ARCHITECTURE FOR INTERLOCK SYSTEMS: RELIABILITY ANALYSIS WITH REGARD TO SAFETY AND AVAILABILITY

S. Wagner, A. Apollonio, R. Schmidt, M. Zerlauth, CERN, Geneva, Switzerland
A.Vergara-Fernandez, ITER Organization, St.Paul-lez-Durance, France

Abstract

In the design of interlock loops for the signal exchange in machine protection systems, the choice of the hardware architecture impacts on machine safety and availability. The reliable performance of a machine stop (leaving the machine in a safe state) in case of an emergency, is an inherent requirement. The constraints in terms of machine availability on the other hand may differ from one facility to another. Spurious machine stops, lowering machine availability, may to a certain extent be tolerated in facilities where they do not cause undue equipment wearout. In order to compare various interlock loop architectures in terms of safety and availability, the occurrence frequencies of related scenarios have been calculated in a reliability analysis, using a generic analytical model. This paper presents the results and illustrates the potential of the analysis method for supporting the choice of interlock system architectures.

INTRODUCTION

For particle accelerators like the LHC and other large experimental physics facilities like ITER, the machine protection relies on complex interlock systems. They are required to trigger machine stops in case of emergency, but not spuriously. *Machine stop* implies, for example, the extraction of the energy stored in magnet powering circuits and, in case of the LHC, the extraction of the beams from the machine.

For the interlock loops protecting the LHC superconducting magnet circuits, spurious triggers of machine stops, lowering availability, can be tolerated to a certain extent since they do not affect the longevity of the equipment. In ITER's case on the other hand, high machine availability, and therefore limited spurious triggers of machine stops are required since each fast stop causes significant magnet aging due to the induced forces. The number of tolerated spurious machine stops for the LHC lies in the range of a few tens per year (around 10% of all fills), while for ITER it is expected to be limited to only a few in the whole lifetime of 20 years .

In conjunction with the development of a prototype for ITER interlock loops, a reliability analysis comparing six possible interlock loop architectures has been performed.

This paper in the first part introduces the method and the generic model used for the analysis. The second part discusses some results of the performed studies. The third part introduces the approach developed for the verification of the model and intermediate verification results.

METHOD

The following sections summarise the most relevant aspects of the interlock loop model used for the analysis. It is based on the method introduced in a study of a part of the LHC Machine Protection System [1].

Interlock Loop Model

The model reflects an interlock loop ('system') with 4 components, as illustrated in Fig. 1.

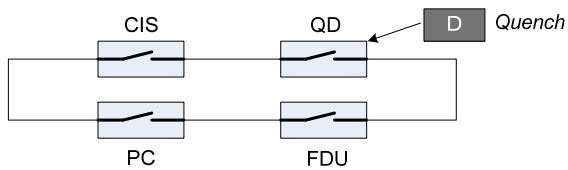

Figure 1: Basic model of interlock loop with 4 components.

The components are considered to be switches, which can fail in two modes, *blind* and *false*, according to failure rates λb and λf (Fig. 2, left). The system demand is modelled by virtual component *D,* following demand rate x (Fig. 2, right).

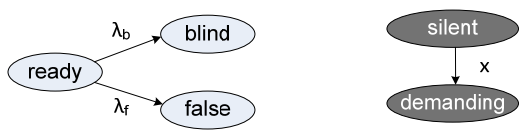

Figure 2: State diagrams reflecting component behaviour and system demand.

The different states represent the following conditions:

- *Ready*: switch closed, ready to open upon demand (initial state)
- *Blind*: failed closed, not ready to open upon demand
- *False*: Switch open, spuriously or upon detection of switch-internal failure (i.e. without demand)
- *Silent*: nominal condition of monitored machine equipment, no demand (initial state)
- *Demanding*: Emergency condition detected, demanding machine stop (loop opening)

The possible state configurations occurring within a given observation time tf, represent four scenarios. They are exemplified by means of a generic quench loop, including components QD (Quench Detection), FDU (Fast Discharge Unit), PC (Power Converter) and CIS (Central Interlock System, Fig. 1). In case a quench of a magnet is detected (i.e. system demand), the QD is triggered to open the loop, thus informing the PC to switch off the power supply and the FDU to extract the energy from the magnet powering circuit:

(1) *Mission completed*: neither quench nor spurious loop opening during an operational cycle
(2) *False trigger* (→Preventive stop): loop opening due to failure of any switch (mode *false*), without quench
(3) *Demand success* (→Emergency stop): loop opening by QD upon quench
(4) *Demand missed* (→Missed emergency stop): missed loop opening upon quench due to QD failed closed (mode *blind*)

Scenario 4 (worst case scenario) includes the potential of severe damage to the machine, hence interfering with machine safety. Together with scenarios 2 and 3, it defines the machine availability reflected by scenario 1.

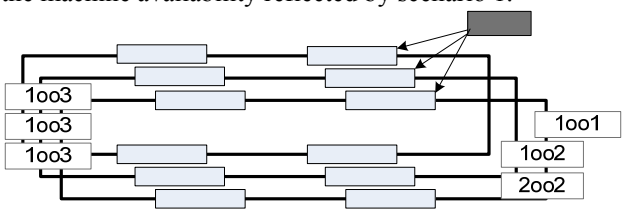

Figure 3: Models of interlock loop for different architectures (featuring up to three redundant lines).

Figure 3 gives an overview on the models for the six architectures under consideration, derived from the generic model introduced above:

- 1oo1: single-line solution, no redundancy
- 1oo2: two redundant lines with 1-out-of-2 logic
- 2oo2: two redundant lines with 2-out-of-2 logic
- 1oo3: three redundant lines with 1-out-of-3 logic
- 2oo3: three redundant lines with 2-out-of-3 voting
- 3oo3: three redundant lines with 3-out-of-3 logic

For a *False trigger* of *2oo2* for example, both lines need to be open due to switch failures.

Model Input Parameters

Table 1 summarises the model input parameters, representing seven 'degrees of freedom' for case studies.

Table 1: Model Input Parameters

Parameter	Description
Components:	
λf	Failure rate *false*
λb	Failure rate *blind*
x	Demand rate
Operation:	
tf	Observation time
Architecture:	
k	Number of lines
n	Number of components/line
-	'Voting'

Model Assumptions

The presented model includes a series of assumptions and simplifications:

- Independent failures of components
- Identical components (with regard to reliability, i.e., failure rate)
- All components in initial state at t=0 (system 'as-good-as-new')

Besides these rather common assumptions, there are a few others more specific to an interlock loops:

- Any switch opening is recognised as 'line opening', independent of the (potentially *blind*) state of components in the same line. This reflects a loop with redundant readout.
- The demand is limited to one loop component (i.e. QD). The demand signal is fault free and, in case of redundant lines, is simultaneously distributed to all lines (Fig. 3). This neglects possible redundancy of the triggering source.
- A switch opening due to failure mode *false* is permanent, i.e. an open switch stays open till the end of current operational cycle. This neglects transient failures.
- The voting (included in the 2oo3 architecture) is fault free. This assumes a technical solution for the voting that does not add significant complexity that might lower reliability.

Analytical Model Description

The model uses an analytical description [1,2] adapted and extended to the characteristics of the system under consideration.

The most relevant improvement concerns the inclusion of voting and the (related) elimination of the *False missed* scenario (being absorbed in the remaining four scenarios).

Model Implementation

The analytical model description is implemented using Maple like in the previous studies [1,2].

RESULTS

Table 2 shows the default values of the input parameters, defined as the starting point for extended case studies.

Table 2: Default Input Parameters

Parameter	Default value		Comment
Components:			
λf	1E-4	[h^{-1}]	MTTF: 12 months
λb	1E-5	[h^{-1}]	MTTF: 15 years
x	2E-4	[h^{-1}]	MTTF: 6 months
Operation:			
tf	720	[h]	30 days
Architecture:			
n	4	[-]	cp. basic model

The values for the component failure rates (λf, λb) and the demand rate (x) are derived from MTTF estimations based on experience with the LHC. The observation time (tf) of 30 days reflects the expected length of an ITER

Table 3: Scenario Probabilities for the Different Architectures (Default Input Parameters)

	1oo1	1oo2	2oo2	1oo3	2oo3	3oo3
Mission completed	6.50E-01	4.88E-01	8.12E-01	3.66E-01	7.31E-01	8.52E-01
False trigger	2.33E-01	4.10E-01	5.68E-02	5.43E-01	1.42E-01	1.40E-02
Demand success	1.17E-01	1.03E-01	1.30E-01	9.08E-02	1.27E-01	1.32E-01
Demand missed	3.99E-04	1.54E-06	7.97E-04	6.57E-09	4.60E-06	1.19E-03

operational cycle, i.e. the continuous operation between two maintenance periods.

The number of components per line (n) corresponds to the basic model (Fig. 1 and 3). The remaining architecture parameters are defined by the architectures under consideration.

Table 3 presents the results for the case study based on the default input parameters:

- With regard to *Demand missed*, the 1oo3 architecture is top (lowest probability), while with regard to *Mission completed* the 3oo3 architecture is (highest probability).
- With regard to the combined aspects, the 2oo3 architecture solely ranks in the 'top three solutions' for both *Demand missed* and *Mission completed*.
- Compared to the 1oo1 architecture (ranking second best with regard to the combined aspects), the 2oo3 architecture features a decrease of *Demand missed* and an increase of *Mission completed*.

Translating these observations in terms of safety and availability, the following statements result (for the given default parameters):

1. With regard to safety, the 1oo3 architecture is top, while with regard to availability it is the 3oo3 architecture.
2. With regard to the combined aspects, the 2oo3 architecture is a best-compromise solution, ranking top three for both safety and availability.
3. Compared to the 1oo1 architecture, the 2oo3 architecture includes an increase of both safety and availability.

In order to prove these statements, a series of sensitivity analyses have been performed. In the following, the results of the variation of failure rate *false* (λf) are presented. The further sensitivity analyses based on the variation of the remaining input parameters (*blind* rate, demand rate, observation time and the number of components per line) are beyond the scope of this paper.

Variation of λf between 1E-7 h^{-1} and 1E-2 h^{-1}

The variation reveals that while statement 1 holds for the entire considered range of λf , statements 2 and 3 are true (T) for λf ≤ 1E-4 h^{-1} only, not for higher λf (Table 4).

The reason is that for higher λf, the 2oo3 architecture exceeds the 1oo1 architecture in terms of *False trigger* (Fig. 4, crossing line), which results in a decrease of *Mission completed* compared to the 1oo1 architecture (Fig. 5). Hence, as of a certain parameter range, the 2oo3 architecture is outperformed by 1oo1 in terms of availability.

Table 4: Assessment for Statements 1 to 3 for λf Varied between 1E-7 h^{-1} And 1E-2 h^{-1}

Stat.	1E-7	1E-6	1E-5	1E-4	1E-3	1E-2
1	T	T	T	T	T	T
2	T	T	T	T		
3	T	T	T	T		

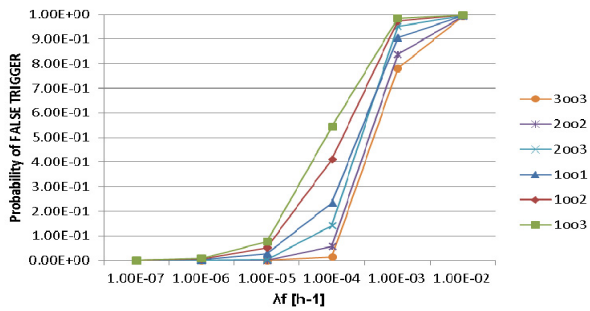

Figure 4: Probability of *False trigger* against λf between 1E-7 h^{-1} and 1E-2 h^{-1}.

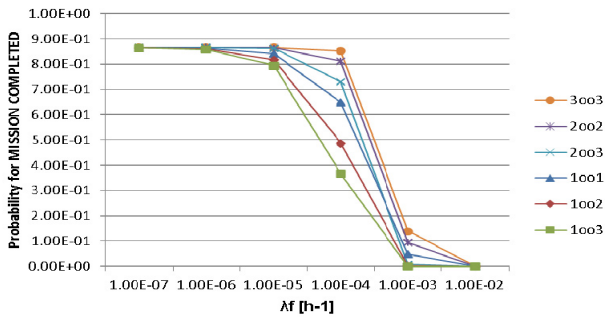

Figure 5: Probability of *Mission completed* against λf between 1E-7 h^{-1} and 1E-2 h^{-1}.

Summarising the above observations, the following extension to the three statements is to be made:

4. Statement 2 and 3 require reasonably low failure rates *false*, λf .

The confirmation of statement 1 is provided by Fig. 5 and 6, showing the advantage of the 3oo3 architecture with regard to availability (Fig. 5) and the advantage of the 1oo3 architecture with regard to safety (Fig. 6).

Discussion

The lower performance of the 2oo3 compared to the 1oo1 architecture for high λf can be explained by the total number of components included in the architectures. As of a certain λf, the voting is no longer able to compensate

for the (three times) higher amount of components. However, such high failure rates are not reflecting electronic devices in use nowadays. Their rates are expected to be in a lower range.

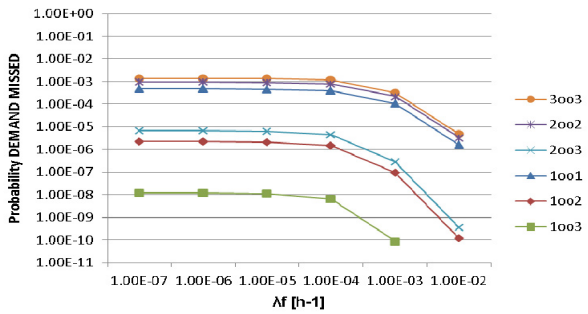

Figure 6: Probability of *Demand missed* against λf between 1E-7 h^{-1} and 1E-2 h^{-1} (logarithmic scale).

The constraint expressed by statement 4 only relates to the availability aspect. The 2oo3 architecture does appear in the top three with regard to safety for the entire considered range of λf, hence outperforming 1oo1 in terms of safety.

The introduced method allows for additional comparison from a different point of view. Instead of assessing the performance of the architectures based on given input parameters, the architectures can be compared in terms of the reliability of the components required to achieve a desired system performance. This may lead to statements like *in order to achieve an availability X, the 2oo3 architecture allows for Y orders of magnitude higher component failure rates compared to other architectures*.

The presented analysis has been taken into account in the decision-making with regard to the design of a prototype for the ITER quench loops. Considering the results of the analysis and the possibility for testing and maintenance during operation provided by redundant architectures (which can counter the related disadvantage of increased amount of components), a 2oo3 solution is being envisaged.

VERIFICATION

As mentioned above, the analytical model description used in this analysis is a further development of the approach introduced in earlier studies. For the verification of the results, and the underlying analytical description, a study based on Monte-Carlo simulation has been started.

The simulation of a single operational cycle includes two basic steps:

- Generation of random numbers representing the times of state transitions (i.e. of component failures or system demand), according to the input parameters (failure and demand rates)
- Assignment of the resulting time sequence of state transitions (within the given observation time) to one of the four scenarios

The simulation of a multitude of operational cycles then allows for statistical analysis:

- Derivation of the relative occurrence frequencies of the different scenarios

The simulations are implemented using Matlab. Two independent approaches are being developed which differ in the scenario assignment step:

- Explicit assignment based on the time sequence of random numbers
- Implicit assignment based on a graphical model representation including step functions and signal transmission (implemented using Simulink)

The intermediate results of the explicit approach show good agreement with the results presented in Table 3, indicating relative errors in the range between 1E-6 and 1E-2 for the frequent scenarios (based on 8E7 simulated cycles). For the rare scenario *Demand missed*, the error is not meaningful since the number of simulated cycles is too low for a reasonable accuracy.

The implicit approach is still under development. Currently, there are results available on the 1oo1 architecture only and with fewer simulated cycles due to a significantly increased need of simulation time compared to the explicit approach. The intermediate results show a relative error in the range between 1E-4 and 1E-1 for the frequent scenarios (based on 5E4 simulated cycles).

CONCLUSIONS

This paper presents the method and results of a reliability analysis addressing the properties of various interlock loop architectures with regard to machine safety and availability. It shows the advantages of a 2oo3 architecture for systems with high requirements in both safety and availability.

Further application and development of the method is ongoing. Subsequent studies are being performed addressing the interface between interlock loops (e.g. quench loop) and the protected machine subsystems (e.g. magnet powering circuits), including detectors.

The Monte Carlo approach for the verification of the different studies is being further developed. In addition, the validation of the models is to be addressed, in particular with regard of the fault-free voting assumption underlying the model.

REFERENCES

[1] Wagner, S. (2010), "LHC Machine Protection System: Method for Balancing Machine Safety and Beam Availability", Doctoral Thesis (Diss. ETH No.19043), ETH Zurich

[2] Wagner, S., et al. (2009), "Reliability Analysis of the LHC Machine Protection System: Analytical Description", in Particle Accelerator Conference 2009 (PAC09), Vancouver, BC, Canada.