DESIGN, DEVELOPMENT AND IMPLEMENTATION OF A HIGHLY DEPENDABLE MAGNET POWERING INTERLOCK SYSTEM FOR ESS

M. Zaera-Sanz, A. Nordt, S. Birch, A. Monera, ESS, Lund, Sweden

Abstract

Approximately 350 resistive magnets and 350 power supplies (PS) will be installed in the 600 m long linear accelerator (LINAC) at the European Spallation Source, ESS, transporting the proton beam from the source to the target station. In order to protect this equipment from damage (e.g. due to overheating) and to take the appropriate actions required to minimise recovery time, a dedicated magnet powering interlock system is being designed. The magnet powering interlock system will safely switch off a PS upon the detection of an internal magnet or PS failure and inform the beam interlock system to inhibit further beam operation. The different failure modes and related mitigation techniques of magnets and their PS will be presented. Failures of the magnet cooling system can be detected for example by interlocking the opening of a thermo-switch or a flow-switch. To achieve the required level of dependability, an interlock system based on safety Programmable Logic Controller (PLC) technology, distributed safety PLC software programming tools, PROFINET fieldbus networking, and current loops for hardwired interlock signal exchanges, has been prototyped and will be discussed.

INTRODUCTION AND REQUIREMENTS

The scope of the magnet powering interlock system is to protect the magnet system from damage in case of a failure in the cooling or powering systems, and to take the appropriate action(s) to minimize time for recovery.

Due to the complexity and requirements of flexibility (not all the powering failures require a stop of beam operation), the magnet powering interlock provides local protection to the magnets and interfaces with the beam interlock system.

To protect the magnets from overheating, a set of normally closed thermoswitches are installed in the magnets and they open as soon as the temperature reaches the threshold level (typically 65ºC). A set of normally closed flow switches are also installed in the cooling system and they open when the threshold flow level is reached. Another possibility is the use of flow meters which involves measuring the actual cooling flow (typically water) and acting when this flow is below a threshold limit.

Following the reception of an overheating (notified by the thermoswitches or the flow sensors), the magnet powering interlock performs two actions: inform to the beam interlock system to stop beam operation, and switch off the corresponding power supply(ies) with a maximum delay of 1 second.

To avoid beam deflections, the above actions must follow a sequence, i.e., first stopping the beam and later switching off the power supply.

In case of a powering fault notified by the power supply to the magnet powering interlock system, the system must inform the beam interlock system in order to stop the beam operation. The power supply will be in this case automatically switched off by itself.

Figure 1 illustrates the systems involved in the execution of the protection functions and their dependencies upon each other.

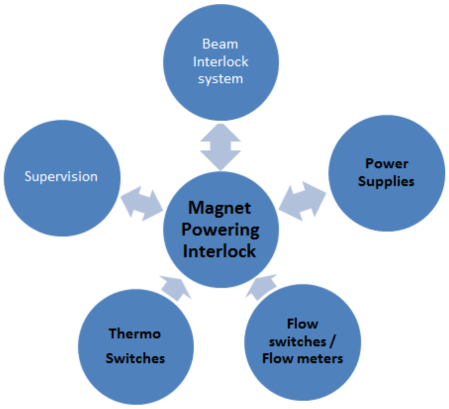

Figure 1: Relationship between the Magnet Powering Interlock system and other systems.

The magnet powering interlock system has to fulfil the following main requirements:

- Protect the magnets in the electrical circuits: in case of overheating, the necessary steps have to be taken to switch off power and stop beam operation.
- Protect the beam: the system should not generate beam stops if this is not strictly necessary. Faulty trigger signals leading to a stop of beam operation must be kept to a strict minimum in order to meet high beam availability requirements for ESS.
- Provide the evidence: in case of an overheating or a powering failure, the operator shall be notified about the root cause. The system must support the identification/diagnosis ability of the initial failure, also in case of multiple alarms (one initial failure that causes subsequent failures).
- Assist improving the operation: the diagnostics for failures should be easy. The status of the system must be clearly presented in the control room and should be transparent to the operator.

To fulfil the above requirements, the implementation of the magnet powering interlock prototype is based on PLC technology which makes use of hardwired current loops,

Copyright © 2015 CC-BY-3.0 and by the respective authors

providing the required dependability of this application. In order to verify the functionality of the interlock prototype a reduced configuration has been implemented (reducing the amount of required PLC modules) while maintaining all possible relationships between the systems involved and in some cases simulating their existence. This reduced configuration implements protection to only one circuit (instead of the finally operational 350 circuits). This allows for an evaluation and verification of the software and hardware architectures and all implemented protection functions. Scaling to the final number of 350 circuits is rather easy from this approach by adding additional PLC modules and the relevant lines of code.

HAZARDS IDENTIFICATION AND ANALYSIS

Taking as a base document the preliminary hazard analysis of the ESS machine protection system for the LINAC [1], several protection functions as well as Protection Integrity Levels and response times were identified. Besides, additional protection systems for target, vacuum and insertable devices were also identified requiring slow protection (milliseconds reaction time) where PLC technology could play a key role.

The set of hazards identified were: loss of power supply, loss of water cooling, malfunction of power supply, malfunction of local sensors (thermoswitches, flow switches/meters), water leaking, unstable power supply and malfunctions of the magnet powering interlock system.

For each of the previous hazards, an analysis has been done identifying the corresponding protection functions related to magnets protection. For instance, in the case of the hazard “loss of power supply”, its consequence could be a misaligned beam which in the case of the dipole bending magnets requires a protection integrity level similar to SIL 3 (IEC 61508) function.

The implementation of the magnet powering interlock system has to strictly comply with all identified protection functions.

HARDWIRED INTERFACES

The exchange of hardware signals is performed using failsafe logic [2]. Nominal operation of the system is represented by an active signal. An active signal corresponds to a flowing current in the loop, while a deactivated signal or a loss of the supply results in a safe state of the system. Figure 2 illustrates as an example the signal exchange corresponding to powering permission provided by the PLC to the corresponding power supply: when the PLC switch is closed, the powering permission is given; when the PLC switch is opened, the powering permission is removed or powering stop is commanded to the power supply.

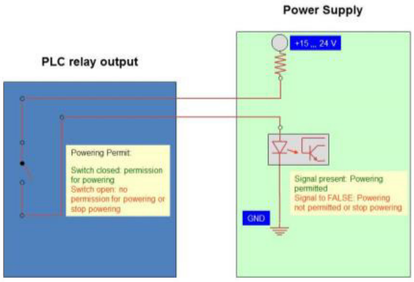
Power Supply
+15 ... 24 V
PLC relay output
Powering Permit:
Switch closed: permission for powering
Switch open: no permission for powering or stop powering
Signal present: Powering permitted
Signal to FALSE: Powering not permitted or stop powering
GND

Figure 2: “Powering Permit/Stop Powering” signal exchange.

According to Figure 3 a set of signals involved have been identified:

- Powering Permit/Stop Powering: generated by the PLC to the Power supply to provide or remove permission for powering.
- Powering Failure: generated by the power supply to the PLC in case of any internal powering malfunction.
- Magnet over heating: generated by the thermoswitches attached to the magnet informing to the PLC that the magnet has reached a threshold temperature limit.
- Flow switch/Flow meter triggered: generated by the flow switch/flow meter in the cooling system informing to the PLC that the minimum threshold of flow has been reached.

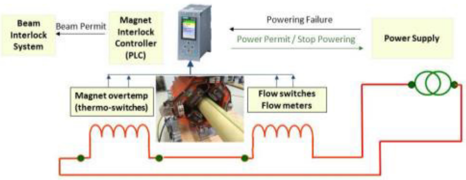
Beam Interlock System
Beam Permit
Magnet Interlock Controller (PLC)
Powering Failure
Power Permit / Stop Powering
Power Supply
Magnet overtemp (thermo-switches)
Flow switches Flow meters

Figure 3: PLC – Power Supply- Magnet thermoswitches–Flow Switches signals exchange.

Additional signals interfacing the beam interlock system are needed. These signals are:

- Beam status: the beam interlock system informs to the PLC about the presence of the beam.
- Beam Permit OK/NOK: the PLC informs the beam interlock system to allow beam operation (OK) or to stop beam operation (NOK case).

The supervision system is using EPICS (Experimental Physics and Industrial Control System) as SCADA (Supervisory Control And Data Acquisition) running a S7 driver in the Siemens PLC CPU and server equipment (Linux based) is foreseen as further work.

PROTOTYPE IMPLEMENTATION

The chosen hardware solution is based on failsafe PLC modules and hardwired current loops. This solution provides the required protection level for the protection functions defined based on the hazard identification and risk analysis. Besides, it provides the required response time and the needed availability of the interlock system.

Copyright © 2015 CC-BY-3.0 and by the respective authors

The controller is based on the new Siemens S7-1500 PLC series and the new ET200SP periphery modules. A redundant powering system based on the Siemens SITOP solution has been also used. Figure 4 depicts the prototype hardware implementation.

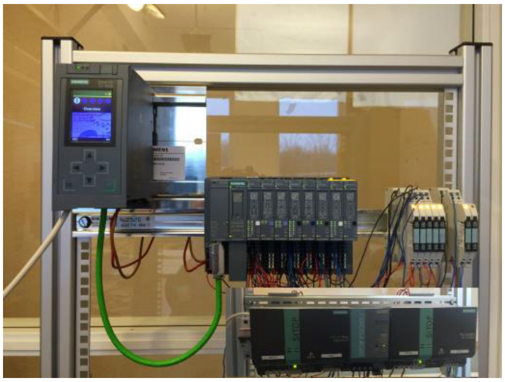

Figure 4: Prototype for magnet powering interlocks.

The whole set of signals coming from the current loops (magnet overheats, flow switch trigger and beam status) to the failsafe CPU, and its reaction (generation of the Beam permit signal OK/NOK towards the beam interlock system and the Powering Permit/Stop powering to the power supply) is depicted in Figure 5.

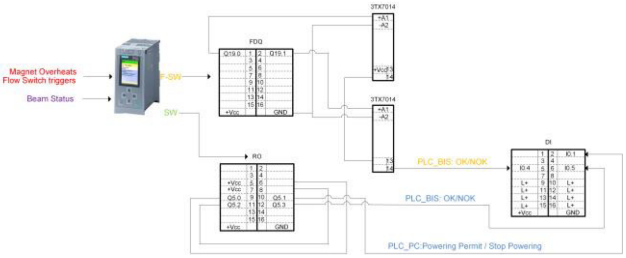

Figure 5: Overall set of signals failsafe and standard programming comparison.

In the above figure, the failsafe CPU commands using failsafe software (orange colour) the beam permit OK/NOK signal by closing/opening the corresponding current loop. The command from the F-CPU is executed by acting on the failsafe digital output connected to two discrete relays in series. This situation is read by the CPU using a digital input. There is another possibility for the generation of the OK/NOK signal using standard relay output modules commanded by the safety software. This last way is depicted by using blue colour, and detected in the CPU using a digital input. The generation of the Powering Permit / Stop Powering signal is done by actuating over two standard relays connected in series, and detected in the CPU using a digital input.

PROTOTYPE EVALUATION

In order to evaluate the response time of the magnet powering interlock system, the measurement in the case of thermoswitch or flow switch triggering has been done:

1. From the detection of magnet overheating until the generation of OK/NOK signal it is 36ms and 20.8ms using relay output module.
2. From OK/NOK signal reception by the beam interlock system until removal of the beam. This time is restricted in [3] to 10µs maximum.
3. From beam not present until Powering stop, it takes 20.8ms.

Regarding the software used for the previous response time computations:

- The PLC program uses one F-runtime group running at 1ms cycle time and priority 12, with a warning cycle time of 5ms and a maximum cycle time of 10ms. The OB used has been OB123.
- The online cycle time of the CPU varies between 1ms and 2ms. This time spreads up to 7ms to 9ms mainly during system initialisation.
- The failsafe digital output module makes three types of self-checking (dark, light and switch pattern tests) where the period is selectable by software to be between 100s or 1000s. The dark test makes microcuts when the output is “1” of around 1ms. The light test is disabled by software. The switch pattern test makes microsets when the output is “0” of around 750µs. All the microcuts/sets are filtered by our discrete relays.

CONCLUSIONS AND FURTHER WORK

The implementation of this first prototype has yielded promising results, both in terms of performance as well as dependability. This prototype has been conceived to scale to 350 circuits needed for the final ESS magnet powering interlock system’s implementation.

Future works include the programming of the supervision interface and CPU communications, additional response time evaluations, and the design of automatic test and diagnostic features to guarantee system integrity though operation.

REFERENCES

[1] Lloyd’s Register, “Preliminary hazard analysis of the ESS machine protection system with emphasis on production and property losses in the ESS-LINAC”, Technical Report, June 2013.

[2] R. Schmidt, P. Dahlen, B. Puccio, M. Zerlauth, “The hardware interfaces between warm magnet interlock system, normal conducting magnets, power converters and beam interlock system for the LHC ring”, Engineering specification, CERN ref. No. LHC-CIW-ES-0001, September 2005.

[3] R. Schmidt, A. Apollonio, D. Curry, A. Nordt, “Architecture of the ESS machine protection system”, European Spallation Source (ESS AB) Technical Report, February 2014.

Copyright © 2015 CC-BY-3.0 and by the respective authors

ISBN 978-3-95450-168-7