THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par : *l'Institut National Polytechnique de Toulouse (INP Toulouse)*
Cotutelle internationale *CERN (European Organisation for the Nuclear Research)*

Présentée et soutenue le *18/12/2013* **par :**

PATRICE NOUVEL

Design of a dependable Interlock System for linear colliders

JURY

PR. JEAN ARLAT		Président du Jury
PR. LIONEL TORRES	Rapporteur	Membre du Jury
DR. YANNICK HERVE	Rapporteur	Membre du Jury
PR. HÉLÈNE TAP		Directrice de thèse
MR. BRUNO PUCCIO		Invité

École doctorale et spécialité :
GEET : Micro et Nanosystèmes
Unité de Recherche :
LAAS (Laboratoire d'Analyse et d'Architecture des Systèmes)

“Seule compte la démarche. Car c’est elle qui dure et non le but qui n’est qu’illusion du voyageur quand il marche de crête en crête comme si le but atteint avait un sens."

Antoine de Saint-Exupéry. Citadelle chap. XLIX

INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE

Abstract

Doctoral School
Génie Electrique, Electronique, Télécommunications

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Design of a dependable Interlock System for linear colliders

by Patrice Nouvel

For high energy accelerators, the interlock system is a key part of the machine protection. The interlock principle is to inhibit the beam either on failure of critical equipment and/or on low beam quality evaluation. The dependability of such a system is the most critical parameter. This thesis presents the design of an dependable interlock system for linear collider with an application to the CLIC (Compact Linear Collider) project. This design process is based on the IEEE 1220 standard and is is divided in four steps. First, the specifications are established, with a focus on the dependability, more precisely the reliability and the availability of the system. The second step is the design proposal based on a functional analysis, the CLIC and interfaced systems architecture. Third, the feasibility study is performed, applying the concepts in an accelerator facility. Finally, the last step is the hardware verification. Its aim is to prove that the proposed design is able to reach the requirements.

INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE

Resumé

Ecole Doctorale
Génie Electrique, Electronique, Télécommunications

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Conception d'un système de verrouillage sûr de fonctionnement pour les collisionneurs linéaires

par Patrice Nouvel

Pour les accélérateurs de particules à hautes énergies, le système de verrouillage est une partie clé de la protection de la machine. Le verrouillage de la machine est l'inhibition du faisceau dès lors qu'un équipement critique tombe en panne et/ou qu'un faisceau est de faible qualité. Pour un système de verrouillage, sa sûreté de fonctionnement est la caractéristique la plus importante. Cette thèse présente le développement d'un système de verrouillage pour les collisionneurs linéaires avec une application au projet CLIC (Compact Linear Collider). Son élaboration s'appuie sur la norme d'ingénierie IEEE 1220 et se décline en quatre parties. Tout d'abord, les spécifications sont établies. Une attention particulière est portée sur la sûreté de fonctionnement, plus précisément, la fiabilité et la disponibilité du système. La deuxième étape est la proposition d'un design. Celui-ci est basé sur une analyse fonctionnelle, les interfaces du système et l'architecture du CLIC. Troisièmement, une étude de faisabilité est effectuée en appliquant les concepts dans un environnement opérationnel. Finalement, la dernière étape est la vérification matérielle. Le but est de prouver que le design proposé est capable de remplir le cahier des charges établi.

Acknowledgements

First of all, I would like to thank the rapporteurs Lionel Torres and Yannick Herve for their valuable advices and the time they spent to read this manuscript.

I would like to warmly thanks my thesis director, Hélène Tap, for her precious guidance which leads me successfully to the thesis defence. A big thanks to Bruno Puccio, my CERN supervisor, who gives me the opportunity to undertaken this PhD. His support, advices and availability during these 3 past years have been a key factor to the thesis success.

I would like to thank Alexey Dubrovskiy for his help for the CTF3 application.

For their help on the dependability study, I would like to thank Benjamin Todd and Sigrid Wagner. For their help on JAVA programming, Maxime Audrain, Rafal Leszko and Jean-Christophe Garnier (and for his help for Linux).

Also, I would like to thank Bernard Collignon and Chistophe Martin for their help on the test bench realisation.

I would like also to thank Andrzej Siemko, the group leader, to allow me to present my works in conferences.

A big thank to the (not yet cited) lunch (and ping pong) and machine interlock team : Ivan, Jakub, Jacek, Andrea, Stephane, Konstatinos, Javier, Daniel, Damien, Scott, Gaetan, Steffen, James, Jonathan, Cristina, Kajetan, Dawn, Alain, Jean-Louis, Jean-Phillipe, Jeremie, Pierre, Juan, Maciej, Markus, Kamil (with the hope I did not forget anybody).

In more general way, I thank my friends, who were tolerant enough to allow me talking about the PhD !

More personally, I thank my family, for their help (special mention to Jeff, who gives me regularly a place to rest myself). At last but not the least, I thank Claire for her constant support on a day basis for this challenge !

Table of Contents

List of Figures

List of Tables

Chapter 1

General Introduction

When entering in the particles accelerators field, the first thought that may arise is to realize the impressive complexity of these machines. Building these huge scientific tools requires the cooperation of many sectors : super-conductive magnets, Radio Frequency cavities, electronics (analog, numeric, microelectronic), cryogenic, vacuum, beam physics, mechanics, electric powering, etc. Building more and more powerful machines has created a need of protection and a new sector dedicated to the machine protection has been set up [10]. Indeed, the energy reached by the beam (360 MJ for the Large Hadron Collider (LHC)) and stocked in the equipment (10 GJ in LHC magnet system) are way more higher than the energy needed to melt on kilogram of copper (i.e. 700kJ) [11]. Consequently, particles accelerators can easily be damaged in case of uncontrolled energy release. The Interlock Systems are part of the machine protection. An Interlock System stops the machine when an unsafe condition occurs. The goal is to stop before the uncontrolled energy deposition.

The European Organisation for the Nuclear Research (CERN) is one of the larger particles physics laboratory. Created in 1954, many machines have been built and part of them are still in operation. However, due to physics challenges evolution, new machines are studied. Among them, CERN has taken a leading part of the Compact Linear Collider (CLIC) [12] [13] [1] study and has started a close collaboration with the International Linear Collider (ILC) project. They both aim to explore new physics revealed by current accelerators and to test predicted theories : Higgs boson [14], dark matter [15], supersymmetrie [16], beyond the standard model [17], etc.

The CLIC design faces several challenges [18]. As it is a linear machine, the acceleration cavities are used only once and require a strong gradient. Thus, a novel two beams acceleration scheme has been introduced. Its feasibility demonstration is a crucial point for the project. Another critical feasibility study is the machine protection and the beam

operation. Part of it, the CLIC Interlock System study has been undertaken in the form of a thesis, presented in this manuscript.

In the CLIC machine protection framework, the Interlock System concepts have been defined [19]. It is based on a beam permit system [20] and a new post-pulse analysis, dedicated to linear colliders.

The thesis works attempt to answer the following question : *how to design an Interlock System for a linear collider ?*

From the state of the art, some works have already been done on the Interlock System design. Indeed, a thesis has been performed on the LHC Interlock System to carry on the work from prototype to a fully tested and operational system [5]. Another example is the recent method to use Programmable Logic Device (PLD) in similar systems [21]. The presented thesis works undertake the design from concepts up to the prototype, thus complementing the two previously mentioned works.

To answer the main problematic, we propose to introduce an industrial methodology inspired by a system engineering standard, and to apply it to the CLIC Interlock System project. The goal is to be transparent on each method steps, thus allowing understanding, enhancement and correction of the design. The idea behind is to be able to use this method as a basis to develop future interlock systems. A special focus is proposed to be taken for the dependability, as it is a critical quality for an Interlock System.

Chapter 2 presents the context, starting from the physics particles challenges up to the CLIC machine protection. It expands on the problematic of the thesis and performs the state of the art on interlock and selected protection systems.

In chapter 3, the conditions of use and the system interfaces are defined. The central part is the establishment of the functional and performance requirements. It is done with an Institute of Electrical and Electronics Engineers (IEEE) standard as a guideline. A part of the chapter is dedicated to reliability and availability requirements determination. It proposes a methodology to verify if a design is compliant with these requirements. The last part explains in details the critical interfaces, extract the constraints, and how the expectations from the Interlock System to these interfaced systems are produced.

Chapter 4 presents the Interlock System design proposal. It explains the functional analysis done with the help of the IEEE standard. Finally, the implementation proposal, based on the functional analysis and concepts to implement, is presented. Going further, it proposes an implementation to the hardware modules level.

In chapter 5, the design verification is explained. The feasibility study performed in CLIC Test Facility 3 (CTF3) is presented : it is studying the post-pulse analysis application

in operational environment through a JAVA software. The hardware demonstration is described from the VHDL blocks up to the whole test bench. The measurements which aim to prove the design compliance are then examined.

Finally, the chapter 6 concludes the thesis works. It is proposing the short and long term improvements that would enhance these works.

Chapter 2

Context and state of the art

2.1 Introduction

This thesis is focused on the design process of a dependable interlock system, applied to the CLIC. Before going into the design process, there are two needs : to explain the context and to define the starting point of the thesis works.

This chapter follows a top-bottom approach. The nowadays challenges in particle physics are introduced. The involvement in this field of the CERN, where the thesis has been done, is presented. Going more specific, the interest is focused on two proposed high energy linear colliders : the CLIC and the ILC. The next step is to give an overview of the CLIC machine protection strategy. It leads to introduce the CLIC Interlock System concepts. At that point, the problematic of the thesis is set up. The two last sections are dedicated to the background on protection systems related to interlock systems. The fifth section presents the interlock systems in a generic way, synthesizing the state of the art. The last section is more specific and presents five selected protection systems which are the main design references for these thesis works.

2.2 Particle Physics and CERN

In order to explain the thesis subject, it is needed to introduce the particles accelerators and therefore their purposes. It starts with the standard model.

2.2.1 Challenges in particle physics

The goal in physics is to understand the basic structures and laws, from infinite high scale (stars, galaxies clusters) to infinite low scale (fundamental particles) [22].

a. Building the standard model

The particle physics has started with the discoveries of different atoms. A great simplification has been made when it has been realized that atoms can be unified with three particles : protons, neutrons and electrons.

In the beginning of the twentieth century, new particles from cosmic rays have been discovered. There was no system to classify them. They have been organized in regard with their properties : mass, charge, spin and lifetime (time before decay in lighter particles).

To simplify this organization, new particles, so-called quarks, have been predicted. Their combination can describe the other particles. This is the birth of the standard model.

The standard model comprises fundamental particles (6 quarks and 6 leptons) and fundamental forces as represented in Figure 2.1, [17]. The forces are represented via force carriers :

– The weak force is seen through the bosons W and Z. It explains the energy production in the sun and the radioactivity.
– The electromagnetic force carrier is the photon. It is responsible for the transmission of light and magnet attraction force.
– The strong force is represented with gluons. It is responsible for nucleus cohesion.

To synthesize, the standard model is unifying the strong, weak and electromagnetic forces. It is very precise at both low and high energy. However, it remains incomplete : new particles and interaction are needed to cover some gaps.

b. Beyond the standard model

The standard model has several limitations [2], [17] :
– It does not explain how gravity is connected to the other fundamental forces. In other words, it does not comprise the Einstein's general theory of relativity.
– It does not explain why the fundamental particles are the quarks and leptons (and their numbers).
– It does not explain the unbalance between matter and antimatter.

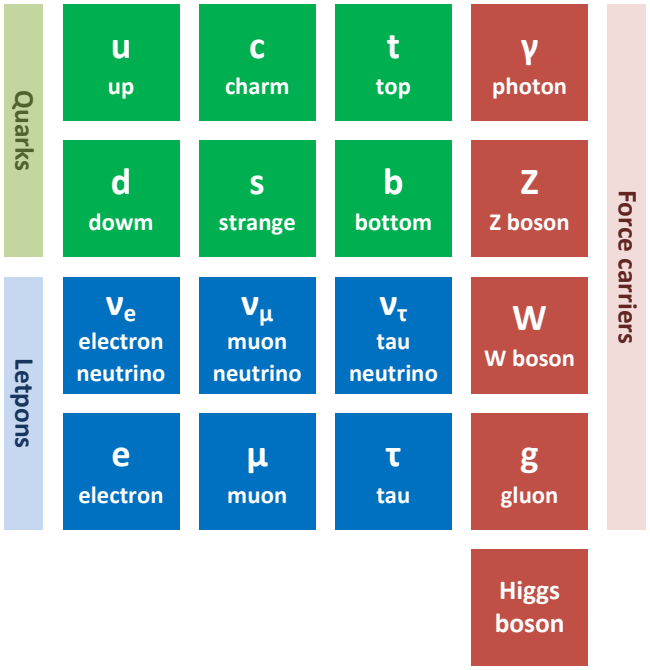

FIGURE 2.1: Standard model particles common representation

– It does not explain the existence of the dark matter and dark energy.
– It does not explain the mass existence of neutrinos.

However, several models beyond the standard model have been predicted. One of them predicts a mechanism called Higgs field [14], which gives mass to fundamental particles. This hypothesis could contain particles with properties similar to dark matter. This Higgs field could be studied through its particle : the Higgs boson.

c. Challenges in particle physics

Hereunder are presented a selected bunch of nowadays challenges in particle physics :

Dark matter/energy The known matter (galaxies) is estimated to account only for 4% of the content of the universe. What remaining is dark matter and dark energy. Despite there are evidences of these phenomenons (gravitational clues), no theories have been proved until now. Some of them are related with particle physics such as the *supersymmetry* theory [16] or the *hidden valley* theory [15].

Supersymmetry The supersymmetry is a theoretical expansion of the standard model. It predicts a partner particle for each particle of the standard model : standard bosons would have supersymmetric fermions and the other way around. This theory

would resolve several gaps of the standard model (among them, the Higgs boson mass). It would unify the force strength at very high energy, making more understandable the state of the early universe. It would be a step closer to the grand unified theory.

Gravity and standard model Several tracks to include the gravity force to the standard model are followed. There is research for the hypothetical gravitons. Another point is to explain why the gravitation is so weak compared to the three other forces. Some hypothesis predict tiny black holes or extra dimensions that could appear during collisions. It could be a solution to this challenge.

Compositeness The compositeness is a theory predicting every particle of the standard model are made up of smaller unit called *preons*.

There are many other challenges that have not been described (neutrino mass, muons physics, extra dimensions, grand unifications). These particle physics challenges are studied by many institutes and laboratories around the world : for instance the Fermi National Accelerator Laboratory (FNAL) in North America, the Shanghai Institute of Applied Physics (Sinap) in Asia, the European Synchrotron Radiation Facility (ESRF) and CERN in Europe. The thesis has been undertaken at CERN.

2.2.2 European Organisation for the Nuclear Research

The CERN is the world's largest particle physicist laboratory. It is made up of 20 member states. More than 600 institutes and universities use CERN facilities. About 10000 scientists working in collaboration and 2400 are employed by CERN.

The CERN's aims is the fundamental research in high energy physics. Its goal is to study fundamental structure of universe and state of the matter. The CERN intends to carry on the challenges previously mentioned.

The research tools used at CERN are particles accelerators. The principle is to accelerate particle beams (protons, leptons or ions) and make them collide together or with a fixed target. The resulting collisions are then studied by detectors.

In Figure 2.2 is represented the accelerator complex at CERN. It is a chain of small accelerators (like Linac 4) pre-accelerating and bunching the beam up to large accelerators like the Super Proton Synchrotron (SPS) or the more known LHC.

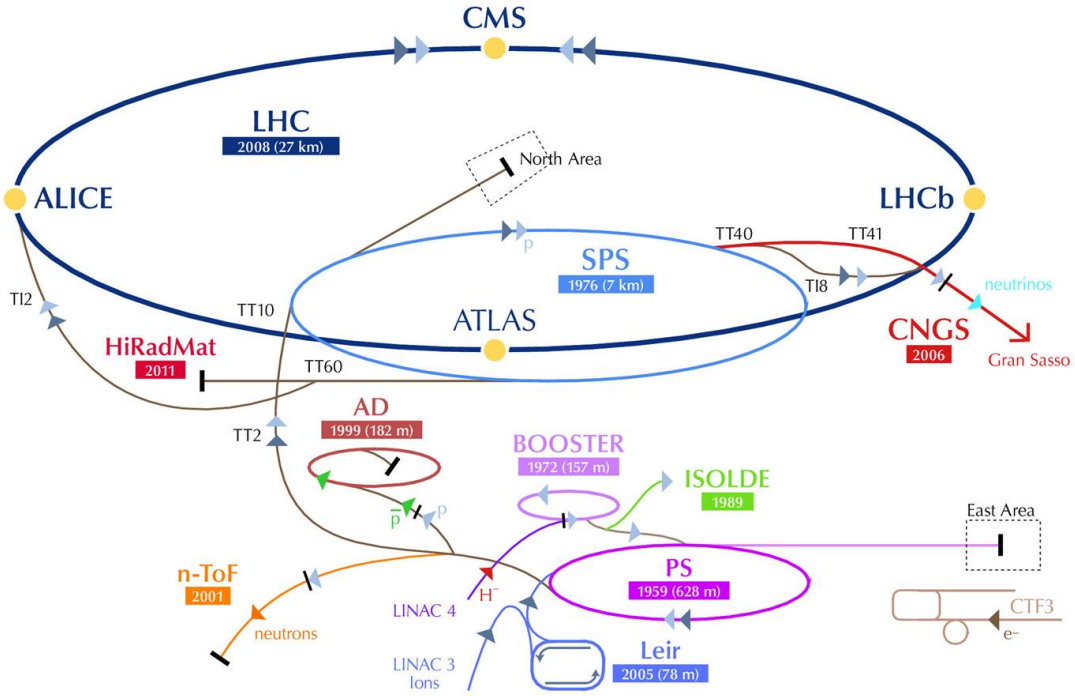

FIGURE 2.2: CERN accelerators complex

The beam collisions are studied by many experiments at different locations of the complex. In the LHC case, there are two multi-purposes detectors : ATLAS (A Toroidal LHC ApparatuS) and CMS (Compact Muon Solenoid). They both look for Higgs boson, extra dimensions and dark matter. In Figure 2.3 is represented the type of event registered with beam collisions.

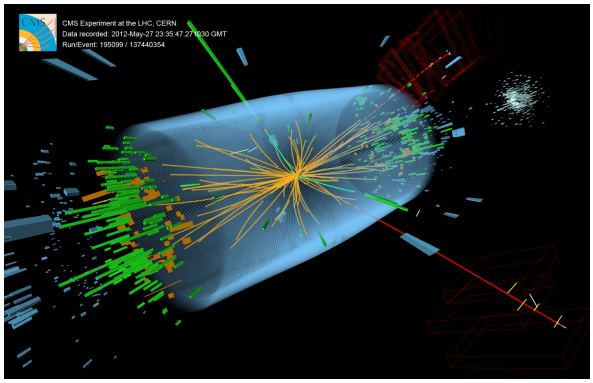

FIGURE 2.3: CMS Higgs Search - collision electrons/muons at 8 TeV

There are also specialized detectors like ALICE (A Large Ion Collider Experiment), studying heavy ions for quark-gluon plasma understanding and LHCb (LHC beauty), studying matter/antimatter through the quark beauty.

Apart LHC, there are many other experiments that use beam collisions : for instance COMPASS (Common Muon and Proton Apparatus for Structure and Spectroscopy), which looks into hadrons structure to study spin property. We can cite CLOUD (Cosmics Leaving Outdoor Droplet), which studies link between cosmic rays and cloud formation.

To finish, the Antiproton Decelerator (AD) is used for many experiments to study anti-matter, from earth gravitational acceleration measurement to cancer therapy suitability.

CERN is not only about high energy physics. It is pushing the technology frontier for supporting the research. The main example is the world wide web created at CERN to share physics data over the world (first website : http ://info.cern.ch/).

2.3 High energy linear colliders overview

The high energy lepton linear colliders are the most desirable high energy facilities after LHC era. The hadrons colliders such as the LHC are used at the energy frontier as discovery facilities. Conversely, leptons colliders are used for precision physics. Currently, two linear colliders are proposed : the ILC and the CLIC. The ILC is based on superconducting technology in the TeV range (0.5 TeV) whereas the CLIC is designed on a new two beams acceleration approach in the multi-TeV (3 TeV) range. The choice of the built machine will be based on one hand on their technological maturity and on the other hand on the requirements from physics results. Therefore, a close and fruitful collaboration is established between ILC and CLIC.

The last lepton collider at CERN was the Large Electron-Positron collider (LEP). This circular collider was energy-limited by the synchrotron radiation effect. This parasite radiation is proportional to the invert of the cubic mass of the particles. Consequently, light particles such as electrons and positrons induce bigger radiation than hadrons. Linear accelerators consequently avoid the synchrotron radiation. The main disadvantage of a linear collider is that the accelerating cavities are used only once, implying a much longer complex than a circular collider for equivalent energy.

2.3.1 CLIC overview

The CLIC is an international project with collaborations with more than 30 institutes around the world. The project is currently in a research and development phase. The next step is to deliver a technical design report (projected for 2016). The main issue is to demonstrate the feasibility of this extensive project, whether in term of cost, time or

technological challenges. Therefore, a test facility named CTF3 has been built for the feasibility study.

The CLIC aims to provide particles collisions at a center-of-mass energy of 3 TeV. The luminosity will be reached with powerful beam (14 MW for the main beam) and collision with extremely small dimensions (emittance of 1 nm on vertical plane). Because the accelerating structures are used only once per pulse, they are required to have a high gradient of *100 MV/m*. The CLIC project foresees to have only one interaction point (IP). At this area, a push-pull concept will allow to have two detectors in the same cavern, as similar to the ILC project (Figure 2.4).

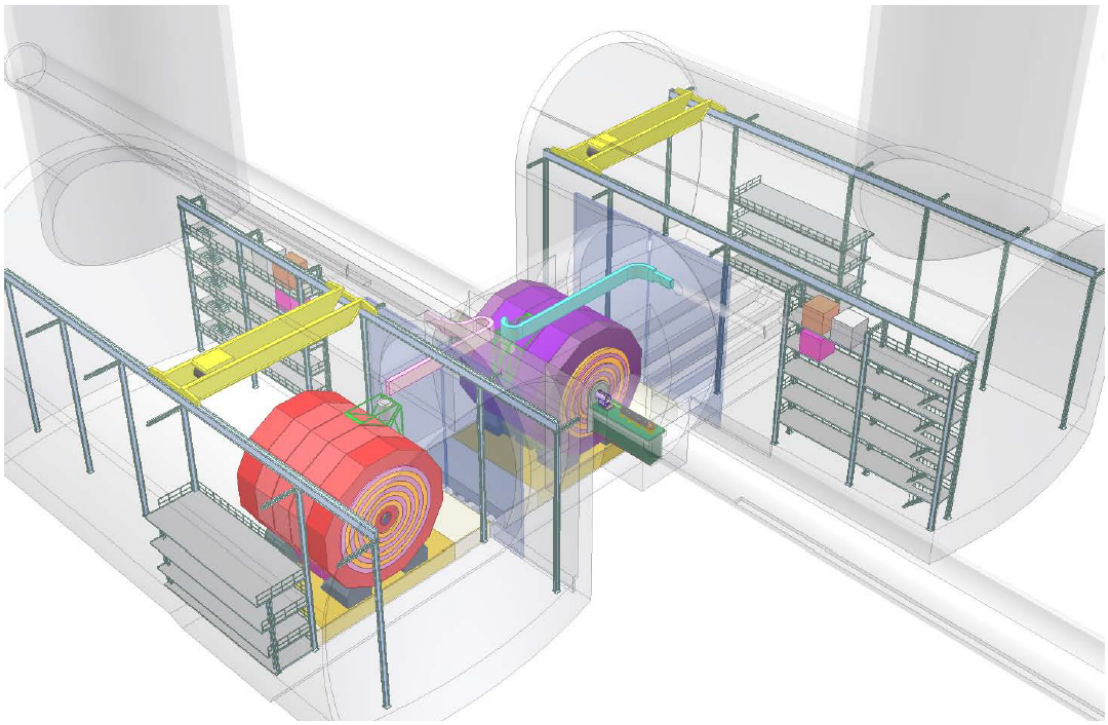

FIGURE 2.4: CLIC detectors push-pull scheme [1]

a. CLIC scheme overview

In this paragraph, a short explanation of the CLIC layout (Figure 2.5) is given.

Main beam complex : The injection complex is the source of particles. It generates 2.4 GeV electrons and positrons. The positrons are generated by shooting some electrons into a hybrid target.

The damping ring aims to reduce drastically the beam emittance. It has to generate the smallest emittance than ever achieved, 500 nm horizontally and 5 nm vertically.

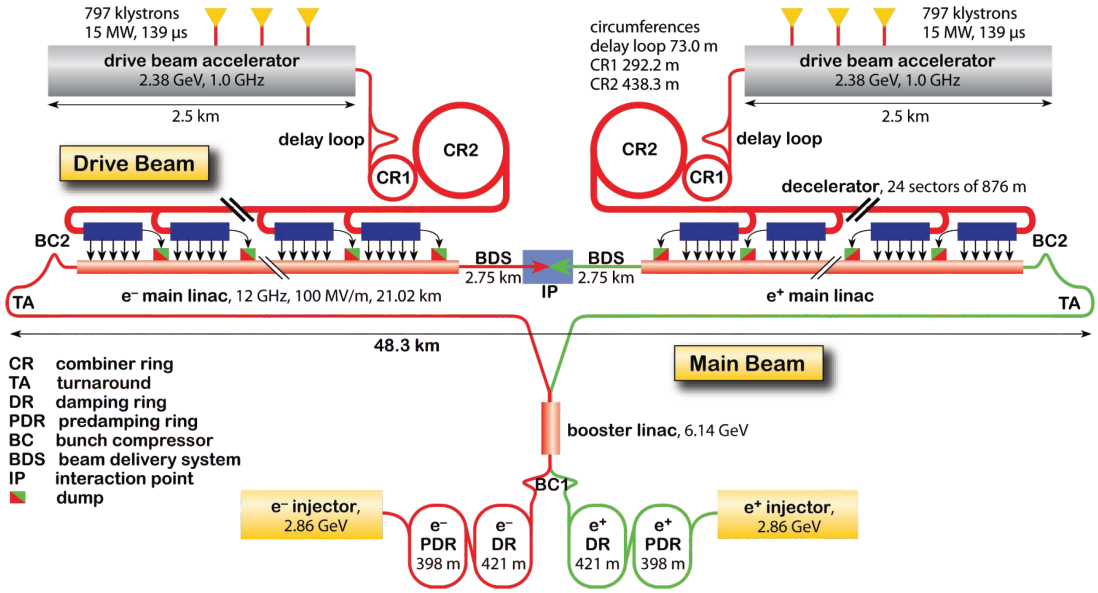

FIGURE 2.5: Schematic overview of the CLIC layout

The Ring To the Main Linac (RTML) aims to prepare the beam to the main linac injection. It is made up of a booster linac, which accelerates the beam at 9 GeV, a transfer line of 21 km, the turnaround, decreasing the emittance through synchrotron radiation and finally the bunch-compressor, delivering the beam to the main linac.

The main linac is a 21 km long accelerator where the main beam energy is increased from 9 GeV to 1.5 TeV. The beam delivery system aims to guide safely the 15 MW beam to the interaction point. At this point, a pair of detectors will be set. The post-collision beam will be then dumped by the beam dumping system.

Drive beam complex : The drive beam complex can be divided in three parts. The first part is where the electron trains are generated and then accelerated up to 2.38 GeV.

The second part is the compression stage. The beam will be compressed through a delay loop and two combiner rings, leading to the beam peak current of 100 A.

The third part is the decelerator stage. The drive beam is made up of 24 trains (after the combiner rings) and each one will go to one of the 24 deceleration areas (blue rectangles in Figure 2.5). At that point, the energy will be extracted from the drive beam to the main beam through several Power Extraction and Transfer Structure (PETS).

b. Feasibility Issue

Before validating the CLIC project, some critical points must be demonstrated as feasible. These feasibility issues [18] are listed hereafter.

The first challenge is the drive beam generation. This beam has to be generated with a 100 A stable intensity, with a 12 GHz bunch generation and a frequency multiplication factor of 24.

The second point is the drive beam Radio Frequency (RF) generation, more precisely, the PETS development. Its principle is to transmit RF power from a low-energy high-intensity beam (drive beam) to a low-intensity high-energy beam (main beam) which will be involved in collisions. This concept is represented in Figure 2.6.

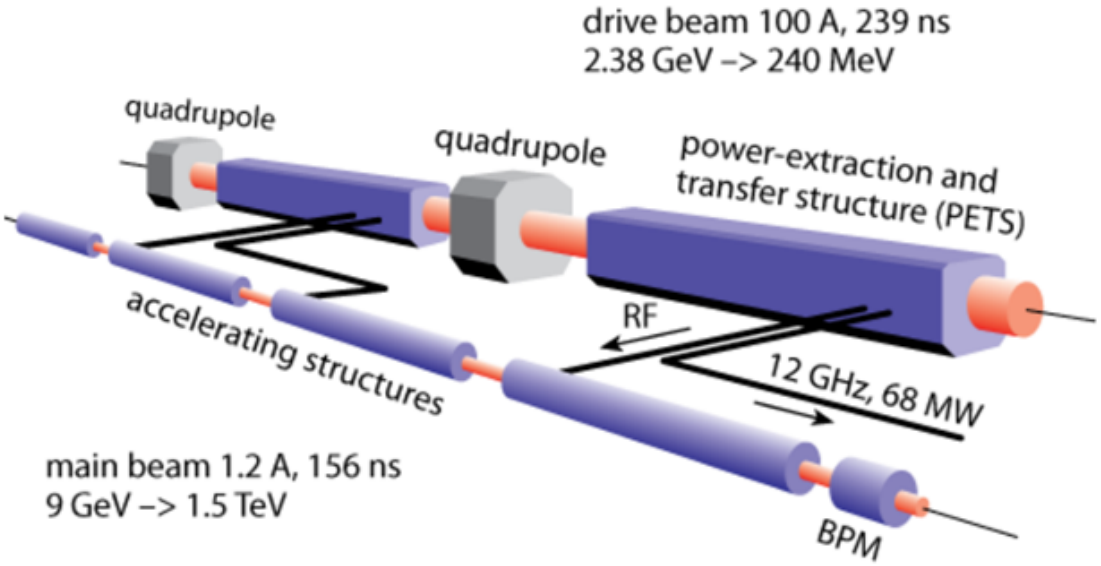

FIGURE 2.6: Illustration of two beam accelerating scheme

The third challenge is the high gradient of accelerating structures (100 MV/m). This parameter must be reached with a RF efficiency of 27% and a breakdown rate lower than $3.10^{-7}.m^{-1}$.

As said before, one of the CLIC novel approaches is the two beams acceleration scheme. This concept has to be demonstrated in compact module, including all technical subsystems such as RF and vacuum. It has to send the RF energy from the drive beam to the main beam with a pulse length of 170 ns. This operation involves a high beam to beam stability (accuracy of 0.07 ps).

A fifth point is the ultra low beam emittance. This parameter is a mandatory condition for high luminosity. The CLIC system has to be able to generate ultra low emittance and to preserve it to reach the expected beam size at the interaction point.

Another challenge is the alignment and the stabilization system. The CLIC needs a 15 μm alignment accuracy, and a vertical displacement lower than 1.5 nm above 1 Hz vibrations.

At least but not the last, the feasibility of the machine operation and the machine protection has to be demonstrated.

c. CLIC operational scenario

The safe operation of the CLIC requires testing each system before starting physics experiments. Thence, an operational scenario has been proposed [19]. It allows to test gradually and safely each system of the two beams trajectory. A beam is considered safe when its energy is under the yield limit in copper (62 J/g).

Main Beam operational scenario The nominal main beam is above safe condition by 4 orders of magnitude. In order to ramp up safely the beam, the strategy is to reduce its luminosity. A first decrease can be done by reducing the number of bunches. A second cut is realizable by reducing the current per bunch. Finally, the last reduction comes from the beam size growing (emittance).

The operational scenario consists to send a safe beam. Then, the aim is to cancel progressively the luminosity reduction explained above as long as the protection systems allow it, to finally reach the nominal main beam.

Drive Beam operational scenario The drive beam is above the safe condition by a factor of 100. A safe drive beam can be generated by reducing the charge density (less particles).

The operational scenario is to increase the charge density step by step as long as the protection systems allow it.

2.3.2 ILC overview

The ILC is a worldwide international collaboration of 300 institutes. Its global design effort, mandated by the International Committee for Future Accelerators (ICFA)), has led to deliver the *reference* design report in 2007. At that point, high risk challenges have been identified and the research and development on them has led to release the *technical* design report in June 2013.

The ILC is a electron-positron collider of 31 km length. It is based on 15000 SuperConductive Radio Frequency (SCRF) cavities expected to deliver an accelerating gradient of 31.5 MV/m. The particles are accelerated with two linacs to have a collision energy of 0.5 TeV. It is foreseen to have a staged construction, thus starting the collision energy at 0.3 TeV and extensible up to 1 TeV. The collision events will be recorded with two detectors at the interaction region. The *push-pull* mode will be used.

a. Physics goals

The purpose of the ILC is to take up several physics challenges. First of it, the study of the Higgs boson and associated particles will start at 125 GeV, the collision energy where it must appear (Figure 2.7). The high precision measurements of the rates of the decay of the Higgs boson will be achieved because lepton colliders have less background events than hadron colliders. Moreover, this study will be completed at others energy (250 and 500 GeV) and by the determination of the Higgs boson self-interaction. One of the question of interest is to determine if the Higgs field is the only one to create mass or if there are additional particles which may contribute.

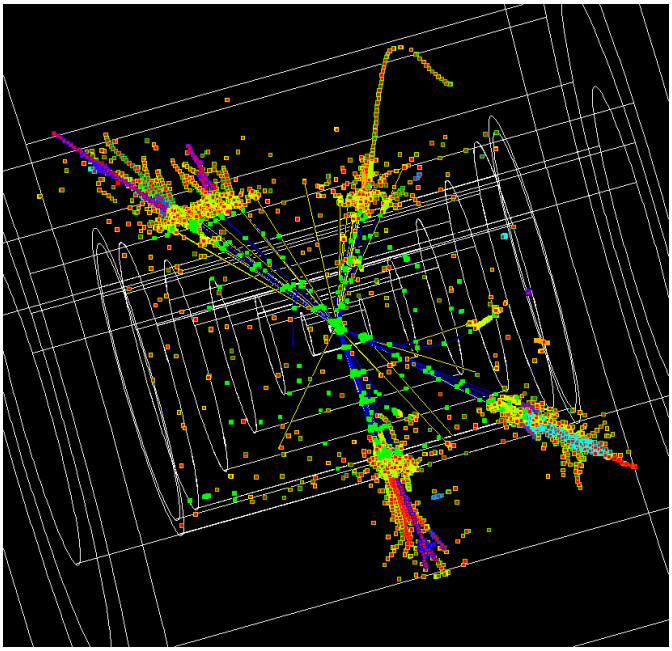

FIGURE 2.7: Simulation of a Higgs decay at ILC detector (courtesy to Norman Graf)

The second challenge that would be undertaken by the ILC is the study of the Supersymmetry. Regarding this theory, it is needed to have a matter-type Higgs particles. The ILC will search for them and measure their properties (quantum numbers and couplings).

A third major challenge to be noticed is the study of new interactions for pair production. It will be focused on W boson and top quark. Moreover the mass of the top quark will be precisely measured. Indeed, this quark is the heaviest fundamental particle in the standard model and may help to understand the Higgs field.

b. ILC scheme overview

In this paragraph, a short overview of the ILC layout (Figure 2.8) will be explained. From the particle sources Interaction Region, the ILC machine is divided in several parts.

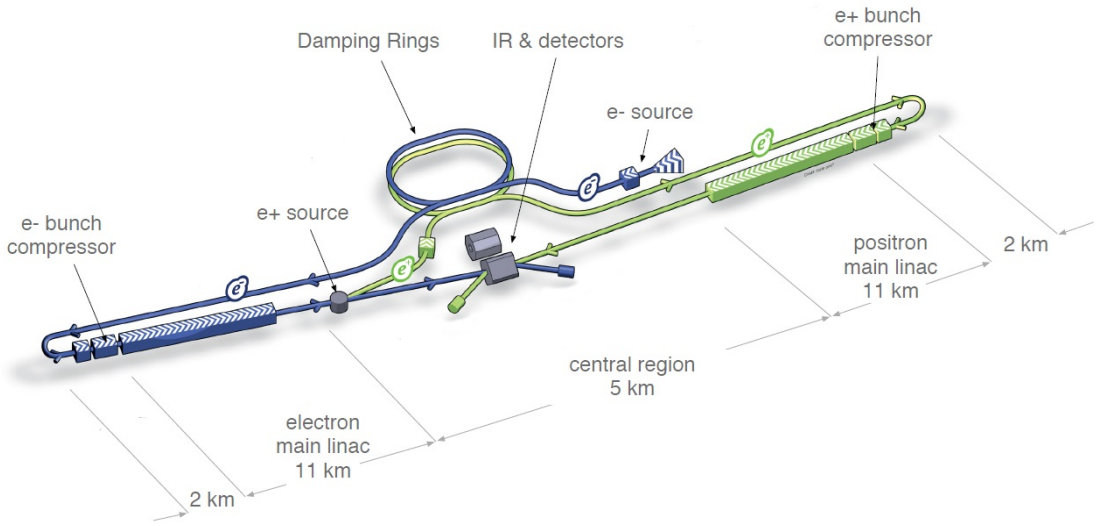

FIGURE 2.8: Schematic overview of the ILC layout [2]

The electrons are generated with a laser/photocathode interaction in a DC gun. Some structures are then bunching and pre-accelerating the particles.

The positrons are generated with the electron beam. The accelerated beam is sent to undulators which generate photons. These photons are then sent to a titanium-alloy target, thus generating electron-positron pairs. A capture system extract the positrons which are then bunched and pre-accelerated.

The next machine parts for both types of particle are the damping rings. They aim to reduce the emittance. They must achieve a vertical emittance of 20 nm (five order of magnitude) and have to deal with beam compression and decompression (factor 90).

The two main linacs accelerate particles from 15 GeV to 250 GeV. It is done with 7400 SCRF cavities. Working at 1.3 GHz, they shall deliver an accelerating gradient of 31.5 MV/m with a spread of +/-20%, useful for physics events variation. The RF power comes from klystrons, each of them generating 10 MW. The klystrons repartition is balanced

between to schemes : either a distributed scheme all along the collider or a cluster scheme where klystrons would be gathered at strategic points. The choice mainly depends of the machine location ground topology. As shown in Figure 2.9, the cavities are gathered in a cryomodule to cool them down at 2 K.

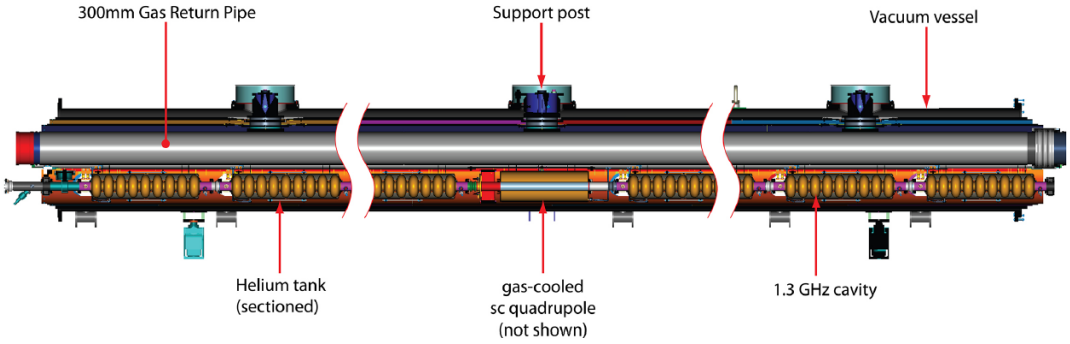

FIGURE 2.9: Schematic the ILC cryomodule [2]

At the interaction region, the particles will collide. To perform the physics measurements, two detectors are foreseen : the Silicon Detector (SiD) and the International Large Detector (ILD), represented in Figure 2.10.

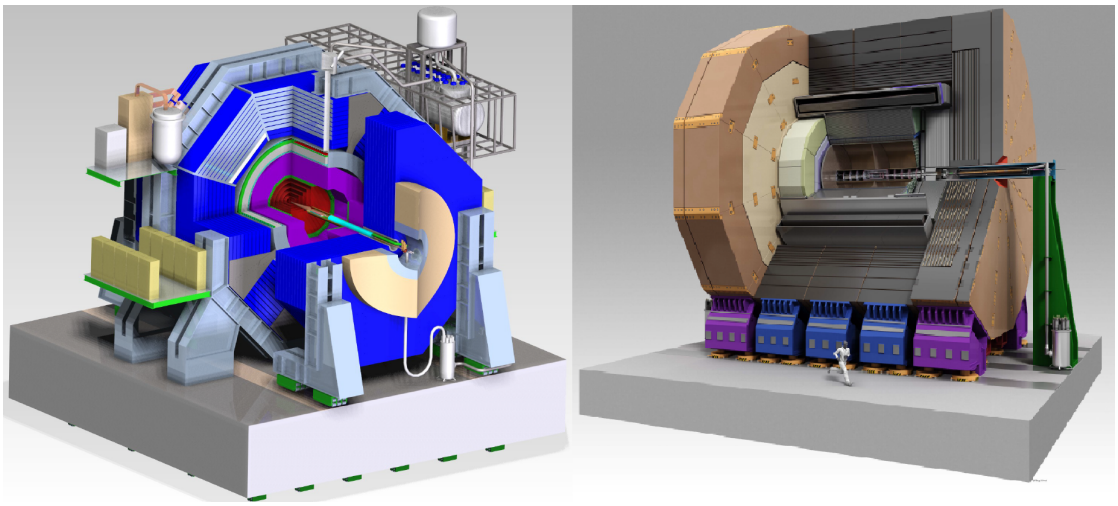

FIGURE 2.10: ILC Detectors - SiD (left) and ILD (right) [2]

Both detectors have a high resolution for events reconstruction through the newly developed particle flow algorithm.

To maximize the detector efficiency, power pulsing have been implemented (switching-off part of equipment between particles trains). Thus, it reduces the heat load and the cooling system, resulting in less *dead* space.

These two detectors will be used at the same interaction region with a push-pull scheme. In order to optimize the ILC integrated luminosity, the swapping operation will take less

than 1 day. While one detector is probing physics events, the other one in is maintenance. The goal is to have two independent, complementary and competitive detectors to find new physics results.

They are based on a combination of tracking systems and electromagnetic and hadrons calorimetry in an intense magnetic field (5 T for SiD and 3.5 T for ILD). On one side, the SiD is designed as *compact*, thus enabling higher granularity of calorimeters detectors. On the other side, the ILD is larger to enable a better particle separation [23].

c. Main R & D effort

During the Technical Design Phase, the main research and development efforts have been focused on the SCRF cavities. The goal has been to achieve these cavities with a gradient of 35 MV/m in a reproducible way. The first step has been to study the limitations, among them, the field emission quench causing surface effect. The next step has been to establish a fabrication process to reach the required gradient and a production yield of 90%. As many institutes have been involved in this research effort, an extra challenge have been to ensure the plug compatibility (integration test) of the different cryomodule. In order to be ready for the mass production, several companies have been enabled to produce cavities compliant with ILC requirements through technology transfer.

2.3.3 CLIC and ILC parameters comparison

In Table 2.1 are listed the main parameters for ILC (500 GeV design) and CLIC (main beam). From interlock system point of view, there are several differences to note. First, the repetition rate has a difference one order of magnitude between the two machines. Performing inter-pulse analysis in ILC would be easier in term of response time constraint. A second difference is the site length which would act in a non-negligible way on the response time for the signal transmission.

2.4 CLIC Machine protection overview

On high energy accelerator projects such as the CLIC, the machine protection is a vital part. The mandate of the machine protection study is to protect various CLIC components from damage which could be caused by uncontrolled energy release (from beam and/or equipments). Its mission is to reduce risk to a tolerable level. A risk is tolerable when the sum of their financial impacts and operational downtime impacts are lower than a few percent of the whole budget and machine availability expectation.

Table 2.1: ILC and CLIC parameters comparison

Parameters	**Unit**	**CLIC**	**ILC**
Center-of-mass energy	TeV	3	0.5
Main Linac RF frequency	GHz	12	1.3
Luminosity	$10^{34}.cm^{-2}.s^{-1}$	5.9	1.8
Luminosity (in 1% of energy)	$10^{34}.cm^{-2}.s^{-1}$	2	1.04
Linac repetition rate	Hz	50	5
No. of particles / bunch	10^9	3.72	20
No. of bunches / pulse		312	1312
Bunch separation	ns	0.5	554
Bunch train length	μs	0.156	300
Beam power	MW	14	18
linac gradient	MV/m	100	31.5
Overall two linacs length	km	42.16	22
Total beam delivery length	km	2 x 2.75	2 x 2.25
Proposed site length	km	48.4	30.5
Total site AC power	MW	582	163
Horizontal emittance	μm	0.66	10
Vertical emittance	nm	20	35

Hereunder are described the failures types and the protection strategies planned. In a second part will be described summarily the machine protection systems.

2.4.1 Failures type and protection strategies

We could separate the CLIC failures in three categories :

Fast failures The time scale of these failures is the same than the beam flight in the accelerator complex. After a certain point, the beam cannot be stopped because of beam travelling at speed of light. The main fast failures come from RF breakdown or kicker misfiring which may send the beam out of its trajectory. Also, it could come from RF klystron trip which could disrupt the beam and involve large losses.

The machine protection strategy against fast failure is based on passive protection.

Inter-cycle failures These failures occur during the time between two pulses, i.e., 20 ms. This type of error could be caused by any sub-systems of the accelerator complex

affecting directly or indirectly the beam safety : for example, power supply, positioning system, vacuum pump.

The machine protection strategy against inter-cycle failure is based on two points : first, an Interlock System which would protect the machine during the first 18 ms. Secondly, a *safe by construction* principle would be applied on sub-systems for the remaining 2 ms.

Slow failures These failures are slower than CLIC repetition rate (50 Hz). They could come from temperature or alignment drifts or from the beam feedback saturation (which is supposed to control drifts).

The machine protection strategy against slow failure is based on the *post-pulse analysis*.

2.4.2 Machine Protection Systems

The CLIC Machine Protection is revolved around 4 main systems described below. Each system is designed for a specific time scale.

Static protections The static protections are passive elements integrated such as collimators and spoilers. There are mostly associated with kickers and are located at extraction points (damping rings, combiner rings and turnaround). They have to be able to withstand the whole pulse.

Real time machine protection Some fast machine protection systems could be developed on a case basis. A real time system will be able to dump (at least partially) an unsafe beam in flight. This can be done through two principles. First, if the beam trajectory is not linear : An unsafe parameter (e.g. beam losses) will be detected and the beam will be stopped by taking a more direct path. The most obvious examples are the rings (damping and combiner rings) and the turnaround. Secondly, if the beam is not going at speed of light : An unsafe parameter will be detected and the beam source will be inhibited. The most obvious example is the drive beam linac.

Interlock System and post-pulse analysis It is the central topic of this thesis and are described longer in section 2.5

***Safe by construction* principle** As the CLIC Interlock system cannot protect the machine at the last moment before the next pulse (because of its response time), this

principle has been set to support this *blind period*. The *safe by construction* principle establishes that CLIC active equipment have to remain within their tolerance for 2 ms when they start to fail. A preliminary study gives an equipment inertia requirement of T > 20 ms. Thus, with this principle, the fault does not affect dangerously the beam in flight and will be caught by the Interlock System during the next inter-cycle (before next pulse).

2.5 CLIC Interlock system and thesis problematic

The CLIC Interlock System is based on two concepts : the beam permit and the post-pulse analysis. They are intended to protect a failure type : inter-cycle for beam permit and slow failures for both concepts .

2.5.1 Beam Permit

The *beam permit* concept is the backbone of the CLIC Interlock System. It is inspired by the LHC Beam Interlock System [5].

The *beam permit* has two states : a PASS decision is authorizing the next pulse operation and a VETO decision is inhibiting next pulses operation. This beam permit is a AND-combination of the local interlock requests. The local interlock requests are received by local nodes (referred later as slave nodes), geographically distributed over the machine. The combination of these local interlock requests to the beam permit is assured by the beam permit loop.

This concept is intended to protect critical equipment failures between two pulses (inter-cycle) and may be used by the post-pulse analysis for slow failures.

This beam permit concept is represented in Figure 2.11 and is explained in deeper detail in the design proposal chapter (cf. A.).

2.5.2 Post-pulse analysis

In linear collider case, once the beam is in the pipe, it is impossible to stop it on a failure detection. Consequently the novel concept of post-pulse analysis has been introduced. The goal is to have a strong confidence for the next pulse stability. Thus, the post-pulse analysis aims to check the last pulse quality. In case of bad quality, the next pulse will be inhibited via the beam permit previously mentioned.

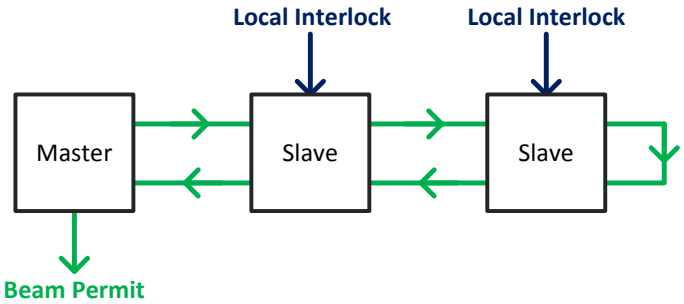

FIGURE 2.11: Beam permit concept

This concept is intended to protect again slow failures with a time scale larger than the machine cycle period, such as alignment drift.

The main systems to be scrutinized on are the Beam Loss Monitors (BLMs) which are the line of last defence for detecting beam failures.

2.5.3 Thesis problematic definition

The thesis presents the **design** of a **dependable** interlock system for **linear colliders**.

Design A previous thesis named *A Beam Interlock System for CERN High Energy Accelerators* [5] has been performed in 2006. It presents the work to design the LHC Beam Interlock System, starting from the prototype systems and finishing with the operating interlock system.

My thesis works are complementary as it is explains the work from the concepts to prototype systems. Endorsing the IEEE 1220 system life cycle terminology (Figure 2.12), my thesis presents the work starting from system definition to the preliminary design.

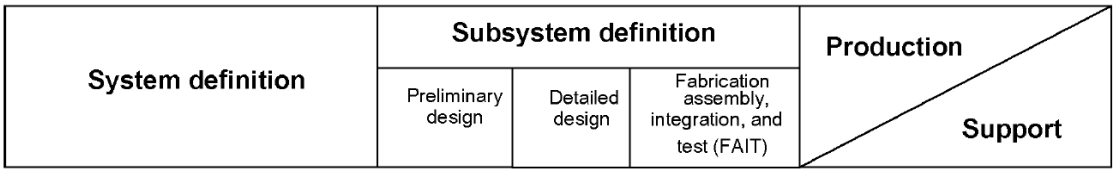

FIGURE 2.12: Typical system life cycle [3]

Dependable The dependability is the main characteristic an interlock system must fulfil. A lots of studies have been performed to evaluate dependability properties of existing interlock systems [24], [25] but few of them at the design phase. The aim of the thesis is to establish them at the design phase, and give a generic methodology to do so.

Linar collider As described previously, the thesis has been performed as part of the CLIC project, with one concept applicable to linear colliders (post-pulse analysis).

2.6 Introduction to interlock systems

This section introduce interlock systems in the field of particle accelerator in a generic way.

The starting point is the need of machine protection : building more and more powerful machines has raised the hazard level because of possibility of uncontrolled energy release, mainly from beam and equipment. Thus, interlock system have been introduced to prevent the damage resulting from these unwanted events.

The focus is done on interlock systems preventing beam hazard. Indeed, equipment interlocks (such as [26] or [27]) are case-specific and may have only the interlocking function as a common basis. In addition, interlock systems deals with machine safety and are usually decoupled with personal safety.

As part of machine protection, interlock systems share common goals. The next points describe the functions and the requirements that interlock systems may have in common, without machine specificity.

2.6.1 Protect the machine - Beam Interlock Function

To prevent the machine from beam damage, the interlock systems are using their main function : stopping beam operation (e.g. [20]) or reducing pulse frequency (e.g. [6]). To detect when the operation is unsafe (i.e., when to stop the beam), the systems get as input monitoring data on equipment that can affect the beam stability (such as power converter or magnets) and monitoring data on equipment probing the beam stability (such as beam position monitors or beam loss monitors).

The core function of interlock systems is to gather critical information and to synthesize them in a permit, affecting the beam operation.

This permit is then released to output devices (such as source gun or extraction/injection/dumping kickers). These outputs will stop beam operation in consistence with the permit state.

The effect of this permit is fundamentally different between circular and linear colliders. For the latter, the permit is able to act only on the next pulse because the speed of

beam is close to the speed of light. In the ring machines, the beam permit will act on the circulating beam and/or the injection of new beams.

2.6.2 High dependability requirements

Failures of interlock systems can have two types of impact : machine damage and/or a decrease of machine availability. Consequently, the interlock systems have stringent dependability requirements, mainly in terms of reliability and availability. Hereunder are listed different ways used to reach these objectives :

Fail-safe design A fail-safe design ensures system failures to lead to safe failures : in interlock systems case, to stop the machine is safer than let it run without safe conditions or the protection system being blind ([11], p.26).

Redundancy One of the most powerful mechanism in order to have a high dependable system is the use of redundancy [28]. The point is to duplicate the system and add a well-designed voting system. Thus, a single element of redundant system has less stringent requirements and the system is more easily designable.

Test and Monitoring Failure rates are usually established considering an interlock system as good as new. To ensure this state, monitoring is required.

Two types of monitoring can be distinguished : on one side, live monitoring ensures proper condition of the system while operating and shows up warning for the next technical stop (e.g. a redundant power supply failure). On the other side, monitoring while not operating can allow more advanced tests and therefore check all functions, especially the barely used. It implies to implement the concept of testability in the early step of the design phase. Finally, knowledge about Mean Time Between Failures (MTBF) of single components allows preventive maintenance.

Flexibility To ensure high availability, interlock systems need to be configurable to improve its flexibility. Indeed, special cases (such as test mode, safe beam mode or special accelerator structure configuration) may require an interlock system to behave differently than initially foreseen (e.g. masking inputs).

2.6.3 Common design

Based on several interlock systems [20], [6], [29], [30], it is possible to describe a generic interlock system :

In a general way, an interlock system is a distributed hardware system. It may be based on Field Programmable Gate Array (FPGA) or Programmable Logic Controller (PLC). The most common architecture is a tree layout but can also be implemented with a circular and/or daisy-chained layout. It usually has a master unit delivering the final beam permit. The data transmission between different modules (e.g., between slave and master modules) requires high speed capacity, noise and radiation immunity. These communication links are often implemented with optical fibres.

Although interlock systems are specific to the machine they are protecting, they usually share the same subsystems. The figure 2.13 gives an systemic overview of a generic interlock system. these subsystems are hereunder described :

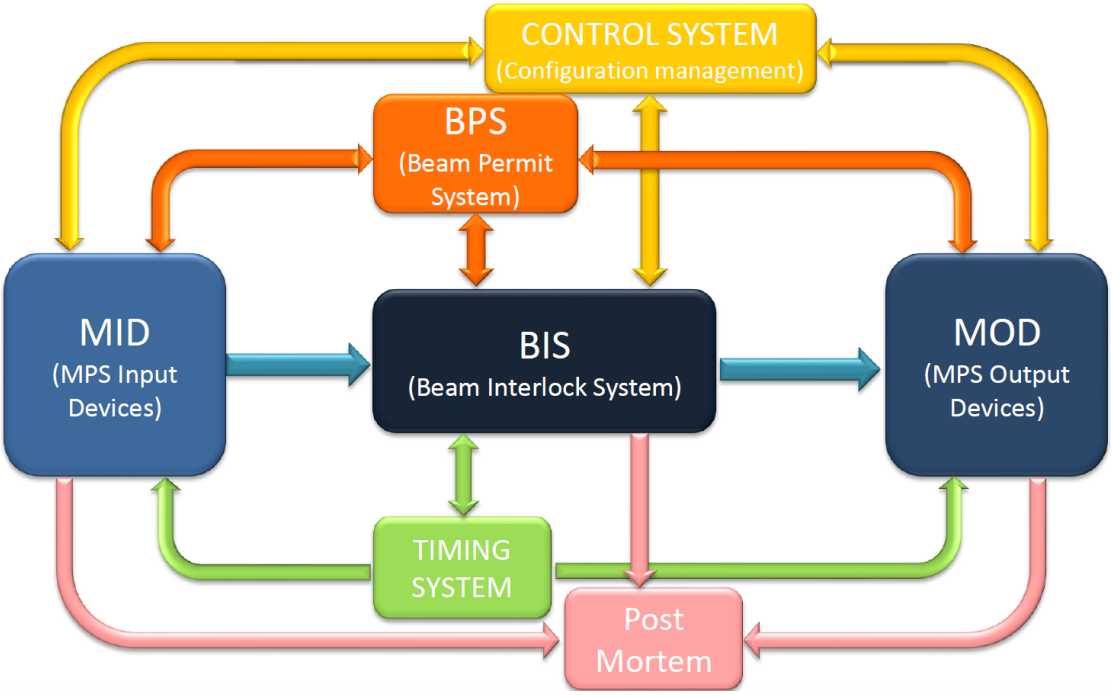

FIGURE 2.13: Generic Interlock System overview [4]

Control system : It is responsible for configuration, update and is usually managed by expert only. It also implements the test and monitoring part.

Timing system : Interlock systems must work in synergy with other machine subsystems and the beam timing. Beam timing is especially crucial for linear colliders. In a less critical way, it is also used to time stamp the data for monitoring purpose.

Post-mortem : In addition to the interlock function, the interlock systems must provide or help to provide evidence when an interlock occurs. It can be done either integrating a post-mortem's like system [31] or providing information (such as time-stamped interlock request data) to this type of analysis system.

Interfaced devices : Interlock systems are interfaced with other systems. A crucial point is the question of the responsibility at the interface. A poor performance from interfaced systems will decrease the interlock function quality. To keep a high dependability level, the boundaries of the interlock systems must be clearly defined. In addition, expectations from interlock systems to interfaced systems, in term of dependability requirements, must be provided.

2.7 Selected protection systems

In this part, the goal is to give an overview of the current level of development in the interlock system field. The selected examples are either interlock systems or protection mechanisms which are strongly linked with CLIC Interlock System. The LHC Beam Interlock System constitutes the main reference work of this thesis.

2.7.1 LHC Beam Interlock System

The LHC is a machine running at high energy, with beam energy higher than 360MJ. It therefore generates beam hazard. Thus, there is a need of protection again uncontrolled beam losses. A Beam Interlock System (BIS) has been designed to prevent part of beam failures [20].

The principle of LHC BIS is to stop beam operation as soon as an unsafe beam state is detected. Beam operation is stopped by extracting the circulating beam (via the dumping beam system) and by inhibiting the beam injection. The beam state detection is based on failures of critical systems and high beam losses detection.

The response time is a stringent requirement and is conditioned by the type of failure and the accelerator architecture. As illustrated in Figure 2.14, the BIS has to transmit information from users interfaces anywhere in the LHC until the beam dumping system within 100 μs.

The dependability is one of the higher requirement. The LHC BIS has been specified to reach Safety Integrity Level (SIL) level 3. This can be translated into a mean time between unsafe failures between 100 and 1000 years.

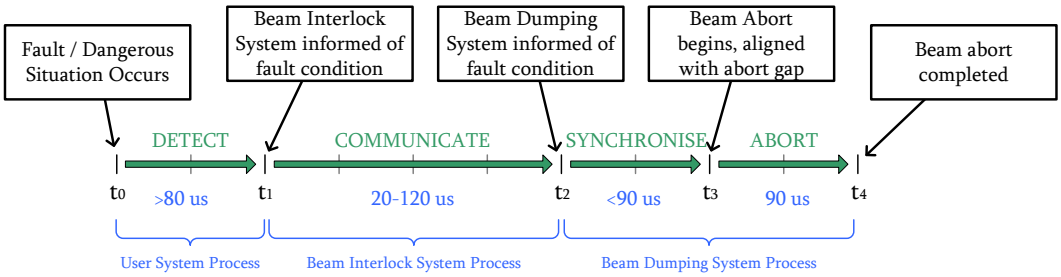

FIGURE 2.14: LHC BIS response time requirement [5]

To cover the full LHC, the LHC BIS uses 140 interfaces with critical equipment. These interfaces are connected to 16 nodes. The actuator used to extract the beam from the LHC is the beam dumping system. The actuators used to inhibit beam injections are the injection kickers. The LHC BIS uses a redundant beam permit loop : it is a 10 MHz square wave signal transmitted clockwise and anticlockwise through optic fibres. Each node can open the loops. The lack of this loop signal leads to interlock. The LHC BIS architecture is represented on Figure 2.15.

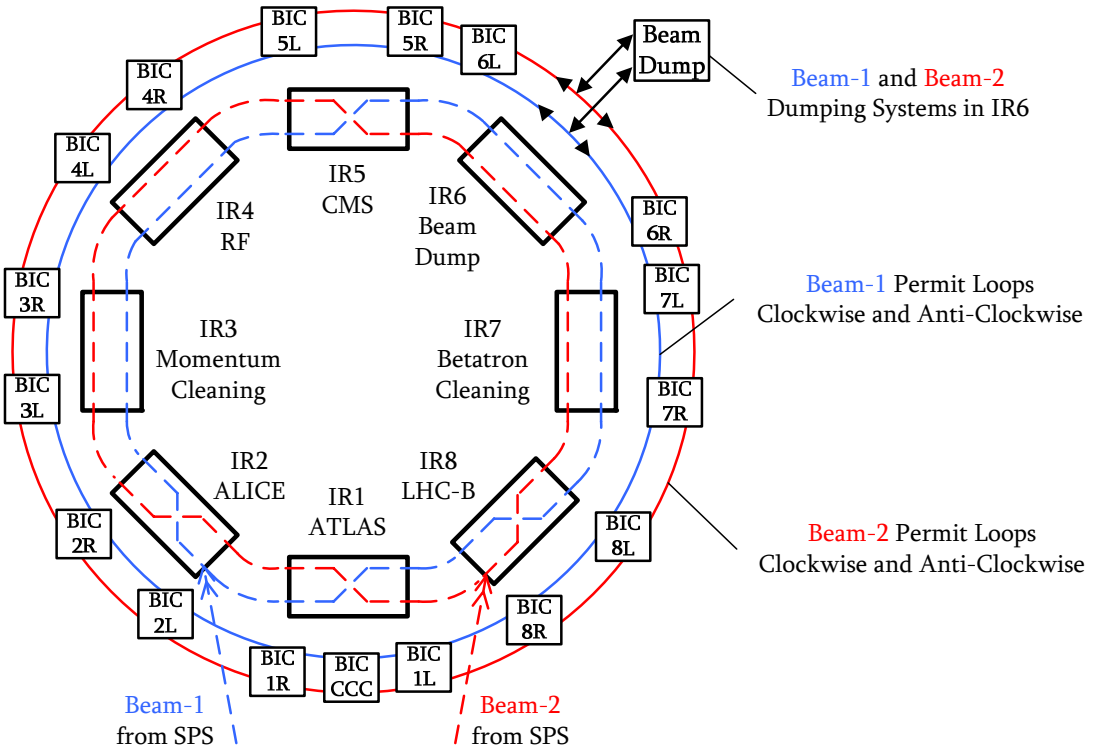

FIGURE 2.15: LHC BIS architecture

The nodes are the main components of the BIS. Their core function is to perform an AND operation of the user permit inputs and allow (or not) propagation of the beam permit loop signal. It is performed by the critical manager board. The other part of the

node is dedicated to live-monitoring and testing. It is performed by a different hardware board, keeping the critical and non-critical part separated. In order to provide evidence, a history buffer is implemented, allowing analysing events before an interlock trigger. A synoptic view of the node is showed on Figure 2.16.

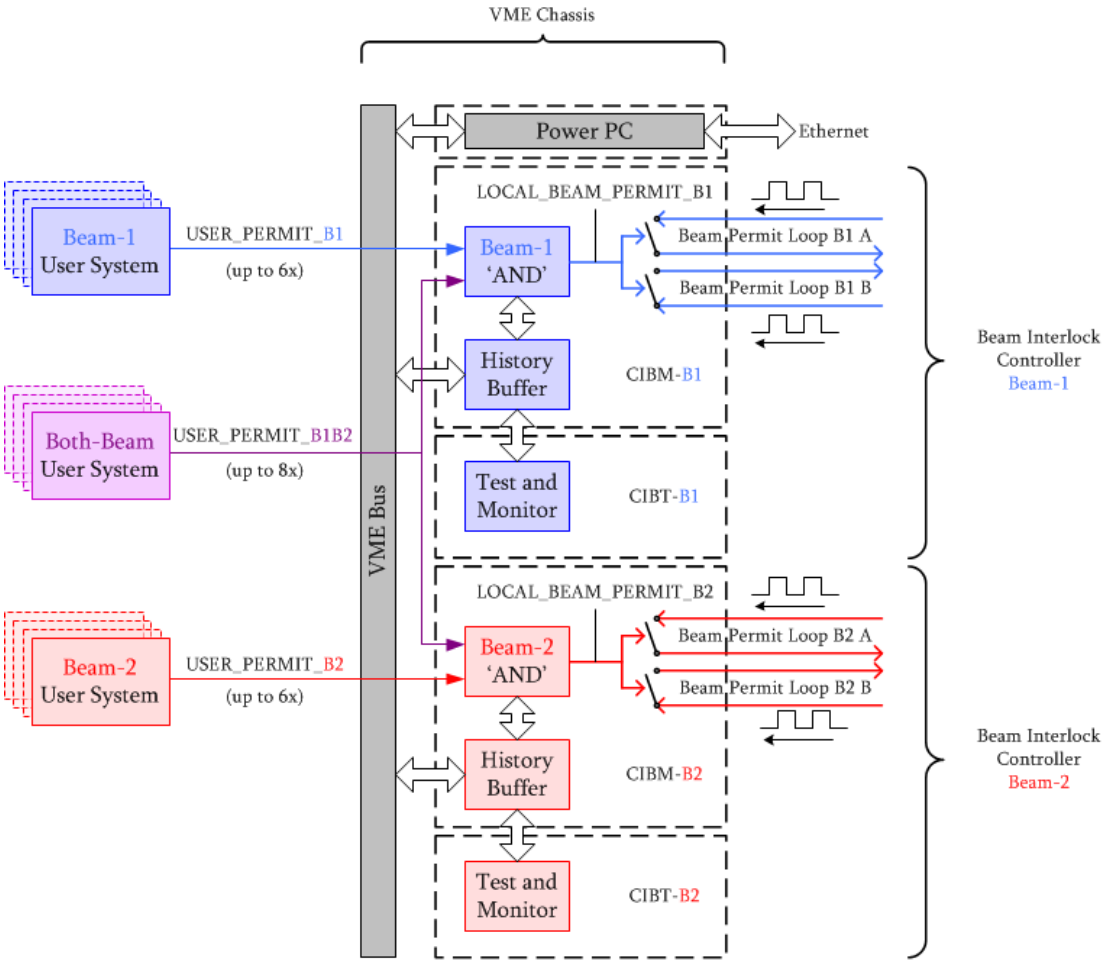

FIGURE 2.16: LHC BIS Node synoptic view

2.7.2 Linac Coherent Light Source Interlock System

The Linac Coherent Light Source (LCLS) is a 2.5 km long linear accelerator, generating highly bright X-rays pulses to probe at the atomic scale.

An interlock system has been designed for the LCLS [6]. It is the main part of its machine protection. It shuts off the beam or reduces its repetition rate regarding the failure severity. To do so, the inputs are signals from beam loss and beam position monitors, among others. At the end, it has about one hundred of interlock request inputs. Concerning the outputs, it has direct access to mitigation devices (such as pulsed kicker magnet or mechanical shutter) to change the machine operation.

There is to note it processes fault data every 2.78 ms, while beam operation is 120 Hz. It accepts both digital and analogue inputs. An interesting fact is the threshold comparison performed on analogue value (to translate them into failures detection).

The interlock system is organized as a tree topology, as shown on figure 2.17. The slave nodes (a.k.a. link nodes) are able to have different configurations, thus adding flexibility to the whole system.

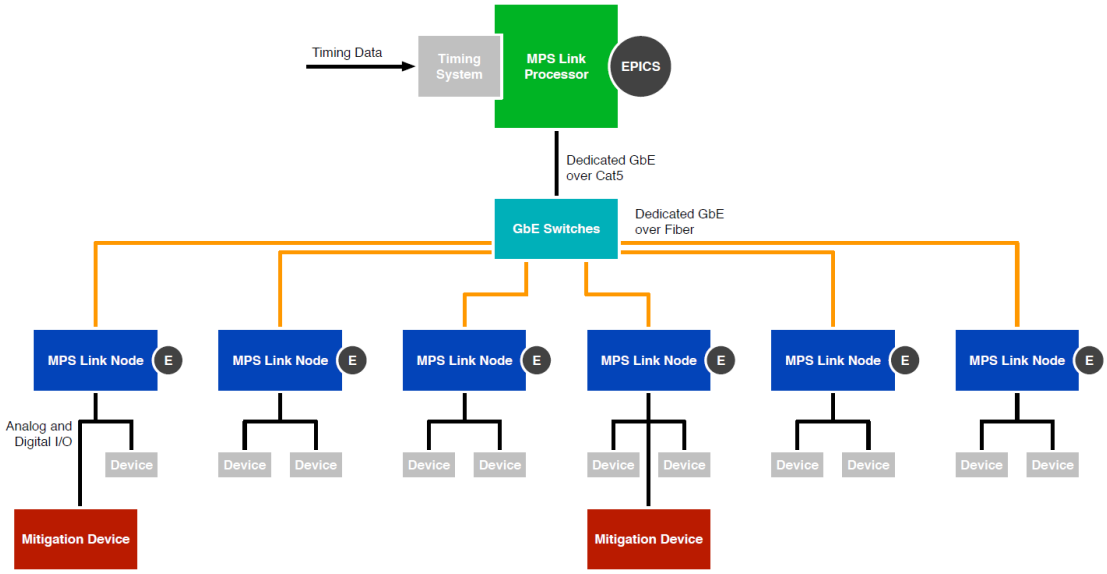

FIGURE 2.17: LCLS Interlock System Architecture [6]

The last point is about the technology : it is a FPGA based system. The critical links between master and slave nodes are made with dedicated gigabit ethernet.

2.7.3 Linac 4 watchdog

the *Linac 4* is a 160 MeV linear accelerator starting the injection complex of the LHC (cf. Figure 2.2). One of its protection strategy is to use an interlock system. It is based on the same hardware as for the LHC but differently configured. As the LHC Interlock System has been already described, this part is focused on one protection mechanism, the watchdog, which is used as an input of the interlock system. The interesting part is the threshold comparison and the post-pulse losses evaluation.

The principle of the Linac 4 watchdog [32] is to compare beam transmission (in number of charges) at different point of the Linac through beam current transformers. An illustration of this implementation is showed on figure 2.18

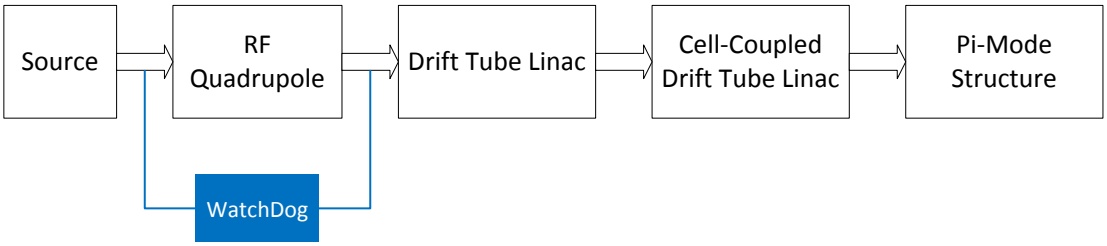

FIGURE 2.18: Linac 4 Watchdog implementation example

These comparisons will permit to detect excessive losses. Each comparison will be an input of the Linac 4 BIS, which will trigger an interlock as soon as one of its input fall down to FALSE state and thus shut off the Linac beam.

For the Linac 4 watchdog, each comparison result (TRUE or FALSE) is configurable by the user following these points :

1. The definition of good pulse is defined through a threshold (above is good, below is bad pulse).
2. A bad-pulse counter is set at its maximum value (maximum value is defined by the user).

On each good pulse, the bad-pulse counter is incremented until its maximum value. On each bad pulse, this counter is decreased. Whenever the counter reaches zero, the watchdog will trigger the comparison result from TRUE to FALSE, leading to an interlock (through BIS). After a TRUE to FALSE transition, the watchdog has to be reset manually (latching mechanism) to restart Linac 4 beam operation.

The technology choice is a hardware FPGA-based solution with an acquisition chain to collect beam current transformer signals. The main reasons of this choice are the reliability and the reaction time offered by this technology. A pure software based watchdog solution would have led to higher operational flexibility. To reach an equivalent flexibility level, the designed system is implementing a software based superstructure in synergy with the hardware structure.

2.7.4 Real-time and post-pulse beam quality assessment for LHC beams

A novel concept for the CLIC Interlock System is the post-pulse analysis, strongly linked to beam quality. Beam quality analysis is also performed for LHC beams. Two solutions have been designed : the *beam quality monitor* in the SPS [33] and the *injection quality check* for the beam transmission between the SPS and the LHC [34].

a. Beam quality definition

In this framework, beam quality is defined in terms of :

- Small emittance
- Uniform bunch intensities (< +/- 10 %)
- Equal beam intensities for both beam (clockwise and anticlockwise beams)
- Low tail population
- Satellite population reasonable
- Low losses

b. Beam quality monitor at the SPS

This is the real time beam quality check. It checks the longitudinal quality of beam in the SPS. It is based on wall current monitor beam time-profile. The system dumps the beam in case of bad quality. The analysis speed is 10 ms of data acquisition and 10 ms of data analysis. The last check is performed 20 ms before the SPS extraction (i.e. LHC injection).

c. injection quality check at the LHC

This is the post-pulse (or post-injection) beam quality check. It inhibits the next injection in case of bad injection. It is based on many beam observation systems (beam loss monitors, beam position monitors, injection kickers, RF phase error). It is a JAVA application using both post-mortem and monitoring framework. The analysis takes up to 8 s. It is mainly used in synergy with the injection sequencer. The injection sequencer is a pre-programmed succession of different injection shots. It goes on next injection request only if the injection quality has been asserted.

2.7.5 Safe Machine Parameters

In high power accelerators, transferring machine parameters is needed for operation. However, some of them are safety relevant : Indeed, a corrupted transmitted parameter (such as safe beam flag) may lead to machine damage. In this purpose, in the LHC framework, the Safe Machine Parameters (SMP) has been developed [7].

The SMP is part of the machine protection and a special focus has been performed on its reliability and availability attributes. Its principle is to generate machine parameters based on a threshold comparison. A schematic overview is given on Figure 2.19.

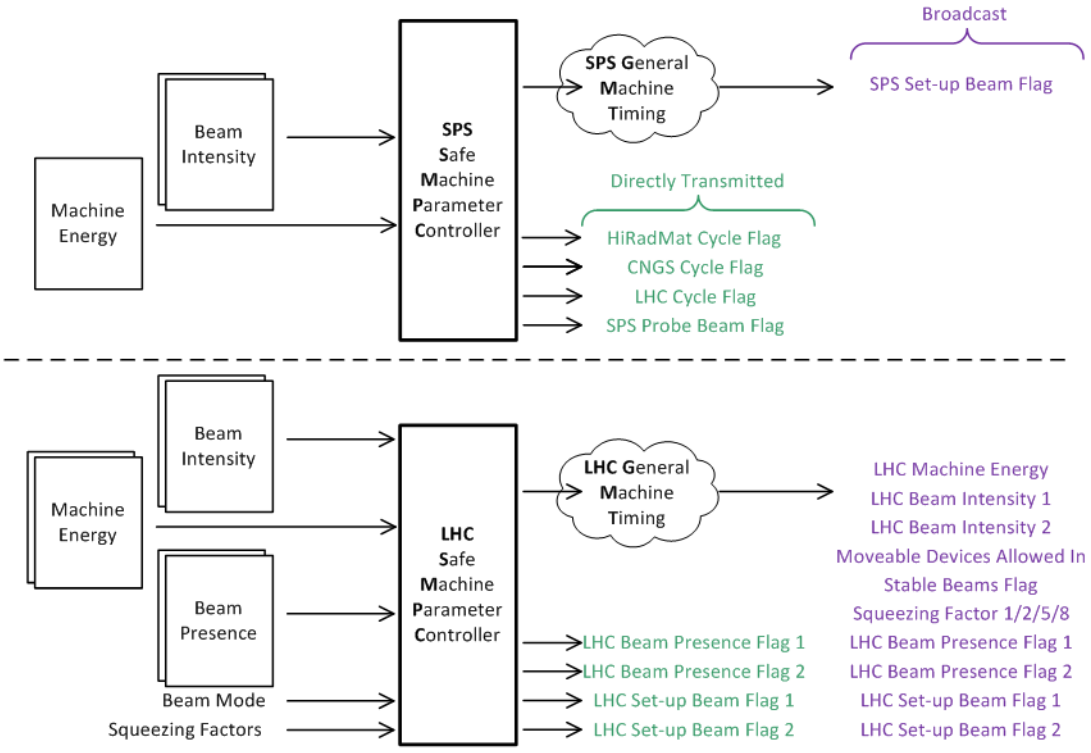

FIGURE 2.19: Safe Machine Parameter Overview [7]

To compute the parameters, the SMP takes as inputs several values, mainly beam related : fast and slow beam current transformer, beam energy meter, beam position meters, beam energy tracking system, sequencer and software interlock system.

The parameters computed (listed on Figure 2.19) are then sent in different ways, regarding their criticality to users. The SMP users are listed hereunder :

- Extraction interlocks
- RF modules
- Beam dumping system
- BIS
- Injection kickers
- Beam loss monitor
- Collimation
- Experiments

An interesting fact to notice is the fail-safe mechanism. When the inputs are not received, the SMP replaces them by the worst case values, generating thus worst case parameters.

The SMP is a distributed hardware system, based on FPGA. To reach dependability requirements, the critical path has been kept as simple as possible and separated from the monitoring (and more complex) part.

2.8 Conclusion

This chapter is mainly a presentation and synthesis work. It has briefly explained the scientific context (particle physics, CERN, linear colliders, ILC, CLIC machine protection) of the thesis and introduced its problematic (CLIC Interlock System).

The state of the art relative to the subject has been described. With this chapter all the concepts (interlock systems, beam permit loop, post-pulse analysis) have been presented. Next chapters will cover the work carried during the thesis.

Chapter 3

Requirements establishment

3.1 Introduction

As described in the previous chapter, the starting point of the CLIC Interlock system project is the concepts (beam permit and post-pulse analysis) and the state of the art about interlock and related systems.

At that time (2013), the CLIC project is in its start of development phase. Consequently, there might be some lack of information (in the external system specifications) or some information may be changed for the final design (for instance, the technology of the interfaced system). Thus, there is a need to have a flexible design process : on one hand, this process must be able to take in account new information and on the other hand, it must be able to modify some parameters. These two expectations must be reached without starting again the process from scratch.

Before starting the design, the first step is to define the specifications. In order to have a rigorous basis, the idea has been to use a standard procedure as a guideline. The procedure chosen is the IEEE 1220-2005 : *Standard for application and management of systems engineering process*. One of its advantages is that it lens easily to iteration, thus reaching the previously mentioned expectations. To compare with others design procedure (ISO-IEC-15288 [35], EIA-632 [36] or MIL-STD-499 [37]), the selected standard is more focused on the design phase but less precise on the product life cycle. Moreover, it is applicable not only for software-based systems (at the opposite of [38]).

The motivation is to define what the system shall be able to accomplish (functional requirements) and how well (performance requirements). The standard gives a complete

approach even if it is not always applicable to the current project. To place this chapter in a formal and standard conception V cycle [39], it corresponds to the functional requirements step.

In this chapter, we will first describe the operational scenarios, the boundaries and interfaces of the system. As a second part, the functional requirements and suggestions will be defined. Thirdly, the performance requirements will be fixed, with a special focus on the dependability. Finally, the critical interfaces will be more deeply studied in order to extract constraints and to fix expectations from the Interlock System to these interfaced systems.

3.2 Operational scenarios and interfaces

In this section, the operational scenarios, the interfaces and boundaries of the CLIC Interlock System are defined. The critical interfaces will be described in an extended way in the design proposal chapter.

Operational scenarios The Interlock System will be used during beam operation. The CLIC is foreseen to be built at different energy stages (0.5, 1.5 and 3 TeV) : these stages will operate beams with different parameters [12].

> *"The lower beam energy has little impact on CLIC operation. The Main Beam has at most 34% larger total energy and charge per beam pulse, which has minor implications for machine protection"* - CLIC Design Report

From Interlock System point of view, the minor implications can be translated in a variation in the number of modules along the main linac.

During commissioning and technical stop, the Interlock System will be used to support machine testing. In this last scenario, some interlock system inputs would need to be masked. The system must be flexible enough to handle these different scenarios. Moreover, staged commissioning of the machine (e.g., beam dumped at the damping ring extraction) must be considered.

Boundaries and interfaces The Interlock System is intended to cover the main linac. Its extensions to the injector parts (Ring to Main Linac or Damping Rings) should be considered but as a secondary goal. To design a system, it is needed to know its interfaces and their different types. For each interface, the system boundaries must be defined in order to know which part is under the design of the Interlock System.

The interfaces can be classified in two types. An interface is considered as *critical* when it has direct impact on the interlock function. At the opposite, an interface is considered as *non-critical* when its outage will not affect directly the interlock function but will induce a degraded function.

The critical interfaces are the control infrastructure and the target systems, there are brievly presented hereunder and are more deeply studied in section 3.5. Adding the Interlock System and the equipment gives the critical path to interlock the CLIC machine. It is represented in Figure 3.1.

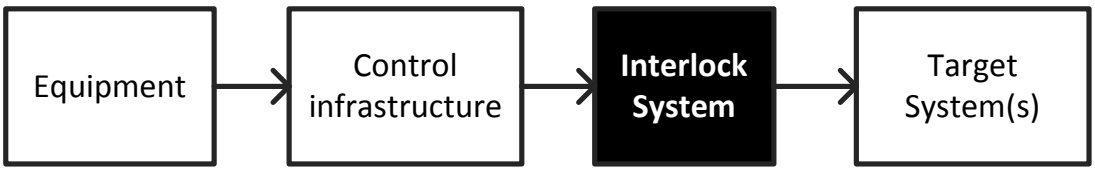

FIGURE 3.1: Machine interlocking critical path

Interface : acquisition and control infrastructure The acquisition and control infrastructure is a critical interface. It is responsible for data acquisition, control signals, data time-stamping and data delivering. The control infrastructure boundary is reached when the data are released to the modules of the Interlock System.

Interface : target systems The target systems are critical interfaces. They are responsible to perform the beam inhibition. For the Main Beam, the main option is to use the Damping Ring and Pre-Damping Ring extraction kickers. There may be another possibility to fully dump the beam at the RTML. For the Drive Beam, the option is to inhibit the sources (thermionic gun RF). This solution is used in the CTF3. The target systems boundaries are reached when the final beam permit reach their control module.

Interface : middleware and human The middleware is a non-critical interface. It is a common infrastructure (mainly made of servers) to machine subsystems used to link equipment data and human interface software application (control, test and monitoring purpose). Its is represented as the middle tier on the Figure 3.2 (extracted from [13] Chap 5.13). In the Interlock system case, it will be used to transfer monitoring, test and off-beam configuration data. The Interlock system boundary is reached when the data are transmitted to the controller. At the other side, the Interlock System boundary start when the data are read from the middleware by the monitoring software. This is the main human interface.

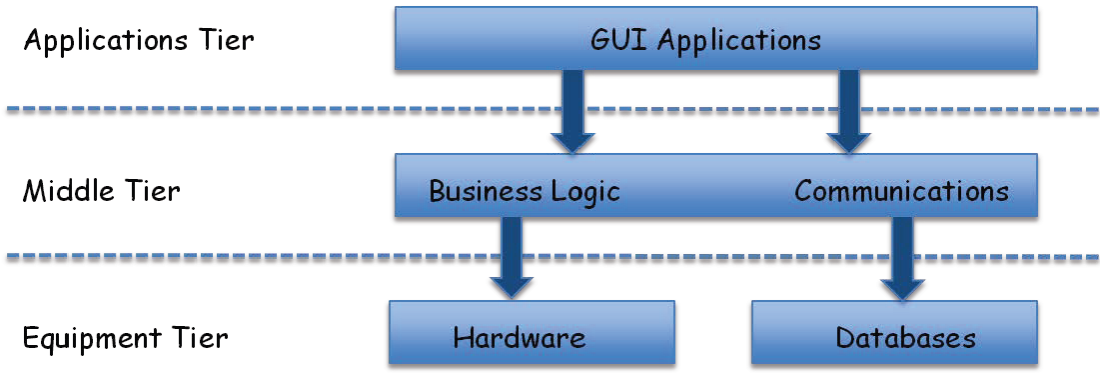

FIGURE 3.2: The CLIC middleware architecture

Interface : machine timing The machine timing is a non-critical interface. It is responsible to spread the "legal" time and some events of interest all over the machine. The boundary is reached when the data is delivered to the Interlock System modules.

Interface : data management service The data management service is divided in two sub-services. The logging facility is mainly used to keep track of data over time for off-line analysis and correlation. The second sub-service is the configuration data. It is used to model the machine and its exploitation. In the Interlock System case, the two sub-services are used. The logging facility is used for the monitoring data. The configuration data facility is used to stock highly critical data (for instance the thresholds to detect unsafe conditions). As seen in Figure 3.2 under the name "database", these services are accessed via the middleware, thus having the same boundaries from the Interlock System point of view.

Interfaces synthesis The interfaces described previously are represented in Figure 3.3. The blue boxes are the critical interfaces and the orange the non-critical.

3.3 Functional requirements

In this section, the goal is to describe which functions must be implemented in the Interlock System and to suggest additional functions that may be required in the future (on the next iterations of the design process). Despite some functions required are obvious, it is needed to list them in order to have rigorous approach.

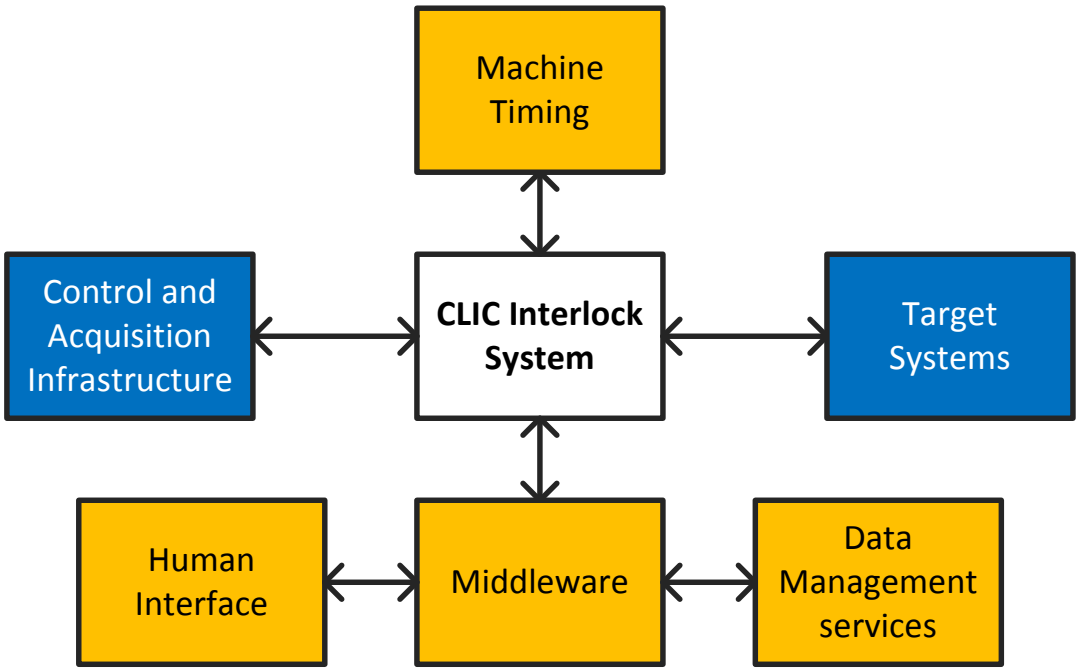

FIGURE 3.3: Interlock System interfaces synthesis

3.3.1 Main functional requirements

The first functional requirement is the machine interlocking function. The Interlock System must be able to trigger a beam operation stop (via actuators). In the CLIC case, it is to inhibit the next pulse.

The second functional requirement is the post-pulse analysis. The Interlock System must be able to evaluate the beam quality of the last pulse. This analysis must be mainly focused on asserting the high probability of stable beam for the next pulse.

The third requirement is the control function. Despite the fact the interlocking function has to be done automatically, some less-critical actions may be controlled by human (from operators to system experts). Thus, the Interlock System must be able to be partially human-controlled. There is to note the human-controlled functions are not listed here and will be defined later. This requirement aims to specify the control-ability of the system.

The fourth requirement is the monitor function. The Interlock System must provide a way to live-monitor its state.

The fifth requirement is the test function. The Interlock System must be able to be tested either during beam operation with reduced testing functionality and during machine stop with full testing functionality (and may include interface testing as well). The beam-off

tests must implement certification tests. These tests assert the system to be " as good as new " and must be performed when configuration data have been changed (for instance, when the thresholds have been changed by the experts).

3.3.2 Functional suggestions

As described the in the state of the art, in LHC, there was a need of Safe Machine Parameters system [7]. A similar system may be required in the future for CLIC. A suggestion is to already think a way to implement or integrate it in the Interlock System.

When an interlock is triggered, the next step is to analyse the cause of this event. In the LHC case, the analysis is orchestrated by the Post-Mortem system [31]. A suggestion to the CLIC Interlock System is to implement facility (such as history records) which would facilitate this post-interlock analysis.

3.4 Performance requirements

After defining *what* the Interlock System must do, it is needed to define *how well* it must do it. This is the purpose of this section. As a first iteration of the design process, the goal is to list the main performance requirements that affect the design itself. Two of them can be identified : the response times and the dependability requirements. Moreover, the dependability requirements on the overall Interlock system can be translated to the node level.

3.4.1 Response times

The response time of a system is the time taken to react for a given input. In the interlock case, there are mainly two times to be considered.

The first response time requirement comes from the CLIC Machine Protection [19] requirement : the response time between a failing equipment and the actual machine interlocking must be inferior to *2 ms*. The Interlock System is on the critical path (cf. Figure 3.1) and must be able to change the permit in a fraction of this time. Indeed, The overall *2 ms* requirement include the failure detection, its transmission until interlock system and the target system response time.

The second response time is related with the post-pulse analysis. As a reminder, this analysis must be done between two pulses. Beam repetition rate in CLIC is expected to be at 50 Hz but as quoted hereunder, a 100 Hz rate can be considered.

> *With further Research and Development, it should be possible to double the repetition rate (i.e., 100 Hz) at lower energy and further enhance the luminosity.* - [13] Chap 8.5.2.

Considering the conservative case of 100 Hz beam operation and a delay of 2 ms to receive beam related data, it leaves a maximum time of *6 ms*, as shown in Figure 3.4.

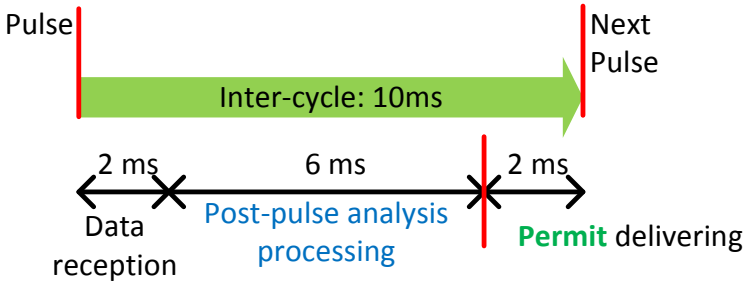

FIGURE 3.4: Post-pulse analysis response time requirement

3.4.2 Establishing dependability requirements

Dependability is a global concept [40] used to describe many aspects of safety engineering. In Interlock System framework, the most important attributes are the *reliability* and the *availability*. To establish them, a systemic methodology has been developed. It has been strongly inspired from the Protection System Life-cycle [21] which is derived from International Electrotechnical Commission (IEC) 61508 Life-cycle [41]. The different stages are described hereafter.

(A) The first step is to understand the machine concepts, its equipment and its operation.

(B) The second step is to identify the failures and the corresponding risks expected to be covered by the Interlock Systems.

(C) The third step is to analyse these identified risks.

(D) The fourth step is to determine the needed risk reduction to reach a tolerable level (tolerable level is defined at the first stage).

(E) The last step is to specify the dependability attributes for the Interlock System which will perform the needed risk reduction.

a. CLIC requirements and parameters

The CLIC is a huge machine with a lot of challenges and requirements. Concerning the Interlock System, the overall machine safety and the beam availability are the two main requirements.

Safety requirements : From CLIC Machine protection study [19], the risks are considered as tolerable when their cumulated impacts lead to less than few percent of downtime or of the yearly operational budget. The risk is defined as the combination between the failure rate and its impact. As a first conservative appreciation, the tolerable risk has been fixed to one catastrophic event every ten thousands years. A catastrophic event is defined as implying more than one year of downtime. The underlying assumption is that non-catastrophic events are assumed to have a risk inferior to the catastrophic one.

$$Tolerable\ catastrophic\ failure\ rate = 1 * 10^{-4} year^{-1}$$

Availability requirement : It comes from the unavailability budget dispatched to several systems. The range allowed to the Interlock System is reported hereunder.

$$Unavailability\ budget\ range = [0.3\% : 0.1\%]$$

During the study, several parameters listed below have been used to compute different rates.

- 200 operating days per year
- 20 hours of operation a day
- 50 pulses per second

b. Risk identification

To identify which risks are expected to be covered by the Interlock System, the goal is to identify which events or conditions are linking failures to machine damage. The chosen way to represent it is a hazard chain. As the machine design is in its early stage, the granularity of this hazard chain is relatively low. The main events where there is a need of risk reduction are represented. An unstable beam turning into energy losses is considered slow when it takes more than one pulse (i.e., 20 ms in CLIC case).

The Interlock System has to prevent uncontrolled energy loss at two different stages. The first stage is to prevent critical equipments failures turning into beam instability. The

second stage is to prevent slow beam instabilities turning into an uncontrolled energy loss. These two stages are represented in Figure 3.5.

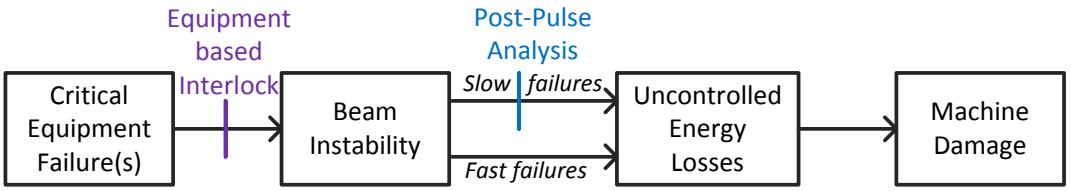

FIGURE 3.5: Hazard Chain for Interlock System

The other events are, when possible, covered by other protections systems (e.g., the collimators are partly protecting against uncontrolled energy losses turning into machine damage).

c. Risk analysis

In both risks previously identified, their impacts without protection system are considered to be identical and catastrophic (conservative case). To determine their likelihood, two methods have been used.

Method 1 - based on operational statistics : As a first calculation, critical equipment failure rate and slow beam instabilities rate are both considered to be in the same order of magnitude as for the LHC case. The data provided by the post-mortem system for the LHC [31] all along the operation year 2011 are therefore used. These two failure rates are summarized in Table 3.1.

TABLE 3.1: Risks analysis synthesis

Type of failure	**Machine Failure Rate**	**Impact**
Critical Equipment	$2.65 * 10^{-7}$ pulse^{-1}	2 years downtime, few % op. budget
	$4.78 * 10^{-2}$ h^{-1}	
Slow Beam instability	$3.33 * 10^{-8}$ pulse^{-1}	
	$6 * 10^{-3}$ h^{-1}	

Summing up these two rates gives an overall rate of :

$$Interlock\ request\ rate \approx 3 * 10^{-7} pulse^{-1}$$

Method 2 - based on assumption on availability : In order to assert the order of magnitude of the rates given by first method, a second estimation has been performed. It is based on the following pessimistic estimations :

- one unstable beam leads to *ten seconds* downtime. Indeed, it would trigger a transient interlock request. Ramping up the beam from the pilot beam until its nominal luminosity will then take these ten seconds (estimation from the expected operational scenario [19]).
- the machine downtime caused by unstable beams must be lower than 10% ; it leads to a maximum rate of one unstable beam every one hundred seconds.
- 1% of unstable beams are leading to non-negligible machine damage, if not inhibited.

These estimations have been based on discussions with machine experts but do not have rigorous sources such as statistics or full failure analysis. This verification method leads us to the probability of interlock request due to unstable beam of $2 * 10^{-6} pulse^{-1}$.

Methods comparison and discussion : There is a factor of 6.7 between both methods. As the second method is purely based on rough estimations, this factor is considered acceptable. For the next steps, the most conservative case of the method 1 will be taken, i.e., the critical equipment failures rate.

d. Risk reduction determination

At this step, the risk reduction to be performed by the Interlock System shall be determined. It means to specify how well the protection system must perform its functions. This can be defined through its failures rate. Two failure modes can be identified :

False Pass decision : It is related to machine safety. It is the rate which defines the risk reduction performed by the Interlock System.

False Veto decision : It is related to machine availability. Depending whether it is a permanent or a transient failure, it will not have the same impact on the overall availability. To compute the impact of these failures, the time to repair needs to be known. It is estimated at *ten seconds* and *four hours* for respectively *transient* and *permanent* failure. The permanent failure repair time is extracted from an availability study [42] with an extra margin of 25%. The transient failure time-to-repair is related to the time needed to ramp the beam intensity back to the nominal value. For information, some studies take in account intermittent failures [43]. This type of failure will be neglected as it is more likely to happen on software-based systems.

The risk reduction is computed by dividing the tolerable risk (defined in Section A.) by the machine failure rate (Table 3.1). It should be noted that the resulting rate is

independent of the demand (i.e., an interlock request). The rate *on-demand* corresponds to the tolerable risk, to be reached.

For the machine availability, the method is to select realistic requirements for the false VETO (permanent and transient) decision rates and verify if their impacts fit within the allowed unavailability budget.

The resulting specifications are summarized in Table 3.2. The units have been chosen to give the most representative rates.

TABLE 3.2: Failure modes requirements

Interlock System Failure Mode	**Failure Rate**	**Unavailability**
False PASS decision (risk reduction factor)	$< 5.2 * 10^{-7}$ pulse^{-1}	0.2 % (financial impact)
Transient false VETO decision	< 0.1 h^{-1}	0.03 %
Permanent false VETO decision	< 2 year^{-1}	0.20 %

For the False PASS decision, the unavailability is not taken in account because there is also a financial impact. Indeed, in most cases, the failure is silent from the operation point of view (no interlock request at the same time). When the failure is not silent, the accelerator is damaged and has a financial impact in addition of the operational unavailability.

e. Interlock System dependability requirements

The last step to establish dependability requirements is to translate the Interlock System failure rates in reliability and availability attributes (following the definitions specified in [40]).

The availability is obtained by subtracting the total time machine outage due to Interlock System from the expected time of operation during a period of time. Normalizing it by the second term gives the result in percentage. The reliability is given by the number of failures over a period. The resulting attributes are summarized in Table 3.3.

The non-negligible number of failures is not an issue. Indeed, it is mainly driven by the transient false VETO decisions which are not safety-relevant.

TABLE 3.3: Interlock System Dependability Attribute

Attribute	**Definition** [40]	**Value**
Availability	readiness for correct service	99.75 %
Reliability (with transient)	failure rate	$5.6 * 10^{-7}$ pulse^{-1}
	continuity of correct service	$1.8 * 10^{6}$pulses
Reliability (without transient)	failure rate	$2.8 * 10^{-9}$ pulse^{-1}
	continuity of correct service	$3.6 * 10^{8}$ pulses

According to the failure definition in [40], false PASS decisions are taken in account in the reliability computation only if they are observed. As it is specified to be less than once every 10 000 years, it does not affect significantly the rate.

3.4.3 Reaching dependability requirements

To reach previously established requirements, several means can be employed : technology choices (e.g., Programmable Logic Devices), design techniques (e.g., fail-safe concept), architecture choices (e.g., redundancy), etc.

The following sections explain and apply the methodology to assert design compliance. This is done by defining the success conditions through a simulation and then, by measuring failure rates on a hardware prototype (done in chapter 5).

The compliance of a design proposal is achieved if it reaches the established requirements. However, at design phase, it is very hard (without simulation) to measure directly these attributes as it would require the complete system. Consequently, a simulation has been performed to define measurable success conditions.

a. Model

The first step to perform the simulation is to define the model.

Following specifications [19], the CLIC Interlock System is implementing a beam permit loop (cf. chapter 4 - design proposal - for more details). As it is a crucial function, duplication of the loop is planned. Its synoptic without redundancy is shown on Figure 3.6.

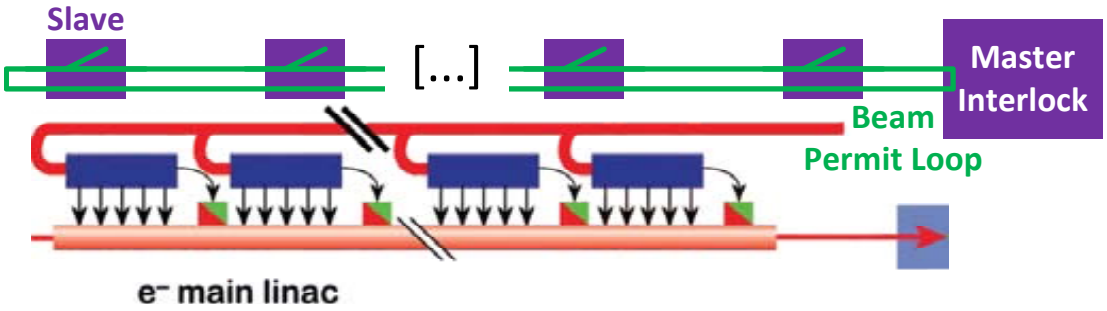

FIGURE 3.6: CLIC Interlock System overview

A signal is generated by the master node on every loop. Every node (a.k.a. the slaves) has the ability to open the loop twice (go and back of the permit loop) and will do so as soon as there is an interlock demand.

The nodes are initially closed (PASS decision) and are supposed to open (VETO decision) as soon as a request is received. The model is represented in Figure 3.7 and its underlying assumptions are listed hereunder :

- Conservative assumption : permanent failures only (transient considered as permanent)
- Independent failures of nodes
- Identical components (with regard to failure rates)
- Fault-free voting system (in case of redundant lines)
- Interlock request signal fault-free and simultaneously distributed to all redundant nodes

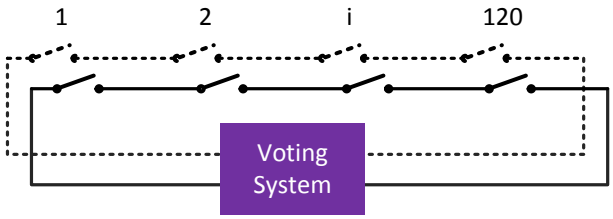

FIGURE 3.7: Architecture model

Different redundancy scenarios (Table 3.4) have been preselected for the study. Each case has its pro and cons and have been described in a previous study [24]. Despite it is not the main challenge, cost is a limiting factor. Thus, the maximum redundant lines have been limited to three.

TABLE 3.4: Redundancy scenario

Voting	**Choice justification**
1 out of 1	No redundancy
1 out of 2	Lowest False PASS decision for double redundancy
1 out of 3	Lowest False PASS decision for triple redundancy
2 out of 3	Best compromise for triple redundancy

b. Methodology and simulation

Once the model has been defined, the goal is to translate the Interlock System dependability requirements to the node level. The idea is to have requirements that will be measurable or estimable with hardware tests.

The approach is to determine the highest false VETO decision and false PASS decision rates needed for the nodes in function of the redundancy. These rates must be compatible with the overall requirements. The compatibility is defined by objectives to be reached (listed in Table 3.5).

TABLE 3.5: Simulation Objectives

Objectives	**Missions** (%)
Mission Completed	46.2
False VETO decision	$1.25 * 10^{-3}$
Demand Success	53.8
False PASS decision	$6.25 * 10^{-8}$

The *Matlab* simulation software (developed in a previous study [24]) generates interlock demands with a user-defined probability. In current case, it is fixed to the critical equipment failure rate. The concept of mission used by the simulation software corresponds to a maximum 10 hours run. The mission ends when the interlock demand is successful, missed or when there is a false VETO decision. The system is simulated with 120 nodes and their user-defined failure rates. The redundancy is user-defined as well.

When running the simulation, it gives the whole system failures rates. Consequently, to determine the tolerable failure rates for a node, it is needed to use the simulation software in the opposite way : the tolerable node failure rates (which determine the design compliance) are obtained by searching the highest nodes failure rate which give a simulation result still compliant with the objectives (system failure rates), for each selected scenarios.

c. Simulation results

The simulation results given in Table E.1 fix the minimum performance level to reach by the nodes with regard to the redundancy. The lower the rates are, the more challenging they are to reach.

TABLE 3.6: Simulation results - single node failure rates

Voting	**False Veto decision rate**	**False Pass decision rate**
1 out of 1	$9 * 10^{-9}h^{-1}$	$1 * 10^{-10}h^{-1}$
1 out of 2	$6 * 10^{-9}h^{-1}$	$5 * 10^{-6}h^{-1}$
1 out of 3	$4 * 10^{-9}h^{-1}$	$1 * 10^{-4}h^{-1}$
2 out of 3	$1 * 10^{-6}h^{-1}$	$3 * 10^{-6}h^{-1}$

The resulted rates are coherent with what was expectable. The more redundant lines are added, the less stringent the requirements are. Concerning the voting systems, the results can be interpreted as their ability to compensate a non-balanced node in term of repartition between false VETO decision rate and false PASS decision rate.

As a conclusion, success conditions have been defined the assert a design compliance for the dependability requirements. This success conditions are measurable with at least one node. These measurements will be performed on several prototype nodes and are presented in chapter 5 (design verification).

3.4.4 Suggestions for the dependability study

The dependability study has described and applied the methodology to determine the dependability requirements. It has presented the process to determine measurable success condition to assert a design compliance. This methodology can be applied for future Interlock Systems at their design phase. Following some assumptions, it can be also generalized to safety-critical electronic systems.

In long-term view, several improvements are proposed. At each iteration of this methodology, several stages could be enhanced. First idea, the machine parameters shall be adapted as the CLIC project goes along, including the underlying requirements (e.g., the precise unavailability budget). A second suggestion is to increase the granularity of the hazard chain. An additional proposal is to improve the machine failures rates accuracy. Indeed, validity of taking data from LHC post-mortem system can be discussed. One option would be to set up a failures catalogue from the components conception. A similar work is experimented for the Linac 4 design [44].

Moreover, the model shall be improved : the voting system failure mode and the target system failure rate (beam permit receiver) should be taken in account. The concept of post-pulse analysis should be integrated as well. Finally, the study [45] divides faults between node and the link faults. This should be applied to the model.

3.5 Interfaces and safety-critical requirements

In this section, the critical interfaces are more deeply described for two reasons. First, it is used as constraints for the design proposal in the next chapter. Secondly, as the impact of the Interlock System on the machine is strongly linked with the interfaced systems performance, specifying expectations from the interlock system to the interfaced system is needed. Indeed, the importance of specifying safety-critical requirements to interface has been established [46] and enhance system reliability [47].

3.5.1 Acquisition and control infrastructure

The Interlock System receives critical data from the acquisition and control infrastructure.

a. Description

The CLIC main linac is made up of about 22 000 modules of 2 meters length. A conceptual view of a CLIC module is shown in Figure 3.8.

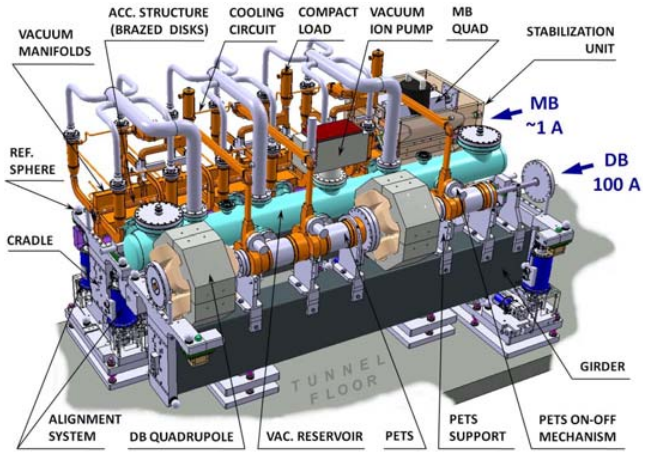

FIGURE 3.8: CLIC module [8]

For each of these CLIC modules is foreseen an acquisition and control crate to perform the data acquisition and provide the control signals [48].

Acquisition crates are located 1 meter away from the CLIC module in the tunnel. Consequently, they have strong constraints in term of radiation hardening and power consumption. Pessimistic simulations estimate a radiation deposit of 1000 Gy a year [49]. For the power consumption, the heat tunnel evacuation ability requires a 50 W crate consumption, leading to a pulsed electronic design. To give an idea, one crate has to acquire more than 200 signals, leading to a data rate higher than 3.7 Mbits/s [12].

These acquisition crates are grouped by 400. They are linked to a concentrator, located in the alcoves. The alcoves are caverns every 800 meters along the main linac, shielded against beam-induced radiation by concrete walls. Most sensitive electronics can be placed at these places.

The concentrator dispatches the data received to 8 dedicated front-end modules. One of them is dedicated to Interlock System. With one concentrator at each alcove, there are 48 Interlock System front-end modules for the main linac.

The acquisition and control infrastructure implementation is represented in Figure 3.9.

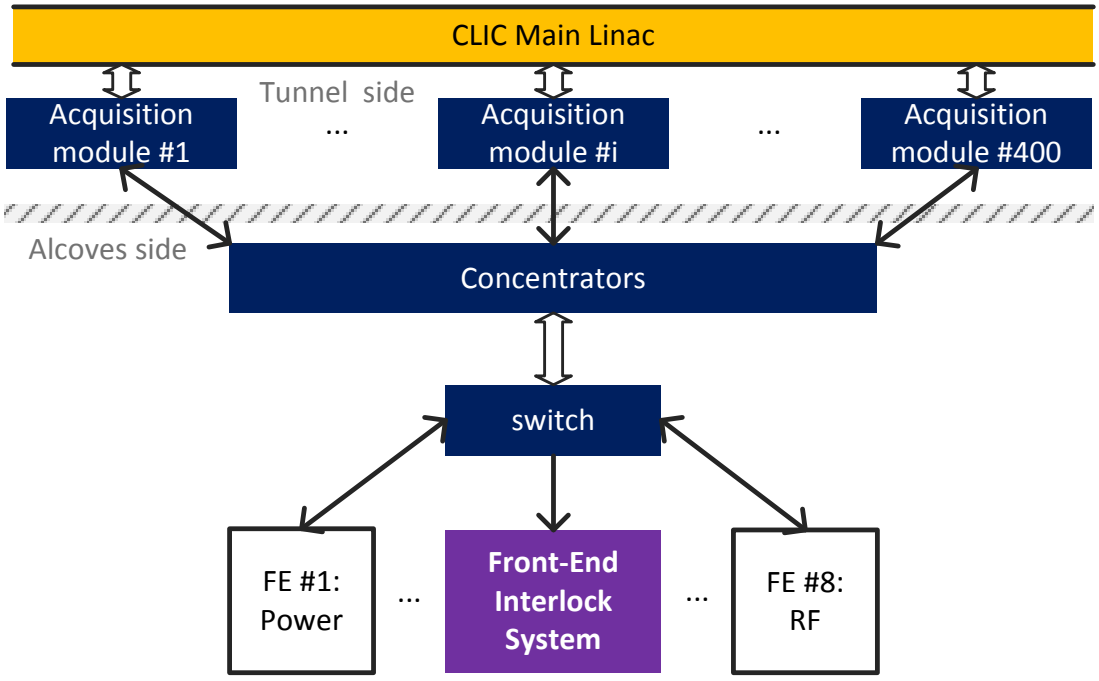

FIGURE 3.9: Acquisition and control infrastructure architecture

Thus, the Interlock System is constrained to be interfaced through these 48 front-end modules. Because of this infrastructure, there is no need to have hard-radiation tolerant electronics. The only events that can arise are Single Event Upset (SEU).

b. Requirements from Interlock System

With about 22 000 acquisition crates in this stressed environment and despite the design effort performed, there will be a non-negligible probability to have one of them failing during beam operation.

From the Interlock System point of view, two failure modes of the acquisition infrastructure can be distinguished : corrupted data that can affect the CLIC safety and lacking data that can affect the machine availability.

Requirements to acquisition infrastructure : machine safety If a critical data is corrupted by the acquisition infrastructure, it leads to a false decision. The conservative case is a data that should have triggered an interlock is turned into a safe data (false PASS).

At the dependability study (cf. 3.4.2), three rates were defined :
– Tolerable catastrophic failure rate = $1.39 * 10^{-13} pulse^{-1}$
– Interlock request rate = $2.98 * 10^{-7} pulse^{-1}$ (method 1)
– Interlock request rate = $2 * 10^{-6} pulse^{-1}$ (method 2)
By dividing the tolerable catastrophic failure rate by the interlock request rate, we can obtain the maximum tolerable corruption rate for the acquisition infrastructure.

It gives the hereunder rates, which are the expectations from Interlock System to the infrastructure :
– Tolerable corruption rate= $4.6 * 10^{-7} pulse^{-1}$ (method 1)
– Tolerable corruption rate= $7 * 10^{-8} pulse^{-1}$ (method 2)
There is to note this rate is independent of the demand. This is the rate for the acquisition infrastructure to corrupt a data, without any assumptions of the type of data corrupted.

Requirements to acquisition infrastructure : machine availability Regarding the fail-safe concept, the default behaviour for the Interlock System when a critical input is lacking, is to trigger an interlock : a false VETO decision is better than the system being blind.

Thus, lacking data may conduct to false VETO decision. In order to optimize machine availability, enhancements have been proposed to the acquisition infrastructure.

There are a set of critical data which will result in a VETO decision as soon as one of them is missing. This set of data is listed in Table 3.7. The proposed enhancement is to implement a redundancy on these signals by connecting a single signal on two different acquisition crates. Thus, a single acquisition crate failure will not lead to an interlock.

TABLE 3.7: Set of critical interlock channels

Channel	**description**
Beam loss monitors	Cherenkov fibers
Power converter	failure time 10-100 ms
RF	beam instrumentation
Wake field monitors	position detectors
Positioning	relative displacement
Vacuum	Valve

If the data missing are not these previously mentioned, the Interlock System shall give a PASS decision as long as two consecutive (geographically speaking) data are not missing (behaviour embedded through local rule). Going further, the next step would be to determine how many consecutive data can be lacking before triggering an interlock. This would avoid decreasing too much the CLIC availability.

3.5.2 Target systems

The Interlock System is providing the *beam permit* to the target systems, the actuators which inhibit the next pulses. For the main beam, the target systems are the dump systems located at the damping rings. For the drive beam, the target systems are the RF gun (RF source), located at the start of the injection complex.

a. Main beam

In order to reach main beam emittance requirements, damping rings have been designed. They receive particle beams from the initial linac and release them to the delay loop.

The beam connections between linac, rings and loop are done with transfer lines. To inject beam from (respectively to) transfer lines, an injection (respectively extraction) kicker is required. Kickers are pulsed magnets delivering a strong magnetic field to modify the beam trajectory.

In Figure 3.10 is represented the damping rings layout and the extraction kickers location (red circles).

At the damping rings extraction points, beam dumping systems have been designed [9]. The concept is to use the extraction kickers but with a higher energy to deviate the beam in the dump line. This concept is represented in Figure 3.11.

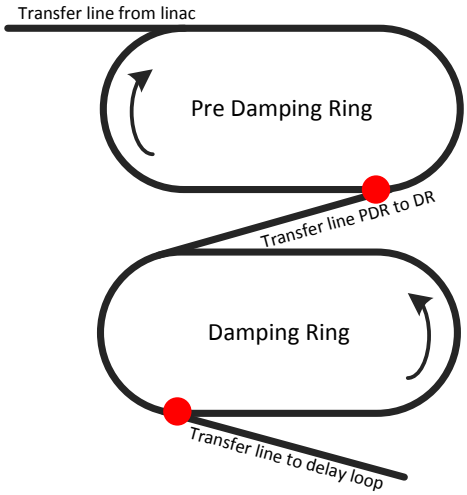

FIGURE 3.10: CLIC Damping rings and extraction kickers

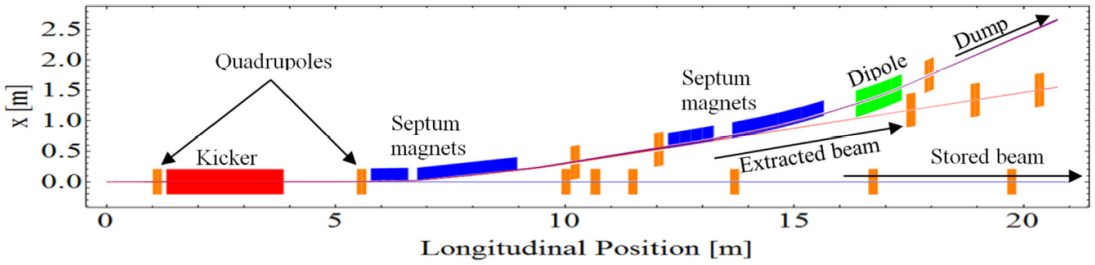

FIGURE 3.11: Damping rings dump system [9]

b. Drive beam

The electron sources for both drive beams are 140 keV electron guns (thermionic gun) [12]. As in CTF3, the guns shall be controlled by PLC based system [50].

These two PLC control systems can receive interlock requests and can inhibit the electrons emission. It is intended to be the target system for the drive beam as there is not full beam dump system foreseen in the drive beam complex. Indeed, there is to note there will be a dump systems the end of the deceleration lines, but these dumps are studied to dump a 90% energy reduced drive beam and are therefore not suitable to dump a full drive beam.

c. Requirements from Interlock System

From Interlock System point of view, the dumping systems and gun control system must not miss a beam inhibition request (i.e., a *beam permit* in VETO state). These failures deal with the machine safety.

As for the acquisition infrastructure, the tolerable rate to miss a beam inhibition request is determined with the same methodology :

- Tolerable catastrophic failure rate : $1.39 * 10^{-13} pulse^{-1}$
- Interlock request rates :
  - $2.98 * 10^{-7} pulse^{-1}$ (method 1)
  - $2 * 10^{-6} pulse^{-1}$ (method 2)
- Tolerable rate to miss an beam inhibition request :
  - $4.6 * 10^{-7} pulse^{-1}$ (method 1)
  - $7 * 10^{-8} pulse^{-1}$ (method 2)

To reach this rate, duplication can be used. For instance, one LHC interlock target system is the beam dumping system. To achieve the predicted safety failure rate of $1.2^{-9} h^{-1}$ [51], duplication of the triggering channels (both at interface with the Interlock System and internal) have been performed [52].

Concerning the machine availability, the Interlock System has not requirements concerning the false beam inhibitions rate performed by the target system. However, a spurious beam inhibitions must be notified to the Interlock System that should trigger the other target systems.

d. Discussion on multiple target systems

With separated target systems that need to be triggered in the same time, an important issue is the confidence that all target systems will dump/inhibit the beams.

Indeed, when an interlock is requested, if the drive beam is stopped and the main beam is not (for instance, due to dump system failure), the main beam would not be accelerated and therefore will lost its synchronisation with magnets, be defocused by the quadrupole and spread out in the structure, thus damaging the machine.

In the other way around (main beam dumped but not drive beam), the drive beam energy will be extracted but not transmitted to the main beam. This RF energy will need to be dissipated and could damage the PETS.

3.6 Conclusion

Based on the IEEE 1220 procedure, this chapter has established the main requirements for and from the CLIC Interlock System project. In other words, the problem to solve has been posed.

After defining the expected conditions of use, the interfaced systems have been presented : the control and acquisition infrastructure, the target systems, the middleware, the human interface, the machine timing and the data management service. Their boundaries with the Interlock System have been defined. Then, the main functional requirements and suggestions have been listed, mainly inspired by the concepts proposed and the state of the art. The performance requirements have been focused on the response times and the dependability requirements. The dependability requirements have been then translated to the node level, thus determining success conditions to assert a design compliance. Finally, the critical interfaces have been more precisely presented as they put constraints to the design. In the other way, based on the dependability requirements, requirements from the Interlock System to these interfaced systems have been specified.

The list of requirements and constraints are summarized in the annex.

The next stage of the design process is to propose a solution which would fulfil these specifications.

Chapter 4

Design Proposal

4.1 Introduction

At that step of the design process, the context is known, the concepts have been explained, the state of the art have been studied and the requirements (functional and performance) have been established. The next step is to propose a design and explain how it has been elaborated.

There are mainly two motivations to satisfy : the first is to keep the design process generic while the second is to continue the case study for CLIC. The main issue has been to allow innovation and creativity while being rigorous and consistent. The resolution of this issue is presented through this chapter. Again, to place this chapter in the V cycle [39], it corresponds to the functional analysis and basic function set-up steps.

The first section presents the functional analysis (function behaviour, functional decomposition proposal, functional architecture). The second section covers the subfunctions and whole system implementation proposal.

4.2 Functional analysis

This section presents a systemic approach for the Interlock System design. The idea is to analyse the functional behaviour of the system and its subfunctions before proposing a technical implementation.

The functional analysis has been done following the *IEEE standard for application and management of the systems engineering process* [3]. It has been used as guideline, especially for the functional decomposition.

4.2.1 System functional behaviour

The goal here is to consider the Interlock System as a black box and to describe the responses expected for different stimuli. Seen as a black box (Figure 4.1), the Interlock System deliver the *beam permit* based on the machine state. As a first approach, three machine states are considered from Interlock System point of view :

– Safe
– Unsafe
– Unknown (blind mode)

The unknown state occurs when there is a lack of data needed to estimate the machine safety. The most likely example is a failure occurring in the acquisition and control infrastructure, resulting in some data not transmitted to the Interlock System.

FIGURE 4.1: Interlock System functional black box

The Interlock systems have only two responses : VETO or PASS decision. In table 4.1 is defined which response is expected regarding the stimuli.

TABLE 4.1: Interlock system functional behaviour

Machine state	**Interlock system response**
Safe	PASS
Unsafe	VETO
Unknown	Variable

When the machine state is considered as unknown, the Interlock System response is defined as variable in order to optimize the machine availability. It is function of which and how much data are missing. This is more deeply explained in subsection 3.5.1.

4.2.2 Functional decomposition

The goal is to describe the subfunctions to implement the CLIC Interlock System concepts. This is a proposal and it has been inspired by the state of the art. However, it needs to be proved that it is feasible and that it will reach the requirements.

The principle of this functional decomposition is to use the divide and conquer paradigm. Once the subfunctions defined and characterized, it will be more easy to propose a technical implementation for each of them (done at 4.3.1).

a. Subfunctions definition and behaviour

The first step is to divide the interlock function in subfunctions and then analyse them. As a first iteration of the design process, three main functions have been proposed, keeping a high level of abstraction. For the next iterations, this level of abstraction shall be lowered.

Individual data analysis : The aim of this subfunction is to detect if a data is in its operational range by performing a simple and fast data analysis. Its black box representation is shown in Figure 4.2.

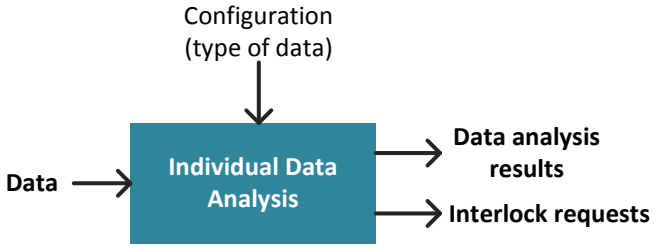

FIGURE 4.2: Individual data analysis functional black box

Two types of incoming data are defined : related to critical equipment and related to beam quality.

There are two types of outputs : the data analysis results and the interlock requests. The data analysis outputs can have four different values : SAFE, WARNING, FAILURE, INTERLOCK (the list can easily be extensible). Regarding the type of data, the data analysis has a different behaviour. In critical equipment related data, the data analysis can only gives a SAFE or INTERLOCK results. In beam quality related data, the output can be SAFE, WARNING or FAILURE.

The interlock request outputs are binary permits (VETO/PASS), linked to the data analysis. If their related data analysis give an INTERLOCK, the interlock request is in VETO state. Otherwise the output will stay in PASS state. For the input data being at the limit of their operational range, the conservative case is kept, thus triggering an interlock request.

This behaviour is synthesized in Table 4.2.

TABLE 4.2: Individual Data Analysis behaviour

Data type / Data range location	**Critical equipment**	**Beam quality**
Out	INTERLOCK	FAILURE
At boundary	INTERLOCK	WARNING
In	SAFE	SAFE

Global analysis : The aim of this subfunction is to perform a synthesis of data analysis results regarding the beam quality data. The synthesis behaviour can be tuned by local rules. Its black box representation is shown in Figure 4.3.

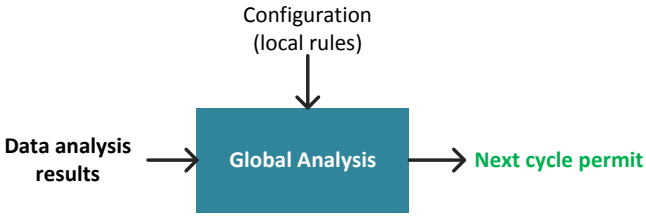

FIGURE 4.3: Global analysis functional black box

The inputs of this subfunction are beam quality related data analysis results. These data come directly from individual data analysis subfunction.

This subfunction gives as output the *next cycle permit*, which represents the synthesis result. It has two states : PASS if the synthesis asserts a good beam quality and VETO if not.

In order to enhance system flexibility, local rules are foreseen to be implementable in this subfunction. For example, two local rules are defined. The first one is similar to the standard behaviour but accepts one input lacking. The second rule is a stressed behaviour which gives a PASS permit only if all the data analysis results are SAFE. The standard and local rules behaviour are illustrated in Table 4.3.

TABLE 4.3: Next Cycle Permit behaviour

Configuration / Data input	**Normal**	**Local rule 1**	**Local rule 2**
SAFE	PASS	PASS	PASS
At least one INTERLOCK	VETO	VETO	VETO
At least one WARNING	PASS	PASS	VETO
only 1 input lacking	VETO	PASS	VETO

Beam permit system : The aim of this subfunction is to gather all the interlock requests received as input and synthesize them in the *beam permit*. Its black box representation is shown in Figure 4.4.

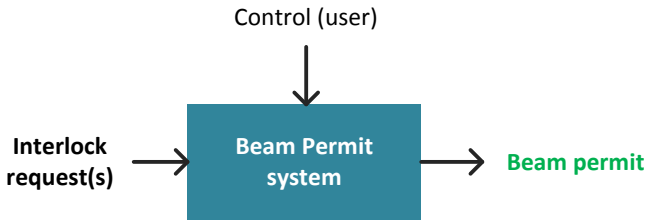

FIGURE 4.4: Beam permit system functional black box

The subfunction receives as input interlock requests (binary signals). The subfunction delivers as output the *beam permit* which can have two states : PASS if no interlock requests or VETO as soon as one interlock request is in VETO state. As it is the backbone of the system, it can be controlled by user (e.g. to trigger manually an interlock).

Control system : Despite this subfunction is not carrying an interlock concept, it is needed to configure and control the other subfunctions. The data analysis subfunctions (individual and global) need to be configurable to optimize their flexibility. The beam permit system subfunction is the backbone of the system and need to be control-able by human users. Its black box representation is shown in Figure 4.5.

FIGURE 4.5: Control system functional black box

The input is the human-system interface (via middleware as described in chapter 3). The outputs are the control and configuration flows to subfunctions.

b. Operational states

The idea is to define operational states of the system which may imply a different behaviour.

In addition of configuration data in individual data analysis (type of data) and global analysis (local rules) subfunctions, two operational states can be defined for the whole system. Either the Interlock System is working while beam operation or when there is no beam operation.

When there is no beam operation, special operation on Interlock System may be allowed (for instance, testing or configuration). In order to address safety issue, the *beam permit* is kept at VETO state.

c. Time line, data and control flows

The goal here is to link together the subfunctions previously defined and determine their time line, in accordance with the response time requirements. The data flows (i.e. type of data transmitted between subfunctions) are defined as well.

In CLIC Interlock System case, two time lines and data flows can be defined, corresponding to both types of input data : critical equipment related (Figure 4.6) and beam quality related (Figure 4.7). Both of them are constrained by the response times requirements.

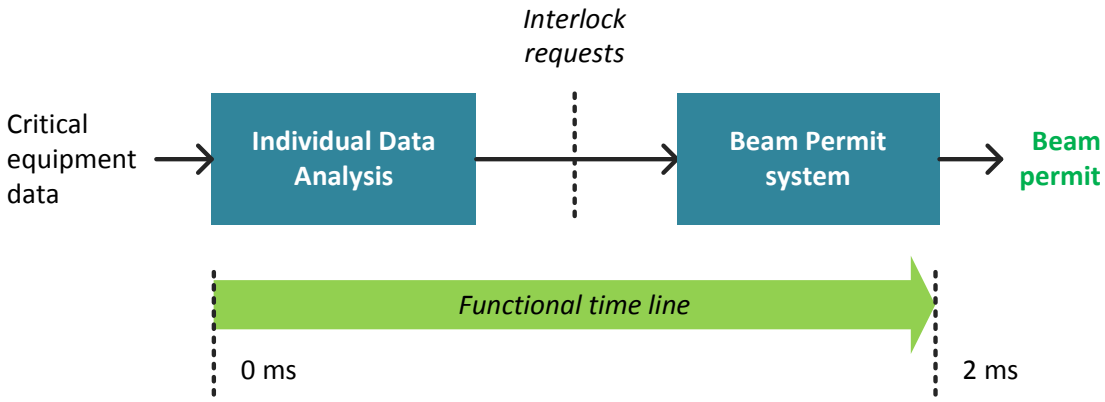

FIGURE 4.6: Functional time line and data flow - critical equipment input

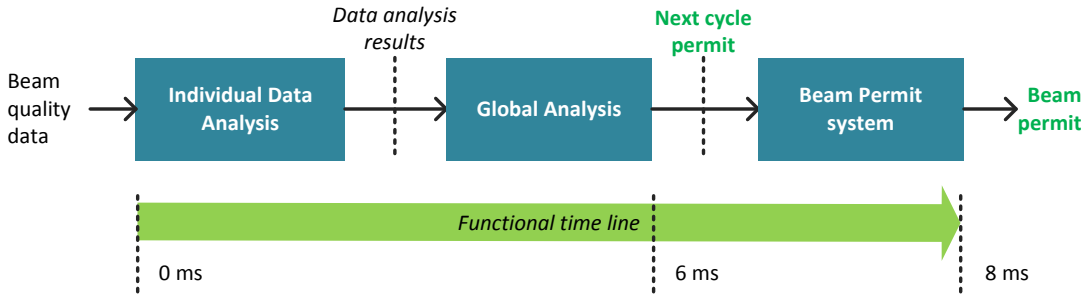

FIGURE 4.7: Functional time line and data flow - Beam quality input

For the control flow, it is done through middleware. The time scale is different as shown in Figure 4.8 and is not time-constrained.

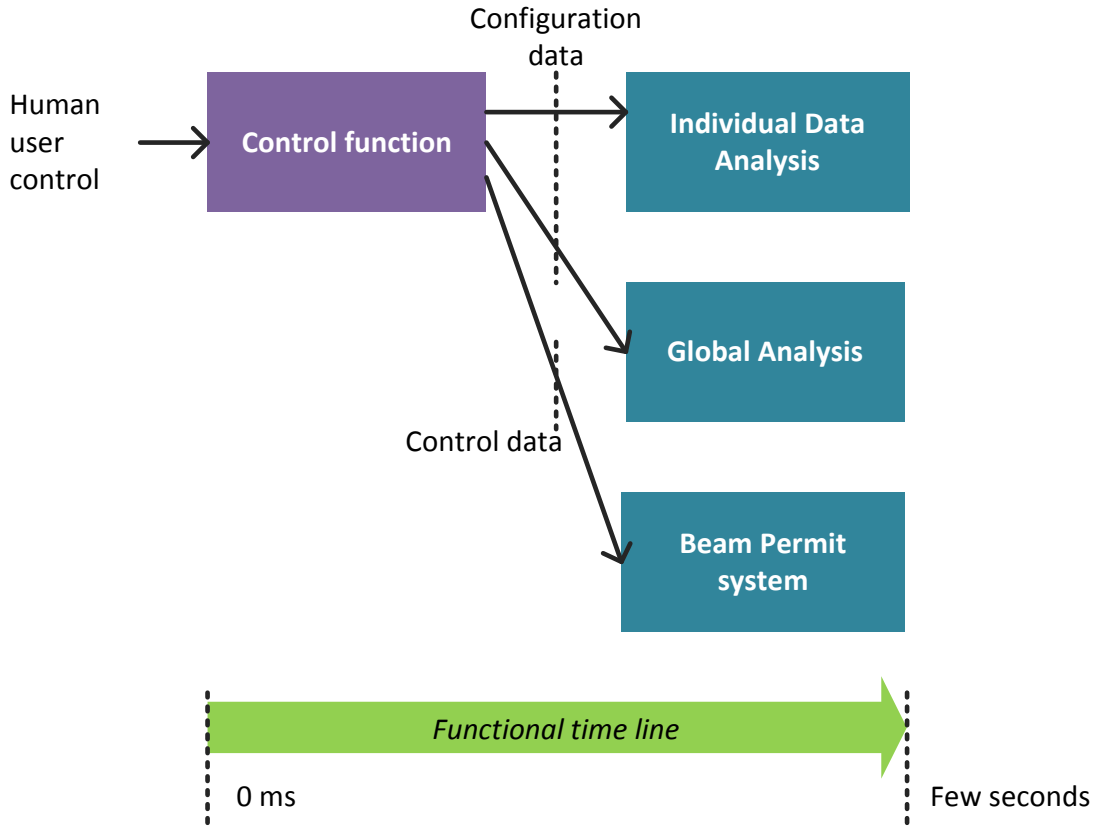

FIGURE 4.8: Functional time line and control flow

d. Failures modes and effect

At this step of the functional analysis, it is needed to study the failures modes of each subfunctions and their effects on the whole system performance.It is done by analysing their outputs.

To simplify the study, all the failures are supposed to occur independently and not in the same time. By default, The most conservative case is taken.

Individual data analysis : For the individual data analysis, there are two outputs where the failure modes can be studied. It is presented hereunder.

For the data analysis results outputs, there are two failure modes :

– **Corrupted output** : the output is not the one expected due to an internal failure. With the worst case consideration :
  - A false SAFE leads to a system false PASS.
  - A false INTERLOCK leads to a system false VETO.

  - A false WARNING leads to a system false VETO if the input is critical equipment related. It leads to a system false PASS if the input is beam quality related.
  - A false FAILURE leads to a system false VETO, whatever the type of input.

– **Lacking output** : it leads to a system false PASS

For the interlock requests output, their failure modes have the same effect on the system. The only failure mode is a **corrupted data**. There is to note the output cannot be lacking as it must be implemented as a persistent signal (no delivering process, its absence equals a VETO state).

Global analysis : For this subfunction, there are two failure modes :

– **Corrupted *next cycle permit*** : if the output is not the one expected due to an internal function failure. This corrupted output has the same effect on the whole system. (e.g. false PASS output leads to *beam permit* false PASS decision)
– **Lacking *next cycle permit*** : it leads to a false PASS.

Beam permit system : This subfunction has one failure mode : **corrupted *beam permit*** (false PASS and false VETO). Indeed, absence of permit (lacking) must be interpreted by the target system as a VETO decision. Its output represents the system output.

Control system : For the control system, there are two outputs where the failure modes can be studied.

For the configuration data outputs, we can consider the failure modes of corrupted data and lacking data. Their effects on the system can be ignored if the configuration data flow is used only during no-beam operation.

For the control data output, as its content is not defined, a pessimistic approach is to say it can trigger a spurious interlock request. In this case, a corrupted data leads to a system false VETO decision.

e. Safety and monitoring function

At this step, the idea is to analyse where safety functions could help to improve the machine safety.

With regard to the fail safe principle, it is better to have a false VETO decision (machine availability) rather than a false PASS decision (machine safety). When analysing

the functional failure modes described at previous paragraph, two types of false PASS decisions can be defined : either it is due to corrupted data or it is due to lacking data.

In the corruption case, the only safety functions available is to duplicate the function and compare their outputs. The redundancy study has been studied in chapter 3 for the beam permit system function.

In lacking case, a watchdog safety function can be implemented. Its principle is to look for outputs delivering and if, after a defined time (consistent with response time requirement), no data output is provided, then the watchdog shall trigger an interlock (VETO decision).

False decisions may have many causes. Consequently, to understand them (and correct them), it is needed to know what happened. This is the purpose of monitoring functions.

4.2.3 Functional architecture

At this synthesis step, the idea is to gather all the subfunctions (including safety-monitoring ones) and aggregate them in one single diagram. It is shown in Figure 4.9.

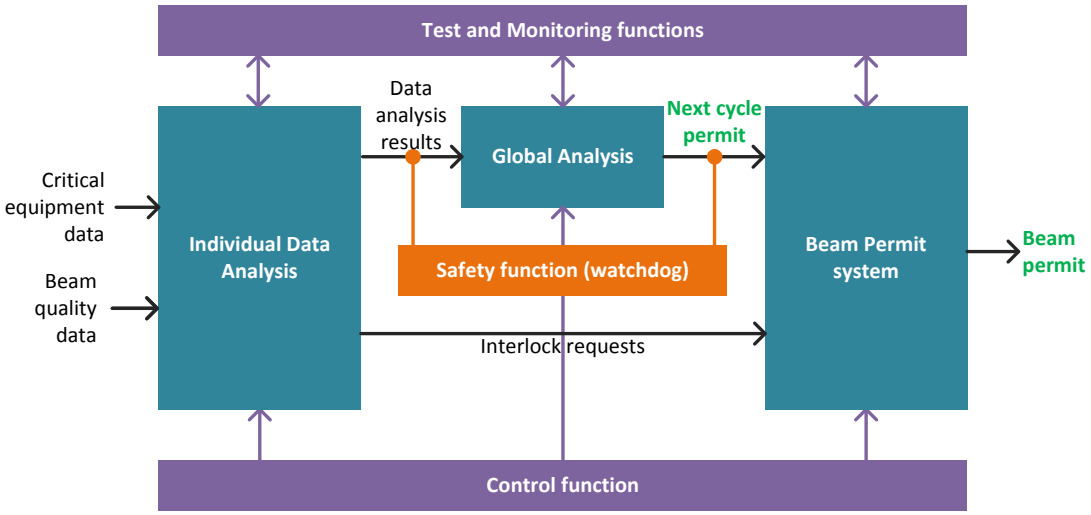

FIGURE 4.9: Functional architecture schematic

The IEEE standard suggests to verify that all concepts and requirements (defined in chapter 3) shall be reached with this functional architecture.

For the functional requirements, they are are reached because all of them are planned to be implemented via this functional analysis.

For the performance requirements, it is not possible at this stage to prove they are reached. However, they can be assigned to subfunctions. The response time requirements

have been already assigned via the time line schematics. For the dependability requirements, they are assigned to individual data analysis, global analysis and beam permit system subfunctions as they carry the Interlock System concepts.

4.3 Implementation proposal

Once the functional analysis has been performed, the last step is to propose the system implementation.

Following the divide and conquer paradigm, this section presents in a first part the subfunctions technical implementation. Then, it describes the system implementation within the machine. Finally, the last part presents the hardware modules design.

4.3.1 Subfunctions implementation

a. Beam permit loop

The beam permit loop is the technical implementation of the beam permit system subfunction.

It is implementing the *beam permit* binary signal in the form of a loop. This loop can be broken at each node. As soon as the loop is broken the *beam permit* falls to a VETO state.

The master node generates the beam permit loop signal. This signal is a pulsed binary signal at a defined frequency. On the loop back (after going via all the slave nodes), the master node checks if the frequency is still the same (with a configurable margin). If no, the master node breaks the beam permit loop (by stopping frequencies generations) and triggers an interlock. A latching system is proposed : to start (or restart after an interlock), the user must (re)arm the beam permit loop.

The slave node receives the beam permit loop and forwards it. Its only ability is to break the beam permit loop, from a local interlock signal.

The beam permit loop implementation is synthesized in Figure 4.10.

b. Threshold comparison

The individual data analysis is the technical implementation proposed is to perform threshold comparison.

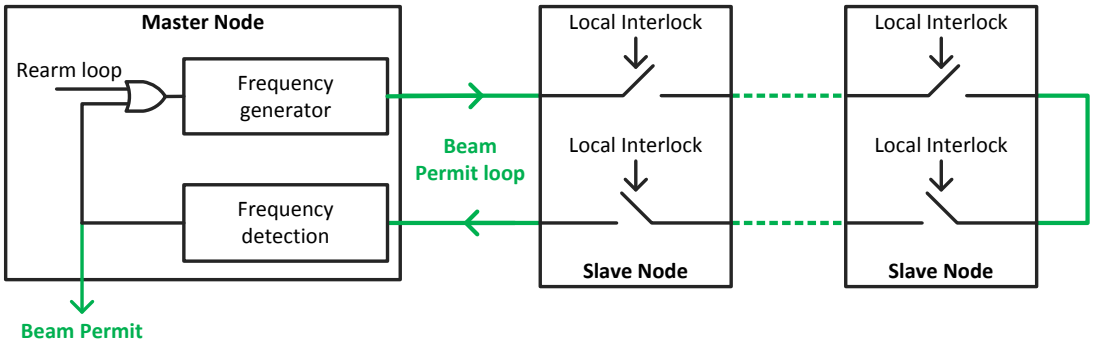

FIGURE 4.10: Beam permit loop implementation

Comparing the data with its related thresholds will lead to determine if the data is in its safe range or must trigger an interlock.

The thresholds are embedded in the hardware modules. These thresholds will be saved as well in an external database (CLIC data management service). When no beam, a cross check process is triggered to compare the embedded value with the one defined in the database. It is allowing to erase effect of SEU and to update these thresholds.

There are two questions arising regarding this proposal. First, why not accept binary signals only ? and at the opposite, why not handling more complex operations within the Interlock System ?

Binary signals only : The LHC Beam Interlock System accepts only binary signals as user inputs. In this case, the Interlock System design is simpler than the proposed one.

However, when investigating how these inputs are generated in the user side, it turns out threshold comparison are done [53], [54], [55].

Therefore, it has been proposed to integrate these threshold comparison within the Interlock System. The thresholds will still be defined by related field experts. The main advantage is the threshold comparison mechanism will be the same for each user. Thus, effort on reliability will be concentrated on one single threshold comparison mechanism.

Anyway, accepting data do not reject receiving binary signals, either between Front-ends (cf. Figure 3.9) or via the concentrator.

Handling more complex operation : More complex operations than threshold comparison could have been proposed. Indeed, operations like averaging, extremum finding, derivating, integration, would be sometimes used by users before delivering final data

to the Interlock System (e.g. beam position monitors, beam loss monitors). An option investigated was to integrate all of them in order to get rid of user inputs except the acquisition infrastructure (delivering the data).

Supporting in a generic way these operations would have added a lot of constraints for the Interlock System in term of technology choice, response time and reliability. Consequently, the choice has been to not support these operations.

However, on a case basis, it can be imagined some dedicated hardware used to perform some advanced operations before releasing the result to the Interlock System. Especially, if the Interlock System hardware modules are embedded in crates like VME, ATCA, μTCA, an option would be to have one (ore more) reserved slot(s) for this dedicated hardware.

c. Summarizers

To perform the global analysis, the technical implementation is proposed to be summarizers. They aim to synthesize the results of the threshold comparisons and deliver the *next cycle permit*.

In order to address the response time requirement, the goal is to perform several levels of synthesis. Consequently, the results of one summarizer can be entered in an hierarchically higher one. The synthesis operation consists in propagate the worst case (FAILURE > WARNING > SAFE). This is suitable for a tree-topology implementation.

Following global analysis subfunction specification, summarizers implement local rules.

4.3.2 System implementation

In this section, the goal is to gather the subfunctions implementation in one system.

As explained in section 3.5.1, the Interlock System starts with 48 dedicated front-end modules where data are received. At the other side, the *beam permit* has to be released to 6 targets systems (2 gun RF, 4 dumps systems at damping rings).

The first obvious choice is to have a master node generating the beam permit loops and to use the front-end modules as slave nodes. These modules host the threshold comparison. Thus, the nodes are linked by the beam permit loop and the interlock requests propagation is assumed. The master node assumes the *beam permit* delivering.

The second proposal is to have one layer of concentrator node to perform part of the global analysis. They are arranged in a tree topology, with the front ends as lower level

and the master as higher level. As there are 48 Interlock System front ends, receiving data from around 400 CLIC modules, it would have been too much data to send to the master and to make it perform the full post-pulse analysis. Thus, adding this layer decreases significantly the amount of data to send to the master node as it performs part of the post-pulse analysis. Moreover, as one concentrator node receives data from several front ends, more advanced local rules can be implemented in the global analysis.

Synthesizing this proposal, the CLIC Interlock System implementation is shown in Figure 4.11.

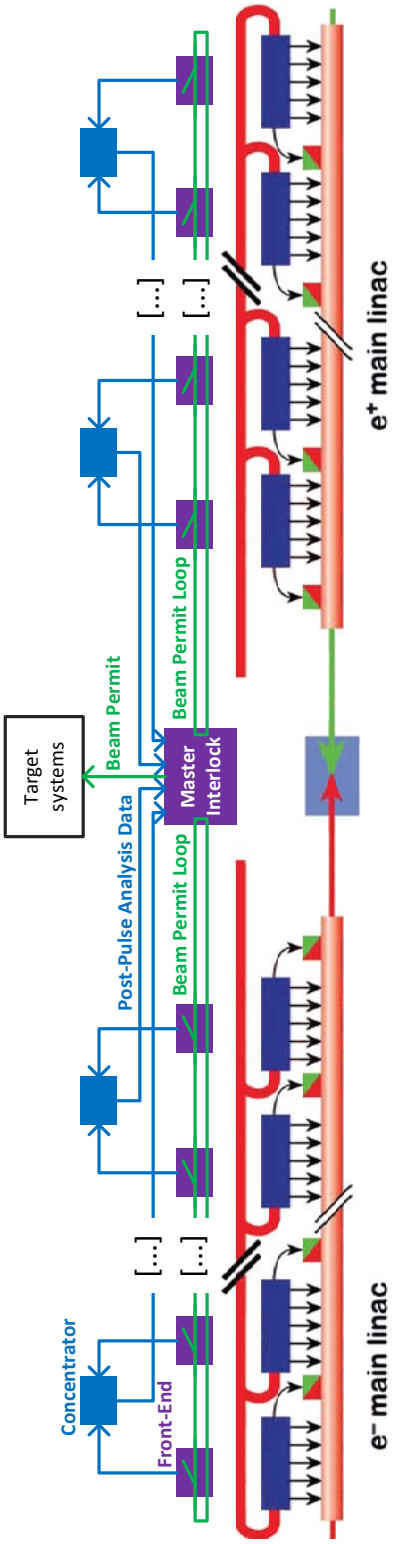

FIGURE 4.11: CLIC Interlock System implementation overview

4.3.3 Hardware modules

Once the system implementation has been proposed, the goal is to describe the elementary blocks of this implementation. The three types of nodes (slave, master, concentrator) are described. As the monitoring part is intended to be the same for each node, it is described apart.

a. Slave nodes

The slave nodes handle the threshold comparisons. A first part of the post-pulse analysis is done via a first layer of summarizer, useful to synthesize the data before sending them to the concentrator node.

They are implementing the slave part of the beam permit loop. It consists of repeaters, stopping their function on a local interlock request, which leads to loop opening. The advantage to use a repeater instead of a simple switch is that the beam permit loop frequency is regenerated, erasing the attenuation effect in the link between the nodes. Moreover, it allows to monitor the beam permit loop and thus informs locally the status of the global *beam permit*.

The slave node hardware module is represented in Figure 4.12.

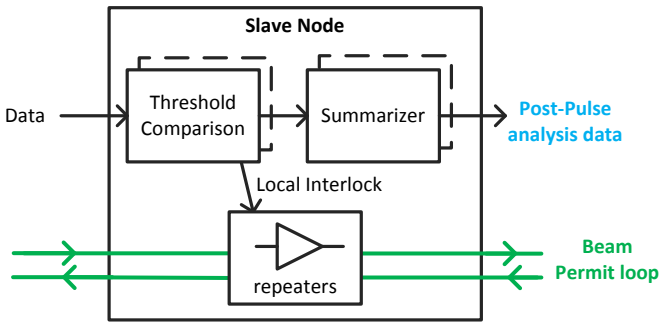

FIGURE 4.12: Slave node hardware module synoptic

b. Concentrator nodes

The concentrator nodes support a part of the post-pulse analysis via a second layer of summarizer. The synthesized data are then sent to the master node.

The concentrator node hardware module is represented in Figure 4.13.

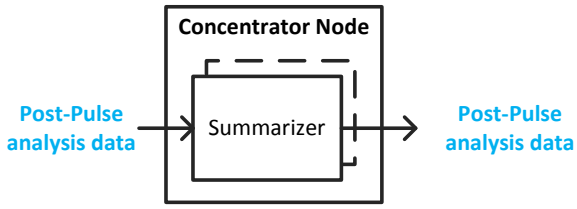

FIGURE 4.13: Concentrator node hardware module synoptic

c. Master node

The master node handles the beam permit loops frequency generation, one for the electron linac and the other for the positron linac. It assumes the frequency detection of these two beam permit loops. When the loop is broken (no frequency), the interlock trigger changes the *beam permit* state from PASS to VETO and stops generating the frequencies.

The master node assumes the final part of the post-pulse analysis. It implements the last layer of summarizer and generates the *next cycle permit*.

The master node hardware module is represented in Figure 4.14.

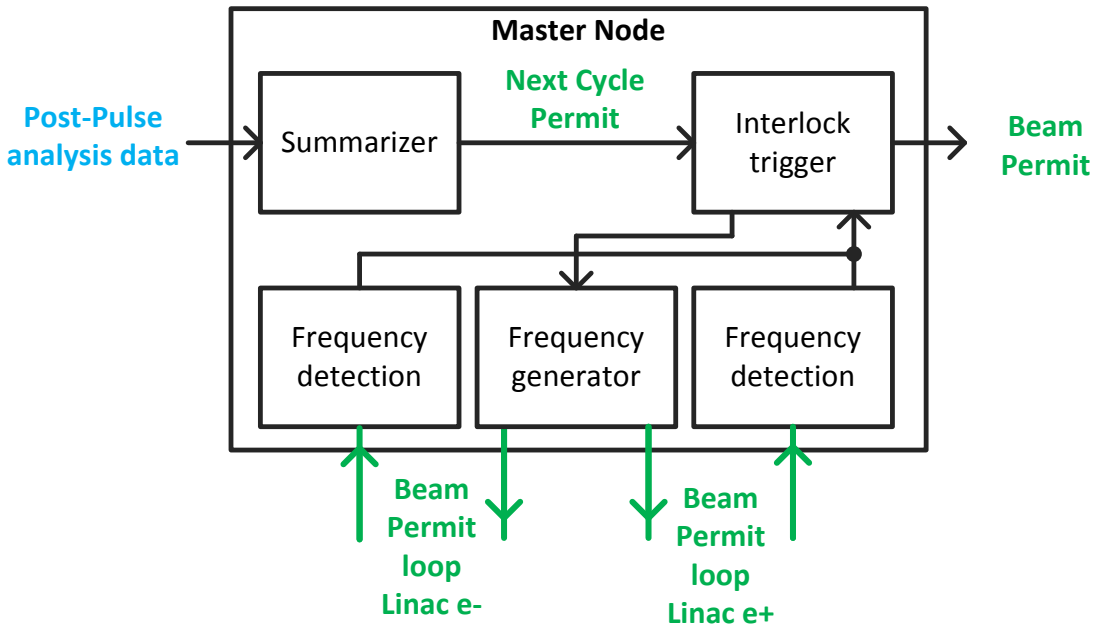

FIGURE 4.14: Master node hardware module synoptic

d. Nodes monitoring

The three types of nodes are proposed to be monitored in the same way. As illustrated in Figure 4.15, the Interlock System boards will be implemented in a crate. The crate technology will be the same as the acquisition and control infrastructure (shared support). The crates have a controller board that can communicate with the middleware. The controller board is able to communicate with the user boards through the crate bus (often implemented in backpanel). Usually, the communication is done through write-read of board registers and buffers.

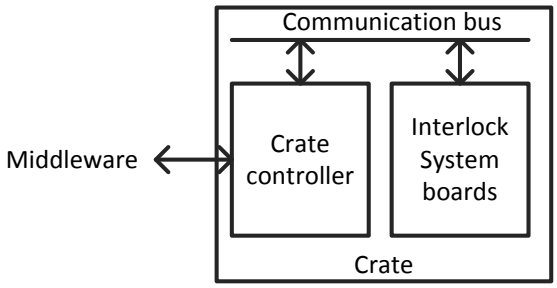

FIGURE 4.15: Nodes monitoring

4.4 Conclusion

This chapter has presented the design proposal for the Interlock System. A methodology has been employed based the IEEE standard in order to perform the functional analysis, which has lead to the implementation proposal.

To synthesize, a design has been proposed to fulfil the requirements. The systemic approach asserts that the design should theoretically works. The next step is to push forward and to prove that the design can, in practice, reach the requirements.

Chapter 5

Design verification

5.1 Introduction

At that point of the design process, the requirements have been established and a design has been proposed. The last step of the design process is to verify the proposal.

From the literature, design verification shall answer the following questions : *are we building the system right* [56] ? *does it work* [57] ? To answer them, two experiments have been performed. The first one aims to prove the concepts feasibility in operational environment. The second experiment is a hardware demonstration which aims to prove that performance requirements can be reached by the proposed design. Again, to place this chapter in the V cycle [39], it corresponds to the prototype step up to the system validation step.

At the first section, the feasibility study is presented and results are discussed. At the second section, the hardware demonstration is introduced, from the VHDL blocks to the whole test bench overview. The results are then discussed.

5.2 Feasibility study

The first experiment led in the verification process has been the feasibility study. The idea was to implement the concepts in an operational environment in order to get feedback on challenges and expectable issues.

There are two concepts to study, the beam permit loop and the post-pulse analysis. Concerning the beam permit loop, it has been implemented in the LHC Beam Interlock

System and is in operation since 2008. Thus, its feasibility has been already amply demonstrated.

Concerning the post-pulse analysis, it has never been implemented, even though some systems are similar [7], [31], [33]. Thus, the feasibility study has been undertaken for this concept.

5.2.1 Operational context

To perform the feasibility study in an operational context, the CLIC test bench has been the obvious choice. The CTF3 is an accelerator facility to demonstrate the feasibility of CLIC technologies. It is mainly focused on two points : the drive beam generation with appropriate time structure and fully loaded acceleration and the two beam acceleration scheme [58].

As illustrated in Figure 5.1, the CTF3 is made up of a drive beam linac, delivering 150MeV electrons. The source is a thermionic RF gun. The CTF3 implements a recombination complex with a delay loop and a combiner ring, enabling a maximum recombination factor of 8. The beam is then release to the CLEX, the experimental area. It is comprising several experimental studies. There is the *test beam line* experiment (TBL in the Figure 5.1) which aims to prove the 90% energy extraction with PETS can be achieved. There is the *two beam test stand* (TBTS in the Figure 5.1) which aims to prove the low breakdown rate of the accelerating structures with the two beams approach. Finally, the *califes* experiment is used to emulating a main beam and is used to study RF guns (based on laser instead of thermionic RF).

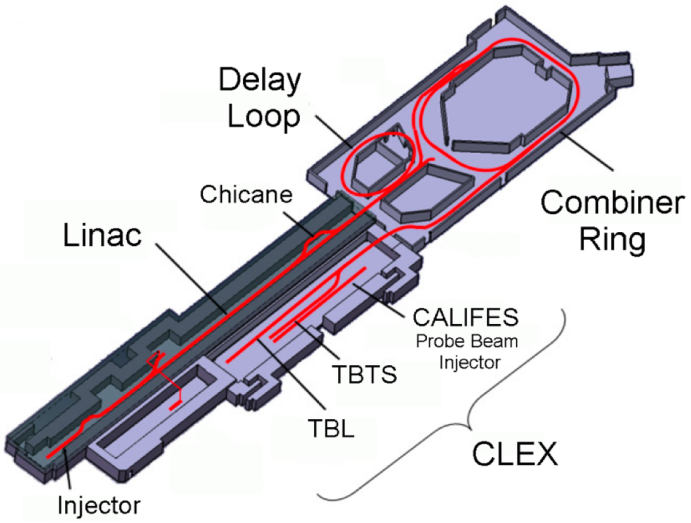

FIGURE 5.1: CTF3 general layout

Concerning the protection of this facility, there is to note the beam is mainly not harmful for the machine. Indeed, the energy per beam pulse is 3 order of magnitude lower than in CLIC case with a repetition rate ten times lower [59]. However, the beam can still damage some structures (e.g. the vacuum valves). In addition, repetitive beam losses can lead to unacceptable radiation levels for personal safety. Consequently, several protection mechanisms have been implemented.

There is a central Interlock System implemented in CTF3. It is a PLC which controls the gun (beam source) and can inhibit it. The klystrons (RF sources to accelerate the beam in the linac) are protected by a hardware Interlock System linked to the gun PLC. The vacuum valves are protected by a software mechanism. It checks if the selected beam path is not blocked by any vacuum valves. Otherwise, the mechanism does not allow the gun to start. In the same way, a software mechanism checks continuously the vacuum level (by threshold comparison). Concerning the beam losses, two JAVA applications are implemented. The first checks the beam losses at the experimental area and disables the gun when there is too much repetitive losses. The second one monitors the radiation level (induced by beam losses) and inhibits the gun before the radiation reach an unsafe level.

5.2.2 Experiment

The idea is to apply the concept of post-pulse analysis in CTF3. The main goal is to collect data and feedback on its use in an operational context. A secondary goal is to improve the CTF3 beam operation, in term of beam availability.

As there is already an Interlock System implemented, the decision has been to not add an extra layer of hardware on it. Indeed, the main requirement of CTF3 is to provide stable beams to the experimental area. Thus, installing hardware is considered only if needed. An extra prototype layer would have decreased the machine availability and thus, is not acceptable.

Consequently, the decision has been taken to apply the concept via a software application. It has the advantage to need less development time and to be more flexible than hardware. However, it has the disadvantage to not be in real-time (software response time is in the order of the second). Due to team experience and support, the JAVA language has been selected.

a. Operational purpose

The CTF3 environment is operationally functional. The first goal has been to find a purpose for the application to apply the post-pulse analysis concept. It has been pointed out that vacuum leak events have occurred and have decreased the CTF3 beam availability. The average downtime for these events during one year is around 3 days. In Table 5.1 are listed the registered events during 2009 and 2011. The registration is done by operators on a log book (logbook page). With the assumption of 200 days of operation, vacuum leak events lead to 1.5% of downtime every year.

TABLE 5.1: CTF3 vacuum leak events

Event	**date (elogbook)**
Delay loop vacuum leak	28.07.2011 09h06
Combiner ring vacuum leak	23.05.2011 14h49
Delay loop vacuum leak	22.03.2011 11h56
Combiner ring vacuum leak	02.09.2010 09h06
Combiner ring vacuum leak	09.11.2009 09h33
Delay loop and Combiner ring vacuum leak	02.03.2009 11h04

One possible cause of these vacuum leak events are repetitive beam losses at same location. Moreover, during night beam operation, beam operation can be stopped by an interlock request. When safe conditions come back, the beam is automatically sent back in the machine at nominal energy. This could be one cause of these vacuum leak event.

b. Application principle

Considering information described at previous paragraph, the application has been proposed to perform an **automatic procedure to restart the beam with safety considerations**.

The principle is, after a beam stop, when condition are safe and no operators are present to supervise CTF3 operation (automatic mode, during night), to send predefined low energy beams (through tuning the beam length). At each pulse, the application checks (post-pulse analysis) if the beam has behaved as expected (beam position and radiation levels). Once the nominal level reached, the application releases the beam control to the standard tools. This principle is summarized in a synoptic in Figure 5.2.

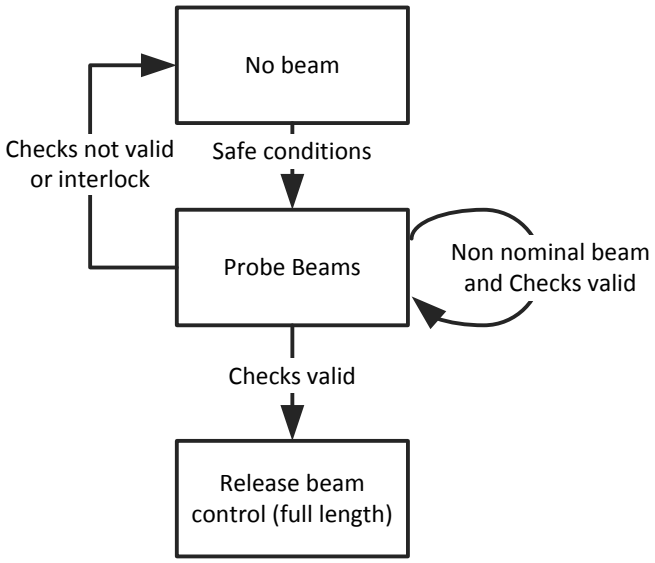

FIGURE 5.2: Application principle synoptic

5.2.3 Technical description

Once the application principle has been explained, the next step is to describe its technical development.

a. Conditions

The application is activated when the CTF3 is interlocked. To restart the beam, the application needs to wait for safe conditions. It is conditioned by valve protection mechanism and klystron Interlock System. The application looks at the gun PLC inhibition input to evaluate the safe conditions.

b. Hardware checks

In addition of safe conditions, additional hardware checks on klystrons are made before restarting the gun. The first check is the voltage value of the pulse-formed network (part of a klystron, LC-filters in cascades delivering a high voltage, high power square pulse). The voltage must be equal (with a configurable margin) to the command. Indeed, reaching in a stable way this voltage requires time and must be accomplished before the beam operation. The second check is the status of the klystron (normal, stand-by, heating or interlock status). Finally, the last check is the automatic rearming procedure. When a klystron has tripped, there is an automatic procedure (not always enabled) which will restart the klystron. The beam must not be restarted if one klystron is being restarted.

c. Beam operation

The main idea of the application is to send several probe beams before allowing the nominal one. Thus, three beams have been defined. The full (or nominal) beam is made up of 8 polarized trains (each train is composed of bunches and a bunch is composed of particles). Two consecutive trains have opposite polarization. It allows to detect which train must be sent in the delay loop and which one must not.

The *first beam* corresponds to the first train, which will go in the delay loop. It aims to test beam stability with the delay loop. The *second beam* is the second train alone. It allows to test beam stability without the delay loop. The *third beam* corresponds to the eighth train. It aims to check beam general stability at the end of the beam (some drifts may occurs between the start and the end of the beam). These staged beam are represented in Figure 5.3.

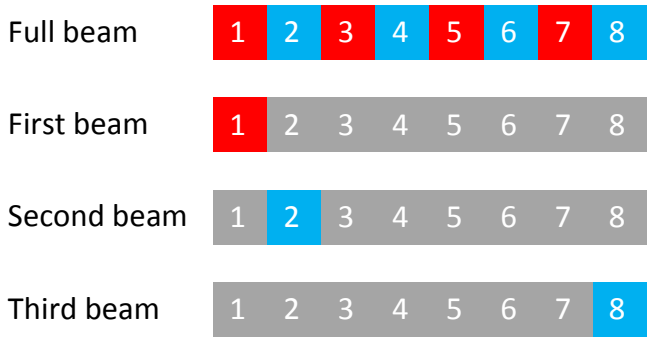

FIGURE 5.3: Application probe beams

Once it is safe to restart the gun, the application configures the *first beam* via the gun PLC and restarts the gun. Then the post-pulse analysis concept is used.

d. Post-pulse analysis

Once a probe beam is sent in the machine, its behaviour is analysed. The post-pulse analysis is based on two types of monitors : beam position and radiation. The monitors used are located at strategic places. Concerning the beam position monitors, there are located at the linac, after the delay loop, at the combiner ring, at the output of the combiner ring and at the experimental area. Concerning the radiation monitors, there are located around the recombination complex where radiations are more likely to occur (synchrotron radiations, kicker extraction/injection). This is represented in Figure 5.4 (printscreen of the JAVA application), the green rectangles are the radiation monitors and the red and grey ones are the beam position monitors.

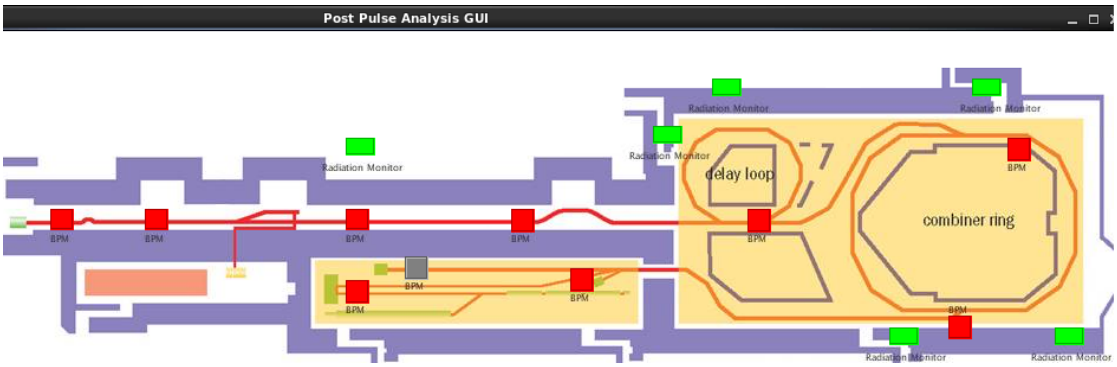

FIGURE 5.4: Application post-pulse analysis GUI

The post-pulse analysis with beam loss monitors is based on three sub-analysis. The first one consists into measuring the maximum value of the the beam intensity and then a threshold comparison is done to ensure there are not beam losses (a too low intensity would mean not enough particles or a recombination system not working).

The second sub-analysis measures the beam length and again, compares it to a predefined threshold. It is a second way to detect beam losses. Indeed, the expected intensity can be reached but not on the whole beam length.

Finally, the third sub-analysis looks at the integrated value, which gives the number of particles per beam (in nC). A threshold comparison is done as well. This last sub-analysis is a combination of both firsts to detect losses but it has the disadvantage to be more complex to implement (need to integrate a signal, which is less easy than threshold comparison for a FPGA). In Figure 5.5 is shown a part of the application General User Interface (GUI) for the beam position monitors.

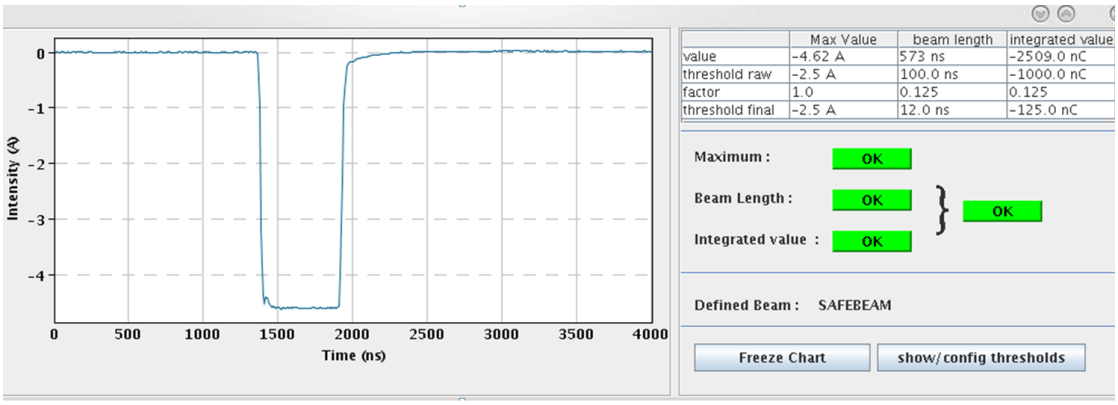

FIGURE 5.5: Application beam position monitor GUI

The post-pulse analysis with radiation monitors is based on two sub-analysis. The first

checks the maximum value of radiation measured and compares it to a predefined threshold. The second checks the mean value by threshold comparison again. This measurement is done every 120 s, so it is needed to wait this time before validate the post-pulse analysis for one probe beam. In Figure 5.6 is shown part of the application GUI for the radiation monitor.

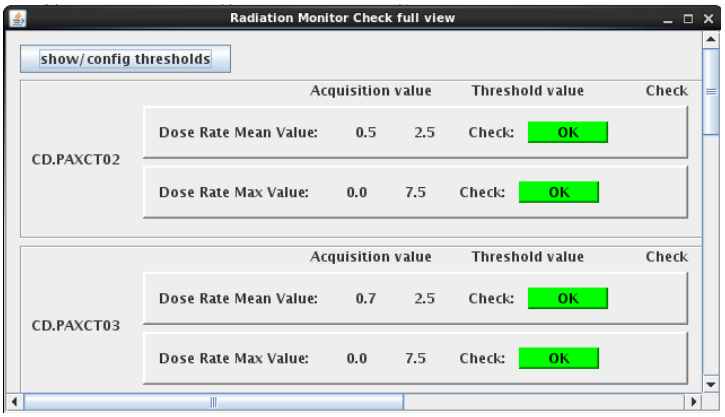

FIGURE 5.6: Application radiation monitor GUI

e. Logging facility

To understand what is happening when the application runs, two logging mechanisms have been developed.

The first logging mechanism aims to debug the application (typically useful for JAVA developers). It is logging all the action performed by the application. for instance, when the user would open a sub-interface, it will be logged in this facility.

The second logging mechanism (called logbook) aims to collect any data related to the restart procedure. More precisely, it will mainly gather the data of the post-pulse analysis. For instance, each time the post-pulse analysis is not successful, it will investigate which device and which threshold comparison have made it fail.

f. Thresholds management

The post-pulse analysis is based on thresholds comparison. As explained hereunder, they need to be configurable and dynamic.

Concerning the beam position monitors, their locations must be taken in account for the threshold definition. For instance, the beam intensity value will not be the same before or after the delay loop. Thus, the thresholds must be configured in accordance.

There are two reasons to have dynamic thresholds. The first reason is the beam operation performed by the application. It modifies the beam length and thus, this change must be impacted on the thresholds. The second reason is the CTF3 operation mode. It often happens that the delay loop and/or the combiner ring are not used, resulting in a different beam dynamics. These changes must be integrated in the threshold mechanism.

To make the threshold dynamic, the application implements a factor mechanism. The factors are lively computed, in function of machine operation and beam length. The factors modify the raw thresholds to give the applied thresholds. This factor mechanism can be seen in Figure 5.5, on the top right table.

5.2.4 Results and discussion

Once the JAVA application has been developed, it has entered in a test and improve process. CTF3 is a complex environment and has required several improvements of the application.

Nevertheless, The application have been tested several times. In Figure 5.7 is shown the logbook extract of the application with a failure of the post-pulse analysis. The failure had been caused by a beam position monitor, which was not correctly windowed. In Figure 5.8 is shown the logbook of a successfully post-pulse analysis. The succession of probe beams can be noted.

```
Thu Mar 28 12:22:48 : set Beam to: FIRSTBEAM
Thu Mar 28 12:22:48 : change Of Beam Length Started
Thu Mar 28 12:22:48 : change Of Beam Length Started
Thu Mar 28 12:22:48 : change Of Beam Length Finished
Thu Mar 28 12:22:49 : Controller=> FastPostPulseAnalysis failed, countdown is: 2
Thu Mar 28 12:22:49 :         Investigation level1 PPA False=> BPMs check guilty
Thu Mar 28 12:22:49 :         Investigation level2 PPA False => CB.STBPM1030S
checkIntegratedSamples guilty (value observed: -176.77499999999998 / ref value: -250.0)
Thu Mar 28 12:22:49 :                          ----------
Thu Mar 28 12:22:49 :         Investigation level2 PPA False => CC.STBPM0130S
checkBeamLength guilty (value observed: 0 / ref value: 0)
Thu Mar 28 12:22:49 :         Investigation level2 PPA False => CC.STBPM0130S
checkIntegratedSamples guilty (value observed: NaN / ref value: -0.0)
Thu Mar 28 12:22:49 :                          ----------
```

FIGURE 5.7: Application logbook - post-pulse analysis failure

From the application test, several comments can be done :

The threshold management is not a trivial part for the post-pulse analysis. The first challenge is to define them accurately. In the application, they have been defined for nominal conditions (full beam, delay loop and combiner ring used), but with consideration

```
Mon Aug 12 11:11:21 : Controller=> Application set by user Active : true
Mon Aug 12 11:11:25 : Controller=> Application is armed now
Mon Aug 12 11:11:25 : set Beam to: SAFEBEAM
Mon Aug 12 11:11:25 : change Of Beam Length Started
Mon Aug 12 11:11:25 : change Of Beam Length Finished
Mon Aug 12 11:11:39 : Controller=> the Klystron are enough stable to rearm the gun
Mon Aug 12 11:11:39 : set Beam to: FIRSTBEAM
Mon Aug 12 11:11:39 : change Of Beam Length Started
Mon Aug 12 11:11:39 : change Of Beam Length Finished
Mon Aug 12 11:11:41 : Controller=> Start the Timer to have a new radiation mean value
Mon Aug 12 11:12:02 : Controller=> Post-Pulse Analysis are valid and stable
Mon Aug 12 11:12:02 : Controller=> there are no radiation issue (mean value), beam can be
increased
Mon Aug 12 11:12:02 : Controller=> increase Beam trigger: FIRSTBEAM to be increased
Mon Aug 12 11:12:02 : set Beam to: SECONDBEAM
Mon Aug 12 11:12:02 : change Of Beam Length Started
Mon Aug 12 11:12:02 : change Of Beam Length Finished
Mon Aug 12 11:12:03 : Controller=> Start the Timer to have a new radiation mean value
Mon Aug 12 11:12:23 : Controller=> Post-Pulse Analysis are valid and stable
Mon Aug 12 11:12:23 : Controller=> there are no radiation issue (mean value), beam can be
increased
Mon Aug 12 11:12:23 : Controller=> increase Beam trigger: SECONDBEAM to be increased
Mon Aug 12 11:12:23 : set Beam to: THIRDBEAM
Mon Aug 12 11:12:23 : change Of Beam Length Started
Mon Aug 12 11:12:24 : change Of Beam Length Finished
Mon Aug 12 11:12:25 : Controller=> Start the Timer to have a new radiation mean value
Mon Aug 12 11:12:45 : Controller=> Post-Pulse Analysis are valid and stable
Mon Aug 12 11:12:45 : Controller=> there are no radiation issue (mean value), beam can be
increased
Mon Aug 12 11:12:45 : Controller=> increase Beam trigger: THIRDBEAM to be increased
Mon Aug 12 11:12:45 : set Beam to: FULLBEAM
Mon Aug 12 11:12:45 : change Of Beam Length Started
Mon Aug 12 11:12:45 : change Of Beam Length Finished
Mon Aug 12 11:12:45 : Controller=> Application success the ramping procedure
```

FIGURE 5.8: Application logbook - post-pulse analysis success

of the device location. The second challenge is to establish the dynamic factors to match with the operation.

As described, information about the beam and machine operation is critical. In the application, these information were available on the technical network (via middleware). In the CLIC case, these data must be transmitted in a dependable way. The middleware is not considered as dependable enough for mission-critical system. A suggestion (to implement in the next iteration of the design process) is to integrate a safe machine parameter system's like within the Interlock System. Technically, extra gigabyte links (through optical fiber) can be set up between the nodes, in the same way than the beam permit loop. The data would be generated by a safe machine parameter generator. It can be considered to implement this data transmission in a form of a loop. In this way, as long as the signal is received by the generator on the loop back, it would ensure that every nodes received the parameters. This proposition is represented in Figure 5.9. There is to note the safe machine parameter generator could be integrated in the master node. The order of the node in the safe machine parameter loop has not any importance.

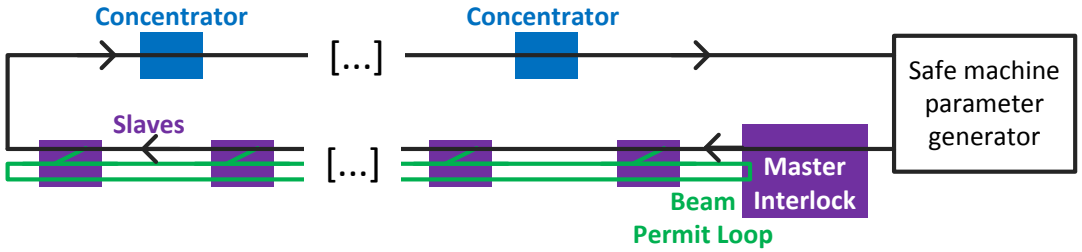

FIGURE 5.9: Suggestion of the safe machine parameter integration

The last topic to discuss about this feasibility study is the post-pulse analysis. In the application, as there are not a lot of steps between the first beam and the nominal beam, it has been affordable to wait 120 seconds to get the radiation mean value. In CLIC case, it is not considerable because there are more steps between the safe beam and the nominal one (estimated around 5000 steps). Consequently, others ways must be found to get equivalent data to check beam losses. The obvious way is the beam loss monitors. The second point about the post-pulse analysis is the computations which have been done in the application. For instance, to get the number of particles (nC), integration of a signal has been needed. This type of computation cannot be natively undertaken by the proposed Interlock System. Consequently, it is required from input users to deliver the data ready to be compared. The time taken to perform this custom computation must be taken in account for the response time requirement.

As a general conclusion of this feasibility study, it has been possible to apply the post-pulse analysis. Several differences with CLIC environment have been pointed out. However, these are not blocking issues and the post-pulse analysis is therefore considered as feasible for the CLIC project.

5.3 Hardware demonstration

At this step of the design process, both concepts have been defined as feasible and a design has been proposed. This step aims to verify the proposed design can reach the established requirements.

This section explains why a hardware demonstration has been selected to perform the verification. It explains the hardware demonstration and its goals. As the hardware selected is based on FPGA, VHDL blocks have been developed and are therefore presented. Their different arrangements in FPGA-based boards are then shown. Next, the test bench and measurement principles are explained. Finally, the measurements and discussion are presented.

5.3.1 Technical discussion

To perform the verifications, several options have been considered : pure software simulation (JAVA), hardware description language for analog and mixed-signal applications (VHDL-AMS [60]) and hardware demonstration with extrapolation. A brief review of these options is given in the next paragraphs.

JAVA is an object-oriented language. This option is interesting because of the language flexibility, low maintenance, community support, productivity. However, JAVA is a high level language, is based on a virtual machine and thus has very low access on the host hardware. Virtual machines with real-time have been specified [61] but safety critical JAVA programming is not mature [62] even though it has been studied. To conclude, the JAVA option is conceivable for a system simulation. However, it is not suitable to implement the Interlock System.

VHDL-AMS is a language to describe digital, analog and mixed-signal systems. It is an extension of VHDL language. VHDL-AMS allows to describe the composition of a system and the interconnection between each sub-systems [63]. It gives the opportunity to simulate the design of a system, with the needed level of abstraction [64]. It is faster and cheaper than a hardware prototype.

The last option considered is a hardware demonstration. It has the advantage to allow direct measurements instead of simulation. Thus, unexpected issue may be found and weak points of the design may be pointed out. However, as specified in [64], the use of a prototype does not guarantee the quality of the system. This is why the measurements done on a hardware demonstration would aim to verify precise points (and not the whole system quality).

Several technologies are suitable for Interlock Systems implementation : PLC, FPGA, microcontroller, ASIC. For the CLIC Interlock System, the technology choice is a tradeoff between the dependability, the cost, the response time and the flexibility of the technology. As the CLIC Interlock System is not going to be built in the next 5 years, some new technologies may arise and may fit better the Interlock System requirements. However, if the technology choice should be taken currently, the FPGA option will be most likely chosen as it offers a good balance between the mentioned attributes. In addition, if the system complexity grows up, a FPGA can implement softcore processor [65] [66] [67] to handle more complex operations.

To synthesize, the VHDL-AMS and JAVA options would simulate the whole system to perform the verification. The VHDL-AMS option has an advantage because the reusability of VHDL code (in case of FPGA option for the technology choice). However,

to make the simulations accurate, it would require the knowledge of the precise layout of the implementation. As the precise layout is not known at this time of the CLIC Interlock System project, the simulation would be lead with a given level of abstraction.

Finally, for the verification step, the hardware demonstration has been selected for several reasons :
- Direct measurements on precise points can prove that the performance requirements can be reached.
- Technology choices had been already defined for the acquisition and control infrastructure (gigabyte link). Thus, it is an opportunity to start to integrate this technology in the Interlock System.
- The hardware demonstration will be a basis for an Interlock System prototype. It will facilitate the integration in a operational environment.

Nevertheless, for future iterations of the design process, the verification step will aim to check the system quality. The use of VHDL-AMS would be recommended to test in a exhaustive way the system functionalities.

5.3.2 Goals

The primary goal of the hardware demonstration is to demonstrate the requirements fulfilment for the proposed design. There are four performance requirements to measure :
- The response time related to the machine interlocking : 2 ms
- The response time related to the post-pulse analysis : 6 ms
- A false VETO rate for a node inferior to $1.10^{-6}.h^{-1}$ with the 2 out of 3 redundancy.
- A false PASS rate for a node inferior to $3.10^{-6}.h^{-1}$ with the 2 out of 3 redundancy.

The hardware demonstration is a down-scaled Interlock System applying the design proposal. The test bench has been set up to measure its attributes.

The secondary goal is to build a prototype. As written in the thesis problematic definition, the goal is to finish the process by being ready to work on the detailed design. In practice, the prototype has been conceived to be ready to integrate an operational environment.

5.3.3 VHDL blocks description

The VHDL blocks have designed following two needs. On one hand, the thresholds comparison, the summarizer and the beam permit loop VHDL blocks have been inspired by the design proposal and more precisely, by the subfunctions implementation. As they are interlock function carriers, they have been carefully tested and optimized to facilitate

their re-usability in the next prototype generation. On the other hand, the monitoring, the control and the gigabyte link VHDL blocks have been design for the test bench needs.

The VHDL blocks are presented in the following sections.

a. Threshold comparison

The threshold comparison VHDL block has been directly inspired by the subfunction technical implementation. It aims to perform a threshold comparison on one defined data. The goal is to have a simple block that will be duplicated for each data, leading to ensure the individual data analysis subfunction.

In Figure 5.10 is shown the block diagram. It takes as input a data flow. This data flow is common to all threshold comparison blocks of one board and contains the data to analyse for each of them. An acknowledgement signal is provided to trigger the data readout.

The block has two outputs. The beam quality analysis delivers, through a vector, the threshold comparison result. The vector contains the block identifier number and the result. The identifier number is used for monitoring purpose. The second output is the interlock decision. It is a binary signal triggering an interlock request if the threshold comparison has given a VETO decision. These two outputs are paired with acknowledgement signals.

The block is configurable through four fields (known as *generic* in VHDL). The first field is the *threshold*. The module will use it to detect unsafe data. The second field is the *data header*. It is used to detect which incoming data must be analysed. The third field determines which *type of data* is expected (critical equipment or beam quality related). It acts on the interlock decision behaviour (a beam quality related data will not trigger an interlock at the threshold level but may do it at the summarizer level). The last field is the block *identifier number*.

The VHDL block implements a Finite State Machine (FSM). As the block has been kept simple, it only implements four states as it can be seen in Figure 5.11. In few words, the block waits for its defined data, performs the threshold comparison and releases the results.

An extract of the VHDL code can be found in the annex.

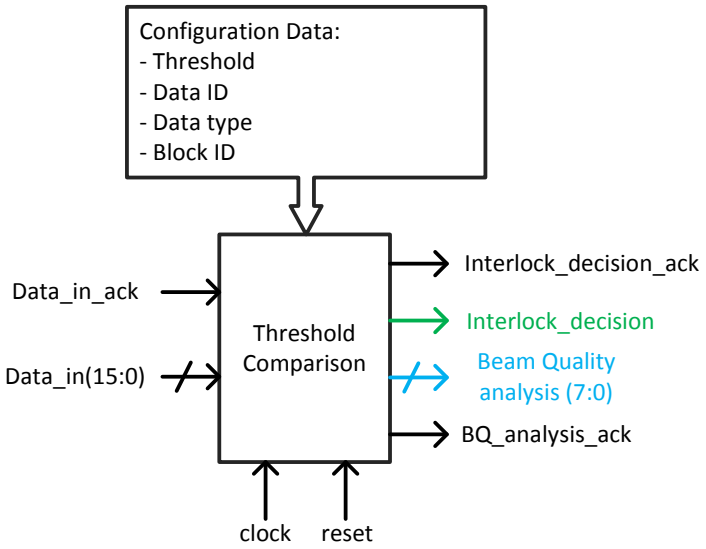

FIGURE 5.10: Threshold comparison VHDL module - synoptic

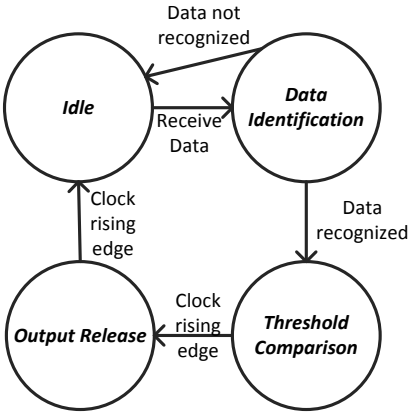

FIGURE 5.11: Threshold comparison VHDL module - state machine

b. Summarizers

The summarizer VHDL block has been inspired by the subfunction technical implementation as well. The goal is to have a simple block that can be chained with others to perform the global analysis function. A summarizer block aims to synthesize a bunch of threshold comparison or previous summarizers results. The last summarizer generates the *next cycle permit*.

In Figure 5.12 is shown the block diagram. It takes as inputs the results of previous blocks (with their acknowledgement signals) and a new pulse signal. This input indicates when a new pulse (emulated in the hardware demonstration) is happening. If the block did not receive all its input data before this new pulse, it means one of them was lacking

and thus deliver a fail-safe result. This watchdog mechanism is directly applied from the safety function analysis at chapter 4.

If none input data is lacking, the block forwards the worst case input (with a acknowledgement signal). The block identifier is added for monitoring purpose. If it is the last summarizer block, it is generating as well the *next cycle permit*.

The block is configurable through four fields. The first field conditions the *number of input data* to summarize. The second field specifies if the block is the last and shall generate the *next cycle permit* (if not, the *next cycle permit* output is always TRUE). The third field specifies if the local rule 1 shall be used. This local rule 1 allows the block to not deliver a fail-safe value if only *one* data is lacking. Other local rules could be implemented in the same way. Finally, the last field is the block identifier number.

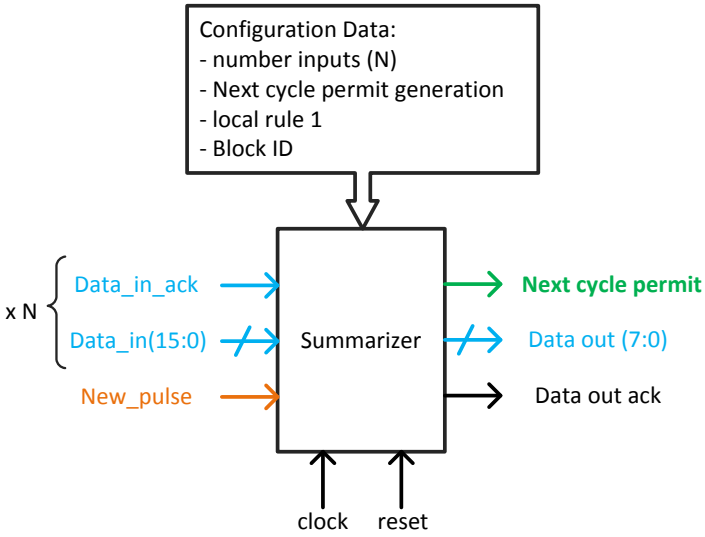

FIGURE 5.12: Summarizer VHDL module - synoptic

The VHDL block implements a FSM. It has four states as it can be seen in Figure 5.13. On a new pulse notification, it waits to collect the data input. Once it is done, it is looking for the worst case to forward it. When two input cases are similar, it forwards the first one. The watchdog function forces the block to release the fail-safe value if all input data have not been received at the end of the inter-cycle (between two pulses).

An extract of the VHDL code can be found in the annex.

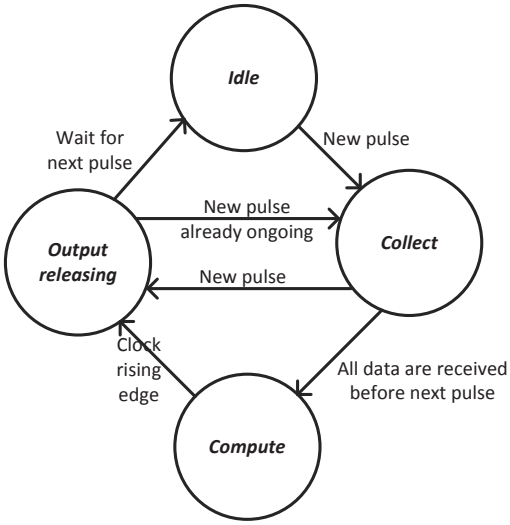

FIGURE 5.13: Summarizer VHDL module - state machine

c. Beam permit loop

The beam permit loop VHDL block has been inspired by the LHC Beam Interlock System (introduced in the state of art).

As seen in the subfunction technical implementation, the beam permit loop VHDL block has two implementations : master and slave. The master implementation generates a frequency (the beam permit loop signal) and checks if this signal is still here at the end of the loop. The slave implementation monitors the frequency signal and repeats it. It has the ability to stop to repeat the signal and consequently, to break the loop.

In Figure 5.14 is shown the master implementation synoptic. It is made up of a frequency generator, able to produce a 10MHz signal, a frequency detector, measuring the frequency every 5 μs and a block manager. The frequency to generate (and receive) is defined by a configurable field. The frequency validity measurement has also a configured margin. As input, it receives the interlock master, which can inhibits the frequency generation. The interlock local output reflects the *beam permit* state, regarding the frequency measurement. The rearm input is used to restart the frequency generation. Indeed, when (re)arming the loop, the frequency generator cannot be inhibited during a defined lapse

of time (via the *initialization time* configurable field), even though the frequency detector is not measuring a valid frequency. Finally, the block has the beam permit loop input and output.

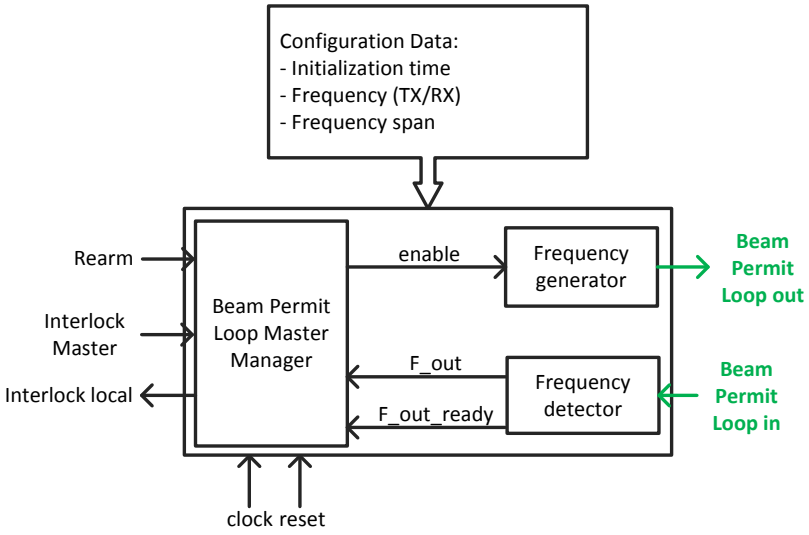

FIGURE 5.14: Beam permit loop VHDL module - master synoptic

The master block manager implements a FSM, represented in Figure 5.15. When (re)arming, it waits for a defined time. After this time has elapsed, if the frequency is still not valid, it goes back to the interlock mode. If the frequency is valid, it goes to lock state and keep generating the frequency. It stays in this state as long as the frequency measurement is valid.

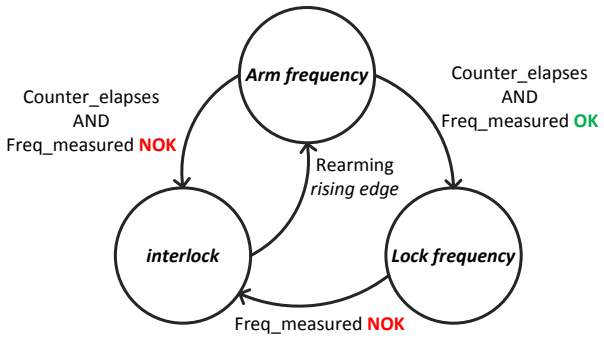

FIGURE 5.15: Beam permit loop VHDL module - master state machine

In Figure 5.16 is shown the slave implementation synoptic. It is made up of two frequency detectors (one for each beam permit loop input), two repeaters, able to repeat or to break the loop and finally a block manager. The inputs and outputs are similar to the master implementation but there is not the rearm signal. There is to note there are four beam permit loop signals (two signals per sense, as the loop does a go and back). The slave block is configurable in the same way than the master block (frequency to receive, margin

on the frequency validity measurement and initialization time), but it can be specified as *single ended*. It means the block is the last of the beam permit loop and have to loop back internally the beam permit signal (rather than loop it externally).

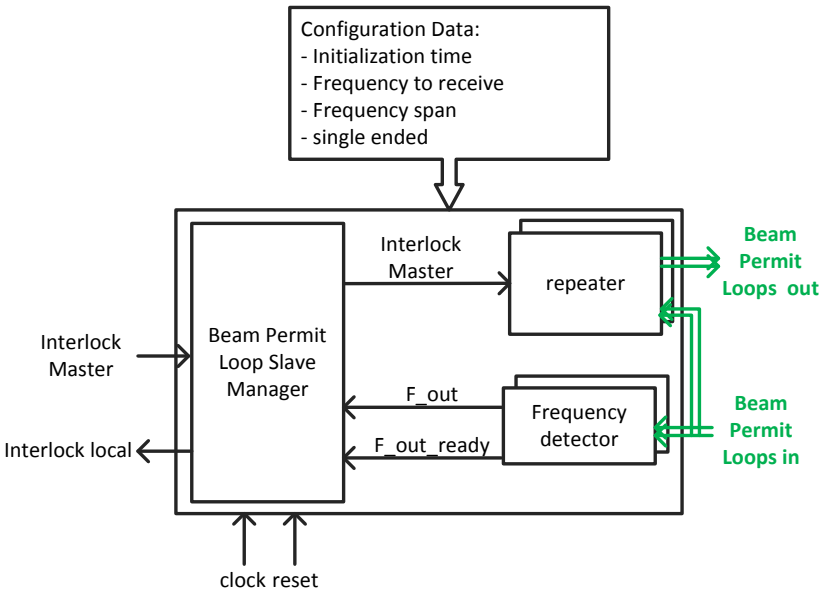

FIGURE 5.16: Beam permit loop VHDL module - slave synoptic

The slave block manager implements a FSM, represented in Figure 5.17. When a frequency detector gets a correct frequency, it waits for the signal to go through all the (hypothetical) following slave nodes. After that *initialisation time*, both frequency detectors must have measured a valid frequency. Otherwise, it goes back to the interlock state. There is to note the slave block does not need to be rearmed after an interlock request. Only the master implementation needs it.

Concerning the frequency detection, the used method is to count the number of rising edges of the beam permit signal on a specified time windows. The time window choice is a trade-off between response time and accuracy. The windows time has been selected to be 5 μs. There is another method which can be implemented (and can decrease the response time for few μs). This second method consists in measuring the number of clock rising edges during one period of the beam permit signal. This is to be considered for upgrade.

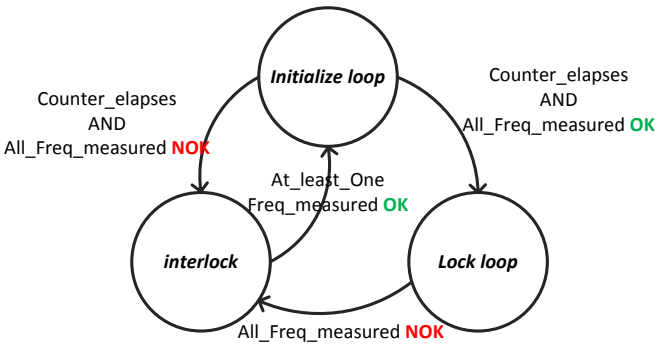

FIGURE 5.17: Beam permit loop VHDL module - slave state machine

d. Monitoring

For the hardware demonstration, it is needed to monitor the boards. As explained later at section 5.3.5, the hardware chosen has an USB Universal Asynchronous Receiver Transmitter (UART) port, which is seen by the FPGA as a standard serial link. Due to its facility to use (driver supported by Labview), this port has been chosen to monitor the board.

The VHDL block synoptic is represented in Figure 5.18. The monitoring block is based on a 8 kBits dual ports Random Access Memory (RAM). Monitored data are register in this RAM (through the monitor block manager). The RAM is continuously read and its data is send to the serial port.

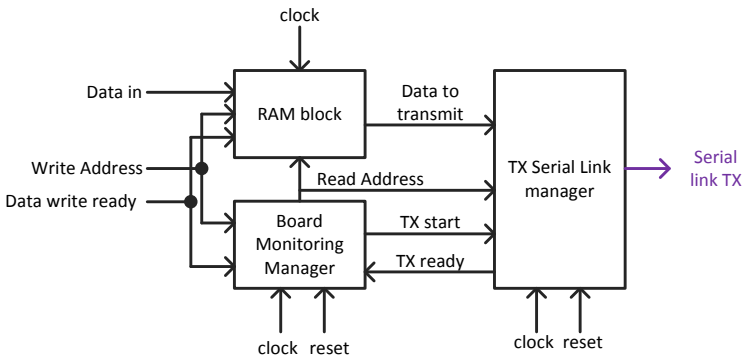

FIGURE 5.18: Board monitor VHDL module - synoptic

The monitor block manager implements a FSM, represented in Figure 5.19. The manager is responsible to perform a continue readout of the RAM. It takes care to not have read-write access conflict.

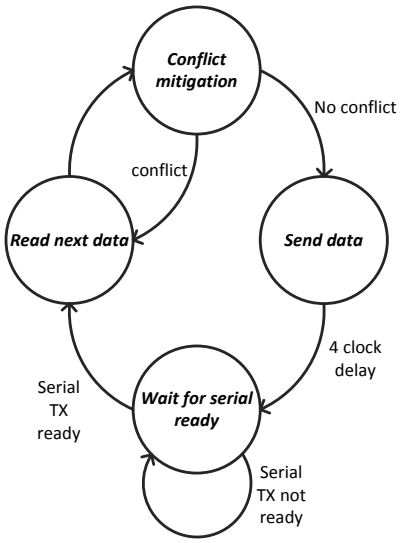

FIGURE 5.19: Board monitor VHDL module - state machine

This monitoring block reaches the hardware demonstration needs. However, for the final Interlock System, this block shall be enhanced. For instance, the communication speed can be raised (currently fixed at 19200 Bauds).

e. Control

In the same way than monitoring, there is a need to control the boards in the hardware demonstration. For the same reasons described previously, the serial link has been chosen. The principle is to write in FPGA control registers from this serial port. Thus, a control VHDL block has been developed.

Its principle is to detect a defined character sequence on the serial link and extract the register address and the data to be written in the register. Its synoptic is presented in Figure 5.20.

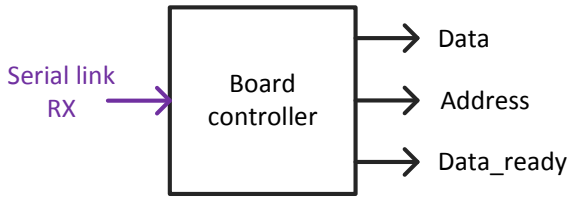

FIGURE 5.20: Board controller VHDL module - synoptic

The character sequence detection is assumed by a FSM, represented in Figure 5.21. The block waits for two defined character (RX in ASCII). The three next bytes represents

the address (one byte) and the data (two bytes) of the register to be written. Finally, the last byte received is for verification purpose (*XOR* combination of the payload bytes).

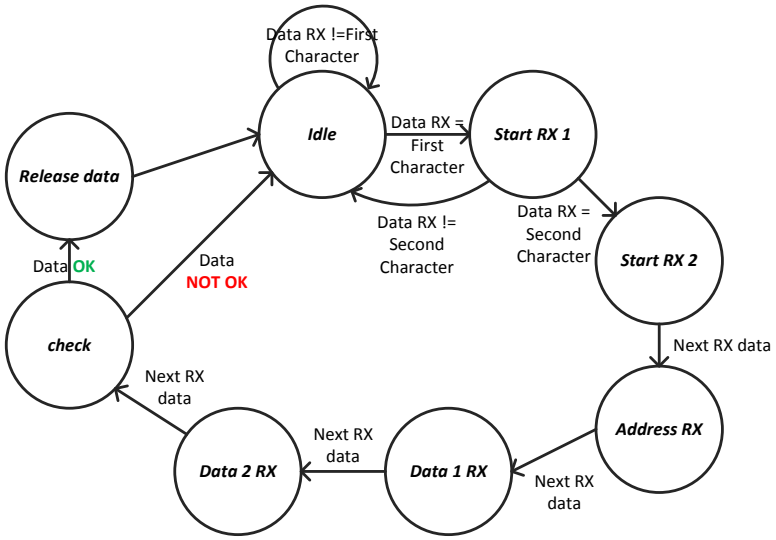

FIGURE 5.21: Board controller VHDL module - state machine

Depending the need, the data can be directly written in a register or in a RAM. The RAM is more convenient when there are a lot of control registers to write.

f. Gigabyte links

The last VHDL block needed for the hardware demonstration is the gigabyte link. These links are used to transmit data between nodes. As explained in the section A., the prototype boards are based on a Xilinx spartan 6 FPGA which have four gigabyte modules embedded. A Xilinx wizard tool gives support to use these embedded module.

A gigabyte link module has different parameters to be specified. Hereunder is listed the main parameters of the link :

- Line rate : 1.25 Gbits/s
- Encoding : 8B/10B
- Alignment character (comma character : K28.5 in 8B/10B encoding). Used every fourth byte.
- Driver configuration : differential voltage maximum, termination resistor grounded, pre-emphasis not enabled.
- Equalization on the receiver side maximum (higher frequency amplified to compensate link loss and distortion)
- 32 bit frames : 1 alignment byte, 1 checksum byte and so, 2 payload bytes.

However, even so configured, the gigabyte link is not totally reliable. Indeed, with the presented configuration, some data were corrupted, most of the time due to misalignment. To reach a correct reliability level, an additional filter block has been added.

This filter block aims to reject corrupted and misaligned frames. Filtering is done in three parts. The first part is to check the frame corruption with the checksum byte. The checksum byte is a weighted addition of the payload bytes (2 times the first byte added to three times the second one). The sum is regenerated at the filter block and the result must correspond to the checksum byte. The second part consists in rejecting misaligned frame. It has been observed that some frames have their bytes disordered. The filter block rejects a frame when the alignment character (so called *comma*) is not at its defined place (less significant byte). The third filtering part is a voting system. As the full gigabyte bandwidth is not needed for the application, each frame is sent at least 10 times. The filter block registers the frames and validates them when 3 frames in a row are similar.

This filter block improves drastically the gigabyte link reliability. However, when increasing the speed of the communication process higher than what is needed by the hardware demonstration (but still in the operational range), a non-negligible error rate is observed. For the future use of this block, the use of more complex protection mechanism shall be considered, for instance cyclic redundancy codes such as [68] or [69].

5.3.4 Nodes description

The previously described VHDL blocks are implemented in the FPGA in different configurations. There are four configurations. The master, slave and concentrator configurations are inspired by the hardware module proposal whereas the test controller configuration is required for the test bench.

a. Master and slave node

As shown in Figure 5.22, the master node receives the emulated acquisition data on a gigabyte link. The data are filtered before being analysed (by the threshold comparison blocks and the summarizer blocks). The partial post-pulse analysis result is forwarded via another gigabyte link. If the analysis triggers an interlock, the local permit is revoked and the beam permit loop generation is inhibited. The master node incorporates a control block, able to (re)arm the beam permit loop on an user demand.

As shown in Figure 5.23, the slave node has a similar configuration than the master node. The only difference is the beam permit loop block. On an interlock request, it is

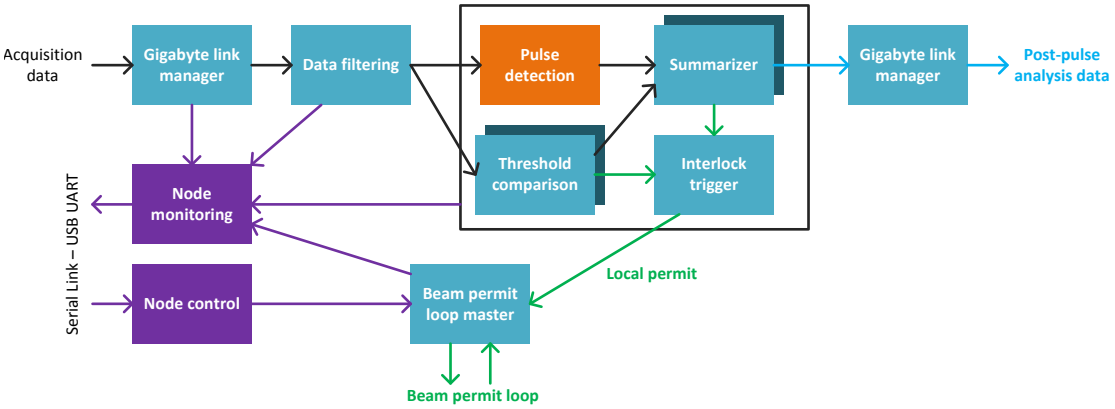

FIGURE 5.22: Master node - VHDL configuration

opening the loop (by stopping repeating the frequency). Moreover, there are no control block because it is not needed to (re)arm the loop in a slave node.

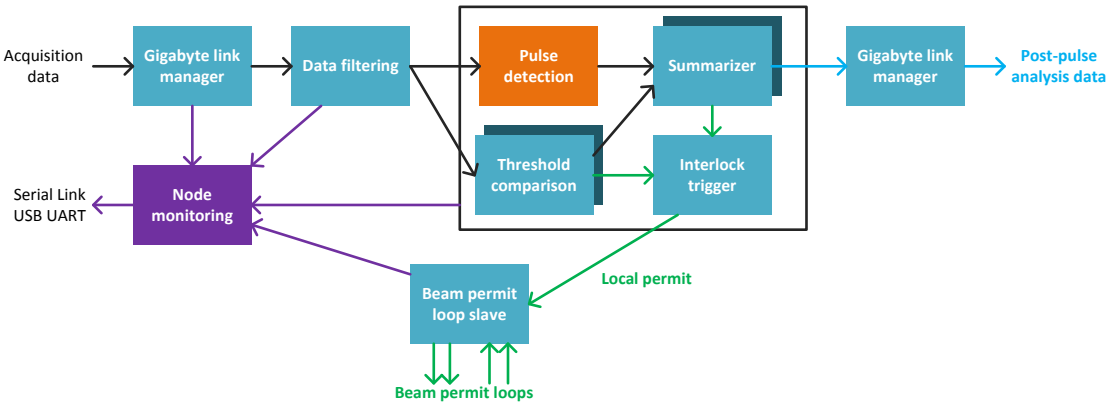

FIGURE 5.23: Slave node - VHDL configuration

b. Concentrator node

The concentrator node aims to finish the post-pulse analysis. As represented in Figure 5.24, it receives the post-pulse analysis data from the slave and master nodes to summarize them and generate the *next cycle permit*.

c. Test controller node

The test controller node is needed by the test bench to generate the acquisition data. As represented in Figure 5.25, it receives the data from the serial link, registers them in a RAM. Then, the RAM is continuously sending the registered data to the gigabyte links.

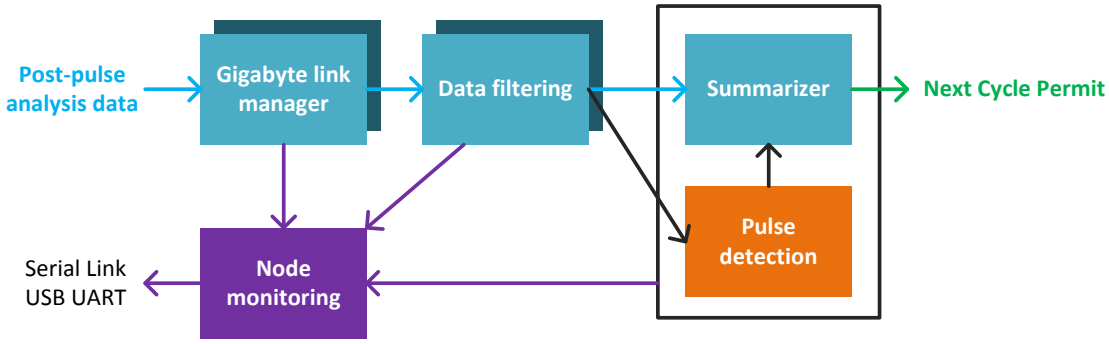

FIGURE 5.24: Concentrator node - VHDL configuration

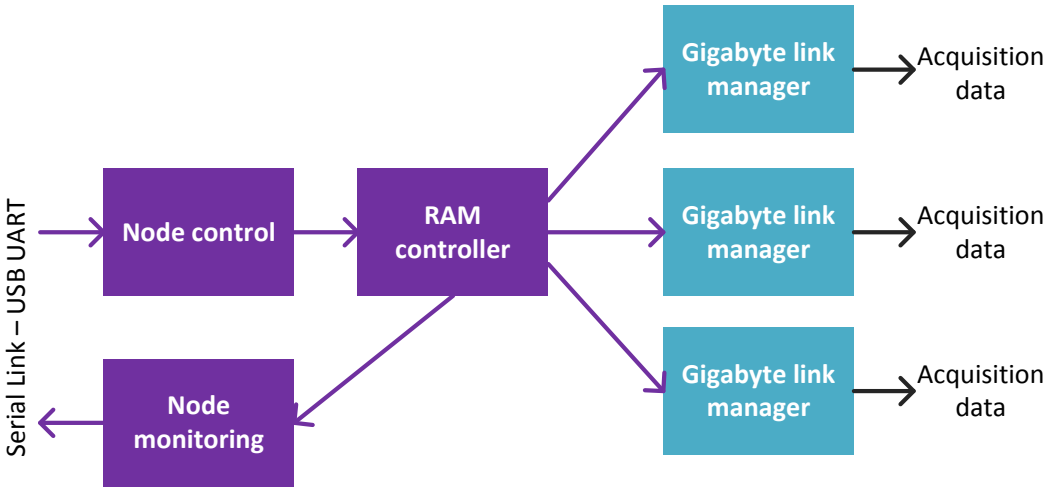

FIGURE 5.25: Test controller node - VHDL configuration

5.3.5 Hardware and test bench description

To explain how the measurements have been done, the hardware and tools used will be described. Then the test bench overview and the measurement procedures will be given.

a. Test bench elements

The main hardware used are the SPEC boards. They have been selected for several reasons :

- The board is FPGA based, VHDL blocks can be implemented.
- The board has gigabyte links, more specifically, Small Form-factor Pluggable (SFP) connectors. They were planned to be used by the acquisition interface (with the *white rabbit* project, [70]).
- The board design has been made at CERN, it is commercially available and it is part of the open hardware initiative (http ://www.ohwr.org/).

- The board has a PCI-express connection facility. It make it easier to integrate it into a an industrial computer.

Concerning the FPGA choice, there were only two requirements :

- Enough space to implement the VHDL blocks.
- Gigabyte link facility.

The similar commercial products from FPGA vendors (Spartan-6 FPGA Connectivity Kit from Xilinx, Stratix V GX FPGA Development Kit from Altera) have been initially considered. However, the price were 3 to 10 times higher from the SFP boards without adding useful facility for the hardware demonstration.

As shown in Figure 5.26, this board is based on a Xilinx Spartan 6 FPGA. It has a FPGA Mezzanine Carrier (FMC) carrier, which allows multi-purpose uses. In the current case, it will be used for communication facility. The board has four gigabyte links : one is transmitted on the SFP connector, two on the Serial Advanced Technology Attachment (SATA) connectors, and the last one is going on the FMC board. The board also implements an USB serial port, used for monitoring. Finally, despite it is not used in the hardware demonstration, there is a PCI Express connector. It allows integrating boards in a industrial computer.

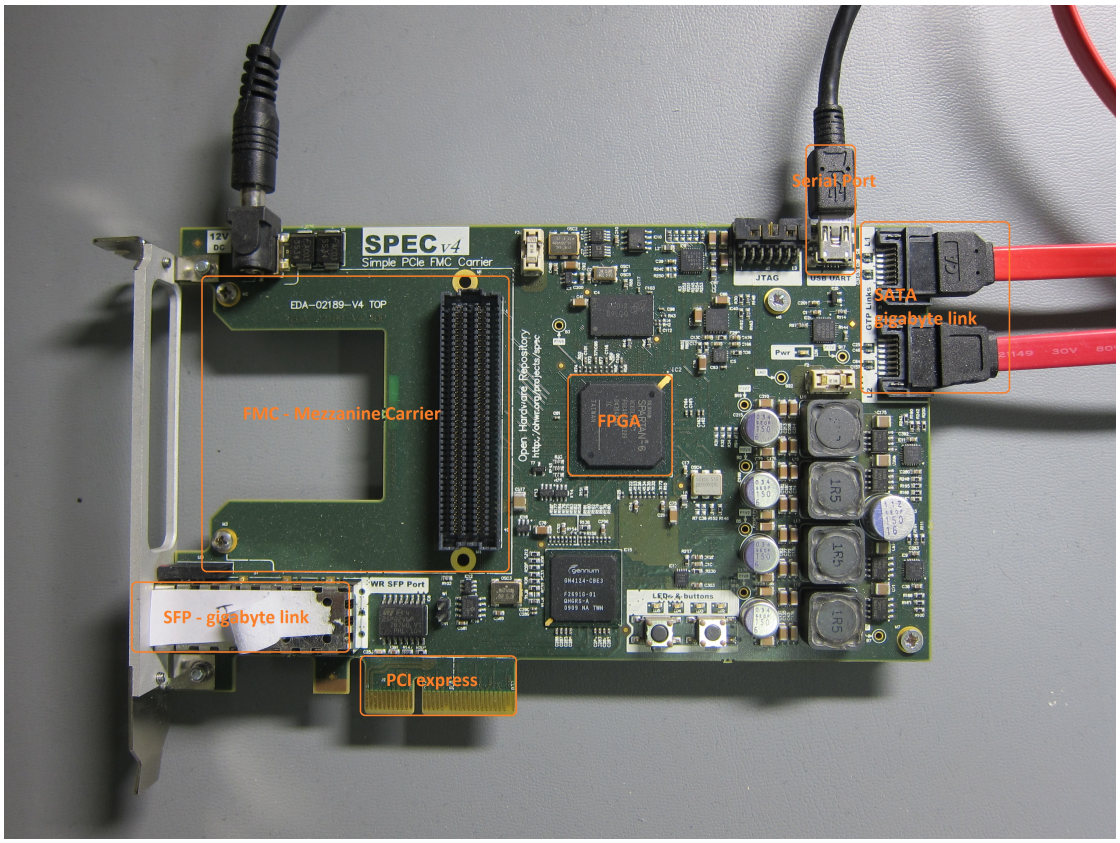

FIGURE 5.26: SPEC board overview

The FMC used is the XM104 from Xilinx, because it has connection facilities. In addition, at the time when to board has been selected, this board was the only one commercially available. The SATA connectors are used in the hardware demonstration (for the beam permit loop). As shown in Figure 5.27, minor modifications have been made on the FMC connector to ensure compatibility between the SPEC board *low-pin* FMC connector and the XM104 board *high-pin* connector.

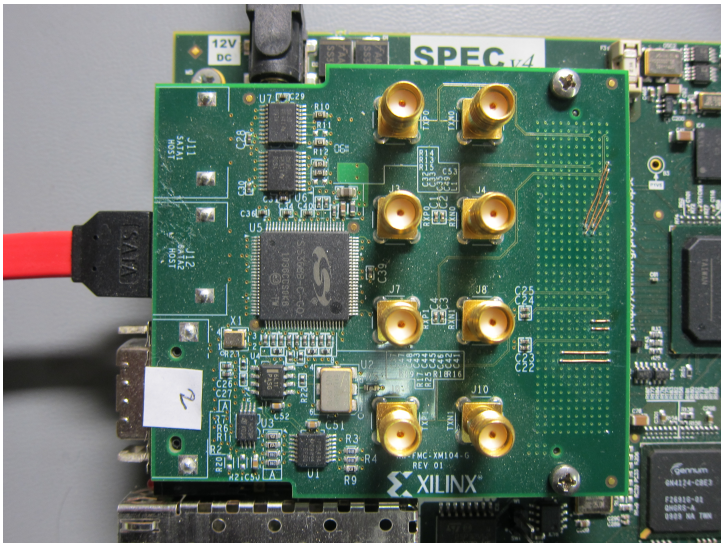

FIGURE 5.27: XM104 FMC board

To monitor the boards and control the test bench, the software Labview has been selected because it is suitable for fast prototyping and instrumentation.

b. Test bench overview

To set up the test bench, the team policy has been applied (project-mitestbench.web.cern.ch). It consists in three blocks (Figure 5.28). The first block is the general tester, which is able to perform automatic and repetitive tests. It corresponds to the Labview software. The second block is the test controller card. It aims to interface the general tester with the device under test in term of voltages, bandwidth, etc. It has also the opportunity to perform real-time operation. For the current case, a SPEC board is used to generate data on the gigabyte links. The last block of the test bench policy is obviously the devices under test. In the hardware demonstration, it is the down-scaled Interlock System, implemented by SPEC boards.

In Figure 5.29 is represented the test bench overview. The prototype Interlock System is made up of four boards. The master node is generating the beam permit loop (only one, no redundancy). It receives acquisition data and transmits post-pulse analysis data

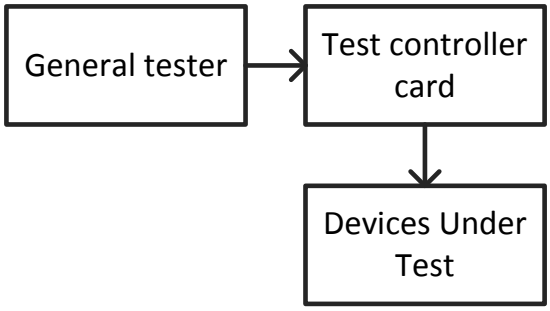

FIGURE 5.28: Test bench policy

to the concentrator. As there is not a target system, the *beam permit* is outputted on a LED and is monitored. Both slave nodes are similar to the master node but they are not generating the beam permit loop. The concentrator receives the post-pulse analysis data from the master and slave nodes. Contrary to proposed design, it generates the *next cycle permit* as it is the last post-pulse analysis module (In CLIC, it would be the master node). The test controller card is sending acquisition data to the master and slave nodes. The data sent is defined in Labview and transmitted to the test controller card. All nodes and the test controller card are monitored directly by Labview via the serial ports.

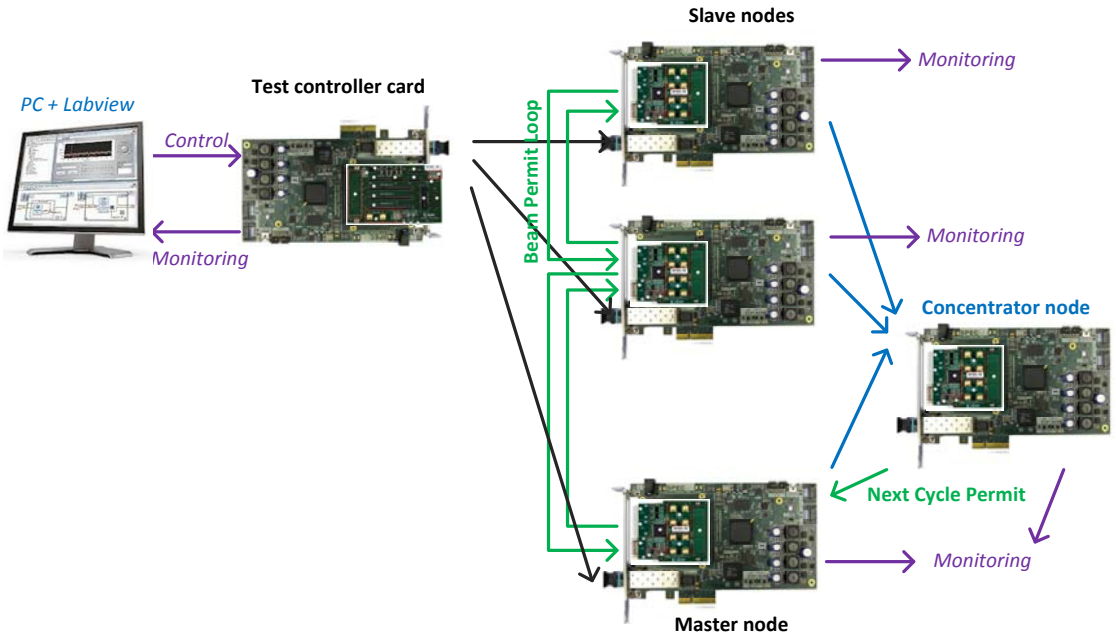

FIGURE 5.29: Test bench overview

To synthesize, the user can define acquisition data (critical equipment and beam quality related) in Labview. These data are transferred to the SPEC test controller card. It is

then emulating the acquisition infrastructure by sending them continuously to the prototype. The prototype is a scale-downed Interlock System similar to the design proposal. It is monitored by Labview for functional verification and measurement purpose.

c. Test bench measurement procedures

As defined in the hardware demonstration goals, there are four measurements to perform. Hereunder are described the measurement procedures.

Machine interlocking response time : One stringent timing requirement is the beam permit loop response time. The Interlock System must be able to inhibit the next beam within **2 ms**, whatever the location of the equipment breakdown or low beam quality assertion.

The requirement to equipment is to handle faults until the next pulse if they occur less than 2 ms before the next pulse (safe by construction principle, cf. CLIC machine protection). In the worst case, if a fault occurs 2 ms before the next pulse, it must trigger an interlock. Then, the Interlock System must successfully inhibit the next pulse. In Figure 5.30 is the global chain of events from equipment fault to next pulse inhibition.

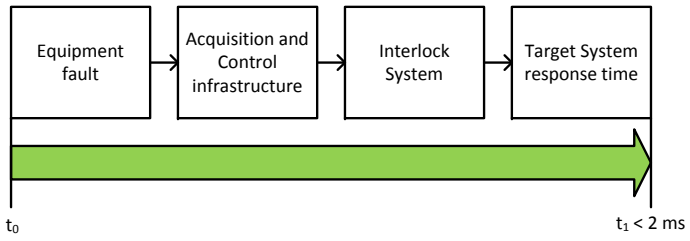

FIGURE 5.30: Machine interlocking global chain of event

To reach this requirement, it is needed to define the measurement boundaries. Acquisition data reception is the starting limit. The other side is the target system receiving the *beam permit*. The time needed to inhibit the beam by the target system will be taken in account in this requirement and so, will be the ending limit.

The goal is to prove this timing requirement can be reached. Consequently, the worst case will be taken in account. Thus, equipment failure at the start of the main linac is considered. Indeed, the slave node receiving the interlock request will be the farthest from the master node, located between both main linacs.

To measure the response time, the first step is to determine the chain of events and functions leading to beam inhibition. It is represented in Figure 5.31. It starts with data

reception. The first function performed is the threshold comparison, which will detect the interlock request. Once detected, the request will break the beam permit loop. The VETO permit will be propagated through nodes and between the nodes (800 m of optical fibres). The master node will have then to detect the permit change. Next, the VETO permit will be released to the target system and we will consider 20 km of optic fibres between the master node and the target system. Finally, the target system response time will be taken in the chain.

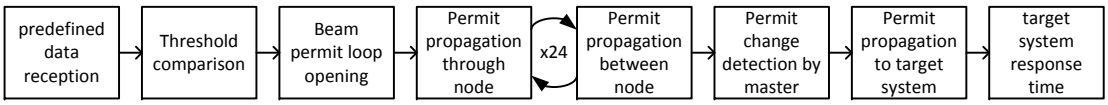

FIGURE 5.31: Machine interlocking system chain of event

The procedure consists in measuring what is possible on the prototype and extrapolating these measurements to CLIC scale. What is not measurable will be estimated.

Post-pulse analysis response time : The Interlock System must be able to perform the post-pulse analysis and to deliver the *next cycle permit* within **6 ms**. Indeed, the requirement to acquisition and control infrastructure is to deliver all beam quality related data 2 ms after the beam passage. As the *next cycle permit* must be delivered 2 ms before the next beam passage, it results, as illustrated in Figure 5.32, in a 6 ms requirement.

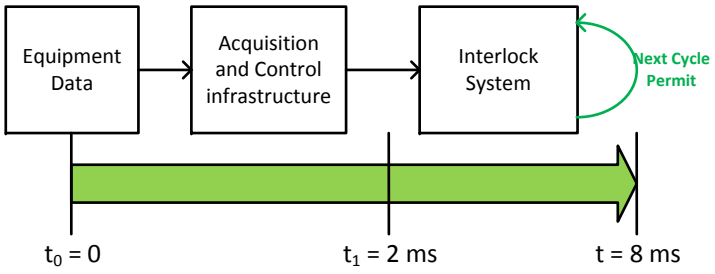

FIGURE 5.32: Post-pulse analysis global chain of event

As for the machine interlocking response time, it is needed to define the measurement boundaries. Acquisition data reception is the starting limit and *next cycle permit* release (in the master node) is the ending limit.

Again, the first step is to determine the chain of events and functions leading to *next cycle permit* release after a beam passage. It is represented in Figure 5.33. It starts with data reception. The first function performed is the threshold comparison. The next module is the summarizer in the slave node. Then, the post-pulse data are sent to the concentrator node via a gigabyte transmitter. For the link between the slave and the concentrator

node, a conservative case of 2600 m (800*3+200) will be taken (3 alcoves and 200 m margin). Next function is the gigabyte receiver (including decoding and filtering). After that, there is again a summarizer module (concentrator). At that point, the succession of the gigabyte transmission, link, gigabyte reception and summarizer module (master) is done again. The link between the concentrator node and the master node is estimated at 20 km.

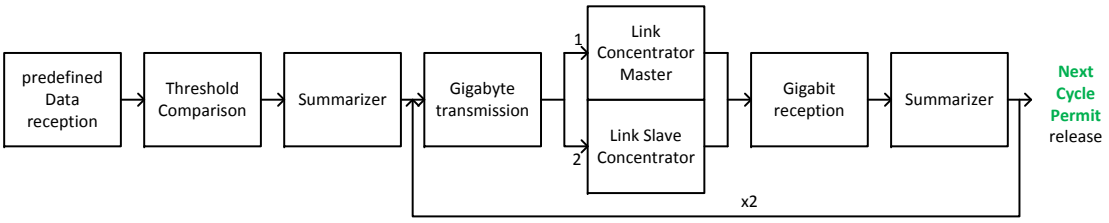

FIGURE 5.33: Post-pulse analysis system chain of event

The measurement procedure is the same than for the machine interlocking response time.

Node false Veto and Pass rates : The failure rates measurement is done in two parts. As false PASS decision is expected to be unlikely, sending a data set with an interlock request from time to time will not make appears a false PASS. Consequently, the measurement has been split.

For the false VETO rate measurement, the data set is defined to *not* trigger interlock requests. The beam permit is observed and if it is going to VETO state, then a false VETO decision is registered. The beam permit is rearmed and the measurement continues.

For the false PASS rate measurement, only *one* data is defined to trigger an interlock request. Indeed, in operational data, the most common case of interlock request is sourced by a single data. Moreover, if only one data is triggering an interlock request, this is the best case to observe a false PASS decision (e.g. lacking data, bad threshold comparison).

In order to assert measured rates are not a special case, the measurements have been repeated on the three prototype nodes.

To measure low rates, it has been needed to accelerate the measurements by accelerated testing. Two ways have been selected. The first way has been to increase the function use rate. The second way has been to use a more stressed environment than the operational one.

Increasing use rate has been done by accelerating the data set readout. Each time the full test controller card RAM has been sent, a pulse has been emulated. A CLIC pulse

corresponds to 20 ms emulated. In real time, it takes about 5 μs to send the full RAM. Thus, it has been possible to perform accelerated testing by a factor 4000.

The measurement has been performed in more stressed environment than final design operational conditions. The main source of stress has been the temperature. To quantify the acceleration factor due to the temperature, the Arrhenius equation [71] has been used :

$$AF_T(T) = \exp(\frac{E_a}{Kb} * (\frac{1}{T_0} - \frac{1}{T}))$$

with :

– E_a : thermal Activation Energy
– Kb, Boltzmann's constant $\approx 8.6^{-5} eV.K^{-1}$
– T : test temperature
– T_0 : standard temperature

For the numerical application :

– T_0 is 298 K, the standard temperature considered for Spartan 6 (the FPGA used) datasheet.
– T is 321.7 K, it has been evaluated from the VHDL design with Xilinx Power Analysis tool.
– E_a is taken at by default at 0.7 eV [72]

It gives an acceleration factor due to temperature of $AF_T(48.7) \approx 8.7$

Despite these acceleration factors, emulating 10^9 hours would take more than 3 years. Consequently, with the current accelerated testing, rates up to 10^{-7} (equivalent to 13 days of measurement) can be measured.

5.3.6 Results and discussion

Once the measurements procedures have been defined and applied, results have been obtained. They are presented hereunder.

a. Machine interlocking response time

The goal is to compute or estimate the response time of each element of the previously defined chain of event (Figure 5.31).

The threshold comparison function response time and the time needed to break the beam permit loop have been measured in the FPGA. Indeed, as these functions are implemented in VHDL, an embedded counter between the data reception and the end

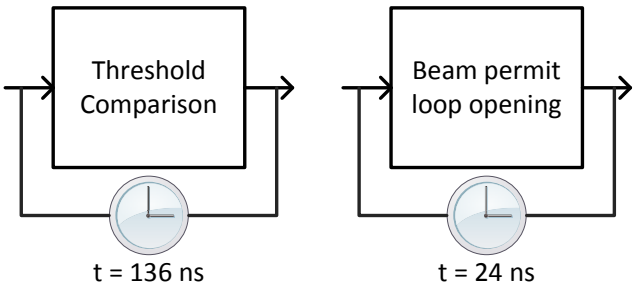

FIGURE 5.34: Machine interlocking response time measurements - inside FPGA

of the function allows measuring the response times. As represented in Figure 5.34, it gives *136 ns* for the threshold comparison and *24 ns* for the beam permit loop opening.

The permit propagation through optical fibres, either between nodes or between the master node and the target system is estimated. The typical core index of refraction of 1,62 is considered [73]. This leads to a time of travel of *4.32 μs* and *108 μs* for the 800 m and 20 km optical fibre length respectively. It is represented in Figure 5.35.

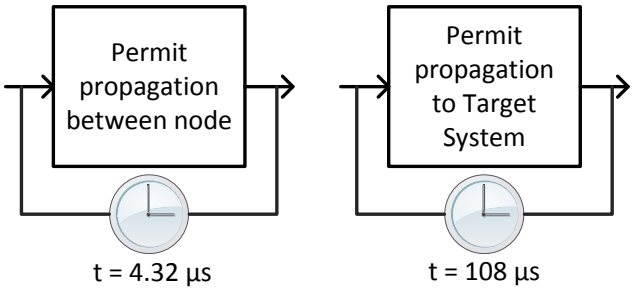

FIGURE 5.35: Machine interlocking response time measurements - fibres

The permit propagation through node has been measured directly on the hardware demonstration. The delay introduced is equal to *15 ns*. In Figure 5.36, the yellow signal is the upcoming beam permit and the teal signal is the outputted signal.

The beam permit loop may use optical propagation because of distance between the nodes (hardware demonstration uses electric propagation). It implies that delays must be added for the optoelectronic conversion. Typical delays for optical transmitters are around 60 ns (taken from Avago HFBR-0400Z datasheet). Considering two conversion delays, the final propagation time is estimated at *135 ns* (60*2+15).

The permit change detection by the master is conditioned by the frequency detection function implementation. As described previously, this VHDL function has a configurable measurement window. A short window (e.g. 1 μs) would result in a short the response time but the inaccuracy of the measurement will be increased (e.g. 1 μs window would

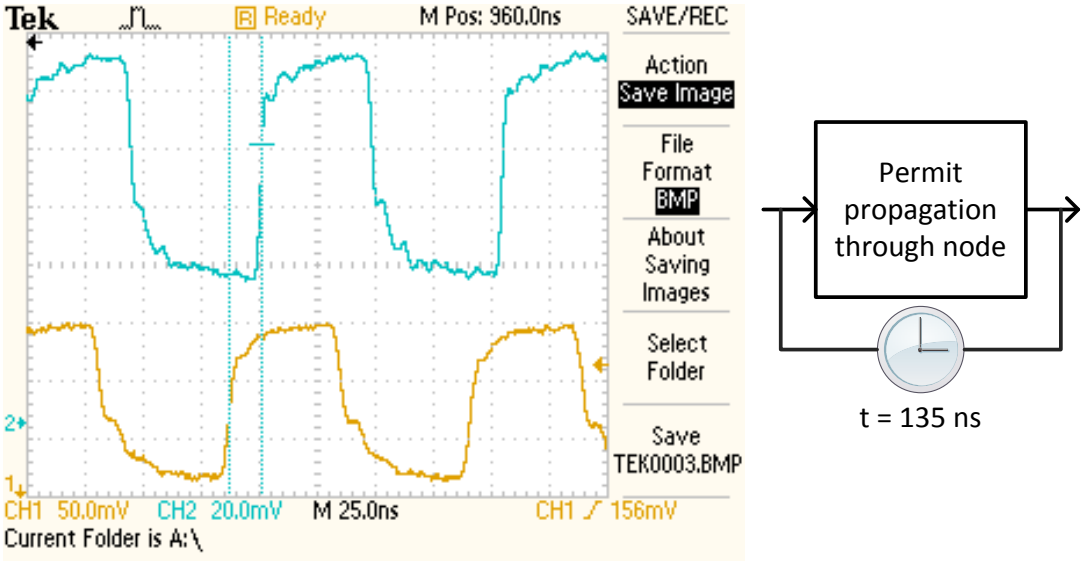

FIGURE 5.36: Machine interlocking response time measurements - nodes

results in +/- 10%). In the hardware demonstration, the window time has been selected to be 5 μs giving a maximum response time of *5,1 μs* (response time plus one beam permit period). To ensure it, measurements have been done on the prototype. In Figure 5.37, the purple signal represents the permit change detection by the master node. The yellow and teal signals are the beam permit. It can be seen the permit fall around 500 ns before its detection.

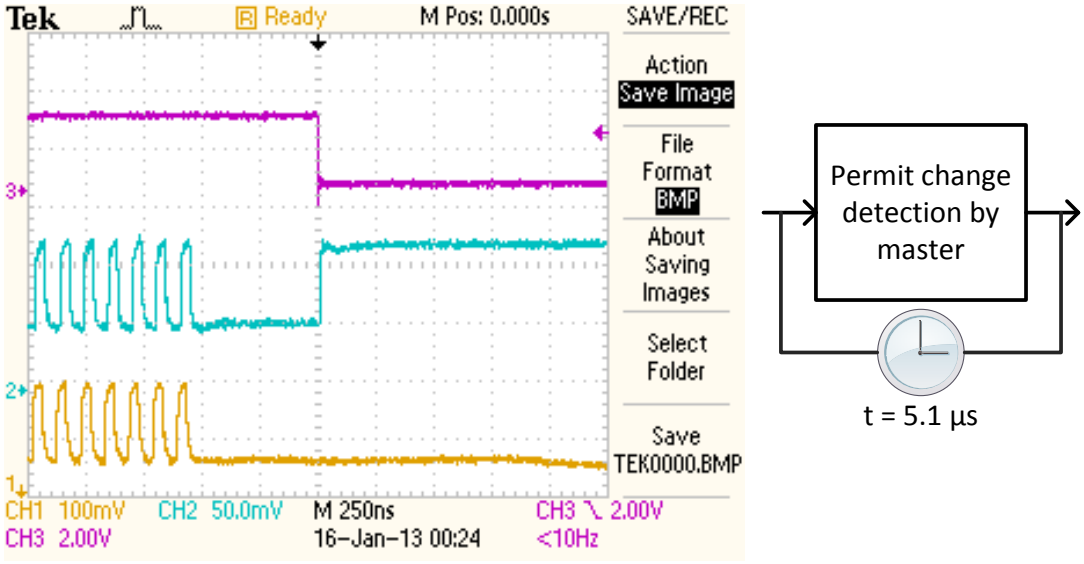

FIGURE 5.37: Machine interlocking response time measurements - frequency detection

Finally, the last function of the chain considered is the target system response time. In

the LHC case, the target system is the Beam Dump System. Its reaction time is less than 200 μs, with around 90 μs needed to synchronise with the beam. For CLIC case, we will consider the response time of a kicker. Its typical response time [74] is conservatively estimated at 100μs.

Adding all the delays gives a total response time of *320 μs*. It is represented in Figure 5.38.

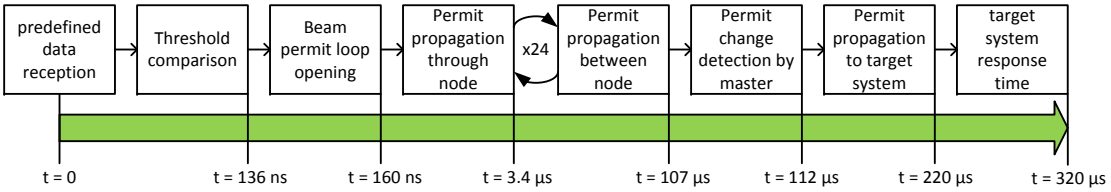

FIGURE 5.38: Machine interlocking response time measurements - synthesis

So, the proposed design is compliant with the machine interlocking response time requirement as long as the equipment fault is transmitted fast enough. To compute what is this maximum time acceptable, one extra delay must be taken in account. Indeed, despite the beam travel at the speed of light, there is a non-negligible delta time between its generation and its collision point. The interlock request must be delivered at the target system before the beam passes the location of the target system (i.e. injectors). Considering the worst case, the extra delay is the time taken by the beam between the target system location and the start of the main linac :

$$\Delta T = \frac{30km}{c} = 100\mu s$$

Consequently, the equipment fault detection and the data delivering to the Interlock System must be lower than :

$$2ms - 0.320 - 0.1 = 1.58ms$$

b. Post-pulse analysis response time

As done previously, the goal is to compute or estimate the response time of each element of the previously defined chain of event (Figure 5.33).

The threshold comparison function response time has been already measured for the machine interlocking response time.

The summarizer function response time has been measured in the FPGA with a counter. It gives a response time of *16 ns*. This time is invariant regarding the location of the function (master, concentrator or slave).

The gigabyte transmission and reception have been measured at the same time. Indeed, in a gigabyte transmission, it is not possible to observe the frame with a standard oscilloscope. To perform the measurement, a pin of the FPGA has been driven high when the transmitter was sending a predefined data (before encoding and protection mechanisms). At the reception side, a pin has been as well driven high when this same predefined data was received (after decoding and filtering). The measurement can then be taken by measuring the delay between these two pin signals rising edges. The measurement is shown in Figure 5.39 and gives a 1.15 μs delay.

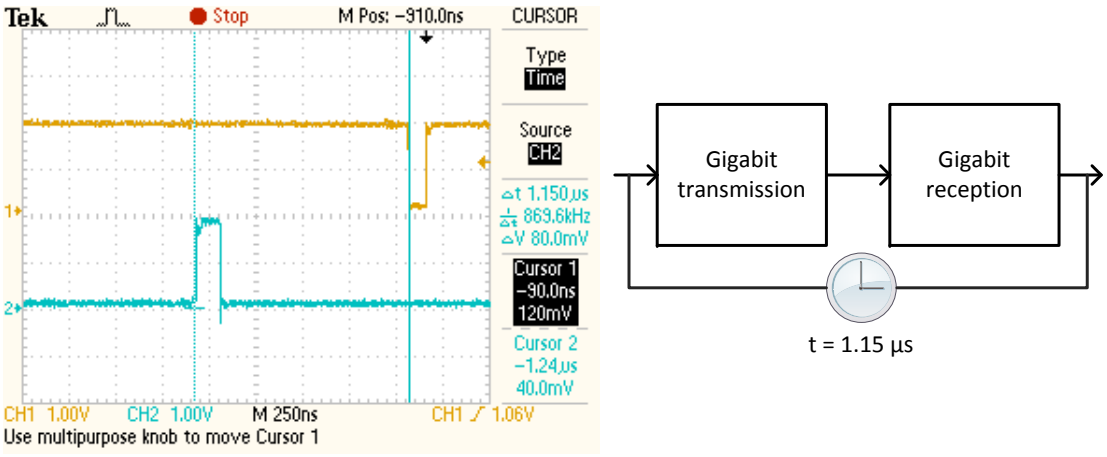

FIGURE 5.39: Post-pulse analysis response time measurements - gigabyte link

Concerning the post-pulse analysis data propagation through optical fibres, both times (slave/concentrator and concentrator/master) are estimated in the same way than for the machine interlocking response time case. This leads to a time of travel of 14.04 μs and 108 μs for the 2.6 km and 20 km optical fibre length respectively.

Adding all the delays gives a total response time of *125 μs*. It is represented in Figure 5.38

As a conclusion, the proposed design is compliant with the post-pulse analysis response time requirement. However, this measurement did not take in account the response time in case of lacking data. In this case, the Interlock System would wait for the watchdog to trigger its fail-safe value. The watchdog response time is configurable and must be adapted to the requirements.

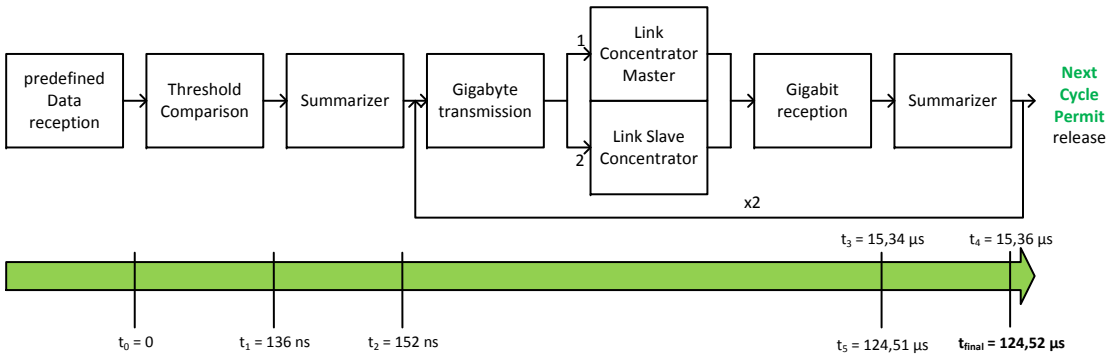

FIGURE 5.40: Post-pulse analysis response time measurements - synthesis

c. Node false Veto and Pass rates

The measurement results are presented in Table 5.2. When the failure rate has an inferior symbol, it means that no failures were observed during the measurement time.

When setting up the test bench, the functions have been configured in a less optimized mode, to make failures appear more often. Thus, the test bench was asserted to be able to capture failures. By modifying several parameters (e.g. the speed of RAM readout), the main source of failure has been identified to be the gigabyte link. Moreover, most of the failures were appearing in the first minutes after powering the boards under test. This can be linked to the typical failure rate for electronic system (bathtub curve).

TABLE 5.2: Measurements results

Rates	**Node 1**	**Node 2**	**Node 3**
false VETO	$< 3 * 10^{-7} h^{-1}$	$< 7 * 10^{-7} h^{-1}$	$7 * 10^{-7} h^{-1}$
false PASS	$< 4 * 10^{-7} h^{-1}$	$< 2 * 10^{-7} h^{-1}$	$< 4 * 10^{-7} h^{-1}$

As the main conclusion, these rates prove the proposed design is able to reach the established requirements with a 2-out-of-3 redundancy. This result is conditioned by the simulation assumptions (cf. chapter 3 dependability requirement establishment). Moreover, the design does not exclude to be compliant with lower redundant lines configurations but more advanced tests are required to prove it.

d. Discussion

Not surprisingly, the response times requirements are reached. Indeed, the requirements had fixed the scale of time (few millisecond) for the Interlock System, thus rejecting pure software solution. In consequence, the design has been proposed to be FPGA-based. This type of technology is fast and thus has easily fulfil the response time requirements.

For the machine interlock response time, the interesting point is to quantify the maximum time for the acquisition infrastructure to deliver equipment failure (1.58 ms).

Concerning the post-pulse analysis, the response time is one order of magnitude lower than the requirement (125 μs for 6 ms). This lets the opportunity to add more advanced computation. More precisely, as seen in the feasibility study, some data may need to be transformed (integration, averaging, ...) before performing a threshold comparison. In a conservative case, this transformation could be assumed by user front-end before release final data to the Interlock System. The timing requirement to the user to perform this transformation is less than **5 ms** (the last 1 ms would be used by the Interlock System for the watchdog system and the post-pulse analysis).

In the short term, several enhancements could be performed for the test bench. First, the test vector should be upgraded to be pseudo-randomly generated for the false decision rate measurement. Indeed, it would test the full combination of possible test vectors and would reveal exceptions. Secondly, the accelerated testing should be upgraded by using more extreme temperature (with dedicated thermal devices). An other option would be to use radiations, to check how reliable is the design with Single Event Upset (SEU may occur in the operational environment).

5.4 Conclusion

The goal of this last chapter has been to verify the design proposal. The two experiments have been performed. They were complementary. One is based on the design proposal, and prove the design compliance regarding the performance requirements. The other one is based on the needs of the operation to apply the post-pulse analysis, giving the design process practical expectations from operation.

The conclusion of this chapter is the following : based on the prototype measurement, based on the operation expectations, by integrating in the design process the remarks occurred in the design verification, the proposed design will work and will behave as required.

The suggestions which have been given in the feasibility study and the hardware demonstration are synthesized hereunder :
- Implement a safe machine parameter system in the Interlock System.
- Implement a mechanism to manage dynamically the thresholds (equations).
- Choose carefully the beam quality related data in order to be able to perform a fast post-pulse analysis.

- The acquisition infrastructure must be able to transmit an equipment fault detection in less than 1.58 ms.
- Advanced operation may be performed by the user at the front-end and shall be done in less than 5 ms before being delivered to the Interlock System.
- The gigabyte links are the reliability weak point of the Interlock System and must be optimized to enhance system dependability
- Dedicated thermal tests shall be done on the prototype to define which beam permit loop redundancy is needed.

The next step would be to develop an second generation prototype to be integrated in operational environment (for instance in CTF3). This would be a closer step to the final Interlock System.

Chapter 6

Conclusion and perspectives

In this thesis, the design of a dependable Interlock System for linear collider has been presented. The works have been divided in three main lines : the design, the dependability study and the application to linear particles accelerators.

The design is structured in three steps. Its methodology has been based on the IEEE 1220 standard. The first step is the requirement establishment, which defines what the system shall do (functional requirement) and to which extent (performance requirement) and lists the expectations to the interfaced system. The second step is the design proposal. It carries on a functional analysis which proposes a functional design and ends up with an implementation proposal at the sub-functions, system and hardware modules levels. The last step is the design verification. It checks that the studied design will work by asserting its feasibility in an operational environment and by proving that the performance requirements can be reached. Although the work has been applied to the CLIC study, a special attention has been spent to keep the design methodology generic. It gives the opportunity to use it as a basis to future electronic protection system.

The dependability is a central part of the Interlock System. We have established a methodology to determine the reliability and availability requirements for the system at its design phase. The idea has been to keep it modular in order be able to complete it with more accurate assumptions in the future. We have proposed and applied a process to check if the Interlock System design is compliant with the established dependability requirements.

The CLIC is a complex machine and a non-negligible part of the thesis work have been spend to understand the machine sub-systems. This knowledge has been a key factor to integrate efficiently the Interlock System in the CLIC environment. Part of it, the

challenges brought by the linear structure have lead to study more carefully the new concept of post-pulse analysis. Its feasibility has been thus studied.

From the thesis, there are two main outcomes. On one hand, there is the design proposal for the CLIC Interlock System. Its requirement establishment, functional analysis and implementation allows to enhance or modify the proposal with regards to new information (CLIC project update or translation to new project). On the other one, an Interlock System prototype has been delivered, inspired by the design proposal and compliant with the established requirements. These two outcomes are addressing the issue of how to design, with a rigorous basis, an Interlock System for linear colliders.

In a short term view, two main tasks could improve the thesis results. the first task is to continue the test-and-improve process for the JAVA application in CTF3. Indeed, it may lead to complete the operational expectations regarding the post-pulse analysis concept. The second task is to use dedicated thermal devices to perform more accelerated testing for the false decision rates measurements. It would effectively help to reach lower rates (up to $10^{-9}.h^{-1}$).

In a long term view, the CLIC Interlock System study shall be continued. The design methodology can be iterated to affine the requirements, the functional analysis, the implementation proposal. The next step would be to integrate the prototype in operational environment, most likely in the CTF3. It would require few modifications (board integration in industrial computer and new monitoring software to develop). Concerning the dependability study, the design compliance has been based on the beam permit loop model. It should be upgraded to integrate a post-pulse analysis model.

Finally, the design proposal and its process could be translated for ILC machine protection study. We are looking forward for the design process application for future electronic protection systems. A new generations of machine are being built and can use this design process. For instance, in the particle accelerator, we can cite the European Spallation Source (ESS) in Sweden [4], the Facility for Antiproton and Ion Research (FAIR) in Germany [75], the Facility for Rare Isotope Beams (FRIB) in USA [76] and the Heavy Ion Accelerator Facility (HIAF) in China [77].

Annex A

Dependability data

The Figure A.1 shows the post-mortem system data on LHC statistics over the operational year 2011. It has been use in the dependability study to establish the critical equipment and unstable beam failure rates.

Post Mortem Statistics over 2011

Beam dump causes

Cause	Dumps	relative
Beam dumped without impact on beam	312	53%
Beam Dumped by Operator	155	26%
Machine Protection Test	57	10%
Beam dumped from beam monitoring (impact on beam)	36	6%
False Beam Dumps (failure in MPS System)	26	4%
total	586	100%

Beam instability

where to find data
https://cs-ccr-oas1.cern.ch/pls/htmldb_dbabco/f?p=117:1

Beam dumps where the beam was NOT affected

Cause	Dumps	relative	relative
Triggers by QPS	49	17%	18%
RF faults	41	14%	15%
Problem with cryogenics	31	11%	11%
Power converter faults	30	10%	11%
Electrical Network	29	10%	10%
Feedback	23	8%	8%
Vacuum system	16	5%	6%
Collimator positions not correct	15	5%	5%
Beam Dumping System	11	4%	4%
Controls system problem	11	4%	4%
Orbit Excursion in IR6	9	3%	3%
Operational error	8	3%	N/A
Powering Interlock System	5	2%	2%
Water cooling	4	1%	1%
Experiments hardware	4	1%	1%
Beam Interlock System	2	1%	N/A
Software Interlock System	2	1%	1%
Access system triggered beam dump	2	1%	N/A
total	292	100%	N/A
total equipment fault	280		100%

Mission aborted by equipment fault

$$= \frac{\text{number of dumps by equipment fault}}{\text{number of dumps}} \quad 48\%$$

47.78%

FIGURE A.1: Post-mortem system data - 2011

Annex B

CTF3 Application details

In this annex are gathered additional technical details on the feasibility study performed in CTF3 via a JAVA application.

B.1 Technical Overview

The Figure B.1 shows an overview of the application JAVA classes. Each box represents a class or a group of classes. The purple arrows represent an interface and their destination are their implementations. The black arrows show which classes instantiate which objects.

The Main class configures, initializes and launches the application. The class RampSafeBeam instantiates all the other group of classes and assumes their synchronisation. The controller class implements the control flow which controls the application behaviour (cf. Figure B.2). The singleton blue classes are use for the two logging facilities. The gun timing group of classes is used to modify the beam length. The Safe conditions and Hardware Check groups of classes are used by the application to check safety of the machine before restarting the gun. The yellow static classes are coding facility for the application. Finally, the post-pulse analysis group of classes is the core of the application. It is based on Radiation monitors and Beam Position Monitor (BPM).

The BPM used and their location are listed hereunder :
- CL.STBPM0402S : Before Delay Loop,
- CL.STBPM0590S : Before Delay Loop,
- CL.STBPM1590S : Before Delay Loop,
- CM.STBPM0110S : After Combiner Ring

- CM.STBPM0550S : After Combiner Ring
- CT.STBPM0515S : Before Delay Loop
- CT.STBPM0155S : After Delay Loop
- CB.STBPM1030S : After Delay Loop
- CR.STBPM0155S : In Combiner Ring
- CC.STBPM0130S : After Combiner Ring

The radiation monitor used and the effect they are monitoring are listed hereunder :

- CD.PAXCT02 : synchrotron radiation
- CD.PAXCT03 : synchrotron radiation
- CR.PAXCT01 : beam injection loss
- CR.PAXCT02 : synchrotron radiation
- CR.PAXCT03 : beam extraction loss
- CT.PAXCT01 : reference, close to control room

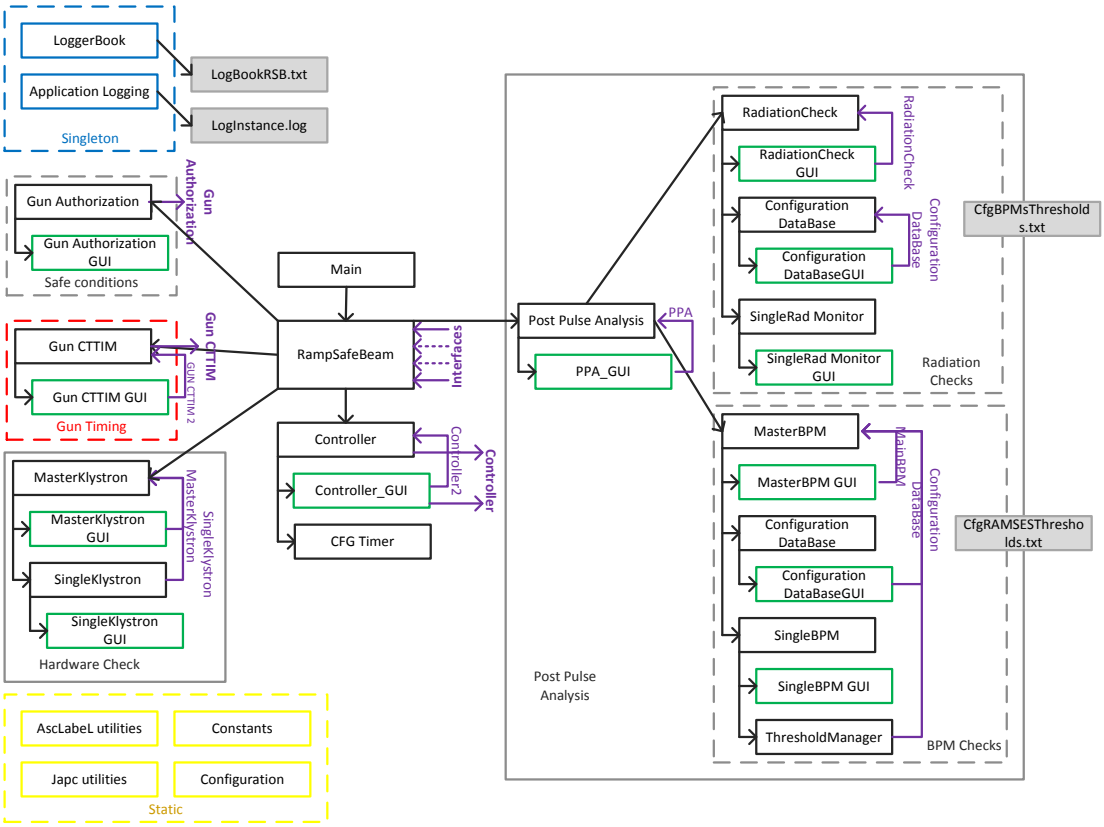

FIGURE B.1: CTF3 Application classes overview

B.2 Finite state machine diagram

The Figure B.2 represents the control flow used in the CTF3 JAVA application. It is trigger each time a beam goes trough the accelerator and the middleware update the value.

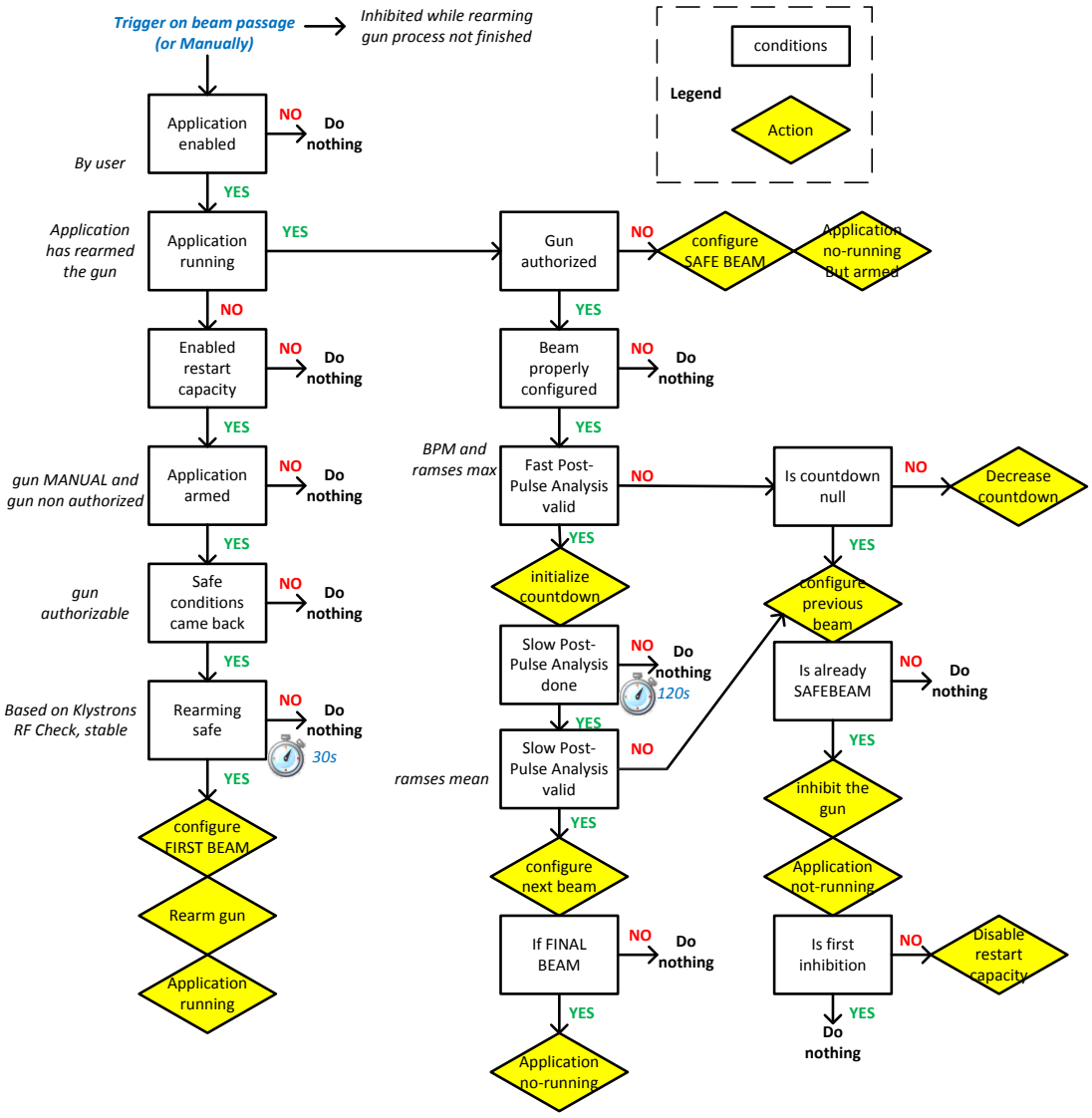

FIGURE B.2: CTF3 Application finite state machine

B.3 Threshold dynamic factors

The Figure B.3 shows the beam operation with different recombination modes. DL and CR acronyms stand for Delay Loop and Combiner Ring. For instance, DL=0 indicates the delay loop is not used.

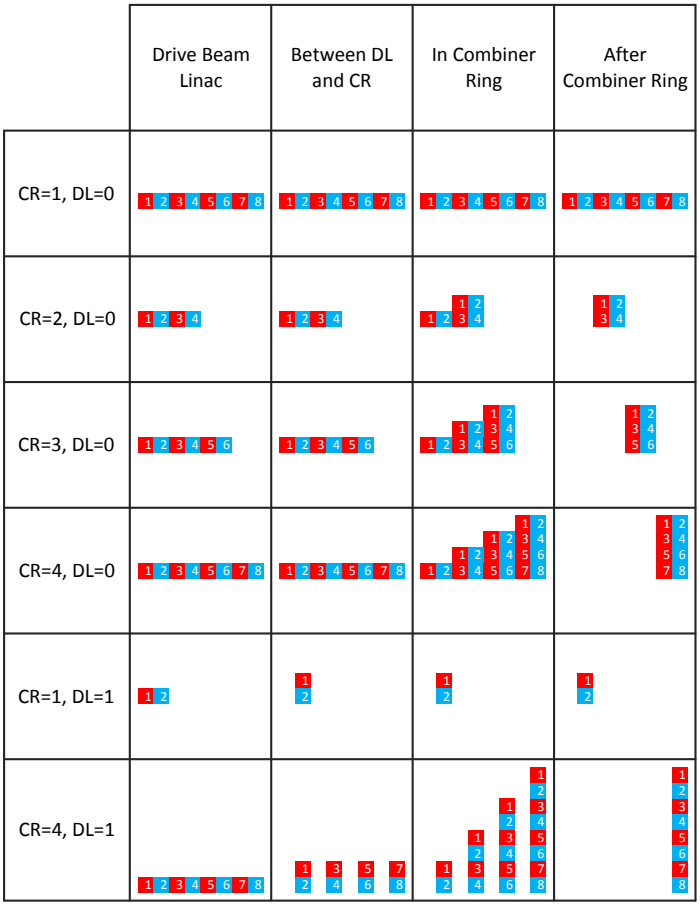

FIGURE B.3: CTF3 Application beam operation

There are three values checked in the BPM :

Maximum Value : the maximum value must be *above* the defined threshold.

Beam Length : the beam Length must beam *larger* than the defined threshold.

Beam Charge (Integration) : the beam Charge must beam *higher* than the defined threshold.

The purpose of these checks is to detect beam losses. These three thresholds are dynamically changed following two main parameters :

- **BPM location** : It specifies if the BPM is before/after the Delay Loop and before/after the Combiner Ring.
- **Current Beam** : it specifies what is the current beam sent into the accelerator complex. It is function of the sub-parameters :
  - **Current step** : There are 5 different steps (SAFEBEAM, FIRSTBEAM, SECONDBEAM, THIRDBEAM, FULLBEAM) and each one determine partially the current beam sent.

- Combiner Ring use : It specifies which recombination factor is used for the Combiner ring (x1, x2, x3 or x4).

- Delay Loop use : It specifies if the Delay Loop is used or not.

Hereunder is described the dynamic factors applied to the raw thresholds to give the applied thresholds. The parameters are formalized in the following way :

$$-\text{BPM Position} : P_{BPM} = \begin{cases} BDL & = & \text{Before Delay Loop} \\ ADL & = & \text{After Delay Loop} \\ ACR & = & \text{After Combiner Ring} \end{cases}$$

$$-\text{ Current Beam} : CB = \begin{bmatrix} CB(1) \\ CB(2) \\ CB(3) \end{bmatrix} = \begin{bmatrix} S(x) & = & x & \forall \text{ x=\{1,2,3,4\}} \\ CR(y) & = & \frac{y}{4} & \forall \text{ y=\{1,2,3,4\}} \\ DL(z) & = & \frac{1}{2-z} & \forall \text{ z=\{0,1\}} \end{bmatrix}$$

with

– S(x) : Current Step of the procedure

– CR(y) : factor from Combiner Ring recombination

– DL(z) : factor from the Delay Loop use

and the factor to determine are noted :

– F_{MV} : Factor Maximum Value

– F_{BL} : Factor Beam Length

– F_{BC} : Factor Beam Charge

B.3.1 Maximum Value

For the Maximum value the factor is defined as described hereunder :

$$P_{BPM} = BDL \Rightarrow F_{MV} = 1$$

$$P_{BPM} = ADL \Rightarrow \begin{cases} CB[1] \neq S(4) & \Rightarrow & F_{MV} = 0.5 \\ CB[1] = S(4) \& CB[3] = DL(0) & \Rightarrow & F_{MV} = 0.5 \\ CB[1] = S(4) \& CB[3] = DL(1) & \Rightarrow & F_{MV} = 1 \end{cases}$$

$$P_{BPM} = ACR \Rightarrow \begin{cases} CB[1] \neq S(4) & \Rightarrow & F_{MV} = 0.125 \\ CB[1] = S(4) & \Rightarrow & F_{MV} = CB[2] * CB[3] \end{cases}$$

B.3.2 Beam Length

For the Beam Length the factor is defined as described hereunder :

$$CB[1] \neq 4 \Rightarrow F_{BL} = 0.25 * CB[2]$$

$$\left\{ \begin{array}{lcl} CB[1] & = & 4 \\ CB[3] & = & 0 \\ P_{BPM} & \neq & ACR \end{array} \right\} \Rightarrow \begin{cases} CB[2] \neq 1 & \Rightarrow & F_{MV} = CB[2] \\ CB[2] = 1 & \Rightarrow & F_{MV} = 1 \end{cases}$$

$$\left\{ \begin{array}{lcl} CB[1] & = & 4 \\ CB[3] & = & 0 \\ P_{BPM} & = & ACR \end{array} \right\} \Rightarrow \begin{cases} CB[2] \neq 1 & \Rightarrow & F_{MV} = 2 \\ CB[2] = 1 & \Rightarrow & F_{MV} = 8 \end{cases}$$

$$\left\{ \begin{array}{lcl} CB[1] & = & 4 \\ CB[3] & = & 1 \\ P_{BPM} & = & BDL \end{array} \right\} \Rightarrow \begin{cases} CB[2] \neq 1 & \Rightarrow & F_{MV} = 1 \\ CB[2] = 1 & \Rightarrow & F_{MV} = 0.25 \end{cases}$$

$$\left\{ \begin{array}{lcl} CB[1] & = & 4 \\ CB[3] & = & 1 \\ P_{BPM} & = & ADL \end{array} \right\} \Rightarrow F_{MV} = 0.125$$

$$\left\{ \begin{array}{lcl} CB[1] & = & 4 \\ CB[3] & = & 1 \\ P_{BPM} & = & ACR \end{array} \right\} \Rightarrow F_{MV} = 1$$

B.3.3 Beam Charge

For the Beam Length the factor is defined as described hereunder :

$$CB[1] \neq 4 \Rightarrow F_{BC} = 0.25 * CB[2]$$

$$\left\{ \begin{array}{rcl} CB[1] & = & 4 \\ CB[3] & = & 1 \end{array} \right\} \Rightarrow F_{MV} = 1$$

$$\left\{ \begin{array}{rcl} CB[1] & = & 4 \\ CB[3] & \neq & 1 \end{array} \right\} \Rightarrow F_{MV} = CB[2]$$

Annex C

Hardware demonstration details

C.1 VHDL blocks details

In these sections are shown extra material that has been judged as useful in case the VHDL blocks are re-used for future projects.

The Figure C.1 shows the simulation undertaken for the threshold comparison block. A code coverage analysis have been performed and the result can be found in Figure C.2.

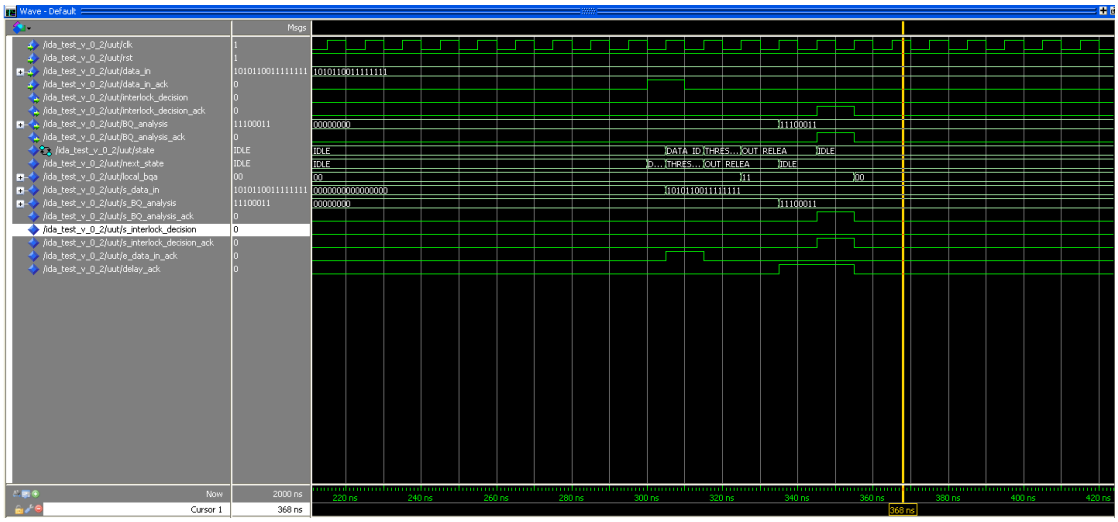

FIGURE C.1: Threshold comparison VHDL block - Simulation

The Figure C.3 shows the simulation undertaken for the summarizer block. Again, a code coverage have been performed and the result can be found in Figure C.4.

The Figures C.5 and C.6 shows the simulation undertaken for the beam permit loop block. The first simulation shows the master implementation. The second simulation shows a complete permit loop (one master and two slaves).

```
Coverage Report Summary Data by file

File: IDA.vhd
    Enabled Coverage        Active      Hits    Misses \% Covered
    ----------------        ------      ----    ------ ----------
    Statements                  55        55         0      100.0
    Branches                    37        37         0      100.0
    FEC Condition Terms          4         4         0      100.0
    FEC Expression Terms         0         0         0      100.0
    States                       4         4         0      100.0
    Transitions                  7         7         0      100.0
    Toggle Bins                130        92        38       70.7
```

FIGURE C.2: Threshold comparison VHDL block - Code coverage report

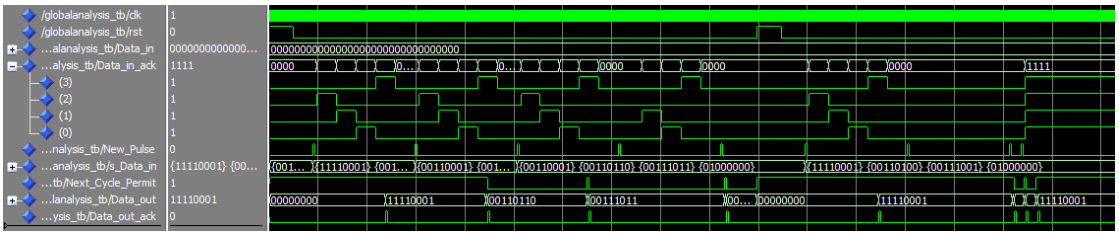

FIGURE C.3: Summarizer VHDL block - Simulation

```
Total Coverage By File (code coverage only, filtered view): 87.0%

File: ../IDA/GlobalAnalysis.vhd
    Enabled Coverage        Active   Hits    Misses   \% Covered
    ----------------        ------   ----    ------   ----------
    Stmts                       67     67         0      100.0
    Branches                    82     81         1       98.7
    FEC Condition Terms         25     21         4       84.0
    FEC Expression Terms         0      0         0      100.0
    States                       4      4         0      100.0
    Transitions                 10      8         2       80.0
    Toggle Bins                126     96        30       76.1
```

FIGURE C.4: Summarizer VHDL block - Code coverage report

The Figure C.7 is shown the two implementations performed in order to prove the VHDL control block is functional.

The Figure C.8 shows a printscreen of the Xilinx wizard to configure the gigabyte modules. It is summarizing the main options chosen.

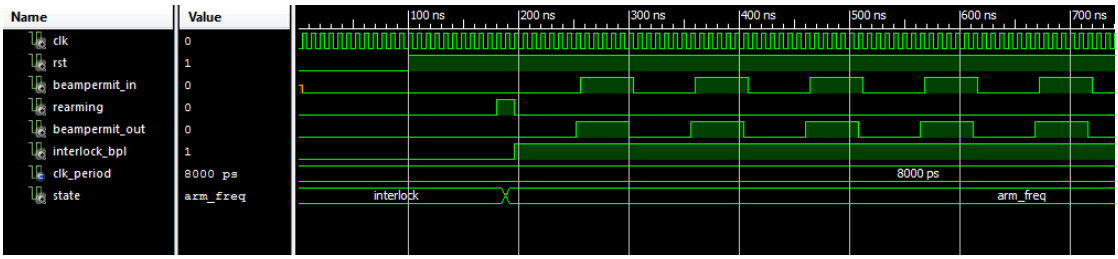

FIGURE C.5: Beam permit loop VHDL block - Simulation master

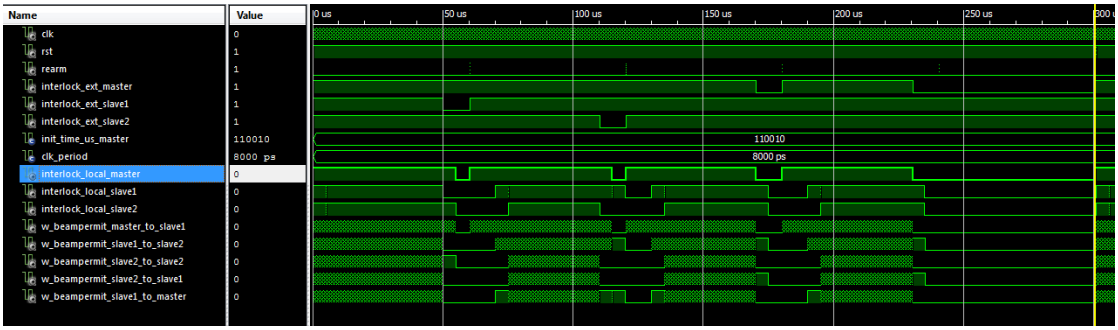

FIGURE C.6: Beam permit loop VHDL block - Simulation complete loop

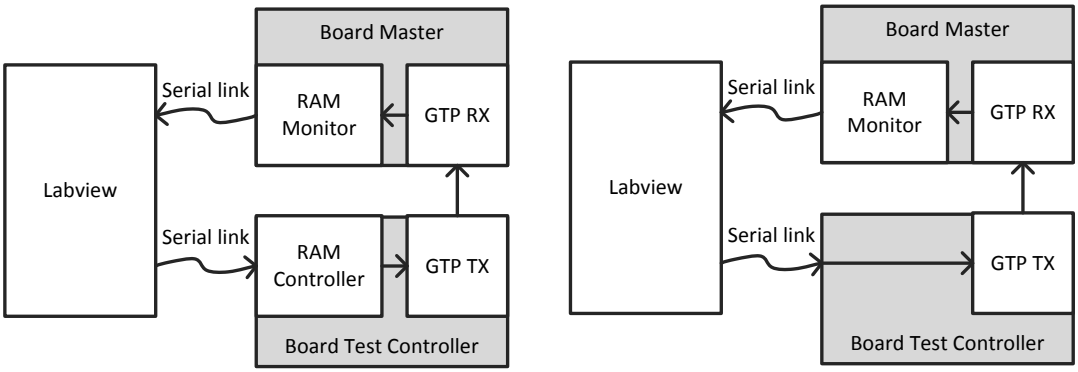

FIGURE C.7: Control VHDL block - implementation

C.2 VHDL code extracts

Hereafter are shown several examples of VHDL code developed :

- In Figure C.9 is shown the use of GENERATE ability to keep the design modular. In this case the threshold comparison module (named IDA) is generated and configured through the generic, defined in a package. This generic array is shown in Figure C.10.
- In Figure C.11 is shown the summarizer core function. It shows how the worst value is extracted to be forwarded at the output (lines 17-19). The fail-safe mechanism is shown too (line 25).

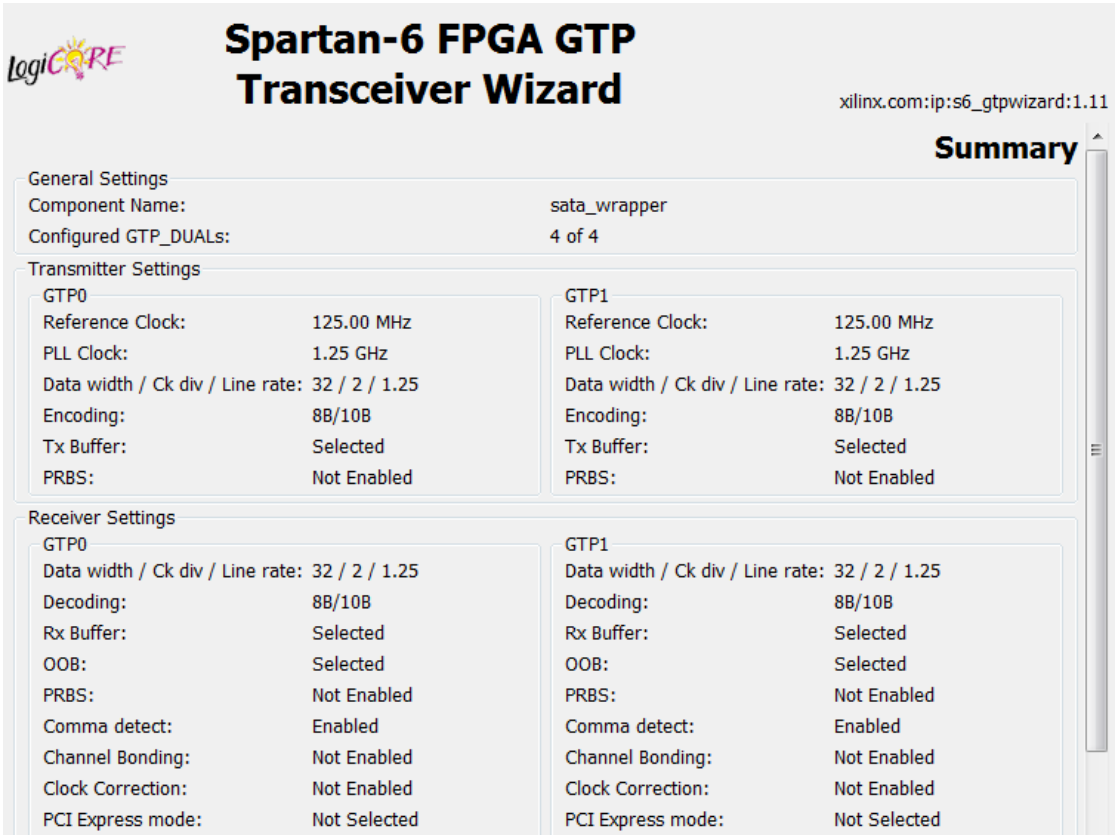

FIGURE C.8: Gigabyte link VHDL block - wizard option

– As explained in the design proposal and verification chapter, the summarizers function can handle local rules. In Figure C.12 is shown the local rule integrated in the prototype. the local rule allows a summarizer to not trigger an INTERLOCK if one input data is missing.

```
1
2  IDA_generation:for i in 0 to my_IDA_array'high generate
3  IDA_inst:IDA
4  Generic map(
5          RESET_ACTIVE    =>  RESET_ACTIVE,
6          REFERENCE_VALUE =>  my_IDA_array(i).Threshold,
7          HEADER_DATA     =>  my_IDA_array(i).Header,
8          UID_IDA         =>  my_IDA_array(i).UID,
9          PPA_MODULE      =>  my_IDA_array(i).PPA
10                                 )
11         Port map (
12                 clk                    => clk,
13                 rst                    => rst,
14                 data_in                => s_IDA_input,
15                 data_in_ack            => s_IDA_input_ack,
16                 interlock_decision     => s_Interlock_IDA(i),
17                 interlock_decision_ack => s_Interlock_IDA_ack(i),
18                 BQ_analysis            => s_BQ_analysis(i),
19                 BQ_analysis_ack        => s_BQ_analysis_ack(i)
20                           );
21 end generate;
22
```

FIGURE C.9: VHDL block - GENERATE illustration

```
1
2
3  constant my_IDA_array: IDA_array := (
4  --    header,  threshold,   UID,   PPA
5     ("00000001","00000001","000001", '0'), -- Alignement critical status
6     ("00000010","00000001","000001", '0'), -- Cooling critical status
7     ("00000011","00101000","000010", '1'), -- Cooling temperature
8     ("00000100","01010001","000011", '1'), -- BLM 1
9     ("00000101","01010001","000011", '1'), -- BLM 2
10    ("00000110","01100101","000100", '1'), -- BPM 1
11    ("00000111","01100101","000100", '1'), -- BPM 2
12    ("00001000","00000001","000001", '0'), -- Beam Instrumentation status
13    ("00001001","00000001","000001", '0'), -- Power status
14    ("00001010","01011101","000101", '1'), -- RF WakeFieldMonitor
15    ("00001011","01100100","000110", '1'), -- RF Intrumentation
16    ("00001100","00000001","000001", '0'), -- RF status
17    ("00001101","00010100","000111", '0'), -- Stabilization relative Positionment
18    ("00001110","00000001","000001", '0'), -- Stabilization Seisometer
19    ("00001111","00110010","001000", '0'), -- Vacuum value
20    ("00010000","00000001","000001", '0'), -- Vacuum valve
21    ("00010001","00000001","000001", '0'), -- Target system state
22    ("00010010","00000001","000001", '0'), -- Collimation status
23    ("00010011","00000001","000001", '0'), -- Experiment status
24    ("00010100","00000001","000001", '0'), -- Crab cavities
25    ("00010101","00000001","000001", '0'), -- Feedback system
26    ("00010110","00000001","000001", '0')-- Operation Manager state
27         );
28
```

FIGURE C.10: VHDL block - Threshold comparison configuration illustration

```
1
2  s_Data_out_proc: process(rst, clk)
3  variable v_Data_in: STD_LOGIC_VECTOR(7 downto 0);
4  begin
5    if rst = RESET_ACTIVE then
6      s_Data_out <= (others=>'0');
7      v_Data_in  := (others=>'0');
8    elsif rising_edge(clk) then
9      if(state=COMPUTE)then --means s_data_in_ack_register=(others=>'1');
10       for i in 0 to (NUMBERS_OF_INPUTS-1) loop
11         if(s_data_in_ack_register(i)='1')then -- for local rule 1
12           if(i=0)then
13             v_Data_in := s_Data_in(i);
14           else
15             -- with this type of comparison, it is mandatory to use
16             -- a variable and not a signal (variable has not delay)
17             if((s_Data_in(i)(1 downto 0))>(v_Data_in(1 downto 0)))then
18               v_Data_in := s_Data_in(i);
19             end if;
20           end if;
21         end if;
22       end loop;
23       s_Data_out <= v_Data_in;
24     elsif(state=COLLECT and next_state=OUT_RELEASE)        then
25       s_Data_out <= UID_IDA & INTERLOCK; -- Fail-safe value
26     elsif(state=OUT_RELEASE and next_state/=OUT_RELEASE)then
27       s_Data_out <= (others=>'0');
28       v_Data_in         := (others=>'0');
29     end if;
30   end if;
31 end process;
32
```

FIGURE C.11: VHDL block - summarizer core function

```
1
2  Local_rule_1_all_data_received_proc: process(rst, clk)
3  variable one_missing: integer;
4  begin
5    if rst = RESET_ACTIVE then
6      Local_rule_1_all_data_received <= '0';
7      one_missing :=0;
8    elsif rising_edge(clk) then
9      one_missing :=0;
10     for i in 0 to (NUMBERS_OF_INPUTS-1) loop
11       if(s_data_in_ack_register(i)='0')then
12         one_missing:=one_missing+1;
13       end if;
14     end loop;
15
16     if(one_missing=0 or one_missing=1)then
17       Local_rule_1_all_data_received <= '1';
18     else
19       Local_rule_1_all_data_received <= '0';
20     end if;
21   end if;
22 end process;
23
```

FIGURE C.12: VHDL block - summarizer local rule example

Annex D

Research trails for the CLIC Interlock System

When undertaking a project as the CLIC Interlock system design, it is hardly possible to cover all the options. Consequently, this annex gathers the main research trails which have not been fully covered in the manuscript but have been suggested at one point of the design process.

D.1 Beam quality

The principle of the post-pulse analysis is to trigger an interlock when a bad beam quality is observed. The definition of beam quality depends of the point of view. On the experiment side, a good beam quality infers a good ratio between collision events and beams. On the machine protection point of view, a good beam quality means low losses.

A research trail to enhance the CLIC Interlock System project would be to define the beam quality and the beam stability with regard to the post-pulse analysis. The main concepts to explore are : the beam baseline tune, chromaticity, emittance, uniform bunch intensity, tail/satellite population, beam halo, drift and obviously beam losses.

D.2 Interlock System and beam operation

Due to the early stage of the CLIC project, the interaction of the Interlock System with the beam operation has not been fully covered. The main points stated in the thesis are :

- A pilot beam is sent to commission the machine. It is a safe beam that can not damage machine structure.

- the ramping procedure is estimated taking around 5000 steps, inferring a 10 seconds ramping time.

The Interlock System primary goals is to ensure the machine safety. However, under the cover this goals is reach, it has to maximize the beam availability. One research trail would be to study in which case an interlock demand would not imply restart the ramping procedure from the pilot beam. For instance, if a data is missing, the Interlock System could *freeze* the ramping process and wait the next pulse if the data is not missing instead of interlocking the machine and start the ramping from the pilot beam.

A second research trail is the implementation of this beam availability maximization. It has been suggested to use several beam permits. For instance, one for the pilot beam, one for the ramping beam and the last for the nominal beam. Another proposition is to implement a beam permit impact signal. It would specify how an interlock request should impact (e.g. *freeze* the ramping procedure, restart from pilot beam)

A sequencer is mentioned in the CLIC Conceptual Design Report (CDR) in the control chapter. It is most likely the system the Interlock System should interact with it to optimize the availability.

D.3 Interlock System and injection complex

In the thesis works, the design process has been focused on the CLIC main linacs. However, the expansion of the Interlock System to the injector complexes could be studied.

A case study could be done for the damping rings, in the main beam injector complex. From discussion with experts, the main post-pulse analysis that should be based on BPM. However, a couple of issues appears :

- The threshold comparison on one value of a BPM is not enough. Drift analysis should be performed on several consecutive BPM. It has to be determined if this analysis could be handle by the Interlock System or should it be done by the client before releasing to the Interlock System.
- Following the BPM mode (linear/non-linear), it may happen that the value given is not absolute. In this case, a threshold comparison cannot be done. However, comparison could be done between BPM.

D.4 Interlock System and radiation

When the thesis has been started, one of the main challenge we expected was the radiation level that may disturb the CLIC Interlock System. Consequently, a study had been started on the radiation impacts on the Interlock System and the mitigation techniques. However, after investigation, the proposed solution for the Interlock System has been to move their implementation in the alcoves (i.e. outside the tunnel). Thus, the expected radiation level has decreased significantly. The only impact expected has been reduced to SEU.

Hereunder are shown the radiation levels and the fluences the Interlock System would have to handle if it was located in the CLIC tunnel (initial plan). A radiation study for CLIC main and drive beam complexes has been performed [49]. This study has been done with the FLUKA tool. FLUKA is an integrated Monte-Carlo simulation package for the interaction and transport of particles and nuclei in matter. The simulations have been done separately for the main and drive beam and are presented in Figure D.1, D.2, D.3 and D.4.

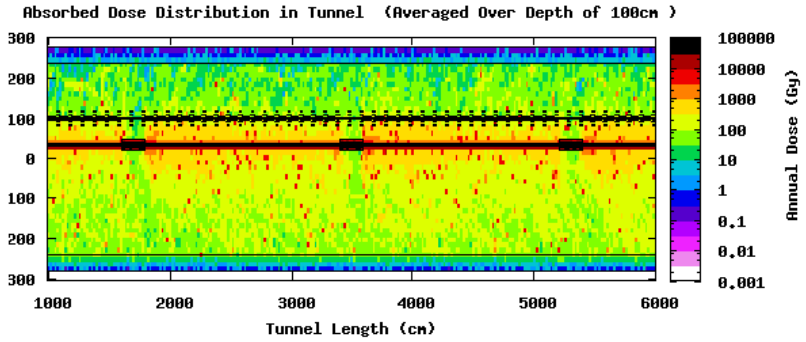

FIGURE D.1: Radiation dose due to the main beam at 1.5 TeV

In Table D.1 is summarized the radiation levels the Interlock System would receive if it was located in the tunnel.

TABLE D.1: Annual CLIC radiation and fluence for electronic systems in the tunnel

	Main beam (1.5 TeV)	**Drive beam (2.4 GeV)**
Annual absorbed dose (Gy)	200	100
Annual 1 MeV equivalent neutrons fluence (cm^{-2})	$1 * 10^{11}$	$1 * 10^{12}$
Annual >20 MeV hadrons fluence (cm^{-2})	$1 * 10^{10}$	$1 * 10^{10}$

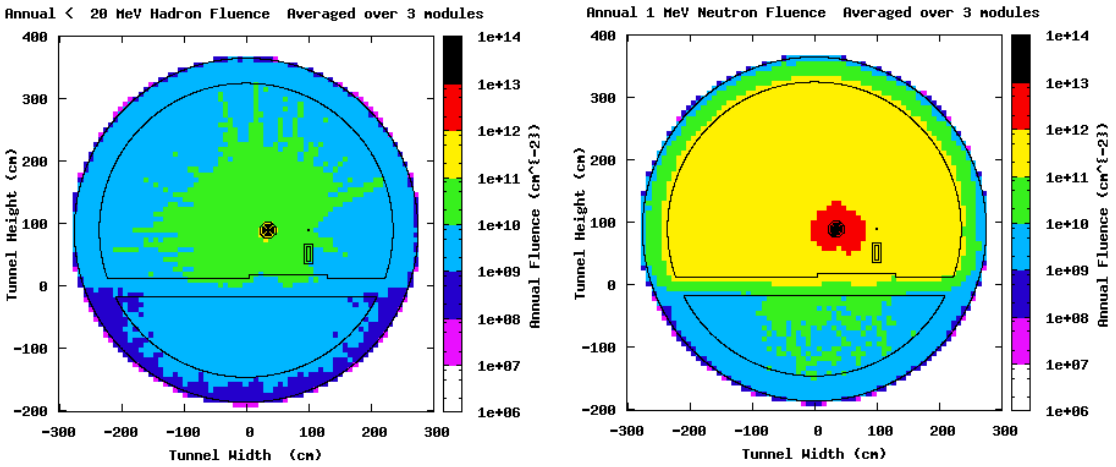

FIGURE D.2: Hadrons and neutrons fluence due to the main beam at 1.5 TeV

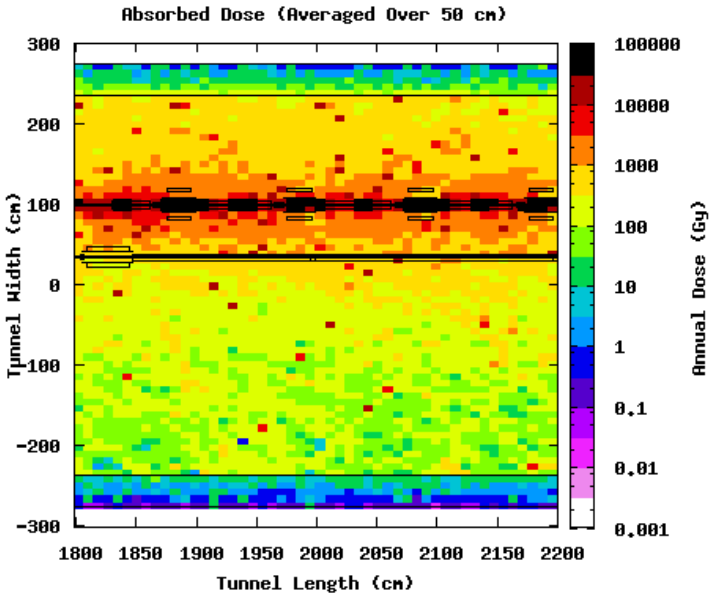

FIGURE D.3: Radiation dose due to the drive beam at 2.4 GeV

With these radiation levels, an Interlock system in the tunnel without adequate protection will suffer high failure rates dues to SEU and lattice displacement damage. Even far from the beam lines, the radiation level will remain high. Consequently, some protections and mitigation techniques would have been needed.

D.5 Interlock System and acquisition infrastructure

In Figure D.5 is shown the amount of signals that need to be acquired on each CLIC module. The machine protection signals are dedicated to the Interlock System. They are

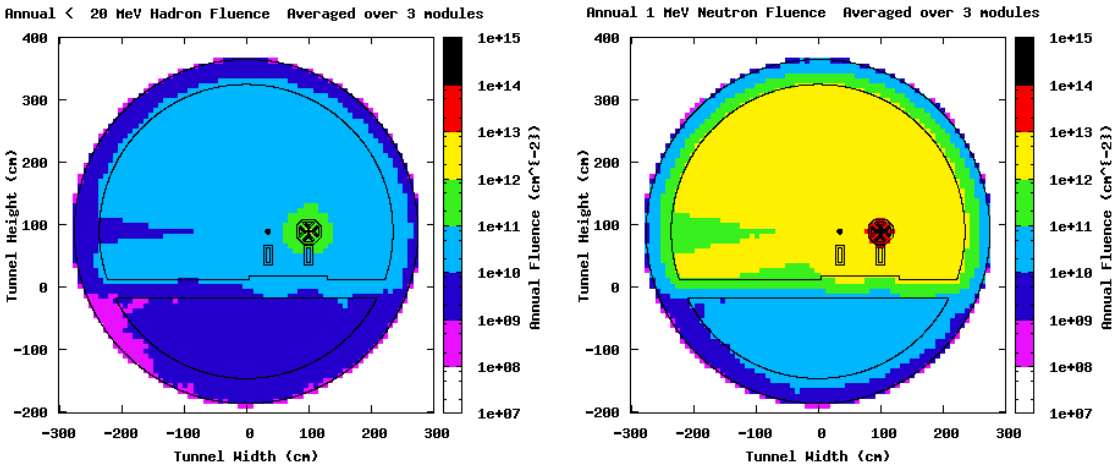

FIGURE D.4: Hadrons and neutrons fluence due to the drive beam at 2.4 GeV

the duplicated signals discussed in the expectations to the interfaced systems (chapter 4).

In the design proposal chapter, the critical signals that should be duplicated in the acquisition infrastructure have been defined. We have defined as critical the signals that would trigger an interlock if they were missing. The others signals are not critical. However, some of them would be used by the Interlock System. If one of these non-critical signals was lacking, a mitigation mechanism would use the consecutive (temporally or geophysically speaking) value.

A proposed research trail would be to determine the tolerable amount of lacking non-critical signal before triggering an interlock.

CLIC - ACM Interfaces

Interface type	# of ch	# /w backups	# of ch / card	# of cards / crate	Spare signals	Comment
V. Fast ADC	2	4	2	2	2	Placed in alcoves 10+b @ 2 GHz
Fast ADC	43	72	8	9	29	14 b @ 200 MHz
Slow ADC	113	192	32	6	79	6 b @ 10 kHz, multiple channels, muxed
Raw DIO	146	256	128	2	110	Check cooling!!
Serial IO	14	32	16	2	18	Serial interfaces (wires/2)
Slow DAC	8	32	32	1	24	18b @ 1kHz
reserved1	0	0	1	0	0	For future use
reserved2	0	0	1	0	0	For future use
Total	324			20		

Helper table:	Alignment	Cooling	Beam Instrumentation	Machine protection	Powering	RF-Instrumenation	Stabilization	Vacuum	Total:Total
V. Fast ADC	0	0	0	2	0	0	0	0	2
Fast ADC	0	0	13	15	0	15	0	0	43
Slow ADC	34	44	4	8	2	0	21	0	113
Raw DIO	0	88	54	0	0	4	0	0	146
Serial IO	14	0	0	0	0	0	0	0	14
Slow DAC	0	0	0	0	2	0	6	0	8
reserved1	0	0	0	0	0	0	0	0	0
reserved2	0	0	0	0	0	0	0	0	0
Total:	48	132	71	25	4	19	27	0	324

FIGURE D.5: CLIC acquisition crate signals list

D.6 Local rules for global analysis

In the functional analysis, we have specified that the global analysis subfunction implements local rules. To complete the Interlock System design, a more exhaustive list of local rules should be listed. Hereunder is proposed additional rules.

- default rule : propagate the worst case.
- stressed rule : any fault severity in input which is not SAFE will trigger an interlock.
- geographic rule : one data in particular is not taken in account when lacking (for instance, because its sensor is subject to radiation and fail often).
- consistency rules : for instance, if a beam current transformer gives an fault severity FAILURE, the following beam current transformers should as well deliver the same fault severity level.
- voting rule : for instance, if only one data is lacking, it is ignored. An other exemple would be to implement a 2 out of 3 voting system for three same type of data.

Annex E

Requirements and constraints list

E.1 Requirements list

In this section are summarized the requirements established from chapter 3.

Concerning the functional requirements, the system shall be able to :
- Interlock the machine by synthesis the local interlock demand
- Perform a post-pulse analysis, by analysing the beam quality of the previous pulse to assert the next pulse stability.
- Perform control functions such as manually interlock the machine.
- Perform monitor functions in order give a representation of the current state of the Interlock System.
- Perform tests functions, such as emulate the inputs to trigger interlocks.
- Mask inputs for commissioning test.
- Increase or decrease the number of modules in the beam permit loop.

Concerning the performance requirements, for the response times :
- 2 ms to interlock the machine, from equipment failure up to actual interlocked machine
- 6 ms to perform the post-pulse analysis (Interlock System only)

Concerning the performance requirements, for the dependability requirements :
- availability 99.75%
- reliability (continuity) with transient : $1.8 * 10^6$ pulses
- reliability (continuity) without transient : $3.6 * 10^8$ pulses

These rates have been translated to the node level. the related node level rates are shown in Table E.1.

TABLE E.1: Simulation results - single node failure rates

Voting	**False Veto decision rate**	**False Pass decision rate**
1 out of 1	$9 * 10^{-9} h^{-1}$	$1 * 10^{-10} h^{-1}$
1 out of 2	$6 * 10^{-9} h^{-1}$	$5 * 10^{-6} h^{-1}$
1 out of 3	$4 * 10^{-9} h^{-1}$	$1 * 10^{-4} h^{-1}$
2 out of 3	$1 * 10^{-6} h^{-1}$	$3 * 10^{-6} h^{-1}$

E.2 Environment constraints list

From the study of the critical interfaces, the following constraint have been extracted :

- 48 front-end modules dedicated to Interlock system to receive data from acquisition infrastructure. TYhese modules are located in the alcoves all long the main linac.
- A gigabyte technology at the front-end modules is planned to be used (type of gigabyte Ethernet, with some precision timing protocol and synchronous-Ethernet).
- 4 target systems (dumping systems and RF sources), geographically dispersed, to inhibit simultaneously.

E.3 External requirements list

From the study of the critical interfaces, the following expectations from the Interlock system to these interfaced systems have been fixed :

To acquisition infrastructure :
- Tolerable corruption rate= $4.6 * 10^{-7} pulse^{-1}$ (method 1)
- Tolerable corruption rate= $7 * 10^{-8} pulse^{-1}$ (method 2)

In addition, a redundancy is asked to implement on these signals :
- Beam loss monitors : Cherenkov fibers
- Power converter : failure time 10-100 ms
- RF : beam instrumentation
- Wake field monitors : position detectors
- Positioning : relative displacement
- Vacuum : Valve

To the target systems :
- Tolerable rate to miss an beam inhibition request=$4.6 * 10^{-7} pulse^{-1}$ (method 1)
- Tolerable rate to miss an beam inhibition request=$7 * 10^{-8} pulse^{-1}$ (method 2)

Annex F

Conferences and workshops

Design process of the Interlock System for the compact linear collider. P. Nouvel, B. Puccio, M. Jonker, H. Tap. *Proceedings of International Particle Accelerator Conference 2013* (IPAC13).

Dependability requirements and design compliance for Interlock Systems. P. Nouvel, B. Puccio, M. Jonker, H. Tap. *Proceedings of International Conference on Control and Fault-Tolerant Systems 2013* (Systol13).

Journée annuelle de l'ecole doctorale GEET 2013 :
Processus de conception du système de verrouillage pour le Collisionneur Linéaire Compact.
March 2013.

CLIC workshop 2013 :
Design Process of the Interlock Systems for CLIC
hyperlink - January 2013.

Workshop on Machine protection, focusing on Linear Accelerator complexes :
CLIC Interlock system : preliminary study
hyperlink - june 2012

MPE Technical Meeting :
CLIC Interlock System study : from Principle to Prototyping
hyperlink - 22-03-2012

Glossary and acronyms

ASCII American Standard Code for Information Interchange, binary code representing a character.

BIS Beam Interlock System.

BLM Beam Loss Monitor.

BPM Beam Position Monitor.

bunch in accelerators, particles are gathered in bunch in order to increase the physics events at collision point.

CDR Conceptual Design Report.

CERN European Organisation for the Nuclear Research.

CLEX in CTF3, the CLEX is the experimental area where the main feasibility are undertaken.

CLIC Compact Linear Collider.

collimator a collimator is a passive device (mask) which clean the beam halo by removing the outer particles of a bunch.

cryomodule In accelerator, a cryomodule is an accelerating/magnet structure encapsulated in a tank which is cooled down, for instance, with liquid helium.

CTF3 CLIC Test Facility 3.

emittance for a beam, it is the average spread of particle coordinates in phase-space.

ESRF European Synchrotron Radiation Facility.

ESS European Spallation Source.

FAIR Facility for Antiproton and Ion Research.

FMC FPGA Mezzanine Carrier.

FNAL Fermi National Accelerator Laboratory.

FPGA Field Programmable Gate Array.

FRIB Facility for Rare Isotope Beams.

FSM Finite State Machine.

gluon Family of bosons (a.k.a. gauge bosons) responsible for the strong force.

GUI General User Interface.

HIAF Heavy Ion Accelerator Facility.

ICFA International Committee for Future Accelerators.

IEC International Electrotechnical Commission.

IEEE Institute of Electrical and Electronics Engineers.

ILC International Linear Collider.

ILD International Large Detector.

JAVA Object oriented programming language. It is used in the feasibility study.

kicker fast magnet used for beam injection or extraction.

klystron conventional RF source (vacuum tube) for beam acceleration purpose.

Labview Labview is a G-based software developed by National Instrument. Its core activity is test bench instrumentation. It is used in the hardware demonstration.

LCLS Linac Coherent Light Source.

LEP Large Electron-Positron collider.

lepton Family of elementary particle. It is made of electrons, muons tauons and their associated neutrinos and their antiparticles.

LHC Large Hadron Collider.

linac abbreviation commonly used for linear accelerator.

luminosity In accelerator physics, the luminosity is related to the number of particles per unit area per unit. It is an important value to characterize the performance of a particle accelerator.

middleware In accelerator context, the middleware is a technical network where devices are connected to send and receive data. Authorized users can access these data and are able to control the devices thus connected.

MTBF Mean Time Between Failures.

PETS Power Extraction and Transfer Structure.

PLC Programmable Logic Controller.

PLD Programmable Logic Device.

quadrupole A quadrupole is a magnet with four poles. In particle accelerator, it is used to focus and to defocus the beam. It is similar to optical lens with light.

quark Family of elementary particle. there are 6 flavours : Down, Up, Strange, Charm, Bottom, Top.

RAM Random Access Memory.

RF Radio Frequency.

RTML Ring To the Main Linac.

SATA Serial Advanced Technology Attachment.

SCRF SuperConductive Radio Frequency.

SEU Single Event Upset.

SFP Small Form-factor Pluggable.

SiD Silicon Detector.

SIL Safety Integrity Level.

Sinap Shanghai Institute of Applied Physics.

SMP Safe Machine Parameters.

SPEC Simple PCI-Express FMC Carrier.

spoiler in accelerators, a beam spoiler is a piece of material used to modify the penetration depth of the particles.

SPS Super Proton Synchrotron.

synchrotron radiation When charged particles are accelerated radially, they produce some electromagnetic radiations so called synchrotron radiations.

UART Universal Asynchronous Receiver Transmitter.

VHDL States for VHSIC Hardware Description Language, it is used to program the Programmable Logic Devices such as FPGA or CPLD. In the thesis works, it is used in the hardware demonstration.

wall current monitor in accelerators, this is a monitoring tool used to observe the time profile of particle beams.

Xilinx American company of semi-conductor, specialized in FPGA. Their tools and products have been used in the hardware demonstration.

Bibliography

[1] European Organization for Nuclear Research(CERN). Physics and detectors at CLIC : CLIC conceptual design report, vol. 2. Technical report, CERN, 2012.

[2] Barry C Barish and S Yamada. The International Linear Collider : Technical design report. volume 1 : Executive summary. Technical Report CERN-ATS-2013-037. ANL-HEP-TR-13-20. BNL-100603-2013-IR. IRFU-13-59. Cockcroft-13-10. CLNS-13-2085. DESY-13-062. FERMILAB-TM-2554. IHEP-AC-ILC-2013-001. ILC-REPORT-2013-040. INFN-13-04-LNF. JAI-2013-001. JINR-E9-2013-35. JLAB-R-2013-01. KEK-Report-2013-1. KNU-CHEP-ILC-2013-1. LLNL-TR-635539. SLAC-R-1004. ILC-HiGrade-Report-2013-003, CERN, Geneva, Jun 2013.

[3] IEEE Computer Society. *Standard for Application and Management of the Systems Engineering Process*. 2005.

[4] ESS Gregor Cuk, Cosylab. Annika Nordt. Machine protection plans in ESS. *Presentation at Machine Protection Workshop focused on Linear Collider*, 2012.

[5] Benjamin Todd. *A Beam Interlock System for* CERN *High Energy Accelerators*. PhD thesis, Brunel University West London, 2006.

[6] S. Norum et al. The machine protection system for the linac coherent light source. *Proceedings of PAC09*, 2009.

[7] Benjamin Todd. Safe machine parameters 3v2, EDMS 1096447. Technical report, CERN, 2011.

[8] A. Solodko G. Riddone A. Samoshkin, D. Gudkov. CLIC two beams module for the CLIC conceptual design and related experimental program. *Proceedings of IPAC11*, 2011.

[9] M. J. Barnes J. Borburgh B. Goddard Y. Papaphilippou J. Uythoven R. Apsimon, B. Balhan. Optics and protection of the injection and extraction regions of the CLIC damping rings. *Proceedings of IPAC13*, 2013.

[10] Oak Ridge TN 37830 USA C. Sibley, SNS ORNL. Machine protection strategies for high power accelerators. *Proceedings of Particle Acclerator Conference*, 2003.

[11] R Schmidt et al. Protection of the CERN large hadron collider. *New Journal of Physics 8*, 2006.

[12] European Organization for Nuclear Research(CERN). The CLIC programme : towards a staged e+e- linear collider exploring the terascale, CLIC conceptual design report, vol. 1. Technical report, CERN, 2012.

[13] European Organization for Nuclear Research(CERN). A multi-tev linear collider based on CLIC technology : CLIC conceptual design report, vol. 3. Technical report, CERN, 2012.

[14] Peter W. Higgs. Broken symmetries and the masses of gauge bosons. *Phys. Rev. Lett.*, 13 :508–509, Oct 1964.

[15] Wojciech Krolikowski. A hidden valley model of cold dark matter. Technical Report arXiv :0803.2977. IFT-08-5, Mar 2008. Comments : 9 pages.

[16] Matti Heikinheimo, Antonio Racioppi, Martti Raidal, Christian Spethmann, and Kimmo Tuominen. Dark supersymmetry. Technical Report arXiv :1305.4182, May 2013. Comments : 7 pages, 5 figures.

[17] Robert Oerter. *The theory of almost everything : The* S*tandard* M*odel, the unsung triumph of modern physics*. Pi Press, New York, 2006.

[18] J.P. Delahaye. Towards CLIC feasibility. *Proceedings of IPAC10, Kyoto, Japan*, 2010.

[19] Michael Jonker et al. the CLIC machine protection. *Proceedings of IPAC10, Kyoto, Japan*, 2010.

[20] Benjamin Todd et al. The architecture, deisgn and realisation of the LHC beam interlock system. *Proceedings of ICALEPCS 2010*, 2010.

[21] Maciej Kwiatkowski. *Methods for the Application of Programmable Logic Devices in Electronic Protection Systems for High Energy Particle Accelerators*. PhD thesis, WARSAW UNIVERSITY OF TECHNOLOGY, 2013.

[22] Steven Holzner. *Physics I for dummies ; 2nd ed.* Wiley, Hoboken, NJ, 2011.

[23] Barry C Barish and S Yamada. The International Linear Collider : Technical design report. volume 4 : Detector. Technical Report CERN-ATS-2013-037. ANL-HEP-TR-13-20. BNL-100603-2013-IR. IRFU-13-59. Cockcroft-13-10. CLNS-13-2085. DESY-13-062. FERMILAB-TM-2554. IHEP-AC-ILC-2013-001. ILC-REPORT-2013-040. INFN-13-04-LNF. JAI-2013-001. JINR-E9-2013-35. JLAB-R-2013-01. KEK-Report-2013-1. KNU-CHEP-ILC-2013-1. LLNL-TR-635539. SLAC-R-1004. ILC-HiGrade-Report-2013-003, CERN, Geneva, Jun 2013.

[24] Sigrid Wagner et al. Artchitecture for interlock systems : Reliability analysis with regard to safety and availability. *Proceedings of ICALEPCS2011, Grenoble, France*, 2011.

[25] Sigrid Wagner. LHC *Machine Protection System : Method for Balancing Machine Safety and Beam Availability.* PhD thesis, ETH ZURICH, 2010.

[26] Ed Kawamura Ying Guo, Xibin Gu and Ralf I. Kaiser. Design of a modular and versatile interlock system for ultrahigh vacuum machines : A crossed molecular beam setup as a case study. *REVIEW OF SCIENTIFIC INSTRUMENTS 77, 034701*, 2006.

[27] F. Rodriguez-Mateos A. Vergara Fernandez. Reliability of the quench protection system for the LHC superconducting elements. *Nuclear Instruments and Methods in Physics Research A 525*, 2004.

[28] Juan R. Pimentel and Mario Salazar. Dependability of distributed control system fault tolerant units. *Proceedings of IECON 02*, 2002.

[29] M. Kago et al. Design of the accelerator safety interlock system for xfel in spring-8. *Proceedings of ICALEPCS 2009*, 2009.

[30] J.W. Lee H.S. Kang J. Choi B.R. Park, J.C. Yoon. Development of machine interlock system HMI for PLS. *Proceedings of EPAC 2006, Edinburgh, Scotland*, 2006.

[31] Markus Zerlauth et al. The LHC post mortem analysis framework. *Proceedings of ICALEPCS 2009*, 2009.

[32] Jose-Luis Sanchez Alvarez Giulia Bellodi, Bettina Mikulec. Linac4 watchdog specifications, EDMS 1155020. Technical report, CERN, 2011.

[33] V. Kain et al. Injection beam loss and beam quality checks for the LHC. *Proceedings of EPAC08*, 2008.

[34] G. Papotti. A beam quality monitor for LHC beams in the SPS. *Proceedings of EPAC08*, 2008.

[35] *Systems and software engineering : system life cycle processes ; 2nd ed.* ISO, Geneva, 2008.

[36] *Processes for engineering systems.* ANSI/EIA, 2004.

[37] *MILITARY STANDARD : SYSTEM ENGINEERING MANAGEMENT.* Departement of defense, 1969.

[38] Richard Barker. *Case Method : Function and Process Modelling.*

[39] Y. HervÉ and P. Desgreys. Functional virtual prototyping design flow and vhdl-ams. In *Forum on specification & Design Languages (FDL'06)*, Darmstadt, Allemagne, 2006. ECSI.

[40] Brian Randell Carl Landwehr Algirdas Avizienis, Jean-Claude Laprie. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 2004.

[41] IEC Functional Safety. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.*

[42] B. Todd et al. A look back on 2012 LHC availability. *LHC Beam Operation workshop - Evian 2012*, 2012.

[43] A. Christy Persya and T.R.Gopalakrishnan. Fault tolerant real time systems. *Proceedings of International Conference on Managing Next Generation Software Application*, 2008.

[44] B. Mikulec B. Puccio J.L. Sanchez A. Apollonio, J.B. Lallement. Reliability approach for machine protection design in particle accelerators. *Proceedings of IPAC13*, 2013.

[45] Chandra Kintala Dongyan Chen, Sachin Garg and Kishor S. Trivedi. Dependability enhancement for ieee 802.11 wireless lan with redundancy techniques. *Proceedings of the 2003 International Conference on Dependable Systems and Networks*, 2003.

[46] Donald Firesmith. Engineering safety requirements, safety constraints and safety-critical requirements. *JOURNAL OF OBJECT TECHNOLOGY*, 2004.

[47] Chandra Kintala Dongyan Chen, Sachin Garg and Kishor S. Trivedi. Dependability enhancement for IEEE 802.11 wireless LAN with redundancy techniques. *Proceedings of the 2003 International Conference on Dependable Systems and Networks*, 2003.

[48] S.Vilalte on behalf the LAPP CLIC group. Acquisition system for the CLIC module. *Proceedings of LCWS11*, 2011.

[49] Thomas Otto and Sophie Mallows. Ionizing radiation estimates for the CLIC main and drive beams. *Presentation at SATIF 10*, 2010.

[50] Günther Geschonke and A Ghigo. CTF3 design report. Technical Report CERN-PS-2002-008-RF. CTF-3-NOTE-2002-047. LNF-2002-008-IR, CERN, Geneva, May 2002. revised version number 1 submitted on 2002-06-19 12 :11 :29.

[51] Roberto Filippini, Etienne Carlier, Laurent Ducimetière, Brennan Goddard, and Jan Uythoven. Reliability analysis of the LHC beam dumping system. (LHC-Project-Report-811. CERN-LHC-Project-Report-811) :4 p, Jun 2005.

[52] N. Magnin J. Uythoven R. Filippini, E. Carlier. Reliability analysis of the LHC beam dumping system taking into account the operational experience during LHC run 1. *Proceedings of ICALEPCS 2013, San Fransisco, USA*, October 2013.

[53] J. Emery J. Fitzek F. Follin S. Jackson V. Kain G. Kruk M. Misiowiec C. Roderick M. Sapinski C. Zamantzas, B. Dehning. Configuration and validation of the LHC beam loss monitoring system. *Proceedings of DIPAC09, Basel, Switzerland*, 2009.

[54] P. Gander M. Jonker M. Lamont R. Losito A. Masi M. Sobczak S. Redaelli, R. Assmann. The LHC collimator controls architecture - design and beam tests. *Proceedings of PAC07, Albuquerque, New Mexico, USA*, 2007.

[55] E Bravin. First results from the LHC beam instrumentation systems. (CERN-ATS-2009-027) :4 p, May 2009.

[56] Mourad Debbabi, Fawzi Hassaine, Yosr Jarraya, Andrei Soeanu, and Luay Alawneh. *Verification and Validation in Systems Engineering*. Springer, Dordrecht, 2010.

[57] Jason Andrews. *Co-verification of Hardware and Software for ARM SoC Design*. Elsevier, Burlington, MA, 2004.

[58] P K Skowroński, J Barranco, S Bettoni, B Constance, R Corsini, M Divall Csatari, A E Dabrowski, S Doebert, A Dubrovskiy, O Kononenko, M Olvegaard, T Persson, A Rabiller, F Tecker, W Farabolini, R L Lillestol, E Adli, A Palaia, and R Ruber. The CLIC feasibility demonstration in CTF3. (CERN-ATS-2011-177) :3 p, Sep 2011.

[59] F. Tecker. Beam loss experience from CTF3. *Presentation at Machine Protection workshop focused on linear accelerator*, 2012.

[60] E. Christen and K. Bakalar. VHDL-AMS a hardware description language for analog and mixed-signal applications. *Circuits and Systems II : Analog and Digital Signal Processing, IEEE Transactions on*, 46(10) :1263–1272, 1999.

[61] J. Gosling B. Brosgol P. Dibble S. Furr Bollella, G. and M. Turnbull. Real-time specification for java (rtsj). Technical report, Addison-Wesley editor, 2000.

[62] T. henties et al. Java for safety-critical applications. Technical report, Elsevier editor, 2009.

[63] Peter J Ashenden, Gregory D Peterson, and Darrell A Teegarden. *The system designer's guide to* VHDL-AMS *: analog, mixed-signal, and mixed-technology modeling*. The Morgan Kaufmann series in systems on silicon. Morgan Kaufmann, San Francisco Calif, 2002.

[64] Yannick Hervé and Arnaud Legendre. *Functional Virtual Prototyping for Heterogeneous Systems*, pages 223–253. Springer Netherlands, 2012.

[65] L. Barthe, L.V. Cargnini, P. Benoit, and L. Torres. Optimizing an open-source processor for FPGAs : A case study. In *Field Programmable Logic and Applications (*FPL*), 2011 International Conference on*, 2011.

[66] D. Lampret. OpenRISC 1200 IP core specification. Technical report, [Online]. Available : http ://www.opencores.org/, 2001.

[67] Xilinx. Microblaze processor reference guide v11.1. Technical report, [Online]. Available : http ://www.xilinx.com/, 2010.

[68] A. Youssef, Y. Crouzet, A. de Bonneval, J. Arlat, J.-J. Aubert, and P. Brot. Communication integrity in networks for critical control systems. pages 23–34, 2006.

[69] M. Paulitsch, J. Morris, B. Hall, K. Driscoll, E. Latronico, and P. Koopman. Coverage and the use of cyclic redundancy codes in ultra-dependable systems. In *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*, pages 346–355, 2005.

[70] J Serrano, P Alvarez, M Cattin, E Garcia Cota, J Lewis, P Moreira, T Wlostowski, G Gaderer, P Loschmidt, J Dedic, R Bär, T Fleck, M Kreider, C Prados, and S Rauch. The white rabbit project. Technical Report CERN-ATS-2009-096, CERN, Geneva, Nov 2009.

[71] A. Mettas F. Bayle. Temperature acceleration models in reliability predictions : justification and improvement. *Reliability and Maintainability Symposium*, January 2010.

[72] Willian J. Vigrass. Calculation of semiconductor failure rates. *Harris Semiconductor*.

[73] Eugene Hecht and Alfred Zajac. *Optics*. Addison-Wesley, Reading, MA, 1980. Reprint of the 1st ed. (1974).

[74] J Uythoven, E Carlier, L Ducimetière, B Goddard, V Kain, and N Magnin. Beam commissioning and performance characterisation of the LHC beam dump kicker systems. (CERN-ATS-2010-135) :4 p, Jun 2010.

[75] O. Kester. Status of the FAIR facility. *Proceedings of IPAC13, Shanghai, China*, 2013.

[76] Y. Zhang et al. Design integration of the FRIB driver linac. *Proceedings of IPAC13, Shanghai, China*, 2013.

[77] Z.J. Wang et al. Conceptual design of superconducting heavy ion linear injector for HIAF. *Proceedings of Linac12, Tel-Aviv, Israel*, 2012.