DESIGN, DEVELOPMENT AND IMPLEMENTATION OF A DEPENDABLE INTERLOCKING PROTOTYPE FOR THE ITER SUPERCONDUCTING MAGNET POWERING SYSTEM

M. Zaera-Sanz, GSI, Darmstadt, Germany
J. Búrdalo, I. Romera, R. Schmidt, M. Zerlauth, CERN, Geneva, Switzerland

Abstract

An interlock system for CERN-LHC superconducting magnets is successfully operating since several years. Based on the experience with this system, CERN has in collaboration with ITER developed a prototype for the central magnet interlock system. Its main mission is to provide the interlocking between the different subsystems for the superconducting magnet system of the ITER Tokamak, storing a total energy of more than 50 Giga Joules [1]. Upon detection of a quench or other critical powering failures, the central interlock system must initiate the extraction of the energy to protect the superconducting magnets. Depending on the operational circumstances, the interlock system must also request to trigger the plasma disruption mitigation to protect against mechanical forces induced between the magnet coils and the plasma. To fulfil this task with the required high level of dependability we have implemented an interlock system based on redundant PLC technology. In order to allow for simple and unique connectivity of all client systems involved in the safety critical protection functions as well as for common remote diagnostics, a dedicated user interface box has been developed.

INTRODUCTION AND REQUIREMENTS

The TE-MPE (Technology Department-Machine Protection and Electrical Integrity group) at CERN is in charge of the agreement No 7 to the 2007 cooperation agreement (CERN ref. No. K1449/AT) between CERN and ITER concerning Magnet and Superconducting Technologies and Electrical Engineering, which defines the cooperation between CERN and ITER in the fields of machine protection and interlock systems [2].

In the context of the above agreement CERN has developed a prototype for the central ITER magnet interlock system. Its main mission is to provide dependable interlocking between the different subsystems for the ITER superconducting (sc) magnet system.

An energy of more than 50 GJ is stored in the coils of the ITER Tokamak: 41 GJ in the toroidal field coils, 4 GJ in the poloidal field coils, 4 GJ in the central solenoid coils and around 1 GJ in the 89 corrector coils, for respective nominal currents of 68 kA in the toroidal magnets, 45 kA in the central solenoid, 48 kA in the poloidal magnets and 10 kA in the corrector magnets.

To protect the superconducting magnets, the Quench Detection system (QD) measures the voltage drop over the different magnet coils through numerous individual quench detectors and informs the Central Interlock System (CIS) in case of an imminent quench (a typical validation time of up to one second is applied to minimise spurious triggers). Following the reception of a quench signal by the QD, the CIS must initiate with a maximum delay of 500 ms the extraction of the energy by requesting the opening of the according Fast Discharge Units (FDUs) and perform a fast power abort of the corresponding power converter(s), and depending on the operational state, request to trigger the plasma disruption mitigation via the CIS for plasma operation. Figure 1 illustrates the systems involved in the execution of the protection functions and their dependencies upon each other.

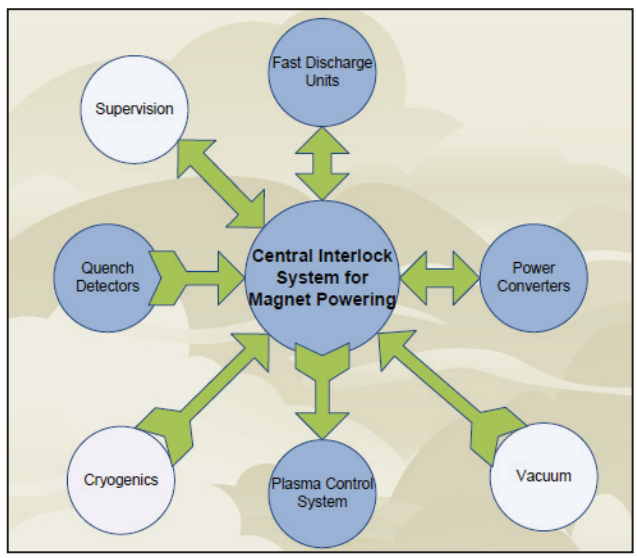

Figure 1: Relationships between the CIS for magnet powering and the involved equipment systems.

The CIS has to fulfil the following main requirements:

- Protect the elements in the electrical circuits: In case of failure, the necessary steps have to be taken to trigger a discharge of the energy stored in the magnets.
- Protect the plasma: The system should not generate powering or plasma aborts if this is not strictly necessary. Faulty trigger signals leading to fast discharges and plasma disruptions must be kept to a strict minimum.
- Provide the evidence: In case of failure, the messages should get to the operator. The system must support the identification of the initial failure, also in case of multiple alarms (one initial failure that causes subsequent failures).

ISBN 978-3-95450-139-7

- 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 mission we have implemented an interlock system based on redundant PLC technology which makes use of hardwired discharge loops in 2oo3 redundancy, providing the best balance between safety and availability for the requirements of this application. In order to verify the operation of our interlock prototype, we have implemented a reduced configuration (reducing the amount of required PLC modules) while maintaining all possible relationships between the four circuit families (toroidal field, poloidal field, central solenoid and correction coils). This reduced configuration implements protection for six circuits (instead of the finally operational 21 circuits): one toroidal field, two poloidal field, two central solenoid and one correction coil 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 21 circuits is rather easy from this approach by adding additional PLC modules and the relevant lines of code.

INVESTMENT PROTECTION FUNCTIONS

The CIS at ITER is solely responsible for the protection of the investment. This protection is performed in two layers: at the plant system level (nearly 160 plants with their local plant interlock systems) and at a global level through the CIS [1]. The ITER magnet interlock system represents one part of the CIS in the overall ITER protection architecture.

In the following the list of investment protection functions (IPFs) that need to be implemented in the magnet interlock system are defined. The following naming convention has been adopted to identify the different levels of IPFs:

- CF: Circuit Function, i.e. such a function will only act on the electrical circuit in question.
- FF: Family Function, i.e. such a function will act on all electrical circuits of a circuit family, e.g. simultaneously on all 9 correction circuits.
- GF: Global Function. Such a function will act simultaneously on all circuit families, e.g. following failures in the cryogenic or vacuum system that would impact all magnet powering of the Tokamak at once.

More than 14 IPFs have been identified. As an example, the global function called “GF-QFCP” is illustrated in the following. The requested protection function is the following: “A Quench or spurious FDU opening or CIS fast discharge request or a power converter fast discharge request in any family of circuits has to result in the opening of the proper FDUs and a fast discharge of the proper power converter(s) depending on the family of circuits implied”.

For each IPF a set of information is collected: description of the risk, probability of occurrence, cost, detectors, actuators, conditions of success and failure, required SIL level, availability/redundancy required and time to react.

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

HARDWARE INTERFACES

In order to allow for simple and unique connectivity of all client systems to the hardwired discharge loops as well as for common remote diagnostics, a dedicated user interface box has been developed [3]. This user interface box provides a homogeneous interface for reading and acting on the quench loops to the different users, whilst maintaining full electrical separation.

The user interface box consists of three main functional blocks:

- Providing continuity of the current loop from the CIS, compliant with the chosen 2003 voting on the hardware level
- The user interfaces for the reading and acting on the current loops
- Monitoring and Diagnostics facilities through a dedicated Profibus/Profinet link for a 2-way communication with the PLC.

Each discharge loop consists of a three independent current loops that will connect one or more user interface boxes in series before returning to the PLC master. The lack of current in each of the loops will be interpreted as a false state. If at least two out of the three loops are without current, this will be interpreted by the CIS, the FDU and the power converters as the command to trigger a fast discharge of the circuit.

The user interface connects the users to the discharge loops, both to command the opening of the discharge loops (for the QD, FDU and power converter) as well as to read the state of the discharge loop (for the FDU and power converter). Figure 2 illustrates the current version of the user interface box.

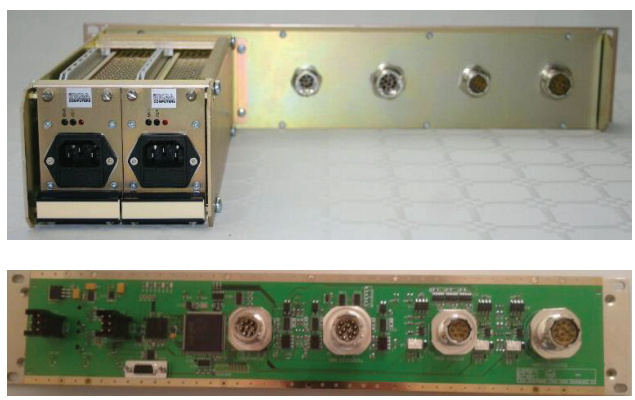

Figure 2: Rear view and electronics inside the user interface box.

ISBN 978-3-95450-139-7

DEPENDABILITY STUDIES ON ITER MAGNET POWERING INTERLOCKS

Dependability requirements of ITER for high safety and availability are huge challenge for machine protection systems. Investment protection requires a high level of safety (probability of a blind failure to occur less than once every 1000 years) as well as a high level of availability (less than 1 false positive in 20 years of operation due to failures of the interlock system). Dependability studies have been performed [4] [5] following a statistical approach, confirming a 2-out-of-3 voting architecture as the only suited candidate to meet the stipulated dependability requirements.

HARDWARE AND SOFTWARE IMPLEMENTATION

The chosen hardware solution is hence based on a 2oo3 voting architecture based on standard PLC modules and hardwired current loops as illustrated in Figure 3. This combination provides the required balance between safety and availability while assuring the required reaction time of the interlock system (hard real-time system). The controller is based on the S7400H PLC technology and ET200M remote periphery modules in 2oo3 redundancy. In order to describe its operation, we can distinguish:

- Processing components: Redundant CPUs and the Boolean Processors
- Periphery I/O: periphery modules interconnected with the processing components through a PROFIBUS network or hardwires. The periphery modules are standard ones, namely analogue input modules to generate and measure the current flowing through the discharge loops and relay output modules able to open/close the discharge loops and discrete relays.

Two racks with identical components compose the H CPU system (Figure 3):

- CPU 414-4H: H CPU with two PROFIBUS connectors
- CP443-1 Adv.: Communication processor providing 1 Gb Ethernet port and up to 4 Ethernet/PROFINET ports

Two PS 407 10A R: Redundant power supply to power the rack.

The Boolean Processors are a set of fast CPU modules based on FPGA technology, capable of providing redundancy and minimizing latency to the processing of the discharge loops, hence increasing the dependability of the overall system. With the implementation of the ITER magnet powering interlocks considering only six circuits, two Boolean Processors are required. Figure 3 illustrates the installation of the Boolean Processors (reachable by the CPUs through the PROFIBUS network) inside the fourth ET200M slave.

The rest of the periphery I/O implements:

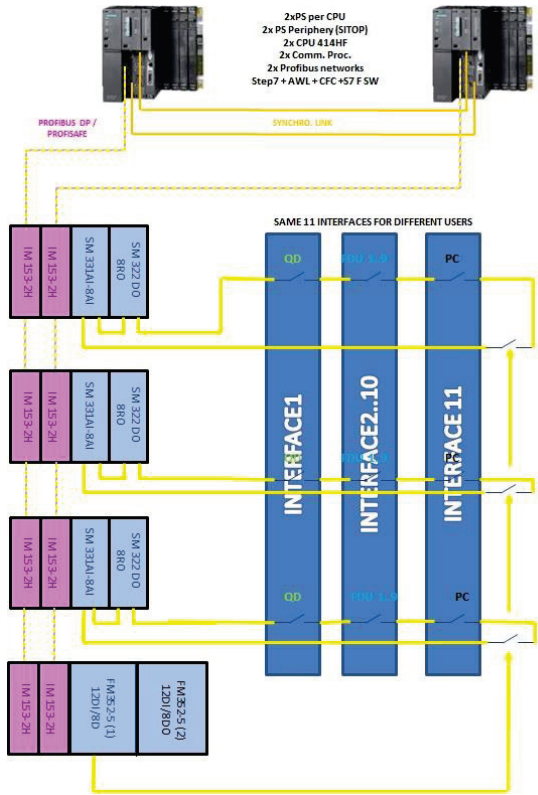

Figure 3: Architecture of prototype system for ITER magnet interlocks.

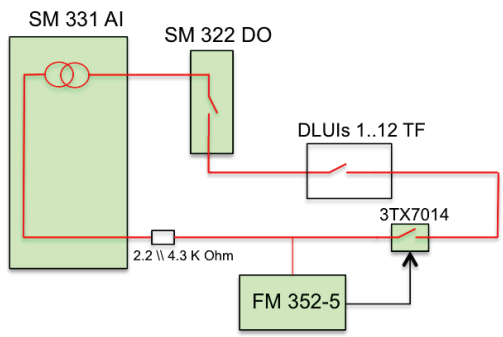

Figure 4: Current loop components.

- The discharge loop in 2oo3 redundancy
- The actuators for the control of the discharge loop using relays.
- The interface with the external clients: Quench detection, Fast Discharge Units, Power Converters and PMS; through the Discharge Loop User Interface boxes.

Each of the 3 additional slaves is composed by:

- Two IM 153-2H modules which provide the PROFIBUS connectivity with the CPUs. Each IM module is connected with one of the CPUs. In this way, both CPUs can access any of the I/O modules.
- One SM331 AI module to generate the current for the discharge loops and to measure this current.
- An SM322 DO (relay output) standard module to open or close the discharge loop according to the control software.

ISBN 978-3-95450-139-7

In order to build a single discharge loop, the components are arranged as shown in Figure 4. Each ET200M slave builds six discharge loops, hence three ET200M slaves are required to build the 18 discharge loops (corresponding to the implementation of 6 circuits).

A software engineering technique specially indicated for real-time safety critical applications known as "N-version programming" has been used for the control of the discharge loops. In this way, the probability of software errors is reduced while improving the reliability thanks to the fault tolerance or redundancy achieved. To perform the implementation of this technique we have used:

- Redundant and independent programs to control the discharge loop: "KOP" program compiled to an FPGA for the code running in the Boolean Processors; and "AWL + KOP" program for the code running on the H CPU system.
- Independent and redundant processing units: H CPU system and Boolean Processors
- Independent and redundant sensing and actuating equipment: Sensing equipment (H CPU system uses the analogue input modules, and the boolean processors use direct connections to the discharge loop), actuating equipment (the H CPU system uses the relay output modules, and the boolean processors use discrete relays). Besides, the PLC modules are arranged into different ET200M PROFIBUS slaves.

Besides the hardware signals described so far, a set of software signals are planned to be connected to the interlocks system through PROFINET (and potentially Profisafe) for software communications. These software signals originate from several Plant Interlock Systems (PISs) like Fast Discharge Units, Quench Detectors, Power Converters and Cryogenics and are processed by the H CPU system. The corresponding will be transmitted to the Power Converters PIS and Plasma Control System PIS trough the Plasma Protection Module.

The software running on the H CPU system has implemented following a formal approach, involving the design of a set of finite states machines described in an oriented graph, and the extraction of a set of logic equations from these graphs.

In the present design, four finite states machines are needed (one per circuit family). From these graphs, a set of logic equations can be easily extracted. These equations are called state and output equations. Figure 5 depicts the state machine for the toroidal field circuit.

For the fast controls, the reaction time between the detection time of a quench in an FM352-5 module until the mechanical relay opens (commanded by the FM module) has been measured to be 5.74 ms. This time corresponds to the execution of the FM program plus the time needed by the mechanical relay to open. For the slow controls, the time elapsed between the quench detection until the opening of the relay output module is 20.4 ms. This time corresponds to the execution of the OB34 program in the H CPU system plus the time needed by the mechanical relay to open.

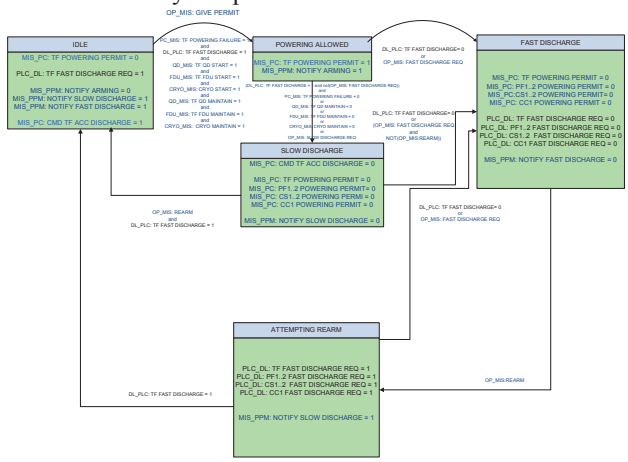

Figure 5: State machine for the toroidal field circuit.

CONCLUSIONS AND FURTHER WORK

The implementation of the first interlock prototype has yielded promising results, both in terms of performance as well as dependability. The system has been conceived to scale easily to the 21 circuits needed for the final ITER Magnet Powering Interlocks implementation.

A lot of effort has been undertaken towards a formalisation of the design specification in collaboration with a company specializing in safety critical systems.

Future works will include the programming of the remaining software signals for CPU communications, additional response time evaluations, and the design of automatic test and diagnostic features to guarantee the system integrity through throughout operation.

ACKNOWLEDGMENTS

We would like to express our gratitude to the CERN TE-MPE group and ITER CODAC, in particular A.Vergara, for their outstanding support and help with the implementation of the project.

REFERENCES

[1] F. Millet, O. Liotard: ISO Ingenierie, L.Scibile, A. Vergara Fernandez, "Requirements Specification and Functions Definition for Machine Protection: Magnets (PBS11)", CHD-CODAC, Case Study ITER Report, January 2010

[2] CERN-ITER agreement: CERN ref. No. K1449/AT

[3] J. Burdalo "User Manual for ITER Discharge Loop User Interface V1", ITER engineering specification, CERN TE-MPE, ITER 2012

[4] S. Wagner, "LHC Machine Protection System: Method for Balancing Machine Safety and Beam Availability", PhD - ETH Zurich, 2010

[5] S. Wagner et al, "Architecture for interlock systems: Reliability analysis with regard to safety and availability", ICALEPCS 2011

ISBN 978-3-95450-139-7