, and IV in the text, in that order.

MACHINE PROTECTION SYSTEMS AND THEIR IMPACT ON BEAM AVAILABILITY AND ACCELERATOR RELIABILITY

R. Andersson, A. Nordt, E. Bargalló, European Spallation Source, Lund, Sweden
E. Adli, University of Oslo, Norway

Abstract

Over the last decades, the complexity and performance levels of machine protection have developed. The level of reliability and availability analysis prior to operation differs between facilities, just as the pragmatic changes of the machine protection during operation. This paper studies the experience and development of machine protection for some of the state of the art proton and ion accelerators, and how it relates to reducing damage to and downtime of the machine. The findings are discussed and categorized, with emphasis on proton accelerators. The paper is concluded with some recommendations for a future high power linear proton accelerator.

INTRODUCTION

As the users of previous generations of research accelerators were mainly the actual developers, only the accelerator physicists themselves were concerned by the lack of protection. However, as the concept of user facilities was incorporated in the 70s, research in other fields became dependent on the accelerators performing as designed [1,2]. With this came higher demands on the machines to be more reliable and available [3]. However, even up to today, though the concepts of reliability and availability are targeted at an early stage, the main goal is still to push the beam parameters beyond existing limits. Once this goal is fulfilled, the machine reliability and beam availability receive more attention.

Because of the very high beam powers and energies in current and future accelerators [3–7], the risk of beam-induced damage is significant. In as little as a few microseconds, the energy from a deposited beam could lead to permanent damage or melting of the equipment [8]. For dealing with this, efficient protection systems need to be implemented together with appropriate monitoring. The beam interlock systems (BIS), receiving beam permit signals from the monitors, play a central role in these protection systems. The BIS creates an overall beam permit signal, which defines if beam operation will be continued or inhibited. For hazards not directly related to beam-induced damage, more sophisticated and flexible local protection systems could be implemented, which act between the monitors or sensors and the beam interlock system.

This paper looks into current state of the art proton and ion accelerator facilities and discusses their machine protection (MP) based on analysis prior to operation, pragmatic changes of the MP, and other measures of improvement.

RELIABILITY AND AVAILABILITY

Two figures to measure the performance of a system are reliability and availability, and this paper uses the following definitions [9].

Reliability is the probability of fulfilling the major design function (MDF) of the system, continuously and without interruptions, for a predefined period of time – for example one hour or one day. Mathematically, reliability is defined as $R(t) = e^{-\lambda t}$, where λ is the failure rate and t the predefined time period.

Availability is the probability to find the machine fulfilling its MDF, when it is claimed to be in operation. Mathematically, and after an extended period of operation (years), the availability can be calculated as $A(t) = 1 - MTBF / (MTBF + MDT)$, where $MTBF$ is mean time between failures and MDT is the mean downtime.

For user facilities especially, where the users are dependent on the accelerator operating as it should, those two figures of merit account to a large extent for the user satisfaction of the facility, and the aim for MP should be to have those numbers optimized.

STORAGE RINGS AND LINACS

The typical solution for MP to avoid beam-induced damage is to stop beam operation. Synchrotrons, such as the Large Hadron Collider (LHC), have the entire beam stored in its storage ring. The only option for protection in case of a hazardous fault is to extract and dump the beam, and then restart the injection and acceleration process [10]. This generally leads to low availability numbers, as much of the operational time is needed to inject and accelerate the beam up to nominal energy [11]. Therefore, the MP reliability has to be very high in order to avoid false dumping procedures.

Linacs, such as the superconducting linac at the Spallation Neutron Source (SNS), tend to aim for high average power, meaning a constant delivery of beam pulses without major interruptions. The advantage of such pulsed machines is, if an error occurs, the ability to ‘skip’ individual or groups of pulses or run in a degraded mode, e.g. at lower beam current or lower repetition rates. When the problem has been resolved, operation can continue as before. For this reason, high-power linacs tend to achieve higher beam availabilities than high-energy proton and ion storage rings. However, putting this simple idea into practice needs an advanced strategy for MP.

Comparing the two types of machines gives that storage rings tend to have a stronger connection between accelerator reliability and beam availability, due to the inevitable downtime associated with each beam dump.

For linacs, on the other hand, accelerator reliability and beam availability are less intertwined in that there is no required downtime for each beam stop, which puts higher pressure on fast beam recovery after a fault. It goes without saying, however, that both types need to aim for high accelerator reliability figures for satisfactory operation.

ARCHITECTURE OF MP

The general architecture for modern MP is a set of local protection systems and monitors that send beam permit signals into a BIS, which combines the different beam permits into a global beam permit, allowing for beam operation. There are strict, hardwired connections between critical equipment and the BIS, together with a software layer for performance optimization.

To achieve successful MP, a post-mortem system that collects data from the faults that cause a beam trip is essential, as well as methods for early fault detection. Within the scope of MP, surrounding features such as preventive maintenance procedures are also included [12].

CURRENT STATE OF THE ART FACILITIES

LHC

CERN is a research organization that has put time, money, and effort into studies and analyses on how to achieve high accelerator reliability and beam availability numbers for systems related to MP [10]. LHC (operative since 2009) has a daisy chain beam interlock system design that has been successful in its performance. It contains a combination of hardware and software interlocks feeding beam permit signals into the BIS.

The detailed design of the MP at LHC received much attention prior to setup [10,13]. Much effort and simulation studies were put together in order to design a robust and reliable BIS as well as critical input systems. This has led to very few false beam trips and the architecture has been the foundation of other machines, such as Linac 4 and the European Spallation Source (ESS). As LHC has been operational over the past years, new ideas and solutions have arisen and been implemented, but the basic concept stays the same.

One of the major MP issues for LHC is the need to push the limits of the hardware in order to reach nominal energies. Each small increase in beam energy implies a higher damage potential that needs to be considered. Even though rigorous analyses were carried out prior to commissioning, some problems arose that were not accounted for and were hard to foresee. One of these is the so-called unidentified falling objects (UFO) [14]. These objects, presumed to be dirt particles, obstruct the beam path and cause beam losses.

To keep track of and analyze beam trips, the LHC implemented an e-logbook where the cause for each beam dump is noted down in detail. However, some faults are

not immediately understood and often an expert is needed for providing a detailed analysis and finding the root cause. This is time consuming and sometimes happens several weeks after the actual fault. For the restart of LHC in 2015, there is an upgraded and automatic version of the e-logbook, which is believed to improve the performance of the post-mortem analysis [15].

In 2005, there were substantiated predictions made on the failure rate of a number of MP-relevant systems for the LHC. These turned out to be very accurate [16], and have been used as goals to meet and guidelines on how reliable a system needs to be. Through better understanding, dedicated tests, and more detailed simulations during the operational period, it has been found that some of the BLM thresholds were initially set too conservatively and that damage or quenches did not occur at the beam loss levels that were predicted. With this information, the dedicated BLM thresholds were relaxed, the sensitivity to false beam dumps was lowered, and the reliability of the machine went up.

SNS

SNS is a high-power (1 MW) neutron spallation facility that started its operation in 2006. It is a collaboration of six labs, involved in and responsible for different components and systems. The operational start of SNS was not preceded by rigorous MP analyses, which became apparent in the first years of operation. However, many improvements have been made during the operational period and accelerator reliability and beam availability numbers have increased steadily [17].

SNS took much of their MP design from previous experience of other laboratories [5]. However, as SNS greatly surpassed previous similar facilities in terms of beam power, there were many complications in the first years of operation. Many of which were due to the collaborative approach of six different labs responsible for different areas in the construction, integration, and coordination of the machine [18].

The SNS MPS uses the concept of a pilot beam, which is a pulse of less than nominal power that checks that everything is in order before full-scale operation is continued after each beam drop [5]. In addition, there is a beam parameter check between each pulse during regular operation, which makes sure that the maximum inter-pulse difference (MAID) of the beam parameters is not above threshold [3]. In case of mismatched beam parameters, the next pulse is inhibited from being injected to the linac.

The SNS MPS has a post-mortem system that collects data when neutron production is on, but only automatically saves the beam trip if it lasts longer than three minutes. There has been an effort to implement an e-logbook for storing fault information, but since this is not automatized at this stage and is dependent on operators manually entering the information, it is partially incomplete [19].

It has been suggested that an automatic reset of the linac in case of a fault would be able to keep some

downtimes below one second. As of now, there is instead a division into the fast protect system between the latched system (FPL), needing manual intervention, and the auto reset system (FPAR), doing what the name suggests [5]. There is also a duality for setting the beam loss thresholds, where the integration time for beam losses is set in the hardware, and the trip point limits and masking capabilities are set in the software, being EPICS [20]. The system itself is flexible in terms of possibilities to add and delete sensors and to bypass the hardware configuration using software inputs. This has helped in the commissioning of the machine, but also adds more complexity and lack of robustness in the machine protection system.

Other Facilities:

CEBAF, SLAC, HERA, and J-PARC

For the Continuous Electron Beam Accelerator Facility (CEBAF), just as for Linac Coherent Light Source-I (LCLS-I) and II, flexibility in the beam interlock system has been a priority [21–23]. This has been a key feature in order to allow for changes and additions to be made on the system. The flexibility of the LCLS MP (both I and II use the same setup) allows for running in degraded mode by lowering the repetition rate of the pulses, in order to keep beam availability numbers up even when a fault is detected. As soon the fault is recovered, the beam is ramped up to nominal power [24]. However, the flexibility in LCLS has also made the beam interlock system and its connecting devices a complex matter, where there are four different kinds of link nodes and many layers included in the communication between the central link processor and the devices – with the need for a special team to support and maintain this system.

Throughout the operational period of the Hadron Elektron Ring Anlage (HERA), availability increases were sought after and achieved through preventive maintenance and improved fault diagnostics. Special attention was paid towards the new technology in the accelerator itself, and the final result was that there were actually more problems with the conventional systems, something that was claimed to be underestimated in the design. The beam interlock system had very low flexibility, which caused a lot of trouble combined with the old controls software that was ‘reused’ for HERA [25,26].

J-PARC has a clear hierarchical structure of the MPS, where a software control system layer is implemented to try to avoid MP actions and excessive use of the actuation system, in order to keep a high reliability and availability [27]. Prior to operation, J-PARC made detailed reliability studies on e.g. the klystrons, and found exact figures on the number of component failures per year [28]. They also found proofs that these component failures tend to follow an increased rather than a constant failure rate distribution.

RECOMMENDATIONS FOR FUTURE MP DESIGNS

From the experience of current state of the art accelerator facilities, the involvement of too many labs in the construction and delivery of equipment tends to lead to complications in terms of responsibility and integration. SNS experienced much trouble in the start with failing systems that had to be exchanged [29]. However, there is a general experience among accelerator facilities that the first few years are much worse in terms of reliability and availability [11,26,29]. As child diseases are cured, thresholds are adjusted, and the operations team has learned from previous mistakes and gets to know the machine, the numbers tend to increase.

There is also a tendency for unexpected faults and beam losses to occur, which were not accounted for in the pre-operational analysis – especially when beam energy and beam power is increased unprecedentedly. Examples are the UFOs in LHC and the slow energy deposit at SNS. These problems had to be accounted for once higher energies and powers were reached, and it is recommended that new machines stay aware and observant of unexpected beam losses. On the other hand, as with the HERA experience, a too comfortable approach towards less advanced conventional systems may also be a danger and lead to unforeseen downtimes.

Discussions on machine downtime issues often lead to the topic of lacking redundancy as an overall flaw among accelerators. Adding redundancy is one of the most frequent approaches to deal with unstable or error-prone equipment, such as power supplies and RF equipment [10,15,30]. It is also suggested that a well thought-through alarm handling strategy is implemented, in order to increase the effectiveness of MP.

The number of MP inputs is in the region of several thousands. Naturally, many of these inputs might fail or send spurious signals. To deal with this, especially during commissioning, a masking method should be present to make operation possible, even with equipment firing erroneous signals [12].

CONCLUSIONS

The different ways of stopping beam operation for storage rings and linacs give different relations between accelerator reliability and beam availability, where storage rings have a closer connection between the two. It is found that rigorous analyses before commissioning of an accelerator is very beneficial to the accelerator reliability, and expert experience from other facilities can only be a first top-level prediction of the design.

Newer facilities have unprecedented beam powers and energies and the upcoming faults are difficult to foresee. This needs to be considered, and planning for redundancy at an early stage is crucial to have successful operation. It is also recommended to stay observant of unexpected problems, as higher beam powers are reached. This should be dealt with using a well-designed alarm handling system, and making good use of post-mortem analyses.

REFERENCES

- [1] V. Ziemann, “Accelerator Physics and Technology”, pp. 1–141 (2011).
- [2] P. Bryant, “A Brief History and Review of Accelerators”.
- [3] C. Sibley, “Machine Protection Strategies for High Power Accelerators”, Proc. PAC03, pp. 607–611 (2003).
- [4] C. Adolphsen et.al. “The Next Linear Collider Machine Protection System”, Proc. PAC99, pp. 4–7 (1999).
- [5] C. Sibley et.al. “The SNS Machine Protection System: Early Commissioning Results and Future Plans”, Proc. PAC05, pp. 1727–1729, (2005).
- [6] A. Nordt, A. Apollonio, R. Schmidt, “Overview on the Design of the Machine Protection System for ESS”, Proc. IPAC2014 (2014).
- [7] P. Saha, “Operational Experience With J-PARC Injection and Extraction Systems”, Proc. HB2010, pp. 324–328, (2010).
- [8] M. Ross et.al. “Single Pulse Damage in Copper”, XX Int. Linac Conf., pp. 47–49, (2000).
- [9] E. Bargalló, “IFMIF Accelerator Facility RAMI Analyses in the Engineering Design Phase”, PhD thesis, Dep. Física i Enginyeria Nuclear, Univ. Politècnica de Catalunya, Spain (2014).
- [10] R. Filippini et.al. “Reliability Assessment of the LHC Machine Protection System”, Proc. 2005 Part. Accel. Conf., pp. 1257–1259, (2005).
- [11] A. Macpherson, “LHC Availability and Performance in 2012”, LHC Beam Operation Workshop - Evian 2012 (Evian-2012-12, 2012).
- [12] C. Hilbes, A. Nordt, “ESS Machine Protection Functional Architecture Concept”, ESS Internal Report ESS-2015-02, 2015.
- [13] B. Todd, M. Kwiatkowski, “Risk and Machine Protection for Stored Magnetic and Beam Energies”, CERN Acc. School: Power Converters (CERN-2014-05, 2014).
- [14] T. Baer et.al. “UFOs in the LHC After LS1”, Chamonix Work. LHC Perform., pp. 294–298, (2012).
- [15] M. Zerlauth, “Private conversations” (2015).
- [16] B. Todd, “A Look Back on 2012 LHC Availability”, LHC Beam Oper. Work. Evian (2012).
- [17] M. Plum, “Beam dynamics and beam loss in linacs”, JAS14 (2014).
- [18] A. E. Pitigoi and P. Fernandez Ramos, “Reliability model of an existing accelerator (SNS linac)”, Eur. Comm. Rep., no. 269565 (2012).
- [19] C. Peters, “Private email conversation” (2014).
- [20] D. Gurd, “SNS Machine Protection System Final Design Review Introduction”, Machine Protection System Final Design Review (SNS-2001-09, 2001).
- [21] C. Hovater et al., “Operational Experience with the CEBAF Control System”, Proc. XVIII Int. Linac Conf., pp. 616–620, (1996).
- [22] J. Dusatko et.al. “Development of the Machine Protection System for LCLS-I” (2011).
- [23] M. Boyes, “LCLS-I/LCLS-II Machine Protection System Overview”, EPICS Collaboration Meeting Fall 2012, (PAL-2012-10, 2012).
- [24] S. Norum et.al. “The Machine Protection System for the Linac Coherent Light Source,” Proc. PAC09, pp. 4856–4858 (2009).
- [25] F. Willeke, “What can be learned from HERA Experience for ILC Availability”, 2005 Int. Linear Collider Physics and Detector Workshop, (Snowmass-2005-08, 2005).
- [26] J. Keil, “Operational Experience With HERA”, Proc. PAC07, pp. 1932–1934 (2007).
- [27] Yoshikawa, “Machine Protection System for j-parc,” Acc. TAC 2004 (2004).
- [28] K. Hasegawa et.al. “Operating Experience of the J-PARC Linac,” Proc. LINAC08, pp. 55–57 (2008).
- [29] R. Cutler and et.al., “Oak Ridge National Laboratory Spallation Neutron Source Electrical Systems Availability and Improvements,” Proc. PAC2011, pp. 1337–1339 (2011).
- [30] O. Nobuo, “Status Report of J-PARC,” J. Korean Phys. Soc., vol. 56, no. 6, pp. 1921–1927, June (2010).

DEVELOPMENT AND STATUS OF PROTECTION FUNCTIONS FOR THE NORMAL CONDUCTING LINAC AT ESS

R. Andersson[†], E. Bargalló, S. Kövecses, A. Nordt, M. Zaera-Sanz

European Spallation Source ERIC, Lund, Sweden

C. Hilbes, M. Rejzek, ZHAW, Winterthur, Switzerland

[†]University of Oslo, Norway

Abstract

The European Spallation Source faces a great challenge in succeeding with its ambitious availability goals. The aim is to construct a machine that allows for 95% availability for neutron beam production. This goal requires a robust protection system that allows for high availability by continuously monitoring and acting on the machine states, in order to avoid long facility downtimes and optimize the operation at any stage. The normal conducting section consists of the first 48 meters of the machine, and performs the initial acceleration, bunching, steering, and focusing of the beam, which sets it up for optimal transition into the superconducting section. Through a fit-for-purpose risk management process, a set of protection functions has been identified. The risk identification, analysis, and treatment were done in compliance with modern safety and ISO standards. This ensures that the risks, in this case downtime and equipment damage, are properly prevented and mitigated. This paper describes this process of defining the protection functions for the normal conducting linac at ESS.

INTRODUCTION

The high neutron production availability goals of ESS require the linear proton accelerator (linac) to produce, bunch, accelerate, steer, and focus the proton beam with high quality and reliability. The first 48 meters consist of normal conducting (NC) structures, and this is the most critical part of the accelerator as the options for retuning or adjustments are minimal. It is critical that the proton beam envelope as well as its beam energy are exact at the exit of the last NC structure to allow for further acceleration and transport, through the superconducting (SC) parts, to the tungsten target wheel. An overview schematic of the ESS linac is seen in Figure 1.

The NC linac, constituting the five leftmost blocks in Figure 1, consists of a 75 keV ion source, low energy beam transport (LEBT) structure, radio-frequency quadrupole (RFQ), medium energy beam transport (MEBT), and five drift tube linac (DTL) tanks. After leaving the last DTL tank, the beam energy is 90 MeV. The proton beam will, at nominal operation and upon exiting the MEBT, have a 2.86 millisecond pulse length with 14 Hz repetition rate [1].

[†] riccard.andersson@ess.se

AVAILABILITY-DRIVEN MACHINE PROTECTION

Machine protection (MP) at ESS has been identified as an important driver for successfully reaching the availability goals of the facility [2]. The MP strategy is to identify and analyze systems and devices that play a role in this goal and, based on the outcome, adapt their functional behavior accordingly. MP is thus classified as a system of systems (SoS) [3], recognizing the complexity of and interactions between several systems that all need to fulfill their role for the overall MP-SoS to succeed.

In order to identify key functions of the MP-SoS, an ESS MP risk management process lifecycle has been developed that identifies and analyzes so-called *damage events* throughout the machine [4]. A damage event is an event that has a facility *downtime* (loss of neutron production) and a *cost* associated to it, whose combination creates a severity category. Based on that severity, the appropriate MP measures are taken. These damage events are then associated with a set of *hazards* that are to be prevented or mitigated by *overall protection functions* (OPF). The risk management process follows the IEC 61508 standard for functional safety [5], as well as the ISO 31000 risk management standard [6].

As the NC linac is found to be critical for the quality and availability of the proton beam, and in extension neutron production at ESS, this part of the machine has been analyzed by the ESS MP team together with the respective system experts to identify damage events, hazards, OPFs, and technology-specific *protection functions* (PF) where applicable. These PFs are then to be implemented into the MP-SoS by making use of the constituent systems as described below.

MP-RELATED NC LINAC SYSTEMS AND DAMAGE EVENTS

The MP-related systems in the NC linac are identified as the linac magnets, interceptive devices, vacuum system, and buncher cavities. In addition, the beam monitoring system is included in several PFs as it is able to monitor the necessary beam parameters, but it does not have any damage events associated to it. These systems are briefly described below.

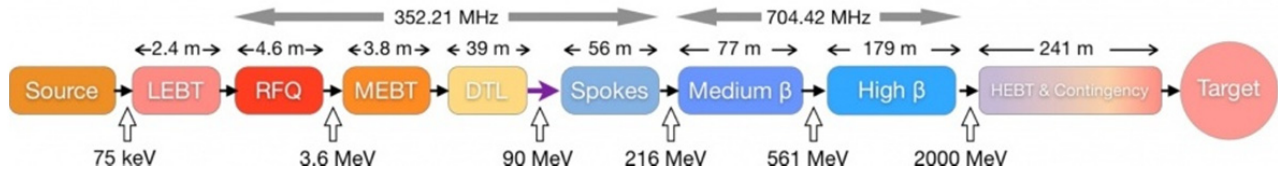


Figure 1: The ESS linac with its different sections, including lengths and nominal beam energies. Source: esss.se/accelerator.

Linac Magnets

The linac magnets consist of quadrupole magnets for focusing and dipole magnets for steering the beam. These are placed together, where the dipoles are located inside the quadrupoles. The quadrupoles are located in FODO lattices for alternated focusing in the two transversal directions. In the NC linac, there are 11 magnet pairs, all located in the MEBT. The damage events associated with these magnets are overheating in case of insufficient water cooling or overcurrent from the power supplies, as well as degradation or damage from particle losses in the equipment.

Interceptive Devices

The category of interceptive devices (ID) includes everything that intercepts (goes into) the proton beam. At ESS, these are beam stops (BS), wire scanners (WS), emittance measurement units (EMU), beam scrapers (movable collimators), and an iris collimator. There is one BS in the LEBT, one in the MEBT, and two in the DTL. WS are located in three locations in the MEBT, and there is one EMU in the LEBT and one in the MEBT. The iris is located at the very beginning of the LEBT to adjust the beam current. All of these are designed to be able to take at least 50 μ s of beam at 1 Hz pulse repetition rate, but the LEBT BS is able to take the full beam. The BSs, EMUs, scrapers, and iris are water cooled, and can thus break from lack of cooling, identified as a damage event. All of the IDs (except for the LEBT BS) have a damage event where they receive too much beam. As a last damage event, the scrapers and WSs can break mechanically by being crushed against each other in the beam pipe.

Vacuum System

The main role of the vacuum system is to keep high quality vacuum conditions in the beam pipe and other areas, such as vacuum shielding. In order to prevent extensive vacuum pollution and equipment damage in case of vacuum losses, or during maintenance periods, there is a set of vacuum gate valves that separate beamline sections from each other when needed. One is located before the LEBT and one after, one before the MEBT and one after, as well as one after DTL tanks 2, 3, 4, and 5. These valves, when located upstream of the beam destination, cannot be closed when beam is operating and the damage event of beam hitting a gate valve is included in the MP analysis. Additionally, a mechanical damage event of the valves is identified and analyzed.

Buncher Cavities

There are three buncher cavities at ESS, located in the MEBT. Their role is, as the name suggests, to bunch the proton beam in order to match the downstream radio frequency structures, such as drift tubes and superconducting cavities. The buncher cavities are water cooled and have the damage event of overheating due to lack of cooling. From beam physics simulations [7], it is also found that buncher cavity 2 and 3 can be hit by the proton beam and deform.

PROTECTION FUNCTION DEFINITION

The definition of PFs follow a process defined in [4], where the damage events are analyzed for the hazards that may lead to damage. Each hazard is then assigned one OPF, which is a generic function to prevent or mitigate the specific hazard. Depending on the severity level of the hazard, the OPF needs to fulfill a certain level of robustness. Up until the OPFs, no technology-specific systems have been identified to treat the hazards. This is instead done in the next PF step, in collaboration between the MP analysis team, integration team, and the system owners (e.g. the vacuum engineers in the case of the vacuum system) in order to define appropriate and implementable functions. The hierarchical analysis flow is seen in Figure 2, starting at the system level.

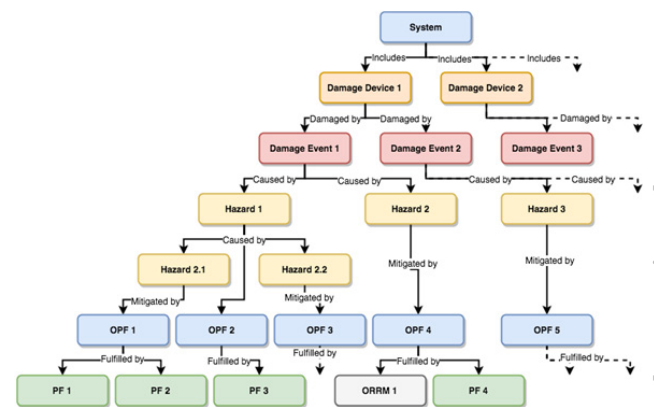


Figure 2: The MP analysis flow, from system, through damage device, damage event, hazards, overall protection functions (OPF), and protection functions (PF).

All of the PFs that are associated with stopping the proton beam to prevent damage will include the ESS beam interlock system (BIS) and a set of beam-stop actuators. The actuation consists in (a) inhibiting the timing system from generating a beam pulse, (b) activating the LEBT chopper and (c) MEBT chopper

continuously, and (d) interlocking the ion source magnetron. In the case of an emergency beam interlock, also the (e) power for the plasma generation and (f) proton extraction mechanisms of the ion source are cut [8]. The protection for all systems described in this paper, except for the buncher cavities, is coordinated by dedicated local protection systems (LPS), controlled by a safety PLC.

Each PF contains a sensor, logic element, actuator, timing requirement, and protection integrity level (PIL) [4,5]. The logic element for all functions is the LPS PLC (except buncher cavities and beam current monitoring) and BIS, and the actuators are as stated above. In the subsections below, the PFs for each system are mentioned and tabulated with their sensor, timing requirement and PIL.

Linac Magnets

The damage events from the linac magnets are handled by PFs that stop beam if the measured beam losses around the equipment are too high and that monitor the magnet temperature, supplied current, and cooling water flow to stop beam and power supply when necessary.

Table 1: Protection function sensor, timing, and PIL for the linac magnets.

Sensors	Timing	PIL
Differential Beam Current Monitors	30 μ s	1
Neutron Beam Loss Monitors	-	0
Thermo-switches	100 ms	1
Current monitors	100 ms	0
Cooling water flow meters	1 s	0

Interceptive Devices

The hazard and risk analysis identifies that inserting a beam of too high current, repetition rate, or too long pulse length while an ID is in has to be prevented, just as inserting an ID if incompatible beam is already running. This can be handled through ID position switches and beam mode consistency checks by the BCMs during beam operation. The water-cooled IDs have the cooling monitored, and the EMUs and iris are also required to have temperature sensors. The scrapers monitor the charge deposition through a dedicated monitor. Finally, beam position monitors (BPM) check whether the beam is in the correct path.

Table 2: Protection function sensor, timing, and PIL for the interceptive devices.

Sensors	Timing	PIL
Position switch (out)	100 ms	2
Position switch (in)	100 ms	1
Proton Beam Mode Consistency	100 ms	1
Cooling water flow meters	1 s	0
Cooling water temperature meters	1 s	1
EMU temperature sensor	1 s	0
Iris temperature sensor	1 s	0
Scraper charge deposition monitor	30 μ s	1
BPM	30 μ s	0

Vacuum System

The vacuum valves cannot be in the pipe while beam is running, and thus have to be extracted before starting beam operation. Just as beam has to be stopped if they are inserted. This is handled by position switches on the valves and through monitoring the dedicated (vacuum interlock) signal that closes the valves.

Table 3: Protection function sensor, timing, and PIL for the vacuum system.

Sensors	Timing	PIL
Position switch (out)	100 ms	2
Position switch (in)	100 ms	1
Vacuum interlock signal	1 s	0
Fast valve controller	3 ms	1

Buncher Cavities

Protection of the buncher cavities is done through measuring the surrounding beam losses in the same way as for the linac magnets, monitoring the beam position fluctuations through BPMs, and monitoring the cooling water flow and temperature and stopping beam if these are wrong.

Table 4: Protection function sensor, timing, and PIL for the buncher cavities.

Sensors	Timing	PIL
Differential Beam Current Monitors	30 μ s	1
Cooling water flow meters	1 s	0
Cooling water temperature meters	1 s	1
BPM	30 μ s	1

CONCLUSIONS

The tough availability requirements on ESS has made machine protection an important tool for the success of the facility. By avoiding long downtimes and costly repairs, the facility can operate at a high power during extended periods of time. The machine protection risk management process that has been developed at ESS is found suitable for the analysis of damage events throughout the facility and ties those to custom protection functions. This paper has presented the protection functions associated to the normal conducting linac and briefly described the process behind their derivation. As the design of the facility is ongoing, the analysis and implementation of protection functions need to be flexible yet robust, and more iterations are foreseen before the complete set can be finalized.

ACKNOWLEDGEMENTS

The authors thank all of the ESS colleagues in the accelerator and ICS divisions that have helped in the analysis of the related systems. This paper has been developed as part of a PhD thesis at the Department of Physics, University of Oslo, sponsored in part by the Norwegian Research Council (Project 234239/F50).

REFERENCES

- [1] Peggs S. (ed.), *ESS Technical Design Report*, ISBN: 9789198017328, 2013.
- [2] Hilbes C., Nordt A., *Machine Protection - Systems Requirements and Architectural Framework*, ESS Internal Document (ESS-0057251), 2015.
- [3] Friedrich T., Hilbes C., Nordt A., *Systems of Systems Engineering for Particle Accelerator based Research Facilities - A Case Study on Engineering Machine Protection*, *SysCon 2017*, Montreal, Canada, 2017.
- [4] Andersson R., Bargalló E., Hilbes C., Nordt A., *Machine Protection Risk Management Process*, ESS Internal Document (ESS-0095000), 2017.
- [5] IEC 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2010.
- [6] ISO 31000: *Risk management - Principles and guidelines*, 2009.
- [7] Miyamoto R., How to estimate the possible max angle for studies of BLM and MPS, <https://jira.esss.lu.se/browse/BPWP-328> (access required, taken 2017-05-02), 2016.
- [8] Rejzek M., Hilbes C., *Fast Beam Interlock System (FBIS) Concept of Operations*, ESS Internal Document (to be published), 2017.

MACHINE PROTECTION RISK MANAGEMENT OF THE ESS TARGET SYSTEM

R. Andersson^{1,†}, E. Bargalló, L. Emås, J. Harborn, A. Lundgren, U. Odén, J. Ringnér, K. Sjögren
European Spallation Source ERIC, Lund, Sweden
¹also at University of Oslo, Norway

Abstract

The European Spallation Source target system is, together with the proton linac, the main component in the spallation process. ESS will use a 4-ton, helium-cooled, rotating tungsten target for this purpose, and its protection and availability is paramount to the success of ESS. High demands are placed on all of the target equipment, including cooling, movement, rotation, and timing, in order to reach the facility-wide 95% availability goal for neutron production. Machine protection has defined a set of protection functions that are to be implemented for the target system. This paper describes the development of these protection functions through the use of classic HAZOPs combined with modern safety standard lifecycle management. The implementation of these functions is carried out through close collaboration between the target system owners and the machine protection group at ESS.

INTRODUCTION

The European Spallation Source (ESS) is to be ready for the first proton beam on target at the end of 2019. This initial operation requires the proton linear accelerator (linac) to be ready to accelerate and direct a 590 MeV beam to the 4-ton, helium-cooled tungsten target wheel. When fully operational, the proton beam will be delivered in 2.86 ms long pulses at 14 Hz repetition rate, and the energy is to reach 1.3 GeV. The target wheel is divided into 36 sections and will rotate so that a new section is hit for each beam pulse. The rotating speed is thus 14/36, or 0.39 Hz.

This initial phase will have an average proton beam power of 3 MW, which will create spallation and thermal neutrons to be moderated to the right energies and reflected towards the 15 experimental stations. In the process, a large amount of heat load will need to be handled by the target cooling system. The exact rotational speed is important for successful experiments and to keep the ESS operation successful. In order to deliver an unprecedented facility experimental availability, a tailor-made risk management process has been developed to cope with the many risks of running such a state of the art research facility, in order to balance equipment protection and system availability. This paper briefly describes this risk management method and its use within machine protection, and describes its application on the ESS target system.

[†] riccard.andersson@esss.se

MACHINE PROTECTION RISK MANAGEMENT AT ESS

Machine protection (MP) systems have held a key role in the success of modern accelerator facilities, such as the LHC, SNS, and J-PARC [1–3]. Their continuous development allows for increasingly fit for purpose solutions and MP plays a key role in avoiding lengthy facility downtimes due to damaged or activated equipment. Building on the success of MP for other facilities, ESS has developed a holistic approach to equipment protection that recognizes the interplay of many systems that are involved in fulfilling the protection goals. MP at ESS is viewed as a system of systems (SoS) and therefore applies some of these features [4].

Risk Management Process

The risk management process for MP at ESS is compliant with the ISO 31000 [5] and ISO 16085 [6] risk management standards as well as the key concepts from the IEC 61508 standard for functional safety [7]. This allows for the same approach, coordinated centrally by the MP personnel, to be taken towards all of the systems and equipment present at ESS, including the target system. The process focuses on managing *damage risk*, defined as a function of the *probability of occurrence* for a certain unwanted damage event, and its *consequence*. Further, the *consequence* has two parameters: the associated *cost* and *downtime*.

By identifying and analyzing each damage event and addressing each *hazard* that could lead to this damage event, through so-called *overall protection functions* (OPF), a *generic* set of objectives is first compiled and associated with each system. The OPFs are then subjected to audit by the associated MP personnel and system experts to derive technology-specific *protection functions* (PF), each containing one or more *sensors* that monitor the hazard, a *logic* element that takes the decision on whether action is required, and one or more *actuators* to carry out this action. In addition, the PFs include a *timing* requirement for how quickly the PF needs to be carried out, and a *protection integrity level* (PIL) that gives requirements on the quality of the PF [8].

All of the information and risk management process steps are required to be traceable and readily available for all interested parties. For these purposes, the collaborative Atlassian JIRA add-on Insight [9] is chosen as the official risk register during the analysis and design process. This allows for a continuous online work flow where all associated parts can follow and contribute to the analysis process. Once a set of PFs has finished its internal

iterations and suitability checks, it is documented and uploaded to the official ESS document management system for approval by the ESS machine protection committee (MPC).

Target System Architectural Setup

The target system is designed and delivered by different in-house and in-kind institutions, each one responsible for supplying the necessary equipment and instrumentation to operate according to specification. All of the constituent systems and their sensors are then integrated into the facility-wide control system framework EPICS 7 [10], whose interface is the designated target controls PLCs. Where relevant, as per the analysis presented in this paper, the sensor signals are split and also sent to the target protection system safety PLC. This PLC performs the initial data analysis and further distributes the signal to the ESS beam interlock system (BIS) when a beam stop is required, to prevent or mitigate a damage event. While all of the sensors are initially selected by the respective system designers, the ones involved in a PF are also checked for their suitability for protection purposes by the system designers and the MP personnel, after the first analysis iteration of PFs has been carried out.

ANALYZED TARGET SYSTEMS

The target system consists of several subsystems and support systems that fulfill specific tasks. The tungsten target itself needs to be adjusted to the correct position in three dimensions (a) as well as rotating with the correct speed during operation (b). The helium cooling system (c) needs to provide the correct cooling capacity to the tungsten target, while two primary water cooling systems (PWCS) provide cooling for the water moderators (d) and reflector structures (e). There is also a liquid hydrogen cryogenic moderator system (f) and a tuning dump system (g) that require attention from MP. These seven systems have been analyzed through individual hazard and operability analyses (HAZOP) by the target system experts, as well as through the ESS MP risk management method in collaboration between MP personnel and target system experts. Thus, the results presented in this paper are aimed at the following target systems:

- a) Target wheel XYZ movement
- b) Target wheel rotation system
- c) Target wheel helium cooling system
- d) Primary water cooling system – Moderators
- e) Primary water cooling system – Reflectors
- f) Cryogenic (LH₂) moderator system (CMS)
- g) Tuning beam dump

The analyses are grouped so that the target wheel (a, b, c) is analyzed as one entity, the PWCS (d, e) as one, while the cryogenic moderator system and tuning beam dump are analyzed individually.

RISK MANAGEMENT ANALYSIS AND PROTECTION FUNCTION DEFINITION

The risk management process identifies and analyzes the damage events that are to be prevented or mitigated. Thus, the support systems, such as the water and helium cooling systems, are rather providers of operationally profitable settings than systems to be analyzed in detail for damage events. It is the responsibility of the system owners to design robust and reliable systems in line with the ESS requirements. The devices that are vulnerable to damage events are thus the target wheel, moderators (water and LH₂), reflectors, and tuning dump. These systems are individually discussed in this section, and a table outlines the associated PFs for each system.

As these systems are already controlled by the control system framework and contain certain protection barriers of their own, categorized as other risk reduction measures (ORRM) in the MP risk management framework, in accordance with the IEC 61508 standard, the remainder of the protection functionality to be carried out by MP-specific PFs during operation are associated with stopping the proton beam in case of overheating equipment or too high system pressure levels. For the sake of brevity, the tabulated PFs in the following subsections do not contain the description and role of the logic elements (the target protection safety PLC and the BIS) and the actuators (timing system/ion source, LEPT chopper, MEBT chopper) as these are the same for all target system-related PFs [11].

Target Wheel

Table 1: Protection Functions for the Target Wheel

Protection Function	Sensor	Timing	PIL
Stop beam if the differential pressure measurements in the helium outflow from the target wheel is too high or too low	Pressure	1 sec	0
Stop beam if the helium mass flow out of the target wheel is too low	Flow	5 sec	0
Stop beam if the helium temperature is too high in the outflow from the target wheel	Temperature	2 sec	0
Stop beam if the target wheel monitoring plug infrared monitor shows too high temperature	IR monitor	1 sec	1
Stop beam if the rotational speed of the target wheel is below minimum or exceeds maximum	Inductive rotational encoder	100 ms	1
Stop beam if the target wheel rotation phase is erroneous	Optical phase monitor	2.5 sec	1

The target wheel associated damage events are overheating from lack of cooling, overheating from the proton beam hitting the wrong position, and mechanical damage [12–14]. While the mechanical damage can be handled to an acceptable level by ORRMs that lock the wheel position before operation, appropriate limit switches, and mechanical structures, the overheating events need to be handled by machine protection PFs. These PFs are seen in Table 1. The estimated values for timing, as well as the usage of sensors, are based on [15].

Water Moderators and Reflectors

The water moderators and reflectors contain similar PWCS water loops and are analyzed identically [16]. As they are designed for full beam power as a nominal setting, their overheating due to receiving too much proton beam is excluded. Their MP-related PFs are thus associated with water cooling of the equipment, listed in Table 2.

Table 2: Protection Functions for the Water Moderators and Reflectors

Protection Function	Sensor	Timing	PIL
Stop beam if the cooling water flow in the moderator or reflector inlet is too low	Flow	1 sec	1
Stop beam if the cooling water flow in the moderator or reflector outlet is too low	Flow	1 sec	1
Stop beam if the cooling water temperature in the moderator or reflector outlet is too high	Temperature	10 sec	1
Stop beam if the cooling water pressure in the moderator or reflector inlet is too high	Pressure	1 sec	1

Cryogenic Moderator System

The CMS contains rigorous internal controls and feedback and has the role to both supply the moderating medium (LH₂) and provide cooling. As the system is cryogenic with an operating temperature between 17 and 20.5 K, it requires vacuum shielding and is analyzed for pressure increases (due to lost vacuum) and lack of cooling for the moderators [17]. The PFs are listed in Table 3.

Tuning Beam Dump

To run the proton beam to the tuning beam dump, the beam power needs to be below 12.5 kW. This means that the beam dump can only take four nominal pulses at full power [18]. To prevent the event of a powerful beam running to the dump, the two dipole magnets in the accelerator-to-target area need to confirm that they are activated before high-power beam is allowed, which would send the beam to the target wheel. However, there

are two beam current monitors (BCM) in the beamline leading up to the beam dump, which are used for a PF as shown in Table 4.

Table 3: Protection Functions for the Cryogenic Moderator System

Protection Function	Sensor	Timing	PIL
Stop beam if LH ₂ flow in the moderator inlet is too low	Flow	1 sec	1
Stop beam if LH ₂ pressure is too high	Pressure (hydrogen)	1 sec	1
Stop beam if LH ₂ temperature in the moderator inlet is too high	Temperature	5 sec	0
Stop beam if LH ₂ temperature in the moderator outlet is too high	Temperature	5 sec	0
Stop beam if the CMS vacuum system pressure is too high	Pressure (vacuum)	5 sec	1

Table 4: Protection Functions for the Tuning Beam Dump

Protection Function	Sensor	Timing	PIL
Stop beam if the dump beamline BCMs detect a beam above 12.5 kW	BCM	280 ms	1
Stop beam if tuning dump temperature sensors notice too high dump temperature	Temperature	3 sec	0

CONCLUSIONS

To reach the high availability requirements of ESS, a holistic approach to machine protection is necessary. The method developed and presented in this paper is applicable to the target systems as well as the accelerator systems, and has derived a set of protection functions from the identified damage events related to operating the analyzed systems. The protection functions will be implemented in the design and commissioning of the ESS machine protection system of systems in the following years.

ACKNOWLEDGEMENTS

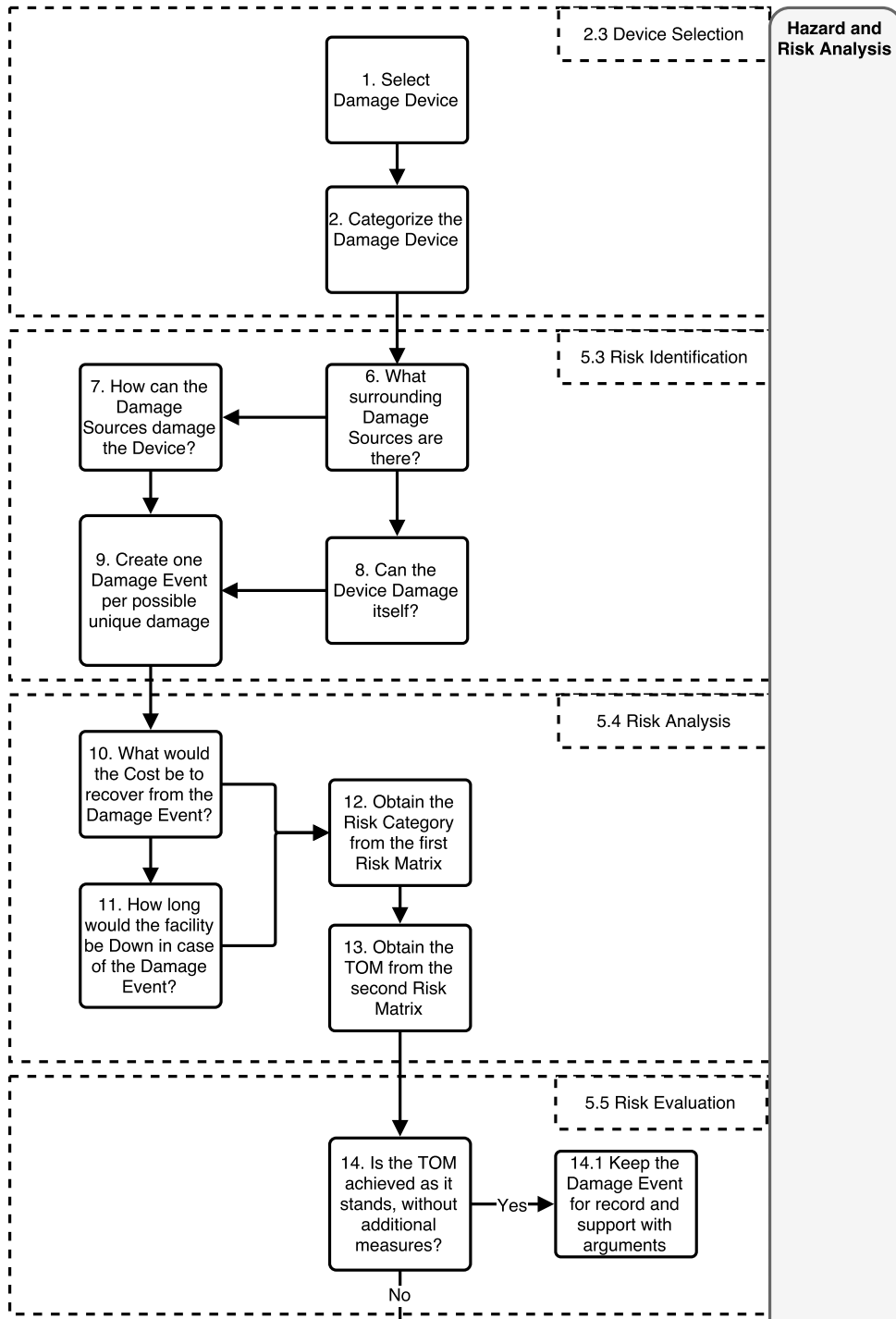
This paper has been developed as part of a PhD thesis at the Department of Physics, University of Oslo, sponsored in part by the Norwegian Research Council (Project 234239/F50).

REFERENCES

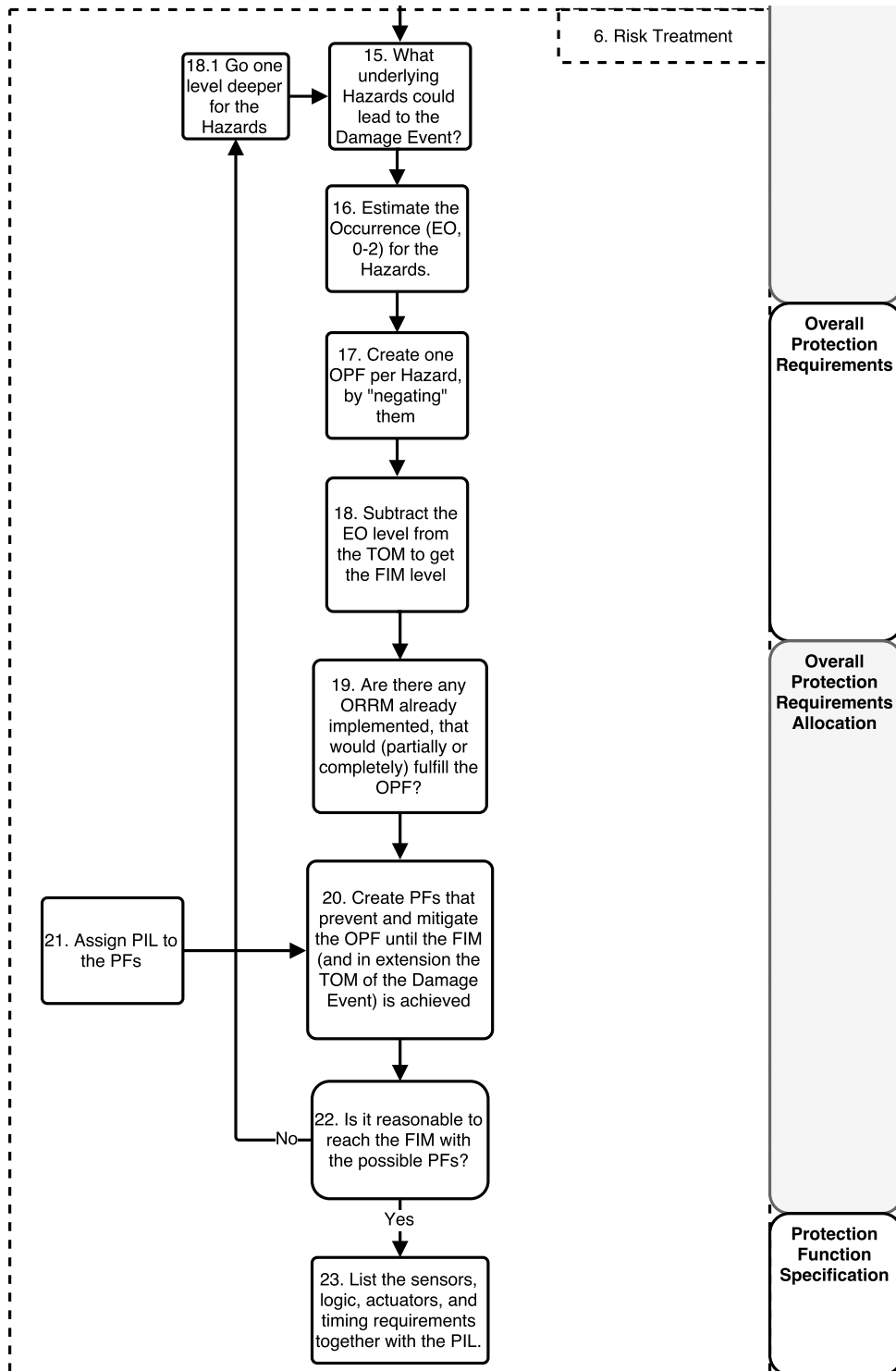
- [1] Andersson R., Nordt A., Adli E., Machine Protection Systems and Their Impact on Beam Availability and Accelerator Reliability, *IPAC2015*, Richmond, VA, USA, 2015.
- [2] Wenninger J., Machine Protection and Operation for LHC. *CERN Yellow Report 2016:377–401*, doi:10.5170/CERN-2016-002.377, 2016.
- [3] Schmidt R., Machine Protection. *CAS Update 2013:1881–3*, doi:10.1016/j.fusengdes.2013.05.065, 2013.
- [4] Friedrich T., Hilbes C., Nordt A., Systems of Systems Engineering for Particle Accelerator based Research Facilities - A Case Study on Engineering Machine Protection, *SysCon 2017*, Montreal, Canada, 2017.
- [5] ISO 31000: *Risk management - Principles and guidelines*, 2009.
- [6] ISO 16085: *Systems and software engineering - Life cycle processes - Risk management*, 2006.
- [7] IEC 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2010.
- [8] Andersson R., Bargalló E., Hilbes C., Nordt A., Machine Protection Risk Management Process, ESS Internal Document (ESS-0095000), 2017.
- [9] Riada AB, Insight for JIRA, <https://riada.se/insight>, 2017.
- [10] EPICS Community, <http://www.aps.anl.gov/epics>, 2017.
- [11] Hilbes C., Nordt A., Machine Protection - Systems Requirements and Architectural Framework, ESS Internal Document (ESS-0057251), 2015.
- [12] Emås L., HAZOP - Target Wheel X-Y-Z movement, ESS Internal Document (ESS-0084807), 2016.
- [13] Harborn J., HAZOP - Target Wheel Helium Cooling, ESS Internal Document (ESS-0081405), 2016.
- [14] Emås L., HAZOP - Target Wheel Rotational speed, ESS Internal Document (ESS-0081414), 2016.
- [15] Sjögreen K., Target wheel, drive and shaft description of loads and operational limits, ESS Internal Document (ESS-0060625), 2017.
- [16] Emås L., HAZOP - Water Moderators Primary Cooling System, ESS Internal Document (ESS-0043423), 2015.
- [17] Emås L., HAZOP - Cryogenic Moderator System, ESS Internal Document (ESS-0092008), 2017.
- [18] Lee Y., Olsson A., Eshraqi M., Miyamoto R., Möller M., Shea T., et al. Working Concept of 12.5 kW Tuning Dump at ESS. *IPAC2017*, Copenhagen, Denmark, 2017.

Appendix B - Steps of the Functional Protection Analysis Technique

This appendix displays a flowchart of the steps in the functional protection analysis technique (starting on the next page), as indicated by the left path of Figure 4.2. The flowchart is referred to on page 45 of this thesis. While the 23 steps in the flowchart can be used as a standalone guide, many of the questions asked and information to obtain require a deeper reading of Chapter 4 to make sense. The different steps are categorized into five dashed boxes, where the box numbers and titles are matched with the corresponding sections in the ISO 31000 standard [99]. To the very right, the column matches the steps with the lifecycle in the IEC 61508 standard [86]. From this, the intention is that the matching of the functional protection method to existing standards is clarified.



Hazard and Risk Analysis

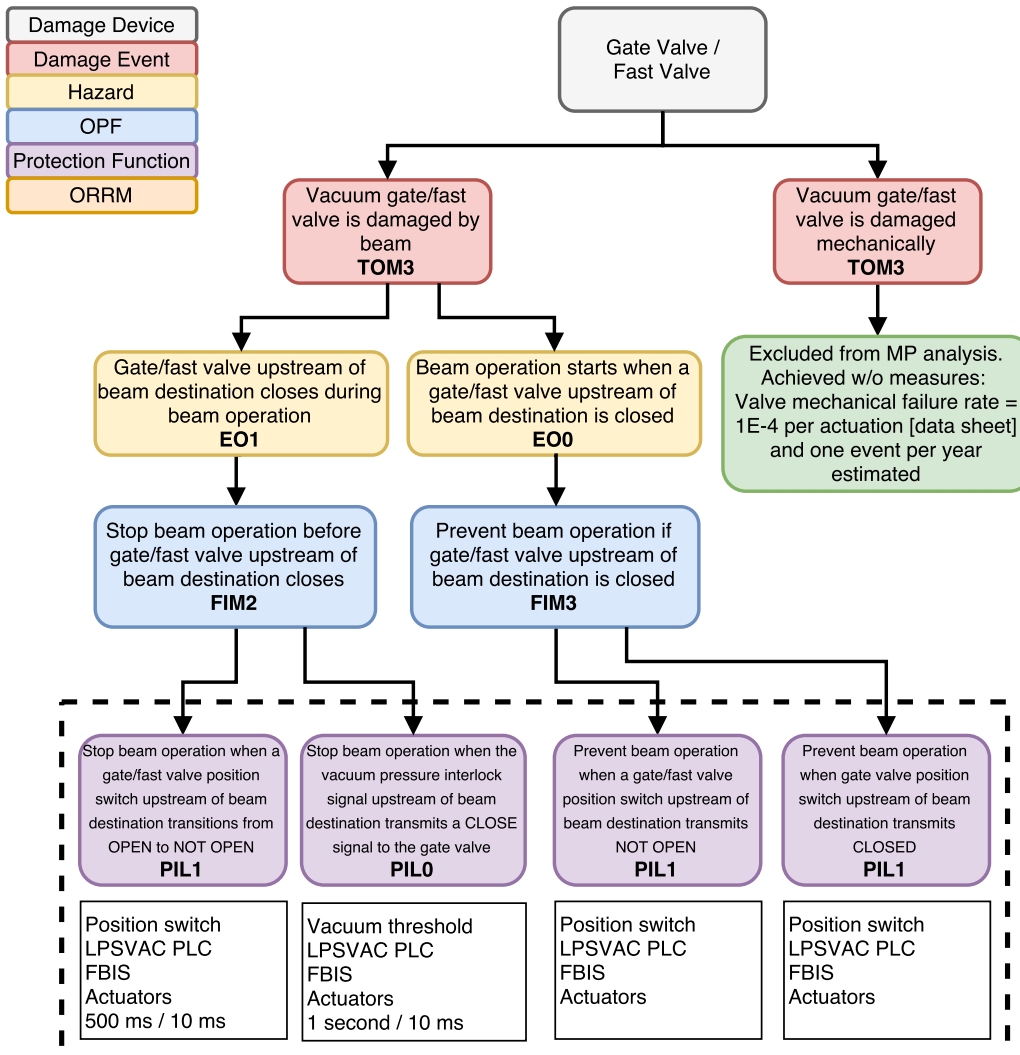


Appendix C - Graphical Functional Protection Analyses

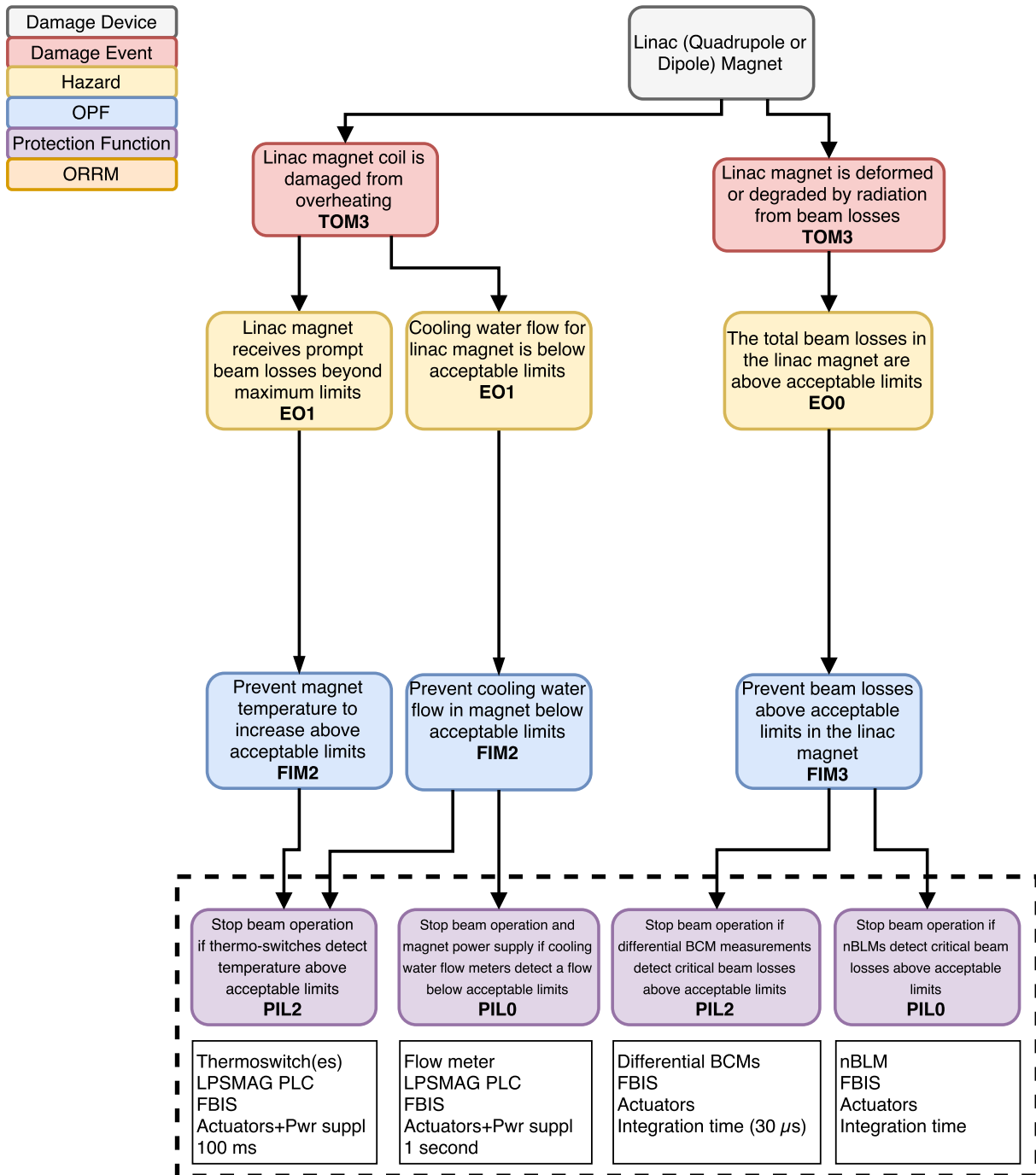
This appendix displays the graphical views of the functional protection analysis of the normal conducting linac and target station systems at ESS. The analysis itself, together with the tabulated outcome, is found in Section 5.3. Note that the interceptive device system is large enough to span over three pages. In this case, a bracket indicates which page of the analysis that is displayed. The analyzed systems are:

- Vacuum System (page 71)
- Linac Magnets (page 74)
- Interceptive Devices (page 75)
- MEBT Buncher Cavities (page 77)
- Target Wheel - Cooling, Movement, and Rotation (page 81)
- Cryogenic Moderator System (page 83)
- Primary Water Cooling System - Moderators and Reflectors (page 85)
- Tuning Beam Dump (page 86)

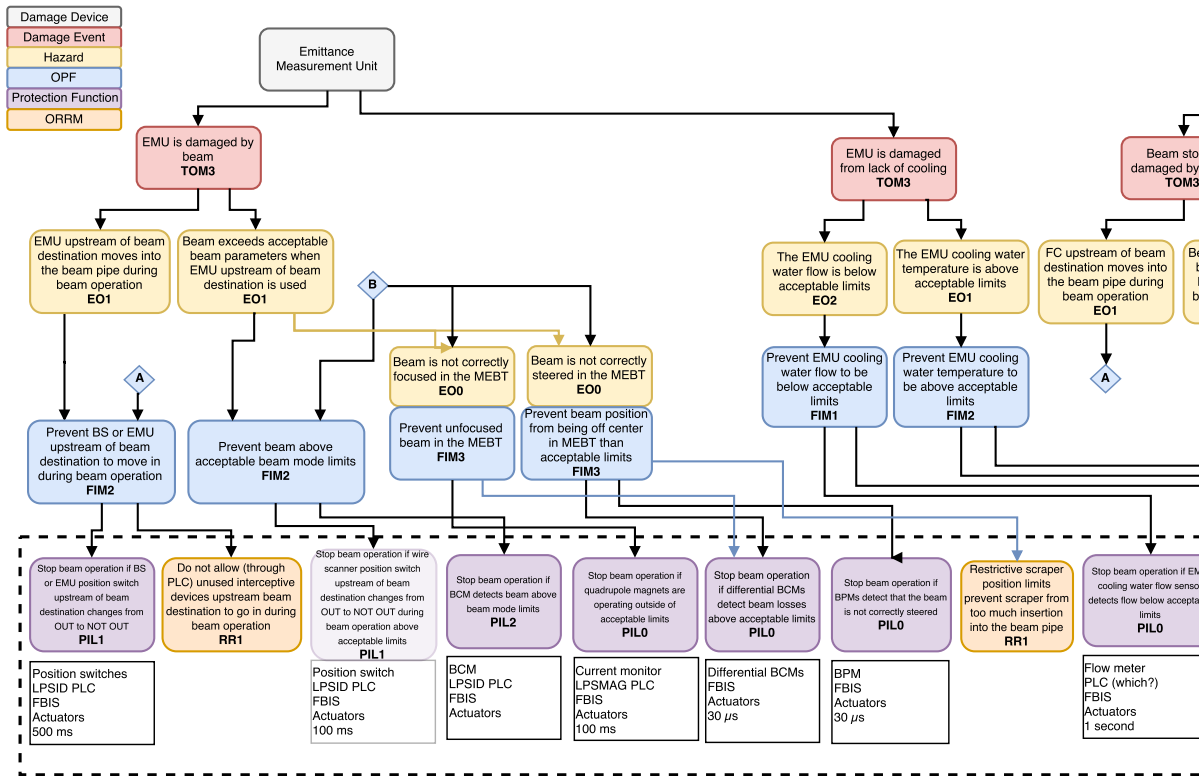
Vacuum System



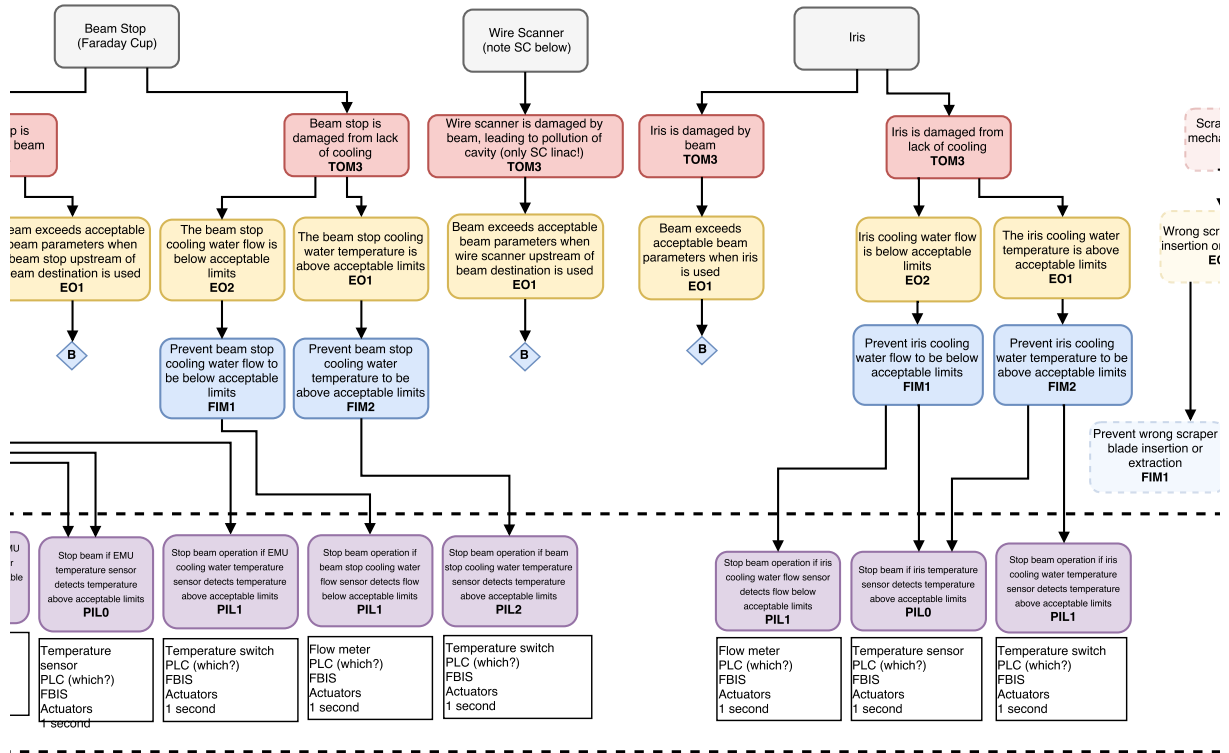
Linac Magnets



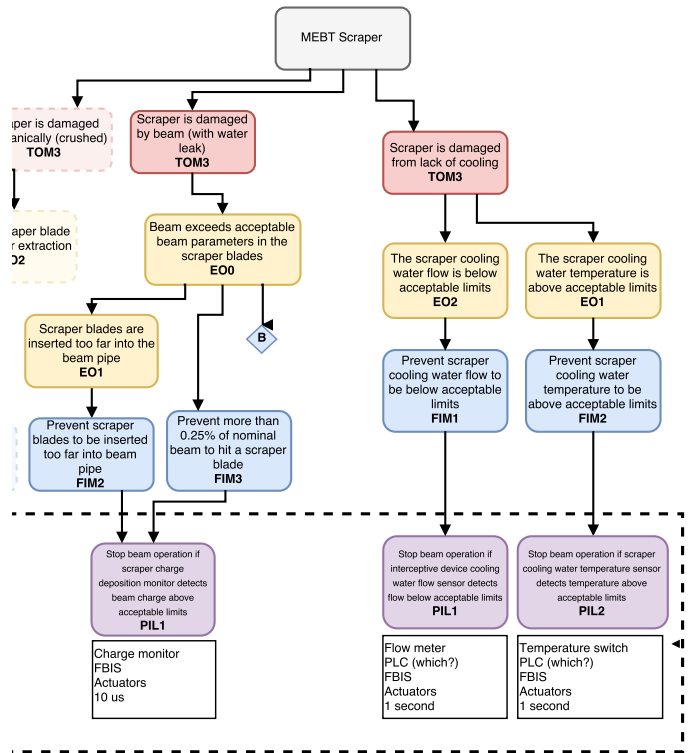
Interceptive Devices (page 1)



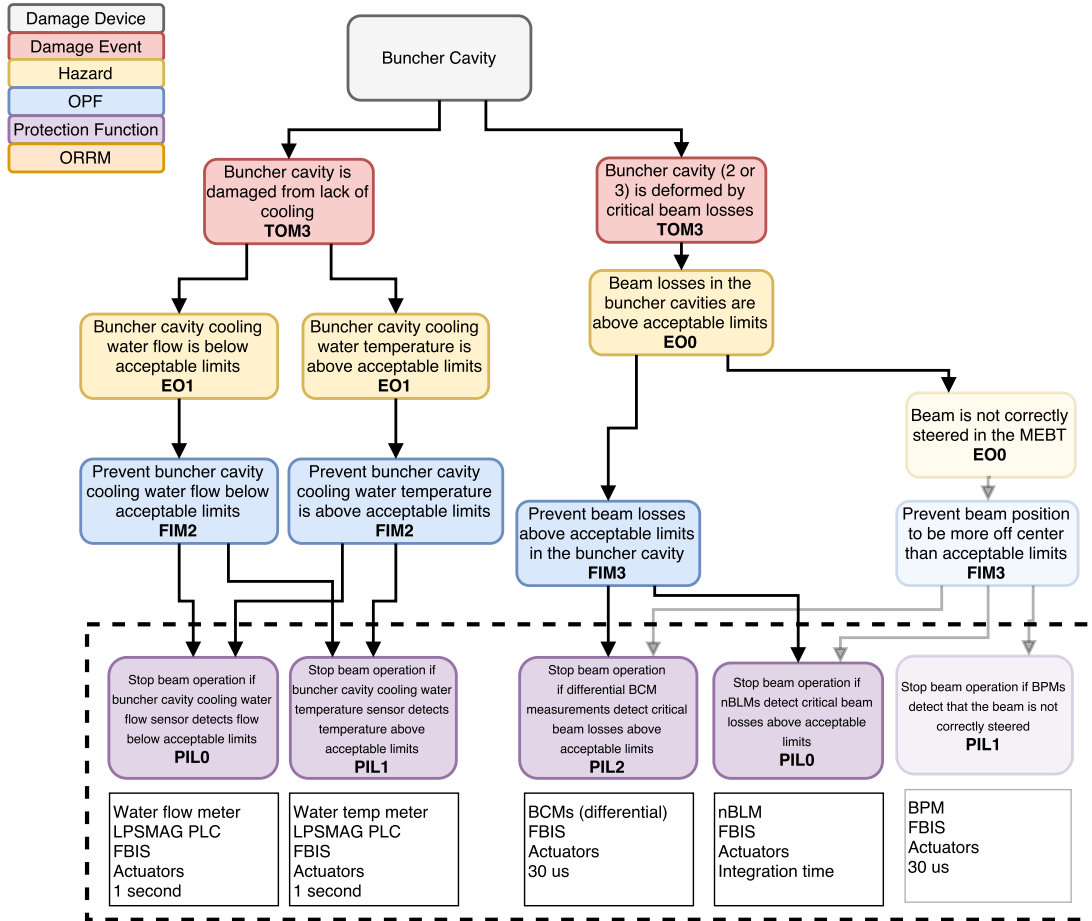
Interceptive Devices (page 2)



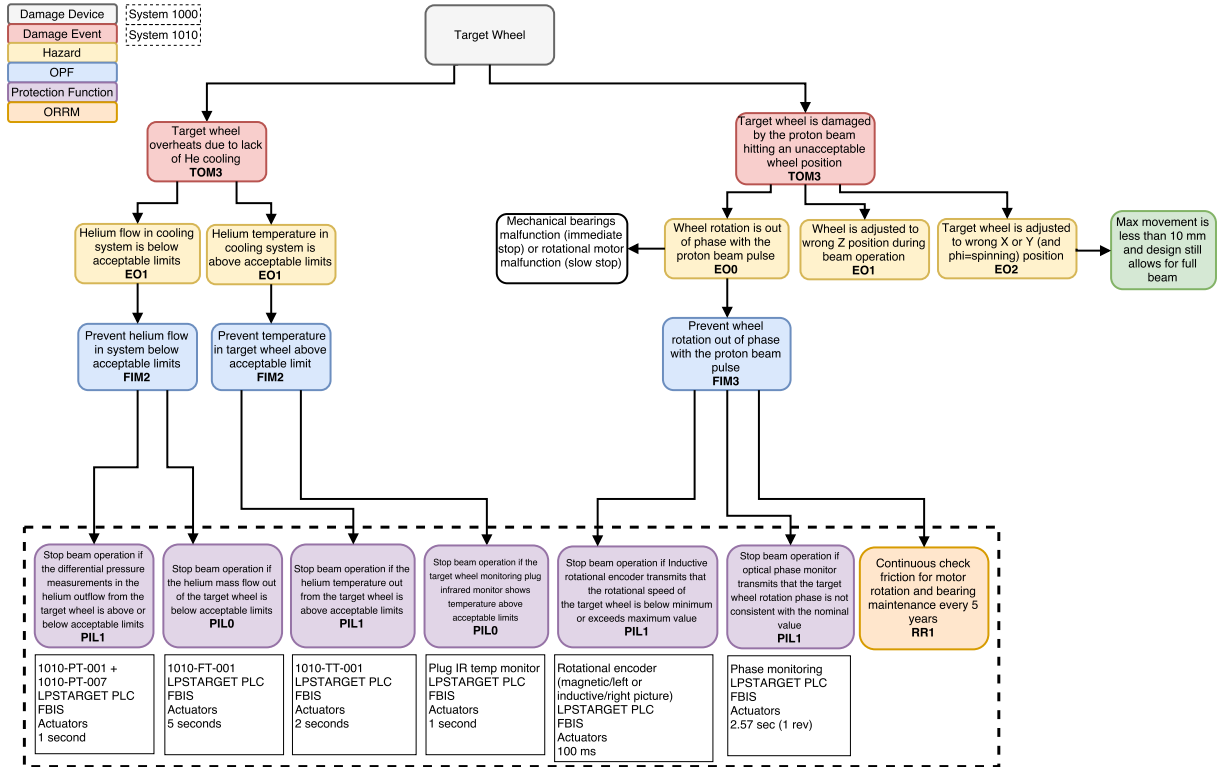
Interceptive Devices (page 3)



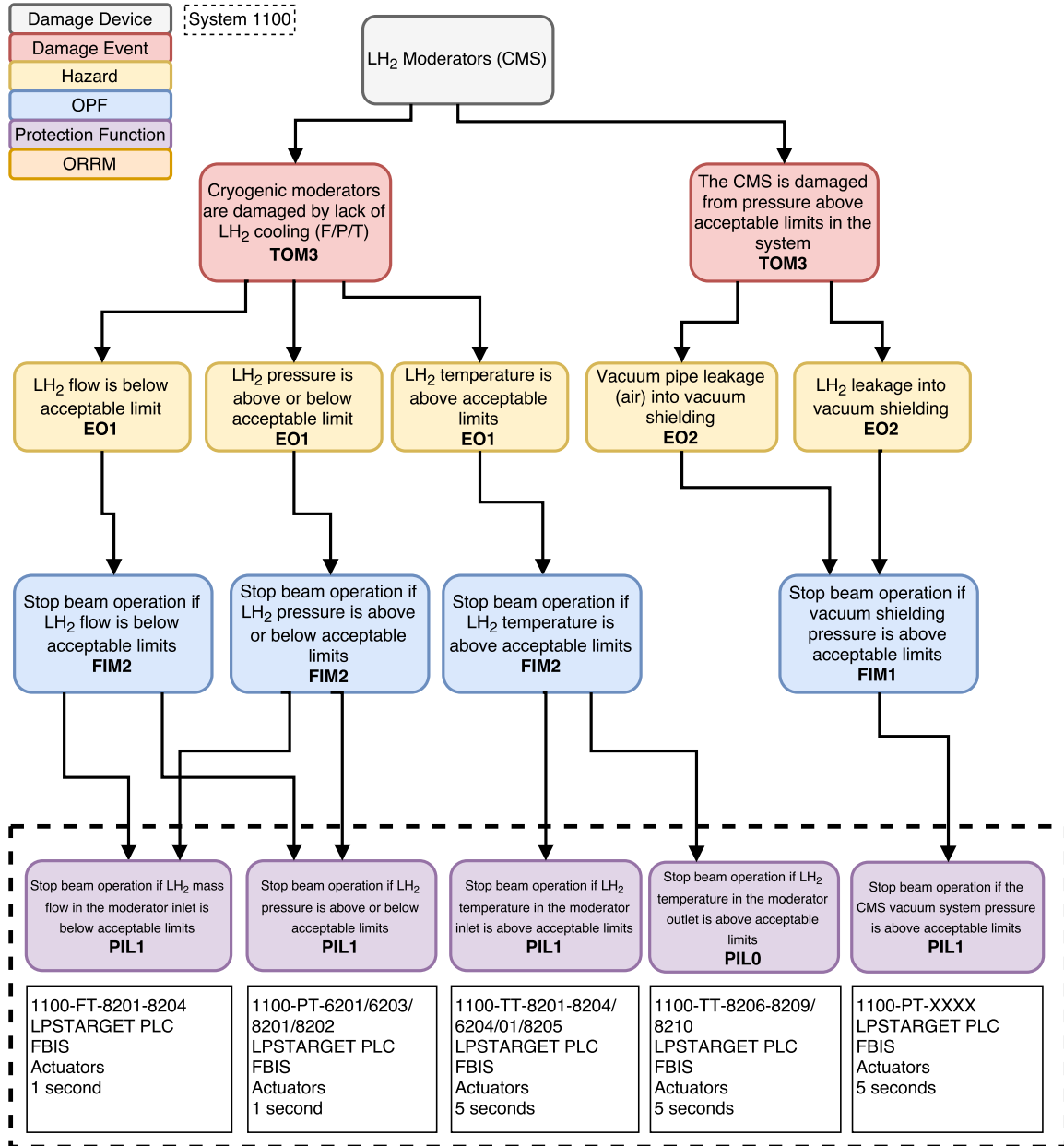
MEBT Buncher Cavities



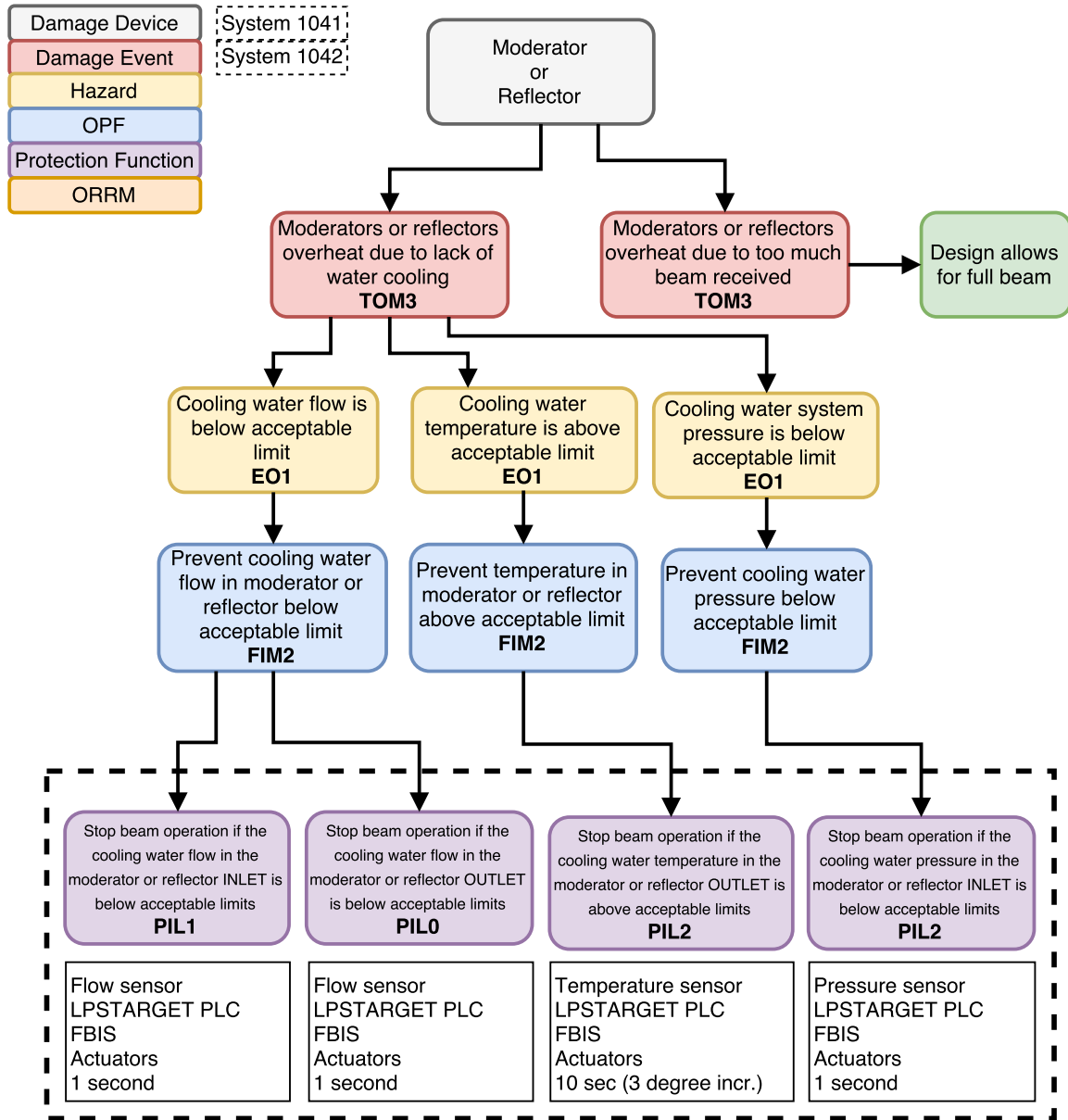
Target Wheel - Cooling, Movement, and Rotation



Cryogenic Moderator System



Water Moderator and Reflector System



Tuning Beam Dump

