MACHINE PROTECTION AND INTERLOCK SYSTEMS FOR LARGE RESEARCH INSTRUMENTS

R. Schmidt, CERN, Geneva, Switzerland

Abstract

Major research instruments such as accelerators and fusion reactors operate with large amount of power and energy stored in beams and superconducting magnets. Highly reliable Machine Protection systems are required to operate such instruments without damaging equipment in case of failure. The increased interest in protection is related to the increasing beam power of high-power proton accelerators such as ISIS, SNS, ESS and the PSI cyclotron, to the large energy stored in the beam (in particular for hadron colliders such as LHC) and to the stored energy in magnet systems such as for ITER and LHC. Machine Protection includes process and equipment monitoring, a system to safely stop operation (e.g. dumping the beam or extracting the energy stored in the magnets) and an interlock system for highly reliable communication between protection systems. Depending on the application, the reaction of the protection function to failures must be very fast (for beam protection systems down to some µs). In this presentation an overview of the challenges for protection is given, and examples of interlock systems and their use during operation are presented.

INTRODUCTION

Accelerators, as all other technical systems, must respect some general principles with respect to safety and protection. Protection of people from different threats (radiation, electrical, oxygen deficiency, ..) has always the highest priority and follows legal requirements. The main strategy to protect people during operation is to keep them away from hazards, ensured by a personnel access system. Protection of the environment is the second priority. In this paper the protection of equipment (the investment) is discussed, e.g. accelerators and beam targets, experiments and fusion reactors. Designing a machine protection system is challenging and requires an excellent understanding of the system and its operation, to anticipate and avoid possible failures that could lead to damage or mitigate the consequences.

Protection of accelerators was to topic of a recent Joint Accelerator School, the proceedings with many relevant contributions will be published by the end of 2015 [1].

In general, risks come from energy stored in a system (measured in Joule) as well as from power when operating the system (measured in Watt). Particle accelerators and fusion reactors are examples of such systems, since they operate with large amount of electrical power (from a few to many MW). The energy and power flow needs to be controlled. An uncontrolled release of energy or an uncontrolled power flow can lead to unwanted consequences such as damage or activation of equipment and loss of time for operation.

MACHINE PROTECTION AT LARGE RESEARCH INSTRUMENTS

Many accelerators operate with high power beams or beams with a large amount of stored energy. Accelerators operating with superconducting magnets require sophisticated systems to protect the magnets in case of a quench.

Accelerators with large stored energy in the beams are hadron synchrotrons and colliders (Figure 1), e.g. LHC, RHIC, SPS and FCC (a study for a proton collider with a circumference of 100 km and 100 TeV cm energy, [2]),

Many proton accelerators operate with high power beam, such as the PSI cyclotron, ISIS, SNS, JPARC and ESS (planned to start operation in 2019 [3]). A particular challenge are future ADS machines (Accelerator Driven Spallation) that require to operate with very high beam power and extremely high availability [4]. A prototype is expected for the next decade.

Machine protection is also relevant for some electron accelerators, e.g. free electron lasers (XFEL), synchrotron light sources, e+e- circular and linear colliders. In particular protection at linear colliders is challenging, with MW beam power and tiny beam spot sizes.

Installations with large superconducting magnet systems are also considered, e.g. fusion reactors such as ITER operate with magnets that store more than 50 GJ of energy.

To get an idea what this amount of energy means some examples are given. The energy of pistol bullet is about 500 J, the energy of 1 kg TNT about 4 MJ. The energy of 1 l fuel is about 36 MJ, to melt 1 kg of steel about 800 kJ are required (the energy to melt 1 kg of copper is similar). An accidental release of an energy above one MJ can cause significant damage. With the energy stored in the ITER toroid magnet it is possible to melt 60 tons of copper. Even an accidental release of a small amount of energy in the order of some hundred Joule can lead to some (limited) damage if the energy is released in sensitive equipment.

HAZARDS AND RISKS

Definition of Risk

A hazard is a situation that poses a level of threat to the installation. Hazards are dormant or potential, with only a theoretical risk of damage. Once a hazard becomes "active" it becomes an incident or accident. An accident is defined as an unfortunate incident that happens unexpectedly and unintentionally, typically resulting in damage or injury.

ISBN 978-3-95450-148-9

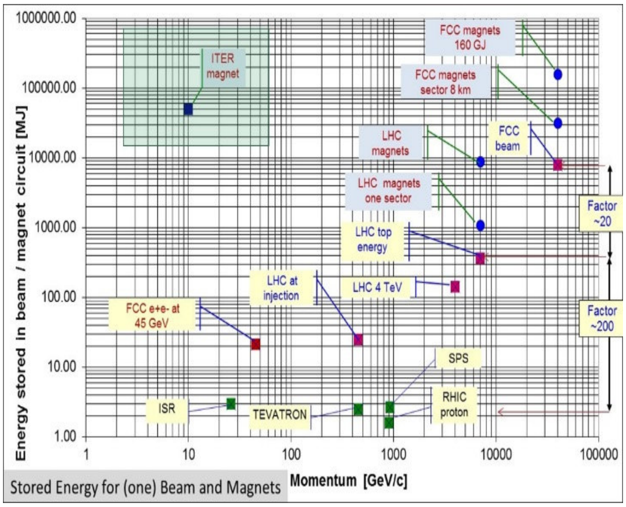

Figure 1: Stored beam energy as a function of particle momentum for a number of accelerators. For comparison, the energy stored in magnet circuits is also shown.

The risk allows to measure the threat of a hazard, by multiplying consequences and probability for a hazard becoming active: **Risk = Probability ∗ Consequences**

Hazards becomes accidents, in general due to a failure or a combination of failures. Related to research instruments, probability and consequences for many different types of failures (e.g. for an accelerator failures leading to beam loss) need to be estimated to evaluate the risk.

Machine protection systems prevent damage to equipment and reduce the risk, either by preventing that a failure occurs, or by mitigating the consequences of a failure. The higher the risk, the more important becomes a robust protection system.

Hazards Related to Magnet Systems

Accelerators and fusion reactors operate with high field superconducting magnets systems. The energy stored in the magnets increased over the years (at TEVATRON, HERA, LHC, ITER, FCC, ….).

Superconducting magnets may quench – and without a protection system such magnets could be damaged. There are many mechanisms that can trigger a quench. A very small amount of energy is sufficient to quench a magnet (down to few mJ). As an example, the loss of a fraction of 10^{-8} of the LHC proton beam in one dipole magnet can lead to a quench. E.g. quenches were induced by the interaction of a dust particle (UFO) with the circulating beam.

Hazards Related to Particle Beams

Regular beam losses during operation lead to activation of equipment and possibly to quenches of superconducting magnets. Radiation induced effects in electronics (Single Event Effects) can perturb the operation of an accelerator.

For accidental beam losses due to failures the hazards need to be understood, e.g. probability and consequences. To understand the consequences, the energy deposition by particles and mechanisms for damage of components need to be estimated.

Examples of Past Accidents

During the first phase of CERN-LHC operation between 2009 and 2013 the magnetic field and therefore the particle momentum was limited to 4 TeV/c. This was the consequence of the 2008 LHC accident that happened during magnet test runs without beam. A magnet interconnect was defective and the circuit opened. An electrical arc provoked a helium pressure wave damaging about 600 m of the LHC and polluting the beam vacuum over more than 2 km. An overpressure from the expansion of liquid helium damaged the structure. A total of 53 magnets had to be repaired [5].

In December 2013 a vacuum leak on a below of LINAC 4 at CERN developed in the MEBT (Medium Energy Beam Transfer) line. The analysis showed that the very low power beam has been hitting the bellow during a special measurement with very small beams in the vertical plane. About 16 % of the beam was lost for about 14 minutes and damaged the bellow. The consequences were minor since LINAC4 is still being commissioned and not used in the chain of LHC injectors. The event demonstrates that beams with very low power (~Joule) can already cause damage.

MACHINE PROTECTION SYSTEM

Figure 2 illustrates an approach to the design of a machine protection system. Hazards are identified and the risk is estimated. Sometimes protection might not be possible, e.g. if a superconducting magnet has a too low ratio between stabilising copper and superconductor, or for devices in an accelerator that can accidentally deflect the beam to the outside of the aperture at an inadequate position.

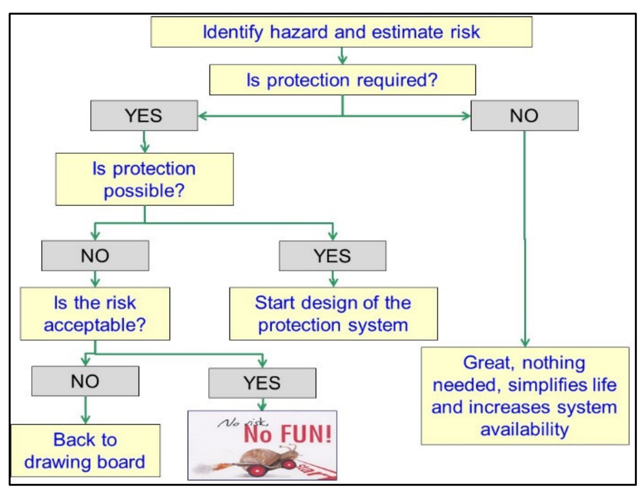

Figure 2: Approach to analyse the need for a protection system starting from the identification of a hazard.

Three Principles for Machine Protection (P3)

Providing equipment for machine protection system is not sufficient to ensure safe operation, other consideration are required:

- Protect the equipment (machine protection systems + interlock systems). The level of protection that is required needs to be defined based on risk.

ISBN 978-3-95450-148-9

- Protect the process (high availability protection systems). Machine protection systems will always contribute to downtime. The protection action should be performed ONLY if a hazard becomes active (e.g. something went wrong threatening to damage equipment).
- Provide the evidence (post mortem, logging of data) [6] for different events: 1) a failure is detected and a protection action is performed, 2) a failure in the protection systems leads to a protection action that is not required, 3) a near miss and 4) an accident. In all cases it is essential to understand the event. All relevant system should record their proper data (e.g. with circular "post mortem" buffers in the equipment to record data, and stop and read out the data after the protection action is performed). Slow logging, typically in the order of one Hz, is also very helpful. Synchronisation of different systems is required, to exactly understand the sequence of events. With such data, post operational checks can be performed by the controls system and/or by operators.

Active Protection

Active protection requires the detection of the failure by a sensor. This could be an instrument in an equipment system, or by beam instrumentation detecting when the beam starts to be affected by the failure (for example, increased beam losses or a different beam trajectory). For superconducting magnets, the quench detection system detects the start of a quench by measuring the resistive voltage across parts of the electrical circuit.

When a failure is detected, operation must be stopped with an actuator. For beam in synchrotrons and storage rings the beam is extracted by a fast kicker magnet and transported to a beam dump block. The block must be designed to accept the beam pulse without being damaged. Injection must be stopped. For linacs beams, the beam is stopped in the low energy part of the accelerator by switching off the source, deflecting the low energy beam by electrostatic plates ("choppers") or by switching off the RFQ for proton linacs. For an accelerator complex with a chain of several accelerators, injection of beam into the next stage of the accelerator complex should be prevented.

For superconducting magnet systems there are several methods to extract the energy from the circuit with the quenched magnet, e.g. to switch a resistor into the circuit and fire quench heaters [7].

Experience from LHC shows that for most type of failures a careful and fast monitoring of hardware parameters allows stopping beam operation before the beam is affected. Parameters monitored include state and analogue signal. As an example, when a trip of a magnet power converter is detected, the beams are extracted before there is any effect on the beam.

It is not always possible to detect failures at the hardware level. The second method is to detect the initial consequences of a failure with beam instrumentation and to stop the beam before equipment is damaged. This requires reliable beam instrumentation such as beam loss, beam position or beam current monitors.

An electronic interlock system links the different parts of the protection system, the sensors and the actuator. For magnets circuits the interlock system informs the system for energy extraction about a quench. The interlock system might include complex logics that depends on the operational state.

Passive Protection

There are failures (e.g. ultra-fast losses) when active protection is not possible. One example is protection against misfiring of an injection or extraction kicker magnet in an accelerator. A beam absorber or collimator is required to stop the mis-steered beam in order to avoid damage. All possible beam trajectories for such failures must be considered, and the absorbers must be designed to absorb the beam energy without being damaged. Another example is a fast extraction of high-intensity beam from a circular accelerator into a transfer line. When the extraction takes place, the parameters of the transfer line, e.g. the current of the magnets, must be correctly set since for a wrong magnet current the beam would be mis-steered and risk to damage vacuum chamber and other components. An installation of absorbers in critical places can mitigate the consequences.

The machine protection system has also to monitor the parameters before the beam transfer, and only allowing extraction if all parameters are within specified limits.

LHC STRATEGY FOR MACHINE PROTECTION AND INTERLOCKS

In this section we discuss the strategy adopted for LHC machine protection from beam hazards and the related systems:

- Definition of the aperture by collimators.
- Stop beam by beam absorber / collimator for specific failures, e.g. at injection.
- Detect failures at hardware level and stop beam operation for critical failures.
- Detect initial consequences of failures on the beam with beam instrumentation.
- Transmit the signal from instrumentation via a highly reliable interlock system to the extraction kickers and injection system.
- Stop beam operation by extracting the beams into beam dump block.
- Inhibit injection into LHC and extraction from the SPS (the pre-accelerator for LHC) in case of a failure.

Figure 3 illustrates the interlock systems for LHC. The core is the Beam Interlock System that receives beam dump requests from many connected systems. The system is based on FPGAs with a μs reaction time. If a beam dump request arrives, a signal is send to the beam dumping system to request the extraction of the beams. At the same time, a signal is send to the injection system to block injection into LHC as well as extraction of beam from the SPS. A third "post-mortem" signal is provided to the timing

ISBN 978-3-95450-148-9

system that sends out a request to many systems for providing data that were recorded just before the beam dump, to understand the reasons for the dump (using data from beam loss, beam position, beam current, magnet currents, etc.).

The most complex technical system of the LHC is the superconducting magnet and powering system. The Powering Interlock System (PIC) ensures communication between systems involved in the powering of the LHC superconducting magnets [8]. This includes power converters, magnet protection system, UPS (uninterruptible power supplies), emergency stop of electrical supplies (AUG) and the cryogenic system. As an example, in case a magnet quench is detected by the quench protection system (QPS) the power converter must stop. When a failure is detected that will stop powering of magnets, a beam dump request is send to the Beam Interlock System.

A second systems is managing interlocks from normal conducting magnets and their power supplies (WIC) that ensures protection of the magnets in case of overheating.

Both Powering Interlock System PIC and WIC are based on PLCs that are much slower than the Beam Interlock System, with ms reaction time.

The machine interlock system is strictly separated from interlocks for personnel safety such as the personnel access system, however, an interlock from the access system is send to the Beam Interlock System.

Many other systems provide also beam dump requests in case of failure: vacuum system, RF, devices that can potentially move into the beam pipe, LHC experiments.

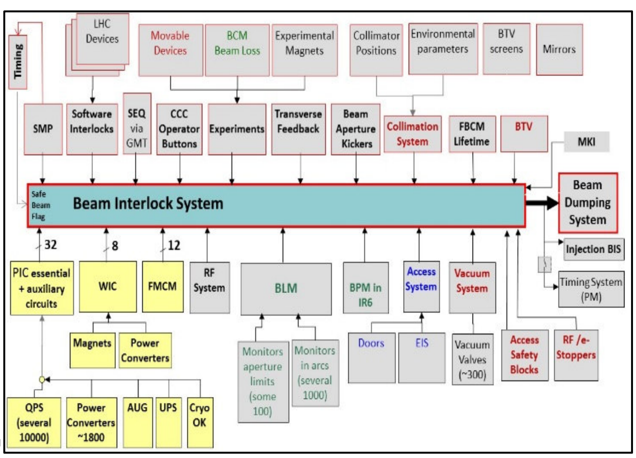

Figure 3: Interlock systems for the CERN-LHC. The core is the Beam Interlock System, many other systems are connected to it that can request a beam dump.

The LHC Software Interlock System ensures redundant protection for many hazards and early detection of failures. It also verifies that the LHC operational parameters remain within well-defined boundaries (e.g. closed orbit deviation within specifications). If a failure is detected, a signal is either send to the Beam Interlock System, or injection is blocked.

In total, there are several 10 thousand interlock signals.

DESIGN OF INTERLOCK SYSTEMS

The most critical parameter for the design of a protection and interlock system is the reaction time. For beam operation in an accelerator there are many failures that require a reaction with a reaction time down to µs. Interlock systems for superconducting magnets require in general a much slower reaction, in the order of milliseconds to seconds.

Fast interlock systems are in general based on hardware (Electronics/Asics), they might include intelligent controllers (FPGAs, DSPs). Such systems can be extremely fast, down to a few ns.

For slower interlock systems, PLCs (Programmable Logic Controllers) are widely used. Using standard PLCs reaction times of one to few ms can be achieved, with safety PLCs the reaction time is in general between several 10 to hundred ms.

At CERN, a Software Interlock System was introduced with great success. Many failures can already be seen seconds before the beam is affected, or a magnet quenches. With the SIS, a reaction time in the order of one second is achieved. During the 6 years of operation no “unsafe” failure of the system was observed.

The second most important parameter for protection and interlock system is the required level of protection. The standard IEC 61508 is a basic functional safety standard for all kinds of industry. The safety integrity level (SIL) provides a target to attain in regards to a system's development that is widely used in industry, mainly for the safety of people. To follow such standard for research instrument turned out to be not very practical, since the procedures to be used by the standard are rather cumbersome. However, for comparing the risk for different hazards and for formulating the requirements for the protection system such approach is very useful. Inspired by the SIL levels, the Protection Integrity Level (PIL) has been introduced, with four levels, from PIL1 (protection for hazards with the lowest risk) to PIL4 (protection for hazards with the highest risks) [9].

There are a number of considerations for selecting a system:

- In a radiation environment (e.g. Single Event Effects) radiation tolerant electronics is required. PLCs are excluded. Whenever possible, an installation in such environment should be avoided!
- An interlock system communicates between several systems. This can be done by current loops, frequency loops, or use of intelligent network (Profibus, Profisafe, Ethernet, ..).
- Time for development (e.g. in-house design of electronics versus buying and programming PLCs, ..) needs to be considered.
- The system should match the lab environment and standards (e.g. hardware such as choice of crates, software, etc.).
- The competence in the lab and the long-term maintainability need to be considered.

ISBN 978-3-95450-148-9

- Interlock systems are not major cost drivers, therefore the cost is not a decisive criterion.

TESTING, COMMISSIONING AND OPERATING

Already during the early phase in the design of the protection system, functional testing needs to be considered. Correct commissioning and regular testing of protection systems is vital to ensure reliable operation.

Repeated testing is very time consuming, can be extremely boring and prone to errors, in particular if done by humans. Automatic test procedures and automatic validation of the results via the controls system are very helpful. For LHC, a framework for automatic testing was developed and used for LHC magnet system commissioning, with ~10000 tests performed about once per year [10].

Partial commissioning of an accelerator, in particular for linacs, should be taken into account for the development of the protection system, to avoid frequent reconfiguration. If only the first part of the linac is commissioned, interlocks using downstream equipment should not obstruct commissioning.

For a large system such as LHC several million parameters for the protection systems need to be maintained. Many parameters can only be defined with operational experience. Management of critical parameters and the access to such parameters need to be considered. Regular comparison ensure that parameters in the database and in the hardware are identical. At CERN access to critical parameters with the highest PIL is not possible via the controls system. Parameter with medium PIL can be changed via the control system, but strict rules are defined, e.g. two people must be present to be perform a parameter change. For low PIL, parameters can be changed via the control system.

Several 10k interlock channels are present, all can prevent operation. This can be a nightmare for starting-up a system, in particular if the risk is (close to) zero, e.g. for the commissioning of an accelerator with very low beam intensity. If the option of bypassing of interlocks is considered during the design phase, bypassing by manual procedures on operator's discretion should be avoided.

DESIGN RECOMMENDATIONS AND AVAILABILITY

Considering the experience at CERN and elsewhere some design recommendations are formulated:

- Avoid (unnecessary) complexity for protection systems.
- Failsafe design and detection of internal faults.
- Possibility for remote testing at regular time intervals, for example between two runs.
- Critical equipment should be redundant (possibly diverse redundancy, using different types of equipment).
- Critical processes not by software and operating system.
- No remote changes of most critical parameters.
- Calculate safety / availability / reliability by methods to analyse critical systems and predict failure rate.
- Managing interlocks, always have a clear view of what is interlocked.
- Bypassing of interlocks is common practice (keep track!). For the LHC, bypassing of some interlocks is possible for "setup" beams (low-intensity beams).
- Time stamping for all system with adequate synchronisation is essential.

Availability

If the only objective is maximising safety and too many interlocks are present, this might reduce the overall availability. The challenge it to find a reasonable compromise between safety and availability.

As a technique to improve availability while maintaining safety, majority voting can be considered. An optimum has been found with 2oo3 voting systems that ensure an excellent level of safety, while not stopping operation if one of the three redundant branches indicates a failure, and therefore increasing the availability [11]. A prototype for the powering interlock system for the ITER superconducting magnets has been build according to this principle [12].

MACHINE PROTECTION AND CONTROLS

The controls system has a very important role in the context of machine protection. In many institutes, the responsibility for the hardware and software of the interlock system is within the responsibility of controls. As already discussed in this paper, many control tools can contribute to safe and efficient operation.

- Logging and Post Mortem recording of data, together with accurate and reliable time stamping.
- Framework for managing critical parameters.
- Framework to relax interlock conditions when risks are low ("masking or bypassing of interlocks").
- Framework for automatic testing of machine protection functionalities.
- Framework to respect operational boundaries (sequencer, state machine).
- Clear on-line display of critical parameters to operators (e.g. display of beam losses).
- Feedback systems to keep parameters within predefined limits (e.g. closed orbit).

ACKNOWLEDGMENT

Many colleagues contributed to these considerations on machine protection systems, and it is not possible to acknowledge all of them. However, I like to mention Jorg Wenninger and Markus Zerlauth, who have been very close collaborators for a period of more than 10 years. Without them, neither the LHC machine protection system nor this paper could have been realised.

ISBN 978-3-95450-148-9

REFERENCES

[1] "Joint International Accelerator School on "Beam Loss and Accelerator Protection"," 2014. [Online]. Available: http://uspas.fnal.gov/programs/JAS/JAS14.shtml.

[2] "FCC Week 2015," 2015. [Online]. Available: http://indico.cern.ch/event/340703/timetable/#all.detailed.

[3] A. Nordt, "DEVELOPMENT AND REALISATION OF THE ESS MACHINE PROTECTION CONCEPT," in *15th International Conference on Accelerator & Large Experimental Physics Control Systems,*, Melbourne, Australia, 2015.

[4] W. Pam, "OVERVIEW OF WORLDWIDE ACCELERATORS FOR ADS," in *IPAC2014*, Dresden, Germany, 2014.

[5] J. Wenninger, "Machine Protection and Operation for LHC," Newport Beach, USA CA, 2014.

[6] M. Zerlauth, "The LHC Post Mortem Analysis Framework," in *12th International Conference on Accelerator & Large Experimental Physics Control Systems*, Kobe, Japan, 2009.

[7] H. Pfeffer, Protection of Hardware: Powering Systems (PC, NC and SC Magnets), Newport Beach, USA CA: JAS / CAS, 2014.

[8] M. Zerlauth, "A Retrospective View to the Magnet Interlock Systems at CERN," in *5th International Particle Accelerator Conference*, Dresden, Germany, 2014.

[9] M. Kwiatkowski, *Methods for the application of programmable logic devices in electronic protection,* Geneva, Switzerland: CERN-THESIS-2014-048, 214.

[10] A. Gorzawski, "The AccTesting Framework: An Extensible Framework for Accelerator Commissioning and Systematic Testing," in *14th International Conference on Accelerator & Large Experimental Physics Control Systems*, San Francisco, CA, USA, 2013.

[11] S. Wagner, "Architecture for Interlock Systems : Reliability Analysis with Regard to Safety and Availability," in *13th International Conference on Accelerator and Large Experimental Physics Control Systems*, Grenoble, France, 2011.

[12] M. Zaera-Sanz, "Design, Development and Implementation of a Dependable Interlocking Prototype for the ITER Superconducting Magnet Powering System," in *14th International Conference on Accelerator & Large Experimental Physics Control Systems*, San Francisco, CA, USA, 2013.

ISBN 978-3-95450-148-9