Reliability Analysis of the ESS Target Safety System

Atefeh Sadeghzadeh
Control engineer – Target safety and control

www.europeanspallationsource.se
17-09-14
Outline

• Short introduction of ESS
• ESS target station
• What is TSS
• Deterministic reliability
• Probabilistic reliability
Model of future ESS
The European Spallation Source (ESS) is a multi-disciplinary research center based on the world’s most powerful neutron source.

Neutron Science Systems
- 22 planned and budgeted neutron scattering instruments
- Neutron beam line lengths ranging from 10 m to 150 m from source

Proton Linear Accelerator
- Pulse frequency 14 Hz
- Proton energy 2 GeV
- Beam power, time averaged 5 MW, within pulse 125 MW
- Beam current 62.5 mA
Site view - status

Monolith area of Target – June 2017

June 2017
Layout of the target station

For more detail see R. Linander talk tomorrow afternoon
Purpose of Target Safety System (TSS)

• TSS is the ESS safety interlock system that shall:
  - ”...protect the public from exposure to unsafe levels of radiation, and preventing the release of radioactive material beyond permissible limits”
  - ”...bring the spallation process into a safe state in case of an abnormal event from nuclear safety point of view...”

• TSS does not consider personnel safety or machinery safety
Systems under consideration - Hazard Analysis Scope

**Fluid Systems**
- Active Liquid Purification system
- Primary Water Cooling Systems
- Intermediate Water Cooling Systems
- Intermediate Water Cooling for Water Systems
- Contaminated Tanks
- Gas Delay Tanks

**Remote Handling Systems**
Active Cells Operations

**Target Systems**
- Target Wheel & He Cooling
- He Purification

**Moderator Systems**
- Water Moderator
- Reflector System
- Cold Moderator
- Target Moderator
- Cryoplant System

**Monolith Systems**
- Monolith vessel incl. covers and penetrations, NBW, PBW
- Shielding systems
- Tuning Beam Dump

**Utility Area**

**High Bay**
Cardinal Hall

**Target HVAC System**

**High bay Crane Access**
Event categories, Safety functions groups and Defence in Depth Levels

**Level 5**: to mitigate the radiological consequences of emissions to the environment that may result from events and circumstances with extensive damage to radiation sources.

**Level 4**: ensure that radioactive emissions to the environment resulting for events and circumstances with extensive damage to radiation sources are as low as is practicable and reasonable.

**Level 3**: minimize the impact of events and circumstances that lead to increased radiation levels and limit dispersion of radioactive substances (within the facility and surrounding areas) as well as counteract extensive damage to the radiation source.

**Level 2**: Detect deviation from normal operation and manage discrepancies to avoid increased radiation levels or dispersion of radioactive substances within the facility.

**Level 1**: Prevent failures and deviations from normal operations + deal with minor deviations to stay in normal conditions

- Operational group
- Safety group
- Mitigation group
- Emergency preparedness plans

Accidental situation off site radiological impact necessitating protective measures

Accidental situation limited off site radiological impact H5

Accidental situation No off site radiological impact or minor H2 + H3 + H4

Authorized operation H1 + H2

Normal operation H1
TSS safety functions

# Safety functions

<table>
<thead>
<tr>
<th>#</th>
<th>Safety functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Target cooling He outlet velocity is below critical limit</td>
</tr>
<tr>
<td>2</td>
<td>Target cooling He outlet pressure is below critical limit</td>
</tr>
<tr>
<td>3</td>
<td>Target cooling He inlet temperature is above critical limit</td>
</tr>
<tr>
<td>4</td>
<td>Target wheel rotational speed is below critical limit</td>
</tr>
<tr>
<td>5</td>
<td>Monolith pressure is above critical limit</td>
</tr>
</tbody>
</table>

- Correlated to bounding events identified in the accident analyses
- Independent of each other
TSS - safety instrumented functions - principal

Read (sensors):
- Target wheel He cooling outlet velocity
- Target wheel He cooling outlet pressure
- Target wheel He cooling inlet temperature
- Target wheel shaft rotational speed
- Monolith pressure

Evaluate (logic solvers):
- If inside all limits:< 35 m/s
  - < 6.2 bar
  - > 230 °C
  - < 11.6 rpm
  - > TBD bar
- If any limit exceeded

Act (final elements):
- If sensor connection lost
- If communication lost
- If control HW failure
- If power lost

Fail safe:
- Close contactors at power circuit to ion source and RFQ
- Open contactors at power circuit to ion source and RFQ= SAFE STATE
Target building
- Sensors (reading Target process variables)
- Logic solvers (located in two different areas)

Front end building
- Final elements (to stop proton beam = safe state)
SSM conditions and ESS rules

• SSM conditions:
  – Survive Single Failure
  – Survive Common Cause Failure
  – Survive Internal and external initiating events and conditions

• ESS Solution
  – Redundancy
  – Independence
  – Physical separation
  – Diversity
System architecture - overview

- He pressure
- He temperature
- Wheel speed
- Monolith atmosphere pressure

Monolith system

Target wheel

Bending magnet

Beam dump

Proton beam
Deterministic reliability analysis (FMEA)

- **SSM conditions**
  - **D1**: “Deterministic [...] methods shall be used to analyze and evaluate [...] the facility’s ability to fulfil the fundamental safety functions”
  - **C19/E10**: Single failure
  - **C20/C21/E11**: Common cause failure
  - **C18**: External events and conditions

- Deterministic criteria were developed in order to account for randomly occurring failures. They are inherently rigid. In deterministic analysis the system should be able to withstand the removal of any single component. This is obviously a worst-case criterion. If the system can withstand the worst case situation, it can withstand the rest.

- **Failure Mode Effects Analysis**
  - An FMEA is often the first step of a system reliability study.
  - It involves reviewing as many components, assemblies, and subsystems as possible to identify failure modes, and their causes and effects.
  - For each component, the failure modes and their resulting effects on the rest of the system are recorded in a specific FMEA worksheet
  - [https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis](https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis)

- **IEC 60812**
  - *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*
Probabilistic Reliability

• SSM conditions
  – D1: “[...] Probabilistic methods shall be used to analyze and evaluate [...] the facility’s ability to fulfil the fundamental safety functions”

• Probabilistic Reliability is
  – the probability that an item (TSS) will perform a required function, under stated conditions, for a stated period of time. TSS is highly reliable if it works for a long time without failing

• IEC 61508 and IEC 61511 is used for probabilistic reliability assessment
  – The risk reduction allocated to a safety function is determined by it’s Safety Integrity Level (SIL)
  – The effectiveness of a safety function is described in terms of “the probability it will fail to perform its required function when it is called upon to do so.” This is its Probability of Failure on Demand (PFD).
### Risk table

<table>
<thead>
<tr>
<th>Severity (mSv)</th>
<th>&lt; 0.1</th>
<th>0.1 – 1</th>
<th>1 – 20</th>
<th>20 – 100</th>
<th>&gt; 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H2</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>H3</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>H4(A&amp;B)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>H5</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Event probability</th>
<th>Tolerable probability</th>
<th>SSM referenced probabilities (see [6], Appendix 1, chapter 4, 2A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H2</td>
<td>10^{-2}</td>
<td>-</td>
<td>10^{-2} &lt;= P</td>
</tr>
<tr>
<td>H3</td>
<td>10^{-3}</td>
<td>10^{-4}</td>
<td>10^{-4} &lt;= P &lt; 10^{-2}</td>
</tr>
<tr>
<td>H4/A&amp;B</td>
<td>10^{-5}</td>
<td>10^{-6}</td>
<td>10^{-6} &lt;= P &lt; 10^{-4}</td>
</tr>
<tr>
<td>H5</td>
<td>-</td>
<td>10^{-7}</td>
<td>P &lt; 10^{-6}</td>
</tr>
</tbody>
</table>
## Target SIL (AA1)

<table>
<thead>
<tr>
<th>Accident Analysis</th>
<th>SIF ID</th>
<th>Initiating Events</th>
<th>Higher occurrence probability</th>
<th>Dose to public (maximum of different scenarios)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA1: Target Wheel stops rotating while the accelerator is in operation and a 5 MW high power beam is impinging upon the target at a rate of 14 Hz</td>
<td>SIF4, SIF2, SIF5</td>
<td>Bearing failure, Motor failure, Power outage, Target positioning system fails, Shaft inner labyrinth rotational seal seize and wheel rotation stops</td>
<td>H2 F &gt; 0.01</td>
<td>18 mSv</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity (mSv)</th>
<th>&lt; 0.1</th>
<th>0.1 – 1</th>
<th>1 – 20</th>
<th>20 – 100</th>
<th>&gt; 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H4(A&amp;B)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

H2 -> H4: $PFD_{avg} = 10^{-6}/10^{-2} = 10^{-4}$ -> SIL 3
Summary of SIL determination

- PLC train only: $PFD_{avg} = 4.84 \times 10^{-4}$
- Relay train only: $PFD_{avg} = 2.73 \times 10^{-3}$
- Total: $PFD_{avg} = 8.90 \times 10^{-4}$

<table>
<thead>
<tr>
<th>SIL</th>
<th>Availability</th>
<th>$PFD_{avg}$</th>
<th>Risk Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>&gt;99.99%</td>
<td>$10^{-5}$ to $&lt;10^{-4}$</td>
<td>100,000 to 10,000</td>
</tr>
<tr>
<td>3</td>
<td>99.9%</td>
<td>$10^{-4}$ to $&lt;10^{-3}$</td>
<td>10,000 to 1,000</td>
</tr>
<tr>
<td>2</td>
<td>99 to 99.9%</td>
<td>$10^{-3}$ to $&lt;10^{-2}$</td>
<td>1,000 to 100</td>
</tr>
<tr>
<td>1</td>
<td>90 to 99%</td>
<td>$10^{-2}$ to $&lt;10^{-1}$</td>
<td>100 to 10</td>
</tr>
</tbody>
</table>
Summary

- TSS design fulfills ESS and SSM conditions for level 3 defense in depth
- Based on deterministic reliability analysis, to handle CCF, TSS shall implement diversity in some components, qualification of the components, separation and periodic proof tests
- The probability of failure of the TSS design is in the SIL3 range