Machine Protection System Design

D. Marcato[1], F. Gelain[1], G. Savarese[1], A. Monetti[1], M. Manzolaro[1], D. Scarpa[1], L. Centofante[1], L. Antoniazzi[1], A. Calore[1], G. Lilli[1], C. Roncolato[1], M. Maggiore[1], L. Pranovi[1], P. Antonini[1], L. De Ruvo[1], M. Gulmini[1], M. Roetta[1], D. Benini[1], M. L. Allegrini[1], D. Bortolato[1]

[1]*INFN, Laboratori Nazionali di Legnaro, Legnaro (Padova), Italy.*

INTRODUCTION

The Machine Protection System (MPS) of the SPES project is responsible for the protection of all the machine elements from damages and unnecessary radiological activations. In addition, it's designed to be the central coordinating system of all the heterogeneous subsystem of the machine, which must work together without interferences.

Here we will present the main functions of the MPS and its high-level design process, which involved different working groups at the lab.

GENERAL DESIGN

The MPS is a distributed system consisting of a redundant central node and multiple peripheric systems. The central node implements all the protection functions related to the equipment directly connected to it. Many other MPS functions are delegated to external controllers, when they achieve the reliability required by the MPS and are directly connected to all the signals required by the protection function.

When coordination of several systems is required to achieve a protection function, each system must talk to the MPS central node, which reads the state of all the systems and implements the logic to grant the permissions and interlocks to the peripherical systems. This creates a tree structure, where the MPS central node is the root of the tree and the leaves only talk with the root, instead of talking to other leaves, so that the systems can be coordinated from a single entity with a complete overview of the whole tree.

These systems, including the peripherical nodes and their interconnections, must provide an industrial level of reliability. This means that the logic must be implemented with PLCs, excluding standard software running on PCs or servers, and the connections can be implemented with wired signals or with network connections using industrial protocols such as MODBUS/TCP. In this case connection status must be constantly monitored, and in the event of a disconnection each system must remain in a safe state.

PROTECTION FUNCTIONS

The MPS must protect the machine from different kinds of threats. Here we will describe the main ones and the corresponding protection functions.

The first threat the MPS must manage is the proton beam itself due its high-power density, which can damage some elements of the beam line. For example, if the wobbler stops working, the beam can damage the target in few milliseconds, so the MPS must be able to stop it within 6ms.

The beam must not reach a target if this target is not ready, meaning that all its operating parameters are reached, so that it can be operated safely. In case just one of the parameters is not nominal the beam must be inhibited or stopped if it is already present. In addiction, the primary beam must be stable and close to the expected current setpoint, and the MPS must intervene if these parameters are wrong. If the primary beam stops unexpectedly the MPS must power on the heater to avoid mechanical stress to the Isol1 target.

Other protection functions include the inhibition of high voltages when the vacuum level is not good and continuously checking the cooling water parameters to enable all the heat sources. In general, the protection function of the MPS should guarantee that each device is used without exceeding its operating range. The MPS will also try to minimize the activation of the instruments on the beam line by stopping the beam in hot areas like the safety Faraday cup to prevent activation of other equipment like the vacuum gate valves.

For simplicity, the MPS also implements the low-level control system of some devices, where the protection function is more complex than the control system. For example, all the Faraday Cups are moved directly by the MPS PLC, according to the protection logic.

COORDINATION FUNCTIONS

Another important aspect of the MPS is its function as coordinator to ensure the human error can't harm the machine. Especially around the Isol1 target area, there are different subsystems mostly independent from each other, which have to share some common resources or have inherent interference. In this case the MPS implements its protection functions by correctly enabling each system to operate avoiding interferences, race conditions and deadlocks.

The first example is the TIS Handling system and the shielding doors, where the MPS must prevent the Handling system from being in the door area when it moves. In addiction, the TIS coupling table and the Vacuum system must be coordinated because the TIS can't be uncoupled while the system is in vacuum and the vacuum can't be reached while the TIS is uncoupled. The

MPS is also used to request to deactivate the high voltage of the ISOL1 platform to the Local Safety System, so that the AGV can enter the bunker.

All these coordinating functions in a distributed system imply that a protocol must be implemented, based on messages to ask for a shared resource (such as the exclusive access to a device to operate without interference) and ACK or NACK to grant or deny the access. In fact, a single enable or interlock signal is usually not sufficient to avoid deadlocks or race conditions.

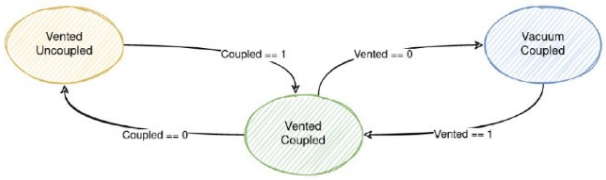

Fig. 1: Example diagram of the states of the vacuum and TIS coupling systems.

LOGICAL INTERFACES

To implement all its functions the MPS must talk with many heterogeneous systems. For example, a specific hardwired interface has been developed to communicate with the Cyclotron Protection and Control System to know the targets of the beams and the energy and current level of both beams. With this key information the MPS can tell the Cyclotron if the selected target is ready or not to receive the beam and interlock it if required.

Other systems are:

- The PLC of the technical plants
- Coupling table and pneumatic movements
- All vacuum PLCs
- Handling PLCs
- Shielding Doors
- Heaters and Gas Panel PLC
- Safety systems
- Laser
- Beam Cooler
- Multi Collimator System
- All beam transport power supplies

Moreover, some additional devices will be developed and connected to the MPS PLC to implement the Fast Interlock System, which must be able to generate an interlock in a few ms. Another required device is a specific diagnostic to read the primary beam current with high accuracy and fast read times.

HARDWARE DEFINITION

One challenge in the design of the SPES MPS is the need to take in to account all the subsystems that will be in operation in the final facility.

Some subsystems are foreseen for future uses of the SPES facility, and they will have the MPS as input in the design process. However, the majority are yet in an advanced design phase or in a construction or commissioning phase.

In this scenario we had to go deep in their design to be sure to develop an interface with the MPS that will be implemented easily from the electrical point of view and the process logic one.

In some cases, like the one of the technological plants servicing the ISOL1 machine, the MPS is also responsible for some control aspects and so it directly manages the field equipment. In this case, we had to collect all the electrical signals from the field, managing it properly using the right PLC interfaces. We had also to design an interface with the controller of the primary water-cooling circuits to prevent pumps overload or other faulty behaviours during the operations planned for the ISOL1 circuits.

In general, we design the SPES MPS as a modular system minimizing the physical interfaces when it's possible to communicate effectively by network.

This modular design has its core in two redundant Schneider PLC CPUs, one in the ADIGE injector area and one in the SPES 1007 area. Different I/O nodes, located as close as possible to the field, are used for the I/O managed directly by the MPS. When the interface needed is only a network protocol, it is managed as Modbus/TCP communication between the CPU and the subsystem controller.

Network interfaces with subsystems are also required in the cases where is not possible to have electrical interfaces due to environment conditions like the presence of HV potential between the MPS CPU and the subsystem (this is the case of all HV platforms). In those cases, an independent PLC is located inside the platform, which guarantees basic functionalities even without network connectivity. When available, it communicates through network protocols over the fibre optic network infrastructure [1] with the MPS CPU to manage high level coordination and protection functions.

CONCLUSION

The SPES MPS will be a key system in the SPES facility where all the procedure usually define for human operations, will be managed by an automatic system to reduce the probability of machine damages, especially in the target areas. Its design and modularity enable future expansions and enhancements.

The first phase of the MPS will include only the ISOL1 target and the beam line up to the S009 area. For this part, the design phase is concluded, the hardware interfaces have been defined and the cabinet can be designed. At the same time, the software can be developed incrementally, and the first parts can be tested as soon as the final hardware is installed.

[1] F. Gelain et al., LNL Annual Report (2022).