RELIABILITY APPROACH FOR MACHINE PROTECTION DESIGN IN PARTICLE ACCELERATORS

A. Apollonio, J.B. Lallement, B. Mikulec, B. Puccio, J-L. Sanchez Alvarez, R. Schmidt, S. Wagner, CERN, Geneva, Switzerland

Abstract

Particle accelerators require Machine Protection Systems (MPS) to prevent beam-induced damage of equipment in case of failures. This becomes increasingly important for proton colliders with large energy stored in the beam such as LHC, for high power accelerators with a beam power of up to 10 MW, such as the European Spallation Source (ESS), and for linear colliders with high beam power and very small beam size. The reliability of Machine Protection Systems is crucial for safe machine operation; all possible sources of risk need to be taken into account in the early design stage. This paper presents a systematic approach to classify failures and to assess the associated risk, and discusses the impact of such considerations on the design of Machine Protection Systems. The application of this approach will be illustrated using the new design of the MPS for LINAC4, a linear accelerator under construction at CERN.

INTRODUCTION

Given the past experience with previous accelerators and the large complexity of the LHC, the MPS design did not follow a formal approach. The increasing need to model the reliability and availability of the LHC to push it towards its operational limits is the driving factor to apply systematic approaches to MPS dependability studies.

In view of the LHC upgrades and the design of new accelerators (e.g. CLIC, ILC, ESS), it was decided to verify the applicability of a dependability-oriented approach for MPS for a smaller installation, LINAC4, with the use of formal hazard analysis techniques.

STPA: APPLICATION TO ACCELERATORS

The System-Theoretic Process Analysis (STPA, [1]) is a hazard analysis technique, which allows taking into account dependability requirements for Safety Critical systems since early design stages. It consists in the definition of few general scenarios in which the target safety could be violated (Accidents), the set of conditions which could potentially lead to their occurrence (Hazards) and the corresponding requirements for the control structures which should handle such scenarios. As the design of the control structures evolves and the knowledge on the system increases, requirements can be refined and control structures detailed accordingly.

This method can be applied to particle accelerators for handling safety from different points of view: personnel, machine and environmental safety are all relevant aspects in this context. The focus of this paper is on machine protection rather than personnel and environmental safety, even though in some cases these aspects, or a combination of them, cannot be treated independently.

The design of MPS is particularly suitable for STPA, as it has to be carried out while other systems are still under design. The choice of defining high-level control structures, which can be refined according to the updated status of the different input systems to the MPS (i.e. user systems), is the best solution for assuring the required flexibility to cope with new hazards, which were not taken into account during previous iterations.

A TEST CASE: LINAC4

In this paper STPA has been applied to a case study for a small accelerator as compared to the LHC: LINAC4, a 160 MeV linear accelerator currently under construction at CERN for H- ions [2]. It will replace LINAC2 as first element in the future injector chain. The H- beam is produced by a RF Source. A Low-Energy Beam Transfer (LEBT, 45 keV) houses a pre-chopper, transports and matches the beam to a Radio Frequency Quadrupole (RFQ). The RFQ bunches and accelerates the beam up to 3 MeV. A Medium-Energy Beam Transfer (MEBT, 3 MeV) houses a chopper and matches the beam with the subsequent accelerating structures. For normal operation the pre-chopper defines the pulse length and the chopper creates the correct beam structure to reduce losses at injection in the Proton Synchrotron Booster (PSB). In case of faults requiring beam interruption, they allow stopping the full beam at low energy (45 keV or 3 MeV). Three accelerating structures (DTL, CCDTL and PIMS) allow reaching the final energy (160 MeV).

Table 1: STPA: definition of Accident, Hazards and High-Level Requirements for the Control Structures

ACCIDENTS	HAZARDS	HIGH-LEVEL REQUIREMENTS
A1: Lack of beam for other accelerators	H1: Beam lost before reaching the transfer lines	Beam must not be lost in the Linac
A2: Damage to equipment	H2: Beam doesn't have the required quality to reach the end of LINAC4	Beam must have the required quality
A3: Release of radioactive material	H3: Radioactive leaks in the environment	Radioactive material must be surveyed
A4: Injuries to staff members	H4: Injuries during installation or maintenance	Procedures must be in place for installation and maintenance

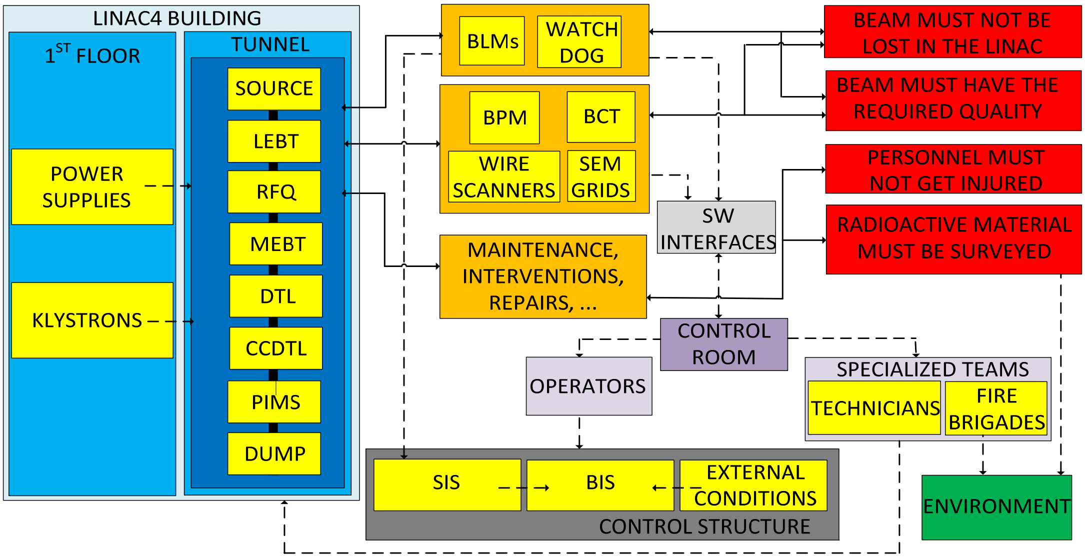


Figure 1: STPA application to LINAC4. LINAC4 is on the left of the picture. High level requirements are highlighted in red, on the right side. The systems or the teams in charge of satisfying the requirements are also shown: Beam Loss Monitors (BLMs) and Watchdogs monitor the beam losses. Beam Position Monitors (BPMs), Beam Current Transformers (BCTs), Wire Scanners and SEM grids monitor the beam quality. Operators, technicians and fire brigades manage maintenance and intervention actions. A control structure, composed of BIS, SIS and EC combines the signals coming from equipment, monitoring systems and operators and ensures safe and flexible operation.

A definition of Accidents, Hazards and MPS Requirements, according to STPA, is proposed in Table 1. Based on the first iteration of the method, the deduced high-level requirements can be fitted in a first (very generic) control structure, with the systems responsible to cope with the listed hazards. By iterating this method, refining the hazards definitions and consequently the requirements for the control structure, a more detailed scheme can be drawn. After a few iterations, the result is already fairly detailed (Fig.1) and useful considerations can be deduced from the scheme.

LINAC4 Machine Protection Systems

For what concerns the first three accidents in Table 1, the adopted control structure is finally based on the same principle as the LHC MPS [3]: a hardware-based interlock system (Beam Interlock System, BIS) is exploited to cope with fast or critical failures. It will act on the RF Source for failures occurring before the DTL; for other failures the action of the pre-chopper and the chopper is exploited to stop the beam at low energy. A software-based interlock system (Software Interlock System, SIS) is used to cope with failures with non-stringent timing constraints or when complex logic has to be implemented. As a general rule, failure modes or systems with high criticality must be surveyed by the BIS, leaving to the SIS a complementary role of protection and allowing for high flexibility. Concerning the BIS, the system topology has also been chosen to match the requirements: a daisy-chain structure is adopted, consisting of 2 Master interlock controllers, each acting on the elements in charge of stopping the beam transfer (i.e. RF Source and Choppers), and 6 Slave controllers, each assigned to a physically different ‘Interlock Zone’.

Besides the need of safety, LINAC4 has stringent requirements in terms of availability ($\geq$ 95%) and proton optimization, being the first element in the future injector chain. Therefore the so-called External Conditions (EC) are also present as a BIS input to optimize proton delivery to the different beam destinations and handle particular user requests.

LINAC4 USER Systems

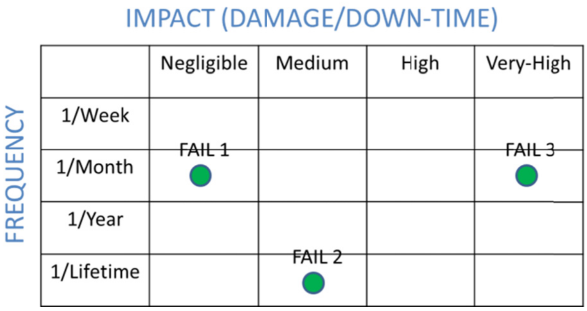
Knowing the failure modes of the user systems (i.e. the input systems of the BIS), besides the ones of the MPS, is a key aspect for correctly designing the MPS itself. A failure catalogue [4] collecting the failure modes of such systems has been finalized in collaboration with system experts. An internal website was developed to store the failure catalogue and share the achieved knowledge among the different teams involved.

The goal of the failure catalogue is to identify the main potential sources of equipment damage and unavailability. For all the failure modes which were identified, the following parameters need to be provided:

- Beam settings (current, energy, etc.)
- Quantification of beam losses (if present)
- Expected location of beam losses (if present)
- Estimated frequency of occurrence
- Estimated down-time
- Estimated damage
- Protection systems (passive/active) able to mitigate the consequences of the failure
- Other details (e.g. simulations results)

One of the direct outcomes of the predictions for frequency and down time of the different failure modes is the possibility of running Monte Carlo simulations to derive estimates of the expected machine availability. This can be done with help of commercial software or through dedicated codes. Studies are currently on-going on the subject.

Based on the parameters collected in the failure catalogue, each of the failure modes can be also inserted in a "Risk Matrix" (Fig. 2, [5]): this allows defining the criticality of the different failure modes, based on the frequency of their occurrence and their impact. The category on the horizontal axis of the matrix quantifies the impact in terms of damage or down-time. The most critical failure modes (high frequency and big impact) are then easily identified and are those requiring mitigation strategies or changes to the control structure, according to the target figures for machine availability and safety.



	Negligible	Medium	High	Very-High
1/Week				
1/Month	FAIL 1 ●			FAIL 3 ●
1/Year				
1/Lifetime		FAIL 2 ●		

Figure 2: Risk Matrix: visual representation of the impact of system failure modes (3 generic failures shown in the figure) on Equipment Safety and Availability.

An advantage of using such matrices is that they allow comparing systems and failure modes belonging to different domains (e.g. vacuum, RF, power converters, etc.) with a coherent and unique interpretation, giving clear indications of the weak points of a project.

This procedure has allowed studying in detail the worst case scenarios, assessing the associated risk and taking the necessary measures to cope with them. The application of such methodology also allowed discovering missing signals for surveillance and stimulated the discussion and collaboration among different groups.

LINAC4 USER Systems: Worst Case Scenarios

For the worst case scenarios, quantitative studies have been performed to carefully assess their impact on operation.

One of the cases studied in detail is a powering failure of the two vertical bending magnets in one of the transfer lines (connected in series), which guide the beam from LINAC4 to the PSB. In case of such an event, the beam, with a total energy of 2.56 kJ in one pulse, would be entirely lost in the bending magnet. Multi-particle transport codes (e.g. FLUKA [6, 7]) were then used to quantify the energy deposition in the 2mm-thick 216LN stainless steel beam pipe and verify the possible damage. It was calculated that ~30% of the energy would be deposited in the pipe, leading to a temperature increase of ~130 °C, well below the critical temperature of stainless steel (833 °C); no harm would be caused to the pipe itself in case of such an event, even though the impact of the remaining 70% of the energy on the magnet still needs to be estimated, because its design was in progress when the simulations were performed.

As it was foreseen since the beginning of the project, the current of all the bending magnets in the transfer lines is monitored via redundant acquisitions of the current values, which are compared with fixed tolerances. Nevertheless, this is a good example of how reliability-oriented design could provide significant inputs to MPS or Users that are identified as potentially critical.

CONCLUSIONS

A formal approach to include dependability considerations in the design of MPS systems is presented in this paper.

A case study for LINAC4 was used to show the application of formal methods to MPS design; a failure catalogue was developed to study the failure modes and to quantify safety and availability of the overall project. The use of the so-called Risk Matrices was exploited to identify weak points of the design.

A direct application of such approaches might be limited by the complexity of an entire large project. In this case the same methods could be successfully applied at the system level and the outcome gathered in a centralized framework (e.g. a website) to dynamically share information and to allow for easy interaction among different teams.

REFERENCES

[1] N. Leveson, "STPA: A New Hazard Analysis Technique", Aeronautics and Astronautics Dept, Massachusetts Institute of Technology, USA. http://csrl.scripts.mit.edu/home/stampstpa-workshop/materials

[2] F. Gerigk and M. Vretenar, "LINAC4 Technical Design Report", CERN-AB-2006-084, ABP/RF, December 2006.

[3] B. Mikulec, B. Puccio et al, "Beam Interlock Specifications for LINAC4, Tranfer Lines and PS Booster with LINAC4", L4-CIB-ES-0001, April 2013.

[4] S. Wagner et al, "A Failure Catalogue for the LHC", Proceedings of IPAC'11, San Sebastian, Spain.

[5] B. Todd et al, "Machine Protection of the Large Hadron Collider", System Safety, 2011 6th IET International Conference, 20-22 Sept. 2011.

[6] A. Ferrari et al, "FLUKA: a multi-particle transport code", CERN-2005-10 (2005), INFN_05/11, SLAC-R-773.

[7] G. Battistoni et al, "The FLUKA code: Description and benchmarking", Proceedings of the Hadronic Shower Simulation Workshop 2006, Fermilab 6--8 September 2006, M. Albrow, R. Raja eds., AIP Conference Proceeding 896, 31-49, (2007).