ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA105

ESS TARGET SAFETY SYSTEM DESIGN

A. Sadeghzadeh†, M. Olsson, O. Ingemansson, L. Coney, M. Mansouri
European Spallation Source ERIC, Lund, Sweden

Abstract

The purpose of the Target Safety System (TSS) is to protect the public from exposure to unsafe levels of radiation, prevent the release of radioactive material beyond permissible limits, and bring the neutron spallation function into a safe state. In order to fulfill the necessary safety functions, the TSS continually monitors critical parameters within target station systems. If any parameter exceeds an acceptable level, the TSS actuates contactors to cut power to components at the front end of the accelerator and prevent the beam from reaching the target. The TSS is classified as a safety structure, system and component, relevant for the safety of the public and the environment. As such, it requires the highest level of rigor in design and quality for interlock systems at the ESS. Standards are applied to provide a guideline for building the TSS architecture and designing in resistance to single failures and common cause failures. This paper describes the system architecture and design of the TSS, including interfaces with target station and accelerator systems, and explains how the design complies with authority conditions and requirements imposed by development standards.

TSS SAFETY FUNCTIONS

The ESS target radiation safety functions were derived from the hazard and accidents analyses of target station systems and areas. A qualitative hazard analysis was performed to identify and evaluate potential radiological accidents, from which a collection of bounding events was selected for further analysis. The accident analysis detailed the identified accidents to determine the related level of risk. This involves quantification of severity, as measured by the dose consequences to both workers and the public, and definition of appropriate control actions to enable an acceptable level of risk.

To mitigate consequences of the accidents, different functions were identified in different levels of defence in depth (DiD) for systems in the target station. Functions to be fulfilled by the TSS were identified in DiD level three. Depending on the level, different constraints shall be applied on the design in terms of conditions from SSM (Swedish Nuclear Safety Authority) and design guidance from applicable standards.

Since the target contains a high inventory, many of the accident analyses address scenarios that could affect the target material or the helium cooling system. The most critical hazards tend to be related to increased temperature of the target wheel tungsten, which, if accompanied by oxidation of the tungsten and a loss of confinement, might have consequences of radiological releases. The following accident scenarios require TSS functions in order to prevent or mitigate the unacceptable consequences:

AA1: Target wheel rotation stop during beam on target

AA2: Proton beam events on target and proton beam window (non-rastered & focused beam)

AA3: Loss of target wheel cooling during beam on target wheel

In these accident scenarios, the increase of temperature in the target material leads to unacceptable radioactive material releases. Since the target is designed so that the decay heat can be dissipated by passive means, removing the beam removes the source of heat and puts the spallation process into the safe-state.

The following safety functions are dedicated to the TSS. The TSS shall monitor process variables in the wheel, helium cooling, and monolith systems to identify if the:

- Target helium cooling outlet velocity is below a certain limit
- Target helium cooling outlet pressure is below a certain limit
- Target helium cooling inlet temperature is above a certain limit
- Target wheel rotational speed is below a certain limit
- Monolith atmosphere pressure is above a certain limit

If any of the above conditions occur, the TSS shall bring the ESS spallation process to a safe-state (in terms of radioactive releases) by turning off the proton beam to prevent escalation of the situation. Figure 1 illustrates the location of the process variable monitored for radiation safety function.

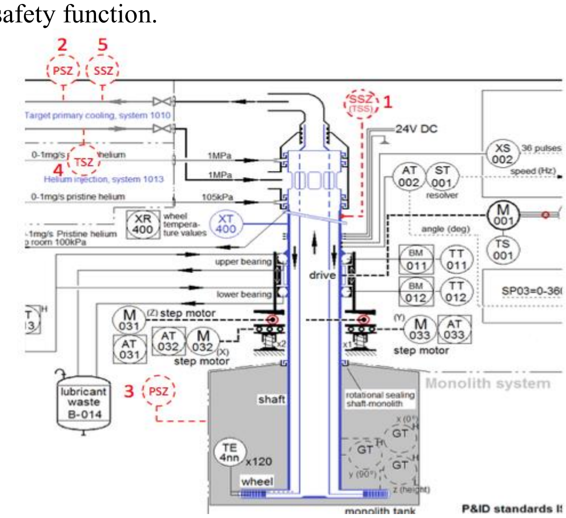

Figure 1: TSS process variables for safety functions.

† atefeh.sadeghzadeh@esss.se

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA105

REQUIREMENTS AND SOLUTIONS

TSS is identified as a safety SSC (Structure, System, Component) [1] in which requires TSS to survive

- Single failure
- Common cause failure
- Internal and external initiating events and condition

As respond to these requirements ESS safety systems shall include redundancy, diversity, independence, and physical separation to the extent that it can meet the SSM conditions for single failures and common cause failures.

Redundancy

Redundancy in TSS will be realized as:

- Two-train architecture: TSS is designed as a two-train interlock system. Either of the TSS trains can execute the expected safety functions.
- Redundant trip devices (contactors) to shut down proton beam production. The contactors will be placed in series on the relevant accelerator power circuits.
- Redundant sensors with a 2oo3 voting functionality in the target helium cooling system, the target wheel rotation system, and monolith system

Diversification

For TSS, diversity will be implemented to prevent internal failure of two independent components at the same time. Diversity will be realized as:

- Diverse technology for platforms (PLC vs. relays)
- Diverse trip mechanisms: Ion source vs. RFQ
- Diverse vendors for sensors and trip devices
- Functional diversity: diverse measurements to identify the same event

Independence

In order to fulfil functional separation, which is a condition from SSM to the safety systems, TSS shall be independent from other systems. Independence will be fulfilled by:

- TSS acts independently of other systems. There will only be one-way communication of monitoring data to other control systems.
- TSS trains act independently of each other with no inter-train safety-credited communication.

Physical Separation

The physical separation will be implemented to maintain functionality in case of an external event, such as fire, that could cause failures in both trains or in redundant components within one train. Realization of physical separation for TSS will be:

- TSS physically separated from other control systems
  - TSS dedicated sensors, logic and trip devices
  - TSS dedicated room for logic
  - TSS dedicated closed trunks/pipes/conduits for cables
- TSS trains physically separated from each other
  - Separate locations for logic devices
  - Separate locations of trip devices
  - Separate racks or cabinets in combined areas
  - Separate closed trunks/pipes/conduits for cables

ARCHITECTURE

The TSS consists of two diverse and independent trains; one train is based on hardwired relays technology and one train is based on distributed PLC technology. Each train consists of three redundant and physically separated channels (A, B and C) and performs all the safety functions independently on the other train. Each process variable is measured by three sensors (A, B and C). All A-sensors are merged to channel A, B-sensors to channel B and C-sensors to channel C. The 2oo3 voting in each train is performed on the three channels (see Figure 2).

The beam is tripped by two diverse, independent and separated mechanisms; power shut-down to the Ion source and power shut-down to the RFQ. Each train acts on both trip mechanisms.

The system architecture is built on fail-safe concept. Any loss of power, sensor signal or communication will be interpreted as an indication for trip (i.e. shut down of the proton beam).

TSS is physically separate and independent of other control systems such as BPCS and MPS.

The three redundant and physically separated channels (A, B and C) consist of sensor measurements. The separation is valid from the sensors, via the A/B/C cabinets in the utility room, and the cable paths to the 2oo3 voting functions.

The two diverse trains consist of diverse 2oo3 voting functions (PLC and relay). Each train acts on separate actuators. The 2oo3 voting functions are placed in physically separated areas; the PLC is placed in Target building and the relay is placed close to the actuators in the Accelerator building.

A Gateway PLC is used in parallel with the channels and the trains for non-safety functions such as monitoring, operator interface and data archiving. The channels and the trains are independent on, and do not share any component with, the Gateway PLC.

The Gateway PLC shares cable paths with the three channels (A, B and C).

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA105

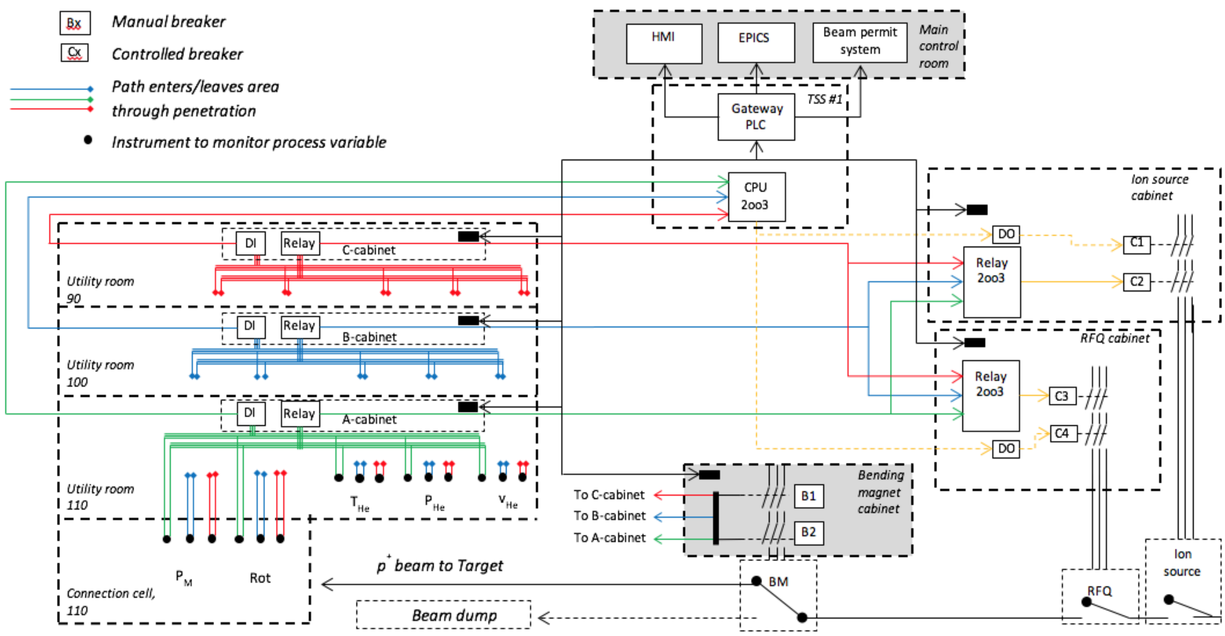

Figure 2: TSS architecture.

2OO3 VOTING LOGIC

Upon receive of work order, the safety functions in each train can be temporarily muted by assuring that the proton beam is directed towards the beam dump instead of the target wheel. The procedure to mute the safety functions is restricted by both manual settings and position feedback signals (see Figure 3). The functionality is foreseen for the situations where target station is not ready to receive beam (e.g. during maintenance) but the accelerator shall tune/test functionality.

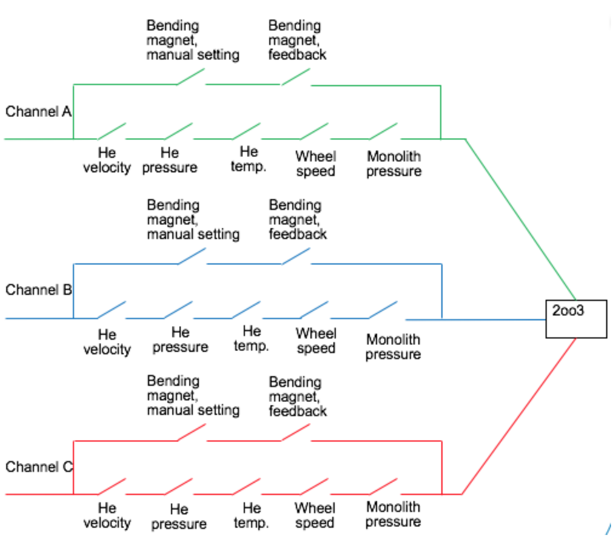

Figure 3: Logic for 2oo3 voting of the channels.

CONCLUSION

TSS is a robust independent safety interlock system. It has dedicated equipment for monitoring, evaluation and actuation. The system architecture is built on fail-safe concept and the actuation of the safety functions are performed by passive means. Any loss of power, sensor signal or communication will be interpreted as an indication for trip (i.e. shut down of the proton beam). TSS is physically separate and independent of other control systems such as BPCS (Basic Process Control System) and MPS (Machine Protection System).

The TSS design includes redundancy and diversity to fulfill SSM conditions for resistance to single failure and common cause failure.

REFERENCES

[1] Francois Javier, “ESS rule for identification and classification of safety important components”, European Spallation Source Report ESS-0016468 (2016)