ISBN: 978-3-95450-231-8 ISSN: 2673-5490 doi: 10.18429/JACoW-IPAC2023-THPA057

RELIABILITY STUDIES FOR CERN'S NEW SAFE MACHINE PARAMETER SYSTEM

M. Blaszkiewicz*, A. Apollonio, S. Bolton, A. Colinet, L. Felsberger, I. Romera, R. Secondo, J. Uythoven, D. Wollmann
CERN, Geneva, Switzerland

Abstract

The Safe Machine Parameter system (SMP) is a critical part of the machine protection system in CERN's Large Hadron Collider (LHC) and the Super Proton Synchrotron (SPS). It broadcasts safety-critical parameters like beam energy, beam intensity, the beta functions and flags indicating safety levels of the beam to other machine protection elements. The current SMP will be replaced by a consolidated system during CERN's Long Shutdown 3, foreseen to start in 2026. In this contribution the results of the reliability study of the new SMP system are presented. This study quantifies the criticality of end-users by identifying the hazard chains leading to potential damage of the involved equipment. Data-driven risk matrices are used to derive acceptable failure frequencies and reliability requirements. The study encompasses Monte Carlo simulations of subsystem level configurations to support the decision-making process in this project.

INTRODUCTION

The original SMP has been in operation since 2008, which means that in LHC's Run 4, starting in 2029, it would be reaching the second decade since its initial launch. A new design, SMPv2, is currently under development. This paper presents a comprehensive overview of a reliability study of the consolidated system, which includes the following:

1. Establishing acceptable failure rates using data-driven risk matrices.
2. Defining critical hazard chains involving SMP and estimating their likelihoods.
3. Predicting failure rates, assigning failure modes and corresponding consequences.
4. Simulating critical failure scenarios involving demand, maintenance and repair policies.

Lastly, the paper summarizes the present findings and provides insights into future work.

System Description

The SMP [1, 2] is a safety-critical system providing information about critical parameters of the accelerator to user systems to implement critical protection functions. As such, it must be highly reliable to avoid lengthy and costly repairs while ensuring high availability.

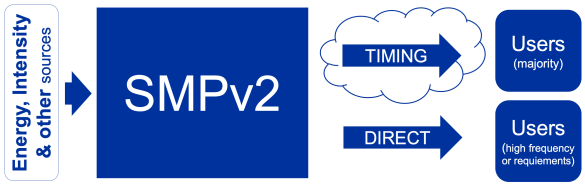

Figure 1: Inputs and outputs of the SMPv2 processing.

As indicated in Fig. 1, the SMPv2 will receive its inputs from energy and intensity sources – and based on those, it will calculate the flags. Those will be sent either via a timing network or through direct user connections. Seven flags will be distributed to thirteen defined users in the LHC and seven flags delivered to nine users in the SPS. Besides the flags, the beam energy, beam intensity and the beta-functions at the LHC experiments will be transmitted.

Figure 2 shows the functional block diagram of the SMPv2. The SMP system is based on VME64x and consists of 7 PCBs divided into three functional groups: receivers, generators and arbiters. Each function is realized on the same type of hardware board, called CISX, using different firmware. Each signal is provided redundantly. Receivers R_C and R_D are handling the input from the fast Beam Current Transformers (BCT). After receiving the inputs, receivers forward them redundantly to two generators. They evaluate the flags by applying logic specific to each case. Next, the flags arrive in the arbiter, which performs logical conjunction on logical flags and selects the highest value for numerical ones. This enhances safety and ensures that the correct values are transmitted to users.

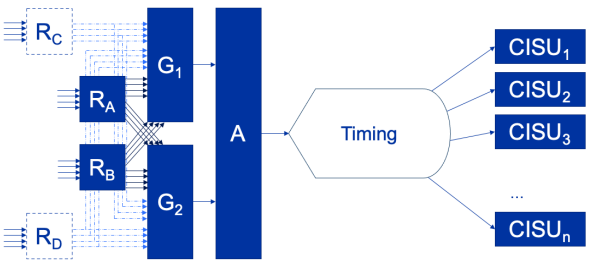

Figure 2: Functional block diagram of the SMP system. Boxes R_A and R_B represent receiver boards, G_1 and G_2 generators, A the arbiter and $CISU$ are boards used to provide flags to the users. R_C and R_D are receivers for the signals from the beam current transformers (BCT).

* milosz.blaszkiewicz@cern.ch

ISBN: 978-3-95450-231-8 ISSN: 2673-5490 doi: 10.18429/JACoW-IPAC2023-THPA057

Most Critical Flags

The most critical flags of the SMPv2 have been identified and are shortly discussed in the following.

The Setup Beam Flag (SBF) in the LHC is provided, among other destinations, to the Ring Beam Interlock System (BIS [3]). The BIS is designed to initiate a beam dump when an unsafe situation is encountered by one of its user systems. To ease the commissioning of the LHC, certain user connections can be masked at the operator's discretion during operation with safe beams (i.e., a combination of sufficiently low intensity and energy), i.e. with SBF set to *TRUE*. These masks are automatically removed, when SBF changes to *FALSE*.

The Movable Devices flag is a safeguard of the mobile equipment used in the LHC experiments. Some of the devices, such as Roman Pots or VELOs, must be placed very close to the beam, however, they cannot remain there all the time. The SMP calculates the flag indicating safe conditions when the devices can be close to the beam and communicates it to the experiments.

The Setup Beam Flag and Probe Beam Flag in the SPS are provided to the SPS Extraction BIS. They ensure that a beam which is to be extracted to the LHC meets the limits so that potential problems can be eliminated before higher beam intensities and energies are involved. Both are essential at the beginning of each fill, as there are specific requirements and order in which combinations of these (and other) flags decide whether and when a beam of given parameters may be injected.

HAZARD CHAINS

The reliability requirements for the SMP are determined by analyzing the acceptable failure frequencies of the systems it safeguards. This involves inspecting each flag and user individually and determining the reliability target based on the most critical case. The acceptable failure frequencies are established using risk matrices.

Not all SMP failures directly translate into critical consequences. Very often, additional conditions mitigate the risk of such an event. Appropriate identification of those circumstances and their corresponding probabilities is essential to avoid overestimation of reliability targets. This is done with hazard chains.

Acceptable Failure Frequencies

Data-driven risk matrices [4, 5] have been developed at CERN in which acceptable failure frequencies are defined for the different CERN accelerators. They properly address the relationship between availability and reliability expectations based on the historical data. Each system is assessed in terms of damage levels, which may be caused by a malfunction after obtaining a wrong flag from the SMP. The criticality of such damage, expressed in the length of the expected recovery is translated into a corresponding acceptable failure frequencies using the risk matrices. For example, an error of the SMP in the context of the Movable Devices In (MDI) flag delivered to the LHC experiments, aside from causing movable devices damage, could also pollute the vacuum and may require a partial warm-up of the LHC to replace equipment. This would require a recovery time of one month to one year. According to the LHC risk matrix, this means that maximally one such failure is allowed within 100 years of operation.

Critical failures of certain users, relying on the SMP, lead to consequences so severe that they should not occur at all. Recovery times after such events in the said systems extend to more than one year, putting all those cases in the most stringent cell of the risk matrix, indicating an acceptable failure rate of one in 1,000 years. This group includes SBF in the LHC and SBF and PBF in the SPS.

Hazard Chain Analysis

The goal of defining elements of hazard chains is to identify circumstances in which an erroneous flag from the SMP may cause a critical failure and physical damage. The aim of the hazard chain analysis is to estimate the probability of these events.

Assumptions & Methods A hazard chain expresses a set of circumstances in which a incorrectly calculated or transmitted flag from the SMP may expose the client system or other equipment to potential danger. After such a scenario is found, it needs a probability estimation so that it becomes possible to assess how exposed a client system is to malfunctions of the SMP. The primary sources of data used in this study are two databases: the Accelerator Fault Tracker tool (AFT) [6] and the Post Mortem system (PM) [7]. Nonetheless, certain probabilities had to be estimated by experts.

Outcomes All the details established for the hazard chain analyses, including their elements and discussions, will be presented in the reports, which show that scenarios leading to critical damage have been found for the majority of flags. The analysis concludes that among the LHC flags, the highest-risk ones are the SBF and MDI flags delivered to the LHC Ring BIS and the experiments.

If the SBF in the LHC experiences a critical malfunction, the initiation of a protection beam dump by the BIS might be missed due to incorrectly masked BIS user channels, possibly causing damage of the accelerator equipment.

The MDI's hazard chain describes the fact that dangerous beam losses appear during an LHC fill while the movable devices are exposed to this situation. Based on historic data, this hazard is expected to appear in 3% of the fills.

The SBF and PBF share similar critical failure scenarios. The risk is that a high-intensity beam might be indicated by SMP as a setup or a probe beam. This unsafe beam would then be allowed to be extracted and finally injected into the empty LHC ring. Based on historical data and past experience, this risk is estimated to be present in 0.12% of all fills.

ISBN: 978-3-95450-231-8 ISSN: 2673-5490 doi: 10.18429/JACoW-IPAC2023-THPA057

PREDICTIONS AND SIMULATIONS

The study also encompasses predictions of the reliability of the SMP CISX/CISU board and simulations on a subsystem level of the entire SMP. The results provide estimations of the expected failure rates, which can be compared with the derived requirements described above.

Reliability predictions of the system boards are a key element of the study. The 217Plus standard - an updated variant of the MIL-HDBK-217F [8] - was used to predict failure rates of electronic components. For components not covered by this standard, data from the manufacturers were used. Each component was assigned failure modes and their probabilities. These data were derived from FMD-91 [9] and, its most recent version, FMD-2016 [10]. This process was automated by software scripts.

For the SMP, four general fault consequences have been defined:

- *blind failure* – not detectable, lingers in the system and eventually critically incapacitates its operation,
- *safe failure* – error which hinders the operation of the system and make it less available,
- *maintenance* – triggering repairs at the next occasion,
- *no-effect* failure.

Each end-effect is associated with a different target. *Maintenance* and *no-effect* failures have the combined probability of almost 65% – but no quantitative target applies to them. Of the remaining 35%, the majority cause safe failures. They affect availability and as such have to agree with the target of one false dump per year. The smallest share constitutes the group of blind failures. Those failures are relevant to the critical hazard chains and corresponding reliability target. The analysis is primarily focused on the latter and specifically on the CISU boards, which are not foreseen to have redundant paths – and, as such, carry greater risk of exposing the user systems to critical failures.

To better understand the failure dynamics of the system and its relation with failure scenarios and maintenance policies, stochastic Monte Carlo models were developed in AvailSim4 [11, 12] for the CISU board. The purpose of such models is twofold: first, to validate the results in scenarios that closely resemble future usage, and second, to provide well-informed recommendations regarding periodic inspections and repair strategies. Due to the flexibility of Monte Carlo simulations, the models incorporate elements of the hazard chains, making the results comparable with the targets defined directly in the risk matrices.

The results obtained for the MDI flag indicate compliance with the reliability targets in all tested scenarios. However, the results for the most critical flag – SBF – are more complex. The tested scenarios which provision annual or no checks of the system, i.e., where failures are usually not removed before critical circumstances arise, fall short of the very stringent reliability targets. The compliance with the requirements is demonstrated in maintenance scenarios where checks are performed every 12 hours, i.e. before or after every LHC fill. By this measure the combined reliability of the system increases tenfold as compared to the annual inspections.

CONCLUSION

A new version of the SMP system is currently under design. Detailed studies have been performed to ensure that the new version fulfills the required reliability criteria. Hazard chains have been defined for each flag and each user system, with the Setup Beam Flag in both, LHC and SPS, as well as LHC Movable Devices and SPS Probe Beam Flag, identified as the most critical. The requirements for those are driving the reliability targets for the SMP hardware. A component-level analysis of the first prototype of the CISU board has been conducted, along with Monte Carlo simulations on a more complex subsystem level for the most critical cases.

The results show that the current design meets the defined reliability requirements when functional checks are performed at defined intervals, e.g. before every fill.

A second prototype of the CISU board with modifications of some components and elements is currently under review and will be built soon. The component-based analysis of this prototype has started and the reliability assessment of the hardware is being updated. In addition, work is ongoing to further refine the hazard chains.

REFERENCES

[1] R. Secondo, *Safe Machine Parameter (SMP) v2 Functional Specification*, EDMS 2517245, 2023. https://edms.cern.ch/document/2517245/2.0

[2] B. Todd, *Safe Machine Parameter System Towards Nominal Beams*, MPP Internal Review, 2010. https://indico.cern.ch/event/91751/contributions/1276462/

[3] I. Romera *et al.*, "Design considerations for CERN´s second-generation Beam Interlock System," presented at IPAC'23, Venice, Italy, May 2023, paper THPA062, this conference.

[4] T. Cartier-Michaud *et al.*, "Data-Driven Risk Matrices for CERN's Accelerators," in *Proc. IPAC'21*, Campinas, Brazil, May 2021, pp. 2260–2263. doi:10.18429/JACoW-IPAC2021-TUPAB325

[5] M. Blumenschein, J. Spasic, J. Steckert, and J. Uythoven, "An Approach to Reliability Assessment of Complex Systems at CERN," in *2019 Annu. Reliab. and Maintainability Symp. (RAMS)*, 2019, pp. 1–6. doi:10.1109/RAMS.2019.8769004

[6] C. Roderick, L. Burdzanowski, D. M. Anido, S. Pade, and P. Wilk, "Accelerator Fault Tracking at CERN," in *Proc. ICALEPCS'17*, Barcelona, Spain, Oct. 2017, pp. 397–400. doi:10.18429/JACoW-ICALEPCS2017-TUPHA013

[7] E. Ciapala, F. Rodríguez-Mateos, R. Schmidt, and J. Wenninger, "The LHC Post-mortem System," CERN, Tech. Rep., 2002. https://cds.cern.ch/record/691828

[8] US Department of Defense, *MIL-217 (1991) Military Handbook: Reliability Prediction of Electronic Equipment: MIL-HDBK-217F*, 1991.

ISBN: 978-3-95450-231-8 ISSN: 2673-5490 doi: 10.18429/JACoW-IPAC2023-THPA057

[9] Reliability Analysis Center RAC, *Failure Mode / Mechanism Distributions – 1991: FMD-91*, 1991.

[10] Quanterion, *Failure Mode / Mechanism Distributions – FMD-2016*, ISBN 978-1-933904-70-2, 2016.

[11] "AvailSim4." (2023), https://gitlab.cern.ch/availsim4/availsim4

[12] "AvailSim4 - PyPI Project." (2023), https://pypi.org/project/availsim4/