ESS
Machine Protection: First Ideas

EUROPEAN
SPALLATION
SOURCE

A. Nordt, R. Schmidt, ESS, Lund/Sweden

PLC Workshop 2013
Lund/Sweden, 29th - 30th of August 2013

CONTENT

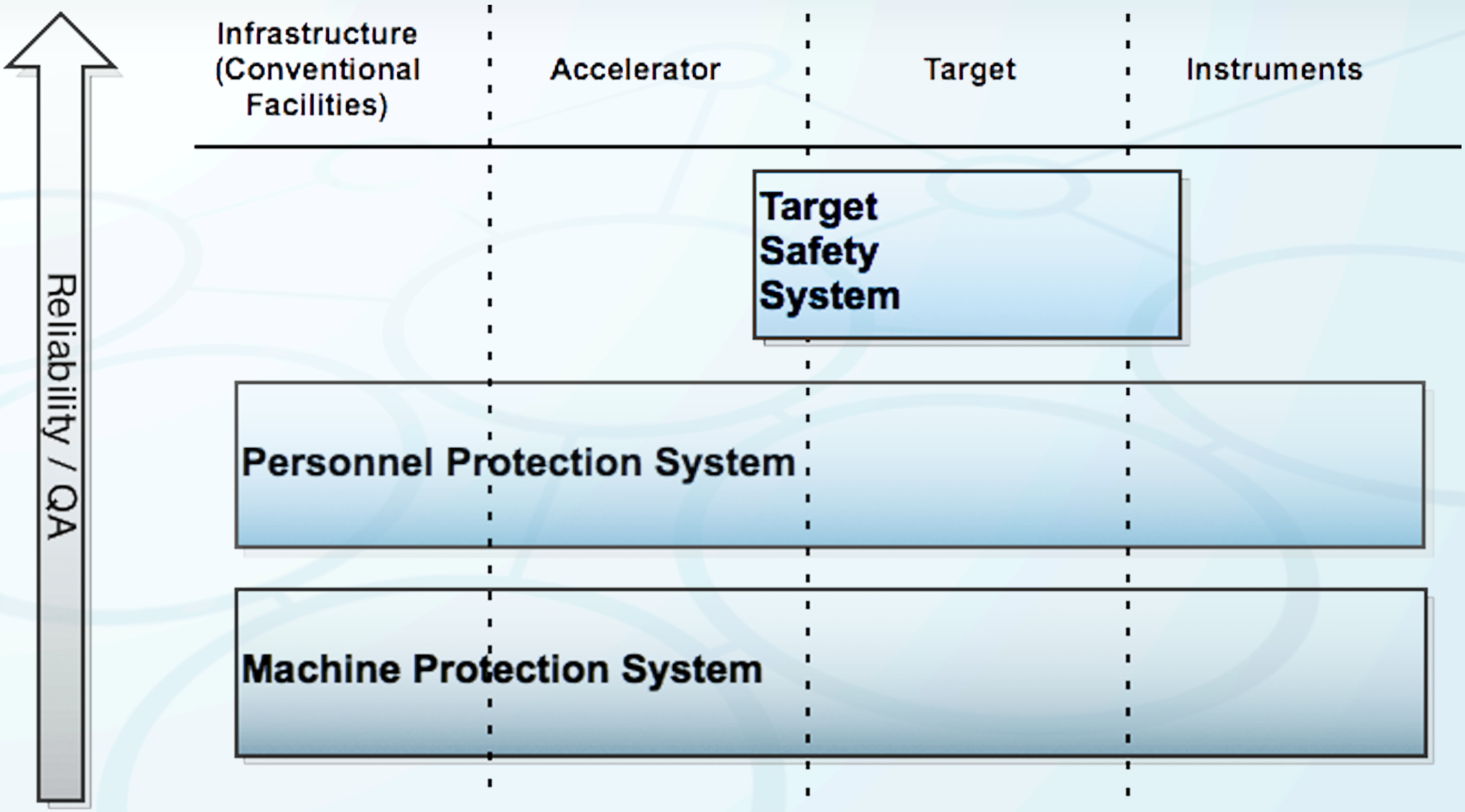
- ESS and its Protection Systems
- MPS Risk Analysis: overview, outcome, results
- First Design Ideas and Requirements
- Fast machine protection system
- Slow machine protection system
- Summary and Conclusions

ESS in Lund/Sweden

- Brightest neutron source worldwide
- 17 European member states
- First Neutrons: 2019
- Full power operation: 2025
- Decommissioning: 2065
- Investment: 1843 MEURO
- Sustainable energy concept
- Beam availability 95%

EUROPEAN SPALLATION SOURCE

PROTECTION SYSTEMS @ ESS



Infrastructure (Conventional Facilities)

Accelerator

Target

Instruments

Target Safety System

Personnel Protection System

Machine Protection System

Reliability / QA

MACHINE **PROTECTION SYSTEM**

Scope of MPS

Protect the machine's equipment from damage due to

- Beam losses
- Malfunctioning equipment.

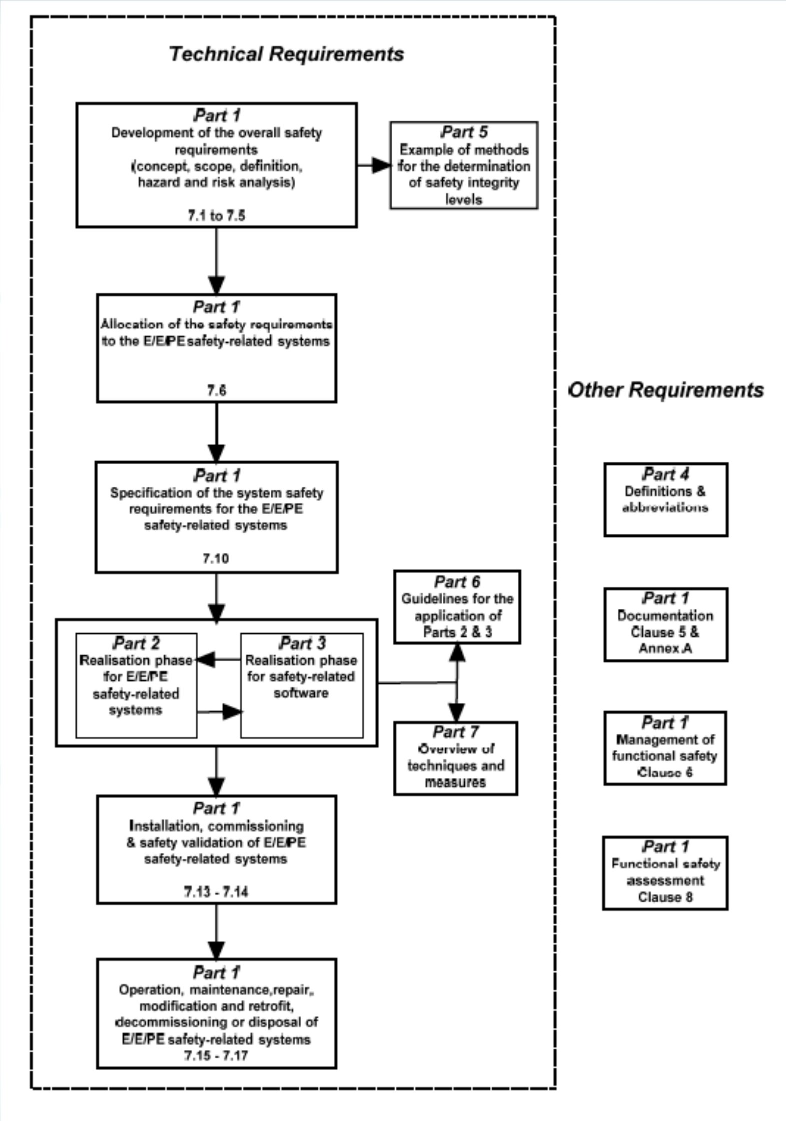
MPS Design Function

- Initiate beam stop upon detection of non-nominal conditions.

MPS Design Approach

- Follow IEC61508 standard, where applicable.
- Optimize integrated machine performance according to ESS overall goal of reaching 95% beam availability with high reliability.

IEC61508 **LIFECYCLE MODEL**


Technical Requirements
Part 1
Development of the overall safety requirements (concept, scope, definition, hazard and risk analysis)
7.1 to 7.5
Part 5
Example of methods for the determination of safety integrity levels
Part 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
Part 1
Specification of the system safety requirements for the E/E/PE safety-related systems
7.10
Part 6
Guidelines for the application of Parts 2 & 3
Part 2
Realisation phase for E/E/PE safety-related systems
Part 3
Realisation phase for safety-related software
Part 7
Overview of techniques and measures
Part 1
Installation, commissioning & safety validation of E/E/PE safety-related systems
7.13 - 7.14
Part 1
Operation, maintenance,repair, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
7.15 - 7.17
Other Requirements
Part 4
Definitions & abbreviations
Part 1
Documentation Clause 5 & Annex A
Part 1
Management of functional safety Clause 6
Part 1
Functional safety assessment Clause 8

Currently working on part 1:

- Definition of concept, scope,
- Hazard and risk analysis
- Definition and allocation of the safety requirements to safety related systems

(source: IEC61508-1 / IEC:2010)

EUROPEAN
SPALLATION
SOURCE

PRELIMINARY **HAZARD IDENTIFICATION**

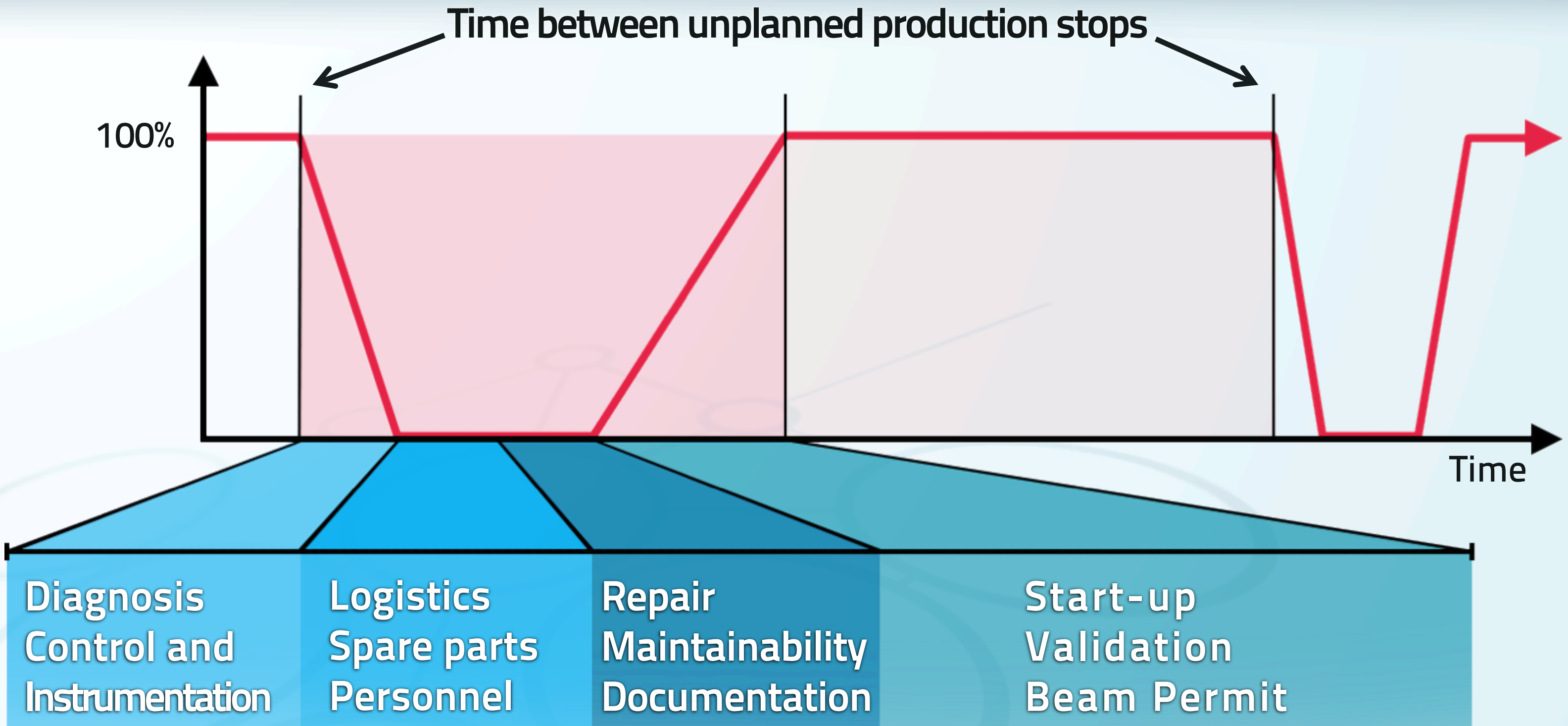
Probability	**Consequence Ranking**			
Frequent: At least once a year	3	4	5	6
Probable: Once between 1 and 10y	2	3	4	5
Rare: Once between 10 and 100y	1	2	3	4
Exceptional: Not in 100y	1	1	2	3
Severity	**Insignificant**	**Moderate**	**Major**	**Catastrophic**
Production Losses/year	<1 day	<1 week	<2 month	≤1 year
Property Losses	<150 KEUR	<1 MEUR	<8 MEUR	≤50 MEUR

Scope

- Identify risks/hazards of MPS related systems and Safety Integrity Level (SIL)
- Identify mitigation methods for all identified (catastrophic) events

Preliminary Hazard Identification done with help from Scandpower

OVERVIEW ON **AVAILABILITY**



Diagnosis
Control and
Instrumentation

Logistics
Spare parts
Personnel

Repair
Maintainability
Documentation

Start-up
Validation
Beam Permit

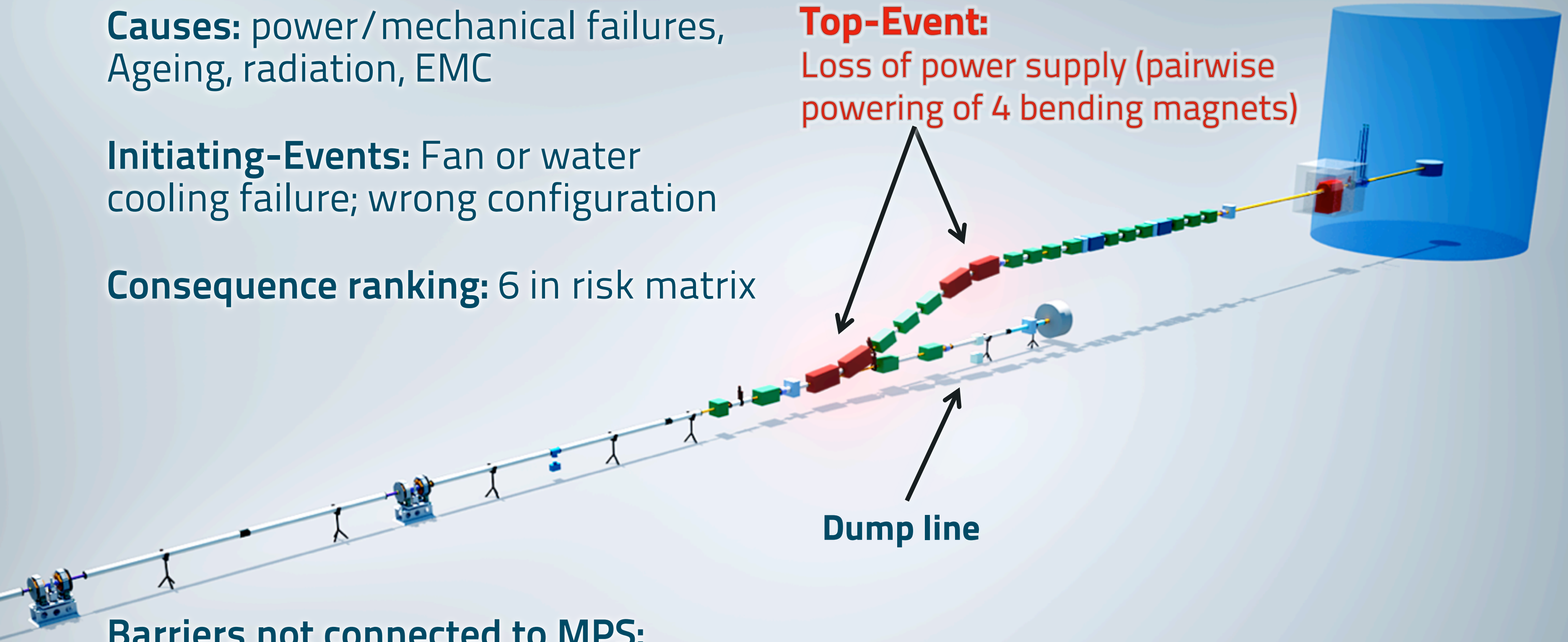
Categorize different sources of downtime/mitigation techniques per event and define impact on overall ESS performance.

EXAMPLE FROM **RISK ANALYSIS**

Causes: power/mechanical failures, Ageing, radiation, EMC

Initiating-Events: Fan or water cooling failure; wrong configuration

Consequence ranking: 6 in risk matrix



Top-Event:
Loss of power supply (pairwise powering of 4 bending magnets)

Barriers not connected to MPS:
Preventive maintenance, closure of fast valve in A2T (accelerator to target) line

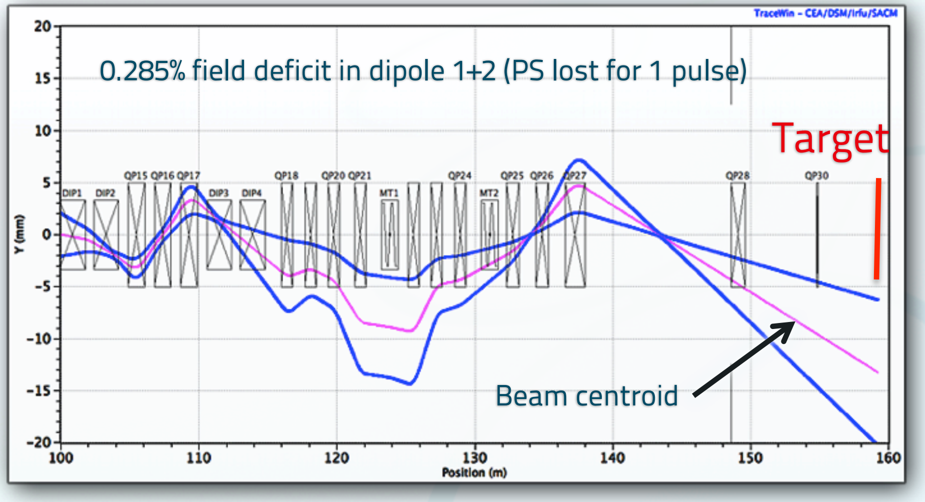
Consequence ranking with barriers: 4 in risk matrix

Safety instrumented systems to be connected to MPS:
Power supplies; BPMs, BLMs close by; vacuum gauge in A2T

LOSS OF POWER FOR **BENDING MAGNETS**

Recommendations from Risk Analysis

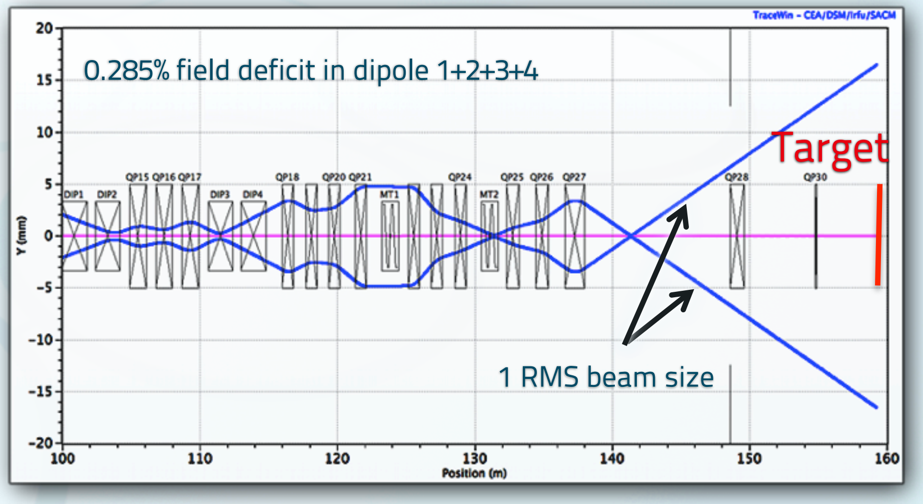
- Check effect of glitches, how long it takes until beam pipe is damaged,
- Consider hot spare for power supply,
- Measure B-field with Tesla-meter and connect to MPS,
- Check different powering schemes: [(1+2+3+4)] or [(1,2,3,4)] or [(1+2), (3+4)].



0.285% field deficit in dipole 1+2 (PS lost for 1 pulse)

Target

Beam centroid



0.285% field deficit in dipole 1+2+3+4

Target

1 RMS beam size

Pairwise powering (1+2) and (3+4):
Unacceptably large beam displacement on the target → **this design was changed !**

Single PS for all 4 magnets (1+2+3+4):
Beam delivered to target is insensitive to non-nominal powering !

Courtesy of H. D. Thomson, Aarhus University, Denmark

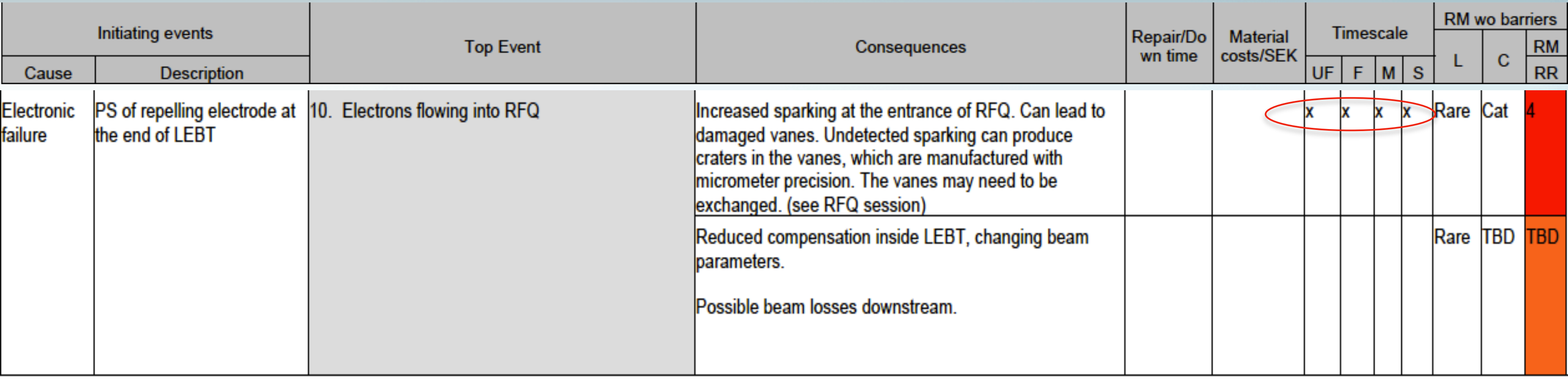
RESULTS FROM **RISK ANALYSIS FOR LINAC**

Outcome

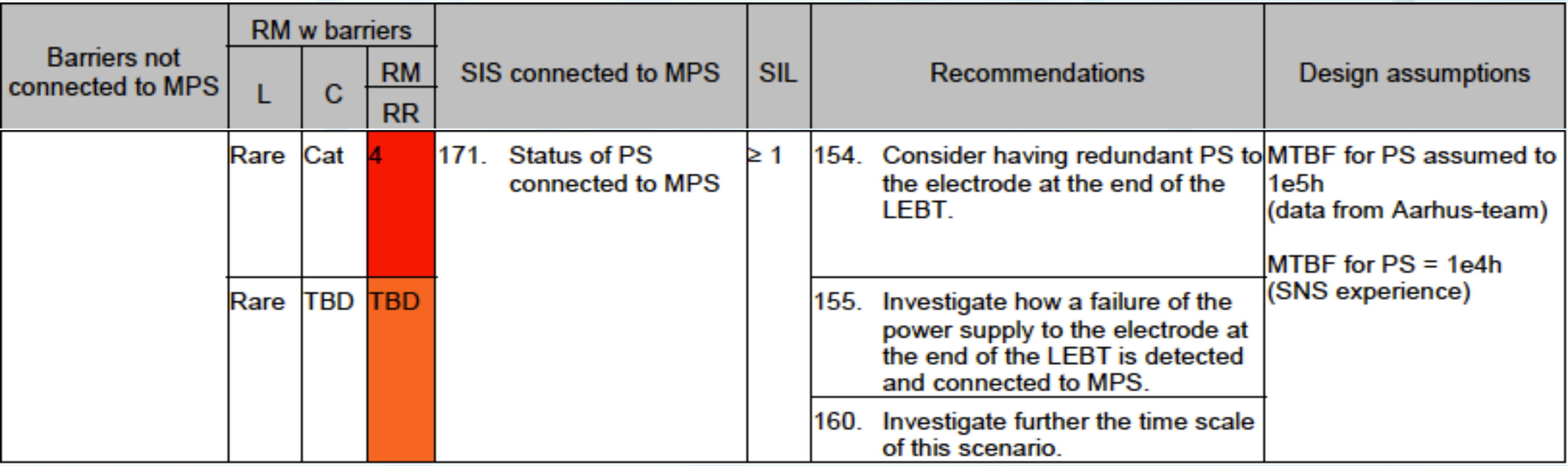
- Catalogue of risks and failures + mitigation techniques
- Overview on downtime, operational procedures, spare policy
- Recommendations for design considerations
- Information will be stored in ESS risk database: follow up of implementation is as important as identification of risks !

- Signals connected to machine interlock system
- MPS functions and related SIL (SIL 2 is recommended)
- Allocation of functions to sub-systems
- Required response time to achieve sufficient protection (10μs)

MPS RESPONSE **TIME: EXAMPLE**



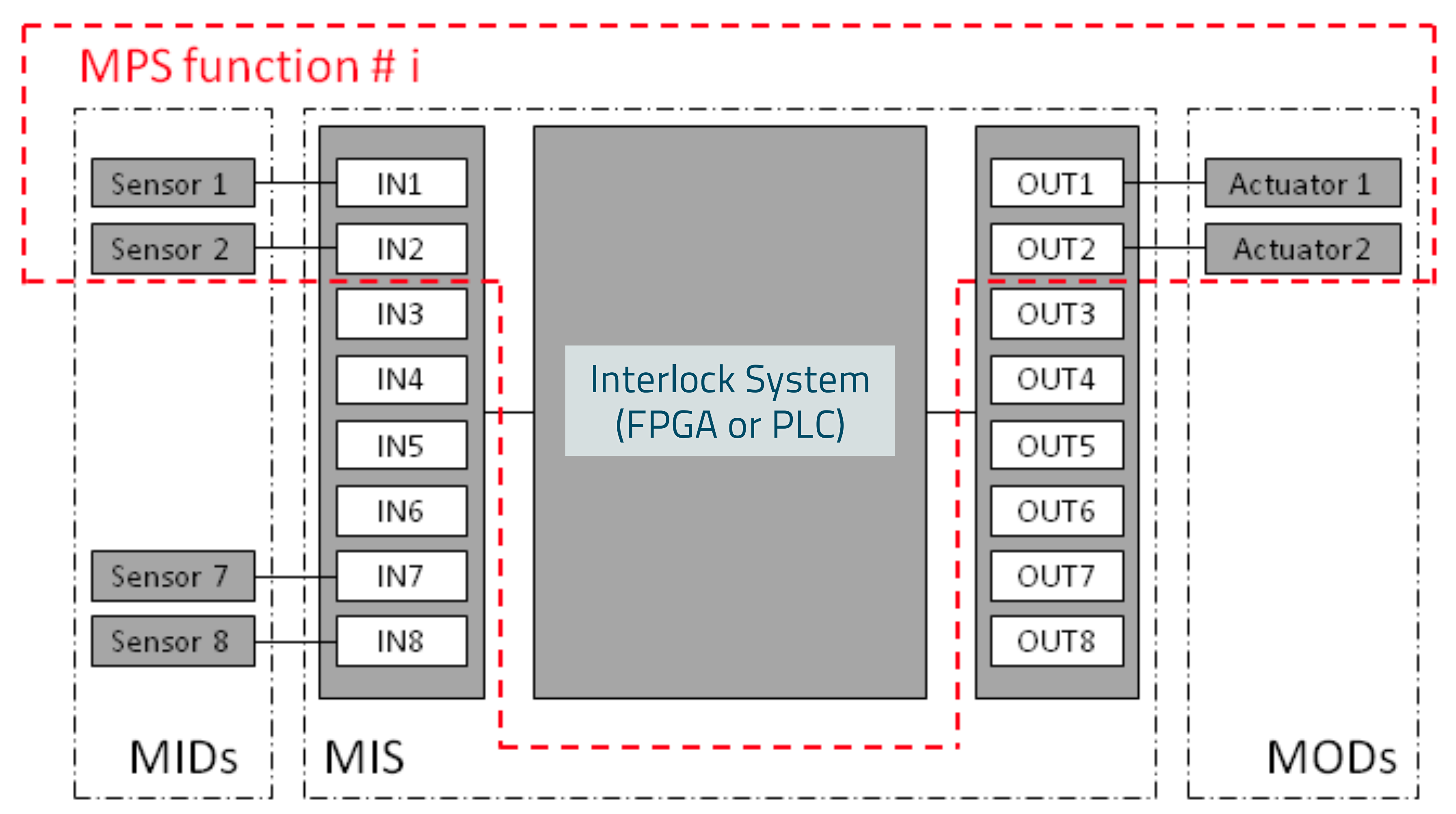
Initiating events		Top Event	Consequences	Repair/Down time	Material costs/SEK	Timescale				RM wo barriers		
Cause	Description					UF	F	M	S	L	C	RM RR
Electronic failure	PS of repelling electrode at the end of LEBT	10. Electrons flowing into RFQ	Increased sparking at the entrance of RFQ. Can lead to damaged vanes. Undetected sparking can produce craters in the vanes, which are manufactured with micrometer precision. The vanes may need to be exchanged. (see RFQ session)			x	x	x	x	Rare	Cat	4
			Reduced compensation inside LEBT, changing beam parameters. Possible beam losses downstream.							Rare	TBD	TBD



Barriers not connected to MPS	RM w barriers			SIS connected to MPS	SIL	Recommendations	Design assumptions
	L	C	RM RR				
	Rare	Cat	4	171. Status of PS connected to MPS	≥ 1	154. Consider having redundant PS to the electrode at the end of the LEBT.	MTBF for PS assumed to 1e5h (data from Aarhus-team) MTBF for PS = 1e4h (SNS experience)
	Rare	TBD	TBD			155. Investigate how a failure of the power supply to the electrode at the end of the LEBT is detected and connected to MPS. 160. Investigate further the time scale of this scenario.	

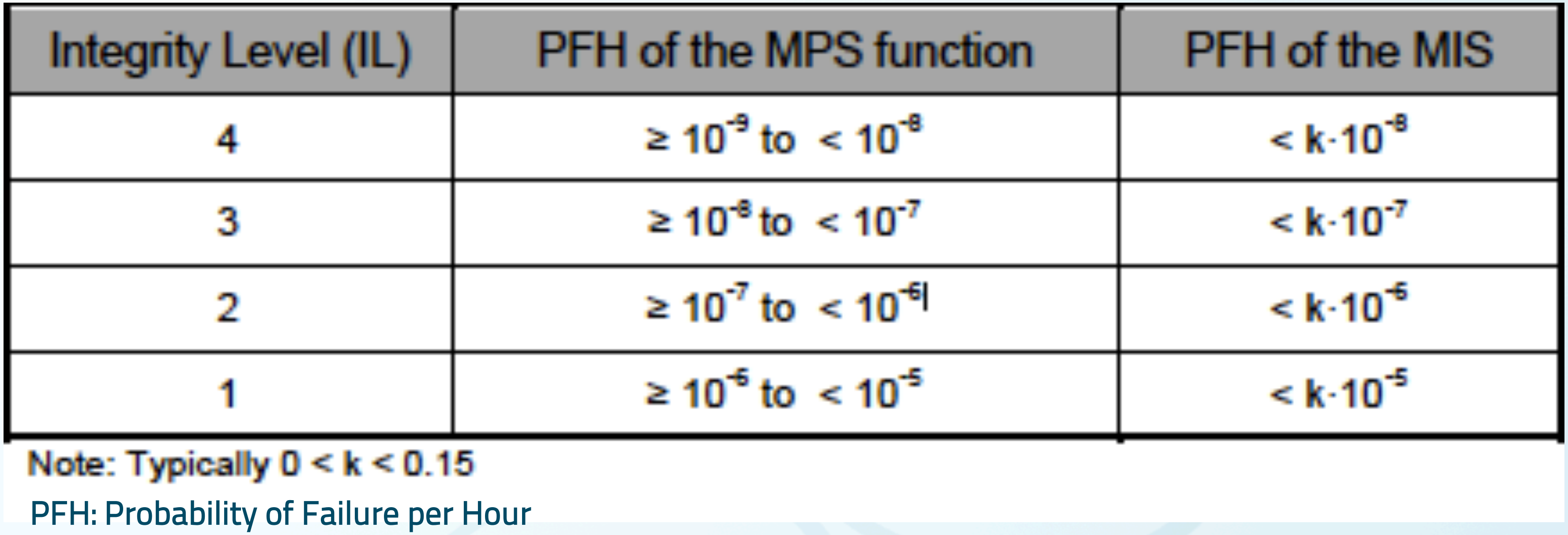
UF: ultrafast=1-10μs, F: fast=10-100μs, M: medium=100μs-1s, S: slow=1-100s

DEFINITION OF MPS **FUNCTIONS**



SAFETY INTEGRITY **LEVELS**

Safety Integrity Level for high demand or continuous mode of operation



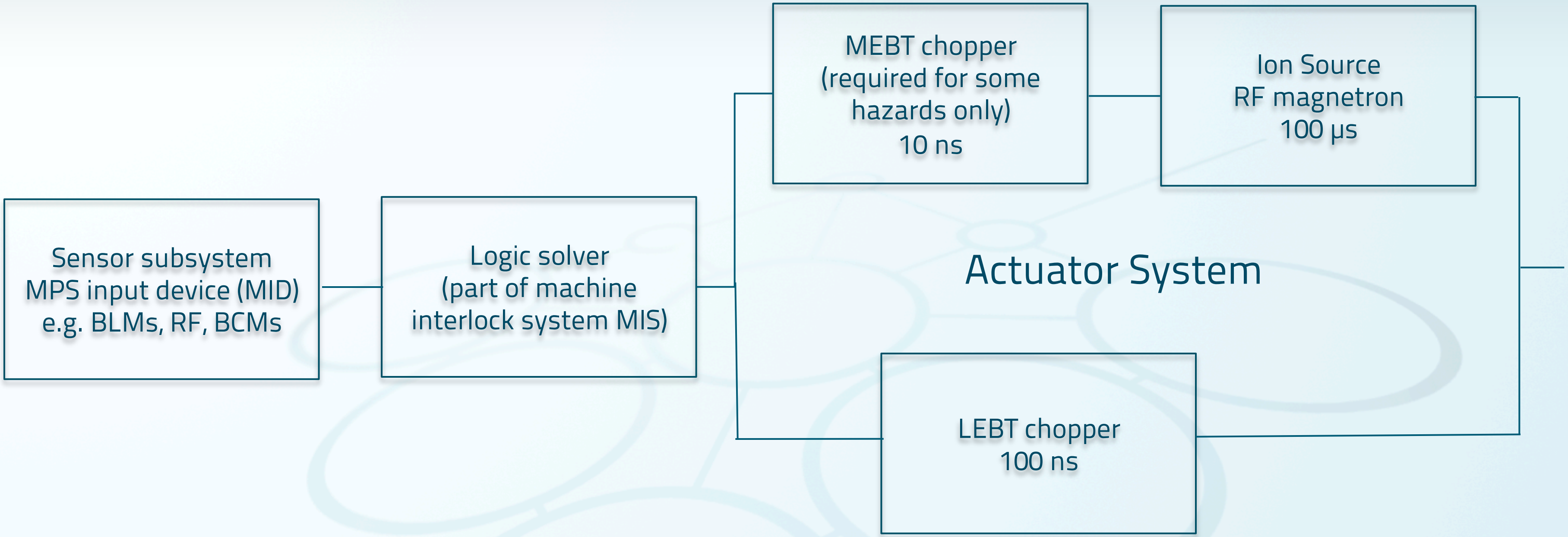
Integrity Level (IL)	PFH of the MPS function	PFH of the MIS
4	≥ 10^{-9} to < 10^{-8}	< $k \cdot 10^{-8}$
3	≥ 10^{-8} to < 10^{-7}	< $k \cdot 10^{-7}$
2	≥ 10^{-7} to < 10^{-6}|	< $k \cdot 10^{-6}$
1	≥ 10^{-6} to < 10^{-5}	< $k \cdot 10^{-5}$

Note: Typically $0 < k < 0.15$

PFH: Probability of Failure per Hour

The SIL sets requirements for **random failure rates for hardware**, **diagnostic coverage and fault tolerance** for the entire MPS function and on techniques and measures to minimize the propensity for systematic failures. The higher the SIL, the more stringent the requirements.

MPS ACTUATORS & RESPONSE TIMES

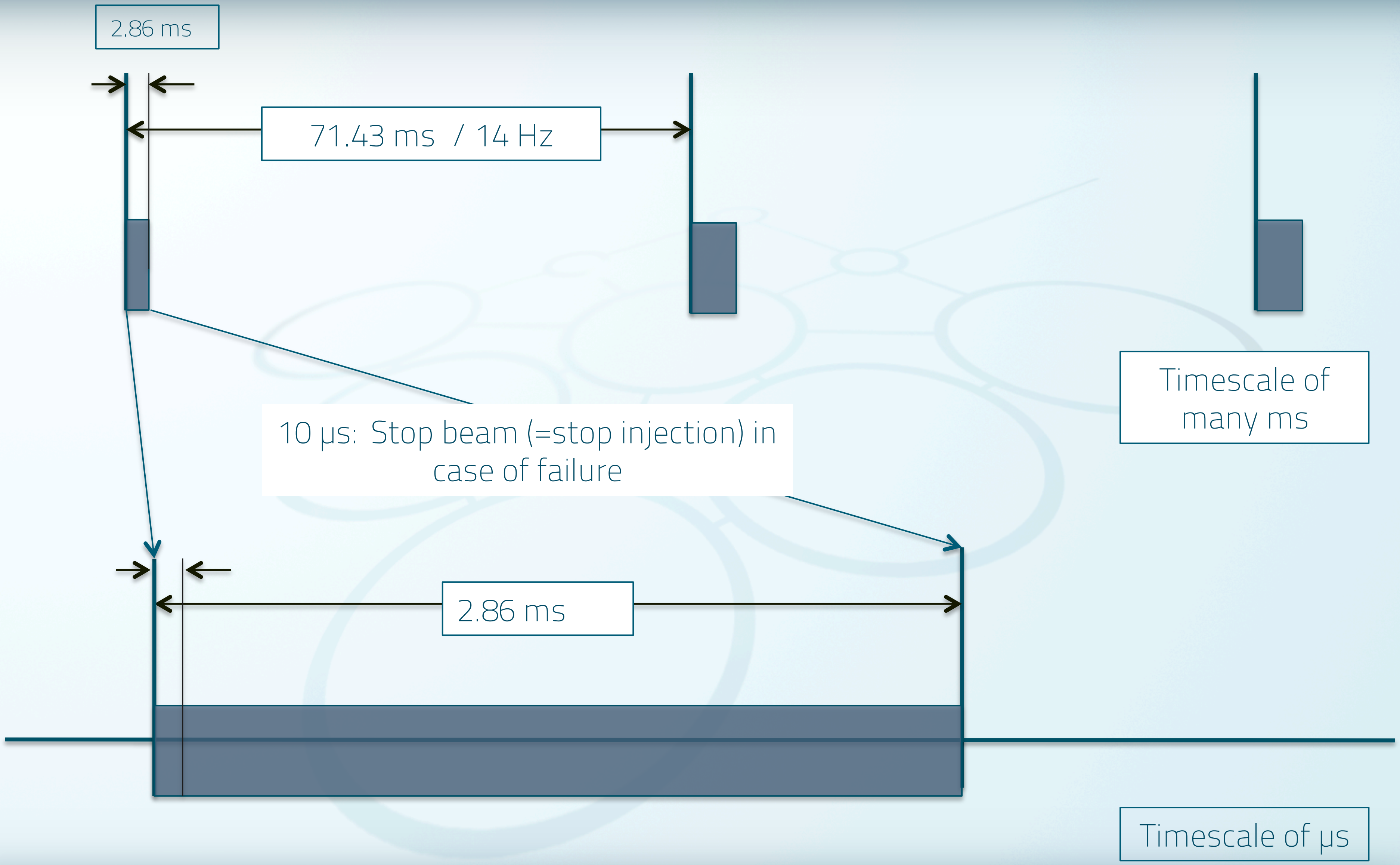


Two different mitigation techniques will be implemented

Intra-pulse (within a pulse): fast beam stop

Inter-pulse (in between pulses): let the current pulse pass (safe beam parameters) BUT inhibit the next *n* pulses

NOMINAL BEAM OPERATION: **TIME SCALES**



2.86 ms

71.43 ms / 14 Hz

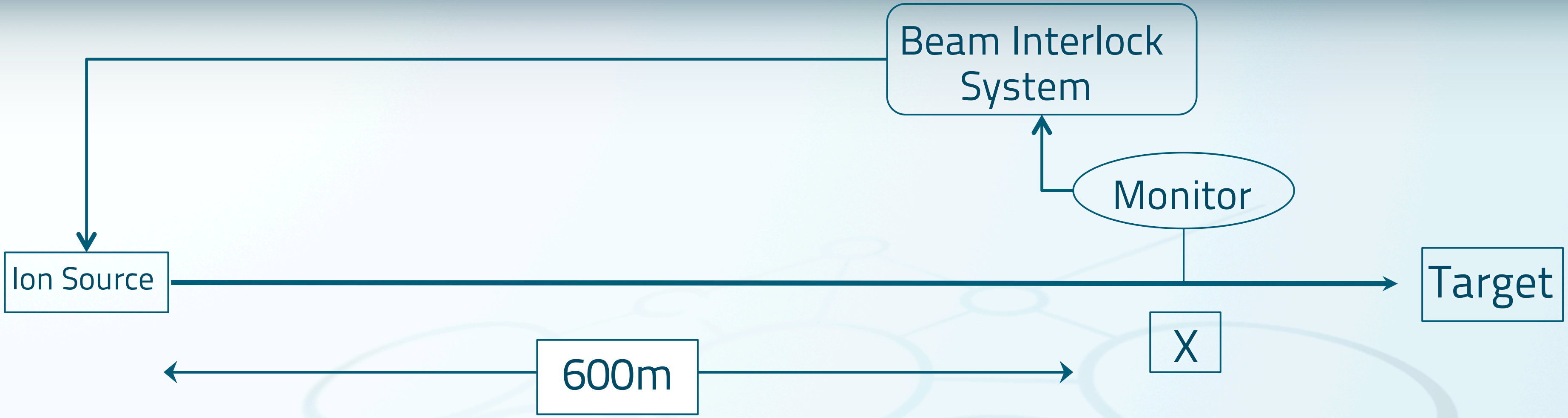
Timescale of many ms

10 µs: Stop beam (=stop injection) in case of failure

2.86 ms

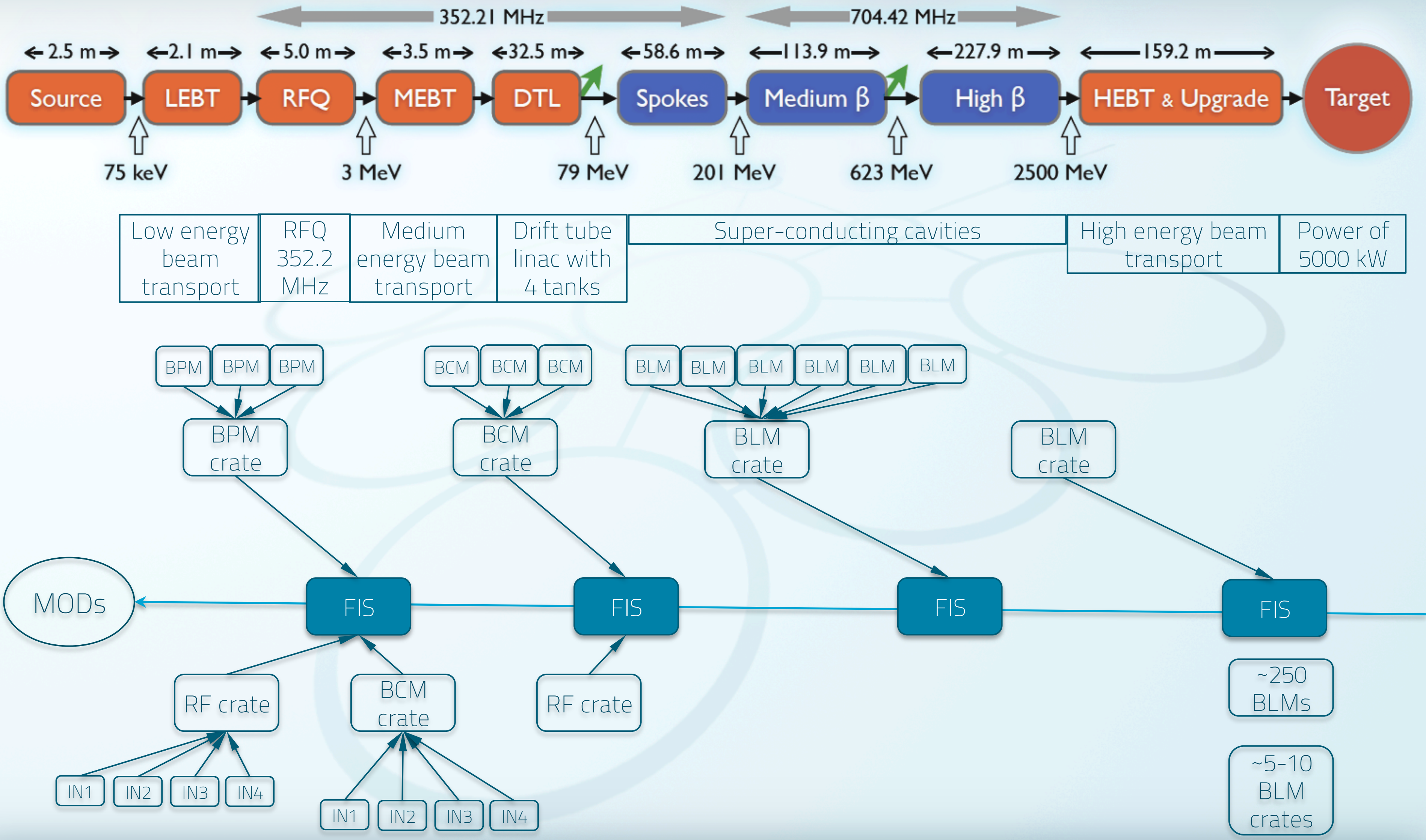
Timescale of µs

MINIMUM TIME TO **STOP BEAM**

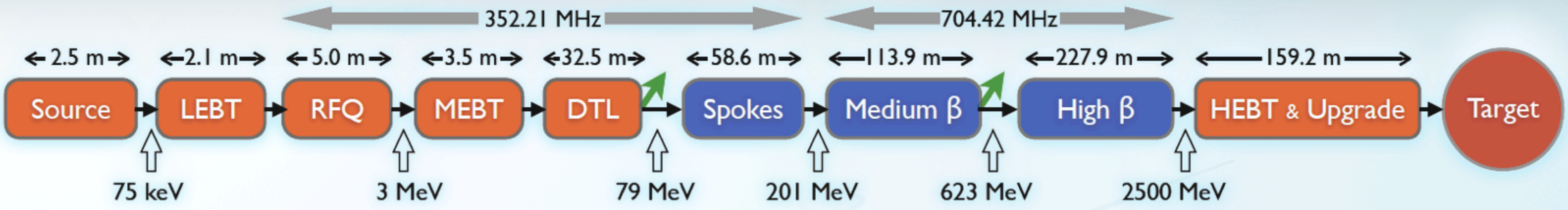


Beam impact at Position X (shown are estimated time-scales !)	
Monitor detects a failure (e.g. beam loss above threshold)	2 μs
Monitor validates failure and informs beam interlock system	1 μs
Beam interlock system records failure and issues beam stop request	1 μs
Signal transmission from Beam Interlock System to Source / Chopper	2 μs
Time to receive stop request at LEBT chopper	2 μs
Time that beam stops at position X	1 μs
Sum	9 μs

FAST **INTERLOCK SYSTEM (FIS)**



SLOW **INTERLOCK SYSTEM**



Low energy beam transport

RFQ 352.2 MHz

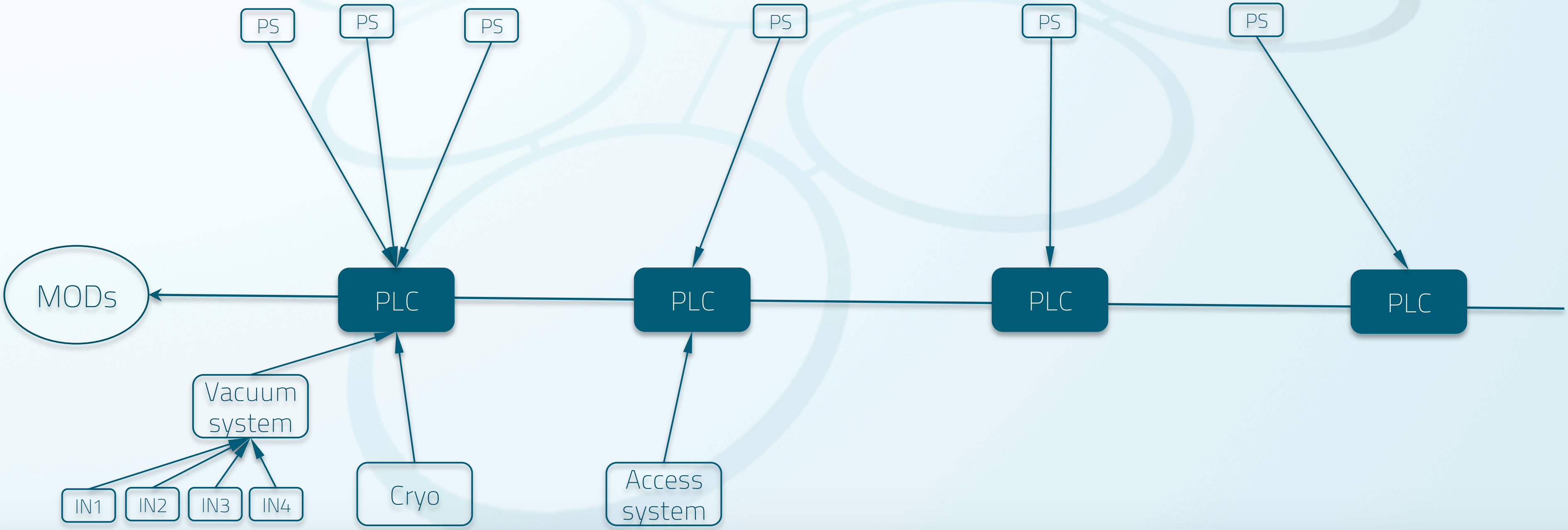
Medium energy beam transport

Drift tube linac with 4 tanks

Super-conducting cavities

High energy beam transport

Power of 5000 kW

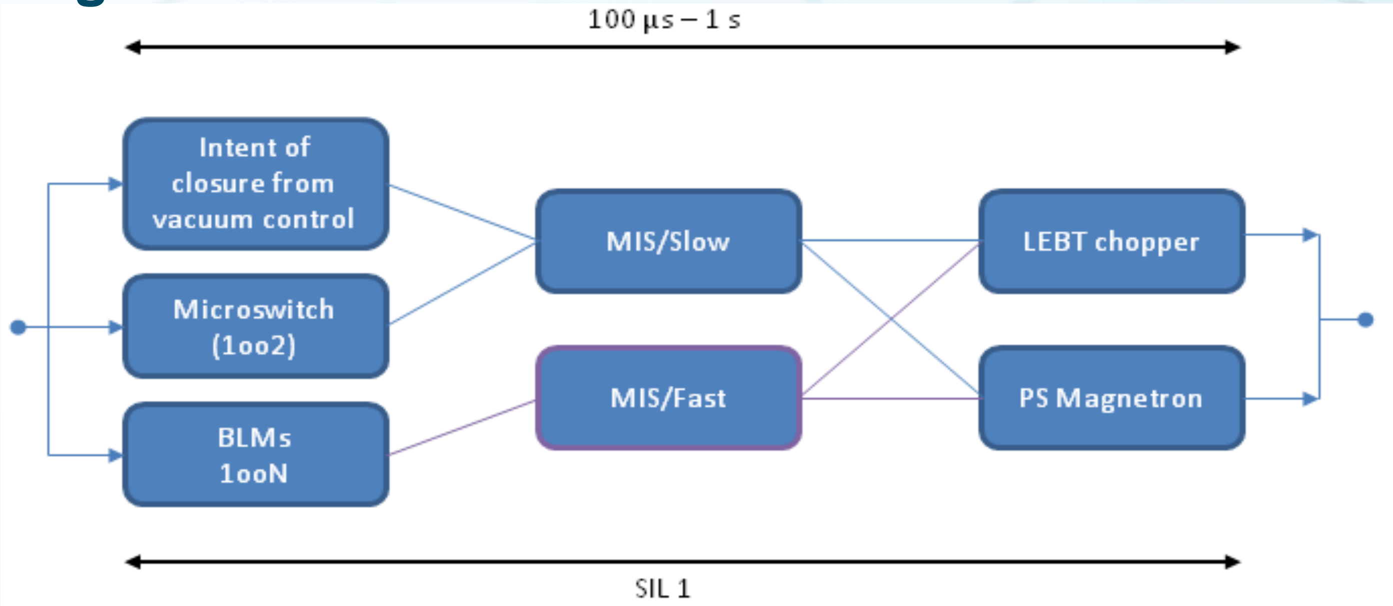


Safety Requirement **Specifications (SRS) I**

Example for fast valve in LEDP (closure within ~10ms):

Safety Integrity Function (SIF): *MPS-LEDP-SRS-001* protects against damage to the fast valve *(LEDP-VAC:FV-01)* in LEDP as result of unintended closure during beam operation in the LINAC

Block diagram:



Definition of boundaries: SIF includes 3 diversified MIDs, fast and slow MIS, 2 MODs

Safety Requirement **Specifications (SRS) II**

Safe State: Switching off PS magnetron or actuation OR actuation of LEBT chopper

Source of Demand: Unintended closure of *LEDP-VAC:FV-01* due to malfunctioning of valve control system OR erroneous operator actions OR spurious signal of valve closure

Mode of Operation: Low demand mode

Dangerous failures:
MID #1 (FV-Ctrl): failure to transmit "intention to close" signal
MID #2 (FV-MS-01 OR FV-MS-02): failure to change state to "open"
MID #3 (BLM): failure to detect beam losses above threshold
MIS: Failure to transmit beam stop signal to MODs
MOD #1: failure to switch off PS magnetron of Source upon request
MOD #2: failure to energize electrodes in LEBT chopper on request

Safety Requirements **Specifications (SRS) III**

Desired response upon detected failure: The system shall fail to safe state

Considerations about common cause failure: Are there any environmental or other parameters (e.g. radiation levels, etc.) that the supplier should consider with respect to propensity for CCF (common cause failure)?

Preliminary SIL/PFD: SIL 1, PFD < 0.1
Allocated PFD Quota: MIDs: 35%, MIS: 15%, MODs: 50%
Demand rate: 0.1-0.01/year (TBC)
Test interval: TBD
Maximum response time: 100μs-1s (preliminary)
Reference: 210650-2-R-001, Node 14, Top Event 14

In total 166 such safety requirements for LINAC MPS

NEXT **STEPS**

Ongoing

Preliminary Hazard Identification (PHI) for MPS related systems in:

- Target Station,
- Neutron Instruments,
- Conventional Facilities.

Derive MPS safety requirements, specifications and corresponding allocation as done for LINAC

Assessment of MPS for target station: is it sufficient to switch off beam only or are other actions required by MPS (acting on pumps, valves, etc)?

RELIABILITY **ASSESSMENT**

Preliminary Analysis for LINAC

- Failure modes and rates for equipment in LINAC
- Mean Time Between Failures (MTBF) with percent of anticipated failures
- Management of equipment (spares, redundancy, etc.)
- Impact of repair policy and Mean Time To Repair (MTTR)
- Time needed to switch system to operational with spare after failure
- Note: Method is adopted from G. Dodson/SNS

RESULTS **RELIABILITY ANALYSIS**

Outcome

- Detailed information on failure rates based on experience and operations data from other similar facilities, suppliers, etc.
- Tool to optimize (check) design and repair policy from early on
- Tool to provide reliability and availability 'goal" numbers to each sub-system

Next

- Update reliability data based on latest ESS design,
- Include target, neutron instruments in analysis,
- Create reliability block diagram for all systems impacting on ESS overall reliability and beam availability

COMBINATION OF **RESULTS**

Outcome

More detailed and extended view on beam/machine availability due to reliability data

- List of ”weak” and ”strong” systems
- Details on sensitivity of components
- Impact of quality assurance during all lifecycle phases

Next

- Event and Fault Tree Analysis for most critical systems
- Database for risk management extended by reliability data
- List of diagnostic data to be logged and analysis tools allowing for early fault detection as well.

SUMMARY AND **CONCLUSIONS I**

Summary

- MPS must support operations to assure maximum protection AND beam availability.
- Close collaboration with experts from accelerator, target, neutron instruments, and conventional facilities required.
- ESS reliability working group.
- ESS risk management.
- MPS working group.

Conclusions

- Risk and reliability assessment must be performed on a regular base and follow up must be done systematically.
- Robust design required in order to reach 95% overall reliability.

SUMMARY AND **CONCLUSIONS II**

- For many failure cases it is sufficient to inhibit the next pulse(s) !
- This can be done with PLC technology.
- For a few failures, the beam needs be stopped **very fast, after a few** μs.
- This requires the MPS to respond with a short delay, not possible with PLC based technology.

Questions to the workshop:

- What is the experience with PLC based interlock systems?
- What are the options for systems with very fast response?
- Is it possible to build a system that can stop beam in 10μs?
- What is the time needed to recover? How fast can we be back into production mode?

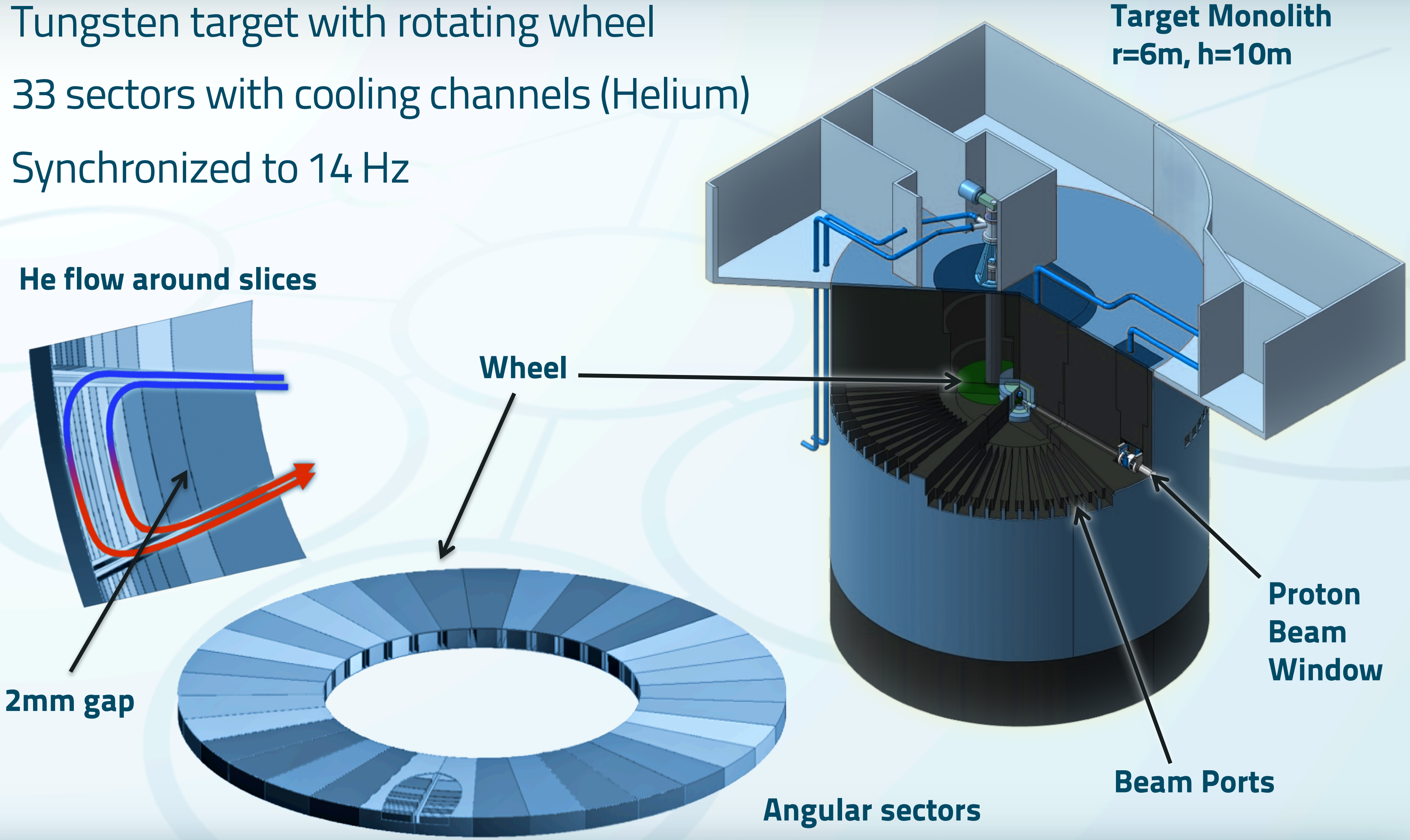
BACKUP **SLIDES**

ESS TARGET STATION

Tungsten target with rotating wheel

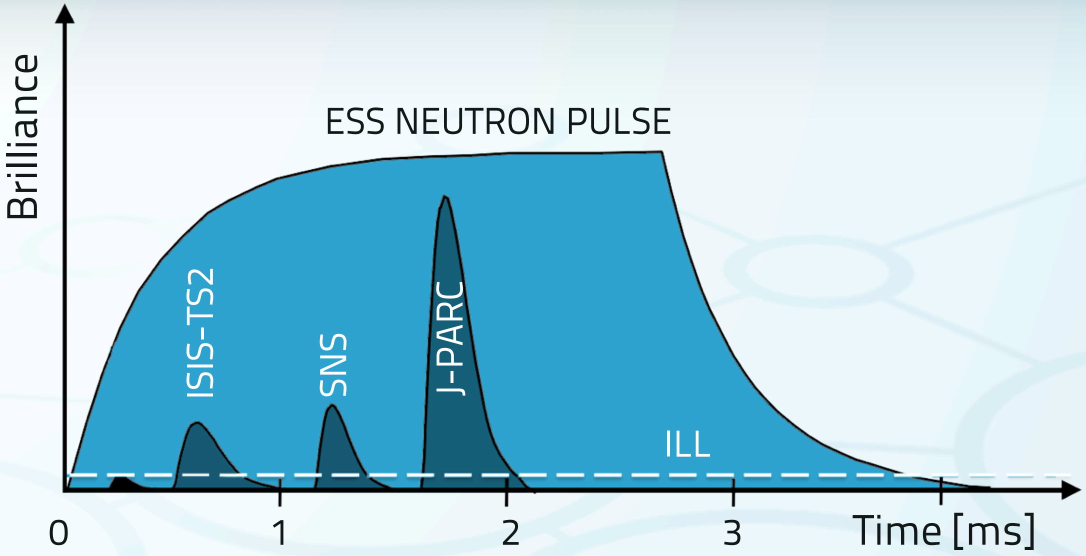
33 sectors with cooling channels (Helium)

Synchronized to 14 Hz



EUROPEAN
SPALLATION
SOURCE

ESS NEUTRON SCIENCE

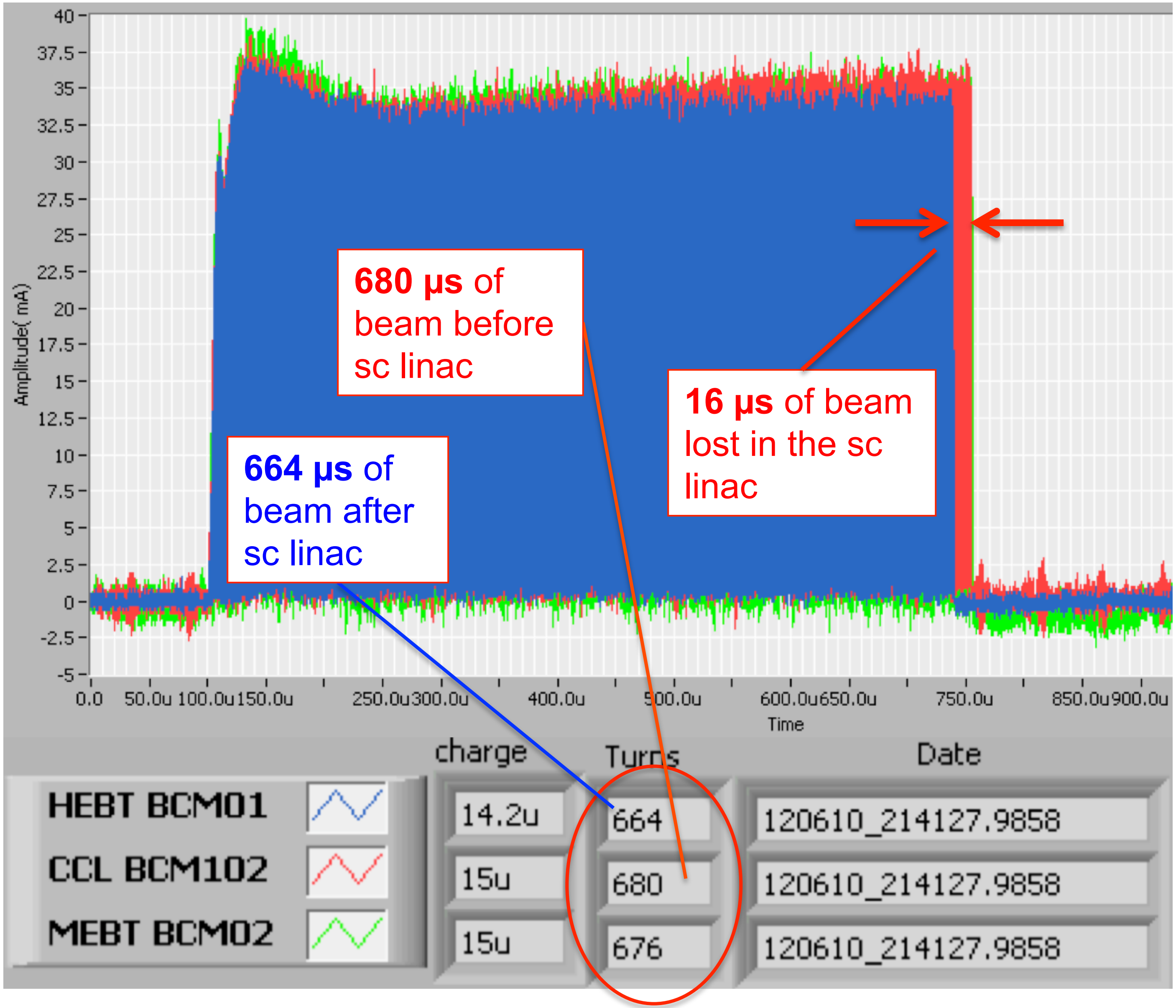


- ESS science lab: discovery potential within many different fields (material-, bio-, nano-science, etc.)
- ~ 5000 users per year
- Long pulses of cold neutrons allow for many different experiments
- 22 beam-lines, not all will be commissioned on day 1

Beam losses in SNS linac

Beam Current Monitors (BCM) measure current pulse at different locations along the linac.

About 16 µsec of beam lost in the superconducting part of linac



680 µs of beam before sc linac

664 µs of beam after sc linac

16 µs of beam lost in the sc linac

	charge	Turns	Date
HEBT BCM01	14.2u	664	120610_214127.9858
CCL BCM102	15u	680	120610_214127.9858
MEBT BCM02	15u	676	120610_214127.9858

Beam energy in 16 µs
End of DTL = 30 J
End of CCL = 66 J
End of SCL = 350 J

Beam loss with low energy deposition

- Beam might hit surface of HV system (RFQ, kicker magnets, cavities)
- Surfaces with HV, after beam loss performance degradation might appear (not possible to operate at the same voltage, increased probability of arcing, …)
- SNS: errant beam losses led to a degradation of the performance of superconducting cavity
  - Bam losses likely to be caused by problems in ion source, low energy beam transfer and normal conducting linac
  - Cavity gradient needs to be lowered, conditioning after warm-up helps in most cases
  - Energy of beam losses is about 100 J
  - Damage mechanisms not fully understood, it is assumed that some beam hitting the cavity desorbs gas or particulates (=small particles) creating an environment for arcing

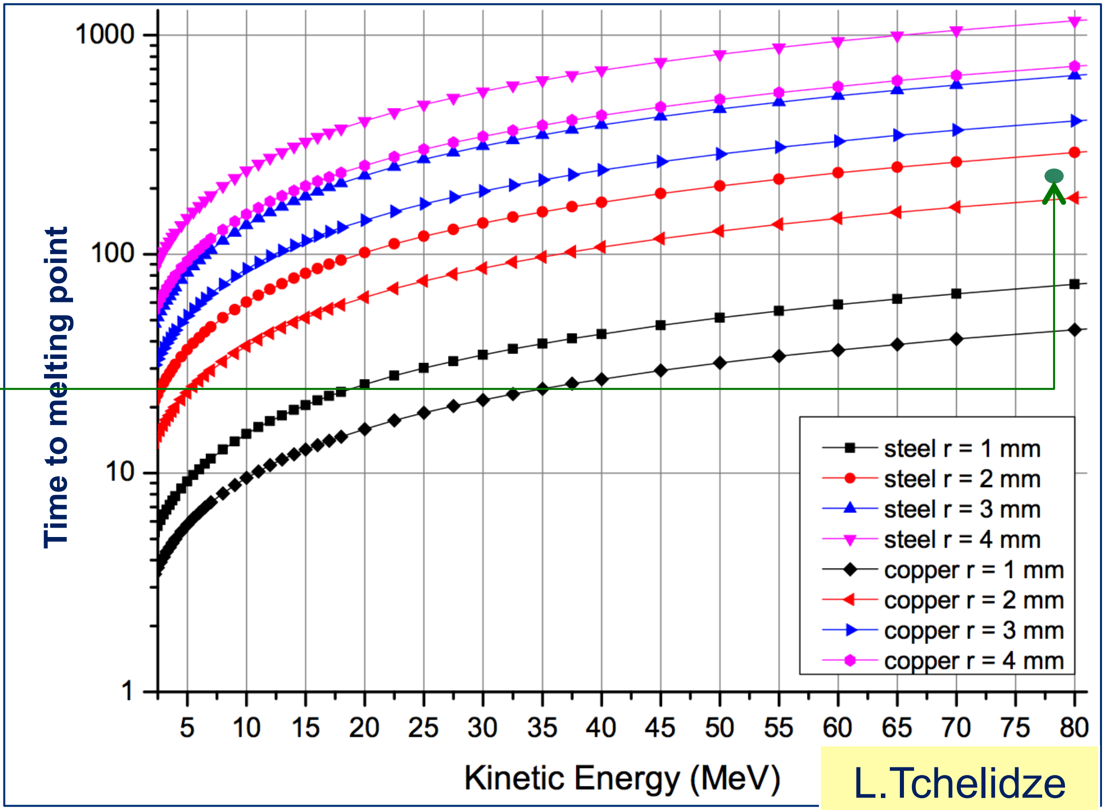
M.Plum / C.Peters

Example for ESS

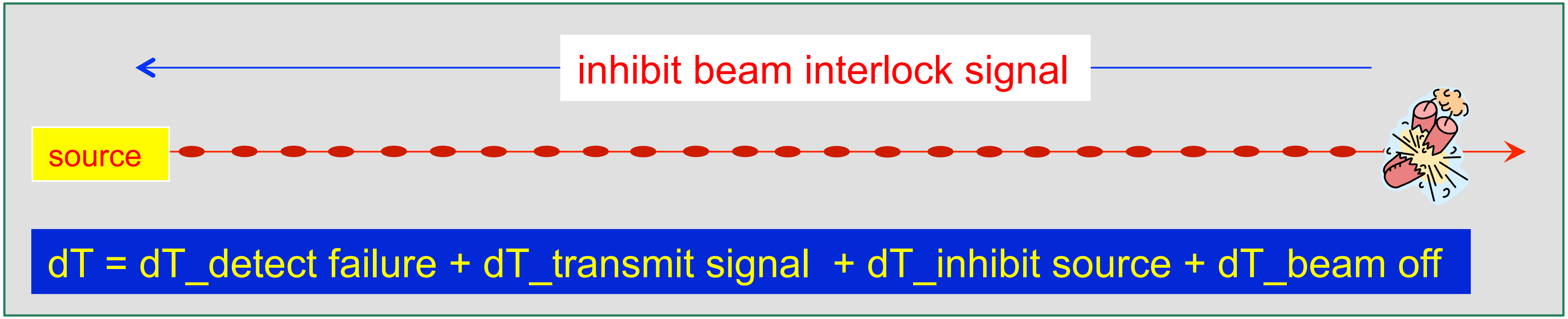
Example:

After the DTL normal conducting linac, the proton energy is 78 MeV. In case of a beam size of 2 mm radius, melting would start after about 200 µs.

Inhibiting beam should be in about 10% of this time.



L.Tchelidze



dT = dT_detect failure + dT_transmit signal + dT_inhibit source + dT_beam off