BIFROST Motion Safety System
- Implementation and Left to Do

Instrument Safety Readiness Review BIFROST

PRESENTED BY THOMAS GAHL

2025-12-05

BIFROST Motion Safety

Instrument Hazard Analysis & Handover to Motion Safety

- 3 risks in the IHA identified for operation, 5 other risks for maintenance.
- Maintenance risks are mainly in areas not accessible to user personnel.
- Transferred to Motion Safety WU of CMCA

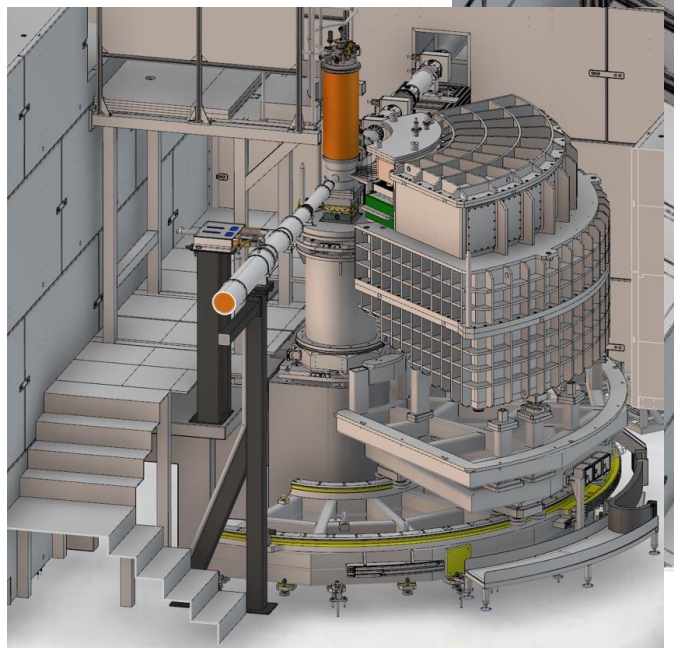
		Component			Accident description			
Hazard number	Building	Instrument System Designation	Sub-System Designation	Motion Control Subsystem	Source of Hazard	Person affected	Initiating event	Accident description
ConHaz35	D03	Beam_Transport_and_Spatial_Conditioning	Beam geometry conditioning	Attenuator Positioner	Motorized components	ESS Staff	Slits moving under maintenance	Pinched finger
ConHaz56	D03	Beam_Transport_and_Spatial_Conditioning	Beam cut off	Shutter	Motorized components	ESS Staff	Pneumatic shutter actuator	Shutter actuator may be activated while being maintained
ConHaz106	E01	Experimental_Cave	Motion Control	Detector Tank	Motorized components	ESS Staff	Tank moves into person	Person trapped between tanks and something else
ConHaz111	E01	Experimental_Cave	Motion Control	Detector Tank	Motorized components	ESS Staff	Tank moves while person maintains movement system	Pinions crush a persons finger
ConHaz124	E01	Experimental_Cave	Utilities Distribution, gases and fluids	Sample Rotation	Motorized components	ESS Staff	Person gets arm cought in sample environment tubes while rotating	Arm caught in tubes
ConHaz144	E01	Sample_Environment_Systems	Sample positioning	Sample Rotation	Motorized components	ESS Staff	Operation	Finger gets pinched in cables, or surfaces
ConHaz141	E01	Beam_Transport_and_Spatial_Conditioning	Beam delivery system	Divergence slits	Motorized components	ESS Staff	Maintenance work on jaws	Finger gets pinched
ConHaz142	E01	Beam_Transport_and_Spatial_Conditioning	Beam_Transport_and_Spatial_Conditioning	Get-lost-tube	Motorized components	ESS Staff	Maintenance work on get-lost tube	Finger gets pinched

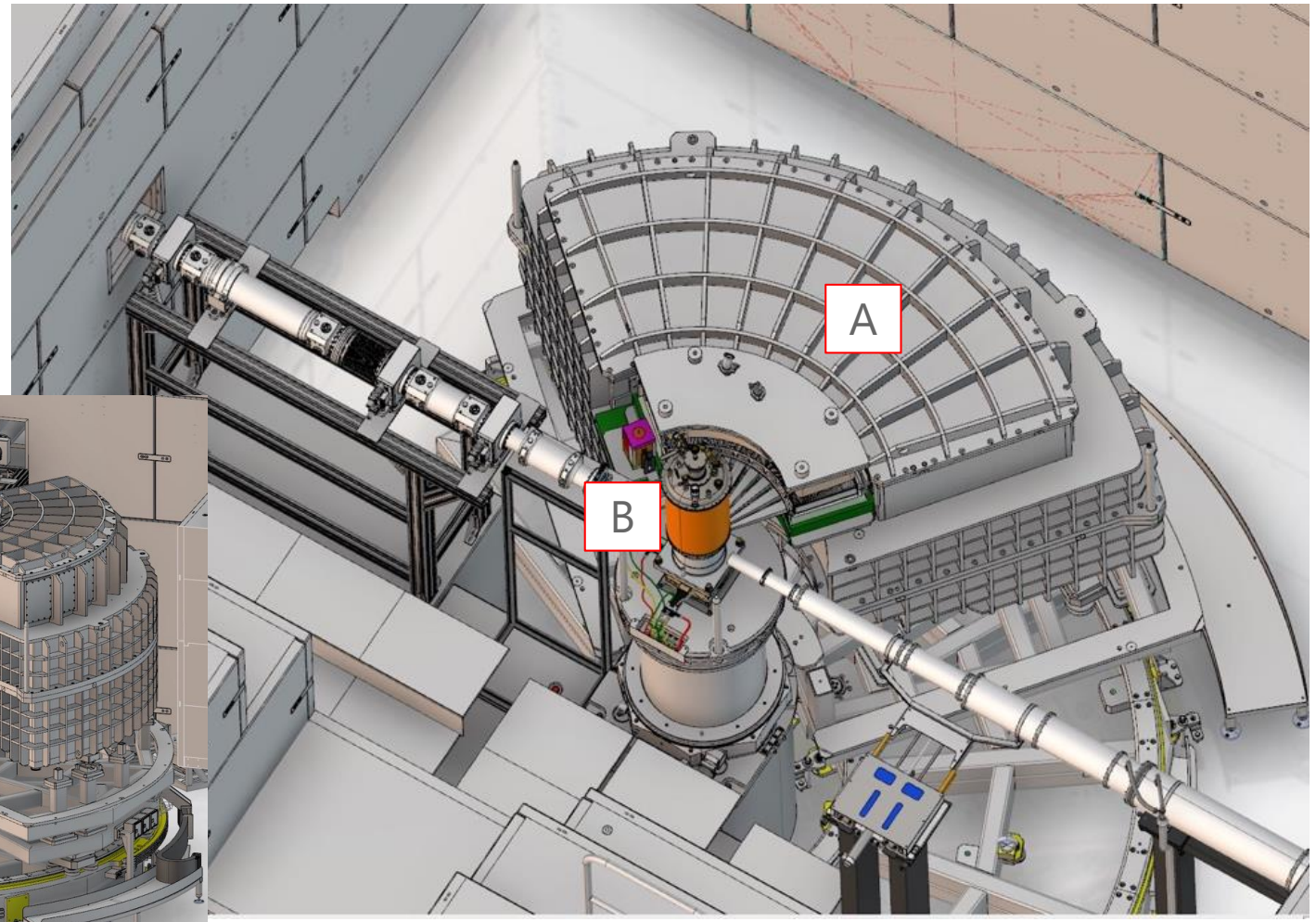
Motion Safety at BIFROST

Areas: Cave

- Accessibility:
  - Bottom floor
  - Elevated floor
  - Top floor
  - All PSS controlled

- Main Hazards:
  - A: Detector Tank Motion
  - B: Sample Positioning





Motion Safety at BIFROST

Safety Output Groups (SO)

- SO1:
  - Axes of this output group are identified as non-hazardous for operational users because they are behind guards or inside (vacuum) housings etc.
  - Special procedures for maintenance apply.
- SO2:
  - Axes of this output group are identified as hazardous for operational users.
  - Linked to special Safety function.
  - Covers also maintenance scenario.
  - Special procedures apply when maintenance work makes it necessary to override these safety functions.

MCC3

SO1

QA601/2

Pin	ID	Axis Description
11	M3	Divergence Slit 1: Left Bl.
21	M4	Divergence Slit 1: Right Bl.
31	M5	Divergence Slit 2: Left Bl.
41	M6	Divergence Slit 2: Right Bl.
51	M7	Divergence Slit 3: Left Bl.
81	M8	Divergence Slit 3: Right Bl.

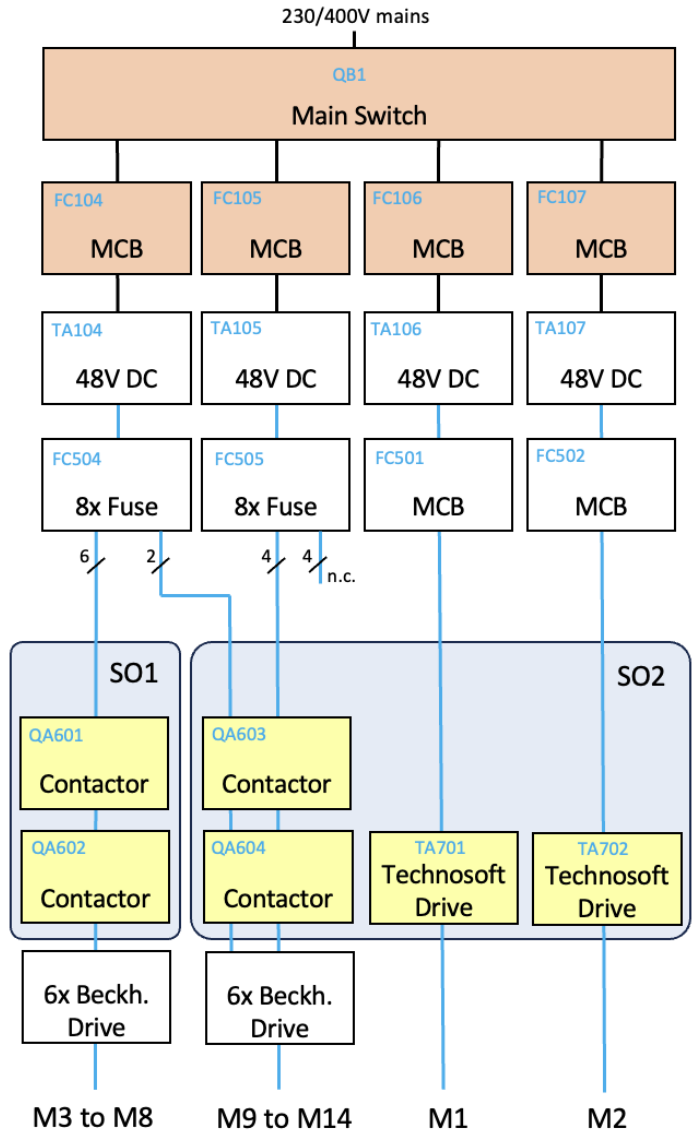
QA603/4

SO2

Pin	ID	Axis Description
11	M9	Goniometer x-axis
21	M10	Goniometer y=axis
31	M11	Spare
41	M12	Spare
51	M13	Spare
81	M14	Spare

STO: TA701 / TA702

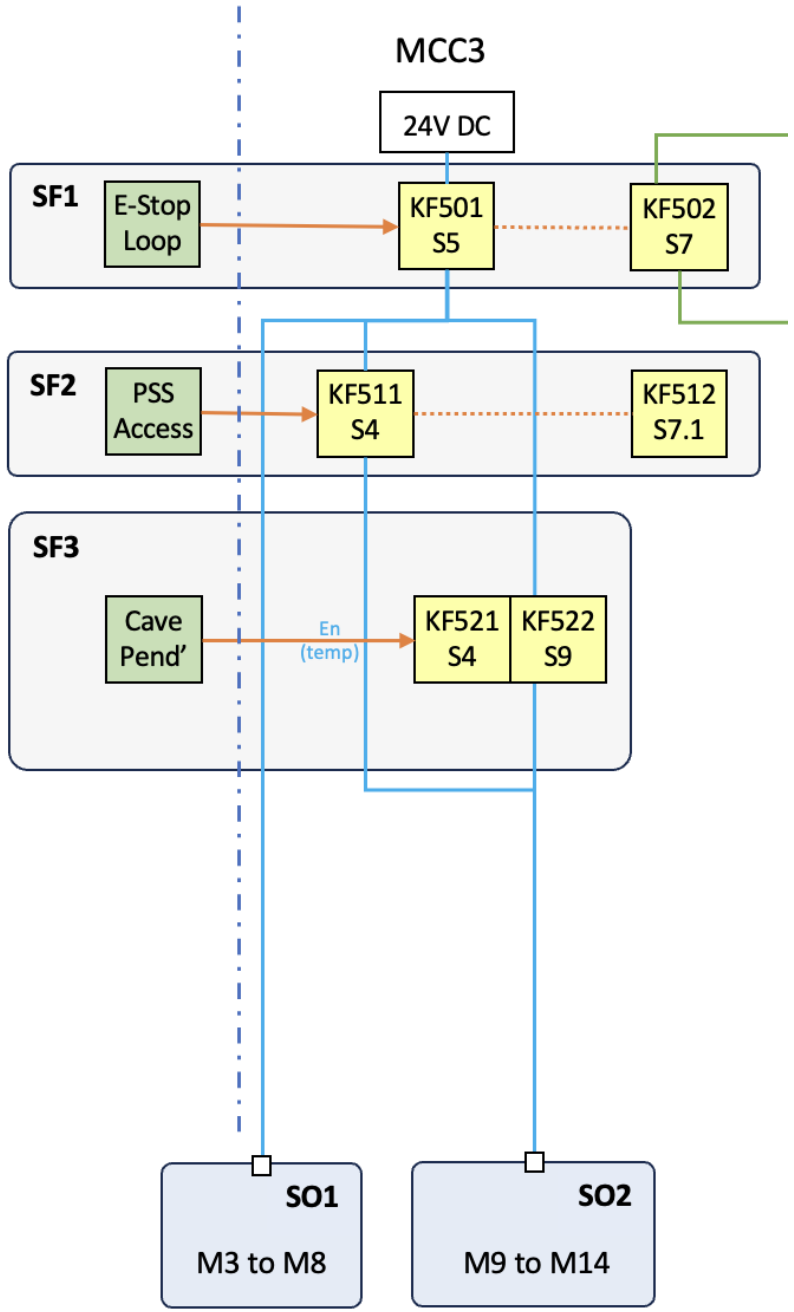
Ch	Axis	Name
1	M1	Sample Stack Rotation
2	M2	Detector Tank Rotation



Motion Safety at BIFROST

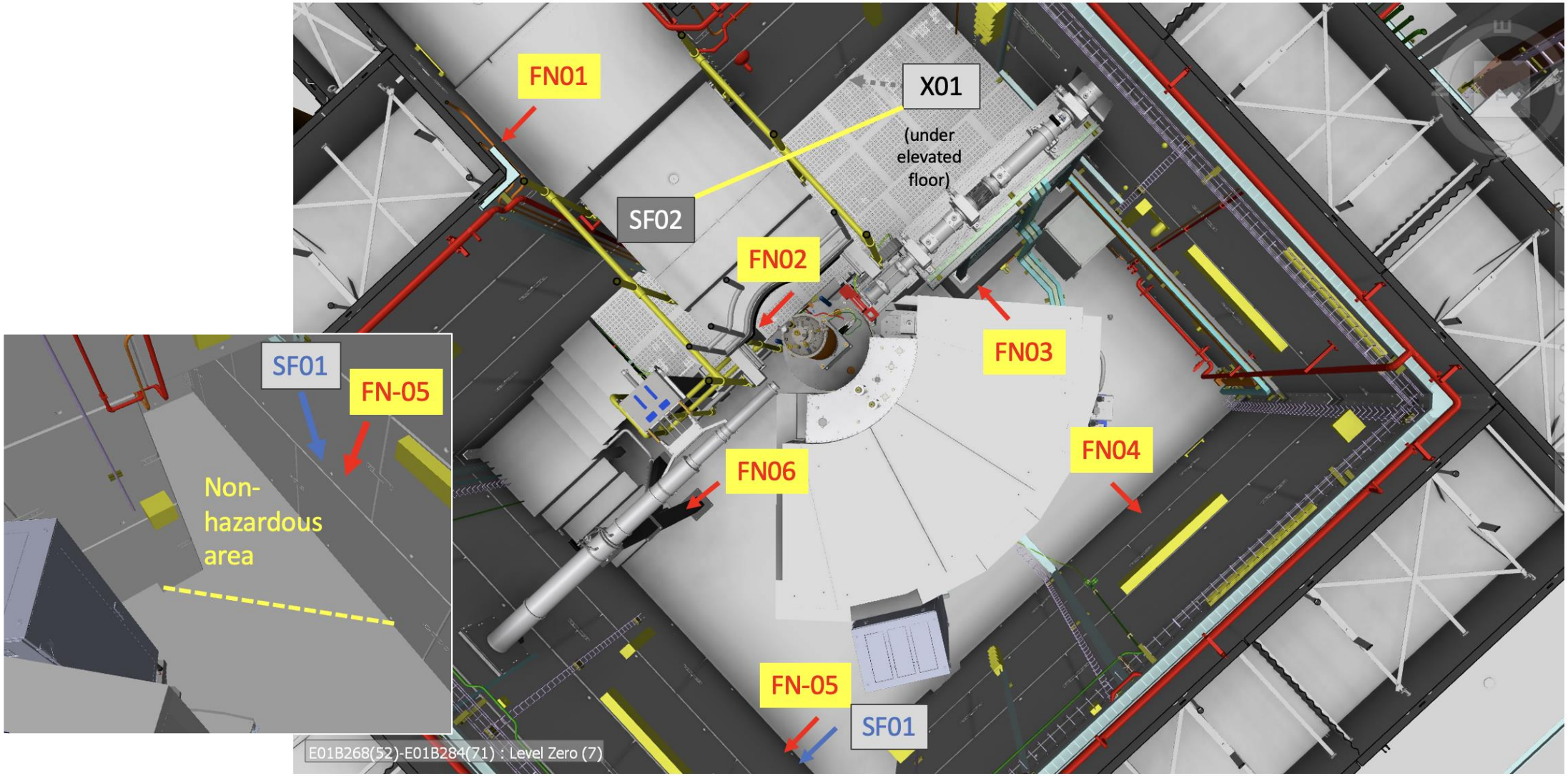
Safety Functions (SF)

- SF1: Motion E-Stop
  - Stops all axes in the cave grouped in both SO1 and SO2 except pneumatic axes (Get-lost-tube)
- SF2: PSS Access
  - Stops all axes in the cave identified as hazardous and grouped in SO2
- SF3: Cave Pendant
  - Overrides SF2 and enables all axes in SO2 for a defined time (currently 2 min); re-triggerable



Motion Safety at BIFROST

Implementation



E-Stop

FN01

Reset

SF01

Op-Control

SF02

Junction Box

X01

Validation

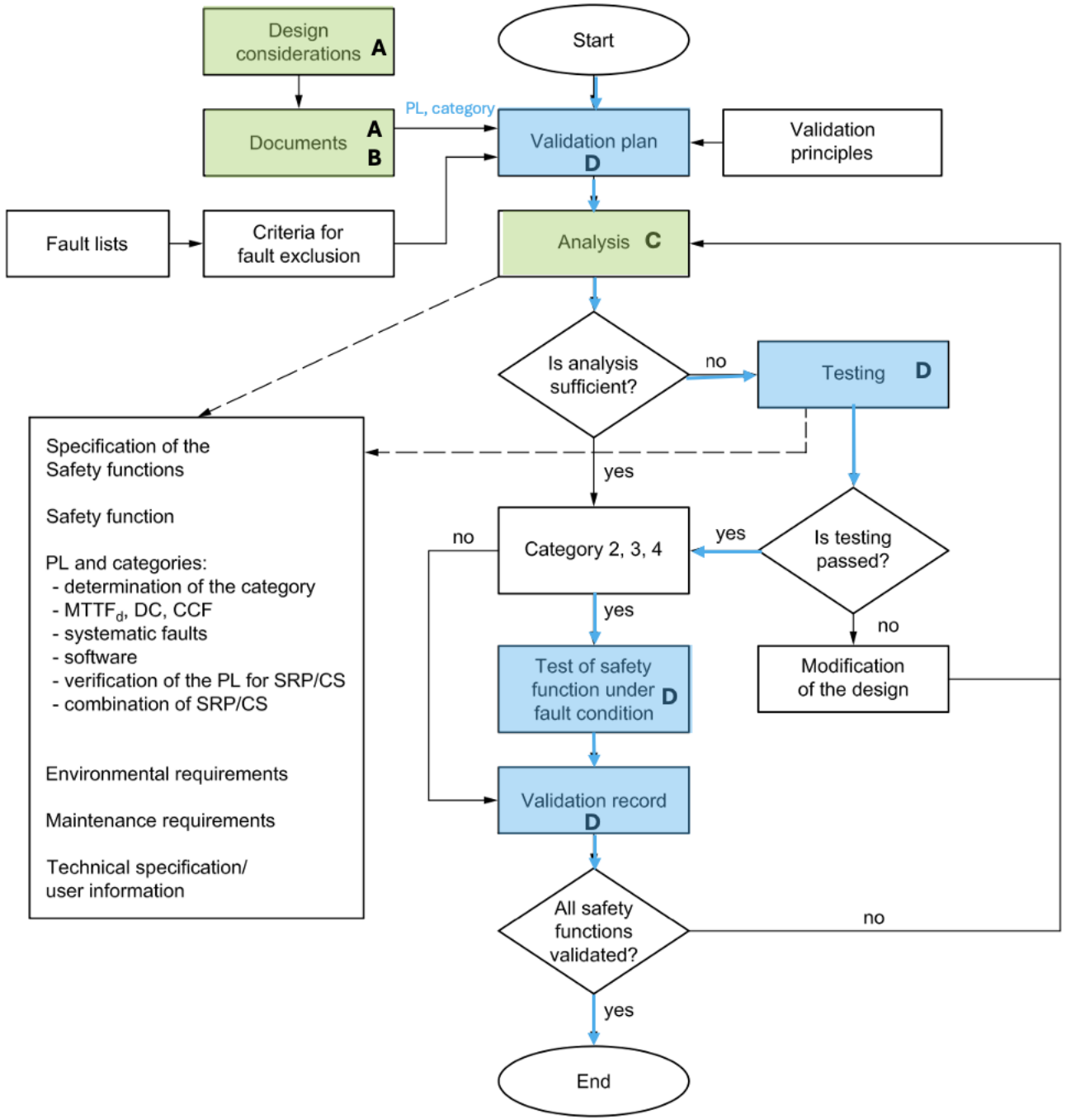
SS-EN ISO 13849-2

A. ESS-5467337 - Motion Risk Analysis of Neutron Instruments.

B. ESS-1798247 - TBL Table-of-Motion (sheet 3).

C. ESS-5944747 - Design Verification Calculation (SISTEMA) for BIFROST Motion Safety

D. ESS-5937539 - Motion Safety Validation Plan for BIFROST
ESS-5944161 - Motion Safety Validation Report for BIFROST



Validation

Validation Test Plan / Validation Test Report

Document Type: Validation Report
Document Number: ESS-5937539

Document Date: Nov 24, 2025
Revision: 1(1)
State: Preliminary

4 FUNCTIONAL TESTS

Description

The following tests prove the behaviour of the safety functions under normal operating conditions.	Fail
Requires a force of the PSS access signal, or temporary switch/bridging wires installed.	Pass
If using jumper wires, be aware that "bouncing" while connecting the second channel may be detected as a faul	N/A
No other special tools or wiring required.	

Motion E-Stop

Description

Verification of the E-Stop response and two channel response of each Stop button. Ensure Both In1/In2 switch between each step.

Step	Element	Action	On/Enabled	Off/Disabled	Pass/Fail	Notes
1	Contactors	Check all drives and STO indicate no supply power		SO1/SO2 - KF7xx Top right LED (See device list for identification Tip);	Pass	Not possible to read STO status in Technosoft drive but axis cannot be enabled. Contact Technosoft for STO
2	E-Stop FN01	Press E-Stop	E-Stop LED	KF501 In1,In2 SF01 Reset	Pass	
3	E-Stop FN01	Release E-Stop	KF501 In1,In2 SF01 Reset	KF501 Out, E-Stop LED	Pass	
4	E-Stop FN02	Press E-Stop	E-Stop LED	KF501 In1,In2 SF01 Reset	Pass	

TEST SUMMARY & APPROVAL

Validation Test Execution	[X] Approved		[ ] Rejected
Date: 2025-12-01	Signature:	Federico Rojas	
Comment:			

Validation Approval	[X] Approved		[ ] Rejected
Date: 2025-12-01	Signature:	Jacob Gillies	
Comment:	The missing diagnostics coverage on the STO inputs of Technosoft drives affects the safety function only in the the long term. Needs to be solved befor ORR. Validation is approved for current trial operation.		

Test Cases performed		Summary Findings					
		Pass	Fail	N/A	Signatures of testers	Date	Comments
1	Hardware Check	x			Federico Rojas Jakob Nilsson	2025-11-24	
2	Output Tests	x			Federico Rojas Jakob Nilsson	2025-11-24	
3	Fault Tests	x			Federico Rojas Jakob Nilsson	2025-11-24	
4	Functional Tests	x			Federico Rojas Jakob Nilsson	2025-11-24	

Validation test has been passed and approved.

Motion Safety at BIFROST

Exclusions

- MCC1:
  - Instrument Shutter (Pneumatics, behind shielding walls > access only for maintenance, trained personnel, LOTO, RAMS)
- MCC2:
  - Attenuator in-beam positioner (Pneumatics, behind shielding walls > access only for maintenance, trained personnel, LOTO, RAMS)
  - Miniature Piezo Actuators for the Sample Slit system (slow speed, low force: < 5N)
- MCC3:
  - Get-Lost-Tube positioner (Pneumatics, in cave, accessible) >> To do list

Motion Safety at BIFROST

Left to do

- Cave Pendant:
  - Currently first design version installed; without indication and operator stop button
  - Requires a skilled user to operate and understand the status.
  - Shall be replaced by the new version (LOKI) for more convenient operation before BOT.

- Get-Lost-Tube positioner
  - Currently no guards; unexpected and fast motion may occur when using the LOTO procedure.
  - In combination with the positioning of the detector tank motion may be automatically initiated (for anti-collision purposes)
  - Requires a skilled user to operate and always a RAMS/LOTO when the cave is accessible and maintenance work in the vicinity of the tube is done.
  - This is good enough to continue commissioning, but for ORR there needs to be a re-evaluation of the hazards and mitigations in place: Guard, standard control and possibly inclusion in the safety functions.

Motion Safety at BIFROST

Reference Documents

Analysis & Requirements	ESS-1075596 - BIFROST Instrument Hazard Analysis (IHA) ESS-5467337 - Motion Risk Analysis of Neutron Instruments ESS-1798247 - BIFROST Table-of-Motion, sheet 3
Design	ESS-5493491 - BIFROST Motion Control System – System Block Diagram ESS-4934946 - BIFRO Motion Control 3 ePlan ESS-5450586 - System Design Description - BIFROST Motion Control System ESS-5944747 - Design Verification Calculation (SISTEMA) for BIFROST Motion Safety
Installation	ESS-5580458 - Electrical inspection BIFROST MC Cabinets ESS-5936122 - MCA Self-Inspection Report for BIFROST Motion Control ESS-5501020 - Inspection and Test Report for BIFROST Motion Control (Electrical)
Validation	ESS-5937539 - Motion Safety Validation Plan for BIFROST ESS-5944161 - Motion Safety Validation Report for BIFROST
Operation	ESS-5669198 - Operation Manual - MCU5001: 16Ax. Motion Control Cabinet

Motion Safety at BIFROST

Applicable Directives and Standards

- EU Directive 2006/42/EC (European Machinery Directive)
- Replaced by: Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery

- SS-EN ISO 12100 Safety of Machinery – General Principles for design – Risk Assessment and Risk Reduction
- SS-EN ISO 13849 Safety of Machinery – Safety Related Parts of the Control System (Parts 1 and 2)
- SS-EN ISO 13850 Safety of Machinery - Emergency stop function - Principles for design

- SS-EN EN 60204-1 Safety of Machinery – Electrical Equipment of Machines

- SS-EN 61800-5-2 Adjustable Speed Electrical Power Drive Systems Part 5-2: Safety Requirements - Functional


Thank You!
2025-12-05

10

Additional Information

Safety Requirements Specification

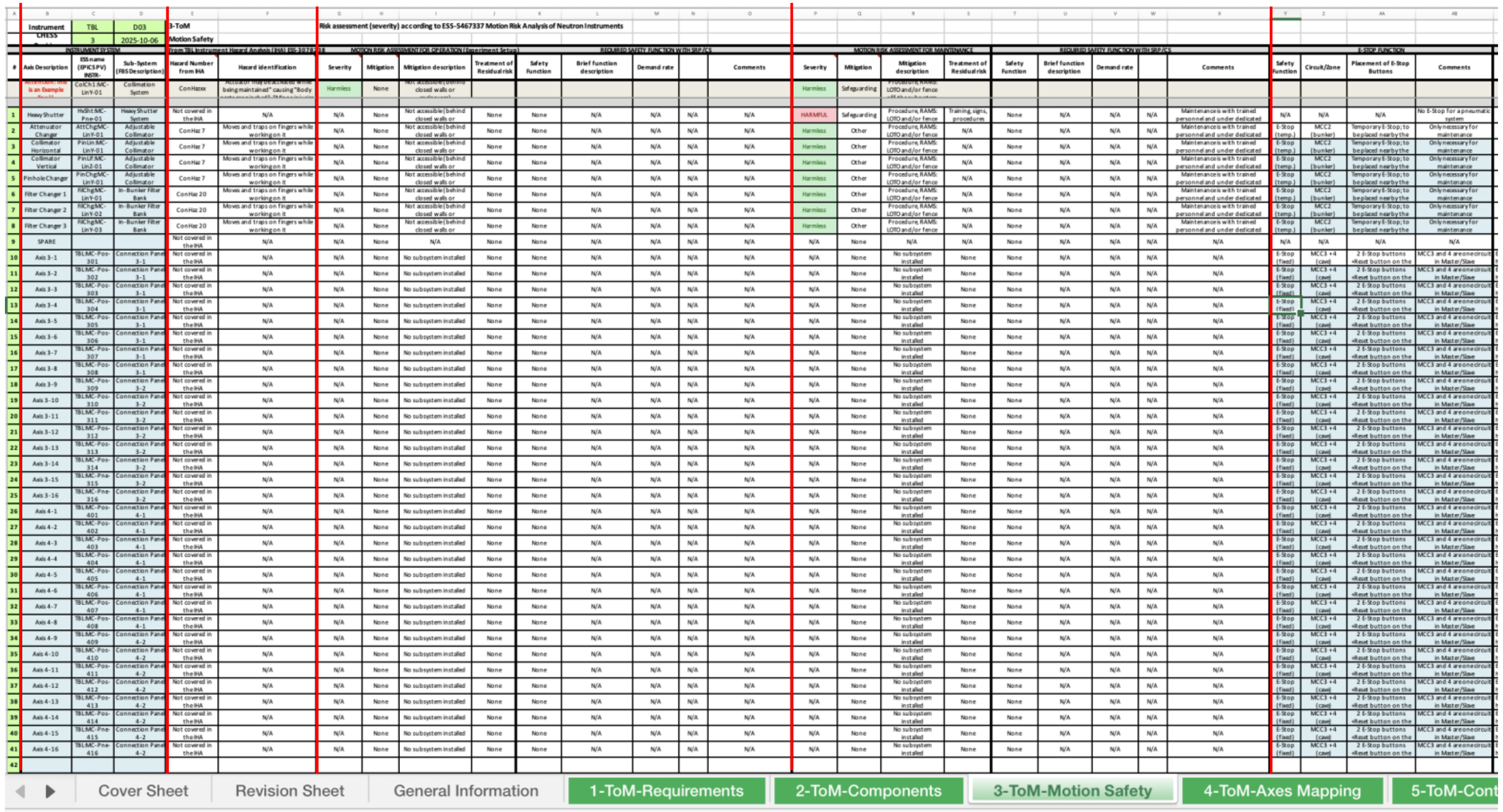
Table-of-Motion, Sheet 3

Axis description | ConHaz ID | Risk assessment & Treatment for Operation | Risk assessment & Treatment for Maintenance | E-Stop

Bunker Area

Axes listing

Cave Area



Safety Requirements Specification

Evaluation

Mitigation	Mitigation description
None	Not accessible (behind closed walls or enclosures)

Severity	Mitigation	Mitigation description	Treatment of Residual risk
HARMFUL	Safeguarding	Procedure, RAMS: LOTO and/or fence off	Training, signs, procedures
Harmless	Other	Procedure, RAMS: LOTO and/or fence off	N/A

ConHaz 7 + 20

Operation

Maintenance

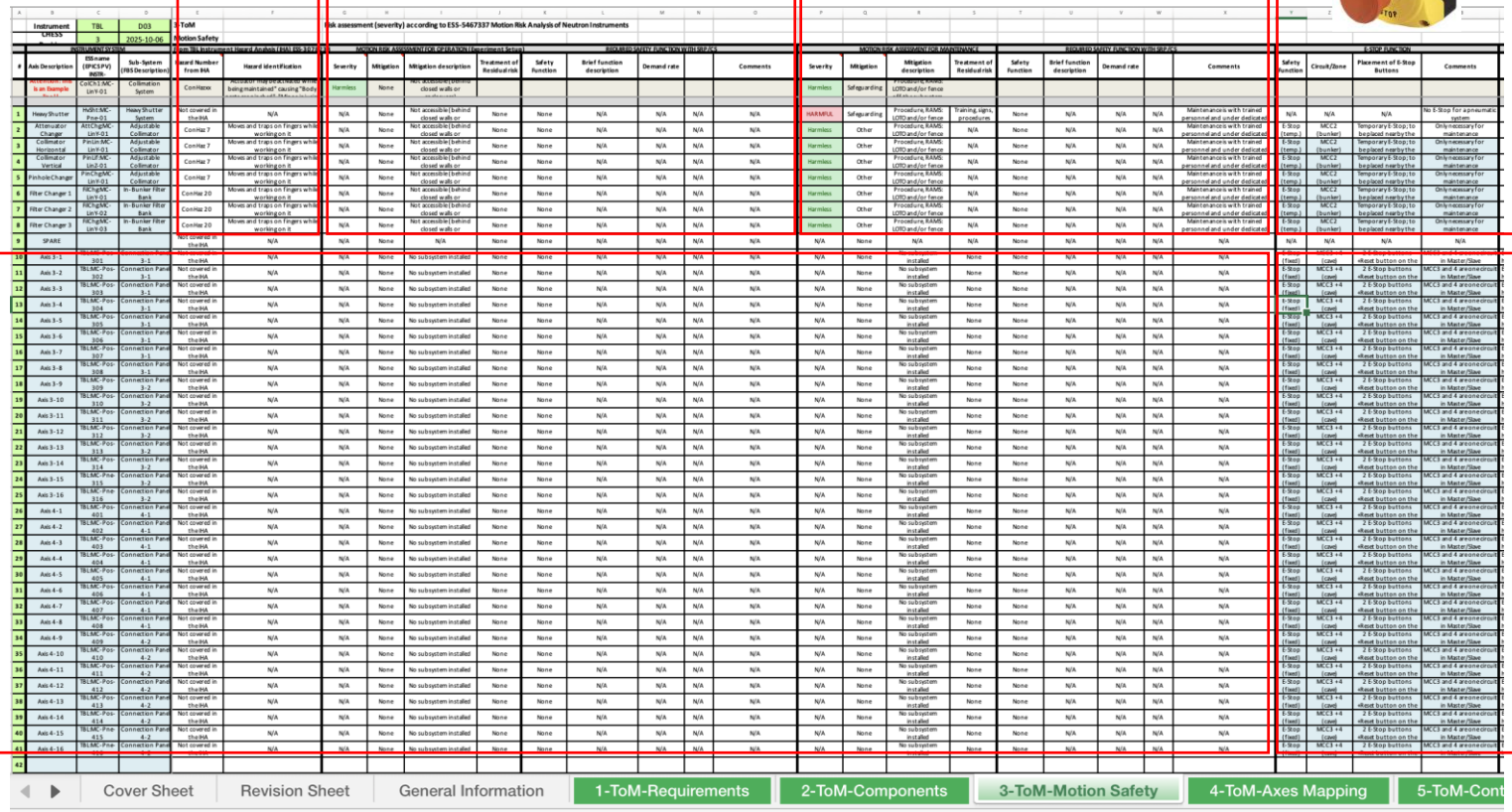
Circuit/Zone	Placement of E-Stop Buttons
MCC2 (bunker)	Temporary E-Stop; to be placed nearby the motion

Bunker Area

Mitigation	Mitigation description
None	No subsystem installed

Cave Area

Circuit/Zone	Placement of E-Stop Buttons
MCC3 + 4 (cave)	2 E-Stop buttons +Reset button on the cave table

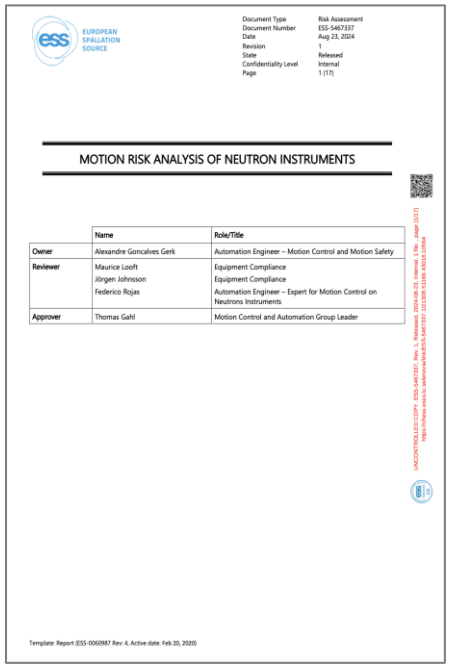


Risk Analysis & Treatment

ESS-5467337 - Motion Risk Analysis of Neutron Instruments

- Limits of System
  1. Area: Motion Safety focusses on areas accessible to instrument users (typically in the cave).
  2. Life phases: Experiment Setup & Local Maintenance considered.

Life phases	Cave (User Access, controlled by PSS)	Cave (Service & Maintenance Access, controlled by PSS)	Beam Line, Bunker (Service & Maintenance Access, controlled by procedures)
TBL Areas	TBL Cave	TBL Cave	TBL In-bunker area
Installation, commissioning and testing	excluded	excluded	excluded
Experiment Run	no risks	no risks	no risks
Experiment Setup	included	N/A (no access)	N/A (no access)
Local maintenance	included	included	excluded
External maintenance (in workshop)	excluded	excluded	excluded


MOTION RISK ANALYSIS OF NEUTRON INSTRUMENTS

ESS-5467337

Risk Analysis & Treatment

ESS-5467337 - Motion Risk Analysis of Neutron Instruments

- Simplified approach for hazard analysis and mitigation.
  1. Motion Safety focusses on areas accessible to instrument users (typically in the cave).
  2. Only two levels defined following the severity path; required Performance Levels a/b and c/d.

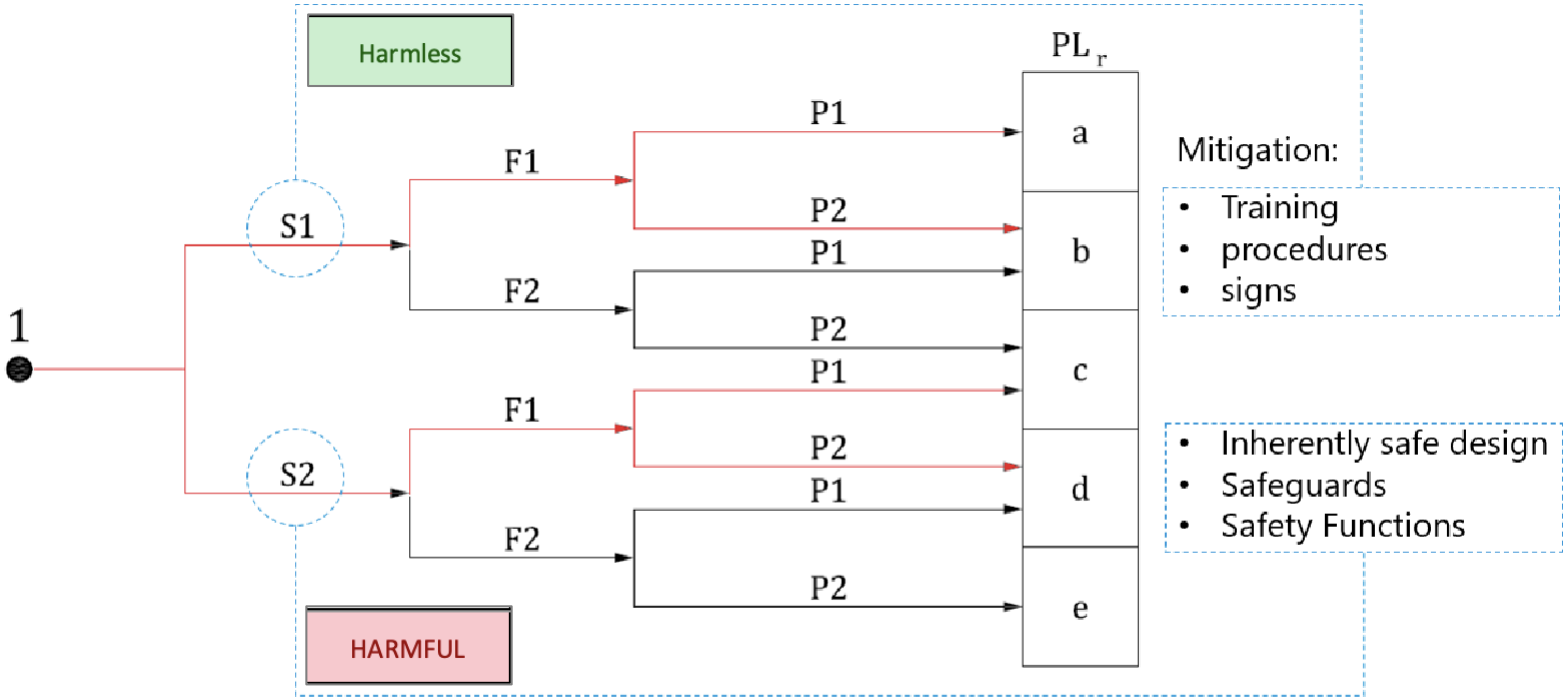
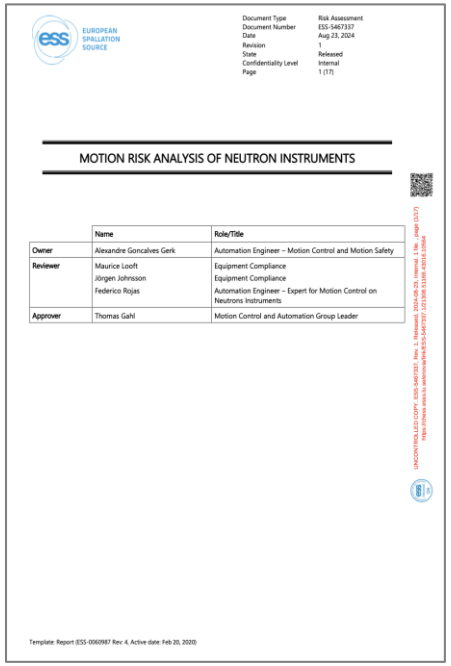


Figure 8 - Risk evaluation


MOTION RISK ANALYSIS OF NEUTRON INSTRUMENTS

ESS-5467337

E-Stop Design

Design Principle

- Modularity: Define different areas; match the area with the respective control cabinets; this includes standardised circuits in the cabinet and and a Master/Slave hierarchy between (if applicable).
- Scalability: A scalable number of fixed installed E-Stop buttons + one Reset button in the areas accessible to normal users (i.e. the cave).
- Performance Level d as a matter of principle.

- Currently Stop Category 0 (STO); design work is ongoing for Stop Category 1 (SS1).

EN 60204-1	**EN 61800-5-2**
Stop category 0	Safe torque off (STO)
Stop category 1	Safe stop 1 (SS1)
Stop category 2	Safe stop 2 (SS2)

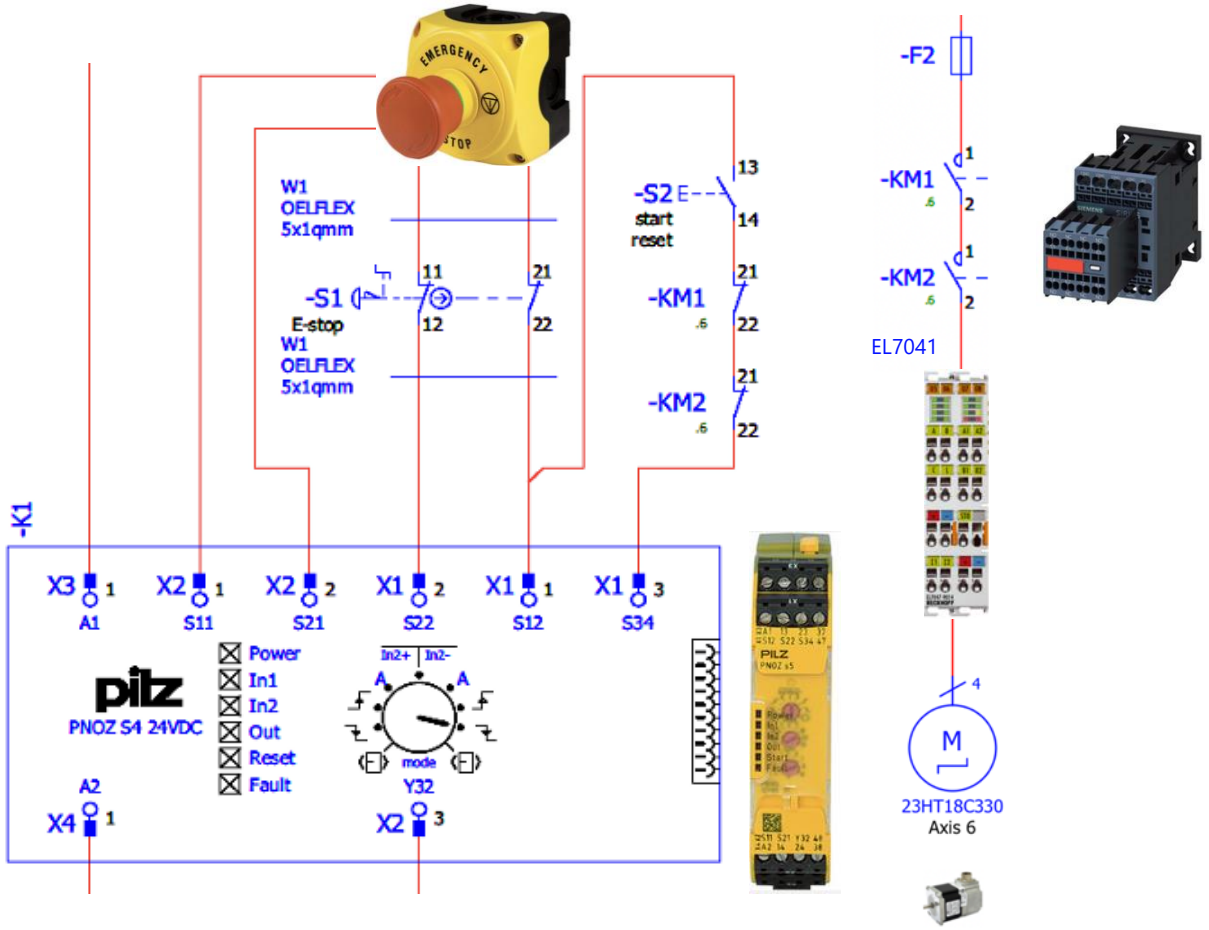
E-Stop Design

Design of E-Stop Circuit

Principle: Contactors are cutting power to the stepper motor drives

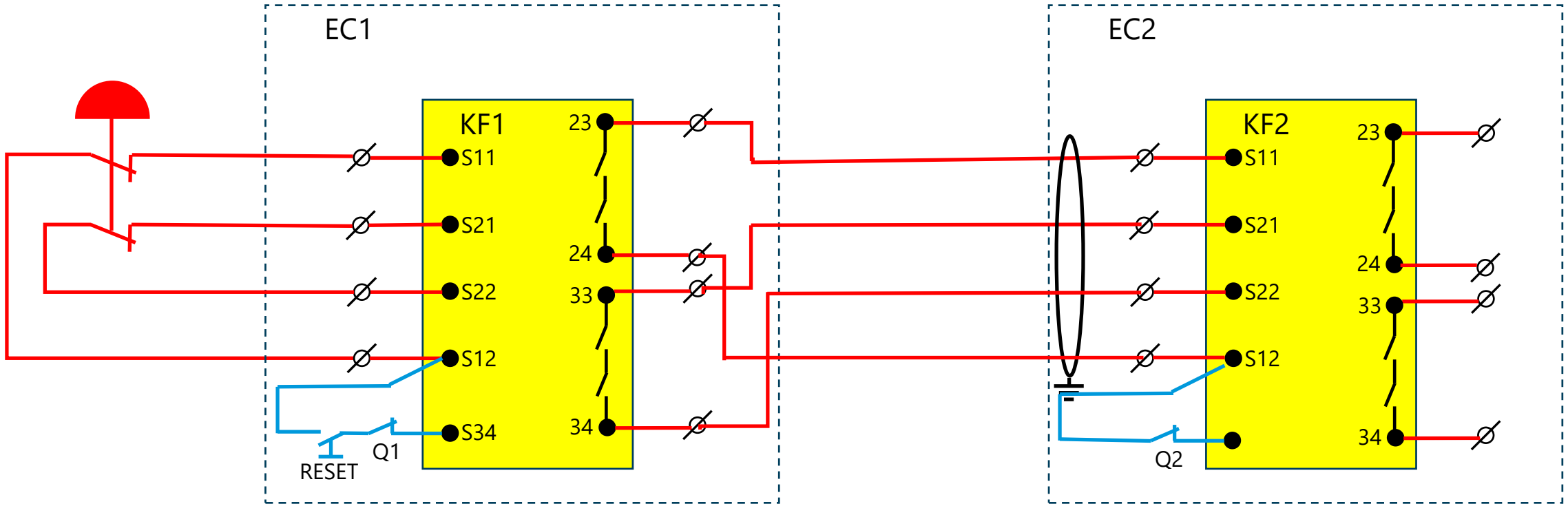
Performance Level d: How to achieve?

- Safety Relay
  - 2 channels
  - With detection of shorts across contacts
  - With detection of shorts to Earth
- Safety contactors
  - Siemens safety contactor type 3RH2262-2BB40
  - 2 in series
  - NC contact in feedback loop



E-Stop Design

Master / Slave



E-stop input

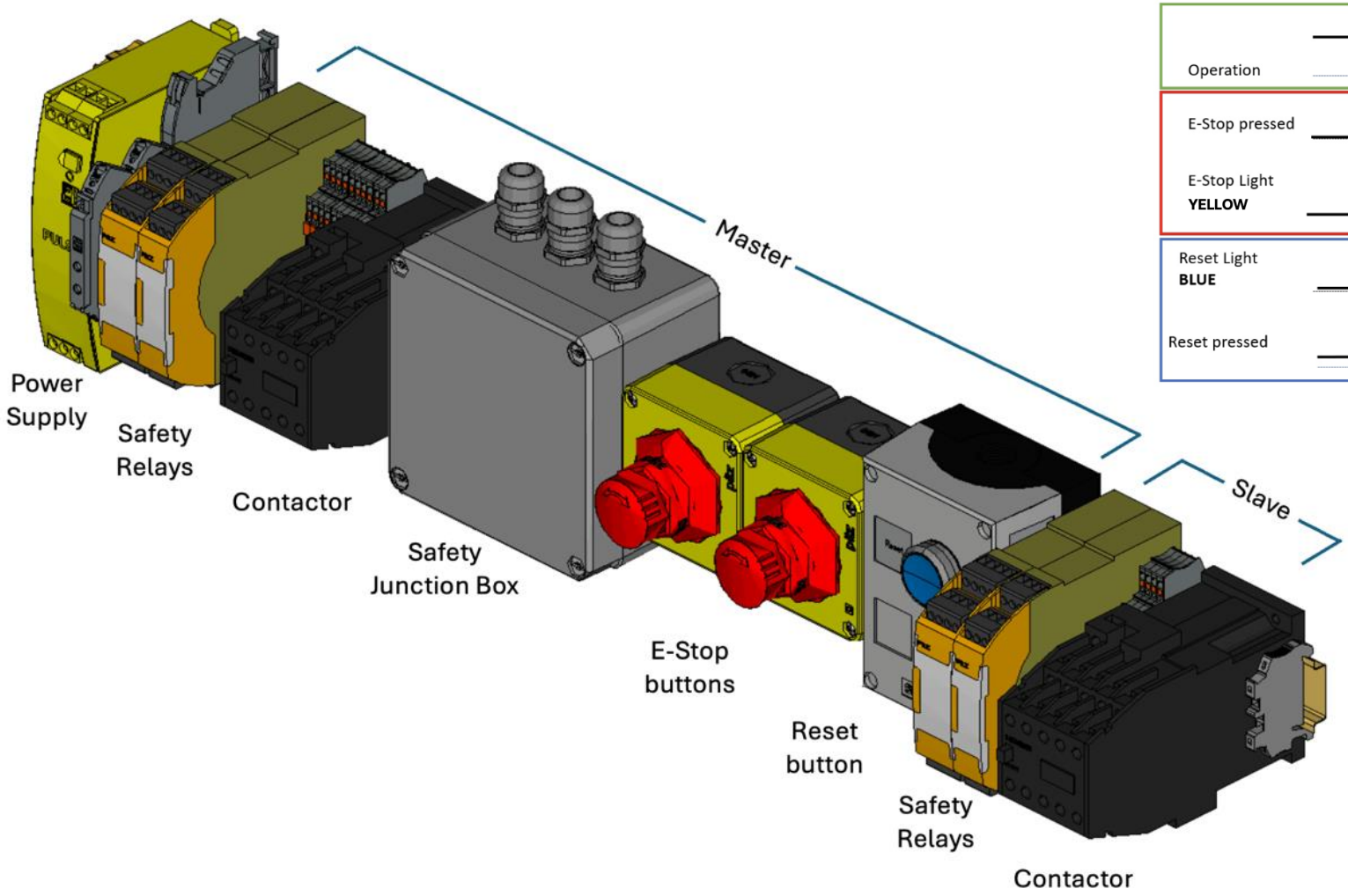
- Dual-channel operation with detection of shorts across contacts.
- Earth fault detection in circuit.
- Reset with falling edge

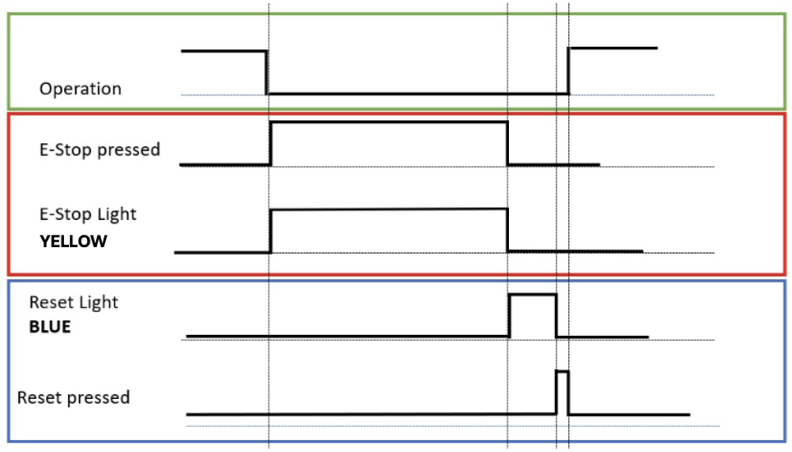
Slave input

- Dual-channel operation with detection of shorts across contacts.
- Earth fault detection in circuit.
- No special cable necessary (just shielded)
- Auto-Reset

Design Verification

Functional Verification – Test Bench





Design Verification

SISTEMA calculation

The SISTEMA analysis for the Motion Safety – E-Stop Circuit has been successfully completed according to EN ISO 13849-1:2023 and ISO 13850:2015.

- The required Performance Level determined by the risk graph was PLd, with a calculated PFH = 1.45E-7 [1/h]; PLd was achieved.
- All subsystems (Pilz E-Stop Boxes, Pilz PNOZ relay, and Siemens SIRIUS contactor relays) demonstrated compliance with relevant requirements for Category 3 or 4 architectures, with high MTTFD values, diagnostic coverage ≥ 90%, and fulfilled Common Cause Failure (CCF) measures.
- No warnings or non-conformities were reported in SISTEMA's evaluation.
- Design of the Motion Safety E-Stop function meets the required safety integrity level.