ISTITUTO NAZIONALE DI FISICA NUCLEARE

Laboratori Nazionali di Frascati

INFN-19-07/LNF
18 Aprile 2019

Advanced beam protection systems for high-brightness electron-beam and linac-based Compton sources

Stefano Pioli[1]
[1)] *INFN, Laboratori Nazionali di Frascati, I-00044 Frascati, Italy*

Abstract

The Gamma Beam System (GBS), within the ELI-NP project, under installation in Magurele (RO) by INFN, as part of EuroGammas association, can provide gamma rays that open new possibilities for nuclear photonics and nuclear physics. ELI-GBS gamma rays are produced by Compton backscattering to get monochromaticity (0,1 % bandwidth), high flux (10^{13} photon/s), tunable directions and energies up to 19 MeV. Such gamma beam is obtained when a high-intensity laser collides a high-brightness electron beam with a repetition rate of 100 Hz in multi-bunch mode with trains of 32 bunches.
An advanced high reliability and availability Machine Protection System, compliant with IEC-61508 Functional Safety regulation, has been developed in order to ensure proper automated operation for this challenging facility. Such system operates on different layers of the control system: it is equipped with an EPICS supervisor for on-line monitoring of all subsystems, different beam loss monitors to verify electron beam transport and gamma beam luminosity, a real-time interlock system based on distributed FPGA over EtherCAT to monitor vacuum and RF systems which requires fast response within next RF pulse.

Published by
Laboratori Nazionali di Frascati

Contents

Introduction **6**

1 ELI-NP-GBS Light source **10**

1.1 Inverse Compton Scattering 10

1.2 Overview and applications 13

1.3 ELI-NP-GBS project 14

1.4 Description of the ELI-NP Linac 17

2 Functional Safety **24**

Scope 25

Fundamental Concepts 26

Compliance 28

2.1 Hardware and Software Requirements 28

Safety Life Cycle 30

Hardware requirements 30

Software design and development 32

Integration and testing 33

Safety validation planning and verification 33

2.2 Availability of industrial systems 35

Reliability “Bathtub” model 35

The Mean Time Between Failures 37
Redundancy 39
From regulation to Machine Protection System 43

3 Risk Analysis and Requirements 48
3.1 High Power RF system 50
3.2 Low Level RF system 52
3.3 Vacuum system 53
3.4 Magnets 62
3.5 Cooling system 64
3.6 Personnel Safety System 65
3.7 Control system 67
3.8 Synchronization 67
3.9 Electron beam diagnostics 68
3.10 Requirements overview 69

4 System Architecture 72
4.1 MPS Framework 72
SIF Definitions 75
Reliability and Redundancy 77
4.2 MPS layers and interfaces 78
4.3 Logic Matrix 84

5 Software and Hardware Design 94
5.1 Fast-Interlock system design 95
WaveForm mask real-time interlock design 104
5.2 EPICS-based Supervisor design 109
5.3 Beam Loss Monitors 111
Cherenkov Beam Loss Position Monitor 112
Hall Probes 117
Beam Position and Current Monitors 121
IP Trajectory feedback 121
5.4 Vacuum design improvements 124

6 Validation and Verification **128**

6.1 MPS framework Validation 128

Verification of requirements 129

6.2 Validation Planning 136

Conclusions **138**

Bibliography **142**

List of Figures **150**

List of Tables **154**

Introduction

New γ and X ray sources are under development in several laboratories thanks to progress in high power lasers and high brightness accelerators. These sources uses Inverse Compton scattering through the collision between a relativistic high quality electron beam and high power laser pulses to generate secondary photon beams of high performances. New technologies applied on this kind of facilities have a wide range of applications and opens new perspectives in research and industrial fields.

In this framework, a very innovative Compton source is under commissioning in Magurele (RO), by the EuroGammaS Association, with the aim to generate photon beams with energy range between $1-20\,\text{MeV}$, characterized by unprecedented performances in terms of mono-chromaticity, brilliance, spectral density, tunability and polarization. Gamma rays with these performances are of great interest for basic and applied research in the fields of nuclear physics and photonics. The realization of this gamma source called ELI-NP-GBS is one of the three pillars of the European Extreme Light Infrastructure (ELI) project that pursues the creation of an international laser research infrastructure.

Challenging parameters of this gamma source rely on the performances of the high-brightness electron Linac accelerator. The Linac consists of two S-band (2856 MHz) and twelve C-band (5712 MHz) RF structures which mainly allow the tunability and the high quality of the electron beam. The accelerator will be operated at a repetition rate of 100 Hz. For every RF pulse up to 32 electron bunches, each one carrying 250 pC of charge, separated by 16 ns, will be accelerated. The Linac is required to achieve a normalized emittance in both planes better than 0.5 mm·mrad and and energy spread below 0.1 %. In order to guarantee all these performances in the most reliable and stable way, an advanced Machine Protection System (MPS) has been developed.

The aim of this thesis is the study, design and commissioning of MPS and its sub-systems to be in charge of beam protection for a state-of-art gamma source such as the ELI-NP-GBS accelerator.

The beam protection for this facility doesn't require just an interlock concentrator, like others available in many facilities, rather an advanced system fully integrated in the accelerator. This system must be able to protect the accelerator equipment, from damages due to the electron beam, and the electron beam itself. Then, the MPS should be able to provide automated procedures during the commissioning and operation of the facility in order optimize operation, monitor gamma and electron beam performances handling and preventing anomalous behavior of the accelerator.

The MPS framework for the ELI-NP-GBS is made of different sub-systems to achieve different requirements as beam performances, reliability and response time. RF sources and vacuum systems are monitored by an high-reliability and very fast fast-interlock system based on distributed real-time FPGA equipped also with a waveform mask for the real-time monitoring of RF signals from accelerating structures. All other accelerator systems are supervised on-line by a dedicated controller integrated with EPICS control system. Four kind of Beam Loss Monitors (BLM) verify electrons transport and electron and gamma beams performances thanks to Cherenkov fibers to localize electron beam loss, Hall probes to avoid beam dispersion inside bending magnets and a trajectory feedback at each Interaction Point (IP) to lock the gamma beam luminosity.

Each part of the MPS has been designed in compliance with International Electrotechnical Commission functional safety guidelines (IEC 61508) following all the criteria required to ensure the proper long time reliability with a dedicated life cycle and achieving the required safety integrity levels (SIL).

Dissertation overview

The work for this dissertation is described in a total of six Chapters.

In Chapter 1 the basic priciples of the Compton backscattering is introduced with a general overview of the Compton sources and their wide range of applications. In this scenario we also discuss the main parameters of the European ELI-NP-GBS project. Finally the Linac parameters and the layout of the machine are reported.

Chapter 2 focuses on the IEC 61508 regulation. The functional safety regulations are summarized togheter with statiscal tools needed to evaluate properly the reliability for the MPS framework. Finally it is reported the life-cycle which I used to develop the MPS framework in order to reach the fully compliancy with the IEC regulation. Next chapters will follow such life-cycle.

In Chapter 3 I illustrate the risk analysis of the ELI-NP-GBS for each system of the accelerator in order to identify the list of requirements for the MPS framework. I'll present an overview each system highlighting main issues and risk that should be avoided or handled by the MPS.

In Chapter 4 with requirements from the IEC guidelines and accelerator's systems, the architecture of the MPS framwork is presented. I will discribe the technology required to achieve the requested reliability and how to interface the monitored equipment according also with the topology of the facility. At the end of the chapter the logic matrix used in the MPS is reported.

Chapter 5 focuses on the description of hardware and software design of each system of the MPS with expected and measured performances.

In the last Chapter, the last part of the framework development, validation and verification planning methodology is shown. I will demostrate how the MPS framework match with all accelerator's requirements, how it is compliant with IEC 61508 evaluating its reliability, and availability. The list of tests plan for the MPS validation and tests scheduled for the periodic verification will be reported.

In the conclusions, perspectives and future works for all these activities are put in evidence.

CHAPTER

1 ELI-NP-GBS Light source

Content

1.1 Inverse Compton Scattering 10
1.2 Overview and applications 13
1.3 ELI-NP-GBS project 14
1.4 Description of the ELI-NP Linac 17

Recent developments in particle accelerators and lasers technology opened new perspectives for the realization of new X and γ ray sources through electron-photon collision. These sources are based on the inverse Compton scattering effect, in which a high brightness electron beam scatters an intense high power laser beam, converting optical photons ($E_{ph} \sim$ eV) into energetic photons ranging from keV to MeV.

1.1 Inverse Compton Scattering

The physics of the inverse Compton scattering effect has been studied extensively and can be described through two different models [1]: classical model and a linear quantum model. In the former the laser pulse field acts as an electromagnetic undulator. Like in a Free Electron Laser (FEL), the electrons oscillating in this field produce spontaneous emission radiation due to the transverse acceleration. This model considers all the collective effects (multi-photon absorption/emission) explaining the beam/laser pulse interaction within certain limits, but does not conserve energy and momentum. In order to take into account the quantum effects and how they impact on the quality of the produced secondary beam, the linear quantum approach is used. It is based on the relativistic kinematics and allows to predict the final characteristics and performances for a high energy Compton source.

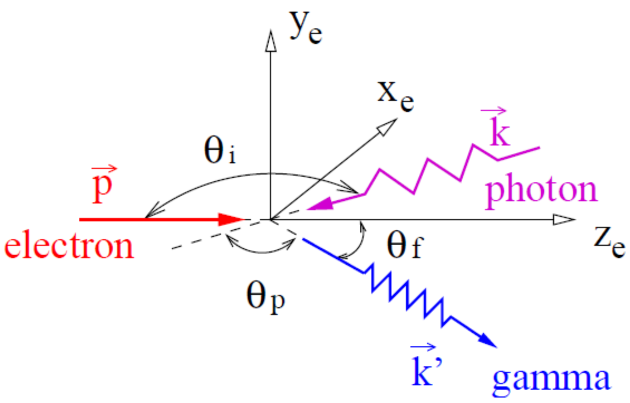

Figure 1.1: Sketch of Compton scattering of an electron and a photon in a laboratory frame coordinate system (x_e, y_e, z_e) in which the electron is incident along the z_e direction. The incident photon is propagating along the direction given by the polar angle θ_i and azimuthal angle ϕ_i. The collision occurs at the origin of the coordinate system. After the scattering, the scattered gamma ray propagates in the direction given by the polar angle θ_f and azimuthal angle ϕ_f. θ_p is the angle between the momenta of incident and scattered photons. The electron after scattering is not shown in the figure.

As reported in [2], in the laboratory frame shown in Figure 1.1 the energy E_γ of the scattered gamma ray, propagating in the direction given by the polar angle θ_f, can be expressed by

$$E_\gamma = \frac{(1-\beta\cos\theta_i)E_p}{1-\beta\cos\theta_f + (1-\cos\theta_p)E_p/E_e} \tag{1.1}$$

where $\beta = v/c$ is the ratio of the incident electron velocity relative to the speed of light, E_e and E_p are the energy of the electron and optical photon before scattering, θ_i is the angle between the momenta of the incident photon and the electron and θ_p is the angle between the momenta of the incident and scattered photons.

In case of head-on collision ($\theta_i = \pi$ and $\theta_p = \pi - \theta_f$) and ultra-relativistic electron ($\gamma \gg 1, \beta \sim 1$), the photon is scattered into a cone with a half-opening angle of $1/\gamma$ along the direction of the incident electron, where $\gamma = E_e/(mc^2)$ is the Lorentz factor of the electron and $E_0 = mc^2$ is its rest energy. For a small scattering angle, ($\theta_f \ll 1$), the equation 1.1 can be simplified to

$$E_\gamma \simeq \frac{4\gamma^2 E_p}{1 + \gamma^2\theta_f^2 + 4\gamma^2 E_p/E_e} \tag{1.2}$$

in which the last term in the denominator accounts for the so called electron recoil effect and it is responsible for the correct energy and momentum conservation in the scattering reaction. This term, that affects the performances of the emitted photon beam, is negligible for X ray Thomson Sources, while it is small but not negligible for higher energy Compton Sources, and becomes the dominant term for deep Compton Sources.

In general is possible to identify three different regimes:

- Thomson elastic regime: negligible electron recoil;
- Quasi-elastic Compton regime: small but not negligible recoil;
- Quantum Compton regime: dominant electron recoil.

As shown by equation 1.2, the photon energy gain factor in the inverse Compton scattering mainly depends on the energy of the colliding electron beam. This beam can be generated by a normal conducting linear accelerator (Linac), a storage ring or a superconducting Linac. Compton sources are easily tunable and their photon beam energies can be extended to cover a wide range from soft X ray to very high energy gamma ray. Due to a high energy gain factor, the Compton sources are considered the most effective ”photon accelerators”, able to produce high power radiation with a required electron beam energy, dimensions and costs significantly lower than those of a synchrotron light source.

Furthermore, secondary photons emitted by inverse Compton scattering present an energy-angle correlation. Hence, by using a collimation system, it is possible to obtain a quasi-monochromatic photon beam, while the forward focusing ensures high spectral densities in small bandwidths. Compared with a Bremsstrahlung beam which is characterized by a broad band spectrum, a Compton beam is narrowly peaked around the desired energy. Another important feature is the preservation of the laser polarization in the scattered photons. Hence, the photon beams produced with this scheme can be highly polarized, and their polarization is controlled by the one of the incident photon beam.

Summarizing the Compton sources are able in producing radiation with high power, short wavelength, quasi-monochromatic spectrum, high directivity, ultrashort time duration and tunability.

1.2 Overview and applications

Compton sources can be seen as electron/photon colliders aimed at producing secondary beams of photons. Unlike normal colliders used for high-energy physics, where collisions are used to study rare physical events, in these machines the emphasis is on the secondary particle beam and his properties.

The idea of using Compton scattering to generate a high-energy X ray or γ ray beam was first proposed in 1963 by Milburn and Arutyunian [3, 4]. The LADON project [5] has been the first facility to produce a monochromatic polarized gamma beam exploiting the collision of a laser with the electrons from the ADONE storage ring [6] in Frascati.

Nowadays several test facilities, that generate γ ray beams by means of Compton scattering are present in different laboratories worldwide [7, 8, 9, 10, 11, 12], together with newly conceived user facilities [13, 14, 2, 15]. This is true both for X-ray sources, which are primarily used for advanced imaging techniques, and for the gamma-ray sources used for research in nuclear physics and industrial purposes. Such a new generation of γ beams allow to probe the matter on microscopic-to-nuclear scales in space and time. They found their natural interest in imaging and nuclear fundamental physics, but their potential application range extends to a large number of fields: medicine, biology, material science, cultural heritage, national security and high energy physics. Photon beams generated by Compton scattering have been successfully used for the implementation of biological computer aided imaging techniques, like for instance phase-contrast tomography at the Munich Compact Light Source [13, 16]. This has been possible thanks to small round source spot size ($\sim 10\mu m$), high spatial ($\sim 80\mu m$) and temporal resolution (ps) and quasi-monochromaticity typical of these sources. Moreover, with respect to the conventional X ray tubes, the absence of low energy tails in the photon spectrum, allows edge enhancement with an overall improvement in the image contour visibility. In particular in the medical field, mammography with mono-chromatic X-rays at 20 keV has been proven far superior in signal to noise ratio with respect to conventional mammographic tubes, with a considerably lower radiation dose to the tissue.

The generation of photons in the gamma range ($E_{ph} > 1$ MeV) is particular interesting for nuclear physics applications, e.g. the Nuclear Resonance Fluorescence technique [17, 18] based on the nuclear absorption and subsequent emission of high-energy photons. This technique provides a versatile method of non-destructive analysis of both radioactive and stable nuclides. Therefore, it finds application for nuclear waste remote sensing and diagnostics, special nuclear material recognition for national security but also in isotope sensitive imaging for medical and cultural heritage purposes. Moreover, several research fields in nuclear physics and astro-physics dealing with fundamental nuclear structure studies such as nucleo-synthesis, clustering phenomena in light nuclei, photo-disintegration cross sections measurements and photo-fission phenomena will be possible by using such advanced gamma sources.

1.3 ELI-NP-GBS project

A new Compton source operating in the gamma energy range (0.2-19.5 MeV) that aims to provide a beam suitable for the applications mentioned in the previous paragraph, is presently under construction in the framework of the Extreme

Light Infrastructure Nuclear Physics Gamma Beam System (ELI-NP-GBS) project.

The ELI-NP-GBS project [19, 20, 21] consists in the realization and commissioning of a gamma ray source that will be hosted in Magurele, near Bucharest (RO). The conceivement and design of this machine has been performed by the EuroGammaS association [22] which gathers academic and research institutions together with commercial companies: Istituto Nazionale di Fisica Nucleare, Università di Roma "La Sapienza", the Centre National de la Recherche Scientifique, ACP S.A.S., Alsyom S.A.S., Comeb Srl and ScandiNova Systems AB. This project has been developed in the framework of the ELI project, born from the collaboration of 13 European countries and aims at the creation of an international laser research infrastructure that will host high-level research on ultra-high intensity laser, laser-matter interaction and secondary light sources. Its scope is to reach pulse peak power and brightness beyond the current state of the art by several orders of magnitude. Because of its unique properties, this multidisciplinary facility will provide new opportunities to study the fundamental processes unfolded during light-matter interaction. ELI will be implemented as a distributed research infrastructure based initially on 3 specialized and complementary facilities (or pillars):

- ELI Beamlines (Prague (CZ)): High Energy Beam Science pillar devoted to the development and usage of dedicated beam lines with ultra short pulses of high energy radiation and particles reaching almost the speed of light.

- ELI Attosecond (Szeged (HU)): Attosecond Laser Science pillar designed to conduct temporal investigation of electron dynamics in atoms, molecules, plasmas and solids at attosecond scale (10^{-18} s).

- ELI-NP (Magurele (RO)): Laser-based Nuclear Physics pillar will generate radiation and particle beams with much high energy and brilliance suited to studies of nuclear and fundamental processes.

At the ELI-NP pillar, the ELI-NP-GBS is foreseen as a major component of the infrastructure, aiming at producing extreme gamma ray beams for nuclear physics and photonics experiments characterized by unprecedented performances in terms of monochromaticity, brilliance, spectral density, tunability and polarization.

The ELI-NP source [21, 23] is a machine based on the collision of an intense high power Yb:Yag J-class laser and an high brightness electron beam with a tunable energy produced by a normal conducting Linac. Referring to equation 1.1 this source operates at the transition between the classical and the quantum regimes, since the required bandwidth is very narrow the quantum effects cannot be neglected. The main specifications of the Compton Source are: photon energy tunable between 0.2 and 19.5 MeV, rms relative bandwidth lower than 0.5% and spectral density larger than $5 \cdot 10^3$ photons/s·eV, with source spot size smaller than 100 μm and linear polarization of the gamma-ray beam larger than 95%. Moreover, the peak brilliance of the gamma beam is expected to be larger than 10^{19} photons/(s·mm^2 $\cdot$ mrad^2 $\cdot$ 0.1$\%$). To reach these challenging specifications, the luminosity $\mathscr{L}$ of the source must be larger than 10^{35} s$^{-1}\cdot$ cm^{-2}, as specified by equation

$$\mathscr{L} = \frac{N_e N_p r}{4\pi\sigma_0^2} \tag{1.3}$$

where N_p are the photons carried by the laser pulse at the collision, N_e the electrons carried in the bunch, σ_0 the spot size at the Interaction Point (IP) and r the repetition rate of the collisions (assuming ideal overlap in space and time of the two colliding pulses, as well as negligible diffraction of the two beams over the interaction distance). The total number of photons scattered per second, all over the spectrum and solid angle, is given by the luminosity multiplied by the total cross section $N = \mathscr{L} \cdot \theta_{tot}$, in our case $N = 7 \cdot 10^{10}$ photons/s. Any Compton source generates polychromatic beam. Hence, in order to produce a monochromatic photon beam it is necessary to select a narrow cone around the electron beam propagation axis by means of special collimators. Therefore, what really matters for experiments and applications is the number of photons carried by the radiation pulse within such a small angle N^{bw}, and their associated rms bandwidth $\Delta\nu_p$. This is the definition of spectral density, which is the figure of merit interesting for nuclear physics and photonics applications. The Spectral Density, defined as

$$SD = \frac{N^{bw}r}{\sqrt{2\pi}\Delta\nu_p} \tag{1.4}$$

is typically expressed in units of photons/$s \cdot eV$. Various generations of machines have improved this parameter, from values of the order of 1 for bremsstrahlung sources, to about 10^2 for the present HiγS facility [2], towards the 10^4 range which is the goal of ELI-NP-GBS. Since the laser pulse carries about 10^{18} photons at the IP, but only a maximum of 10^7 photons are scattered at each collision (in other words the electron beam is almost transparent to the laser pulse), the laser pulse can be "re-used" bringing it back to a new collision at the same IP with a new incoming electron bunch. To recirculate the laser pulse an advanced and innovative laser re-circulator has been developed and it is presently under test. A full description of this new optical device can be found in [24, 25].

To achieve this outstanding performance the laser pulse needs to be recirculated 32 times at the interaction point and consequently the Linac will accelerate 32 electron bunches (separated by 16 ns) within the same RF bucket, with a repetition rate of 100 Hz. The final parameters of the gamma beam of ELI-NP GBS are summarized in table 1.1 and the layout of the entire building is shown in Figure 1.2.

1.4 Description of the ELI-NP Linac

In order to reach these challenging performances that are at least two orders of magnitude higher than the present state of the art (in terms of gamma beam bandwidth, brilliance and spectral density) innovative and advanced components have been developed specifically for this machine. In particular, to accelerate the multi-bunch electron beam, the ELI-NP-GBS adopts an S-band (2856 MHz) photo-injector coupled to a C-band (5712 MHz) radiofrequency (RF) Linac capable to bring the electron beam up to an energy of 740 MeV with outstanding

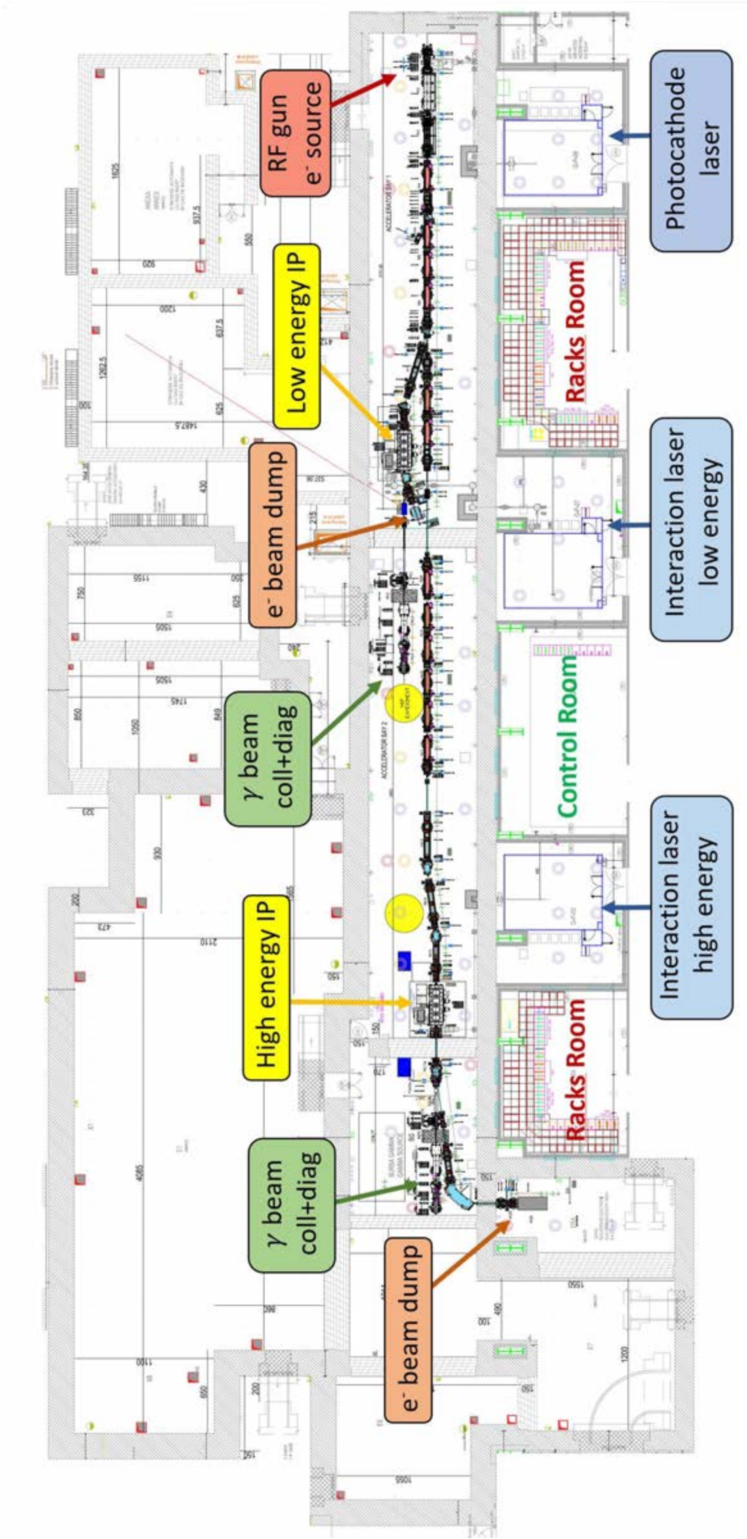

Figure 1.2: ELI-NP-GBS layout.

Parameter	Value
Energy [MeV]	$0.2 - 19.5$
Spectral density $[ph/s \cdot eV]$	$0.8 - 4 \cdot 10^4$
Bandwidth rms [%]	≤ 0.5
# photons/pulse within FWHM bdw	$\leq 2.6 \cdot 10^5$
# photons/s within FWHM bdw	$\leq 8.3 \cdot 10^8$
Source rms size $[\mu m]$	$10 - 30$
Source rms divergence $[\mu rad]$	$25 - 200$
Peak brilliance $[N_{ph}/s \cdot mm^2 \cdot mmrad^2 \cdot 0.1\%]$	$10^{20} - 10^{23}$
Radiation pulse length rms [ps]	$0.7 - 1.5$
Linear polarization [%]	> 99

Table 1.1: Main parameters of the ELI-NP-GBS Gamma beam.

beam quality [26]: normalized rms emittance in both planes below 0.5 mm $\cdot$ mrad and energy spread below 0.1%. In table 1.2 are summarized the main required parameters of the electron beam. As already mentioned, to increase as much as possible the number of collision per second, the Linac will work at 100 Hz repetition rate and in multi-bunch scheme. These requirements have direct impact on the design of accelerator's systems like the accelerating structures, the overall RF system and any vacuum region. To realize a reliable and compact machine a hybrid S/C-band scheme has been chosen. The combination of C-band acceleration with an S-band injector allows to obtain good performance in terms of beam quality [27]. The injector is derived from the one of SPARC_LAB Linac [28, 29] at INFN Frascati laboratories and is composed by one 1.6 cell RF gun with copper photo-cathode and emittance compensation solenoid, followed by two SLAC-type 3 m long Travelling Wave (TW) sections. The picture of the ELI-NP-GBS injector assembled at INFN-LNF is given in Figure 1.3. To compensate space charge effect in the gun region and to reduce the bunch length, the velocity bunching technique [30] is applied in the first accelerating section placed after the gun. This technique consists in injecting a non-relativistic beam in an RF structure with a phase near the zero crossing of the acceleration field. In this way the beam slips back up to the acceleration phase undergoing a quarter of synchrotron oscillation and is chirped and compressed. In the ELI case,

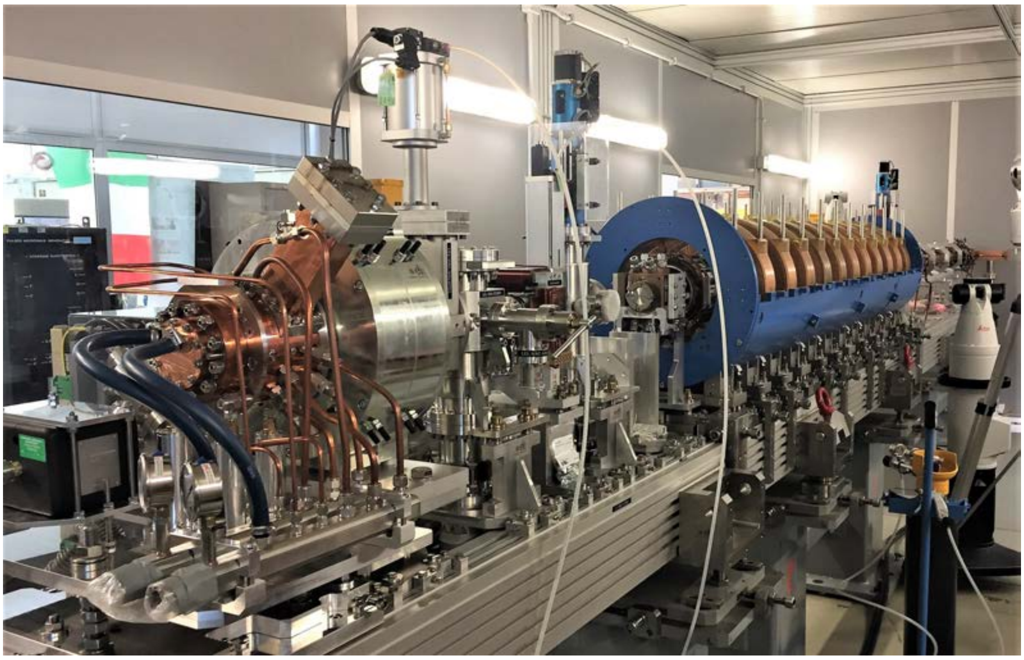

Figure 1.3: Picture of the assembled ELI-NP-GBS S-band injector.

a “gentle” velocity bunching (compression factor < 3) in the first accelerating section allows injecting into the C-band booster a beam that is short enough to reduce the final energy spread, avoiding also emittance degradation. In the first accelerating section, the transverse emittance dilution is controlled by using a solenoid embedding the RF compressor. The C-band booster comprises twelve TW C-band room temperature accelerating structures, downstream of the S-band photo-injector.

Two beamlines are planned to deliver the electron beam at the two Compton IPs: one at low energy ($E_{e^-} = 75 - 312$ MeV) and one at high energy (E$_{e^-}$ up to 740 MeV). Downstream the injector and the first four C-band structures, a dogleg with two dipoles provide an off axis deviation towards the low energy interaction point. At the end of the Linac a second dogleg drives the beam to the high energy Compton IP. After each interaction point the electron beam is driven through dipoles towards the low and high energy dump, while the Compton radiation proceeds in straight direction towards the collimator and the γ ray diagnostics (Compton spectrometer, calorimeter etc.) in the experimental rooms. The lattice design of the Linac takes into account a diagnostic section after the first C-band structure. This will perform the 6-D phase space characterization at the exit of the photoinjector, by means of an RF deflector combined with an adjacent spectrometer using the quadrupole scan technique. Another diagnostic station with RF deflector is foreseen after the first dogleg. In Figure 1.4 a detailed schematic of the Linac is shown, reporting also the position of all the quadrupoles, dipoles, beam position monitors and steerers along the machine. The overall accelerator has been divided in 36 modules that have been pre-assembled and tested, in order to reduce the time needed to install the machine on site. The total length of the accelerator is about 90 m.

Parameter	Value
Energy [MeV]	$75 - 740$
Bunch charge [pC]	$25 - 400$
# bunch per pulse	32
Bunch distance [ns]	16
Bunch length [μm]	$100 - 400$
Energy spread (rms) [$\%$]	0.04 - 0.1
Normalized emittance [$mm \cdot mrad$]	0.4
RF pulse repetition rate [Hz]	100

Table 1.2: Electron beam parameters of the ELI-NP-GBS Linac.

Parameter	Value
Pulse energy [J]	$0.2 - 0.4$
Wavelength [nm]	515
Photon energy [eV]	2.4
Pulse length [ps] rms	1.5
Focal spot size w_0 [μm]	28
Laser M^2	< 1.2
rms bandwidth	< 0.1
Laser parameter a_0	0.02 - 0.04
Collision angle α [°]	172
Repetition rate [Hz]	100
Recirculator rate per laser pulse	32

Table 1.3: Laser pulse main parameters of the ELI-NP-GBS.

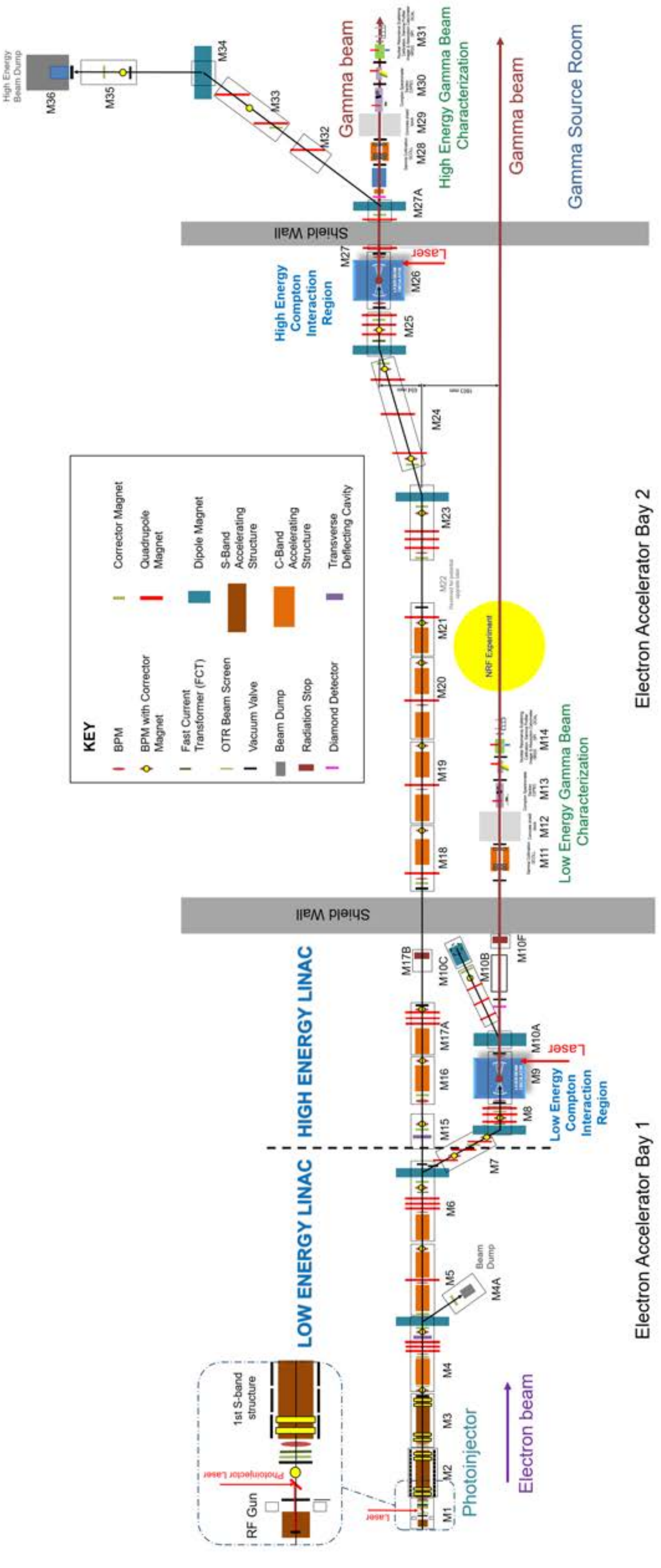

Figure 1.4: ELI-NP-GBS Linac layout.

CHAPTER

2 Functional Safety

Content

Scope . . . 25

Fundamental Concepts . . . 26

Compliance . . . 28

2.1 Hardware and Software Requirements . . . 28

Safety Life Cycle . . . 30

Hardware requirements . . . 30

Software design and development . . . 32

Integration and testing . . . 33

Safety validation planning and verification . . . 33

2.2 Availability of industrial systems . . . 35

Reliability “Bathtub” model . . . 35

The Mean Time Between Failures . . . 37

Redundancy . . . 39

From regulation to Machine Protection System . . . 43

In order to develop a proper MPS design, the first step is to understand what is mandatory or suggested for accelerator systems by law and/or international industrial standards. In this chapter I'll present the functional safety standard developed by International Electrotechnical Commission named IEC 61508. I'll highlight how to design the MPS project and how to benchmark it through statistical tools.

IEC 61508 [31] is an international standard for the "functional safety" of electrical, electronic, and programmable electronic (E/E/PE) equipment. This standard started in the mid 1980s when the International Electrotechnical Committee Advisory Committee of Safety (IEC ACOS) set up a task force to consider standardization issues raised by the use of programmable electronic systems. At that time, many regulatory bodies forbade the use of any software-based equipment in safety critical applications.

Although the standard was initially criticized for its "extensive" documentation requirements and use of unproven "statistical" techniques for hardware failures, it represents a great step forward for the safety of industries procedures. The standard focuses its attention on risk-based safety-related system design, which should result in far more cost-effective implementation. The standard also requires the attention to detail that is vital to any safe system design. Because of these features and the large degree of international acceptance for a single set of documents, the standard is considered to be a major advance for the technical world.

Scope

The 61508 standard covers safety-related systems when one or more of such systems incorporates mechanical/electrical/electronic/programmable electronic devices. These devices can be of different types from ball valves, solenoid valves, electrical relays and switches through to complex Programmable Logic Controllers (PLCs). The standard specifically covers possible hazards created when failures of the *safety functions* performed by E/E/PE safety-related systems occur. The overall program to insure that the safety-related E/E/PE system brings about a safe state when called upon to do so is defined as "functional safety."

IEC 61508 does not cover safety issues like electric shock, hazardous falls, long-term exposure to a toxic substance, etc.; these issues are covered by other standards. IEC 61508 also does not cover low safety E/E/PE systems where a single E/E/PE system is capable of providing the necessary risk reduction and the required safety integrity of the E/E/PE system is less than *Safety Integrity Level* 1, i.e., the E/E/PE system is only available 90% of the time or less.

IEC 61508 is concerned with the E/E/PE safety-related systems whose failure could affect the safety of persons and/or the environment. However, it is recognized that the methods of IEC 61508 may apply to business loss and asset protection as well. Human beings may be considered part of a safety-related system, although specific human factor requirements are not considered in detail in the standard. The standard also specifically avoids the concept of "fail safe" because of the high level of complexity involved with the considered E/E/PE systems.

Fundamental Concepts

The standard is based on two fundamental concepts: the *safety life-cycle* and *Safety Integrity Levels*. The *safety life-cycle* is defined as an engineering process that includes all of the steps necessary to achieve required functional safety.

The basic philosophy behind the *safety life-cycle* is to develop and document a safety plan, execute that plan, document its execution (to show that the plan has been met) and continue to follow that safety plan through to decommissioning with further appropriate documentation throughout the life of the system. Changes along the way must follow similarly the pattern of planning, execution, validation, and documentation.

The *safety life-cycle* can be viewed as a logical "identify-assess-design-verify" closed loop. The intended result is the optimum design where the risk reduction provided by the safety-related system matches the risk reduction needed by the process. The first part of the *safety life-cycle*, known as the analysis portion, covers:

- Concept and scope of the system or equipment under control;

- Hazard and Risk Analysis to identify both hazards and the events that can lead to them;
- Creation of overall safety requirements and identification of specific *safety functions* to prevent the identified hazards;
- Safety requirements allocation, i.e., assigning the *safety function* to an E/E/PE safety-related system, an external risk reduction facility, or a safety-related system of different technology.

This also includes assigning a safety integrity level (SIL) or risk reduction factor required for each *safety function*. *Safety Integrity Levels* are order of magnitude levels of risk reduction. There are four SILs defined in IEC 61508. SIL-1 has the lowest level of risk reduction. SIL-4 has the highest level of risk reduction. The SIL table for "demand mode" and continuos mode is shown in Table 2.1.

Safety Integrity Level	On Demand mode	Continuos mode
SIL-1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
SIL-2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
SIL-3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
SIL-4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

Table 2.1: Safety Integrety Levels definitions as probability of failure for both on demand mode and continuos mode.

The mode differences are:

- Low demand mode: where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency;
- High demand or continuous mode: where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.

Note that the proof test frequency refers to how often the safety system is completely tested and insured to be fully operational. While the continuous mode appears to be far more stringent than the demand mode, it should be remembered that the units for the continuous mode are per hour. The demand mode units assume a time interval of roughly one year per the definition. Considering the fact that there are about 10000 hours in a year, the modes are approximately the same in terms of safety metrics.

Basically speaking, functional safety is achieved by properly designing a Safety Instrumented System to carry out a *Safety Instrumented Function (SIF)* at a reliability indicated by the *Safety Integrity Level (SIL)*.

Compliance

The IEC 61508 standard states: "To conform to this standard it shall be demonstrated that the requirements have been satisfied to the required criteria specified (for example *Safety Integrity Level*) and therefore all the objectives have been met."

In practice, demonstration of compliance often involves listing all of the IEC 61508 requirements with an explanation of how each requirement has been met. This applies to both products developed to meet IEC 61508 and specific application projects wishing to claim compliance.

Because IEC 61508 is technically only a standard and not a law, compliance is not always legally required. However, in many instances, compliance is identified as best practice and thus can be cited in liability cases. Also, many countries have incorporated IEC 61508 or large parts of the standard directly into their safety codes, so in those instances it indeed has the force of law. Finally, many industry and government contracts for safety equipment, systems, and services specifically require compliance with IEC 61508. So although IEC 61508 originated as a standard, its wide acceptance has led to legally required compliance in many cases.

2.1 Hardware and Software Requirements

IEC 61508 Part 2 and 3 covers specific requirements for safety-related hardware and software. As in other parts of the standard, a *safety life-cycle* is to be used as the basis of requirement compliance.

The hardware and software *safety life-cycle* is an expanded plan of the overall *safety life-cycle* that is focused on the design of the control hardware and softwtare for safety systems. As for the overall *safety life-cycle*, there are requirements for a functional *safety management plan* and safety requirements specification, including all verification and assessment activities.

A functional *safety management plan* (either as a part of other documentation or as a separate document) shall define the strategy for the software procurement, development, integration, verification, validation, and modification as required for the SIL level of the hardware. The plan must specify a configuration management system.

This functional *safety management plan* must:

- manage software changes to ensure that the specified requirements for software safety are satisfied;
- guarantee that all necessary activities have been carried out to demonstrate that the required software safety integrity has been achieved;
- accurately maintain all documentation and source code including the safety analysis and requirements;
- prevent unauthorized modifications;
- document modification/change requests;
- analyze the impact of a proposed modification;
- approve or reject the modification request;
- establish baseline software and document the (partial) integration testing that justifies the baseline;
- formally document the release of safety-related software.

Master copies of the software and all documentation should be maintained throughout the operational lifetime of the released software.

Safety Life Cycle

Part 2 and 3 requires that a process (such as the *safety life-cycle*) for the development of functional safety system shall be selected and specified during safety planning. Note that the exact process is not specified, it may be customized according to company preference. Appropriate quality and safety assurance procedures must be included. Each step of the software *safety life-cycle* must be divided into elementary activities with the functions, inputs, and outputs specified for each phase.

The standard has complete details of an example *safety life-cycle*. Many practitioners use a version of the V-model.

The standard says, "If at any stage of the *safety life-cycle*, a change is required pertaining to an earlier *life-cycle* phase, then that earlier *safety life-cycle* phase and the following phases shall be repeated".

Hardware requirements

The safety requirements specification shall include details on both the safety function and the *Safety Integrity Level* of that function. Some of these *safety function* details are:

- how safe state is achieved;
- response time;
- operating modes of equipment under control;
- required E/E/PES behavior modes;
- start-up requirements.

Some of the *Safety Integrity Level* details are:

- SIL for each function;
- high or low demand class for each function;
- environmental extremes.

One particular aspect of the hardware design and development requirements is the limit on the *Safety Integrity Level* achievable by any particular level of fault tolerant safety redundancy.

The required SIL for each function could be estimated with risk table (frequencies vs damages) shown in Table 2.2. Damages rows describe the severity of the issue if the system fail. The column is related to the frequency of the fault.

The functional safety requirements for software must be specified. This can be done in a separate document or as part of another document. The specification of the requirements for software safety shall be derived from the specified safety requirements of the safety-related system and any requirements of safety planning.

The requirements for software safety shall be sufficiently detailed to allow design and implementation and to allow a functional safety assessment. The software developers should review the document to verify that it contains sufficient detail. It should be noted that this is often another iterative process.

The requirements must be clear, precise, verifiable, testable, maintainable, and feasible. The requirements must also be appropriate for the *Safety Integrity Level.* and traceable back to the specification of the safety requirements of the safety-related system. Terminology must be clear and understandable by those using the document. All modes of operation for the safety-related system must be listed. The requirements must detail any relevant constraints between the hardware and the software.

Since the software is often called upon to perform much of the online diagnostics, the requirements must detail all software self-monitoring, any diagnostic tests performed on the hardware, periodic testing of critical functions, and means for online testing of *safety functions*. If the software also performs *non-safety function*, means to insure that the software safety is not compromised (non-interfering) must also be specified.

	Extremely unlikely (less then $10^{-3}\, per\ year^{-1}$)	**Remote possibility** (up to $10^{-2}\, per\ year^{-1}$)	**Possible occur** (up to $10^{-1}\, per\ year^{-1}$)	**Will probably occur** (up to $1\, per\ year^{-1}$)	**Almost certain** (more then $1\, per\ year^{-1}$)
Insignificant damage (non-relevant damages, no healthy issue)					
Non-reportable injury (some damages, first assistance required)					SIL-1
Reportable injury (several damages, serius health problems)			SIL-1	SIL-1	SIL-2
Major injury (lot of damages, at least one death)			SIL-1	SIL-2	SIL-3
Major injury (lot of damages, at least one death)			SIL-1	SIL-2	SIL-3
Catastrophic injury (complete loss of production, several death)	SIL-1	SIL-1	SIL-2	SIL-3	SIL-3

Table 2.2: Risk matrix for the SIL evalutation. Thanks to this scheme is possible define the required SIL for a SIF. Columns show the likehood of the hazard happening while rows list the severity of the potential injury. The indicated SIL is the minimum required for the combination of frequencies vs damages. If the SIL is not expressed means that the combination require a SIL lower then SIL-1 then such SIF doesn't require to follow the IEC 61508.

Software design and development

Design methods shall be chosen that support abstraction, modularity, information hiding, and other good software engineering practices. The design method shall allow clear and unambiguous expression of functionality, data flow, sequencing, and time-dependent data, timing constraints, concurrency, data structures, design assumptions, and their dependencies.

During design, the overall complexity of the design, its testability, and the ability to make safe modifications shall be considered. The entire design is considered safety-related even if non *safety functions* are included unless sufficient independence between safety and non-safety can be demonstrated. If different *Safety Integrity Levels* are part of the design, the overall design is only valid for the least stringent SIL of the component parts.

The design must include software functions to execute proof tests and all online diagnostic tests as specified in the requirements. Software diagnostics shall include monitoring of control flow and data flow.

It is assumed and permitted that iteration occurs between the design and the requirements phases. Any resulting changes in requirements must be documented and approved.

Integration and testing

Tests of the integration between the hardware and software are created during the design and development phases and specify the following:

1. test cases and test data in manageable integration sets;
2. test environment, tools, and configuration;
3. test criteria;
4. procedures for corrective action on failure of test.

Safety validation planning and verification

A plan must be set up to demonstrate that the software satisfies the safety requirements set out in the specification. A combination of analysis and testing techniques is allowed and the chosen techniques must be specified in the plan.

The plan must show how assessment will be done, who will review the plan, and the assessor's level of independence.

Software validation is done as an overall check to insure that the software design meets the software safety requirements and must include the appropriate documentation. The validation may be done as part of overall system validation or it may be done separately for the software.

If discrepancies occur, a change request must be created and an analysis must be done to determine if the validation may continue.

The software verification process tests and evaluates the results of the software *safety life-cycle* phases to insure they are correct and consistent with the input information to those phases.

Verification of the steps used in the *safety life-cycle* must be performed according to the plan and must be done concurrently with design and development. The verification plan must indicate the activities performed and the items to be verified (documents, reviews, etc.). A verification report must include an explanation of all activities and results. Verification must be performed on:

- software safety requirements;
- hardware safety requirements;
- software architecture design;
- software system design;
- software module design;
- software source code;
- data;
- software module testing;
- software integration testing;
- hardware integration testing;
- software safety requirements testing (software validation).

2.2 Availability of industrial systems

In order to evaluate the SIL and handle verification and maintenance of the *safety life-cycle* it is important introduce some concept like availability, reliability and Mean Time Between Failures.

Accelerators are required to be highly reliable and the beam is required to be available at scheduled times. Usually the availability should be over the 95%. In order to reach this result is important follow some aspects like: design, self-diagnostics, maintenance, test, spare parts and training. Methods for assessing reliability have been developed in and for industry and are well suited to assess reliability and lifetime of mass-produced units. Basis of modeling are idealizing assumptions: such as that failures interpreted as statistical events.

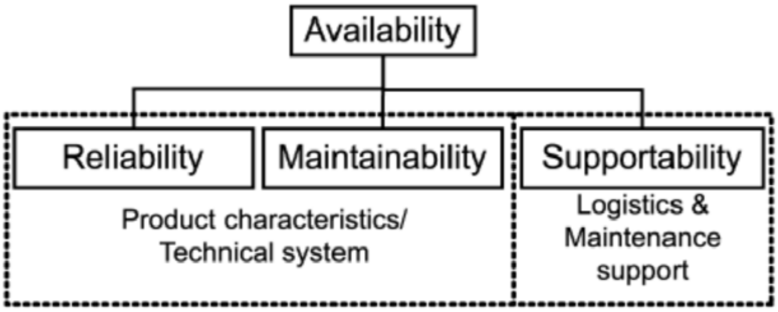

Figure 2.1: Functional dependencies of availability with reliability, Maintainability and Supportability.

Reliability "Bathtub" model

The life of a population of units can be divided into three distinct periods. Figure 2.2 shows the "bathtub curve" which models the cradle to grave instantaneous failure rates vs. time. If we follow the slope from the start to where it begins to flatten out this can be considered the first period. The first period is characterized by a decreasing failure rate. It is what occurs during the early life of a population of units. The weaker units die off leaving a population that is more rigorous. This first period is also called infant mortality period. The next period is the flat portion of the graph. It is called the normal life. Failures occur more in a random sequence during this time. It is difficult to predict which failure mode will manifest, but the rate of failures is predictable. Notice the constant slope. The third period begins at the point where the slope begins to increase and extends to the end of the graph. This is what happens when units become old and begin to fail at an increasing rate.

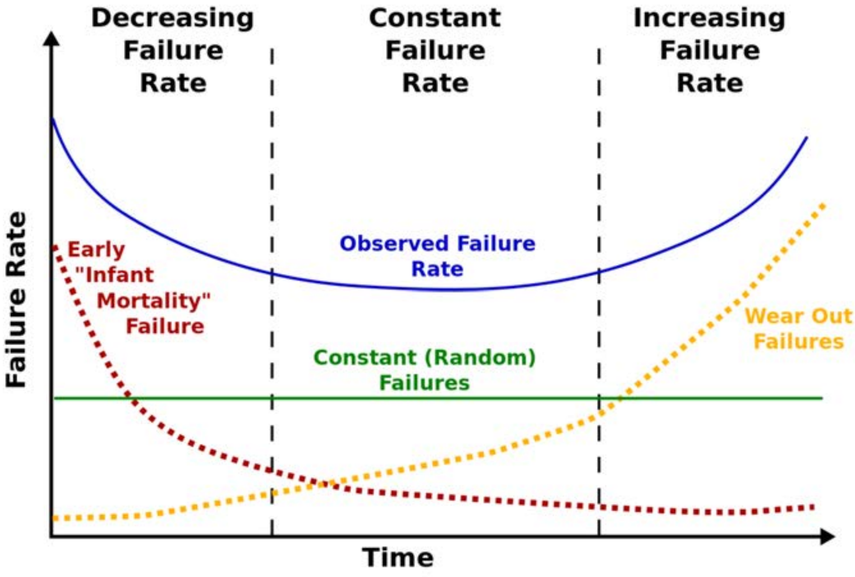

Figure 2.2: The “bathtub curve” is a curve of failure rate function of time. The “bathtub” shape in blue comes from contribution of the exponential trends of erly mortability (in red), the constant presence of random failures (in green) and the exponential trends of equipment wear out (in yellow).

Weibull Analysis [32] can be used as a method of determining where a population of modules is on the bathtub curve. The Weibull distribution is a 3-parameter distribution. The three parameters that make up the Weibull distribution are slope β, scale parameter η and time. According with the Weibull model we can define the density function as 2.1 then the reliability function as 2.2 and the failure rate as 2.3.

$$f(t) = \frac{\beta}{\eta} \cdot \left(\frac{t}{\eta}\right)^{\beta-1} \cdot e^{-(\frac{t}{\eta})^{\beta}} \tag{2.1}$$

$$R(t) = 1 - F(t) = 1 - \int_0^t f(\tau)d\tau = \exp\left(-\frac{t}{\eta}\right) \tag{2.2}$$

$$h(t) = \frac{\beta}{\eta} \cdot \left(\frac{t}{\eta}\right)^{\beta-1} \tag{2.3}$$

When $\beta < 1$, the Weibull distribution models early failures of parts. When $\beta = 1$, the Weibull distribution models the exponential distribution. The exponential distribution is the model for the useful life period, signifying that random failures are occurring. When $\beta = 3$, the Weibull distribution models the normal distribution. This is the early wear out time. When $\beta = 10$, rapid wear out is occurring.

The Mean Time Between Failures

In the industrial field each device is provided by the manufacture with a MTBF (Mean Time Between Failures) [33] for repairable product or a MTTF (Mean Time To Failure) for non-repairable product. The MTBF is the total uptime (in hours) divided by the number of failure or in percent failed per million hours.

The early mortability is due to manufacturing, shipping, storage, etc. of the equipment then this phase of the model could be ignored with a proper testing of the hardware during the initial phase of development of the project. The Wear Out could be complitely avoided scheduling the replacement of the hardware according with the reliability of the whole system. For these reasons the MTBF take in account random chance of failure during the Useful life phase. MTBF should not be used to calculate how long the system should last (when the system will enter Wear Out), rather its sole purpose is to calculate the probability of success (reliability) and the probability of being ready to do its job (availability) during Useful Life. Reliability $R(t)$ is defined as the probability that a device or a system will function as expected for a given duration in an environment. Thus from this point to evaluate parameters in Useful life, following equations will assume the β equal to 1 then the failure rate 2.3 constant.

The reliability of a system, following the Weibull model, could be related to the MTBF as 2.4 [34] which relate it with the scale parameter η from formula 2.1. Then from equation 2.5 and 2.6 is possible estimate the MTBF from reliability or failure rate and viceversa.

$$MTBF = \int_0^\infty R(t)dt = \int_0^\infty \exp\left(-\frac{t}{\eta}\right) dt = \eta \tag{2.4}$$

$$R(t) = \exp\left(-\frac{t}{MTBF}\right) \tag{2.5}$$

$$h(t) = \frac{1}{MTBF} \tag{2.6}$$

The availability of a system is defined as the ratio between uptime and scheduled uptime then is also possible define this parameter from the MTBF and the MTTR (Mean Time To Repair defined as the total downtime in hours divided by the number of failure). The availability could be evalueted as:

$$Availability = 1 - \frac{MTTR}{MTBF + MTTR} \tag{2.7}$$

Often is not possible evaluate directly the MTBF of a system because it is made of several different sub-system and/or devices. The same issue affect also the evaluation of availability and reliability. In order to compute the MTBF of the whole system is mandatory know at least one parameter between MTBF, availability and realiability of each element part of the system and know also the dependencies between such sub-system and/or devices.

Dependencies should be treated as series or parallel connections [35]. When two or more chained device depends by functionality of another device this is assumed as connected in series. When two or more device work independently this is assumed as connected in parallel.

Assuming as $p_j(t)$ the probability of working properly of the $j-th$ system at the fixed time and $m_j(t) = 1-p_j(t)$ the probability of failure of the $j-th$ system at the fixed time, the probability of working properly for the whole system P_s comes for devices running in series according with formula 2.8 and running in parallel with the formula 2.9.

$$P_s = \prod_{j=1}^{n} p_j = 1 - M_s \tag{2.8}$$

$$M_s = \prod_{j=1}^{n} m_j \tag{2.9}$$

When P_s is computed such probability describe the reliability of the whole system then it is possible convert this value to the MTBF of the whole system from formula 2.7. When this last step is done is possible evaluate the SIL of the system.

Redundancy

Redundancy is a common approach to improve the reliability and availability of a system. Adding redundancy increases the cost and complexity of a system design and with the high reliability of modern electrical and mechanical components, many applications do not need redundancy in order to be successful. However, if the cost of failure is high enough, redundancy may be an attractive option to reach functional safety parameters as the *Safety Integrity Level*.

Models of Redundancy

While there are various methods, techniques, and terminologies for implementing redundancy, the following models represent the more common ones used in industry. The three main models described are called “Standby Redundancy”, “N Modular Redundancy”, and “1:N Redundancy”.

- **Standby Redundancy** - is when you have an identical secondary unit to backup the primary unit. The secondary unit typically does not monitor the system, but is there just as a spare. The standby unit is not usually kept in sync with the primary unit, so it must reconcile its input and output signals on takeover of the monitored device. Is also needed a watchdog, which monitors the system to decide when a switchover condition is met and command the system to switch control to the standby unit, and a voter, which is the component that decides when to switch over and which unit is given control of the device. The system cost increase for this type of redundancy is usually about 2 times. In Standby redundancy there are two basic types, “Cold Standby” and “Hot Standby” as in Figure 2.3 and 2.4.

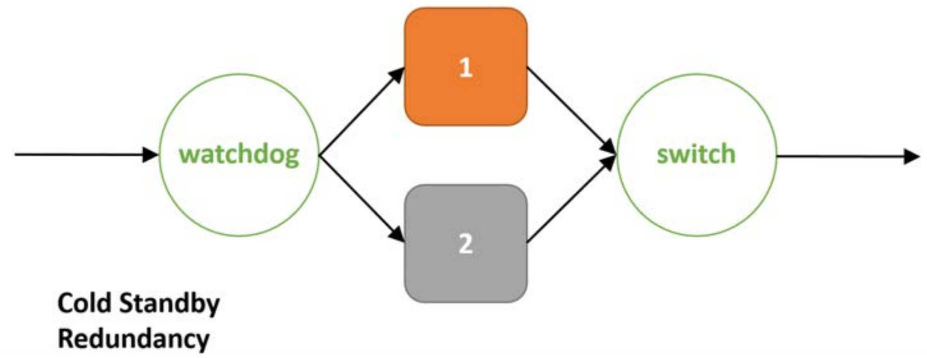

Figure 2.3: Standby Redundancy. Cold Standby model - in orange the active unit, in grey the auxilliary one.

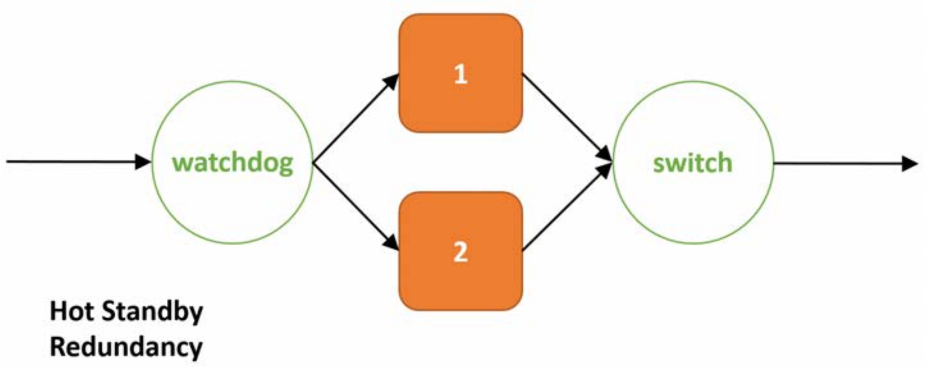

Figure 2.4: Standby Redundancy. Hot Standby model - in orange active units.

- **Cold Standby** - the secondary unit is powered off, thus preserving the reliability of the unit. The drawback of this design is that you have to power up the standby unit and bring it online into a known state. This makes it more challenging to reconcile synchronization issues.
- **Hot Standby** - the secondary unit is powered up and can optionally monitor the device. If you use the secondary unit as the watchdog

and/or voter to decide when to switch over, you can eliminate the need for a third party to this job. This design does not preserve the reliability of the standby unit as well as the cold standby design. However, it shortens the downtime, which in turn increases the availability of the system.

- **N Modular Redundancy** - refers to the approach of having multiply units running in parallel, Figure 2.5. All units are highly synchronized and receive the same input information at the same time. Their output values are then compared and a voter decides which output values should be used. This model easily provides bumpless switchovers. This model typically has faster switchover times than Hot Standby models, thus the system availability is very high, but because all the units are powered up and actively engaged with the monitored device. If you have more than two units, is important define the tecnique used by the voter to choose which one you are going to trust. In N Modular Redundancy, there are three main typologies: Dual Modular Redundancy, Triple Modular Redundancy and Quadruple Redundancy.

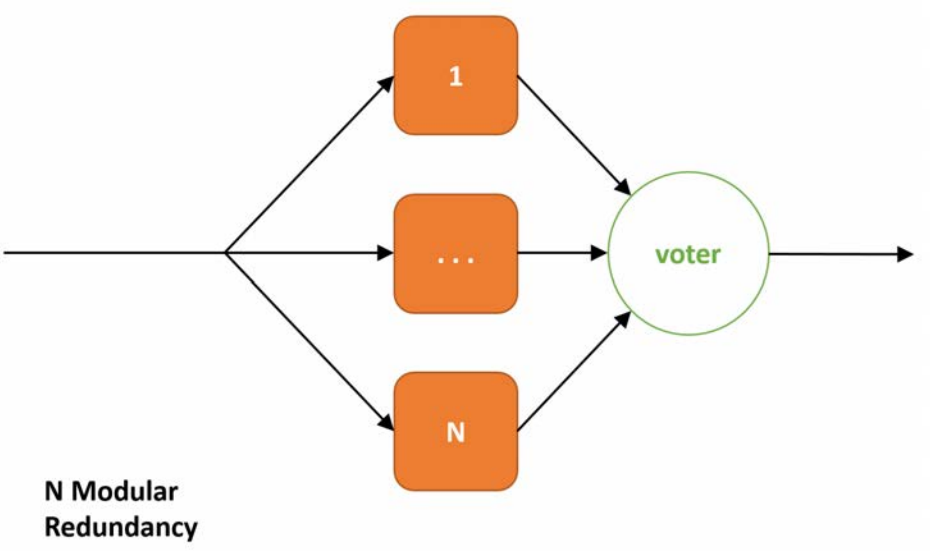

Figure 2.5: N Modular Redundancy - in orange active units.

  - **Dual Modular Redundancy** - uses two functional equivalent units, thus either can control the monitored device. The most challenging aspect of this schema is determining when to switch over to the secondary unit. Because both units are monitoring the application, you have to decide what to do if they disagree. The average cost increase of this kind of redundancy is about twice that of a non-redundant system, due to the cost of the additional hardware and the extra software development time.

  - **Triple Modular Redundancy** - uses three functionally equivalent units to provide redundant backup. This approach is very common in aerospace applications where the cost of failure is extremely high. This kind of redundancy is more reliable than previous one and make simpler the voter that can follow the majority but the drawback of this approach is cost that increase at least of 3 times.

  - **Quadruple Modular Redundancy** - is fundamentally scaled from previuos models four units to increase the reliability. This approach is common in army applications. The obvious drawback is the increase in system cost of 4 times.

- **1:N Redundancy** - is a design technique, as Figure 2.6, used where you have a single backup for multiple systems and this backup is able to function in the place of any single one of the active systems. This technique offers redundancy at a much lower cost than the other models by using one standby unit for several primary units. This approach only works well when the primary units all have very similar functions, thus allowing the standby to back up any of the primary units if one of them fails. Other drawbacks of this approach are the added complexity of deciding when to switch and of a switch matrix that can reroute the signals correctly and efficiently.

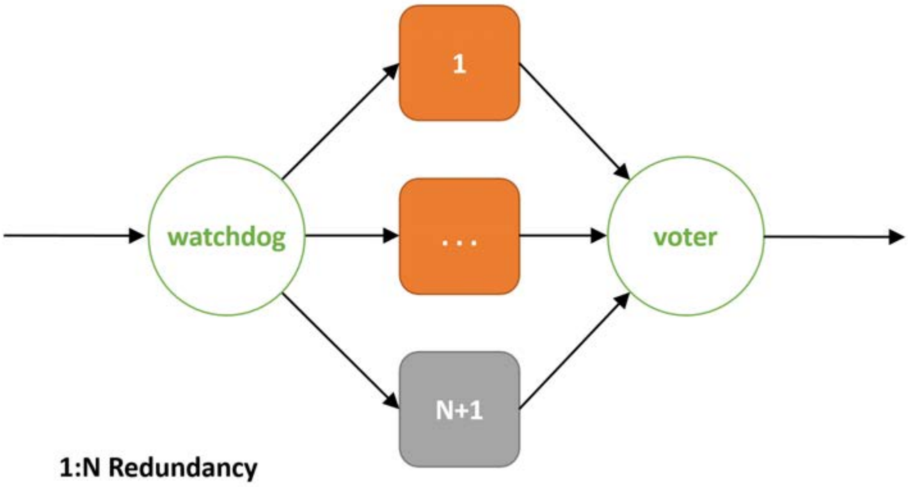

Figure 2.6: 1:N Redundancy - in orange active units in grey the auxilliary one.

From regulation to Machine Protection System

In order to realize a Machine Protection System compliant with the IEC 61508, I followed the list of task previously described. The standard required a detailed study of two fundamental concepts: the *safety life-cycle* and *Safety Integrity Levels*.

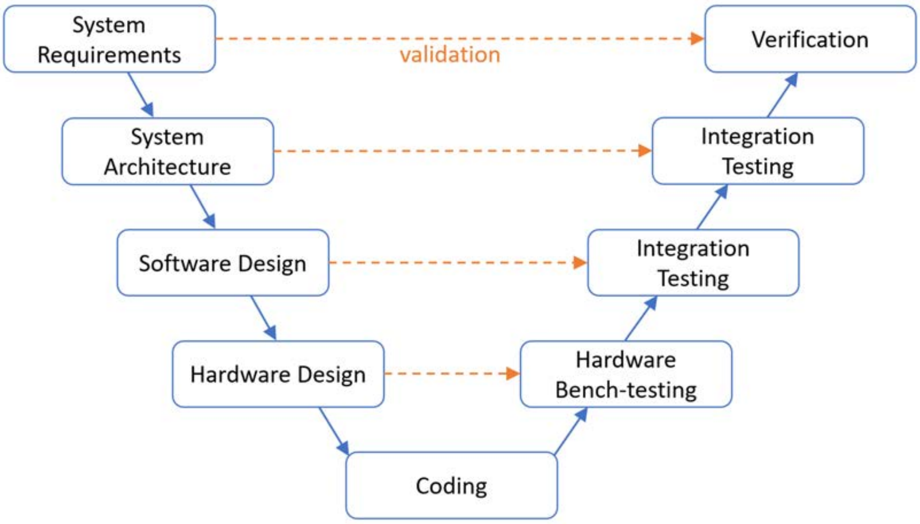

Figure 2.7: The ELI-NP-GBS Machine Protection System V-model for the life cycle development.

I chose to follow the *safety life-cycle* of “identify-assess-design-verify” closed loop developing a dedicated V-model, as shown in Figure 2.7:

1. A risk analysis should be done in order to identify any possible failure of the accelerator and the required action to avoid damages to people and equipment without affecting the facility operation, if not required. The result of this phase has been a list of requirement for the software and the hardware of the MPS.

2. With the requirements of the previous point and with the guidelines of the IEC 61508, the architecture of the system has been designed in order to follow this functional *safety management plan*:

   a) The logic of the software was developed from logic matrix which collects all the possible failure of any surveyed system of the accelerator. Such matrix was filled up collecting requirements from expert of each technical team of the facility iterating several review to inspect the best solution and analyze the impact of any error handling strategy to avoid damages without inconsistency inside the logic.

   b) For any failure of the logic matrix was paired a unified error code traceable inside the software code.

   c) About the prevention of unauthorized modifications, great part of the software is coded in FPGA devices. With this framework it is possible benefit of:

      i. VHDL programming language used inside FPGA chips works deterministically then, excluding error inside software logic, is always possible know the output due to a certain input;

      ii. There are no viruses for the VHDL language;

      iii. Physical access to the FPGA chip is strictly controlled inside solid state flash memory not available for the direct access and especially not available for the online programming while another software is running.

   The remaining part of the code, inside EPICS servers it is protected with password.

Communication of the FPGA or EPICS servers with the Control System (CS) will happen through a dedicated network VLAN where only EPICS servers can share data. Only con CS people can operate on such network and servers with dedicated procedures.

3. Next step of V-model is the software design. Software interacts with hardware in order to guarantee all the requirements and to collect required data from MPS subsystems and from the CS. The strategy to minimize software failure were a scheduling of several tests and a special attention to the redundancy of the hardware.

4. When all the requirements from the accelerator's risk analysis, the software and the regulation were collected, the phase of hardware design started. This point of the model is strictly connected to the very important evaluation of the required *Safety Integrity Level.*

   According with regulation, together with the SIL class is also guarantee that each SIF works on different layer of the MPS framework, the response time of each SIF matches with the requirements of the risk analysis, how safe state of MPS and devices interfaced with it is achieved when a failure of the MPS happens.

5. Climbing back to the top of the V-model there is a first step of hardware bench-testing according with the specification of design with all the related test criteria, setup, results and eventually corrective actions on the hardware design when a failure happen.

6. When the hardware framework is tested there is a second step testing and integration of the software in order to check capability of the MPS to communicate with monitored devices, verify if its matches with the logic matrix and all other requirements of the MPS.

7. The last phase is the validation of the MPS through the verification of the requirements and scheduling a safety validation planning.

   The verification of the system all requirements are verified looking for each condition of the Logic Matrix then it is possible to go through a check-list with a series of documented procedures to investigate all startup, reset, shutdown and fail-safe capability of the whole MPS. A log is devoted to take notes of every expected output or results of these tests, if a test of the check-list is passed or failed and eventually some note is filled inside the logbook. If an unexpected failure happens this it is investigated in order to understand if comes from software or hardware, from the realization or from design and then fixed. When all the requirements are satisfied and all tests passed the system is assumed verified.

The safety validation planning of the MPS is a scheduled periodical verification of the check-list in order to identify ageing issues of the hardware and, according with the evaluation of the MTBF of each SIF, the total replacement of the hardware to anticipate ware out failures of the hardware. For each verification results of the check-list will be reported on the logbook.

In next chapters I will present the risk analysis for the ELI-NP-GBS accelerator and the related list of requirements for MPS, the architecture of the MPS with detailed design of core systems and auxiliary sub-systems and any related integration testing and bench test. Due to the initial state of the facility installation it has not been possible to show the on-site validation of the system (Site Acceptance Test) because it will be installed in next years anyway I will show the safety validation planning and the results of the verification check-list made in the development site (Factory Acceptance Test) to match all the requirements of the system.

CHAPTER

3 Risk Analysis and Requirements

Content

3.1 High Power RF system 50
3.2 Low Level RF system 52
3.3 Vacuum system 53
3.4 Magnets 62
3.5 Cooling system 64
3.6 Personnel Safety System 65
3.7 Control system 67
3.8 Synchronization 67
3.9 Electron beam diagnostics 68
3.10 Requirements overview 69

The ELI-NP-GBS accelerator is made of different systems which require to operate in the proper way to guarantee the challenging performances of the facility. Some system are equipped with their own protection device while others need to be completely surveyed by an external protection system. A Machine Protection System, able to supervise all the critical systems, is generally required in order to: monitor all interactions between such systems; handle any kind of error/malfunction/working point able to compromise the accelerator performances; solve issues to optimize accelerator up-time.

As general requirements for the Machine Protection System of the ELI-NP-GBS it is also important to consider that: this accelerator is a new facility with in a new building with new plants; EuroGammaS operators, coming from different countries all over Europe, will be always on-site but they could be not enough specialized to handle all systems while expert teams can be remotely connected or contacted. Then the MPS must be able to provide automatic procedures to handle all issues, to monitor electron and gamma beam performances minimizing intervention of operators without affecting the machine uptime.

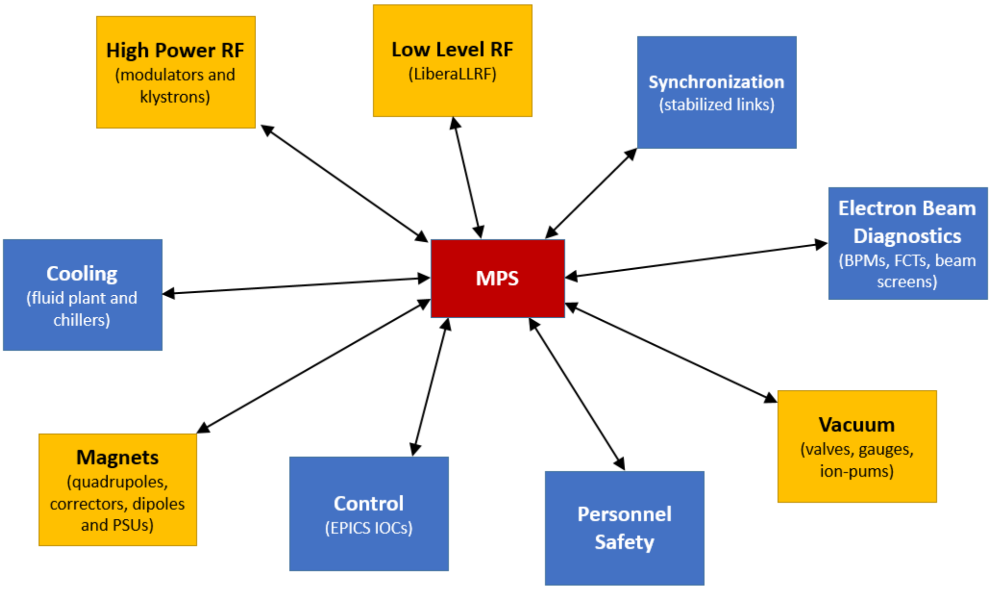
High Power RF (modulators and klystrons)
Low Level RF (LiberaLLRF)
Synchronization (stabilized links)
Electron Beam Diagnostics (BPMs, FCTs, beam screens)
Cooling (fluid plant and chillers)
MPS
Vacuum (valves, gauges, ion-pums)
Magnets (quadrupoles, correctors, dipoles and PSUs)
Control (EPICS IOCs)
Personnel Safety

Figure 3.1: MPS risk analisys - Schematic of accelerator systems involved in the MPS. In yellow, critical systems to be controlled; in blue, less critical systems.

The main tasks of the MPS, as sketched in Figure 3.1, are the monitoring of RF signals, vacuum and magnets systems. For these reasons, in the following chapter, it will be widely described the design of such a systems, their reliabilities and capabilities to provide (or not) diagnostics on their performances. Other systems of the accelerator (such as cooling, personnel safety, control, synchronization and electron beam diagnostics systems), which are already fail-safe and/or standalone, are briefly summarized to illustrate supervision activities required for the MPS.

In the following chapter I will illustrate the risk analysis that has been performed for each accelerator system in order to extract requirements needed for the development of the MPS. Risks analysis of laser systems are not treated because such systems are standalone systems and fully monitored by embedded MPS systems.

3.1 High Power RF system

The 15 accelerating structures are individually fed by dedicated power stations (except the last 4 TW structures that are powered in parallel by 2 klystrons), which allows to have a higher operational flexibility [36].

A schematic layout of the 13 RF power plant is shown in Figure 3.2. Every power unit, consists of a ScandiNova [37] pulsed HV solid state modulator, a Toshiba klystron tube (model E37314 for S-band and E37212 for C-band) and a Microwave Amplifier 400 W solid state driver amplifier (model AM10 for S-band and AM61 for C-band).

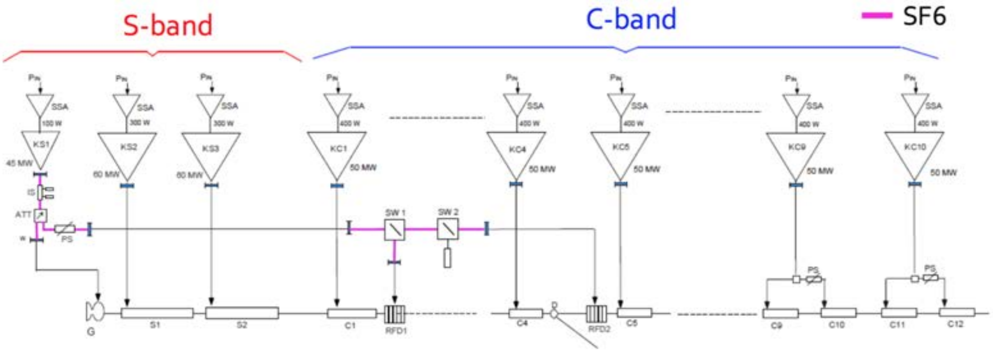

Figure 3.2: ELI-NP RF power sources and distribution system. Three power units are used for the S-band injector, ten units for the C-band booster. In magenta the waveguide system with components (isolator, attenuators, phase shifters and RF-switches) under sulfur-exafluoride (SF6).

A 45 MW source feeds all the SW cavities: the RF-gun and two RF deflectors, while two 60 MW power units are needed for the two S-band TW structures of the photo-injector. The remaining 10 C-band power sources are 50 MW units. The modulators have been manufactured using solid-state technology that offers, with respect to the standard pulse forming network and tube switching devices, excellent performance in terms of repeatability and amplitude stability of the high voltage pulses (high-voltage equipment is fully embedded inside the tank), compactness, ease of maintenance and operational safety (due to their modular design).

Each ScandiNova [37] modulator is equipped with a Beckhoff PLC operating in real-time through an optical fiber network to the FPGA board that handle, monitor and trigger each one of the several switching units and the RF Amplifier.

This PLC-based control system has the capability to run the modulator and klystron in proper operation and provide fail-safe procedures when issues happen. According to specifications, the PLC is able to propagate signals from the contact interface within 10 μs. It is possible communicate with the PLC through ModBus interface and a contact interface for the hardwired control of:

- External Interlock: the lack of this input signal switch the modulator mode from running state “Trigger” to the “Standby” mode in which just the filament is switched on but there are no RF power amplification.

- Trigger enable: until this input signal is missing the modulator persist in “Trigger” mode but the trigger to all switching units is removed then the high-voltage output pulse doesn’t arrive to the klystron.

- Sum Interlock: this output signal is the logic OR of any internal interlock detected by the Beckhoff PLC, the lack of this signal means that at least one interlock was detected.

The idea of a “Trigger enable” procedure is a useful tool to inhibit RF pulses to the accelerator. The best way for this kind of operation is to set the modulator in “diode mode” removing the RF signal in input to the klystron. Unfortunately the ScandiNova “Trigger enable” procedure doesn’t put the RF source in “diode mode” and it switch off, temporarily, the power transformer introducing a deprecated temperature and electric stresses that could damage the klystron in long period operation.

The PLC could be also interfaced with one Directional Coupler (DC) to monitor reflected RF signal and inhibit modulator's operation until a threshold is exceeded. In the ELI-NP this signal is taken from the DC immediatly after the klystron output. This configuration guarantee protection of the klystron if a line mismatch (due, as example, to vacuum leak or arcing events) occurs near to RF source but, due to threshold calibrated for events nearby the klystron, this system can be not sensitive to events happening, for example, in accelerating structures.

The ScandiNova [37] control system is fully able to handle normal and anomalous condition of the modulator but it doesn't take into account interaction with other systems of the facility like safety devices or the vacuum system. The MPS should be able, therefore, to stop or inhibit properly modulator's operation within the next RF pulse and propagate the interlock status of the modulator.

3.2 Low Level RF system

The LLRF system [36] generates the RF pulses used to drive the power units, acquires and monitors the RF signals picked-up along the accelerator (e.g. from the waveguide network or accelerating cavities). Moreover, it allows to generate suitable control signals, either manually or through feedback loops, to set the required levels and phases of the RF fields in any RF device of the machine.

The ELI-NP LLRF system is made of 13 "Libera LLRF" temperature stabilized digital boards manufactured by Instrumentation Technologies [38]. The system consists of 3 S-band and 10 C-band units (as for modulators, one for each power unit). This choice has been made in order to guarantee the maximum flexibility in terms of RF pulse shaping and machine operation stability. One of the main advantages of a digital LLRF system is, in fact, the possibility to perform a pulse-by-pulse feedback interactively choosing from control system the target signals for amplitude and phase loops. Thanks to this pulse shaping capability is possible minimize the energy spread along the bunch train due to beam loading effects.

Each board monitoring the TW structures will acquire 6 RF signals (solid state amplifier output, klystron output and section output forward and reflected power signals from DCs), with the exception of the last four sections that will be squeezed in two boards equipped with two sampling modules each, in order to manage 12 RF signals. All the signals from the SW cavities, instead, will be acquired by the first S-band board. In this case also three RF probes will be acquired to monitor the fields in the cavities, for a total of 13 RF signals.

Each Libera system could be controlled through the integrated EPICS IOC and a couple of contacts for the hardwired communication: one input signal to interlock the board and stop the LLRF signal to the driver and one output signal that is a logic OR of any internal interlock detected by the board.

The FPGA-based control system of each Libera board is able to handle any issue of the board and it is possible configure some peak detector interlock from collected RF signals in order to monitor performance of the whole RF station (LLRF, Power RF system and accelerating structure) and the quality of involved vacuum region. According to the FPGA code, this kind of interlock is intended to shut down completely the LLRF unit then should be configured to handle critical scenario while another solutions can be implemented to handle random arcs or slow vacuum increase.

The only requirements for the MPS is to trigger LLRF board interlock when the related modulator is tripped by an interlock (and vice versa) within the next RF pulse.

3.3 Vacuum system

Togeether with RF system the vacuum is a critical and awkward system that should be carefully monitored by the MPS.

The RF WaveGuides network, Figure 3.3, is made of 13 lines (WR284 for the S-band injector and WR187 for the C-band booster). Each line is segmented both from klystron and from linac with a ceramic window while Agilent [39] 55 $\frac{l}{s}$ UHV ion pumps are used for pumping. On RF Gun waveguide line, there are 5 segments includeing 2 pressurized 2 atm with sulfur-exafluoride (SF6) since they include ferrite materials (for isolators) or movable components (RF switches) that cannot operate in vacuum.

The whole linac is splitted in 20 vacuum regions, Figure 3.4-3.5-3.6-3.7-3.8, with a pneumatic valve at each boundary. According to the accelerator layout has been possible group vacuum region in four zones: “Linac”, “Transfer lines”, “Laser circulator” and “Gamma characterization”.

As shown in Table 3.1, Agilent [39] Thermo Couple (TC) vacuum gauges and Cold Cathod (CC) vacuum gauges monitor the vacuum in the whole accelerator. In Linac and transfer lines zones there are several Agilent 75 $\frac{l}{s}$ UHV ion pumps while inside Laser circulator [40] and Gamma characterization [41] zones the pumping system is kept by turbomolecular and scroll pumps manufactured by Edwards [42].

Zone	# Regions	Valve	CC Gauge	TC Gauge	Ion Pumps	Turbo Pumps	Scroll Pumps	Pressure
Linac	7	7	16	6	42			10^{-9} mbar
Transfer lines	7	4	12	7	20			10^{-8} mbar
Laser circulator	2	4	2	4		4	2	10^{-9} mbar
Gamma characterization	4	4	8	12		10	4	10^{-9} mbar
RF WaveGuides	17				70			10^{-8} mbar

Table 3.1: Vacuum regions overview groupped by accelerator’s zone.

Both types of vacuum gauges are controlled by Agilent XGS-600 controllers. For each gauge it is possible to configure up to 2 SetPoints for a total of 8 SetPoints for each controller. The logical state of each SetPoint could be monitored from MobBus protocol, 8 relay contacts and 8 open-collector contacts.

All Ion Pumps are controlled by Agilent 4UHV Ion Pump controllers. Each pump has a related SetPoint for a total of 4 SetPoint. The logical state of each SetPoint could be monitored from MobBus protocol and 4 relay contacts.

Turbo pumps have a dedicated controller for each unit. A series of relay contacts communicate “normal state” or not of pump’s rotor.

Pneumatic valves are controlled by 6 Omron [43] CJ2M PLCs through hardwired contact interface.

Ion pumps controllers of RF WaveGuides network are located on the Roof level with all other RF system. Turbo pumps controller of Laser circulator zones are nearby the module on the experimental bays while controllers of the Gamma characterization zones are located on the Roof Level. Linac Ion Pumps and vacuum gauges controllers are splitted in the 2 technical rooms on the ground level (one segment cover low energy line and the booster, from Module 1 to Module 21, the other segment the remaining part of high energy line, from Module 22 to Module 36).

The vacuum system requires several interactions with the MPS in order to protect the accelerator performances, RF system, detectors and the vacuum equipment itself. MPS should be able to handle, properly, issues from different zone of the accelerator (e.g. a detected leak in RF WaveGuides involves just the related modulator while a leak in Linac involves all RF sources of the corresponding vacuum region). MPS has to provide fastest control on vacuum equipment in order to localize vacuum issues and stop or inhibit the related RF sources and, if needed, dissect as soon as possible the vacuum region where a leak is detected.

Due to the tricky equipment of some zones of the accelerator, it is required a review of the design with the vacuum team to better guarantee the hardware safety. Zones which require improvements in vacuum system are:

- Laser circulator and Gamma characterization areas that have pumping system made by turbo and scroll pumps. Failure of these devices could damage gamma-rays detectors, disalign laser circulator mirrors and vent the linac. Backing line require vacuum gauges and valve to isolate leaked line.

- Due to the energy and charge of the electron beam, vacuum windows before the three electron dumps should be carefully simulated to avoid thermal damages able to broke such windows causing vacuum leak.

- RF Gun needs a strategy to avoid accidental venting of the gun itself that can damage the photo-cathode (e.g. due to a critical vacuum leak somewhere in the accelerator) comprimising its performances.

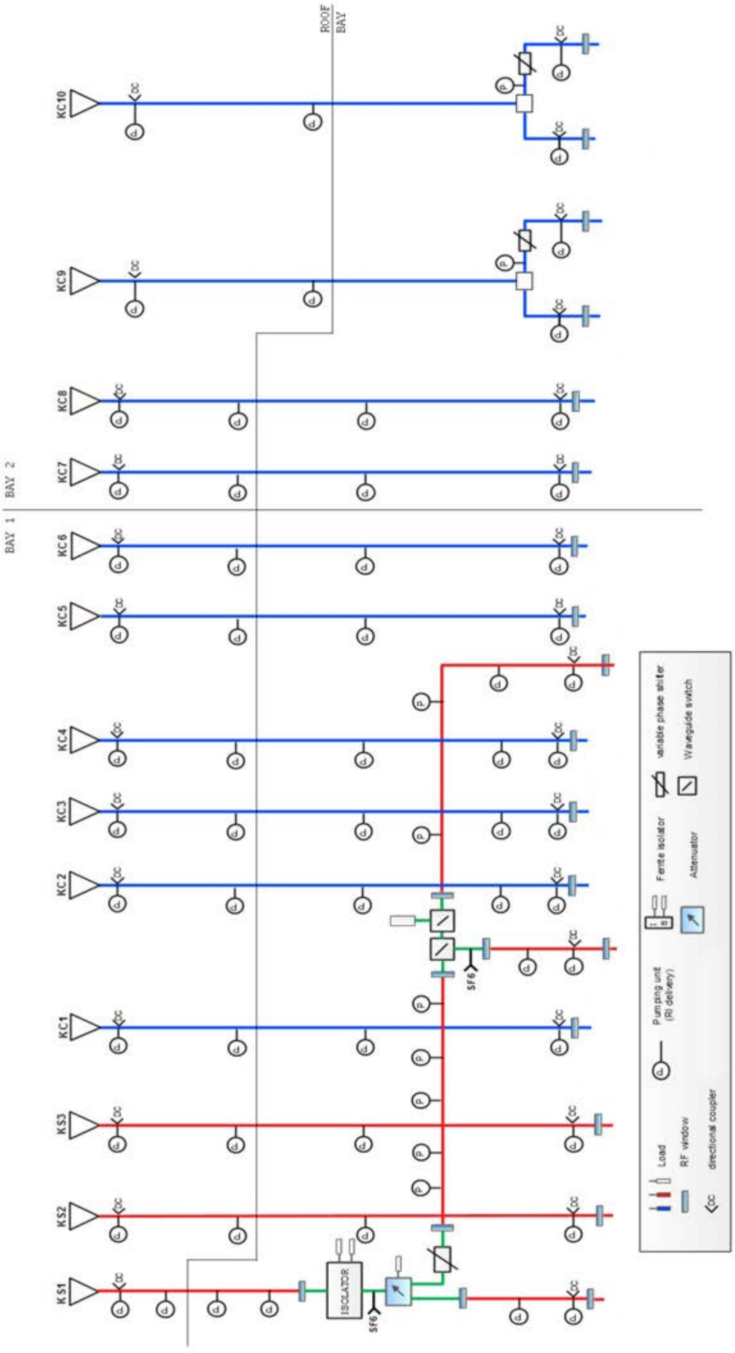

Figure 3.3: RF Wave Guides layout schematic.

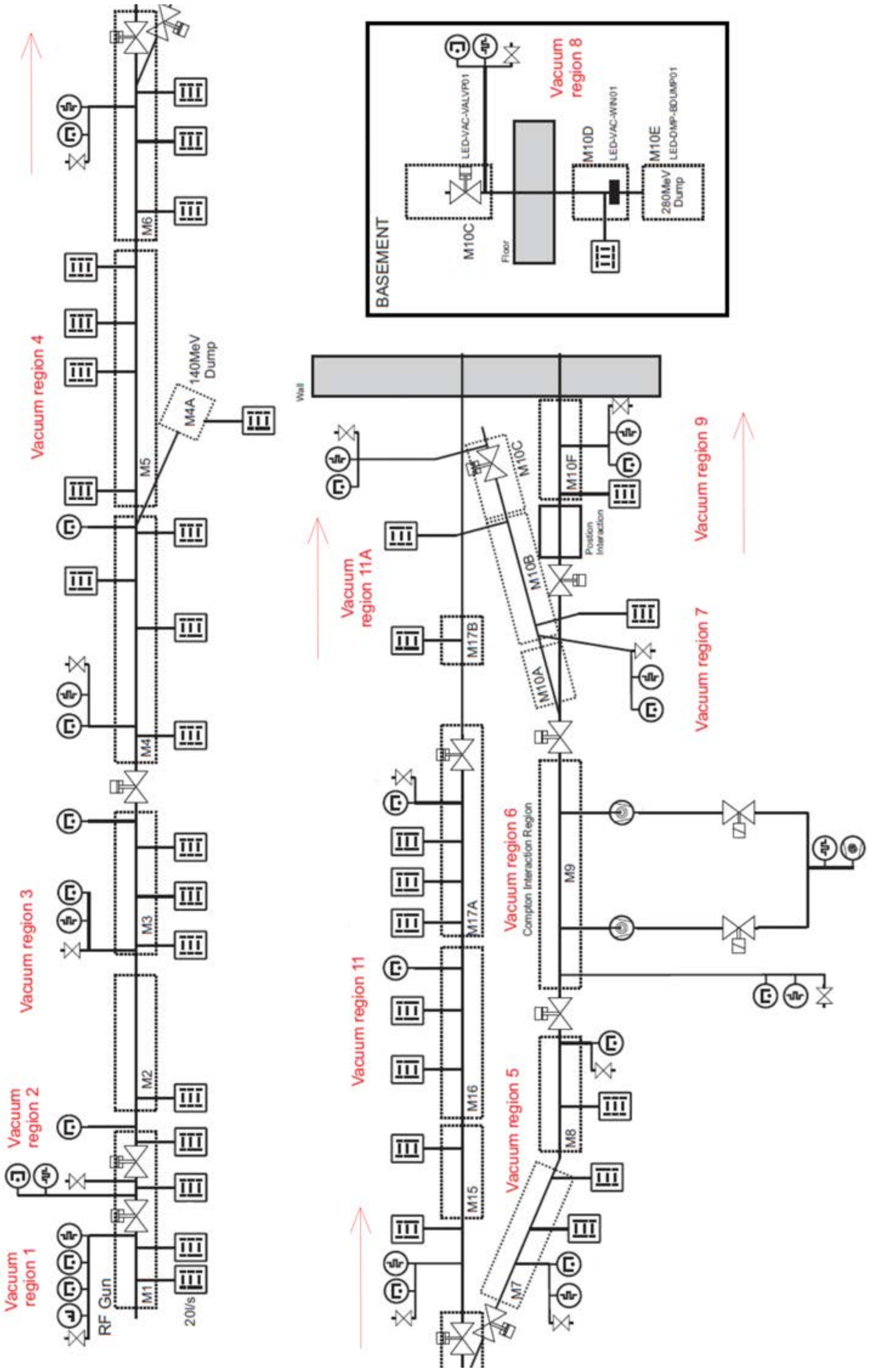

Figure 3.4: Linac layout schematic - low energy zones and interaction point.

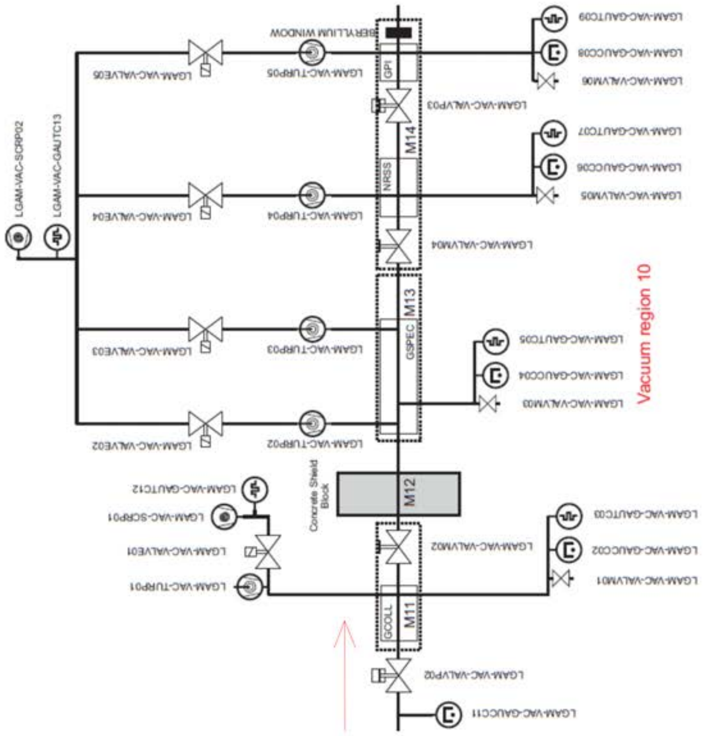

Figure 3.5: Linac layout schematic - low energy gamma characterization.

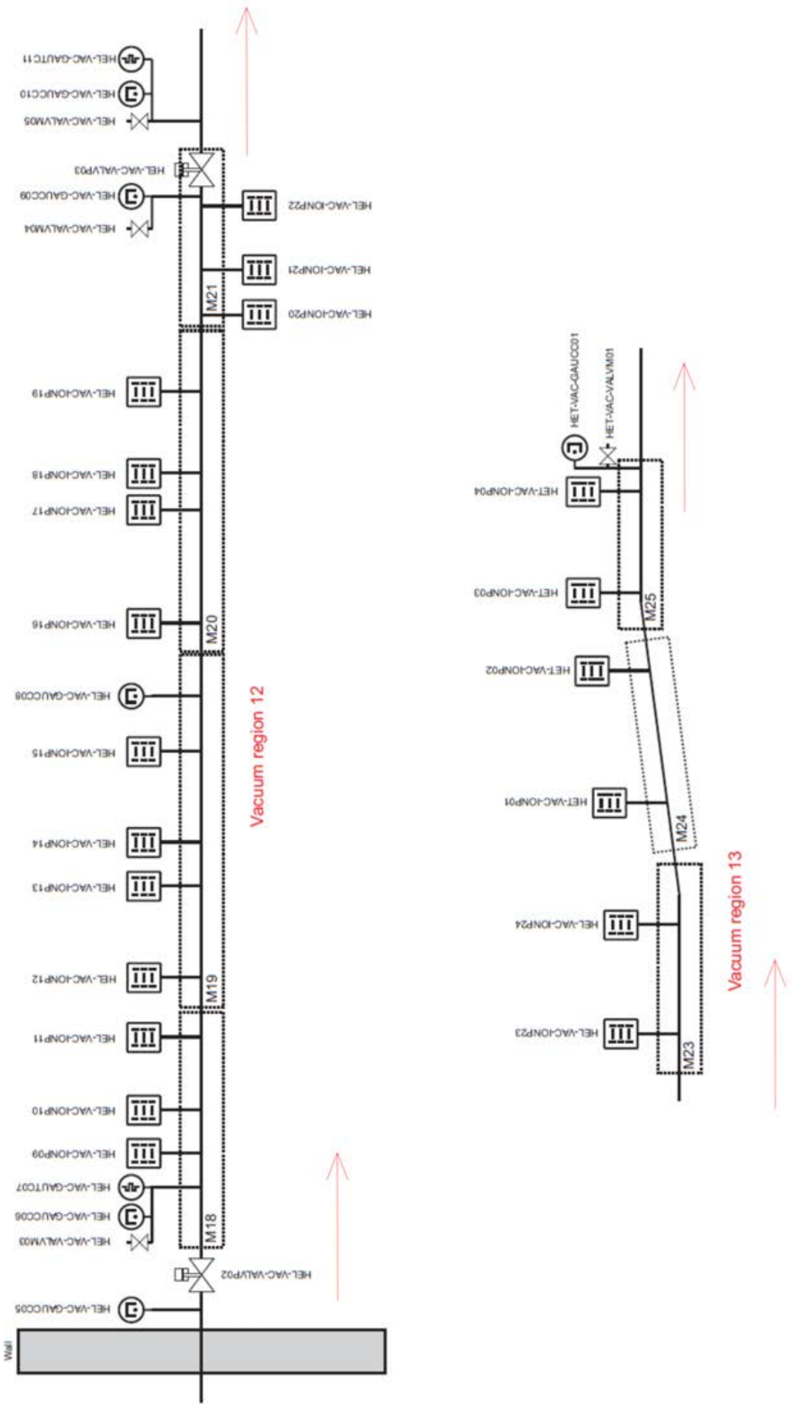

Figure 3.6: Linac layout schematic - high energy zones.

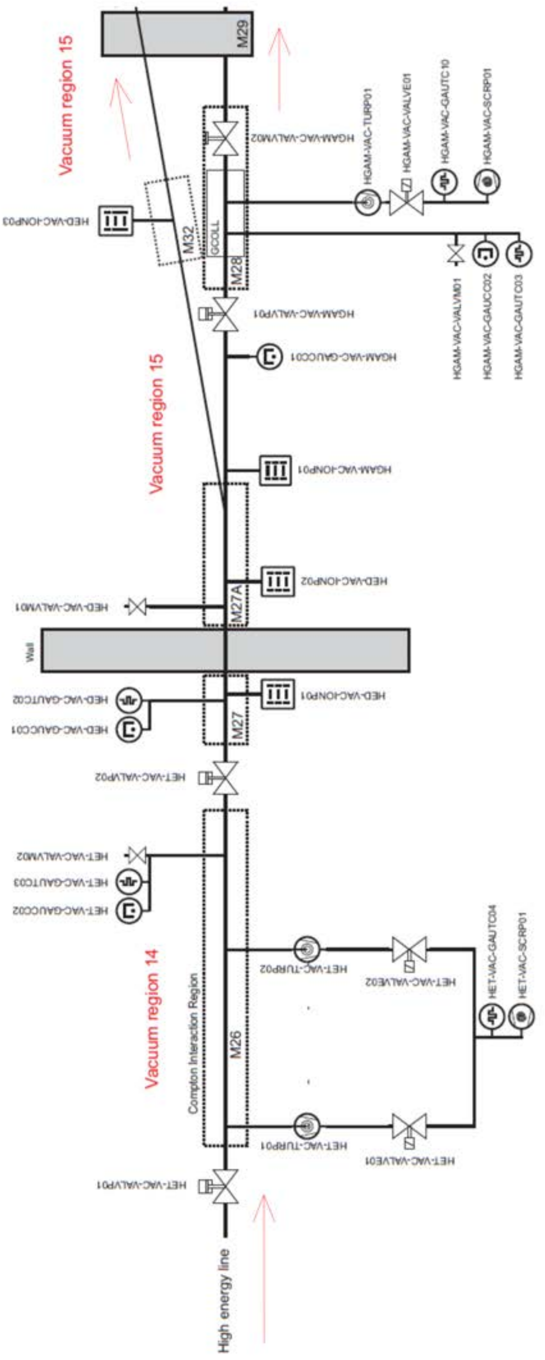

Figure 3.7: Linac layout schematic - high energy interaction point.

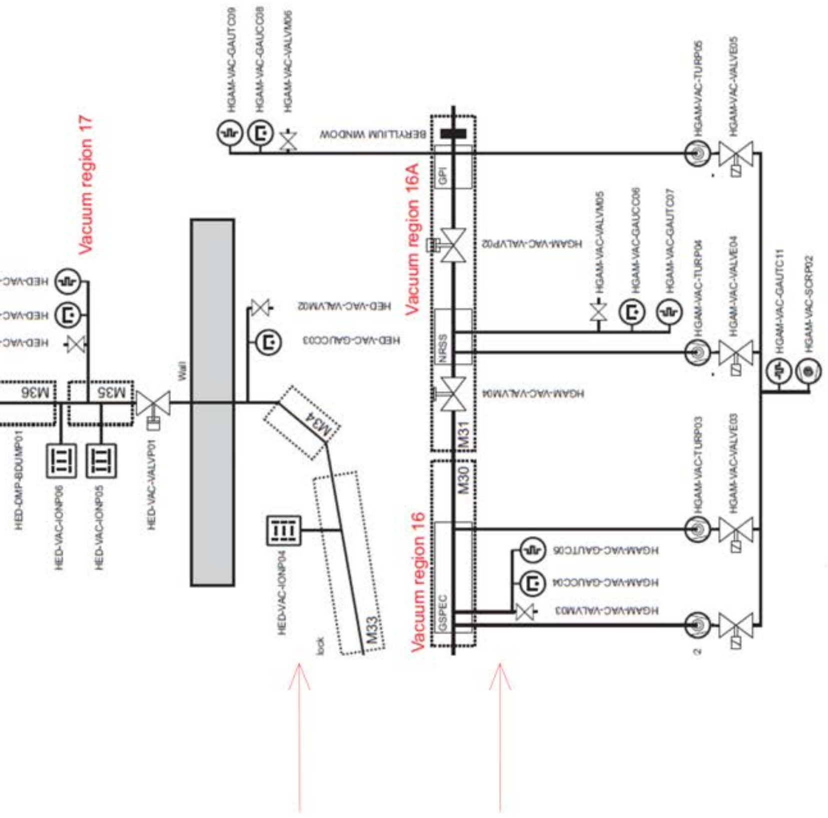

Figure 3.8: Linac layout schematic - high energy gamma characterization.

3.4 Magnets

Magnetic elements for linac includes 78 magnets (11 are part of the photo-injector, 29 are in the low energy line and 38 in the high energy line). There are 2 solenoids, 9 dipoles, 37 quadrupoles and 30 steerers. All the magnets operates in DC.

- **Bending magnets** - There are 6 type of dipoles **??** each one has a full iron yoke with the poles in low carbon steel while the rest of the yoke is composed by normal steel. Except for the second dipole of the low energy transfer line that has a C-shape profile, all the other ones has a H-shape profile. Dipoles are equipped with a polarity reversal module in order to cancel the residual field due to hysteresis. The magnet fields go from 0.5 T to 1.8 T, the current range from 95 A to 175 A and the power supply could reach a maximum power of 11 kW.

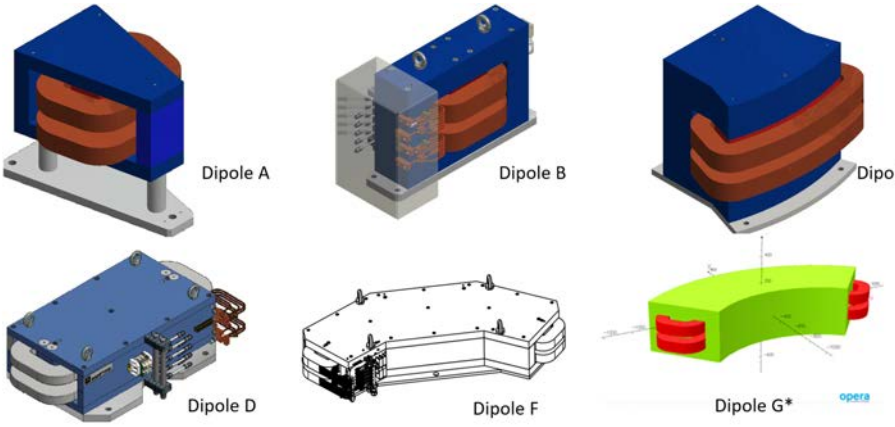

Figure 3.9: Dipoles 3D models - Type A, B, C and D on transfer lines bend electrons from about 15 to 40 degrees. Type F and G on dump linee bend electrons of about 90 degrees.

- **Focusing magnets** - There are 5 different type of quadrupoles 3.10, all in full iron yoke and with the same configuration of the dipoles. All the quadrupoles have a polarity reversal module. The gradients goes from 18 $\frac{T}{m}$ to 30 $\frac{T}{m}$, the current range goes from 47 A to 90 A and the bore is for all of them 30 mm.

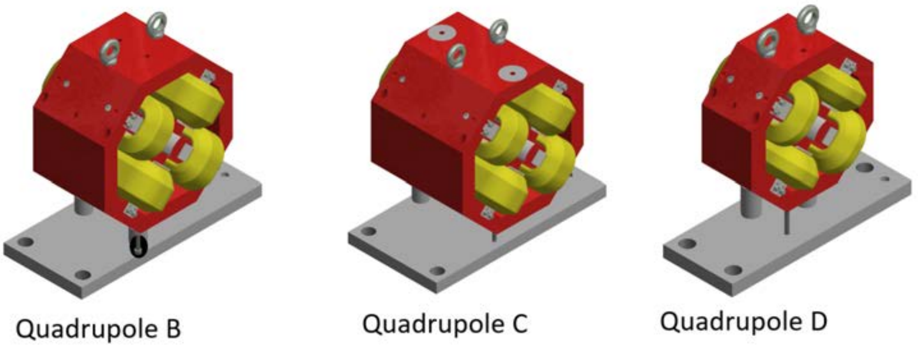

Figure 3.10: Quadrupoles 3D models - Type A, B and C used in drift beam pipes whyle Type D used in triplets.

- **Corrector magnets** - Steerers there are mainly two different types 3.11: the steerers on the S-band accelerating structures that have a $\cos\theta$ configuration and the others with a square cross section iron yoke composed by steel. The field goes from 33 G to 140 G, the current from 1.2 A to 8 A.

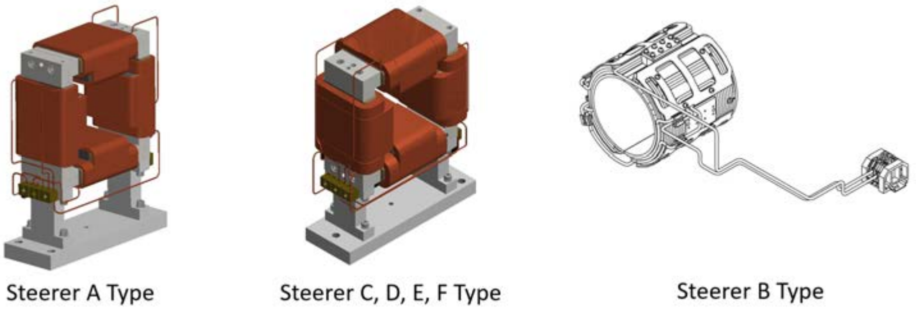

Figure 3.11: Steerers 3D models - Type B is used at beginning and end of accelerating structures while other types on beam pipes.

All the magnets are water cooled with exception of steerers that are air-cooled.

Dipoles and quadrupoles are supplied by Start series Power Supply Units manufactured by SigmaPhi [44]. This PSUs are able to provide up to 200 A of DC current at 55 V of voltage and a ripple of less than 20 ppm. Steerers are supplied from PSU crates manufactured from iTest [45] able to provide ±15 A of current at 8 V and with a ripple of less than 7 ppm.

All PSUs could be controlled from ethernet interface or through two relay contacts that are currently interfaced with thermo-switches on magnets and flow-switches on water cooling inlet of each accelerator module. In first instance PSUs could provide the required machine safety for the facility but, due to the challenging performances required by the accelerator, is important that MPS improves diagnostics of beam transport along the whole accelerator. Then the MPS should monitor if there is mismatch in optical line due to the fault state of a power supplies. In addition to this, due to the power of the electron beam, is very important verify the magnetic field dipoles in order to check that they bend electrons out from the trajectory of gamma diagnostic or other equipment.

3.5 Cooling system

The cooling system for the accelerator is made of fluid plant located in building basement to thermalize demineralized water and treat its hardness. This plant provides in output two lines: a $19°C$ for laser systems and accelerating structures' chillers and a pre-heated line at $30°C$ for magnets and RF system cooling.

The cooling plant is controlled by a CJ2M Omron PLC able to control pumping units and valves for the water distribution. The PLC can communicate with protocol RS485 to make possible monitor temperatures, valves and pumps status and provide an automated procedure to switch on/off the plant. It is also possible interface the PLC through two output contact:

- the first one signaling problems during the refill of the plant due to a low level water in the reservoir.

- the second one checks temperature stability for the $30°C$ circuit providing an error when it drifts over $\pm 2°C$.

As anticipated, 10 Chillers get water from the fluid plant to stabilize temperature of accelerating structures. Every chiller is conneted to a couple of structures with the exception of RF Gun and the two deflecting cavities that have a dedicated chiller.

All chillers are chained together to communicate with RS485 protocol then it is possible the remote control of critical parameters like temperature and flow rate.

The MPS must be interfaced with both contacts, available for the Fluid plant, in order to switch off in the properly way RF, laser and magnets systems to avoid possible damages due to over-heating cooling. About chillers, the MPS must monitor chillers parameters to handle RF frequency drifting due to temperature drifts.

3.6 Personnel Safety System

The Personnel Safety System is another safety equipment, like the MPS, in charge of personnel protection from ionization radiation exposure.

Following radiation protection team instructions, I developed also this system to provide the personnel safety for the ELI-NP-GBS facility. The task of the system is to guarantee safe operation for the personnel in the 3 operation mode of the accelerator:

- **Linac off** - in this mode RF and laser systems cannot be activated then there are no ionization radiation in the building. Access control is disabled and gates unlocked.
- **Linac on** - in this mode the whole accelerator could be activated then accesses to bays are forbidden while, on the roof, the system could be bypassed just for RF team personnel with the supervision of an operator in control room.
- **Low energy linac** - this mode is required for fast operation in the second bay with low energy accelerator running in the first bay. In this mode accesses are forbidden just in first bay, interaction laser is interlocked to stop gamma production and it is also mandatory a cross check from beam stoppers and beam loss minitors to guarantee a properly dumped electron beam inside the first accelerator bay.

This system is made of 4 sub-systems:

- **Relays crates** - is the core of the system, it collects double hardwired signals from emergency buttons distributed in the whole building and checks: micro-switch installed on each access of bays and roof level; ionization chambers (for electrons, gamma and neutrons) placed in the building; the sequence of interactions with search buttons to authorize the accelerator operation. This sub-system is covered by the IEC 61508 with SIL-3 class.

- **Ionization chambers** - 7 ionization chambers are located in technical rooms and over electron beam dumps to monitor radiation dispersion in the facility. A gas analyser checks for activated gasses in the outcoming channel of air distribution system of the building. This sub-system is interfaced through a double harwired line with Relays crates and with closed ethernet network where a dedicated server monitor and log exposure data measured by each device.

- **Access control** - this sub-system cover just the access to accelerator bays providing the control of photo-electric barriers and gates to identify and count personnel through a required personal RFID badge to enter/exit from a bay. Access control is interfaced with a double hardwired signal with Relays crates to forbid the authorization to run the accelerator if personnel is registred inside an accelerator bay.

- **Supervisor unit** - An FPGA unit checks the status varius auxiliary contact available in Relays crates in order to: ring bells in the building when the machine is authorized for operation; handle information monitors with the overview of accelerator status at each access of bays and roof level; make available in control room, thanks to an integrated EPICS IOC, the status of emergency buttons, search buttons and accelerator operation mode.

- **Beam Stoppers** - Two beam stoppers, one along the linac booster at the end of AB1 and one just after the low energy IP are able to stop the electron and gamma beams to avoid the radiation transport in AB2 thanks to a tungsten-copper block. These beam stoppers are required by the “Low Energy Linac” operation-mode which require radiation limited in AB1 while technical team access AB2. A controller unit in GP08 allow to control and reabback beam stopper position through a contact interface.

The PSS must be interfaced with the MPS to distribute the authorization signals to enable electron beam shutters, RF and laser systems guaranteeng as reliable as possible the safety for personnel.

3.7 Control system

The Control System of ELI-NP-GBS is based on EPICS framework distributed over 31 IO Controllers (IOCs) of Dell PowerEdge R320 servers or EKF Groove CPU and 6 consoles in control room. A dedicated server with redundant hard disks logs control system data on-line.

IOCs are dislocated around the whole facility to reach easily the monitored device and share the related Public Variables (PVs) over the accelerator data network.

Each IOC has a dedicated scope of work: 5 collect data from Basler [46] CCD camera of OTR electron beam screen; 3 has Agilent [39] m9210 digitizers to sample fast current transformer signal; 13 are interfaced with magnets power supplies, vacuum controllers and PLCs; 1 for ScandiNova [37] modulators; 1 for chillers and the fluid plant; 1 for Menlo femtosecond synchronization equipment; 7 for picosecond timing network.

Inside the EPICS code, for each IOC, is available as PV a watchdog to monitor from remote if the IOC is properly running. For any IOC disk exists an image backup, then the MPS must monitor the watchdog of each IOC to highlight possible issues.

3.8 Synchronization

This system distributes a stable RF reference throughout the facility. The timing distribution system, located in PC Laser clean room, is equipped with a laser master oscillator at 62.08 MHz. Through locking electronics, this signal is locked with a reference RF signal at 2856 MHz. Such signal, with a stability of about 70 fs, is distributed to client with optical stabilized links: the S-band and C-band LLRF distribution racks and the IP Laser. On clients side an amplifier increase the power level up to the required level.

This is system is interfaced through RS232 protocol to monitor critical parameters of the system. Generally the system doesn't require special attentions from the MPS with the only exception of amplifier on client side that that should be switched off if in operation without an input signal.

3.9 Electron beam diagnostics

The electron beam diagnostic is made of different type of equipment:

- **Beam Position Monitors** - 29 BPMs monitored by 7 LiberaBPM Single Pass Type-E, manufactured by Instrumentation Technologies [38], track the electron beam position on transverse plane. The LiberaBPM, with an integrated EPICS IOC, let the communication of BPMs data and set parameters (e.g. attenuation, sampling specifications, etc...).

- **Cavity Beam Position Monitors** - 4 CBPMs monitored by 2 LiberaCBPM manufactured by Instrumentation Technologies [38] monitor the beam position of micro-bunches on transverse plane just before and after each laser circulator [40]. As for the LiberaBPM, communication and settings are totally handled by the Libera FPGA.

- **Fast Current Transformer** - 4 FCTs sampled by Agilent [39] m9210 digitizers measure beam charge. As anticipated the digitizers are included in a dedicate EPICS IOC to acquire FCT data.

- **OTR beam screen** - 23 OTR screen distributed along the whole machine are used to map electron beam size and position over electron transverse plane. Each screen has a stepper motor controlled by Technosoft [47] driver with RS232 protocol and Basler [46] CCD camera to collect optical data through GigE protocol.

Libera FPGA framework, as anticipated in LLRF section, is able to completely handle any issues while Agilint digitizer are already integrated with the control system IOC. Then diagnostic readout electronics doesn't have requirements for the MPS.

While damages on BPMs, CBPMs and FCTs can occur just due to beam losses, beam screens interacts with the electron beam: this is not a problem when the OTR layer is inserted in the vacuum chamber but could be a problem for the screen support during the movement. Then for this system, the only requirements for the MPS is monitor the healthy status of sceens' motors and inhibit electron beam during screens movement.

3.10 Requirements overview

From the risk analysis reported in this chapter, the following Table 3.2 the list of requirements for the MPS.

Thanks to these informations is now possible continue through the project V-model to define in first instance the Architecture of MPS, at the end as reference to validate the MPS itself and at each periodical verification and maintenance of the system.

System	**Requirements**
General	Monitor electron and gamma beam perfomances; provide automatic procedure to handle easily equipment issues and operate the accelertor.
High Power RF	Install a hardwired network from vacuum and LLRF to detect issue; integrate a temporary inhibit to RF pulses; Develop a RF signal shape monitor to interlock RF source. Required fast interlock within 10 ms.
Low Level RF	Install a hardwired network from/to modulators. Required fast interlock within 10 ms.
Vacuum	Handle vacuum activities from different zones and regions; install a hardwired network to RF systems and valves' PLCs; review vacuum design in tricky zones (Laser circulator, Gamma characterization, beam dump windows and RF Gun); Required fast interlock within 10 ms.
Magnets	Check PSUs fault state; monitor electron beam transport; verify bending field in dipole magnets.
Cooling	Hardwired network to check fault in fluid plant; monitor chillers operating parameters.
Personnel Safety	Install high reliability hardwired network to RF systems to distribute enabling signal for the accelerator; monitor electron transport along dumping line to enable "Low Energy Linac" operation mode; Required fast interlock within 10 ms.
Control	Monitor IOCs watchdogs to handle control's post-mortem.
Synchronization	Verify if stabilized link amplifiers are working without input signals.
Electron Beam Diagnostics	Check fault state of beam screens' motors; inhibit electron beam while the screen is moving.

Table 3.2: ELI-NP-GBS requirements for the Machine Protection System.

CHAPTER

4 System Architecture

Content

4.1 MPS Framework 72
SIF Definitions 75
Reliability and Redundancy 77
4.2 MPS layers and interfaces 78
4.3 Logic Matrix 84

After the risk analysis I could proceed through the definition of the MPS framework architecture. In this chapter I will analyse the requirements in order to: introduce the MPS framework defining its reliability and *Safety Instrumented Functions* with related *Safety Integrity Levels* (according to the IEC 61508); describe how the MPS is interfaced with accelerator's systems and produce the logic matrix with instructions to handle accelerator's issues.

4.1 MPS Framework

From a first overview of ELI-NP-GBS requirements, it results that there are three class of constraints.

- High Power RF, LLRF, vacuum and personnel safety systems require high reliability, hardwired networks between devices and fast intervention time, tipically before the next RF pulse (less then 10 ms).
- Other systems collect data from control system and their issues could be handled with its update rate of about 100 ms (max EPICS data update rate is 10 Hz).
- From general requirements, magnets and personnel safety systems appear the necessity of beam loss monitors of different type to guarantee the electron beam transport, magnetic field in bending magnets and gamma beam production.

I choose to define MPS subsystems [48], Figure 4.1, and related technologies according to these three classes:

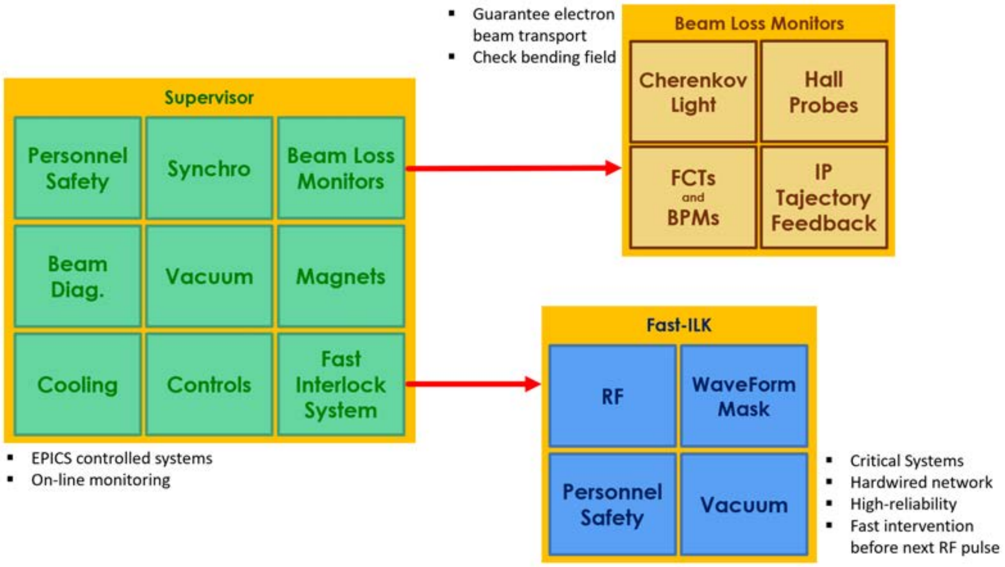

Figure 4.1: MPS Framework - In blue the fast-interlock system hardwired to critical accelerator systems, in green systems monitored under EPICS Control System and in yellow the beam loss monitors to check performances.

- **Fast-Interlock system** - This is a real-time FPGA-based system hardwired to vacuum gauges and ion-pumps of the accelerator, RF modulators and LLRF units and to a digitizer able to collect RF signals to compute a waveform mask [49]. It is also interfaced with EPICS Control System in order to make available an operator interface in control room and receive software interlock. When an issue is detected, the proper procedure to solve it (or to save the equipment) is performed. Taking in account the position of vacuum controllers (on the roof and in two technical rooms of ground floor) Fast-Interlock required a distributed architecture. This system, protecting critical systems, has been designed to provide the proper reliability and operate within next RF pulse.

- **EPICS-based Supervisor** - This system is an on-line EPICS IOC able to monitor PVs from equipment, to detect issues and to warn the operator interface about the problem or triggering the Fast-Interlock system. The Supervisor monitor also watchdogs from all MPS subsystems handling the post-mortem of the system.

- **Beam Loss Monitors** - In order to cover different requirements about electron and gamma beam performances, 4 type of loss monitors have been designed:

  - **Beam Loss Position Monitor** - It is a distributed system of Cherenkov fibers installed on beam pipe and accelerating structures along the whole accelerator to detect and localize mismatch in the electron beam transport line.
  - **Dipole Beam Loss Monitor** - They are a series of hall probe installed inside each dipoles (near to vacuum chamber and inside the good-field region of the magnet) to measure magnetic fields. From field measurement, the current inside coils is estimated to detect issues related to dipole coils or PSU.
  - **Fast Current Tranformers and Beam Position Monitors** - These two families of diagnostic devices from the electron beam diagnostics have been used to localize electron beam loss along the transport line.

  - **Gamma Beam Feedback** - This feedback monitors the luminosity at each Interaction Point (IP) and corrects the electron beam matching if a loss of performances is detected in gamma beam flux. Such monitor involves for each Interaction Point two CBPMs, two of XY correctors before the IP and the luminosity monitor just after the IP.

The framework has to be fail-safe then, after partial or global failure of the system, the MPS provide safe shutdown of critical systems.

According to general requirements, the MPS has been developed as a weak artificial intelligence (AI) fully autonomous and unsupervised system. In order to operate as a human-like experience, the algorithm coded performs a state-machine operating a “identify-solve-execute” closed loop.

As part of the programmed weak AI, the MPS will provide automatically different solution for any issue of the monitored systems. In particular, vacuum events will be handled by the vacuum zone where the problem is detected or by type of accelerator operation (if it is in conditioning or normal operation) up to catastrophic scenario, in which dissect the vacuum will be required.

SIF Definitions

In order to satisfy the IEC 61508 regulation, when the architecture of framework is defined, it is possible define the *Safety Instrumented Functions (SIFs)* of the MPS and, for each one, the required Safety Integritu Level (SIL). All the required operation, due to different constraints in terms of response time, were grouped in three family of operation:

- **SIF-1: Real-time control and intervention on critical accelerator systems.** The Fast-Interlock system handles failures of the RF sources, vacuum systems and it is a gateway for the enabling signal from personnel safety system. Then, a high reliability is required in order to avoid serious damage to the hardware and injury to people.

- **SIF-2: On-line control and intervention on accelerator systems.** The Supervisor monitors the proper operation of systems which require just on-line monitoring (including the hardware related to Function 1 and 3). Issues to such systems can damage hardware and cause loss beam performances.

- **SIF-3: Electron and Gamma Beam Loss Monitors.** Several sub-systems of beam loss monitors to check electron and gamma beam loss to identify bad operation point or malfunctions in devices which may compromise performances and damage equipment of the accelerator.

According to Table 4.1 as anticipated in Functional Safety chapter, I assumed:

- **SIF-1:** the frequency of hazard is assumed “almost certain” while the effect of the hazard is “catastrophic injury” then this *safety function* need at least SIL-3.

- **SIF-2:** the frequency of hazard is assumed “almost certain” while the effect of the hazard is “reportable injury” then this *safety function* need just the SIL-2 without any mandatory requirements.

- **SIF-3:** the frequency of hazard is assumed “almost certain” while the effect of the hazard is “insignificant damage” then this *safety function* has a safety level lower than SIL-1 then it is not covered by the IEC 61508.

For the first two functions, the frequency of demands is greater than twice the test frequency of the whole system then the SIL should be assumed in “continuous mode”. According to SIL classes in Table 2.1, it should be achieved a failure rate of at least 10^{-7} or less for SIF-1 and at least 10^{-6} or less for SIF-2.

	Extremely unlikely	Remote possibility	Possible occur	Will probably occur	Almost certain
Insignificant damage (non-relevant damages, no healthy issue)					🟩
Non-reportable injury (some damages, first assistance required)					SIL-1
Reportable injury (several damages, serius health problems)			SIL-1	SIL-1	SIL-2
Major injury (lot of damages, at least one death)			SIL-1	SIL-2	SIL-3
Major injury (lot of damages, at least one death)			SIL-1	SIL-2	SIL-3
Catastrophic injury (complete loss of production, several death)	SIL-1	SIL-1	SIL-2	SIL-3	SIL-3

Table 4.1: Risk matrix for the SIL evalutation - Columns show the likehood of the hazard happening while rows list the severity of the potential injury. The blue cell is the required SIL for Fast-Interlock system (SIF-1). The green cell is the required SIL for Supervisor (SIF-2). The yellow cell is the required SIL for Beam Loss Monitors (SIF-3).

Reliability and Redundancy

In order to guarantee the compliance of the MPS with IEC 61508, such safety system has been designed to achieve the requested failure rate for each of its part. To match these requirements from regulation I choose to improve the reliability of the system increasing redundancy of the framework.

The general drawback of redundancy schemes are the increasing of costs, then different solution have been assumed for the two sub-systems of the MPS:

- **SIF-1 - Fast-Interlock system:** the reliability of this system is improved through Dual Modular Redundancy: the hardware of whole system is duplicated. The two active systems work always in parallel with the same scope of work that means to double hardware with same software. This scheme increases the cost of the system over a factor two due to the doubled hardware and the related hardwired network with clients; anyway the critical systems monitored by the Fast-Interlock justify this design.

- **SIF-2 - Supervisor:** to improve the reliability of this system I choose the Hot-Standby Redundancy which requires to duplicate the system. A first master unit is active and fully operating. The second passive unit, the auxiliary one, is always powered and equipped with a watchdog in order to reduce and trigger the startup of the second system when the first one fails activating the auxiliary unit. With this scheme the hardware is doubled and the software is quite the same in both unit (auxiliary unit has also the watchdog module); the cost of the system is doubled but anyway the Supervisor is made of common control system servers that doesn't have an expensive cost.

4.2 MPS layers and interfaces

The architecture of MPS, from hardware point-of-view, requires different layer as show in Figure 4.2. This aspect of the fremework, according to the IEC 61508, is able to guarantee different dedicated hardware layer for each subsystem (SIF) to: avoid single point of failure of the system and proper fail-safe interfaces with monitored devices; guarantee reliability and required response time by the system.

The Fast-Interlock system requires a link to Personnel Safety, RF systems and related vaccum equipment. To reach the required reliability and response time faster then 10 ms an hardwired contacts network to each monitored device has been installed.

The Supervisor and Beam Loss Monitors require just interfaces with EPICS network to communicate with accelerator sub-systems through the EPICS data network.

These two networks represent the two independent layers of the MPS framework: either able to match SIF requirements and fail-safe.

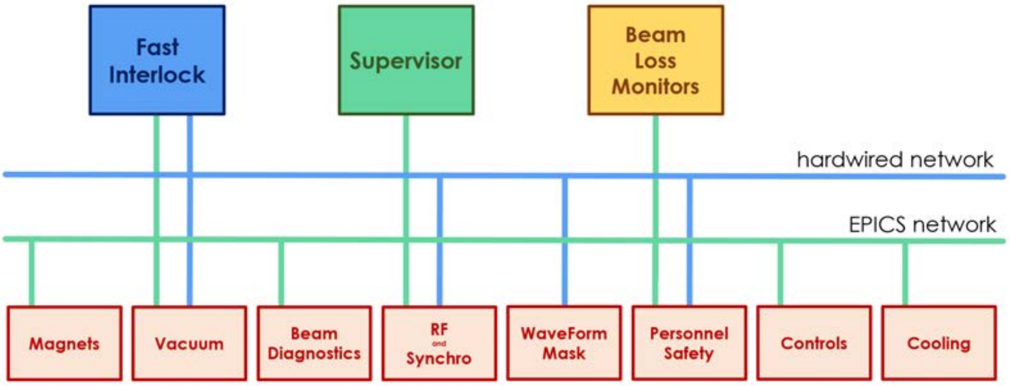

Figure 4.2: MPS Framework layers - Blue links make the hardwired network which allow the high-reliability communication between Fast-Interlock and monitored systems; Green links show the EPICS data network provided by the control system that is used by to share data between all systems.

While the data network for the Supervisor system and Beam Loss Monitors is part of the EPICS control system of the accelerator, then already integrated with whole facility, the hardwired network for the Fast-Interlock system has been designed and installed. First of all, to design this network I had to investigate the location of monitored device according to the topology of the building, available in Figure 4.3.

RF Modulator unit, LLRF crates, WaveForm Mask system and ion-pumps controller for waveguides are located on the Roof level while pneutmatic valves' PLCs, vacuum gauges and ion-pumps controllers for first 21 modules, laser shutters controller, Fluid Plant PLC and Personnel Safety system are in the first technical room at ground floor (called GP08). The remaining vacuum PLCs and controllers are in the second technical room (called GP04, far about 80 m from GP08). The hardwired network reach equipments located accross the building. In order to guarantee the performances of the Fast-Interlock, I choose to avoid a star-center architecture with a big FPGA linked with all the monitored devices (very chaotic to manage and maintain, high voltage drop, etc...) and I prefered to adopt distribute Fast-Interlock units in strategic places. In this way I obtained

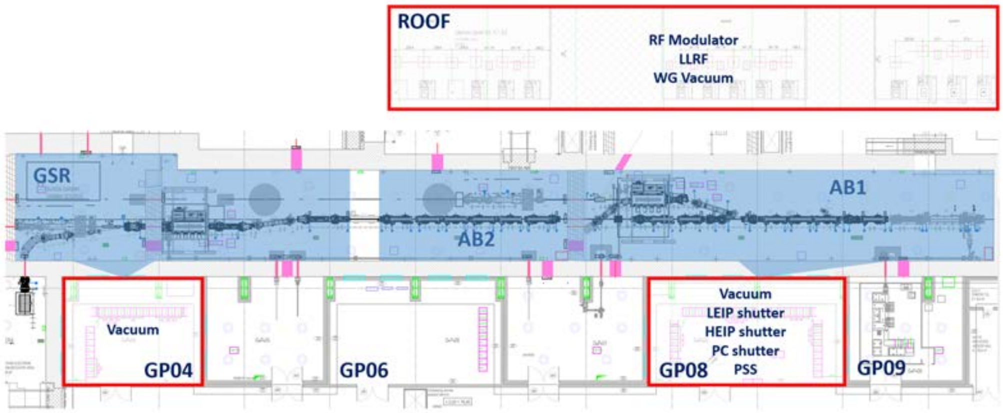

Figure 4.3: Fast-Interlock system monitored devices topology - RF Modulators, LLRF crates and WaveGuides vacuum controller placed on the Roof Level; Vacuum controller and PLCs for modules from 1 to 21, Personnel Safety System (PSS), low energy IP (LEIP), high energy IP (HEIP) laser and photo-cathode (PC) laser shutters placed in GP08 technical room on ground level; Vacuum controller and PLCs for modules from 22 to 36 placed in GP04 technical room on ground level.

smart FPGA devices, easy to manage, near to the equipment with short hardwired link to monitored devices.

As show in Figure 4.4, taking in account the topology of monitored devices, the Fast-Interlock system results: a master unit placed on the Roof level, a fist slave unit in GP08, a second slave unit in GP04. In order to preserve requirements about reliability and real-time response of the whole system, master and slaves units are chianed in a private etherCAT (ethernet Control Automation Technology) [50] network which provide high-speed and deterministic communication protocol. As anticipated in Redundancy section, the Fast-Interlock system is doubled with a second equal system wich work in parallel.

The master unit on the roof is in charge of quite all outputs of the Fast-Interlock (due to near RF systems), while quite all input comes from technical rooms (where vacuum controllers are placed). In order to interface the Fast-Interlock system with monitored devices, I had to design custom links to all equipment. As described in the previous chapter, many controllers have contact interface already available for this system. In few cases, I had to review the monitored hardware itself in order to obtain a proper contact interface:

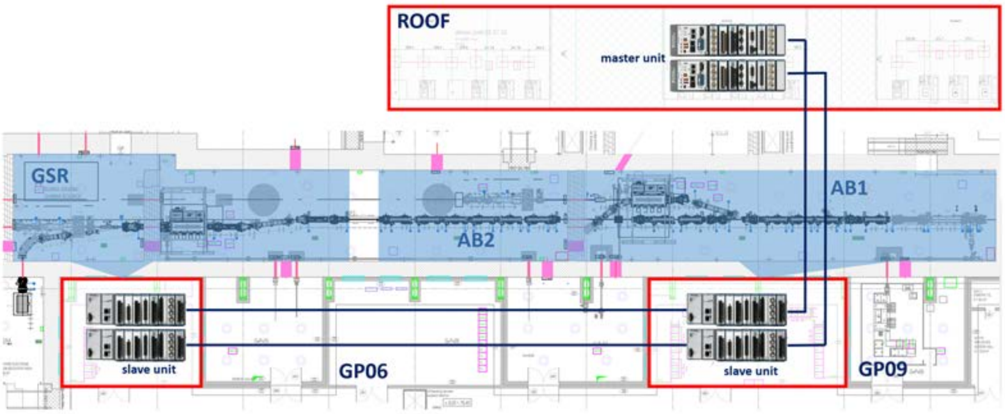

Figure 4.4: Fast-Interlock system topology - Master units placed on the Roof levelel collect data from the slave units chains from GP08 and GP04. The two chains are fully independent as required from Dual Modular Redundancy schema.

- As anticipated during the risk analysis, RF Modulators require a fast system to inhibit RF pulses sending the modulator in diode-mode. I choose to add this feature operating on the RF driver that is equipped with a TTL enable signal; according to ScandiNova design, such enable signal is always provided to the driver. I unplugged this connection and provide such a signal (or remove it) from the Fast-Interlock. When the RF driver is not enabled, the LLRF signal in input is zeroed and the klystron stopped.

- For many requirements, the best way to protect the accelerator is to remove the electron and/or the gamma beam.

  - When the enabling signal from Personnel Safety is missing, MPS had to inhibit all lasers and RF sources. While RF stopped through External Interlock to modulators, I had to integrate into Fast-Interlock system the control on lasers' shutters which are located at the beginning of each transfer line.

  - For many issues (e.g. vacuum activities in linac modules), it is required not only to stop involved RF sources (with Trigger Enable or External Interlock) but also to stop the production of dark current. Then, I choose to operate the laser shutter of the photo-cathode laser and the RF Gun's modulator when it is required to completely stop the electron beam.

Laser shutters, of all three transfer lines, are controlled through contact interface from a PLC in GP08.

- I asked to vacuum team a review of PLCs for pneumatic valves, to improve contact interface in order to await an enabling signal from both Fast-Interlock systems for each valve. When one of such signals are missing the valve is forced to close.

After the definition of topology and Fast-Interlock and how to interface it with accelerators' sub-systems, I had to designed the hardwired contacts links based on the common standard operating at 24 VDC.

The first requirement for such links were the fail-safe behaviour which guarantee a safe state of critical equipment if the framework (or part of this) fail (e.g. link cable trunked/unplugged, power failure of a Fast-Interlock unit, etc...). These fail-safe links were obtained assuming the interlock logic state "true" with 0 VDC and the state "false" with 24 VDC. In this way: when a device doesn't need to be tripped, the voltage level should be maintained at high voltage; while, if the interlock happens, the state level should go at low voltage.

According to this logic, all the monitored devices gates, interfaced with Fast-Interlock system, were "Normally Open" to understand and produce proper interlock states. If an interlock happen, a Fast-Interlock unit or a monitored device has a power loss, then, the interlock logic state becomes "true" and monitored devices are automatically tripped.

Following the scheme of two independent systems, I splitted monitored devices, when it was possible, between the two Fast-Interlock systems looking for two completely independent systems up to accelerator devices. As described in Table 4.2, to follow this scheme I designed different solutions based on available interfaces of controllers:

- **Direct link** - when the monitored device has got two logic gate with same function that are both wired to the two Fast-Interlock systems.

- **Grouped direct link** - when monitored vacuum devices of the same vacuum region are splitted, and maybe chained, in two group wired directly to Fast-Interlock systems.

- **Splitted link** - when the monitored device allow just one output logic gate, this is wired with two parallel link to the two Fast-Interlock systems.

- **Chained link** - when the monitored device allow just one input logic gate, this is wired with chained link from the two Fast-Interlock systems.

Monitored device	Signal type	Link type	Location	# link
Vacuum gauges	input	grouped direct	GP08 GP04	22 7
Vacuum ion-pumps	input	grouped direct	GP08 GP04 ROOF	7 3 17
Pneumatic valves	output	direct	GP08 GP04	13 5
Laser shutters	output	chained	GP08	3
Personnel Safety (enabling signal)	input	direct	GP08	1
Personnel Safety (dumped electron beam)	output	chained	GP08	1
LLRF (Interlock input)	output	chained	ROOF	13
LLRF (Interlock status)	input	splitted	ROOF	13
Fluid Plant	input	direct	GP08	2
WaveForm Mask	input	splitted	ROOF	13
Modulator (External Interlock)	output	direct	ROOF	13
Modulator (Trigger Enable)	output	chained	ROOF	13
Modulator (Sum Interlock)	input	splitted	ROOF	13

Table 4.2: Hardwired links for the Fast-Interlock system - For each monitored device: the signal type from the Fast-Interlock point-of-view, the required link type, the location inside the accelerator building and the required number of links for each one of the two Fast-Interlock system.

Inside MPS racks in GP08, GP04 and on the ROOF a 24 VDC redundant power supply, able to provide up to 480 W, is interfaced with the Uninterruptible Power Supplies (UPS) network of the facility. Such PSUs supply Fast-Interlock units and the hardwired links. Reference voltage is short-circuited with grounding network of the building.

4.3 Logic Matrix

Once all the requirements of the accelerator are well identified, the technology requested to guarantee reliability and response time are defined, MPS interfaces and equipment are designed, it is possible complete the description of the framework architecture through the Logic Matrix: the list of issues (interlock conditions) handled by the MPS with related actions operated to solve (or monitor) the problem.

Two aspects of the following matrix should be taken in account before reading:

- According to requirements and considering the finite number of contacts available on vacuum gauges controllers, I cannot monitor both thermocouple (TC) and cold-cathode gauges (CC) then the first type, required only for the pre-vacuum, is monitored just from EPICS Supervisor while the Fast-Interlock monitors CC ones. To improve performances of the MPS, I asked to program controllers with two SetPoint for each CC gauge (one for warning and one for alarm pressure level).

- At the end of the matrix, issues of the MPS itself are handled. This because, as request by IEC 61508, not only interfaces should be fail-safe but also the framework itself. It must be able to treat the post-mortem of the whole system (or part of this) leaving always the accelerator in a safe state.

In following pages the matrix in a easy to read version with all the interlock scenario recognized grouped by sub-system and the related procedure.

- High Power RF System

  - **Modulator Internal Interlock**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists;
    3. interlock the LiberaLLRF chassis.

- Low Level RF System
  - **LiberaLLRF Internal Interlock (Reflected Power)**:
    1. close photo-catode laser shutter;
    2. external interlock to the modulator;
    3. inhibit Trigger to Gun's modulator until the issue exists.

- Vacuum System: Accelerating structures regions
  - **Vacuum gauge (CC) out of SetPoint (low-treshold)**:
    1. inhibit Trigger to vacuum region's modulator until the issue exists;
    2. inhibit Trigger to Gun's modulator until the issue exists.
  - **Vacuum gauge (CC) out of SetPoint while LiberaLLRF chassis is ramping (low-treshold)**:
    1. inhibit Trigger to vacuum region's modulator until the issue exists;
    2. inhibit Trigger to Gun's modulator until the issue exists;
    3. vacuum region's LiberaLLRF chassis feedback SetPoint -10%.
  - **Vacuum gauge (CC) out of SetPoint after 3 restoring attemps (low-treshold)**:
    1. close photo-catode laser shutter;
    2. external interlock to vacuum region's modulator;
    3. inhibit Trigger to Gun's modulator until the issue exists.
  - **Ion-pump out of SetPoint (high-treshold)** *or*
  - **Vacuum gauge (CC) out of SetPoint (high-treshold)**:

    1. close photo-catode laser shutter;
    2. external interlock to vacuum region's modulator;
    3. inhibit Trigger to Gun's modulator until the issue exists;
    4. close M1 valve;
    5. dissect the loss of vacuum.

- **WaveForm Mask - RF reflected signal mask broken**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to the modulator until the issue exists.
- **Ion-pump - OFF or in Fault state** *or*
- **Vacuum gauge (CC) - Emission OFF**:
    1. warning on MPS overview.
- **All ion-pumps of the region OFF or in Fault state** *or*
- **All Vacuum gauges (CC) of the region in Emission OFF**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to vacuum region's modulator until the issue exists;
    3. inhibit Trigger to Gun's modulator until the issue exists;
    4. close M1 valve;
    5. dissect the loss of vacuum.
- **Valve - Conflict between Operation-Mode and closed valve**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists.
- **Fast Valve - Valve closed**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists;
    3. close M1 valve;
    4. dissect the loss of vacuum.
- **Fast Valve - Gauge not ready** *or*

  - **Fast Valve - Valve not armed**:
    1. warning on MPS overview.

- Vacuum System: transfer lines regions
  - **Ion-pump out of SetPoint (high-treshold)** *or*
  - **Vacuum gauge (CC) out of SetPoint (high-treshold)**:
    1. close photo-catode laser shutter;
    2. external interlock to vacuum region's modulator;
    3. inhibit Trigger to Gun's modulator until the issue exists;
    4. close M1 valve;
    5. dissect the loss of vacuum.
  - **Ion-pump - OFF or in Fault state** *or*
  - **Vacuum gauge (CC) - Emission OFF**:
    1. warning on MPS overview.
  - **All ion-pumps of the region OFF or in Fault state** *or*
  - **All Vacuum gauges (CC) of the region in Emission OFF**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to vacuum region's modulator until the issue exists;
    3. inhibit Trigger to Gun's modulator until the issue exists;
    4. close M1 valve;
    5. dissect the loss of vacuum.
  - **Valve - Conflict between Operation-Mode and closed valve**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists.
- Vacuum System: RF WaveGuides regions
  - **Ion-pump out of SetPoint (high-treshold)**:
    1. close photo-catode laser shutter;

        2. external interlock to vacuum region’s modulator;
        3. inhibit Trigger to Gun’s modulator until the issue exists.

    - **SF6 pressure switch interlock**:
        1. close photo-catode laser shutter;
        2. inhibit Trigger to Gun’s modulator until the issue exists.
    - **Attenuator Motor error** *or*
    - **Phase Shifter Motor error**:
        1. warning on MPS overview.
    - **all ion-pumps of the channel OFF or in Fault state**:
        1. close photo-catode laser shutter;
        2. inhibit Trigger to Gun’s modulator until the issue exists;
        3. inhibit Trigger to the modulator until the issue exists.

- Vacuum System: Gamma characterization regions
    - **Vacuum gauge (CC) out of SetPoint (high-treshold)** *or*
    - **all Vacuum gauges (CC) of the region in Emission OFF**:
        1. close photo-catode laser shutter;
        2. inhibit Trigger to Gun’s modulator until the issue exists;
        3. close M1 valve;
        4. dissect the loss of vacuum.
    - **Scroll’s Vacuum gauge (TC) out of SetPoint (high-treshold)***or*
    - **Turbo pump - OFF or in fault state** *or*
    - **Scroll pump - OFF or in fault state**:
        1. close photo-catode laser shutter;
        2. dissect the loss of vacuum.
    - **EM valve closed**:
        1. warning on MPS overview.
    - **Valve - Conflict between Operation-Mode and closed valve**:

1. close photo-catode laser shutter;
2. inhibit Trigger to Gun's modulator until the issue exists.

- Vacuum System: Laser IP regions
  - **Vacuum gauge out of SetPoint (high-treshold)** *or*
  - **all Vacuum gauges (CC) of the region in Emission OFF**:
    1. close photo-catode laser shutter;
    2. close laser shutter until the issue exists;
    3. inhibit Trigger to Gun's modulator until the issue exists;
    4. close M1 valve;
    5. dissect the loss of vacuum.
  - **Scroll's Vacuum gauge (TC) out of SetPoint (high-treshold)** *or*
  - **Turbo pump - OFF or in fault state** *or*
  - **Scroll pump - OFF or in fault state**:
    1. close photo-catode laser shutter;
    2. close laser shutter until the issue exists;
    3. close M1 valve;
    4. dissect the loss of vacuum.
  - **EM valve closed**:
    1. warning on MPS overview.
  - **Valve - Conflict between Operation-Mode and closed valve**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists.
- Magnets
  - **Dipole - unexpected magnetic field from the Hall probe** $(> 5\%)$ *or*
  - **Dipole - PSU in Fault state** *or*
  - **Dipole - Module flow switch tripped** *or*

  - **Dipole - Thermo switch tripped** *or*
  - **Dipole - PSU out of current SetPoint when idle** ($> 5\%$):
    1. close photo-catode laser shutter;
    2. inhibit Trigger to all modulators until the issue exists.
  - **Quadrupole - PSU in Fault state** *or*
  - **Quadrupole - Module flow switch tripped** *or*
  - **Quadrupole - Thermo switch tripped** *or*
  - **Corrector - PSU in Fault state** *or*
  - **Corrector - Module flow switch tripped** *or*
  - **Corrector - Thermo switch tripped**:
    1. warning on MPS overview.

- Cooling System
  - **Fluid-Plant - Primary pumping unit - Temperature out of SetPoint** ($> 10\%$) *or*
  - **Fluid-Plant - Magnets pumping circuit - Flow switch alarm** *or*
  - **Fluid-Plant - RF pumping circuit - Flow switch alarm** *or*
  - **Fluid-Plant - Laser pumping circuit - Flow switch alarm** *or*
  - **Fluid-Plant - Chiller pumping circuit - Flow switch alarm** *or*
  - **Fluid-Plant - Conductivity after resin treatment out of SetPoint** ($> 10\%$):
    1. warning on MPS overview.
  - **Fluid-Plant PLC - Primary pumping unit - low pressure for more then 3 minute** *or*
  - **Fluid-Plant PLC - Temperature or Flow switch interlock**:
    1. close all laser shutter;
    2. external interlock to all modulators;
    3. interlock all LiberaLLRF chassis.

  - **Chiller - not Running** *or*
  - **Chiller - SetPoint and Discarge Temp. Mismatch** ($> 10\%$):
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists;
    3. inhibit Trigger to the modulator until the issue exists.
  - **Chiller - Temperature Sensor failure** *or*
  - **Chiller - Flow rate too low** *or*
  - **Chiller - Chiller - Low level in Tank**:
    1. warning on MPS overview.

- Personnel Safety System
  - **AB2 access mode requested**:
    1. close all laser shutter;
    2. external interlock to HEL modulators;
    3. interlock HEL LiberaLLRF chassis;
    4. insert both beam stoppers;
    5. enable BeamDumped signal to PPS with no beam loss.
  - **Beam Stopper - mismatch between position SetPoint and readback**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists.
  - **Enabling signal removed**:
    1. close all laser shutter;
    2. external interlock to all modulators;
    3. interlock all LiberaLLRF chassis.

- Control System
  - **IOC health failure**:
    1. warning on MPS overview.

- Synchronization
  - **Synchronization link amplifier active without signal**:
    1. switch-off the link amplifier.
- Electron beam diagnostics
  - **Beam Loss Monitors - unexpected loss**:
    1. close photo-catode laser shutter;
    2. inhibit Trigger to Gun's modulator until the issue exists.
  - **Fast Current Transformer - unexpected loss (difference $> 10\%$)** *or*
  - **Beam Screen Motor error**:
    1. warning on MPS overview.
  - **Beam Screen Motor is running**:
    1. close photo-catode laser shutter until a screen is moving;
    2. inhibit Trigger to Gun's modulator until the issue exists.
- Machine Protection System
  - **Fast-Interlock PostMortem - First or Second system fail (missing heartbeat)**:
    1. close all laser shutter;
    2. inhibit Trigger to all modulators until the issue exists;
    3. close M1 valve;
  - **Fast-Interlock PostMortem - all systems fail (missing heartbeat)**:
    1. close all laser shutter;
    2. external interlock to all modulators;
    3. inhibit Trigger to all modulators until the issue exists;
    4. interlock all LiberaLLRF chassis;
    5. close all valves.
  - **Beam Loss Monitors - system fail (missing heartbeat)** *or*

- **WaveForm Mask - system fail (missing heartbeat)**:
  1. close photo-catode laser shutter;
  2. inhibit Trigger to Gun's modulator until the issue exists.
- **Supervisor - First/Aux IOC fail (missing heartbeat)**:
  1. close all laser shutter;
  2. external interlock to all modulators;
  3. interlock all LiberaLLRF chassis;
  4. close all valves.
- **Fast-Interlock system - dummy signal from diagnostic probe**:
  1. close all laser shutter;
  2. external interlock to all modulators;
  3. inhibit Trigger to all modulators until the issue exists;
  4. interlock all LiberaLLRF chassis;
  5. close all valves;
  6. insert both beam stoppers.
- **Fast-Interlock system - all monitored vacuum's devices in a region/channel bypassed** *or*
- **Fast-Interlock system - PSU self-diagnostic issue**:
  1. warning on MPS overview.

CHAPTER

5 Software and Hardware Design

Content

5.1 Fast-Interlock system design 95

WaveForm mask real-time interlock design 104

5.2 EPICS-based Supervisor design 109

5.3 Beam Loss Monitors 111

Cherenkov Beam Loss Position Monitor 112

Hall Probes 117

Beam Position and Current Monitors 121

IP Trajectory feedback 121

5.4 Vacuum design improvements 124

The philosophy behind the MPS is provide a fully automated system able to operate accelerator's equipments independently by operator activities, without affect accelerator up-time. In order to realize this sort of "ghost-operator", all software has been developed to perform un-latched operation: equipment is tripped just when an interlock condition occurs and automatically released when the condition doesn't exists anymore.

Thanks to a proper setup of critical systems that I performed, if a critical issue happens, it is the equipment itself to provide latched interlocks (which require operator intervention to restore normal condition). For example: the MPS can close a pneumatic valve, when a vacuum leak is detected, but only operators can reopen it; the MPS can trigger the modulator's external interlock, to completely stop the RF source, but only operators can restore it.

In this way I developed a Machine Protection System able to emulate the knowledge of an operator moreover capable to operate the accelerator in real-time shot-to-shot in order to minimize or avoid critical issues.

In this chapter I will focus on the software and hardware design and related bench-testing which made up my MPS. For each system of the MPS framework, expected and/or measured performances will be reported.

5.1 Fast-Interlock system design

As anticipated in the previous chapter, this system is based on distributed real-time FPGA units with a chain of master and slave units [48]. This system has stringent requirements on response time and reliability. To obtain the required response time performances, it is needed that the system identifies an issue and operates a solution before the next RF shot (then faster than 10 ms). The high-reliability of the system should be supported by the hardware involved in the Fast-Interlock system and, as anticipated, by implementing a redundancy model and reliable links with monitored devices.

Hardware Design

I choose to involve the Field-Programmable Gate Array (FPGA) because it is able to run software faster than a millisecond, to provide the proper reliability and to allow the reconfiguration of hardwired signal through the code. This technology is made of array of programmable logic blocks, thanks to a reconfigurable interconnects layer, this logic block could be programmed to perform simple logic operation (e.g. AND, OR, XOR, etc...) up to sophisticated digital operations. This technology take advantage of several features:

- **Performance** - Taking advantage of hardware parallelism, FPGAs accomplish more digital operations per clock cycle. Monitoring inputs and outputs at the hardware level provides faster response times and specialized functionality to closely match application requirements. A system designed to operate at low level with digital signal it is, basically, ready to be interfaced with hardwired network links.

- **Reliability** - While software tools provide the programming environment, FPGA circuitry is truly a “hard” implementation of program execution. Processor-based systems often involve several layers of abstraction to help schedule tasks and share resources among multiple processes. The driver layer controls hardware resources and the OS manages memory and processor bandwidth. For any given processor core, only one instruction can be executed at a time, and processor-based systems are continually at risk of time-critical tasks pre-empting one another. FPGAs, which do not use OSs, minimize reliability concerns with true parallel execution and deterministic hardware dedicated to every task.

- **Cost** - For custom chips, it should be await time for the prototyping and assembly costs must be reduced with mass production. FPGA production means that the hardware is the same for any customer, then fabrication costs are implicitly reduced compared to custom chip. In addition to this, when system requirements change, the cost of making changes to FPGA designs is negligible when compared to the large expense of respinning a custum chip.

I choose the CompactRIO platform (Compact Riconfigurable Input/Output) manufatured by National Instruments (NI) [51] which allows an infrastructure able to integrate FPGA, collect data from distributed units through etherCAT [50] network and from the Supervisor (because not all the interlock are triggered by hardwired links).

CompactRIO is reconfigurable embedded system that contains three components: a processor running an embedded controller with real-time operating system, an FPGA and interchangeable I/O modules. Thanks to LabView Real-

Time module installed on the controller is possible monitor the execution of the FPGA and exchange data with it.

For the Fast-Interlock (Fast-ILK) system, as in Figure 5.1, I designed one powerful master unit (both for controller and FPGA) and two slave unit with an entry-level performances. In this way, slave units just have to collect data from I/O module with the performance and reliability of an FPGA while the real-time controller monitors the FPGA, packing data and streaming it through etherCAT network. All smart operations are performed from the master unit use the controller for two main purposes: communicate with the etherCAT network and with the EPICS data network. Data from Fast-ILK slave units and from the MPS Supervisor is pushed from controller to FPGA where software monitor the accelerator status tripping or not interlock according to the Logic Matrix. The FPGA of master unit is also equipped with its own I/O module to local links. Thanks to the real-time OS on controller, any choice of the FPGA is streamed back to the etherCAT network to update output gate on slave units and to the EPICS network to show the status of Fast-ILK on the MPS overview (in an operator interface in control room).

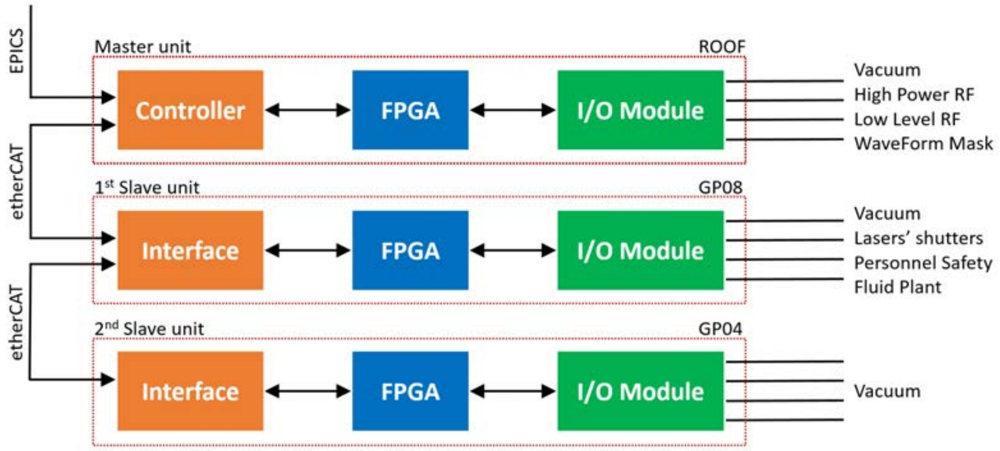

Figure 5.1: Fast-Interlock system - Hardware design.

For the master unit I chose the NI cRIO-9039 crate and for slave units the NI-9144 crate. The first one is equipped with Kintex-7 7K325T FPGA while second ones with a Spartan-3 2M FPGA both manufactured by Xilinx. While in slave units there are just an interface to let real-time deterministic communication of FPGAs through the etherCAT protocol, the master unit has a controller with Intel Atom Quad-Core E3845 processor, 2 GB of memory and 16 GB of SSD disk with NI Linux Real-Time (64-bit) installed. Both kind of crates are able to host up 8 I/O modules. As anticipated in the Architecture chapter, all the hardware is duplicated to increase the global reliability of the Fast-ILK system.

I/O Modules depends by links type, as already listed in the previous chapter in Table 4.2. All modules interpret $0-24$ VDC signals from hardwired network as Digital Inputs (DI) sinked or sourced, as sourcing Digital Outputs (DO) for direct links and as Solid State Relays (SSR) for chained links; the only exception is the TTL module used as DI to collect signals from WaveForm Mask. In the following Table 5.1 Fast-ILK I/O modules are reported grouped by unit.

I/O Module type	**# in Master [ROOF]**	**# in 1^{st} Slave [GP08]**	**# in 2^{nd} Slave [GP04]**
NI-9425 32 ch. Sinking DI	2	1	1
NI-9426 32 ch. Sourcing DI		1	1
NI-9476 32 ch. Sourcing DO	1	1	1
NI-9403 32 ch. TTL DIO	1		
NI-9485 8 ch. SSR	4	1	

Table 5.1: Fast-ILK I/O Modules - For each type of I/O Modules the related number connected into master and slave units.

The last hardware feature that I'd like focus is the etherCAT protocol [50] for communication between master and slave units. Compared to TCP protocol, involved in common ethernet network, the etherCAT is able to guarantee real-time and deterministic data streaming.

TCP is based on query between clients connected to a server. When the server establish the connection with the client, a data package is sent. The receiver read the header chunk, at the beginning of the package, to discover the package size then maintain open the connection until the whole package is received. When different units have to exchange several packages, queries are pooled in order to allow that a connection is closed before starting a new one.

While TCP is widely used for general purpose (e.g. internet and intranet networks), in Automation field, data exchanged is commonly the same data streamed periodically. In etherCAT protocol a connection is established between a master and several chained slave units. In first instance, clocks of each slave unit are synchronized to master unit's clock with a jitter less than 1 μs. Then the master unit queries to slave units the size of data to be read and write that have to be exchanged each time; such size is used to start the streaming of a long package big enough to contain all slave units data. Such package continously run from master to slaves and back to master in a closed loop; each slave unit have its own fixed allocation space inside the package where the data must be write and/or read.

The pooling and the variable size of TCP packages cause network latencies of milliseconds. EtherCAT clients have just to wait the arrival of the long shared package with pre-defined memory allocation, without any pooling which allow to reduce latencies to the order of nanoseconds; in addition to this feature, the synchronization, between master and slaves, guarantees also the determinism of data exchanged.

In Fast-ILK system a private etherCAT link goes from master to first slave unit then from first to second slave unit. Thanks to the protocol performances, communication between distributed FPGAs guarantees anyway the real-time requirements of the system.

Software Design

Basically the idea of Fast-ILK software is that all input from slave unit FPGAs (or Supervisor) are collected by the master unit controller; transfered to the FPGA and matched with the coded Logic Matrix then, if an interlock condition are satisfied, the related output is tripped to stop the accelerator equipment. The involved interlock condition is highlighted back to the controller in the EPICS network up to the MPS overview (shown in control room).

Also if usually FPGA should be programmed in VHDL language, thanks to the LabView FPGA and Real-time modules, it has been possible to program both controller and FPGAs code with wiring diagram while Labview provide the conversion to VHDL for the code compilation on FPGAs. This approach usually doesn't guarantee the best performances of the FPGA program but several tricks were followed to optimize the code (e.g. best use of FPGA shared memory, use just logic operator, etc...).

The first feature to implement with the code was the standardisation of data streaming. All the interlock conditions of the Logic Matrix are paired with a univocal numeric code. Digital Input signals from I/O Modules are grouped in boolean arrays, according to device type (e.g. vacuum gauges, ion-pumps, etc...), then each array is converted to a word. Vice versa for Digital Output signals, from a word are extracted boolean values.

This approach, when used in slave units, drastically reduce the code and simplify the FPGA workload, as in Figure 5.2: input variable are forwarded to the master unit controller, output variable (read by controller) are applied to output gate of I/O Modules.

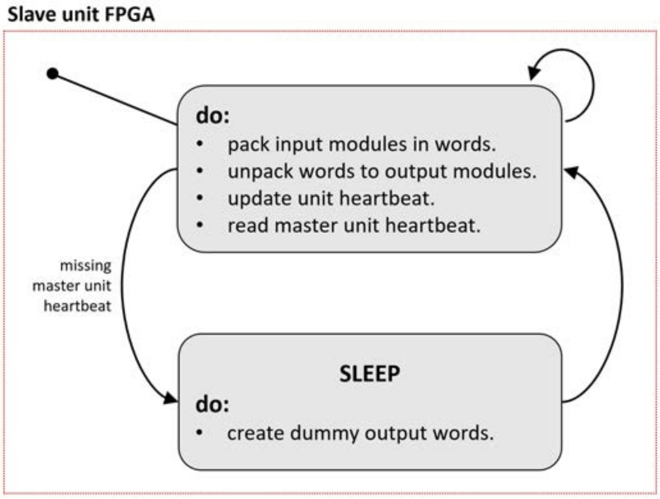
Slave unit FPGA
do:
• pack input modules in words.
• unpack words to output modules.
• update unit heartbeat.
• read master unit heartbeat.
missing master unit heartbeat
SLEEP
do:
• create dummy output words.

Figure 5.2: Fast-Interlock system - Slave units state-chart.

Inside the master unit controller, two parallel loop run for fast and slow operation, as shown in Figure 5.3. The fast loop operates at 10 kHz (in real-time with the FPGA process) as bridge between the etherCAT network and the master FPGA to exchange input and output words; this loop is also in charge of the incremental update of tripped interlock list from the master FPGA to the EPICS network (for logging). The slow loop runs at 1 Hz monitoring Fast-ILK's watchdogs; it is in charge of communication with the EPICS network to receive interlock trigger from the Supervisor and the list of bypassed interlock condition by the operator interface.

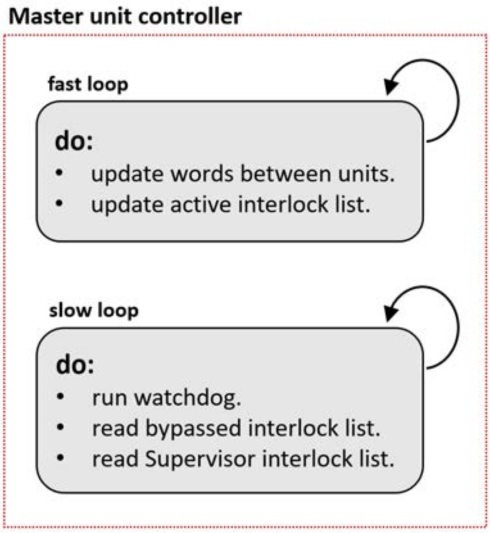
Master unit controller
fast loop
do:
• update words between units.
• update active interlock list.
slow loop
do:
• run watchdog.
• read bypassed interlock list.
• read Supervisor interlock list.

Figure 5.3: Fast-Interlock system - Master unit controller state-chart.

The master FPGA, as shown in Figure 5.4, performs a state-machine with a "identify-solve-execute" loop or goes in sleep-mode to guarantee the fail-safe of the software:

- **Identify** - All input words from each unit go through the coded Logic Matrix to produce the list of interlock conditions violeted.

- **Solve** - The list from previous state and the one from Supervisor (through the controller) are parsed to define logic state for output modules of each unit. The list of occurring interlocks is filled and sent back to controller for the MPS overview. Each interlock condition is compared with the bypass list (that always come from the controller) in order to avoid the tripping of equipment.

- **Execute** - Logic state for each output gate of the Fast-ILK system is directly applied to I/O Modules of master unit and sent through controller (and ethrCAT netwrok) to be applied on I/O Modules of slave units.

- **Sleep** - This state is designed just for fail-safe (or maintenance) of the Fast-ILK system. If the watchdog on controller detect an integrity issue in the Fast-ILK system, the state-machine is trapped in this state. It is just a dummy version of "Identify" one, in which all the output gates are set to trip the equipment. It is possible to exit from this state fixing the integrity issue and refreshing of the system from MPS overview. For the maintenance of the system, thanks to a physical button on the master unit, it is possible send/free the state-machine to/from this state.

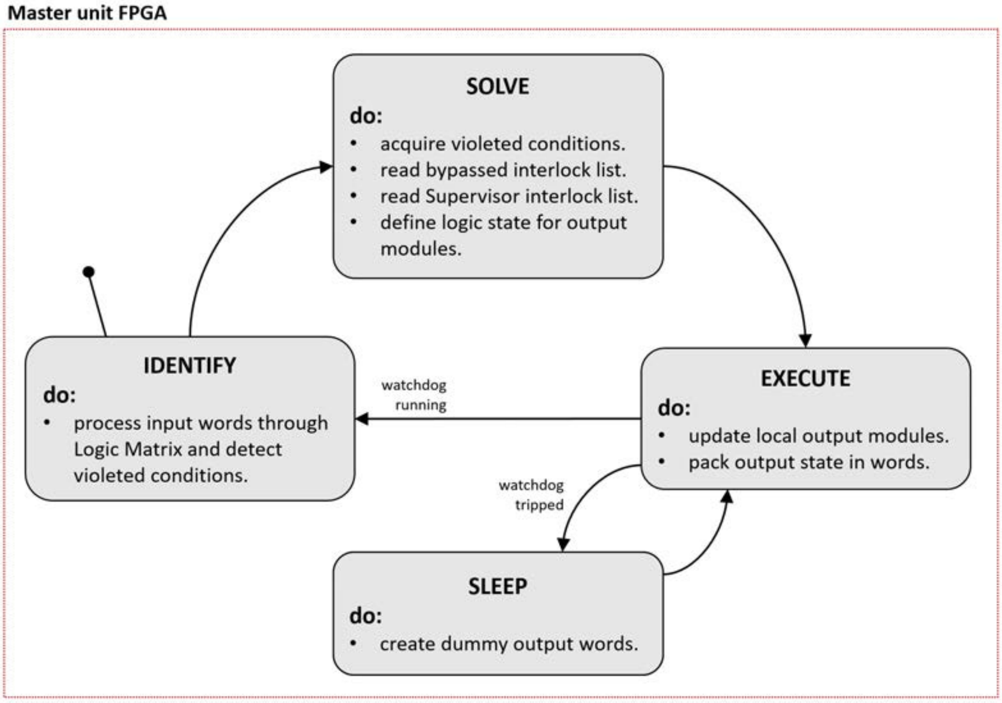
Master unit FPGA
SOLVE
do:
• acquire violeted conditions.
• read bypassed interlock list.
• read Supervisor interlock list.
• define logic state for output modules.
IDENTIFY
do:
• process input words through Logic Matrix and detect violeted conditions.
watchdog running
EXECUTE
do:
• update local output modules.
• pack output state in words.
watchdog tripped
SLEEP
do:
• create dummy output words.

Figure 5.4: Fast-Interlock system - Master unit FPGA state-chart.

As anticipated, in order to guarantee the fail-safe of the system, a watchdog system has been developed. In the slow loop inside the controller of the master unit, a watchdog monitors heartbeat signals from the 3 FPGAs to verify the integrity of the Fast-ILK system. If the FPGA software is not running, the etherCAT network broken or there are PSU units fault, then the integrity of system is violated.

The watchdog sends also an heartbeat from master unit controller to slave units. In this way if part of the Fast-ILK is isolated by the master controller (then unable to reach the “sleep” state), it can detect the missing heartbeat and reach by itself the “sleep” state tripping all the equipment.

In order to help during a visual inspection of the hardware, a led over master and slave units shows the current status of the FPGA program: if it blinks, the Fast-ILK is running; if it switched on, the Fast-ILK is in “sleep” mode.

Performances

Several tests were performed to verify behaviour of the system on long-term stability and on-demand availability.

Once coded the Logic Matrix and finalized the communication protocol between units of the Fast-ILK, I leaved the system running totally unplugged by terminals for 90 days. At the end of the test the system was still operating and no issue or “sleep” state were assumed in this period.

In order to measure performances of the Fast-ILK, I benchmarked the system in the more time-consuming scenario: triggering an interlock signals from an input gate of a slave unit to verify how much time later is triggered the interlock on the output gate of another slave unit. In this way I tested, once togheter, the execution time of: slave unit, the etherCAT network, the FPGA of the master unit and the propagation to the slave unit to show the output interlock signal. The result of this test repeated several times show an average execution time of about 200 μs.

I performed also test on accelerator’s equipment in order to verify how much time is required by the device to be tripped after the arrival of the interlock signal. While this execution time is negligible for ScandiNova modulators and LiberaLLRF crates which require about 10 μs, laser shutters need about 10 ms and Omron PLCs need 25 ms to command to close pneumatic valves which require 1 s to dissect vacuum regions.

WaveForm mask real-time interlock design

The WevaForm Mask system [49] has been developed to introduce a common tool like the waveform mask analysis on RF signal hardwired with Fast-ILK to trip RF source in real-time within the next RF shot.

The choice to develop a pulse-to-pulse interlock system resides in the intrinsic slow response time of a vacuum system, which is of the order of hundreds of milliseconds from the breakdown occurrence to the interlock signal delivery to the RF source. Being 10 ms the maximum delay acceptable, an effective real-time interlock system has been developed digitizing the reflected power signal picked up at the RF Gun input port and down-converted with a schottky diode.

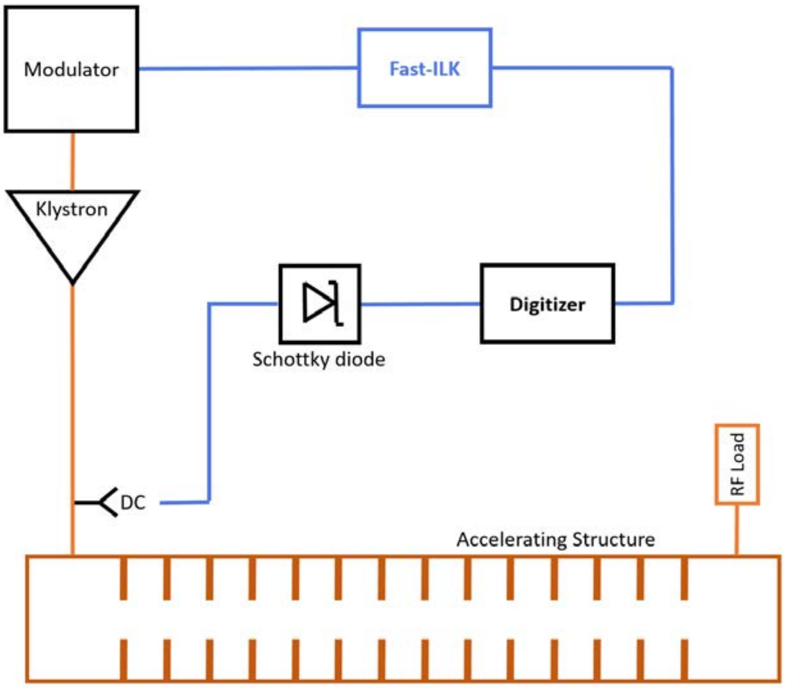

Figure 5.5: Fast-Interlock system - WaveForm Mask design.

As report in Figure 5.5, main elements of the system are a schottky diode, a server equipped with a digitizer and an hardwired feedback to the RF source. In this interlock system the RF signal from a directional coupler (DC) is collected by a peak detector (the schottky diode) which produce a signal acquired by digitizer. Here the RF signal shape is analyzed with waveform mask algorithm to trigger or not the Fast-ILK to stop the RF source.

This system will be involved during the conditioning of all accelerating structures and, during the whole commissioning of the facility, to protect the RF Gun. About the first task, it will monitor RF reflected signals while, for the second one, it will monitor RF reflected signal and the probe just inside the gun.

Hardware Design

The server for the WaveForm Mask is equipped with high-performance digitizer to solve carefully a short signal, like the RF one, that in this case is 1.5 μs long.

I choose for this purpose the WaveCatcher [52] (8 channels, 3.2 $\frac{GS}{s}$, 12 bit sample depth, 4 kb of memory and 500 MHz of bandwidth) connected through USB interface to the server. Thanks to this digitizer it possible sample a RF signal of the facility with up to 4800 samples.

The server it is equipped with a DAQ from National Instruments PCIe-6341 able to produce TTL signals that are hardwired to the Master unit of Fast-ILK system.

Software Design

Thanks to LabView driver which I developed for the WaveCatcher, I have been able to create a simple software able to acquire waveforms, analyze them, trigger the Fast-ILK through the NI DAQ and send data about detected breakdowns over the EPICS network. As in Figure 5.6, this is the WaveForm Mask algorithm performed in real-time:

1. During the initialization, the algorithm acquires the waveform to produce two arrays. The first one is the waveform plus a constant while the second is the waveform minus a constant. The difference between such constants identifies the region of tolerance (the so called mask).

2. For each acquired waveform, the algorithm checks if each sample is included in the mask region.

3. If so, the waveform is assumed “healthy” and no interlock is generated. The actual waveform is used as reference to update the region of tolerance and the loop restarts from previous point.

4. If not, the mask it is “broken”, then the software collects a screenshot of the waveform and changes the TTL Digital Output available on the DAQ inside the server. This interlock signal is propagated through the Fast-ILK system for 30 seconds.

Through the diode calibration all waveforms are converted to show RF signals power.

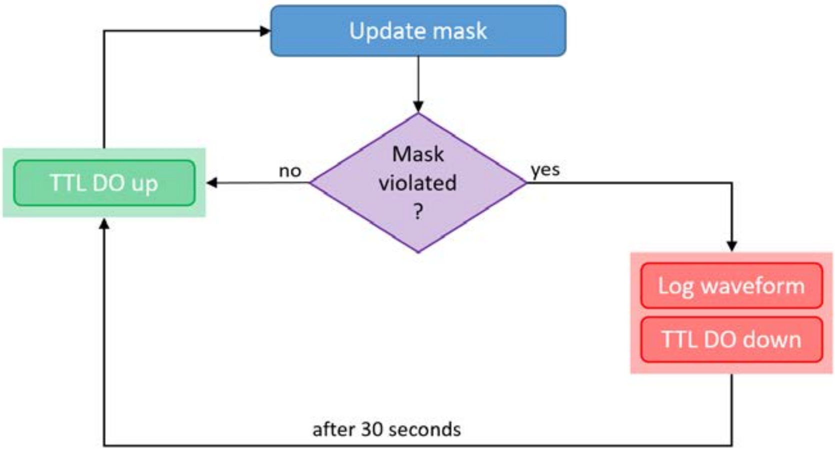

Figure 5.6: Fast-Interlock system - WaveForm Mask algorithm flow-chart.

Performances

I performed several tests with a 100 Hz source as trigger and waveforms of 1.5 μs to check if the system match the real-time requirement.

Thanks to the LabView software, sampling performances has been monitorated in order to verify the real-time capability of all the 8 channels (sampled simultaneously) on the WaveCathcer due to the possible use of such system for the conditioning of several structures in parallel.

From this tests results that WaveForm Mask system is able to treat the 8 channels in real-time up to 800 Hz.

As reported below, the proof of principle to verify the functionality of the algorithm were performed during the conditioning of the ELI-NP-GBS RF Gun.

Prototype test during RF Gun conditioning at HELSA

During December 2015, the RF Gun [53] was conditioned at the Bonn University were the HELSA facility is located.

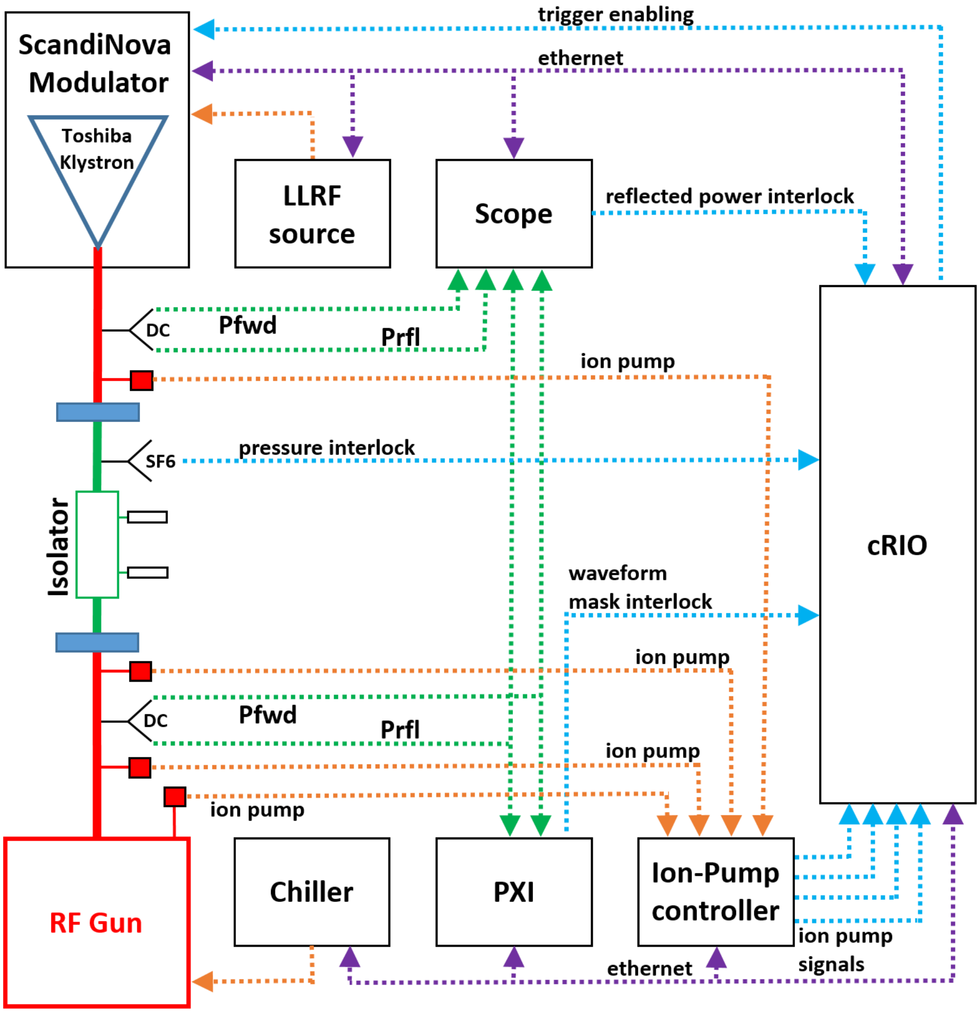

Figure 5.7: Fast-Interlock system - WaveForm Mask hardware design during ELI-NP-GBS RF Gun conditioning at HELSA.

The setup arranged, as reported in Figure 5.7, was very near to real one that will be installed in Magurele: a ScandiNova S-band modulator with a Toshiba klystron; a RF waveguide channel with DCs and an isolator in SF6; a chiller for thermal stabilization of the gun; a NI cRIO to collect data from ion-pumps and from an oscilloscope operating as peak interlock on RF signal. In this context I integrated a NI PXI unit interfacing it with RF reflected signal in entrance to the RF Gun (from the DC) and with the cRIO to propagate the waveform mask interlock.

In this prototype I used as digitizer the NI PXI-5154 (2 channels, 2 $\frac{GS}{s}$, 8 bit sample depth, 32 Mb of memory and 1 GHz of bandwidth).

Nevertheless, thanks to the waveform mask algorithm, it has been possible to detect about 550 breakdowns that were not detected by the conventional vacuum interlock method, an example is shown in Figure 5.8. Thus, such system allowed to carry out a safer conditioning both in terms of RF source and RF Gun operation.

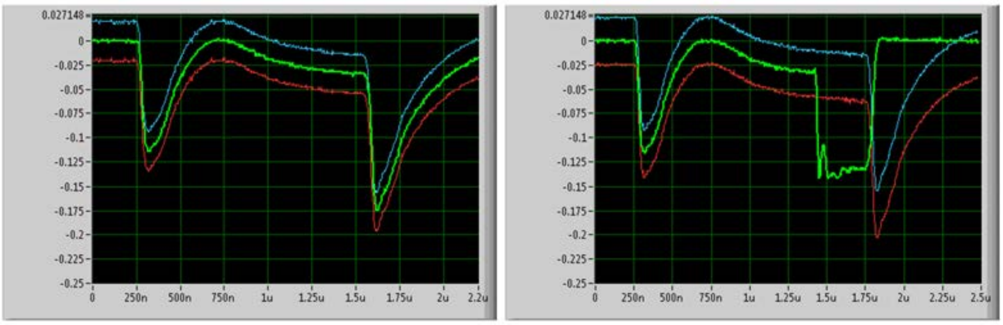

Figure 5.8: WaveForm Mask - Algorithm functionality example on RF reflected signal: on left, an “healthy” signal; on right, the mask broken when a breakdown happens. Green curve is the current waveform while the blue and red curves identify the region of tolerance.

Thanks to this test the algorithm was certified reliable by RF experts and evaluated for the commissioning of the ELI-NP-GBS accelerator.

Also if this setup worked properly, I choose to leave the NI environment due to the high cost of the equipment. Also if the not negligible cost of the PXI crate is ignored, the digitizer cost of 7500 $\frac{€}{channel}$ has been substitute with a WaveCather, with much channels and resolution, which costs just 400 $\frac{€}{channel}$.

5.2 EPICS-based Supervisor design

This system has been developed as EPICS IOC servers devoted to all interlock conditions, of the Logic Matrix, which don't have to react within the 10 ms. For this reason the system is based on simple servers located in control room.

Hardware Design

The Supervisor is based on two PowerEdge R330 manufatured by DELL equipped with an Intel Xeon E3-1220 3.0 GHz, 16 GB of RAM, 1 TB of hard disk. I choose this hardware in order to follow the hardware of the control system and optimize spare parts.

As in Figure 5.9, these servers are plugged to the EPICS data network of the building through 1 $\frac{Gbit}{s}$ ethernet port which allow the interface between Supervisor and all other monitored systems.

The required reliability is obtained through the hot-standy redundancy model in which one system is operating and the other one is passive with a watchdog (which monitors faults of first unit to activate the second one).

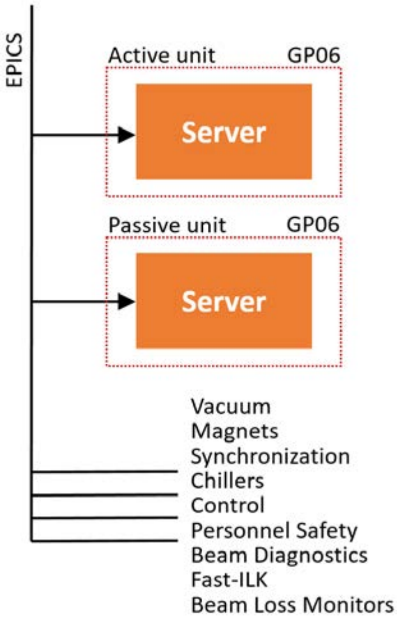

Figure 5.9: EPICS-based Supervisor - Hardware design.

Software Design

I developed the Supervisor as an EPICS client, continously running, to monitor Public Variables (PV) over the EPICS data network. All the interlock conditions from Logic Matrix which don't require the real-time but just the on-line intervention are provided by such client.

Supervisor operation are basically of two type: in first one, it monitors and operates through EPICS PVs from accelerator sub-systems; in second type, PVs are monitored but solutions are operated triggering the Fast-ILK system with dedicated words.

As part of the Logic Matrix, the Supervisor follows the heartbeat from the whole MPS (both Fast-ILK systems, WaveForm Mask and Beam Loss Monitors servers signaling to the MPS overview in control room the proper integrity of the whole MPS system.

The state-machine operated by Supervisor, as in Figure 5.10, is quite similar to the one running on the Fast-ILK system:

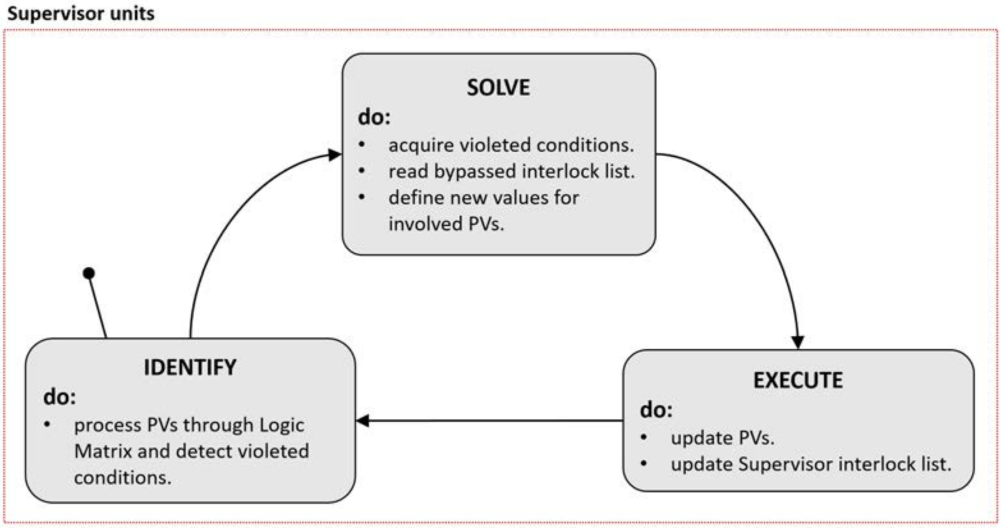
Supervisor units
SOLVE
do:
• acquire violeted conditions.
• read bypassed interlock list.
• define new values for involved PVs.
IDENTIFY
do:
• process PVs through Logic Matrix and detect violeted conditions.
EXECUTE
do:
• update PVs.
• update Supervisor interlock list.

Figure 5.10: EPICS-based Supervisor state-chart.

- **Identify** - PVs from involved system are processed through the coded Logic Matrix to produce the list of interlock conditions violeted.

- **Solve** - The list from previous state are parsed to define new values for involved PVs. The list of occurring interlocks is filled. Each interlock condition is compared with the bypass list in order to avoid the tripping of equipment.

- **Execute** - New values for each PV are updated to operate accelerator's systems. For interlock condition which required Fast-ILK intervention, the list of Supervisor interlocks is arranged and transmitted to Fast-ILK controller as EPICS PV.

Performances

The Supervisor requirements request just the on-line monitoring of accelerator's systems over EPICS control system. For this reason, to evaluate performances of the Supervisor, I considered that EPICS framework can refresh PVs with a maximum refresh rate of 10 Hz while I ignored the latency of the data network that is estimated of about 1.5 ms then negligible compared to the 100 ms of the control system framework.

Benchmark on software has been carried out together for stability and performances. Software run for 90 days with dummy PVs to simulate random interlocks; no error were reported and the average execution time results of about 2 ms.

5.3 Beam Loss Monitors

This equipments of the MPS are required to monitor the electron and gamma beam transport of the accelerator. For these reasons, I developed four Beam Loss Monitors (BLM) system. They could be assumed of two types. The first two are distributed BLMs with dedicated equipment placed along the whole accelerator. The last two BLMs are based on software algorithms which operate collecting data from accelerator's equipment.

About the first two BLMs reported, the design requires the installation of hardware nearby vacuum chambers of the accelerator. Before design such systems I had to investigate if take in account the radiation damage effect. This threshold effect requires, for semiconductor electronics devices, to reach 10 Gy to cause injury to the equipment. According to Radiation Protection team, for an electron beam of 840 MeV (maximum electron beam energy according to Technical Report of the accelerator) and an estimated up-time of 3000 $\frac{hour}{year}$, we reach a dose of about 0.12 Gy. The factor about two of difference were enough to let me ignore radiation damage effect for my equipment.

Cherenkov Beam Loss Position Monitor

The first tool that I designed to monitor the electron beam transport is a BLM able to localize the position of the loss. From the many detectors available for this purpose, taking in account the electron beam energy, I choose to involve Cherenkov detector being a good compromise between performances and costs.

Optical fibers, placed nearby beam pipes, drive cherenkov light produced by the interaction of electrons escaped by the pipe (or electrons shower). The interaction of charged particle with the core of the fiber produce the cherenkov light. Computing the time-of-flight of the light signal acquired by photon-multipliers (or solid-state detectors), placed upstream to electron beam direction, allow to localize the where the electron beam loss happened.

The main issue of this type of detector, applied on electron linac, is the transport along the whole accelerator of the dark current (accessory electrons produced by photo-cathode with energy distribution between the desired electron beam energy and about zero). Until the beam is not bended, dark current is transported up to the end of the linac. Indeed, in storage rings this problem is negligible due to the continous bending of the beam.

Then each time that the electron beam bends, due the action of magnetic elements, dark current dispersion cause a lot of cherenkov light production. This undesired noise increase the background, up to the complete saturation of the electronics, then such effect completely hide the interesting signal of the electron beam loss.

This problem is usually solved involving this kind of BLM for short section of the accelerator, after bending magnets (which allow the transport just of electrons with proper beam energy) and where is very important localize beam losses. An example of this design, is the cherenkov BLM of FERMI accelerator [54] placed on FEL lines in which it involves Multi-Pixel Photon Counter (MPPC) to acquire fiber signals. Many other similar solution are available for electron linac like at XFEL and SACLA [55, 56].

In my cherenkov BLM, I found a possible solution for the dark current issue "splitting" the accelerator in several short trunks. The splitting strategy assumed that for each segment: it must be long at maximum 25 m; when the beam is heavily bended by a dipole, a it must finish just before and new one must start just after. In this way the effect of dark current is minimized and becames negligible for trunks after dipoles.

I choose to review the design used at FERMI due the specification of their solid-state detectors (like MPPCs) which, compared to photo-multipliers, allow to: avoid the necessity of high-voltage power supply, ignore magnetic interferences, adopt compact design and reduce costs. All these features are much more important when, like in this case, the BLM is distributed then it is made of several detectors.

Hardware Design

As reported in the BLM design of FERMI, I used optical fiber with high-OH silica core of 300 μm, two cladding of 330 μm and 370 μm, black nylon jacket of 850 μm, refractive index $n = 1.48$ and numerical aperture (NA) of 0.22.

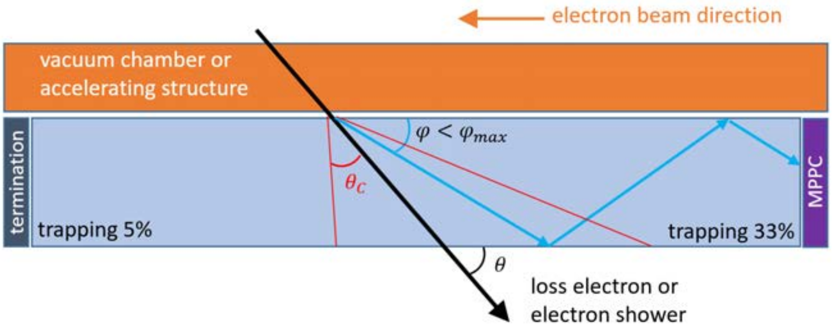

Figure 5.11: Black arrow show primary electrons or electrons shower losses which cross the fiber with a θ angle. When the cherenkov light (blue arrow) with θ_C semi-cone angle is trapped inside fiber this could reach: upstream the MPPC and downstream the fiber termination cut to minimize reflection and avoid echos.

With optical fibers specifications, I calculated the total reflection limit angle as in Formula 5.1.

$$\varphi < \varphi_{MAX} = \sin^{-1}\frac{NA}{n} = 8.4^\circ \tag{5.1}$$

According to cherenkov light theory, the energy threshold and the range for the cone semi-angle were evaluated as in Formula 5.2, 5.3 and 5.4.

$$\cos\theta_C(\lambda) = \frac{1}{\beta \cdot n(\lambda)} \tag{5.2}$$

$$\cos 0 = \frac{1}{\beta \cdot n(\lambda)} \qquad \Longrightarrow \qquad \beta_{th} = \frac{1}{n} \approx 0.7 \tag{5.3}$$

$$\theta_C = \begin{cases} 17^\circ & if\,\beta = 0.7 \\ 48^\circ & if\,\beta = 1 \end{cases} \tag{5.4}$$

Then I could estimate the number of cherenkov photons (N) produced by a single charged particle as in equation 5.5 where the cherenkov photons wavelength (λ) is in the range between 400 – 500 nm.

$$\frac{dN}{dx\,d\lambda} = \frac{2\pi\alpha}{\lambda^2}\sin^2\theta_C = \begin{cases} 2\,\frac{ph}{mm} & if\,\theta_C = 17^\circ \\ 13\,\frac{ph}{mm} & if\,\theta_C = 48^\circ \end{cases} \tag{5.5}$$

The result of Formula 5.5 show a number of expected photons not far from the design at FERMI [54]. According to this data had been possible use the same conditioning electronics to acquire signals from optical fibers: MPPCs, manufactured by Hamamatsu, with 400 pixels of 50 μm, that thanks to several avalanche photo-diodes in parallel for each pixel, guarantee a rise time of 100 ps and a gain of $10^5 - 10^6$ near to photo-multiplier one.

With these data, I defined topology of different optical fibers trunks by splitting the accelerator in 9 trunks, as reported in Figure 5.12 and in Table 5.2.

Upstream to each fiber, on accelerator girders, an MPPC (with its electronics) convert the optical signal in electrical which is acquired with a digitizer. Thanks

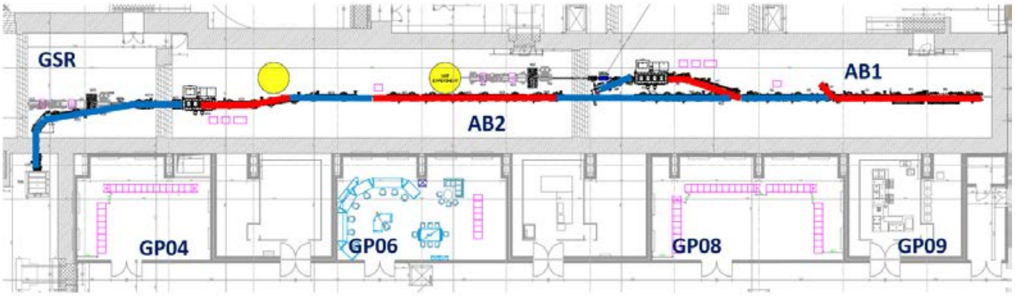

Figure 5.12: Cherenkov BLM - blue and red segments show the different optical fibers trunks along the accelerator.

Trunk	from module	to module	Room	Fiber length [m]
1	M2	M4A	AB1	20
2	M5	M6	AB1	15
3	M7	M8	AB1	10
4	M10A	M10E	AB1	10
5	M15	M17C	AB1	25
6	M18	M21	AB2	25
7	M22	M23	AB2	10
8	M24	M25	AB2	10
9	M27	M35	AB2	25

Table 5.2: Cherenkov BLM - list of optical fibers required to cover the whole accelerator.

to similar requirements, in terms of sampling rate and resolution, I choose to involve the same digitizer used for the WaveForm Mask system.

Two servers, with a 8 channel WaveCatcher digitizer [52], collect: one in AB1, signals from the 5 MPPCs and the other one, in AB2, the remaining 4 signals.

Software Design

The software, the same on both server, is a LabView tool which acquire waveforms from WaveCatcher. Such tool computes the time-of-flight through the Formula 5.6 converting time to relative spatial data.

$$\Delta s = \Delta t \cdot c \left(\frac{1}{\beta} + n \right)^{-1} \tag{5.6}$$

This computation let to estimate the distance from the MPPC where the cherenkov light is created. Then I thought up to calibrate such space-time conversion in order to match clearly the spatial data with accelerator devices. By inserting into a vacuum chamber an electron beam screen (then creating huge electron losses), I found a way to correlate a peak on BLM with a device on the accelerator. Repeating this procedure for each trunk allow to calibrate the whole BLM. In this way, I have an absolute reference in space for any detected peak.

At the end, the waveform acquired from each MPPC is projected over the EPICS network to show, on MPS overview, all the beam loss data.

Performances

From Formula 5.6, by assuming the maximum sampling rate for the Wave-Cather of 3.2 $\frac{GS}{s}$, has been possible to evaluate the resolution of the system of about 4 cm.

Proof of principle of cherenkov BLM on noisy linac injector (from dark current point of view) and a test of my calibration process were performed at SPARC_LAB facility.

Benchtest at SPARC_LAB

To perform this test I choose to use the SPARC_LAB electron accelerator which is essentially the same type of injector of the ELI-NP-GBS. In addition to this, due to aging problem of the photo-cathode, I realize this test with the hardest scenario: an electron beam with 2400 pC of beam charge where 2000 pC are the measured dark current. Along the whole accelerator a fiber of 20 m has been placed.

Waveforms are acquired with a NI digitizer operating at 1 $\frac{GS}{s}$ which can solve signal with a space resolution of 15 cm.

As shown in Figure 5.13, two beam screens are involved: one before and one after the second S-band accelerating structures. The scope of this test was to

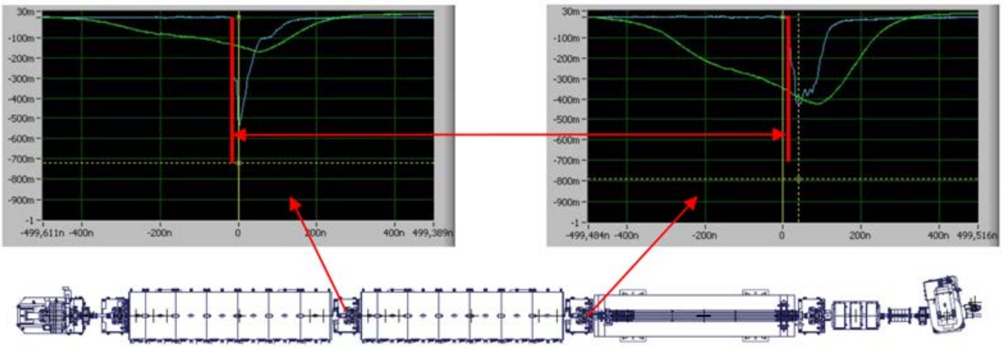

Figure 5.13: Cherenkov BLM benchtest at SPARC˙LAB. Bottom, the SPARC accelerator lattice; on the top, BLM signal (blue curve) with first screen (left) and with second screen (right) inserted.

measure the distance between such screens through the BLM. From AutoCAD design, these beam screens results a distance of 3.5 m.

Inserting the first beam screen and then the second one, were possible identify without problem two big peaks. Then, assuming the front of such peaks the place where electrons hit the screen, I found a difference of 30 ns.

From the time-of-flight calibration I get a distance of 3.6 m that is reasonable with the resolution of the digitizer. In this way I verified that use a reference peak (for example the first beam screen), it allow to calibrate peaks (over the same trunk) with elements of the accelerator (as done to find the position of second screen).

Hall Probes

To improve the safety of accelerator equipment, the risk analysis highlighted the necessity to monitor bending field inside the 9 dipoles of the accelerator. This requirement is due to high electron beam energy and together with high bending angles (two magnets bend the beam over 80 degrees and five over 30 degrees). If a mismatch in beam transport happens this could cause a loss of performances and possible damages in equipment electronics.

During operation, dipoles current could be applied by operators (or other automated tool) to correct the electron beam trajectory. Then it is not possible to define, easily, if the current setpoint guarantees the proper trajectory. By assuming that such setpoints are always the right one, I designed a system of distribute Hall probes, one for each dipole, to verify the truthfulness between expected and applied bending field.

According to field map, provided by magnets team, each probe will be installed nearby the vacuum chamber inside the good field region of the dipole.

Hardware Design

From beam dynamics and magnets specification, I identified maximum magnetic field range between 1.8 T then I choose to procure epoxy glass laminated hall probes manufactured by Group3.

Such probes have a full-scale range of 2 T with an accuracy of ±0.03 % and equipped with a signal conditioning electronics that produces an analog signal.

This is the topology of the Hall probe BLM as reported in Figure 5.14 and in Table 5.3.

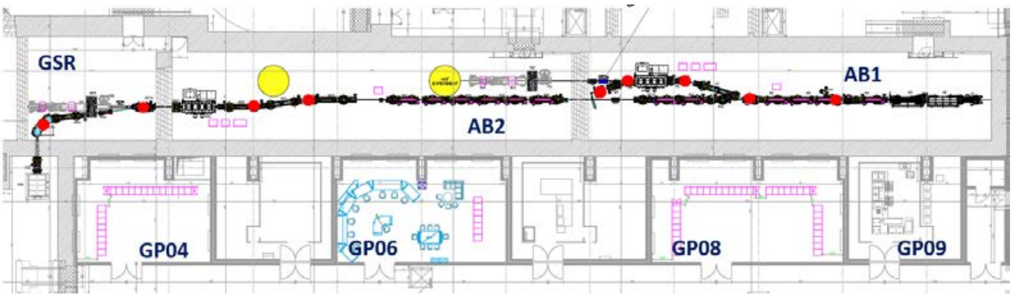

Figure 5.14: Hall probes BLM - red dot show all dipoles of the accelerator where an hall probes are installed.

Analog signal from each probe is acquired by the same server involved for the cherenkov BLM, through the same NI DAQ used for WaveForm Mask. In this way, I have in MPS framework 3 identical servers equipped with one WaveCathcer and one DAQ which allow to optimize spare parts and maintenance of the system.

Dipole	Module	Room	Peak Magnetic Field [T]	Peak Current SetPoint [A]
LEL-MAG-DIP01	M4	AB1	1	155
LEL-MAG-DIP02	M6	AB1	1.8	200
LET-MAG-DIP01	M8	AB1	1.8	200
LED-MAG-DIP01	M10A	AB1	1.3	200
LED-MAG-DIP02	M10C	AB1	1.3	140
HEL-MAG-DIP01	M23	AB1	0.6	110
HET-MAG-DIP01	M25	AB2	0.6	110
HED-MAG-DIP01	M27A	AB2	0.6	110
HED-MAG-DIP02	M34	GSR	1.8	200

Table 5.3: Hall probe BLM - list of bending magnets where an hall probe is placed.

Software Design

The software, developed in LabView, runs online collecting analog data from probes. The scope of this algorithm is verify if current setpoint from dipole PSU, provide the expected bending field inside the dipole.

To verify unexpected fields, the algorithm performs online this sequence of tasks:

1. **Hall probe calibration** - The analog signal from probe is calibrated, through the technical note produced by the manufacturer, to convert the signal from voltage to magnetic field intensity.

2. **Excitation curve calibration** - This second calibration is obtained through dipole excitation curve of each dipole; such curve relates the magnetic field intensity with current in magnet's coils.

3. **Monitor estimated vs setpoint currents** - With the data from the previous step, the algorithm estimate the current flowing in magnet's coils according to hall probe. This value is compared on-line with dipole PSU setpoint (acquired through EPICS network).

4. **Interlock** - If results a not negligible difference between applied and estimated currents, an interlock signal is forwarded to stop the electron beam.

As for the cherenkov BLM, data of magnetic field intensity and estimated currents inside coils are communicated to EPICS network to be shown on the MPS overview in control room.

Performances

The Hall probe BLM allow to monitor performances of each dipole and the related PSU and cabling. Thanks to this BLM, is possible identify not only mismatch between expected and measured magnetic field but also tricky issues (e.g. when partial short-circuit in coils lets anyway the current flow, without alert the PSU, while the induced field is not as expected).

Currently the only excitation curves available are provided during factory acceptance test of each magnet. Such measurements are made with hall probe in the focal point while hall probes of the MPS will be placed at centimeters from that point (outside the vacuum chamber); this drift cause an error estimating coil's current. During first phase of the commissioning, I will work with magnet experts to produce new excitation curves to compensate the error, with my hall probes installed in their final position.

Proof of principle of the algorithm has been performed at Magnets Laboratory of INFN-LNF together with its experts.

Benchtest at LNF

With this test I would like to investigate the performances and the reliability of the Hall probe BLM. The setup involves a sample quadrupole magnet, the calibrated Hall probe of the Magnet Labs and one of my Hall probes.

The BLM probe is installed over the calibrated one, the distance between them is measured and the field drift, due to such distance, is evaluated from the field map available for this sample magnet.

Thanks to a motorized support, both probes are moved inside the good field region of the magnet. From comparison of the two values, estimated current in coils and PSU setpoint have been compared and it results fully matched with a precision of ±1 A.

On-site probes will be calibrated directly on dipole an not through compensation of another probe. This better calibration procedure let me assume this good result as base-line for the precision of the system in final setup.

Beam Position and Current Monitors

This is one of the two BLMs, based on software algorithm, which monitors beam performances through other accelerator equipment.

This simple BLM involves the 29 BPMs and the 4 FCTs from electron beam diagnostics.

Position monitors work as BLM operating as flag to show where the electron beam is transported. By setting properly LiberaBPMs, I made these devices able to warn when beam signal is below the detection threshold. In this way, when the beam transport is mismatched, the low or totally missing beam signal triggers the warning from LiberaBPMs. Such warnings, communicated to the EPICS network, became the flags used from the BLM to show electron beam losses.

Current monitors verify the difference of beam current between one FCT and the next one. If the difference between two FCTs exceed a threshold this triggers an interlock.

IP Trajectory feedback

This BLM verify the trajectory of the electron beam at each IP when results a loss of performances from the gamma beam flux measured by the luminosity monitor.

As reported in Figure 5.15, this algorithm involves: the two Cavity BPMs before and after the IP, the last two XY correctors (so operating on beam transvere plane) before the IP and the diamond detector working as luminomiter just after the IP.

This BLM operates in two phase: the first one, when the accelerator working point is applied and electron beam transported to the dump with a spatial stability of 1% (according to ELI-NP-GBS Technical Report), the calibration procedure should be performed once; the second phase, when the gamma production is

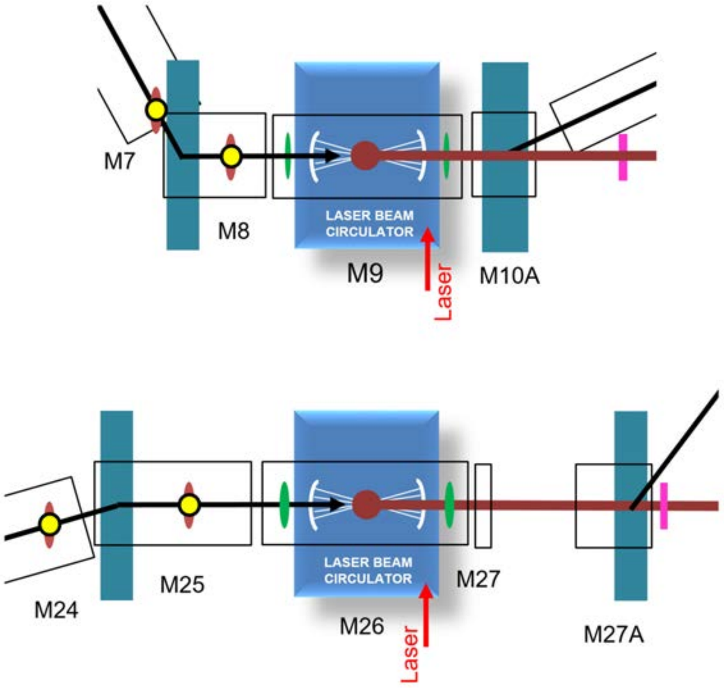

Figure 5.15: IP Trajectory feedback - Lattice of low (up) and high (down) energy IPs. In green CBPMs, in yellow XY correctors, in purple the diamond detector.

optimized, operators run the on-line feedback which it will lock the luminosity of gamma beam.

During calibration phase, current setpoint of both correctors is scanned in order to move the electron beam over the transverse plane with different kicks (beam bumps [57]). For each step of this scan, position from both CBPMs and the luminosity are acquired. The range of the correctors scan is limited to allow a kick 2 μrad on both X and Y (to guarantee always spatial matching with laser beam). At the end, the algorithm fills a matrix which, for each step of the scan, relates: current setpoint, the displacement from IP focal point and the luminosity.

The set of current setpoints for the scan is provided through an Elegant simulation to perform the proper beam manipulation. In this way the electron beam could be bumped with proper precision and compensating the dispersion due to the bending magnet located between the two correctors.

When the accelerator working point is applied and the compton interaction is running, operator can start the feedback to lock gamma source performances.

The algorithm starts assuming as target values the current electron beam trajectory (from CBPMs) and the luminosity. Then, as in Figure 5.16, this procedure runs on-line:

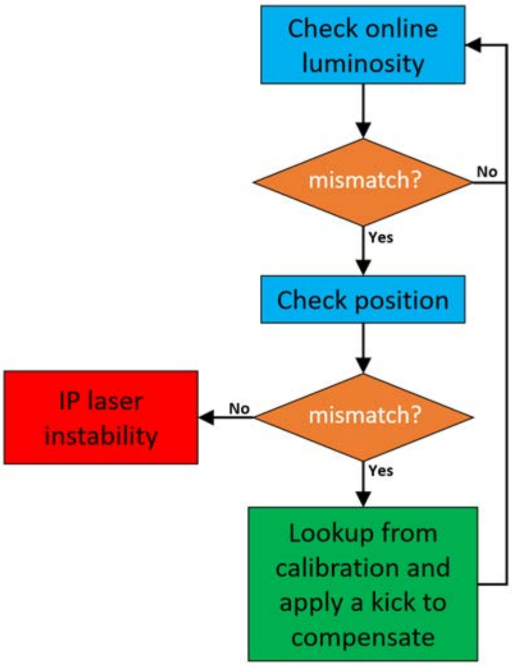

Figure 5.16: IP Trajectory feedback algorithm flow-chart.

1. Compare current luminosity with the target one.

2. If there is a mismatch, check if it is due to a change of the electron beam trajectory.

3. If not, the are problem of stability in the interaction laser. If so, new current setpoint for correctors is looked up from the calibration matrix. A displacement of the electron beam on X (or Y), from the related target value, allows to evaluate the current setpoint correction to restore the target trajectory of the electron beam. When the loop restarts, if the luminosity is not restored, the algorithm will continue to compensate the electron beam trajectory.

The algorithm lock the target luminosity with a precision related to the resolution of PSU of correctors. Such PSUs are able to apply current setpoint with a resolution of 20 μA.

5.4 Vacuum design improvements

During development of MPS framework I discussed with different teams to identify critical issues and suggest review of their system. Hugh part of these activities involve RF and vacuum systems. Exactly on vacuum system I follow the review of three main aspects which are strictly related to machine protection theme: avoid venting the RF Gun; improve reliability of vacuum regions pumped with scroll; design alluminium windows for electron beam dumps.

Fast Valve design for RF Gun

Laser circulator and Gamma characterization regions are pumped in ultra-high vacuum through turbo and scroll pumps, there is not negligible probability that a critical leak vents the whole linac. While this is not big issue for accelerating structures, the photo-cathode can loss performances due to exposition with air.

I asked to place a pneumatic fast-valve just after the pneumatic valve (which require 2 s to be operated) located in front of the gun. The fast-valve, manufactured by VAT, has a closed loop with its own vacuum gauge to trigger the fast closure.

In order to choose the position of the fast-valve's vacuum gauge, I had to measure the execution time of the VAT system and the available time required to detected a vacuum leak. I measured that the VAT system requires 5 ms to detect a leak and close the valve. Then I choose a position for the gauge which allow to detect leaks from both low and high energy IPs and , at the same time, far enough from the RF Gun to allow the intervention of the fast-valve. I assumed the worst scenario with a huge vacuum leak that produce a mach-2 shockwave then I choose to place such gauge on M6 module (just before the low energy dogleg), far 20 m from gun. In this way I protected both IPs and when the mach-

2 shockwave pass through the gauge, the VAT system has 30 ms to trigger the fast-valve.

Backing line design review

IP and Gamma characterization regions are equipped with degassing devices which doesn't allow to be pumped in utra-high vacuum with ion-pump, rather with a backing line made of a scroll pump and turbo pumps.

I worked together with vacuum team to include between turbo pumps and the scroll one a series of EM-valves and a Thermo-Couple gauge in order to monitor anomalous vacuum activity in the backing line and segment it if needed.

Aluminum windows design

I also verified the reliability of vacuum system close to beam dump. Just before each of the 3 dumps of the accelerator, a vacuum window should be placed as termination of the high-vacuum region.

To design such windows I made a MonteCarlo (MC) simulation with software FLUKA to verify the heat load. I get the beam specifications from beam dynamics team and I choose to investigate performance of windows made of a layer of aluminium with a thickness of 2 mm. Evaluating spot size of the electron beam in the 3 dumps, I thought to simulate just the high energy one because it shown the worst scenario: highest electron beam energy and smaller spot size of the beam.

FLUKA simulation were performed with these parameters, as shown in Table 5.4, obtaining a dose to the aluminium target of 846 $\frac{keV}{electron}$ as reported in Figure 5.17.

Assuming to have 32 micro-bunches with 400 pC of charge each one and running at 100 Hz, the heat load results of 1.2 W which is easily supportable by this type aluminium windows. The same window is produced for all dumps of the accelerator.

Parameter	**Value**
Electrons energy	750 MeV
Energy spread	1%
Transverse beam shape	gaussian XY
Beam size (σ_X, σ_Y)	1560 μm, 170 μm
Primaries	$5 \cdot 10^6$
Material	Aluminium
Target	$15.2 \cdot 15.2 \cdot 0.2\, cm^3$
Binning	$0.1 \cdot 0.1 \cdot 2\, mm^3$

Table 5.4: FLUKA simulation parameters for the evalutation of the heat load on vacuum windows of the high energy dump.

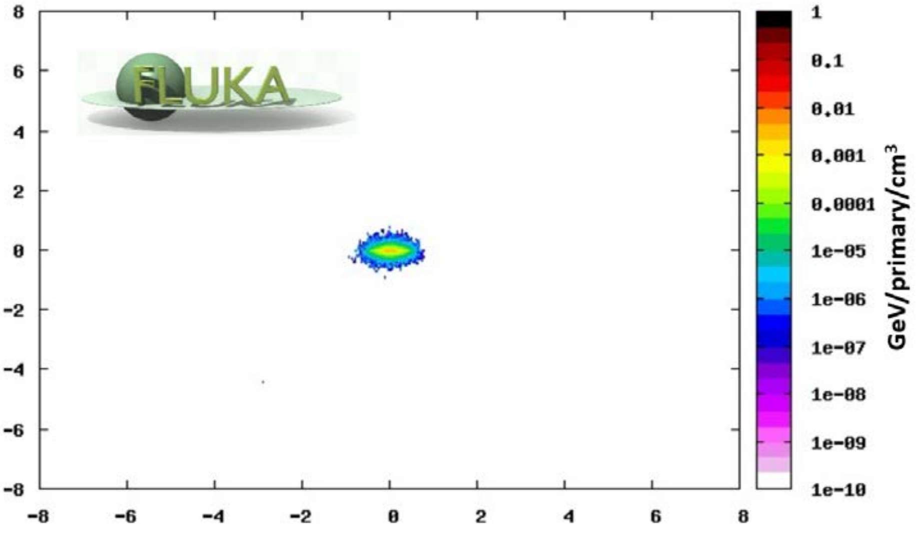

Figure 5.17: Vacuum windows - Energy deposition on transverse plane for the windows of the high energy dump.

CHAPTER

6 Validation and Verification

Content

6.1 MPS framework Validation 128
Verification of requirements 129
6.2 Validation Planning 136

6.1 MPS framework Validation

As reported at the end of the MPS V-model and defined at the end of Functional Safety chapter 2.7, I completed the MPS project with the verification of whole system according to requirements: achieve the requested *Safety Integrity Levels (SIL)* assumed for each *Safety Instrumented Function (SIF)*; close the safety *life-cycle* by satisfy all the constraints defined at the beginning in the accelerator risk analysis.

In this last chapter I will focus on the verification of the MPS and I will define the periodic validation planning scheduled for the system.

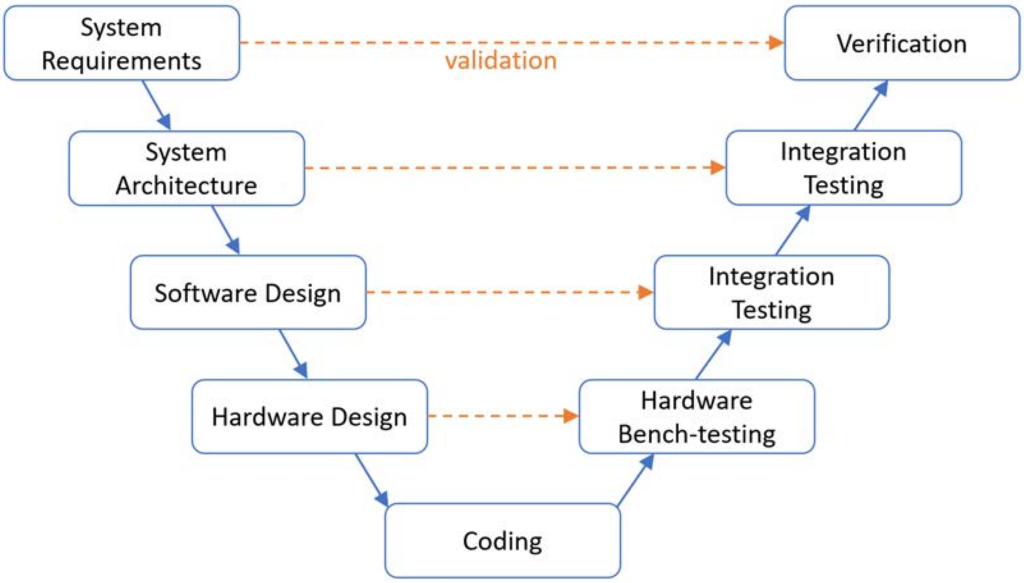

Figure 6.1: The ELI-NP-GBS Machine Protection System V-model for the *life-cycle* development.

Verification of requirements

I will report the criteria for the verification of the MPS from software and hardware point of view and, finally, I will present all tests performed to certify the MPS, during the Factory Acceptance Test (FAT).

All requirements for the MPS, as reported in the Risk Analisys chapter and summarized in Table 3.2, were used to filling up the Logic Matrix presented at the end of Architecture chapter.

The software, for each part of the MPS, is based on deterministic code. Then interlock conditions, which allow to handle all risks highlighted in the related analysis, have to trip the required accelerator equipment. When all conditions are verified, the MPS software could be assumed asverified.

As anticipated in previous chapter, the verification of MPS hardware requires a comparison between the required SIL (of each SIF) and the achieved one. As discussed in the Architecture chapter, summarized in Table 4.1 the Fast-ILK system (SIF-1) requires the SIL-3, the EPICS-based Supervisor (SIF-2) requires SIL-2 while the BLM system (SIF-3) doesn't require to achieve any SIL class.

In order to evaluate achieved SIL classes, failure rates have been computed for the first two SIFs. The Weibull model allow to estimate reliability and failure rate of devices through the study of Mean Time Between Failure (MTBF). In this way, I computed for the Fast-ILK and Supervisor systems the reliability, failure rate and availability; this last parameter is not required by regulation but it provides the information about the probability of the be ready when needed (while the reliability is the probability of the system to do its purpose) through MTBF and Mean Time To Repair (MTTR) parameters. Usually MTBF of the equipment is available from the manufacture of the device but, like in this case, each SIF is made of different components then to compute the MTBF has been required to combine reliability (or failure rate) as series or parallel dependency between the involved devices. I choose to compute the SIL classes and availabilities of the two SIFs I had to use this procedure:

1. Identify dependencies between devices of the system;
2. Use the reliability of each device (converted from MTBF) together with system dependencies to compute the reliability of the whole system;
3. Convert the system reliability in the system MTBF parameter to obtain the failure rate;
4. Establish the SIL class of the system from failure rate;
5. Establish the availability of the system through the MTBF and the MTTR.

As illustrated in the Functional Safety chapter, it is possible convert each MTBF value in reliability $R(t)$ (success probability for the device to be working after a certain period t) according to Formula 6.1. With the reliability of all devices, the combined reliability of the whole system is obtained analyzing system dependecies. Such value reverted provide the MTBF which, through Formula 6.2, allow to evaluate the failure rate $h(t)$ of whole system and to define the achieved SIL class. The availability of a system is related to the MTBF and MTTR through the Formula 6.3; this second parameter for the hardware involved in both SIFs could be easily procured then, in both cases, has been assumed a MTTR of 30 days (or 720 hours).

$$R(t) = \exp\left(-\frac{t}{MTBF}\right) \tag{6.1}$$

$$h(t) = \frac{1}{MTBF} \tag{6.2}$$

$$Availability = 1 - \frac{MTTR}{MTBF + MTTR} \tag{6.3}$$

SIF-1: Fast-ILK system

Considering the dependencies of different devices of the Fast-ILK, I followed a bottom-up strategy analyzing from slave units up to the master one. As shown in Figure 6.2, the strategy to identify dependency highlighted that:

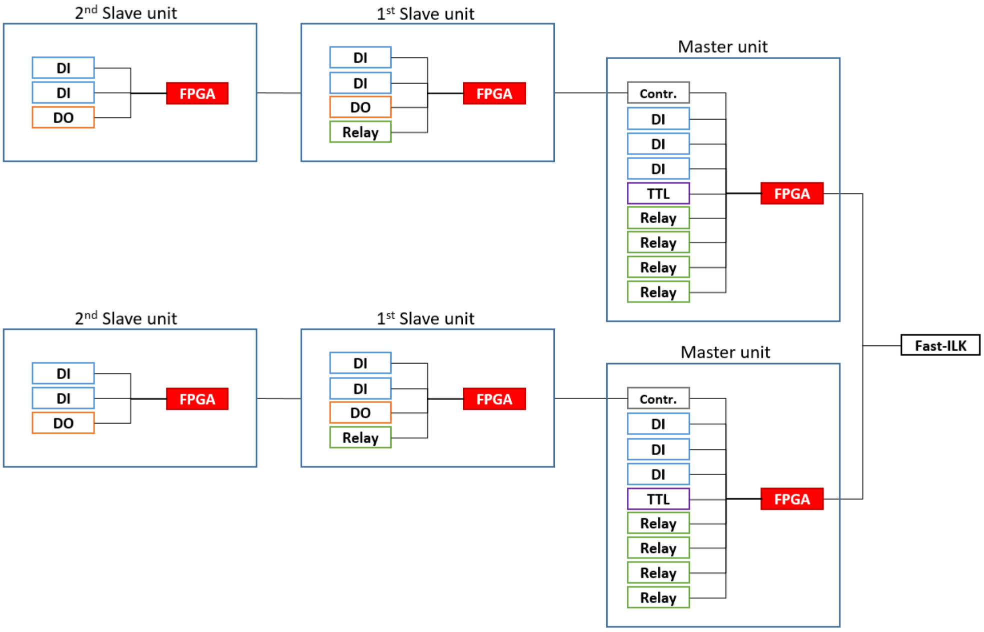

Figure 6.2: Fast-Interlock system Verification - Functional dependencies of between the two Fast-ILK systems in parallel, their master and slave units and I/O Modules. This schema take in account both hardware dependency (like the eterCAT network) and software one (slave communication through master unit controller).

- I/O Modules of each unit are assumed in parallel with their own FPGA (according to the architecture of the FPGA technology);
- Slave units are chained with the controller of the master unit (according to the etherCAT network design);
- Master unit controlled together with I/O Modules are in parallel with the master FPGA;
- All dependencies of one system is parallel with the second one (according to the dual modular redundancy schema).

As reported in National Instruments datasheets, MTBFs for each part of the Fast-ILK are listed in Table 6.1.

Device	**MTBF [hours]**
cRIO-9039 Master Unit Controller	264000
Xilinx Kintex-7 Master Unit FPGA	41500000
NI-9144 Slave Unit	460000
NI-9425 32 ch. Sinking DI	1250000
NI-9426 32 ch. Sourcing DI	110000
NI-9476 32 ch. Sourcing DO	955000
NI-9403 32 ch. TTL DIO	1000000
NI-9485 8 ch. SSR	2170000

Table 6.1: Mean Time Between Failures reported for each element of F-ILK system.

The period t required to compute the reliability, inside Formula 6.1, has been assumed to cover the total operation life of the accelerator, then about 20 years (or 175 200 hours). From dependencies between devices, I evaluated a combined reliability $R(175200\,hours) =\sim 100\%$. Reverting Formula 6.1, I get the MTBF of the whole system equal to $1 \cdot 10^{10}\,hours$. With such value inserted in Formula 6.2, I obtained a failure rate $h(175200\,hours) = 1.006 \cdot 10^{-10}$. The availability has been estimated of about $\sim 100\%$.

From the comparison with SIL classes defined in IEC 61508, as in Table 2.1, the Fast-ILK system achieved the SIL-4 class (the maximum one) while the required level was just SIL-3.

SIF-2: EPICS-based Supervisor system

Concerning the Supervisor system, the dependencies analysis takes in account the constraint from the hot-standby redundancy scheme only, which requires to assume the reliability of the two servers as two devices in parallel.

As reported by DELL datasheet, the MTBF of server involved in this system is 600 000 hours.

The period t required to compute the reliability, Formula 6.1, has been assumed to cover a reasonable period, for this type of hardware, of about 10 years (or 86 700 hours). From dependencies between devices, I evaluated a combined reliability $R(86700\,hours) =\sim 92\%$. Reverting Formula 6.1, I get the MTBF of the whole system equal to $1 \cdot 10^{6}\,hours$. With such value inserted in Formula 6.2, I obtained a failure rate $h(86700\,hours) = 9.7 \cdot 10^{-7}$. The availability has been estimated of about $\sim 100\%$.

From the comparison with SIL classes defined in IEC 61508, as in Table 2.1, the EPICS-based Supervisor system achieved the SIL-2 class that match with the required level of safety.

Test Plan

Last Part of the verification process involves tests campaign to verify the behaviour of MPS when triggered by proper signal (or not) and the fail-safe capability of the whole system. Here the list of tests passed during FAT of the system at Frascati:

- **Check Fast-interlock sw matches with Logic Matrix**
  - **Method** - Each input gate has been triggered in order to verify that the correct output gate is tripped, according to the Logic Matrix coded in FPGA.
  - **Result** - Test passed for each interlock condition.
- **Check Supervisor sw matches with Logic Matrix**
  - **Method** - Dummy EPICS PVs has been used to trigger and verify that the proper interlock PVs are tripped, according to the Logic Matrix compiled on the server.
  - **Result** - Test passed for each interlock condition.
- **Check Fast-interlock matches response time**
  - **Method** - As presented in Design chapter, response time of the whole system has been measured (setup included a dummy etherCAT connection of 100 m to simulate distances between units); an input gate has been triggered from one slave unit and to monitor, with an oscilloscope, how much time is required to trigger the output gate on the other one slave unit.
  - **Result** - Test passed. Real-Time monitoring capability achieved, the result of this test repeated several times shows an average execution time of about 200 μs.
- **Check Supervisor matches response time**
  - **Method** - As presented in Design chapter, response time has been measured through performance benchmark monitor inside the software itself.
  - **Result** - Test passed. On-line monitoring capability achieved, the result of this test repeated several times shows an average execution time results of about 2 ms.

- **Test Fast-Interlock integrity**
  - **Method** - Several tests verified the capability of wacthdog to detect integrity issues due to missing communication slave units and master unit FPGA. In first part of the test, EtherCAT network has been trunked to isolate master unit from slave units (in first instance from one unit then from both ones). In second part, the test has been repeated trunking PSU connections.
  - **Result** - Tests passed. In etherCAT scenario, all units of the Fast-ILK system went in sleep-mode. In power supply scenario, the unpowered unit trip all linked accelerator devices while other units went in sleep-mode.
- **Test EPICS Supervisor integrity**
  - **Method** - Active server unit has been powered off to verify if the watchdog switch in operation the second server unit.
  - **Result** - Test passed. Second unit become active in 100 ms (just the EPICS data refresh latency).
- **Verify post-mortem handling of an Fast-Interlock system**
  - **Method** - In first part of the test, one of the two Fast-ILK system has been switched off the verify that: all monitored devices have been tripped; this didn't have to affect the second system; the Supervisor had to detect the issue. In second part of the test, both system were switched off to verify that all accelerator has been tripped.
  - **Result** - Test passed. Whole accelerator tripped.
- **Verify post-mortem handling of Beam Loss Monitor servers**
  - **Method** - Each server has been switched off to verify that the Supervisor detected the issue.
  - **Result** - Test passed.

- **Verify post-mortem handling of Supervisor system**
  - **Method** - Both servers have been switched off in order to verify if the MPS overview in control room starts to signaling the issue.
  - **Result** - Test passed. Operator interface detect the fault in 100 ms (just the EPICS data refresh latency).

Thanks to all these tests and all the achieved performance in term of SIL classes, I closed the *life-cycle* process by demonstrating the compliancy of the MPS with all requirements from both accelerator and Functional Safety regulation point of view.

6.2 Validation Planning

The validation planning process has been planned in order to repeat all tests performed during the verification process. This procedure has been scheduled to be repeated every 6 months in order to avoid wear out issue for the hardware, as presented in Weibull model discussed Functional Safety chapter.

During such validation sessions any anomalous result must be documented. If a test fail, I should investigate if it is related to an hardware fault (and provide its substitution) or to a change of requirements from the accelerator which requires the re-design of the MPS system following the same *life-cycle* V-model: risk anlysis, architecture, design, integration testing and verification.

Conclusions

In this Ph.D. thesis I illustrated the development of the Machine Protection System related to the ELI Nuclear Physics Gamma Beam System (ELI-NP-GBS) project.

In ELI-NP-GBS a high power Laser pulse is Compton scattered with an electron beam generated through an high brightness Linac. In this way a highly polarized, and nearly mono-energetic γ ray beam with a tunable energy from about 0.2 MeV to 19.5 MeV and a high spectral density (10^4 photons/s·eV) is produced. This unique gamma-ray beam has a wide range of applications from nuclear physics to astrophysics, from medical research to homeland security and industrial applications. The photon beam performances impose strong requirements on the electron beam and, as consequence, on the accelerator system and related RF system. The Linac is required to achieve a normalized emittance in both directions lower than 0.5 mm·mrad and an energy spread below 0.1%. Moreover to increase the maximum photon flux the Linac has to work in multi-bunch mode with a repetition rate of 100 Hz.

In order to guarantee the performances of the facility and to protect the facility itself, I designed an advanced MPS. It has been designed to be compliant with Functional Safety international regulation (IEC 61508) which provide guidelines to develop safety system with proper reliability.

I started the design activity defining the *life-cycle* of the project and the related V-model as roadmap for the development of the MPS. A risk analysis of each system of the accelerator has been performed involving experts from all sub-systems of the accelerator. Safety requirements and vulnerabilities have been highlighted to drive the creation of the MPS architecture. RF sources and vacuum systems, greatly in charge of quality of the gamma beam source, required a real-time and high-reliability system able to monitor electron beam performances shot-to-shot. Other systems of the accelerator, such as magnets and electron beam diagnostics, required an on-line monitoring to stop abnormal behaviour of such equipment.

Due to requirements from Functional Safety and accelerator operation, I developed a distributed Fast-Interlock system based on FPGAs which, thanks to an hardwired network, allow to monitor vacuum gauges and ion-pumps from the whole accelerator and control RF Modulators, LLRF, laser shutters and vacuum valves. From several test-benches, I measured the execution time of the system which is able to operate in 200 μs. I equipped also the system with WaveForm Mask able to analyze RF signals and provide in real-time diagnostics about vacuum activities and RF breakdowns. Then I developed an EPICS-based Supervisor able to monitor, through control system, all accelerator's systems which require on-line monitoring of their activities in less then 2 ms. Finally, in order to cover all the requirements in terms of performance in electron beam transport and gamma beam production, I setup and designed a series of Beam Loss Monitors based on distributed cherenkov detectors and hall probes, beam position and current monitors and trajectory feedback on each interaction points. This system has been designed to be a fully automated system able to follow the ELI-NP-GBS commissioning and operation in order to handle any kind of issues without the requirement of expert team on-site.

The developed MPS has been followed in order to obtain a system fully compliant with safety regulation. I improved the design with redundancy schemes, fail-safe capability and integrity monitors to achieve the proper level of safety for each part of the system. The Fast-Interlock system has been verified to be beyond the required SIL-3 class achieving the SIL-4 class (the maximum one). The EPICS-based Supervisor system achieved the planned SIL-2 level required for its scope of work. In conclusion, I performed the Factory Acceptance Test of the MPS and scheduled the periodic validation of the system to monitor its performance and reliability.

In the near future upgrades of the MPS will be considered in order to: improve FPGA software to increase the throughput of the Fast-Interlock system; improve electron beam performance monitor through microbunches data from FCTs and cavity BPMs; improve the trajectory feedback including not only the flux but also evaluating gamma beam bandwidth; calibrate BPMs data with FCTs to localize electron beam losses by mapping the charge transported.

Moreover the National Instruments company is interested on the certification and acquisition of this safety system, compliant with Functional Safety, to acquire a new field of market.

In collaboration with the collegues of the Laboratoire de l'Accelerateur Lineaire (LAL) in Orsay, where the WaveCatcher digitizer has been developed, we are thinking to design smarter digitizer with embedded FPGA software. The idea I proposed is to program directly the digitizer with software on the FPGA on-board (e.g. like the one in WaveForm Mask or the one in cherenkov BLM) and avoid the bottle-neck due to a server which is used to analyze waveforms and produce intelock signals.

Bibliography

[1] V. Petrillo, A. Bacci, R. B. A. Zinati, I. Chaikovska, C. Curatolo, M. Ferrario, C. Maroli, C. Ronsivalle, A. Rossi, L. Serafini *et al.*, “Photon flux and spectrum of γ-rays Compton sources,” *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, vol. 693, pp. 109–116, 2012.

[2] C. Sun and Y. K. Wu, “Theoretical and simulation studies of characteristics of a Compton light source,” *Physical review special topics-accelerators and beams*, vol. 14, no. 4, p. 044701, 2011.

[3] R. H. Milburn, “Electron scattering by an intense polarized photon field,” *Physical Review Letters*, vol. 10, no. 3, p. 75, 1963.

[4] F. Arutyunian and V. Tumanian, “The Compton effect on relativistic electrons and the possibility of obtaining high energy beams,” *Physics Letters*, vol. 4, no. 3, pp. 176–178, 1963.

[5] L. Federici, G. Giordano, G. Matone, G. Pasquariello, P. Picozza, R. Caloi, L. Casano, M. P. De Pascale, M. Mattioli, E. Poldi *et al.*, “Backward Compton scattering of laser light against high-energy electrons: the LADON photon beam at Frascati,” *Il Nuovo Cimento B (1971-1996)*, vol. 59, no. 2, pp. 247–256, 1980.

[6] F. Amman, R. Andreani, M. Bassetti, M. Bernardini, A. Cattoni, V. Chimenti, G. Corazza, D. Fabiani, E. Ferlenghi, A. Massarotti *et al.*, "Two-beam operation of the 1.5 GeV electron-positron storage ring adone," *Lettere Al Nuovo Cimento (1969-1970)*, vol. 1, no. 15, pp. 729–737, 1969.

[7] C. Vaccarezza *et al.*, "The SPARC˙LAB Thomson source," *Nucl. Instrum. Meth.*, vol. A829, pp. 237–242, 2016. doi: 10.1016/j.nima.2016.01.089

[8] C. Tang, W. Huang, R. Li, Y. Du, L. Yan, J. Shi, Q. Du, P. Yu, H. Chen, T. Du *et al.*, "Tsinghua Thomson scattering X-ray source," *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, vol. 608, no. 1, pp. S70–S74, 2009.

[9] W. Brown, S. Anderson, C. Barty, S. Betts, R. Booth, J. Crane, R. Cross, D. Fittinghoff, D. Gibson, F. Hartemann *et al.*, "Experimental characterization of an ultrafast Thomson scattering x-ray source with three-dimensional time and frequency-domain analysis," *Physical Review Special Topics-Accelerators and Beams*, vol. 7, no. 6, p. 060702, 2004.

[10] F. E. Carroll, M. H. Mendenhall, R. H. Traeger, C. Brau, and J. W. Waters, "Pulsed tunable monochromatic X-ray beams from a compact source: new opportunities," *American journal of roentgenology*, vol. 181, no. 5, pp. 1197–1202, 2003.

[11] S. Kashiwagi, R. Kuroda, T. Oshima, F. Nagasawa, T. Kobuki, D. Ueyama, Y. Hama, M. Washio, K. Ushida, H. Hayano *et al.*, "Compact soft x-ray source using Thomson scattering," *Journal of applied physics*, vol. 98, no. 12, p. 123302, 2005.

[12] E. Miura, S. Ishii, K. Tanaka, S. Kashiwaya, R. Kuroda, and H. Toyokawa, "X-ray generation via laser Compton scattering using quasi-monoenergetic electron beam driven by laser-plasma acceleration," in *Advanced Accelerator Concepts: 15th Advanced Accelerator Concepts Workshop*, vol. 1507, no. 1. AIP Publishing, 2012, pp. 304–309.

[13] E. Eggl, M. Dierolf, K. Achterhold, C. Jud, B. Günther, E. Braig, B. Gleich, and F. Pfeiffer, "The Munich Compact Light Source: initial performance measures," *Journal of Synchrotron Radiation*, vol. 23, no. 5, pp. 1137–1142, Sep 2016. doi: 10.1107/S160057751600967X. [Online]. Available: https://doi.org/10.1107/S160057751600967X

[14] A. Bacci *et al.*, "The Star Project," in *Proceedings, 5th International Particle Accelerator Conference (IPAC 2014): Dresden, Germany, June 15-20, 2014*, 2014, p. WEPRO115. [Online]. Available: http://jacow.org/IPAC2014/papers/wepro115.pdf

[15] A. Variola, A. Loulergue, F. Zomer *et al.*, "ThomX conceptual design report," *LAL RT*, vol. 9, p. 28, 2010.

[16] E. Eggl, S. Schleede, M. Bech, K. Achterhold, R. Loewen, R. D. Ruth, and F. Pfeiffer, "X-ray phase-contrast tomography with a compact laser-driven synchrotron source," *Proceedings of the National Academy of Sciences*, vol. 112, no. 18, pp. 5567–5572, 2015.

[17] R. Hajima, T. Hayakawa, N. Kikuzawa, and E. Minehara, "Proposal of nondestructive radionuclide assay using a high-flux gamma-ray source and nuclear resonance fluorescence," *Journal of Nuclear Science and Technology*, vol. 45, no. 5, pp. 441–451, 2008.

[18] T. Shizuma, T. Hayakawa, R. Hajima, N. Kikuzawa, H. Ohgaki, and H. Toyokawa, "Nondestructive identification of isotopes using nuclear resonance fluorescence," *Review of Scientific Instruments*, vol. 83, no. 1, p. 015103, 2012.

[19] "The White Book of ELI Nuclear Physics," 2011. [Online]. Available: http://www.eli-np.ro/documents/ELI-NP-WhiteBook.pdf

[20] C. Vaccarezza *et al.*, "A European Proposal for the Compton Gamma-ray Source of ELI-NP," *Conf. Proc.*, vol. C1205201, pp. 1086–1088, 2012.

[21] L. Serafini *et al.*, "Technical Design Report EuroGammaS proposal for the ELI-NP Gamma beam System," 2014.

[22] "EuroGammaS Association." [Online]. Available: http://www.e-gammas.com/

[23] L. Serafini, D. Alesini, N. Bacci, N. Bliss, K. Cassou, C. Curatolo, I. Drebot, K. Dupraz, A. Giribono, V. Petrillo *et al.*, "High intensity X/γ photon beams for nuclear physics and photonics," in *EPJ Web of Conferences*, vol. 117. Nuclear Structure, 2016, p. 05002.

[24] K. Dupraz, K. Cassou, N. Delerue, P. Fichot, A. Martens, A. Stocchi, A. Variola, F. Zomer, A. Courjaud, E. Mottay *et al.*, "Design and optimization of a highly efficient optical multipass system for γ-ray beam production from electron laser beam Compton scattering," *Physical Review Special Topics-Accelerators and Beams*, vol. 17, no. 3, p. 033501, 2014.

[25] K. Dupraz, "Conception et optimisation d‚Äôun recirculateur optique pour la source haute brillance de rayons gamma d‚ÄôELI-NP," Ph.D. dissertation, Paris 11, 2015.

[26] A. Bacci, D. Alesini, P. Antici, M. Bellaveglia, R. Boni, E. Chiadroni, A. Cianchi, C. Curatolo, G. Di Pirro, A. Esposito *et al.*, "Electron linac design to drive bright Compton back-scattering gamma-ray sources," *Journal of Applied Physics*, vol. 113, no. 19, p. 194508, 2013.

[27] V. Fusco and M. Ferrario, "Beam dynamics study of a C-band linac driven FEL with S-band photo-injector," *Proceedings of PAC09, Vancouver, May 2009*, vol. TH5PFP066.

[28] D. Alesini, S. Bertolucci, M. Biagini, C. Biscari, R. Boni, M. Boscolo, M. Castellano, A. Clozza, G. Di Pirro, A. Drago *et al.*, "Status of the SPARC project," *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, vol. 528, no. 1, pp. 586–590, 2004.

[29] A. Mostacci, D. Alesini, M. Anania, A. Bacci, M. Bellaveglia, A. Biagioni, F. Cardelli, M. Castellano, E. Chiadroni, A. Cianchi *et al.*, "Operational experience on the generation and control of high brightness electron bunch

trains at SPARC-LAB," in *SPIE Optics+ Optoelectronics*. International Society for Optics and Photonics, 2015, pp. 95 121Q–95 121Q.

[30] M. Ferrario, D. Alesini, A. Bacci, M. Bellaveglia, R. Boni, M. Boscolo, M. Castellano, E. Chiadroni, A. Cianchi, L. Cultrera, G. Di Pirro, L. Ficcadenti, D. Filippetto, V. Fusco, A. Gallo, G. Gatti, L. Giannessi, M. Labat, B. Marchetti, C. Marrelli, M. Migliorati, A. Mostacci, E. Pace, L. Palumbo, M. Quattromini, C. Ronsivalle, A. R. Rossi, J. Rosenzweig, L. Serafini, M. Serluca, B. Spataro, C. Vaccarezza, and C. Vicario, "Experimental Demonstration of Emittance Compensation with Velocity Bunching," *Phys. Rev. Lett.*, vol. 104, p. 054801, Feb 2010. doi: 10.1103/PhysRevLett.104.054801. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.104.054801

[31] International Electrotechnical Commission, "Functional Safety IEC 61508:2010," 2017. [Online]. Available: https://webstore.iec.ch/publication/22273

[32] W. Weibull, "A statistical distribution function of wide applicability," *J. Appl. Mech.-Trans. ASME*, vol. 3, pp. 293–297, 1951.

[33] J. Lienig and H. Bruemmer, *Fundamentals of Electronic Systems Design*, 1st ed. Springer International Publishing, 2017. ISBN 978-3-319-55839-4

[34] I. Bazovsky, *Reliability Theory And Practice*, 1st ed. Prentice-Hall, Inc., 1961. ISBN 61-15632

[35] D. O'Conner and A. P., Kleyner, *Practical Reliability Engineering*, 5th ed. Prentice-Hall, Inc., 1961. ISBN 978-0-470-97981-5

[36] L. Piersanti, D. Alesini, M. Bellaveglia, R. Boni, F. Cardelli, G. D'Auria, A. Gallo, L. Palumbo, and A. Variola, "The RF System of the ELI-NP Gamma Beam Source," in *Proceedings, 7th International Particle Accelerator Conference (IPAC 2016): Busan, Korea, May 8-13, 2016*, 2016. doi: 10.18429/JACoW-IPAC2016-MOPMW006 p. MOPMW006. [Online]. Available: http://inspirehep.net/record/1469620/files/mopmw006.pdf

[37] “ScandiNova Systems.” [Online]. Available: http://www.scandinovasystems.com/

[38] “Instrumentation Technologies.” [Online]. Available: http://www.i-tech.si/

[39] “Agilent Technologies.” [Online]. Available: https://www.agilent.com/home

[40] K. Cassou *et al.*, “Laser beam circulator for high brightness Inverse Compton Scattering Sources,” in *Proceedings, 3rd European Advanced Accelerator Concepts Workshop (EAAC 2017): La Biodola, Italy, September 24-30, 2017*, 2017.

[41] M. Lenzia *et al.*, “A new-concept gamma calorimeter at ELI-NP,” in *14th Topical Seminar on Innovative Particle and Radiation Detectors (IPRD16)*, 2016.

[42] “Edwards Vacuum.” [Online]. Available: https://www.edwardsvacuum.com/

[43] “Omron.” [Online]. Available: https://industrial.omron.it/it/home

[44] “SigmaPhi.” [Online]. Available: http://www.sigmaphi.fr/

[45] “I-Test.” [Online]. Available: http://www.bilt-system.com/appli_acc.html

[46] “Basler.” [Online]. Available: https://www.baslerweb.com/

[47] “Technosoft Motion.” [Online]. Available: http://www.technosoftmotion.com/en/

[48] S. Pioli *et al.*, “The Machine Protection System for the ELI-NP Gamma Beam System,” in *Proceedings, 8th International Particle Accelerator Conference (IPAC 2017): Copenhaghen, Denmark, May 14-19, 2017*, 2017. ISBN 978-3-95450-182-3 pp. TUPIK058 – pag. 1824. [Online]. Available: http://accelconf.web.cern.ch/AccelConf/ipac2017/papers/tupik058.pdf

[49] ——, “The Real Time Waveform Mask interlock system for the RF Gun conditioning of the ELI-NP Gamma Beam System,” in *Proceedings, 8th International Particle Accelerator Conference (IPAC 2017): Copenhaghen, Denmark, May 14-19, 2017*, 2017. ISBN 978-3-95450-182-3 pp. TUPIK057 – pag. 1822. [Online]. Available: http://accelconf.web.cern.ch/AccelConf/ipac2017/papers/tupik057.pdf

[50] “EtherCAT Technology Group.” [Online]. Available: https://www.ethercat.org/default.htm

[51] “National Instruments.” [Online]. Available: http://www.ni.com

[52] D. Breton *et al.*, “The WaveCatcher Family of SCA-Based 12-Bit 3.2-GS/s Fast Digitizers,” in *Proceedings, 19th Real-Time Conference: Nara, Japan, May 2014*, 2014.

[53] D. Alesini *et al.*, “High Power Test Results of the ELI-NP S-Band Gun Fabricated With the New Clamping Technology Without Brazing,” in *Proceedings, 8th International Particle Accelerator Conference (IPAC 2017): Copenhaghen, Denmark, May 14-19, 2017*, 2017. ISBN 978-3-95450-182-3 pp. THOBB1 – pag. 3662. [Online]. Available: http://accelconf.web.cern.ch/AccelConf/ipac2017/papers/thobb1.pdf

[54] D. Di Giovenale *et al.*, “A read-out system for online monitoring of intensity and position of beam losses in electron linacs,” *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, vol. 665, no. 1, pp. 33–39, 2011.

[55] X. Marechal *et al.*, “FIRST OPERATION OF A FIBER BEAM LOSS MONITOR AT THE SACLA FEL,” in *Proceedings, 2th International Particle Accelerator Conference (IPAC 2011): San Sebastian, Spain, 2011*, 2011, pp. WEPC164 – pag. 2367. [Online]. Available: http://accelconf.web.cern.ch/AccelConf/IPAC2011/papers/wepc164.pdf

[56] A. Kaukher *et al.*, “XFEL BEAM LOSS MONITOR SYSTEM,” in *Proceedings, 10th Beam Diagnostics and Instrumentation for Particle*

Accelerators Conference (DIPAC 2011): Hamburg, Germany, May 16-18, 2011, 2011, pp. TUPD43 – pag. 401. [Online]. Available: http://accelconf.web.cern.ch/AccelConf/DIPAC2011/papers/tupd43.pdf

[57] S. Y. Lee, *Accelerator Physics*, 1st ed. World Scientific Publishing Co. Pte. Ltd., 1999. ISBN 981-02-3709-X

List of Figures

1.1 Sketch of Compton scattering of an electron and a photon in a laboratory frame coordinate system (x_e, y_e, z_e) in which the electron is incident along the z_e direction. The incident photon is propagating along the direction given by the polar angle θ_i and azimuthal angle ϕ_i. The collision occurs at the origin of the coordinate system. After the scattering, the scattered gamma ray propagates in the direction given by the polar angle θ_f and azimuthal angle ϕ_f. θ_p is the angle between the momenta of incident and scattered photons. The electron after scattering is not shown in the figure. . 11

1.2 ELI-NP-GBS layout. 18

1.3 Picture of the assembled ELI-NP-GBS S-band injector. 20

1.4 ELI-NP-GBS Linac layout. 23

2.1 Functional dependencies of availability with reliability, Maintainability and Supportability. 35

2.2 The “bathtub curve” is a curve of failure rate function of time. The “bathtub” shape in blue comes from contribution of the exponential trends of erly mortability (in red), the constant presence of random failures (in green) and the exponential trends of equipment wear out (in yellow). 36

2.3 Standby Redundancy. Cold Standby model - in orange the active unit, in grey the auxilliary one. 40

2.4 Standby Redundancy. Hot Standby model - in orange active units. 40

2.5 N Modular Redundancy - in orange active units. 41

2.6 1:N Redundancy - in orange active units in grey the auxilliary one. 43

2.7 The ELI-NP-GBS Machine Protection System V-model for the life cycle development. 43

3.1 MPS risk analisys - Schematic of accelerator systems involved in the MPS. In yellow, critical systems to be controlled; in blue, less critical systems. . 49

3.2 ELI-NP RF power sources and distribution system. Three power units are used for the S-band injector, ten units for the C-band booster. In magenta the waveguide system with components (isolator, attenuators, phase shifters and RF-switches) under sulfur-exafluoride (SF6). 50

3.3 RF Wave Guides layout schematic. 56

3.4 Linac layout schematic - low energy zones and interaction point. 57

3.5 Linac layout schematic - low energy gamma characterization. 58

3.6 Linac layout schematic - high energy zones. 59

3.7 Linac layout schematic - high energy interaction point. 60

3.8 Linac layout schematic - high energy gamma characterization. 61

3.9 Dipoles 3D models - Type A, B, C and D on transfer lines bend electrons from about 15 to 40 degrees. Type F and G on dump linee bend electrons of about 90 degrees. 62

3.10 Quadrupoles 3D models - Type A, B and C used in drift beam pipes whyle Type D used in triplets. 63

3.11 Steerers 3D models - Type B is used at beginning and end of accelerating structures while other types on beam pipes. 63

4.1 MPS Framework - In blue the fast-interlock system hardwired to critical accelerator systems, in green systems monitored under EPICS Control System and in yellow the beam loss monitors to check performances. 73

4.2 MPS Framework layers - Blue links make the hardwired network which allow the high-reliability communication between Fast-Interlock and monitored systems; Green links show the EPICS data network provided by the control system that is used by to share data between all systems. 79

4.3 Fast-Interlock system monitored devices topology - RF Modulators, LLRF crates and WaveGuides vacuum controller placed on the Roof Level; Vacuum controller and PLCs for modules from 1 to 21, Personnel Safety System (PSS), low energy IP (LEIP), high energy IP (HEIP) laser and photocathode (PC) laser shutters placed in GP08 technical room on ground level; Vacuum controller and PLCs for modules from 22 to 36 placed in GP04 technical room on ground level. 80

4.4 Fast-Interlock system topology - Master units placed on the Roof levelel collect data from the slave units chains from GP08 and GP04. The two chains are fully independent as required from Dual Modular Redundancy schema. 81

5.1 Fast-Interlock system - Hardware design. 97

5.2 Fast-Interlock system - Slave units state-chart. 100

5.3 Fast-Interlock system - Master unit controller state-chart. 101

5.4 Fast-Interlock system - Master unit FPGA state-chart. 102

5.5 Fast-Interlock system - WaveForm Mask design. 104

5.6 Fast-Interlock system - WaveForm Mask algorithm flow-chart. 106

5.7 Fast-Interlock system - WaveForm Mask hardware design during ELI-NP-GBS RF Gun conditioning at HELSA. 107

5.8 WaveForm Mask - Algorithm functionality example on RF reflected signal: on left, an “healthy” signal; on right, the mask broken when a breakdown happens. Green curve is the current waveform while the blue and red curves identify the region of tolerance. 108

5.9 EPICS-based Supervisor - Hardware design. 109

5.10 EPICS-based Supervisor state-chart. 110

5.11 Black arrow show primary electrons or electrons shower losses which cross the fiber with a θ angle. When the cherenkov light (blue arrow) with θ_C semi-cone angle is trapped inside fiber this could reach: upstream the MPPC and downstream the fiber termination cut to minimize reflection and avoid echos. 113

5.12 Cherenkov BLM - blue and red segments show the different optical fibers trunks along the accelerator. 115

5.13 Cherenkov BLM benchtest at SPARC˙LAB. Bottom, the SPARC accelerator lattice; on the top, BLM signal (blue curve) with first screen (left) and with second screen (right) inserted. 117

5.14 Hall probes BLM - red dot show all dipoles of the accelerator where an hall probes are installed. 118

5.15 IP Trajectory feedback - Lattice of low (up) and high (down) energy IPs. In green CBPMs, in yellow XY correctors, in purple the diamond detector. 122

5.16 IP Trajectory feedback algorithm flow-chart. 123

5.17 Vacuum windows - Energy deposition on transverse plane for the windows of the high energy dump. 126

6.1 The ELI-NP-GBS Machine Protection System V-model for the *life-cycle* development. 129

6.2 Fast-Interlock system Verification - Functional dependencies of between the two Fast-ILK systems in parallel, their master and slave units and I/O Modules. This schema take in account both hardware dependency (like the eterCAT network) and software one (slave communication through master unit controller). 131

List of Tables

1.1 Main parameters of the ELI-NP-GBS Gamma beam. 19

1.2 Electron beam parameters of the ELI-NP-GBS Linac. 22

1.3 Laser pulse main parameters of the ELI-NP-GBS. 22

2.1 Safety Integrety Levels definitions as probability of failure for both on demand mode and continuos mode. 27

2.2 Risk matrix for the SIL evalutation. Thanks to this scheme is possible define the required SIL for a SIF. Columns show the likehood of the hazard happening while rows list the severity of the potential injury. The indicated SIL is the minimum required for the combination of frequencies vs damages. If the SIL is not expressed means that the combination require a SIL lower then SIL-1 then such SIF doesn't require to follow the IEC 61508. . 32

3.1 Vacuum regions overview groupped by accelerator's zone. 54

3.2 ELI-NP-GBS requirements for the Machine Protection System. 70

4.1 Risk matrix for the SIL evalutation - Columns show the likehood of the hazard happening while rows list the severity of the potential injury. The blue cell is the required SIL for Fast-Interlock system (SIF-1). The green cell is the required SIL for Supervisor (SIF-2). The yellow cell is the required SIL for Beam Loss Monitors (SIF-3). 77

4.2 Hardwired links for the Fast-Interlock system - For each monitored device: the signal type from the Fast-Interlock point-of-view, the required link type, the location inside the accelerator building and the required number of links for each one of the two Fast-Interlock system. 83

5.1 Fast-ILK I/O Modules - For each type of I/O Modules the related number connected into master and slave units. 98
5.2 Cherenkov BLM - list of optical fibers required to cover the whole accelerator.115
5.3 Hall probe BLM - list of bending magnets where an hall probe is placed. . 119
5.4 FLUKA simulation parameters for the evalutation of the heat load on vacuum windows of the high energy dump. 126

6.1 Mean Time Between Failures reported for each element of F-ILK system. . 132