Document Type	Report
Document Number	ESS-0052608
Date	Apr 2, 2019
Revision	1 (32)
State	Review
Confidentiality Level	Internal
Page	1 (13)

TSS Probabilistic Safety Assessment

	Name	Role/Title
Owner	Atefeh Sadeghzadeh	Control engineer, Target Control
Reviewer	Ola Ingemansson Mikael Olsson	Instrument engineer, Target Control Control engineer, Target Control
Approver	Linda Coney	Group Leader, Target Control

TABLE OF CONTENT PAGE

1. SCOPE

This document describes the probabilistic safety assessment of the Target Safety System (TSS) and fulfils TSS requirements, TSS-TSS-001, TSS-TSS-002, TSS-TSS-003, TSS-TSS-004, TSS-TSS-005, TSS-TSS-202 and TSS-TSS-408 see [7]. TSS requirement for the probabilistic assessment, TSS-TSS-408, is based on SSM condition, see [11] ch4-D1 and ch4-E17.

2. CONTRIBUTORS

N/A

3. ISSUING ORGANISATION

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

4. INTRODUCTION

The objective of this work is to verify that safety instrumented functions that are identified for the TSS [7], will meet the corresponding probabilistic reliability. The hardware reliability analysis methodology of this study is in accordance with IEC 61511– Part 1[3], and reliability block diagram approach was selected based on IEC 61508-6:2010, annex B[1]. IEC 61508 formula and the simplified version of it, based on [2], was considered in calculation see Appendix [12]. Results obtained from both method ([1] and [2]) are very similar and comparable.
Based on [7], because the design of TSS is based on [10], the acceptable level of probabilistic reliability of 10^{-4} which is equal to the probabilistic failure rate goal for SIL3 system as described in [3] is considered as goal for verification of probabilistic safety assessment.

5. ASSUMPTIONS

The following assumptions were made in order to do the analysis:

- The period of test (T1) considered to be 1 year or 8760 hours
- TSS train 1 is based on safety PLC
- TSS train 2 is based on relays
- Source of the reliability data is datasheet or the manufacture
- Sensors considered to be redundant (equal with same PFDs)
- Common-cause failure rate (β) considered to be 20% [1].
- The diagnostic coverage (DC) was considered conservatively 0%.

6. RELIABILITY ANALYSIS

6.1. Definition

In [1], **Safety integrity level** (**SIL**) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function (SIF). It is expressed in terms of either:

- the probability of failure on demand (PFD), where the function operates in "low demand mode" [1] or "demand mode" [3]
- the probability of failure per hour (PFH), where the function operates in "high demand mode" or "continuous mode" [1] or only "continuous mode" [3]

Definition of the modes are presented in [1] section 3.5.16 and IEC 61511-1 [3] sections 3.2.43.1 and 3.2.43.2.

Based on these definitions, the mode of operation for each of the TSS SIF's will be "low demand mode" [1] or "demand mode" [3]. The reasons are:

1. TSS acts with a specified action in response to process conditions, to transfer the process into a safe state
2. TSS does not act as part of the normal operation
3. Both TSS and the process must fail to have a hazard
4. TSS is demanded for H2 (10^{-2}) or less probability

According to [7] the PFD for each radiation safety function shall be 10^{-4} or less. There is no further requirement for a specific SIL level related to system probabilistic reliability.

6.2. PFD determination

The PFD of a system, (in short: PFD_{Sys}) is determined by the calculation and summation of the PFD values of the sensor, logic and actuator (final element) subsystems according to IEC 61508 – 6 [1] section B.3.2.1:

$$PFD_{Sys} = PFD_S + PFD_L + PFD_{FE}$$

The procedure explained in [1] and [2] was used to determine PFD_{Sys}.

6.2.1. IEC 61508 formula:

Following Table 1 shows formulas for calculation of PFD. As mentioned before, the diagnostic coverage is conservatively considered 0%. As [1], IEC61508-6, table B.1, MRT (Mean repair time) is considered 8 hours.

Table 1: PFD formula based on [1]

$\lambda_D = \lambda_{DU} + \lambda_{DD}$
$\lambda_{DU} = \lambda_D(1 - DC)\,;\lambda_{DD} = \lambda_D DC$
$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
$PFD_{1oo1} = 1 - e^{\lambda_D t_{CE}} \approx \lambda_D t_{CE}$

$PFD_{1oo2} = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$
$PFD_{2oo3} = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$
$MRT = 8\ hours\ ; DC = 0\%$

β is the fraction of undetected failures that have a common cause (expressed as a fraction in the equations and, as a percentage elsewhere) [1] and defines the number of undetected faults with a common cause (CCF), that will influence all channels at the same time in a redundant system. A method for evaluating of β is described in IEC 61508-6, Annex D. In practical use the value of β is normally in the range 1% to 10% [1].
The susceptibility of the subsystem to common cause failures is important to consider when the subsystem is realized by using subsystem elements. In this case, it is important to estimate the contribution of common cause failure (CCF) by calculating the β-factor. In our calculation, β-factor considered to be 20%. It means in 20% of the faults of components of the same function, all of them will fail.

6.2.2. Proximity formula

In another trial, to calculate the PFDs, the following formula that is retrieved from VDI/VDE 2180 [2] is used.
Table 2 shows formula for some of the most common MooN (M out of N).

$$PFD_{MooN} \approx \frac{N!}{(M-1)!\,(N-M+2)!}\lambda_{DU}^{N-M+1}T_1^{N-M+1} + \beta.\frac{1}{2}\lambda_{DU}.T_1$$

Table 2 proximity PFD

$PFD_{1oo2} \approx \frac{4}{3}.PFD_{1oo1}^2 + \beta.PFD_{1oo1}$
$PFD_{1oo3} \approx 2.PFD_{1oo1}^3 + \beta.PFD_{1oo1}$
$PFD_{2oo2} \approx 2.PFD_{1oo1}^2$
$PFD_{2oo3} \approx 4.PFD_{1oo1}^2 + \beta.PFD_{1oo1}$

7. RELIABILITY CALCULATION FOR EACH SAFETY FUNCTION

Table 3 shows the reliability data of the common components for all safety functions which were used for the reliability calculation.

Table 3 PFD used for preliminary analysis

component	PFD	λ_D	source of data	B10d*	Model
DI module	4,38E-06 (calculated from λ_D)	1,00E-09	Siemens		Siemens 1500 series
PLC	4,38E-06 (calculated from λ_D)	1,00E-09	Siemens		Siemens 1500 series
DO module	4,38E-06 (calculated from λ_D)	1,00E-09	Siemens		Siemens 1500 series
Switch disconnector for RFQ	2E-04	4,56E-08	Manufacturer	25000	ABB 1SDA068208R1
Relay	2e-5	4,56E-09	Manufacturer	250000	Schneider CA4KN40BW3
Fiber communication	1,18E-02	2,70E-06	Manufacturer (MTBF)		EES receiver module 97BLBGCN1BX1
					EES sender module 97BLBGAN1BB1
Stop relay	7,45E-04	4,56E-09	Schneider	250000	Schneider CA4KN40BW3
contactor for Ion source	6.67e-6	1.52E-9	ABB	750000	ABB 1SBL387001R1100
* for some of the components PFD are calculated from the data sheet information. For example, the supplier candidate for the switch disconnector can give us B10d value. B10d is a measure of time where 10% of a population of devices should have failed. Generally, it is a measure of expected end of life or "useful life" as defined by the reliability engineering community. It is mentioned in IEC/ISO 13849-1 functional safety. However, some believe that B10d should never be used for calculation of PFD [13].					

Following sections includes the reliability calculation for different TSS safety functions.

7.1. TSS-TSS-101—Function for HE cooling mass flow

For this function, TSS has two sensor candidates. Both claims they can reach the SIL2 reliability. For the analysis, we considered lowest SIL2 PFD equal to 0.01.

A signal conditioner after the sensor/transmitter unit adjusts the output to fit the PLC/relay.

Table 5, shows the reliability calculation for this safety function considering 20% of CCF. It means in 20% of the cases equal components fail at the same time. This number is very highly conservative.

Table 4 reliability data for mas flow sensor sub-system

component	PFD	λ_D	source of data	model
Sensor and transmitter package	0.01	1,00E-06	Datasheet (SIL2)	Yokogawa EJX910A
				Rosemount 3051SMV3M12A3R2E12A1BB4L4Q4

Signal conditioner	**0.01**	**1,00E-06**	**Datasheet (SIL2)**	**Peperl+Fuchs KFD2-CRG2-1.D**

Table 5 probability of failure for TSS-TSS-101

	Sensors part	Logic		Final elements		System		
Beta	**PFD_s**	**PFD_{L_PLC}**	**PFD_{L_relay}**	**PFD_{FE_PLC}**	**$PFD_{FE\text{-}relay}$**	**PFD_{Sys_PLC}**	**PFD_{Sys_relay}**	**PFD_{Sys}**
20% (based on [1])	4.51e-3	6.14e-6	7.51e-5	1.78e-9	4e-6	4.52e-3	4.59e-3	2.77e-5
20% (based on [2])	4.8e-3	6.13e-6	7.49e-5	1.78e-9	4e-6	4.81e-3	4.88e-3	3.13e-5

7.2. TSS-TSS-102 —Function for HE cooling outlet pressure

For this function, a mechanical switch, measures the process condition. Both candidates claim SIL2 certified. The lowest SIL2 PFD range is considered for analysis.

Table 6 reliability data for He pressure sensor sub-system

component	PFD	λ_D	source of data	model
Switch	0.01	1,00E-06	Datasheet (SIL2)	BETA C2-P508H-S2B-B1-N2
				Ashcroft B7=61=S<=IP=06=FS=MD=CD2=C4

Table 7 probability of failure for TSS-TSS-102

	Sensors part	Logic		Final elements		System		
Beta	**PFD_s**	**PFD_{L_PLC}**	**PFD_{L_relay}**	**PFD_{FE_PLC}**	**$PFD_{FE\text{-}relay}$**	**PFD_{Sys_PLC}**	**PFD_{Sys_relay}**	**PFD_{Sys}**
20% (based on [1])	2.26e-3	6.14e-6	7.51e-5	1.78e-9	4e-6	2.26e-3	2.34e-3	7.05e-6
20% (based on [2])	2.4e-3	6.13e-6	7.49e-5	1.78e-9	4e-6	2.41e-3	2.48e-3	7.95e-6

7.3. TSS-TSS-103—Function for HE cooling inlet temperature

An analogue pt100 measures the process condition and it is connected to the rest of the loop with a signal converter.

Table 8 reliability data for He temperature sensor sub-system

component	PFD	λ_D	source of data	model
Sensor	0.01	1,00E-06	Datasheet (SIL2)	Pt-100 sensor by Pentronic
				Pt-100 sensor by INOR
Signal conditioner	0.01	1,00E-06	Datasheet (SIL2)	Peperl+Fuchs KFD2-GUT-1.D

Table 9 probability of failure for TSS-TSS-103

	Sensors part	Logic		Final elements		System		
Beta	PFDs	PFD$_{L\_PLC}$	PFD$_{L\_relay}$	PFD$_{FE\_PLC}$	PFD$_{FE\text{-}relay}$	PFD$_{Sys\_PLC}$	PFD$_{Sys\_relay}$	PFD$_{Sys}$
20% (based on [1])	4.51e-3	6.14e-6	7.51e-5	1.78e-9	4e-6	4.52e-3	4.59e-3	2.77e-5
20% (based on [2])	4.8e-3	6.13e-6	7.49e-5	1.78e-9	4e-6	4.81e-3	4.88e-3	3.13e-5

7.4. TSS-TSS-104—Function for Target wheel rotational speed

This TSS function is the most un-known regarding sensor reliability data.

Note: Calculation of this function's reliability is based on assumptions and shall be done again when the sensor's data is available.

Table 10 reliability data for rotation sensor sub-system

component	PFD	λ_D	source of data	model
Sensor and transmitter package	0.01	1,00E-06	Datasheet (SIL2)	Inductive sensor by Emerson PR6423/003-0D1
Signal conditioner	0.01	1,00E-06	Datasheet (SIL2)	

Table 11: probability of failure for TSS-TSS-104

	Sensors part	Logic		Final elements		System		
Beta	PFDs	PFD$_{L\_PLC}$	PFD$_{L\_relay}$	PFD$_{FE\_PLC}$	PFD$_{FE\text{-}relay}$	PFD$_{Sys\_PLC}$	PFD$_{Sys\_relay}$	PFD$_{Sys}$
20% (based on [1])	4.51e-3	6.14e-6	7.51e-5	1.78e-9	4e-6	4.52e-3	4.59e-3	2.77e-5

	Sensors part	**Logic**		**Final elements**		**System**		
Beta	**PFDs**	**PFD$_{L\_PLC}$**	**PFD$_{L\_relay}$**	**PFD$_{FE\_PLC}$**	**PFD$_{FE-relay}$**	**PFD$_{Sys\_PLC}$**	**PFD$_{Sys\_relay}$**	**PFD$_{Sys}$**
20% (based on [2])	4.8e-3	6.13e-6	7.49e-5	1.78e-9	4e-6	4.81e-3	4.88e-3	3.13e-5

7.5. TSS-TSS-105—Function for Monolith pressure

For this function, a mechanical switch, measures the process condition. Both candidates claim SIL2 certified. The lowest SIL2 PFD range is considered for analysis.

Table 12 reliability data for monolith pressure sensor sub-system

component	PFD	λ_D	source of data	model
Switch	0.01	1,00E-06	Datasheet (SIL2)	Barksdale D2T-M18SS BETA C2-V506H-S2B-B1-N2

Table 13: probability of failure for TSS-TSS-105

	Sensors part	**Logic**		**Final elements**		**System**		
Beta	**PFDs**	**PFD$_{L\_PLC}$**	**PFD$_{L\_relay}$**	**PFD$_{FE\_PLC}$**	**PFD$_{FE-relay}$**	**PFD$_{Sys\_PLC}$**	**PFD$_{Sys\_relay}$**	**PFD$_{Sys}$**
20% (based on [1])	2.26e-3	6.14e-6	7.51e-5	1.78e-9	4e-6	2.26e-3	2.34e-3	7.05e-6
20% (based on [2])	2.4e-3	6.13e-6	7.49e-5	1.78e-9	4e-6	2.41e-3	2.48e-3	7.95e-6

7.6. TSS-TSS-202—Manual Safety Stop

For this function, a spring return pushbutton from Harmony is used to stop the beam which is connected to both PLC and Relay. However, in this case there is no voting so less relays are affected.

Table 14 reliability data for manual safety stop button

component	PFD	B10d	source of data	model
Pushbuttons	2.19e-3	1,00E07	Manufacturer	XB4BA42

Table 15 probability of failure for TSS-TSS-202

	Sensors part	**Logic**		**Final elements**		**System**		
Beta	**PFDs**	**PFD**$_{L\_PLC}$	**PFD**$_{L\_relay}$	**PFD**$_{FE\_PLC}$	**PFD**$_{FE\text{-}relay}$	**PFD**$_{Sys\_PLC}$	**PFD**$_{Sys\_relay}$	**PFD**$_{Sys}$
20% (based on [1])	2.19e-3	6.14e-6	1.87e-4	1.78e-9	4e-6	2.20e-3	2.38e-3	6.98e-6
20% (based on [2])	2.19e-3	6.13e-6	1.9e-4	1.78e-9	4e-6	2.2e-3	2.38e-3	6.98e-6

8. CONCLUSIONS AND RECOMMENDATIONS

We show in the probabilistic reliability analysis that the target PFD (e-4) is achievable having redundancy for sensor and actuator subsystems. The TSS design is based on redundant but similar sensors for one safety function and using diverse actuators for removing power from ion source and RFQ.
Diverse trains of PLC and Relay highly improves the reliability because the common cause factor is zero between the trains.
A strong point for TSS which is used for the deterministic analysis [9] is that all accidents are detected using at least two different safety functions. Since the two safety functions are having diversity over sensors, the probability of failure will be even lower to e-9.

9. GLOSSARY

Term	Definition
TSS	Target Safety System
CPU	Central Process Unit
DI	Digital Input
DO	Digital Output
F-DI	Failsafe DI
F-DO	Failsafe DO
HFT	Hardware Fault tolerance
PFD	Probability of Failure on Demand
PLC	Programmable Logic Controller
SIL	Safety Integrity Level
SIF	Safety Instrumented Function
SIS	Safety Instrumented System

10.REFERENCES

[1] IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems

[2] VDI/VDE 2180 Safeguarding of industrial process plants by means of process control engineering Verification of the hardware safety integrity of safety instrumented systems

[3] IEC 61511-1:2016, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

[4] T-Book, reliability data of components in Nordic nuclear power plants, 7th edition

[5] ESS-0045067, TSS architecture

[6] ESS-0054158, ESS rules for radiation safety classification of Electrical and Instrumentation & control equipment including design and quality requirements

[7] ESS-0002776, TSS system requirements specification

[8] ESS-0118082, ESS Rules for qualification of electrical and instrumentation & control equipment

[9] ESS-0047128, TSS FMEA

[10] IEC 61226:2009, Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions

[11] ESS-0018828, Official permit from SSM (the Swedish Radiation Safety)

[12] ESS-0052608_Appendix

[13] http://www.exida.com/Blog/machine-safety-NEVER-Use-B10-Values-for-PFDavg-Calculations

DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	First issue	Atefeh Sadeghzadeh	2019-04-02