RISK ANALYSIS OF THE LHC UNDERGROUND AREA

FIRE RISK DUE TO FAULTY ELECTRICAL EQUIPMENT

Angela Harrison, MEng.

Thesis submitted to The University of Leoben
for the degree of Doctor mont. (Ph.D.)

**Institute for Process Technology
and Industrial Environmental Protection**

Supervisor: O.Univ.Prof. Dipl.-Ing. Dr.mont. Werner L. Kepplinger

Leoben, Austria

CERN - European Organisation for Nuclear Research

Supervisor: Dipl.-Ing. Dr. Friedrich Szoncsó

Geneva, Switzerland

July 2007

STATUTORY DECLARATION

I herewith declare on oath that I have produced the enclosed Ph.D. thesis independently and without using any other than the sources or means listed. Any thoughts directly or indirectly taken from somebody else's sources are made discernible as such.

To my son Felix,
who in the face of adversity never failed
to put a smile on my face and in my heart.

Abstract

The European Organisation for Nuclear Research (CERN) in Geneva, Switzerland, is currently building the latest generation of particle accelerators, the LHC (Large Hadron Collider). The machine is housed in a circular tunnel of 27 km of circumference and is situated approximately 100 metres beneath the surface astride the Franco-Swiss border.

Electrically induced fires in the LHC are a major concern, since an incident could present a threat to CERN personnel as well as the public. Moreover, the loss of equipment would result in significant costs and downtime. However, the amount of electrical equipment in the underground area required for operation, supervision and control of the machine is essential. Thus the present thesis is assessing the risk of fire due to faulty electrical equipment in both a qualitative as well as quantitative way.

The recommendations following the qualitative analysis suggest the introduction of fire protection zones for the areas with the highest risk of fire due to a combination of possible ignition sources and combustible material in the vicinity. In order to be able to conduct regular follow-up examinations to obtain more precise results for the quantitative analysis in the future, the creation of a material data inventory and the collection of failure probability data throughout the lifetime of the LHC are recommended.

Kurzfassung

Die Europäische Organisation für Kernforschung (CERN) in Genf errichtet zur Zeit die jüngste Generation von Teilchenbeschleunigern, den sogenannten LHC (Large Hadron Collider). In einem kreisförmigen Tunnel von 27 km Umfang in einer Tiefe von durchschnittlich 100 m untergebracht, verläuft dieser Beschleuniger unter der schweizerisch-französischen Grenze.

Elektrisch verursachte Feuer im LHC sind von besonderem Interesse, da ein Unfall eine Bedrohung für das Personal und auch die Öffentlichkeit sowie den Betrieb des Beschleunigers darstellen kann. Darüber hinaus würde ein Verlust der Anlagen bedeutende Kosten und eine erhebliche Stillstandszeit nach sich ziehen. Dennoch sind die elektrischen Anlagen im Untertagebereich für Betrieb, Überwachung und Steuerung des Beschleunigers unerlässlich. Daher untersucht die vorliegende Doktorarbeit das Feuerrisiko aufgrund von fehlerhaften elektrischen Anlagen auf qualitative als auch auf quantitative Weise.

Der der qualitativen Analyse folgende Vorschlag empfiehlt die Ausweisung von speziellen Feuerschutzzonen für diejenigen Untertagebereiche, die aufgrund der Kombination von möglichen Zündquellen und nahe gelegenen brennbaren Materialien das höchste Feuerrisiko aufweisen. Damit in der Zukunft regelmäßige Nachuntersuchungen zur Ermittlung genauerer Ergebnisse der quantitativen Analyse durchgeführt werden können, werden die folgenden Maßnahmen empfohlen: zum einen soll eine Datenbank bezüglich der Materialeigenschaften der verwendeten Anlagen die Bestimmung der Brandlast erleichtern, zum anderen sollen anlagenspezifische Ausfallsdaten während der gesamten Lebensdauer des LHC erfasst werden.

Contents

Chapter 1

Introduction

The Large Hadron Collider (LHC) is a large and complex project of the European Organisation for Nuclear Research (CERN) in the High Energy Physics field. This particle accelerator will be housed in a tunnel with a circumference of approximately 27 km and an average distance from the surface of 100 metres. Designed to help physicists investigate deeper into matter than ever before, it will analyse particle collisions at very high energies. These collisions will take place in the so-called experiments, which are situated within the LHC perimeter and are housed in huge caverns.

Statistics about electrically induced fires in Finland show that accidents in electrical installations occur quite frequently compared to the total number of fires. Of special concern is the fact that in the majority of cases the fire origin is unknown, as the actual fire cause is not obvious and no fire investigations are performed [1].

The main purpose of this thesis is the assessment of the fire risk in the LHC tunnel originating from electrical equipment in order to quantify the anticipated fire frequency and subsequently suggest measures to improve the situation in the future. Human error and technical breakdown are discussed as main possible causes.

Using the latest technologies for the LHC implicates a high amount of surveillance and control equipment, which will basically consist of electrical and electronic apparatus situated in technical galleries and alcoves next to, but also inside the main tunnel. As the LHC will pass below residential areas between the Geneva Lake and the Jura mountains, the subject of safe machine operation and sufficient prevention measures is under question.

The complexity and dimensions of the LHC make it impossible for a single person to carry out a risk analysis including not only fire risk, but also mechanical, chemical, biological and radiation risk as well as impacts from the outside (i.e. plane crash, seismic activity), which would be the most suitable study.

This thesis concentrates on the analysis of fire risk due to faulty electrical equipment because of the amount of electrical equipment used and the diversity of electrical modes of operation. Moreover, there have been three major incidents involving fires due to faulty electrical equipment in CERN's history. Fortunately there were no casualties, but the damage of equipment and buildings as well as the downtime of the accelerator were significant.

The four experiments of the LHC were developed for different objectives, thus each of their designs and operation modes is just as diverse. Considering these particularities and complexities, the fire safety aspects of the experiments will not be included in the present thesis, which will therefore focus on the main tunnel as well as the technical galleries and alcoves.

The construction of the LHC includes different project phases such as installation, commissioning and operation. It was decided to analyse the fire risk of the LHC during operation, which implies the period of time between commissioning and trouble-shooting or maintenance shut-downs. It is assumed that during this phase there are no workers in the tunnel.

Within these boundaries, this thesis is aiming at revealing sensitive areas where the highest fire risk is suspected due to the available amount of combustible material and the presence of electrical equipment as potential ignition source. In addition to this qualitative analysis, a quantification of the fire risk in the tunnel in terms of frequency of occurrence will also be completed.

After introducing CERN and the subject under investigation for this study, the LHC, different methods of analysing risk will be presented and discussed in the theoretical part. Then the boundary conditions for the analysis will be described, including a step by step explanation about how the problem is going to be approached. Following these guidelines, the actual qualitative and quantitative analyses will be performed. Finally, the results are going to be discussed and measures for improvement will be proposed.

Chapter 2

Executive Summary

The identification of hazardous areas in terms of fire risk due to faulty electrical equipment was determined with the help of a Failure Modes and Effects Analysis (FMEA) for electrical installations. Basic electrical failures such as short circuit or overheating were examined regarding their possible causes and consequences. Alongside this analysis the material data of equipment installed in the tunnel were collected and the combustible portion determined. Their combination revealed areas in the LHC tunnel which could be particularly susceptible to developing a fire, since any concurrence of combustible material and faulty electrical equipment as possible ignition source in the vicinity creates a dangerous situation. The areas of concern include the following:

- The injection areas at points 2 and 8 due to the silicone fluid contained in the high voltage pulse generators,
- point 4 due to a very high energy conversion of the radio frequency system and also the appearance of silicone fluid,
- the LHC arcs due to the presence of combustible material and the lack of fire and smoke detectors,
- and at last the alcoves due to the housing of major parts of the electrical distribution equipment together with part of the UPS system and therefore their importance for LHC operation.

By taking the Failure Modes and Effects Analysis one step further, the failure modes were assessed by means of an expert judgement. Their frequency of occurrence and the severity of their consequences were judged by three experts in electrical and electronic engineering at CERN using pre-determined classifications.

Once the risk matrix was drawn, the majority of the failure modes were situated within the transition area between the acceptable and unacceptable risk areas. However, due to the already advanced stage of the LHC project, an intervention in order to shift the frequency/consequence pairs into the acceptable risk area was not possible. Since the expert judgement does not assess fire risk directly, but only failure modes possibly leading to a fire, the outcome of this quantitative analysis does not necessarily enforce any actions, though it draws attention to the importance of fire risk for experts working in this field.

A fault tree analysis (FTA) was carried out in order to obtain a more accurate quantification of the fire risk. A Boolean algebra computing programme was used to calculate the top event probability of having a fire in the LHC underground.

The basis for the fault tree analysis was a so-called risk layer along the tunnel, assuming an average amount of electrical equipment along the underground area. Thus the outcome of the fault tree was treated as an average value valid anywhere in the tunnel.

With estimated failure probability values for the basic events, the probability of fire in the LHC tunnel due to faulty electrical equipment was calculated at $9.23 \cdot 10^{-7}$, which means once every 217 years. Because of the structure of a fault tree, this result does not only include technical failures, but also human error and special circumstances such as the lack of fire and smoke detectors in certain areas. Keeping this in mind, a fire probability in the range of 10^{-7} is a very low value. However, its inaccuracy due to inexistent failure rate data and therefore only estimations for the basic events in the fault tree is worrying. Though the tree was developed for an equally distributed risk layer, in reality this value might increase in certain areas as a result of the accumulation of electrical equipment and combustible material.

The hazardous areas defined previously are identified as fire protection zones including special rules and regulations. It is suggested to reinforce fire and smoke detection, mark them with particular signboards, complete a Risk Description form in order to support the fire brigade's development of intervention plans and make all personnel familiar with the rules of good housekeeping.

Concerning the quantitative assessment of the fire risk in the tunnel, two measures of improvement are suggested. In order to develop the identification of hazardous zones and also facilitate the identification and quantification of combustible materials contained in the underground area, it would be advantageous to create a material data inventory which would be regularly updated. Although for this thesis inflammable material data have been collected, their acquisition should become part of a safety management system and its inaccuracy should be eliminated for future application and re-analyses.

The second suggestion is heading towards the same direction, namely the collection of failure probability data throughout the lifetime of the LHC. System-dependent failure data could then be available for a reassessment of the present results, providing a more accurate idea of the fire risks involved in the operation of electrical equipments.

Chapter 3

The Large Hadron Collider

3.1 CERN

CERN is the European Organization for Nuclear Research, the world's largest particle physics centre. Founded in 1954 by 12 signatories, it was one of Europe's first joint ventures, and over time membership has grown to today's 20 member states. The laboratory is situated astride of the Franco-Swiss border west of Geneva at the foot of the Jura mountains.

Some 6,500 visiting scientists, half of the world's particle physicists, are using CERN's facilities, representing 500 universities and over 80 nationalities. CERN itself employs about 3,000 people in a variety of disciplines to collaborate and provide support and infrastructure to all the physicists taking advantage of the laboratory's installations. In addition, various contracted firms support CERN staff in matters of civil engineering, installation, operation and periodic maintenance of equipment as well as repair and modification of installations [2].

CERN's main field of study is particle physics or High Energy Physics (HEP), as it is mostly referred to, where physicists investigate the constituents of matter at the subatomic level.

Throughout the twentieth century, important progress was made in the field of particle physics, from discovering the electron to the atomic nucleus and its constituents, from special relativity to quantum mechanics. With the foundation of CERN at the beginning of the 1950's and hence the cooperation of European countries, sufficient financial means were available for more systematic and detailed particle physics research [3].

The necessary tools provided by CERN are particle accelerators which recreate the conditions that existed just after the Big Bang, aiming at the discovery of what the Universe is made of and how it works. By accelerating the particles to very high energies and smashing them into each other, physicists can identify their components or create new particles, revealing the nature of the interactions between them [4].

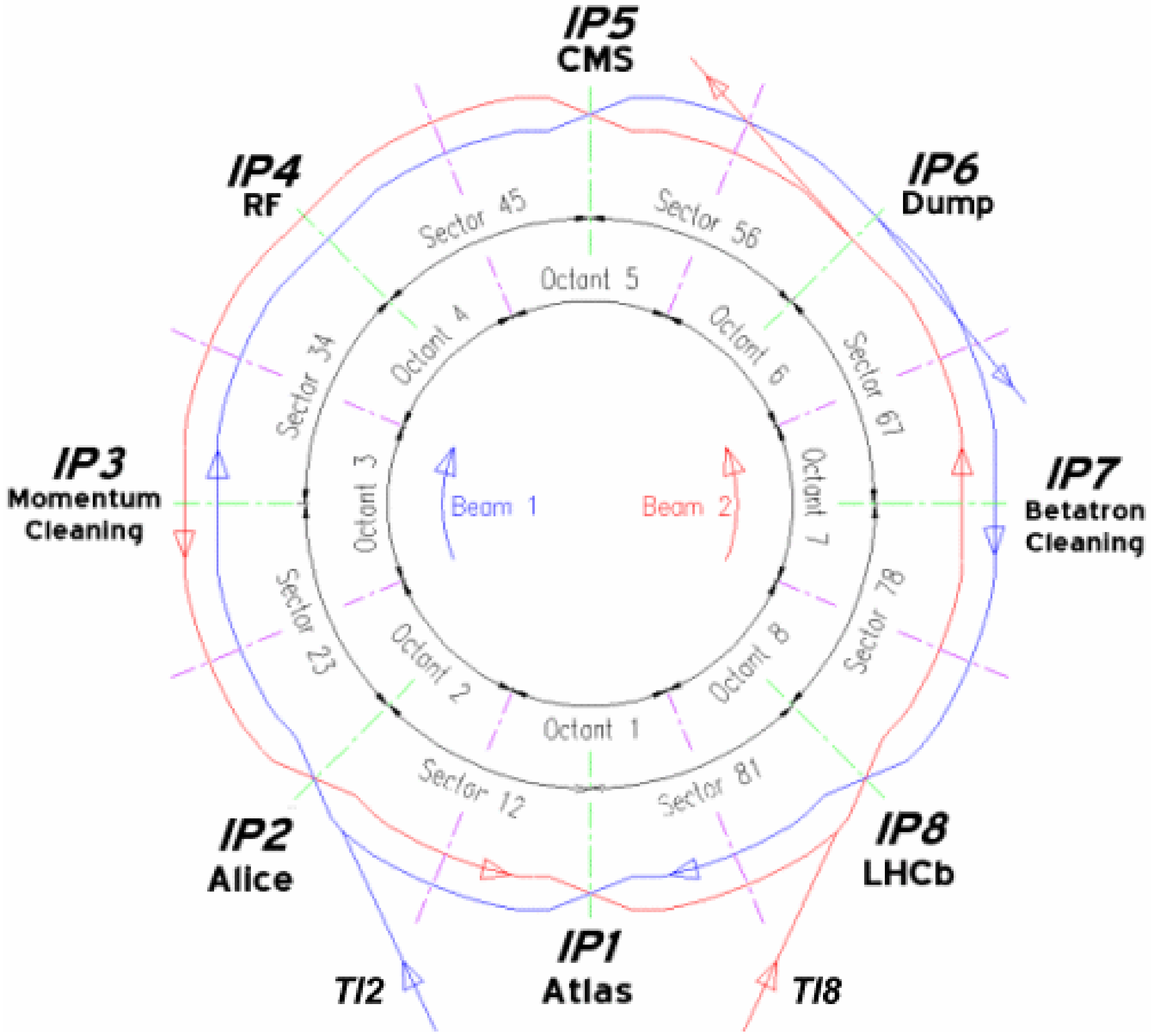


Figure 3.1: Schematic layout of the LHC tunnel [5]

3.2 The LHC Project

The Large Hadron Collider (LHC) is the next generation of particle accelerators built at CERN, investigating deeper into matter than ever before. As the most powerful particle accelerator, the largest machine and the largest cryogenic installation in the world it will push boundaries in science and engineering [6, 7].

The LHC will be housed in a circular tunnel of almost 27 km of circumference, approximately 100 metres below the surface (Figure 3.2). After dismantling the Large Electron-Positron Collider (LEP), the predecessor of the LHC, the civil engineering work required a number of local changes in order to make way for the installation of the LHC.

Two counter rotating beams of protons or heavy ions will be circulating in two separate

Figure 3.2: View of the LHC tunnel [8]

vacuum pipes, directed by a large number of superconducting magnets. Beam collisions will take place inside the four main detectors (experiments) of the LHC in order to find answers for the most fundamental questions concerning the understanding of our universe: supersymmetry, dark matter and the origin of mass. At injection, each beam will have an energy of 450 GeV, reaching 7 TeV after acceleration and hence giving a total of 14 TeV. The beams will be stored at high energy for approximately 10 hours during which the collisions will take place.

The LHC tunnel is divided into eight equal parts, the so-called octants (Figure 3.1) [9]. Situated in the middle of the octants are the interaction points, which are usually big caverns. Sectors range from one interaction point to the other, with the approximately 3.3 km long arc in the middle. The accelerator will bend along the arcs and has so-called long straight sections (LSS) at the interaction points. Technical galleries run in parallel to the main tunnel and alcoves exist in the form of smaller lateral tunnels; both are dedicated to the housing of required installations.

According to the purpose of the eight interaction points, the LHC can be divided into two main parts: on the one hand the machine and on the other hand the experiments. At points 1, 2, 5 and 8 the experiments ATLAS, ALICE, CMS, LHCb and TOTEM are found. The remaining points are occupied by the collimation system, the radio frequency system and the beam dump. Close to points 2 and 8 the beam injection system kicks the injection beams onto the orbit of the machine.

In the following sections LHC machine and experiments will be introduced briefly.

Moreover, the main systems operating the machine will be described.

3.2.1 The LHC Machine

In order to be able to operate the LHC at the energy of 14 TeV, some of the most impressive and innovative engineering achievements are involved in the project [9].

Superconducting magnets:

As the beams have a very high momentum, they require a very high magnetic field in order to bend them around the tunnel, thus superconducting magnets are needed. The magnets are cooled down to almost absolute zero (1.9 K), reaching the superconducting state. It allows the specially designed cables of the magnets to conduct current without resistance and produce the required magnetic field at zero electrical loss.

Cryogenic system:

In order to keep the magnets cold, a huge cryogenic system is required. A 1.9 K bath of superfluid helium at atmospheric pressure contains the magnets' windings, which will be cooled by low pressure liquid helium flowing in heat exchanger tubes along the magnets. A mass of 96 tons of liquid helium will be needed within the cryogenic system.

Vacuum system:

The beams are travelling in two separate beam tubes housed in the same physical structure of the magnets. In order to avoid collisions of the beams with residual gas particles and increase the lifetime and stability of the beams, the requirements for the beam vacuum are very high. The vacuum levels of the insulation vacuum systems for the cryomagnets and the helium distribution line are less stringent, but the necessity of three systems is a specific feature of the LHC.

Power Converter system:

The power converters feeding the superconducting magnets will supply large currents at low voltages, with different converter types providing up to 13 kA per circuit. Because of the constraints of the already existing infrastructure of the tunnel, reduced volume and high efficiency was a must. In total, there will be more than 1,700 power converters installed in the tunnel, with a total current supply of approximately 1,850 kA.

Machine Interlock systems:

As the energy stored in the beams (340 MJ each) and the magnet system (10 GJ without experiments) is unprecedented, the protection of the machine is of utmost importance. In case of failure, the beam has to be dumped and the stored energy dissipated safely in order to prevent equipment damage. Two systems, namely the powering interlock and the beam interlock system, communicate with several complex protection systems as well as other main LHC systems and assure the safe operation of the machine.

The following systems are found at different interaction points of the LHC, dedicated to different tasks in order to operate the machine [9].

Injection System (TI2 and TI8):

Following the accelerator complex of CERN, the particle packets will be injected into the LHC from the SPS (Super Proton Synchrotron) via the transfer lines TI2 and TI8. Injection kicker magnets and septum magnets deflect the beam horizontally and vertically onto the LHC orbit. In order to protect the equipment against any injection error, various elements, such as shielding elements and collimators, are installed.

Beam Cleaning and Collimation System (IP3 and IP7):

Due to the stored beam energy of 340 MJ each, any occurring beam losses can have severe effects for the equipment. In order to avoid the damage of equipment and ensure the survival of components against radioactive dose, the collimation system is designed to capture beam losses. At the interaction points 3 and 7 the beam losses are absorbed by different types of collimators [10].

Radio Frequency system (IP4):

As the beams are injected at only 450 GeV, they have to be accelerated until they reach their maximum energy of 7 TeV each. This is done by the so-called RF cavities at point 4 of the LHC, which capture the beam and transfer energy of radio waves to the beams (total RF power in the range of several MW). Each beam has its own independent acceleration system comprising eight superconducting, four normal conducting cavities and other corresponding equipment [4, 11].

LHC Beam Dump system (IP6):

The beam dumping system has to be the most reliable system of the LHC, as the high energy and therefore destructive power of the beams require a safe extraction in any case and, above all, in case of trouble. At point 6 of the LHC, extraction kicker magnets kick the beams off the orbit horizontally (0.33 mrad). Subsequently, they are deflected vertically (2.4 mrad) and guided towards the absorber block by additional magnets. The absorber blocks are situated at the end of two straight tunnels in a beam dump cavern, one for each beam, consisting of a graphite core assembly and associated steel and concrete shielding. This block is the only equipment of the LHC ready to receive the full power of the beams without damaging the machine [12].

3.2.2 The LHC Experiments

The collisions of the beams will take place in the four main experiments of the LHC, each dedicated to finding information on specific phenomena of particle physics. In addition, the fifth LHC experiment does not focus on particle collisions, but measures other physics phenomena along the LHC beams.

As the detectors have to be able to see up to 600 million collision events per second and trace particle trajectories, they have to be tremendously big. For example, the cavern housing the biggest experiment ATLAS is as big as the nave of Notre Dame Cathedral in Paris [13].

ATLAS (A large Toroidal LHC ApparatuS):

ATLAS is a general-purpose experiment designed to search for new particles such as Higgs bosons and supersymmetric particles. It will cover the largest possible range of LHC physics, investigating beyond the Standard Model of particles and forces. With approximately 1,800 physicists from more than 150 universities and laboratories in 35 countries working for ATLAS, it is one of the largest collaborations in the field of physics sciences [14, 15].

ALICE (A Large Ion Collider Experiment):

Recreating the conditions of the Universe just shortly after the Big Bang, ALICE will study heavy-ion collisions in order to explore the basic structure of ordinary matter. In such a way the current understanding of the evolution of the early Universe and the structure of the atom and its nucleus will be carried further [14, 16].

CMS (Compact Muon Solenoid):

As the second general-purpose experiment of the LHC, CMS is also designed to explore fundamental particle physics phenomena such as the discovery of the Higgs boson and supersymmetric particles. Moreover, additional subsystems are able to measure the energy and momentum of charged particles. Compared to the ATLAS experiment, CMS is smaller in size but weighs much more [14, 17, 18].

LHCb (Large Hadron Collider beauty):

The purpose of the LHCb experiment is to investigate the asymmetry between matter and antimatter in the Universe. As matter and antimatter were created in equal amounts in the Big Bang, physicists today are occupied by the question why the antimatter disappeared and where it has gone [14, 19].

TOTEM (TOTal cross-section and Elastic scattering Measurement):

Compared to the remaining experiments, TOTEM is rather small and moderately priced. Since the general-purpose experiments of the LHC are not able to cover all aspects of physics, its purpose is the measurement of the total proton-proton cross-section as well as elastic scattering and diffractive dissociation. With CMS as its host experiment, TOTEM will reach into the tunnel on both sides of the main experiment, accomplishing its task very close to the LHC beams [14, 20].

Chapter 4

Risk Analysis

Risk analysis and risk assessment form the two major phases of risk management, being separate, but closely related activities. While risk analysis is concerned with the identification of hazards and their frequency and consequences, risk assessment is needed for their quantitative evaluation, thereby being able to check on previously set goals or acceptance criteria (Figure 4.1) [21].

The basic guideline shown in Figure 4.1 does not only show the successive approach to risk analysis and assessment, but even leads one step further to the field of risk management and control.

Before starting an analysis it is of great importance to pay attention to analysis preparation and system definition. Without considering these two steps previously, the analysis will miss its objective, which certainly makes it hard to focus on where to go and what should and can be achieved. The analysis preparation is aiming at a full understanding of the system under examination and the collection of all necessary data. A definition of the objectives, the clarification of the applied methods, the procedure, the scope of resources and the precise determination of the object of analysis with its system boundaries are then needed for the system definition.

Once these steps are accomplished, the hazards of the system are identified and their frequency of occurrence and severity of consequences are determined. For these steps the already known risk analysis methods are indispensable, approaching the problem successively as well as providing guiding principles and overview. A risk analysis is then completed by depicting the revealed risks of the system in form of graphics in order to present them in a concise way.

Looking at the results of a risk analysis certainly raises the question of meaningful conclusions and resulting consequences for the system. Thus in order to be able to assess the results, it is necessary to compare them to previously set acceptance criteria. These criteria can either be legal requirements or might well be individual goals defined by the organisation itself. In case the study shows that the risks are above the acceptance criteria, risk reducing measures have to be considered and implemented. The intention of risk management and control is then to observe their implementation and control their consequences and effectiveness upon the system in a repetitive loop.

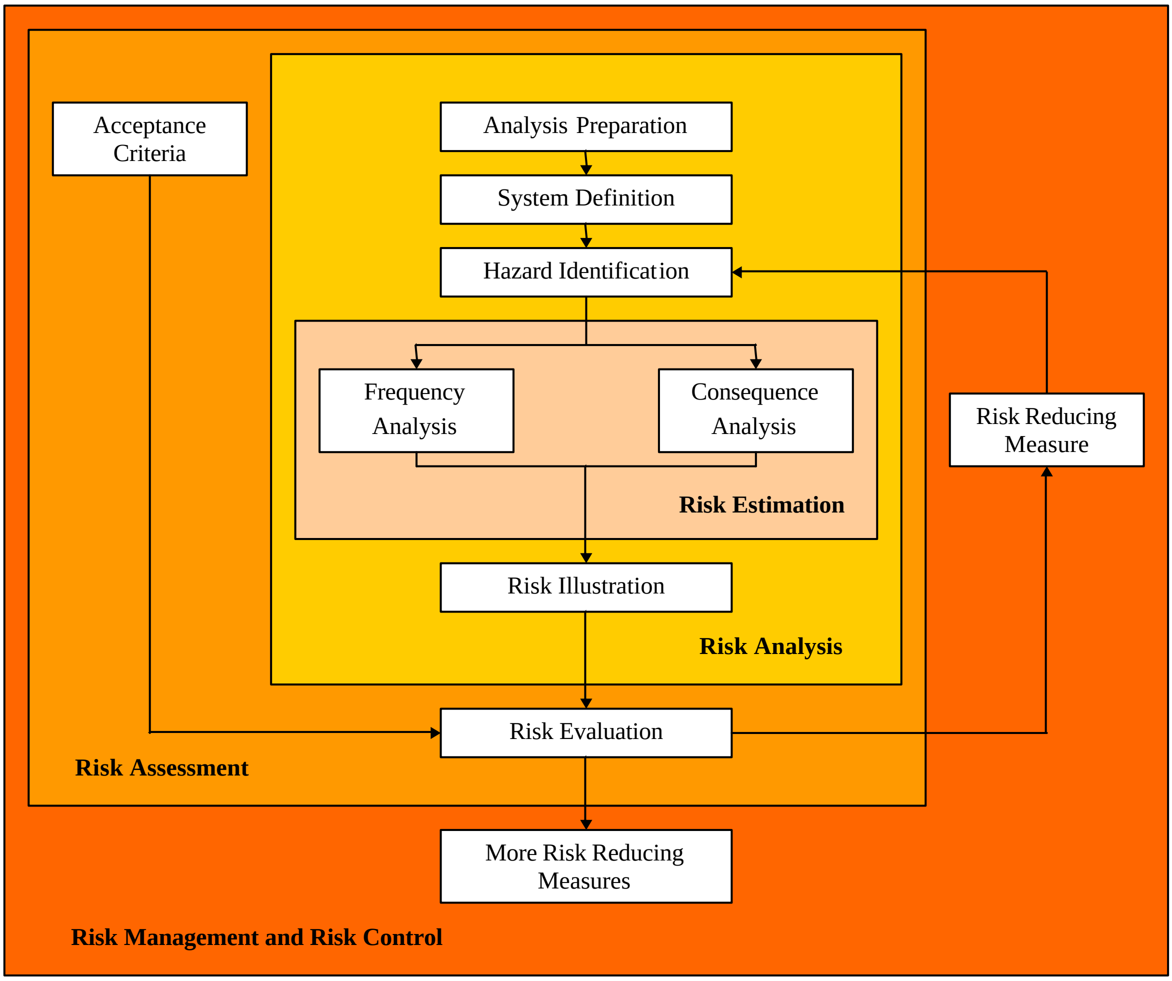


Figure 4.1: The procedure of risk analysis [21]

The present chapter is intended to give an insight into the field of risk analysis and risk assessment, which aims to provide a background for the subsequent following performance of the risk analysis of the LHC underground area.

4.1 Historical review

During World War II, the armed forces in the US as well as in Europe observed major problems with the reliability of their armament. After the war, studies were carried out in order to analyse the origin of these problems, and the first steps towards reliability and risk analysis were taken. The results revealed in the majority of cases that the equipment's availability was far too low, and the cost for maintenance and repair during the lifetime of the equipment exceeded the cost of production by far. Although not yet performed in a systematical and consistent way, these early studies marked the beginning of the discipline of reliability and risk analysis [22].

In the 1960's the aerospace and nuclear industries launched their first attempts on setting goals for their safety policy and quantifying the risks of success or failure of their endeavours. In the US aerospace sector this rethinking was raised by an accident of the Apollo test AS-204 in 1967, which resulted in enormous additional costs and provoked a considerable loss of public support. The results of early estimates on the probability of catastrophic failures posed a threat to the plausibility of the entire space programme.The probability results were very high, and means for identifying these probabilities were not yet available and limited the possibilities of taking the step from mere qualitative studies to meaningful quantitative analysis. NASA has since been working in the field of quantitative risk analysis, and with its help could even reassure the US Congress that the money spent on shuttle development has not been in vain.

Although the basic methods of probabilistic risk analysis originated in the aerospace industry, the nuclear sector was then the first industry to actually carry out a full scale risk analysis. The Reactor Safety Study WASH-1400 was published by the US Nuclear Regulatory Commission (NRC) in 1975, which included a complex study of accident consequences. The reception of this study in the scientific world was very controversial, and ended in an alienation of the NRC itself following review reports which stated that the conclusions of the Reactor Safety Study were “greatly understated”. With this development the future of probabilistic risk analysis did not look very bright. However, when in 1979 the Three Mile Island - 2 accident happened and it was revealed that the Reactor Safety Study had actually predicted this particular accident scenario, two independent analyst teams recommended to make greater use of probabilistic methods in judging nuclear plant risks [23].

The methodology of probabilistic risk analysis has since developed very rapidly, which is approved by numerous publications during the last 25 years extending the subject from the aerospace and nuclear sectors to industries as different as business management and banking. New approaches to risk analysis and assessment have been developed, now taking into account many different aspects of risk, and trying to achieve far more demanding safety goals set to protect people and the environment as well as the business itself.

4.2 Definitions

In the field of probabilistic risk analysis, terms and definitions are often used with different meanings, depending on the type of industry being analysed and also on the persons in charge and their background. In order to avoid confusion and misunderstanding, the terms with their meanings used throughout this work will be subsequently given [24–27]:

Hazard describes a condition or activity, which has the potential of causing a dangerous or undesired event. In this way, a bucket of petrol considered on its own would not yet present any hazard, but concretising this danger to people, environment or machines does result in a serious hazard.

Risk (R) is a measure for the magnitude of a hazard, covering two parameters: the expected frequency (F) and the possible consequences (C) of an undesired event. The definition

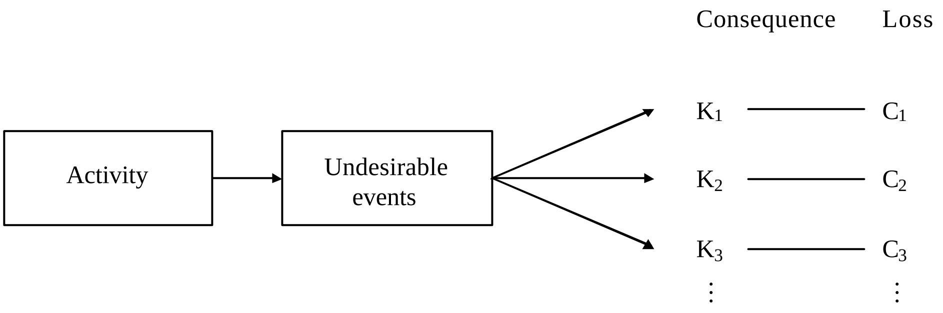


Figure 4.2: General risk model [24]

of risk is then:

$$R = F \cdot C \tag{4.1}$$

Or for an activity causing consequences of different magnitude i with their corresponding frequencies:

$$R = \sum F_i \cdot C_i \tag{4.2}$$

The consequences of an undesirable event are usually very diverse concerning their scale of measurement. For example, the bursting of a pressure vessel can be caused by a subsystem or component failure and results in fatalities, personal injuries, environmental damage and/or loss of equipment or economic value. In order to be able to compare these consequences with each other, they would have to be converted into a numerical loss using the same scale of measurement. However, this conversion is difficult to undertake and is therefore replaced by separate analyses of the different groups of consequences (Figure 4.2).

Graphically, the relation between the frequency and the consequence of an undesirable event is represented in a so-called risk curve (Figure 4.3). The consequence is displayed on the horizontal axis, in ascending order from the least to the worst; the corresponding frequency is displayed on the vertical axis. If the relation is shown in the form of a complementary cumulative distribution curve, as illustrated in Figure 4.3, the curve gives the frequency of an undesired event to produce a damage of the magnitude X or greater. As the definition of risk as pointed out in equation (4.1) gives only information about one frequency/consequence pair, it is suggested to obtain a risk curve for assessing risks whenever possible.

Risk analysis is the process of systematically analysing risk, consisting of the following steps: system definition, identification of hazards, frequency and consequence analysis and illustration of risk (possibly in a risk curve). The definition of **risk assessment** is the quantification of the frequency of an undesired event and its measurable consequences, as already addressed above. Moreover, the comparison of these results with previously defined goals to achieve or acceptance criteria. This definition shows that risk assessment and risk analysis are very closely related to each other, and their meanings can therefore be easily confused.

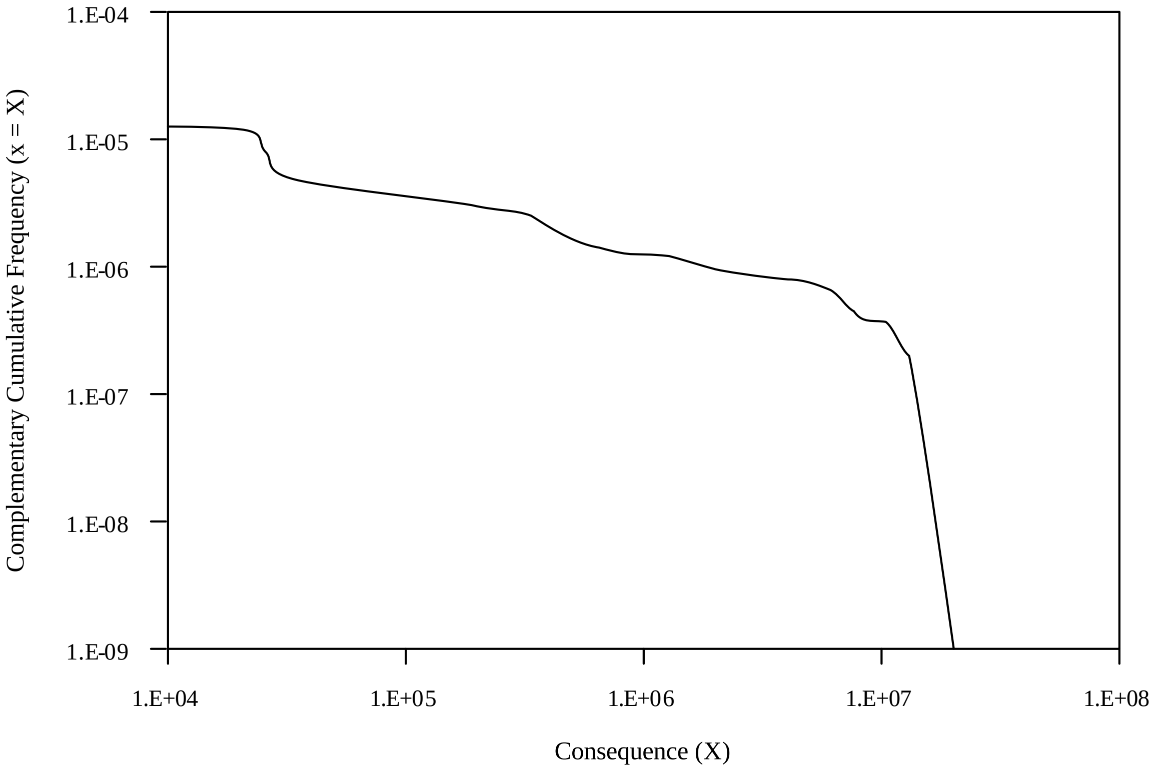


Figure 4.3: Risk curve

The term **risk management** summarises all before mentioned definitions and concludes the step-by-step process with the control and communication of risk. In case the assessment results in unacceptable risks, adequate risk reducing measures are introduced and their execution and effect on the system are being observed. Risk management must therefore be seen as a continual mission and be integrated in the activities of an organization or company.

Reliability is defined as the ability of a component or a system to perform a specific function within a given time period at default conditions, expressed as a probability. Similar to the definition of a risk analysis, the **reliability analysis** is a systematic analysis of the reliability of a component or a system. It is essentially the prediction of the frequency of an undesired event, which connects closely the terms of risk and reliability analysis, as the latter might form part of a risk analysis. When executing a reliability analysis, the main focus is on the component failure. On the contrary, a risk analysis rather focuses on the identification of undesirable events and their consequences for the system, thus resting on component reliability.

In contrast to reliability, the **availability** of a component or a system includes maintenance, thus gives the probability that at a specific point in time the component or system will be in a functional state.

In IEC Standard 61508, “Functional safety of electrical/electronic/programmable elec-

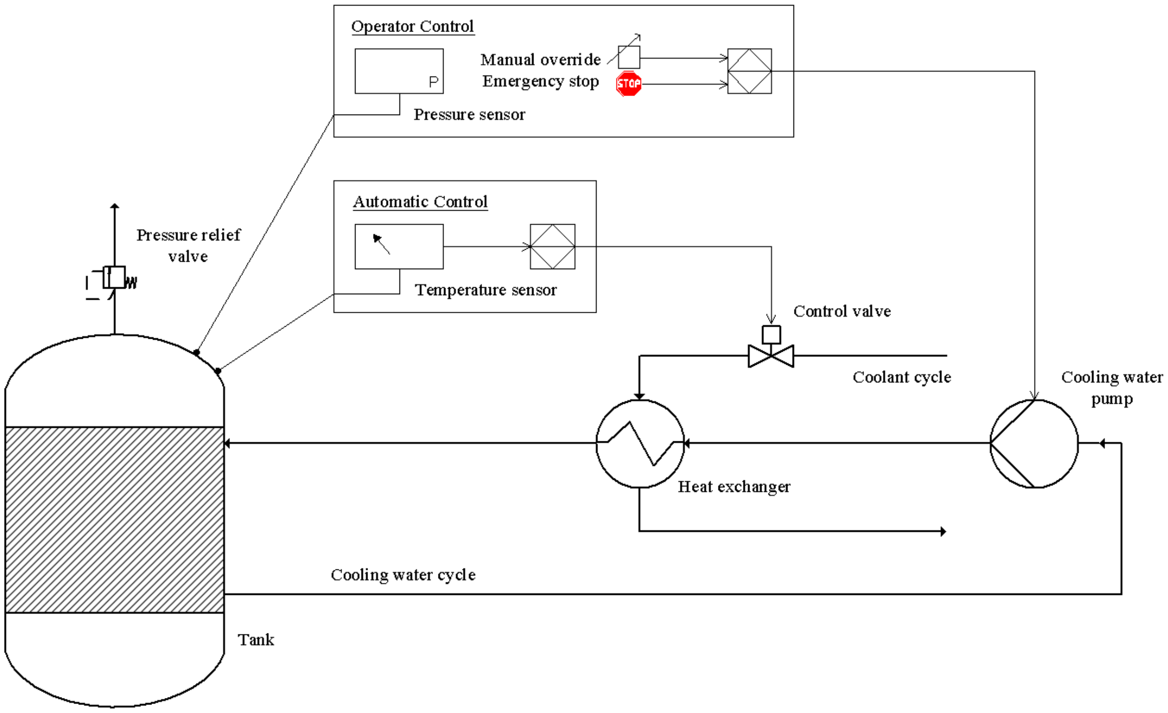


Figure 4.4: Exemplary plant

tronic safety-related systems", the term **safety** is defined as "freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment" [28].

4.3 Methods, Application and Justification

The intention of the following chapter is to give an overview of some of the most common reliability and risk analysis methods. Their basic principles and their execution will be explained, and the reasons for choosing one of these for the present risk analysis will be discussed.

In order to point out the differences between the methods, their applications will be demonstrated with reference to the following exemplary plant (Figure 4.4, following [21]): The system comprises a tank in which an exothermic reaction takes place and therefore has to be cooled, a heat exchanger and a cooling water pump. The amount of required coolant for the heat exchanger is regulated by a control valve which is connected to the cooling water pipe via a temperature sensor. In case the pressure sensor in the tank indicates an overpressure, the operator can step in and increase the output of the pump. In case of emergency, the operator can stop the pump via an emergency stop switch. Moreover, the tank is equipped with a pressure relief valve.

Guide Word	Meaning
NO/NOT	Negation of intention
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative increase
PART OF	Qualitative decrease
REVERSE	Logical opposite of intention
OTHER THAN	Complete substitution

Table 4.1: HAZOP - Commonly used guide words [22]

4.3.1 Hazard and Operability Study

The Hazard and Operability Study (HAZOP) [22,27] was designed for the qualitative analysis of the processes in a technical system by means of so-called guide words. The application of these guide words should identify the causes and effects of a deviation from the intended design condition. By this means possible hazards in the system and caused by the system, as well as the causes of operational failures and abnormalities compromising regular production can be discovered. Originally HAZOP was aimed at continuously producing plants, but by appropriately adapting the guide words it can also be applied to discontinuous processes.

4.3.1.1 The Principle of HAZOP

In order to carry out a HAZOP analysis, a full description of the process and the engineering line diagram of the plant must be available. By questioning every part of it, the deviations from the design intent are supposed to be revealed, and their causes and consequences can be examined. Attention has to be paid to the required documentation, as it is absolutely necessary that all data are up-to-date and consistent. At this point it is important to mention that HAZOP is not meant to be a compensation for good design. In case the analysis shows a high number of basic design faults, there is something fundamentally wrong and the engineering plan should be reassessed.

Commonly used guide words and their meanings are given in Table 4.1. In order to give an example of how to apply these guide words, some possible process parameter deviations of a technical system are listed in Table 4.2. It must be pointed out that this basic set of guide words has to be changed naturally according to the different requirements of the process parameters. However, their basic meaning as given in Table 4.1 does not change.

Process Parameter	**Deviation**
Flow	**NO** flow **REVERSE** flow **MORE** flow
Temperature	**HIGHER** temperature **LOWER** temperature
Pressure	**HIGHER** pressure **LOWER** pressure
Volume	**HIGHER** level (in a tank) Volume rate changes **FASTER** than expected **PROPORTION** of volumes is **CHANGED**
Composition	**MORE** component A **LESS** component B **MISSING** component C
pH	**HIGHER** pH **LOWER** pH
Viscosity	**HIGHER** viscosity **LOWER** viscosity
Phase	**WRONG** phase **EXTRA** phase

Table 4.2: Process parameter deviations for HAZOP [27]

4.3.1.2 Execution of HAZOP

In order to facilitate the performance of a HAZOP analysis and to provide a guideline throughout the whole process, a HAZOP form is filled out. It contains all features ranging from the guide word and its corresponding deviation over possible causes and consequences to necessary actions to be taken. Following this form step by step for each process parameter enforces a gradual way of thinking and by this means helps to avoid ignoring important aspects of the technical system.

Table 4.3 shows one possibility of filling in a HAZOP form. In this example, any cause can result in any consequence for each guide word.

4.3.2 Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) [29] is another major method of identifying the hazards of a technical system. Different from the HAZOP method, the FMEA systematically reviews the system on a component-by-component basis. So starting from the possible failure

Guide Word	Deviation	Possible causes	Consequences	Action required
NO	No flow of cooling water	Blockage in the pipe before the tank	No cooling of the tank	Install flow indicator in the cooling water cycle
		Blockage in the pipe after the tank	Overpressure in the tank, potential explosion	Redundant cooling water cycles
		Rupture of the pipe	Release of cooling water	Regular maintenance measures
		Failure of the pump	Overheating of the pump	Redundant pumps
				Automatic shut-down of the pump at maximum capacity and shut-down of the system
LESS	Decreasing flow of cooling water	Failure of the pump	Reduced or no cooling of the tank	Automatic shut-down of the pump at maximum capacity and shut-down of the system
		Failure of heat exchanger	Overheating of the pump	Regular maintenance measures
		Partial blockage	Overpressure in the tank	Redundant pumps
		Rupture of the pipe	Negative effects for the process cycle (incorrect process parameters)	Install flow indicator in the cooling water cycle
			Release of cooling water	Redundant cooling water cycles
MORE	...	...	...	...
NO	No flow of coolant	Blockage of the pipe	No cooling of the tank	Regular maintenance measures
		Rupture of the pipe	Overpressure in the tank, potential explosion	Install flow indicator in the coolant cycle
		Failure of heat exchanger	Release of coolant	Install temperature alarm device (above maximum cooling water temperature)
		Failure of temperature sensor		Redundant sensors
		Failure of control valve		
LESS	...	...	...	...

Table 4.3: HAZOP form (following [22])

modes of each component, the effects on the adjacent units and then the whole system are detected. Experience shows that 80% of failures, which occur during the lifetime of components, are due to weak points in their design and development [21]. Thus by starting the analysis at a component level and bearing in mind these elementary failure modes, adequate safety measures for the whole system can be proposed.

A further development of the FMEA, which provides the analyst not only with a qualitative, but also a quantitative analysis, is the Failure Modes, Effects and Criticality Analysis (FMECA). The identified failure modes are assessed by means of two more parameters, the frequency of occurrence of a failure mode and the severity of its consequences. Depending on the needs of the study, either FMEA can be carried out on its own or in combination with a criticality analysis.

4.3.2.1 Execution of FMEA

Guidance on FMEA and FMECA is given in BS 5760, "Reliability of systems, equipment and components, Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA)", out of which the general principles to be illustrated in this work are taken.

Like for the HAZOP method, a FMEA form is filled out in order to proceed gradually and to maintain overview throughout the study (Table 4.4). In this way all components are listed, their possible failure modes identified and then examined with respect to possible failure causes and consequences.

As a component can fail in more than one way, and moreover the failure causes might as well be multiple, it is very important to deal with each of these parameters in detail. The list of failure modes of a single component can be very extensive, as shown in a list of generic failure modes (Table 4.5). Moving on from a list of different failure modes to their possible causes is then again a significant step with regard to the possibly following criticality analysis, for which, depending on the identified failure causes, the frequency of occurrence is estimated.

4.3.2.2 Criticality Analysis

When analysing a system with a view to criticality, the previous worksheet for the FMEA is extended by two more columns, frequency of occurrence and severity of consequences.

By assigning frequency and severity to each failure mode of a component, a so-called risk matrix can be obtained, in which the frequency is displayed on the vertical axis and the severity on the horizontal axis. Plotting all frequency - severity pairs results in a visual presentation of the relative importance of each failure mode. When the area of the matrix is divided into four zones (A, B, C and D), as shown in Figure 4.5, the pairs located in zone D indicate those cases with the highest frequency of occurrence and the most significant consequences. Therefore these cases are revealed as those with the highest priority in terms of corrective actions.

Item Ref	Item Description	Failure Entry Code	Failure Mode	Possible Causes	Possible Consequences	Compensating Provisions
1	Pump	1.1	Leakage	Faulty sealing, wear, corrosion	Reduced or no cooling, overpressure in the tank, incorrect process parameters, release of cooling water, overheating of the pump	Flow indicator in the cooling water cycle, corrosion protection, redundant pumps
		1.2	Blockage	Impurities	No cooling, overpressure in the tank (potential explosion), overheating of the pump	Automatic shut-down of the pump at maximum capacity and shut-down of the system, filter and flow indicator in the cooling water cycle, redundant pumps
		1.3	Breakdown	Failure of the engine, power failure	No cooling, overpressure in the tank (potential explosion)	Regular maintenance measures, redundant pumps
2	Heat exchanger	2.1	Leakage (cooling water and coolant)	Faulty sealing, wear, corrosion	Reduced or no cooling, overpressure in the tank, incorrect process parameters, release of cooling water and coolant	Temperature alarm device, flow indicators in both cycles, corrosion protection
		2.2	Blockage (cooling water and coolant)	Impurities	No cooling, overpressure in the tank (potential explosion), overheating of the pump	Temperature alarm device, flow indicators in both cycles, filters in both cycles
3	Control valve	3.1	Fails open	Mechanical breakdown	Incorrect process parameters	Flow indicator in the coolant cycle
		3.2	Fails closed	Mechanical breakdown	No cooling, overpressure in the tank (potential explosion)	Flow indicator in the coolant cycle
		3.3	Opens/closes partially	Faulty data transmission, mechanical breakdown	Incorrect process parameters	Flow indicator in the coolant cycle
		3.4	Leakage	Faulty sealing, rupture, wear, corrosion	Incorrect process parameters	Regular maintenance measures, corrosion protection
4	...	4.1	...	...	...	...

Table 4.4: FMEA worksheet (following [29])

1	Cracked/fractured	21	Binding/jamming
2	Distorted	22	Loose
3	Undersize	23	Incorrect adjustment
4	Oversize	24	Seized
5	Fails to open	25	Worn
6	Fails to close	26	Sticking
7	Fails open	27	Overheated
8	Fails closed	28	False response
9	Internal leakage	29	Displaced
10	External leakage	30	Delayed operation
11	Fails to stop	31	Burned
12	Fails to start	32	Collapsed
13	Corroded	33	Overloaded
14	Contaminated	34	Omitted
15	Intermittent operation	35	Incorrect assembly
16	Open circuit	36	Scored
17	Short circuit	37	Noisy
18	Out of tolerance (drifted)	38	Arcing
19	Fails to operate	39	Unstable
20	Operates prematurely	40	Chafed

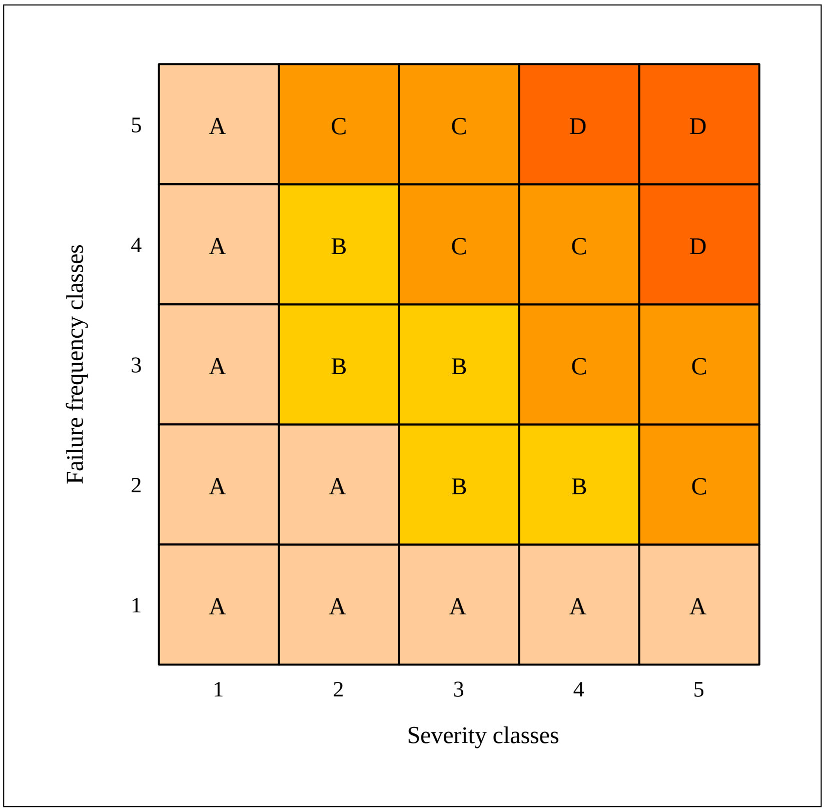
Table 4.5: Generic failure modes [29]

In reference to the exemplary plant, an assessment of a blockage of the pump (failure entry code 1.2 in Table 4.4) could reveal e.g. a frequency of class 4 and a severity of class 5. These values would place it into zone D of the risk matrix and therefore rate it as a failure mode for which improvement measures have to be implemented without the least delay. On the contrary, a control valve failing open (failure entry code 3.1 in Table 4.4) may occur less often and may have less severe consequences for the system, thus is situated in zone A of the risk matrix.

4.3.3 Fault Tree Analysis

After analysing the system, identifying inherent hazards and studying possible consequences by means of a HAZOP or FMEA/FMECA, the next step is a failure frequency analysis. Technical systems are usually very complex, and the interaction and linking of the components are difficult to determine. It is therefore rather impossible to identify the frequency of a system failure without reverting to the history leading up to it.

A fault tree analysis (FTA) [22, 23, 30] is a graphical method which allows the analyst



	1	2	3	4	5
5	A	C	C	D	D
4	A	B	C	C	D
3	A	B	B	C	C
2	A	A	B	B	C
1	A	A	A	A	A

Figure 4.5: Risk matrix for FMECA [29]

to illustrate the events which result in a defined system failure. By applying simple logical relationships in order to define the behaviour of components, it is possible to reproduce the system and represent it in a methodical structure. Boolean algebra is then used to calculate a system failure rate based on identified component failure rates.

4.3.3.1 Fault Tree Elements and Symbols

The basic elements for the construction of a fault tree are the top event, intermediate events, basic events and the logic gates. The top event is usually defined as an undesired event. As the failure of the whole system is hard to specify, it is rather defined as the failures of certain functions which significantly affect the performance of the entire system, i.e. fire, explosion, toxic release. Starting from this top event, the fault tree is then developed top down over intermediate to finally basic events. These basic events represent the failure of a component and are not further developed. All elements and their graphical representation can be found in Table 4.6.

In order to link all elements of a fault tree together, logic gates are needed. A gate always consists of several input events and one output event. The logic gate then illustrates how the input events are interacting with each other in order to result in the output event. The two main gates used are the AND gate and the OR gate. The output event of an AND

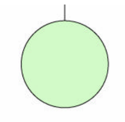
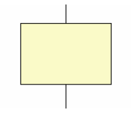
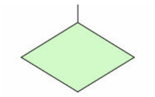
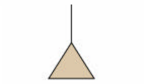
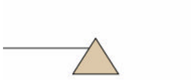
Symbol	Function	Description
	Basic event	Event requiring no further development
	Intermediate event	Event which occurs due to antecedent causes acting through a logic gate
	Undeveloped event	Event for which further subdivision was not done
	Transfer in	Symbol indicating that the tree is developed further at the corresponding Tranfer out symbol
	Transfer out	Symbol indicating that the portion of the tree below the symbol is to be attached to the main tree at the corresponding Transfer in symbol

Table 4.6: Elements of a fault tree analysis [22, 30]

gate only occurs if the input events all occur at the same time. As opposed to this, the condition for an OR gate is that at least one out of all input events must occur in order to cause the output event to happen. There are a small number of other gates, shown and explained in Table 4.7.

4.3.3.2 Fault Tree Construction

The first step in the procedure of constructing a fault tree is the definition of the system under discussion with its boundaries and the determination of a top event. As the fault tree is a logic representation of reality, it is important to define the system very precisely. Depending on the type of system (i.e. system with a reactor, safety system) and the purpose of the analysis, the boundaries have to be set in a reasonable way in order to avoid leaving out important components or, on the contrary, taking too many components into account which are not directly associated with and might not even influence the top event.

When the top event is defined, the tree is developed top down by finding all necessary causes, which should be components where failures provoke the top event to occur. This is done step by step, first the immediate events which are then further developed and therefore become more detailed, finally leading to the basic events. It is very important to describe the state of each event, intermediate as well as basic, in order to avoid misunderstanding and confusion (Figure 4.6) [23].

Guidelines for the construction of a fault tree are given in [Kumamoto and Henley, 1996, p. 184]:

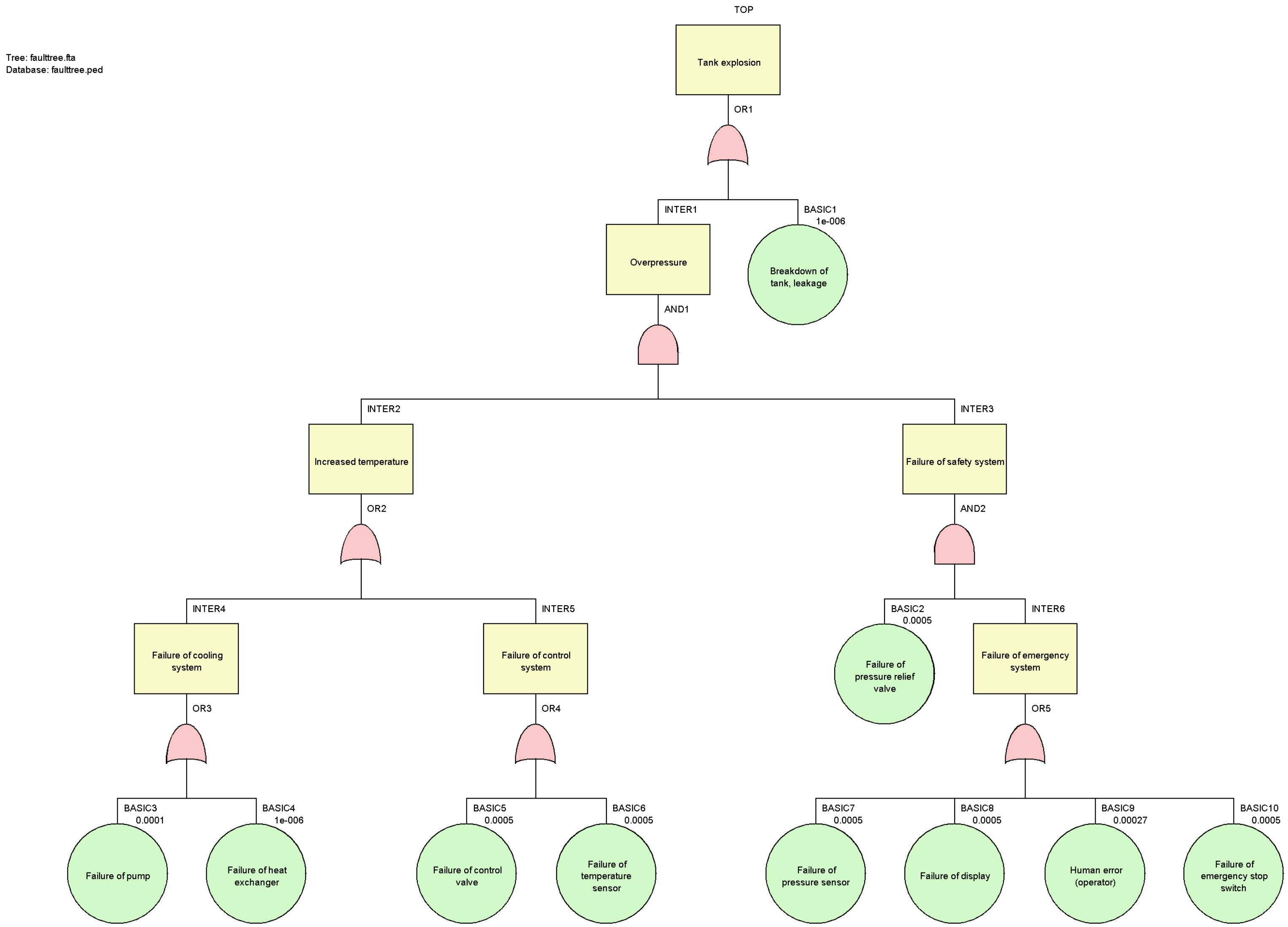


Figure 4.6: Quantitative analysis of a fault tree

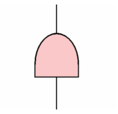
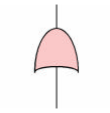
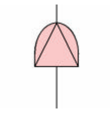
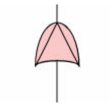
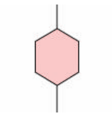
Symbol	Function	Description
	AND gate	Event occurs only if all input events occur simultaneously
	OR gate	Event occurs if one or more of the input events occur
	PRIORITY AND gate	Event occurs only if all input events occur in a specific sequence (specified by conditioning event to the right of the gate)
	EXCLUSIVE OR gate	Event occurs only if one of the input events occurs alone
	INHIBIT gate	Event occurs only if input event attached to the right occurs while the event attached to the bottom and forming the condition is in force

Table 4.7: Symbols of a fault tree analysis [22, 30]

1. Replace an abstract event by a less abstract event.
   Example: “motor operates too long” versus “current to motor too long”.

2. Classify an event into more elementary events.
   Example: “tank rupture” versus “rupture by overfilling” or “rupture due to runaway reaction”.

3. Identify distinct causes for an event.
   Example: “runaway reaction” versus “large exotherm” and “insufficient cooling”.

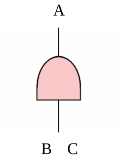
4. Couple trigger event with “no protective action”.
   Example: “overheating” versus “loss of cooling” coupled with “no system shutdown”.

5. Find cooperative causes for an event.
   Example: “fire” versus “leak of flammable fluid” and “relay sparks”.

6. Pinpoint a component failure event.
   Example: “no current to motor” versus “no current to wire”. Another example is “no cooling water” versus “main valve is closed” coupled with “bypass valve is not opened”.

4.3.3.3 Quantitative Analysis

When a fault tree is analysed in a quantitative way, probability data for each basic event are required. Based on that, probability values of the intermediate events can be calculated according to the logic structure of the tree, finally producing the probability of occurrence

Symbol	Boolean Algebra Relation	Probability Relation
	A = BC	P(A) = P(B)P(C)

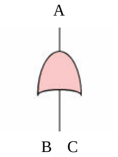
	A = B + C	P(A) = P(B) + P(C) - P(B)P(C)
		Provided that the probabilities are low:
		P(A) $\approx$ P(B) + P(C)

Table 4.8: Probability relations for a quantitative fault tree analysis [22]

of the top event. The probability relations for the two main logic gates of a fault tree are shown in Table 4.8.

If a basic event occurs more than once and in case the tree is large with e.g. 20 or more basic events, the help of computer programmes is needed.

The quantification of the fault tree in Figure 4.6 has been done manually following the probability relations in Table 4.8. After defining the basic events' failure probabilities, the top event probability has been calculated at $1.00 \cdot 10^{-6}$.

4.3.4 Event Tree Analysis

Compared to a fault tree analysis, an event tree analysis (ETA) [22, 26] does not present the events leading up to, but shows the possible consequences of a failure of the system. It is developed bottom-up, so starting from an initial event all possible outcomes after reaction of subsequent safety-engineering systems are illustrated. If it is used in a qualitative way, the result is a list of possible states of the system after an initiating event. However, used in a quantitative way, also the probability of each individual outcome can be determined.

4.3.4.1 Event Tree Construction

The first step to the construction of an event tree is the definition of an initial event. This can be either an accident due to the failure of a system component or an external impact on the system, i.e. explosion, toxic release, flooding. The second step is the definition and identification of all safety systems which could be triggered after the accident. They are arranged in their order of coming into operation as headings of the event tree. Once this is done, the possible consequences following the initial event are deduced and pictured in so-called branches, each representing a different sequence of events and resulting in a defined final system state. The initial event is usually placed on the left, and the branches are drawn

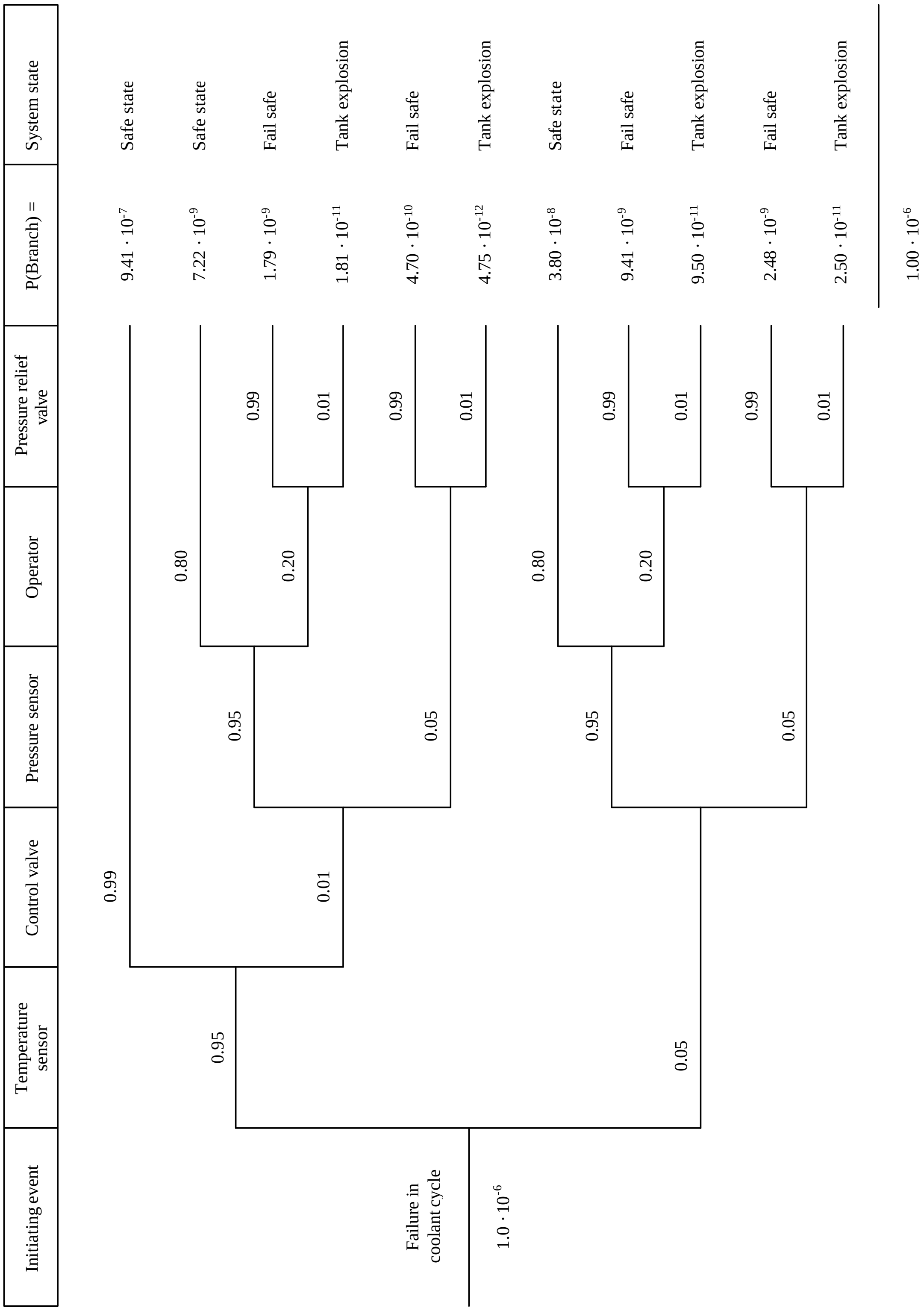


Figure 4.7: Quantitative analysis of an event tree

Criteria	HAZOP	FMEA	FTA	ETA
Applicability	1	2	2	0
Significance	1	1	2	0
Traceability	1	2	2	0
Σ	3	5	6	0

Table 4.9: Overview of risk analysis methods

to the right (Figure 4.7).

In order to be able to draw the branches it is necessary to define one success and one failure state for each safety system. So in case the safety system would be a pressure relief valve, the corresponding success state would be the safe release of overpressure from the tank and the failure state the breakdown of the valve resulting in a tank explosion. Each of these two states gives a branch of the tree. Once the states for each system are defined, the accident sequences linked to the initial event can be obtained step by step by applying binary logic to each safety system which is demanded. The final system states are then a combination of either success or failure of each safety system during the development of the tree. The standard tree structure is thereby defined with the success states above the failure states.

4.3.4.2 Quantitative Analysis

The objective of evaluating an event tree is the determination of the probability of each accident sequence and therefore the probability of all possible system states, provided the initial event has occurred.

For the calculation, the conditional probabilities of success and failure states of each safety system have to be defined and the frequency of occurrence of the initial event has to be known. Then this frequency has to be multiplied by the conditional probabilities of the safety systems for each branch. In this manner, the frequencies of all possible final system states are determined. The sum of all these frequencies has to produce the frequency of the initial event, the conditional probabilities have to sum up to 100 (Figure 4.7).

4.3.5 Risk Analysis Methods at a Glance

Table 4.9 gives an overview of the previously introduced risk analysis methods in view of the problem at hand, the fire risk due to faulty electrical equipment in the LHC tunnel. The three criteria are assessed for each method and the rating is added up, thereby revealing the most adequate technique. For the assessment, the subsequent classification is used: good (2), medium (1), bad (0).

In order to be able to judge the risk analysis methods on the basis of the three criteria, they will be explained and discussed briefly.

The highest score for applicability is assigned to a method if its procedure and intended outcome match the requirements for the present problem. A method is applicable to assessing the fire risk in the LHC tunnel if the results can actually reveal frequency and consequences of an incident. Determining the significance of a method then goes one step further and has to decide if the outcome does have a meaning for the analysis. Although applicability might be good, the significance of the results could turn out not to be meaningful for the assessment of the situation. The highest score for significance can only be assigned if an actual probability of having a fire in the LHC tunnel can be determined. Finally, traceability of a method is judged in order to evaluate how easily the procedure can be traced and understood.

The rating shows that a fault tree analysis as well as a Failure Modes and Effects Analysis are considered the best options for the analysis of the LHC fire risk. On the other hand, a Hazard and Operability Study and an event tree analysis are less appropriate.

With the least possible score the event tree analysis is not suitable for analysing and assessing fire risk. It is a method intended to reveal the consequences of an initial event (e.g. fire) relating to the answers of subsequent safety systems. This means that by definition it cannot be applied for determining the probability of fire risk in the tunnel.

Conducting a Hazard and Operability Study would in principle be possible; however, applying guide words to electricity in respect to electrical equipment complicates their specific definition. Moreover, faulty electrical equipment does not only include failures related to a deviation of the power supply, but also failures referring to mechanical malfunctions. The significance of a HAZOP study for the present problem is only minor, as no quantitative assessment is possible. Traceability of this method would be slightly difficult, as the question of how to apply guide words to electricity is not always clear.

With a score of 5 points out of 6, the Failure Modes and Effects Analysis is certainly applicable to the problem of determining the fire risk in the LHC tunnel. A controlled way of defining failure modes of the system as well as their possible causes and consequences provides a list of events which can occur. The quantitative analysis by means of frequency and consequence analysis then allows for a classification of failures and the setting of priorities regarding improvement measures. However, in terms of significance a FMEA would not be able to deliver suitable results, as it is not possible to estimate a total probability of fire.

This problem leads directly to the last method to be discussed, the fault tree analysis. The significance of this technique was judged slightly better than of the FMEA, because as an overall result a system failure rate can be calculated. Developing the tree top-down with fire in the LHC tunnel as the top event leads to the basic events to which failure rates can be assigned. With the help of Boolean algebra the probability of a fire in the LHC underground can then be calculated.

The highest scores for applicability, significance and traceability were assigned to the fault tree analysis, and therefore it will be chosen for analysing the present problem. However, since it would not be able to provide with a concise and easily understandable listing of system failure modes and their possible causes and consequences, it will be coupled with a Failure Modes and Effects Analysis.

4.3.6 Justification

As illustrated in the previous chapters, an extensive risk analysis and assessment requires a precise knowledge of the entire system. Depending on the purpose of the study and the available resources, different risk analysis methods can be applied. Before going into the detailed analysis, basic questions such as clarification of methods, procedure, scope of resources, definition of objectives, determination of the object of analysis and its system boundaries, and specification of the system status to be analysed have to be considered.

The present chapter gives explanations concerning the development from original ideas of an overall risk analysis of the LHC underground, including all subsystems, to the actual subject of this thesis.

In the history of CERN, several risk analyses for the detectors of the Large Electron-Positron Collider have been carried out [31–34]. Although for some of those known risk analysis methods have been used, they were not presented in a detailed way, showing progressively the development from hazards over causes and consequences to resulting safety measures. Others were undertaken only by compiling lists of possible hazards in combination with the already existing safety measures and then deriving arrangements for improvement. As in the 1980's the risk analysis methods were not yet as mature and in-depth as we know them today, the way of approaching the problem by logical listing of hazards and structuring of the system is understandable. However, without thinking extensively about possible causes and consequences of failures, the accident scenarios cannot be judged correctly and may not lead to the deduction of the actually necessary safety measures. Moreover, the following of a certain technique and its guidelines would help to keep an overview and not to overlook important facts.

For the LHC, the situation is slightly different. Public interest in safety as well as the scope of the field of risk analysis has increased. CERN has to try for safe operation of the machine in view of public acceptance and the protection of people, environment and equipment from major hazards. Risk analyses for single systems of the LHC, e.g. the cryogenic system, have been undertaken in order to arrange appropriate safety measures in case of operating problems [35]. However, the interaction with other systems and a view to the entire system of the LHC was not approached.

The original idea of the present study was to prepare an extensive risk analysis for the entire LHC tunnel and its systems. Following the basic guideline (Figure 4.1), the first approach to define the system was done as shown in Figure 4.8.

As the LHC is a complex system, it was essential to reduce the boundaries in order to be able to consider the LHC as a whole. Thus the vital subsystems were chosen and classified in three different groups by their function and objective for the whole system, which is mostly corresponding to the conventionally used classification at CERN. The three main groups are therefore the Machine Operation system, the Machine Protection system and the General Safety system.

The Machine Operation system includes all systems which are necessary to operate the machine, thus superconducting and conventional magnets, powering network and electrical distribution, power converters (PCs), cryogenics system, vacuum system (VAC), cooling and

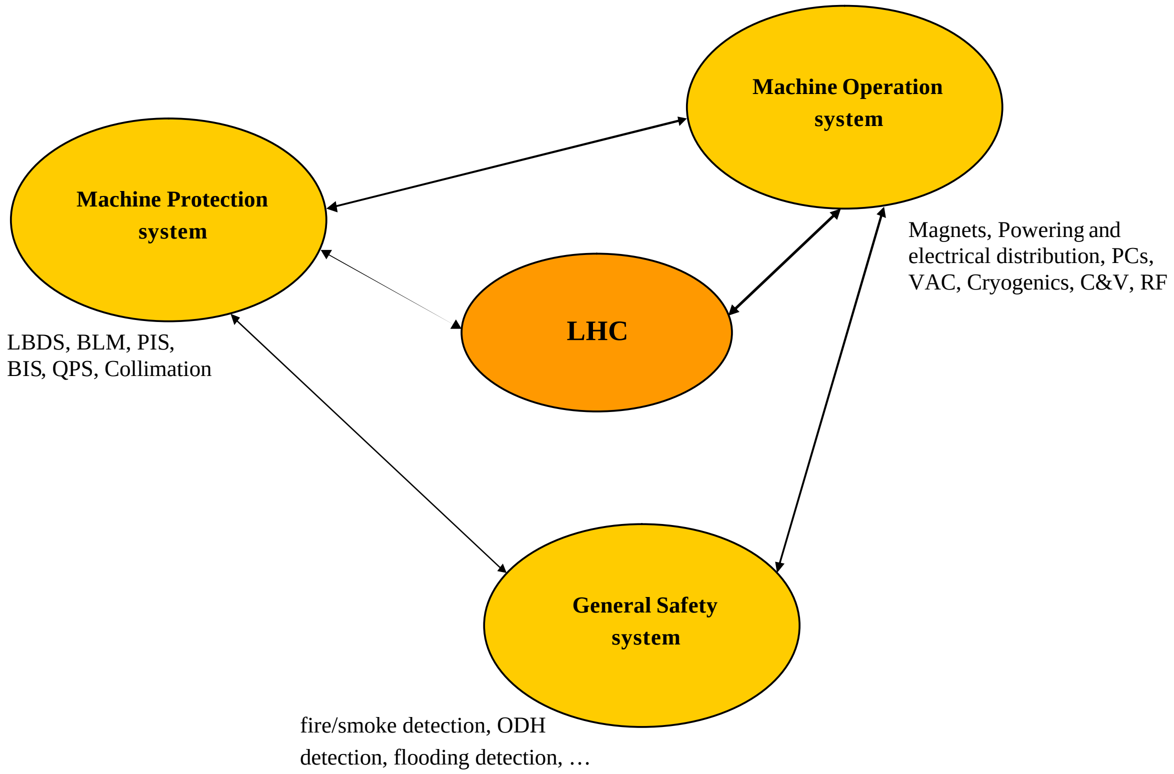

Machine Operation system
Machine Protection system
LHC
General Safety system
Magnets, Powering and electrical distribution, PCs, VAC, Cryogenics, C&V, RF
LBDS, BLM, PIS, BIS, QPS, Collimation
fire/smoke detection, ODH detection, flooding detection, …

Figure 4.8: System definition of the LHC underground

ventilation (C&V) and radio frequency system (RF). All these were designed with intrinsic safety measures, such as e.g. overpressure valves for the cryogenic system. However, in order that the operation of the machine is kept under control, the Machine Protection system is needed [36].

The aim of the Machine Protection system is to protect all equipment against uncontrolled release of energy stored in the magnets and the beams. This means that in case of triggering the Beam Interlock system (BIS), the beams are dumped safely via the LHC Beam Dumping system at point 6 (LBDS). Other systems making a contribution to the protection of the machine are the Beam Loss Monitors (BLM), the Power Interlock system (PIS), the Quench Protection system (QPS) and the Collimation system. With the Machine Operation system and the Machine Protection system in place the LHC is ready for operation and very well covered from the point of view of machine and equipment safety.

The General Safety system [37] is designed for personnel and environmental safety, as there still remain general risks which are not related to radiation: external risks (such as earthquake, flooding, fire or plane crash) and internal risks (such as dissemination of radioactive or toxic material, internal/external exposure to ionizing radiation, fire, explosion, chemical risks, mechanical risks or cryogenic risks) [38]. They consist of different safety systems with the aim of primarily preventing any accident to happen. However, in case an existing risk does cause an accident, they protect personnel and environment by reducing its severity. The following systems form part of the General Safety system: fire and smoke detection, flammable gas detection, Oxygen Deficiency Hazard (ODH) detection, Emergency Communication system, Emergency Evacuation system, emergency stop, flooding detection and Blocked Lift Alarm system.

The LHC Access systems [39], the CERN Safety Alarms Monitoring system (CSAM) [40] and the Radiation Monitoring System for the Environment and Safety (RAMSES) [41] also play an important role for safety, but are not part of the General Safety system.

The LHC Access systems comprise the following elements: the LHC Access Safety system (LASS) and the LHC Access Control system (LACS). The former ensures that during operation of the machine personnel is protected against radiation hazards resulting from accelerator operation. On the other hand, while the machine is not operating, the latter system identifies personnel requesting access and verifies the required qualifications (safety training) and authorisations (access rights).

CSAM is responsible for receiving and transmitting all alarms triggered by safety systems of the LHC to the fire brigade. Thereby it is guaranteed that a professional intervention of the fire brigade is possible.

RAMSES was originally designed for radiation protection; however, today it also includes conventional environmental measurements. Its principal duty though is the monitoring of the ambient dose equivalent rate in the LHC underground areas as well as on the CERN surface sites.

A risk analysis can be applied at any state of a project, starting with the research and development phase over planning, installation, commissioning and operation phases to shutdown and removal of the plant. In the case of the present thesis it was in the interest of CERN to analyse the remaining risks of the machine after examining all technical and safety systems and possibly discovering inconsistencies. Thus it was decided to prepare the analysis for the state of machine operation. This condition implies that there are actually no people in the tunnel and therefore environmental and machine safety was stressed. The objectives behind it were the discovery of high risk interdependencies and an input for improved protection of environment and equipment with regard to the already existing safety systems.

The determination of the object of analysis and its system boundaries then was a complicated task to accomplish. At first it seemed to be rather easy, taking the entire LHC with all its different subsystems as defined in Figure 4.8 into account. However, the setting of system boundaries turned out to be very problematic. The problem specification was actually limited to the LHC underground, but most of the subsystems are connected to the surface in such a way that it is difficult to draw a line between important interactions and those which can be omitted for the study. Moreover, their interactions with each other are very complex and barely definable in a concise way. So e.g. a leak in the cryogenic system could lead to problems in the vacuum system, an embrittlement of mechanic structures, a magnet quench and a contamination of the tunnel with helium. The number of involved systems concerning the consequences is very high, but it is even higher when considering all safety systems which are supposed to respond as well.

Another demanding subject in connection with the definition of the system is the level of detail, so the analysis depth up to which the problem should be questioned. With that many subsystems and different technical equipments involved, it was impossible to find the same level for all systems which would not distort the final results.

Summarising all the difficulties and problems mentioned above, and also thinking about the fact that an extensive risk analysis of this size would require a much higher manpower, it was then decided to concentrate on only one important aspect for a detailed study.

In order to operate the LHC and at the same time take care of machine and environmental safety, a great number of electronic and electrical equipment for operation as well as control and surveillance is installed in the underground area. Therefore the emphasis of the present thesis was laid on fire risk due to faulty electrical equipment. The history of incidents involving fires at CERN shows that the chosen issue is of interest, as actually all of them were caused by failures in electrical installations. Although fortunately there were no casualties, the damage caused was quite impressive: burnt equipment, superficial damaging of the building and surroundings and/or downtime of the machine. The cost of repair in one case even amounted to 11 million CHF.

When considering a cost of a magnet of 1 million CHF, the consequences of an incident in these contained conditions are amplified in respect of both cost and downtime. Coupling this with the radiation risk demonstrates the extreme safety concerns for the machine, its personnel, the public and the environment.

The new definition of the problem, namely a fire in the LHC underground caused by a failure in electrical equipment, reduced the complexity of the analysis and simplified the definition of systems involved: the LHC as a whole will be seen as an electrical installation, thus only one system is to be examined.

The methodical way of solving the problem is based on a combination of existing risk analysis methods. Following the comparison of different methods and their rating in view of the present problem, two methods were chosen: the Failure Modes and Effects Analysis and the fault tree analysis.

As the full understanding of the system is the most important factor for a meaningful result, the FMEA was chosen for this first step. It forces the analyst into successive thinking and provides a concise overview of possible failure modes of electrical equipment and subsequently their causes and consequences. A breakdown of the entire system can be achieved and all actually involved participants can be identified. The possibility of including frequency and consequence analysis (Figure 4.1) allows for an assessment of how probable electrical failures are and how severe their consequences could be.

Alongside the FMEA the question of location and material properties of the LHC subsystems is also to be examined, as among the main influencing factors for fire risk in the tunnel is actually the presence of inflammable material and its vicinity to possible ignition sources. Thus the collecting of material properties of the LHC subsystems and their location in the tunnel form an important part of the thesis. The combination of location of inflammable material and electrical equipment then allows for the discovery of all the areas significantly affected.

Once the first step of the study is completed, the question how high the risk of fire in the LHC underground is still remains unanswered. The method to be used when asking for a probability of occurrence of a fire is the fault tree analysis. With the help of the tree structure the failure sequences can be illustrated in a descriptive and clear way. By assigning failure rates to basic events in the fault tree and applying Boolean algebra calculations, the overall risk of fire in the LHC tunnel can be determined.

4.4 Failure Rate Data

The correct identification of failure rate data for a quantitative risk analysis is the most complex and intense part of the entire procedure [21].

Internally collected system-dependent failure rate data of a facility are the best source for reliable data. In order to be able to create a database of the components in use and their behaviour during operation, documentation concerning failures together with the operational circumstances and their frequency of occurrence should be kept. In this manner, the validity of the data is beyond doubt and can be used for a quantitative analysis.

In case no system-dependent data are available, generic data can be useful. They are usually deduced or calculated data issued in general publications. However, since these data are taken from comparable facilities and transcribed to the object under investigation, their validity for the present application is not always beyond doubt. In order to be able to apply this data, it is necessary to be absolutely sure about the characterisation of the object and the operating conditions for which the data were recorded. However, if exercised with caution, these data can be used and do present an augmentation of the base data.

The last possible approach to assessing the frequency of occurrence would be an estimation done by experts concerning the behaviour of the item under consideration. An expert in this case would be a person working with the object, preferably with some years of experience. Although it is a rather dissatisfactory solution for the analysis, it is often the only possibility.

Chapter 5

Fire Risk

5.1 Fire Risk of Electrical Installations

The subject of fire hazards due to electrical equipment failures has not been addressed extensively in literature. Although there is information available, the majority of these studies usually focuses only on 120/240 V distribution systems and the failures involving electrical household appliances. So according to fire statistics in the 1990's concerning home structure fires in the US, the cause of electrical distribution failures accounts for 9.7% of the total number of fires. Electrical distribution failure is therefore ranked fifth concerning the cause of fires, ranked fourth concerning the cause of fire fatalities, and ranked second concerning the cause of property loss.

Though international databases providing fire statistics do exist, there are some difficulties to keep in mind before applying this data. Research about the actual physical mechanisms of faulty electrical equipment leading to a fire is generally scarce. Moreover, the detailed reporting concerning the real cause of the fire is often missing, thus not permitting to draw conclusions without uncertainty of the data [42].

By analysing the existing statistical data, Keski-Rahkonen, Mangs and Turtola (1999, 2002) study the electrical causes of fires in both nuclear and non-nuclear installations [1,43]. Statistics according to the Federation of Finnish Insurance Companies were analysed concerning large fire accidents in Finland from 1980 - 1993. Using the national accident database ONTIKA (1991) the total number of fires in Finland in 1994 and 1995 were investigated, focussing on electrical fire causes. A level of uncertainty of the statistics applies to both cases, as either detailed fire investigations were not conducted at all or the fire causes were just roughly guessed.

Concerning nuclear installations the Advanced Incident Reporting System (AIRS) database (1997) was used, which is a database maintained by the Nuclear Energy Agency (NEA) and the International Atomic Energy Agency (IAEA). The authors state that the most frequent types of electrical ignition mechanisms in nuclear installations are short circuit, ground fault, arcing and overheating. Compared to that, loose connections as the cause of a fire do not occur as often. However, since the group of unknown failure mechanisms accounts for more than 30% of the events, the uncertainty of the analysed data is apparent. Additionally, the problem of defining the true cause of a fire is aggravated by the fact that usually not only one failure mechanism occurs, but a chain of faults.

When a fire occurs, it has to be distinguished between the first failed component and the first ignited component or material. These two classes do not necessarily have to coincide, as a fault in one electrical device can provoke a chain of faults eventually leading to ignition of another device.

In non-nuclear facilities the first failed components are electrical distribution cables and other components connected therewith. In contrast, the first material ignited is oil from transformers, breakers, etc., followed by cable insulation. The authors therefore come to the conclusion that cable insulation is the most important flammable material at the initial phase of a fire due to electrical equipment failures. In nuclear installations wiring and cables are not as frequently the first failing components due to stricter quality control.

The LHC project is a large electrical installation, containing high amounts of cables and electrical equipment and involving both high and low power distribution systems. Bearing the afore mentioned statistical information concerning nuclear and non-nuclear installations in mind, the study of fire risk in the LHC tunnel is of very high importance.

5.2 Historical Review about Fires at CERN

In CERN's history there have been a few fires with rather severe consequences, fortunately not involving casualties. The damage is limited to burnt equipment, superficial damaging of the building and surroundings and/or downtime of the machine. The following accidents have one common feature: their actual cause is the failure of electrical equipment. The development of these fires did not occur in the presence of workmen causing it through any human failure, but purely from an internal failure of equipment.

The number of fires at CERN in total is certainly higher than those mentioned above; however, in this study only those where the causes can not be attributed directly to human intervention or human failure will be discussed.

In 1975 a temporary patch panel in the PS (Proton Synchrotron) complex caught fire, propagating towards the gallery underneath and through the cable trays towards the PS substation [44]. The actual cause of the fire could not be defined precisely; however, in the final report it was stated that its origin was electric: either arcing or overheating. Metal incrustations in the concrete found close to the patch panel, which could be an indication of an electric arc between cables and metal.

The fire was actually detected by a failure report in the Control Room concerning the temporary patch panel. After an inspection on the spot, smoke was detected underneath the panel.

Where the fire had spread, the equipment and surrounding was totally damaged. Within a wider perimeter, the equipment was internally damaged because of corrosive smoke. Buildings in the surrounding area were superficially damaged due to the deposition of hydrochloric acid (HCl). Approximately 400 kg of PVC were burnt, releasing about 400 kg of hydrochloric acid (36%).

After the fire, the measures taken were primarily focusing on reconsidering the use of other types of insulation than PVC and PE, the better configuration of equipment to allow cooling and the arrangement for smoke, temperature and/or fire detection. As during the incident there have also been detected problems with the emergency stop and the emergency lightening systems, their improvement was proposed.

In 1982 a magnet in building EHN2 of the SPS (Super Proton Synchrotron) complex caught fire [45]. It originated from the signal cables BICC which, for any reason, were overloaded by an unacceptable current. Tests on these cables showed that given certain conditions a fire could emerge, causing the ignition of the Macrolon protection of the magnet. During a short circuit test of the cables carried out over some hours, the whole system heated up and the cables started to deform. The current increased, suddenly a flash occurred (probably on the metallic support of the cables) and a small fire appeared in the mass of cables. In fact, it was the plastic support of the BICC cables which burned.

The fire was detected only due to the coincidental presence of a person in the vicinity.

The Macrolon protection of the upper part of the magnet was completely burnt. Due to burning and dropping of the material the signal cabling of the lower part was also damaged. Control circuits and signal cabling (PVC) were burnt. As a rather low quantity of PVC was involved, the measures of hydrochloric acid (HCl) at selected points of the magnet did not show an exceedance of the given limit. The magnet had to be demounted for reparation.

As no fire detection existed despite propositions made, it was decided to install fire detectors before the anew start-up of the machine. In addition, a study concerning smoke extraction systems for all experimental halls at CERN was proposed, be it either a mobile or a stationary system.

The most recent fire at CERN occurred in 1997, when a new oil capacitor caught fire in building BA3 of the SPS Zone 3 [46]. After a short circuit of the capacitor of the snubber network (18 kV busbar), the glowing resistor ignited the transformer oil.

As the fire detection of the building was out of service at the time because of maintenance measures, the fire was not detected. Only when the fire detection was triggered in a building close-by, the passing fire brigade discovered smoke coming from building BA3 coincidentally. It turned out later on that no fire occurred in the building where the alarm was actually triggered.

The consequences of this fire were quite severe, including a downtime of the machines of two months. The BA3 radio frequency installation was corroded because of the burning PVC, and the 18 kV system was destroyed. In total, the damage accounted for approximately 11 million CHF.

After the accident an inquiry was conducted, identifying a major modification of the installation without a subsequent re-commissioning as the cause of the fire. An element with a built-in protection device was replaced by an oil capacitor without such protection equipment. The installing of a protection device in series would have been enough to secure safety.

As a consequence, electrical inspections of installations and also the re-commissioning of installations after major modifications were thereafter enforced with much more rigour.

5.3 Other Fire Risks

Although there are obviously other fire risks which threaten the operation of the LHC machine, they will only be mentioned briefly, as the main focus of this thesis is the fire risk due to electrical equipment failures.

Swamp gas:

Swamp gas present in the LHC tunnel would mean a significant increase of the risk of explosion, as it consists of 55 - 75% of Methane. However, experience from LEP shows that swamp gas is no actual threat, as the tunnel is located in average 100 metres below the surface, a depth where swamp gas is not produced anymore.

Other gases:

In the LHC machine tunnel there is on the one hand helium gas in large quantities used for the cryogenic system and on the other hand only a few other types of gases in rather small quantities. However, for the fire risk assessment they do not play a decisive role. Other different gases are used for the experiments, but they do not form part of the present study.

External events:

In terms of possible external events being able to cause a fire in the LHC, it is the access pits which pose a threat. There are two potential scenarios: either burning substances may fall down and set fire to equipment or inflammable gas might be sucked in through the pit.

Malicious activity:

Although conceivable, malicious activity is not part of the fire risk consideration.

Chapter 6

Risk Analysis - The Boundary Conditions

The present chapter is focussing on the successive procedure of the risk analysis for the LHC tunnel, giving explanation and reasons for the actions taken step by step.

6.1 Identification of Material Data

Three conditions have to be fulfilled in order that a fire can develop:

- the presence of oxygen,
- an ignition source,
- and inflammable material in the immediate vicinity.

In the case of the LHC tunnel, a failure in the electrical installation (i.e. an electric arc, a short circuit fault) is a possible cause of generating an ignition source. With two of the three conditions fulfilled, the remaining variable and the most important factor is actually the different materials present in the tunnel and their properties. Consequently, the determination of material data, their properties and location presents a vital part of the analysis.

6.1.1 CERN Regulations

As CERN is an international organisation and carries out works which are unique in Europe, it also has its own specific safety regulations. Although based on the member states' rules, at least the same level of safety as in force in the host states, Switzerland and France, has to be guaranteed. In case CERN believes that a more rigorous level should be maintained, it can certainly put its own special regulations into force. In general, safety instructions and safety codes are mandatory documents, whereas safety notes and safety bulletins are only meant to provide further information on safety [47].

Concerning the fire risk in the tunnel due to the presence of inflammable materials, CERN's Safety Instructions (IS) 23 and 41 have to be applied [48,49]. The former one deals with criteria and test methods for the selection of electric cables and wires with regard to fire safety and radiation resistance, the latter is concerned with the use of plastic and other non-metallic materials at CERN in general, but also with reference to fire safety and radiation resistance.

These two safety instructions both certainly refer to standards and publications of the International Electrotechnical Commission (IEC) and other internationally recognised bodies. For the different material properties and requirements that have to be met, they give the appropriate standards which have to be applied.

The requirements for all materials given in both instructions are the following:

- Electrical, mechanical, chemical, thermal and environmental resistance properties suitable for the desired application, and conforming to the appropriate standards
- Flame retardant characteristics satisfying the relevant standards
- Halogen and sulphur free
- Low smoke density
- Low toxicity of gases from fires
- Low corrosivity of gases from fires
- Adequate radiation resistance

With these requirements in mind, some generally used materials such as polyvinyl chloride (PVC), chlorosulphonated polyethylene (Hypalon), polychloroprene (Neoprene), fluorocarbons (i.e. Teflon) and other halogenated or sulphur containing compounds are excluded from usage in the installations.

IS 41 provides a classification of plastics for use at CERN, specifying not only the suitable base materials, but also restrictions for others and eventually the prohibited materials (Table 6.1). It is intended to be used only as a preliminary selection criterion, and where deviations from these rules are suspected, the materials should be tested before use. The instructions have to be followed for all new installations as well as for modifications to existing installations.

IS 23 and 41 are supplemented by Electrical Safety Code C1, which deals with regulations for the construction, installation and use of electrical equipment in order to protect personnel and property. As well as defining requirements for manufacturing, installing and operating electrical equipment and specific qualifications on the part of personnel, it also refers to the appropriate choice of material used for this equipment concerning fire safety and makes reference to the safety instructions mentioned before. This document is of course also based on the latest standards and recommendations of the International Electrotechnical Commission (IEC) and the European Committee for Electrotechnical Standards (CENELEC) [50].

Suitable base materials	Melamine formaldehyde, phenol formaldehyde Polyamide imide Polyarylate Polybenzimidazole Polyether ether ketone Polyether imide Polyimide Urea formaldehyde
Suitable only with incorporation of fire retardant NOT containing halogen, sulphur or phosphorus	Epoxy resin Ethyl acrylate rubber Ethylene propylene diene Ethylene propylene rubber Ethylene vinyl acetate High/low density polyethylene Polyamide Polyaryl amide Polybutylene, polybutylene terephthalate Polycarbonate Polyethylene terephthalate Polyisocyanurate Polyphenylene ether Polyphenylene oxide Polypropylene Polyurethane Polyvinyl acetate, polyvinyl alcohol Silicones
Prohibited materials	Acetal Acrylonitrile Acrylonitrile butadiene styrene copolymer (ABS) Acrylonitrile styrene acrylic ester copolymer Ethylene tetrafluoroethylene copolymer Natural rubber Perfluoroethylene propylene Polychlorotrifluoro ethylene Polymethyl methacrylate Polyoxymethylene Polystyrene Polytetrafluoroethylene(PTFE) Polyvinyl chloride (PVC) Polyvinyl fluoride Polyvinylidene chloride Polyvinylidene fluoride Styrene acrylonitrile copolymer Styrene butadiene copolymer

Table 6.1: Classification of plastics for use at CERN [49]

6.1.2 Material Data Project

Material data of the most important equipment families installed in the LHC tunnel have been collected in order to be able to estimate the existing fire load.

The list of equipment families was intended to cover all involved LHC groups, certainly aiming at the most significant and comparatively largest equipments. It has to be pointed out clearly that not all equipments present in the tunnel could be included, as the number of different LHC subsystems and their corresponding equipments is vast. The material data given do not claim to be extensive and correct, as it certainly depends on the collaboration and accuracy of the responsible person providing the data. A template was prepared in order to give a guideline and it was asked, where possible, for specifications as exact as possible (e.g. position of equipment in the underground area, combustible material exposed to air, quantity of combustible material). Considering the size and complexity of the LHC, unfortunately in most cases this was not achievable. Thus the major part of the data only gives an estimation of the actual quantity of materials and working fluids. As different people respond differently to the same demand, the level of uncertainty cannot be easily determined. However, though the present database is not exhaustive, the major components and major risk materials are covered.

The data were collected octant by octant, again due to the fact that giving the detailed location of each item was too elaborate, in some cases not even possible (e.g. pipes, cables). However, the data added up for one octant are too inaccurate to be used as a basis for the analysis. So in order to be able to judge the potential fire risk, the data of each equipment family have to be examined separately considering their location and adjacent equipment and installations with regard to CERN's civil engineering nominations. An accumulation of combustible material in one specific spot without any ignition source nearby has then to be regarded as less hazardous than a smaller amount of inflammable material close to a possible source of ignition. In the case of equipment which cannot be divided into single items, it should be considered as more or less equally distributed along the tunnel and technical galleries, respectively.

Another very important issue for the analysis is the position of combustible material within the boundary of the equipment itself. It has to be taken into consideration that in fact there might be inflammable material present, but it is an inherent part of the equipment and not normally exposed to air. In this case it is of course contained in the list of material data, but has to be discussed with special attention.

The data concerning plastics used in the tunnel is classified according to IS 41:

- Group 1: Suitable base materials
- Group 2: Suitable only with incorporation of fire retardant NOT containing halogen, sulphur or phosphorus
- Group 3: Prohibited material
- Group 4: As for some of the equipment families no detailed specifications about the plastics were provided, they were classified as undefined and added up in this group.

The warm cables, that is to say all cabling outside the magnets' cryostats, were not included in the general collection of material data, but extracted from a special database for the entire tunnel in total. The result is a list of more than 200 different types of cables in use. Unfortunately, the specifications of these cable types are not included in the database, so their analysis is rather difficult. The mass given for each meter of cable type summarises both the metal and the insulation part, thus a separated examination of the insulation is not possible unless the specification for each type is provided. The detailed analysis is therefore replaced by an overall estimation for the fractions of plastics and metal.

The extracted data from the database have to be handled with great care, as some of its features make it difficult to obtain the exact data. The sum of the mass of cables of all octants does not give the same result as the global sum of the mass of cables within the LHC. This is due to the fact that some of the cables are running over more than two octants (i.e. from octant 2 to octant 4) and are therefore only included in the global sum. This means that the sum per octant misses out a certain mass of cables. However, as the quantities of the materials are high, the final result will only be affected to a limited extent.

6.1.3 Material Properties

After determining all types of combustible material in the tunnel, the next step towards assessing fire risk is the examination of their material properties. In the following, these properties are discussed for all appearing combustible materials in the specified areas.

Polymers of Group 1 pass the standard fire tests relating to properties such as low smoke density, low toxicity and low corrosiveness of fire gases and a satisfactory fire performance (ease of ignition, etc.). They are naturally fire retardant, in some cases even self-extinguishing, and therefore do not propagate the fire.

As mentioned above, **polymers of Group 2** are only considered suitable if they contain fire retardant without halogen, sulphur or phosphorus. These polymers maybe resist a fire better than polymers of Group 1, but once a fire is in progress, they will not be self-extinguishing and will certainly continue to burn.

Since **polymers of Group 3** contain fire retardant such as halogen or chloride, they will certainly resist a fire for a certain amount of time. However, if the ignition source is big enough and the combustion is started, they will burn easily and release toxic, corrosive and very dense gases.

With no specification available, **polymers of Group 4** present a special case concerning the identification of their fire load. At worst, they have the same fire properties as polymers of Group 3, which is why these two groups will be treated equally.

Graphite is basically a combustible material which can be ignited by friction, heat, sparks or flames; auto ignition is started at about 450°C. Once a fire has developed, irritating and/or toxic gases may be released [51].

Based on a sample of an electronic rack of the LHC Power Interlock system, an estimation of the constituents reveals that about 30% of the materials are polymers of various types, and the remaining components are made up mainly by aluminium, copper and a few other metals. Therefore **electronic components** do present a certain fire load. Due to the unknown specifications of the polymers, its magnitude can not be determined in detail. However, for the analysis of fire risk, electronic components cannot be neglected.

The only inflammable liquid used in the LHC tunnel within the boundaries of this study is **silicone oil**. Depending on the supplier and the type of product, its properties may vary slightly. However, it is a combustible liquid with a flash point of about 300°C. During a fire, the decomposition products may include hazardous gases such as carbon oxides and incompletely burned carbon compounds, silicone dioxide and formaldehyde [52, 53].

Due to the remarkable number of cable types and missing specification details, the actual fire load of the **warm cables** has to be estimated. For this analysis it will be assumed that the insulation of a cable makes up about 80% of its total weight, whereas the remaining 20% comprise its metal part. This assumption is only true for certain cable types, namely signal and high voltage cables. However, this overestimation of the proportion of the plastics will affect the analysis in such a way that the result is on the safe side.

IS 41 does restrict the usage of insulation material which is not either suitable base material or suitable base material incorporating fire retardant. Consequently the assumption concerning the types of polymers used as cable insulation material and therefore the fire properties of the cables is based thereon. However, it also has to be assumed that there might be a number of cables which do not abide by this regulation. This means that the fire load of the warm cables is mainly defined by polymers of Group 1 and 2 with possible outliers of polymers of Group 3.

6.1.4 Location of Combustible Material

In order to finish the overall analysis of the materials and their contribution to a fire risk in the tunnel, the determination of their position with respect to each other and their position with regard to possible ignition sources is essential. As the number of different equipment families in total is rather high, only the largest and the most influential equipment families will be taken into account.

The material data inventory will give both location of equipment families with their amount of inflammable material and location of electrical equipment (being part of some of the equipment families). However, it will not be possible to cover all electrical equipment. High voltage transformers as well as low power apparatus (switchgears, batteries, UPS systems, electronic racks and computers for supervision) are distributed over the entire underground area and cannot be included in the material data in a precise way.

The localisation of equipment families will be estimated, as most of them are spread over a large area in the tunnel. It will only be possible to provide approximate positions with respect to CERN's civil engineering terminology.

Class	Frequency	Range [event/year]
1	Impossible	$\ll$
2	Improbable	10^{-7} - 10^{-8}
3	Rare	10^{-4} - 10^{-7}
4	Occasional	10^{-2} - 10^{-4}
5	More frequent	10^{-1} - 10^{-2}
6	Frequent	10^{-1} - 1

Table 6.2: Classification of frequency

6.2 Fire Risk of Electrical Installations

The failure of electrical equipment can lead to the creation of an ignition source, either indirectly through an abnormal rise of temperature or directly through e.g. the generation of sparks or an electric arc. As the LHC is mainly built up by electrical equipment and besides that combustible material is present, the combination of an accidentally created ignition source together with inflammable material in the vicinity is a fact that gives rise to a measurable risk. As a consequence, a possible fire can affect the equipments installed in the tunnel and therefore also the operation of the machine.

In order to be able to get an overview of possible failure modes in electrical installations which can develop an ignition source eventually leading to a fire, a FMEA was undertaken. As this analysis is not aiming at detecting each particular failure mode of a single component, but an electrical installation as a whole, no item description was necessary. Instead, only the possible failure modes as well as their causes and consequences were listed. It is important to mention that the collection of consequences is only focussing on possible ignition sources, as fire risk is the prime motivation of this thesis.

This presentation of possible fire hazards caused by simply operating an electrical installation is a forerunner to a more detailed analysis and is therefore intended to become familiarised with problems that might arise and are able to lead to more severe issues if occurring in the appropriate conditions.

A FMEA usually includes a study of prevention measures which have been integrated in the design in order to prevent any incidents. However, as this thesis is aiming at the fire risk beyond intrinsic safety measures (such as the prohibition of PVC in the tunnel or the deliberate choice of dry-type transformers), the prevention measures for the LHC are not discussed.

6.3 Combined Risks

The Failure Modes and Effects Analysis of the previous chapter is aiming at discovering failures which can occur inside a technical system as a result of their operation. For the remaining risks compensating measures should be implemented to be able to keep them under control. However, in case of an incident despite of foreseen prevention measures, the consequences of these failure modes have to be judged correctly by additionally taking into account the surrounding conditions. So when talking about combined risks for this analysis, one is referring to the presence of combustible material in the LHC tunnel.

As addressed before, only the combination of inflammable material and an ignition source in the vicinity can lead to an unexpected incident with regard to fire risk. This implies that after the first step of analysing the situation by identifying and locating combustible materials and carrying out the FMEA for the electrical installation, it is the second step which has to combine both factors in order to find out about the actual impact on the system. In fact it is this combination which allows a real estimation of the consequences, and therefore forms a continuation of the consequence analysis of the FMEA for electrical installations. When considering the location of combustible materials, the consequences can be narrowed down to the areas where an ignition source actually can coincide with inflammable material.

6.4 Frequency and Consequence Analysis

The identification of hazards and failure modes in the course of the analysis forms an essential part of the overall risk analysis procedure (see Figure 4.1). Frequency and consequence analysis present the continuation of the process from a qualitative to a quantitative analysis and allow an estimation of risk. Only by determining the frequency of occurrence of a failure mode and the severity of its consequences, a judgement can be made concerning the impact on the equipment itself, the adjacent installations and subsequently the entire system. Although consequences have already been addressed by means of the Failure Modes and Effects Analysis, they do not yet show a measure of damage and therefore have to be examined further.

In order to be able to judge frequency of occurrence and severity of consequences, acceptance criteria have to be defined beforehand. Without identifying objectives for the risk analysis in the form of acceptable/unacceptable risks, the results do not mean anything. Once the acceptance criteria are set, priorities for closer examination can be determined and improvement measures can be discussed.

6.4.1 Frequency Analysis

In order to be able to assess the frequency of occurrence and to illustrate the risk, a classification of the frequency has to be drawn up (Table 6.2). The derivation of the so-called frequency classes depends on the respective analysis, its object under investigation and its purpose. The classification is intended to facilitate the process, and in case more experts are contributing to the assessment, it allows keeping track of the consistency of opinions.

Class	Severity	Description
1.a	Negligible	No malfunction of the machine
1.b		No effect on equipment
1.c		No effect on people
2.a	Small	Breakdown of one subsystem, machine stays operational
2.b		Slight degradation of equipment
2.c		Minor effects on people
3.a	Significant	Propagation of incident, breakdown of more than one subsystem, machine is not operational
3.b		Damage of equipment
3.c		Fair effect on people, injury with full recovery
4.a	Severe	Cut-off of one sector of the machine, machine is not operational
4.b		Significant damage of equipment
4.c		Severe effect on people, injury with long-term damage
5.a	Critical	Complete breakdown of the machine
5.b		Loss of equipment
5.c		Fatal injury

Table 6.3: Classification of consequences (following [29])

6.4.2 Consequence Analysis

The determination of the consequences in the Failure Modes and Effects Analysis only shows qualitatively the impact on the system. For quantitative risk estimation it is necessary to define the severity of the consequences. Thus, such as done for the frequency analysis, also for the consequence analysis a classification has to be created. The definition of the consequence classes is thereby concentrating on the effect of a certain failure on the system. The severity ranges from impacts kept within the local equipment to impacts that can even pass beyond the equipment boundaries and affect the surroundings as well as the entire system. As one of the preconditions for this study is the absence of personnel in the tunnel during operation, Table 6.3 only includes effects on people for the sake of completeness.

6.4.3 Risk Matrix and Acceptance Criteria

With the help of frequency and consequence analysis, the risks can now be illustrated in a risk matrix. The previously introduced classifications of frequency of occurrence and severity of consequences make it possible to present the risks in a descriptive way and reveal those with the highest frequency of occurrence and the most severe consequences. In this manner, the most hazardous incidents can be chosen and discussed more into detail.

Figure 6.1 shows the risk matrix for the present problem including acceptance intervals

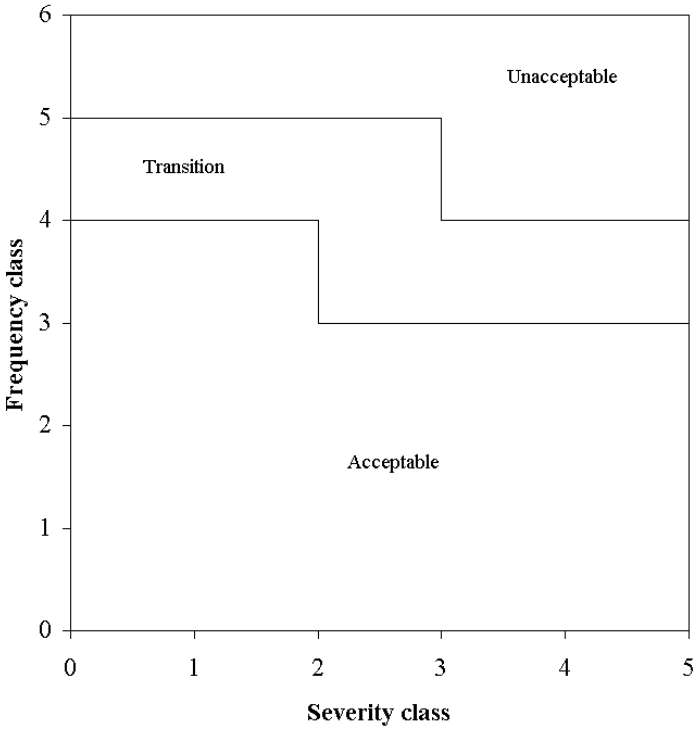


Figure 6.1: Risk matrix with acceptance intervals

with intergradations: acceptable risks, transition area (acceptability of the risk under certain conditions needs to be discussed), unacceptable risks. It shows the relationship between frequency and consequences, clearly outlining the high risk area.

Acceptance intervals or criteria, respectively, are essential for a conclusive performance of a risk analysis. Without defining objectives and determining criteria for interpretation, the results of the analysis do not bear a meaning. For example, a frequently occurring incident on the shop floor with severe consequences for production would without doubt be investigated more into detail, as the predicament is obvious. However, the assessment of another incident threatening production just as severely, but with a lower frequency of occurrence, is much more difficult. Depending on the acceptance criteria set beforehand, it is possible to decide if the risk is still acceptable or measures have to be taken to improve the situation.

In the case where a frequency/consequence pair is set in the transition area, a consideration of interests is necessary. Generally, the ALARP principle is applied: As Low As Reasonably Practicable. Thus a balance between the costs of improvement measures and the costs of indemnity in case the incident actually occurs has to be found. For the remaining two areas of the risk matrix the procedure is clear: either the risk is acceptable or actions have to be taken in order to reduce the risk, thereby prioritizing disastrous scenarios.

Establishing acceptance criteria can take place in various ways. They may be imposed by law or competition on the market, but a company may also follow its own target values for production and quality.

For the present thesis, considerations concerning the foreseen lifetime of the LHC have dictated the establishing of the acceptance intervals. Beginning with the lowest severity class, the intervals are derived from the following basic assumptions:

- With an expected operation time of 20 years, frequency classes 5 and 6 imply that an incident may happen between 0.2 and 20 times per LHC lifetime. Incidents found within this frequency range are by no means acceptable.
- Between frequency classes 4 and 5 (0.002 to 0.2 times per LHC lifetime), incidents fall into the transition area and decisions have to be made according to the circumstances.
- Below frequency class 4 (less than 0.002 times per lifetime), risks are acceptable. With a growing severity class, apparently the intervals have to be adjusted downwards gradually.
- From severity classes 2 to 3, the state of the machine goes from operational to non-operational. As this is a significant indication that effects are being more severe, this is the point from which the intervals decline.

Once the highest severity class is reached, the area of unacceptable risks has come down to frequency class 4. Considering the lifetime of the LHC, this frequency does not actually have a great importance. However, an incident with these characteristics has the potential to cause a fire and threaten the operation of the machine to an even greater extent (disaster).

Considering the area of acceptable risks in comparison to the areas of transition and unacceptable risks, the intervals seem to be fairly generous. The reason for this lies in the fact that the Failure Modes and Effects Analysis is not trying to assess fire risk, but failure modes which eventually might lead to a fire. So these slightly more tolerant acceptance intervals imply that there is more to a fire than just the failure of electrical equipment.

6.5 Fire Risk - Fault Tree Analysis

So far during the course of the analysis no actual evaluation of the fire risk has been carried out. The frequency and consequence analysis described in the previous chapter only assesses the frequency and consequences of the failure modes of electrical installations, but not the risk of having a fire in the underground area. Moreover, the material data project has one downside which has not yet been overcome by any of the before mentioned analysis steps, namely the uncertainty of the collected data.

Therefore a so-called risk layer for the entire underground area is defined, which presents inflammable material together with electrical equipment (possible ignition sources) as a layer equally distributed along the underground. For this risk layer a fault tree with the top event “fire in the LHC underground” (due to faulty electrical equipment) will be developed and analysed, revealing the probability of occurrence of a fire in the tunnel as well as the logic correlations between the events leading to it.

Chapter 7

Fire Risk Analysis of the LHC Underground Area

The actual fire risk analysis of the LHC tunnel will be undertaken as laid out in theory in the previous chapter.

7.1 Qualitative Analysis

7.1.1 Material Data - Combustible Material

In order to be able to isolate the areas in the tunnel where an actual fire risk exists, the location of combustible material and the accumulation of electrical equipments have to be taken into account.

Table 7.1 lists combustible materials and fluids present in the LHC tunnel. The total amount of combustible material is made up of polymers, graphite and electronic components. On the part of inflammable working fluids there is only silicone liquid present in the tunnel.

Polymers of Group 1 are mainly coming from the superconducting main dipoles and quadrupoles, and are therefore more or less uniformly distributed along the tunnel. The increased amount of these polymers in octant 6 can be attributed to the ejection dump kicker generators. As suitable base material, these polymers do not have first priority in terms of fire risk. Moreover, they are located inside the magnet assembly, thus not directly exposed to air.

Polymers of Group 2 are treated similarly to polymers of Group 1, as they are only allowed to be used in the tunnel with the incorporation of fire retardant not containing halogen, sulphur and phosphorus. Mainly contributing to the presence of these polymers are the superconducting main dipoles, main quadrupoles and insertion quadrupoles, as well as the warm magnets, the cryogenic distribution line, the cryostats housing the magnets, power converters and beam position monitors. In octants 2, 6 and 8 the amounts of these materials

Octant	**Material**						**Working fluid**
	Polymers (groups according to IS 41) [t]				Graphite [t]	Electronic components [t]	Silicone fluid [m^3]
	Group 1	Group 2	Group 3	Group 4			
Octant 1	12.9	38.1	0.4	0.2	0.0	1.6	0.00
Octant 2	12.9	48.6	0.2	0.2	0.0	1.7	7.60
Octant 3	12.6	36.6	1.2	0.2	0.1	1.5	0.00
Octant 4	13.1	38.9	0.2	0.2	0.0	3.5	7.32
Octant 5	12.9	38.1	0.4	0.2	0.0	1.6	0.00
Octant 6	18.6	96.1	7.5	0.3	9.1	1.7	0.00
Octant 7	12.6	36.3	1.1	0.2	0.2	1.5	0.00
Octant 8	12.9	48.6	0.2	0.2	0.0	1.7	7.60
Total	108.5	381.3	11.2	1.7	9.4	14.8	22.52

Table 7.1: Location of combustible material (February 2007)

increase noticeably due to the injection and extraction kicker generators. In general, any magnets as well as the cryogenic distribution line are situated along the main tunnel, though the rest of contributing equipments is found in the technical galleries.

Polymers of Group 3 according to IS 41 are prohibited materials for the usage in the LHC underground. However, some remarkable amounts of these materials are found in the main tunnel and technical galleries. The contributing equipments are the warm magnets and the septa magnets as well as the kicker generators. Outstanding is the amount of more than seven tons in octant 6 due to the ejection kicker generators. Derogations to IS 41 have been granted for the amounts contained within the magnets by Safety Commission due to the fact that because of radiation requirements the choice of adequate material is limited. In contrast to that, up to the present state of this thesis no derogations have been requested concerning the polymers of the generators in octant 6.

The last group of polymers is the group of undefined materials. They are generally situated in the technical galleries, contained in electrical control equipment. In comparison to polymers of Groups 1, 2 and 3, their amount is negligible in terms of fire risk. However, together with the group of electronic components the undefined polymers call attention to a general problem of the material data project, namely the unknown amounts of electronic control equipment in the underground area. Due to the fact that it is very laborious to specify this type of equipment in detail, it has to be assumed that in many cases data were either not provided or just summed up in a single figure. Thus the actual amount and the actual location of electronic equipment together with the contained plastics will stay unknown.

The group of electronic components mentioned in Table 7.1 is mainly made up by the Quench Protection system, in particular the protection racks situated underneath the main dipoles in the tunnel. In octant 4 it is the radio frequency system which contributes noticeably. However, as mentioned before, the amount of electronic equipment either not

Octant	**Warm cables [t]**
Octant 1	195
Octant 2	498
Octant 3	242
Octant 4	314
Octant 5	198
Octant 6	208
Octant 7	105
Octant 8	435
Total	2,195

Table 7.2: Location of warm cables (October 2005)

provided or included in one of the other combustible material groups is not known. Thus it has to be assumed that the number of unreported cases is much higher and probably uniformly distributed along the underground areas.

The last combustible material in Table 7.1 is graphite, which is contained within the collimators as well as the LHC Beam Dump system. The amounts are rather small compared to the rest of the groups. Moreover, it is located within the collimators in vacuum, thus not directly exposed to air [54]. In octant 6, it is the external beam dump for the ejected beam which accounts for the better part of graphite. There are 4.5 tons of graphite on either side of point 6 at each end of the two straight tunnels leading away from the main tunnel. As these amounts are about 600 metres away from the main tunnel and the blocks are air-cooled and under nitrogen atmosphere, the beam dump tunnels are not considered dangerous in terms of fire risk.

Silicone oil is used within the injection kicker generators in octants 2 and 8 as well as for the radio frequency system. The amount is remarkable, and although good fire properties of the product are assumed, its examination for the fire risk analysis is important.

As mentioned in the previous chapter, the warm cables present a matter which has to be discussed separately (Table 7.2).

The superconducting cables do not have any insulation, since they are an integral part of the superconducting magnets and are therefore not particularly mentioned in the comments above.

In Table 7.2 the total weight of all non-superconducting cables is made up of more than 200 different types of cables, including both the fractions of metal and insulation. With an estimated value of 80% of insulation and 20% of metal per cable (see 6.1.3), the entire underground area of the LHC comprises about 1,756 tons of polymer insulation. As mentioned before, the bigger part of these insulation materials will be polymers of Group 1 and 2. Since also some prohibited polymers are expected due to disregard of regulations, the fire properties of the warm cables play an important part in the fire risk analysis. Moreover, it is their sheer quantity which implies significance in view of creating an ignition source while conducting current because of a failure as well as presenting a considerable fire load because of the properties of the polymers. The latter fact is supported by a study analysing existing statistical data on electrical causes of fires in nuclear and non-nuclear installations, which concludes that cable insulation is the most important combustible material at the initial phase of a fire (see 5.1).

7.1.2 Analysis of the Electrical Installation

The first step for an extensive analysis is the understanding of the system and in particular the understanding of possible failures of the equipment and the resulting consequences. The Failure Modes and Effects Analysis for electrical installations is presented in Table 7.3.

The number of different failure modes shown illustrates clearly how an ignition source in the tunnel might emerge. It has to be pointed out that there has not been considered any deliberate malpractice or malice, but simply the operation of electrical equipment. Certainly for the possible causes human failure has been taken into consideration (e.g. incorrect installation).

The generation of an ignition source is determined by the presence of a high temperature, leading to a fire if combustible material is located in the vicinity. The causes for an unusual high temperature are various, ranging from the failure of the electrical insulation over incorrect installation to the internal failure of equipment. The consequences thereafter might be the generation of sparks, arcing, overheating of equipment or the accumulation of flammable gases in the air. Although causes and consequences show different possible combinations and different sequences of events, the actual origin of a fire is always a cable junction or other interconnections where the failure occurs. Thus the conclusion is that the fire can only develop where cable junctions are found or accidentally created by whatever failure, or where electrical equipment is defective (e.g. switch gear, power supply, magnet). Cables in general are not regarded as being responsible for the generation of a fire, but they do present an important fire load and contribute to fire propagation.

Following the comments concerning the origin of a fire above, the inflammable material in the tunnel is mainly made up by cable insulation and other plastics in the different equipments. According to IS 23, all cables used in the tunnel are supposed to be flame retardant. This means that they do not contribute to an initiating fire and have to resist it for a certain time, in compliance with the applying IEC standards. However, once a smoulder or a fire occurs and is (under appropriate conditions, such as malfunction of fire and smoke detectors) able to outlive the fire retarding property of the cables, a significant amount of combustible material has to be considered, also taking into account the density of cables within the cable trays and panels.

A particularly precarious issue in terms of possible ignition sources in the tunnel are bad cable connections. The actual physical process is an abnormal rise of contact resistance, and as a result the slow increase of temperature and the possible smouldering of cables. Different from a short or ground circuit fault, bad connections do not show their impact immediately,

FM Ref	Failure Mode	Possible Causes	Consequences
1	Overheating	Failure of electrical insulation	Gradual temperature rise
		Incorrect installation	Accumulation of heat and effluent in the vicinity
		Bad contacts	Spark generation
		Overcurrent in a cable	Thermal ageing of insulating material
		Misuse (i.e. running a high-powered appliance off a low-power extension cable)	Accumulation and diffusion of flammable gases in air may give rise to an ignition or explosion
		Short and ground circuit fault	
		Mechanical distortion modifying electrical contacts or insulating material	
		Failure of a component, an internal part or an associated system (i.e. ventilation)	
		External heating (ambient temperature in the LHC tunnel approximately 30°C)	
2	Short circuit and ground fault	Mechanical impact (i.e. during installation, maintenance)	Abnormal temperature rise (significant after short time, localised)
		Incorrect installation	Possible emission of light, smoke, flammable gases
		Defective cables	Release of glowing materials or substances
		Disengaged conductors, bad contacts	Arcing
		Ingress of conducting foreign bodies	
		Sudden failure of component or internal part	
		Failure of electrical insulation	
		Flooding	
3	Arcing	Failure of electrical insulation (damage)	Intensive heat in a small volume
		Overcurrent	Point source ignitor
		Incorrect installation (action exposing live parts or bringing them together)	Possible emission of light, flammable gases and flames
		Short and ground circuit fault	
		Rupture of a contact	

continued on next page

continued from previous page

FM Ref	Failure Mode	Possible Causes	Consequences
		Sudden failure of component or internal part	
		Mechanical impact (i.e. during installation, maintenance)	
4	Bad contacts	Abrasion	Gradual temperature rise
		Mechanical distortion modifying electrical contacts	Accumulation of heat in the vicinity
		Incorrect installation	Short circuit and ground fault
		High transition resistance	Overheating
		Mechanical impact (i.e. during installation, maintenance)	Accumulation and diffusion of flammable gases in the vicinity
		Corrosion	
5	Failure of electrical insulation	Mechanical impact (i.e. during installation, maintenance)	Accumulation and diffusion of flammable gases in the vicinity
		Bad quality	Overheating
		Abrasion (i.e. friction)	Arcing
		Conducting dust	Gradual temperature rise
		Humidity	Accumulation of heat in the vicinity
		Conducting foreign bodies	Short circuit and ground fault
		Ageing	
		Incorrect installation	
		Damage	
6	Circuit-circuit fault	Mechanical impact (i.e. during installation, maintenance)	Possible emission of visible light, flammable gases and flames
		Squashed cables	Accidental coupling of two circuits
		Incorrect installation	Short circuit and ground fault
			Spark generation
7	Protection failure	Internal failure of protection device	Overload
		Ageing	Short circuit and ground fault
		Mechanical impact (i.e. during installation, maintenance)	

continued on next page

continued from previous page

FM Ref	**Failure Mode**	**Possible Causes**	**Consequences**
8	Transfer of component failure	Internal failure of equipment	Transfer of failure to the power system
		No protection device to avoid transfer	
		Failure of protection device	
9	Missed quality control	Mechanical impact after commissioning (i.e. during installation of adjacent equipment)	Degradation of the system
		No inspection, no commissioning	Power failure
		Incorrect installation	

Table 7.3: Failure modes for electrical installations (following [55])

but with a delay of hours, days or even weeks. As the performance of the cables is still acceptable and the consequences of a bad connection are not instantly obvious to the operation, this failure mode is easily overlooked during installation, commissioning or maintenance. With respect to the amount of cables and cable junctions in the tunnel, its possible frequency of occurrence has to be considered as being of special concern. As above all the detection of bad connections is hampered by its slow and unobtrusive development, this failure mode has to be regarded as significant for this thesis.

If a bad cable connection happens to occur within the superconducting cable network, that is to say the warm part feeding the superconducting circuits, there is no possibility of fast interruption. Thus the current flows until the energy of the magnet is fully consumed, thereby smouldering cables. With the rise of the temperature of the cable also its resistance increases, and even more energy is transformed. Due to the available amount of energy within the magnet system, these conditions may lead to a fire.

The situation may look slightly different for cables of the distribution network. Bad connections stay undiscovered for a rather long time, as the detection during operation is very difficult. The connections are usually invisible and the effects do not appear immediately. However, if a short circuit - and therefore a current ten to twenty times higher than nominal current - occurs in addition to a high transition resistance, there is suddenly enough energy for a fire available.

The supervision of electrical junctions could be done with the help of infra-red cameras. Regularly taking pictures during operation would allow for an early detection of deteriorating connections and subsequently problem areas. However, as the radiation level in the tunnel restricts the application of these cameras, CERN is not able to employ a systematic control of electrical junctions.

Although the common failure mode of short circuit and ground fault is mentioned in the FMEA, the circuit-circuit fault is noted in particular because of its significance for this study. The disposable space for equipment in the LHC is limited due to the fact that the tunnel itself is already more than 20 years old. This means that with the given tunnel profile, the final assembly for the LHC had to be adapted to restricted space. As a consequence, the space left for people and equipment to pass is limited and makes the installation vulnerable to external damage during installation and maintenance. The possibility of generating a circuit-circuit fault by accidentally coupling two independent circuits without noticing is hence apparent.

Usually electrical equipment is provided with inherent protection devices in order to detect a failure within the equipment and secure its safe shutdown. However, the protection device itself has a certain level of reliability and can therefore fail. Certainly the reliability of the various equipments has been considered in the design phase, but as there is always a margin for equipment failure, it cannot be neglected.

In case an internal failure of equipment occurs and the protection device does not respond correctly, the failure might be transferred from the equipment to the power system. Although the transfer can only happen when both failure modes occur at the same time (internal failure of equipment and failure of the protection device), they are mentioned separately in the FMEA. The reason is that in spite of their close connection, both failure modes may occur independently and have different consequences for the installation.

Quality control plays a very important role for the installation and operation of a complex system like the LHC and cannot be neglected. The passing of technical inspections of all electrical equipment is a basic requirement for the start-up of the machine. But since its complexity makes all the difference compared to a small manageable technical system, the "failure mode" of missed quality control has to be mentioned and considered in the fire risk analysis. Although it is not a failure mode in terms of technical problems of an electrical installation, it can present the origin of electrical failure modes.

As mentioned previously, general fire prevention measures for the equipments situated in the tunnel and neighbouring galleries, junctions and alcoves were not implemented, mainly because of the shortage of space. Different subsystems of the LHC do have their appropriate failure prevention measures; however, these measures are not coordinated among each other and are therefore not a facility applicable for the electrical installation as a whole. Instead, an automatic fire and smoke detection system for the LHC underground areas has been implemented in order to detect a developing fire as soon as possible and mitigate the consequences [56].

The fire and smoke detectors are planned to be located in areas with a significant amount of inflammable material or areas where the consequences of a fire would be unacceptable (the experimental halls, the tunnel enlargements, junctions and alcoves). Once an alarm is triggered, the fire brigade and the Technical Control Room (TCR) are informed via the CERN Safety Alarm Monitoring system. Then a decision has to be made in order to determine which actions have to be taken. The detectors are connected to Control and Indicating Equipment (CIE) in the service areas of the tunnel, such as luminous panels providing a visual warning to the occupants. However, there is no automatic evacuation alarm triggered and no automatic power-off of the corresponding area.

In case of fire, one of the subsystems of the LHC monitoring the beam operation and environment will trigger an error which will lead to a beam dump and interrupt the operation of the machine. Yet if the detectors are not able to discover the fire, the reason behind the problem of the subsystem will stay unclear, and appropriate action regarding the fire cannot be taken as fast as actually desired or required.

7.1.3 Specified LHC Areas Concerning Fire Risk

The combination of the results of the material data inventory, that is to say the location of combustible material as well as the accumulation of electrical equipment, with the Failure Modes and Effects Analysis for electrical installations reveals the following areas of concern:

Points 2 and 8:

The silicone fluid contained in the high voltage pulse generators of the injection kickers in the underground areas of points 2 and 8 make these areas especially interesting from the point of view of fire risk. Although the silicone oil is well contained and protected, there is an actual accumulation of electrical equipment in the close vicinity increasing the probability of a potential fire. The generators are situated in the technical galleries parallel to the main tunnel, where not just low power apparatus is found, but also a number of electronic racks and high energy equipment (i.e. power converters).

In case any mechanical failures of the container (leakage, residual liquid on the floor, frequent maintenance activities required, etc.) appear simultaneously to an emerging fire, the consequences of such an incident are enormous.

The injection system is responsible for the safe injection of the beam onto the orbit of the LHC. If the system fails, extensive effects could be provoked concerning surrounding equipment and infrastructure as well as the operation of the machine. The fire itself and its effects (quench, explosion, etc.) would damage the magnets and other neighbouring equipments as well as the building itself. Subsequently a serious downtime of the machine would have to be expected.

The technical galleries where the pulse generators are located are equipped with fire and smoke detection. In addition, mechanical and hydraulic measures are taken in order to monitor the silicone liquid. Interlocks and the general surveillance system of the kicker generators, such as surveillance of the liquid level within the enclosures or temperature detection, guarantee further securing of the area [57].

The inventory of the material data of the kicker generators reveals that their structure does contain significant amounts of polymers. In addition to suitable base material, polymers of Group 2 amount to approximately 16 tons in total for points 2 and 8, and prohibited material of Group 3 (including polyacetal and polymethyl methacrylate alias Plexiglas) add up to about 250 kg. Up to the present day, no derogations to IS 41 for the latter were requested.

Point 4:

The radio frequency system at point 4 of the LHC is using silicone liquid, therefore also presenting a problem in view of fire risk. A very high energy conversion in this area favours the development of unintended heat sources; a concentration of electrical equipment provides the potential ignition sources. In principle the same situation as for the injection system applies, as any problem with the silicone liquid might lead to an unexpected fire incident.

Being in charge of acceleration and storage of the beams, the RF system is vital for the operation of the machine. The effects of a fire in this area compromise not only the intended purpose of the RF system by deteriorating the parameters of the beams, but can also lead to serious damage of the equipments and building due to the beams' stored energy. Necessary downtime of the machine would represent additional trouble.

The fire and smoke detection system is present in most places, but not sufficiently in the entire area occupied by the RF system. From the cavern at the interaction point, RF equipment spreads out into the main tunnel and the technical galleries. Fire and smoke detectors are located in the technical areas, but not in the main tunnel.

The material inventory of the RF system does not contain any prohibited polymers with respect to IS 41. Polymers of Group 2 are present, but only add up to minor quantities. In the cavern, the amount of electronic components (racks) constitutes nearly 2 tons.

Arcs:

The LHC arc is mainly taken up by the superconducting magnets, the cryogenic distribution line and cable trays along the wall of the tunnel. In addition, there are low voltage power converters (dipole orbit correctors) and protection racks of the Quench Protection system (containing capacitors) beneath the magnets. Although this is combustible material in rather high quantities distributed over a fairly long distance coupled with a lot of cables in its vicinity, there is no fire and smoke detection foreseen in the LHC arcs. With a potential and significant fire risk present, this thesis is an attempt to reassess the necessity of fire and smoke detectors in these areas.

In case a fire does develop, it could be detected indirectly via an error of certain LHC subsystems. However, this shows a failure in the system and not a fire, and therefore this way of detection takes up too much time and might allow a fire to develop and even propagate. Once the fire is in progress, not only a dangerous effort of the fire brigade due to limited access to the zone has to be taken into consideration, but also the effects on the machine.

The energy stored in one LHC dipole is 7.6 MJ, thus with 1,232 dipoles in the LHC arcs in total this amounts to 9.4 GJ. This latter value corresponds to the energy stored in 2 tons of TNT, which could melt 20 tons of copper [8]. It is therefore clear that the consequences of a fire in one of the LHC arcs can cause unforeseen damage (e.g. explosion).

Although the magnets do contain polymers of Group 2, the fire load of the area is mainly determined by the amount of cables. The polymers of the magnets are an inherent part of the mechanical structure and are not directly exposed to air, whereas the cables in the cable trays along the wall of the tunnel are openly accessible. In addition, power converters and quench protection racks underneath the magnets present a possible source of ignition and combustible material.

A fire simulation conducted for another part of the LHC tunnel at point 7 assumes a fire originating in the cable trays and shows that once this fire is in progress, it can cause serious damage. Besides the generation of smoke and soot, peak temperatures can reach up to approximately 1,500 K. Depending on the configuration of the ventilation system (open and closed), considerable amounts of combustible material are consumed and the duration of the fire varies between 3,000 and 700 seconds. Although this study states that the probability of a fire occurring in this area is close to zero due to preventive measures, it nevertheless gives serious weight to the installation of fire and smoke detectors [58].

Alcoves:

The alcoves of the LHC, located at both sides of the arcs, mainly house the electrical distribution equipment for the LHC machine and the UPS system. A fire in these areas is a major concern with regard to severe consequences for LHC operation and an extended downtime.

The limited space and layout of the alcoves has lead to a rather close assembly of equipment, thereby increasing the potential development of heat and ignition sources. With transformers, switchboards and the UPS system some vital equipments are housed in these areas, and a fire is therefore by no means acceptable. The history of fires at CERN shows that three of them occurred as a result of faulty electrical equipment, that is to say signal cables, a patch panel and a transformer. Keeping this experience in mind, the combination of electrical equipment as the failure cause as well as the combustible material in the alcoves, importance has to be attached to these areas.

These sensitive areas are also equipped with fire and smoke detectors. However, due to the amount of equipment in a small area, the frequency of occurrence remains unclear. Therefore the alcoves are included in this list of hazardous areas.

7.2 Quantitative Analysis - Expert Judgement

In order to be able to quantify the frequency of occurrence and the severity of consequences, the Failure Modes and Effects Analysis for electrical installations was extended by an expert judgement (Table 7.4).

Three experts in electrical and electronic engineering with many years of experience at CERN were chosen. With the help of the pre-determined frequency and severity classifications, each failure mode was assessed. Concerning the severity, the failure modes were judged independently regarding (a) global consequences for the LHC machine operation and (b) local consequences for equipments. Then the average of all three subjective opinions was taken and the results presented in risk matrices (Figures 7.1 and 7.2).

It must be mentioned that actually all failure modes potentially threatening the operation of the machine are situated within the transition area of the risk matrix. Regarding local consequences for equipment in the tunnel a similar situation is arising, except for one failure mode being situated in the unacceptable risk area. The FMEA on which these risk matrices are based, is showing possible ways of creating ignition sources; it does not necessarily imply the emerging of a fire as a consequence. Nevertheless the judgement rates the failure modes as most likely hazardous for machine operation and equipments.

By definition for any frequency/consequence pair located within the transition area the necessity of risk-reducing measures has to be discussed. In the present case it is debatable if improvement is required or even possible. During the design phase of individual systems failures have been considered naturally and taken care of. However, the complexity of the whole structure does imply unexpected incidents and adverse combinations of incidents eventually leading to more severe consequences. Due to the space restrictions in the tunnel and the advanced project stage at the present time, modifications of the original design or additional arrangements would be difficult to implement and rather costly in terms of time and money.

This risk matrix does not directly show the fire risk within the LHC, but only possible initial events. Although the possibilities of intervening at the present stage are low, this assessment done by internal experts certainly directs attention to fire risk in the LHC and recalls the importance of regular check-ups. With respect to the areas of concern (see 7.1.3) it is justified to question if existing prevention and safety measures are sufficient.

The failure modes of overheating as well as short circuit and ground fault are situated in the same area of the risk matrix concerning the operation of the machine. This assessment was expected, as these two failure modes are connected closely in the way that one can cause the other and vice versa. However, it is significant that local effects of overheating on equipment is rated as much more severe than the general effects on machine operation, since this shifts it into the unacceptable risk area. In spite of the LHC cooling and ventilation system, the expert judgement still points out a particular hazard through local overheating

FM Ref	Failure Mode	Possible Causes	Consequences	Severity Class	Frequency Class
1	Overheating	Failure of electrical insulation Incorrect installation Bad contacts Overcurrent in a cable Misuse (i.e. running a high-powered appliance off a low-power extension cable) Short and ground circuit fault Mechanical distortion modifying electrical contacts or insulating material Failure of a component, an internal part or an associated system (i.e. ventilation) External heating (ambient temperature in the LHC tunnel approximately 30°C)	Gradual temperature rise Accumulation of heat and effluent in the vicinity Spark generation Thermal ageing of insulating material Accumulation and diffusion of flammable gases in air may give rise to an ignition or explosion	2.3a/3.3b	4.3
2	Short circuit and ground fault	Mechanical impact (i.e. during installation, maintenance) Incorrect installation Defective cables Disengaged conductors, bad contacts Ingress of conducting foreign bodies Sudden failure of component or internal part Failure of electrical insulation Flooding	Abnormal temperature rise (significant after short time, localised) Possible emission of light, smoke, flammable gases Release of glowing materials or substances Arcing	2.3a/2.3b	4.7
3	Arcing	Failure of electrical insulation (damage) Overcurrent Incorrect installation (action exposing live parts or bringing them together) Short and ground circuit fault	Intensive heat in a small volume Point source ignitor Possible emission of light, flammable gases and flames	3.3a/3.3b	3.0

continued on next page

continued from previous page

FM Ref	**Failure Mode**	**Possible Causes**	**Consequences**	**Severity Class**	**Frequency Class**
		Rupture of a contact Sudden failure of component or internal part Mechanical impact (i.e. during installation, maintenance)			
4	Bad contacts	Abrasion Mechanical distortion modifying electrical contacts Incorrect installation High transition resistance Mechanical impact (i.e. during installation, maintenance) Corrosion	Gradual temperature rise Accumulation of heat in the vicinity Short circuit and ground fault Overheating Accumulation and diffusion of flammable gases in the vicinity	2.0a/2.3b	5.0
5	Failure of electrical insulation	Mechanical impact (i.e. during installation, maintenance) Bad quality Abrasion (i.e. friction) Conducting dust Humidity Conducting foreign bodies Ageing Incorrect installation Damage	Accumulation and diffusion of flammable gases in the vicinity Overheating Arcing Gradual temperature rise Accumulation of heat in the vicinity Short circuit and ground fault	3.0a/3.0b	3.7
6	Circuit-circuit fault	Mechanical impact (i.e. during installation, maintenance) Squashed cables Incorrect installation	Possible emission of visible light, flammable gases and flames Accidental coupling of two circuits Short circuit and ground fault Spark generation	3.3a/3.0b	3.3

continued on next page

continued from previous page

FM Ref	**Failure Mode**	**Possible Causes**	**Consequences**	**Severity Class**	**Frequency Class**
7	Protection failure	Internal failure of protection device	Overload		
		Ageing	Short circuit and ground fault	3.7a/4.0b	3.3
		Mechanical impact (i.e. during installation, maintenance)			
8	Transfer of component failure	Internal failure of equipment	Transfer of failure to the power system	4.0a/4.0b	3.7
		No protection device to avoid transfer			
		Failure of protection device			
9	Missed quality control	Mechanical impact after commissioning (i.e. during installation of adjacent equipment)	Degradation of the system	2.7a/2.3b	4.7
		No inspection, no commissioning	Power failure		
		Incorrect installation			

Table 7.4: Failure modes for electrical installations - integration of frequency and consequence analysis (following [55])

of equipment. Although the cooling and ventilation system is already in place as a risk reducing measure, this outcome again advises special caution and suggests frequent and numerous check-ups as often as temporary machine shutdowns allow it.

Similar to a short circuit and ground fault is the accidental coupling of two independent circuits. More severe regarding global than local effects, this failure mode overall is rated with a rather high severity compared to a short circuit and ground fault. Contrary to expectations, its frequency is fairly low. Due to space restrictions in the tunnel and therefore possible mishaps during installation, maintenance and trouble-shooting, its frequency of occurrence was anticipated to be much higher.

The failure mode of bad contacts is located right on the upper bound of the transition area in both matrices. This reflects what has been mentioned before: because of the amount of cables and therefore cable junctions in the LHC its frequency of occurrence is presumably rather high. Its severity with respect to local effects on equipment is judged even more significant, which is a reasonable result.

Missed quality control has worse effects on the operation of the machine globally than locally on the equipment itself. Good design of equipment is a key characteristic for a flawless operation. However, quality control is essential in order to check on correct installation and make sure the components can actually work according to their intended purpose. For an installation such as the LHC, inspection of equipment is a major undertaking and might imply both overlapping as well as overlooking of important details.

The failure of electrical insulation is hazardous to the same degree on a local as well as a global level. The reason for this can be attributed to the fact that once a cable is destroyed, it also constrains an electrical circuit which may be important for one or more LHC subsystems. Although this failure mode can have quite severe consequences such as overheating, short circuit and ground fault, arcing or the accumulation and diffusion of flammable gases in the vicinity, the result of the expert judgement is not as pessimistic as expected.

The severity of an internal failure of protection devices of a LHC subsystem is judged as being able to threaten the operation of the machine severely, and even more so the state of equipment locally. Closely connected is the transfer of this failure from the individual component to the power system. Regarding effects on machine operation, this is the failure mode with the most severe consequences. This is plausible, as any fault affecting the power system has to be a hazard for operation. Since a transfer can only happen when an internal failure of equipment and a malfunction of the protection device occur at the same time, its frequency of occurrence is higher than the value for a protection device failure on its own, as anticipated. This also reflects the high reliability values of state-of-the-art electronic devices.

At last, arcing is the failure mode with the lowest frequency, but a fairly high severity for both machine operation and equipment. As it is situated on the lower bound of the transition area, it is actually judged as presenting the smallest risk with respect to creating ignition sources.

In conclusion, all failure modes but one assessed by means of an expert judgement are situated within the transition area of the risk matrices. This means that necessary actions must be discussed and justified both in terms of financial impact as well as time and effort concerning re-design, purchasing and installation. Due to the advanced stage of the LHC

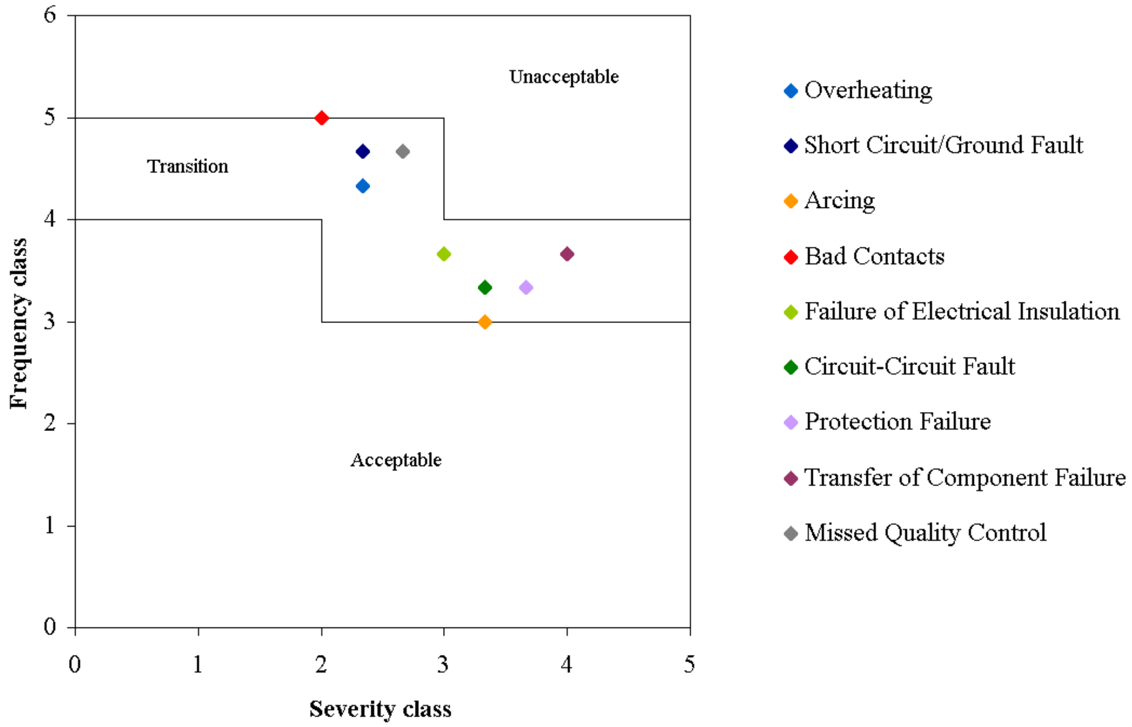


Figure 7.1: Risk matrix - Consequences for machine operation (a)

project, inherent measures to the entire system can not be implemented. Actions must be arranged concerning effectiveness and sufficient employment of already existing safety measures. This concerns systems which come into play after an incident has occurred and are actually designed to mitigate its effects, i.e. fire and smoke detectors and the training of personnel.

7.3 Quantitative Analysis - A Detailed Approach

The material data of the different LHC subsystems and their location in the underground area formed the basis for the fire risk analysis of the previous chapter. Due to the size and complexity of the LHC, the uncertainty of the collected data was expected, even the deliberate omission of certain equipment families. The combination of the Failure Modes and Effects Analysis with the material data project revealed hazardous areas in the LHC underground area. With the help of frequency and consequence analysis based on expert judgement, an assessment of possible fire causes (ignition sources) could be carried out. However, a magnitude for the fire risk in the tunnel could not be given yet. In consequence, an assessment of the fire risk including all electrical equipment will be approached in the following chapter.

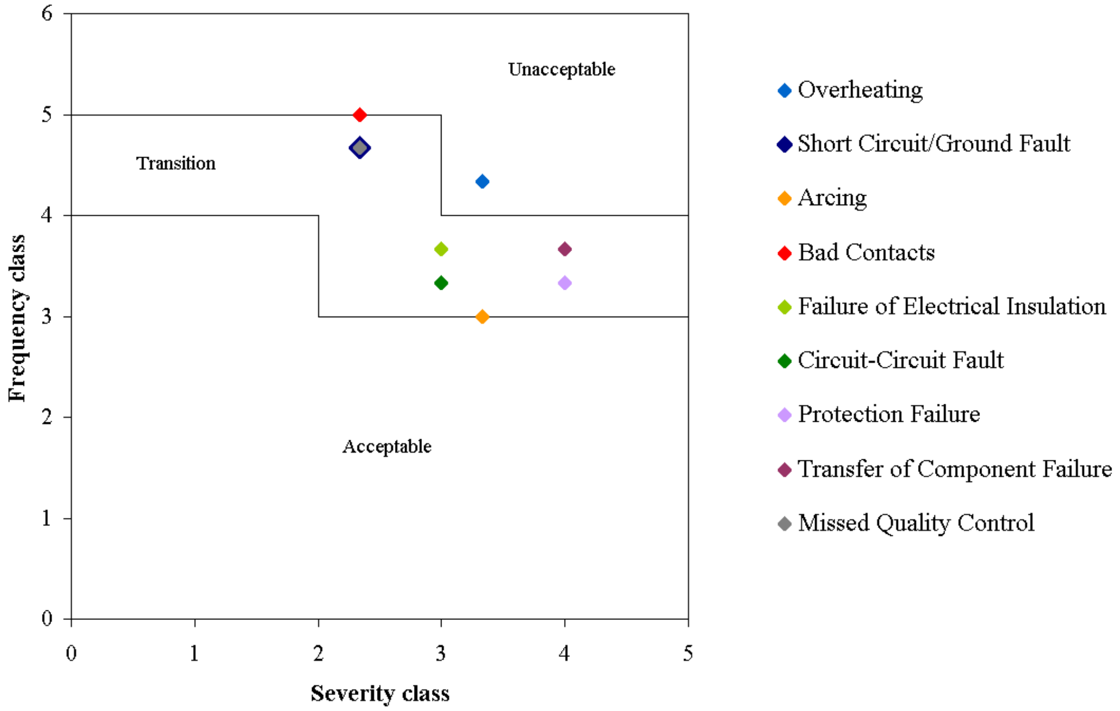


Figure 7.2: Risk matrix - Consequences for the equipment (b)

7.3.1 Risk Layer Along the Underground Area

As mentioned previously, there is electrical equipment in the underground area which has not been included in the study, as it was not possible to integrate it into the material data project. As the project was aiming at collecting data concerning the most important and comparatively largest equipments, this equipment has not been entirely included. Although for some of the equipment families their electrical components have been integrated, other equipments have not even been mentioned. This means that the actual amount of electrical equipment and thus on the one hand combustible material and on the other hand potential ignition sources is even higher than shown in Table 7.1.

The type of equipment concerned comprises mainly high voltage transformers as well as low power apparatus such as switchgears, batteries, UPS systems, electronic racks and computers for supervision, distributed over the entire underground area. The detailed recording of these equipments and their integration into the assessment of the fire risk is difficult to carry out. Moreover, the warm cables of the LHC posed another difficulty in terms of fire risk assessment. The amount of different cable types and therefore varying fire properties so far could not be integrated into the study in a feasible way.

For this reason, the nomination of a risk layer is introduced. As locating all combustible material in the tunnel in detail is impossible, the risk layer is supposed to present the amount of inflammable material as well as electrical equipment as the possible ignition sources as a layer equally distributed along the main tunnel, technical galleries and alcoves. Included in this risk layer will be the warm cables and all equipment mentioned previously which has not been incorporated in the material data project. Independent of the accumulation of combustible materials in certain areas, the evaluation of fire risk due to electrical equipment will be calculated as equal in every position in the underground.

The objective of this thesis is to give an order of magnitude for the fire risk of this risk layer in the LHC underground. The reasons for introducing this equally distributed risk layer can be derived from two different motivations. On the one hand the inability of incorporating every type of equipment in the material database implicates an imprecision of the analysis carried out in chapter 6. And on the other hand the fact that fires in low power apparatus do occur quite frequently has to be taken into account. Since low power equipment is not controlled as strictly as high power equipment, the possibility of failures occurring is increasingly apparent. With the idea of a risk layer along the underground areas, these concerns are being taken into account.

Although the approximation is rather inaccurate, the complexity of the LHC nevertheless justifies a preferably simple and safe approach to estimating fire risk. Since also quantitatively unknown inflammable material will be included in the results, the possibility exists that in this way the fire risk will be overestimated. However, as the LHC is such a prestigious project, where a fire accident could mean an extended downtime and involve high costs, it is reasonable to be on the safe side.

7.3.2 Fault Tree Analysis

The Failure Modes and Effects Analysis for electrical installations is intended on the one hand to describe the system under investigation and on the other hand to identify failure modes which can lead to a fire. In addition, the frequency and consequence analysis and eventually the creation of a risk matrix presents a transition from a qualitative to a quantitative analysis. As the assessment of frequency of occurrence and severity of consequences is actually based on expert judgement and is therefore rather unsatisfactory, a way of approaching the problem of a more in-depth assessment and the examination of the failure origin is a fault tree analysis.

A fault tree analysis is a graphical and very descriptive way of illustrating the events leading to the system failure, determining the causes of the incident on a more detailed level compared to the FMEA. The most important advantage though from the point of view of frequency analysis is the determination of the basic events. As these are intended to describe faults on the lowest level of the analysis concerning the component structure of the system, it is supposed to be much easier to assign a value to the frequency of occurrence. Through applying basic Boolean algebra starting from the basic events at the bottom of the tree up to the top event, the probability of failure of the entire system can be calculated.

The top event for the fault tree will be defined as “fire in the LHC underground” due to faulty electrical equipment. With this universal approach it is possible to determine the probability of fire in the tunnel, revealing also the development and the contributing factors.

Certainly the results of the fault tree analysis have to be discussed according to the source of the frequency values attributed to the basic events. Depending on the source, they can vary to a great extent. However, in comparison to the FMEA, the fault tree analysis addresses the global system failure and asks progressively about the contributing factors, which means that the core of the problem is tackled and examined. In the case of the LHC, the occurrence of an ignition source would be tracked to the bottom of the problem, aiming at the triggering factors.

7.3.2.1 Fault Tree Development

In this chapter, the assessment of the risk layer in the LHC tunnel is completed by means of a fault tree analysis. As mentioned above, the fault tree has been developed in a universal way, valid for any position in the tunnel (Figures 7.3, 7.4 and 7.5).

The fault tree has been drawn up with the help of a software programme which allows to arrange the structure clearly and also includes features for qualitative as well as quantitative analysis. OpenFTA is an open source programme and was developed by Formal Software Construction Limited [59].

As the present fault tree is very complex and a fault tree analysis does have some restrictions concerning the events and their interactions, explanations will be given in the following paragraphs.

The tree was developed top down with a possible fire in the LHC underground due to failures of electrical equipment as the top event. Following the three basic conditions for the general development of a fire, the first level of intermediate events was apparent: an ignition source, inflammable material and oxygen. However, oxygen has not been included formally into the fault tree, as oxygen in the form of air is available anywhere in the tunnel. As the failure probability of this basic event is 1 and it is logically linked with an AND gate, it would not influence the quantitative analysis of the fault tree.

One of the reasons for the execution of this study was the worry about sufficient safety measures such as fire and smoke detectors. As these detectors are only found in certain areas of the LHC, the possible states of this system (non-existent, failing and reacting too late) have to be taken into account. Therefore the possibility of a non-detected fire or smoke had to be included at this stage of the analysis. The case in which the fire brigade does not respond to a given alarm is added, as human error concerning the correct reaction as well as technical problems is probable. The causes involved could be mistaking the alarm for a test or the dysfunction of the Safety Control Room (SCR).

Two causes influence the presence of inflammable material. On the one hand it can be the poor fire reaction of certain material. On the other hand a failure of an associated system (cooling and ventilation) can create extreme thermal conditions (overheating), thereby promoting a poor fire reaction of usually fire-resisting material.

The question why there is actually any material present with poor fire properties can be answered quite simply. First, inflammable material is necessary for certain equipment types. This fact is supposed to be reported by the responsible group and approved by the competent authorities in the form of derogations to existing rules and regulations (e.g. septa

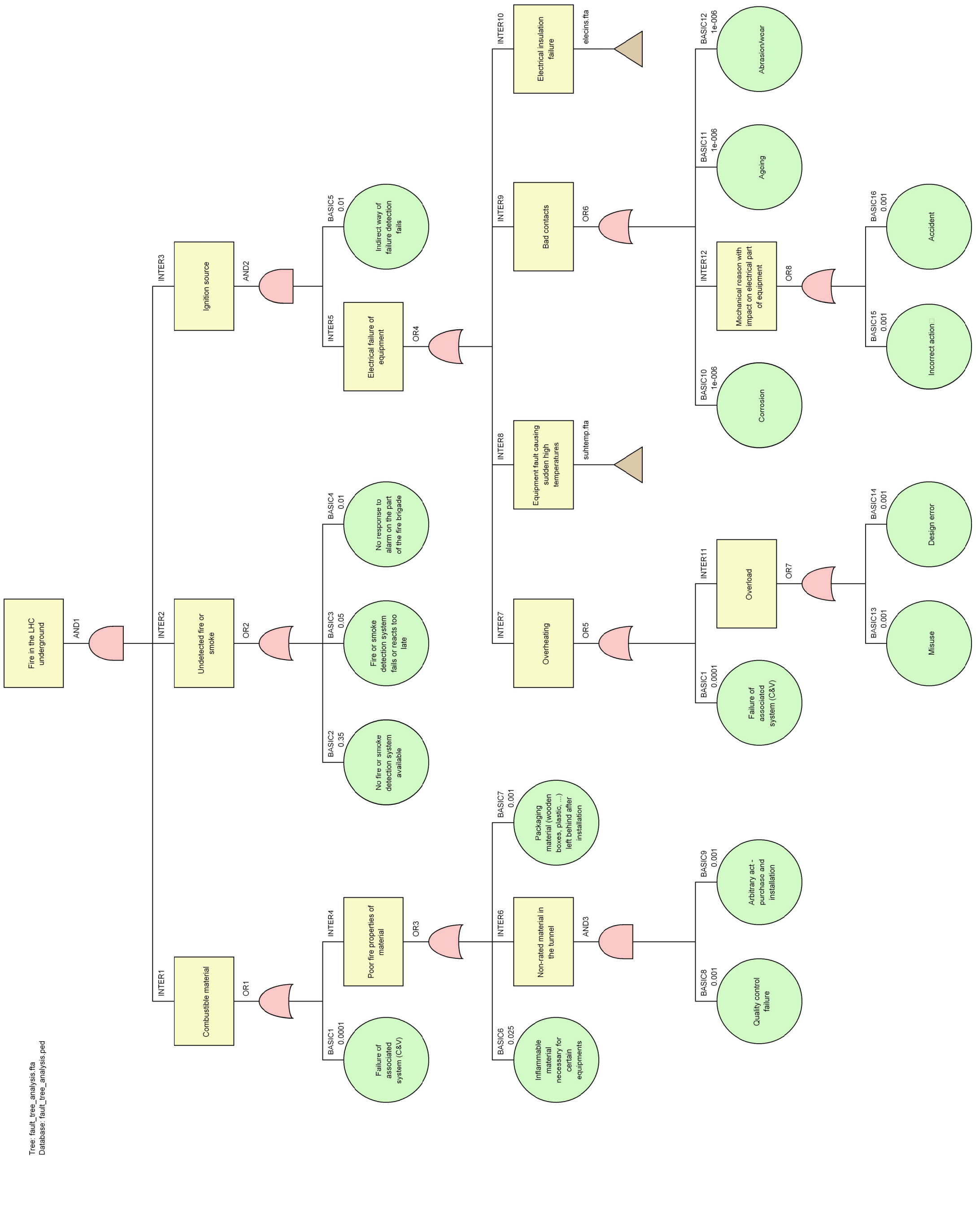

Tree: fault_tree_analysis.fta
Database: fault_tree_analysis.ped
Fire in the LHC underground
AND1
INTER1
Combustible material
OR1
INTER2
Undetected fire or smoke
OR2
INTER3
Ignition source
AND2
BASIC1 0.0001
Failure of associated system (C&V)
INTER4
Poor fire properties of material
OR3
BASIC2 0.35
No fire or smoke detection system available
BASIC3 0.05
Fire or smoke detection system fails or reacts too late
BASIC4 0.01
No response to alarm on the part of the fire brigade
INTER5
Electrical failure of equipment
OR4
BASIC5 0.01
Indirect way of failure detection fails
BASIC6 0.025
Inflammable material necessary for certain equipments
INTER6
Non-rated material in the tunnel
AND3
BASIC7 0.001
Packaging material (wooden boxes, plastic, ...) left behind after installation
INTER7
Overheating
OR5
INTER8
Equipment fault causing sudden high temperatures
suhtemp.fta
INTER9
Bad contacts
OR6
INTER10
Electrical insulation failure
elecins.fta
BASIC8 0.001
Quality control failure
BASIC9 0.001
Arbitrary act - purchase and installation
BASIC1 0.0001
Failure of associated system (C&V)
INTER11
Overload
OR7
BASIC10 1e-006
Corrosion
INTER12
Mechanical reason with impact on electrical part of equipment
OR8
BASIC11 1e-006
Ageing
BASIC12 1e-006
Abrasion/wear
BASIC13 0.001
Misuse
BASIC14 0.001
Design error
BASIC15 0.001
Incorrect action
BASIC16 0.001
Accident

Figure 7.3: Fault tree analysis - Top event “Fire in the LHC underground”

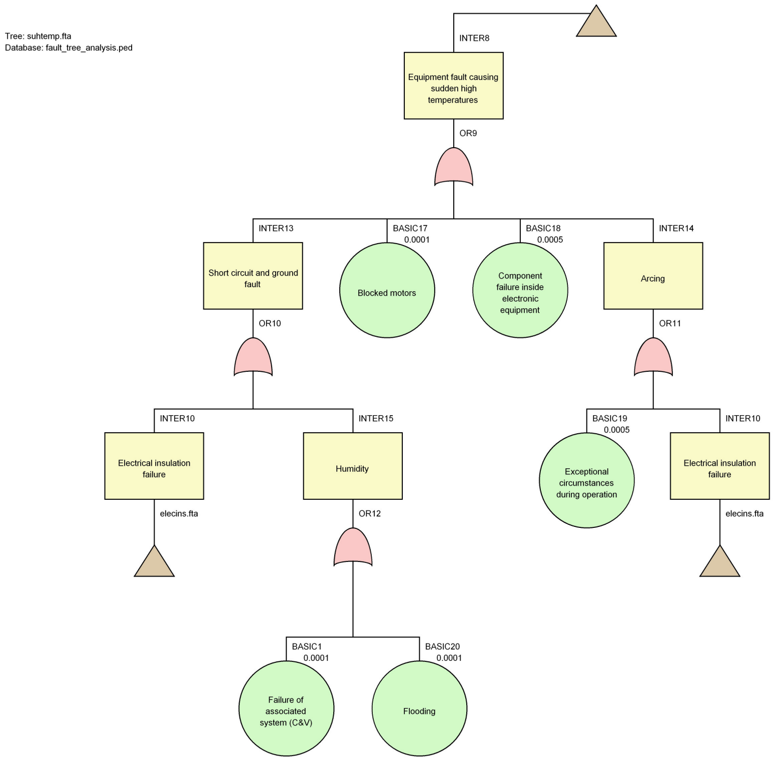

Tree: suhtemp.fta
Database: fault_tree_analysis.ped
INTER8
Equipment fault causing sudden high temperatures
OR9
INTER13
Short circuit and ground fault
BASIC17
0.0001
Blocked motors
BASIC18
0.0005
Component failure inside electronic equipment
INTER14
Arcing
OR10
OR11
INTER10
Electrical insulation failure
INTER15
Humidity
BASIC19
0.0005
Exceptional circumstances during operation
INTER10
Electrical insulation failure
elecins.fta
OR12
elecins.fta
BASIC1
0.0001
Failure of associated system (C&V)
BASIC20
0.0001
Flooding

Figure 7.4: Fault tree analysis - Subtree 1

magnets). Second, packaging material such as wooden boxes or plastics has been left behind by workmen after installation, either due to carelessness or malice. Third, non-rated material was installed in the tunnel (i.e. non-standard cables). This is possible when at the same time people have arbitrarily decided to violate the rules and quality control (i.e. inspections) of installed equipment has failed. The latter two failures are both down to human error.

The analysis of the development of an ignition source due to the failure of electrical equipment in the LHC underground obviously makes the biggest part of the fault tree. In case a smoulder or fire occurs e.g. in an electronic rack, the affected system would not give green light for operation. This means that in the CERN Control Centre (CCC) the operators would have to trace the problem of this system, which would eventually involve people being sent to the tunnel for investigation. This would present an indirect way of detecting a possible ignition source, if the time between the occurrence of the problem and the actual physical intervention is not long enough for a fire to develop. However, if this indirect possibility of detection fails, the equipment failure might cause a source of ignition.

The subject of electrical faults and the detailed analysis of their causes are very complex and delicate. As Babrauskas [42] mentions in his article about electrical faults associated with wiring or with wiring devices in 120/240 V distribution systems, the evolution of an electrical failure is usually not just one, but a chain of events. As an example, faulty cable insulation can lead to a short circuit, which on his part can provoke electric arcing. The lack of studies dealing with the basic physical mechanisms of electrical faults and the possibilities of their

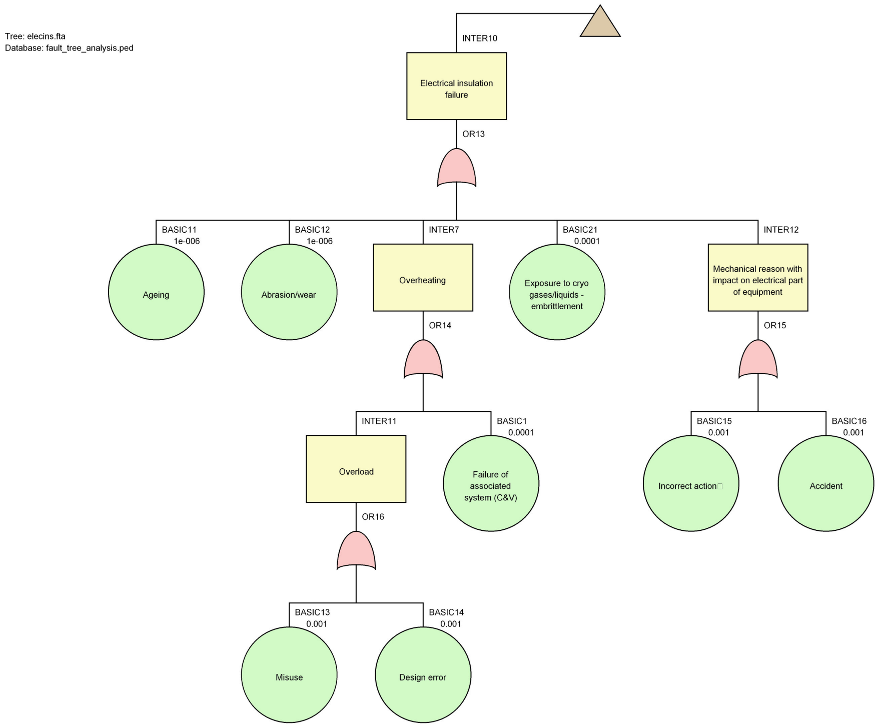


Figure 7.5: Fault tree analysis - Subtree 2

origins makes their investigation even more difficult.

Most of the electrical failures shown in the fault tree are dependent on each other and can occur in almost any sequence. As an example, on the one hand a faulty insulation can lead to overload and eventually to a short circuit. But overload of a cable due to design failures or misuse can on the other hand provoke a faulty insulation and then a short circuit. The different possibilities of interconnections among these different fire causes present a circumstance which makes the development of the fault tree rather complicated. However, questioning the actual cause (basic events) and the subsequent development of a failure is essential for the fault tree analysis.

As the system description for a fault tree analysis is always static and the failures are not time-dependent, the fault tree shows the state of the system in one particular moment in time. It presents a way of tracking possible failure sequences from the basic event up to the top event, but does not take into account any time dependencies of the failures with one another. So it would only reveal the probability that at one particular moment a bad contact, a short circuit or any other of the mentioned failures occur, but not how this failure state has developed over time.

A second and also important issue for the development of a fault tree is the fact that it is not possible to include any loops. Possible ignition sources do not only occur once, but a few times. It was decided that some of these fire causes in certain cases do not directly lead to an ignition source, but may provoke other faults which eventually present an ignition source. In this way some chains were deliberately included in the fault tree, but any inverse direction was avoided in order not to create loops.

It has to be stressed that the fault tree at hand is only one possibility of presenting the subject of fires due to failures of electrical equipment. Keeping the afore made assumptions and preconditions in mind, the final result for the fire risk in the LHC tunnel has to be discussed with furthermost caution.

The equipment failures due to electrical reasons were divided into the following groups: overheating, bad contacts, electrical insulation failure and faults causing sudden high temperatures. The first three are distinguished from the latter, as they are characterised by a rather gradual temperature rise over a long period of time compared to a significant temperature rise within a short period of time. The last group is further classified and contains short circuit and ground fault, arcing, component failures inside electronic equipment and blocked motors.

A few more failures within the latter group could be mentioned (such as explosion of capacitors or winding short circuit). However, they present special cases of the basic failures with actually the same causes. They will not be included in this fault tree, since the repetition of the basic events for very similar immediate events would distort the result for the top event.

Overheating of a cable can be caused by an overload or the failure of an associated system such as cooling and ventilation [60]. By failing to cool the equipment itself or neighbouring systems, external heat sources and therefore extreme thermal ambient conditions can be created. External heat sources might even emerge in spite of a perfect design, as the operation of the machine can lead to non-intended conditions (long-term effects). The causes for overload can either be a design failure or the misuse of electric equipment, such as feeding more consumers than actually designed for or running the equipment under abnormal conditions. Both are human failures, but they are not mentioned together, since their origins are of a different nature.

Unlike overheating, bad contacts do not occur along the full length of the cable, but only at cable junctions or interconnections. These are the spots where corrosion, ageing and abrasion appear, or where a mechanical problem can lead to a loose connection and an abnormally high transition resistance. The transformation of this high resistance into heat energy can lead to glowing connections [42]. A bad contact would be very difficult to detect, as its development can take weeks. This means that during the progress of transition resistance rise-up until the failure becomes acute, the connection is still working.

Mechanical reasons for bad contacts are generally caused by human error. This failure “mode” is mentioned twice, once implying an incorrect human action, and once meaning an accident or mishap. Incorrect human action could be failures during installation or commissioning or even malice; accidents are unintended actions such as a mishap with the transport vehicle or a handling accident.

The amount of cables and the number of different cable types in the tunnel is very high, the problem of failing cable insulation is therefore apparent. On the one hand there are natural causes of failure such as abrasion and ageing of material, and on the other hand there is certainly possible mechanical impact damaging the insulation from the outside as well as overheating leading to carbonizing and melting of insulation [60]. A special danger for insulation material in the LHC tunnel is the presence of cryogenic gases. In case of leakage of helium from the cryogenic system, the insulating material may embrittle and deteriorate faster than actually expected. Regarding the mechanical causes of insulation failure, the same explanations as for bad contacts apply.

Short circuit or ground fault occur when either two conductors of different potentials are in contact or current flows between a conductor and the earth. As the resistance is very low, the short circuit current is between 10 to 20 times higher than nominal current. Because of the released heat energy, short circuit or ground fault may be ignition sources and cause fires or explosions [60].

Reasons for the occurrence of short circuits or ground faults can be an electrical insulation failure or an abnormally high humidity. The latter can allow the current to flow along a different path than intended (water as the conducting material). This may happen either directly due to a flooding or indirectly due to the failure of an associated system (i.e. condensation).

An electric arc is created when current flows through air from one conductor to the other. Air is usually an insulator; however, if the surrounding conditions (sufficient electric field strength to exceed its dielectric strength) allow the air to be ionised, it can become conductive. Extremely high temperatures of a few 1,000°C and therefore a vaporization of metal create high pressure and cause a blast [61, 62].

Similar to the causes of a short circuit or ground fault, electrical arcing is provoked through a failure of electrical insulation or exceptional circumstances during operation. Exceptional circumstances can create unexpected conditions and facilitate the development of an arc (i.e. inappropriate electrical switching or an interlock override).

Blocked motors as well as failures of components inside electronic equipment are also failures causing sudden high temperatures.

The failure mode of human error has the greatest influence on the final result. It is represented in most of the subtrees, thereby stressing its importance for the analysis. Although any mistake or mishap should be reported, this is dependent on the advertency as well as the sincerity of the individual. The fault tree was not developed in any more detail concerning failures of personnel (including noticing/not noticing and reporting/not reporting an accident or incorrect action, etc.), as human error would have been overrated.

7.3.2.2 Qualitative Analysis

After developing the fault tree, the qualitative analysis is done by determining its minimal cut sets. A minimal cut set is the smallest set of a minimum number of failing basic events which result in a breakdown of the system, thus the top event. If one basic event is removed, the remaining basic events are not a cut set anymore, which means that they are not able to lead to a system failure.

In the OpenFTA software the determination of minimal cut sets is an integrated feature for the analysis. The following report is generated:

```
Minimal Cut Sets
================

Tree:  fault_tree_analysis.fta
Time:  Tue Mar 13 10:47:06 2007

Method:  Algebraic

No.  of primary events = 21
Minimal cut set order = 1 to 21

Order 1:

Order 2:

Order 3:
1) BASIC1 BASIC2 BASIC5
2) BASIC1 BASIC3 BASIC5
3) BASIC1 BASIC4 BASIC5

Order 4:
1)  BASIC10 BASIC2 BASIC5 BASIC6
2)  BASIC10 BASIC2 BASIC5 BASIC7
3)  BASIC10 BASIC3 BASIC5 BASIC6
4)  BASIC10 BASIC3 BASIC5 BASIC7
5)  BASIC10 BASIC4 BASIC5 BASIC6
6)  BASIC10 BASIC4 BASIC5 BASIC7
7)  BASIC11 BASIC2 BASIC5 BASIC6
8)  BASIC11 BASIC2 BASIC5 BASIC7
9)  BASIC11 BASIC3 BASIC5 BASIC6
10) BASIC11 BASIC3 BASIC5 BASIC7
11) BASIC11 BASIC4 BASIC5 BASIC6
12) BASIC11 BASIC4 BASIC5 BASIC7
13) BASIC12 BASIC2 BASIC5 BASIC6
14) BASIC12 BASIC2 BASIC5 BASIC7
15) BASIC12 BASIC3 BASIC5 BASIC6
16) BASIC12 BASIC3 BASIC5 BASIC7
17) BASIC12 BASIC4 BASIC5 BASIC6
18) BASIC12 BASIC4 BASIC5 BASIC7
19) BASIC13 BASIC2 BASIC5 BASIC6
20) BASIC13 BASIC2 BASIC5 BASIC7
21) BASIC13 BASIC3 BASIC5 BASIC6
22) BASIC13 BASIC3 BASIC5 BASIC7
23) BASIC13 BASIC4 BASIC5 BASIC6
24) BASIC13 BASIC4 BASIC5 BASIC7
25) BASIC14 BASIC2 BASIC5 BASIC6
26) BASIC14 BASIC2 BASIC5 BASIC7
27) BASIC14 BASIC3 BASIC5 BASIC6
```

```
28) BASIC14 BASIC3 BASIC5 BASIC7
29) BASIC14 BASIC4 BASIC5 BASIC6
30) BASIC14 BASIC4 BASIC5 BASIC7
31) BASIC15 BASIC2 BASIC5 BASIC6
32) BASIC15 BASIC2 BASIC5 BASIC7
33) BASIC15 BASIC3 BASIC5 BASIC6
34) BASIC15 BASIC3 BASIC5 BASIC7
35) BASIC15 BASIC4 BASIC5 BASIC6
36) BASIC15 BASIC4 BASIC5 BASIC7
37) BASIC16 BASIC2 BASIC5 BASIC6
38) BASIC16 BASIC2 BASIC5 BASIC7
39) BASIC16 BASIC3 BASIC5 BASIC6
40) BASIC16 BASIC3 BASIC5 BASIC7
41) BASIC16 BASIC4 BASIC5 BASIC6
42) BASIC16 BASIC4 BASIC5 BASIC7
43) BASIC17 BASIC2 BASIC5 BASIC6
44) BASIC17 BASIC2 BASIC5 BASIC7
45) BASIC17 BASIC3 BASIC5 BASIC6
46) BASIC17 BASIC3 BASIC5 BASIC7
47) BASIC17 BASIC4 BASIC5 BASIC6
48) BASIC17 BASIC4 BASIC5 BASIC7
49) BASIC18 BASIC2 BASIC5 BASIC6
50) BASIC18 BASIC2 BASIC5 BASIC7
51) BASIC18 BASIC3 BASIC5 BASIC6
52) BASIC18 BASIC3 BASIC5 BASIC7
53) BASIC18 BASIC4 BASIC5 BASIC6
54) BASIC18 BASIC4 BASIC5 BASIC7
55) BASIC19 BASIC2 BASIC5 BASIC6
56) BASIC19 BASIC2 BASIC5 BASIC7
57) BASIC19 BASIC3 BASIC5 BASIC6
58) BASIC19 BASIC3 BASIC5 BASIC7
59) BASIC19 BASIC4 BASIC5 BASIC6
60) BASIC19 BASIC4 BASIC5 BASIC7
61) BASIC2 BASIC20 BASIC5 BASIC6
62) BASIC2 BASIC20 BASIC5 BASIC7
63) BASIC2 BASIC21 BASIC5 BASIC6
64) BASIC2 BASIC21 BASIC5 BASIC7
65) BASIC20 BASIC3 BASIC5 BASIC6
66) BASIC20 BASIC3 BASIC5 BASIC7
67) BASIC20 BASIC4 BASIC5 BASIC6
68) BASIC20 BASIC4 BASIC5 BASIC7
69) BASIC21 BASIC3 BASIC5 BASIC6
70) BASIC21 BASIC3 BASIC5 BASIC7
71) BASIC21 BASIC4 BASIC5 BASIC6
72) BASIC21 BASIC4 BASIC5 BASIC7
```

```
Order 5:
1)  BASIC10 BASIC2 BASIC5 BASIC8 BASIC9
2)  BASIC10 BASIC3 BASIC5 BASIC8 BASIC9
3)  BASIC10 BASIC4 BASIC5 BASIC8 BASIC9
4)  BASIC11 BASIC2 BASIC5 BASIC8 BASIC9
5)  BASIC11 BASIC3 BASIC5 BASIC8 BASIC9
6)  BASIC11 BASIC4 BASIC5 BASIC8 BASIC9
7)  BASIC12 BASIC2 BASIC5 BASIC8 BASIC9
8)  BASIC12 BASIC3 BASIC5 BASIC8 BASIC9
9)  BASIC12 BASIC4 BASIC5 BASIC8 BASIC9
10) BASIC13 BASIC2 BASIC5 BASIC8 BASIC9
11) BASIC13 BASIC3 BASIC5 BASIC8 BASIC9
12) BASIC13 BASIC4 BASIC5 BASIC8 BASIC9
13) BASIC14 BASIC2 BASIC5 BASIC8 BASIC9
14) BASIC14 BASIC3 BASIC5 BASIC8 BASIC9
15) BASIC14 BASIC4 BASIC5 BASIC8 BASIC9
16) BASIC15 BASIC2 BASIC5 BASIC8 BASIC9
17) BASIC15 BASIC3 BASIC5 BASIC8 BASIC9
18) BASIC15 BASIC4 BASIC5 BASIC8 BASIC9
19) BASIC16 BASIC2 BASIC5 BASIC8 BASIC9
20) BASIC16 BASIC3 BASIC5 BASIC8 BASIC9
21) BASIC16 BASIC4 BASIC5 BASIC8 BASIC9
22) BASIC17 BASIC2 BASIC5 BASIC8 BASIC9
23) BASIC17 BASIC3 BASIC5 BASIC8 BASIC9
24) BASIC17 BASIC4 BASIC5 BASIC8 BASIC9
25) BASIC18 BASIC2 BASIC5 BASIC8 BASIC9
26) BASIC18 BASIC3 BASIC5 BASIC8 BASIC9
27) BASIC18 BASIC4 BASIC5 BASIC8 BASIC9
28) BASIC19 BASIC2 BASIC5 BASIC8 BASIC9
29) BASIC19 BASIC3 BASIC5 BASIC8 BASIC9
30) BASIC19 BASIC4 BASIC5 BASIC8 BASIC9
31) BASIC2 BASIC20 BASIC5 BASIC8 BASIC9
32) BASIC2 BASIC21 BASIC5 BASIC8 BASIC9
33) BASIC20 BASIC3 BASIC5 BASIC8 BASIC9
34) BASIC20 BASIC4 BASIC5 BASIC8 BASIC9
35) BASIC21 BASIC3 BASIC5 BASIC8 BASIC9
36) BASIC21 BASIC4 BASIC5 BASIC8 BASIC9

Order 6:

Order 7:

Order 8:

Order 9:

Order 10:
```

```
Order 11:

Order 12:

Order 13:

Order 14:

Order 15:

Order 16:

Order 17:

Order 18:

Order 19:

Order 20:

Order 21:

Qualitative Importance Analysis:

Order          Number
-----          ------
1              0
2              0
3              3
4              72
5              36
6              0
7              0
8              0
9              0
10             0
11             0
12             0
13             0
14             0
15             0
16             0
17             0
18             0
19             0
20             0
21             0
ALL            111
```

The report states the name of the file as well as the time when the report was generated. With 21 basic events (called primary events in OpenFTA) within the fault tree structure, the total number of minimal cut sets is 111, divided into minimal cut sets of orders 3, 4 and 5.

The qualitative importance analysis shows that there are 3 minimal cut sets of order 3, 72 of order 4, and 36 of order 5. The order of a cut set determines the number of affected basic events, therefore in the present case 21 minimal cut set orders could be anticipated. However, the structure of the tree allows only for minimal cut sets of orders 3, 4 and 5.

The lower the order, the more influential is a minimal cut set concerning the appearance of the top event. This comes from the fact that the simultaneous occurrence of e.g. three failing basic events is much more probable than the occurrence of five failing basic events.

In the present case the majority of minimal cut sets is of order 4, which means that at least four basic events have to fail at the same time in order that the system is failing. Together with minimal cut sets of order 5 they present about 97% of the total sum. However, the combination of four or five basic events is expected to happen rather infrequently, which means that attention has to be turned to the minimal cut sets of order 3. Clearly depending on their failure probabilities, these basic events will play an important role within the fault tree.

The qualitative analysis of a fault tree provides an overview of minimal cut sets as well as their distribution to orders. Furthermore, it gives an idea of the importance of particular combinations of basic events involved in the occurrence of the top event, thus facilitating the understanding of the fault tree structure. However, without failure probabilities assigned to the basic events, their effective influence on the top event cannot be identified.

As the basis for the quantitative analysis, the minimal cut sets present an important step towards assessing a fault tree.

7.3.2.3 Quantitative Analysis

After analysing the fault tree in a qualitative way, the next step leads on to answering the question of how probable it is that a fire in the LHC underground occurs due to faulty electrical equipment. In this chapter, failure probabilities of the basic events together with explanations concerning their origin will be discussed and the final result presented.

The failure probabilities will be given as relative frequencies, not refering to unit of time. Due to the probability relations for the quantitative analysis of a fault tree, only values independent of time can be applied without restrictions (see chapter 4.3.3.3).

7.3.2.3.1 Failure Probabilities of Basic Events

Essential for the evaluation of a fault tree is the definition of failure probabilities for the basic events. A difference will be made between failures related to human error and those related to technical breakdown.

It has to be stated that the definition of failure probabilities for the present fire risk analysis of the LHC tunnel is a very difficult task. Unfortunately no detailed records have been kept from the LEP operation time containing failures as well as their causes and consequences. Thus no statistical evaluation resulting in system-dependent failure probability data could be conducted. For the fault tree at hand this means that for the bigger part of the basic events' probability data only estimations were possible. Where feasible, data were taken from related statistics and failure probabilities for the basic events were deduced. However, the background information concerning these values comes from different origins, and the directly available probability data were not taken from one common source. This means that the quantitative analysis leaves room for uncertainty.

The subject of determining probabilities concerning human error is a very delicate issue. The range of human actions and responses to present situations is broad, and so is the range of human unreliability values. In the present fault tree human error plays an important role, as it is part of almost all possible ignition sources. However, as the human behaviour is a complex subject and the possibilities of incorrect actions or reactions within the boundaries of this work are numerous, only rough estimates for the failure probabilities are feasible. Therefore a general distinction between two particular forms of human behaviour (action and reaction) has been made and the corresponding probability values have been estimated (following [22]).

Whenever a task has to be accomplished, a human action is required. Within this task, a failure can occur either deliberately or undeliberately. However, as it is assumed that the person is trained adequately and does not intend to harm the project willingly, the failure probability of the first group (action) is estimated to be $1.0 \cdot 10^{-3}$.

In case of an alarm or error signal in the control room, a response of the operator to the new conditions is required. In a situation like this, where a reaction is needed in order to restore the system or initiate emergency assistance, the person in charge is usually under time pressure and outside of his/her routine. Due to this fact, the failure probability of the second group (reaction) is estimated to be higher and is therefore $1.0 \cdot 10^{-2}$.

In the following, the basic events involving human error are grouped according to the determined distinction.

ACTION:

BASIC 7: Packaging material (wooden boxes, plastic) left behind after installation

This basic event is determined by human inadvertency as well as neglect of written instructions.

BASIC 8: Quality control failure

Any failure concerning the technical inspections of electrical equipment in the LHC tunnel occurs either due to inadvertency or due to excessive demand because of the complexity of the project.

BASIC 9: Arbitrary act - purchase and installation

This basic event represents an apparent neglect of instructions.

BASIC 13: Misuse

The misuse of equipment is usually unintended and rather a result of inadvertency or unexpected operating conditions.

BASIC 14: Design error

A failure of equipment design is clearly caused by inadvertency of design engineers. Although this failure is prone to be discovered during various equipment tests, it cannot be ruled out completely.

BASIC 15: Incorrect action

This basic event includes any incorrect action during installation, whether it is a mistake or failures due to inadvertency.

BASIC 16: Accident

Working in the tunnel always implies the possibility of accidents with any tools or transport vehicles.

REACTION:

BASIC 4: No response to alarm on the part of the fire brigade

This basic event is not only influenced by human error, but also by the possibility of a technical problem, such as the dysfunction of the Safety Control Room. However, the great difference of the order of magnitude of failure probabilities between a technical system and human error certainly shifts the emphasis towards human error. The present case requires a reaction of the fire brigade to an alarm, where a misinterpretation of the signal is possible (e.g. mistaken for a test, assuming a faulty channel, as it has been problematic prior to the event) and the person in charge is under pressure.

BASIC 5: Indirect way of detection fails

The indirect detection of a fire or smoulder is dependent on whether or not the concerned subsystem is equipped with a possibility to send an error message as well as on the reaction of the operator in the CCC. Out of these two factors it is the human intervention which has the higher failure probability and is therefore affecting this basic event more significantly.

Failures related to a technical breakdown are presented subsequently:

BASIC 1: Failure of associated system

This basic event mainly concerns a failure within the cooling and ventilation system, with the emphasis on elements such as pumps or filters. These are active components, and their probability of failure is estimated to be $1.0 \cdot 10^{-4}$ [21].

BASIC 2: No fire or smoke detection system available

The ratio of the area without fire and smoke detectors to the entire underground area was taken as an indication for the probability of a fire occurring in an unequipped location. The number of civil works concerned by this study is approximately 170, of which 40 are provided with detectors. Therefore the "failure" probability is about 7.5 $\cdot 10^{-1}$. The underground area is a single compartment, and cooling and ventilation can propagate smoke. This means that about 25% of the underground area is directly covered by fire and smoke detection, and a fire in the remaining 75% would be detected with delay. Thus the probability of a fire occurring in an unequipped area was adjusted downwards to $3.5 \cdot 10^{-1}$.

BASIC 3: Fire or smoke detection system fails or reacts too late

The efficiency factor of the used fire and smoke detectors is 95%, which results in a failure probability of $5.0 \cdot 10^{-2}$ [63].

BASIC 6: Inflammable material necessary for certain equipments

The ratio between the total amount of materials in the tunnel to the amount of combustible material is taken as an indication for the probability of finding inflammable material in the LHC tunnel. Referring to the material inventory of the material data project, the total amount of materials used for equipments is approximately 47,082 t, and the total quantity of cables in the underground area amounts to approximately 2,194 t. The sum of 527 t of combustible material and 1,756 t of insulation polymers represents approximately 5% of the total amount of combustibles. Considering the fact that polymers of Group 1 and 2 are presenting the biggest part of the combustibles and moreover not all materials are exposed directly to air, the probability of finding inflammable material in the LHC tunnel is adjusted downwards to $2.5 \cdot 10^{-2}$.

BASIC 10: Corrosion

Corrosion is the deterioration of material properties due to the material's reaction with its surroundings [64]. It is a passive process and the probability of e.g. cable junctions corroding is therefore $1.0 \cdot 10^{-6}$.

BASIC 11: Ageing

Components are usually in use over a certain time period, and with time their properties deteriorate. Ageing is again a passive process; the probability of e.g. ageing cable insulation is $1.0 \cdot 10^{-6}$.

BASIC 12: Abrasion/wear

When the surface of a component is in contact with another solid, fluid or gaseous body, material can be gradually removed from its surface [64]. As a passive process, the probability of e.g. wearing cable insulation is $1.0 \cdot 10^{-6}$.

BASIC 17: Blocked motors

Motors are active elements and their failure probability is approximately $1.0 \cdot 10^{-4}$ [21].

BASIC 18: Component failure inside electronic equipment

The failure of components inside electronic equipment are assessed as the malfunction of electromechanical parts, thus their failure probability is estimated to be $5.0 \cdot 10^{-4}$ [21].

BASIC 19: Exceptional circumstances during operation

As there is no experience available concerning the operation of a machine such as the LHC, exceptional circumstances during operation are to be expected. As this is mainly due to failures of electromechanical parts, the failure probability of this basic event is $5.0 \cdot 10^{-4}$ [21].

BASIC 20: Flooding

Although the LHC is running through the territory of a few municipalities, only one of them had as much as three floodings between 1983 and 2004, the remaining ones even less than three [38]. As there have been no reported consequences for the LHC tunnel, a natural cause for flooding will not be the crucial factor for the determination of the probability of occurrence. In case of flooding due to the breakdown of C&V equipment, a cascade of pumps in the tunnel is designed to take on the excess of water [65]. Although the pumps are redundant, the estimation for the analysis will be based on the failure probability of one pump. As an active element, its failure probability is $1.0 \cdot 10^{-4}$ [21].

BASIC 21: Exposure to cryo gases/liquids - embrittlement

Due to its cryogenic temperature and therefore ability to freeze any substance, a helium spill could lead to the embrittlement of surrounding materials. Within the LHC tunnel it is the cryogenic distribution line as well as the so-called jumper connections which could present a source of problems. The latter contains active components such as valves; therefore the failure probability of this basic event is $1.0 \cdot 10^{-4}$ [21].

7.3.2.3.2 Failure Probability of the Top Event

As mentioned before, OpenFTA uses the minimal cut sets of the qualitative analysis as a basis in order to obtain a failure probability of the top event. This is done by calculating the probability of each minimal cut set and subsequently the probability of at least one minimal cut set occurring. The latter value is then the failure probability of the top event.

In OpenFTA the following quantitative report is generated:

```
Probabilities Analysis
======================

Tree:  fault_tree_analysis.fta
Time:  Tue Mar 13 10:59:33 2007

Number of primary events = 21
Number of minimal cut sets = 111
Order of minimal cut sets = 21

Unit time span = 1.000000

Minimal cut set probabilities:
```

```
1   BASIC1 BASIC2 BASIC5                    3.500000E-007
2   BASIC1 BASIC3 BASIC5                    5.000000E-008
3   BASIC1 BASIC4 BASIC5                    1.000000E-008
4   BASIC10 BASIC2 BASIC5 BASIC6            8.750000E-011
5   BASIC10 BASIC2 BASIC5 BASIC7            3.500000E-012
6   BASIC10 BASIC3 BASIC5 BASIC6            1.250000E-011
7   BASIC10 BASIC3 BASIC5 BASIC7            5.000000E-013
8   BASIC10 BASIC4 BASIC5 BASIC6            2.500000E-012
9   BASIC10 BASIC4 BASIC5 BASIC7            1.000000E-013
10  BASIC11 BASIC2 BASIC5 BASIC6            8.750000E-011
11  BASIC11 BASIC2 BASIC5 BASIC7            3.500000E-012
12  BASIC11 BASIC3 BASIC5 BASIC6            1.250000E-011
13  BASIC11 BASIC3 BASIC5 BASIC7            5.000000E-013
14  BASIC11 BASIC4 BASIC5 BASIC6            2.500000E-012
15  BASIC11 BASIC4 BASIC5 BASIC7            1.000000E-013
16  BASIC12 BASIC2 BASIC5 BASIC6            8.750000E-011
17  BASIC12 BASIC2 BASIC5 BASIC7            3.500000E-012
18  BASIC12 BASIC3 BASIC5 BASIC6            1.250000E-011
19  BASIC12 BASIC3 BASIC5 BASIC7            5.000000E-013
20  BASIC12 BASIC4 BASIC5 BASIC6            2.500000E-012
21  BASIC12 BASIC4 BASIC5 BASIC7            1.000000E-013
22  BASIC13 BASIC2 BASIC5 BASIC6            8.750001E-008
23  BASIC13 BASIC2 BASIC5 BASIC7            3.500000E-009
24  BASIC13 BASIC3 BASIC5 BASIC6            1.250000E-008
25  BASIC13 BASIC3 BASIC5 BASIC7            5.000000E-010
26  BASIC13 BASIC4 BASIC5 BASIC6            2.500000E-009
27  BASIC13 BASIC4 BASIC5 BASIC7            1.000000E-010
28  BASIC14 BASIC2 BASIC5 BASIC6            8.750001E-008
29  BASIC14 BASIC2 BASIC5 BASIC7            3.500000E-009
30  BASIC14 BASIC3 BASIC5 BASIC6            1.250000E-008
31  BASIC14 BASIC3 BASIC5 BASIC7            5.000000E-010
32  BASIC14 BASIC4 BASIC5 BASIC6            2.500000E-009
33  BASIC14 BASIC4 BASIC5 BASIC7            1.000000E-010
34  BASIC15 BASIC2 BASIC5 BASIC6            8.750001E-008
35  BASIC15 BASIC2 BASIC5 BASIC7            3.500000E-009
36  BASIC15 BASIC3 BASIC5 BASIC6            1.250000E-008
37  BASIC15 BASIC3 BASIC5 BASIC7            5.000000E-010
38  BASIC15 BASIC4 BASIC5 BASIC6            2.500000E-009
39  BASIC15 BASIC4 BASIC5 BASIC7            1.000000E-010
40  BASIC16 BASIC2 BASIC5 BASIC6            8.750001E-008
41  BASIC16 BASIC2 BASIC5 BASIC7            3.500000E-009
42  BASIC16 BASIC3 BASIC5 BASIC6            1.250000E-008
43  BASIC16 BASIC3 BASIC5 BASIC7            5.000000E-010
44  BASIC16 BASIC4 BASIC5 BASIC6            2.500000E-009
45  BASIC16 BASIC4 BASIC5 BASIC7            1.000000E-010
46  BASIC17 BASIC2 BASIC5 BASIC6            8.749999E-009
```

```
47 BASIC17 BASIC2 BASIC5 BASIC7            3.500000E-010
48 BASIC17 BASIC3 BASIC5 BASIC6            1.250000E-009
49 BASIC17 BASIC3 BASIC5 BASIC7            5.000000E-011
50 BASIC17 BASIC4 BASIC5 BASIC6            2.500000E-010
51 BASIC17 BASIC4 BASIC5 BASIC7            1.000000E-011
52 BASIC18 BASIC2 BASIC5 BASIC6            4.375000E-008
53 BASIC18 BASIC2 BASIC5 BASIC7            1.750000E-009
54 BASIC18 BASIC3 BASIC5 BASIC6            6.250000E-009
55 BASIC18 BASIC3 BASIC5 BASIC7            2.500000E-010
56 BASIC18 BASIC4 BASIC5 BASIC6            1.250000E-009
57 BASIC18 BASIC4 BASIC5 BASIC7            5.000000E-011
58 BASIC19 BASIC2 BASIC5 BASIC6            4.375000E-008
59 BASIC19 BASIC2 BASIC5 BASIC7            1.750000E-009
60 BASIC19 BASIC3 BASIC5 BASIC6            6.250000E-009
61 BASIC19 BASIC3 BASIC5 BASIC7            2.500000E-010
62 BASIC19 BASIC4 BASIC5 BASIC6            1.250000E-009
63 BASIC19 BASIC4 BASIC5 BASIC7            5.000000E-011
64 BASIC2 BASIC20 BASIC5 BASIC6            8.749999E-009
65 BASIC2 BASIC20 BASIC5 BASIC7            3.500000E-010
66 BASIC2 BASIC21 BASIC5 BASIC6            8.749999E-009
67 BASIC2 BASIC21 BASIC5 BASIC7            3.500000E-010
68 BASIC20 BASIC3 BASIC5 BASIC6            1.250000E-009
69 BASIC20 BASIC3 BASIC5 BASIC7            5.000000E-011
70 BASIC20 BASIC4 BASIC5 BASIC6            2.500000E-010
71 BASIC20 BASIC4 BASIC5 BASIC7            1.000000E-011
72 BASIC21 BASIC3 BASIC5 BASIC6            1.250000E-009
73 BASIC21 BASIC3 BASIC5 BASIC7            5.000000E-011
74 BASIC21 BASIC4 BASIC5 BASIC6            2.500000E-010
75 BASIC21 BASIC4 BASIC5 BASIC7            1.000000E-011
76 BASIC10 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-015
77 BASIC10 BASIC3 BASIC5 BASIC8 BASIC9     5.000000E-016
78 BASIC10 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-016
79 BASIC11 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-015
80 BASIC11 BASIC3 BASIC5 BASIC8 BASIC9     5.000000E-016
81 BASIC11 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-016
82 BASIC12 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-015
83 BASIC12 BASIC3 BASIC5 BASIC8 BASIC9     5.000000E-016
84 BASIC12 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-016
85 BASIC13 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-012
86 BASIC13 BASIC3 BASIC5 BASIC8 BASIC9     5.000001E-013
87 BASIC13 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-013
88 BASIC14 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-012
89 BASIC14 BASIC3 BASIC5 BASIC8 BASIC9     5.000001E-013
90 BASIC14 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-013
91 BASIC15 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-012
92 BASIC15 BASIC3 BASIC5 BASIC8 BASIC9     5.000001E-013
```

```
93  BASIC15 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-013
94  BASIC16 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-012
95  BASIC16 BASIC3 BASIC5 BASIC8 BASIC9     5.000001E-013
96  BASIC16 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-013
97  BASIC17 BASIC2 BASIC5 BASIC8 BASIC9     3.500000E-013
98  BASIC17 BASIC3 BASIC5 BASIC8 BASIC9     5.000000E-014
99  BASIC17 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-014
100 BASIC18 BASIC2 BASIC5 BASIC8 BASIC9     1.750000E-012
101 BASIC18 BASIC3 BASIC5 BASIC8 BASIC9     2.500000E-013
102 BASIC18 BASIC4 BASIC5 BASIC8 BASIC9     5.000001E-014
103 BASIC19 BASIC2 BASIC5 BASIC8 BASIC9     1.750000E-012
104 BASIC19 BASIC3 BASIC5 BASIC8 BASIC9     2.500000E-013
105 BASIC19 BASIC4 BASIC5 BASIC8 BASIC9     5.000001E-014
106 BASIC2 BASIC20 BASIC5 BASIC8 BASIC9     3.500000E-013
107 BASIC2 BASIC21 BASIC5 BASIC8 BASIC9     3.500000E-013
108 BASIC20 BASIC3 BASIC5 BASIC8 BASIC9     5.000000E-014
109 BASIC20 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-014
110 BASIC21 BASIC3 BASIC5 BASIC8 BASIC9     5.000000E-014
111 BASIC21 BASIC4 BASIC5 BASIC8 BASIC9     1.000000E-014

Probability of top level event (minimal cut sets up to order 21 used):

1 term   +9.753211E-007 = 9.753211E-007 (upper bound)
2 terms  -5.320028E-008 = 9.221208E-007 (lower bound)
3 terms  +8.199447E-010 = 9.229408E-007 (upper bound)
4 terms  -1.134826E-010 = 9.228273E-007 (lower bound)

Primary Event Analysis:

Event          Failure contrib.          Importance

BASIC1         4.100000E-007             44.43%
BASIC10        1.066041E-010             0.01%
BASIC11        1.066041E-010             0.01%
BASIC12        1.066041E-010             0.01%
BASIC13        1.066041E-007             11.55%
BASIC14        1.066041E-007             11.55%
BASIC15        1.066041E-007             11.55%
BASIC16        1.066041E-007             11.55%
BASIC17        1.066041E-008             1.16%
BASIC18        5.330206E-008             5.78%
BASIC19        5.330206E-008             5.78%
BASIC2         8.325916E-007             90.22%
BASIC20        1.066041E-008             1.16%
BASIC21        1.066041E-008             1.16%
BASIC3         1.189416E-007             12.89%
BASIC4         2.378832E-008             2.58%
BASIC5         9.753211E-007             105.69%
```

```
BASIC6          5.435575E-007               58.90%
BASIC7          2.174230E-008               2.36%
BASIC8          2.174230E-011               0.00%
BASIC9          2.174230E-011               0.00%
```

Similar to the qualitative report, the quantitative report starts off with the listing of all minimal cut sets. However, this time the failure probability of each minimal cut set is included, providing information about how probable it is for each basic event combination to occur. The three minimal cut sets with only three basic events affected have a rather high failure probability compared to the remaining cut sets. Following the discussion of the qualitative analysis, this was an already expected outcome due to their low order.

The probability of the top event is then calculated using the failure probabilities available for each minimal cut set. Since a minimal cut set is the minimum number of failing basic events leading to a system failure, the probability of the top event occurring is:

$$\begin{aligned} P(topevent) &= P(M_1 \; OR \; M_2 \; OR \; M_3 \; \ldots \; OR \; M_n) \\ &= P(M_1 \cup M_2 \cup \ldots \cup M_n) \end{aligned} \tag{7.1}$$

In formula (7.1) M is a minimal cut set and n is the total number of minimal cut sets for a fault tree. Since basic events may not only occur once, but several times in a fault tree, and the minimal cut sets are neither mutually exclusive nor independent, it follows that

$$\begin{aligned} P(topevent) &= \sum_{i=1}^{n} P(M_i) \\ &- \sum_{i=2}^{n} \sum_{j=1}^{i-1} P(M_i \cap M_j) \\ &+ \sum_{i=3}^{n} \sum_{j=2}^{i-1} \sum_{k=1}^{j-1} P(M_i \cap M_j \cap M_k) \\ &- \ldots \\ &+ (-1)^{n-1} P(M_1 \cap M_2 \cap \ldots \cap M_n) \end{aligned} \tag{7.2}$$

The number of terms is dependent on the number of minimal cut sets, thus 2^n. Therefore the calculation of an even rather small fault tree would take a prohibitively long time. In the present case, 21 basic events result in 111 minimal cut sets, which would require to calculate 2^{111} (more than 10^{30}) terms to determine the probability of the top event.

OpenFTA compasses this problem with an approximation for equation (7.2), giving results close to the exact value:

$$\begin{aligned}
P_1 &\equiv \sum_{i=1}^{n} P(M_i) \\
&\equiv P_1 - \sum_{i=2}^{n}\sum_{j=1}^{i-1} P(M_i \,\cap\, M_j) \\
&\equiv P_2 - \sum_{i=3}^{n}\sum_{j=2}^{i-1}\sum_{k=3}^{j-1} P(M_i \,\cap\, M_j \,\cap\, M_k) \\
&\dots
\end{aligned} \tag{7.3}$$

With 2n terms in total, the first term is the sum of all minimal cut set probabilities adjusted towards the exact result by each additional term. Every other increment is negative, which means that the exact value is approximated alternately with an upper and a lower bound. Usually it is not necessary to use more than three terms for the calculation, the result is sufficiently accurate.

For the fault tree at hand, a failure probability of the top event of $9.23 \cdot 10^{-7}$ is calculated. Four terms have been used for the calculation, showing a gradual approximation to the exact value. With a correction of only -$1.13 \cdot 10^{-10}$ for the fourth term, the precision of the result is certainly sufficient.

In addition to providing a failure probability of the top event, the quantitative analysis also includes a primary event analysis. This analysis specifies the contribution of each basic event towards the system failure and presents it as a percentage importance value. Again based on the minimal cut sets determined in the qualitative analysis, all minimal cut set probabilities which affect one single basic event are added up and taken as a percentage of the top event failure probability. As an example, the basic event "failure of associated system" (BASIC1) is contained in three minimal cut sets; the sum of their probabilities is $4.10 \cdot 10^{-7}$, which is 44.43% of $9.23 \cdot 10^{-7}$.

The present fault tree has been developed for a risk layer along the LHC tunnel, assuming that combustible material and possible ignition sources are equally distributed. Taking into consideration that in some areas there are accumulations of electrical equipments and inflammable materials close by, an even higher probability of fire can be expected. This is particularly true for the specified areas concerning fire risk (see chapter 7.1.3).

As an average fire probability due to faulty electrical equipment valid for the entire underground area, $9.23 \cdot 10^{-7}$ presents a plausible result. Considering approximately 5,000 operating hours of the LHC per year, a fire would occur every 217 years. With an expected lifetime of the LHC of 20 years, the risk of fire in the LHC tunnel is very low.

The expert judgement of the previous chapter assessed the failure modes of an electrical installation, their frequency of occurrence and the severity of their consequences, but it did not assess directly the risk of having a fire in the underground area. Different to that, the fault tree analysis goes one step further and asks for the events leading to these electrical failure modes and their interactions among each other as well as with external circumstances relating to the top event. Due to the way of developing a fault tree, it does not only include the apparent problems of failure in electrical equipments, but also criticised circumstances such as insufficient fire and smoke detection in some areas as well as the impact of human failure. Taking these issues and also the complexity of the LHC into consideration, a fire risk of $9.23 \cdot 10^{-7}$ is a very low value. In these calculations only failures due to faulty electrical equipment are included, for an overall fire risk for the LHC tunnel including any possible causes certainly a higher failure probability has to be expected.

Although the result seems to be an acceptable outcome, it does not reveal any conclusions relating to the level of uncertainty. In this context, the influence of certain basic events on the failure probability of the top event, as shown in the primary events analysis, is an interesting as well as important subject to discuss. The importance is dependent on the number of minimal cut sets a basic event is involved in. So if the probability values of basic events with a high importance are very uncertain i.e. due to lack of basis data, the result for the top event is highly probable to have a wide range of uncertainty as well.

In the present fault tree, the basic event “indirect way of detection fails” (BASIC5) has an importance of 105.69% and has consequently the greatest influence on the top event. Since it is actually contained within all 111 minimal cut sets, a modification of its probability value would certainly show an impact on the final result. By changing the human error probability from $1.0 \cdot 10^{-2}$ to $1.0 \cdot 10^{-3}$, the system failure goes down to as much as $9.23 \cdot 10^{-8}$, a drop of factor 10, whereas the importance value distribution stays approximately the same. If the human error probability is increased, an opposite effect on the top event failure probability can be observed, but again the primary event analysis is unaffected.

On the contrary, if a probability value of a basic event with a low importance value is modified, the impact on the overall system failure and the importance value distribution is minor or even negligible.

The most influential basic events are the failure of an associated system (BASIC1, 44.43%), the lack of sufficient fire and smoke detection (BASIC2, 90.22%), the inability of detecting a developing fire indirectly (BASIC5, 105.69%) and the presence of inflammable material (BASIC6, 58.90%). Interestingly, there is only one basic event concerning human error included in this group. This means that the emphasis on the complex subject of estimating human error probabilities is shifted, only leaving one instead of nine basic human events to be analysed within the fault tree.

With the human error estimation of $1.0 \cdot 10^{-2}$ for reacting and detecting a fire indirectly, this study is intended to show a conservative approach. In case of an even more extreme assumption of $1.0 \cdot 10^{-1}$ for the human error probability of reacting on a new situation, the order of magnitude of the occurrence of the top event is shifted towards 10^{-6}. However, if assuming a trained and experienced operator, the latter value of 10^{-6} is rather unlikely.

The remaining basic events with the highest importance values are all failures related to a technical breakdown or a given technical condition. The one with the highest level of uncertainty is the question whether there is sufficient fire and smoke detection in the entire underground area. If the value of “no fire or smoke detection system available” (BASIC2) is modified to the most extreme value possible, that is to say $7.5 \cdot 10^{-1}$ (thereby only including areas equipped with direct fire and smoke detection), the probability of system failure increases to $1.82 \cdot 10^{-6}$ and the importance of the availability of fire and smoke detection to

98.23%. On the contrary, assuming that there are actually fire and smoke detectors almost everywhere in the tunnel (failure probability of $1.0 \cdot 10^{-2}$), the top event value would drop to $1.64 \cdot 10^{-7}$ and the importance of the availability of fire and smoke detection to 14.54%. This means that fire risk could be reduced almost by a factor 10 by increasing the number of detectors. However, the gain of safety has to be weighed against the cost of the necessary equipment.

The basic events concerning the failure of an associated system and the presence of inflammable material in the tunnel present fairly safe estimations or are given values. Moreover, any modifications of their failure probabilities result in only minor changes of the top event result, which remains within the order of magnitude of 10^{-7}.

Chapter 8

Discussion of the Results

The purpose of the thesis was not only a qualitative as well as quantitative analysis of the risk of fire in the LHC tunnel, but also the identification of the main reasons for this risk in order to reduce its probability. Therefore proposals for improvement of the problems identified during the performance of the risk analysis will be made in the following sections.

The impossibility of changing the configurations of materials and/or electrical equipments in the LHC limits the actions to be taken in order to reduce the fire risk. A possible way of approaching this problem would be to gain deeper knowledge of the subject by monitoring it in the future, which will eventually allow for a refinement of its results.

8.1 Fire Protection Zones

The fire protection zones are sensitive areas in the LHC tunnel in terms of fire risk outlined by this thesis. However, their identification is not sufficient and further action is required with the purpose of improving fire safety in these and other underground areas.

Safety measures must be implemented in order to either prevent an incident from happening or to mitigate its effects. Concerning the LHC, the recommended actions will be focusing on the prevention as well as on the mitigation of consequences: the areas will be marked as special fire protection zones implying reinforced fire and smoke detection as well as special indication, rules and responsibilities.

The principle of identifying protection zones is applied in industry in relation to explosion protection. Areas with the potential to create an explosive atmosphere are divided into zones depending on its residence time. The mixture of air and combustible gases, vapour or mist can be frequently (Zone 0), occasionally (Zone 1) or temporary (Zone 2) available. Adequate safety measures aim at the removal of ignition sources or, if this is not possible, the reduction of their frequency of occurrence [66].

With regard to the LHC, grading of the fire hazardous zones is not required, since any risk, however small, needs to be addressed. Therefore only two classifications exist: fire risk

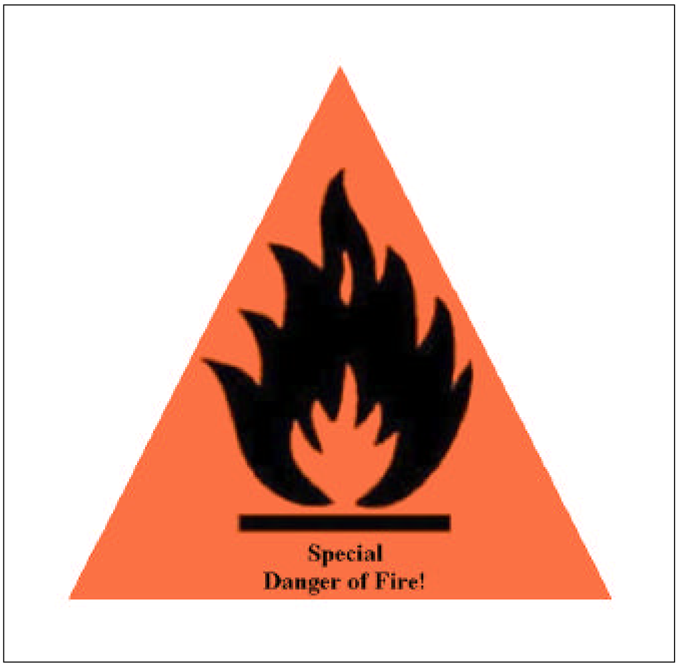


Figure 8.1: Signboard for fire protection zones

and no fire risk.

8.1.1 Reinforced Fire and Smoke Detection

Fire and smoke detection is of principal importance in all the underground areas, but even more within these particularly sensitive zones. Some areas of the LHC tunnel are already equipped with detectors, but other areas, which have been analyzed here, do not have any fire and smoke detection equipment as a consequence of underestimating their fire risk elsewhere.

The recommendation given is to urgently re-design the layout and increase the number of the detectors in the tunnel in order to improve the coverage. The quantitative analysis of the previous chapter revealed that fire risk could be reduced almost by a factor 10 by increasing the number of detectors (see chapter 7.3.2.3.2).

8.1.2 Signposting

Following the Council Directive 92/58/EEC of June 24th, 1992, on the minimum requirements for the provision of safety and/or health signs at work, and in order to make people aware of the special risk of the areas, eye-catching signposting must be provided (Figure 8.1) [67].

The signs must be easily recognisable and members of personnel have to be able to associate them with the corresponding rules.

8.1.3 Risk Description

The LHC underground area has a special status regarding the efforts of the fire brigade. With only eight access points for a total tunnel length of 27 km and the restricted access within the underground area to a possible fire, the fire brigade's response to a fire must be cautiously coordinated. As CERN has its own fire service department, personnel are trained for this particular working environment. However, the knowledge about special areas at risk can help even further to provide the best possible assistance and preventive action.

In order to support the fire brigade, the persons in charge of the fire protection zone (from the department operating the hazardous equipment) should complete a so-called Risk Description form. In this form data should be provided in such a way that based on these the fire brigade can develop their intervention plans for the underground areas in case of fire.

The fire brigade's intervention plan includes the following issues [68]:

- Location and access of the zone,
- description of the zone including its purpose, dimensions and structure,
- description of the type of hazards,
- details concerning active as well as passive prevention measures,
- instructions concerning the intervention,
- and the names, functions and telephone numbers of the persons in charge.

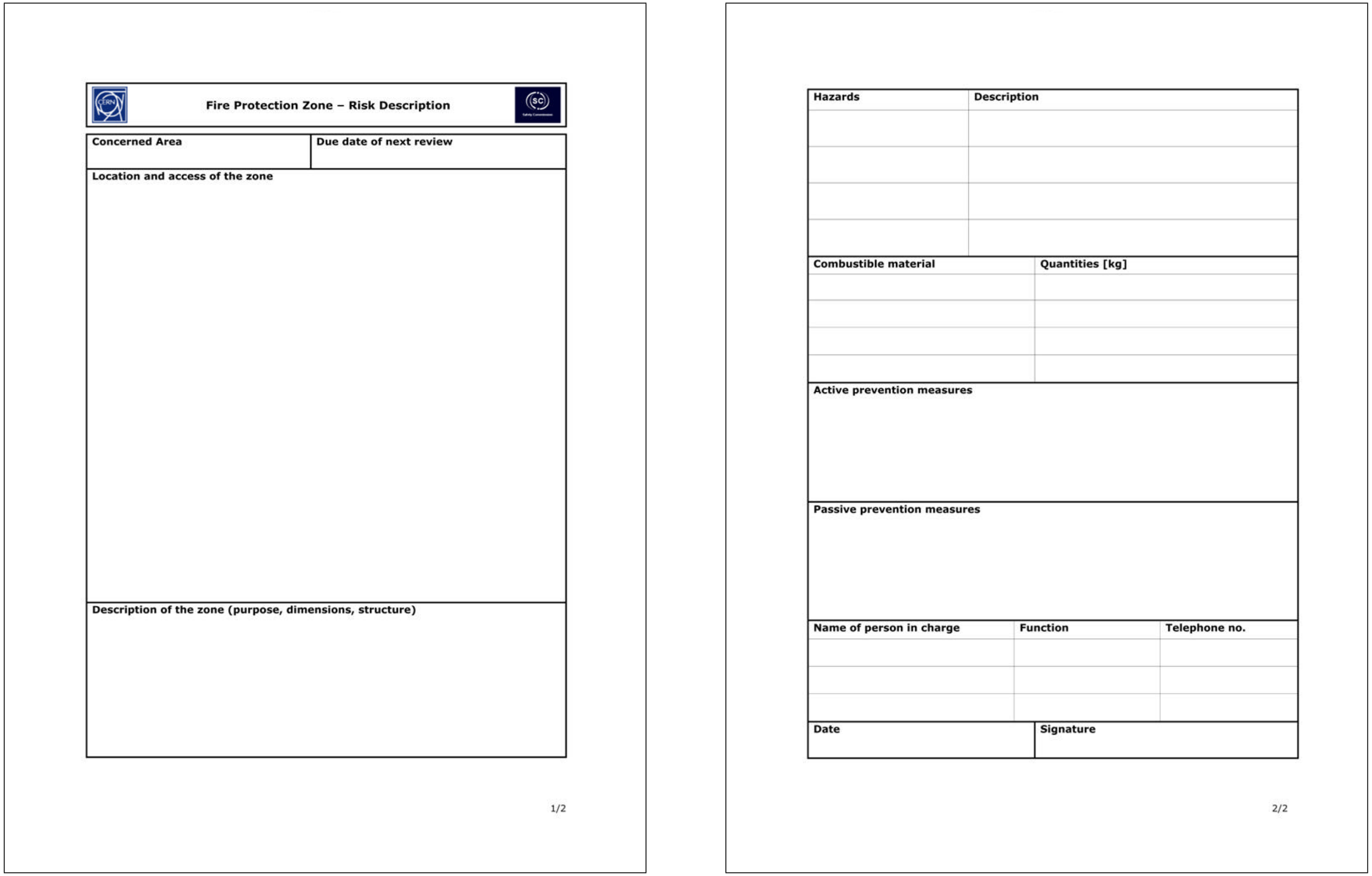
Based on this, the Risk Description form was developed to provide a background for each topic in order to reduce the amount of enquiry for the fire brigade. Figure 8.2 shows an example of how regular reviews of the situation in each area of interest may look like.

In order to complete the form correctly, the recommendations below must be followed.

The area of special fire risk must be indicated using CERN's civil engineering terminology. A detailed plan of the area must be provided, showing all possibilities of access. The description of the zone includes information concerning the purpose of the activities, the dimensions of the building as well as the number of access possibilities and floors.

Depending on the equipment and materials in the fire protection zone, the hazards are diverse. This section is supposed to provide the fire brigade with all types of hazards which could aggravate a mission. Thus the kind of hazard has to be mentioned (e.g. due to electrical equipment, cryogenic equipment, radiation, explosion) together with a more detailed description of why and how it presents a hazard. In connexion with this, all combustible materials as well as their quantities must be listed. The total amount of inflammable material then gives an idea of the fire load available, impacting greatly on how the fire brigade will deal with an incident.

Once the hazards of the zone are known, the active and passive prevention measures have to be mentioned in particular. Active prevention measures may include fire and smoke



Fire Protection Zone – Risk Description

Concerned Area	Due date of next review

Location and access of the zone

Description of the zone (purpose, dimensions, structure)

1/2

Hazards	Description

Combustible material	Quantities [kg]

Active prevention measures

Passive prevention measures

Name of person in charge	Function	Telephone no.

Date	Signature

2/2

Figure 8.2: Risk description form

detectors, evacuation alarm or ODH detectors. On the contrary, passive prevention measures could be structural fire protection or a retention basin.

The above mentioned specifications then help the fire brigade to determine details concerning the intervention, such as special personal protection equipment or specific behaviour for the types of hazards mentioned.

The last entry of the Risk Description form names the persons in charge of the zone in terms of safety and their functions (e.g. Territorial Safety Officer) as well as telephone numbers.

Revision periods should be based on existing maintenance cycles, otherwise a periodic check of the situation may be done every year. In case of modifications to the system, it is the responsibility of the persons in charge of the modification to report to the fire brigade. If alterations with major impacts on the zone are carried out, a review of the Risk Description must be performed immediately; it is not acceptable to wait until the following due date of revision. Without considering modifications, the effective efforts of the fire brigade may be jeopardised and people put at risk.

Keeping descriptions simple is a generally applicable rule for completing the Risk Description form, since complicated explanations concerning the background of equipment and activities would not be of any help for the firemen. Therefore the data should be presented in a comprehensible manner, able to be understood by the fire brigade.

8.1.4 Code of Conduct for Personnel - Housekeeping

The present thesis refers to fire risk during the operation of the machine, not installation, trouble-shooting or maintenance phases. However, whenever people are working in these sensitive zones, they have to be reminded of the special impact which any of their actions might have on machine operation.

The precondition for preventing any fire incident in the first place or facilitating the actions of the fire brigade is good housekeeping [69]. Housekeeping in general includes keeping the work place in a clean state as well as removing waste. It has to be made top priority, since any other administrative procedures enforced by management will not be sustainable in the long term.

In order that the process is successful, housekeeping must be part of the daily practices of all personnel. Hence the training of personnel in housekeeping practices is essential. It is the responsibility of the persons in charge of works conducted in these areas to train their personnel adequately and make sure the rules of housekeeping are abided by.

Basically there are three important housekeeping rules for the fire protection zones in the LHC:

1. Take any rubbish away when leaving the area

   During troubleshooting and maintenance periods, repairs and replacements are being carried out, which implicate boxes of new equipment and casing material. This packaging material is made up mainly by combustibles, i.e. wooden boxes or plastic wrapping. When the machine is in operation again, such material left behind presents an additional fire load.

2. Keep the area clear of obstructions

   Besides packaging material also tools are brought along for the works to be done in the area. Once these assignments are finished, every member of the personnel has to make sure that the work place is clean and no tools are left behind. A clean floor free of obstructions (especially walkways and entrances) is essential for a successful effort of the fire brigade.

3. Report mishaps, accidents and also near misses

   Where people are working, accidents and mishaps will happen. As no human is perfect, human failure is likely to occur during any activity. Hence it is important to report every incident in order to allow for inspection and re-commissioning accordingly. Any unreported damage to equipment due to accidents and mishaps may provoke unexpected failures with serious consequences which safety systems have not been designed for. In this context near misses have to be mentioned in particular. Although the word already implies that no accident has happened, side-effects might have gone unnoticed and practices may need to be modified.

These housekeeping rules should be respected everywhere in the underground area. However, it is particularly important for the protection zones due to a higher fire risk.

8.2 Material Data Inventory

Two different motivations favour the creation of a material data inventory: firstly, the identification of hazardous zones can be continued more into detail, and secondly, material properties are made available to be studied more into depth to examine their behaviour and determine if the fire load is tolerated.

Although a material data collection has been conducted for the present analysis, it is not sufficiently detailed yet. Improvements can be made regarding several issues.

The fact that most of the designs for the LHC machine were already done when this study was initiated was probably the most problematic issue of all. Since the state of the project was advanced and people had to deal with additional problems, cooperation and willingness to provide basic data was sparse. If people are obliged to keep a list of materials involved in their equipments as well as their quantities, it rather becomes part of the procedure and does not present any further work load. Safety authorities at CERN should make it mandatory and a culture to report the types of materials, quantities and locations. The adequate way of collecting this data has to be determined according to the workforce available.

In doing so, it will be assured that all equipment families are included in the inventory and no important elements are left out. The data should be easily available for everybody to stop repeatedly investigating material properties of equipments which are used by more than one department. Moreover, they should be communicated to the design and installation departements in order to be able to place combustible materials the greatest distance away from potential sources of ignition, or in certain extremes put protection barriers into place. A culture of greater awareness of each other's equipment allows this process to be efficient and not more work.

Connected with the creation of a material data inventory is the problem of reporting material which is necessary for the equipment, but actually prohibited by certain regulations. In the course of this thesis, prohibited material in rather large quantities was reported in one case, but there were no derogations found in the database of the safety authorities. Since personnel in charge of safety should not be contacting each department separately in order to ask for material data and possible conflicts with the rules, it is a reason more to push the routine collection and transmission of data. In this manner, derogations will be automatically taken care of. In case unauthorized materials are still used and this information is not passed on to the safety authorities, a culture of disciplinary action should be enforced.

After including a material data inventory in everyday work, attention can be turned to the details of how to efficiently collect the data. In order to give the fire brigade a better idea of the fire hazard zones, the location of the materials within the building as well as their location within the equipment itself is of importance. The latter is referring to two definitions: either directly exposed to air or contained within other materials.

The advantages of providing a more precise location of combustible materials are the following: the Risk Description form can be completed more detailed and the fire load of a specific area may be determined much easier. Moreover, combustibles not directly exposed to air can still be included in the study, but with less importance.

Although the LHC project is coming to an end with view to design and choice of equipment, it is worthwhile to work on the existing data and eliminate the uncertainties. This will be a more precise input for the quantitative analysis, which can then be re-examined and, if necessary, be corrected.

8.3 Collection of Failure Probability Data

With the help of a fault tree analysis, the probability of having a fire in the tunnel due to faulty electrical equipment was assessed. However, there were no system-dependent failure probability data available, since no reliable records were kept from the former particle accelerator LEP.

Since the LHC is only at the beginning of its operation time, the opportunity to collect specific data in the event of fire is still possible. Most of the LHC subsystems have an integral feature of post mortem analysis. However, it will not be able to use these data for identifying fire causes and failure probabilities, as it is too detailed and focussing only on a single subsystem.

The collection of data in the event of fire should be done in form of detailed reports with certain key points. These key points should include the following:

- Possible causes,
- consequences,
- the initiating event,
- the chain of following events,
- and the equipments as well as materials and quantities involved.

It is recommended to have only a limited number of people in charge of this data collection, thus the process of entering data can be supervised adequately and the same method can be assured for each incident.

With this reporting system in place, the failure probabilities of the basic events in the fault tree of the previous chapter can be determined by system-dependent data in the future, which will eventually allow for a much more accurate result on which adequate safety measures are based. Apparently it will not be easy to create such detailed reports, but even more difficult will be the correct statistical evaluation of the input data. However, the collection of system-dependent data and their analysis should be made first priority with regard to a result as close as possible to reality during future re-analyses.

Chapter 9

Conclusion and Outlook

The first beam will be injected into part of the LHC in November 2007 at low energy as a test run, after which the winter close-down will be used for further refinement of the machine. The final start-up is scheduled for spring 2008.

The fault tree analysis revealed a top event probability of having a fire in the LHC underground due to faulty electrical equipment of $9.23 \cdot 10^{-7}$, which corresponds to one fire every 217 years or approximately 0.1 fires during the LHC lifetime. This is an acceptable value relating to a machine operating in such an extreme environment.

Once the machine is running, current operating data are available and can be used for regular analyses. Since the procedure of risk management does not only focus on the qualitative and quantitative assessment, but also includes a regular reassessment and control of the implementation of risk reducing measures, the subject of this thesis should be followed up repeatedly. If system-dependent failure data from the LHC operation are applied to the present analysis, the results can be corrected and measures can be re-adapted accordingly. Moreover, a better understanding of the system and its mechanisms can be achieved.

The thesis at hand has been focussing on a technical risk analysis to better understand the system and identify the fire risk in the LHC tunnel due to faulty electrical equipment. In the future, CERN will have to evolve towards an integral application of risk management in all possible fields, not only fire risk. CERN has begun this journey with the introduction of the Environmental Management System (EMS) and the new Safety Management System (SMS).

Glossary

AIRS	Advanced Incident Reporting System
ALICE	A Large Ion Collider Experiment
ATLAS	A large Toroidal LHC ApparatuS
BIS	Beam Interlock system
BLM	Beam Loss Monitor
C	Celsius
C&V	Cooling & Ventilation
CCC	CERN Control Centre
CENELEC	European Committee for Electrotechnical Standards
CERN	Conseil Européen pour la Recherche Nucléaire European Organisation for Nuclear Research
CHF	Swiss Franc
CIE	Control and Indicating Equipment
CMS	Compact Muon Solenoid
CSAM	CERN Safety Alarms Monitoring system
EMS	Environmental Management System
ETA	Event Tree Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FTA	Fault Tree Analysis
GeV	Giga electron volt
GJ	Giga Joule
HAZOP	Hazard and Operability Study
HCl	Hydrochloric acid
HEP	High Energy Physics
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IP	Interaction point
K	Kelvin
kA	Kiloampere
kg	Kilogram
km	Kilometre
LACS	LHC Access Control system
LASS	LHC Access Safety system
LBDS	LHC Beam Dump system

LEP	Large Electron-Positron Collider
LHC	Large Hadron Collider
LHCb	Large Hadron Collider beauty
LSS	Long Straight Section
m	Metre
MJ	Mega Joule
mrad	Milli Radian
MW	Mega Watt
NASA	National Aeronautics and Space Administration
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission
ODH	Oxygen Deficiency Hazard
P(X)	Probability of X
PC	Power Converter
PE	Polyethylene
PIS	Power Interlock system
PS	Proton Synchrotron
PVC	Polyvinyl chloride
QPS	Quench Protection system
RAMSES	Radiation Monitoring System for the Environment and Safety
RF	Radio frequency
SCR	Safety Control Room
SMS	Safety Management System
SPS	Super Proton Synchrotron
t	Tons
TCR	Technical Control Room
TeV	Tera electron volt
TI	Transfer and Injection
TNT	Trinitrotoluene
TOTEM	TOTal cross-section and Elastic scattering Measurement
UPS	Uninterruptible Power Supply
V	Volt
VAC	Vacuum system

List of Tables

List of Figures

Bibliography

[1] O. Keski-Rahkonen, J. Mangs. Electrical ignition sources in nuclear power plants: statistical, modelling and experimental studies. *Nuclear Engineering and Design 213*, pages 209 – 221, 2002.

[2] TIS - Division de l'Inspection Technique et de la Sécurité. *Règles de sécurité applicables aux activités des entreprises sur le domaine du CERN.* CERN/TIS-GS/98-10, CERN, 1998.

[3] CERN. LHC General Info. <http://lhc.web.cern.ch/lhc/general/gen_info.htm> Accessed: 02 August, 2005.

[4] CERN. CERN - The world's largest particle physics laboratory. <http://public.web.cern.ch/public> Accessed: 01 August, 2005, and 12 September, 2006.

[5] CERN. EDMS Web Navigator - Naming & Conventions. <http://edms.cern.ch/cedar/plsql/navigation.tree?cookie=2887135&p_top_-id=1894086584&p_top_type=P&p_open_id=1894086584&p_open_type=P> Accessed: 07 May, 2007.

[6] CERN. LHC Machine Outreach. <http://lhc-machine-outreach.web.cern.ch> Accessed: 11 September, 2006.

[7] J. Gillies. Introducing the Large Hadron Collider. *Symmetry Magazine*, Volume 03, Issue 06, August 2006.

[8] R. Schmidt. Powering LHC, 2007. Presentation given at the Training for Commissioning of the LHC powering system.

[9] J. Poole. LHC Design Report, Volume I, 2004.

[10] R. W. Assmann et al. The final collimation system for the LHC. In *European Particle Accelerator Conference EPAC 2006.*

[11] T. Taylor. Superconducting Magnets and RF Cavities for the LHC. In *38th INFN Eloisatron Project Workshop: Superconducting Materials for High Energy Colliders "Ettore Majorana"*, 1999.

[12] R. Filippini, E. Carlier, L. Ducimetière, B. Goddard, J. Uythoven. Reliability Analysis of the LHC Beam Dumping System. In *Particle Accelerator Conference PAC 2005*.

[13] J. Gillies. Extracting Physics from the LHC. *Symmetry Magazine*, Volume 03, Issue 06, August 2006.

[14] CERN Annual Report 2005. CERN Communications Group.

[15] CERN. The ATLAS Experiment. <http://atlas.ch> Accessed: 12 September, 2006.

[16] CERN. Alice Experiment: The ALICE Portal. <http://aliceinfo.cern.ch> Accessed: 01 September, 2006.

[17] CERN. The Compact Muon Solenoid Experiment. <http://cms.cern.ch> Accessed: 01 September, 2006.

[18] Wikipedia, the free encyclopedia. Compact Muon Solenoid. <http://en.wikipedia.org/wiki/Compact_Muon_Solenoid> Accessed: 01 September, 2006.

[19] CERN. Large Hadron Collider beauty experiment. <http://lhcb-new.web.cern.ch/LHCb-new> Accessed: 01 September, 2006.

[20] The TOTEM Collaboration. Total Cross Section, Elastic Scattering and Diffraction Dissociation at the Large Hadron Collider at CERN. CERN-LHCC-2004-002, TOTEM-TDR-001, CERN, 2004.

[21] W. Kröger. *Methoden der Risikoanalyse und des Risikomanagements.* Eidgenössische Technische Hochschule (ETH) Zürich - Laboratorium für Sicherheitsanalytik (LSA), 2004. Skriptum zur Vorlesung.

[22] F. P. Lees. *Loss Prevention in the Process Industries - Hazard Identification, Assessment and Control*, volume 1. Butterworth-Heinemann, 2. edition, 1996.

[23] T. Bedford, R. Cooke. *Probabilistic Risk Analysis: Foundations and Methods.* Cambridge University Press, 2001.

[24] T. Aven. *Reliability and Risk Analysis.* Elsevier Science Publishers Ltd, 1992.

[25] D. J. Smith. *Reliability, Maintainability and Risk - Practical methods for engineers.* Butterworth-Heinemann, 6. edition, 2001.

[26] N. J. McCormick. *Reliability and Risk Analysis.* Academic Press, 1981.

[27] H. Kumamoto, E. J. Henley. *Probabilistic Risk Assessment and Management for Engineers and Scientists.* Wiley-IEEE Press, 2. edition, 2000.

[28] International Electrotechnical Commission. *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety/related systems*, 2005.

[29] British Standards Institution. *BS 5760: Reliability of systems, equipment and components Part 5 - Guide to failure modes, effects and criticality analysis (FMEA and FMECA)*, London, 1991.

[30] British Standards Institution. *BS 5760: Reliability of systems, equipment and components Part 7 - Guide to fault tree analysis*, London, 1991.

[31] R. Davies. Risk Analysis of the L3 Detector. CERN/EF/4062H/RD/sb, CERN, 1988.

[32] R. Davies. Risk Analysis of the Delphi Detector. CERN/EF/4035H/RD/sb, CERN, 1988.

[33] R. Davies. Risk Analysis of the Aleph Detector. CERN/EF/3750H/RD/sb, CERN, 1988.

[34] P. Peyron. Etude de sécurité Aleph. Technical report, CERN, 1985.

[35] M. Chorowski et al. Preliminary Risk Analysis of the LHC Cryogenic System. LHC Project Note 177, CERN, 1999.

[36] F. Bordy, R. Denz, K. H. Mess, B. Puccio, F. Rodriguez Mateos, R. Schmidt. Machine Protection for the LHC: Architecture of the Beam and Powering Interlock Systems. LHC Project Report 521, CERN, 2001.

[37] A. Chouvelon, A. Faugier. Système Généraux de Sécurité du LHC. LHC-P-ES-0002 v.1.1, CERN, 2002.

[38] R. Trant. Rapport provisoire de sûreté du SPS/CNGS et du LHC - Section I.7 Présentation des risques potentiels. RPS I.7 v.1.0, CERN, 2006.

[39] E. Cennini, G. Roy. The LHC Access Control System. LHC-Y-ES-0006 v.1.0, CERN, 2004.

[40] E. Manola-Poggioli, L. Scibile. CERN Safety Alarm Monitoring System. In *Proceedings of EPAC 2006.*

[41] L. Scibilie. Radiation Monitoring System for the Environment and Safety (RAMSES). LHC-P-ES-0003, CERN, 2006.

[42] V. Babrauskas. How do electrical wiring faults lead to structure ignitions? In *Proc. Fire and Materials 2001 Conf.*, London, 2001. Interscience Communications Ltd.

[43] O. Keski-Rahkonen, J. Mangs, A. Turtola. Ignition of and fire spread on cables and electronic components. Espoo, 1999. Technical Research Centre of Finland, VTT Publications 387.

[44] Rapport d'enquête sur l'incendie du PS du 29.8.1975. 7/HS/SY/IS/GL/jl, CERN, 1975.

[45] Rapport d'enquête sur l'incendie de l'aimant NA9 (EHN2). HS/SY/GL/fp, CERN, 1982.

[46] Private conversation with Fritz Szoncso, 10 October, 2006.

[47] CERN. Safety Commission. <http://safety-commission.web.cern.ch/safety-commission/SC-site/index.html> Accessed: 17 November, 2005.

[48] Safety Commission/General Safety. *Safety Instruction 23 rev.3: Criteria and Standard Test Methods for the Selection of Electric Cables and Wires with respect to Fire Safety and Radiation Resistance.* CERN, 2005.

[49] Safety Commission/General Safety. *Safety Instruction 41 rev.1: The Use of Plastic and other Non-Metallic Materials at CERN with respect to Fire Safety and Radiation Resistance.* CERN, 2005.

[50] Safety Commission/General Safety. *Electrical Safety Code.* CERN, 1990.

[51] The University of Akron - Hardy Research Group. Graphite. <http://ull.chemistry.uakron.edu/erd/chemicals/7000/6547.html> Accessed: 23 February, 2007.

[52] Dow Corning Silicones. Dow Corning 561 Silicone Transformer Liquid. <http://www.dowcorning.com> Accessed: 02 April, 2007.

[53] Bluestar Silicones. Rhodorsil 47V50. <http://www.rhodia-silicones.com/silicones/home.jsp> Accessed: 02 April, 2007.

[54] R. Assmann. New Machine Layout in IR3 and IR7. LHC-LJ-EC-0002 v.1.0, CERN, 2004.

[55] International Electrotechnical Commission. *IEC 60695: Fire hazard testing*, 1999.

[56] R. Nunes, F. Bonthond. Automatic Fire Detection System for the LHC Underground Areas. LHC-SF-ES-0001 v.5.4, CERN, 2004.

[57] E. Carlier, L. Ducimetiere, V. Mertens. Surveillance and Over-Temperature Protection for the High Voltage Pulse Generators of the LHC Injection Kickers. LHC-MKIGA-ES-0001 v.1.0, CERN, 2005.

[58] I. Zaidi, F. Corsanego. Computer Fluid Dynamic Fire Simulation LHC Point 7. CERN-SC-2005-011-GS-TN v.3, CERN, 2005.

[59] Formal Software Construction Limited. *OpenFTA Version 1.0 User Manual*, 2005.

[60] International Labour Organisation. Sources of Fire Hazards. <http://www.ilo.org/encyclopedia/?docnd=857100195> Accessed: 05 October, 2006.

[61] Wikipedia, the free encyclopedia. Electrical breakdown. <http://en.wikipedia.org/wiki/Electrical_breakdown> Accessed: 07 November, 2006.

[62] T. Crnko, S. Dyrnes. Arcing Flash/Blast Review With Safety Suggestions for Design and Maintenance. <http://www.efcog.org/wg/ism_esip/index.htm> Accessed: 07 November, 2006.

[63] Private conversation with Fabio Corsanego, 08 March, 2007.

[64] W. Beitz, K.-H. Grote. *Dubbel - Taschenbuch für den Machinenbau.* Springer, 19. edition, 1997.

[65] Consigne Intervention - Pompage d'eau dans les UX-LHC. Cons-int-2006-05-fr, CERN Fire Brigade, 2006.

[66] Hauptverband der gewerblichen Berufsgenossenschaften - Fachausschuss Chemie. *BGR 104 Explosionsschutz-Regeln - Regeln fuer das Vermeiden von Gefahren durch explosionsfähige Atmosphäre mit Beispielsammlung*, 2005.

[67] Council Directive 92/58/EEC of 24 June 1992 on the minimum requirements for the provision of safety and/or health signs at work, 1992. OJ L 245.

[68] Pierre Rool. Plans d'interventions des bâtiments 180, 2173, 3585. IUT LORIENT - HSE 2004/2005, CERN et Institut Universitaire de Technologie Lorient, 2005.

[69] A. I. Olò Martinez. Analysis and Reduction of Workplace accidents at at particles physics laboratory: CERN. Master's thesis, Universidad de Oviedo - Escuela Técnica Superior de Ingenieros de Minas, 2007.