TSS System Requirements Specification

	Name	Role/Title
Owner	Mikael Olsson	Control Engineer, Target Controls and Safety, Target Division
Reviewer	Thomas Hansson	Senior Radiation Safety Engineer, ES&H Division
	Ulf Odén	Work Package Manager, Target Systems, Target Division
	Sara Ghatnekar Nilsson	Work Package Manager, Monolith Systems, Target Division
	Linda Coney	Group Leader, Target Controls and Safety, Target Division
Approver	Mark Anthony	Division Head, Target Division

TABLE OF CONTENT **PAGE**

1. SCOPE 3
1.1. Objective 3
1.2. Purpose 3
1.3. Context 4
2. ISSUING ORGANISATION 4
3. REQUIREMENTS 5
3.1. Definitions 5
3.2. Functional Requirements 5
3.3. Constraint Requirements 8
3.4. Environmental Requirements 12
3.5. Conventional Safety Requirements 12
3.6. Radiation Safety Requirements (SSM conditions) 12
3.7. Interface Requirements 17
4. GLOSSARY 18
5. REFERENCES 19
DOCUMENT REVISION HISTORY 20

1. SCOPE

The scope of this document is Target Safety System (TSS) system requirements.

To get a more general overview and overall understanding of TSS, please refer to ESS-0037596 [1].

This document is written to accommodate IEC 61511-1 [28] and relates to lifecycle phase 3, see Figure 1 below.

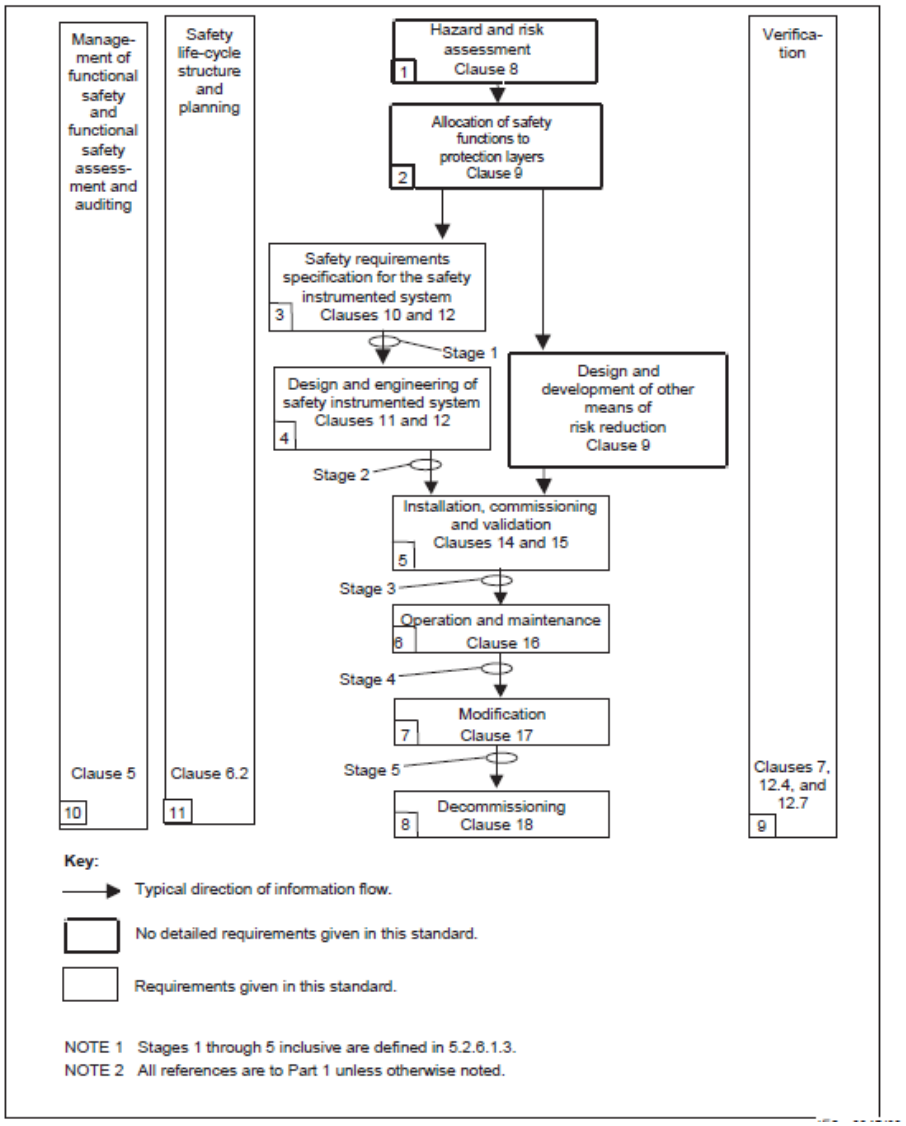

Figure 1 Overall safety life cycle of IEC 61511-1

1.1. Objective

The objective of this document is to define the system requirements for TSS.

1.2. Purpose

The purpose of this document is to define all system requirements for TSS.

The document will be used for:

- Design of TSS
- Test and verification of TSS
- Quality assurance of TSS

1.3. Context

The context of the TSS system requirements is described in Figure 2.

Radiation safety functions are derived from the accidents analyses of Target Station systems and areas. A set of these safety functions are allocated to the TSS and are further detailed in this document. The classification of the TSS safety functions provides constraints on design and quality.

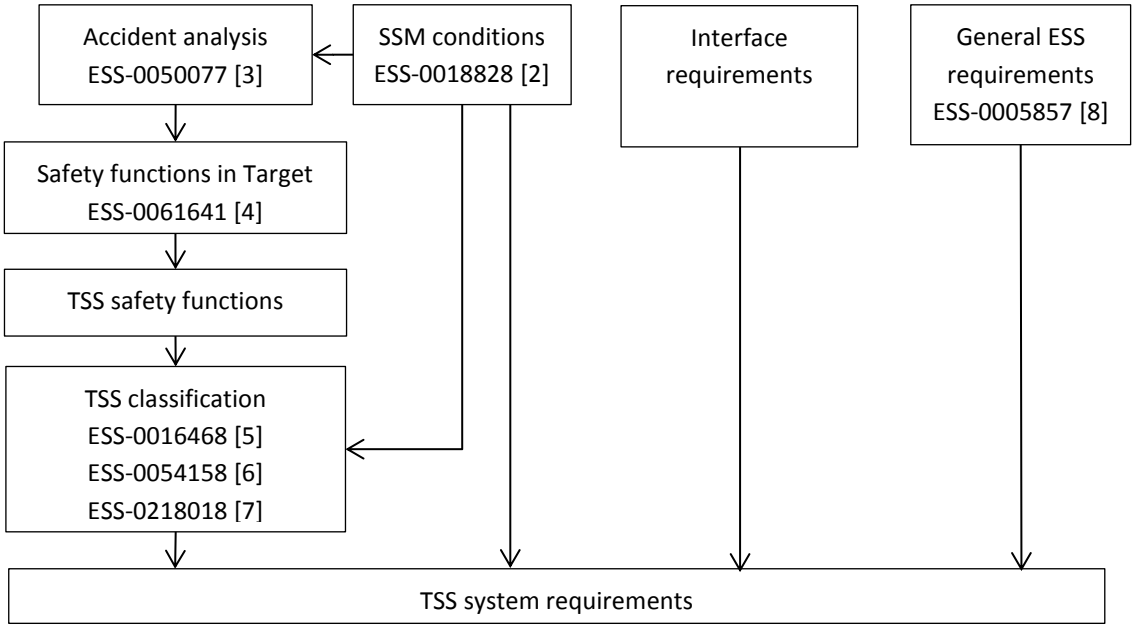

Figure 2 TSS requirements context

2. ISSUING ORGANISATION

This document is issued by Target control (WP7) within the Target Division.

3. REQUIREMENTS

3.1. Definitions

The following requirements are definitions to be used in later sections. The requirements are directly linked to SSM conditions.

Table 1 TSS definition requirements

Id	Definition	Trace up to
TSS-TSS-001	TSS safe state The safe state provided by TSS, 'TSS safe state', is defined as beam prevented from reaching target and with no possibility to spuriously reach target. *Note: the general ESS facility safe state may have a wider definition, see for example chapter 9 in [13].* Rationale Under normal conditions, the proton beam is the energy source heating the tungsten and leading to oxidisation or melting and release of radioactive material.	SSM-ch4-C6

3.2. Functional Requirements

Table 2 TSS functional requirements

Id	Function	Trace up to
TSS-TSS-101	Function for He cooling outlet mass flow TSS shall achieve and maintain the TSS safe state if the target He cooling outlet mass flow is below a critical limit (trip limit). • Trip limit: according to ESS-0287373 [12] • Trip time: according to ESS-0287373 [12] • Classification: according to ESS-0218018 [7] Rationale Function: accident AA3 in ESS-0051595 [11]	RSF-72 in ESS-0061641 [4] SSM-ch4-C8
TSS-TSS-102	Function for He cooling outlet pressure TSS shall achieve and maintain the TSS safe state if the target He outlet pressure is below a critical limit (trip limit) • Trip limit: according to ESS-0287373 [12] • Trip time: according to ESS-0287373 [12] • Classification: according to ESS-0218018 [7] Rationale Function: accident AA3 in ESS-0051595 [11]	RSF-69 in ESS-0061641 [4] SSM-ch4-C8

Id	Function	Trace up to
TSS-TSS-103	Function for He cooling inlet temperature TSS shall achieve and maintain the TSS safe state if the target He inlet temperature is above a critical limit (trip limit) • Trip limit: according to ESS-0287373 [12] • Trip time: according to ESS-0287373 [12] • Classification: according to ESS-0218018 [7] Rationale Function: accident AA3 in ESS-0051595 [11]	RSF-71 in ESS-0061641 [4] SSM-ch4-C8
TSS-TSS-104	Function for target wheel rotational speed TSS shall achieve and maintain the TSS safe state if the target wheel rotational speed is below a critical limit (trip limit) • Trip limit: according to ESS-0287373 [12] • Trip time: according to ESS-0287373 [12] • Classification: according to ESS-0218018 [7] Rationale Function: accident AA1 in ESS-0050081 [9] Classification: ESS-0218018 [7]	RSF-68 in ESS-0061641 [4] SSM-ch4-C8
TSS-TSS-105	Function for monolith atmosphere pressure TSS shall achieve and maintain the TSS safe state if the monolith pressure is above a critical limit (trip limit) • Trip limit: according to ESS-0287373 [12] • Trip time: according to ESS-0287373 [12] • Classification: according to ESS-0218018 [7] Rationale Function: accident AA2 in ESS-0063901 [10]	RSF-70 in ESS-0061641 [4] SSM-ch4-C8
TSS-TSS-201	Static permit for beam production TSS shall be able to give a static permit for beam production independent of the target mode. Static permission of beam shall only be possible if there is no risk of release of radioactive material; i.e. when the TSS radiation safety functions are not needed. This implies that the produced beam shall be directed to the beam dump or other intermediate destinations closer to the ion source. • Classification: according to ESS-0218018 [7] Rationale To increase availability of the accelerator. The Accelerator Division requires beam production for maintenance purposes (test, calibration, etc.) when the target is not ready for beam (target maintenance, target start-up, etc.).	ESS-0030068 [19], ACC-TSS-001

Id	Function	Trace up to
TSS-TSS-202	Manual safety stop TSS shall allow the operator to force the system into the TSS safe state by manual action. • Classification: according to ESS-0218018 [7] Rationale To be able to set TSS in a safe state manually for potential radiation safety reasons. Note that ESS-0121507 [14], section 11.2, states "*In the event of intentional neutron production, SSM deems that the operators shall be able to manually shut down the accelerator with safety systems and safety components in defence in depth level 3."* Function covered, but not deemed necessary, by IEC 61226 [27]: "*These [Cat A] functions play a principal role in the achievement or maintenance of the non-hazardous stable state"* with a footnote stating "*For slower transients, stable conditions can be obtained using manual actions, provided such actions are considered after a grace time*".	SSM-ch4-C25 ESS-0121507 [14], section 11.2
TSS-TSS-203	Operational monitoring TSS shall provide TSS status and status history to the operator in the main control room. For example status information, alarms and archiving of data. • Classification: according to ESS-0218018 [7] Rationale To allow monitoring of TSS safety functions by the operator during normal operation. Function covered by IEC 61226 [27]: "*functions that provide continuous or intermittent tests or monitoring of functions in category A and B to indicate their continued availability for operation and alert control room staff to their failures*".	SSM-ch4-C3 SSM-ch4-C29

Id	Function	Trace up to
TSS-TSS-204	Manual operational start/stop TSS shall allow the operator to start and stop the system for normal operation. Start of the system means intentional permit of beam production (provided that TSS radiation safety functions TSS-TSS-101 – TSS-TSS-105 do not prevent it). Stop of the system means setting the system into the TSS safe state. • Classification: according to ESS-0218018 [7] Rationale To allow normal operation of TSS by the operator. It is assumed that this function is used as part of a sequence of actions defined for operation of the facility. The stop of the system is intended for, but not limited to, controlled stop of the facility and to set TSS in a maintenance mode.	SSM-ch4-C25
TSS-TSS-205	Safety monitoring TSS shall provide critical TSS status to the operator in the main control room. For example, but not necessarily, if TSS managed to reach the TSS safe state when demanded. • Classification: according to ESS-0218018 [7] Rationale To provide critical TSS status to the operator during defence in depth level 3. It may be a subset of the status monitored by TSS-TSS-203. Note that this function is not credited to be used to provide information to perform manual actions.	SSM-ch4-C3 SSM-ch4-C29

3.3. Constraint Requirements

Table 3 TSS constraint requirements

Id	Constraint	Trace up to
TSS-TSS-301	TSS safe state maintenance No active control shall be required to maintain the TSS safe state. No manual action shall be required to maintain the TSS safe state. Rationale To minimise the dependency on actions from control systems and from humans in order to maintain the safe state.	SSM-ch4-C6 SSM-ch8-D34

Id	Constraint	Trace up to
TSS-TSS-302	System maintenance It shall be possible to maintain (inspect, test, maintain, calibrate, repair, and replace) the system throughout the intended lifetime. It shall be possible to maintain the system periodically related to the ESS schedule for accelerator shutdown in ESS-0011768 [18]. Rationale To maintain high quality.	SSM-ch4-C16
TSS-TSS-303	Passive design The system shall be designed based on passive methods and technology. Rationale The system shall achieve a preferential position; i.e. TSS safe state achieved automatically in case of failure.	SSM-ch4-C22 SSM-ch4-C24
TSS-TSS-304	System access Only authorised people shall have physical and logical access to the system. Rationale To prevent unauthorised persons from changing parameters and other configurable values of the TSS radiation safety functions.	SSM-ch8-D19 SSM-ch8-D30 SSM-ch8-D31 SSM-ch8-D32
TSS-TSS-305	Availability (maximum allowable spurious trip rate) The mean-time between spurious trips (due to system internal failures) shall be more than 10000 hours. Rationale MTBF = 1/(1 – Availability) Assuming the availability of TSS shall be 99.99 % compared to ESS's overall availability of 95 %, according to ESS-0064499 [26]. *Note: Requirements for TSS availability missing.*	TS.FR.2 in ESS-0005857 [8].
TSS-TSS-306	Probability of failure on demand (PFD) The PFD for any TSS function that is classified to follow Cat A in IEC 61226 shall be $\leq 10^{-4}$. Rationale IEC 61226 [27], states for Cat A in section 7.3.2.1: "*For an individual system which is specified and designed in accordance with the highest quality criteria, a figure of the order of 10^{-4} failure/demand may be an appropriate overall limit to place on the reliability…"*	SSM-ch4-C10

Id	Constraint	Trace up to
TSS-TSS-401	Design standards and rules The following design standards and rules shall apply for the design of TSS radiation safety functions: • IEC 61226 [27], Cat A – system design • IEC 60709 [29] (or IEEE 384 [30]) – separation • IEC 61511 [28], SIL3 – software design • IEC 62443 [32] – network and system security • ESS-0015433 [15] – electrical design Rationale To obtain high quality in structures, systems, and components of importance to safety. Classification according to ESS-0218018 [7]. Network and system security according to ESS-0144417 [17].	SSM-ch4-C10 SSM-ch4-C13 SSM-ch4-C14 SSM-ch8-D19 SSM-ch8-D23 SSM-ch8-D28
TSS-TSS-402	Quality standards and rules The following standards and rules shall apply for the quality assurance of TSS radiation safety functions: • IEC 61511 [28] – system lifecycle • IEC 61511 [28], SIL3 – software quality • ESS-0118082 [16] – component qualification (Cat A functions) • ESS-0015433 [15] – system and installation test Rationale To obtain high quality in structures, systems, and components of importance to safety. Classification according to ESS-0218018 [7].	SSM-ch4-C10 SSM-ch4-C13 SSM-ch4-C14 SSM-ch4-C15
TSS-TSS-403	Redundancy The TSS design of radiation safety functions shall include a relevant level of redundancy. Rationale To maintain functionality in case of independent single failure. General design requirement for SSC Cat. 1 in ESS-0016468 [5].	SSM-ch4-C19 SSM-ch4-E10
TSS-TSS-404	Diversity The TSS design of radiation safety functions shall include a relevant level of diversity. Rationale To maintain functionality in case of independent common cause failure. General design requirement for SSC Cat. 1 in ESS-0016468 [5].	SSM-ch4-C20 SSM-ch4-C21 SSM-ch4-E11

Id	Constraint	Trace up to
TSS-TSS-405	Functional separation The TSS design of radiation safety functions shall include a relevant level of functional separation (independence). Rationale To prevent functionality in redundant parts from being knocked out by the same event or circumstance. General design requirement for SSC Cat. 1 in ESS-0016468 [5].	SSM-ch4-C7 SSM-ch4-C18 SSM-ch4-C23
TSS-TSS-406	Physical separation The TSS design of radiation safety functions shall include the relevant level of physical separation. Rationale To prevent functionality in redundant parts from being knocked out by the same event or circumstance. General design requirement for SSC Cat. 1 in ESS-0016468 [5].	SSM-ch4-C18 SSM-ch4-C23
TSS-TSS-407	Deterministic analysis A deterministic reliability evaluation of the design of TSS radiation safety functions shall be performed by an FMEA by following IEC 60812 [31]. Rationale High assurance of reliability in terms of resistance to single failure and common cause failure. Required by ESS-0054158 [6] for Cat A and Cat B SSC.	SSM-ch4-D1
TSS-TSS-408	Probabilistic analysis A probabilistic reliability evaluation of the design of TSS radiation safety functions shall be performed according to the PFD calculations in IEC 61511 [28] or similar. Rationale High assurance of reliability.	SSM-ch4-D1 SSM-ch4-E17

Id	Constraint	Trace up to
TSS-TSS-409	Environmental resistance TSS components shall consider the following environmental conditions: External events: • Earthquake up to and including H2 load (loads above H2 will be handled by a separate system if necessary) • Extreme climatic conditions (rain, lightning, etc.) • External flooding • External fire • Hazards from industrial and transport environment • Airplane crashes Internal events: • Mechanical impact (drop loads, explosion, etc.) • Internal flooding • Internal fire • Electric/magnetic fields (including surges and lightning) • Radiation level • Temperature • Humidity • Chemical • Human factors Rationale To ensure adequate reliability of TSS radiation safety functions in the environmental conditions in which they shall be able to perform. Aggressors' checklist in ESS-0016468 [5].	SSM-ch4-C14

3.4. Environmental Requirements

TSS has no impact on the environment.

3.5. Conventional Safety Requirements

TSS is an electrical and I&C system and shall follow the ESS rules for electrical design in ESS-001533 [15], as stated in TSS-TSS-301.

3.6. Radiation Safety Requirements (SSM conditions)

The following requirements are extracted from SSM conditions related to TSS. They are referenced in previous sections.

Table 4 SSM conditions related to TSS

Id	Text	Trace up to
SSM-ch4-C3	It shall be possible to monitor the facility in such a way so it is possible to ensure that the necessary safety functions are maintained.	ESS-0018828 [2], Appendix 1, chapter 4, C3
SSM-ch4-C6	The facility shall be designed so that structures, systems and components that maintain the fundamental safety functions in defence in depth levels 2, 3 and 4 respectively can take the facility to a safe state in conjunction with relevant events or circumstances.	ESS-0018828 [2], Appendix 1, chapter 4, C6
SSM-ch4-C7	[…] Structures, systems, and components of importance to safety shall, as far as reasonably possible, be independent from the structures, systems and components of importance to safety in other defence in depth levels, as follows: a. defence in depth level 4 shall be independent of defence in depth level 1-3, and b. defence in depth level 3 shall be independent of 1 and 2.	ESS-0018828 [2], Appendix 1, chapter 4, C7
SSM-ch4-C8	All structures, systems and components of importance to safety shall be classified based on their function and safety significance.	ESS-0018828 [2], Appendix 1, chapter 4, C8
SSM-ch4-C10	Structures, systems and components of importance to safety shall be designed, constructed and maintained in such a way that their quality and reliability are consistent with their importance to safety.	ESS-0018828 [2], Appendix 1, chapter 4, C10
SSM-ch4-C13	Structures, systems and components of importance to safety shall be based on proven technologies and proven methods, and be tested before use. If parts of structures, systems and components of importance to safety are based on lesser proven technologies or methods, these shall be compensated with research and increased testing of the technologies or methods.	ESS-0018828 [2], Appendix 1, chapter 4, C13

Id	Text	Trace up to
SSM-ch4-C14	Facility structures, systems and components of importance to safety shall be designed with such a high quality and reliability for the environmental conditions, loads, and other effects that may occur so that their function can be ensured during the events and circumstances in which they shall contribute to fulfilment of the fundamental safety functions. A high quality in structures, systems and components of importance to safety shall be obtained through the appropriate selection of standards, materials, manufacturing processes, installation processes and qualification processes.	ESS-0018828 [2], Appendix 1, chapter 4, C14
SSM-ch4-C15	The time during which the facility's structures, systems and components of importance to safety can be used in a safe manner shall be determined. Sufficient margins shall be in place against aging and other degradation to ensure functionality and integrity during their designed lifetime.	ESS-0018828 [2], Appendix 1, chapter 4, C15
SSM-ch4-C16	Facility structures, systems and components of importance to safety shall be designed so that sufficiently high quality can be maintained throughout the intended lifetime. It shall be possible to maintain quality shall be maintained through structures, systems and components of importance to safety being, as a minimum, inspected, tested, monitored, maintained, calibrated, repaired and replaced to the extent necessary in order to ensure proper function and maintain integrity during the facility's lifetime in a way that ensures radiation protection for employees.	ESS-0018828 [2], Appendix 1, chapter 4, C16
SSM-ch4-C18	The facility's safety groups shall be designed so that the redundant parts within each safety group have sufficient physical and functional separation to prevent the safety group's function from being knocked out directly or as a result of the same event or circumstance. Separation within the safety groups shall, to a sufficient extent, be possible to maintain at all times and in all operating conditions, and in all other circumstances expected to arise at the facility during maintenance, testing, repair or shutdown.	ESS-0018828 [2], Appendix 1, chapter 4, C18
SSM-ch4-C19	Safety groups accredited for events and circumstances in event classes H2-H4A, as well as mitigating groups, shall, as far as reasonably possible, be designed so that the fundamental safety functions can be maintained when an arbitrary independent failure occurs in a random structure, system or component, regardless of operating conditions.	ESS-0018828 [2], Appendix 1, chapter 4, C19

Id	Text	Trace up to
SSM-ch4-C20	During the design, construction and operation of the facility's fundamental safety functions, technical and administrative measures shall be taken that can minimise the impact of common cause failures as far as reasonably possible. The following diversification principles, in order of priority, shall be taken for all parts of the fundamental safety functions, as far as reasonably possible: a. Functions are performed in physically different ways. b. Functions are performed by different technologies/design solutions. c. Structures, systems or components are from different manufacturers. d. Structures, systems or components are installed on different occasions. e. Structures, systems or components are verified, validated, maintained and tested at different times and by different personnel.	ESS-0018828 [2], Appendix 1, chapter 4, C20
SSM-ch4-C21	Safety groups accredited for events and circumstances in event class H4B shall, as far as reasonably possible, be designed so that the fundamental safety functions can be maintained when an arbitrary independent common cause failure occurs in two or more safety structures, safety systems or safety components, regardless of operating conditions.	ESS-0018828 [2], Appendix 1, chapter 4, C21
SSM-ch4-C22	In the event of a failure in structures, systems and components of importance to safety, an acceptable and preferential position for facility safety shall be adopted for these, as far as this is reasonably possible.	ESS-0018828 [2], Appendix 1, chapter 4, C22
SSM-ch4-C23	The design of the facility shall ensure that structures, systems and components belonging to a higher safety class are protected against the effects of possible failures of the structures, systems and components belonging to a lower safety class.	ESS-0018828 [2], Appendix 1, chapter 4, C23
SSM-ch4-C24	The function of the facility's safety and mitigating groups shall be passive or designed so that the necessary activation and operational change of these occur automatically, as far as is reasonably possible.	ESS-0018828 [2], Appendix 1, chapter 4, C24
SSM-ch4-C25	The design shall allow that manual activation and operational change of a safety or mitigating group can occur if personnel are given sufficient time – respite – to implement the measures in a safe manner.	ESS-0018828 [2], Appendix 1, chapter 4, C25

Id	Text	Trace up to
SSM-ch4-C29	A control room shall be found at the facility so that the fundamental safety functions and the protection of the same can be monitored and governed during all events and circumstances.	ESS-0018828 [2], Appendix 1, chapter 4, C29
SSM-ch4-D1	Deterministic and probabilistic methods shall be used to analyse and evaluate the facility's defence in depth, with the associated barriers, and the facility's ability to fulfil the fundamental safety functions. The analyses shall be facility-specific and include all radiation sources in the facility.	ESS-0018828 [2], Appendix 1, chapter 4, D1
SSM-ch4-E10	In the analysis of events and circumstances in event classes anticipated events, unanticipated events, and improbable events (H2- H4A) the most adverse single failure shall be applied in the safety group. A single failure in active structures, systems and components shall be applied at the most adverse time. A single failure in passive structures, systems and components shall be applied at the most adverse time, but no earlier than 12 hours after the event and circumstance occurred. Furthermore, unavailability due to preventive maintenance during operations shall be presumed if it is permitted in the facility's operational limits and conditions. To demonstrate independence between defence in depth levels 2 and 3, events and circumstances in event class anticipated events (H2) shall either harness only safety-related structures, systems and components in operating groups to protect the barriers, or only structures, systems and components in safety groups to limit the consequences of the event.	ESS-0018828 [2], Appendix 1, chapter 4, E10
SSM-ch4-E11	Within the event class events with multiple failures (H4B) common cause failures in a safety group shall be applied instead of a single failure, in the same way as in condition E10. In the analysis of the event class events with multiple failures, realistic methods and input data may be used without a statistical uncertainty analysis.	ESS-0018828 [2], Appendix 1, chapter 4, E11
SSM-ch4-E17	The analysis with probabilistic methods shall, as far as reasonably possible, be realistic and use the best available methods and data. When using conservative methods and data, the impact on results shall be evaluated. The analysis shall as far as reasonably possible reflect the facility's current design and operation.	ESS-0018828 [2], Appendix 1, chapter 4, E17

Id	Text	Trace up to
SSM-ch8-D19	Digital control systems shall be designed to minimise the system's vulnerability to cyber attacks or improper use.	ESS-0018828 [2], Appendix 1, chapter 8, D19
SSM-ch8-D23	Wireless networks shall not be used in digital control systems if this can affect operational safety.	ESS-0018828 [2], Appendix 1, chapter 8, D23
SSM-ch8-D28	Computers used for setting parameters shall only be used for this purpose, and may only be used in the zone where the parameterisation takes place.	ESS-0018828 [2], Appendix 1, chapter 8, D28
SSM-ch8-D30	Only authorised persons shall have physical and logical access to digital control systems. The restriction shall be made in terms of both duration and number of systems. Physical access to digital control systems shall be controlled.	ESS-0018828 [2], Appendix 1, chapter 8, D30
SSM-ch8-D31	Access to the setpoints and calibration functions by unauthorised persons shall be prevented.	ESS-0018828 [2], Appendix 1, chapter 8, D31
SSM-ch8-D32	Unauthorised persons shall not have access to the adjustment options of parameters and other configurable values in digital control systems.	ESS-0018828 [2], Appendix 1, chapter 8, D32
SSM-ch8-D34	Digital control systems shall be designed so that dependency on human action to maintain a safe state of the system is minimised.	ESS-0018828 [2], Appendix 1, chapter 8, D34

3.7. Interface Requirements

The requirements to or from external systems are defined in separate ICD-Rs, see Table 5.

Table 5 TSS interface requirements

Interface requirements
TSS – Accelerator, see ESS-0030068 [19]
TSS – Site Infrastructure, see ESS-0030063 [20]
TSS – ICS, see ESS-0249257 [21]

Interface requirements
TSS – Target Helium cooling, see ESS-0016380 [22]
TSS – Target wheel, drive and shaft, see ESS-0022915 [23]
TSS – Target monolith systems, see ESS-0032009 [24]
TSS – Target electrical, see ESS-0198545 [25]

4. GLOSSARY

Term	Definition
ACC	Accelerator
ICD	Interface Control Document
ICD-R	Referenced Interface Control Document
ICS	Integrated Control System
SIL	Safety Integrity Level
SSC	Structures, Systems and Components
SSM	Svenska Strålskyddsmyndigheten (Swedish Radiation Safety Authority)
TSS	Target Safety System

5. REFERENCES

[1] ESS-0037596, TSS concept specification
[2] ESS-0018828, Official permit from SSM (the Swedish Radiation Safety
[3] ESS-0050077, An overview of Target Station Radiological Hazard Analysis documentation
[4] ESS-0061641, Safety functions and DID in Target Building D02
[5] ESS-0016468, ESS rule for identification and classification of safety important components
[6] ESS-0054158, ESS rules for radiation safety classification of Electrical and Instrumentation & control equipment including design and quality requirements
[7] ESS-0218018, TSS classification
[8] ESS-0005857, Target Station System Requirement Document: Target Station, Rev 2
[9] ESS-0050081, AA1 – Accident analysis report: Target Wheel rotation stop during beam on Target
[10] ESS-0063901, AA2 – Accident analysis report: Proton beam events on Target and Proton Beam Window
[11] ESS-0051595, AA3 – Accident analysis report: Loss of target wheel cooling during beam on target
[12] ESS-0287373, TSS trip parameters
[13] ESS-0000002, Preliminary Safety Report (PSAR)
[14] ESS-0121507, SSM Permit for Installation Appendix 1 Review Report (English)
[15] ESS-0015433, ESS rules for electrical design
[16] ESS-0118082, ESS rules for qualification of Electrical and Instrumentation & control equipment
[17] ESS-0144417, ESS Response to SSM Conditions on Digital instrumentation and control systems with significant influence on radiation safety
[18] ESS-0011768, Updated Report on Operations
[19] ESS-0030068, ICD-R TSS - Accelerator
[20] ESS-0030063, ICD-R TSS – Site infrastructure
[21] ESS-0249257, TSS Monitoring System – System requirements
[22] ESS-0016380, ICD-R 1010 (Target helium cooling system) - TSS
[23] ESS-0022915, ICD-R Target wheel, drive and shaft - TSS
[24] ESS-0032009, ICD-R TSS – Covers, penetrations and monolith vessel
[25] ESS-0198545, ICD-R Target electrical - TSS
[26] ESS-0064499, ESS Neutron Source Reliability and Availability Requirements
[27] IEC 61226:2009, Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions
[28] IEC 61511:2003 + corrigendum 2004, Functional safety – Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements
[29] IEC 60709:2004, Nuclear power plants - Instrumentation and control systems important to safety – Separation
[30] IEEE 384, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits
[31] IEC 60812:2006, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)
[32] IEC 62443, Network and system security for industrial-process measurement and control

DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	Approved as baseline before PDR	Mikael Olsson	2016-02-08
2	Approved for PSAR	Mikael Olsson	2016-03-24
3	Approved for updated PSAR	Mikael Olsson	2017-02-20
4	Approved for updated PSAR. Added design and quality conditions related to electrical and I&C classification. Removed design specific requirements. More aligned to ESS requirement template. Requirements IDs updated/changed.	Mikael Olsson	2018-03-23
5	Treat TSS trip parameters in reference ESS-0287373 Treat TSS classification in reference ESS-0218018 Treat interface to ICS in reference ESS-0249257 Changed title of TSS-TSS-202 and 204 Clarified TSS-TSS-202, 203 and 204. Added TSS-TSS-205, TSS-TSS-306 and SSM-ch4-C29	Mikael Olsson	2018-12-05