ISBN: 978-3-95450-132-8 doi:10.18429/JACoW-IPAC2014-THPME058

RISK ANALYSIS AND MACHINE PROTECTION OF SIS100

C. Omet*, M. Mandakovic, D. Ondreka, P. Spiller, J. Stadlmann
GSI Helmholtzzentrum für Schwerionenforschung GmbH, D-64291 Darmstadt, Germany

Abstract

To ensure safe functionality and reduce unnecessary shutdowns, a risk analysis of the main driver accelerator for the FAIR project SIS100, has been done. The analysis includes all major technical systems and was done accordingly to EN 61508. Results of the analysis and appropriate countermeasures for detection and/or mitigation of the failures are presented. Furthermore, an estimation of the accelerator's availability is given.

INTRODUCTION

In view of the procurement progress of components with long delivery times for SIS100 (e.g. dipoles, quadrupoles, RF acceleration systems, etc.), some of these are related to the machine's overall safety in the one or other way. Therefore, a study on safety related functions has been started. These functions must be clearly distinguished between machine safety related topics (i.e. protecting the machine from destruction by the high intensity ion beam or electrical / pressure related hazards) and personnel safety topics.

This article concentrates on the electrical functional safety of the SIS100 alone, i.e. experiment / detector protection is not addressed. Furthermore, errors introduced by the machine operator personnel, setting value generation software and beam instabilities are currently ignored. Proposed measures to deal with these (and failures not found by analysis) will be the use of a low-intensity pilot beam after change of crucial settings and the beam loss monitoring system. The latter will help to find obstacles like forgotten objects in the beam pipe (as we had one in SIS18 in 2014), too.

The topic has been studied using a failure mode and effects analysis on the system level (S-FMEA) and assessed using the procedure described in DIN EN 61508 or the approach for simplified system architecture analysis described in EN ISO 13849. The latter has been performed using the tool "SISTEMA" [1]. During this analysis, first each failure mode and effect is assessed by its severity, the stay time of personnel in the hazardous area, the probability of avoidance and the likelihood of occurrence. This leads to a *SIL*[1] category necessary for safe detection of this failure. Afterwards, the system is characterized by its MTTFd[2], the probability to detect the failure and its MTTR[3]. Later, when details on its architecture do exist, it is scrutinized on a part level using FIT[4] values. Finally, for all subsystems leading to the failure, PFH[5] and DCavg[6] values are calculated.

MACHINE PROTECTION

Compared to other accelerators, the destruction capability of the ion beam itself is low (which will be shown below). Therefore, only the first three of the four following failure effects have been identified to be potentially dangerous for the machine already at their first occurrence:

1. Quench of magnets/busbars,
2. Helium supply line pressure rise, leakage or rupture,
3. Horizontal "spiraling" of the beam towards the outside of the synchrotron and
4. Focusing of the beam onto a perpendicular thin wall (e.g. vacuum chamber).

Further (non-destructive) events have been found to be the effect of other failures:

- Beam blow up (which will hit the halo collimators),
- Horizontal closed orbit distortion to the inside of the synchrotron (which will hit the cryocatchers) and
- Vertical beam loss (which will hit the halo collimators)

Most of these events will lead to beam loss in a short amount of time (μs. . .ms). If the beam is not lost completely, its emittance is blown up or distorted in a way that it is not longer usable by the designated experiment (or even can destroy sensible detectors, etc.). Therefore, an emergency dump will be initiated by a fast failsafe optical signal. For failures which are not critical in this meaning, a simple interlock will be generated to stop further injections into the synchrotron and a post-mortem analysis can be done. Each effect will be addressed in the following sections.

Quench Detection and Protection

The QD/QP system of SIS100 consists of a quench detection system utilizing voltage taps on each half of the magnet coil and busbar soldering connection. The system has been analyzed by a risk graph and must fulfill the *SIL3* criteria. The voltage across two symmetric s.c. magnet coil parts will be measured by a redundant read out measurement bridge. When a bridge voltage threshold of 100 mV is reached for 10 ms, a failsafe signal is sent to start the emergency beam dump. Shortly (1 ms) afterwards, the magnet current dump

* c.omet@gsi.de
[1] SIL = Safety Integrity Level.
[2] MTTFd = Mean Time To dangerous Failure
[3] MTTR = Mean Time To Restauration
[4] FIT = Failures in Time = failures in 1×10^9 h
[5] PFH = Probability of dangerous failures per hour
[6] DCavg = Diagnostic coverage

ISBN: 978-3-95450-132-8 doi:10.18429/JACoW-IPAC2014-THPME058

resistor is switched on. Roughly 20% of the voltage taps will be kept as redundant replacements to ensure a good availability of the machine. Table 1 shows the result of the preliminary system architecture analysis acc. to EN ISO 13849 for a single dipole (the values for the other magnet families differ only slightly). The desired safety level *SIL3* is reached.

Table 1: Dipole QD/QP Analysis Results

Component	PFH / h^{-1}	DCavg / %
Voltage taps	2.29×10^{-7}	90
Quench detection card	9.34×10^{-8}	70
Current dump resistor	2.29×10^{-7}	90
Overall QD/QP system	5.51×10^{-7}	

Helium Pressure Rise or Leakage/rupture

In view of the catastrophic LHC event, a detailed analysis of possible liquid helium (LHe) supply line ruptures, insulation vacuum breaks and their effects has been done [2]. As a result of this study, each quadrupole cryostat (i.e. each 12.9 m) is designed to be equipped with a safety blow valve which opens at 0.3 bar cryostat overpressure. The opening cross section of DN 100 has been chosen to ensure a safe pressure release even when one safety valve is blocked (e.g. by multilayer insulation debris). The system is safe in acc. to the Pressure Equipment Directive (PED) 97/23/EC.

Horizontal Beam Loss onto Electrostatic Septum

As the electromagnetic septum for slow extraction is situated at the outside of the synchrotron and defines its acceptance, its wires are prone to damage by beam impact. The wires are made of 25 μm thin tungsten. Depending on the ion species and energy (and hence its dE/dx), the beam energy deposition in the wires could be large enough to heat the wires up to a loss of mechanic stability [3]. This in turn will produce a large downtime of the accelerator for repair which has to be avoided. The safety function to avoid this event has been analyzed by a risk graph and must fulfill the *SIL2* criteria.

Failures leading to a slow, spiraling movement of the full beam into the septum wires are: Main dipole quench[7] or power converter (PC) failures, horizontal steerer quench or PC failures, chromaticity sextupole quench or PC failures, octupole quench or PC failures, resonance sextupole PC failures, acceleration RF failures.

Some of these failures are becoming critical only during slow extraction and high beam intensities. To simplify the system design, an emergency dump will be initiated whenever a failure is detected directly by the devices itself or indirectly by the beam loss monitoring system (independent from the machine cycle or beam intensity). The power converter values have been estimated, an example can be seen in tab. 2. As some system architectures are currently not designed, PFH rates are not available.

Table 2: Dipole Power Converter Failure Rates

Component	FIT	DCavg / %
Media sensors	1000	60
Current control loop	10 138	91
Parallel feed in	19 000	99
Primary voltage	100	0
Sum	30 238	95

(No) Melting of Steel

The maximum total SIS100 beam energy for 2×10^{13} protons is 93 kJ and for 5×10^{11} U^{28+} ions 51.5 kJ. This is comparable to the CERN PS which has a maximum total proton beam energy of 97 kJ and no destructive event recorded in history. If the beam would be strongly focused in both vertical and horizontal planes, one could theoretically reach an energy density large enough to melt metal. The specific energy density necessary to melt steel is: $E_{melt,total} = c_u \cdot \Delta T + h_{melt}$.

Starting at cryogenic temperatures of 15 K and ending at 1921 K (ΔT = 1906 K), a specific heat capacity of steel $c_u \approx 0.49\,\mathrm{J\,g^{-1}\,K^{-1}}$ and a latent melting enthalpy $h_{melt} = 270\,\mathrm{J\,g^{-1}}$, we get $E_{melt,total} = 1.2\,\mathrm{kJ\,g^{-1}}$. The ion range in steel, until half of the maximum beam's energy is lost, is $\approx$ 50 mm for both ions and protons at extraction. Therefore, the necessary spot radius to achieve melting has to be $r <$ 0.2 mm.

Assuming single device errors, this small spot size is not achievable with the synchrotron's focusing structure and given beam size (beam radius in horizontal direction at extraction is at least 6 mm for ions and 1.5 mm for protons with γ_t-shift optics settings). Shock waves created by the beam impact, on the other hand, can damage the material by repeated impact of the beam [4]. Therefore, failures leading to this effect have only to be detected and ensured that they do not happen repeatedly (i.e. stop further injections into the synchrotron by means of the interlock system, *no SIL* classification).

Beam Loss on Halo Collimators, Cryocatchers or Other Devices

The halo collimators (both primary and secondary) and cryocatchers are designed to withstand a single impact of a full ion or proton beam, therefore failures leading to this impact are not being taken into account as dangerous events. Nevertheless, standard engineering techniques are used to avoid or detect these failures to a reasonable amount (i.e. *no SIL* level is necessary). By means of the ion current readout from the cryocatcher and coupling to the interlock system, it can be ensured that these events do not happen repeatedly.

Analyzed events which cause these beam loss mechanisms are (excluding the ones which are already covered

[7] Quenches always are accounted for the magnet coil itself, busbars, interconnections and current leads.

ISBN: 978-3-95450-132-8 doi:10.18429/JACoW-IPAC2014-THPME058

above): Main quadrupole quench or PC failures, vertical steerer quench or PC failures, fast tuneshift quadrupole PC failures, resonance sextupole PC failures, accelerating RF failures, injection/extraction kicker failures and beam pipe vacuum leaks.

Emergency dump of SIS100

To use the emergency dump during the whole cycle of SIS100, the extraction kickers are ramped, bipolar devices. If they kick upwards, the beam will enter the 3-stage magnetic septum and extracted to the experiments. If they kick downwards, the beam will hit the emergency dump, which is situated below the magnetic septum #3, see fig. 1. If one of the kickers fail, the emergency dump will still be hit by most of the beam. It has been shown that the remaining dose of beam fragments will not lead to a quench of the following quadrupoles [**?**].

The dump is composed of a 20 cm long carbon block, followed by an up to 2 m long tungsten block. To smear out the bragg peak in the absorber material, the front surface of the block is inclined by 20 °. This simple measure already will reduce the peak temperature in the absorber by a factor of 4 compared to a perpendicular angle of incidence.

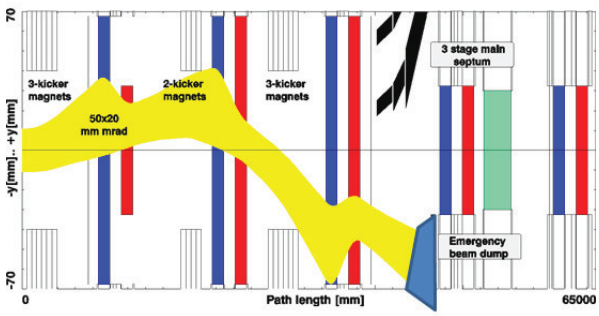

Figure 1: Vertical optics of SIS100. Emergency dump (blue) at bottom, magnetic septum (black) at top.

PERSONNEL SAFETY

The field for personnel safety is wide. Therefore, only some items are shown here at a glance regarding possible hazards by the machine during its operation (i.e. not taking into account mounting/assembly, catastrophic events coming from the outside world like fire, floods, earthquakes, etc.):

- Prevention of access to radiation protected areas and local cryogenic areas during magnet powering,
- Avoiding oxygen deficiency in tunnels during helium blow events,
- Electrical power emergency shut down and
- Avoiding activation of machine parts beyond hands-on-maintenance limits

As for every accelerator complex, the Personnel Safety System (PSS) will not allow access to sensible areas together with a door locking mechanism. From risk graph analysis, this safety function has to fulfill the *SIL3* criterion.

Access to local cryogenic areas during magnet powering has been decided to be forbidden as a consequence of the LHC event. The risk at SIS100 for this type of catastrophic failure with arc ignition is not as big as for LHC, because the amount of LHe ($\approx 1\ m^3$) and stored magnet energy is orders of magnitude lower. Furthermore, the type of cable cooling and quench detection / supervision of busbar interconnections is different. Nevertheless, *SIL3* has to be achieved. In case of forced access (e.g. by mechanic destruction of the locking device), the magnet power has to be shut off by the dump system described above.

In case of a helium safety valve blow or LHe supply line rupture event, the personnel has to be protected from oxygen deficiency. As mentioned before, the amount of LHe in the machine is low; furthermore, LHe supply will be stopped by shut-off-valves when a pressure loss is detected. Only in three local cryogenic niches, the amount of LHe is large enough to pose a treat to working personnel. Additionally to oxygen deficiency sensors, oxygen masks will be placed and/or have to be carried by the workers in these areas.

For emergency cases during maintenance times, a suitable fast power-off *SIL2* capable system is under development which will act directly on the low voltage distribution for the accelerator components in a defined way (e.g. crucial systems like cryogenics have to be kept on power to not further increase the risk).

To facilitate hands-on-maintenance on the accelerator, a limit of $10\ W\ m^{-1}$ average beam loss has to be respected. This will be ensured by the beam loss and transmission monitoring system. Here, *no SIL* level is necessary.

As the above mentioned systems have not been designed at the moment of writing, PHF rates can not be given.

CONCLUSION

Taking into account the already analyzed probabilities of failures (i.e. safe and dangerous failures), an availability of SIS100 can be calculated. Assuming a interruption time of 10 min after quench events and 2 min after emergency dump events, the overall availability per year has been estimated to be $\approx$ 4357 h out of 6000 h (73 %).

REFERENCES

[1] SISTEMA. `http://www.dguv.de/ifa/Praxishilfen/Software/SISTEMA/index.jsp`, 2014.

[2] A. Kade, M. Kuhn, and Gunar Schroeder. ILK-B-1-13-169a, ILK Dresden, 5 2013.

[3] S. Damjanovic. SIS100 - Extraction Straight Section 5: First results from Fluka simulations. CERN, 6 2011.

[4] N. A. Tahir, A. Shutov et.al. Ion Beam Driven High Energy Density Physics Studies at FAIR at Darmstadt. *Contributions to Plasma Physics*, 53(4-5):292–299, 2013.

[5] C. Omet. SIS100: Emergency dumping of protons and ions. 10th MAC, GSI, 11 2013.