EUROPEAN SPALLATION SOURCE

Reliability Analysis of the ESS Target Safety System

Atefeh Sadeghzadeh

Control engineer – Target safety and control

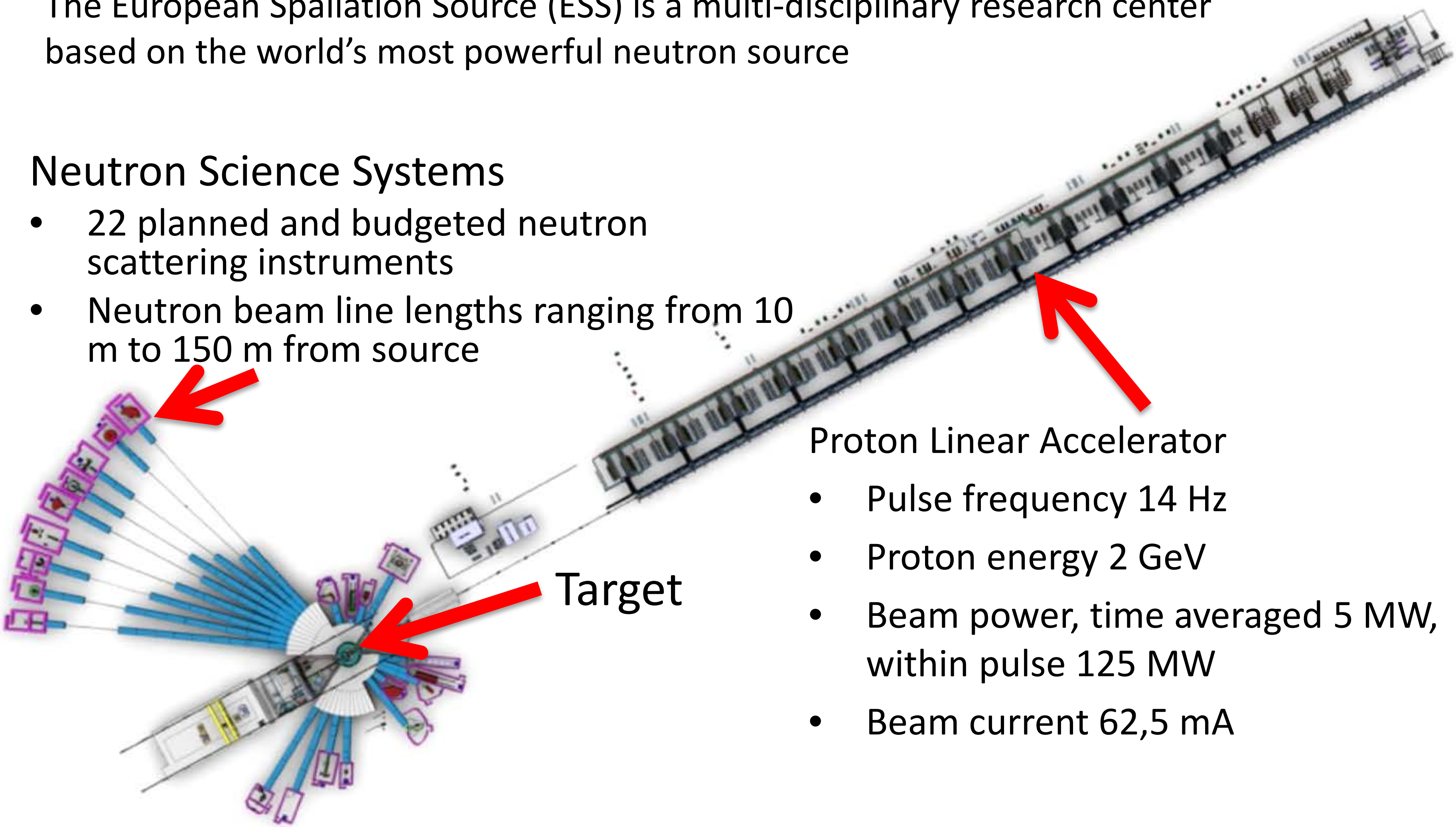
Outline

- Short introduction of ESS
- ESS target station
- What is TSS
- Deterministic reliability
- Probabilistic reliability

Model of future ESS

The ESS facility layout
Main parts

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

Target

Proton Linear Accelerator

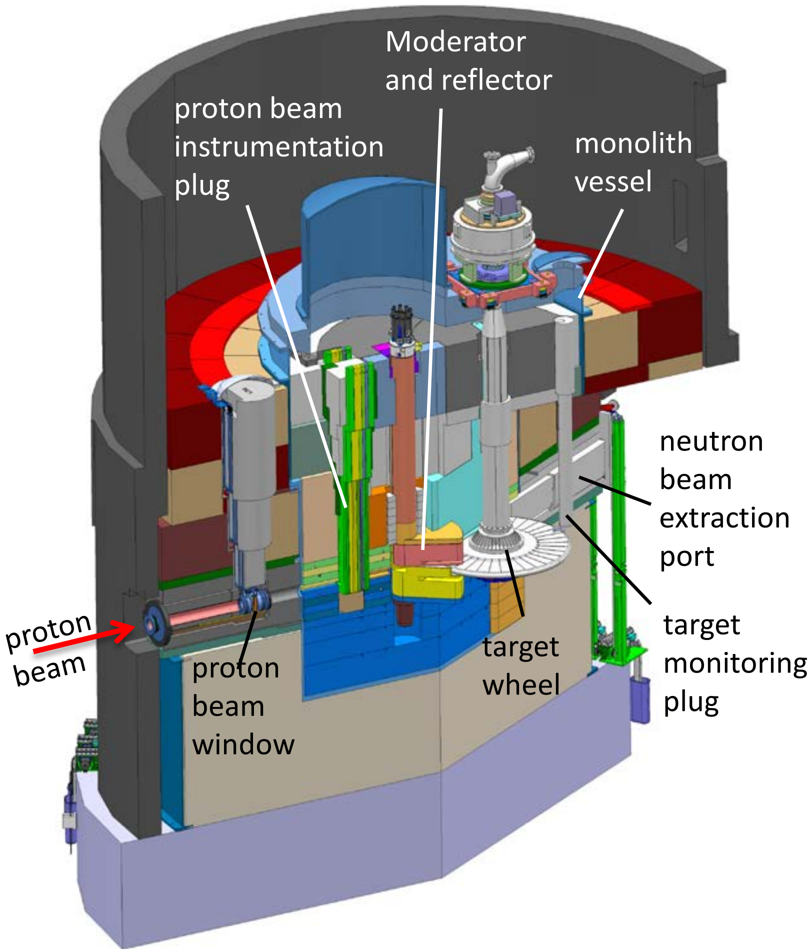
- Pulse frequency 14 Hz
- Proton energy 2 GeV
- Beam power, time averaged 5 MW, within pulse 125 MW
- Beam current 62,5 mA

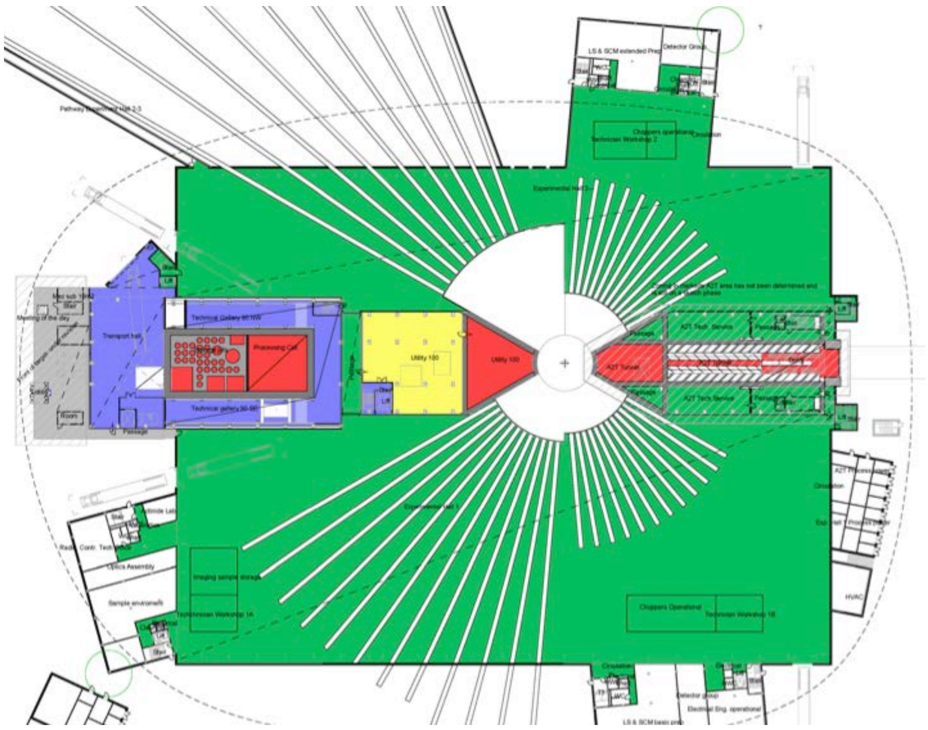
Site view - status

June 2017

Monolith area of Target – June 2017

Layout of the target station





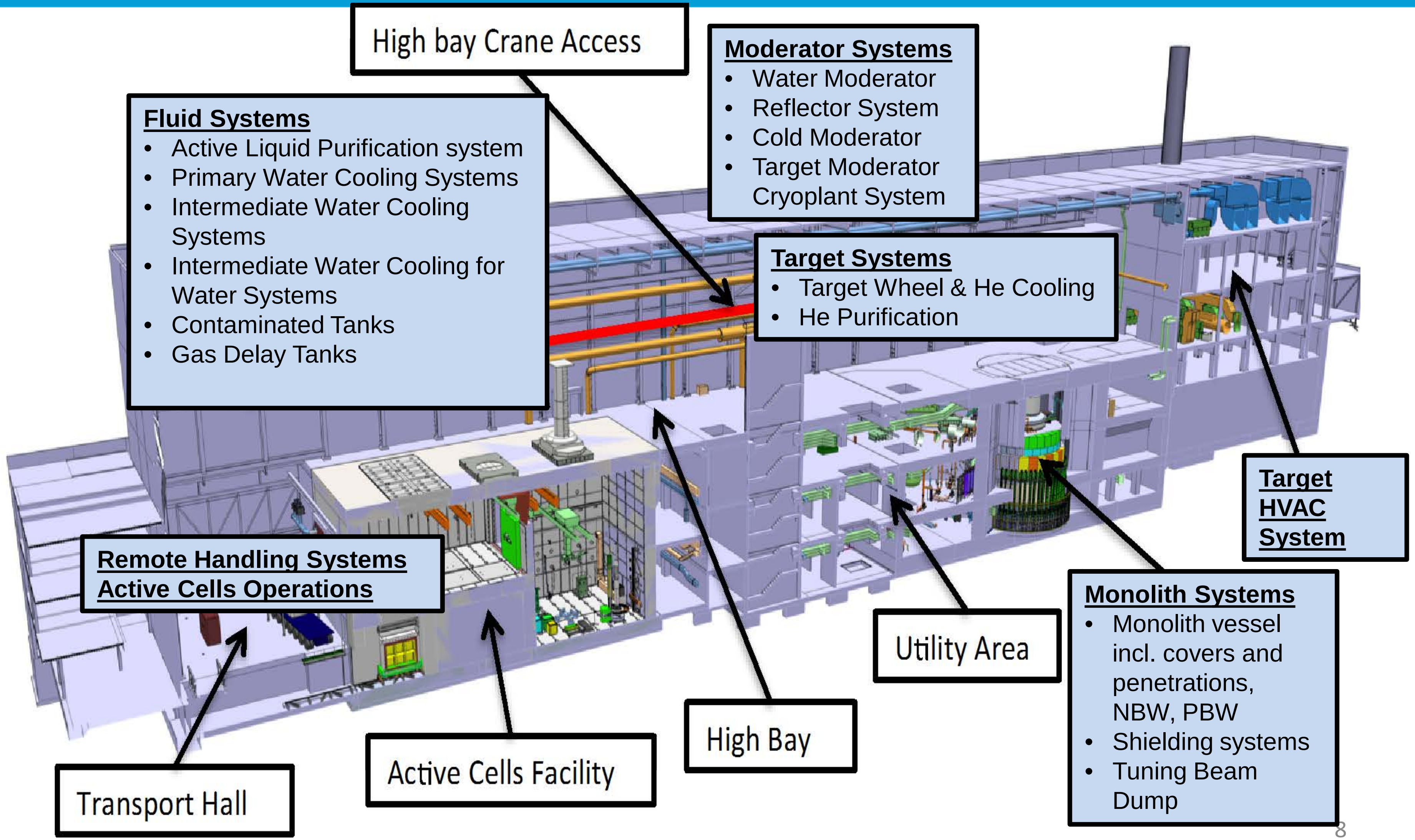
For more detail see R. Linander talk tomorrow afternoon

Purpose of Target Safety System (TSS)

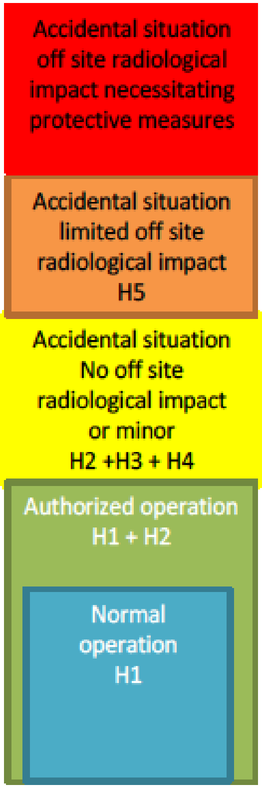
EUROPEAN SPALLATION SOURCE

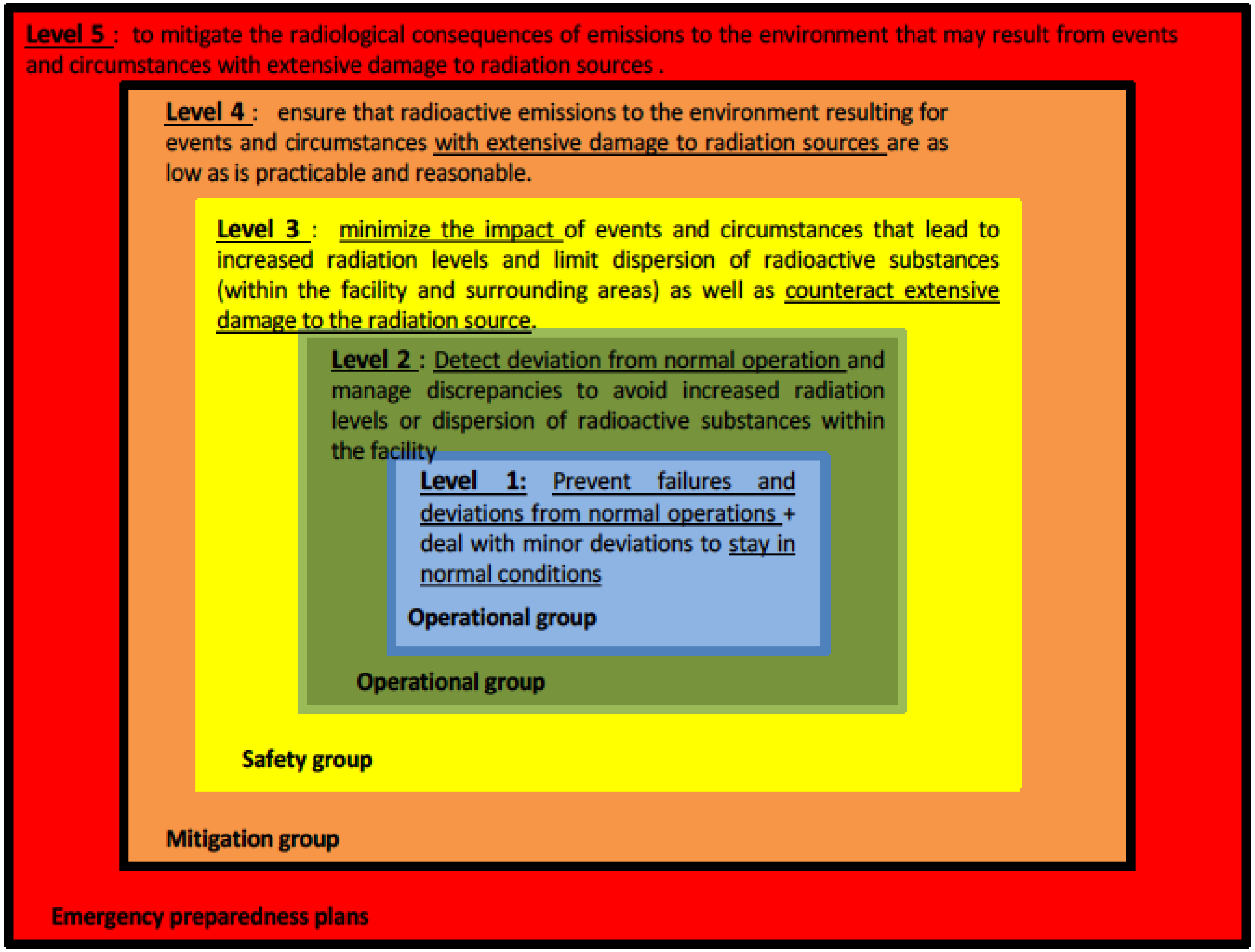
- TSS is the ESS safety interlock system that shall:
  - ”…protect the public from exposure to unsafe levels of radiation, and preventing the release of radioactive material beyond permissible limits”
  - ”…bring the spallation process into a safe state in case of an abnormal event from nuclear safety point of view…”
- TSS does not consider personell safety or machinery safety

Systems under consideration - Hazard Analysis Scope

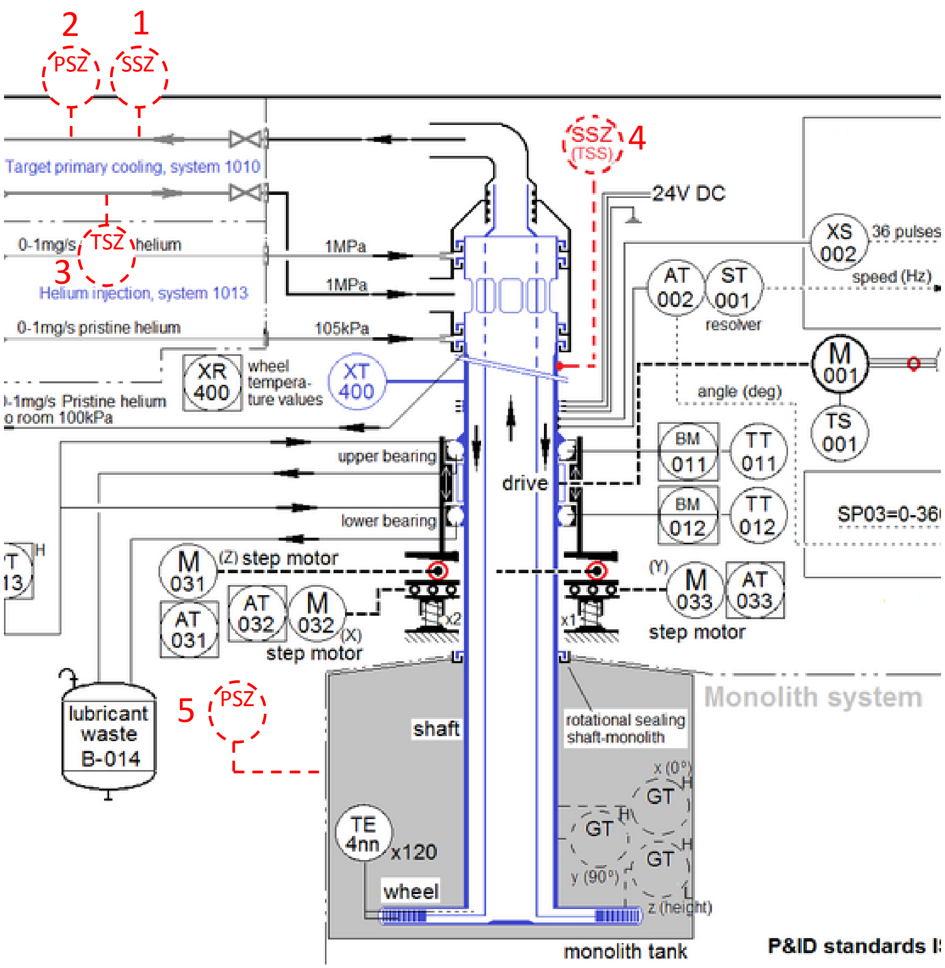


Event categories, Safety functions groups and Defence in Depth Levels





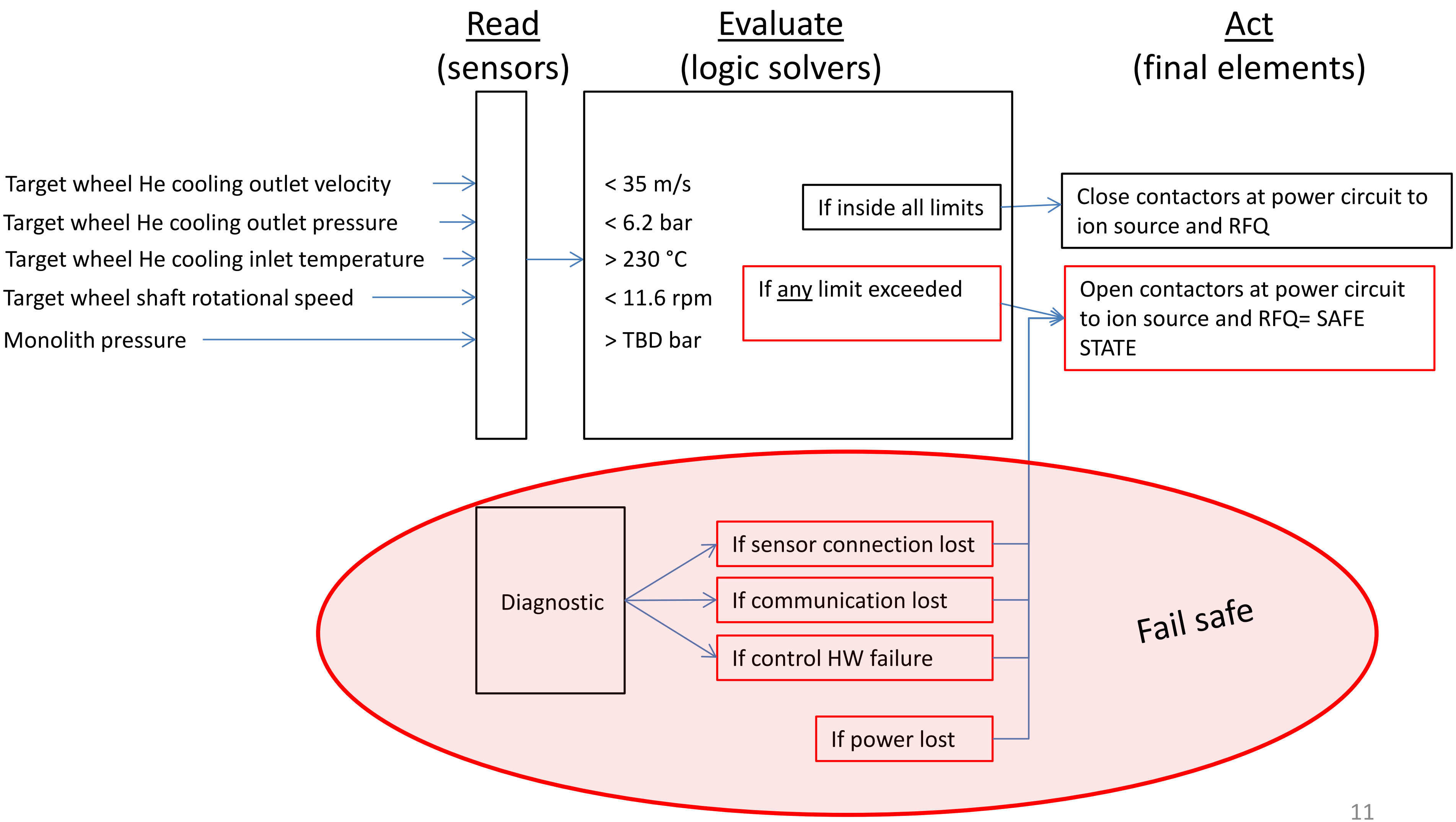
TSS safety functions



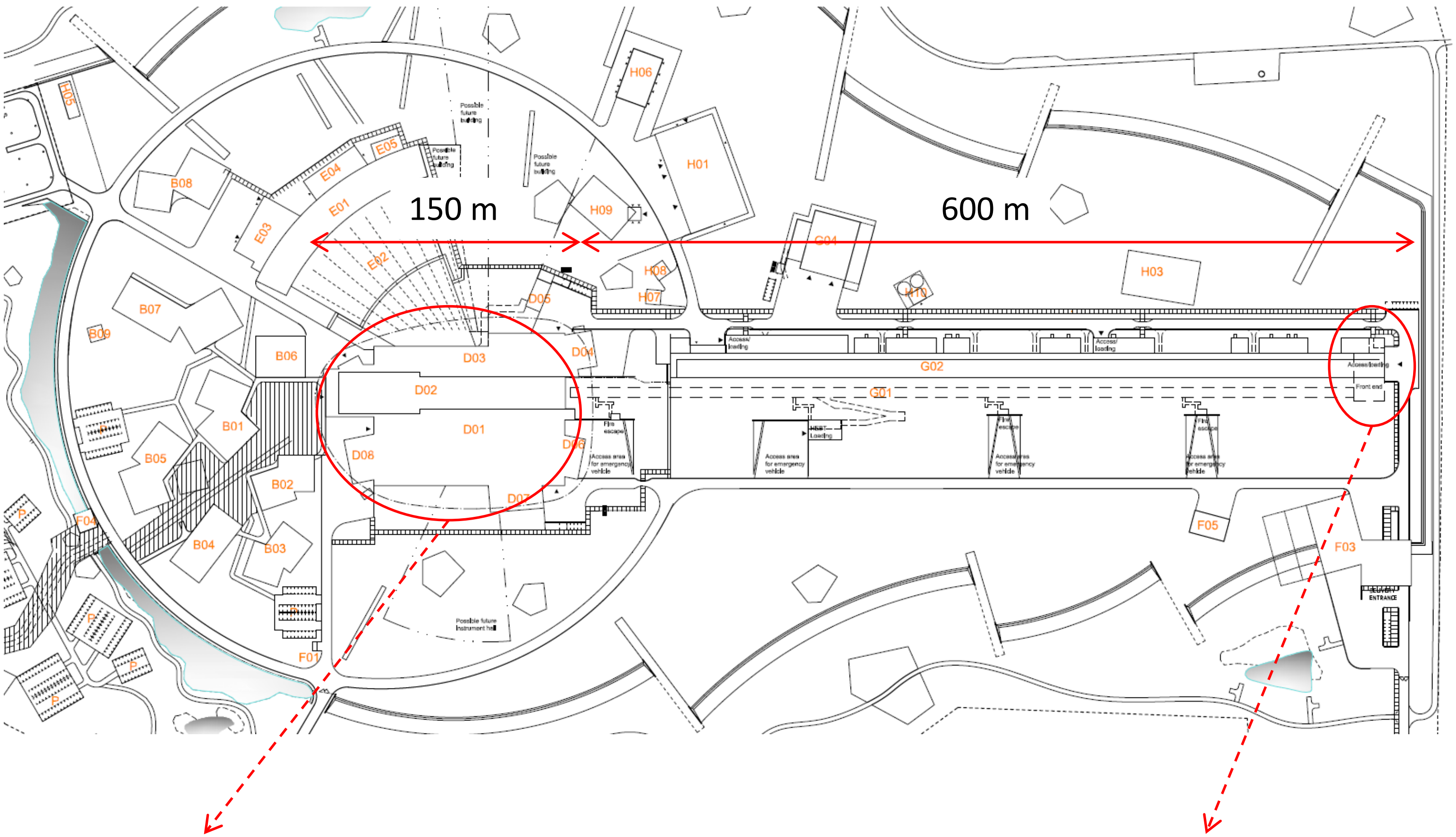
#	Safety functions
	TSS shall prevent proton beam from reaching target if any of these is fulfilled…
1	… target cooling He outlet velocity is below critical limit
2	… target cooling He outlet pressure is below critical limit
3	… target cooling He inlet temperature is above critical limit
4	… target wheel rotational speed is below critical limit
5	… monolith pressure is above critical limit

- Correlated to bounding events identified in the accident analyses
- Independent of each other

TSS - safety instrumented functions - principal



TSS main areas on ESS



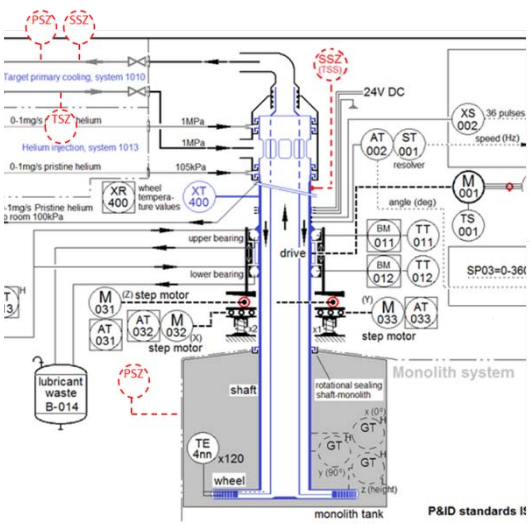
Target building
- Sensors (reading Target process variables)
- Logic solvers (located in two different areas)

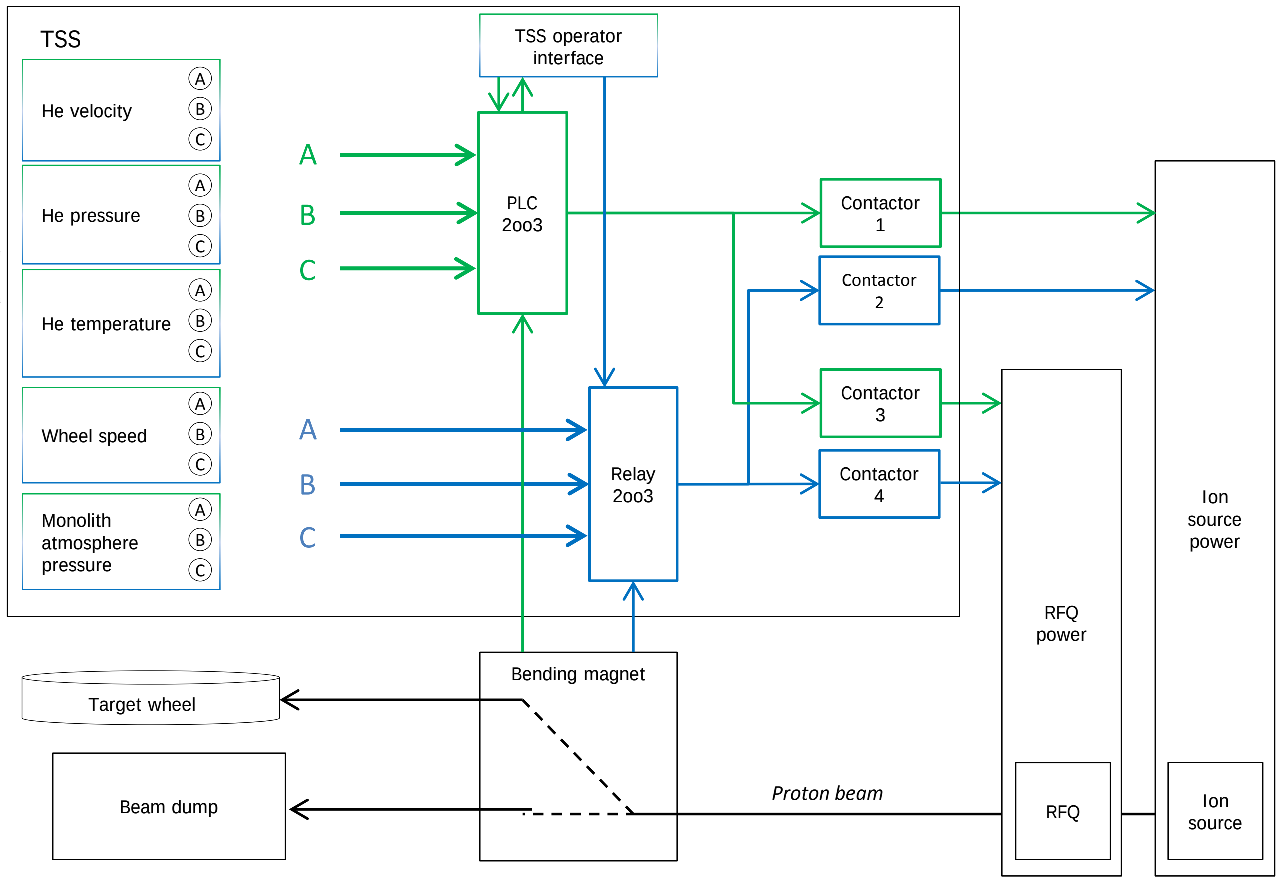
Front end building
- Final elements (to stop proton beam = safe state)

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





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*
- 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

Severity (mSv) Probability	< 0.1	0.1 – 1	1 – 20	20 – 100	> 100
H2					
H3					
H4(A&B)					
H5					

Event	Event probability	Tolerable probability	SSM referenced probabilities (see [6], Appendix 1, chapter 4, 2A)
H2	10^{-2}	-	$10^{-2} <= P$
H3	10^{-3}	10^{-4}	$10^{-4} <= P < 10^{-2}$
H4A/B	10^{-5}	10^{-6}	$10^{-6} <= P < 10^{-4}$
H5	-	10^{-7}	$P < 10^{-6}$

Target SIL (AA1)

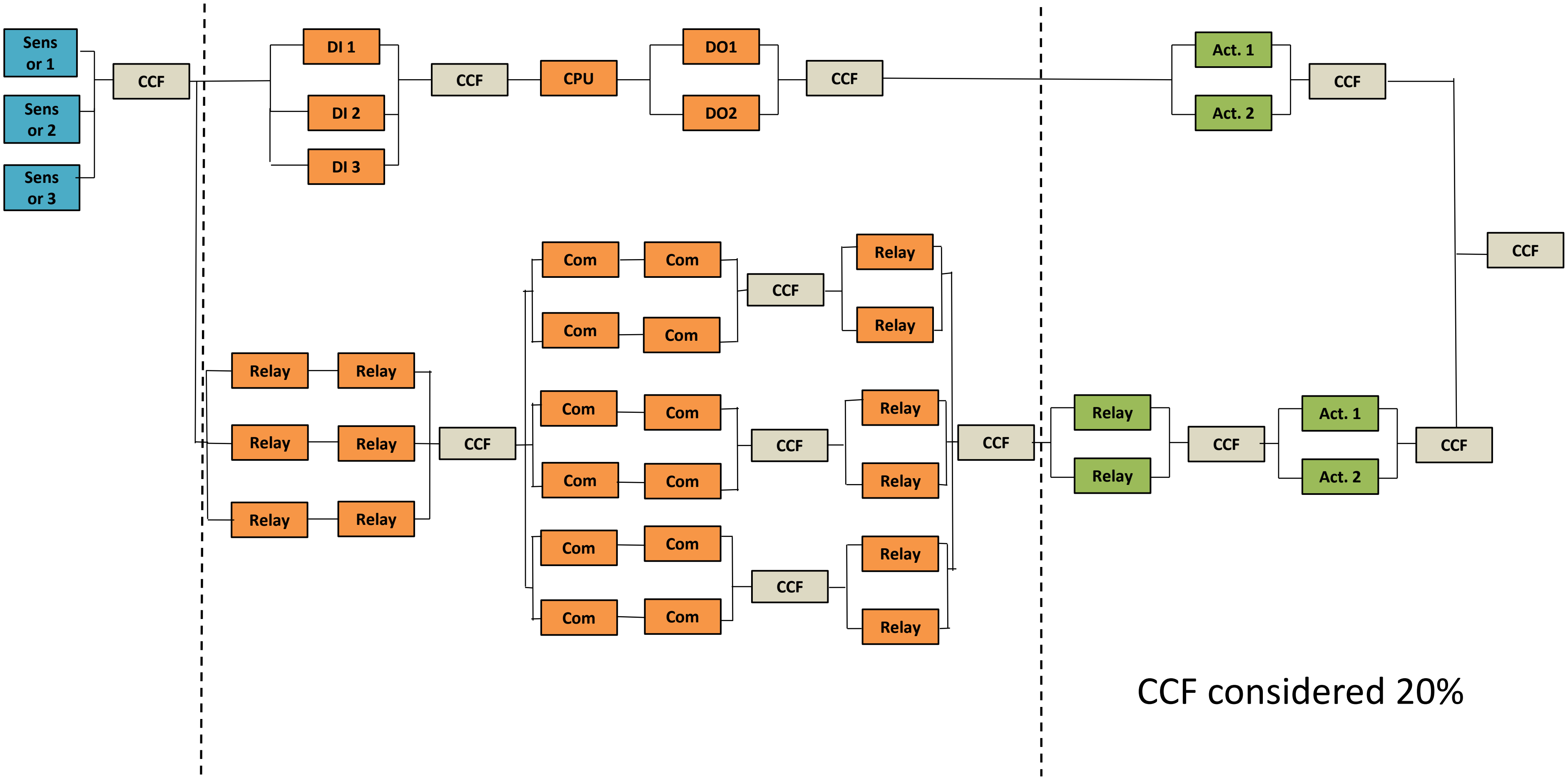
Accident Analysis	SIF ID	Initiating Events	Higher occurrence probability	Dose to public (maximum of different scenarios)
AA1: Target Wheel stops rotating while the accelerator is in operation and a 5 MW high power beam is impinging upon the target at a rate of 14 Hz	SIF4, SIF2, SIF5	Bearing failure,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

Severity (mSv) / Probability	< 0.1	0.1 – 1	1 – 20	20 – 100	> 100
H2					
H3					
H4(A&B)					
H5					

SIL	Availability	PFDavg	Risk Reduction
4	>99.99%	10^{-5} to $<10^{-4}$	100,000 to 10,000
3	99.9%	10^{-4} to $<10^{-3}$	10,000 to 1,000
2	99 to 99.9%	10^{-3} to $<10^{-2}$	1,000 to 100
1	90 to 99%	10^{-2} to $<10^{-1}$	100 to 10

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

Reliability block diagram



CCF considered 20%

Summary of SIL determination

- PLC train only: PFD_{avg}= 4.84e-4
- Relay train only: PFD_{avg}= 2.73e-3
- Total : PFD_{avg}= 8.90e-4

SIL	Availability	PFDavg	Risk Reduction
4	>99.99%	10^{-5} to $<10^{-4}$	100,000 to 10,000
3	99.9%	10^{-4} to $<10^{-3}$	10,000 to 1,000
2	99 to 99.9%	10^{-3} to $<10^{-2}$	1,000 to 100
1	90 to 99%	10^{-2} to $<10^{-1}$	100 to 10

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