Dependability Requirements and Design Compliance for Interlock Systems

Patrice Nouvel, Puccio Bruno, Jonker Michael, Hélène Tap

Dependability Requirements and Design Compliance for Interlock Systems

P. Nouvel[1,2,3], B. Puccio[1], M. Jonker[1], H. Tap[2,3]
[1] CERN, Geneva, Switzerland
[2] CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France
[3] Univ de Toulouse, INP, F-31400 Toulouse, France

***Abstract*— In systems engineering process, an early stage is to set up and analyze the system requirements. In high energy machine field, the protection systems have challenging dependability requirements to reach the needed system safety level. This paper presents a new methodology to determine dependability requirements for Interlock systems. This methodology is applied to the future Compact LInear Collider (CLIC) study. Going further, it is extended to check a design proposal compliance with these requirements.**

I. Introduction

In high energy particles accelerators field, Interlock Systems are key part of the machine protection systems. At CERN (European Organisation for the Nuclear Research), a central Interlock System has been designed for the Large Hadron Collider (LHC). Its development process has brought to use a safety-system and systemic approach, resulting in a formalization of the life-cycle of a protection system [1].

With new generation of high energy machines such as the Compact LInear Collider (CLIC) or the International Thermonuclear Reactor (ITER), protection systems will benefit from this experience and shall integrate it in the early stage of their design process.

A lot of work and studies have been done to evaluate and analyse the dependability of existing interlock or interlock-related systems [2], [3] [4], but none have previously investigated a systemic methodology to determine dependability requirements. This is the motivation of this study: to propose a generic methodology that can be implemented at the design phase level. This study is coupled with an application to the CLIC Interlock System design proposal [5]. Going further, the methodology is extended to determine if the proposed design is compliant with the established requirements.

In the first part of this paper, the dependability requirements are fixed. This is done through a reusable methodology, inspired by previous work in the machine protection field. The second part proves the compliance of the proposed design.

II. CLIC Interlock System Framework

The CLIC is a linear lepton (positron-electron) collider. It is designed with a new two beams acceleration approach in the multi-teraelectronvolt (3TeV) range [6]. It aims to perform precision physics based on new physics discovered by hadrons colliders (such as the LHC) [7].

The CLIC has a high beam power (up to 70MW), able to destruct easily part of the machine equipment. Moreover, there are many types of failures which can lead to machine damage: fast failures (e.g., accelerating structure breakdown), inter-cycle failures (e.g., equipment breakdown) and slow failures (e.g., alignment drift). Consequently, several protection strategies have been foreseen [8]: e.g. passive protection, preventing system.

The purpose of an interlock system is to increase the machine safety while not decreasing significantly its availability. It is done by preventing uncontrolled energy losses. The main ability of an Interlock System is to inhibit (respectively to trigger a dump) the next (respectively the current) beam.

In the CLIC case, each inter-cycle (i.e., between two pulses), a beam permit is released. This beam permit can have two states: a VETO decision inhibits the next beam while a PASS decision does not. This inhibition can be triggered on two types of stimulus. The first type comes from critical equipment of the machine. Equipment is considered as critical when its failure mode may lead to beam instability. The second type of stimulus comes from a post-pulse analysis. This analysis performs a fast beam quality analysis during the inter-cycle in order to assert the beam stability.

III. Establishing dependability requirements

Dependability is a global concept [9] used to describe many aspects of safety engineering. In Interlock System framework, the most important attributes are the *reliability* and the *availability*. To establish them, a systemic methodology has been developed. It has been strongly inspired from the Protection System Life-cycle (previously mentioned [1]) which is derived from IEC-61508 Life-cycle [10]. The different stages are described hereafter.

(A) The first step is to understand the machine concepts, its equipment and its operation.
(B) The second step is to identify the failures and the corresponding risks expected to be covered by the Interlock Systems.
(C) The third step is to analyse these identified risks.
(D) The fourth step is to determine the needed risk reduction to reach a tolerable level (tolerable level is defined at the first stage).

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

A. CLIC requirements and parameters

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

1) Safety requirement: From CLIC Machine protection study [8], the risks are considered as tolerable when their cumulated impacts lead to less than few percent of downtime or of the yearly operational budget. The risk is defined as the combination between the failure rate and its impact. As a first conservative appreciation, the tolerable risk has been fixed to one catastrophic event every ten thousands years. A catastrophic event is defined as implying more than one year of downtime. The underlying assumption is that non-catastrophic events are assumed to have a risk inferior to the catastrophic one.

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

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

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

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

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

B. Risk identification

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

The Interlock System has to prevent uncontrolled energy loss at two different stages. The first stage is to prevent critical equipments failures turning into beam instability. The second stage is to prevent slow beam instabilities turning into an uncontrolled energy loss. These two stages are represented in Figure 1.

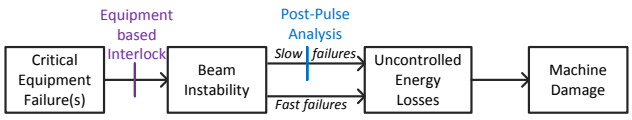

Fig. 1. Hazard Chain for Interlock System

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

C. Risk analysis

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

1) Method 1 - based on operational statistics : As a first calculation, critical equipment failure rate and slow beam instabilities rate are both considered to be in the same order of magnitude as for the LHC case. The data provided by the Post Mortem system for the LHC [11] all along the operation year 2011 are therefore used. These two failure rates are summarized in Table I.

TABLE I
RISKS ANALYSIS SYNTHESIS

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

Summing up these two rates gives an overall rate of:

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

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

- one unstable beam leads to *ten seconds* downtime. Indeed, it would trigger a transient interlock request. Ramping up the beam until its nominal luminosity will then take these ten seconds (estimation from the expected operational scenario [8]).
- the machine downtime caused by unstable beams must be lower than 10%; it leads to a maximum rate of one unstable beam every one hundred seconds.
- 1% of unstable beams are leading to non-negligible machine damage, if not inhibited.

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

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

D. Risk reduction determination

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

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

b) False VETO *decision:* It is related to machine availability. Depending whether it is a permanent or a transient failure, it will not have the same impact on the overall availability. To compute the impact of these failures, the time to repair needs to be known. It is estimated at *ten seconds* and *four hours* for respectively *transient* and *permanent* failure. The permanent failure repair time is extracted from an availability study [12] with an extra margin of 25%. The transient failure time-to-repair is related to the time needed to ramp the beam intensity back to the nominal value. For information, some studies take in account intermittent failures [13]. This type of failure will be neglected as it is more likely to happen on software-based systems.

The risk reduction is computed by dividing the tolerable risk (defined in Section III-A) by the machine failure rate (Table I). It should be noted that the resulting rate is independent of the demand (i.e., an interlock request). The rate *on-demand* corresponds to the tolerable risk.

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

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

TABLE II
FAILURE MODES REQUIREMENTS

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

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

E. Interlock System Dependability requirements

The last step to establish dependability requirements is to translate the Interlock System failure rates in terms of dependability attributes (following the definitions specified in [9]).

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

TABLE III
INTERLOCK SYSTEM DEPENDABILITY ATTRIBUTE

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

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

According to the failure definition in [9], false PASS decisions are taken in account in the reliability computation only if they are observed. As it is specified to be less than once every 10 000 years, it does not affect significantly the rate.

IV. REACHING DEPENDABILITY REQUIREMENTS

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

The following sections explain and apply the methodology to prove the proposed design compliance. This is done by defining the success conditions through a simulation and then, by measuring failure rates on a hardware prototype.

Compliance of a design proposal is achieved if it reaches the established requirements. However, at design phase, it is impossible to measure directly these attributes. Consequently, a simulation has been performed to define measurable success conditions.

A. Model

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

Following specifications [8], the CLIC Interlock System is implementing a beam permit loop. As it is a crucial function, duplication of the loop is planned. Its synoptic without redundancy is shown on Figure 2.

A signal is generated by the master node on every loop. Every node (a.k.a.the slaves) has the ability to open the loop

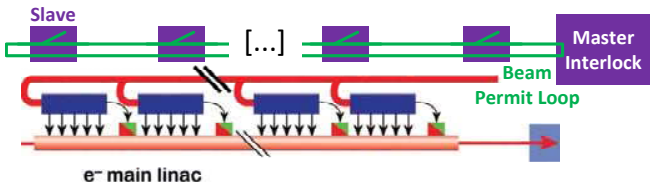

Fig. 2. CLIC Interlock System overview

twice (go and back of the permit loop) and will do so as soon as there is an interlock demand.

The nodes are initially closed (PASS decision) and are supposed to open (VETO decision) as soon as a request is received. The model is represented in Figure 3 and its underlying assumptions are listed hereunder:

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

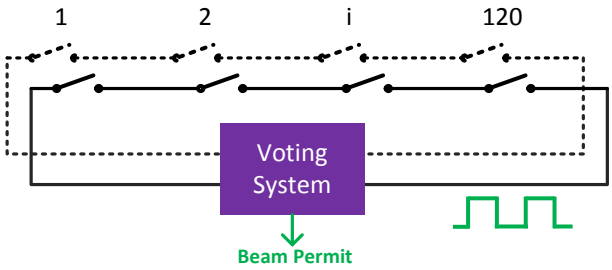

Fig. 3. Architecture model

Different redundancy scenarios (Table IV) have been pre-selected for the study. Each case has its pro and cons and have been described in a previous study [2]. Despite it is not the main challenge, cost is a limiting factor. Thus, the maximum redundant lines have been limited to three.

TABLE IV
REDUNDANCY SCENARIO

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

B. Methodology and simulation

Once the model has been defined, the goal is to translate the Interlock System dependability requirements to the node level. Indeed, this will lead to measurable success conditions for design compliance.

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

TABLE V
SIMULATION OBJECTIVES

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

The Matlab simulation tool (developed in a previous study [2]) generates interlock demands with a user-defined probability. In current case, it is fixed to the critical equipment failure rate. The system is emulated by 120 nodes and their user-defined failure rates. The redundancy is user-defined as well. The simulation gives then the system failure rates. the concept of mission used by the simulation software corresponds to a maximum 10 hours run. The mission ends when the interlock demand is successful, missed or when there is a false VETO decision.

The results of the tolerable failure rate are obtained by searching the highest node failure rates while still compliant with the objectives, for each selected scenarios.

C. Simulation results

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

TABLE VI
SIMULATION RESULTS - SINGLE NODE FAILURE RATES

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

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

D. Prototype

A hardware demonstration including a prototype node has been performed. An overview of this demonstration is given on Figure 4. It is implementing a one-out-of-one beam permit loop with three nodes (one master and two slaves).

The goal is to be as close as possible to what is the expected final node. Consequently, the prototype node uses technologies planned to be employed, both inside the node

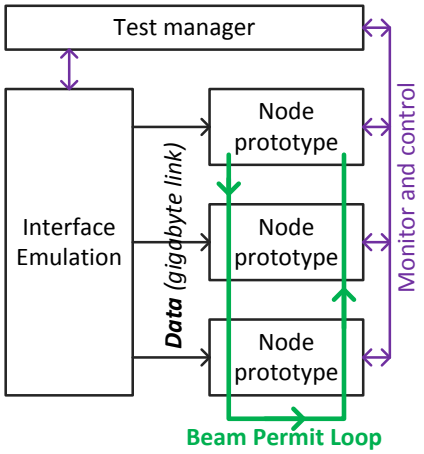

Fig. 4. Hardware Demonstration Synoptic

(functions implemented in FPGAs) and at its interface with the control system (Gigabyte transceivers).

In figure 5 is represented an internal view of the prototype node. The black boxes are the sub-functions conditioning the node behaviour. The purple boxes represents the sub-functions needed to perform the failures rates measurement.

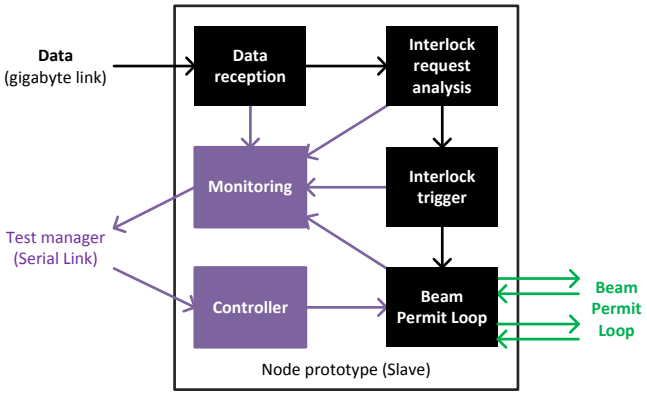

Fig. 5. Prototype node functional overview

The measurement consists to send continuously a set of 32 values via the gigabyte link. In the current case, this set of data is sent from a RAM (Random Access Memory). At the data reception, data is filtered and corrupted data are rejected as no error correction mechanism has been implemented. Then, a fast and simple data analysis is performed to detect if a interlock is requested. This analysis is based on thresholds comparison. The result of this sub-function is given to the interlock trigger which will open the loop if an interlock is requested.

E. Measurements and accelerated testing

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

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

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

In order to assert that measured rates are not linked to a specific prototype node, the measurements have been repeated on the three prototype nodes.

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

Increasing use rate has been done by accelerating the data set readout. Each time the full RAM has been sent (30 values), a pulse has been emulated. A CLIC pulse corresponds to 20 ms emulated. In real time, it takes about 5 μs to send the full RAM. Thus, it has been possible to perform accelerated testing by a factor 4000.

The measurement has been performed in more stressed environment than final design operational conditions. The main source of stress has been the temperature. To quantify the acceleration factor due to the temperature, the Arrhenius equation [14] has been used:

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

with:

- E_a: thermal Activation Energy
- Kb, Boltzmann's constant $\approx 8.6 * 10^{-5} eV.K^{-1}$
- T: test temperature (in K)
- T_0: standard temperature (in K)

For the numerical application:

- T_0 is 25 °C, the standard temperature considered for Spartan 6 (the FPGA used) datasheet.
- T is 48.7 °C, it has been evaluated from the VHDL design with Xilinx Power Analysis tool.
- E_a is taken at by default at 0.7eV [15]

It gives an acceleration factor due to temperature of $AF_T(48.7) \approx 7.4$

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

F. Results and discussions

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

When setting up the test bench, the functions have been configured in a less optimized mode, to make failures appear

more often. Thus, the test bench was asserted to be able to capture failures. By modifying several parameters (e.g. the speed of RAM readout), the main source of failure has been identified to be the gigabyte link. Moreover, the failures were appearing in the first minutes after powering the boards under test. This behaviour may be linked to the temperature stabilization in the electronic system.

TABLE VII
MEASUREMENTS RESULTS

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

As the main result, these rates prove the proposed design is able to reach the established requirements with a 2-out-of-3 redundancy. This result is conditioned by the simulation assumptions. Moreover, the design does not exclude to be compliant with lower redundant lines configurations.

V. FUTURE WORK

The presented study has described and applied the methodology to determine the needed dependability requirements.

It has applied the process to measure the dependability attributes of a proposed design and in order to prove its compliance.

This methodology can be applied for future Interlock Systems at their design phase. Following some assumptions, it can be also generalized to electronic protection systems, in high energy machine field.

In the short term, several enhancements could be performed for the test bench. First, the test data should be upgraded to be pseudo-randomly generated. Indeed, it would test the full combination of possible test vectors. Secondly, the accelerated testing should be upgraded by using more extreme temperature (with dedicated thermal devices).

An other option would be to use radiations, to check how reliable is the design with Single Event Upset (SEU can occur in the operational environment).

As a long-term view, several improvements can be proposed. Indeed, this study lends itself to iteration process. Each iteration, several stages of the methodology could be ripened. First idea, the input machine parameters shall be adapted as machine design goes along, including the underlying requirements (e.g., the precise unavailability budget). A second suggestion is to increase the granularity of the hazard chain. An additional proposal is to improve the machine failures rates accuracy; indeed, validity of taking data from LHC post-mortem system can be discussed. One option would be to set up a failures catalogue from the components conception. A similar work is ongoing for the Linac 4 design [16].

Another proposal would be to investigate less critical but still important dependability attributes for the Interlock Systems, such as the maintainability and the integrity. Moreover, the model shall be improved: the voting system and the target system (beam permit receiver) should be taken in account.

Finally, the hardware demonstration should be enhanced to become closer to the expected final conditions. A special effort should be dedicated to the gigabyte links which seems to be the weak point of the system.

REFERENCES

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

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

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

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

[5] Patrice Nouvel et al. Design process of the interlock system for the compact linear collider. *Proceedings of IPAC13, Shanhai, China*, May 2013.

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

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

[8] Michael Jonker et al. The CLIC Machine Protection. *Proceedings of IPAC10, Kyoto, Japan*, 2010.

[9] Algirdas Avizienis, Jean-Claude Laprie, and Brian Randell. Fundamental concepts of dependability. 2001.

[10] IEC Functional Safety. Functional safety of electrical/electronic/programmable electronic safety-related systems.

[11] R. Schmidt J. Wenninger E. Ciapala, F. Rodriguez Mateos. The LHC post-mortem system. Technical report, CERN, 2002.

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

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

[14] A. Mettas F. Bayle. Temperature acceleration models in reliability predictions: justification and improvement. *Reliability and Maintainability Symposium*, January 2010.

[15] Willian J. Vigrass. Calculation of semiconductor failure rates. *Harris Semiconductor*.

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