RELIABILITY ANALYSIS OF THE LHC MACHINE PROTECTION SYSTEM: ANALYTICAL DESCRIPTION

S. Wagner, R. Nibali, Laboratory for Safety Analysis, ETH Zurich, Zurich, Switzerland
R. Schmidt, J. Wenninger, CERN, Geneva, Switzerland

Abstract

The design and operation of the LHC Machine Protection System (MPS) implicates a trade-off between machine safety and beam availability. A simulation-based methodology has been developed to address that trade-off. It yields the probability of the relevant scenarios *missed emergency beam dump* and *false beam dump*. This paper introduces an analytical description of the underlying model, which provides an accurate verification of the simulation results and the chance for an adequate alternative to the simulations. The paper indicates the extent to which the simulations can be replaced by the analytical model description and where the latter reaches its limits.

INTRODUCTION

The trade-off between LHC machine safety and beam availability is defined by the MPS reliability with regard to the scenarios *missed emergency beam dump* and *false beam dump*. Estimated probabilities for missed emergency beam dumps and false beam dumps are obtained by Monte Carlo simulation based on a modular model. The feasibility and usability of this methodology have been demonstrated [1, 2]. The common underlying MPS model [1] includes 4768 components modelled as individual objects, covering the Beam Loss Monitor System and the Beam Interlock System.

In search of an accurate verification of the simulation results, an analytical description of the MPS model has been developed and implemented. It provides the requested verification and supersedes simulations to a certain extent. This paper introduces the analytical description by means of the basic component model applied to a six-component system. In the second part, the results of its implementation according to the MPS model are presented. A set of cross-checks is described which allow for checking the implementation and the accuracy of the results. The comparison with the respective simulation results provides their verification.

ANALYTICAL DESCRIPTION

The component model represents the basic module of the MPS model and its analytical description. The described events are the basis of the scenarios *missed emergency beam dump* and *false beam dump*.

Basic Component Model

The component model [1] bases upon the state diagram illustrated in Fig. 1. Besides the initial state *ready*, the component can take the states *false* and *blind*, referring to different failure modes. The transition to either state, i.e. the failure of the component, is defined by the probability density function $f(t)$. It represents the distribution of the time to transition T, if the transition is considered independently.

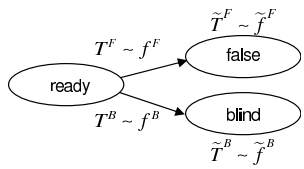

Figure 1: Component state diagram, T: Time to transition, $f(t)$: Probability density function.

Since *blind* and *false* are absorbing states, i.e. the component once in a state of failure is locked, the transitions are not independent. The dependency is described on the basis of the *false* failure mode and applies to the *blind* mode accordingly. The component going *false* at time t conditions that it has not gone *blind* at time $t' < t$, i.e. it survived with regard to the *blind* mode up to time t. The related probability density function is given by

$$\tilde{f}^F(t) = f^F(t)(1 - F^B(t)) \tag{1}$$

where $F^B(t)$ is the failure probability with regard to the *blind* mode defined by

$$F^B(t) = \int_0^t f^B(t')dt' \tag{2}$$

The probability of the component going *false* during time period t with Eq. 1 becomes

$$\tilde{F}^F(t) = \int_0^t \tilde{f}^F(t')dt'. \tag{3}$$

The probability of the component surviving with regard to the *false* mode is given by

$$\tilde{R}^F(t) = 1 - \tilde{F}^F(t). \tag{4}$$

Six-Component System

Fig. 2 illustrates a system of six identical components according to the basic component model, representing a signal path from the virtual component S (start) to E (end).

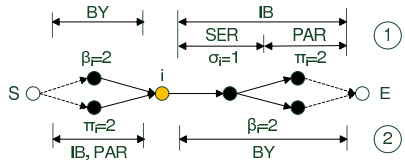

Figure 2: Six-component system representing a signal path from S to E.

The behaviour of component S follows the state diagram illustrated in Fig. 3. A signal is triggered upon component S going *system demanding* or upon a component going *false* (Fig. 1), and it is absorbed by *blind* components. The system features 1-out-of-2 redundancy at the start and end of the signal path.

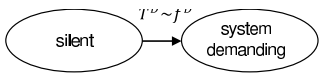

Figure 3: State diagram of component S. T: Time to transition, $f(t)$: Probability density function.

The analytical description is demonstrated on two basic events:

- **Event 1** A signal is triggered in component i within time period t (due to i going *false*) and reaches the end of the signal path E.
- **Event 2** A signal is triggered in component S within time period t (due to S going *system demanding*) and is absorbed by component i (due to i having gone *blind*).

Both events exclude signal triggering by other components during time period t.

The subdivision of the signal path with regard to Event 1 is illustrated in Fig. 2 (top). IB marks the relevant section in-between the signal triggering component i and the end of the signal path E. BY marks the section beyond the relevant section IB. Section IB is further divided into subsections SER (including components connected in series) and PAR (including components connected in parallel). β, σ, π refer to the number of components within the related section.

The probability of a signal being generated in component i during time period t and reaching the end of the signal path E (Event 1) derives from Eq. 1, 3 and 4 to

$$P^F(false_{i\rightarrow E}, t) = \int_0^t \widetilde{f}_i^F I_S I_{BY} I_{SER} I_{PAR} dt'. \quad (5)$$

Event 1 conditions

- component i going *false*: $\widetilde{f}_i^F$
- the survival of component S: $I_S = 1 - F^D$
- the survival of the components in BY with regard to the *false* mode: $I_{BY} = (1 - \widetilde{F}^F)^{\beta_i}$
- the survival of the component in SER: $I_{SER} = ((1 - F^F)(1 - F^B))^{\sigma_i}$
- the survival of the redundant components in PAR with regard to the *false* mode, excluding the case with both components *blind*: $I_{PAR} = (1 - \widetilde{F}^F)^{\pi_i} - (\widetilde{F}^B)^{\pi_i}$.

The related global probability (i.e. any component going *false*) results to

$$P^F(false_{\rightarrow E}, t) = \sum_{i=1}^{6} P^F(false_{i\rightarrow E}, t) \quad (6)$$

due to the mutually exclusive events $P^F(false_{i\rightarrow E}, t)$ for different components i.

With path subdivision according to Event 2 (Fig. 2, bottom), the probability of a signal being generated in S during time period t and being absorbed by component i analogously derives to

$$P^D(S_{\rightarrow blind\ i}, t) = \int_0^t f^D I_{IB} \widetilde{F}_i^B I_{BY} dt'. \quad (7)$$

Event 2 conditions

- component S going *system demanding*: f^D
- the survival of the redundant components in IB with regard to the *false* mode, excluding the case with both components *blind*: $I_{IB} = (1 - \widetilde{F}^F)^{\pi_i} - (\widetilde{F}^B)^{\pi_i}$
- component i going *blind*: $\widetilde{F}_i^B$
- the survival of the components in BY with regard to the *false* mode: $I_{BY} = (1 - \widetilde{F}^F)^{\beta_i}$.

The related global probability $P^D(S_{\rightarrow blind}, t)$ results from summing up all signal absorbing events, taking into account the redundancies.

Given the signal generated in S representing an emergency beam dump request, $P^D(S_{\rightarrow blind}, t)$ corresponds to the probability of scenario *missed emergency beam dump* (affecting machine safety). With the signal generated upon a component going *false* representing a false beam dump request, $P^F(false_{\rightarrow E}, t)$ (Eq. 6) corresponds to the probability of scenario *false beam dump* (affecting beam availability).

RESULTS

The analytical description according to the MPS model derives from the above description of the six-component system. It was implemented using Maple 12. The calculation was performed with t=12 hours, corresponding to the typical length of a LHC store ('mission'), and a precision of 15 decimal places for the numerical integration based on Maple's default integration method. The calculation time amounted to a few minutes on a common desktop computer.

The results obtained by numerical integration are shown in Fig. 4. They comprise five scenarios including *false beam dump* (III) and *missed emergency beam dump* (IV).

Verification of Analytical Results

The analytical description and its implementation are verified by the following cross-checks:

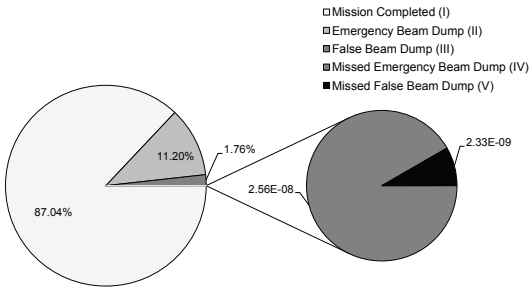

Figure 4: Probabilities of the MPS scenarios including *false beam dump* and *missed emergency beam dump*.

$$1 - P^D - P^F - P^N = 0 \quad (8)$$

$$P^D - P^D(S_{\rightarrow E}) - P^D(S_{\rightarrow blind}) = 0 \quad (9)$$

$$P^F - P^F(false_{\rightarrow E}) - P^F(false_{\rightarrow blind}) = 0 \quad (10)$$

Cross-check 1 (Eq. 8) takes into account the three basic events *emergency beam dump request signal triggered* (P^D), *false beam dump request signal triggered* (P^F) and *no signal triggered* (P^N), which are complementary. Once a signal is triggered it either goes through to the end of the signal path or is entirely absorbed by *blind* components. This characteristic is reflected in the cross-checks 2 and 3 (Eq. 9, 10).

The results satisfy Eq. 8 - 10, thus proving the analytical description and its implementation to be correct. The accuracy of the results depends on the precision chosen for the numerical integration. The precision indicates to which decimal place accuracy is guaranteed. The cross-checks of the results show the expected accuracy. Tests performed with precision set up to 45 (at the expense of calculation time) yield according accuracies.

Verification of Simulation Results

Simulation results based on 10^5 missions have been published previously [1]. For the benefit of a more advanced verification, the results of 10^7 simulated missions are used for comparison. The relative error of the simulation results is presented in Table 1 for the five MPS scenarios. The results of the analytical approach are rounded off, taking into account the limited number of missions underlying the simulation results.

The comparison shows very good accordance of the simulation and analytical approach for the frequent scenarios. The relative error with regard to Scenarios IV and V is not available because 10^7 missions are below an adequate quantity of simulation data to provide significant results.

CONCLUSIONS

The analytical description of the MPS model is introduced by means of the basic component model applied to a six-component system. Its results base upon numerical integration using Maple and include five scenarios with *missed emergency beam dump* and *false beam dump* being the most relevant with regard to LHC machine safety and beam availability. A set of cross-checks prove the implementation of the analytical description to be correct and accurate. The obtained reliability numbers are in very good accordance with related simulation results, thus representing a measure for the verification of the latter.

Table 1: Error of simulation results for MPS scenarios.

Scenario	Simulation	Analytical Description	|Rel. Error|
I	8.703938E-1	8.703698E-1	2.76E-5
II	1.120218E-1	1.120422E-1	1.821E-4
III	1.75843E-2	1.75849E-2	2.047E-4
IV	1E-7	(1E-8)	NA
V	0	(1E-9)	NA

The analytical description is on a par with the simulation approach in terms of the covered scenarios. It is superior with regard to the accuracy of the results and the insignificant calculation time compared to the extensive simulation time needed due to the rare events involved in the model. As for the used MPS model, the analytical approach thus supersedes simulations. It is to be further investigated to which extent this applies to advanced models. First attempts towards an analytical description of a MPS model including a more advanced system demand pattern and the feature of component masking [2] indicate that the advanced demand pattern inflates the analytical description in terms of complexity and the effort for its implementation. In contrast, the implementation of the advanced demand pattern in the simulations is clear and straight-forward.

In view of the apparent advantages of both the simulation and analytical approach, the merging of the two approaches represents an obvious starting point for further development. An algorithm for the automatic set-up of the analytical equations based on the graphical model representation underlying the simulations would provide an accurate and fast calculation, thus saving the user the effort of their complex and time-consuming implementation.

ACKNOWLEDGEMENT

The authors thank Daniel Alai from the Department of Mathematics at ETH Zurich for the helpful initial discussions on the analytical description.

REFERENCES

[1] Wagner, S., et al. (2008), “Balancing Safety and Availability for an Electronic Protection System”, in European Safety and Reliability Conference 2008 (ESREL 2008), Valencia, Spain.

[2] Wagner, S., et al. (2008), “Reliability Analysis of the LHC Machine Protection System: Terminology and Methodology”, in European Particle Accelerator Conference 2008 (EPAC’08), Genoa, Italy.