Aalborg University
Institute of Electronic Systems
Fredrik Bajers Vej 7
DK-9220 Aalborg Øst
Denmark

European Laboratory for Particle Physics
SL - Division
CH-1211 Geneva 23
Switzerland

Title: Fault Detection on the LHC Beam Dump Kicker System
Author: Torben Dissing
Supervisors: Mogens Blanke (Aalborg University)
Johan Dieperink (CERN)
Project Period: December 1st 1998 - May 31st 1999

This report describes a proposal for fault detection on the LHC beam dump kicker system. As a result of a fault analysis two fault detection modules are proposed; A off-line test and a continuous surveillance.
The fault detection, needing continues data, and the requirements to the data acquisition is given special attention.
The off-line test declares the system, including stand-by components, fault free prior to beam injection.The test comprises parameter estimation using the sensitivity approach requiring an ADC with better than 7 bit precision and a sampling frequency above $133kHz$.
The continuous surveillance comprises a model based fault detection method, based on analytical redundancy. The system requirements are a 13 bit (excl. sign bit) DAC and an 15 bit (excl. sign bit) ADC with a sample frequency above $1.54Hz$.

I denne raport beskrives et forslag til fejl detektion på LHC beam dump kicker systemet. Som resultat af en fejl analyse foreslås to moduler; en off-line test og en kontinuerlig overvågning.
Fejl detektion, der har behov for kontinuerte data, og kravene til den nødvendige data opsamling har fået speciel opmærksomhed.
Off-line testen erklærer system, inklusiv stand-by komponenter, fejlfrit før partikel injektion. Testen består af parameter estimation med sensitivitets metoden krævende en ADC med mere end 7 bits precision og en sample frekvens over $133kHz$.
Den kontinuerte overvågning består af en model baseret metode, baseret på analytisk redundans. System kravene er en 13 bit (excl. fortegnsbit) DAC og en 15 bit (excl. fortegns bit) ADC med en sample frekvens over $1.54Hz$.

Preface

This report describes the work I have done for my MScEE degree at Aalborg University, Institute of Electronic Systems, department of control engineering.

The work has been done at CERN in the SL/BT group, under the technical student programme, in the period from December 1st 1998 to May 31st 1999.

The primary focus of the work have been fault analysis and fault detection on the LHC beam dump kicker system. However since this is a system still under construction, with some subsystems still in the early design phase during the project period, not all subsystems is treated.

The report are targeted at supervisors and students within control engineering and the people, who in the future are going to implement the LHC beam dump kicker surveillance system.

I would like to thank all the people who have been helping and supporting me, in the project period. Specifically I would like to thank Johan Dieperink for his patience explaining the beam dump system and evaluating all of my ideas, good as well as bad.

Table of Contents

Chapter 1

Introduction

The LHC (Large Hadron Collider) is the next large particle accelerator at CERN. The purpose of the LHC is to penetrate further into the structure of matter and recreate the conditions prevailing in the Universe just $10^{-12}s$ after the "big bang" where the temperature was 10^{16} degrees [Gro91]. The LHC is to accelerate protons in order to make proton - proton collisions. It is foreseen that the LHC should also accelerate heavier particles such as lead-ions. By reinstalling some LEP[1] components on top of the LHC, electron - positron collision should also be possible[Gro95]. The LHC is to be installed in the existing LEP tunnel thus minimising the amount of civil engineering needed.

The basic principle of the LHC is to accelerate and store the particles in a circular ring using electro-magnetic fields. Using super-conductive magnets generating a magnetic field of 8.4Tesla allow circulating proton beams of $7TeV$[Gro95]. This means that the particles are to be accelerated from an injection energy of $450GeV$[Gro91] to the maximum energy of $7TeV$ where physics is to take place.

More information on the LHC is available in [Gro91] and [Gro95].

To be able to extract the beam from the LHC at the end of a physics run or in case of machine failure, a beam dump system is needed. The energy of the beam is to high for the beam to be dumped in or close to the machine[Gro91]. This is why the beam dump system deflects the beam onto a dump block made of graphite, aluminium and iron located approximately $750m$ along a tunnel placed tangentially to the LHC ring [Gro95].

The subsystem responsible for the horizontal deflection of the beam is the beam dump kicker system, described in Chapter 2. Unavailability of the beam dump kicker system leads to failure of the beam dump system which in turn may become dangerous to the LHC. As a safeguard against the beam dump kicker system becoming unavailable it is monitored for faults by a surveillance system.

This report describes a proposal for the fault detection part of the surveillance system.

In Chapter 3 a brief overview of the surveillance system performing the fault detection is

[1]Large Electron - Positron collider, the present large accelerator at CERN with a circumference of $27km$. In LEP electrons and their anti-particles positrons are accelerated to energies of $100GeV$ [Gro91].

given, including the fault detection requirements.

To find the faults to be detected and where to detect them a fault propagation analysis, described in Chapter 4, is performed.

The result of the fault propagation analysis is used as a basis to make an off-line test used to declare the system fault free before start up. The test which is comprised of status bits an processing of the measured output pulse is described in Chapter 5.

The beam dump kicker system is continuously monitored to ensure that it does not become unavailable. This is done by the surveillance described in Chapter 6. The surveillance is comprised of status bits and a model based fault detection method based on analytic redundancy.

For both the off-line test and the continues surveillance an estimate of the requirements to the analog data acquisition is given.

1.1 Definitions

To avoid confusion, some of the commonly mistaken terms, are defined below, in the way they are used in this report.

Failure The termination of the ability of a system or subsystem to accomplish its required function within previously specified limits.[Fuq87]

Fault A change in the characteristics of a part or component such that its mode of operation or performance is changed in an undesired way. Required specifications are no longer fulfilled. [Bla97]

Fail - safe system A system where a fault leads to the system going into a safe state.

Fault tolerant system A system where a fault may lead to change of operation or reduced performance but a single fault does not develop into a failure on a subsystem or system level.[Bla97]

Reliability The probability that a system, subsystem or component will perform its intended function for a specified period of time under stated conditions.[Fuq87]

ADC	Analog to Digital converter
DAC	Digital to Analog converter
ZOH	Zero order hold (models sample and hold circuit)
$UID(\mu, \sigma^2)$	Uniform white noise with mean μ and variance σ^2
WSSR	Weighted sum squared residual

Table 1.1: Table of abbreviations

Chapter 2

Description of the LHC Beam Dump System

The LHC beam dump system has to perform the task of dumping the beam at all energies from the filling stage at $450GeV$ to the maximum energy of $7TeV$ [BCD+97]. Dumping the beam is the action of deflecting the beam from the closed orbit of normal operation to a dump area, where the beam is stopped and its energy released into a dump block. This means the extraction of $540MJ$ in $86\mu s$ giving a maximum power dissipation into the absorber within the dump block of $6300GW$ with a peak density of $1GW/cm^3$ [ZP97]. Dumping the beam is necessary either when a physics run has ended or some failure of the LHC has occurred.

The elements of the LHC beam dump are shown on Figure 2.1

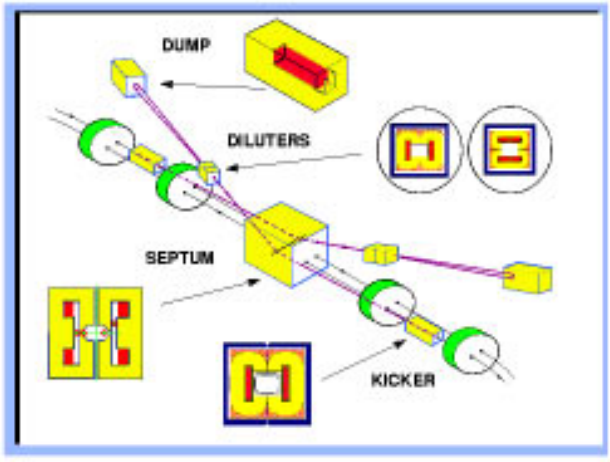

Figure 2.1: *The LHC beam dump system. Figure from [ZP97].*

When the beam is to be dumped, the kicker magnets produce a magnetic field, that deflects the beam horizontally from orbit into the dump tunnel. The vertical deflection is done by the septum magnet. Further downstream in the dump tunnel the diluter magnets spread the beam across the dump block so that the beam energy density on the dump block is reduced.

Since there are two rings with beams travelling in opposite directions the described beam dump system is doubled, so that each ring has its own beam dump system.

2.1 The Beam Dump Kicker System

In this project, special attention is given to the beam dump kicker system so it is described further. A simplified version of the functional layout of the beam dump kicker system is given in Figure 2.2

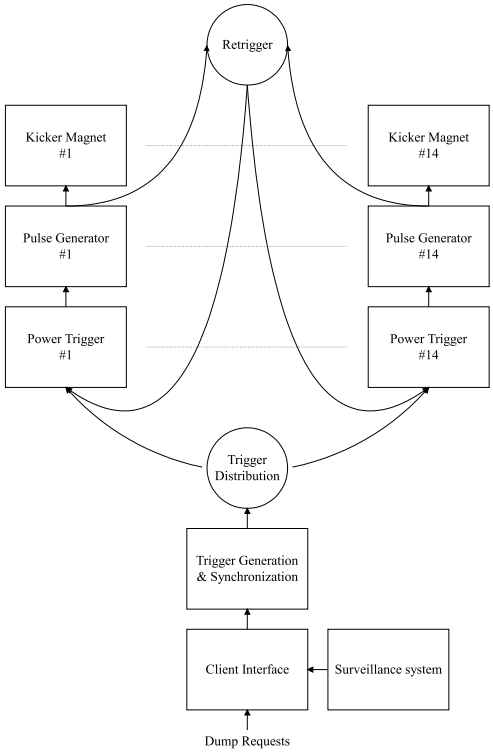

Figure 2.2: *Functional layout of the beam dump kicker system.*

The handling of a beam dump request is initiated by the trigger generation & synchronisation block. This block generates a trigger signal which is synchronised with the beam, so that the triggering happens in the particle free gap[1]. The triggering must be in the particle free gap to ensure that no part of the beam is only partially deflected due to rise-time in the kicker magnets.

When the triggering signal is generated it is distributed to 14 identical trigger execution chains[2]. Each of these chains consists of a power trigger, a pulse generator and a magnet.

Naming the deflection made by magnet 1, F_{M1}, the total deflection is

$$\text{Deflection} = \sum_{i=1}^{14} F_{Mi}$$

[1]The beam makes one revolution in $89\mu s$ which has a particle free gap of $3\mu s$.
[2]The 14 kicker magnets are placed on an $33m$ long straight section of the LHC[BCD+97].

The pulse generator is a device consisting of a number of semiconductor switches and capacitors. When these switches are closed the capacitors are discharged through the magnet, giving rise to a magnetic field deflecting the beam. This field must have a rise-time no longer than the particle free gap and a duration of at least one revolution period to be able to dump the beam safely.

The energy needed to close the semiconductor switches in the pulse generator comes from the power trigger. The power trigger has, like the pulse generator, a number of semiconductor switches. When these switches are closed capacitors are discharged to the pulse generator.

The retrigger protects the LHC from damage due to partial beam deflection caused by internally generated triggering of one of the execution chains. The retrigger relays the information from a number of trigger pick-up sensors in the pulse generator to the 13 not triggered chains as fast as possible. These chains then immediately trigger and the beam is dumped.

The surveillance system monitors the beam dump kicker system as described in Chapter 3.

2.1.1 Auxiliary systems

To complement the parts described in the previous sections there are a number of auxiliary systems.

Power Supply and tracking system

The power supplies charge the capacitors of the pulse generators so that the capacitors are charged with the energy needed to deflect the beam. The amount of energy is dependent on the energy of the beam and must be within the limits given by the angle to the dump tunnel (see Figure 2.1). The tracking of the energy of the LHC is done by the tracking system. A simplified block-diagram of the tracking system is shown on Figure 2.3.

The beam energy measuring device can be local to the beam dump system and/or it can be a value retrieved from other LHC systems.

There are two voltages involved per execution chain; the voltage of the primary circuit and the voltage of the compensation circuit. The primary circuit supplies the energy needed to get the rise-time of the magnetic field fast enough, $t_r < 3\mu s$. The compensation circuit supplies the energy to prolong the existence of the magnetic field to completely dump the beam.

Personal safety

Personal safety is the system preventing personnel from electric hazards. This includes emergency stops, manual safety switches and electrical discharge switches. The electrical discharge switches short-circuits the capacitors through a resistor to ensure that the ca-

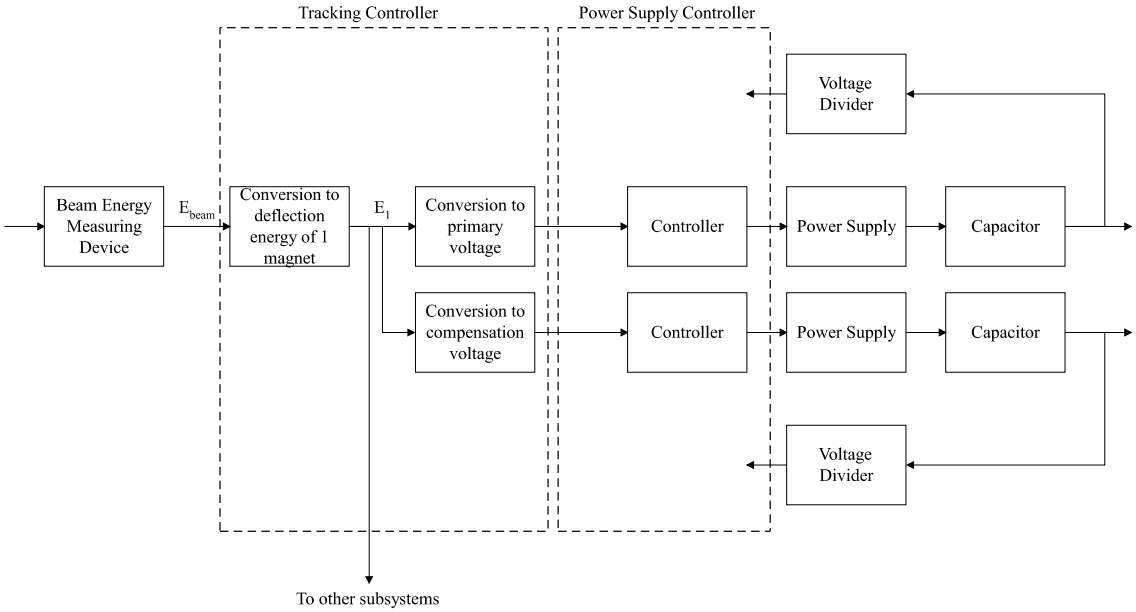

Figure 2.3: *Block diagram of the power supply and tracking system.*

pacitors are discharged in a safe way. After this the safety switches can be closed and the charging of the capacitors are inhibited.

2.1.2 Operating modes

The beam dump system has three modes of operation[3]as shown on Figure 2.4

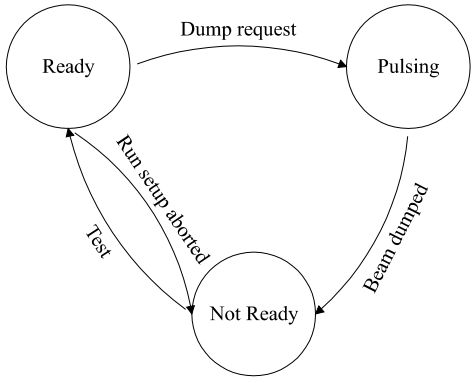

Figure 2.4: *Operating modes of the beam dump kicker system.*

These operating modes are:

Ready The system is ready to service a beam dump request. This system is in this mode for the duration of the physics run (10 hours).

[3]The LHC may pass through several modes of operation within the not ready and ready mode.

Pulsing The system is servicing a beam dump request. This lasts for as long as it takes to dump the beam ($89\mu s$).

Not Ready The system is not ready to service a dump request. Injection of beam into the LHC is inhibited in this mode.

2.1.3 Performance requirements

The performance requirements for the beam dump kicker system can be summarised as [BCD+97, Chap. 2]:

1. All beam dump requests must be honoured. The failure rate must be better than 1 failure/10^6 hours.
2. Operation of 13 out of 14 magnets is sufficient to dump the beam safely. However if one magnet becomes unavailable the beam must be dumped. This operation must have a failure rate better than 1 failure/10^6 hours.
3. Spurious and spontaneous triggering in one subsystem must result in triggering the remaining subsystems. The retriggering must have a failure rate better than 1 failure/10^6 hours.
4. The rate of spurious trigger events must be less than 1 event/year.
5. The reliability must be such that the availability of the LHC for physics is not reduced significantly [DBC+97].

The failure behaviour of the systems shall be [DBC+97]:

- The trigger generation and execution must be fault tolerant.
- The surveillance system and the fault detectors must be fault tolerant.

Due to the demands of reliability and availability of the beam dump kicker system, it consists of a number of redundant subsystems.

Chapter 3

General Overview of the surveillance system

The surveillance system is continuously monitoring the beam dump kicker system. This comprises the tasks of:

- Verifying the functioning of the beam dump kicker system continuously and taking adequate actions when a fault occurs. This includes verification of the correct functioning of the surveillance system itself.
- Providing information to the operations crew and logging data for later analysis.
- Protecting the hardware from dangerous operating conditions and inappropriate parameters.

The beam dump kicker system is an important part of the safety system of the LHC, so the only action available upon detection of a fault is issuing a beam dump request.

3.1 Requirements

The qualitative requirements for the fault detection are:

- Detection of every possible fault leading to subsystem failure before so much energy, on the pulse generator capacitors, has been lost that the beam no longer can be dumped safely.
- Detection of every possible fault of the surveillance system that leads to inconsistency between the status generated by the surveillance system and the actual status of the beam dump kicker system.

Considering that the time constant of the capacitors on the pulse generator is $\tau \approx 200s$ and the maximum allowed energy loss for safe dumping is 1 %, the time to detect a fault must be below $2s$.

From the general requirements of the beam dump kicker system, see section 2.1.3, requirement 2, and the envisaged run time of 10 hours it can be seen that only 1 fault per 10^5 runs may be missed. This gives the probability of missed detection for one execution chain per run as, $P_m < 10^{-5}$.

The reliability of the surveillance system must be such that it does not significantly reduce the availability of the beam dump system resulting in reduced availability of the LHC for physics. A significant reduction is considered to be when over 5% the beam dumps requested by the surveillance system are not necessary. This leads to a probability for total system false alarm per run of $< 5\%$. The probability of false alarm on one execution chain is thus $P_f < \frac{5\%}{14} = 0.36\%$.

The quantitative requirements can be summarised per run/subsystem as

- Time to detect $< 2s$
- Probability of missed detection $P_m < 10^{-5}$
- Probability of false alarm $P_f < 0.36\%$

Since the only possible action upon detecting a fault is dumping the beam, fault identification is not a requirement.

3.2 Structure

The hardware platform of the surveillance system is envisaged as a number of distributed data processing units e.g. PLC's, communicating by a network e.g. a field-bus.

In order to reduce the requirements of the network, specifically reliability and timing, the basic design philosophy is to make the software modules as autonomous as possible i.e. making the network interface as small as possible.

The information to the operations crew and protection against inappropriate operating conditions and parameters is a matter of communication with the surrounding higher level systems. These issues are not treated further in this report. Furthermore this report does not deal with the logging of data for analysis.

It is envisaged that the surveillance system is to be build entirely from commercially available industrial components[1]. The design should however, if possible, not be committed to a specific manufacturer or technology in order not to be dependent on outdated and possibly unavailable components at the time of implementation[2]. If this is not possible the design should be so modular, that the exchange of one component does not destroy the design.

The surveillance system is designed with three primary modules:

[1] Also referred to as COTS: Commercially Off The Shelf.
[2] The beam dump system is scheduled for implementation in 2001 or 2002.

Not Ready Test Test based on the data from the last beam dump to determine if there exists any faults in the beam dump kicker system prior to the next beam injection.

Ready Mode Surveillance Continuously verification of the power supply-, tracking- and charging systems. Furthermore the trigger-generation, -timing and -distribution is verified in this module.

Post Mortem Acquisition Data acquisition of the dump pulse needed in the next not ready test.

The interaction of the modules is shown on Figure 3.1

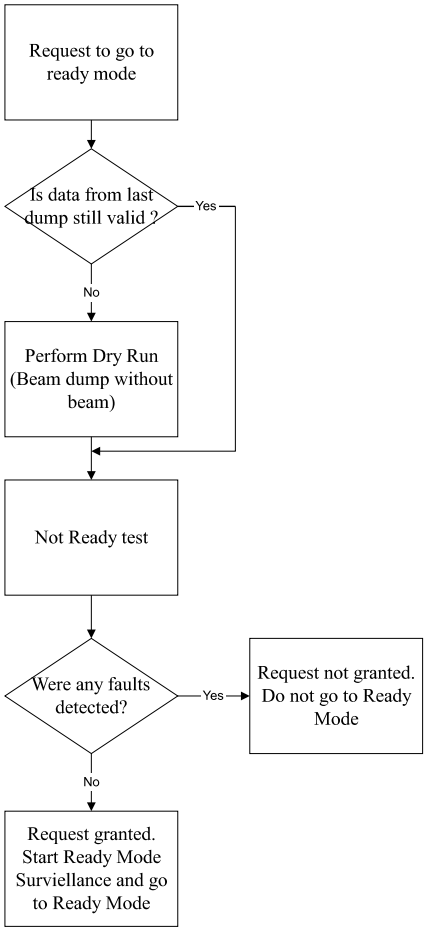

Figure 3.1: *The usage of the modules of the surveillance system. The data from the last dump is invalid if the power to the beam dump kicker system has been cut, since this might indicate that maintenance has been performed. The Ready Mode Surveillance is also active during a dry run to verify the functioning of power supply-, tracking- and charging systems.*

In this report only fault detection of the pulse generator, power trigger, retrigger and power supply systems are treated further.

Chapter 4

Fault analysis of the Beam Dump Kicker System

To find the faults to be detected by the surveillance system a fault and fault propagation analysis is performed. The fault propagation analysis has the purpose to find the way faults propagate through the system in order to find the system locations where fault propagation is stopped. These locations, together with the output, are the only places where it is necessary to make measurements for fault detection[1].

The analysis is done by constructing fault trees, see Section 4.4, structured to show the fault propagation of each subsystem. To be able to make the analysis the construction of each subsystem has to be known. The subsystems are described in the following sections.

4.1 Description of the pulse generator

The pulse generator is the subsystem responsible for delivering the current to the magnets generating the deflecting electro-magnetic field.

The pulse generator consists of two branches, each having a primary and a compensation circuit. The operation of the pulse generator can be performed by one branch only and the second branch is providing redundancy and thereby a better reliability of the pulse generator. The principle circuit diagram of the pulse generator is shown on Figure 4.1.

To charge the capacitors two power supplies are used[2]: The primary power supply at $31kV$ and the compensation power supply at $0.5kV$. The following description of the pulse generator principle is for the A branch. The B branch is working in the same way.

The primary circuit consisting of CpA, GTOpA and DpA provides the energy needed to give the magnet a pulse with a rise time of $3\mu s$. This is done by closing the GTO switch

[1]The location where fault propagation is stopped is not necessarily the best location for fault detection measurements due to fault effect damping. However the fault propagation analysis gives a good first indication on where to make the fault detection measurements.

[2]The values are for the single branch prototype.

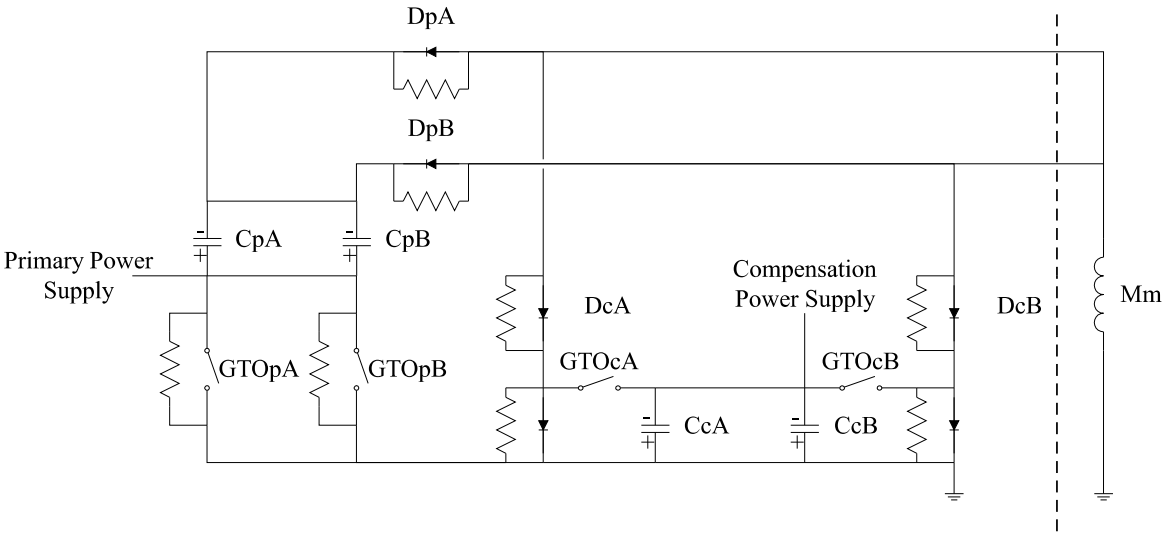

Figure 4.1: *Principle circuit diagram of the dual branch pulse generator.*

GTOpA which in turn discharges the capacitor CpA. When the voltage on CpA drops the series diode DpA closes and the free wheel diode DcA of the compensation circuit opens.

If the GTO switch GTOcA is closed the compensation capacitor CcA is discharged to prolong the pulse to the wanted pulse length of $90\mu s$.

The resistors on Figure 4.1 provide the right voltage distribution for the semiconductor components and the damping of the pulse.

To be able to generate the correct pulse the GTO switches of both the primary and the compensation circuit must be closed at the same time. This is done using a trigger transformer which is shown on Figure 4.2

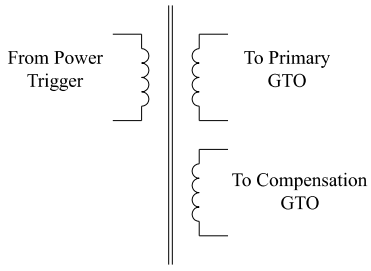

Figure 4.2: *Principle of the trigger transformer.*

Each branch of the pulse generator has its own trigger transformer.

To improve the reliability of the pulse generator two bars are connecting the primary capacitors ensuring that both capacitors are discharged if one of the primary switches does not close. One bar is connecting the compensation capacitors to ensure that they are both discharged if one of the compensation switches does not close.

4.2 Description of the power trigger

The power trigger is the subsystem responsible for delivering the power needed to close the GTO switches in the pulse generator. A principle diagram of the power trigger is shown on Figure 4.3

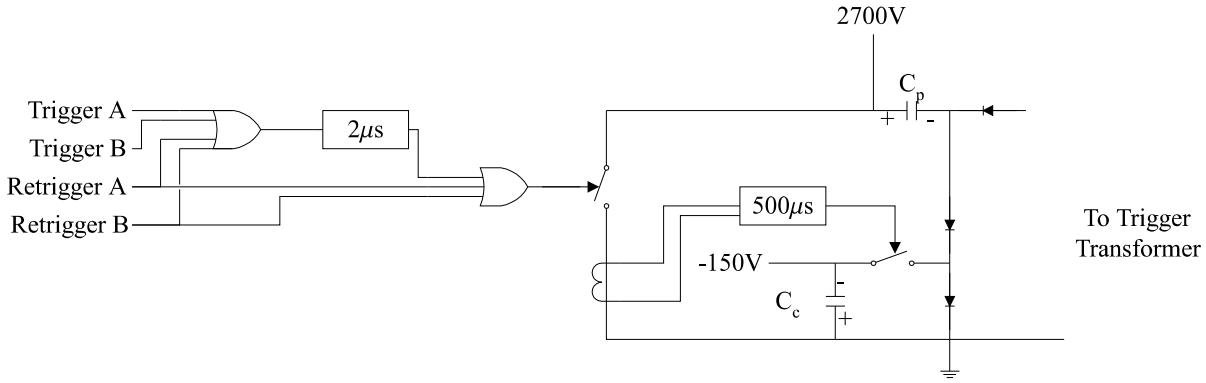

Figure 4.3: *Principal diagram of the power trigger.*

Upon reception of an input on one of the lines: Trigger A, Trigger B, Retrigger A or Retrigger B, the primary GTO switch is closed and the capacitor C_p is discharged giving an output pulse with an amplitude of $320A$. The input signal has only a short duration so a mono-stable prolongs its duration to $2\mu s$. The retrigger input is at first bypassing the input mono-stable to make the response to a retrigger signal faster. To make the duration longer the signal is subsequently prolonged by the input mono-stable.

The energy from C_p is used to generate a pulse with fast rise-time. The current from the discharging of C_p is picked up and used in a mono-stable that prolongs the pulse to $500\mu s$. The output of the mono-stable is used to close the compensation switch, which in turn leads to the discharge of capacitor C_c. The energy of C_c is used to ensure that the switches in the pulse generator are closed during the whole dump.

To improve overall system reliability the power trigger is redundant.

4.2.1 Internal status generation

The power trigger generates a number of status bits internally. This status information can be divided into two parts

- Static voltages
- Input/output pulse information

The static voltages are acquired by comparators which gives one bit for the voltages:

- $15V$, used for the input logic.

- $48V$, used for the input logic.
- $150V$, used for charging the compensation capacitor.
- $2.7kV$, used for charging the primary capacitor.

The input pulse information are status bits that indicate that the following input lines have been used:

- Trigger A
- Trigger B
- Retrigger A
- Retrigger B

The output pulse information are status bits of

- The amplitude of the output voltage, generated by a comparator connected to a flip-flop.
- The amplitude of the output current, generated by a comparator connected to a flip-flop.
- The length of the output pulse generated by a counter, see Figure 4.4.

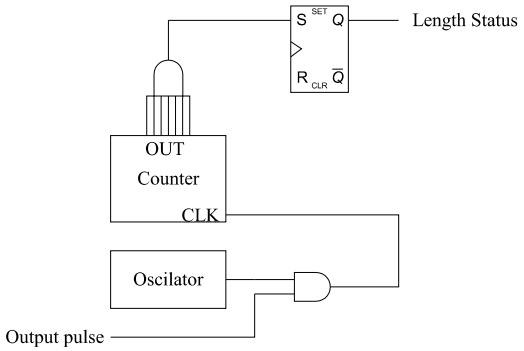

Figure 4.4: *The pulse length verification circuit of the power trigger.*

4.3 Description of the retrigger system

The retrigger system is the subsystem responsible of triggering all execution chains if a spontaneous trigger occurs in one chain.

The principle of the retrigger system is shown on Figure 4.5

The retrigger picks up the execution of a pulse by 5 pick ups in the pulse generator:

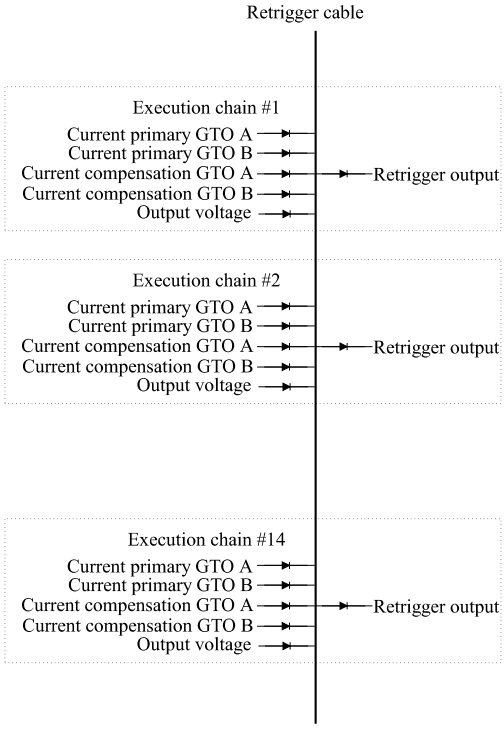

Figure 4.5: *Principle of the retrigger.*

- Current of primary GTO switches, by current transformers.
- Current of compensation GTO switches, by current transformers.
- Voltage at the output of the pulse generator, by a voltage divider.

The current from the pick-ups are measured by current transformers and used to set flip-flops indicating the source of the retrigger signal.

To monitor if the retrigger cable is broken or connected wrong a constant stand-by signal is applied. The amplitude is smaller than the diode voltage and does therefore not interfere with the operation of the retrigger system.

Verification of the stand-by signal is done in hardware e.g. by a comparator or a retriggerable mono-stable.

To improve overall system reliability the retrigger system is redundant.

4.4 Component fault tree analysis

This section describes the parts of the fault tree analysis method used in this project. For a more thorough description of fault trees, the reader is referred to the literature on reliability analysis e.g. [Ave92].

The fault tree analysis is a graphical "top - down" tool to investigate the reasons for an unwanted event. The unwanted event, named the top event, is investigated by repeatedly asking the question "What have caused this failure to happen ?". The answers are then combined using the symbols in Figure 4.6[3]. The analysis is stopped when the required level of detail is reached e.g. component level faults. The events/faults at this level are called basic events.

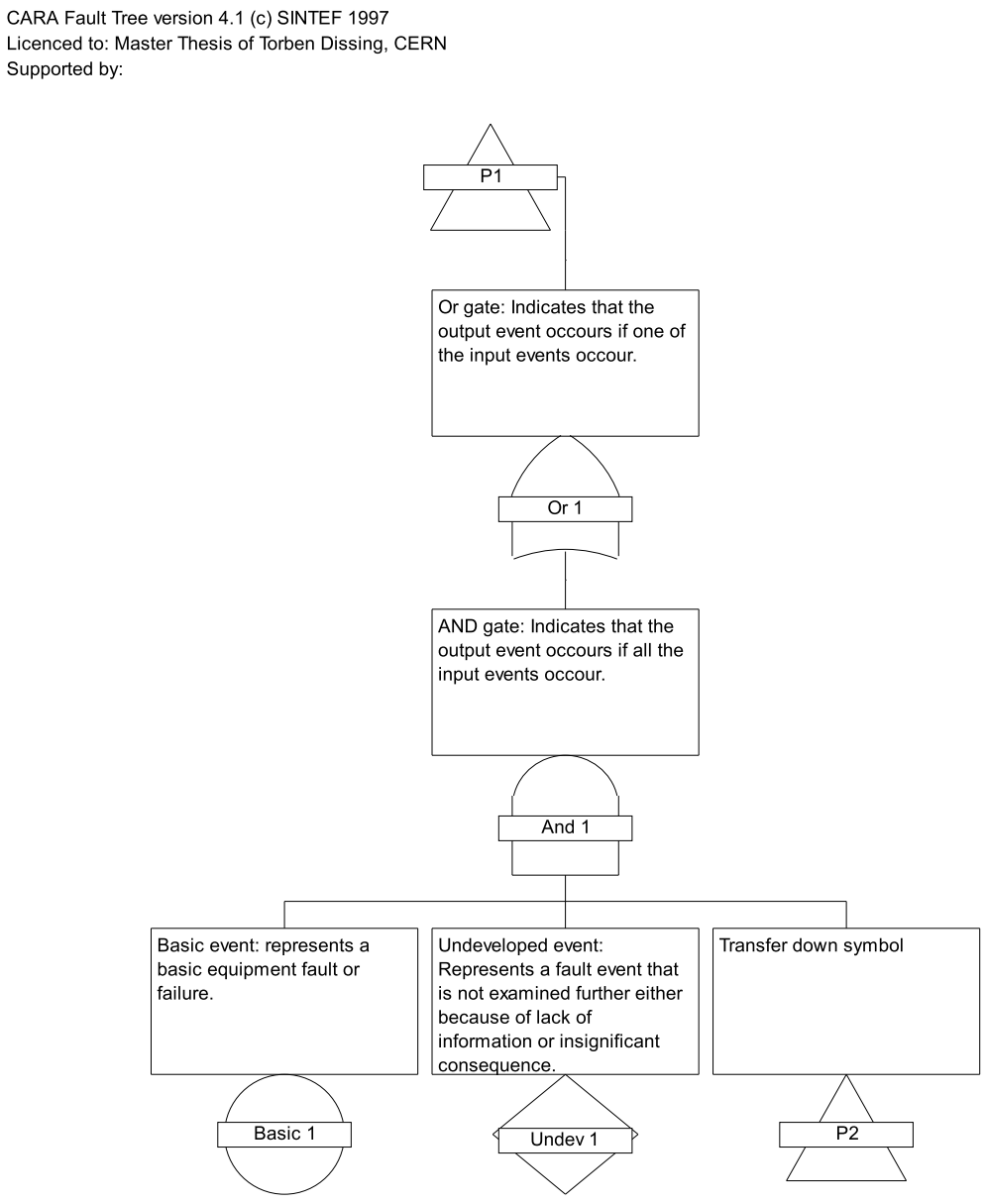

Figure 4.6: *Symbols used in the fault tree analysis.*

The component fault tree is a way of structuring the fault tree so that it reflects the fault propagation in the system. When using the fault tree in this way every basic event represents a fault/failure mode of a component.

[3]The figure describes the symbols used in this report. The fault tree approach includes more symbols such as e.g. k-out-of-n and inhibit gates.

The top event is always the event of system/subsystem failure, or a measurement indicating system/subsystem failure. The top event is connected to events representing the end effects of the system/subsystem by an or-gate. The next level down represents the components directly connected to the output. Input, output and component failures are connected as basic events. The effects of the input components are connected by the gate describing the fault propagation.

An inventory of the faults to be detected can be made by listing all the basic events.

By structuring the fault tree as a component fault tree, the minimum cut sets with only one element represents the faults propagation to the end effects.

A cut set is a set of basic events whose (simultaneous) occurrence ensures that the top event occurs[CAR].

A minimal cut set is a cut set, that can not be reduced without losing its status as a cut set[CAR].

4.5 Fault tree for the power trigger

Figure 4.7, 4.8, 4.9 and 4.10 shows the fault tree for the power trigger. The fault tree's for the remaining subsystems are in Appendix E.

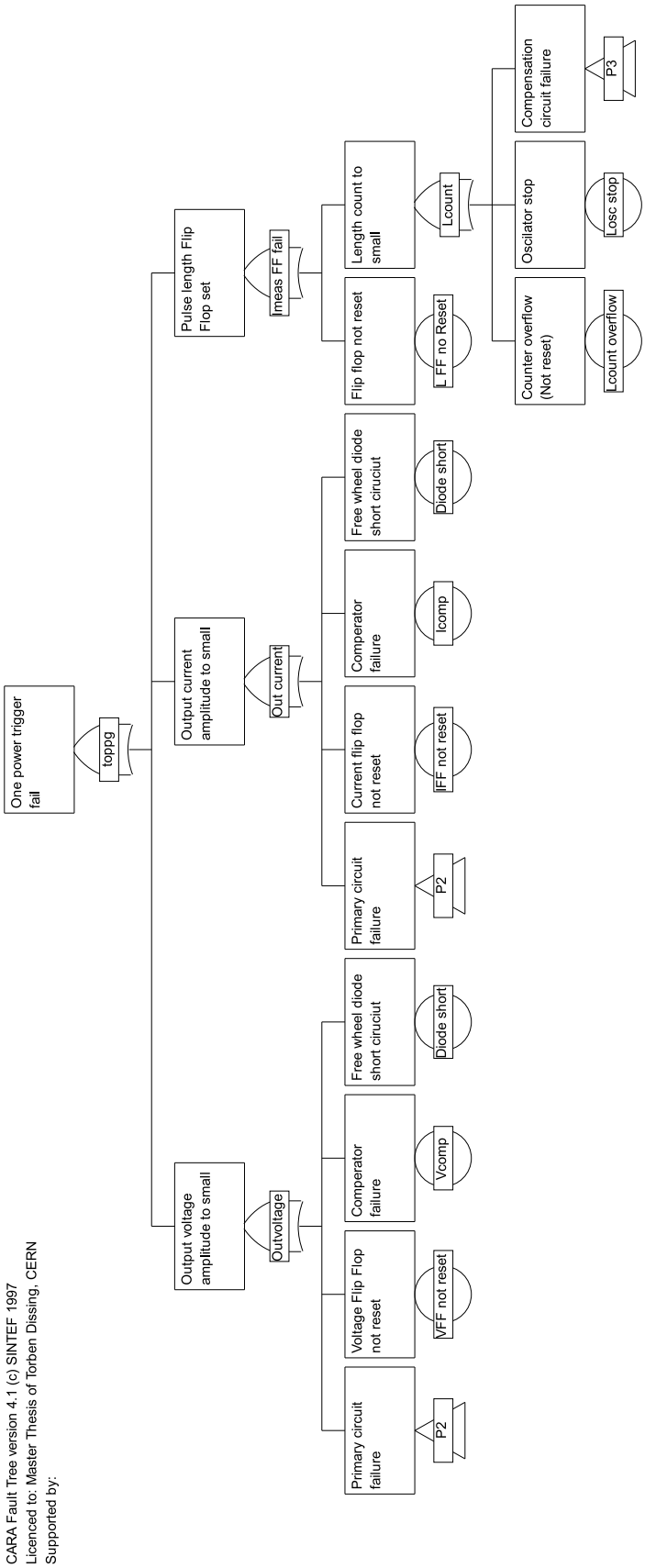

Figure 4.7: *Fault tree page 1 for the power trigger.*

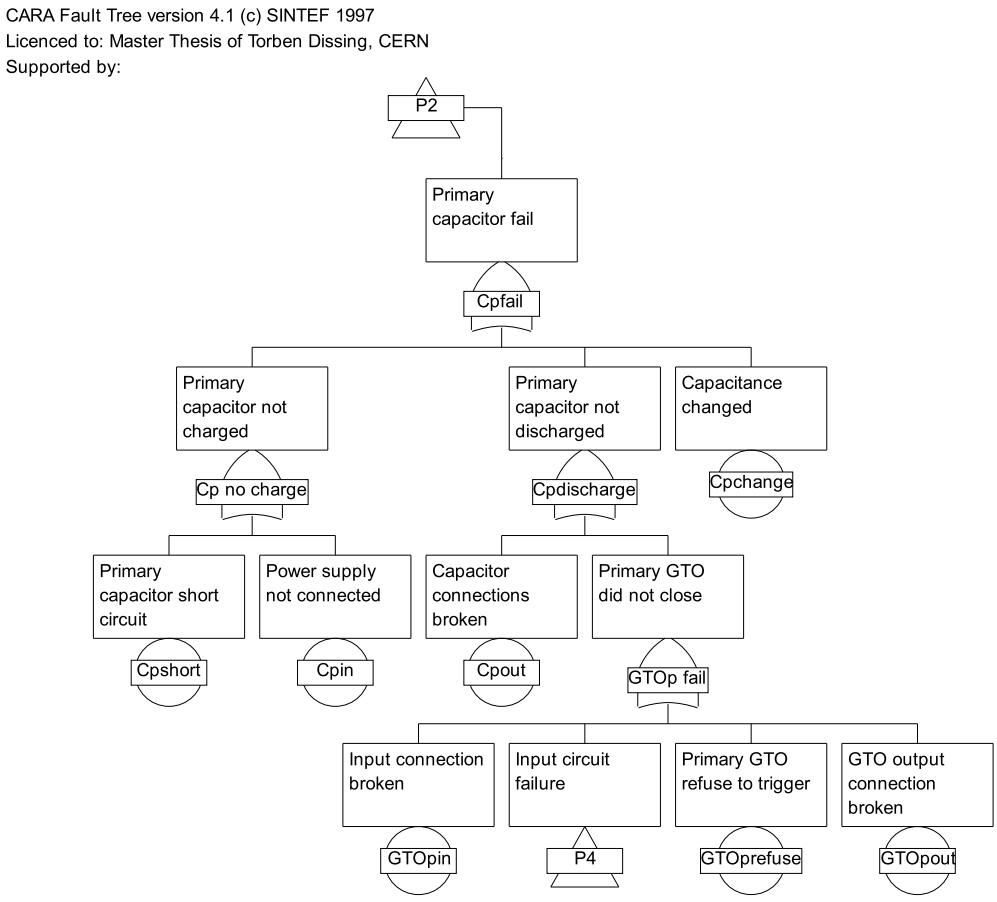

Figure 4.8: *Fault tree page 2 for the power trigger.*

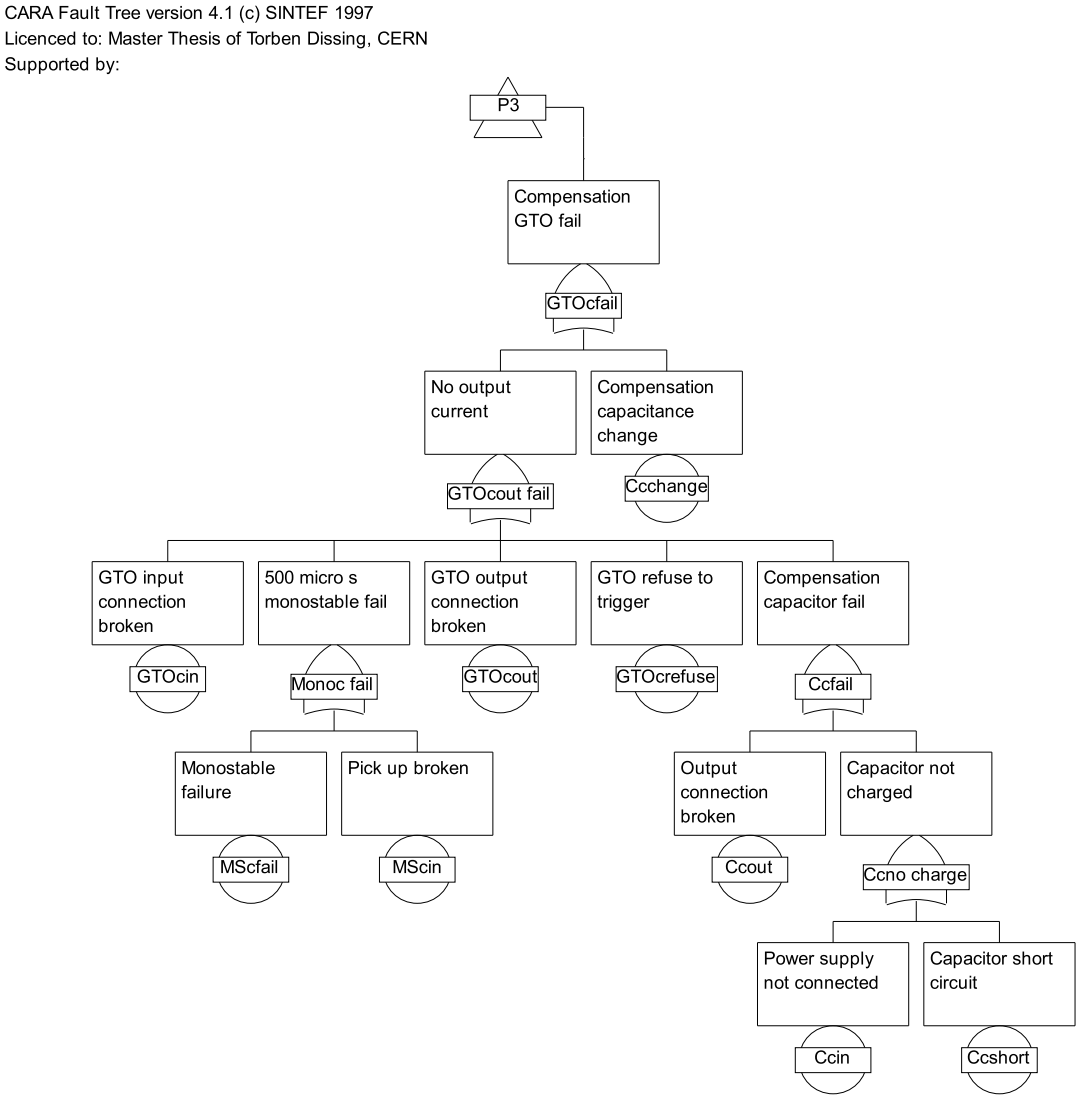

Figure 4.9: *Fault tree page 3 for the power trigger.*

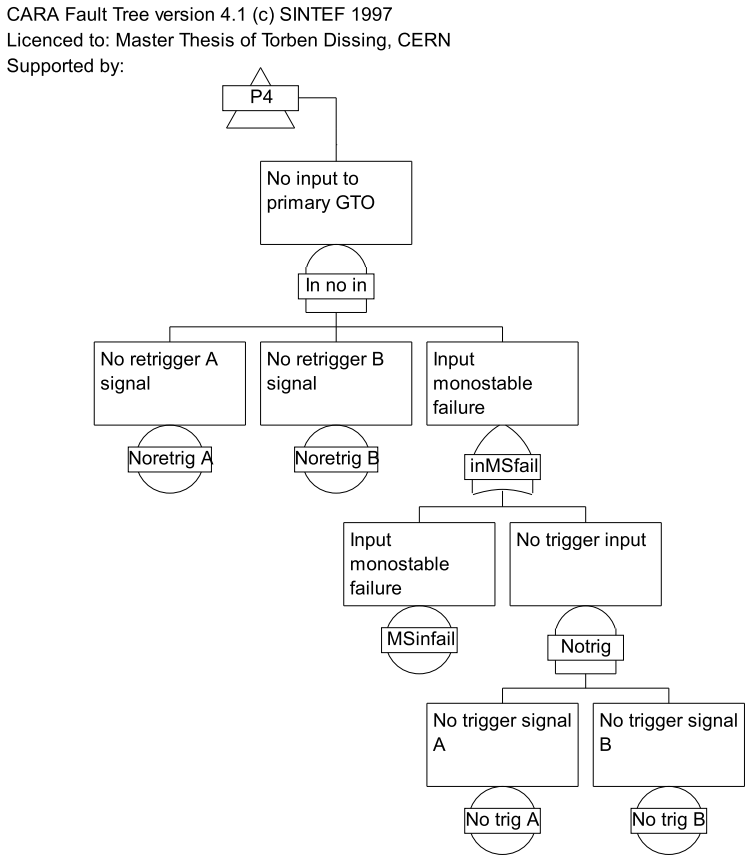

Figure 4.10: *Fault tree page 4 for the power trigger.*

Chapter 5

Not Ready Test

The Not Ready Test is the test performed when making the transition from not ready mode to ready mode. The purpose of the test is to verify that there are no faults existing in the beam dump kicker system prior to injection of beam into the LHC.

In the following sections the test needed for each subsystem is described.

5.1 Test of the pulse generator

Analysis of the fault tree, see Appendix E, shows that some faults do not propagate to the end effects. These faults can not be detected by looking at the end effects and must be detected by other means. The components having non propagating faults are the GTO switches.

Since all faults of the Trigger transformers propagate to the GTO switches and the effect of GTO failure is GTO switch not closed, the detection of faults in the trigger transformers can be done by verifying that the GTO switches have closed.

When the GTO switches close a retrigger signal is generated so this event can be detected by the status monitoring of the retrigger system.

To test if all capacitors have been discharged the fact, that if one capacitor is not discharged the equivalent capacitance of the parallel capacitors will be half of the nominal value, is used. For the pulse generator four scenarios of capacitor output faults are simulated.

1. Working system.
2. Primary capacitor output connection broken.
3. Compensation capacitor output connection broken.
4. Primary and compensation output connection broken.

A simulation of the magnet current using the model described in Section 5.2 with the component values of Table 5.1[1] is shown on Figure 5.1. The simulation is made with the assumption that the primary capacitor is charged to $-31kV$ and the compensation capacitor is charged to $-0.5kV$, which corresponds to maximum beam energy.

Component	**Value**
C_p	$1.3\mu F$
C_c	$4mF$
L	$2.73\mu H$
R_m	0.02Ω

Table 5.1: *Component values for a working pulse generator.*

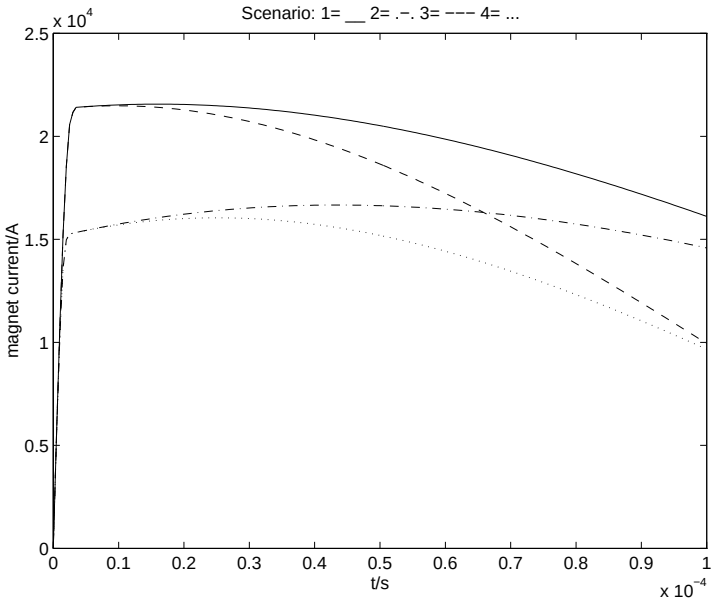

Figure 5.1: *Simulated magnet current for the four different scenarios. 1:Working system, 2:Primary capacitor broken, 3: Compensation capacitor broken, 4: Primary and compensation capacitor broken.*

By checking if the magnet current is below a threshold given by the working system at time $t \approx 70\mu s$ it can be seen if any of the capacitors have failed. The threshold used cannot be fixed because the amplitude of the magnet current is linked to the beam energy. Therefore the magnet current should preferably be a sampled analog value and the threshold test performed by software.

Another possibility is to integrate the magnet current. This gives the value in Table 5.2

Using the integrated value care must be taken because two different signals can integrate to the same value, which could lead to an undiscovered fault.

An alternative method giving more specific fault information is to estimate the capaci-

[1]The component values are the values used in the single branch prototype in operation on 22th February 1999. Source: Gene Vossenberg, CERN SL - division. The value of R_m is a guess made by the author and does not reflect the value existing in the prototype.

Scenario	Integrated value
1	$3.94 \cdot 10^6$
2	$3.19 \cdot 10^6$
3	$3.49 \cdot 10^6$
4	$2.83 \cdot 10^6$

Table 5.2: *Values of the integrated magnet current. Scenario 1:Working system, 2:Primary capacitor broken, 3: Compensation capacitor broken, 4: Primary and compensation capacitor broken.*

tances of the pulse generator. This is described in Section 5.3.

Short circuit of the series or free wheel diodes is detectable by analysis of the output pulse. A possible analysis method is described in Section 5.3

The magnet and the connections to the magnet are tested by measuring the magnet current. The connection to the magnet is made by a number of cables in parallel. It can be tested if all cables are connected by estimating the inductance and the resistance of the combined pulse generator and magnet. This approach is described in Section 5.3.

The faults having the effects of the capacitors not being charged are detected by the power supply and tracking system surveillance, described in Chapter 6.

The pulse generator is ready for operation if there have been no faults detected by the power supply and tracking system surveillance and the tests summarised in Table 5.3 gives acceptable results. The tests are performed using data from a dump or a dry run.

Test number	Purpose	Test action	Sensors
PG1	Test of primary GTO's and trigger transformers	Test output current of primary GTO's	Retrigger status bits
PG2	Test of compensation GTO's and trigger transformers compensation coil	Test output current of compensation GTO's	Retrigger status bits
PG3	Test of capacitors, compensation diodes and magnet	Test of magnet current below threshold at $t \approx 70\mu s$, integration or parameter estimation	CT1m, CT2m

Table 5.3: *Additional tests needed to declare the pulse generator ready for operation.*

5.2 Hybrid mathematical model of the pulse generator

In this section a model of the pulse generator is made. This model is used for simulation and as a reference model used for fault detection using parameter estimation.

Since the voltage difference between cathode and anode of the diodes is in a large interval, from approximately $0V$ to approximately $30kV$, it is not possible to make a linear model valid for the whole operating range of the system. To deal with this problem a non-linear model using the diode equation can be used. Another possibility is to make an ideal model

of a diode as an open connection if

$$V_{\text{anode}} - V_{\text{cathode}} < \text{threshold}$$

and as a short circuit otherwise.

With ideal diodes the pulse generator can be split up into two models

Primary model Used when the current flows through the series diodes DpA and DpB.

Compensation model Used when the current flows through the free wheel diodes DcA and DcB.

It is assumed that the two models are not active at the same time i.e. the current does not flow through both the series and the free wheel diodes at the same time.

Assuming that all GTO switches are closed the pulse generator and magnet can, for both models, be described by the circuit diagram on Figure 5.2

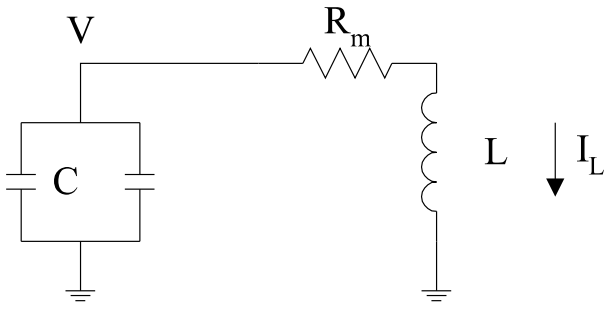

Figure 5.2: *Circuit diagram used for the hybrid model of the pulse generator. C are the primary capacitors in the primary model and the compensation capacitors in the compensation model.*

R_m is the total resistance of the pulse generator and magnet. L is the the total inductance. R_m and L are assumed to have the same value in both the primary and the compensation model.

Due to the assumption that all GTO switches are closed the system is autonomous and can be described by Equation 5.1 and 5.2. Furthermore due to the assumption of ideal diodes the transfer between the primary and the compensation circuit[2] is not modelled.

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} \tag{5.1}$$
$$y = \mathbf{C}\mathbf{x} \tag{5.2}$$

The choice between primary and compensation model is made as:

[2]Referred to as the dip.

- Use primary model if $V_c > V_p + \text{threshold}$

where V_c is the voltage over the compensation capacitors and V_p is the voltage over the primary capacitors.

5.2.1 The primary model

The primary model is described by the differential equations

$$\begin{aligned} \dot{V}_p &= \frac{1}{C_p} I_L \\ \dot{I}_L &= -\frac{1}{L}(V_p - R_m I_L) \end{aligned}$$

where $C_p = CpA \parallel CpB$.

Choosing the primary state vector as

$$\mathbf{x}_p = \begin{bmatrix} V_p \\ I_L \end{bmatrix}$$

the system matrices of Equation 5.1 and 5.2 becomes

$$\begin{aligned} \mathbf{A}_p &= \begin{bmatrix} 0 & \frac{1}{C_p} \\ -\frac{1}{L} & -\frac{R_m}{L} \end{bmatrix} \\ \mathbf{C}_p &= \begin{bmatrix} 0 & K_m \end{bmatrix} \end{aligned}$$

K_m is the amplification of the measuring equipment i.e. the current ratio of the current transformer.

5.2.2 The compensation model

The compensation model can be described by the same differential equations as the primary model by exchanging V_p by V_c and C_p by C_c. By choosing the compensation state vector as

$$\mathbf{x}_c = \begin{bmatrix} V_c \\ I_L \end{bmatrix}$$

the system matrices of Equation 5.1 and 5.2 becomes

$$\begin{aligned} \mathbf{A}_c &= \begin{bmatrix} 0 & \frac{1}{C_c} \\ -\frac{1}{L} & -\frac{R_m}{L} \end{bmatrix} \\ \mathbf{C}_c &= \begin{bmatrix} 0 & K_m \end{bmatrix} \end{aligned}$$

5.2.3 The hybrid model

The hybrid model is obtained by combining the two state vectors $\mathbf{x}_p$ and $\mathbf{x}_c$ to

$$\mathbf{x} = \begin{bmatrix} V_p \\ V_c \\ I_L \end{bmatrix}$$

This yields the system matrices

$$\begin{aligned} \mathbf{A}_p &= \begin{bmatrix} 0 & 0 & \frac{1}{C_p} \\ 0 & 0 & 0 \\ -\frac{1}{L} & 0 & -\frac{R_m}{L} \end{bmatrix} \\ \mathbf{A}_c &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \frac{1}{C_c} \\ 0 & -\frac{1}{L} & -\frac{R_m}{L} \end{bmatrix} \\ \mathbf{C} &= \begin{bmatrix} 0 & 0 & K_m \end{bmatrix} \end{aligned}$$

The rule for the use of the $\mathbf{A}$ matrices is

- Use $\mathbf{A}_p$ when $V_c > V_p + \text{threshold}$, otherwise use $\mathbf{A}_c$

5.2.4 System bandwidth

In order to know the minimum sampling frequency, knowledge of the bandwidth of the system is required. Calculation of bandwidth from the definition as the maximum frequency at which the system output can track an input sinusoid satisfactorily [FPEN94, p.343] is not possible due to the autonome behaviour of the pulse generator. The bandwidth of the system is therefore calculated as the bandwidth of the measured output signal. This is the frequency f_{bw} of the sinusoid having a rise time of t_r i.e. the sinusoid which goes from zero to the maximum amplitude in t_r. Calculating the rise time from 0% to 95% of the maximum amplitude gives

$$A\sin(2\pi f_{bw}t_r) = 0.95A \tag{5.3}$$

Using the specification rise time of $t_r = 3\mu s$ in Equation 5.3 yields a bandwidth of the magnet current pulse of

$$f_{bw} = 66.5kHz$$

This is to be regarded as the minimum bandwidth since the pulse generator is designed with a safety margin and in the event of a primary capacitor failure the bandwidth will increase together with an amplitude decrease.

To meet the Nyquist criterion the minimum sampling frequency must be

$$f_{smin} = 133kHz$$

A higher sampling frequency than f_{smin} is preferred to avoid aliasing in the event of capacitor failure. However a very high sampling frequency is not desirable due to the increase of noise sensitivity at increasing frequency.

5.3 Fault detection by parameter estimation

The section describes a method of performing the test PG3 of Table 5.3 that gives a more detailed image of the state of the pulse generator. It suffers however of the disadvantage of being more complicated.

The method is based on direct parameter estimation [Knu96] of selected parameters of the pulse generator.

The parameter estimate is based on having a simulation model

$$y_m(k) = F(u_N, \theta) \tag{5.4}$$

where y_m is the output and F is the simulation function. F is a function of the input vector u_N with N samples and the parameters θ. The model used is the hybrid model of the pulse generator described in Section 5.2. The hybrid model describes an autonomous system and has therefore no input so the system response is based on the initial state $\mathbf{x}_0$ instead of the input.

Taking a measured signal y, the goal is to minimise the quadratic performance function $V(\theta)$

$$V(\theta) = \frac{1}{2N} \sum_{k=1}^{N} \epsilon^2(k, \theta) \tag{5.5}$$

where N is the number of samples and the model error ϵ is

$$\epsilon(k) = y(k) - y_m(k) \tag{5.6}$$

The parameter estimate θ_N is the value of θ that minimises the performance function in Equation 5.5

$$\theta_N = \arg_\theta \min V(u_N, y_N, \theta)$$

The parameter vector θ for the pulse generator is

$$\theta = \begin{bmatrix} C_p \\ C_c \\ L \\ R_m \end{bmatrix}$$

The model is transformed into a time discrete model using the ZOH transform [FPW90].

The value of θ_N can for simple systems be found analytically, but for most systems a numerical solution is needed. To find θ_N the Gauss-Newton minimisation algorithm is used, see Appendix D.

In general the model described by Equation 5.4 can be non-linear which results in the possibility of the performance function, Equation 5.5, having more than one minimum.

It is also not guaranteed that the minimum found by the numerical minimisation algorithm is the global minimum. In order to avoid this problem the initial parameter vector, θ_0, should be as close to the real parameters as possible. For this application the choice of initial parameter vector is the nominal values of the components of a working system.

When using a numerical minimisation technique it is not guaranteed that it will be convergent if the initial parameter vector is too far from the parameter vector giving the minimum value of the performance function. Choosing the initial parameter vector with the nominal component values, the lack of convergence of the algorithm indicates a fault either in the pulse generator or the surveillance system.

Since the model is autonomous there is no input and therefore no way of designing the input to obtain large parameter sensitivity. Large parameter sensitivity is needed in order to obtain accurate parameter estimates [Knu96, p. 6].

The sensitivity measure of interest here is the minimum sensitivity S_{imin} of every parameter because it is needed for the calculation of the parameter uncertainty, see Equation 5.8. The goal is to get these sensitivities as large as possible. There are more sensitivity parameters, but since input signal design is not possible for this application, they will not be discussed.

S_{imin} can be calculated from the second derivative of the performance function with respect to the parameter vector $\mathbf{H}_{rn}(\theta_N)$. This is the Hessian matrix, see Appendix D, at the optimal parameter vector with N samples, when relative parameters and normed signals are used. S_{imin} is [Knu96]

$$S_{imin} = \sqrt{\{\mathbf{H}_{rn}^{-1}(\theta_N)\}_{ii}^{-1}}$$

Relative parameters and normed signals are used in order to be able to compare different sensitivities. The relative parameter vector θ_r is

$$\theta_r = \mathbf{L}^{-1}\theta \tag{5.7}$$

where

$$\mathbf{L} = \mathbf{I}\theta_0$$

Again the relative parameter vector is most useful when input signal design is possible.

The value of S_{imin} is taken not to be depending on the sampling frequency. Since $\mathbf{H}_{rn}$ is dependent on the model some dependency on the sampling frequency is expected due to the discrete time model dependency of sampling frequency. However this dependency, which is decreasing with frequency, is neglected.

The model is furthermore not linear in the parameters which is why the sensitivity is expected to be different for different parameter values i.e. the sensitivity is expected to be different for each capacitor fault scenario.

For a beam dump at full energy the initial state is

$$\mathbf{x}_0 = \begin{bmatrix} -31kV \\ -0.5kV \\ 0A \end{bmatrix}$$

and the initial parameter vector is

$$\theta_0 = \begin{bmatrix} 1.3\mu F \\ 4mF \\ 2.73\mu H \\ 0.02\Omega \end{bmatrix}$$

A simulation of the magnet current assuming a measurement amplification $K_m = \frac{1}{5000}$ is shown on Figure 5.3. Using this simulation the sensitivities in Table 5.4 are found.

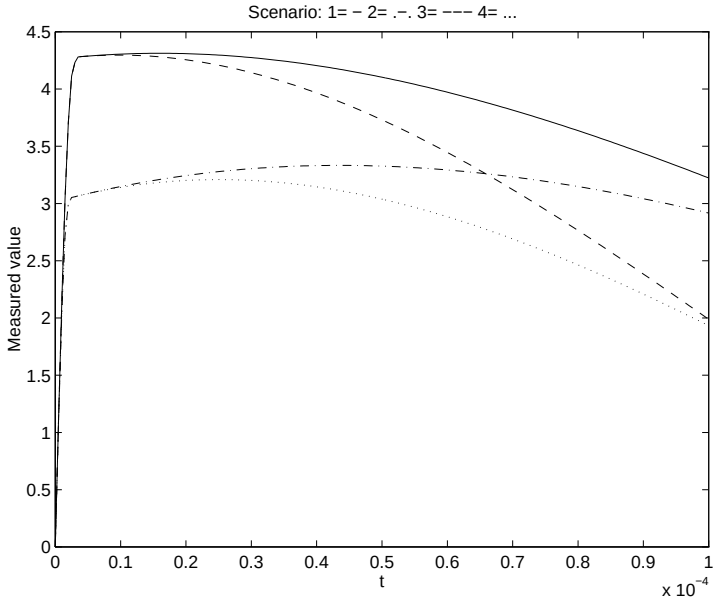

Figure 5.3: *Simulation of the magnet current for the four different scenarios; 1:Working system, 2:Primary capacitor broken, 3: Compensation capacitor broken, 4: Primary and compensation capacitor broken.*

Parameter\Scenario	**1**	**2**	**3**	**4**
C_p	0.616	0.110	0.131	0.121
C_c	0.144	0.0322	0.0737	0.0622
L	0.615	0.0673	0.167	0.0753
R_m	14.0	0.0505	0.0624	0.0597

Table 5.4: *Value of S_{imin} for the four different scenarios; 1:Working system, 2:Primary capacitor broken, 3: Compensation capacitor broken, 4: Primary and compensation capacitor broken.*

The lowest value of S_{imin} is that of estimating C_c in scenario 2: primary capacitor broken. In general for all four scenarios the parameter C_c has the lowest sensitivity and is therefore the parameter most vulnerable to noise and modelling errors.

By extending the model used for parameter estimation to include the diodes described by the diode equation, detection of partial diode short circuits is possible. It is however not seen as a feasible possibility due to decrease in sensitivity. The decrease in sensitivity is caused by the increased number of parameters and their non-linear properties together with the missing possibility of designing suitable input signals.

5.3.1 Sampling frequency and resolution requirements

The total relative parameter uncertainty, $\tilde{\theta}_{ritot}$, of the ith parameter is in the presence of quantisation noise, see Appendix A

$$\tilde{\theta}_{ritot} = \frac{1}{S_{imin}} \left(\frac{A2^{-d}}{y_{RMS}\sqrt{12}\sqrt{N}} + \epsilon_{m,RMSn} \right) \tag{5.8}$$

where A is the amplitude range of the ADC and d is the number of bits not counting the sign bit.

$\epsilon_{m,RMSn}$ is the value of the performance function, Equation 5.5, that is due to under modelling[3]. Since the topic of this section is sampling frequency and resolution the model is assumed to be perfect and thus $\epsilon_{m,RMSn}= 0$.

The number of samples N is dependent on the sampling frequency, f_s, since the data acquisition is limited in time to $t_{duration} = 100\mu s$. This gives

$$N = int(f_s t_{duration})$$

where int denotes the operation of truncation to an integer value. Under the assumption that the ADC range is $\pm 10V$ the total relative parameter uncertainty is shown on Figure 5.4 for C_c in scenario 2.

Choosing a sample frequency of $f_s = 200kHz$, which is well above the minimum sampling frequency of Section 5.2.4, gives the total relative parameter uncertainty shown on Figure 5.5

As can be seen from Figure 5.5 the uncertainty by sampling with more than 8 bits and a sign bit is below 1%. Compared to expectations of uncertainty from other sources such as component tolerance, see Section 5.3.2, an uncertainty from quantisation of 1% is considered to be neglectable.

The above considerations are made for a beam dump at full energy, that is with a signal RMS value $= 3.19V$ for scenario 2. From Equation 5.8 it can be seen that the parameter uncertainty increases with decrease of signal RMS value. This means that to get the same parameter uncertainty for low energy beam dumps the precision of the ADC must be increased. However post mortem data from low energy beam dumps will, as it will be shown in Section 6.2.3, be considered invalid, requiring a full energy dry run. To conclude, low energy beam dumps require better ADC precision, but since there will be made no decision on low energy beam dump post mortem data, the above calculation will be used as a guideline for choosing ADC precision.

[3]Under modelling is a term describing the fact, that the model does not complete describe the real world.

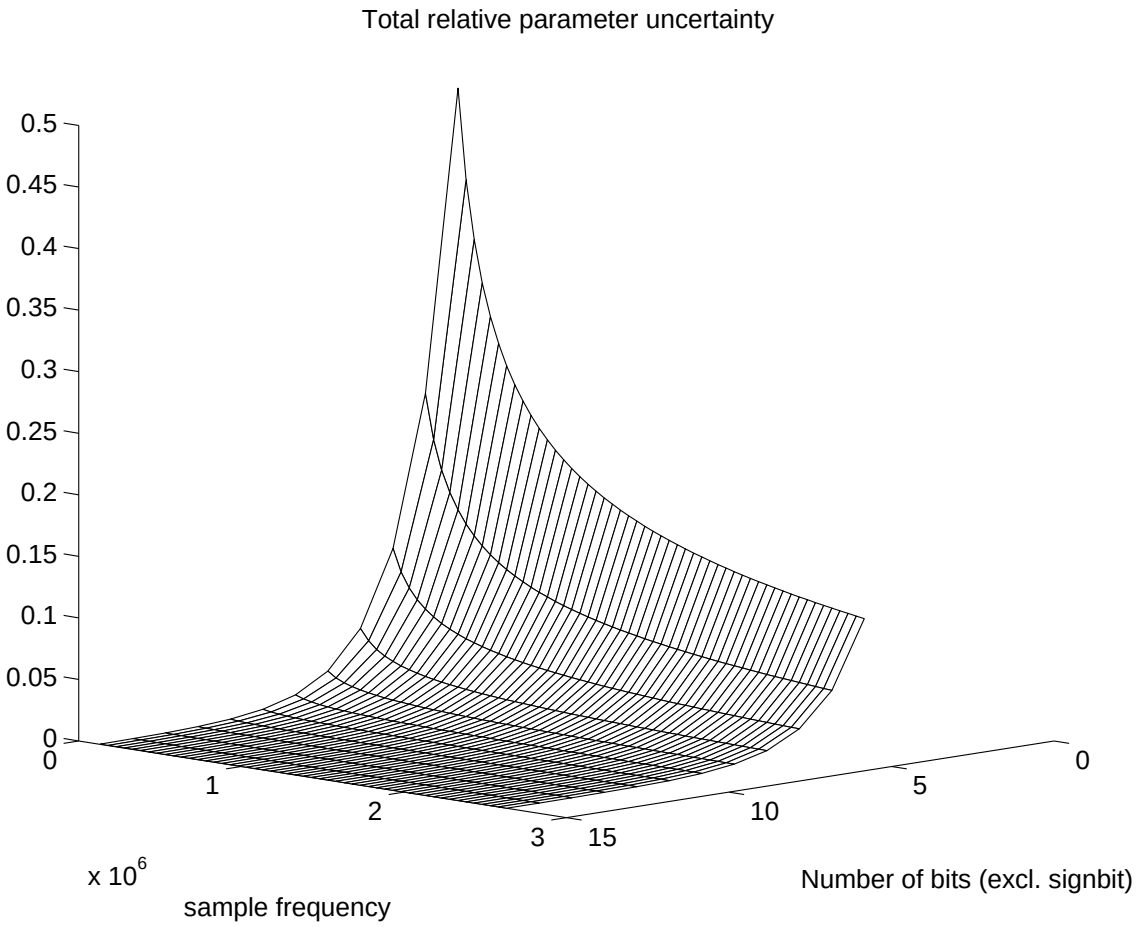

Figure 5.4: *Total relative parameter uncertainty. The plot is made using S_{imin} for C_c in scenario 2: Primary capacitor broken. This is the smallest value of Simin giving the largest parameter uncertainty.*

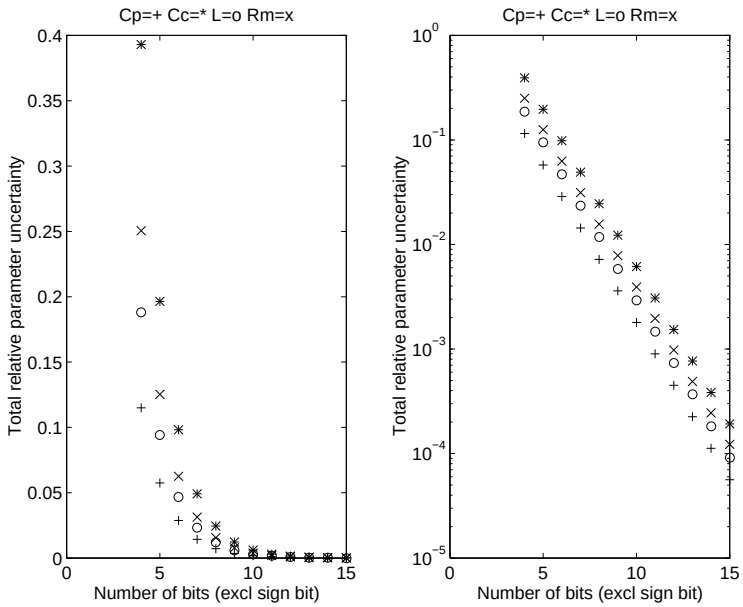

Figure 5.5: *Total relative parameter uncertainty, for scenario 2 (primary capacitor broken), at sampling frequency* $fs = 200kHz$.

5.3.2 Choice of threshold

In this section the thresholds used to declare the pulse generator without faults is calculated. This calculation is based on the availability of an 8 bit ADC. From Section 5.3.1 it is known that this ADC precision will give a small but not neglectable parameter uncertainty.

The choice of threshold is made by using the parameter variance which is the sum of the total parameter uncertainty and the component tolerance. The total parameter uncertainty are found from the total relative parameter uncertainty by

$$\tilde{\theta}_{itot} = \mathbf{L}_i \tilde{\theta}_{ritot}$$

Assuming a component tolerance of $\pm 2.5\%$ and deviation due to under modelling of $\pm 5\%$ of the nominal component values, gives the standard deviation of the parameters in Table 5.5 for scenarios 1 and 2.

Parameter\Scenario	**1**	**2**
C_p	$0.101\mu F$	$0.117\mu F$
C_c	$0.335mF$	$0.496mF$
L	$0.211\mu H$	$0.269\mu H$
R_m	$2.50m\Omega$	$2.10m\Omega$

Table 5.5: *Standard deviation of the parameter estimates assuming* $f_s = 200kHz$*, component tolerance* $\pm 2.5\%$*, under modelling deviation* $\pm 5\%$ *and an 8 bit ADC. Scenario 1 is a working system, scenario 2 is primary capacitor broken.*

Looking specifically to estimating C_p in scenario 2, which is the scenario having the smallest sensitivities, gives the parameter distribution shown on Figure 5.6

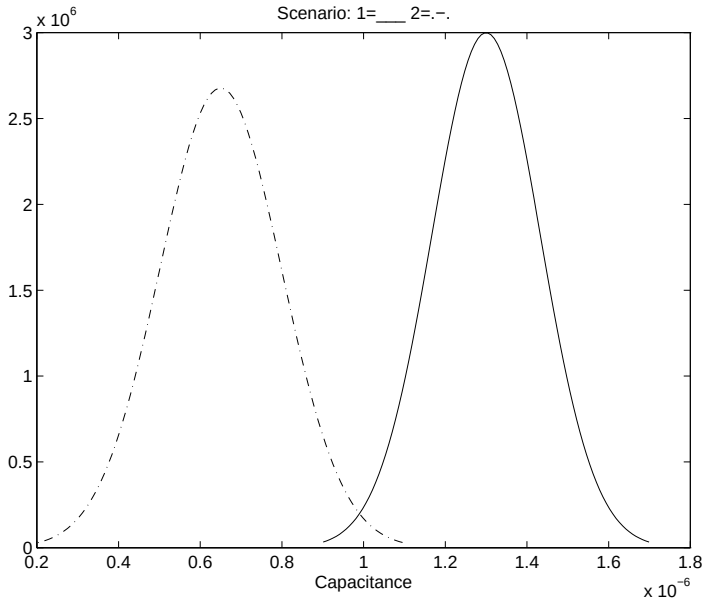

Figure 5.6: *Distribution of the estimation of C_p in scenario 1(working system) and 2(primary capacitor broken).*

Given these distributions a decision threshold, to decide if a fault has happened fulfilling the requirements to the probability of missing a failure $P_m < 10^{-5}$ and the probability of false alarm $P_f < 0.36\%$, can be found. Since there are four parameters used for the decision, the individual probability of false alarm must be $P_f < 0.089\%$

Selecting a threshold, th, the probability of missing a primary capacitor fault is

$$P_m = P(\text{Fault and } \tilde{C}_p > th)$$

where $\tilde{C}_p$ is the estimated value of C_p. This can be written as

$$P_m = P(\tilde{C}_p|\text{Fault} > th)P(\text{Fault}) \tag{5.9}$$

The probability of false alarm can in the same way be found as

$$P_f = P(\tilde{C}_p|\text{Working} < th)P(\text{Working}) \tag{5.10}$$

The probability $P(\tilde{C}_p|\text{Working})$ is found using the mean and variance of scenario 1 (working system). The largest parameter variance is from scenario 2 (Primary capacitor broken), so the variance from this scenario is used to find $P(\tilde{C}_p|\text{Fault})$.

The failure rate of one execution chain is assumed to be 10^{-4} per hour [BCD+97, chap. 5], which, with a run time of 10 hours, becomes 10^{-3} per run, thus

$$\begin{aligned} P(\text{Fault}) &= 10^{-3} \\ P(\text{Working}) &= 1 - P(\text{Fault}) \end{aligned}$$

The threshold is found by specifying the value of P_f in Equation 5.10. The value of th is found by using standard normal distribution tables. Since the failure behaviour of L and R_m is unknown i.e. the location of the mean is not known, the value of P_f must be calculated as a two sides value, using $\frac{P_f}{2}$ instead of P_f.

The threshold values in Table 5.6 indicate the interval in which the parameter value will be considered as originating from a working system.

Parameter	**Threshold**	P_m	P_f
C_p	$> 0.986\mu F$	$2.10 \cdot 10^{-6}$	0.089%
C_c	$> 2.69mF$	$2.62 \cdot 10^{-5}$	0.089%
L	$(2.73 \pm 0.703)\mu H$	—	0.089%
R_m	$(20 \pm 5.00)m\Omega$	—	0.089%

Table 5.6: *Threshold values and probability of missed detection and false alarm. The values are found using the tables of [Ros87].*

Table 5.6 shows that the requirement $P_m < 10^{-5}$ is not meet for all parameters. To meet this requirement a better parameter estimate is needed. This is obtainable by using an ADC with higher precision.

Another way of obtaining better parameter estimates is to improve the model used, so that parameter uncertainty due to under modelling is decreased. This improvement could be modelling the transfer between primary and compensation circuit (the dip).

The estimate could also be improved by measuring every component before installation thereby eliminating the uncertainty due to component tolerance. This measuring could be done by running the algorithm a number of times on a pulse generator know to be working and in this way obtain better reference values than the one given by the nominal component values.

5.4 Test of the power trigger

Analysis of the fault tree for the power trigger shown in Section 4.5, reveals that all failures except missing input and failure of the $2\mu s$ input mono-stable is propagated to the output.

Failure of the primary GTO switch, the primary capacitor and the diodes is detectable by measuring the maximum amplitude of the output pulse. The power generator must always deliver so much energy to the trigger transformer that the GTO switches of the pulse generator can be closed and remain closed for the $90\mu s$ duration of the dump. This

means that the power generator does not have to follow the beam energy and a fixed threshold test can be used. This test is performed internally in the power trigger, setting a status bit.

Failure of the compensation GTO, the $500\mu s$ mono-stable and the compensation capacitor is detectable by measuring the pulse length which is done internally setting a status bit.

Every input is separately evaluated and sets a status bit if used.

Failure of the $2\mu s$ input mono-stable is not detectable by the internal status generation available. To be able to detect this fault, verification of the output of the mono-stable is needed. This could be done by counter circuit like for the output pulse.

The tests needed in addition to the continues surveillance are summarised in Table 5.7.

Test number	**Purpose**	**Test action**	**Sensors**
PT1	Test of primary circuit	Test maximum output current amplitude	Current amplitude flip-flop
PT2	Test of compensation circuit	Test pulse length	Pulse length flip-flop
PT3	Test of input signal	Verify presence of trigger A and B and retrigger A and B	Input signal flip-flops

Table 5.7: *Additional tests needed to declare the power trigger ready for operation.*

These tests have to be performed on both power trigger modules A and B.

5.5 Test of the retrigger system

The retrigger system provides information on the origin of the retrigger and the connection to retrigger line by current status bits. This information is used to detect pick up faults.

Fault of the retrigger output is detected by test PT3 of the power trigger.

The tests needed in addition to the continues surveillance are summarised in Table 5.8.

Test number	**Purpose**	**Test action**	**Sensors**
RT1	Test of pick ups.	Verify current from every pick up	Retrigger status bits

Table 5.8: *Additional tests needed to declare the retrigger system ready for operation.*

These tests has to be performed on both retrigger A and B.

5.6 Summary

The Not Ready Test can be summarised as in Table 5.9.

Test number	**Purpose**	**Test action**	**Sensors**
PG1	Test of primary GTO's and trigger transformers	Test output current of primary GTO's	Retrigger status bits
PG2	Test of compensation GTO's and trigger transformers compensation coil	Test output current of compensation GTO's	Retrigger status bits
PG3	Test of capacitors, compensation diodes and magnet	Test of magnet current below threshold at $t \approx 70\mu s$, integration or parameter estimation	CT1m, CT2m
PT1	Test of primary circuit	Test maximum output current amplitude	Current amplitude flip-flop
PT2	Test of compensation circuit	Test pulse length	Pulse length flip-flop
PT3	Test of input signal	Verify presence of trigger A and B and retrigger A and B	Input signal flip-flops
RT1	Test of pick ups.	Verify current from every pick up	Retrigger status bits

Table 5.9: *The not ready test.*

Chapter 6

Ready Mode Surveillance

The Ready Mode Surveillance is the module with the responsibility of continuously verifying the functioning of the beam dump kicker system.

6.1 Model of the power supply system

This section describes the mathematical model of the charging of the primary capacitors of the pulse generator. The model is used for simulating the power supply charging system and as reference model for the fault detection method described in Section 6.2.

On Figure 6.1 a block diagram of the power supply system charging the primary capacitors is shown[1].

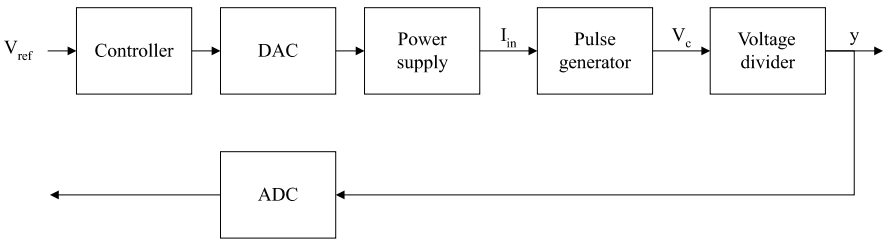

Figure 6.1: *Block diagram of the power supply system charging the primary capacitors.*

For the modelling the following assumptions are made in respect to the circuit diagram on Figure 4.1:

- The primary capacitors are charged via the magnet.
- The resistors over the series diodes are much smaller than the resistors over the GTO switches and are thus considered as short circuits.

[1]The controller is an open-loop controller to avoid decrease in reliability arising from having the ADC in the loop.

- The capacitance over the GTO switches are considered small compared to the primary capacitors i.e. having faster dynamics.
- The Power supply is considered to be a current source with much faster dynamics than the pulse generator.

Under these assumptions the circuit diagram of the primary charging circuit can be drawn as shown on Figure 6.2, where R_{71} is resistance in the power supply connection circuit and L_m is the inductance of the magnet.

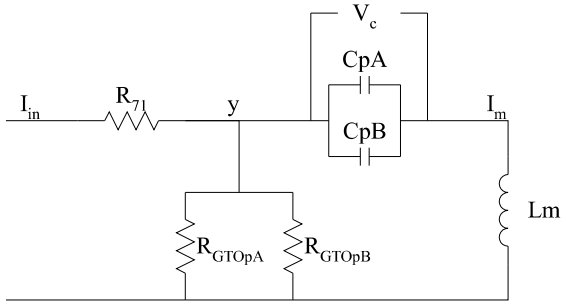

Figure 6.2: *Circuit diagram for the charging of the primary capacitor*

6.1.1 Model of the primary charging circuit

Choosing the state vector as

$$\mathbf{x}_{ps} = \begin{bmatrix} V_c \\ I_m \end{bmatrix}$$

where V_c is the voltage over the primary capacitor and I_m is the current through the magnet, gives the equations

$$\dot{V}_c(t) = \frac{1}{C_p} I_m(t) \tag{6.1}$$

$$\dot{I}_m(t) = \frac{1}{L_m}(R_G(I_{in}(t) - I_m(t)) - V_c(t)) \tag{6.2}$$

where $C_p = CpA \parallel CpB$ and $R_G = R_{GTOpA} \parallel R_{GTOpB}$.

The measured output, y, is the divided voltage over the resistor R_G. y is found from

$$y(t) = R_G(I_{in}(t) - I_m(t))K_{ps} \tag{6.3}$$

where K_{ps} is the ratio of the measuring voltage divider.

The state space model of the primary charging circuit is

$$\begin{aligned} \dot{\mathbf{x}}_{ps}(t) &= \mathbf{A}_{ps}\mathbf{x}_{ps}(t) + \mathbf{B}_{ps}I_{in}(t) \\ y(t) &= \mathbf{C}_{ps}\mathbf{x}_{ps}(t) + D_{ps}I_{in}(t) \end{aligned}$$

where the system matrices are given by Equation 6.1, 6.2 and 6.3 as

$$\begin{aligned} \mathbf{A}_{ps} &= \begin{bmatrix} 0 & \frac{1}{C_p} \\ -\frac{1}{L_m} & -\frac{R_G}{L_m} \end{bmatrix} \\ \mathbf{B}_{ps} &= \begin{bmatrix} 0 \\ \frac{R_G}{L_m} \end{bmatrix} \\ \mathbf{C}_{ps} &= \begin{bmatrix} 0 & -R_G K_{ps} \end{bmatrix} \\ D_{ps} &= R_G K_{ps} \end{aligned}$$

Using the values of Table 6.1, the locations of the poles and zeros of the second order system are found to be: Poles at $-7.75 \cdot 10^{13}$ and 0, Zeros at $3.60 \cdot 10^{-3} \pm 6.20 \cdot 10^{5} j$.

Parameter	**Value**
C_p	$1.3\mu F$
R_G	$155M\Omega$
L_m	$2\mu H$
K_{ps}	$\frac{1}{5000}$

Table 6.1: *Parameter values used to simulate the primary charging circuit.*

The spread of the poles and zeros indicates that a simpler model can be used to describe the dominant low frequency dynamics. The dominant low frequency dynamics are mainly due to the primary capacitors, therefore the dynamics of the magnet are neglected. The circuit diagram resulting of this simplification is shown on Figure 6.3.

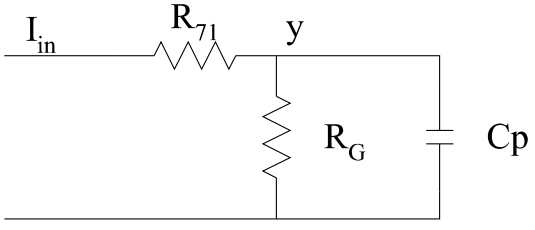

Figure 6.3: *The resulting circuit diagram of the primary charging circuit after simplification to a first order system.*

The voltage V_c for the simplified circuit is

$$V_c(s) = \left(R_G \parallel \frac{1}{sC_p} \right) I_{in}(s)$$

which can be written as

$$\begin{aligned} \dot{V}_c(t) &= -\frac{1}{R_G C_p} V_c(t) + \frac{1}{C_p} I_{in}(t) && (6.4) \\ y(t) &= K_{ps} V_c(t) && (6.5) \end{aligned}$$

Equation 6.4 of the simplified system can also be found by letting $L_m \to 0$ in Equation 6.2.

The simplified system matrices becomes

$$\begin{aligned} \mathbf{A}_{ps} &= -\frac{1}{R_G C_P} \\ \mathbf{B}_{ps} &= \frac{1}{C_p} \\ \mathbf{C}_{ps} &= K_{ps} \\ D_{ps} &= 0 \end{aligned}$$

6.1.2 Model of the power supply

The power supply is a assumed to be a current source with a current limit.

Furthermore the power supply has an internal feedback of the power supply output voltage. Assuming that R_{71} is much smaller than R_G the power supply output voltage is equal to V_c and the internal feedback can be simulated using V_c.

Taking the above into consideration the power supply can be modelled by Equation 6.6.

$$I_{in}(t) = sat_{-\frac{V_c(t)}{R_G}}^{I_{max}-\frac{V_c(t)}{R_G}} \left(\frac{V_{ps}(t) - V_c(t)}{R_{ps} + R_{71}} + \frac{V_c(t)}{R_G} \right) \quad (6.6)$$

where $sat_{low}^{high}(\cdot)$ describes the function of saturating the variable to be within the interval given by low and $high$.

The addition of $\frac{V_c(t)}{R_G}$ is done to eliminate steady state error on V_c due to current through R_G.

V_{ps} is found from the output of the DAC, V_D, as

$$V_{ps} = K_{ps,in} V_D$$

The value of $K_{ps,in}$ is assumed to be 5000.

The value of R_{ps} is used to adjust the tracking properties of the simulated power supply to match those of the real power supply. In the simulation the following value is used

$$R_{ps} + R_{71} = 1M\Omega$$

6.1.3 Model of the ADC and DAC

The ADC and DAC are modelled in the same way although they serve two different purposes. The model used for the ADC/DAC is shown on Figure 6.4

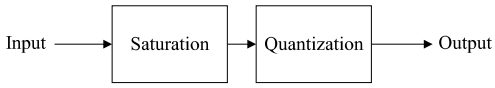

Figure 6.4: *Model of the ADC and DAC.*

The input is saturated to the maximum voltage/number of the ADC/DAC and then quantised.

6.1.4 System bandwidth

Knowledge of the system bandwidth is needed to be able to determine the sampling frequency to be used by the power supply system surveillance.

Combining the model of the primary charging circuit and the power supply model into the linear model described by

$$\begin{aligned}
\mathbf{A}_{cl} &= \mathbf{A}_{ps} + \mathbf{B}_{ps} \frac{R_{ps} + R_{71} - R_G}{R_G(R_{ps} + R_{71})} = -\frac{1}{R_G C_p} + \frac{R_{ps} + R_{71} - R_G}{C_p R_G (R_{ps} + R_{71})} \\
\mathbf{B}_{cl} &= \mathbf{B}_{ps} \frac{K_{ps,in}}{R_{ps} + R_{71}} = \frac{K_{ps,in}}{C_p(R_{ps} + R_{71})} \\
\mathbf{C}_{cl} &= \mathbf{C}_{ps} + D_{ps} \frac{R_{ps} + R_{71} - R_G}{R_G(R_{ps} + R_{71})} = K_{ps} \\
D_{cl} &= D_{ps} \frac{K_{ps,in}}{R_{ps} + R_{71}} = 0
\end{aligned}$$

gives the system bandwidth

$$f_{bw} = 0.769Hz$$

The minimum sample frequency is thus $1.54Hz$.

6.1.5 Modelling of faults

This section describes the modelling of the effects of the faults found by the fault analysis described in Chapter 4. These faults are arranged in two fault vectors; $\mathbf{f}_{\text{controller}}$ for the controller and $\mathbf{f}_{\text{pcharge}}$ for the primary charging circuit. The fault vectors are:

$$\mathbf{f}_{\text{Controller}} = \begin{bmatrix} \text{DAC not reset} \\ \text{DAC broken} \\ \text{ADC not reset} \\ \text{ADC broken} \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \end{matrix}$$

and

$$\mathbf{f}_{\text{pcharge}} = \begin{bmatrix} \text{Voltage divider: Output short circuit to input} \\ \text{Voltage divider: Output connection broken} \\ \text{Voltage divider: Output short circuit to ground} \\ R_{GTOpA}\text{: Short circuit} \\ R_{GTOpA}\text{: Open circuit} \\ C_{pA}\text{: Input connection broken} \\ C_{pA}\text{: Short circuit} \\ R_{GTOpB}\text{: Short circuit} \\ R_{GTOpB}\text{: Open circuit} \\ C_{pB}\text{: Input connection broken} \\ C_{pB}\text{: Short circuit} \\ \text{Manual safety switch closed} \\ \text{Electrical safety switch closed} \\ \text{Power supply failure} \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \\ 11 \\ 12 \\ 13 \\ 14 \end{matrix}$$

To have both poles of the capacitors short circuited to ground, the manual safety switch consists of two separate switches, but since the effect of closing a switch is the same for both switches, they are considered as the same fault.

The faults in $\mathbf{f}_{\text{pcharge}}$ behave in a binary manner so the values in the fault vector can be described by a unit step function.

The DAC broken and ADC broken faults are modelled by setting the output to a random value within the amplitude range .

The ADC not reset and DAC not reset faults results in an unchanged output, which is modelled by setting the output to its last value.

The fault effects of $\mathbf{f}_{\text{pcharge}}$ are modelled with the assumptions:

- R_{GTO} short circuit is similar to one resistor in the stack short circuiting thus a resistance decrease by 10%.
- R_{GTO} open circuit will increase the voltage over the GTO switch leading to short circuit of the switch. Therefore R_{GTO} open circuit has the same effect as R_{GTO} short circuit.
- If one capacitor is short circuited the other is short circuited immediately afterwards.
- Closing the manual safety switch is simulated by connecting the capacitors to ground by a $1m\Omega$ resistor.
- Short circuiting the capacitors corresponds to a very fast discharge simulated in the same way as closing the manual safety switch.
- The resistance of R_{61p} (The resistor used for discharging the capacitors when the electrical safety switch is closed) is much smaller than R_G.

Including the faults the primary charging model is

$$\begin{aligned} \dot{\mathbf{x}}_{ps}(t) &= (\mathbf{A}_{ps} + \Delta\mathbf{A}_{ps}(t))\mathbf{x}_{ps}(t) + (\mathbf{B}_{ps} + \Delta\mathbf{B}_{ps}(t))I_{in}(t) \\ y(t) &= (\mathbf{C}_{ps} + \Delta\mathbf{C}_{ps}(t))\mathbf{x}_{ps}(t) + (D_{ps} + \Delta D_{ps}(t))I_{in}(t) \end{aligned}$$

Looking at the relative fault effect the elements of $\Delta\mathbf{A}_{ps}(t)$ can be described as

$$\Delta A_{ps,ij} = A_{ps,ij}\mathbf{F}_{A,ij}\mathbf{f}_{\text{pcharge}}(t)$$

where $\mathbf{F}_{A,ij}$ is the fault entry matrix for element ij. The elements of $\Delta\mathbf{B}_{ps}$, $\Delta\mathbf{C}_{ps}$ and ΔD_{ps} are described in the same way.

The fault entry matrices are found by solving Equation 6.7 for the kth failure of $\mathbf{f}_{\text{pcharge}}$.

$$A_{ps,ij}(1 + \mathbf{F}_{A,ij,k}\mathbf{f}_{\text{pcharge},k}(t)) = A_{fail,ij,k} \tag{6.7}$$

Solving Equation 6.7 gives the elements of the fault entry matrices as in Table 6.2, see Appendix B

Index	$\mathbf{F}_{A,1}$	$\mathbf{F}_{B,1}$	$\mathbf{F}_{C,1}$
1	0	0	$\frac{1-K_{ps}}{K_{ps}}$
2;3	0	0	-1
4;5;8;9	$\frac{1.9}{1.8}-1$	0	0
6;10	1	1	0
7;11;12	$\frac{R_G}{1m\Omega}-1$	0	0
13	$\frac{R_G}{R_{61p}}-1$	0	0
14	0	-1	0

Table 6.2: *Elements in the fault entry matrices.*

6.2 Surveillance of the power supply system

In this section the continues surveillance of the power supply system charging the primary capacitors of the pulse generator is described.

The power supply system charging the compensation capacitors is not described since the surveillance of the charging of the compensation capacitors is similar to the surveillance of the charging of the primary capacitors.

The compensation charging circuit can be described by the circuit diagram on Figure 6.3 with $R_G = \infty$. From this it can be seen that the compensation charging model can be found from the primary charging model, by letting $R_G \rightarrow \infty$ and using the capacitor values from the compensation circuit.

There is however a difference in the fault model since the R_{GTO} faults are not existing for the compensation circuit.

The structure of the power supply system surveillance is shown on Figure 6.5

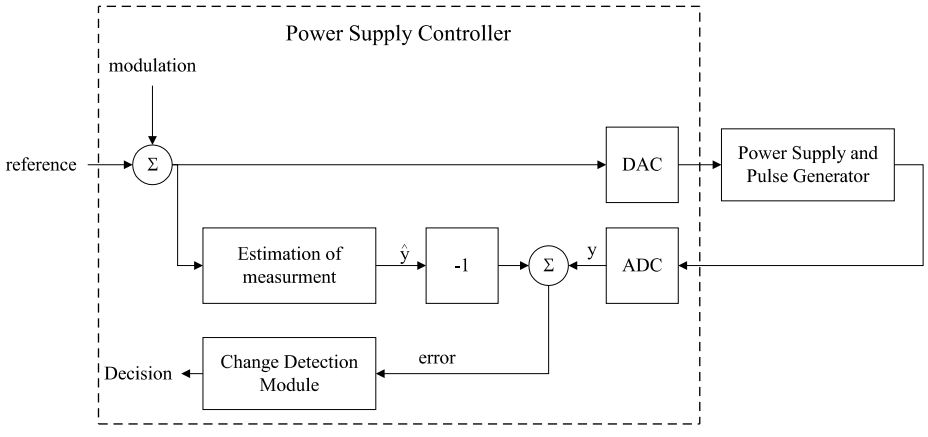

Figure 6.5: *Structure of the surveillance of the power supply system.*

The reference signal is the voltage corresponding to the actual beam energy. This signal is modulated so that it is possible, at a constant beam energy, to detect faults in the dynamics of the power supply system, e.g. capacitor faults. The modulation furthermore

makes it possible to detect faults of the ADC and DAC since the value of the ADC and DAC will never be the same between two samples.

The estimation of the measurement is done using the model described in Section 6.1.

The sample frequency of the power supply system surveillance is chosen to be $2Hz$, which is above the minimum sample frequency of $1.54Hz$.

With this assumption the error $e = y - \hat{y}$ can be found as, see Appendix C

$$e(s) = y(s) - \hat{y}(s) = H_e(s)f(s) + \eta$$

where η is the quantisation noise, f is a given fault and H_e is the fault to error transfer function at a given time. This transfer function is time-varying because it is not possible to define an operating point before the beam has reached maximum energy, which will happen 25 minutes after the start of acceleration[CLR99, Fig. 7].

Using an operating described by V_{C0} and V_{D0} the transfer function H_e is for the ith fault, see Appendix C

$$\begin{aligned} H_{e,i}(s) &= \frac{Kps\left(-\frac{V_{C0}}{R_G C_p}F_{A,1,i} + \frac{1}{(R_{ps}+R_{71})R_G C_p}((R_{ps}+R_{71}-R_G)V_{C0} + R_G K_{ps,in} V_{D0})F_{B,1,i}\right)}{s + \frac{1}{(R_{ps}+R_{71})C_P}} + \\ & K_{ps}V_{C0}F_{C,1,i} \end{aligned} \tag{6.8}$$

Using an operating point corresponding to maximum energy gives the transfer functions in Table 6.3 for the faults in $\mathbf{f}_{\text{pcharge}}$.

Index	$H_e(s)$	**Time constant**
1	$31 \cdot 10^3$	—
2;3	-6.20	—
4;5;8;9	$\frac{-1{,}71 \cdot 10^{-3}}{s+0.769}$	$1.3s$
6;10	0	—
7;11;12	$\frac{-2.38 \cdot 10^3}{s+0.769}$	$1.3s$
14	$\frac{-0.465}{s+0.769}$	$1.3s$
16	$\frac{-6.20}{202s+1}$	$202s$

Table 6.3: *Error transfer functions for the faults in* $\mathbf{f}_{pcharge}$ *at the operating point* $V_{C0} = 31kV$ *and* $V_{D0} = 6.2V$.

Equation 6.8 can not be used to calculate $H_{e,16}$ for the power supply fault, since this faults breaks the closed loop of the internal power supply feedback. The error signal for the power supply fault is described by the natural discharge of the primary capacitors so

$$H_{e,16} = -\frac{K_{ps} * V_{C0}}{R_G C_p s + 1}$$

Since the faults of $\mathbf{f}_{\text{pcharge}}$ can be described as step functions, it is seen from the error transfer functions in Table 6.3, having non-zero DC gain, that all except the capacitor input broken faults, index 6 and 10, will give a change of mean value of the error signal.

The capacitor input broken faults halves the capacitance of the charging circuit. This means that the damping of input noise in the charging circuit is reduced leading to an increase of error signal variance.

From Table 6.3 it is seen that the faults of $\mathbf{f}_{\text{pcharge}}$ giving the smallest mean value change is the R_{GTO} faults, index 4,5,8 and 9.

From Equation 6.8 it can be seen that the DC gain and thus the error signal increases in amplitude with increasing operating point i.e. capacitor voltage.

The ADC not reset fault changes the measured value to a constant giving the error signal

$$e(s) = k - H_y(s) I_{in}(s)$$

The DAC not reset fault changes the power supply input to a constant giving the error signal

$$e(s) = H_y(s)(k - I_{in}(s)) + \eta_A$$

η_A is the quantisation noise from the ADC.

The ADC broken fault changes the mean of the measurement to zero and increases the variance to $\frac{(2A_A)^2}{12}$, where A_A is the amplitude range of the ADC. The error signal is thus

$$e(s) = \eta_f - H_y(s) I_{in}(s) \quad , \eta_f \sim \text{UID}(0, \frac{(2A_A)^2}{12})$$

The DAC broken fault changes the mean of the input to the power supply to zero and variance to $\frac{(2A_D)^2}{12}$, where A_D is the amplitude range of the DAC. However due to the lower limit of I_{in} negative voltage reference will have no effect. The error signal is then

$$e(s) = H_y(s)(\eta_f - I_{in}(s)) \quad , \eta_f \sim \text{UID}(\frac{A_D}{2}, \frac{A_D^2}{12})$$

From the above it is concluded that the ADC not reset and DAC not reset faults has the smallest effect of the faults in $\mathbf{f}_{\text{controller}}$.

6.2.1 Residual Generation

The error signal is filtered through a bank of two filters turning it into two residuals[2] having the properties of being sensitive to either the mean value or the variance of the error signal.

Since the mean value of the error signal changes in steps, the residual r_m sensitive to mean changes must be sensitive to DC changes. To detect the power supply fault within $2s$, r_m must be sensitive to error signals with a time constant of $202s$. The remaining faults, giving mean change, have a time constant below $2s$ which means that they will reach the DC level faster than the power supply fault. r_m is found by low pass filtering the error signal with a filter cut off frequency of $6mHz$.

The residual r_v sensitive to variance is found by high pass filtering the error signal removing the mean of the signal. To be non-sensitive to the faults giving mean change, the cut off frequency must be so high that r_v is not sensitive to signals with a time constant of $1.3s$. The cut off frequency for the high pass filter is $0.8Hz$.

The amplitude response of the used filters are shown on Figure 6.6

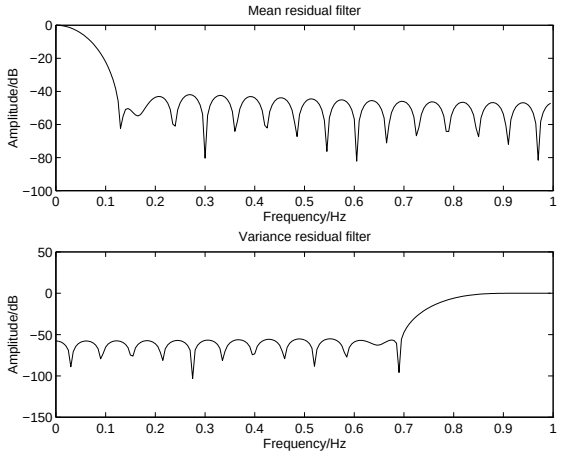

Figure 6.6: *Amplitude response of the residual generation filters. The filters used are 32th order FIR filters.*

6.2.2 Fault detection

To meet the the time to detect $< 2s$ requirement it is chosen to test for faults every $2s$. With an envisaged run time of 10 hours the probability of missed detection, P_m, and probability of false alarm, P_f, requirements becomes, per test

$$\begin{aligned} P_{f,test} &= 2.0 \cdot 10^{-7} \\ P_{m,test} &= 5.6 \cdot 10^{-10} \end{aligned}$$

[2]Residuals are signals, that carry information of the systems operational conditions[Bla97]

Using the same values as in Section 5.3.2 for the working system probability per run and failed system probability per run, gives the probabilities per test

$$\begin{aligned} P(\text{Fault}) &= 5.6 \cdot 10^{-8} \\ P(\text{Working}) &= 1 - P(\text{Fault}) \end{aligned}$$

Detection of mean change

The detection of mean change is performed by testing the hypothesis

$$\begin{aligned} H_0 &: \mu_{rm} = 0 \\ H_1 &: \mu_{rm} \neq 0 \end{aligned}$$

When H_0 is accepted the system is decided to be fault free and when H_1 is accepted then it is decided that the system has a fault.

To detect changes of mean the WSSR method is used. The WSSR approach uses the sum of the squared residual for a number of samples, the observation window, to test the hypothesis H_0 against H_1[Bla97]. When the residual is normally distributed the sum of the squared samples will follow a χ^2 distribution.

The WSSR test is performed by making the sum M

$$M = \sum_{i=k-1-N}^{k} \frac{1}{\sigma_{rm}^2} r_m(i)^2$$

where k is the current sample, N is the observation window size and σ_{rm}^2 the variance of the residual. M is only calculated for each N samples i.e. the observation windows do not overlap.

With a threshold value th the following rules are applied:

$$\begin{aligned} &\text{Accept } H_0 \text{ if } M \leq th \\ &\text{Reject } H_0 \text{ if } M > th \end{aligned}$$

The use of σ_{rm}^2 to normalise the sum makes it possible to use standard χ^2 tables to determine the value of th. Using the same approach as in Section 5.3.2 to calculate P_m and P_f yields the following requirements to M

$$P(M|\text{Fault} < th) < 1 \cdot 10^{-2} \quad (6.9)$$

$$P(M|\text{Working} > th) < 2 \cdot 10^{-7} \quad (6.10)$$

Detection of variance change

The detection of variance change is done by testing the hypothesis

$$\begin{aligned} H_0 &: \sigma_{rv}^2 = \sigma_0^2 \\ H_1 &: \sigma_{rv}^2 \neq \sigma_0^2 \end{aligned}$$

σ_0^2 is the variance for the residual when there is not faults existing.

Assuming that the residual is ergodic, the sample variance S^2 for the observation window with length N is

$$S^2 = \sum_{i=k-1-N}^{k} \frac{(r_v(i) - \bar{r}_v)^2}{N-1}$$

where $\bar{r}_v$ is the estimated mean value of the residual. The mean value of r_v is zero, because of the residual generation high pass filter.

Since $V = \frac{(N-1)S^2}{\sigma_0^2}$ follows a χ^2 distribution [Ros87], the following rules are applied

Accept H_0 if $th_{low} < V < th_{high}$
Reject H_0 otherwise

The threshold values th_{low} and th_{high} are found using standard χ^2 tables.

The calculation of V can be simplified to

$$V = \sum_{i=k-1-N}^{k} \frac{1}{\sigma_0^2} r_v(i)^2$$

which makes the calculation of V equal to the calculation of M, which as for M is only calculated for each N samples.

The following requirements to V can be found

$$P(th_{low} < V | \text{Fault} < th_{high}) < 1 \cdot 10^{-2} \quad (6.11)$$

$$P(\text{V}|\text{Working} < th_{low} \text{ or } V|\text{Working} > th_{high}) < 2 \cdot 10^{-7} \quad (6.12)$$

6.2.3 Determination of the modulation signal

A deviation of 2% is allowed between the tracking reference and the capacitor voltage. This deviation determines the maximum modulation amplitude.

The modulation signal must be so that the following is fulfilled:

- The error signal is time invariant i.e. independent of the reference signal for the fault free case.
- Sufficient signal separation between the non-failed and failed residuals to meet the requirements given by Equation 6.9, 6.10, 6.11 and 6.12.
- No possibility of correlation between the modulation of the 14 execution chains, to avoid the modulation having effect on the beam deflection.

To be able to make the non-failed error signal time invariant the modulation must be such that the error made by quantisation does not significantly depend on the reference signal. This excludes the use of signals who, when quantised in time fall into a limited number of discrete values[3].

A signal fitting the above is a uniform white noise signal generated by different seeds for each execution chain.

Modulation amplitude

The minimum modulation amplitude is the amplitude that makes the quantisation noise, and thus the error signal, independent of the reference.

With a white noise modulation the minimum amplitude, A_m of the modulation is

$$A_m > \frac{q_D}{2}$$

where q_D is the DAC quantisation step.

Under the assumption that the modulation signal and the DAC noise are white and independent the autocorrelation function, R_w, of the input noise can be calculated as

$$R_w = \sigma_m^2 + \sigma_D^2$$

where σ_m is the standard deviation of the modulation signal and σ_D is the standard deviation of the DAC noise.

[3]This excludes such signals as square wave and PRBS.

With uniform distributed white noise R_w is

$$R_w = \frac{(2A_m)^2}{12} + \frac{q_D^2}{12} > \frac{q_D^2}{12} + \frac{q_D^2}{12}$$

The effect of the input noise on the measured value before it is quantised by the ADC can be found by solving the matrix equations [FPW90]

$$\mathbf{R}_x = \Phi \mathbf{R}_x \Phi^T + \Gamma R_w \Gamma^T \tag{6.13}$$

and

$$R_y = \mathbf{C}\mathbf{R}_x\mathbf{C}^T + DR_wD^T \tag{6.14}$$

where Φ, Γ, $\mathbf{C}$ and $\mathbf{D}$ is the discrete time equivalents of the system matrices for the combined power supply and charging circuit models described in Section 6.1.4.

The maximum value of R_y is found by the 2% maximum deviation as

$$\sqrt{R_y} < 0.02 \cdot \text{Injection voltage}$$

Assuming that the capacitor voltage rises linearly with the beam energy, the injection voltage is

$$\text{Injection voltage} = \frac{\text{Maximum voltage}}{15.6} = \frac{31kV}{15.6} \approx 2kV$$

To make the noise from the ADC independent of the reference, the following requirement to the precision of the ADC can be made, under the assumption that the effect of the DAC noise and modulation on the measurement is white

$$\sqrt{R_y} > \frac{q_A}{2}$$

where q_A is the ADC quantisation step. The minimum number of bits, d_A, in the ADC, not counting the sign bit, is then

$$d_A > -\frac{\ln\left(\frac{2\sqrt{R_y}}{A_A}\right)}{\ln(2)}$$

where A_A is the amplitude range of the ADC.

The following calculation is made under the assumption that the ADC amplitude range is $A_A = \pm 10V$ and the DAC amplitude range is $A_D = \pm 10V$.

Calculating different values for R_w, corresponding to different DAC precisions, and solving Equation 6.13[4] and 6.14 gives the minimum modulation amplitudes and ADC precisions shown on Figure 6.7.

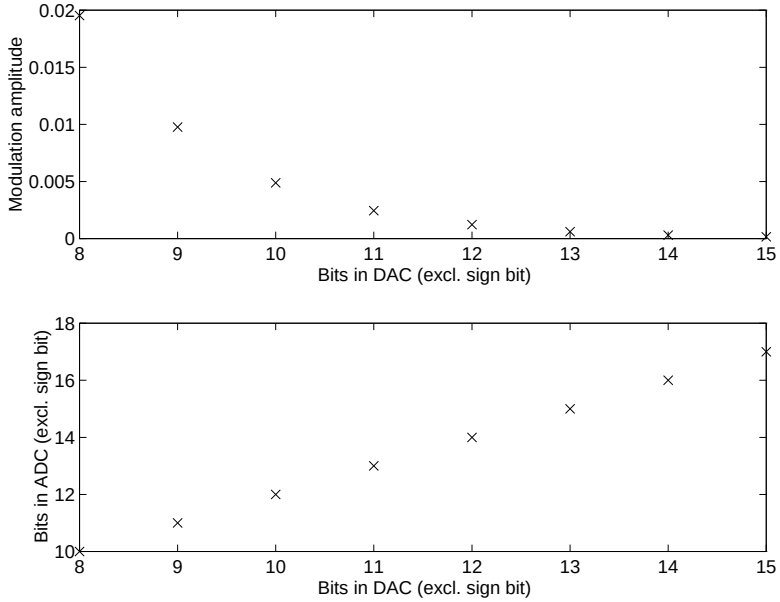

Figure 6.7: *Precisions of the DAC with corresponding minimum modulation amplitudes and ADC precisions, giving a capacitor voltage deviation below 2% of injection voltage.*

A modulation amplitude above the 2 % deviation limit (0.008) is not a good choice due to the non-linearity of the system given by faster charging than discharging of the capacitors. Following Figure 6.7 a DAC with 10 bits and a sign bit is chosen. This means an ADC with 12 bits and a sign bit and a modulation amplitude of 0.005 (1.3% of injection voltage).

On Figure 6.8 it can be seen that the there is no significant change in the mean value or variance of the residuals during the ramp and when the ramp is finished. From this it is concluded that the error signal can be assumed time invariant.

When the residuals are ergodic, the value of σ^2 used to normalise the WSSR sums can be found as the sample variance of the residuals obtained with no faults present.

Using the tables of [Ros87] it can be seen that the upper thresholds, th and th_{high}, must be $\gg 14.9$ and the lower threshold $th_{low} \ll 0.007$ to meet the requirement for false alarm, given by Equation 6.10 and 6.12, for an observation window length of 4 samples.

It can be seen on Figure 6.8 that the requirement to missed detection, given by Equation 6.9 and 6.11, can not be met by the minimum setup of ADC, DAC and modulation amplitude.

[4]Equation 6.13 is solved using the MATLAB command dlyap.

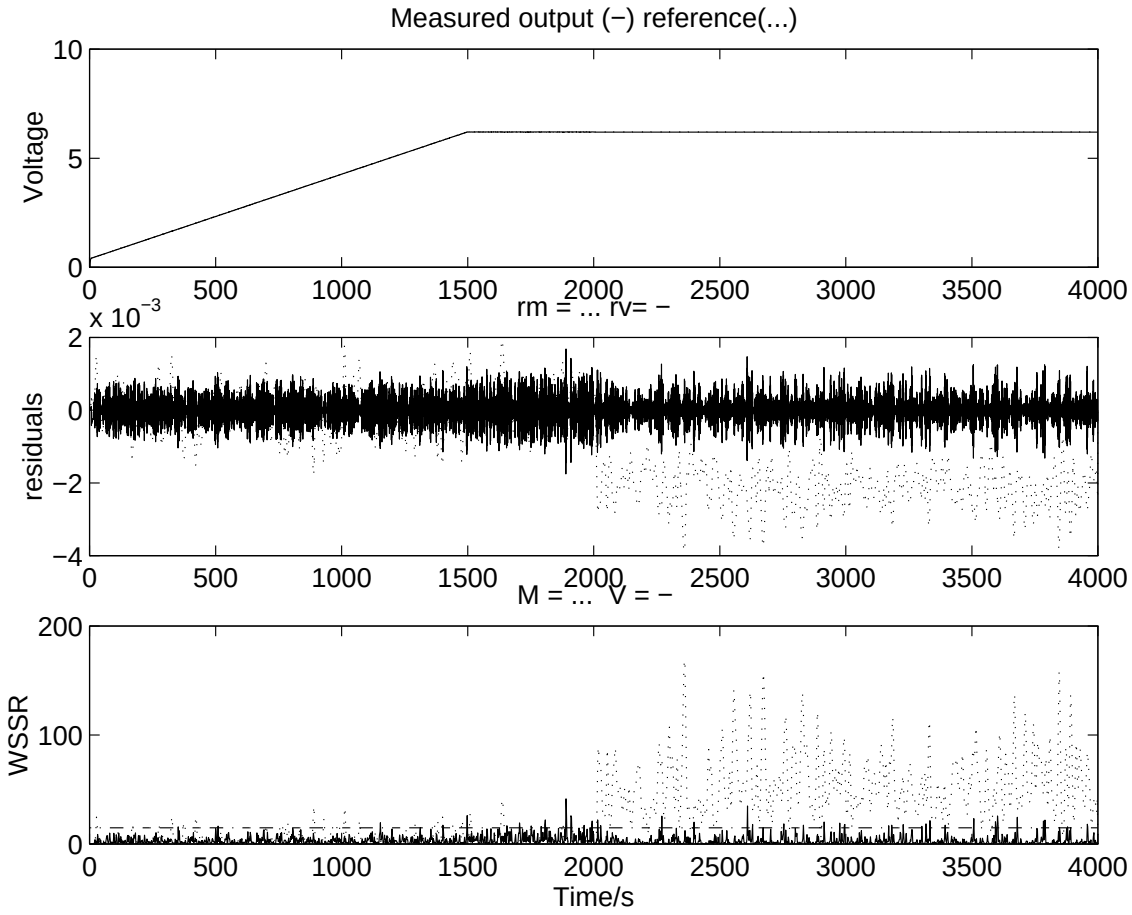

Figure 6.8: *Simulation showing the ready mode fault detection signals. The simulation uses a modulation signal with amplitude 1.3% of injection voltage, 12 bit ADC precision and 10 bit DAC precision. A R_{GTO} fault occurs at* 2000*s, showing to little signal separation.*

Further simulation with the maximum capacitor voltage, shows that the requirements to P_m and P_f can be meet with a DAC precision with 13 bits and a sign bit. The corresponding ADC precision is 15 bits and a sign bit. The modulation amplitude is 0.3% of injection voltage.

Figure 6.9 shows that it is possible, for the capacitor input connection broken fault, detected by variance change, to meet the P_m and P_f requirements.

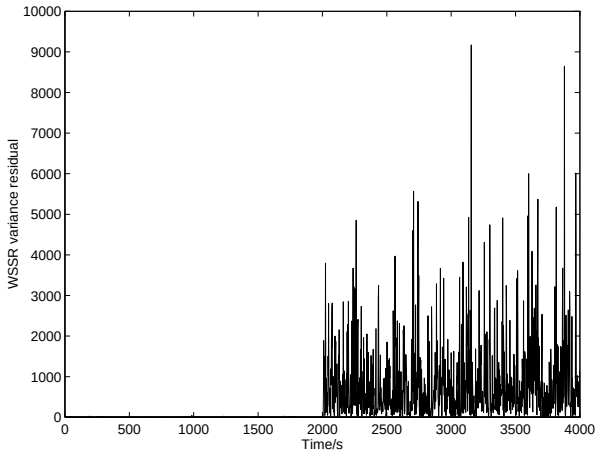

Figure 6.9: *WSSR sums at maximum voltage with 13 bits DAC precision, 15 bits ADC precision and modulation amplitude 2% of injection voltage. A capacitor input connection broken fault occurs at 2000s, showing signal separation.*

From the WSSR sums on Figure 6.10 it can be seen that the P_m requirement can not be met at injection voltage for the faults of $\mathbf{f}_{\text{pcharge}}$.

From this it is concluded that dry runs have to be performed at maximum voltage and that post mortem data, from the ready mode surveillance, from low energy beam dumps must be considered invalid.

Verification with the faults of $\mathbf{f}_{\text{controller}}$ shows that the requirements can be met for the faults of the controller, see Figure 6.11

6.2.4 Simulation Results

This section gives the time to detect faults with the modulation amplitude, DAC size and ADC size found in Section 6.2.3.

The following thresholds are used:

$$\begin{aligned} th &= 70 \\ th_{high} &= 70 \\ th_{low} &= 0.001 \end{aligned}$$

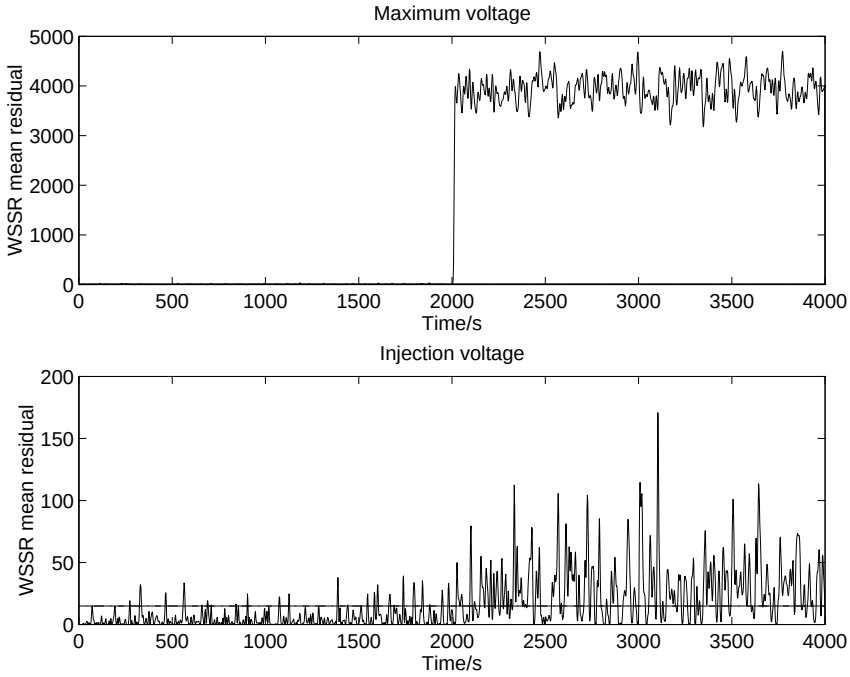

Figure 6.10: *WSSR sums with 13 bits DAC precision, 15 bits ADC precision bits and modulation amplitude 2% of injection voltage. A R_{GTO} fault occur at 2000s, showing insufficient signal separation at injection energy.*

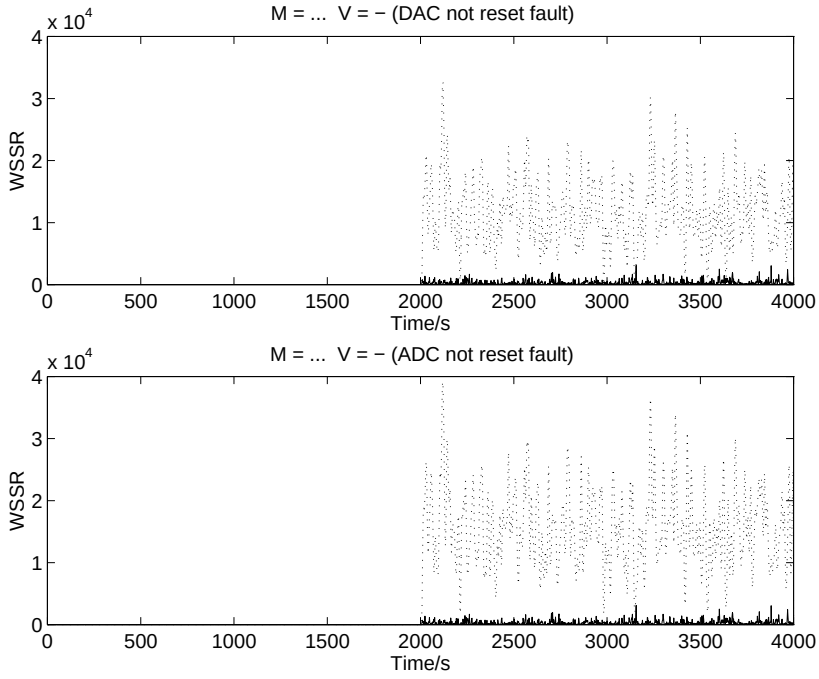

Figure 6.11: *WSSR sums with 13 bits DAC precision, 15 bits ADC precision and modulation amplitude 2% of injection voltage. Faults occur at 2000s verifying the signal separation.*

The fault detection times are given for the three different cases:

1. Fault present before start-up
2. Fault occurs during ramping. Fault occurrence moment = $500s$
3. Fault occurs at maximum energy. Fault occurrence moment = $2000s$

The fault detection times are given in Table 6.4:

Fault	**Case 1**	**Case 2**	**Case 3**
DAC not reset	18.0s	6.4s	6.0s
DAC broken	18.0s	2.2s	2.0s
ADC not reset	18.0s	4.0s	7.0s
ADC broken	18.0s	2.0s	2.0s
Voltage divider: Output short circuit to input	18.0s	2.0s	2.0s
Voltage divider: Output connection broken	18.0s	2.0s	2.0s
Voltage divider: Output short circuit to ground	18.0s	2.0s	2.0s
R_{GTOpA}: Short circuit	79.6s	9.4s	6.8s
R_{GTOpA}: Open circuit	70.8s	9.8s	7.0s
C_{pA}: Input connection broken	18.0s	5.8s	9.2s
C_{pA}: Short circuit	18.0s	2.0s	2.0s
R_{GTOpB}: Short circuit	77.4s	9.4s	6.8s
R_{GTOpB}: Open circuit	90.8s	6.2s	7.0s
C_{pB}: Input connection broken	18.0s	6.2s	9.2s
C_{pB}: Short circuit	18.0s	2.0s	2.0s
Manual safety switch closed	18.0s	2.0s	2.0s
Electrical safety switch closed	18.0s	2.0s	2.0s
Power supply failure	18.0s	3.6s	2.0s

Table 6.4: *Mean fault detection times for 10 simulations.*

Detection times larger than $16s$ in case 1 is due to the fact the fault detectors are not started until after $16s$ to allow the residual generation filters to initialise.

Table 6.4 shows that the time to detect requirement can not be meet. To meet the requirements better precision of the DAC and ADC is needed in order to detect smaller changes.

6.3 Surveillance of the power trigger and retrigger

The only effect detectable in the ready mode for the power trigger is the capacitors not being charged.

The power trigger operates at a constant voltage independent of the beam energy. Furthermore there are no interconnections between the two redundant power triggers so the

test of the power trigger can be done by verifying the capacitor voltage. This is done by verifying the four status bits for the voltages: $15V$, $48V$, $150V$ and $2.7kV$.

The only possible fault to detect in the ready mode for the retrigger is retrigger cable break. The status of the retrigger cable is given as a status bit on the stand-by signal.

6.4 Summary

The ready mode surveillance is summarised by subsystem in Table 6.5

Subsystem	**Surveillance**	**Purpose**	**sensors**
Pulse generator	Analytic redundancy on power supply system	Verify charging of capacitors	Voltage dividers DV1pA and DV1cA or DV1pB and DV1cB
Power trigger	Status of power supply connected	Verify voltage on capacitors and input logic.	Power trigger status bits
Retrigger	Verification of stand-by signal	check for cable break	Retrigger cable status bit

Table 6.5: *The ready mode surveillance by subsystem.*

Chapter 7

Conclusion

In this report a proposal for the fault detection part of the beam dump kicker system surveillance system is made.

The proposal consists of two major parts: The Not Ready Test and the Ready Mode Surveillance.

The Not Ready test verifies that the are no faults in the beam dump kicker system prior to beam injection. The test comprises verification of a number of hardware generated status bits and a parameter estimation based on the sensitivity approach.

The minimum setup for the analog data acquisition needed to perform the parameter estimation is found to be an 8 bit ADC sampling at $133kHz$.

A simulation with an 8 bit ADC sampling at $200kHz$ shows that this setup does not provide enough difference between failed and non-failed estimates to meet the requirements of missed detection probability and false alarm probability.

In order to meet the requirements it is proposed to increase the ADC precision, improve the model used for the parameterisation or improve the knowledge of the installed component values.

The Ready Mode Surveillance monitors the subsystems who are active before the beam is dumped.

On subsystems not required to track the beam energy the fault detection is done by hardware generated status bits.

On the pulse generator, the only subsystem required to track the beam energy, the fault detection is done by analytical redundancy. Since the beam energy is constant for a long time, the tracking reference is modulated by a white noise signal making fault detection of dynamic components possible.

At an upper modulation limit of 2% of the voltage corresponding to injection energy the minimum setup for the surveillance system is an 15 bit (excl. sign bit) ADC and a 13 bit (excl. sign bit) DAC, both sampling at $1.54Hz$.

Simulations with the minimum ADC and DAC setup, sampling at $2Hz$, shows that the requirements to missed detection probability and false alarm probability can be meet at maximum energy, but not at injection energy.

The time to detect requirement is not met and it is proposed to increase the ADC and DAC precision to meet the requirement.

Bibliography

[Ave92] Terje Aven. *Reliability and Risk Analysis*. Elsevier Science Publishers, 1992.

[BCD+97] J.L. Bretin, E. Carlier, J.H. Dieperink, L. Ducimetière, G.H. Schröder, and E. Vossenberg. Reliabilty design study for the lhc beam dump kicker system. Lhc project report, CERN - SL Division, Geneva, Switzerland, 1997. Draft.

[Bla97] Mogens Blanke. Fault tolerant control - an engineering approach. ., Department of Control Engineering, Aalborg University, September 1997. Email: blanke@control.auc.dk.

[CAR] Cara v.4.02b on-line help. Windows help file.

[CLR99] M. Chorowski, Ph. Lebrun, and G. Riddone. Preliminary risk analysis of the lhc cryogenic system. Lhc project note 177, CERN, 1999.

[DBC+97] J.H. Dieperink, J.L. Bretin, E. Carlier, L. Ducimetière, G.H. Schröder, and E. Vossenberg. Design aspects related to the reliability of the lhc beam dump kicker systems. In *Procedings of 1997 Particle Accelerator Conference : PAC '97 Vancouver, Canada*, May 1997. LHC Project Report 113.

[FPEN94] Gene F. Franklin, J. David Powell, and Abbas Emami-Naeini. *Feedback Control of Dynamic Systems*. Addison-Wesley, third edition, 1994.

[FPW90] Gene F. Franklin, J. David Powell, and Michael L. Workman. *Digital Control of Dynamic Systems*. Addison-Wesley, second edition, 1990.

[Fuq87] Norman B. Fuqua. *Reliability Engineering for Electronic Design*, pages 9 – 12. MARCEL DEKKER, INC., 1987. ISBN: 0-8247-7571-6.

[Gro91] The LHC Study Group. Design study of the large hadron collider (lhc) - a multiparticle collider in the lep tunnel. ., CERN, May 1991.

[Gro95] The LHC Study Group. The large hadron collider - conceptual design report. . CERN/AC/95-05(LHC), CERN, 1995.

[Knu93] Torben Knudsen. Systemidentifikation. . AUC-PROCES-U-93-4008, Institut for elektroniske systemer, Aalborg Universitet, Frederik Bajers Vej 7,DK-9220 Aalborg Ø, Januar 1993. Danish.

[Knu96] Morten Knudsen. *SENSTOOLS - A Matlab toolkit for parameter estimation in linear and nonlinear systems using a sensitivity approach*. Department of Control Engineering, Aalborg University, Fredrik Bajersvej 7, DK-9220 Aalborg Ø, September 1996. mk@control.auc.dk - http://www.control.auc.dk/∼mk.

[Ros87] Sheldon M. Ross. *Introduction to Probability and Statistics for Engineers and Scientists*. John Wiley & Sons, 1987.

[ZP97] Jan M. Zazula and Serge Péraire. Design studies of the lhc beam dump. Lhc project report 112, CERN, CH 1211 Geneva 23, Switzerland, June 1997.

Appendix A

Calculation of parameter uncertainty

In this appendix calculation of parameter uncertainty of the direct parameter estimation method, due to quantisation noise, is described.

The model error used in the performance function, Equation 5.5, is

$$\epsilon(k,\theta) = y(k) - y_m(k,\theta)$$

When quantisation noise from A/D conversion is present the model error can be described as

$$\epsilon(k,\theta) = y(k) + \eta - y_m(k,\theta) \quad , \eta \sim \text{UID}(0, \frac{q^2}{12})$$

where η is the noise from the quantisation. Under the assumptions that the input signal changes several quanta between each sample, the quantisation noise can be modelled by a uniform white noise process with mean 0 and variance $\frac{q^2}{12}$ [FPW90, Chap. 7]. q is the quantisation step. The assumption that the input signal changes several quanta between each sample holds for the primary model, since this is used during the rise-time of the pulse, but the assumption does not hold for the flat top which is maintained by the compensation circuit. Here some correlation between the samples could be expected, but this effect is neglected.

The model error can be split into three parts [Knu96]:

$$\epsilon(k,\theta) = \epsilon_x(k) + \epsilon_m(k) + \epsilon_p(k,\theta)$$

where ϵ_x is due to to noise, ϵ_m is due to under modelling and ϵ_p is due to the parameter vector θ being different from the optimal value.

By inspection

$$\epsilon_x(k) = \eta$$

When ϵ is linearised around $\theta = \theta_N$, where θ_N is the optimal parameter vector with N samples, the three parts of the model error are independent [Knu96].

The estimated relative parameter spread due to noise, of the ith parameter, is under the assumption that ϵ_x is white and normal distributed [Knu96]

$$\sigma_{r,\theta i} \approx \frac{\epsilon_{x,RMSn}}{S_{imin}} \frac{1}{\sqrt{N}} \tag{A.1}$$

where S_{imin} is the minimum sensitivity of the ith parameter.

$\epsilon_{x,RMSn}$ is the normed RMS value of ϵ_x and is found by [Knu96]

$$\epsilon_{x,RMSn} = y_{RMS}^{-1} \epsilon_{x,RMS}$$

where

$$y_{RMS} = \sqrt{\frac{1}{N} \sum_{k=1}^{N} y^2(k)}$$

The RMS value of ϵ_x is

$$\epsilon_{x,RMS} = \sqrt{\frac{1}{N} \sum_{k=1}^{N} \eta^2(k)} \tag{A.2}$$

Using the fact that $\mu_\eta = 0$ and assuming η is ergodic and N is large Equation A.2 becomes

$$\epsilon_{x,RMS} \approx S$$

where S is the sample standard deviation.

Since $S \approx \sigma_\eta$

$$\epsilon_{x,RMS} \approx \sigma_\eta$$

where

$$\sigma_\eta = \sqrt{\frac{q^2}{12}}$$

q is the quantisation step and can be found from

$$q = A2^{-d}$$

where A is the amplitude range of the ADC and d is the number of bits not counting the sign bit.

Using the central limit theorem $\epsilon_{x,RMS}$ approximates a normal distribution for large N [Ros87]. This is the case since $\epsilon_{x,RMS}$ is found from a sum of identically distributed independent random variables. The variables are independent due to the white noise assumption.

This makes it possible to use $\epsilon_{x,RMSn}$ in Equation A.1, giving the relative parameter spread as

$$\sigma_{r,\theta i} \approx \frac{A2^{-d}}{S_{imin} y_{RMS} \sqrt{12} \sqrt{N}} \tag{A.3}$$

The total relative parameter uncertainty $\tilde{\theta}_{ritot}$ is [Knu96]

$$\tilde{\theta}_{ritot} = \sigma_{r,\theta i} + \tilde{\theta}_{ri} \tag{A.4}$$

where $\tilde{\theta}_{ri}$ is the relative parameter error due to under modelling. $\tilde{\theta}_{ri}$ has its maximum value at [Knu96]

$$\tilde{\theta}_{rimax} = \frac{\epsilon_{m,RMSn}}{S_{imin}} \tag{A.5}$$

Using Equation A.3 and A.5 in Equation A.4 gives the total relative parameter uncertainty as

$$\tilde{\theta}_{ritot} = \frac{1}{S_{imin}} \left(\frac{A2^{-d}}{y_{RMS} \sqrt{12} \sqrt{N}} + \epsilon_{m,RMSn} \right)$$

Appendix B

Calculation of fault matrices

This appendix describes the reasoning behind the element values of the fault matrices for the power supply system charging the primary capacitors.

Faults of the voltage divider is modelled as output failure and does therefore determine the elements of $\mathbf{F}_{C,1}$.

Short circuiting the input and output means that there will be no division of the voltage which is equal to $\mathbf{C}_{ps}$ being 1, thus

$$F_{C,1,1} = \frac{1 - K_{ps}}{K_{ps}}$$

Short circuit of the output to ground or a broken output connection leads to the measured voltage being zero. This can be described as a change of -100%, so

$$F_{C,1,2} = F_{C,1,3} = -1$$

The rest of the faults are modelled as acting on the system dynamics and does as such determine the elements of $\mathbf{F}_{A,1}$ and $\mathbf{F}_{B,1}$.

A short circuit across one of the resistors in the stack over the GTO switches gives a decrease of resistance of the stack of 10%. The resulting change of resistance of the A stack is (change of resistance of the B stack has the same result)

$$R_{Gfail} = 0.9R_{GTOpA} \parallel R_{GTOpB} = \frac{1.8}{1.9}R_G$$

so

$$F_{A,1,4} = F_{A,1,9} = \frac{1.9}{1.8} - 1$$

If one of the resistors becomes an open circuit the corresponding GTO switch will be damaged due to a too large stand by voltage and become a short circuit. This results in the resistor open circuit fault having the same effect as the resistor short circuit fault, thus

$$F_{A,1,5} = F_{A,1,10} = \frac{1.9}{1.8} - 1$$

Breaking one of the capacitor input connections corresponds to halving the capacitance, thus

$$F_{A,1,6} = F_{A,1,10} = 1$$

and

$$F_{B,1,6} = F_{B,1,10} = 1$$

Short circuit of the capacitor and closing the manual safety switch gives a very fast discharge, simulated by having the capacitor connected to ground by a $1m\Omega$ resistor, thus

$$F_{A,1,7} = F_{A,1,17} = F_{A,1,12} = \frac{R_G}{1m\Omega} - 1$$

Closing the electrical safety switch discharges the capacitor through the resistor R_{61p} so

$$F_{A,1,13} = \frac{R_G}{R_{61p}} - 1$$

Power supply failure is modelled by cutting of the input giving $\mathbf{B}_{ps} = 0$ which is equal to a parameter change of -100% thus

$$F_{B,1,14} = -1$$

Appendix C

Calculation of error transfer function

In this appendix the fault to error signal transfer function used in the Ready Mode Surveillance is found.

Assuming a good model fit, the estimated measurement, $\hat{y}$, is

$$\hat{y}(s) = H_y(s)V_D(s)$$

Since there are no external disturbance, such as load fluctuations, the measured value, y, is for a given fault f

$$y(s) = H_y(s)V_D(s) + H_e(s)f(s) + \eta$$

where η is the quantisation noise.

The error signal, e, is

$$e(s) = y(s) - \hat{y}(s) = H_e(s)f(s) + \eta$$

To find H_e the fault model from Section 6.1.5 is combined with the power supply model, without quantisation noise, to

$$\begin{aligned}
\dot{\mathbf{x}}_{ps}(t) &= \left(\mathbf{A}_{ps} + \Delta\mathbf{A}_{ps}(t) + (\mathbf{B}_{ps} + \Delta\mathbf{B}_{ps}(t))\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)\mathbf{x}_{ps}(t) + \\
&\quad (\mathbf{B}_{ps} + \Delta\mathbf{B}_{ps}(t))\frac{K_{ps,in}}{R_{ps}+R_{71}}V_D(t) \\
y(t) &= \left(\mathbf{C}_{ps} + \Delta\mathbf{C}_{ps}(t) - (D_{ps} - \Delta D_{ps}(t))\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)\mathbf{x}_{ps}(t) + \\
&\quad (D_{ps} + \Delta D_{ps}(t))\frac{K_{ps,in}}{R_{ps}+R_{71}}V_D(t)
\end{aligned}$$

The fault effect is described, without element indexes to simplify notation, for the first order power supply charging system by

$$\Delta\mathbf{A}_{ps}(t) = \mathbf{A}_{ps}\mathbf{F}_A\mathbf{f}(t)$$

and so forth for the other fault matrices.

Linearising around an operation point, described by $\mathbf{x}_{ps0}$ and V_{D0}, for a given fault at a given time yields

$$\begin{aligned}
\dot{\mathbf{x}}_{ps}(t) &= \left(\mathbf{A}_{ps} + \mathbf{B}_{ps}\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)\mathbf{x}_{ps}(t) + \mathbf{B}_{ps}\frac{K_{ps,in}}{R_{ps}+R_{71}}V_D(t) + \\
&\quad \left(\left(\mathbf{A}_{ps}\mathbf{F}_A + \mathbf{B}_{ps}\mathbf{F_B}\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)\mathbf{x}_{ps0} + \mathbf{B}_{ps}\mathbf{F}_B\frac{K_{ps,in}}{R_{ps}+R_{71}}V_{D0}\right)f(t) \\
\mathbf{y}_{ps}(t) &= \left(\mathbf{C}_{ps} + D_{ps}\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)\mathbf{x}_{ps}(t) + D_{ps}\frac{K_{ps,in}}{R_{ps}+R_{71}}V_D(t) + \\
&\quad \left(\left(\mathbf{C}_{ps}\mathbf{F}_C + D_{ps}\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)\mathbf{x}_{ps0} + D_{ps}F_D\frac{K_{ps,in}}{R_{ps}+R_{71}}V_{D0}\right)f(t)
\end{aligned}$$

The transfer function H_e can now be found as

$$\begin{aligned}
H_e(s) &= \left(\mathbf{C}_{ps} + D_{ps}\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)\left(s - \mathbf{A}_{ps} + \mathbf{B}_{ps}\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\right)^{-1}\cdot \\
&\quad \left(\mathbf{A}_{ps}\mathbf{F}_A\mathbf{x}_{ps0} + \mathbf{B}_{ps}\mathbf{F}_B\left(\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\mathbf{x}_{ps0} + \frac{K_{ps,in}}{R_{ps}+R_{71}}V_{D0}\right)\right) + \\
&\quad \mathbf{C}_{ps}\mathbf{F}_C + D_{ps}\mathbf{F}_D\left(\frac{R_{ps}+R_{71}-R_G}{R_G(R_{ps}+R_{71})}\mathbf{x}_{ps0} + \frac{K_{ps,in}}{R_{ps}+R_{71}}V_{D0}\right)
\end{aligned}$$

which can be rewritten, for the ith fault, to

$$H_{e,i}(s) = \frac{Kps\left(-\frac{V_{C0}}{R_G C_p}F_{A,1,i} + \frac{1}{(R_{ps}+R_{71})R_G C_p}((R_{ps}+R_{71}-R_G)V_{C0} + R_G K_{ps,in} V_{D0})F_{B,1,i}\right)}{s + \frac{1}{(R_{ps}+R_{71})C_P}} +$$

$$K_{ps} V_{C0} F_{C,1,i}$$

Appendix D

The Gauss-Newton minimisation algorithm

This appendix describes the Gauss-Newton algorithm for finding a local minimum of a performance function $V(\theta)$. The performance function used in the context of system-identification or parameter estimation is

$$V(\theta) = \frac{1}{2N} \sum_{k=1}^{N} \epsilon^2(k)$$

where ϵ is the difference between the wanted value y and the value y_m calculated with the parameter vector θ, that is

$$\epsilon(k) = y(k) - y_m(k, \theta)$$

The Gauss-Newton algorithm consists of the steps [Knu93]:

1. Calculate $V(\theta_i)$, the gradient $\mathbf{G}(\theta_i)$ and the Hessian matrix $\mathbf{H}(\theta_i)$.
2. Try updating by

   $$\theta_{i+1} = \theta_i - (\mathbf{H}(\theta_i) + \delta \mathbf{I})^{-1} \mathbf{G}(\theta_i)$$

   Calculate $V(\theta_{i+1})$
3. Test update. If $V(\theta_i) < V(\theta_{i+1})$ then $\delta = \frac{1}{2}\delta$ else $\delta = 2\delta$ and go to 2
4. Test convergence. If $\max(\theta_{i+1} - \theta_i) < \kappa$ then $\theta = \theta_{i+1}$ and stop the iteration else $i = i + 1$ and go to 1

The algorithm is also stopped indicating non-convergence if δ becomes smaller than a predefined limit.

In the Gauss-Newton algorithm the gradient and the Hessian is calculated by the model gradient

$$\Psi(k,\theta) = \frac{\partial y_m(k,\theta)}{\partial \theta}$$

The gradient is

$$\mathbf{G} = \frac{\partial V(\theta)}{\partial \theta} = \frac{1}{N}\sum_{k=1}^{N} \Psi(k)\epsilon(k)$$

and the Hessian is

$$\mathbf{H} = \frac{\partial^2 V(\theta)}{\partial \theta \partial \theta^T} = \frac{1}{N}\sum_{k=1}^{N} \Psi(k)\Psi^T(k)$$

The model gradient Ψ can be found by numerical differentiation. The jth element Ψ_j is calculated by giving the jth parameter a small deviation $\Delta\theta_j = d\theta_j$ where d is a small value e.g. 10^{-3} [Knu96]. The jth element is then

$$\Psi_j(k) \approx \frac{\Delta y_m(k,\theta_j)}{\Delta \theta_j} = \frac{y_m(k,\theta_j + \Delta\theta_j) - y_m(k,\theta_j)}{\Delta \theta_j}$$

Appendix E

Fault trees

This appendix shows the fault trees generated by the component fault tree analysis. Only fault trees for the pulse generator, retrigger and power supply system are given, the fault tree for the power trigger is available in Section 4.5

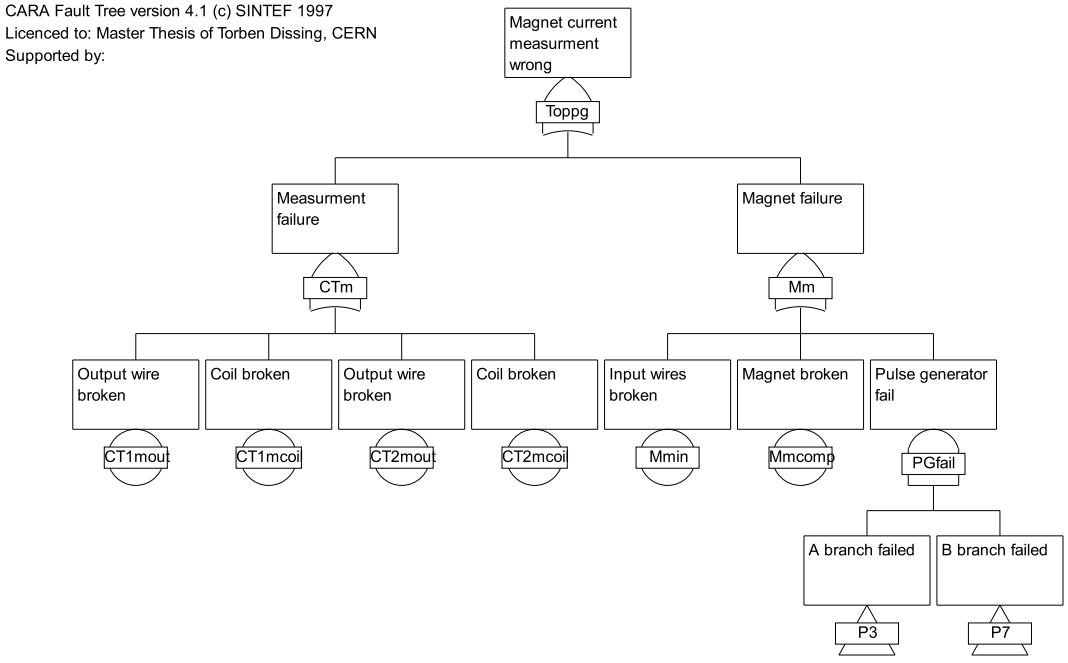

Figure E.1: *Fault tree for the pulse generator page 1*

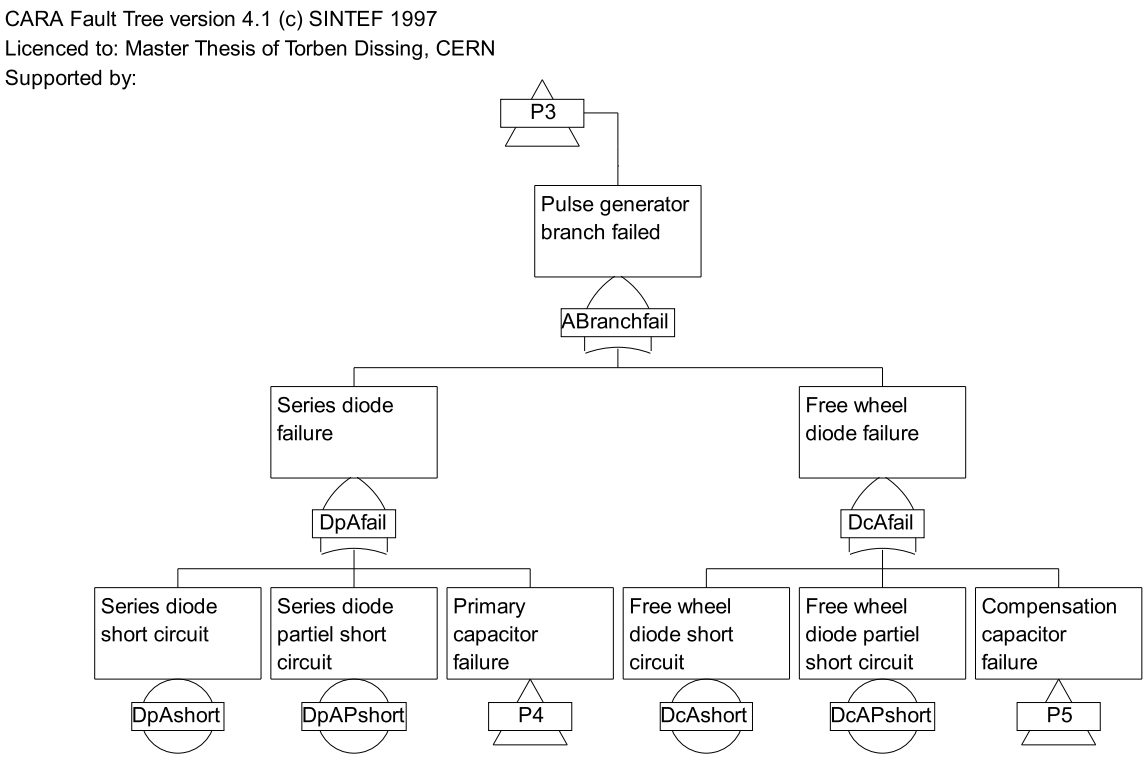

Figure E.2: *Fault tree for the pulse generator page 3*

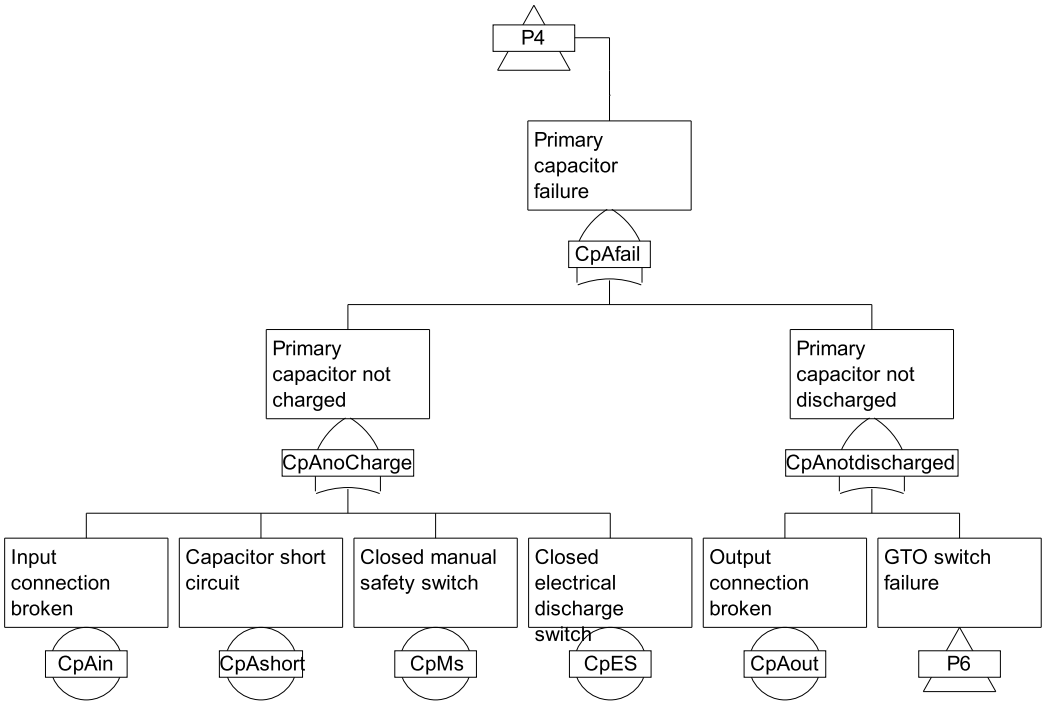

Figure E.3: *Fault tree for the pulse generator page 4*

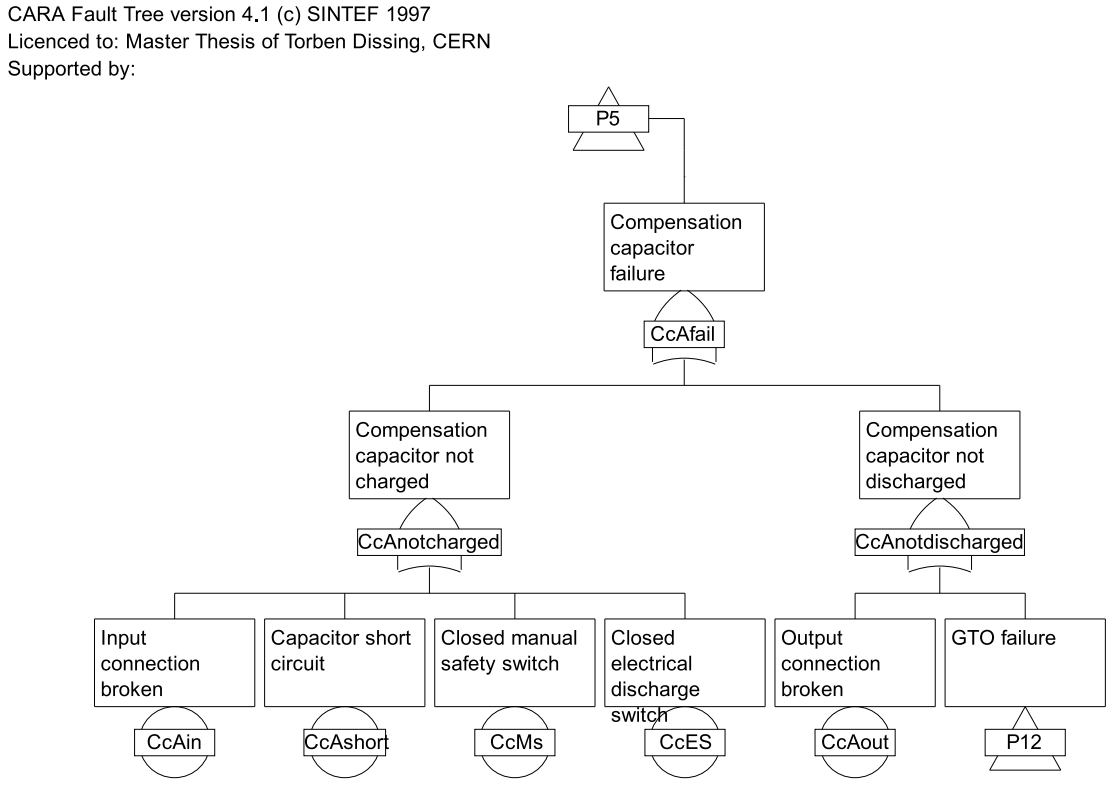

Figure E.4: *Fault tree for the pulse generator page 5*

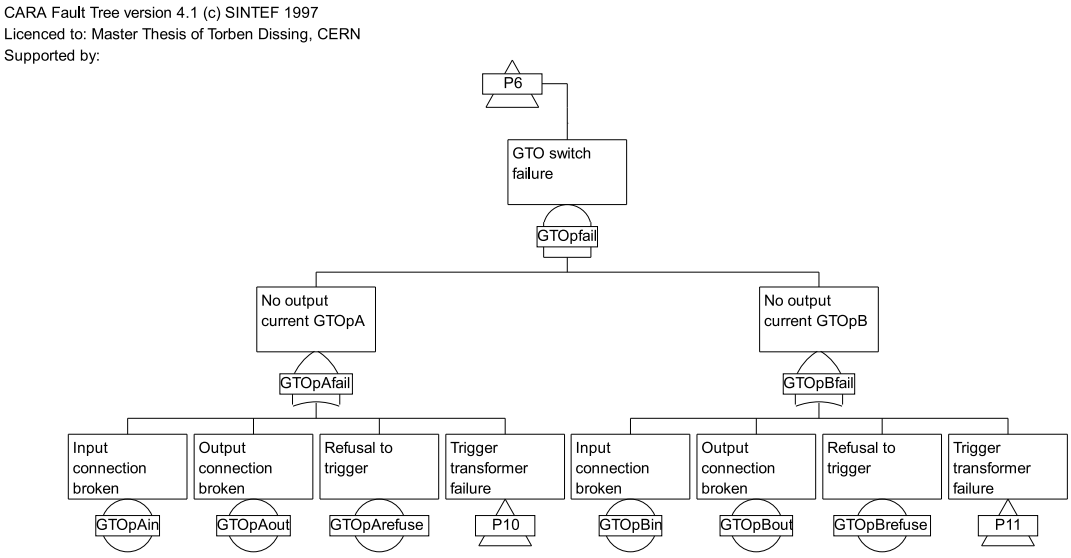

Figure E.5: *Fault tree for the pulse generator page 6*

CARA Fault Tree version 4.1 (c) SINTEF 1997
Licenced to: Master Thesis of Torben Dissing, CERN
Supported by:

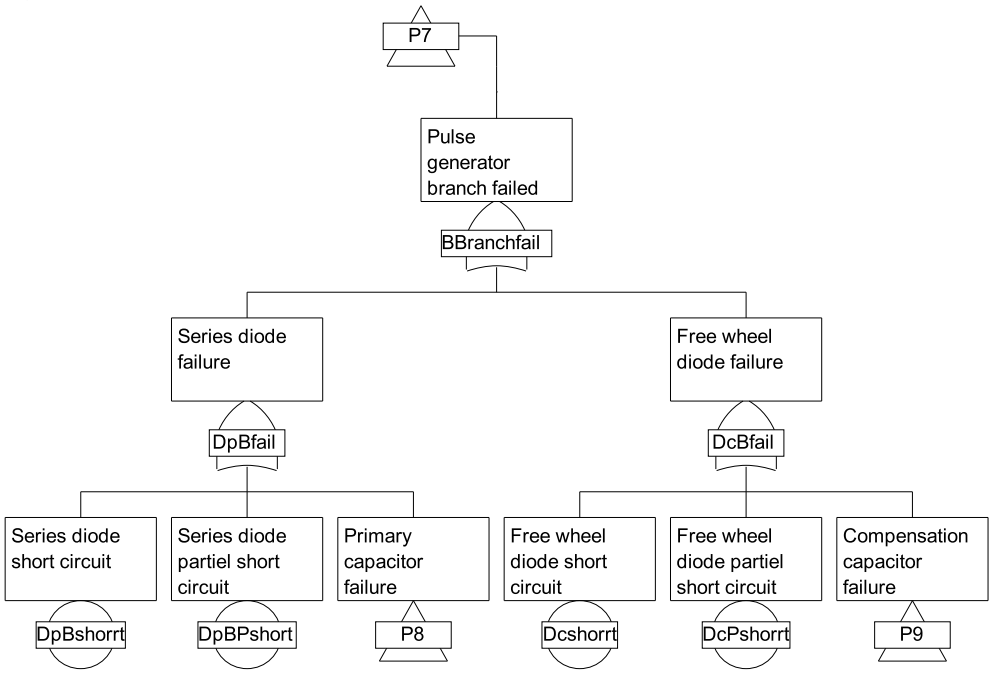

Figure E.6: *Fault tree for the pulse generator page 7*

CARA Fault Tree version 4.1 (c) SINTEF 1997
Licenced to: Master Thesis of Torben Dissing, CERN
Supported by:

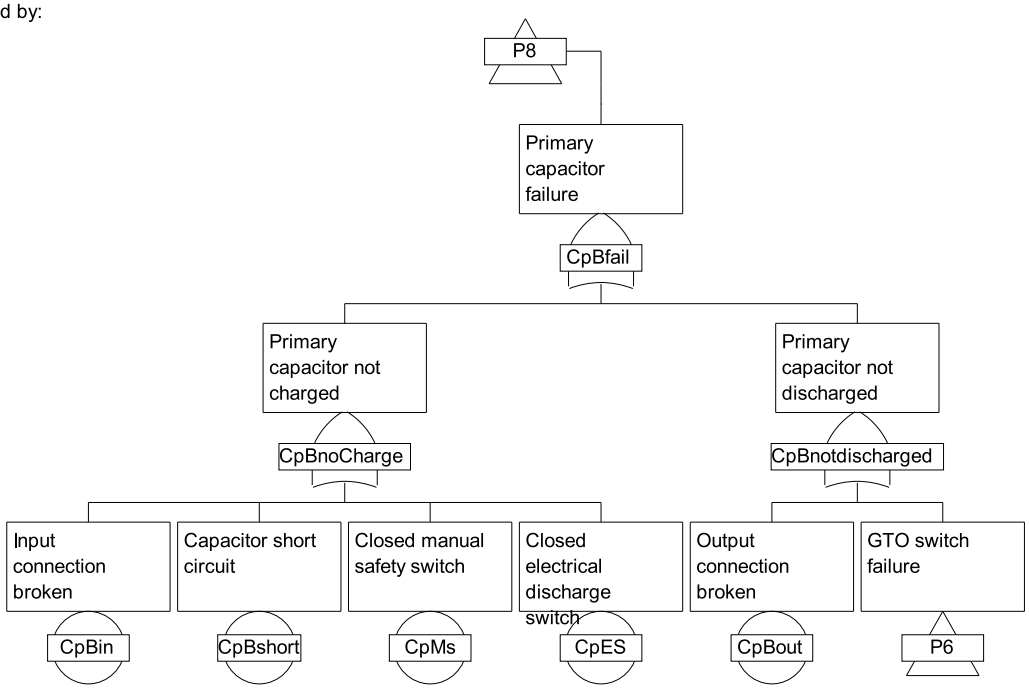

Figure E.7: *Fault tree for the pulse generator page 8*

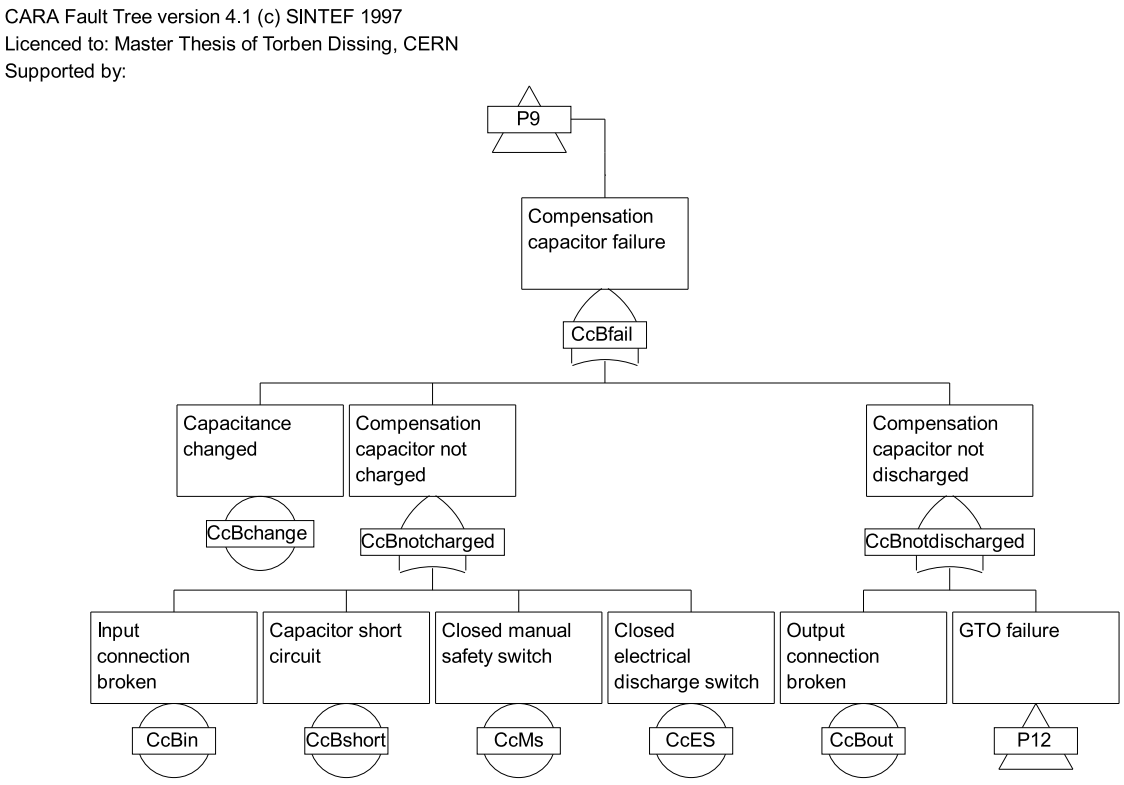

Figure E.8: *Fault tree for the pulse generator page 9*

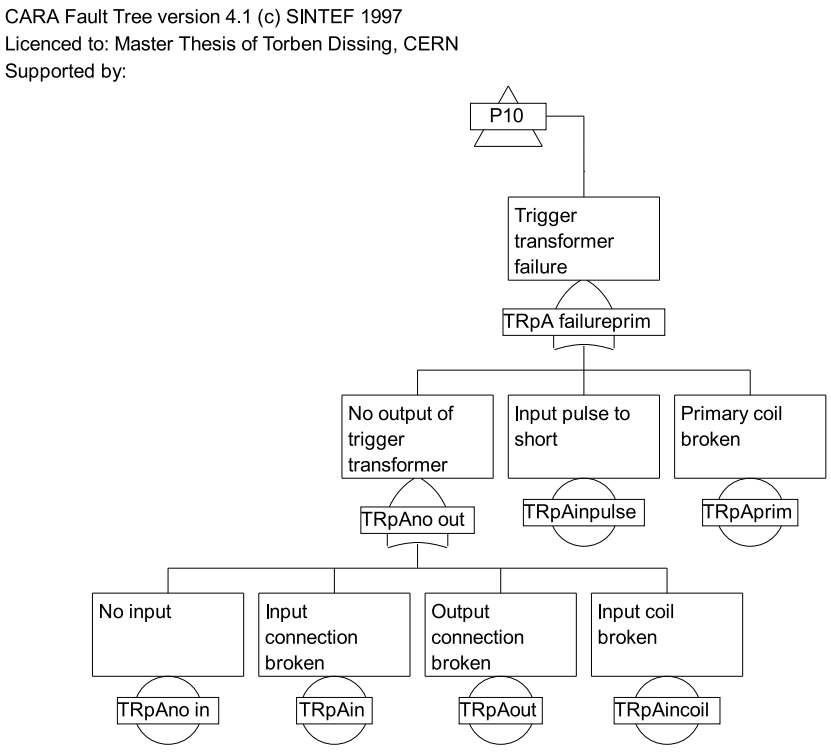

Figure E.9: *Fault tree for the pulse generator page 10*

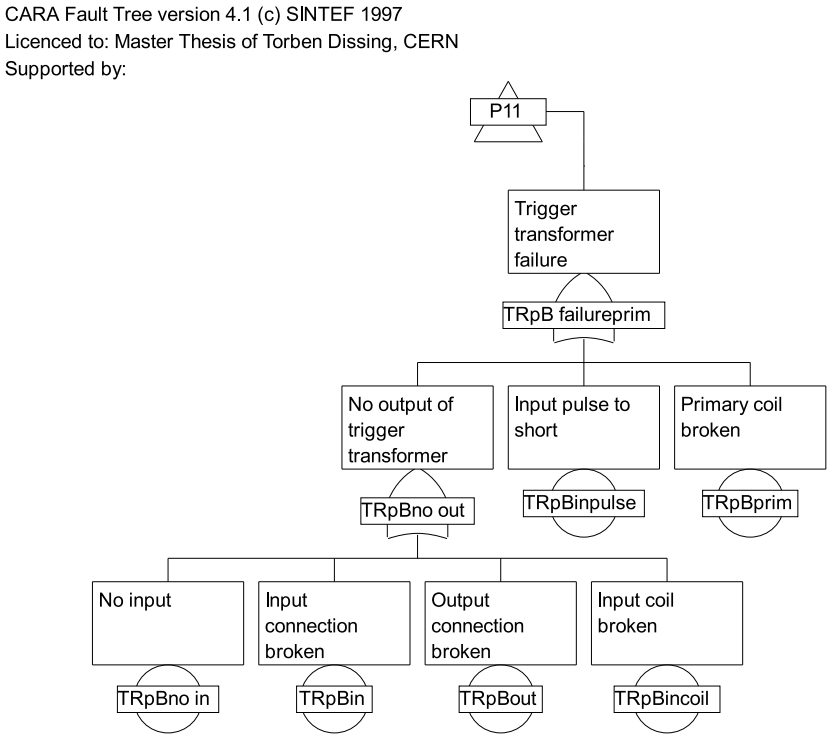

Figure E.10: *Fault tree for the pulse generator page 11*

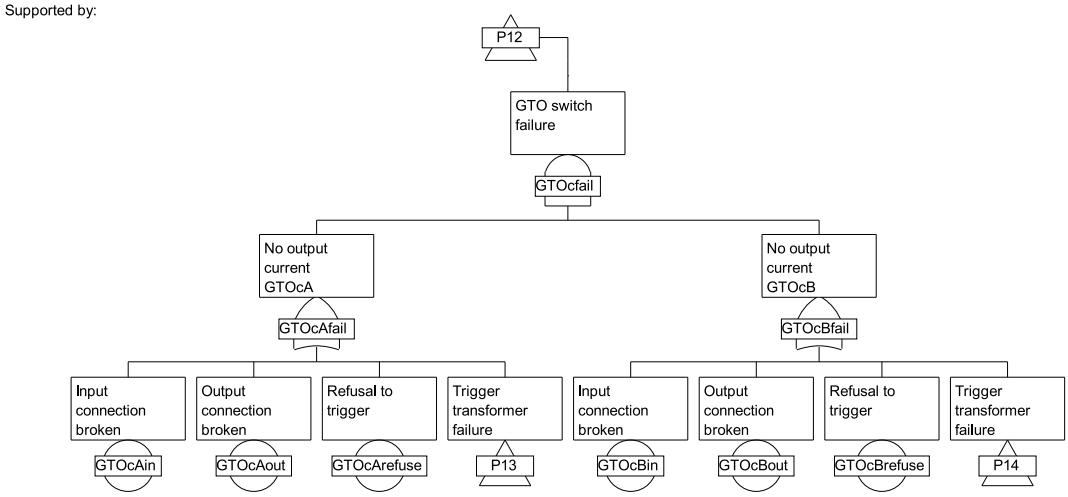

Figure E.11: *Fault tree for the pulse generator page 12*

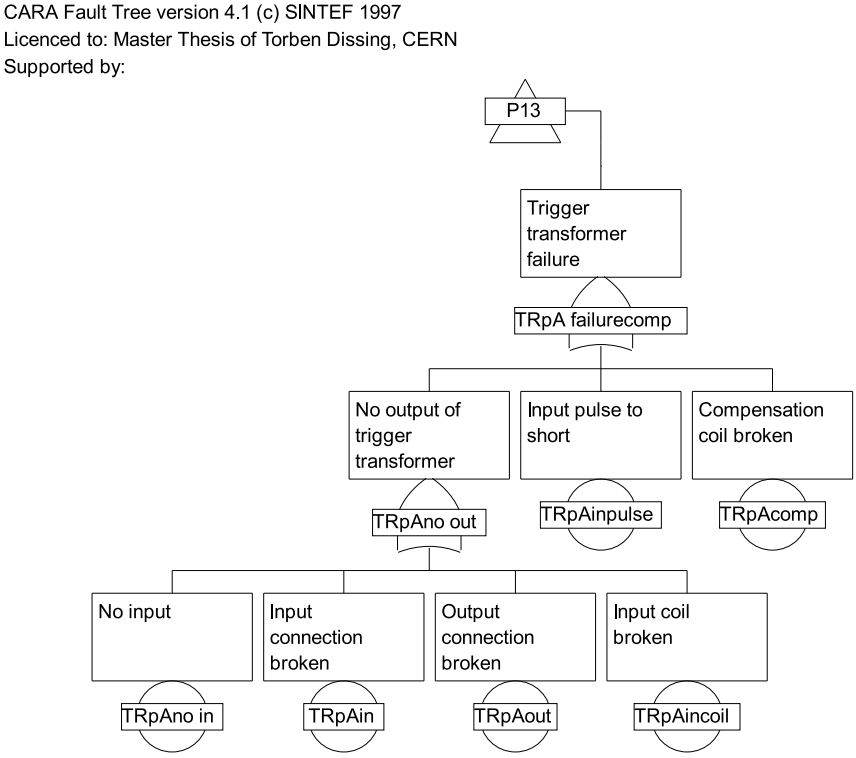

Figure E.12: *Fault tree for the pulse generator page 13*

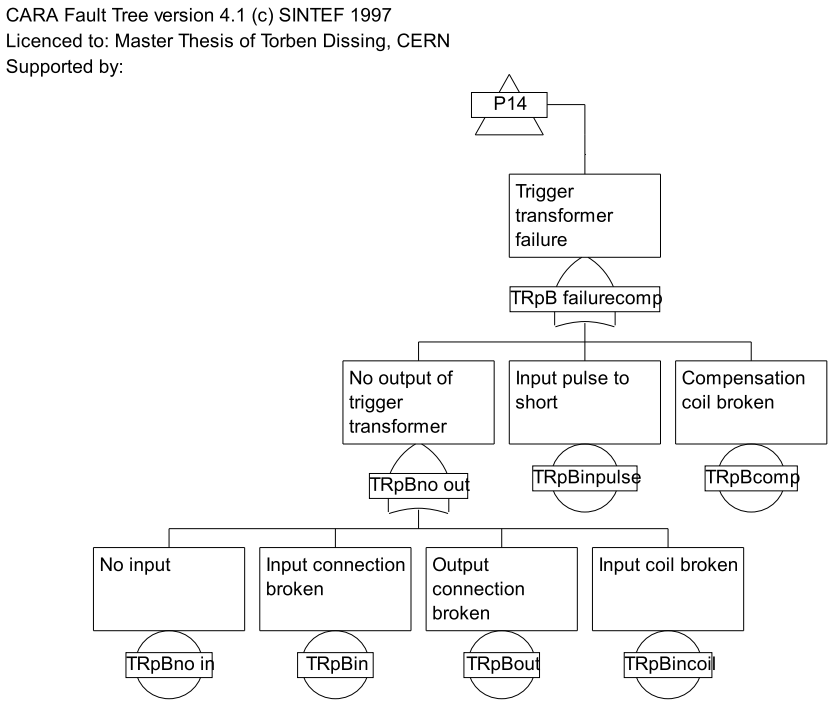

Figure E.13: *Fault tree for the pulse generator page 14*

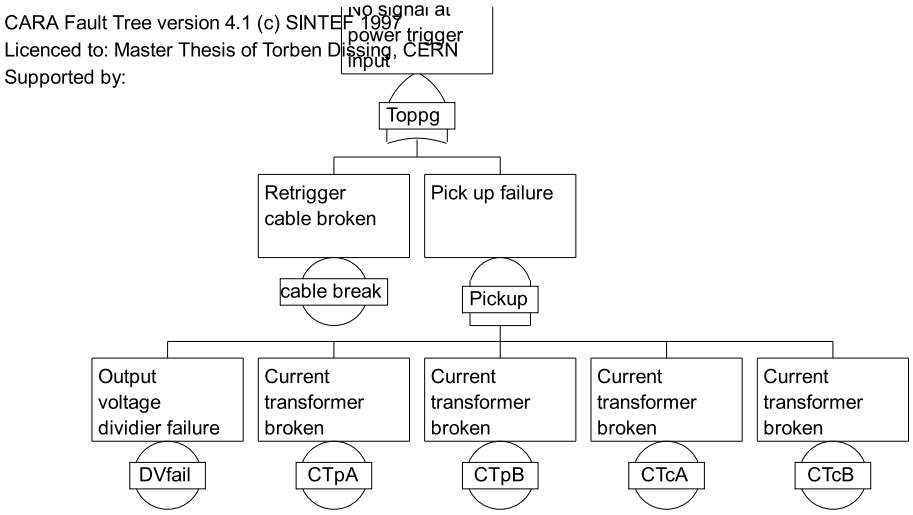

Figure E.14: *Fault tree for the retrigger page 1*

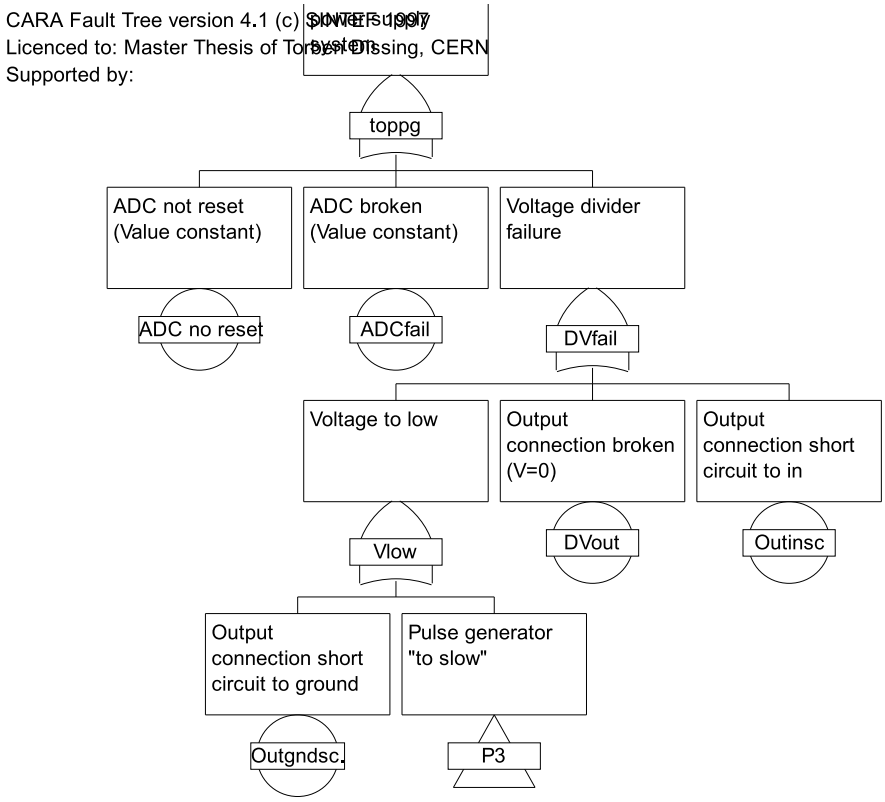

Figure E.15: *Fault tree for the power supply system page 1*

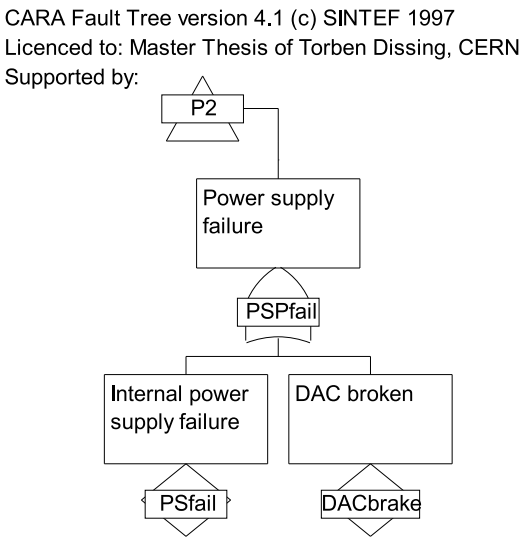

Figure E.16: *Fault tree for the power supply system page 2*

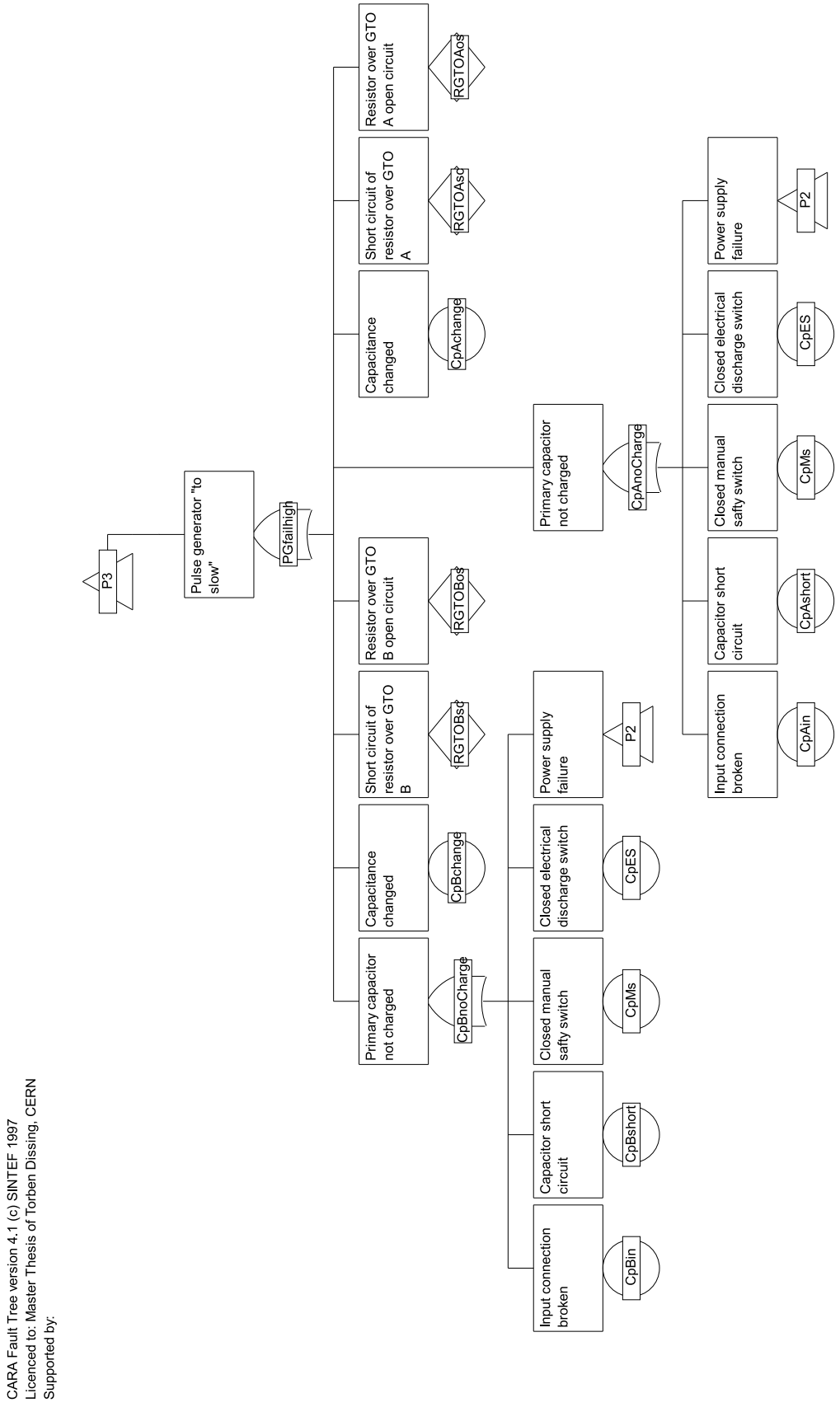

Figure E.17: *Fault tree for the power supply system page 3*