Target Safety System design for the ESS target station

Atefeh Sadeghzadeh¹, Mikael Olsson¹, Linda Coney¹
¹European Spallation Source Eric, Tunavagen 24, 223 63, Lund, Sweden

Atefeh.sadeghzadeh@esss.se, mikael.olsson@esss.se, linda.coney@esss.se

Abstract. The European Spallation Source (ESS) will be a 5 MW neutron spallation research facility where an energetic proton beam incident upon a helium-cooled tungsten target is converted to neutron beams. The liquid hydrogen moderator, water moderator, and reflector systems within the target monolith slow the high-energy spallation neutrons down to cold and thermal neutrons suitable for use by experiments. Several layers of control, protection, and safety systems will be implemented in order to ensure safe operation of this advanced facility.

The Target Safety System (TSS) is part of the overall radiation safety plan for the Target Station. As such, in case of an abnormal event, the TSS will 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. This safe state is defined as no beam incident upon the target. Since the target is the source of the release of radiation in the presence of the beam, putting the target station into the safe state (no beam), brings the spallation process to the safe state.

The TSS safety functions are based on the results from hazard and accident analyses done to evaluate radiation hazards within the target station. The most critical hazards are related to increased temperature of the target wheel tungsten, which can be the result of cooling system malfunctions or stopping of the rotating target. Therefore, the TSS will monitor parameters related to the cooling conditions and rotation of the target.

As a safety system, the TSS is subject to requirements from the Swedish Nuclear Safety Authority (SSM), including single failure and common cause failure criteria. These requirements impact the system architecture in terms of redundancy, separation and diversity. Dedicated redundant and diverse TSS sensors are connected to two diverse and separated trains performing the same safety functions. Each train acts on diverse and separated mechanisms to stop the beam from reaching the target.

This paper will describe the design and architecture of the TSS, which implements the safety functions identified in the radiation safety analyses and fulfils the SSM conditions.

1. 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 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 accident analyses (AAs) and location of the process variable monitored for each radiation safety function.

Figure 1 TSS process variables for safety functions

2. TSS Requirements
TSS is identified as a safety SSC (Structure, System, Component) in [1] which requires TSS to include redundancy, diversity, independence, and physical separation to the extent that it can meet the SSM
conditions for single failures and common cause failures.

2.1. Redundancy
In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system [2]. 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

2.2. Diversification
ESS general implementation rule states that diversity shall be implemented for a safety SSC to prevent common cause failures in redundant parts. For TSS specifically, 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) and cable material (fibre vs. copper)
- Diverse trip mechanisms: Ion source vs. RFQ
- Diverse vendors for sensors and trip devices
- Functional diversity: diverse measurements to identify the same event

2.3. Independence
In order to fulfill 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.

2.4. Physical separation
Physical separation shall be implemented for a safety SSC to minimize the risk that events give rise to failure in redundant parts. For TSS specifically, 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 rooms 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

3. TSS Architecture
The TSS architecture is fundamentally a two-train fail-safe interlock system. TSS will continuously monitor safety parameters in the target He cooling, wheel, and monolith atmosphere systems, evaluate their condition, and shut down the accelerator if necessary. Figure 2 shows the layout of TSS
equipment within the ESS facility, highlighting the locations relevant to each train. It also illustrates the physically separated cable routes of the two trains through different areas of the facility.

**Figure 2 TSS layout**

As shown in Figure 3, the two trains will measure the same process variables and perform the same logical evaluation of the variables, but will act on separate mechanisms to shut down the beam. The system will be independent of other systems and will rely solely on its own dedicated equipment.

**Figure 3 TSS architecture**

Each train can prevent the beam from reaching the target by removing the active control signal to contactors on the power circuits to the ion source or to the RFQ. The control signal to the contactors must remain active in order to produce the proton beam, i.e. the system is fail-safe.
Diverse sensors will measure each process variable, and all sensor values will be sent to both trains. The logic handler of each train treats input from the redundant sensors with a 2oo3 voting function. The logic solvers are pieces of diverse control equipment to be located at physically separated areas within the Target Building. They will evaluate the sensor information and control the contactors.

The actuators are diverse and physically separated power contactors. They will be located at the front-end of the accelerator tunnel and act on the power circuits feeding the equipment that generates the proton beam at the ion source and the RFQ. If any of these power circuits is broken, no proton beam can be propagated through the accelerator to the target.

TSS is a fail-safe system. The PLC will continuously run diagnostic tests of status on its own HW, connected cables, and feedback from actuators. Any failure will force the system to the safe-state. Back-up power is not accredited for any of the TSS safety functions. TSS components have a pre-defined fail-safe state in case of loss of power, leading to the safe-state of the system. While not accredited, back-up power will be used for availability reasons.

4. TSS Interfaces
The TSS will interface with other ESS systems according to Figure 4. From the target station systems, critical process values are monitored and evaluated continuously. Any sign of failure will cause the action to go to the safe state. The TSS will extract information from accelerator systems related to operational modes. TSS has its own circuit breaker in the power line of the dogleg bending magnets to force the beam direction to the dump while continuously monitoring feedback from these breakers. In this way, the accelerator can send beam to the dump while the target is not ready to receive beam. The status of the TSS will be available for monitoring to operations personnel in the main control room.

5. Conclusions
The TSS is a robust and independent safety interlock system. It has dedicated equipment for monitoring, evaluation, and actuation, and does not rely on any other system in order to perform its safety functions. The design is fail-safe and the actuation of the safety functions is performed by passive means. The TSS design includes redundancy and diversity, which fulfils 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)
[2] https://en.wikipedia.org/wiki/Redundancy_%28engineering%29