Institut für Maschinenelemente
Direktor: o. Prof. Dr.-Ing. Bernd Bertsche Prof. Dr.-Ing. habil. Werner Haas
UNI STUTTGART
Lehre und Forschung: Antriebstechnik • CAD • Dichtungstechnik • Zuverlässigkeitstechnik

Dennis Hügle

System Theoretic Dependability Analysis of the LHC Superconducting Magnet Circuit Protection

Masterarbeit 2017

Abstract

Subject of the present work is the application of the methods STPA (System Theoretic Process Analysis) and CAST (Causal Analysis based on STAMP) to analyze the protection systems of the superconducting magnet circuit of the LHC at CERN, Geneva. The named methods are derived from the at MIT developed STAMP (System Theoretic Accident Model and Processes) accident model.

The CAST method was applied to the analysis of the 2008 Incident during the Hardware Commissioning. An incorrect interconnection between two magnets damaged the accelerator severely. The analysis defines the control structure of the Commissioning and investigates every subsystem and the interaction between the components. The results were social and technical requirements. Among others, it shows the necessity for safety culture at CERN and a revision of the magnet interconnection process. The present analysis found the same root causes for the incident than a task force did in 2009. Further, the CAST analysis found more, socio-technical root causes and defined requirements to eradicate them.

The second study concerns the focusing magnets enclosing the CMS and ATLAS experiments (inner triplets), which will be renewed as part of the High Luminosity Upgrade. The STPA analysis investigates the protection mechanisms of these magnets and defines a control structure. The components within this structure communicate with control actions. It is investigated, how these control actions can turn unsafe and what can cause these unsafe control actions. The results include requirements for operational safety, reliability, availability and maintainability. Especially the analysis shows, that an additional supervision unit for surveilling accidental CLIQ Unit triggering is needed. The analysis showed the safety of the protection layout of the inner triplets and added requirements for more dependability.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Explanation
AUG	Arret d'Urgence General (General Emergency Stops)
BIS	Beam Interlock System
CAST	Causal Analysis based on STAMP
CCC	CERN Control Centre
CERN	European Organization for Nuclear Research
CLIQ	Coupling-Loss Induced Quench
Cryo	Cryogenic System
DQHDS	Quench Heater Discharge Supply
EiC	Engineer in Charge
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HL-LHC/Hi-Lumi LHC	High Luminosity Large Hadron Collider
HWC	Hardware Commissioning
I/O-QH	Inner/Outer Layer Quench Heaters
IT	Inner Triplets
LBDS	LHC Beam Dumping System
LHC	Large Hadron Collider
LS	Long Stop
MIT	Massachusetts Institute for Technology
MP3	Magnet Circuits, Powering and Performance Panel
MPS	Machine Protection System
OOS	Operator on Shift
PC	Power Converters

Abbreviation	Explanation
PO	Point Owner
PIC	Powering Interlock System
QDS	Quench Detection System
QL	Quench Loop
QPS	Quench Protection System
RBAC	Role-based Access Control
RPN	Risk Priority Number
STAMP	System Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
TFR	Task Force Report
UCA	Unsafe Control Action
UPS	Uninterrupted Power Supply
UR	Part of the underground tunnels, parallel to the LHC. Storage for LHC equipment
XSTAMPP	Extensive STAMP Platform

Terminologies

Terminologies	Explanation	Examples[1]
Accident	An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution and so on)	Colliding vehicles. Space mission pollutes other planets
Hazard	A system state or set of conditions that, together with a set of worst-case environment conditions, can have the potential to lead to an accident (loss)	Inadequate distance between vehicle in front and in behind. Toxins near space shuttle launch station on earth
Safety	Freedom of accidents [1, p. 467]	-
Dependability	The ability [of a system] to perform as and when required [under defined conditions] [2] ; Dependability in this context includes availability, maintainability, reliability, and safety.	-
Reliability	Reliability is the probability that a product does not fail during a defined period under given functional and surrounding conditions [3, p. 19]	-
Availability	The availability is the probability that a system is in a functional condition at the time t or during a defined time span, under the condition that it is operated and maintained correctly" [3, p. 356]	-

[1] Examples taken from: [53]

1 Introduction

The Large Hadron Collider (LHC) is the flagship research tool of CERN, the European Organization for Nuclear Research. It is the biggest particle collider in the world and perceived world-wide public attention for providing verification of the existence of the Higgs-Boson [4]. Two proton beams are accelerated in a variety of accelerators and ultimately injected into the LHC, where they are accelerated to their final kinetic energy of 6.5 TeV, reaching nearly the speed of light. At the four experiments of the LHC – ATLAS, CMS, LHCb and ALICE – the beams cross. When two protons collide, the kinetic energy is converted to pure energy which in its turn leads to the creation of new subatomic particles. [5]

To sustain European leadership in particle physics, the upgrade to the High-Luminosity LHC (HL-LHC or Hi-Lumi LHC) was permitted by the European Strategy for Particle Physics. The Luminosity corresponds to the expected amount of collisions a collider can produce and therefore related to the discovery potential. The HL LHC will exceed the LHC Luminosity by the factor of 10. The upgrade is foreseen to be put in place 2024. [6]

The more than 10,000 LHC magnets store about 10 GJ of energy and the circulating beam energy can exceed 700 MJ [7] [8, p. 215]. This is more than enough to permanently damage the accelerator magnets and to cause several months of downtime and immense repair costs. Small losses of the beam to the magnet can induce a heat load that leads to a loss of the superconducting state – a so-called quench. This causes a rapid heat development; thus, all superconducting elements require protection from a quench [9]. The Quench Protection System (QPS) detects the loss of superconductivity and triggers the magnet protection. CLIQ (Coupling-Loss Induced Quench) is a novel protection technology, which will be used at CERN for the first time in the HL-LHC upgrade. It creates losses in the magnet by inducing an oscillating current to the circuit, leading to a homogenous distribution of the energy to the magnet coils. [10] [11]

The focusing magnets enclosing the experiments are the so-called inner triplet. These magnets are the backbone of the LHC upgrade. They need fast and reliable protection, due to the high magnetic fields and the physical position next to the experiments, where collision debris induces a high heat load. The inner triplet magnets are protected by CLIQ and Quench Heaters. [8]

Aim of the present work is to identify weaknesses in the dependability of the magnet protection system. The present work starts by explaining the necessary foundations in chapter 2, introducing the analyzed technologies and the used methodologies STPA and CAST. Both methods are based on the recently at MIT developed accident model STAMP. Chapter three provides the results of the CAST analysis of the 2008 incident. During a test of the machine a highly powered bus bar broke apart and built up a severely damaging electrical arc causing months of downtime. Chapter four is dedicated to a top-level STPA dependability analysis of the magnet protection system of the HL LHC inner triplets with CLIQ. This analysis follows

on a top-down approach to investigate the system's interactions of the protection mechanisms. [1] [12]

Concluding, Chapter 5 shows an overview on the results of the thesis and an outlook to future dependability analyses. Further it shows an evaluation of the applicability of the used methods for accelerators. It shows an analysis of strengths and limitations of the method and a comparison to the more widely known method Failure Mode and Effects Analysis (FMEA).

2 Context and Background

This chapter presents the fundamentals for the analysis of the superconducting circuit protection. The first part deals with an overview of CERN and its flagship research tool – the Large Hadron Collider (LHC). The second part presents state-of-the-art magnet protection mechanisms and the machine interlocks – the central node of the machine protection. The used dependability methods have been developed at the MIT Partnership for a Systems Approach for Safety (PSAS) and are introduced in the last sections of this chapter.

2.1 The European Organization for Nuclear Research

CERN, the European Organization for Nuclear Research, is the world's largest particle physics laboratory. Founded in 1954 by twelve states, CERN subsequently grew bigger, brought nations together and provided huge progress in the field of particle physics. It recently confirmed the existence of the Higgs-boson that was predicted by the standard model and created inventions that define modern life, like the internet or the capacitive touch screen. [13] [14] [15]

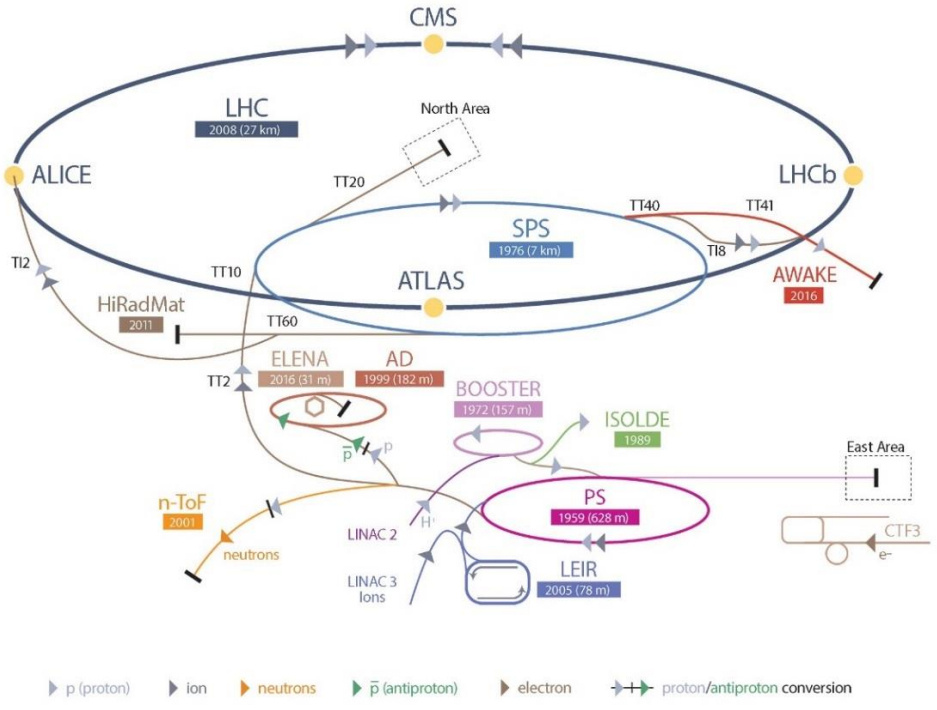


Figure 2-1: Overview on the CERN accelerator complex [16].

CERN's research tools – the accelerators, decelerators and detectors – explore matter at the most fundamental level. Even though the LHC is the most publicly perceived accelerator, it is by far not CERN's only one as shown on Figure 2-1. Particles undergo a chain of different

accelerators and transfer-lines before entering the LHC: The Linear Accelerator (LINAC), the BOOSTER, the Proton Synchrotron (PS) and the Super Proton Synchrotron (SPS). Ultimately, the beam in the LHC reaches a velocity of 99.9999991 % of the speed of light and an energy of 6500 GeV [5]. A wide variety of experiments are built up at CERN from which the four experiments ATLAS, CMS, ALICE and LHCb are implemented in the LHC ring. [17]

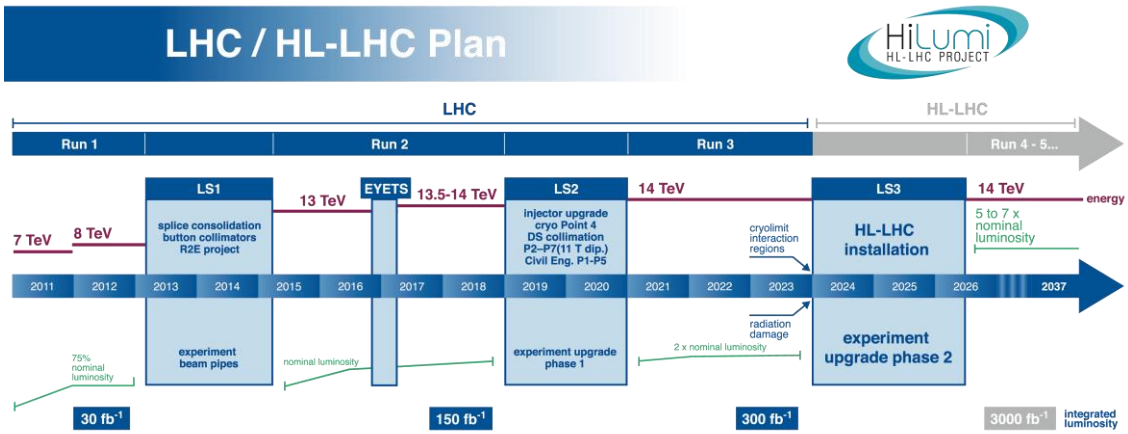


Figure 2-2: HL-LHC Upgrade Schedule [6].

During the Long Shutdowns, the LHC is upgraded step-by-step to the High Luminosity LHC (HL-LHC). The upgrade to the HL-LHC will increase the number of expected collisions of the LHC by a factor of 10. An overview on the upgrade schedule to the HL-LHC is shown in Figure 2-2. The upgrade affects nearly every system. It includes among others an upgrade of the injectors, new underground galleries and an upgrade of the final focusing magnets – the inner triplets. The upgrade should be finalized in 2025. [8]

2.2 The Large Hadron Collider

The LHC is the biggest particle collider in the world with a circumference of 27 km. It is a circular synchrotron collider, i.e. the power in the bending magnets is ramped up synchronously while the beam energy is increased by the Radio-Frequency system.

2.2.1 The LHC Operation

The LHC is operated by Physicists and Engineers in the CERN Control Centre (CCC) in Prevessin 24 h per day for the whole year. The standard year for the High Luminosity LHC is divided in to dedicated phases. The foreseen phases per year for the High Luminosity LHC are shown in Table 1. [18]

Table 1: Foreseen Standard Year of the HL-LHC [8]

Activities	**Time [days]**	**Notes**
Christmas technical stop including HWC	91	The Technical Stop over Christmas is longer than the standard technical stop and includes more time for hardware commissioning
Commissioning with beam	21	Commissioning of the installed hardware
Machine Development	22	Foreseen time for experiments with the machine, e.g. beam loss studies
Scrubbing	7-14	Cleaning of the vacuum pipes with beam
Technical Stop	15	Three technical stops are foreseen per year
Technical Stop Recovery	6	Recovery from the technical stop, such as cool down
Physics including preparation	196	Proton, Ion and special physics runs

Table 2: Rough estimations for typical HL-LHC turnaround time [8]

Mode	**Time [min]**	**Notes**
Ramp down / pre-cycle	60	Ramp down, recovery from the previous operation.
Pre-injection set-up	15	Setting up the injection
Set-up with beam	15	Injection of a pilot beam, a single beam bunch with little energy that cannot harm the machine
Nominal Injection	20	Injection of the beam
Prepare Ramp	5	-
Ramp	25	Ramping up the current with of the bending magnets with10 A/s and increase of the beam energy
Flat-Top	5	The highest powering level is called flat-top
Squeeze	25	The beam is squeezed at the interaction points to obtain minimum cross section
Adjust/collide	10	-
Stable Beams	-	Stable beams produce collisions at the experiments.

Access to the LHC tunnel is only possible during technical stops; repair, maintenance and installation of new equipment must be limited to this time. The Hardware Commissioning (HWC) investigates the new hardware and ensures the safe operation. Machine Development is dedicated time for investigations on new technology, machine behavior or machine optimization. [8] [19]

The LHC operation with particle beam is performed in cycles. A cycle ends, when the beam is dumped. When the operator dumps the beam, the LHC must prepare for the next fill. Table 2 shows the activities between two fills. The sum of the time between a beam dump and the next declaration of stable beams is called turnaround time. Once the beams are adjusted, the LHC can produce collisions for over 20 h, the optimum for the HL-LHC is 7.2 h [8]. [20]

2.2.2 The LHC Layout

The LHC is built in eight octants with eight arc sections and eight long straight sections. Each octant is dedicated to a defined function, the particles are accelerated by the radio frequency facilities in sector 4 and the LHC beam dumping system (LBDS) is in sector 6. Sector 3 and 7 are dedicated to momentum and betatron cleaning of the particle beam, i.e. absorbing part of the beam halo and parts of the secondary radiation [21]. The beams collide in the LHC experiments in the Interaction Points (IP) 1, 2, 5 and 8. An overview on the LHC Layout is presented in Figure 2-3 [5].

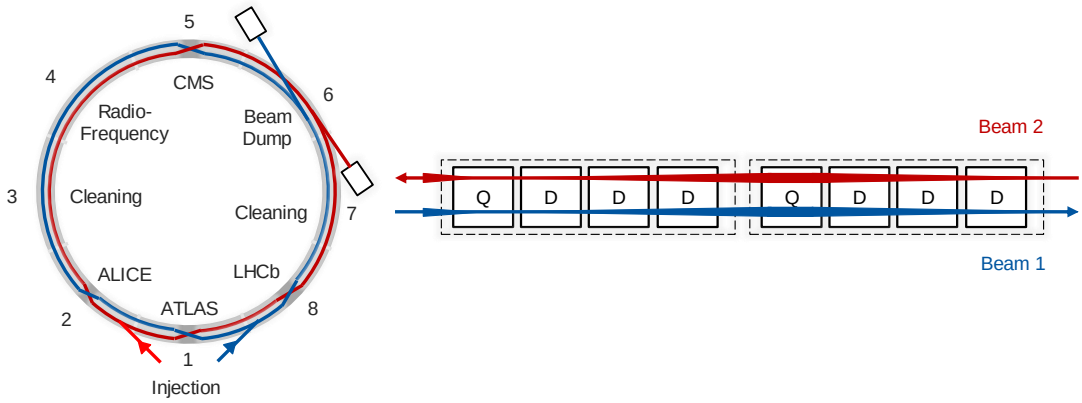


Figure 2-3: Left: The LHC Layout. Right: A FODO[1] Cell of the LHC.

Each arc is built of 23 identical cells, each cell consisting of six dipole and two quadrupole magnets, as shown in Figure 2-3 on the right. Multiple higher order magnets are also part of one cell, but are for the sake of simplification not explained here. The sequence of two cells containing one quadrupole magnet followed by three dipole magnets each, is referred to as *FODO* Lattice. A quadrupole field, such as the left part of Figure 2-4, focuses the beam in one

[1] The word FODO refers to the magnet layout: „Focusing Quadrupole – “O” (Empty space, filled with Dipoles) – Defocusing - “O” (Empty space)

plane, while defocusing in the perpendicular plane. Looking at only one plane, one cell consists of a focusing and a defocusing quadrupole. A dipole field, such as Figure 2-4 right, bends the beam in one direction. Individual bus bars connect the dipole magnets, the focusing main quadrupole magnets and the defocusing quadrupole magnets. [9] [22]

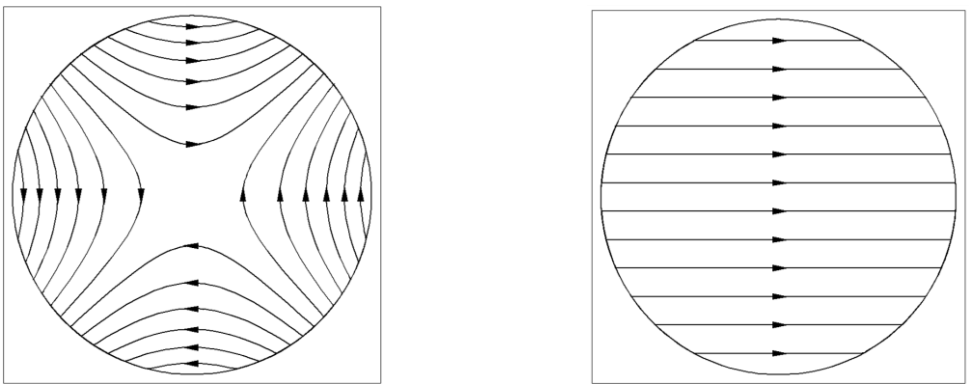


Figure 2-4: Pure Quadrupole Field (left) and pure dipole field (right) [23].

2.2.3 Superconductors

To squeeze the beam to a tiny cross-section and to keep the beam on a constant orbit, a strong magnetic field is needed, requiring high currents in the circuit. The heat output in a normal conductor scales with the square of the current and the conductor's resistance.

The current in a typical magnet circuit in the LHC is in the order of magnitude of 10-20 kA. To control the resulting heat development in this circuit, the material must have a vanishing small resistance. Under certain conditions, such properties can be found in materials called Superconductors – which can have zero resistance.

The condition in which such material becomes superconducting depends on its temperature T [K], the magnet field density B [T] and the induced current density J [Am^{-2}]. Those three values form the so-called critical surface, as displayed in Figure 2-5. The surface shows for each combination of the three values if the conductor remains in the superconducting state [11].

When local conditions in terms of temperature, current density or magnetic field do not allow the conductor to stay superconducting, the material switches to the normal conducting behavior. This switch in state is called a quench. A quench is defined as a sudden and unexpected transition to the normal state of the superconductor [11] [24].

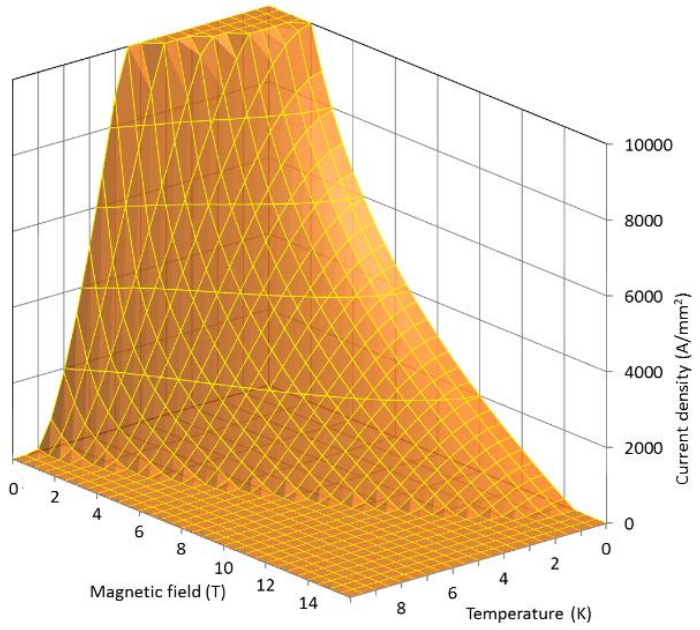


Figure 2-5: Critical surface of a superconductor [25].

Especially during the first operations, the forces during powering cause micro-movements in the coils and lead to quenches. These so-called training quenches stop after some operations, leading to a fairly constant behavior. Failures in the cooling, debris from the experiments or fluctuations in the powering can also cause a quench. If no measures are taken, the magnet could heat up beyond melting point of the material and could be destroyed. [26]

2.2.4 The Inner Triplet Magnets

The inner triplet magnets (IT) are the three quadrupole magnets at either side of the experiments, i.e. the last focusing magnets before the collision of the beams. The physical position next to the experiments, leads to a high radiation load for the magnets. For the HL-LHC upgrade, the experiments ATLAS and CMS will be equipped with new inner triplet magnets, as those magnets reached their radiation lifetime. Common superconducting magnets are built of NbTi. The inner triplets are made up novel Nb_3Sn technology. The layout of the magnets is presented in Figure 2-7. The magnets are numbered Q1, Q2 and Q3, starting from the experiments. Q1 and Q3 are built in the same way. [27]

As displayed on the right horizontal temperature axis in Figure 2-5, the superconducting state is only possible close to absolute zero. To cool the quadrupole to such low temperatures, the magnet is surrounded by a so-called cryostat. The cryostat of an Q1 magnet is shown in Figure 2-6. The cryostat surrounds the magnet and is completely flooded with pressurized, static superfluid Helium at a temperature of 1.9 K. [28]

A so-called bayonet heat exchanger is installed in the cooling channel. The heat exchangers are made from copper and are filled with pressurized, flowing superfluid helium. The developing heat by debris or a quenching magnet is conducted radially to the heat exchangers and out of

the system by the pressurized helium in the heat exchangers. In case of a quench, the helium will be blown out and the magnets will warm up. [28]

Appendix A shows the detailed distribution of the helium with respective pressure and temperature in the cryostat of the inner triplet.

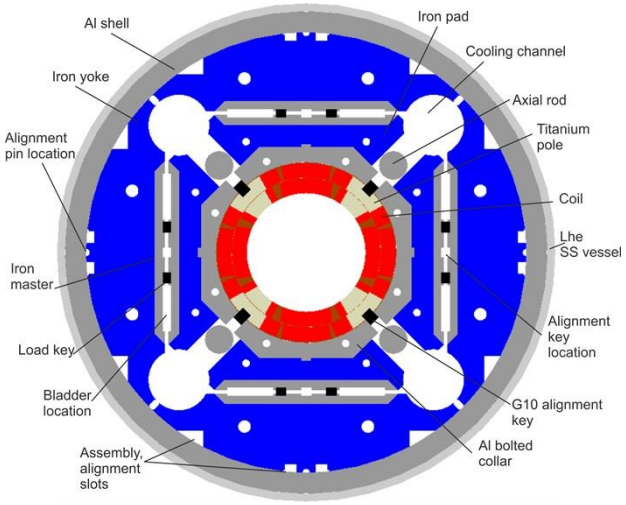


Figure 2-6: The cryostat of a Q1 inner triplet magnet.

The magnet poles are powered in series by three power converters and two trim converters. The main power converter delivers maximum 18 kA of DC current. The trim power converters deliver a positive or negative DC current of up to 2 kA to adjust the current independently. Appendix B shows the detailed circuit layout of the inner triplet powering. [8] [29]

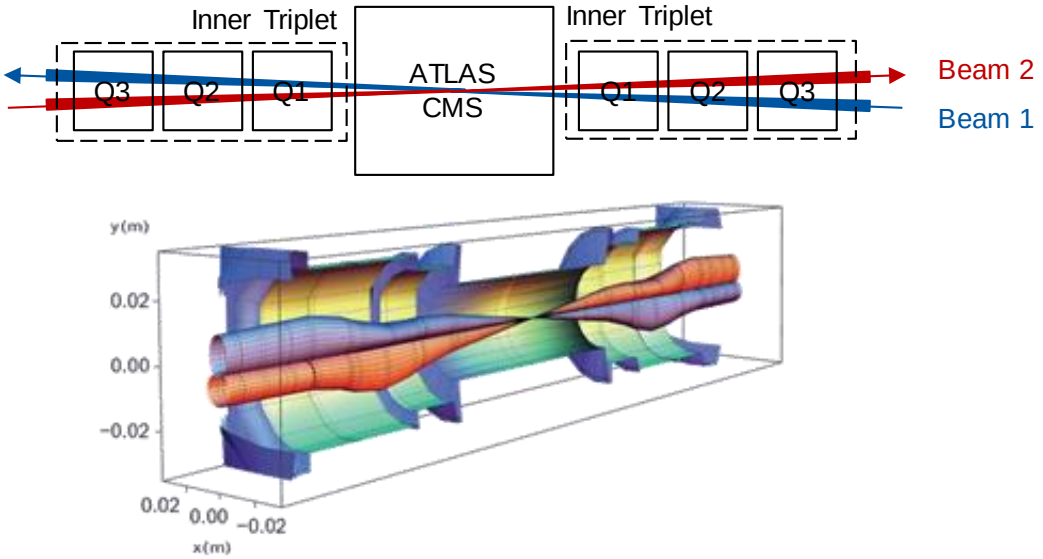


Figure 2-7: Inner Triplet Magnets focusing the beam [30].

These magnets promise to squeeze the beam to a tinier cross-section, thus increasing the probability of collisions in the experiments. It is these collisions that create a particle debris, hitting the inner triplet magnets, generating heat and making a quench more likely than in other magnets at the LHC. [31] [28]

Different approaches for protecting the magnet have been tested. The results are summarized in [32]. Either inner-layer and outer layer quench heaters (I-QH), outer layer quench heaters only (O-QH) or outer layer quench heaters and CLIQ. These protection mechanisms are explained in Chapter 2.3.3. The current protection baseline is O-QH and CLIQ.

2.3 The Machine Protection System

The machine protection system (MPS) of the LHC guarantees a safe operation. The main objectives of the MPS are defined in [33] as:

- Protect the machine: The machine and its equipment must be protected from the magnetic energy, helium, beam, etc.

- Protect the beam: The beam must not be dumped unnecessary. The machine must provide high availability.

- Protect the evidence: In case of a failure or a beam dump, the initial failure must be detectable

- Improving the Operation: Diagnostics must be easy and system status must be clearly presented to the control room and the operators.

The Machine Interlock architecture was derived from these objectives. It consists of multiple systems with dedicated functionalities: The Beam Interlock System (BIS) allows the injection of the beam(s). It further triggers the dump of the beam in case the operation is unsafe. The Powering Interlock System allows the powering of the superconducting magnets, when predefined conditions are met for safe operation. It aborts the powering in case of a failure, such as a quench. The Powering Interlock System is a user of the BIS, ensuring that the beam is dumped when powering failures happen. The next sections explain the MPS subsystems that are important for the present work: The Beam Interlock System, the Powering Interlock System and the Quench Protection System. [33]

2.3.1 The Beam Interlock System

The energy of the beam is 700 MJ and well beyond damage potential for the LHC. The Beam Interlock System (BIS) is an important part of the machine protection system and permits or inhibits operation with beam. It is built as two redundant optical loops in parallel to the LHC. Two Beam Interlock Controllers are implemented left and right to each interaction region (IR), plus one in the CCC making it 17 in total. During normal operation, a 10 MHz signal is sent

through this loop and is read in IR6 by the LHC Beam Dumping System (LBDS). A correct frequency represents a *Beam Permit True* signal for the LBDS in sector 6, i.e. no measures are taken. [33] [34]

In case of a failure, a Beam Interlock Controller interrupts the optical loop. The signal travels both ways with the speed of light, ensuring that the shortest path is taken from a controller to the LBDS. The optical loop is visualized in Figure 2-8.

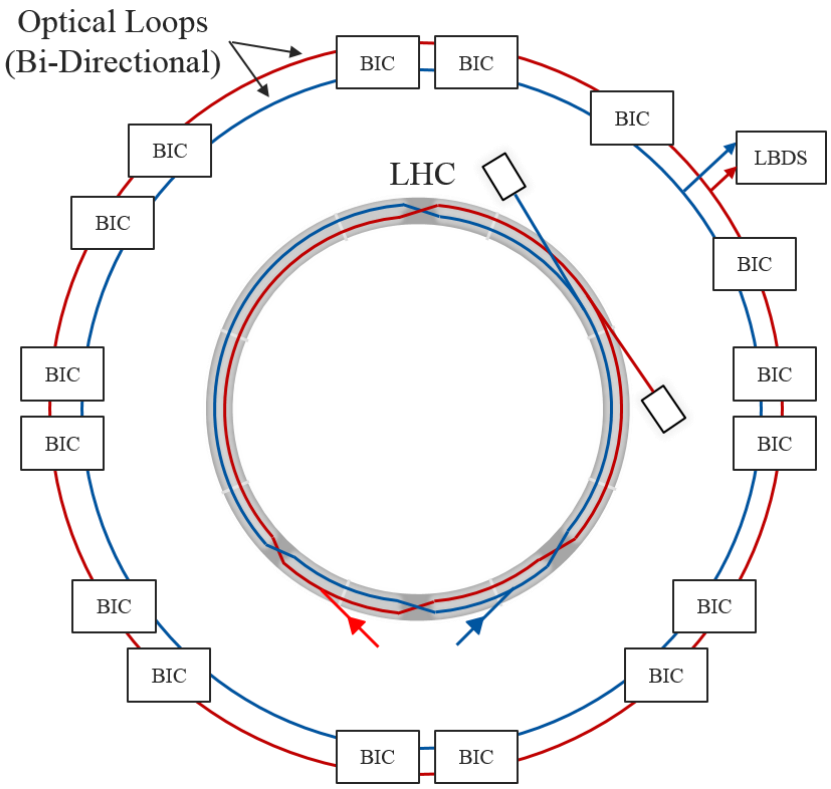


Figure 2-8: Optical Loop of the Beam Interlock System; inspired by [29].

A possible failure is lost beam hitting the equipment. Hazardous beam loss must be prevented before the beam can damage the LHC. Possible causes for beam losses are fluctuations in the magnetic field, the beam hitting falling microparticles or particle debris from the colissions in the experiments [35].

Multiple systems are implemented to detect hazardous beam behavior, such as the beam loss monitors (BLMs), the beam position monitors (BPMs), or the Powering Interlock System. These systems are BIS users and permit the beam circulation while in a safe state. In total, almost 200 systems are BIS Users. [34]

Once triggered, the LBDS synchronizes with the so-called abort gap, an intentionally empty space between two bunches and triggers extraction magnets to kick the beam out of the LHC.

The standard gap between two bunches is 25 ns, the abort gap is 3 µs. After loop interruption, it takes up to 3 turns to completely extract the beam, corresponding to roughly 270 µs. [36]

2.3.2 The Powering Interlock System

The LHC is powered in sectors to keep each sector independent from possible failures of other sectors. The energy in the circuits is potentially hazardous to the machine, thus safe powering conditions must be ensured. The Powering Interlock Controller (PIC) is the monitoring unit for the electrical circuits of a powering subsector.

The PIC has an interface to the Power Converters (PCs), the Quench Protection System, the Uninterrupted Power Supplies (UPS), the Cryogenic System (Cryo), the emergency buttons (AUG) and the Beam Interlock System (BIS) as it can be seen in Figure 2-9.

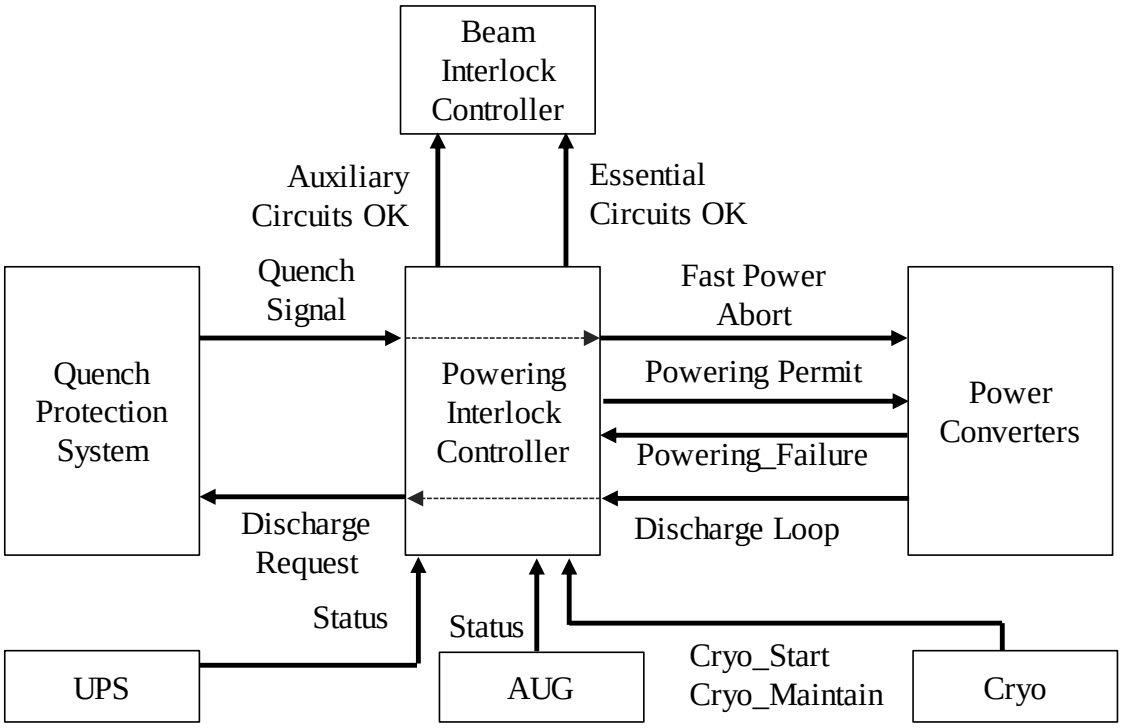


Figure 2-9: Overview on the Powering Interlock System

The PIC has two circuits interfacing the BIS. The essential circuit and the auxiliary circuit interface. The PIC has a built-in logic to decide which signals are processed by which circuit. Signals are processed by the essential circuit, if a failure requires an immediate Beam Dump. If a failure of a component does not necessarily need a Beam Dump the signal is processed by the auxiliary circuit. E.g. a loss of single corrector magnets does not require a beam dump and the operation can continue. In the essential circuit, signals are processed by the CPLD on a microsecond timescale. The auxiliary circuit signals are processed by a PLC that is significantly slower and less secure, operating on a millisecond timescale. The auxiliary circuit also acts as

a redundancy for the essential circuit, processing the signals of the essential circuit as well. [37] [33]

The PIC permits the powering of the PCs if predefined safe conditions are met. The UPS/AUG, the QPS and the Cryo must send their OK-signal to start the system. If all conditions are safe, the Operator can start the powering. The Powering Permit Signal is issued from the PIC to the Power Converters and the powering starts. While the Powering Permit Signal is *true,* the powering is permitted. If the signal goes to *false* during operation, the power converters ramp down slowly (Slow Power Abort, SPA). [33]

The cryogenic system sends the Cryo_Start and the Cryo_Maintain signals. Cryo_Start is a condition for the powering start. The maintain-signal is the Cryo permit for maintaining the powering. If the Cryo_Maintain Signal is withdrawn (due to internal errors, cryo-power issues, etc.) the PIC initiates an SPA. [38] [39]

If the QPS detects a quenching magnet, the QPS interrupts the hardwired Quench Loop. This loop is read as "Quench Signal" by the PIC. As soon as the loop is interrupted, the Powering Interlock Controller withdraws the Essential Circuits OK Signal, requesting a beam dump of both beams. The PCs read the Quench Signal as Fast Power Abort (FPA) request, shutting down the power. [33] [40]

The Power Converters are cooled by water and are connected with normal conducting wires to the current leads and the superconducting magnets. In case of a PC-Internal failure (e.g. of the water cooling) the Power Converters can abort the Powering themselves, not depending on the PIC. The failure is communicated by the Powering Failure Signal and the Discharge Request Signal. While the first does not require an action by the QPS, the Discharge Request requires a firing of Quench Protection. [40]

The Powering Interlock Controller is powered by an uninterrupted power supply. In the case of a failure in the mains, the UPS provides emergency power long enough to safely extract the energy. The UPS and the emergency buttons AUG are also connected to the PIC with a hardwired status loop. If a UPS detects an internal failure, the powering is aborted via an FPA. [41] [40]

The hardwired current loops between the PIC and its users are built fail-safe, i.e. if the signal goes low, an action is automatically triggered. The loop-opening interfaces are built, so that they open, when the powering is lost. [40]

2.3.3 The Quench Protection System

Goal of the Quench Protection System is to detect the quench and to protect the magnets from its effects by e.g. extracting the energy to an external device and to evenly distributing the energy to the whole magnet by firing quench heaters and the CLIQ system. [9]

When a quench is detected, the QPS takes multiple actions. The quench causes changes in the magnetic field, which might lead to hazardous beam excursions, thus the QPS must trigger a beam dump via the PIC. The powering converters must stop and the energy, stored in the magnets must be discharged. For the inner triplet of the HL LHC, no spot in the magnets must be warmer than 350 K when the heaters are fired. [32]

Quench Detection System (QDS)

The detection hardware is an important part of the quench protection. A schematic diagram of the Quench Detection System is displayed in Figure 2-10. To control the subsequent heat development after a quench, a rapid detection of the resistive voltage is needed. The detection must work in every operational mode, including the system ramp up [42]. The inductance of the coils induces a voltage proportional to the current change, this voltage must be compensated and must not trigger a detection. Therefore, a built-in logic in the QDS reads the voltage over multiple coils and the current change in the magnet circuit.

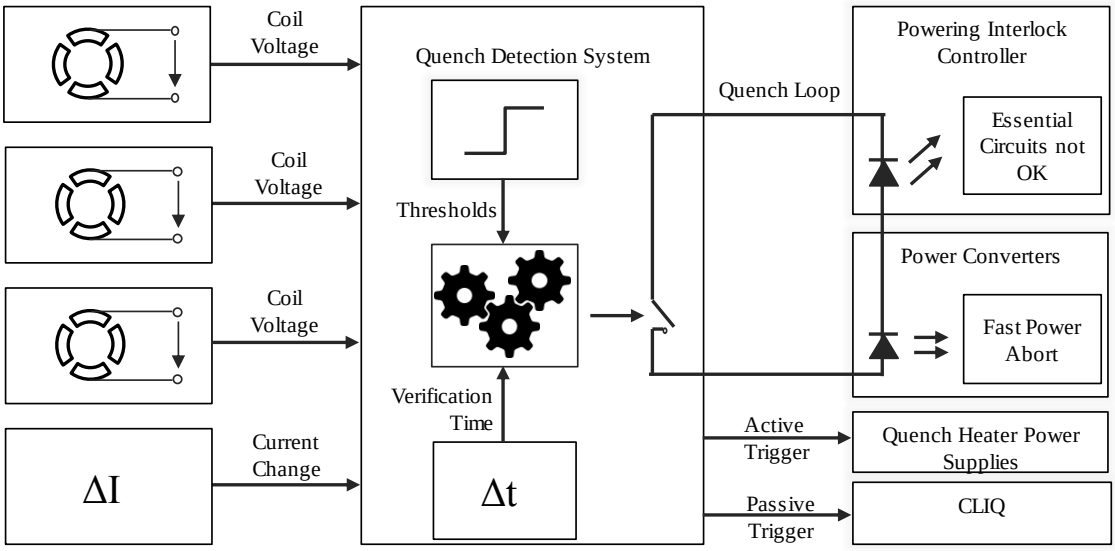


Figure 2-10: Quench Detection System Schematics

Implemented voltage thresholds and verification times are considered by the QDS. These parameters and more can be changed by the system expert even after the QDS is built. If the internal logic decides that the quench is detected and verified, the QDS interrupts the Quench Interlock Loop (QL). This loop connects all Quench Detection Units of the powering circuit to the PIC and the Power Converters. For the inner triplet, every quench detection system will have a redundant second system with interfaces to the quench loop [43]. The QDS does only interrupt the QL and does not read it. The voltage drop in the QL is read by the PIC. The PIC then requests a beam dump via the Essential Circuit-signal. The PCs read the Quench Loop as well and initiate an immediate Power Abort if the loop is interrupted. [33] [40]

The Quench Detection System triggers the protection mechanisms. For the inner triplet circuit, outer layer Quench Heaters and the CLIQ System is foreseen. The Quench Heater Power Supplies (DQHDS) are triggered by an active pulsed signal, i.e. the signal goes high when a discharge is needed. The CLIQ Systems are triggered by the signal going low when the discharge is needed. [43] [44]

The new Nb_3Sn magnet technology makes the detection especially challenging because it suffers from flux jumps that interfere with the detection thresholds. Therefore, filters are implemented in the detection system. The filtering time-window causes a delay between the measurable quench and the quench trigger. The timescale between a measurable quench and the trigger signal leaving the QDS is roughly 10 ms. [45]

Protection through Copper Stabilization

Protection mechanisms of superconducting magnets can be classified to passive protection i.e. protected by design – or active protection, meaning an external trigger is needed to activate the protection mechanism. With passive protection mechanisms, the local ohmic heat during a quench leads to a growth of the normal zone in the superconductor by conduction. If this process is fast enough, this is a cost-effective and if correctly installed a low-effort/high reliable protection mechanism. The cryogenics can even be designed to cope with the heat development, so that the quench returns to the normal state before the operation must be aborted. [11]

Figure 2-11: The bus bar in the LHC: Superconductors embedded in copper [46]

An example of this kind of protection is the busbar in the LHC. The busbar connects two magnets and is completely embedded in copper. The protection relied on the heavy copper stabilization. In case of a quench, the now normal conducting material will be bypassed by the copper and the heat will be transported away from the interconnection. The material returns to superconducting state or a voltage threshold is exceeded, and the powering is aborted, and the circuit energy is extracted from the circuit. [9] [12] [47]

Quench Heaters

As seen in Figure 2-5 a magnet is superconducting if the magnetic field, the temperature and the current density are below critical values. Therefore, raising one of these over the critical values results in a quench. A straightforward approach to force-quench a magnet is to install heating strips on the coils that – once triggered by the QDS after a quench –heat up the magnets.

The coil next to the heater strips will exceed the critical temperature and force-quench. This creates a greater normal conducting part of the magnet, so that the energy in the circuit is distributed to a big part of the magnet. The heating of the magnet is based on the conduction of the heat from the discharge strips to the coils. A simplified Quench Heater System Scheme is displayed in Figure 2-12 (left). It is built up of a capacitor C, a switch with two positions and the heating strips R, that are attached to the coils. Before operation the capacitor is charged by the voltage supply U_C. The connection to the voltage supply is closed. When a quench is detected by the QDS powers the relay RL(SW1). When the relay is powered for roughly 5 ms, the switch SW1 goes to the upper position. The capacitor energy is released through the normal conducting wires and the heater strip R_H. The powered heater strip creates ohmic losses in form of heat that emits to the coil-part L. The coil is developing a resistive zone R_C, propagating the normal zone of the magnet. For the HL-LHC inner triplet, 12 quench heater circuits are foreseen per magnet, placed outside the coils as displayed Figure 2-12 right. If a quench in one of the inner triplet magnets is detected, all protection mechanisms discharge, leading to a force quench of the triplet [32].

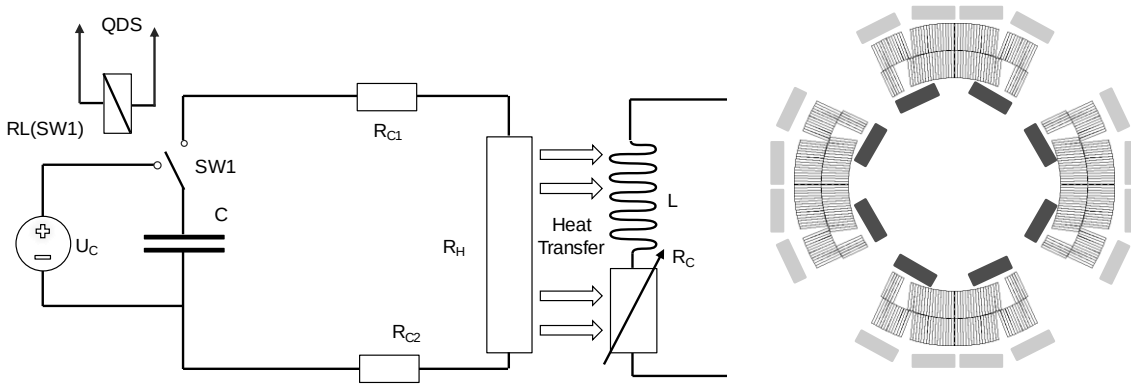


Figure 2-12: Left: Quench Heater System scheme to the magnet coil part L with the resistive zone R_C
Right: I-QH (dark gray) and O-QH (bright gray) Quench Heaters, attached to a quadrupole magnet

This technology has multiple downsides: The conduction of the heat takes time to bring the coil back to the normal state. It is stated in [32], that the QH technology is limited to time margins between 50-200 ms. Nb_3Sn based magnets (such as the inner triplet) however need protection in 20-50 ms [48]. Therefore, Quench Heaters alone are not sufficient to protect the inner triplet. The quench heating technology is often root of failures, such as during the tests of an inner triplet short model: Inner layer quench heaters created unacceptable bubbles after a quench, and

during cold powering, 2 out of 8 I-QH were lost after training quenches [49]. Even though the quench heaters are not directly connected to the magnet circuit, the discharging current in the heaters causes a magnetic field which can interfere with the beam trajectory. All the capacitors of a Quench Heater Power Supply can discharge within roughly 50 µs [11].

Coupling-Loss Induced Quench (CLIQ)

To overcome the limitations of present protection technology, CERN is constantly investigating new protection technologies. One outcome of this research is CLIQ. It is a novel quench protection technology developed at CERN. On contrary to other protection systems it directly discharges a current in the magnet circuit. The heating of the magnet relies on the subsequent fluctuations in the circuit powering. These fluctuations cause coupling-losses between the strands and filaments inside the magnet [11].

Figure 2-13 displays the schematic CLIQ System during a discharge after a detected quench and the currents in the circuit over time. t = 0 s is here defined as the time when the CLIQ Thyristor receives the trigger.

In Figure 2-13 A, the CLIQ capacitor C is charged by the voltage supply U_C and is connected with the normal-conducting leads R_{L1} and R_{L2} to the magnet coils L_1 and L_2. The coils are during normal operation connected to the Power Converter PC, which supplies the current for the magnets. While no quench is present, the Thyristors Th_{FW} and Th_{BW} are not conducting in any direction. Thus, the capacitor is not able to discharge and stays loaded.

In Figure 2-13 A, a quench is developing in the magnet coil L_1. When the QDS logic detects this quench, a trigger signal is sent to the Thyristor Th_{FW}. The thyristor Th_{FW} then becomes forward conducting, as seen in B. A current is discharged from the capacitor into the coils. The backwards Thyristor Th_{BW} is then triggered leading to a current backflow, C. As tests showed, the backwards Thyristor increases the effectiveness by far [50]. The current oscillates forwards and backwards through the Thyristors (D-E) and decreases to zero in roughly 0.2 seconds. This creates a more homogeneous force-quench of the magnet and leads to lower hot-spot temperatures than the presently introduced Quench Heaters [51].

The respective currents in the circuit to the given time in the upper images is displayed in graph F. The power converters are simultaneously decoupled from the magnets to protect them from the CLIQ-current.

The effectiveness of this protection mechanism is highly dependable on the connection of the current leads to the magnet. Losses are especially created, where opposing CLIQ currents are physically near to each other. The current is directly induced to the magnet circuit, meaning it interferes with the produced magnetic field and therefore also with the beam. [50]

The benefit of this technology is a faster, more equal distribution of heat and a lower hot-spot temperature after the quench in the magnet. Also, the current discharge induces changes in the magnetic field slower compared to the Quench Heaters. [52].

However, to protect the magnets sufficiently, high energies and thus big capacitors are needed. This is restrained by the increasing voltage to ground. The induced current that is sufficient to quench the magnet in flat-top powering, where the magnet is operated at the quench limit, may not be sufficient to quench the magnet during ramp-up. [11]

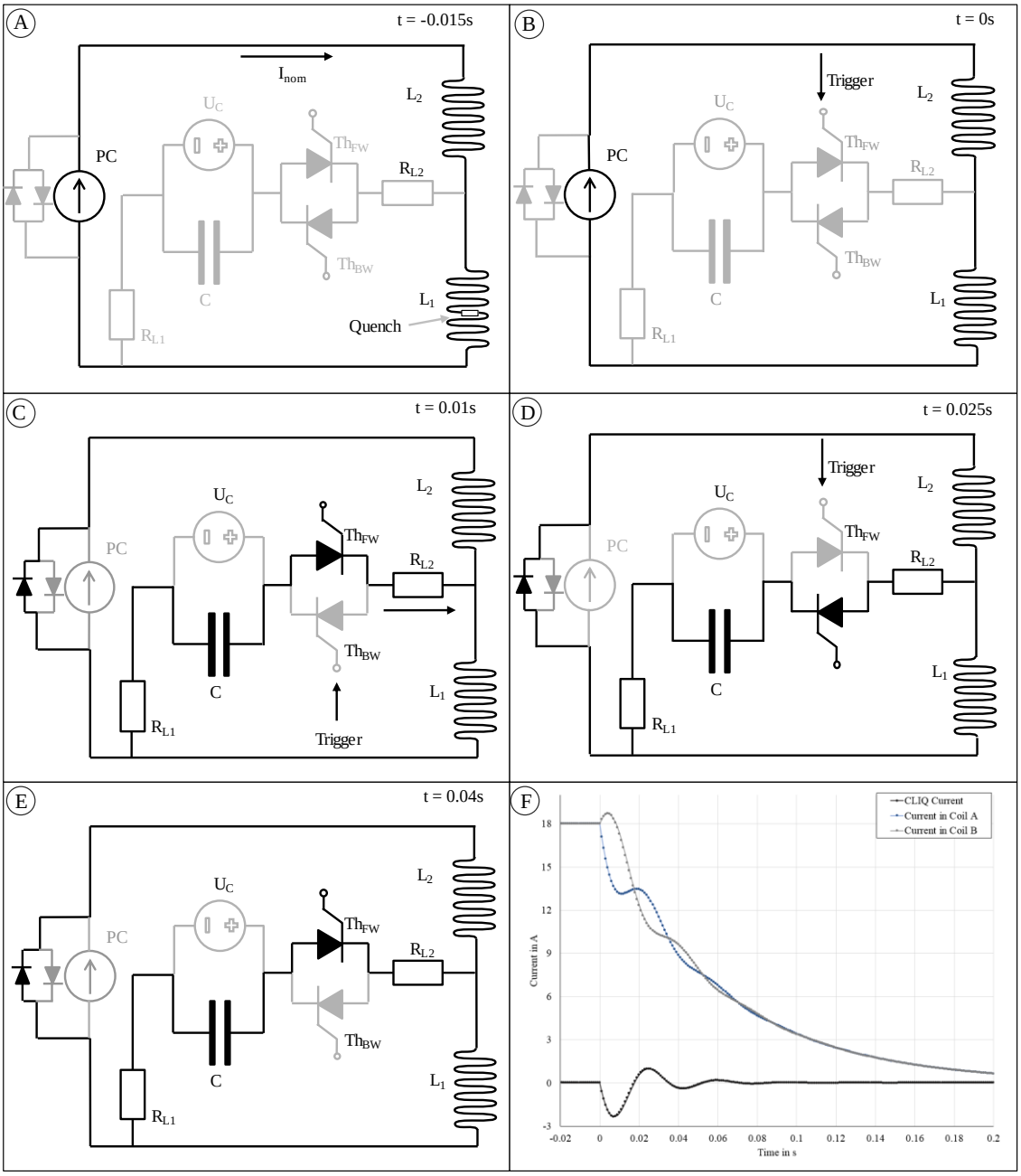


Figure 2-13: CLIQ System Scheme during a discharge in the magnet coils L_1 and L_2

For the triplet, a combined scheme of CLIQ and QH is foreseen. In addition, for the dipole magnets of the *Future of Circular Colliders (FCC)*, the 100-km circumference accelerator study [53]. Appendix C shows the detailed layout of a CLIQ Unit Power Supply v3 and Appendix B shows the connection of CLIQ Units to the magnet circuit.

2.4 System Theoretic Accident Model and Processes

The accident model STAMP (System-Theoretic Accident Model and Processes) is a recently developed causality model that is described in *Leveson's* book *Engineering a Safer World*. The content of this chapter is based on this book [1].

It is stated, that the big changes in engineering during the past 20 years such as growing system complexity, digitalization and automation need new methodologies for analyzing hazards, which focus not only on component failures, but also on system interaction failures, where every component fulfills its defined requirements, but accidents happen nevertheless.

Within STAMP, accidents happen when the system fails to keep itself in a safe state. The system must cope with external disturbances or degrading components and fall in a safe state if a failure happens. Therefore, the system is seen as a loop that controls the hazardous behavior and takes actions to keep the system safe. With this different approach it is obvious that increasing component reliability is not necessarily leading to a more dependable or safer system.

The system control structure has the shape of control loops. One example for a control loop can be seen in Figure 2-14. A control structure consists of controllers, actuators, controlled processes and sensors, these may be human or electronic. Each subsystem uses so-called control actions, as seen on the arrows in the Figure. The arrows indicate the direction of the control.

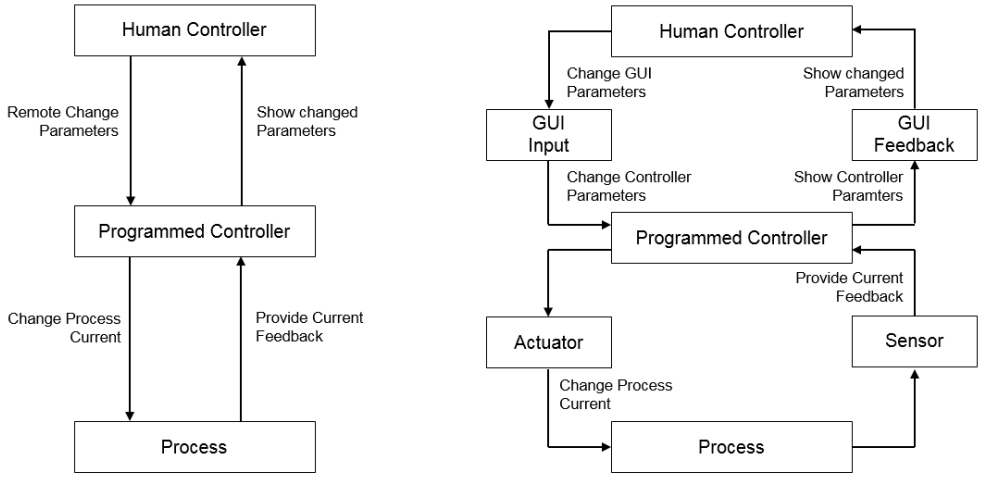


Figure 2-14: A typical control structure within a STAMP method (left) and the refined control structures with actuators and sensors (right)

The example in the figure above shows the control structure for a controller that surveils the process current. The controller itself is surveilled by a human that can change the parameters. The control action of the human is therefore *Change Parameters.* A communication between a controller and another controller or a controller and a process can be refined to display the actuators and sensors that are used by the controllers to realize the control action. The analysis

method is top-down, meaning the control structure starts with a high level of abstraction and refines until a suitable level of detail is displayed.

On the foundation of this accident model, different types of analysis methods emerged. An analysis of the already happened incidents, such as the 2008 LHC event is analyzed with CAST (Causal Analysis based on STAMP). The methodology STPA (System Theoretic Process Analysis) is used to analyze system hazards.

2.4.1 Incident and Accident Analysis with CAST

The causality model of STAMP can be applied to given incidents. To gain the maximum knowledge possible from a happened incident, one must investigate both technical and social aspects of failures. By only looking at the mere technical failure, chances to investigate on needed structural changes are missed. It is recalled by *Leveson* that this leads also often to a different view on the cause of incidents, leading to additional information. The analysis has three major steps that can be seen in Table 3.

The first analysis step is to define accidents and hazards that were involved. A typical accident includes buzzwords like *damage, loss, failure or pollution*. The hazard is not an accident itself, but a system state, that together with environmental conditions or further unsafe control actions might lead to an accident. Furthermore, the incident must be documented in a proximate event chain. This displays a series of events that – in the end – lead to a loss. Multiple examples for these event chains are given in *Leveson's* book.

Table 3: Major Steps of a CAST Analysis; Inspired by the XSTAMPP[1] Procedure

Analysis Step	**Content**
Establishing the Fundamentals	Define accidents and hazards that were involved with the loss. Derive analysis system boundaries, and system safety constraints. Create a proximate event chain.
Documentation of the Control Structure	Build the system top-down from the derived boundaries of the previous step. Document responsibilities in place.
Analysis	Analyze the physical loss. Move up the control structure and determine how every controller contributed to the loss. Consider dynamic system changes.

The following step of the analysis is to establish the system control structure as explained in the previous chapter. Responsibilities and constraints must be defined for every controller.

[1] XSTAMPP (eXtensible STAMP Platform) is a program made by the University of Stuttgart. It is assisting engineers in using STPA and CAST.

Environmental and behavior shaping factors of each controller must be documented for the later analysis, to determine why a certain control action was given.

The first step of the analysis is to analyze the failure at the physical level. It must be investigated how and why the error occurred and why the control-mechanisms in place were not effective in preventing the system from drifting to the hazardous state.

Then, the control structure is analyzed. The share of every controller to the failure must be investigated. Goal of the analysis must be to find out, why it made sense from the controller's perspective to act the way it did [1, p. 357]. Trigger words like *should have, could have* are usually a sign of assigning blame and being biased. To understand how an accident could occur, it must be assumed, that no one comes to work to do a bad job. Therefore, factors like *history, resources, tools and interfaces, training, human cognition characteristics, working under pressure, safety culture, communication* and *human physiology* must be considered [1, p. 361].

When every controller has been analyzed, the overall communication must be examined. Attention must be payed to *confusion of responsibilities, conflicting control actions* and *incorrect or missing coordination.* A control action might not be given, because a person is afraid of the consequences of reporting a problem. Further, the system may change over time. Failure messages may occur that often, that they are not considered dangerous anymore. A person might be very cautious, so that reported failures are not taken seriously anymore. Components may degrade, or workers may get fatigued working over multiple shifts. These system-dynamics must be considered.

Result of a CAST analysis is then a set of requirements. This includes suggestions to change the system layout, restructure responsibilities or changing process models or human or automated controllers. These changes can then be – if needed – analyzed with an STPA.

2.4.2 Hazard Analysis with STPA

A hazard analysis can be described as "*investigating an accident before it occurs"* [1, p. 101]. *Leveson* states that current hazard analysis techniques see failures as randomly occurring and therefore using those techniques would lead to a reaction-based approach towards hazard analysis. Therefore, STPA was developed by the Partnership for a Systems Approach to Safety (PSAS). Figure 2-15 and Figure 2-16 summarize the steps of analyzing a system with an STPA.

An STPA can be used to derive system and component requirements for a high system dependability. The analysis starts off with defining the accidents that the system must cope with. To create an exhaustive list of accidents, it is important to not start with a long list of detailed accidents. Starting off with a high level of detail inevitably leads to a high chance of missing an accident or hazard [54]. From this list of accidents, the system-level hazards are derived. A hazard describes system state in which accidents can happen, but not the failure itself. From this hazard list, the system control structure is derived. This structure is then refined until a suitable degree of detail is reached.

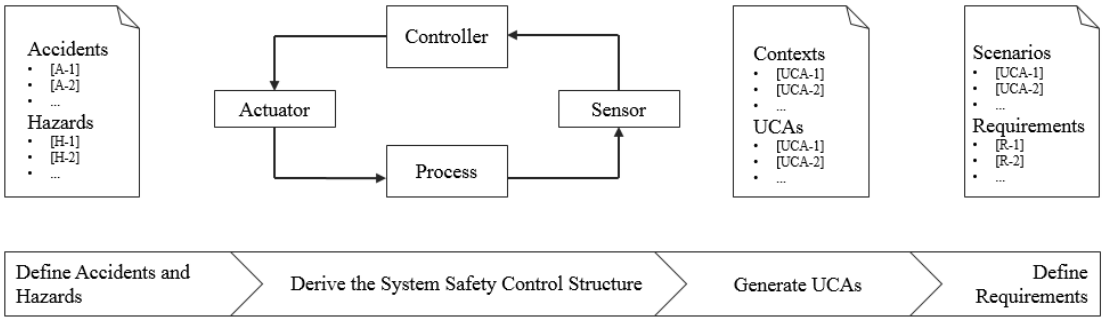


Figure 2-15: STPA procedure as used in this thesis; Inspired by the XSTAMPP procedure [55]

The system controllers (may be humans or computers/electronics devices) avoid the hazards by providing control actions. System safety and dependability emerge then as attributes of the interaction of all subsystems [1, p. 75].

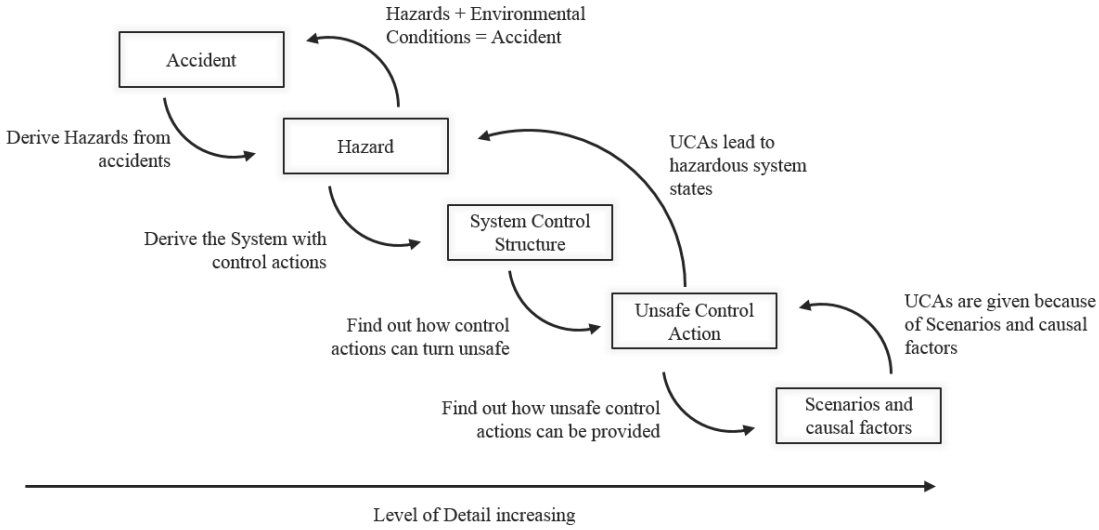


Figure 2-16: The connection of the different STPA Steps and terminologies

An example for such a control loop is given in Figure 2-17. It shows a simplified Quench Protection System. An accident for this system would be a permanent damage to the magnet, and the system hazard is an exposure of the magnet to the high electrical energy, stored in the magnet circuit.

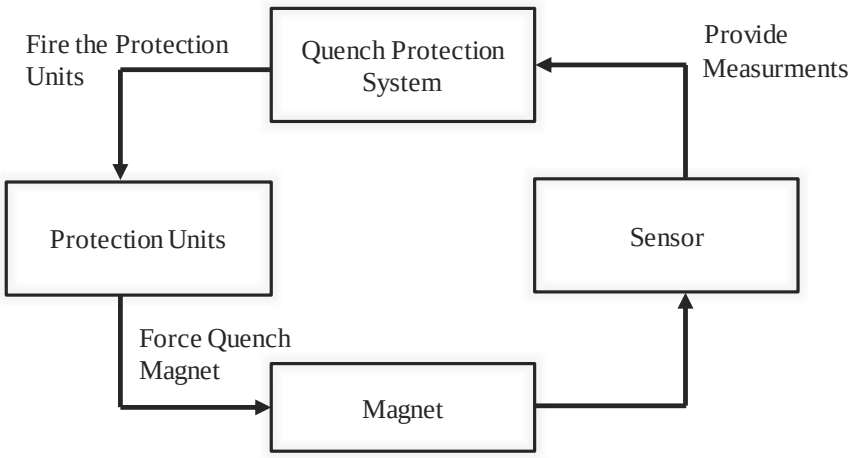


Figure 2-17: Example Control Structure of a simplified Quench Protection System

This system layout is now investigated. A hazardous system state is caused by an *Unsafe Control Action* (UCA). To find the unsafe control actions, multiple ways are suggested in [1, p. 213 ff.] [54] [56]. The first way is to categorize the ways a control action can become unsafe into the four categories:

- A control action may not be provided
- A control action itself is hazardous, because it is provided incorrectly
- A control action is provided in the wrong context
- A control action is applied too long or aborted too early

An example is the control action: *Fire the Protection Units*. In nominal conditions, the Protection Units must be triggered by the Quench Detection System. The following unsafe control actions can derive from the four described ways:

- The Protection Units are not fired when requested
- The Protection Units are fired, but too weak to heat up the magnets sufficiently
- The Protection Units are fired in the wrong context, meaning when no quench is present
- The Protection Units heat up the magnet too long or short

The unsafe control actions are then linked to the pre-defined hazards to assess the possible hazard of the control action. In this case they are all linked to the same hazard: Exposing the magnets to the electrical circuit energy.

It becomes obvious, that for the unsafe control actions, the *wrong context* is not easy to find. Many different contexts are possible in which a quench heater can be fired. To find all contexts in which a control action is hazardous is not trivial, especially as the LHC has many system states and many components that could fail. Therefore, *Thomas* suggested [56], to generate all possible contexts with so-called context tables. The engineer must define certain number of variables that define a context (E.g. *Beam Presence*). Each of these variables can take on different values (e.g. *Not present* or *Low-intensity* or *nominal intensity*). The recombination of all variable values is then the context in which the control action may or may not be provided. The list of possible contexts is defined, and it must be asserted if providing or not providing a control action is hazardous.

Result of this operation is also a list of unsafe control actions. For the given example in Table 4 the refined unsafe control actions are:

- The Quench Heaters are fired, when the beam is present while the magnets and Power Converters are okay.

- The Quench Heaters are fired, when the beam is not present while the magnets and the Power Converters are okay.

Table 4: Context Table for „Firing Protection Units: Quench Heaters"

Variable: Value #1: Value #2:	Beam Presence Beam No Beam	Magnet Status Quench No Quench	PC Status Failing OK	Hazardous? Yes No
	No Beam	Quench	OK	No
	No Beam	No Quench	Failing	No
	Beam	No Quench	OK	Yes
	No Beam	No Quench	OK	Yes

Both UCAs are spurious Quench Heater behavior and are hazardous to the magnets. Yet it is not asserted if and how these control actions could be reached. Therefore, the second step of the STPA is needed. Causal factors are searched that lead to a scenario. This scenario then leads to the unsafe control action. Help is provided by Figure 2-18, yet it is stated that one must try to avoid searching for trigger words and must brainstorm himself or possibly with the help of experts to find an exhaustive list of scenarios and causal factors. Typical causal factors for a generic control loop are shown there, e.g. an inadequate sensor operation leading to inadequate or missing feedback. The controller must be able to spot this behavior and fall in a fail-safe mode.

For these detailed failure scenarios and causal factors, a list of safety requirements can be derived to deal with them. For the first unsafe control action in the given list, the scenarios and causal factors could be like shown in Table 5.

If the requirements cause changes in the system control structure or cause new control actions, an iteration over the changes can assure that the system is dependable. STPA is a purely qualitative analysis and does not produce a probabilistic assessment of the dependability.

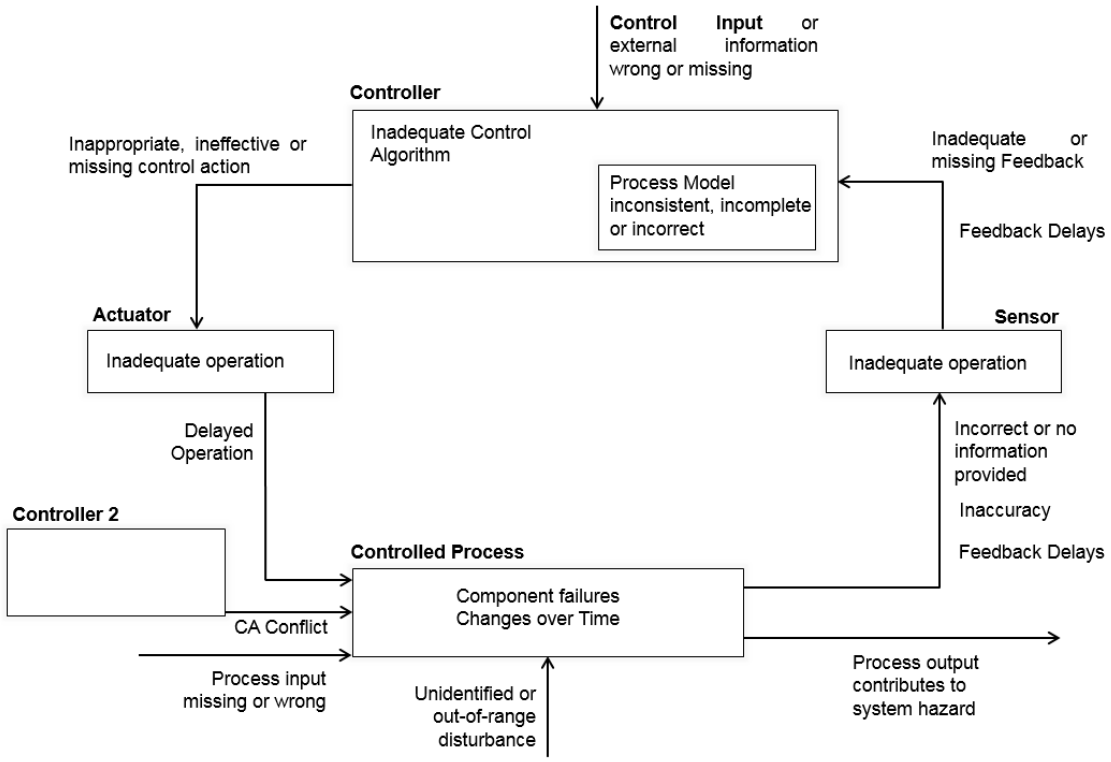


Figure 2-18: The 2nd Step of an STPA, inspired by [54]

Table 5: Scenarios, causal factors and requirements for the discussed UCA

Scenarios	**Causal Factors**	**Requirements**
The implemented detection parameters trigger on non-hazardous signals	The parameters have been changed in a previous run and have not been changed back	Include a manual parameter check of the detection before starting the operation
The actuator receives no trigger, but fires the heaters	A component in the actuator fails and triggers a discharge	A dedicated campaign must be performed to show the effect of a spurious discharge

2.4.3 Software-Tools for STAMP

Different software tools for STPA are available – usually for free if one requests the software at the authoring institute. XSTAMPP (eXtensible STAMP Platform) was developed at the University of Stuttgart and is used for assisting the works in this thesis [55]. The program version in the presented work is 2.3.0. Multiple tutorials, the hardware requirements and the downloadable program can be found online at [57].

3 Analysis of the 2008 LHC Incident

Analyzing accidents and incident offers the unique opportunity to find flaws in a realized system and to prevent similar failures for future systems. The publicly perceived 2008 LHC incident was analyzed with the recently at MIT developed method CAST. As an in-depth technical analysis is already written, it is possible to compare the results of this analysis technique with the given recommendations. Chapter 5 provides the evaluation of the method and a comparison of the results to the task force report.

The present chapter will first give a brief introduction to the incident followed by a dedicated section to each analysis step. To keep the analysis concise, the appendix will provide additional information.

3.1 Introduction to the Incident

The LHC construction was permitted in 1994. The magnets for the LHC were produced and tested in industry, the installation in the former LEP-tunnel was also done by an external consortium consisting of three companies. The Hardware Commissioning Group started after the magnets were interconnected in the tunnel. Aim of the commissioning is to ensure a safe testing and starting of the system, e.g. to make sure that no short circuits are installed or that the communication between the subsystems work as intended. While commissioning, sector 3-4 was the last one to check. The powering was ramped up in several tests. As the forces onto the magnets scale with the circuit current, the current was increasing with each test. During a powering test in this sector on 19.10.2008 a so-far undetected resistive voltage in an interconnection busbar between a quadrupole magnet and a dipole magnet built up. Protection mechanisms failed handling the quench. The busbar interconnection heated up and broke apart leading to an electrical arc damaging a vacuum line and a helium enclosure, leading to severe damage and displacement of the magnets. A typical interconnection can be seen in the top image of Figure 3-1. Part of the damage done by the arc and the severe displacement of the magnets can be seen in the bottom two pictures. [58]

This incident caused over half a year of repair time and roughly 40 million CHF repair costs. This remains until today the only event at CERN leading to significant damage. [59] [60]

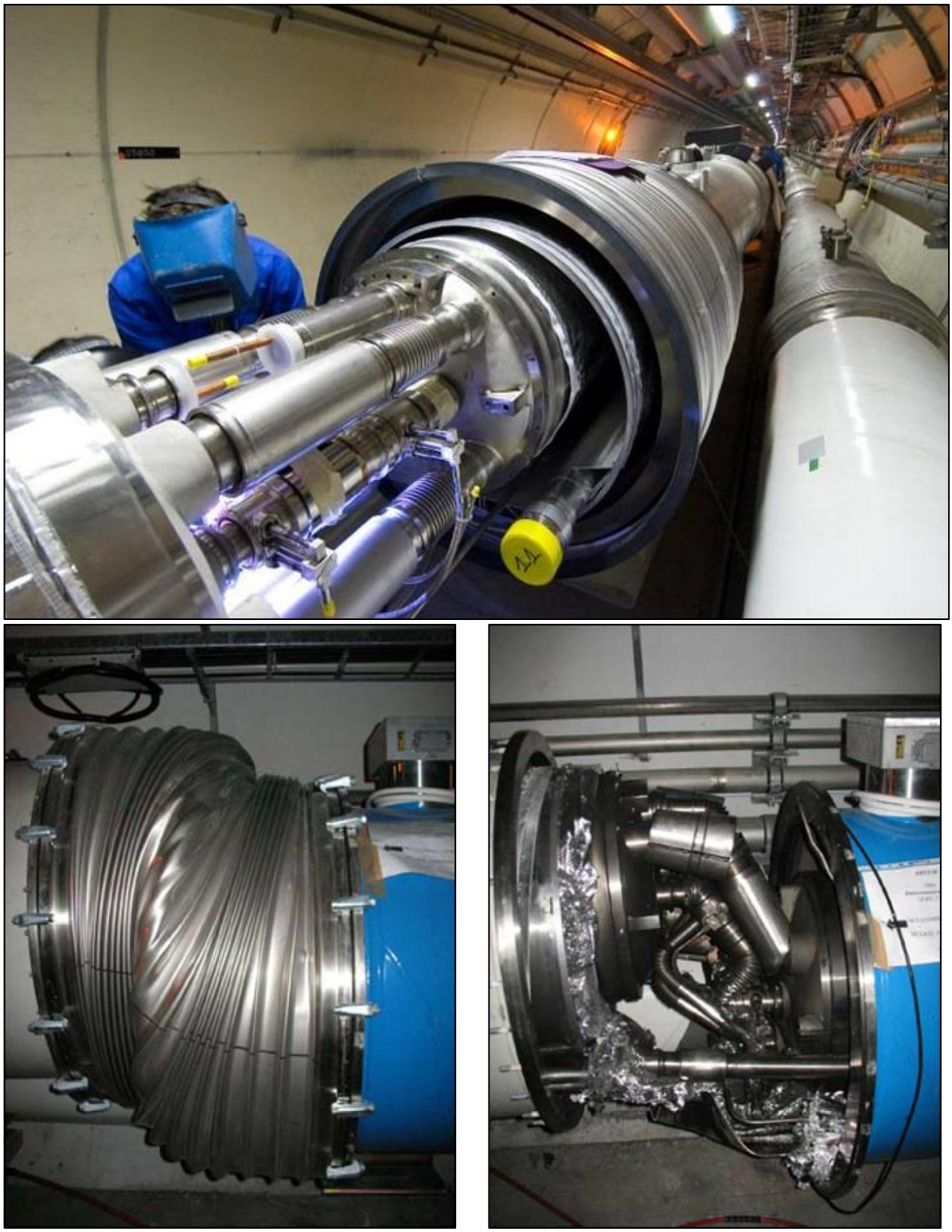


Figure 3-1: Top: A technician installing an interconnection and damage of the LHC after the 2008 Incident [12] [61]

The assembly of an interconnection busbar is shown in Figure 3-2. The busbars from both magnets are put together with tin layers in between into a soldering machine that then executes the soldering process. The copper functions as a passive protection mechanism as explained in chapter 2.3.1. An incorrect interconnection is today the most likely root of the incident. An

omitted soldering can explain the estimated resistance following simulations after the incident. [62]

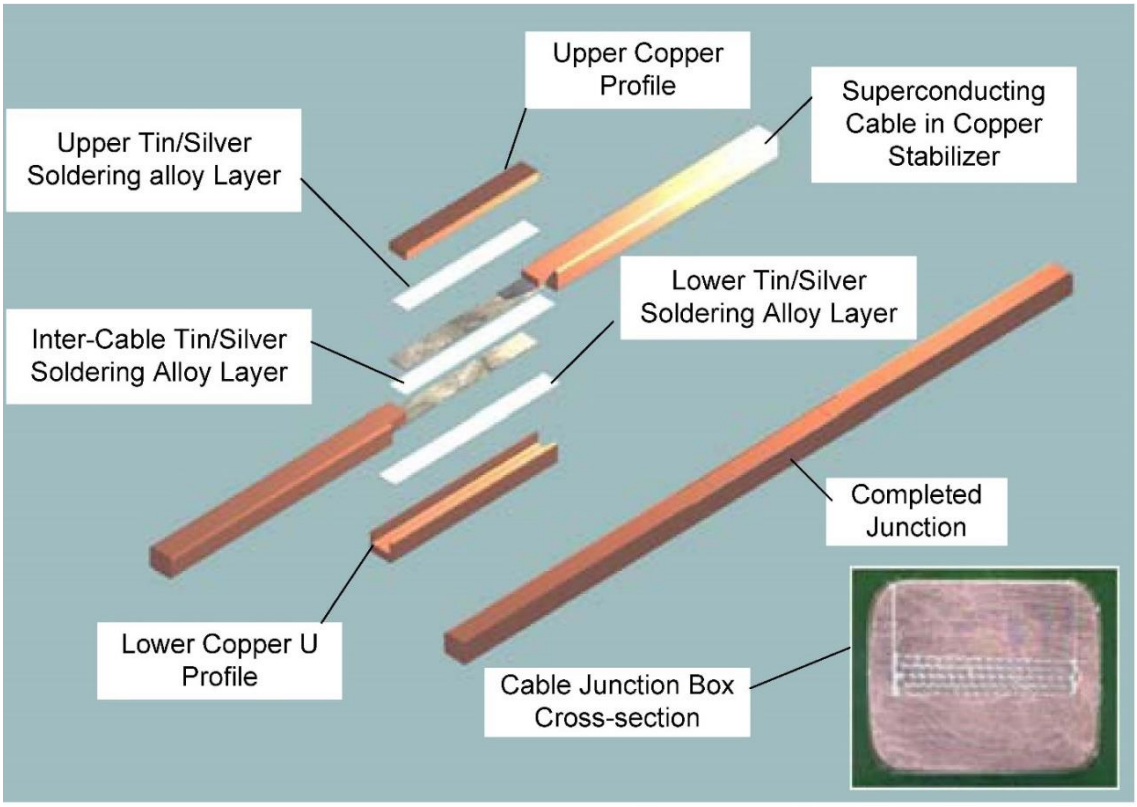


Figure 3-2: Assembly of an interconnection and cross section of a correct junction box

After the incident, a taskforce was built up to investigate the root of this failure based on the logged post mortem data and physical inspection. The mandate of the task force was to establish the sequence of events, analyze and explain the developments of events and to give recommendations to prevent similar incidents in the future. [12]

3.2 Fundamentals of the CAST Analysis

The fundamentals of the analysis include defining the involved hazards, the event chain, the system control structure, the responsibilities and the environmental and behavior shaping factors of each controller.

The system(s) and hazard(s), that were involved in the loss must be defined. The accident happened during a powering test of the Hardware Commission Group after the installation of the LHC. The identified system hazard is: “Resistive voltage in the circuit after installation.” This hazard, together with environmental conditions, such as not detecting the flawed interconnection, led to the actual accident.

The subsystems, that were involved in this hazard are shown in in Table 6. The safety goal of the system is to enable a safe hardware installation in the tunnel, a safe start-up of the machine and to protect humans from dangerous areas.

Table 6: Identified subsystems for the CAST Analysis

Identified Subsystem	**Why was this system included?**
LHC Project Management	Provides budget, schedule, safety culture
Interconnection Team	Does the physical work of the interconnection
Interconnection Design Team	Delivers the procedure of interconnecting the magnets
Hardware Commission	Is responsible for the start-up of the system
Physical LHC	Includes the technical aspect of the accident.

The interconnection team, consisting of a consortium of external contractors did the physical work of interconnecting the magnets in the tunnel. The design team's task was to deliver a safe interconnection design, which is why they were included in the analysis. The Hardware commission must spot and repair all potential flaws in the electrical circuit. The LHC was included to also analyze the technical aspects of the failure.

3.2.1 Documenting the Proximate Event Chain

The sequence of events that led to the loss is shown in Table 7. The starting point for this analysis was the start of the interconnection process in September 2006. The interconnection procedures of sector 3-4 started in 2006 and ended nearly a year later. Was the schedule too ambitious? What were the working conditions like during installation?

The Hardware Commissioning Group investigated the hardware of the sector subsequently. Aim of the commissioning is to verify the operation of the LHC. As the forces in the magnets increase with the powering, the powering was increased in steps test by test. The nominal powering value was foreseen to be roughly 12 kA. The sector was already stable at 7 kA before the accident happened in the following days at 8.7 kA. What was the working conditions like during HWC? Could bad working quality be the result from pressure from the management? When the Hardware Commission was testing sector 3-4, why did nobody check the temperature sensors?

The energy extraction was activated after the voltage threshold of 1 V in the whole circuit was exceeded, was the foreseen protection suitable to handle the failure?

Table 7: Description of proximate events [12]

Date (&Time)	Event Description	Notes
10.2006	Installation of Sector 3-4 started	How were the working conditions like?
07.2007	Interconnection Sector 3-4 finished	Schedule too ambitious?
07.2008	Hardware Commission of Sector 3-4 started	How was the Atmosphere during HWC?
15.09.2008	Sector 3-4 stable at 7 kA	-
15.09.2008, 19:00h	Increase of Temperature in the cold mass of sector 3-4 during the 7 kA powering test	Why was this not checked?
19.09.2008, 11:00h	Ramping up to 12 kA started	-
19.09.2008, 11:18h	Ramping up to 8.7 kA successful	
19.09.2008, 11:18h	Resulting Voltage in the whole circuit over 300 mV	Protection mechanisms sufficient?
19.09.2008, 11:18h	Measured current not following reference current	-
19.09.2008,11:18h	Fast Power Abort triggered	-
	Electrical Arc developing	-
	Damage to Helium Enclosure	-
	Helium released to vacuum	-

3.2.2 Documentation of the Safety Control Structure

The chosen subsystems from Table 6 are modelled as a safety control loop. This control loop assigns responsibilities to each controller. Figure 3-3 shows the first iteration of modelling the subsystems.

The LHC Management defines budget, environmental conditions, provides the safety culture and the timescale for the other system components. The respective subsystems deliver feedback for the given decisions.

The interconnection is designed by the design team. They provide help and counsel to the HWC and the interconnection teams. The manual work of interconnecting the magnets is done by staff and technicians of industry contractors. The Hardware Commission must test the built hardware and verify the operation of the LHC.

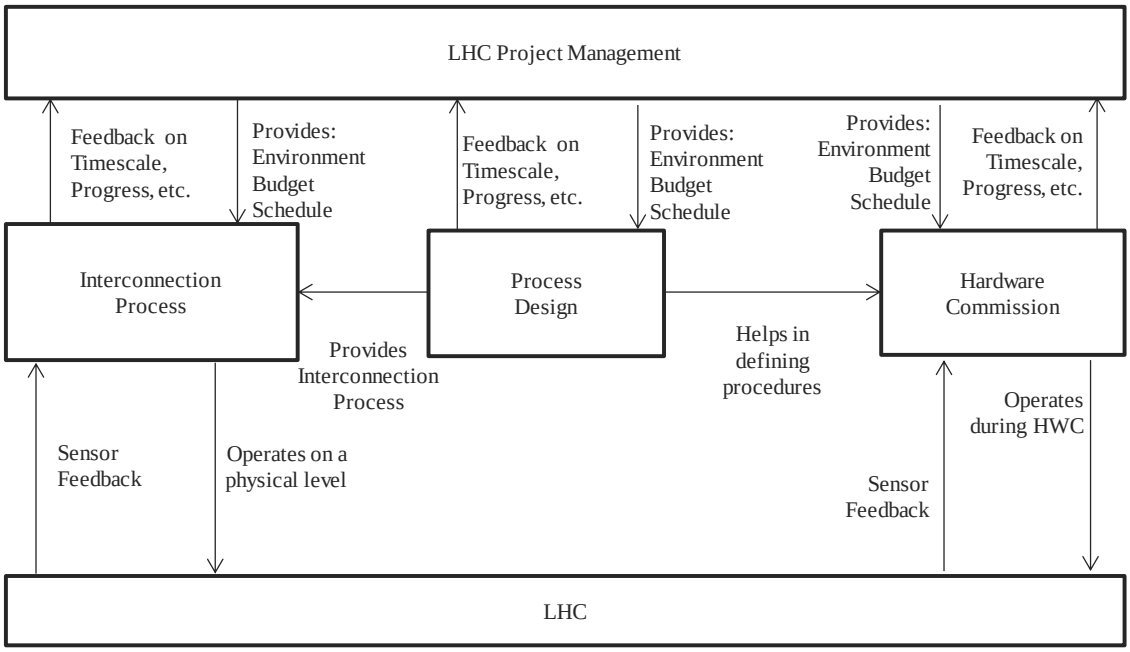


Figure 3-3: Control structure after the first iteration of the analysis

In the following sections, every subsystem is refined and described. Appendix C shows the detailed overview on the responsibilities, safety constraints and behavior shaping factors of the refined controllers.

Interconnection Process

The physical work of the interconnection process was done by the interconnection team. Inputs to this system are the developed interconnection procedure by the design team, the timescale, budget etc. of the management and the feedback of the LHC in terms of test results and the soldering sensors.

Figure 3-4 shows the refined structure of the interconnection process. The interconnection process itself was outsourced to industry to make the process less expensive and the tools more industrial. The consortium consisting of three companies, provided the improved tools and the workers for the interconnection. The detailed composition and responsibilities have been defined in an expert meeting and with the paper presented in [63] and [64] showing the organizational structure.

The interconnection operators did most of the manual work. They assemble the parts and start the soldering process. The interconnection procedure can be described as manual work with human quality control. The quality assurance of was based on a closed-loop data recording of the process temperature and the process pressure. The installations in sector 3-4 were facing the worst working conditions of all sectors “due to high humidity and low temperature” [12, p. 2]. In addition, it was not sure whether the workers could continue to work for their employer [12, p. 5].

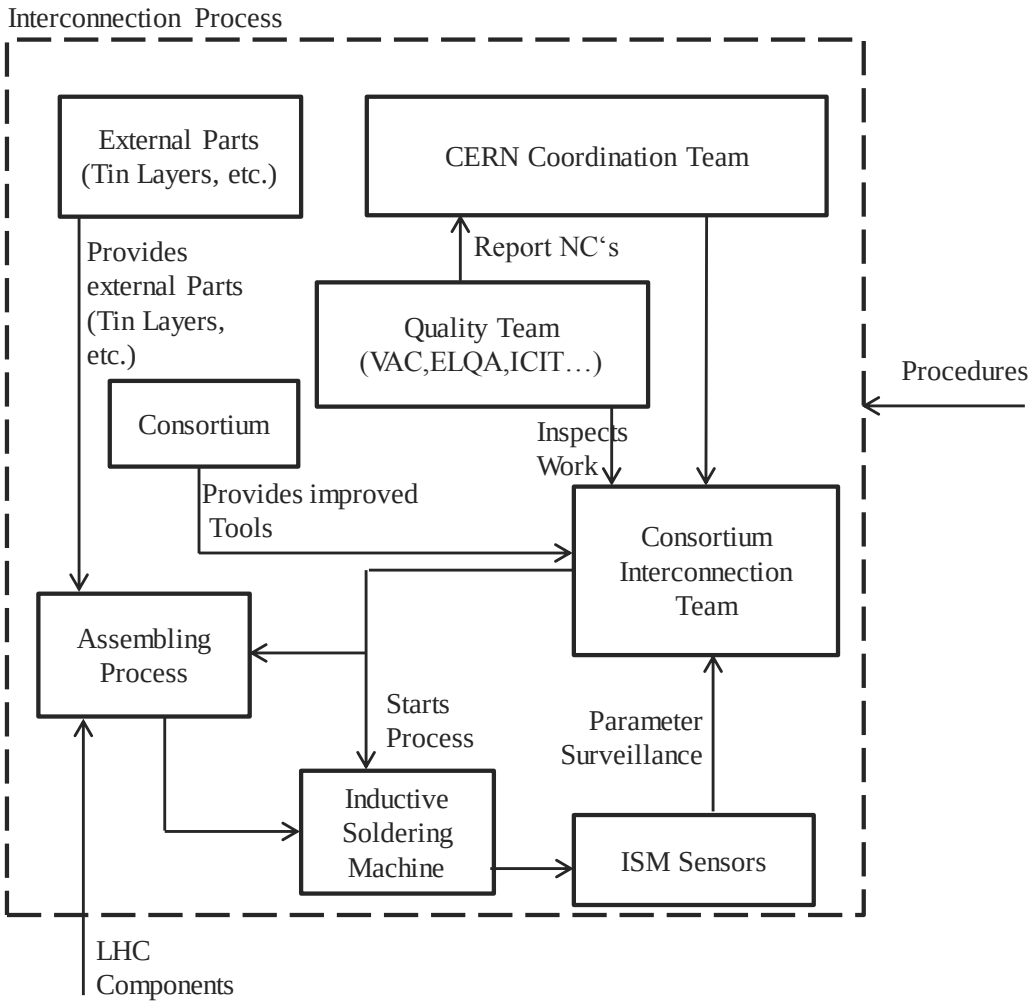


Figure 3-4: STAMP Control Structure of the interconnection Process

The Coordination Team consists of CERN Staff and oversees the soldering progress and manages the Consortium Interconnection Team and the Quality Team. When non-conformities are reported, the coordination team calls the special assembling team (not shown in the graphic).

Additionally, the CERN Quality Team, consisting of CERN and experts from a collaborating institute made a visual quality check of the interconnections. Once there were no flaws in the interconnection spotted and the process parameters pressure and temperature of the soldering machine were in defined thresholds, the interconnection was marked done on a checklist. The CERN Quality Team reported non-conform interconnections to the CERN Coordination Team. The Coordination team can then take appropriate measures. [63] [64]

Process Design

Task of the process design was to design the interconnection. Following the design, the procedures of the interconnection must be defined in a reliable way. The development strategy

is documented in [65]. The design engineers suggested the design to the project engineers, that then revise and approve the design ultimately. The specification committee approved the suggested design after it was approved by the project engineers after checking it for costs, schedule and safety.

Many different methods to solder the interconnection were studied. From those studied methods the inductive soldering seemed to be the most promising due to low heating time and reliability. Multiple experiments showed the allegedly reliable process, where no tested splice was above the defined limit of resistance. Also in-situ measurements after the soldering were tested, yet no method was delivering satisfactory results and therefore a closed-loop parameter surveillance was chosen to control the process: The soldering machine monitored the pressure and the temperature of the soldering process. When the values exceed certain values, a failure is spotted. [66]

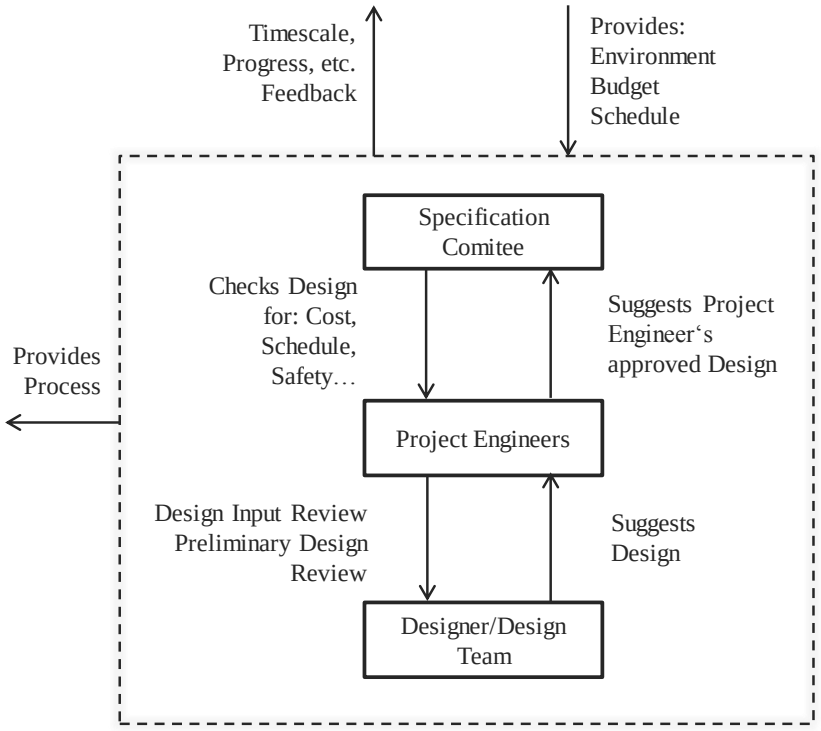


Figure 3-5: Engineering Process at CERN

Hardware Commission (HWC)

It took several months to commission every LHC sector. The hardware commissioning team consists of experts who – once the system is installed – bring the machine into service without beam. Every sector consists of many different subsystems that needs to be checked. Figure 3-6 shows the composition of the Hardware Commission. [67]

The Operator on Shift (OoS) executes the tasks defined by the Engineer in Charge (EiC). He is an accelerator technician with experience in of the LHC injectors or with the test facilities in

SM18. He executes the defined test plans and further assists the EiC in handling the access. [67]

The System Expert (SE) is an engineer, physicist or technician with experience in one of the involved systems of the powering tests. He prepares his system for the HWC in the field or from the CCC. It is his responsibility to monitor, analyze and manage the performance of his system during HWC. [67]

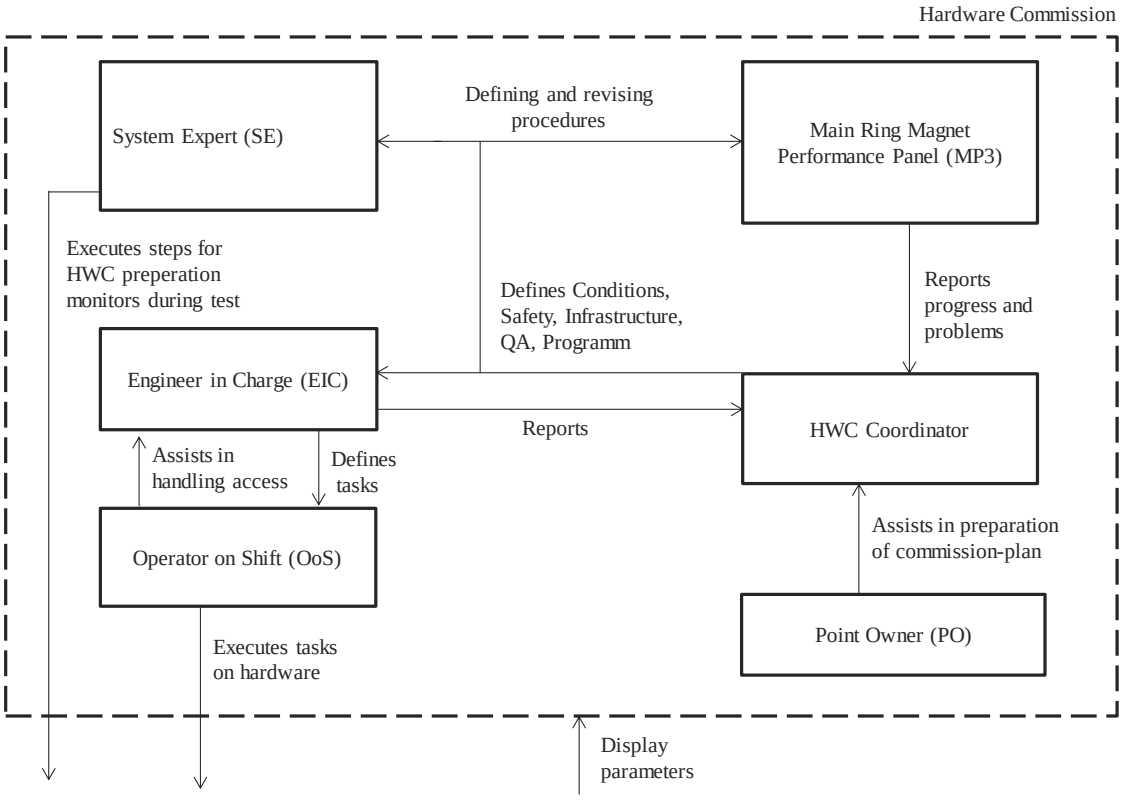


Figure 3-6: Hardware Commission Control Structure

The Engineer in Charge (EiC) is an accelerator Engineer or Physicist with at least 2 years of experience in the operation of CERN Accelerators. He is responsible for safety, ensures the execution of the plan and contributes to the execution by his expertise. Documentation of tests and the progress is also his task. Further, he coordinates the access together with the OoS and the Point Owners (PO). [67]

The HWC Coordinator is an engineer/physicist with experience in superconducting circuits. He defines the commissioning program together with the system expert. He prepares the conditions for the commissioning regarding safety, environment, infrastructure and quality assurance. [67]

The procedures are supervised by the Main Ring Magnet Performance Panel (MP3). The panel acts as the final controlling organ of this structure. They define and revise the procedures for the tests and monitor/analyze all aspects of the magnet performance. They communicate the

progress to the community and the LHC Project Management. The measurements from the LHC sensors was closely monitored by the system experts. This structure proved to be working for the other sectors, where commissioning went exceptionally well. [67]

LHC Project Management

The LHC Project Management is the highest level of hierarchy still considered in this analysis. It provided schedule, budget, coordination and environmental conditions (e.g. safety culture) to the other subsystems. It was bound to the budget constraints by the member states.

The LHC

The LHC was designed by CERN engineers and was built by CERN with part of the equipment outsourced to industry. The interconnections between the magnets in the tunnel were executed by an industrial consortium. It provides feedback to the HWC personnel with the built-in sensors.

The dedicated bus bar quench detection system was cut during the development process, as the budget fell short. The protection of the bus bar then relied on the heavy copper stabilizer until the energy is discharged. Multiple experiments were made to show that a quench in the bus bar is very unlikely.

3.3 Analysis of the Control Structure

To start with the analysis, the physical failure is analyzed: A resistance in the bus bar connection caused a quench that led to heat development. This caused the bar to fall apart and built up an electrical arc, damaging the interconnection. Today's knowledge points at an absence of soldering as the most likely cause for the incident. Figure 3-7 shows, how each top-level controller contributed to the incident.

The designed quench protection system for the busbar interconnection was designed to detect a quench in the busbars as well at first. It must be noted, that this safety mechanism could have prevented the incident. So, why was the bus bar quench detection not built in? Even the present voltage taps were enough to detect quenches in the bus bars. Quenches in the busbars were considered very unlikely. The interconnection procedure was tested and found to be very safe. When the budget fell short, something had to be cut. As it did not seem to be the most imminent safety mechanism, the decision fell on deleting the bus bar quench detection. The protection of the busbars relied therefore only on the copper stabilizer surrounding the interconnection until the voltage in the circuit exceeds 1 V. Then the energy is extracted via energy extraction systems.

The interconnection team connected the magnets. The sheer number of interconnections led to a highly repetitive work, where concentration went lower, and motivation might have reduced over time. As already mentioned, the working conditions were the worst among all the sectors. Furthermore, the interconnection in sector 3-4 was when the continuity of the working contracts

was not guaranteed, again leading to a decrease of motivation of the workers. The contracts with the companies were result-based. This might have created a quantity over quality mindset.

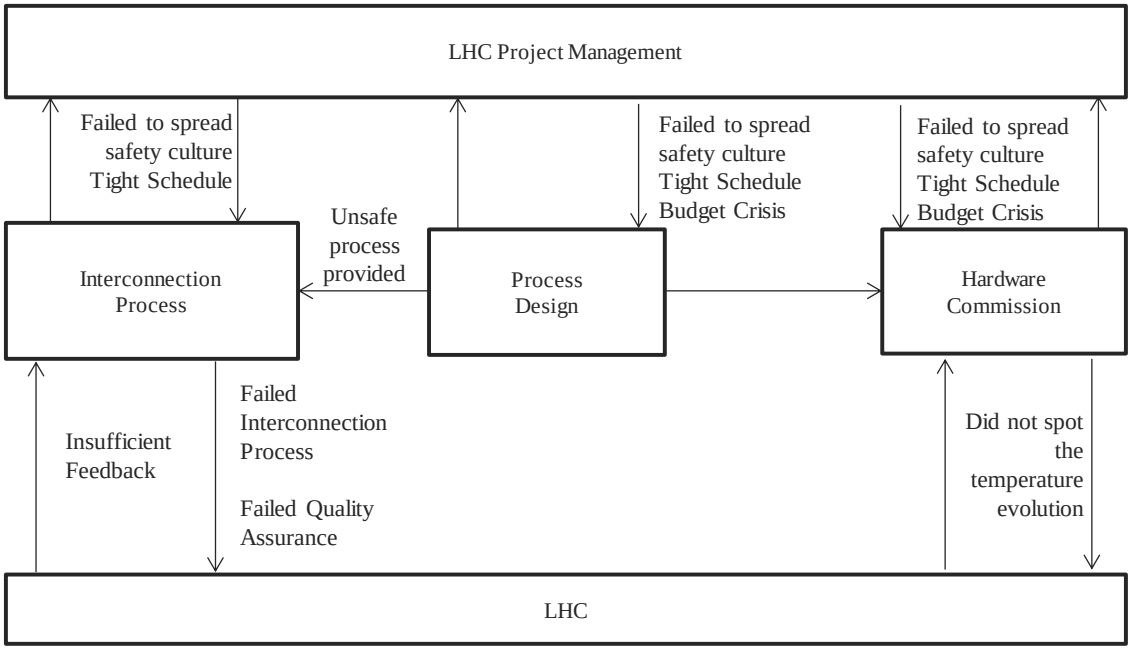


Figure 3-7: Failures in the control structure

The CERN Quality Team was supposed to find and report bad soldering spots to the CERN Coordination Team. They failed to find and report the critical soldering spot and (as it was revealed during reparations) many other bad soldering spots. How could this happen? As for the interconnection team, the working conditions were bad in this sector. The interconnection process was considered very safe and reliable and led together the repetitive work (>1700 joints) and a reduction in concentration. A documentation the interconnection quality was applied, however it was also documented as being correct for the questionable interconnection [68]. This shows, that the documentation in place was not sufficient. Furthermore, the feedback from the process was limited: Judging the quality of the interconnection based on the parameters and visually turned out to be totally insufficient.

The CERN Coordination Team had no knowledge about the failure and could not intervene.

The design process did not deliver a process that was safe enough. Also, the decision not to implement the dedicated bus bar quench detection turned out to be unsafe. This decision was made under the circumstances of a budget crisis. Furthermore, an expert meeting revealed that there were safety and hazard analyses foreseen for the design of the interconnection, but those were not formalized, and the systematic development approach was not followed. The strategic development procedure was not followed. During the time of the LHC construction, CERN had a general lack of awareness of the necessity of hazard analyses and strategic development.

The System Expert of the cryogenic system did not check the temperature evolution during the powering test on the 15th of September. The previous, very successful machine-checkouts led to a very confident mindset of the Hardware Commission. The absence of critical failures during the test of interconnections led to the wrong assumption that the powering is safe. Therefore, the attention was not as high as necessary, and the temperatures were not checked.

The LHC Project Management provided the timescale for the large-scale project that is often described as too ambitious. However, the Project Management is bound to member state's budget promises and therefore decided on the budget and time plan. The budget crisis led to the necessity of shortening the budgets. It must also be the responsibility of the management to spread the awareness for hazard analyses. However, reliability research was not common around in the accelerator industry. The general lack of hazard awareness led to a missing willingness of spending budget and time on dedicated safety and reliability research; also the methods were not known to all engineers.

3.4 Recommendations

Result of the CAST analysis is a set of recommendations. This set is presented in this chapter. A comparison to the results of the Task Force Report is done in Chapter 5.

The CAST analysis showed, that the interconnection process was failing on multiple levels. It is not only the failure of single persons working badly in the tunnel, but also of the procedure leading to a high amount of repetitive work under bad working conditions. Future projects, like the four times as large in circumference FCC, might lead to even more repetitive work for the interconnections.

The analysis, done in 2008 revealed that the cause of the incident is most likely a bad soldering spot. Within the CAST method, it must be assumed that *nobody comes to work to do a bad job.* This implies, that the failure is not a one-time event of a frustrated worker, but is the effect of a systematically incorrect interconnection process. Therefore, all other splices must be checked for bad soldering spots. This was already done and revealed many other bad soldering spots that have been repaired. [12, p. 16]

The analysis of the behavior shaping factors of the interconnection team revealed the bad working conditions. Making sure, that all workers have sure contracts for the time they work at CERN can improve the motivation and therefore also the quality of the work. Using result-based contracts might improve the speed of the workings, but can also lead to a quantity-over-quality mindset. For future projects, the usage of result-based contracts must be rethought.

The proximate event chain shows, that the temperature evolution hints at an incorrect splice resistance. For future powering tests, the temperature sensors of the powered sectors must be used to check the temperature evolution. Detected non-conformities must cause an investigation.

The analysis also showed, that the system is not capable of returning to a safe state, when a localized quench in the busbar occurs. It is therefore recommended to add a dedicated quench detection for the busbars again. This was already done by using voltage taps that were already implemented to the magnets.

The mentioned dedicated quench detection system for busbars was initially implemented, but was cut due to budget reasons. This hints at a lack of safety awareness at the time of the incident. This was confirmed to be true by discussions with experts. No dedicated dependability strategy and no reliability analysis methodologies such as FMEA have been made for designing the interconnection. For future projects, a mandatory hazard analysis for safety-relevant features must be formulated. This can be compared to the mandatory FMEA for ISO 16949. Failing human actions must be considered as a failure mode in the analysis. The task of the project management to choose a sufficient hazard analysis technique or a pool of techniques that engineers must choose from. Further, the management of future projects must keep the awareness for hazard analyses. While the incident dramatically showed the necessity of hazard analysis techniques, the absence of critical failures must not lead to an incorrect assumption of general safety. The management must realize its mandate to keep the safety culture high, also for the future.

The effect of the bad soldering spot was a breaking of the interconnection that grounded the voltage. The analysis of the physical failure and the proximate event chain show the direct link between the breaking and the electrical arc between the bus bar and the helium enclosure. An additional safety system must be implemented, that eradicates this link. This was also already done by installing additional clamps which – in case the interconnection is done incorrectly – hold the interconnection together. [69]

The bad soldering spot was most likely caused by an absence of soldering material in the interconnection. To eradicate the possibility of forgetting the soldering, an automated documentation of the interconnection procedure must be discussed for future projects. Figure 3-8 shows a suggested improvement to the interconnection process. The soldering machine is connected to a controller, that runs a monitoring algorithm. The interconnection team scans the components for the interconnections, and the controller only starts the process, if all components have been scanned for this position. The controller marks the position as “done” if the supervised parameters of the soldering machine were inside defined thresholds and the Quality Team marked it as okay. This ensures that the interconnection was done in the nominal procedure, and it was checked by the Quality Team.

The analysis of the CERN Quality Team and the overall communication shows, that the system passed the quality control. This hints on an insufficient quality management. The quality management was based on a closed-loop process, with additional visual control by experts. This should have been further improved, by measuring the resistance with high precision voltmeters to find abnormal connections. This was already done after the incident and revealed bad soldering spots. This shows that the measure is applicable.

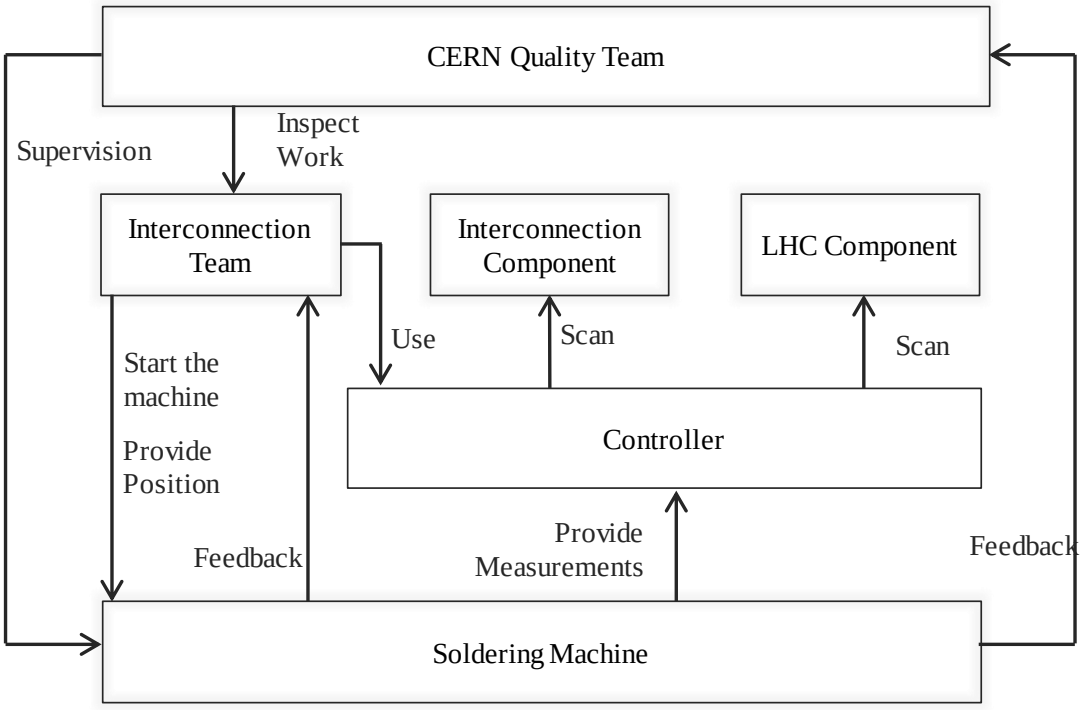


Figure 3-8: Recommended, new interconnection process

The complexity of the LHC is immense, but will rise even further when further upgrades of the machine take place – which is why standardization and hazard analyses become more and more important. Future projects, like the FCC or the High Luminosity LHC, need even more analysis for safer systems with more reliable components.

4 Analysis of the LHC Inner Triplet Protection System

The High Luminosity Upgrade of the LHC will provide ten times more collisions at the high luminosity experiments ATLAS and CMS. As the radiation next to these experiments is very high, the inner triplets reached their radiation lifetime and must be exchanged. The new inner triplet magnets are the backbone of the upgrade and will be installed during LS3[1]. The novel Nb_3Sn magnet technology promises the field gradient of 143.2 T/m when cooled to 1.9 K and powered with 17.9 kA and therefore more collision data for the experiments. This corresponds to the so-called ultimate current, which is 108 % of the nominal circuit current, 16.5 kA. [70]

The debris from the experiments and the high current in the magnets leads to a necessity of highly reliable protection mechanisms against magnet quenches. The mechanisms consist of complex systems; the high amount of boards and components make an exhaustive quantitative analysis at the present design stage not feasible. Therefore, the focus of this dependability analysis will be to investigate the mere qualitative aspect of finding flaws in the system layout and the system interaction using the STPA technique which is explained in Chapter 2.4.2. The outcome will be a set of requirements, that will be reported to the other working-groups of the LHC Machine Protection Panel. Chapter 5 provides an evaluation of the method and compares it to an FMEA.

4.1 Fundamentals of the Analysis

The system boundaries are derived in a top-down approach, beginning with the definition of the considered accidents. The hazards derive from those accidents and the system boundaries are set to control these hazards. This chapter shows the process of finding the system boundaries.

4.1.1 Definition of Accidents and Hazards

Generating data at the experiments ATLAS and CMS, which are enclosed by the inner triplet magnets, is the aim of LHC runs, damaging the experiments must be considered an accident. The efficiency of the LHC would be severely mitigated if an inner triplet magnet takes damage. If LHC equipment in the tunnel and in the new UR Galleries takes damage, the LHC is down for months. The availability of the LHC is crucial, as is directly corresponds to the discovery potential of the machine. Loss or injury of human life is the most significant accident, yet the

[1] LS3 is the Long Stop 3 that will start in 2023 and will last roughly 30 months [71]

scope of the present thesis was defined on operational dependability of the system. The identified accidents and the derived hazards are shown in Table 8.

The system hazards are derived from the accidents. The most concise, yet complete list of hazards was defined as: The electrical energy, the Helium, the beam energy, the vacuum, the radiation and the high system complexity. Table 8 shows the derived hazards and how the accidents and hazards are linked.

The electrical energy can lead to experiment, inner triplet or equipment damage. When the magnetic field is incorrect it leads to a hazardous beam excursion. When the inner triplet is quenching, it is suddenly exposed to the electrical energy of the circuit, leading to an increased temperature of the magnets. As equipment is accessible, the electrical energy of the equipment can also harm personnel.

The helium, stored in the cryostat and cryo lines can lead to an oxygen deficiency hazard in the tunnel or to damage of the LHC and its equipment. Increased helium pressure in the cryostat could damage the inner triplet. If the helium stops, it can also lead to the first hazard where magnets are quenching.

The vacuum in the beam pipes can damage the surrounding systems by leading to hazardous beam losses, or by incorrectly provided the insulation vacuum of the cryostat leading to a quench.

Table 8: Accidents and corresponding hazards

ID	**Accidents**	**ID**	**Hazards**	**Link**
[A-1]	Damage to the experiments (ATLAS, CMS)	[H-1]	The electrical circuit energy	[A-1] [A-2] [A-3]
[A-2]	Damage to the inner triplet magnets	[H-2]	The Helium, stored in the Cryostat and Cryo lines	[A-2] [A-3]
[A-3]	Damage to other mandatory operational system.	[H-3]	The beam energy	[A-1] [A-2] [A-3]
[A-4]	Availability Targets not reached	[H-4]	The vacuum	[A-1] [A-2] [A-4]
		[H-5]	The radiation in the tunnel	-
		[H-6]	The high system complexity	[A-4]

The energy of the circulating beam is – especially when focused – able to damage magnets, experiments and equipment. When the beam hits a coil, it can cause physical damage or cause heat loads that lead to a quench.

The radiation in the tunnel is hazardous to CERN Personnel and a causal factor for component degradation. The system complexity means incorrect personnel decision, that lead to missing availability targets or accidents.

4.1.2 System Control Structure

The control structure is derived from the system hazards as described in Chapter 2.4.2. The system control structure is displayed in Figure 4-1. This section provides an overview on the system interaction and the control actions of the system.

The inner triplet magnets provide the magnetic focusing field for the LHC beam. The Vacuum System controls vacuum related hazards and provides the beam vacuum for the LHC Beam.

The CERN Personnel is modeled as system experts, technicians and CCC operators. The LHC must not rely on human reaction during operation as accidents can happen much faster than the average human reaction time. The operators still have the responsibility to start the system, to monitor the operation and can request a beam dump or an abort of the powering if necessary. The system experts provide and change the Detection Parameters of the Quench Detection System and monitor individual systems – e.g. the QPS sends a mail to the QPS Expert in case redundancy is lost. The technicians do the physical works, e.g. settings up the protection units in the UR Galleries. [71]

The Beam Interlock System (BIS) controls the beam related hazards. It provides its status to the CERN personnel. It also triggers the beam extraction if necessary via the LBDS. The BIS decides to trigger the beam extraction based on the inputs provided by the BIS users. The Powering Interlock System provides the PIC beam permit. Systems, that are not explicitly mentioned here provide the beam measurements. The BIS is powered by the UPS.

The circuit energy hazards are controlled by the PIC and the QPS, which is why they are summarized as Circuit Energy Controllers. They provide their system status to the CERN Personnel and powered by the UPS. The PIC and the QPS communicate with the each other and the Power converters by current loops, that are explained in Chapter 2.3.2. These loops are modelled as the control actions: Permit Powering and Request Fast Power Abort. The PIC is modelled as the controller, that controls the power and the inner triplet is the powered process. The QPS fires the protection units CLIQ and Quench Heaters to protect the magnet and receives measurements from the voltage taps and the current change sensors.

The helium related hazards are controlled by the Cryogenic System. It provides the helium for the cryostats and sends a start interlock signal called Cryo_Start and a maintain interlock called Cryo_Maintain to the PIC. The Cryogenic controls are connected to a UPS. The detailed interaction between the PIC, QPS, PC, UPS and Cryo is provided in Chapter 2.3.2f.

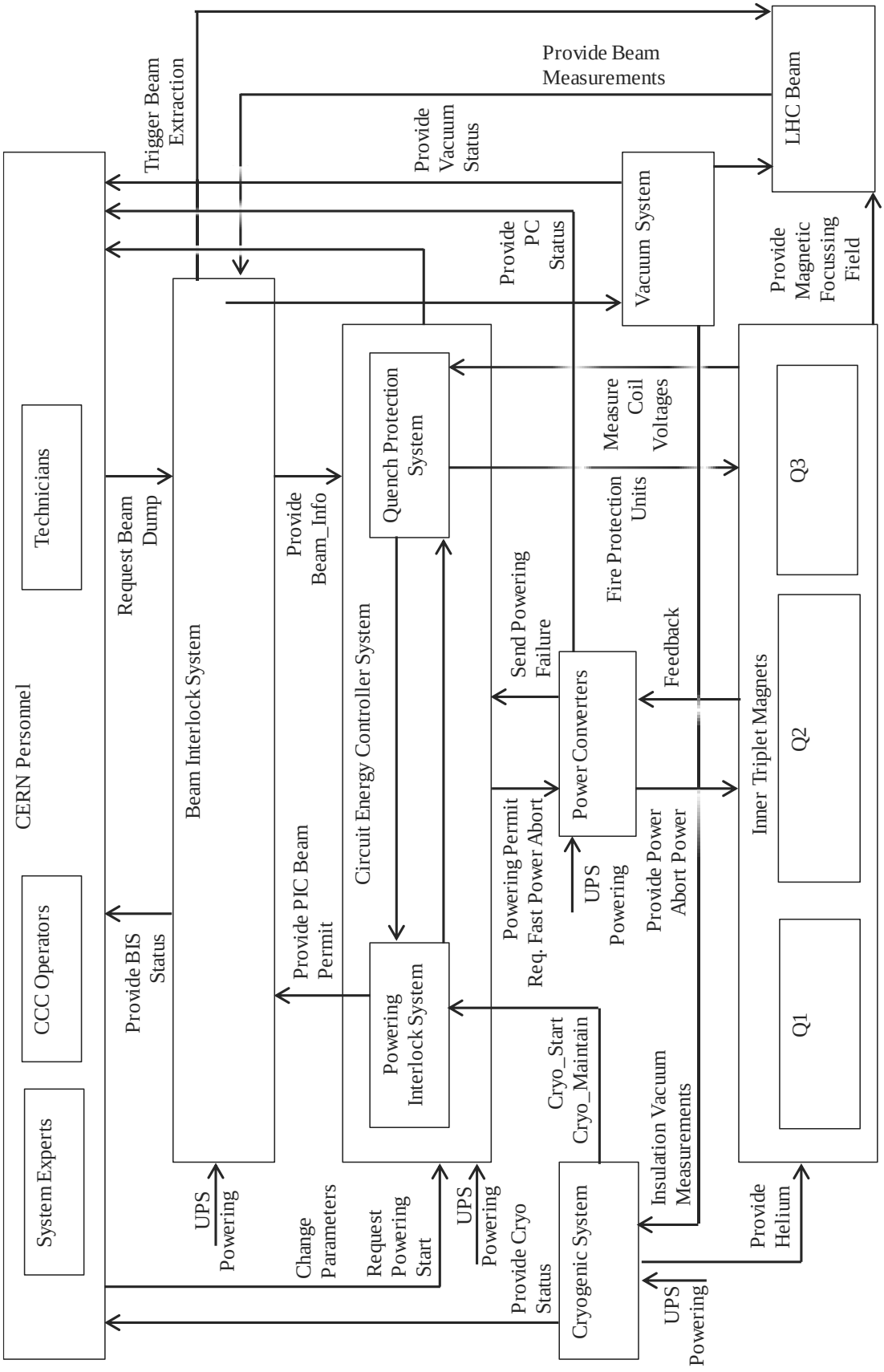


Figure 4-1: Control structure of the inner triplet and the surrounding systems

4.2 Derived Unsafe Control Actions

The control actions are shown in Figure 4-1. Many of them are already realized in the present system layout, the addition of CLIQ and the other HL LHC upgrades change the system. It must be ensured, that this control actions are also safe for the HL LHC. Chapter 2.4 describes multiple ways how to investigate control actions. How the control actions can turn unsafe is described in the following sections; the number of control actions does not allow a complete discussion in the text, which is why the most important topics are presented here and a full list of UCAs is provided in Appendix E. This chapter discusses the control actions related to starting and aborting the powering, firing and not firing of the protection units, dumping or not dumping the beam and changing the protection parameters.

Each subsection in this chapter is dedicated to a control action, that can be found in the control structure in Figure 4-1. Each section explains the nominal operation of a control action and shows a refined control structure. Then the corresponding unsafe control actions are presented as subsections that contain a discussion on the scenarios and causal factors. Requirements are then formulated to prevent the causal factor from happening or to mitigate the effect of the unsafe control action.

4.2.1 Control Action: Fire Protection Units

When detecting a quench in one of the inner triplet magnet coils, the QDS must trigger and fire both CLIQ and Quench Heaters of all inner triplet magnets. The quench heaters are fired by providing current for a relay that then closes the current circuit between the Quench Heater capacitors and the heater strips.

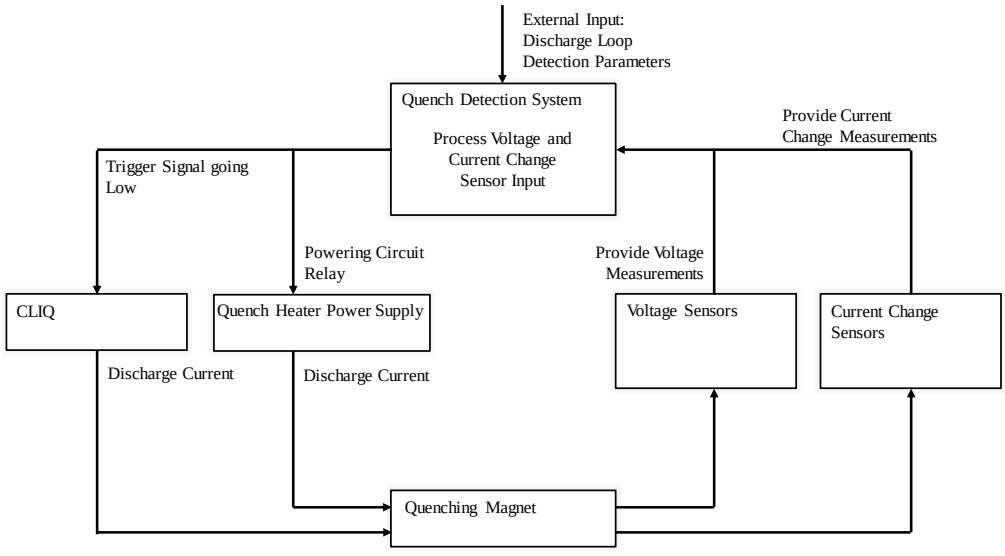


Figure 4-2: Refined Control Structure of firing CLIQ and the Quench Heaters

The CLIQ Units are connected with a cable to the QDS. During nominal operation, the current in this circuit is at least 20 mA. If the current goes lower, the CLIQ Units generate a trigger signal and trigger two two-ways thyristors. Figure 4-3 shows the refined control structure of

this control action. During the discharge of the protection units, the magnet hot-spot temperature must be lower than 350 K and the voltage to ground must be below 1000 V.

The control action of firing the protection units is heavily relying on the context in which it is provided. It was therefore decided to follow *Thomas* approach (See: Chapter 2.4.2) and create context tables to discuss the hazardousness of the control action in different contexts.

Table 9: Context Variables and values for “Discharge Protection Units”

Variables	**Values**	**Notes**
Magnet Status	No Quench Quench	A quench describes the loss of superconductivity.
Protection Status	Charged Not charged	Armed protection mechanisms can fire, unarmed cannot.
Beam Potential	Damage Potential No damage Potential	The nominal beam energy is beyond damage potential. Before injecting a beam that is potentially damaging, a so-called pilot beam is injected. This beam consists of one bunch that has no damaging potential.
Circuit Powering	High Low PC Failing	The current of the magnets directly correlates to the provided field. High Powering means the modes: Squeeze or Flat-top. Low includes injection-level powering and ramping.
Cryo Status	Cryo OK Cryo Failing	The Cryo status includes things like: Working pumps, correct helium temperature, lines not rupture, etc.
Vacuum Status	Vacuum OK Vacuum failing	An incorrect vacuum could lead to a beam induced quench.

The values given in the second column are recombined and the hazardousness of providing or not providing the control action in the given context is assessed. The following unsafe control actions are the result of the combination. Appendix E shows the context table for firing/not firing the protection units.

Quench Heaters or CLIQ Units not firing during a magnet quench

As described in Chapter 2, a quench leads to hazardous temperatures in the magnet hot-spot and must therefore be detected by the Quench Detection System. It must then trigger all Quench Heaters and CLIQ Units of the inner triplet. The full table of scenarios, causal factors and requirements can be found in Appendix E.

The refined control loop with possible failure scenarios of not firing the CLIQ and QH Units is displayed in Figure 4-3. The QDS is provided with measurements of the voltage sensors and current change sensors and decides, based on this input to fire the quench heaters and CLIQ.

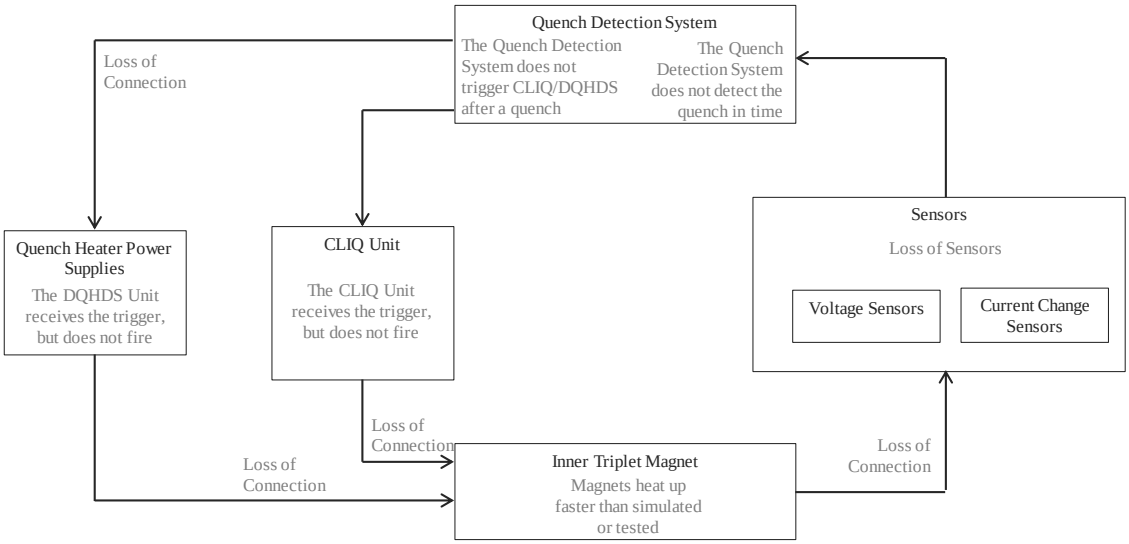


Figure 4-3: Control Loop between the QDS and CLIQ and Quench Heater Units with possible scenarios for not firing

Table 10 shows scenarios and causal factors for not firing the Quench Heaters and CLIQ Units. The parameters in the QDS must be set by system experts. These experts can implement incorrect thresholds or verification times, theoretically even during operation. These incorrect parameters might lead to a delayed detection of the quench or a delayed triggering of the CLIQ and DQHDS Units. To prevent obsolete or incorrect parameters, the system experts must define a safe range. The safe range defines a leeway that cannot be exceeded by the parameters. If an expert tries to implement parameters outside of the defined leeway, the GUI will return an error. To prevent a workaround or a failure of this safety mechanism, an automated check must be implemented; the QPS Supervision will therefore read the parameters in short interval and compares them to a set of defined master-parameters. For further analysis, see Chapter 4.2.4.

The Quench Heater Units are triggered by powering a relay that closes the electrical circuit between the heater strips and the power supplies. If this relay is stuck, the current cannot discharge, and the heaters are not fired – the communication is lost. To prevent damaging temperatures in the coil hot-spot, the heaters must provide redundancy, so that one heater circuit not firing does still lead to a temperature lower than the defined critical value of 350 K. To spot faulty DQHDS Circuits, the discharge data must be checked after every trigger. A regular check must be discussed, firing the quench heaters on purpose to check the correct operation of the Quench Heater Units.

Table 10: Some scenarios and causal factors for not firing the QH/CLIQ Units

Scenarios	**Causal Factor**	**Requirements**
The Quench Detection System does not detect the Quench	Obsolete or incorrect voltage threshold or verification time parameters implemented to the QDS.	The maximum safe range of detection parameters must be defined and implemented to the QDS, so that unsafe parameters cannot be implemented. Introduce Operational Checks: QPS Supervision must read the QDS all n minutes to verify correct operation.
The QDS is detecting the quench, but does not trigger QH or CLIQ Units	The relay that is triggering DQHDS Units is stuck and does not provide the needed signals	One lost DQHDS Circuit must still lead to HS-Temperatures below 350 K. Regular checks must verify the functionality of the relays
The DQHDS/ CLIQ Units receive the trigger, but do not fire	CERN Personnel damaging DQHDS/CLIQ Units	The CLIQ/DQHDS Units must be protected against unwanted interaction from CERN Personnel. The charge of the DQHDS/CLIQ Units must be measured and failures must cause a beam dump and a power abort.
	CERN Personnel maintains the DQHDS/CLIQ Units causing a discharge	A policy must be defined: No maintenance of the CLIQ/DQHDS Units during operation
	The CLIQ/DQHDS Units lose connection to the magnets due to degradation/CERN Personnel	A maintenance strategy, triggered by schedule or actions must be defined to check the lead between CLIQ/DQHDS and the magnets
	DQHDS/CLIQ Units lose connection to the powering	The loss of a single UPS must not lead to an unprotected magnet. Suitable Distributions of CLIQ Units to the UPSs F3 and F4 must be found or the CLIQ Units must be powered be redundant UPSs. A failure of the UPS Powering must be spotted and cause a power abort.
The QDS does not receive the needed signals to detect the quench	Loss of voltage taps	A loss of voltage taps must cause a beam dump and a power abort. The voltage taps must be redundant to ensure a supervised shutdown

Moving further in the control loop, the next scenario is that the QDS is correctly triggering the CLIQ and Quench Heater Units and the CLIQ or Quench Heater Units do not fire. The CLIQ or Quench Heater Units might be damaged accidentally from CERN Personnel. To prevent CERN Personnel acting on CLIQ Units, the Units must be protected against the unwanted interaction, e.g. by fencing them off. The technicians must be trained on not touching the surrounding units during operation. Also, a procedure must be defined, what the technician must do if he accidentally damages a connection. A maintenance of CLIQ/DQHDS Units during operation by CERN Personnel must be forbidden.

The CLIQ Units are connected to the magnets directly via cables, that can be damaged. The connection between the CLIQ Units and the magnets must be protected from unwanted interaction with CERN Personnel. Further, a regular maintenance/inspection strategy must be defined to ensure a correct connection.

Radiation or coil movement during cooldown can damage the connection of DQHDS Units to the heater strips. The previously stated requirements on the Quench Heater redundancy and the discharge monitoring together with the regular inspections are also needed to protect against this causal factor.

The CLIQ Units are charged by the mains and need power to generate the trigger signal for the thyristors. To prevent all CLIQ Units failing due to a power malfunctioning, the CLIQ Units must be powered by the UPS. To prevent a failing UPS, the status of the UPS must be surveilled and cause a power abort, if failures are spotted. To prevent a blind shutdown in case the UPS is not responding when requested or experiences a failure itself, the CLIQ Units and DQHDS Units must be powered by redundant UPS or the powering of the units must be split on two different UPS.

The QDS relies on the input gets from multiple sensors, such as the voltage measurements. In case a voltage tap is lost, the operation must be aborted. A redundant voltage tap must provide the needed redundancy to ensure a supervised power abort. Faulty sensors must be detected by the QPS (e.g. by detecting a stuck value). A dedicated analysis must assess the optimal logic between the sensor signals.

Quench Heaters or CLIQ Units not firing after a Cryogenic failure that leads to a quench

If the cryogenic system fails, the temperature is rising in the cryostat and leads ultimately to a quench if there is current in the circuit. To not end up in a quench, the Cryogenic System must withdraw the Cryo Maintain Signal at the Powering Interlock Controller in case of a failure and lead to a slow power abort. If this fails, the subsequent quench must be detected by the QDS, discharging the magnet energy. The cryostat itself must be protected from overpressure by two redundant valves in different locations, that are monitored, when triggered.

Quench Heaters or CLIQ Units not firing after a Power Converter Failure

The Power Converters are connected to the Powering interlock with multiple current loops: The Powering Permit loop, the Powering Failure Loop and the Discharge Request Loop. If the

power converters fail, the nominal way is to open the powering failure loop, leading to a power abort. Some failures of the power converters need a firing of the protection units, e.g. when the water cooling is failing. This UCA describes a failure in the PCs that would need a firing of the protection units.

Table 11: Scenarios and causal factors for not firing the CLIQ and Quench Heaters after a PC failure

Scenarios	**Causal Factor**	**Requirements**
The Power Converters detect the failure, but do not open the discharge loop	Stuck discharge loop interface	The operation of the discharge loop interface of the power converters must be verified during HWC. A regular maintenance and inspection strategy must be defined to find faulty interfaces.
The power converters interrupt the loop interface, but the QPS does not receive the signal	Short circuit in the discharge loop	The discharge loop must be tested on short circuits during HWC. After every intervention, inspection and maintenance, the loop must be tested again on short-circuits.
The loop is interrupted, but the QPS does not fire the protection units	Failure in the QPS	See: Quench Heaters not firing

To prevent the discharge loop interface from being stuck, regular checks, including HWC, must be defined. Short-circuits in the discharge loop are potentially hazardous and must be protected against. The operation of the discharge loop must be verified regularly, especially after every intervention, inspection and maintenance.

Quench Heaters or CLIQ Units firing incorrectly in amplitude

An incorrect firing of Quench Heaters or CLIQ Units must be prevented to protect the magnets from overheating hot-spots or high voltages to ground. The arrangement of the heaters is also defined to minimize the effect of the beam in case of a spurious firing.

The CLIQ Unit's voltage depends on the magnet of the inner triplet. To adjust the voltage, a CLIQ Unit is built with a voltage selector – currently consisting of 10 voltage stages. The technician installing the CLIQ Unit must set the voltage. To prevent the CLIQ Unit being set to the incorrect voltage (both too high and too low), the voltage selector should be removed. Different voltage settings in the charger must replace the physical selector.

The CLIQ Unit's effectiveness also depends on the connection to the magnet. Heating losses are especially created, where opposing CLIQ induced currents are physically near [11]. In case the CLIQ Unit is connected to the wrong coil ends, it becomes less effective, the voltage to

ground might increase and the effect of a spurious discharge might have a higher impact on the beam. To prevent these failures, the Hardware Commission must check the correct discharge of the CLIQ Unit to the magnets.

Further, an incorrect polarity of the CLIQ Unit can limit the effectiveness. The Hardware Commission must also test the correct polarity of the CLIQ Unit. When the CLIQ Unit is maintained or repaired, these actions must be repeated.

A spurious firing of the heaters together with an incorrect arrangement is a failure mode with the potential to permanently damage the magnet. The connection of the heater strips to the power supplies must be made with high precision and caution. The technicians must be trained on this severe failure mode to minimize the probability of occurring. The correct arrangement must be checked after installation by the Hardware Commission. The actions must be repeated after interventions, maintenance and repair. A maintenance and inspection strategy must be defined.

Quench Heaters or CLIQ Units firing spuriously

In 2016, periodic beam losses were observed right before a quench. A spurious firing of the quench heater units was determined to be the reason for the losses. Even though the quench heaters are not directly connected to the superconducting magnet circuit, the discharge current of the quench heaters builds up a magnetic field, interfering with the beam trajectory [52]. The CLIQ discharge causes also a quench of a fraction of the magnet – an accidental CLIQ discharge must cause a retrigger of the other protection units in under 1 ms to protect the magnet from overheating. 40 LHC turns, corresponding to 3.56 ms were defined as preliminary timespan to dump the beam after a spurious firing of one CLIQ Unit.

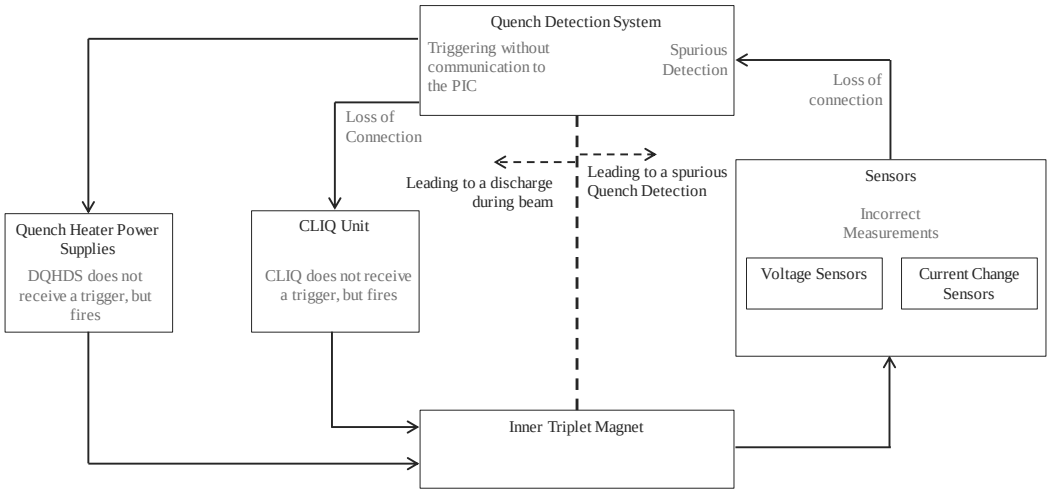


Figure 4-4: Control Loop between the QDS and CLIQ and Quench Heater Units with possible scenarios for firing spuriously

The scenarios in Figure 4-4 have been identified: In principal, two different kinds of spurious firings are possible: Endangering the availability goals due to false triggers with correct protection, or incorrect and false firings endangering the magnets and the beam.

The first scenario is the QDS detecting the quench, but not communicating it to the PIC. Causal factors for this scenario are analyzed in chapter 4.2.3.

The CLIQ Units receive at least 20 mA current when no action is needed. When the current drops, the CLIQ Units are triggered. A loss of connection can therefore cause a spurious trigger. The CLIQ Units are continuously accessible; the connection must be protected from unwanted interaction with CERN Personnel.

A component failure in the CLIQ Unit, e.g. the forward blocking thyristor falling in short-circuit (see: Figure 2-13 and Appendix D), causes an accidental discharge. The protection against this is detecting the subsequent quench: The Quench Detection system needs time to detect (5 ms) and to verify (5 ms) the quench. Then it opens the Quench Loop and therefore triggers the PIC, that needs roughly some hundred µs to process the signal, interrupt the beam permit loop and dump the beam. The quench detection alone needs over 10 ms to detect the quench, making the spurious detection via the quench detection system not suitable. As component failures cannot be excluded, an interlock is needed that reads the CLIQ Units discharge sensor and triggers a re-triggering of the other protection units. Further, the CLIQ Unit interlock must cause a power abort and a beam dump. Different options for realizing the interlock have been discussed with experts:

- Connecting the CLIQ Unit Interlock to the Powering Interlock Controller
- Connecting the CLIQ Unit Interlock to the Beam Interlock System
- Detecting the current change in the magnet circuit

The CLIQ is directly connected to the powering circuit, therefore connecting the interlock to the PIC is the most preferred option. This must be studied, and the interlock must be defined.

A spurious Quench Heater firing is also hazardous, especially as the Heaters fire within half a turn. Studies show the hazardous effect of the DQHDS Unit discharge to the beam [52]. Component failures, such as a relay falling in short circuit or closing spuriously can cause an accidental discharge. To protect from such an event, the DQHDS Units must be re-arranged to provide a focusing field instead of kicking the beam. Alternatively, a DQHDS Interlock can be defined to retrigger the other DQHDS Units and dump the beam. If the heaters are properly arranged and all units fire simultaneously, the effects cancel out and the beam distortion gets smaller.

The thresholds and verification timings must be changeable remotely to adapt to occurring false triggers. This leads again to hazards that are analyzed in 4.2.4. A loss of voltage taps is detected by the QPS and causes a power abort. To prevent false triggers due to incorrect measurements, filters and logics for the QDS must be defined.

Appendix E shows a more detailed table with scenarios and causal factors for firing the quench heaters spuriously.

Table 12: Scenarios and causal factors for firing spuriously

Scenarios	**Causal Factor**	**Requirements**
The QDS does not detect a quench, but the CLIQ Units receives a trigger	CERN Personnel (or others) act on the connection during operation	The connection between CLIQ and QDS must be protected from accidental contact with CERN Personnel. E.g. By fencing off the CLIQ Units.
A CLIQ Unit receives no trigger, but discharges	A component in the CLIQ Unit fails and causes a discharge of the CLIQ to the magnet	A Protection Unit Interlock must be designed. The protection unit interlock must detect an unwanted current discharge through a Thyristor in a CLIQ Unit. The Post-Mortem Data must show the cause of the spurious discharge to fasten repairment.
A DQHDS Unit receives no trigger, but discharges	The connecting relay between the capacitor and the discharge strips is falling short	The heater strip connection scheme must be changed to produce a quadrupole field when discharged to mitigate the effects of a spurious triggering. Alternative: Interlock Quench Heaters to prevent worst-case scenario of one DQHDS circuit firing.
	CERN Personnel damages the DQHDS Unit that leads to a discharge (...accidentally)	The DQHDS Units must be protected from unwanted interaction with CERN Personnel; e.g. by fencing off the units
The QDS detects a false quench	Material properties	The detection parameters must be changeable to deal with the Nb3Sn Flux Jumps Filters must be defined to delete the flux jump measurements
	Incorrect measurements from the sensors	Faulty sensors must be spotted and repaired A dedicated analysis can define the suitable distribution and logic between the sensor measurements

Quench Heaters or CLIQ Units not firing after a simultaneous failure in the interrupted powered systems that leads to a quench

Multiple systems are powered by the mains, such as the Cryogenic System, the Vacuum System or the Magnet Circuits. During a power cut, a nominal operation of these systems cannot be expected – a quench might be the result. To protect all circuits during the ramp down of the power after a power cut, the uninterrupted power supplies (UPS) were defined. These provide 10 minutes of backup power to discharge the energy of the circuit safe. However, also UPS failed before. To actively monitor the ramp down, the QDS must be powered redundantly by two redundant UPS. The UPS status must be surveilled continuously, and a failure of one UPS must lead to an abort of the powering. If the second UPS fails, the protection is not armed.

The CLIQ Units are retriggering while the beam is present

To protect from the effect of a spurious firing of single CLIQ Units, an interlock must be defined that retriggers all other CLIQ Units of one triplet. The system interacts like displayed in Figure 4-5. The Interlock must detect a discharging CLIQ Unit and trigger the Powering or Beam Interlock Controller to dump the beam (depending on the chosen solution). The CLIQ Interlock must then trigger all CLIQ Units.

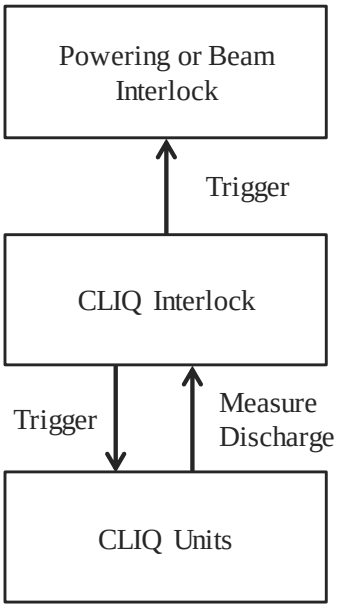


Figure 4-5: Control Loop between the CLIQ Interlock and the CLIQ Units

The interlock may be not able to trigger the Powering or Beam Interlock controller, because the loop interface is stuck. As this is a highly hazardous unsafe control action, the Interlock must provide redundancy towards the beam dump request.

Further, the cabling between the Interlock and the Powering or Beam Interlock Controller may be incorrect – a short circuit could prevent communication. The Hardware Commissioning Group must verify the correct operation of the Interlock, also regarding the timing. Further, a

maintenance and inspection strategy must be defined to eliminate possible short-circuits in the communication.

The CLIQ Interlock itself could – due to a failing component – cause a simultaneous discharge of all Units. The CLIQ Units must be arranged to mitigate the effect on the beam if all are triggered together. If the baseline layout changes, the effect on the beam of a common firing must be evaluated again. The CLIQ Interlock must be able to trigger a beam dump, even though it just fired all units.

The CLIQ Unit Interlock is not retriggering, or retriggering too late

The CLIQ Interlock operation must be verified during Hardware Commissioning by e.g. firing low-charged units and the implemented sensors must be used to monitor the retriggering of the interlocked units. As the actual retriggering due to a discharging CLIQ Unit is such a rare event, the normal triggers can be used to verify the interlock operation. When the protection units are fired after a quench, it must be checked, if the interlock has also detected the discharge. This way, faulty discharge sensors must be detected.

4.2.2 Control Action: Powering Permit/Fast Power Abort

The control action *Start Powering* and *Abort Powering* is given by the PIC and upon request of the CCC Operator and received by the inner triplet Power Converters. Figure 4-6 shows the interaction between the PIC, PC and magnets. After creating context tables, the UCAs in the upcoming sections have been identified.

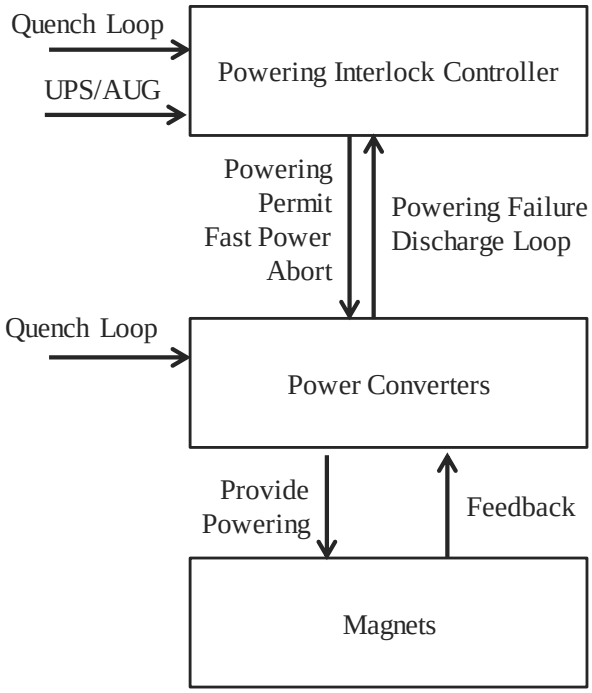


Figure 4-6: Control Structure of powering the magnets

The powering of the LHC is provided spuriously

The PIC allows the start of the powering by closing the Powering Permit current loop. To prevent a spurious powering start, the LHC Operators must also give their individual request to power via software and the powering must not automatically start on a closing circuit. According to experts, the probability of a spurious powering is neglectable.

The powering is not aborted after a quench

The powering of the circuit must be aborted to protect the magnets and the power converters. The powering not shutting off is mentioned as a hazard in CERN reports, such as [40]. For the HL LHC during high powering levels (flat-top or squeeze), the subsequent CLIQ Units firing are sufficient to build up a voltage, that the power converters cannot follow anymore and shut off. The Power Converters do not depend on a signal from the PIC or the QPS for this. According to experts, the additional energy in the circuit and the time delay of the PCs is neglectable.

It must be investigated, if the CLIQ Unit firing during low and medium level powering levels is still sufficient to safely shut down the power converters.

The powering is not aborted after a spurious discharge of a CLIQ Unit

According to magnet experts, the subsequent voltage of the CLIQ Unit discharging is still sufficient to trip off the power converters. (See: The powering is not aborted after a quench) However, an investigation must show, that this is also the case during low-level powering levels.

The Power Converters are not decoupled or decoupled too late from the CLIQ current

The 18 kA Power Converter of the circuit can only provide current in one direction. If there is an opposing current, the PC takes damage. To protect the 18 kA from a spurious CLIQ firing during low current, a backwards diode must be implemented, that bypasses the Power Converters.

The Powering cannot be started or maintained due to the QPS, endangering availability goals

To increase availability for the HL LHC, this UCA investigates, how the QPS could endanger the availability goals. Together with experts, the following requirements have been defined:

To enhance reparations, spare boards and board components must be built. In order to repair units faster and more reliable, an automatic parameter configuration of the Quench Detection Boards must be defined. This can improve the maintainability of the system.

If the QPS does spuriously not provide the QPS_OK Signal (e.g. due to loose contacts), the signal must be maskable. This improves the availability of the system, but reduces the safety

4.2.3 Control Action: PIC Beam Permit

The Powering Interlock Controller allows the operation if the powering is in a safe state. The Beam Interlock System has been designed for maximum reliability and operational safety (For a description of the BIS, see Chapter 2).

Figure 4-7 shows the nominal communication between the interlocks. When a quench is detected, the Quench Detection System interrupts the Quench Loop, The PIC reads the quench loop and the signal is processed by the PIC internal logic. The PIC then interrupts a current loop that connects the PIC of the inner triplet to the PIC of the arcs. Each PIC (left arc and right arc) reads the interrupted current loop and triggers a beam dump request via two redundant channels.

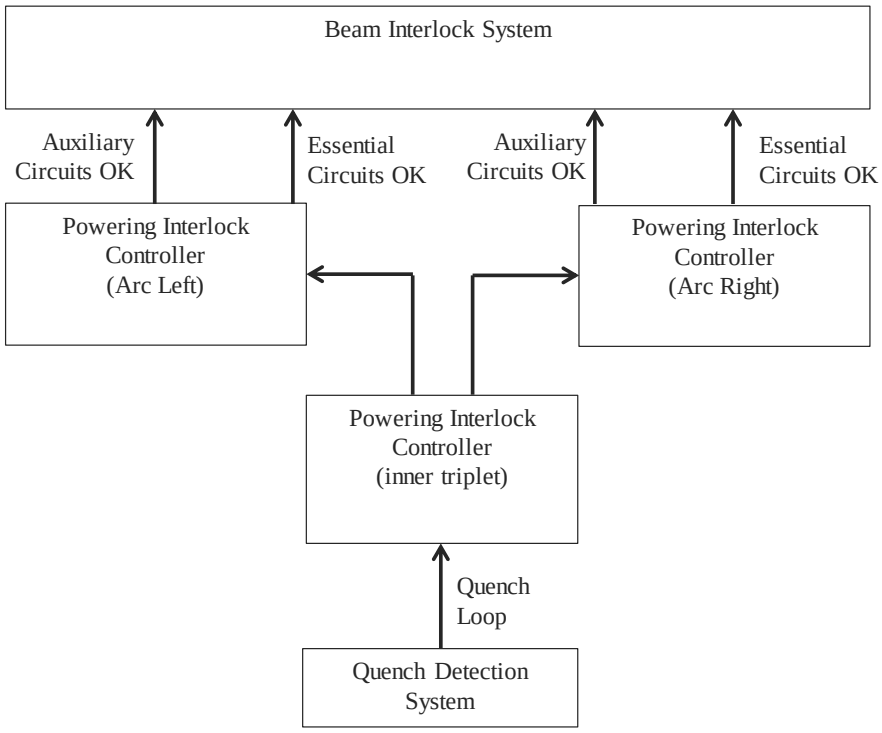


Figure 4-7: Refined Control Structure of the Powering Interlock triggering the Beam Interlock after a quench

An analysis of the Beam Interlock System is not part of the present analysis. Yet, how the beam dump request may not arrive at the BIS, is part of this thesis. The UCAs in the upcoming sections have been identified.

Powering Interlock Controller does not (in time) request the Beam Dump at the BIS

The Powering Interlock Controller surveils the status of the Quench Loop. If the quench loop has a short-circuit, the interruption of the quench loop cannot be noticed by the interlock controller. If the interlock controller cannot notice the quench, the beam is not dumped. A full discharge of the protection units while the beam is present is the consequence of this failure. To prevent this, the hardware commissioning team must assess the correct operation of the

interlock chain and a maintenance and inspection strategy must be defined to check the interlock loop. This strategy must consider actions after interventions and regular checks.

In case the signal arrives at the interlock controller, a failure in the controller can lead to the signal not being processed. The Quench Loop is connected to the essential circuits loop of the interlock controller. If this loop fails, the auxiliary loop is redundantly processing the signal with roughly 1 ms delay. When defining the CLIQ or Quench Heaters Interlock, this delay must be considered. The Post-Mortem Analysis must reveal the correct operation of the interlock controller after a request.

During nominal operation, the PIC of the inner triplet interrupts the essential circuits OK loop and communicates the failure to the PICs of the neighboring arcs that then interrupt the Beam Interlock Loop. To prevent short-circuits in these loops, a maintenance and inspection strategy must be defined.

The PIC Beam Permit is withdrawn when not needed

On contrary to the previous UCA, the powering interlock controller might also withdraw the beam permit, when not needed, i.e. when the operation is safe.

Table 13: Consequences of loss of protection redundancy

Redundancy Loss	**Safe Current**	**Notes**
No Failures	Ultimate	-
One DQHDS Unit Fails	Ultimate	Replace DQHDS Unit with next Access
Two DQHDS Unit Fail or One DQHDS Circuit is permanently damaged + One DQHDS fails	Ultimate	Launch Analysis and Repair circuit with next tunnel access
One CLIQ Unit loses redundancy	Ultimate	CLIQ Unit is still expected to work due to the internal redundancy
One CLIQ Unit + One/More DQHDS Unit fail	Nominal	Replace CLIQ Unit/DQHDS Unit with next possibility
All Quench Heater Supplies of one Magnet are lost	-	The CLIQ Technology cannot quench the magnet alone at low current.

To prevent an incorrect setup or wiring of the loops to cause a false operation abort, the HWC must test the full PIC interlock chain and verify its operation. The operators can also request a false abort, especially during a nightshift, when experts are not around to provide help. To prevent this, a dedicated campaign must assess new features of the HL LHC and train operators on them. This must be done for all systems.

A loss of single DQHDS or CLIQ Units must not automatically cause a power abort. When a single DQHDS Units is lost, a quench is still sufficiently protected. Therefore, a dedicated campaign must assess the acceptable losses of protection redundancy. Together with experts, the statements in Table 13 have been made: The table shows the acceptable safe magnet circuit current for the redundancy losses provided on the left column. A loss of single Heater Circuits does not lead to a hazardous hot-spot temperature in case of a quench. However, the losses of redundancy have implications on other systems: If single Heater Circuits are lost, this can enhance the effect of a full firing of quench heaters on the beam. This must be investigated, once the baseline is decided. The acceptable losses of redundancy must also consider the powering redundancy of the protection. One UPS that is not responding after a request must be considered, i.e. if multiple units from a single UPS are lost, and the other UPS does not provide power after a request, the magnet must not be unprotected. The heater circuits and the CLIQ Unit layout have been defined to also minimize the voltage to ground. A loss of redundancy must not lead to a hazardous voltage to ground during operation.

4.2.4 Control Action: Change Detection Parameters

As flux-jumps of the Nb_3Sn Technology interfere with detection thresholds and tests or simulations may not always be perfectly accurate, the detection parameters are changeable remotely. The system expert can access the parameters via a GUI and change the parameters. Therefore, it might happen, that the parameter change is leading to a hazard. The following unsafe control actions have been identified and are discussed in the upcoming sections.

The detection parameters are not changed when needed.

The detection parameters might not be changed, even though it is hazardous because the experts see no necessity to change them. To prevent this, the hardware commission group must provoke quenches and verify the operation of the foreseen parameters. The system experts must surveil the performance of the quench detection system during the Hardware Commission and during the first weeks of operation. Non-conformities and parameter changes must be discussed.

The detection parameters are changed, but lead to a hazard.

Many ways are possible how the system expert might implement the parameters incorrectly and how they might lead to a hazard. Untrained Personal can use the GUI incorrectly and put in incorrect parameters. To ensure that untrained personnel cannot change the implemented parameters, the Role-based Access Control (RBAC) was defined. The RBAC is an “approach to restrict system access to authorized users” [72, p. 1]. With this tool, whoever wants to change parameters must authenticate himself with his CERN account. Access to the parameter changes must be restricted to system experts.

As also system experts are not immune to failures, a safe-parameter space must be defined in which the parameters can be changed. If one tries to implement incorrect parameters, a failure message must occur, and the parameters must not be changed. For the High-Luminosity LHC a Parameter Checking System, that reads the parameters in a defined time span, must be defined.

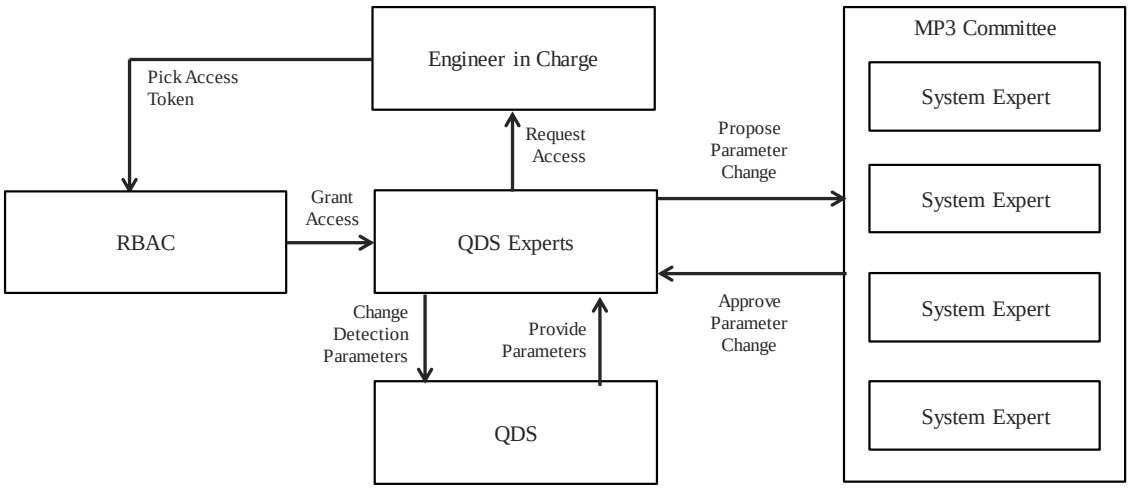


Figure 4-8: Refined Control Structure: Change Detection Parameter

Detection thresholds are a trade-off between safety and availability. To prevent system experts from using the changeable parameters to improve the availability of their subsystem, while limiting the machine's dependability, the parameters must be approved by the Magnet circuits, Powering and Performance Panel (MP3 Committee). Multiple experts join this meeting and must provide their view on the parameter change. The parameter changes must be approved by the MP3 Committee.

The detection parameters are changed during operation and lead to a QDS shutdown

This unsafe control action is mitigated by the RBAC and the implemented procedure. The system expert, that wants to implement new parameters must call in the control room and explain which parameters he wants to change and why. The Engineer in Charge (EiC) must define if the access will be granted to the system expert. For example, the EiC will not grant access to change quench detection parameters during operation, as this could lead to a restart of the detection parameter changes. The changes are logged to a system, so that changes can be traced, in case someone wanted to harm the machine. It must also be the responsibility of the system expert to not change the parameters to a hazardous time. The EiC is not an expert for all systems that use the RBAC. It must therefore also be the responsibility of the system expert to provide the true reasons of the access request to the EiC.

To prevent spuriously given access, by e.g. a miss click, the software windows are self-closing after a certain time of inactivity. The access for the system expert is withdrawn after a pre-defined period.

Essential parameter changes are not communicated.

The QDS parameters are crucial for the operation of the LHC. The Quench Detection System parameters, such as verification time and voltage thresholds are approved by the MP3 Committee. The parameters must be accessibly documented and continuously updated by the QDS System experts on the MP3 Website.

5 Conclusions and Outlook

The present thesis contains two different analyses of the LHC superconducting magnet circuit: the analysis of the 2008 Incident at CERN and the analysis of the protection mechanisms CLIQ and Quench Heaters applied to the inner triplet upgrade of the HL-LHC. The conclusions of the present work are split into two different topics. The conclusions show a brief overview on the results and then evaluate the methods, also giving an overview on the experiences made during the analysis.

5.1 Conclusions of the CAST Analysis

The present thesis was the first CAST analysis at CERN – investigating the 2008 incident. For the same incident, a Task Force Report (TFR) was already written [12]. It is not stated, if a specific method was used or not by the Task Force. The TFR shows an in-depth analysis of the technical failure and gives recommendations to prevent such a failure in the future. Some of the results of the TFR are the result of in-depth simulations, these results cannot be compared to the results of the present CAST Analysis, as it is not a simulation methodology.

The CAST analysis shows, that the bad soldering spot is not a one-time event, but the result of a failing safety system layout, which is why all soldering spots must be checked. The TFR states the same recommendation with more technical details on how to do it.

Further, adding the behavior shaping factors into the analysis revealed the bad working conditions, due to environmental conditions in the tunnel and the unsure contracts. The TFR does not state a recommendation on the unsure contracts or on rethinking the result-based contracts.

As the proximate event chain showed, the temperature evolution of the subsectors must be checked in the future. This recommendation is given as well in the task force report.

The insufficient layout of the quench detection system was uncovered as well during the analysis. The recommendation to re-think the quench detection system corresponds to a recommendation of the task-force report.

The safety system of the bus bar quench detection was cut due to budget reasons and the strategic hazard analysis techniques were not followed. This hints at a lack of safety culture during the time of the incident and was confirmed by experts. The requirement of the present thesis – to enhance safety culture and to raise the awareness for the necessity of strategic development and hazard analyses – finds no comparison in the task force report.

To mitigate the failure consequences of an incorrect interconnection by securing the interconnection from falling apart is also mentioned in the task force report and has already been done with the new interconnection design shown in Figure 5-1.

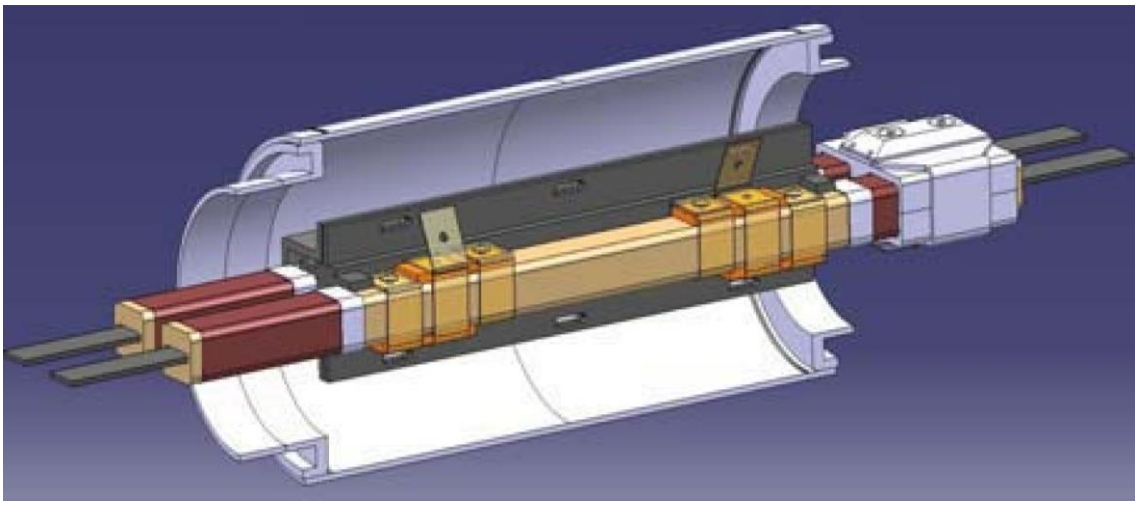


Figure 5-1: Revised Interconnection Design with additional clamps [69]

To further monitor the interconnection procedures, a component-scanning method was proposed. This provides further control that all the components have been used and the automatic documentation makes sure, that all interconnections have been soldered correctly. This also finds no comparison in the task force report.

The Task Force consisted of multiple system experts, who were able to provide in-depth technical knowledge on each subsystem. Considering the system borders, the CAST Analysis came up with similar recommendation than the task force report. CAST showed a sufficient set of requirements that were not as in-depth technically, but included socio-technical failures as well. These are important, as the most fundamental level of failure was the missing safety culture, leading to a missing awareness of the necessity of hazard analysis. Hazard analyses were not popular in the accelerator sector.

CAST proved itself a useful technique throughout the analysis. The procedure is easy to understand, and the system-based thinking can be found on many levels of the analysis. Including social factors as well as revealing management flaws, that were not formalized so far. Also, the idea of STAMP, that accidents are the result of a failing system and not the results of failing components, can be confirmed by the present analysis. However, further guidance is needed for deriving the system borders. It is not clear, which systems to include in the analysis and where to stop. It is also not trivial to decide on a suitable level of detail of each subsystem.

At CERN, the 2008 incident marks a special day for many researchers and engineers. If asked – most of the people remember what they did this day. Many things improved to since: The awareness for strategic hazard analyses improved by far and dependability is today a more important criterion when developing new accelerators. In a meeting, an expert said: "*It seems*

like we're forgetting some of the learned lessons". As stated in this thesis, it is the responsibility of the management to keep the safety culture high. This does not only mean safety of the personnel, but also protecting the discovery potential of CERN. The absence of critical failures does not mean, that hazard analyses become less important. The opposite is true: Analyzing hazards and failures becomes more and more important, as technologies improve, and CERN builds more and more complex accelerators.

5.2 Conclusions of the STPA Analysis

The mechanisms of the inner triplet protection with CLIQ/QH Units were analyzed with the recently at MIT developed method STPA. It promised to focus on system interaction rather than system components. The inner triplet protection mechanisms are still in an early design stage, many components are not yet defined, making a component-level analysis not feasible. This chapter also shows an overview on the results and a comparison of the STPA to the wider known method FMEA.

The result of the present thesis is a set of requirements. These requirements have been reported to the respective working groups and have partially been commented by the respective system experts. For over 150 causal factors, requirements have been formalized. Not only were the requirements found useful, it was one of the results of this thesis to bring experts together to discuss dependability of their system and to formalize the foreseen safety mechanisms in form of the requirements.

It has been found, that the current loops connecting the PIC, QPS and PCs are a potential weak point in the structure. Regular inspection strategies must be defined to limit the probability of an installed short-circuit. The protection units firing, while the quench cannot be communicated due to such a short-circuit is a highly hazardous scenario that must be avoided. The Powering Interlock Controller is a central node of the system that – if failing – can lead to many different hazards.

The spurious firings of CLIQ Units and Quench Heaters have been revealed by context tables. A spurious firing is just one component failure away and so far, it is not sufficiently protected. To detect the spurious firings of CLIQ and QH Units, an interlock must be defined. It must detect the firing, dump the beam, abort the powering and re-trigger all other protection units.

The High Luminosity upgrade includes the building of new underground galleries for the protection units of the HL LHC. These galleries are radiation free and accessible by CERN Personnel for maintenance and inspection. Humans working and accidentally acting on protection units while the machine is in operation must be included as failure causes for hazard analyses in the future.

Further studies are needed to assess the hazardousness of a spurious firing during magnet current ramp up or injection. Further studies are also needed to assess the possibility of a power converter not being shut off after a quench in low powering levels. Dedicated analyses must

assess the new features of the HL LHC and train operators on it. A policy must be defined for technicians in the galleries, what to do in case they damage surrounding system. It must be discussed, where emergency buttons must be implemented to the underground areas that are able to abort the operation.

In [1] and [54], Leveson claims, that STPA is applicable to early design levels, which the inner triplet protection system is. Ideas of how to build up the system are there, yet they often were not formalized, neither specified in any document. STPA proved to be useful at this early level of design. Even though components were not defined, it was already possible to spot unsafe control actions and causal factors and to derive requirements to eradicate or mitigate flaws in the system. Also, the way to display the system – as a control loop – was found to provide a good foundation for discussion during meetings with system experts.

It was found that STPA is a great method to simplify complex systems, making an analysis of complex systems possible. The inner triplet protection system is complex, and every subsystem consists of thousands of components, that one does not need to analyze to already find suitable requirements.

It is often stated [1] [54] [73], that an advantage of STPA is to also include software and human failures. Because no other hazard analysis technique was used to analyze the system, a comparison cannot be made. Yet, the requirements indeed include human failures, such as a technician selecting the incorrect voltage to a CLIQ Unit. Software failures are included as well, such as the Quench Detection System software being not capable of detecting the quench.

Throughout the method, some negative aspects have been found. In the book Engineer a Safer World, Leveson provides the idea of scenarios and causal factors leading to unsafe control [1]. Yet, a clear definition of the terminology and the abstraction level is not given. As also the STPA is still at a very young age compared to FMEA or FTA, the terminologies are not known by experts, and therefore talking with experts about scenarios and causal factors always needs a brief introduction to the method.

The second step of finding root causes for unsafe control is based on guided brainstorming [54]. Following this does not provide a method for ending the analysis. It is not clear, when to stop and if all possible causes have been gathered.

It was also found during this thesis, that the most input for finding reasons for unsafe control is gathered by meeting expert groups. To prevent following only the thoughts of experts, that may be biased towards their own system, the safety engineer must first provide a draft of unsafe control actions, possible scenarios and causal factors.

Lacking quantification and risk prioritizing was also found to be negative within this method. It is stated in [54, p. 22], that “the only way to generate such a probability of an accident for complex systems is to omit important causal factors that are not stochastic, or which probabilistic information does not exist. Producing probabilistic analyses that do not accurately reflect the true risk can be dangerously misleading and lead to complacency and not fixing design flaws that lead to accidents because they are not considered or are unrealistically

discounted in importance.” Even though it is true, that incorrect quantification may lead to an incorrect assumption of safety, one cannot avoid quantification at all and expect to end up in a safer system. Not ranking the hazardousness of unsafe control or causal factors may even lead to an incorrect assumption about priority and lead to the wrong failures being fixed, while more important ones are neglected.

Comparing STPA with “traditional” techniques like FMEA, the main difference lies in the foundation, STAMP. STPA assumes, that accidents happen, when the system fails to keep itself in a safe state – FMEA has its roots in reliability research, which is why it focuses on component failures. This leads to different procedures and terminologies. Figure 5-2 shows a comparison of the steps done in a (System-) FMEA and an STPA.

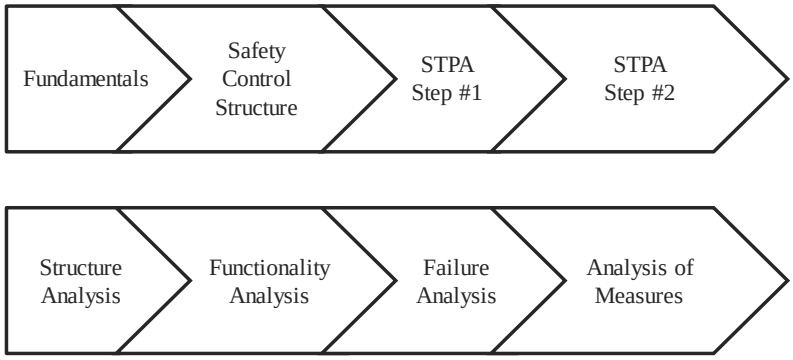


Figure 5-2: Comparison of the procedures of an STPA with a (System-) FMEA

Both STPA and an FMEA start by defining the system. The FMEA analyses the structure of the system to divide the system into subsystems with help of e.g. part lists. The structure of the system is then displayed as on the left side of Figure 5-3. The STPA starts by defining accidents and top-level hazards and derives the system to cope with the hazards. The system is then displayed as a control loop, as shown on the right side of Figure 5-3. The controller QPS provides the control action “Fire Quench Heaters and CLIQ”. Even though the procedure is different, both steps are analyzing the structure of the system. It is inevitable to analyze the structure of the system at some point of the analysis.

From the derived structure, the FMEA defines functions and sub functions to each component, that are then derived to failing functions. The STPA provides more guidance to find the failure functions. It sees the function of a component as the control action that it is providing and gives four ways how this control action can get unsafe. The context tables provide a guided approach to find incorrectly timed control actions.

During the measures analysis, the FMEA uses the defined causality of failure effect, failure and failure cause. It classifies the failure in severity, detectability and occurrence. This also provides help in finding appropriate measures to cope with the failure cause; if the severity of the failure is very high, the engineer must try to mitigate the effect of the failure to reduce the Risk Priority Number (RPN) of the failure. This also provides a ranking of the most hazardous failure causes

and shows the engineer, which failures he must approach first. The STPA does not provide a quantitative measure of risk or safety. Yet, an FMEA-like approach to measure risk is not impossible. The engineer could define a severity of the accidents or of the unsafe control action and could then quantify the occurrence and detectability of each causal factor or scenario. However, as some papers suggest, a quantification is not wanted within this methodology [74].

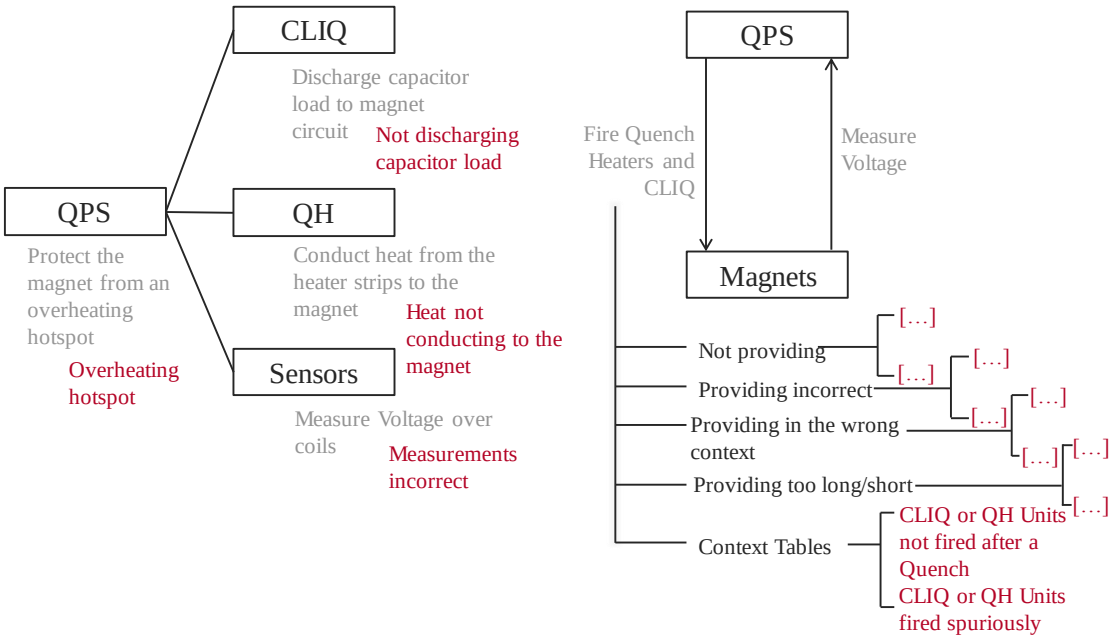


Figure 5-3: Where the structure analysis, function analysis and failure analysis of the FMEA can be found in the STPA

It was found at multiple stages of the analysis, that mixing the methods could be useful. The structured way of the context tables to find correctly provided control actions at the incorrect time can be implemented to find failing functionalities during the function analysis of the FMEA. As proposed before, an FMEA-like ranking could theoretically be implemented to the STPA.

STPA was found to rely significantly on the input that experts provide. It is easy to come up with unsafe control actions or a draft of the system control loop, but if asked specifically about causes or failure modes, they can provide useful input for the method. For future applications of STAMP analyses, it is therefore recommended to do regular meetings in a big round with engineers from all systems, e.g. in the following schedule:

- When Accidents and Hazards are defined, and a very top-level preliminary control structure is drawn. Experts can provide input on missing systems and missing system interactions.

- After the definition of UCAs: Experts can provide useful input, which UCAs are neglectable or missing. It must be assessed which UCAs should be further investigated with an analysis of the scenarios and causal factors.

- After defining scenarios and causal factors: Requirements often address multiple systems, therefore bringing the respective experts at one table leads often to discussions and an exchange of experiences with possible requirements.

6 Bibliography

[1] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, Cambridge, Massachusetts: The MIT Press, 2011.

[2] International Electrotechnical Commission, "Electropedia," 02 2015. [Online]. Available: http://www.electropedia.org/iev/iev.nsf/ display?openform&ievref=192-01-22. [Accessed 03 07 2017].

[3] B. Bertsche, Reliability in Automotive and Mechanical Engineering, Heidelberg: Springer-Verlag Berlin Heidelberg, 2008.

[4] CERN, "Cern Homepage, Topic: Higgs Boson," CERN, [Online]. Available: https://home.cern/topics/higgs-boson. [Accessed 1 10 2017].

[5] CERN, "LHC - The Guide," [Online]. Available: https://cds.cern.ch/record/2255762/files/CERN-Brochure-2017-002-Eng.pdf. [Accessed 13 07 2017].

[6] CERN, "HL-LHC Homepage," [Online]. Available: http://hilumilhc.web.cern.ch/. [Accessed 03 07 2017].

[7] CERN, "LHC Machine Outreach," CERN, [Online]. Available: http://lhc-machine-outreach.web.cern.ch/l. [Accessed 13 07 2017].

[8] G. Apollinari, I. Alonso, P. Fessia, M. Lamont, L. Rossi and L. Tavian, High-Luminosity Design Report V.01, Geneva: CERN, 2017.

[9] A. Fernandez, Reliability of the QPS, Geneva: Universitat de Catalunya, 2003.

[10] CERN Courier, "Safeguarding the superconducting magnets," CERN, 19 08 2013. [Online]. Available: http://cerncourier.com/cws/article/cern/54383. [Accessed 01 10 2017].

[11] E. Ravaioli, CLIQ - A new quench protection technology for superconducting magnets, University of Twente, Netherlands, 2015.

[12] "Report of the Task Force on the Incident of 19 September 2008 at the LHC," CERN, Geneva, 2009.

[13] CERN, "CERN Homepage: Member States," CERN, [Online]. Available: http://home.cern/about/member-states. [Accessed 08 08 2017].

[14] CERN, "Cern Homepage: The Birth of the Web," [Online]. Available: https://home.cern/topics/birth-web. [Accessed 08 08 2017].

[15] CERN, "CERN Bulletin: Another of Cern's many inventions!," 22 03 2010. [Online]. Available: http://cds.cern.ch/journal/CERNBulletin/2010/13/News%20Articles/1248908?ln=de. [Accessed 08 08 2017].

[16] Science and Technology Council Homepage, "Stock Exhange," [Online]. Available: http://www.stfc.ac.uk/stfc/includes/themes/Mura STFC/assets/legacy/LHCinteractive/LHC_default.jpg. [Accessed 02 09 2017].

[17] Education, Communication and Outreach Group, "Cern Document Server: LHC-The Guide (faq)," 02 2017. [Online]. Available: http://press.cern/press-kit. [Accessed 08 08 2017].

[18] P. Sollander, R. Martini, K. Sigerud, N. Stapley and A. Suwalska, "Alarms Configuration Management," in *ICALEPCS*, Knoxville, Tennesee, 2007.

[19] D. Rivorion, "Hardware Comissioning Working Group," CERN, 02 09 2004. [Online]. Available: http://lhc-hcwg.web.cern.ch/lhc-hcwg/HCWGmandat.htm. [Accessed 11 10 2017].

[20] M. Lamont, "LHC Commissioning Web," 06 2016. [Online]. Available: https://lhc-commissioning.web.cern.ch/lhc-commissioning/performance/2016-performance.htm. [Accessed 05 10 2017].

[21] R. Assmann, A. Ferrari, M. Magistris, M. Santana-Leitner, K. Tsoulou and V. Vlachoudis, *Energy Deposition Studies for the Betatron Cleaning Insertion (IR7) of LHC*, Geneva: CERN, 2005.

[22] L. Belova, M. Genet, J.-L. Perinet-Marquet, P. Ivanov and C. Urpin, "Design and Manufacture of the Superconducting Bus-bars for the LHC Main Magnets," in *International Conference on Magnet Technology*, Geneva, 2002.

[23] W. Andrzej, *CERN Accelerator School: Maxwell's Equations for Magnets*, 2009.

[24] H. ten Kate, "Superconducting Magnets: Quench Propagation and Protection," in *CERN Accelerator School*, 2013.

[25] P. Ferracin and E. Todesco, "Indico.cern.ch," 22 05 2015. [Online]. Available: https://indico.cern.ch/event/440690/contributions/1089760 /attachments/1143852/1639310/U16_final.pdf. [Accessed 03 07 2017].

[26] F. Sonnemann, Resistive Transition and Protection of LHC Superconducting Cables and Magnets, Aachen: RWTH Aachen, 2001.

[27] S. Yammine and H. Thiesen, "HL-LHC Inner Triplet Powering and Control Strategy," in *International Particle Accelerator Conference*, Copenhagen, 2017.

[28] G. Bozza, *Milestone Report: Study of the superfluid He Cooling*, Geneva: CERN, 2014.

[29] O. Brüning, P. Collier, P. Lebrun, S. Myers, R. Ostojic, J. Poole and P. Proudlock, LHC Design Report, Geneva: CERN, 2004.

[30] M. Lamont, "CERN Courier, Aug. 2013," CERN LHC Team, 19 08 2013. [Online]. Available: http://cerncourier.com/cws/article/cern/54381. [Accessed 11 10 2017].

[31] M. Breschi, E. Felcinni and L. Bottura, "Quench Level of the HL-LHC Nb3Sn IR Qudarupoles," in *IEEE Transactions on Applied Superconductivity*, Geneva, 2017.

[32] E. Ravaioli, "Quench Protection Studies for the High Luminosity LHC Inner Triplet Circuit," CERN, Geneva, 2016.

[33] F. Bordy, R. Denz, K.-H. Mess, B. Puccio, F. Rodriguez-Mateos and R. Schmidt, Machine Protection for the LHC: Architecture of the Beam and Powering Interlock Systems, Geneva: CERN, 2001.

[34] B. Todd, A. Dinius, P. Nouci, B. Puccio and R. Schmidt, "The Architecture, Design and Realisation of the LHC Beam Interlock System," in *International Conference on Accelerator and Large Experimental Physics Control Systems*, Geneva, 2005.

[35] S. Wagner, LHC Machine Protection System: Method for Balancing machine Safety and Beam Availability, Zurich: ETH Zurich/CERN, 2010.

[36] R. Schmidt, A. Dinius, R. Giachino, J. Gimeno Vicente, B. Puccio, P. Nouchi and J. Wenninger, "Beam Interlocks for LHC and SPS," CERN, Geneva, 2003.

[37] M. Zerlauth, Powering and Machine Protectioon of the Superconducting LHC Accelerator, Graz: Graz University of Technology, 2004.

[38] E. Blanco, "Cryogenics Control: PIC-Cryo Communications," CERN, Geneva, 2006.

[39] E. Veyrunes, "Operator Workshop Machine Checkout: Cryogenics," CERN, Geneva, 2007.

[40] R. Schmidt, B. Puccio and M. Zerlauth, "The Hardware Interfaces between powering Interlock System, Power Concerters and Quench Protection System," CERN, Geneva, 2007.

[41] H. Thiesen, "Risks due to UPS Malfunctioning," in *Proceedings of Chamonix Workshop of the LHC Performance*, Chamonix, 2009.

[42] R. Denz and F. Rodriguez-Mateos, "Detection of Resistive Transitions in the LHC Superconducting Components," in *Proceedings of the 2001 Particle Accelerator Conference*, Chicago, 2001.

[43] *Personal Conversation with R. Denz, 09.10.17.*

[44] D. Carillo, "Technical Specification CLIQ," CERN, Geneva, 2017.

[45] J. Steckert, *Conceptual Design Review of the Magnet Circuits for the HL-LHC: Quench Detection for HiLumi,* Geneva: CERN, 2016.

[46] CERN COURIER, "LS1: reawwakening the accelerators," 22 05 2014. [Online]. Available: http://cerncourier.com/cws/article/cern/57283. [Accessed 01 09 2017].

[47] K. Dahlerup-Petersen, R. Denz, J. Gomez-Costa, D. Hagedorn, P. Proudlock, F. Rodriguez-Mateos, R. Schmidt and F. Sonnemann, "The Protection System for the Superconducting Elements of the Large Hadron Collider at CERN," CERN, Geneva, 2002.

[48] E. Todesco, "Quench Limits in the Next Generation of Magnets," in *Workshop on Accelerator Magnet, Superconductor, Design and Optimization*, Geneva, 2013.

[49] S. Izquierdo Bermudes, J. Ferradas Troitino, P. Ferracin, J. Perez, G. Vallone, S. Florence Gayot, S. Tavares, G. Maury and N. Bourcey, *MQXS Inner Layer Quench Heaters*, Coil Structure Working Group, 2018.

[50] E. Ravaioli, "New, Coupling Loss Induced, Quench protection System for Superconducting Accelerator Magnets," *IEEE Transactions on Applied Superconductivity*, vol. 24, no. 3, p. 5, 2014.

[51] E. Ravaioli, V. Datskov, G. Kirby, H. ten Kate and A. Verweij, *CLIQ - Coupling-Loss Induced Quench System for Protecting Superconducting Magnets,* Geneva: CERN, 2014.

[52] M. Valette, L. Bortot, A. Fernandez Navaroo, B. Lindström, R. Schmidt, A. Verweij and D. Wollmann, Effect of Quench Heater and CLIQ Firing on the HL-LHC Circulating Beam, Geneva: CERN, 2017.

[53] G. Sabbi, J. Blomberg Ghini, S. Gourlay, M. Marchevsky, E. Ravaioli, H. ten Kate, A. Verweij and X. Wang, "Design Study of a 16-T Block Dipole for FCC," *IEEE Transactions on Applied Superconductivity*, vol. 26, no. 3, 2016.

[54] N. Leveson, *An STPA Primer,* 2013.

[55] A. Abdulkhaleq and S. Wagner, *An eXtensible STAMP platform as tool support for safety engineering,* Universität Stuttgart, 2015.

[56] J. Thomas, Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis, Cambridge,MA: MIT Press, 2013.

[57] Institut of Software Technology, "xstampp.de," [Online]. Available: http://www.xstampp.de/Download.html. [Accessed 12 09 2017].

[58] J.-P. Tock, F. Bertinelli, P. Fessia, A. Jaquemod, A. Musso and A. Poncet, "The Interconnections of the LHC Cryomagnets at CERN: Strategy applied and first results of the industrialization process," CERN, Geneva, 2007.

[59] Der Standard, "derstandard.at - Wissenshaft - Technik," Der Standard, 25 01 2009. [Online]. Available: http://derstandard.at/1231152807922/Schaden-am-Teilchenbeschleuniger-unterschaetzt. [Accessed 03 09 2017].

[60] BBC, "BBC Science & Environment," BBC, 09 11 2009. [Online]. Available: http://news.bbc.co.uk/1/hi/8369853.stm. [Accessed 03 09 2017].

[61] G. Dissertori, "The large Hadron Collider at CERN: Entering a new era in Particle Physics," [Online]. Available: http://www.sps.ch/artikel/diverse-artikel/the-large-hadron-collider-at-cern-entering-a-new-era-in-particle-physics/. [Accessed 10 10 2017].

[62] A. Verweij, "BUSBAR AND JOINTS STABILITY AND PROTECTION Busbar and Joints Stability and Protection," in *Proceedings of Chamonix on LHC Performance*, Charmonix, 2009.

[63] F. Bertinelli, D. Bozzini, P. Cruikshank, W. Maan, A. Poncet, S. Russenschuck and F. Savary, "The Quality Control of the LHC Continous Cryostat Interconnections," in *EPAC08*, Genoa, 2008.

[64] P. Fessia, F. Bertinelli, D. Bozzini, P. Cruikshank, A. Jacquemod, W. Maan, A. Musso and L. Oberli, "The LHC Continous Cryostat Interconnections: The Organization of a Logistically Complex Worksite Requiring Strict Standards and High Output," in *EPAC08*, Genoa, 2008.

[65] M. Mottier, *Quality Assurance Procedure: Design and Quality Control*, Geneva: CERN, 1999.

[66] A. Jacquemod, A. Poncet, F. Schauf, B. Skoczen and J.-P. Tock, "Inductive Solderings of the Junctions of the Main Superconducting Busbars of the LHC," CERN, Geneva, 2003.

[67] G. Arduini, "Organization," in *Charmonix 2009 Workshop on the LHC Performance*, Charmonix, 2009.

[68] 1. Meeting with J.-P. Tock.

[69] F. Bertinelli, N. Catalan Lasheras, P. Fessia, C. Garion, M. Mathot, A. Perin, S. C. and S. Sgobba, "Towards a Consolidation of the LHC Superconducting Splices for 7TeV Operation," CERN, Geneva, 2010.

[70] R. Carcagno, "Functional Specification: MQXFA Magnets," U.S. HL-LHC Accelerator Upgrade Project, 2017.

[71] M. Zerlauth, *Private Mail Conversation*, Geneva: -, 2017-08-04.

[72] P. e. a. Charrue, "Role-Based Access Control for the Accelerator Control System in the LHC Era - Design," CERN, Geneva, 2007.

[73] T. Ishimatsu and N. Leveson, "Modeling and Hazard Analysis Using STPA," MIT Press, Massachusetts, 2012.

[74] R. Feodoroff, *STPA versus FTA: In search of Stable Patterns of Hazard Analysis Technique for URN,* Edinburgh: -, 2015.

[75] D. Berkowitz, "Prelimary Naming, Operatoinal Parameters and Flow Diagrams of the Cryogenic Distribution Lines for HL-LHC," CERN, Geneva, 2016.

[76] J.-P. Tock, *Expert Talk with J.-P. Tock, 11.05.2017, 14:00*, Geneva, CERN, 2017.

[77] P. Faugeras, "Quality Assurance Policy and Project Organization," CERN, Geneva, 1999.

[78] W. Herr, B. Muratori and J. Holzer, "Concept of Luminosity," in *Design and Principles of Synchrotrons and Circular Colliders*, Heidelberg, Springer-Verlag Berlin Heidelberg, 2013, pp. 361-377.

[79] W. Riegler, "LHC Experiments Look in the Future," CERN, 15 05 2014. [Online]. Available: http://ep-news.web.cern.ch/content/lhc-experiments-look-future. [Accessed 13 07 2017].

[80] J. Gomez and J. Pedersen, *Underground Uninterrupted Power Supply (UPS) for the LHC,* Geneva: CERN, 2003.

[81] G. Cumer, *Description of the CERN Electrical Network,* Geneva: CERN, 2015.

[82] A. Navarro, *Dependability Analysis of a Quench Protection System for HL-LHC,* Geneva: CERN, 2016.

[83] A. Albee, C. Leising, S. Battel, D. MacPheson, R. Brace, W. Menard, G. Burdick, R. Rosé, P. Burr, R. Sackheim, J. Casini, A. Schallenmuller, D. Dipprey, C. Whetsel and J. Lavell, "NASA Press Release," 22 03 2000. [Online]. Available: https://spaceflight.nasa.gov/spacenews/releases/2000/mpl/mpl_report_1.pdf. [Accessed 18 07 2017].

[84] A. Abdulkhaleq and S. Wagner, "A controlled experiment for the empirical evaluation of safety analysis technicques for safety-critical software," in *19th International Conference on Evaluation and Assessment in Software Engineering*, Nanjing, China, 2015.

[85] A. Apollonio, Machine Protection: Availability for Particle Accelerators, Wien: Vienna University of Technology, 2015.

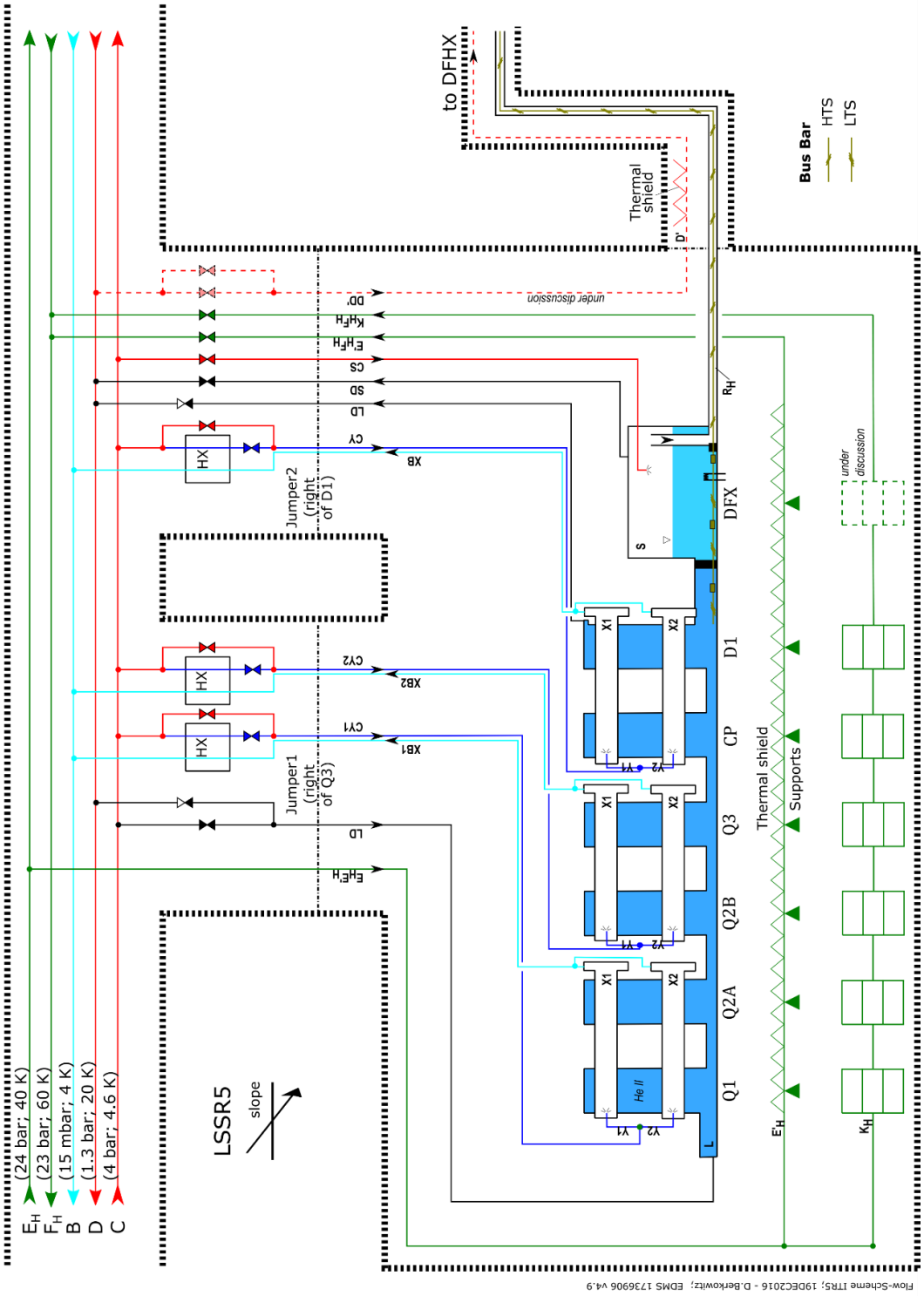
[86] CERN, "Cryogenics: Low temperatures, high performance," CERN , [Online]. Available: https://home.cern/about/engineering/cryogenics-low-temperatures-high-performance. [Accessed 01 10 2017].

[87] CERN, "The Height Of Cool," CERN Bulletin, 23 03 2007. [Online]. Available: http://cds.cern.ch/journal/CERNBulletin/2007/17/News%20Articles/1027044?ln=en. [Accessed 01 10 2017].

[88] D. Meschede, Lehrbuch der Experimentalphysik, Band II, Berlin: Springer Verlag, 1971.

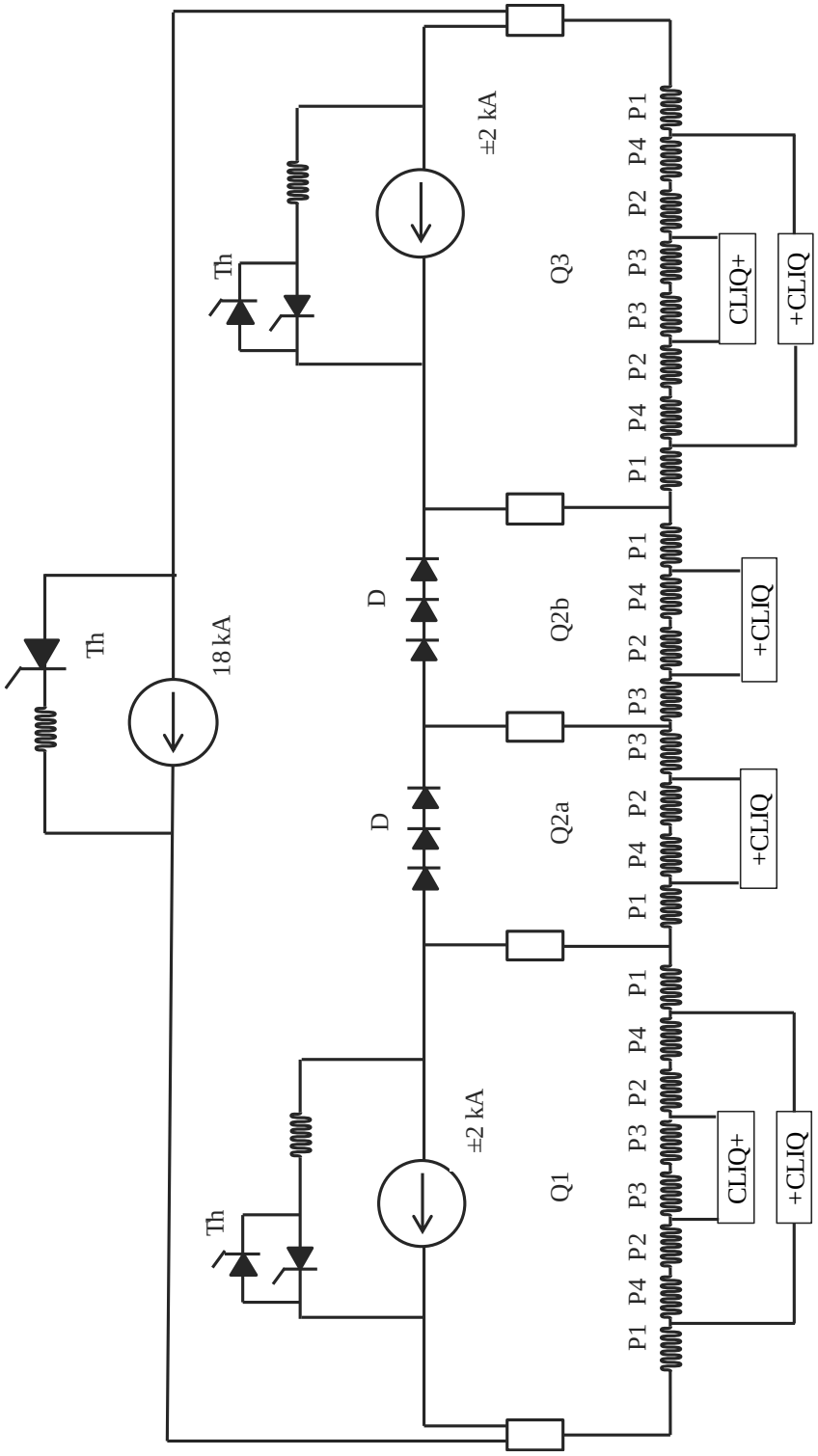
7 Appendix

A Cryogenic Distribution Lines



Source: [75]

B Inner Triplet Powering Baseline



Powering of the Inner Triplet Q1 – Q3 as at June 2017 with the connection of CLIQ. The "+" indicates the direction of the first current discharge of the CLIQ Units

C Responsibilities of the Controllers of the CAST Analysis

Interconnection Team [12] [58] [64] [76]

- Roles/Responsibilities:
    - Executes Main Part of the Work (Soldering, moving)
    - Improve the current laboratory tools for interconnection
- Safety Constraints
    - Execute assembling and soldering as defined
- Environmental and behavior-shaping factors
    - Educated on superconductors
    - Result-based working contract
    - Bad environmental conditions: High humidity/low Temperature
    - Unsure contracts

Quality Team [12] [58] [64] [76]

- Roles/Responsibilities
    - Visually inspects soldered interconnection
    - Report and document non-conformities and report them to the CERN Coordination Team
- Environmental and behavior-shaping factors
    - Bad working conditions
    - Limited Feedback from interconnection process
    - High educated specialists consisting of CERN engineers and specialists from a collaborating institute
- Safety Constraints
    - Find and report bad soldering spots to the coordination team

Point Owner [67]

- Roles/Responsibilities:
    - Assist HWC Coordinator and EiC in the definition of the commissioning plan
- Environment and behavior shaping factors
    - Engineer/Physicist with knowledge of 2 sectors at least
    - Absence of failures led to the incorrect assumption about safety and a decrease of awareness

CERN Coordination Team [64]

- Roles/Responsibilities
    - Coordinates all Activities
    - Final responsibility for quality
    - Spread the necessary Information
- Environmental and behavior-shaping factors
    - CERN Staff with high knowledge on the LHC
    - Timetable pressure
- Safety constraints
    - Ensure electrical continuity

Inductive Soldering Machine

- Role
    - Provides heat for soldering Process
- Safety Constraint
    - Display flawed interconnections by surveillance of process parameters

Process Design Team [77] [58]

- Roles/Responsibilities:
    - Provide safe and reliable interconnection process
    - Provide parameters and definitions for tools, developed by contractors
    - Each engineer is responsible for the quality of his/her work and the work of his/her subordinates
- Safety constraints:
    - Ensure safe and reliable process
- Environment and behavior shaping factors
    - Busbar never showed quenches in experiments
    - Education: Engineers/Physicists

HWC Coordinator [67]

- Roles/Responsibilities:
    - Prepares conditions for commissioning
    - Safety
    - Environment
    - Infrastructure
    - Quality assurance (Assisted by point owner)
    - Defines commissioning
    - Reports progress and problems to project manager
- Environment and behavior shaping factors
    - Engineer/Physicist with experience
    - Absence of failures led to the incorrect assumption about safety and a decrease of awareness
- Safety Constraints
    - Define safe commissioning procedures (see MPP)
    - Provide overall safety

EiC on Shift [67]

- Roles/Responsibilities:
    - Safety
    - Controls execution
    - Documents the tests
- Environment and behavior shaping factors
    - Accelerator Engineer/Physicist with at least 2 years of experience
    - Absence of failures led to the incorrect assumption about safety and a decrease of awareness
- Safety Constraints
    - Disable Access for hazardous areas (see OoS)

Accelerator System Experts [67]

- Roles/Responsibilities
    - Executes Steps required for the preparation of the HWC on the field in the field and in CCC
    - Monitors performance of his/her system

- Environment and behavior shaping factors
    - One with experience in one of the systems involved with the powering tests (Cryo, QP, etc...)
    - Absence of failures led to the incorrect assumption about safety and a decrease of awareness
- Safety constraints
    - Find and report suspicious behavior during the commissioning of his/her system

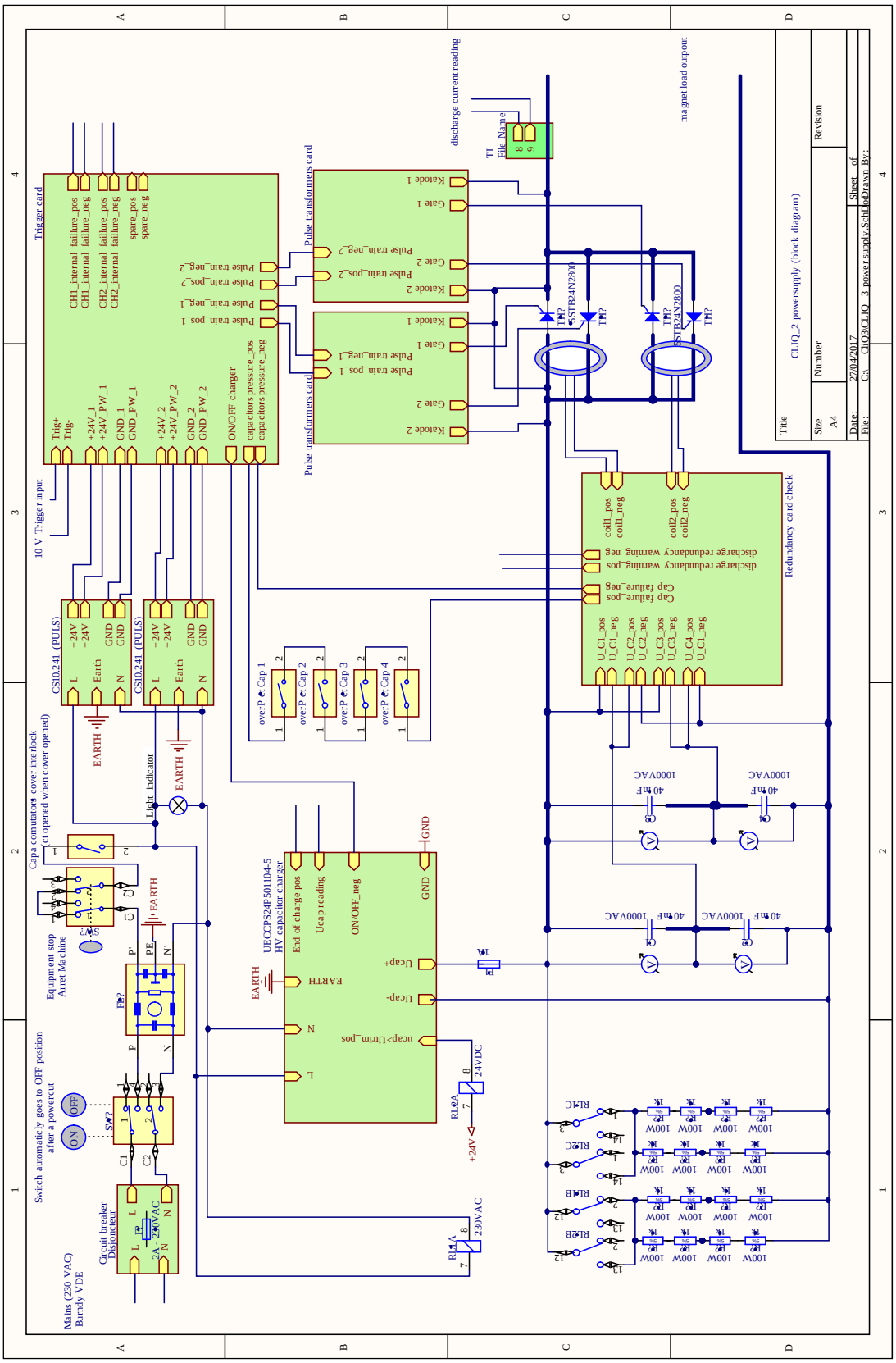
Operator on Shift [67]

- Roles/Responsibilities
    - Executes Test Plan
    - Assists the EiC in handling Access
- Environment and behavior shaping factors
    - Accelerator Technician with experience in the operation of the magnet test facility in SM18.
    - Absence of failures led to the incorrect assumption about safety and a decrease of awareness
- Safety Constraints
    - Disable Access to hazardous areas

MPP (Main Ring Magnet Performance Panel) [67]

- Roles/Responsibilities
    - Acting as „control body “
    - Defining/Revising the procedures for the tests
    - Monitoring, analyzing and managing magnet performance
    - Detecting, diagnosing, correcting and mitigating problems
- Environment and behavior shaping factors
    - Panel consists of SC Magnet Experts, Magnet Protection Experts, Cryogenics’ Experts
    - Absence of failures led to the incorrect assumption about safety and a decrease of awareness
- Safety Constraints
    - Define safe and revise unsafe testing procedures

D Layout of a CLIQ 3 Unit



E Links

This appendix provides links for the lists of Unsafe Control Actions, Scenarios, causal factors and requirements at the CERN electronic document server (EDMS)

List of Unsafe Control Actions, Scenarios, Causal Factors and Requirements

https://edms.cern.ch/file/1870633/1/SupportingDoc_UCAs_Scenarios_CausalFactors.xlsx

List of Context Tables

https://edms.cern.ch/file/1870633/1/SupportingDoc_ContextTables.xlsx