LOKI Motion Safety System
- Implementation and Left to Do

Instrument Safety Readiness Review LOKI

PRESENTED BY THOMAS GAHL

2025-12-05

LOKI Motion Safety

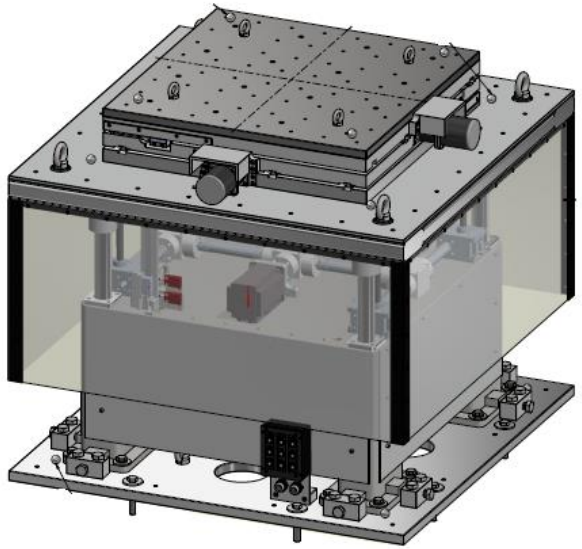
Instrument Hazard Analysis & Handover to Motion Safety

- 6 risks in the IHA identified for operation.
- All in the cave; all related to the Sample Stack.
- Maintenance risks are mainly in areas not accessible to user personnel.
- Transferred to Motion Safety WU of CMCA.

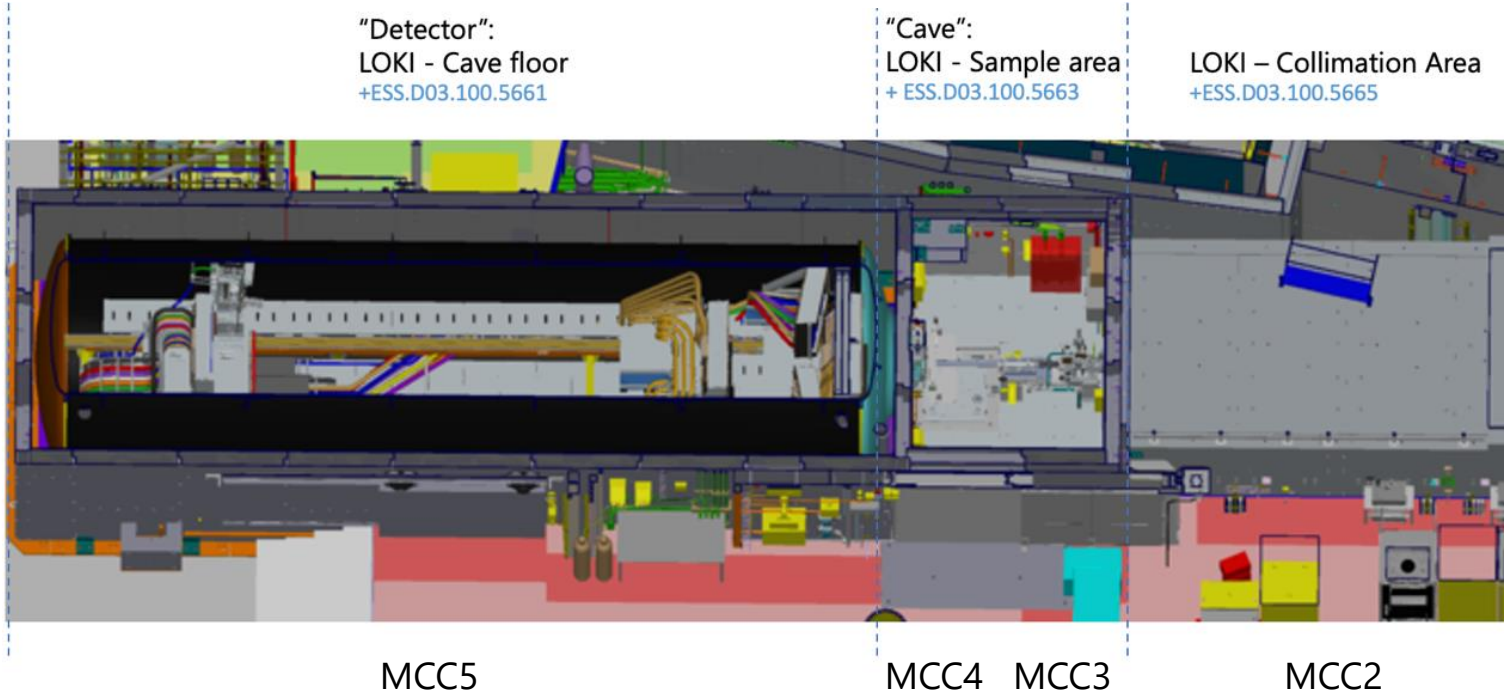
Hazard number	Building	Instrument Area	Instrument System Designation	Equipment	Hazard Category (mechanical, chemical, ergonomic...)	Source of Hazard	ESS Staff	Users	Visitors	Initiating event	Accident description
ConHaz58	D03	Sample Area	Sample Exposure System	Sample Stack	HazMechanical	Motorized components	X	X		Driving sample stack in lowest position and with ramp in lowered position crushes foot	ramp in lowered position does not meet minimal stopping distances - foot crushed
ConHaz60	D03	Sample Area	Sample Exposure System	Sample Stack	HazMechanical	Motorized components	X	X	X	Remote operation of UNLOADED sample stack whilst someone is in area	Person without control of equipment exposed to moving machinery
ConHaz61	D03	Sample Area	Sample Exposure System	Sample Stack with Trolley attached	HazMechanical	Motorized components	X	X	X	Operation of sample stack with sample trolley with body part located in between snout column or detector nose cone	Crushing hazard
ConHaz62	D03	Sample Area	Sample Exposure System	Sample Stack with unknown SE equipment	HazMechanical	Motorized components	X	X	X	Local operation of sample stack with sample trolley loaded with unknown SE equipment that presents a	Crushing hazard
ConHaz63	D03	Sample Area	Sample Exposure System	Sample Stack with unknown SE equipment	HazMechanical	Motorized components	X	X	X	Remote operation of sample stack with sample trolley loaded with unknown SE equipment that presents a	Crushing hazard
ConHaz64	D03	Sample Area	Sample Exposure System	Sample Stack with Trolley attached	HazMechanical	Motorized components	X	X	X	Sample trolley (or SE equipment) on Sample stack is driven into detector vessel or snout	Damage to vacuum vessels, fractured parts

LOKI Motion Safety

Areas: Cave & Detector Area



- Accessibility Cave:
  - Motorized door at the side.
  - Very compact area, no safe area inside the cave.
- Accessibility Detector Area:
  - Door in the shielding + flange for access to the vacuum tank.
  - Access only for maintenance.
- PSS Access Control is for both areas
- Main Hazard:
  - Sample Stack (Cave).

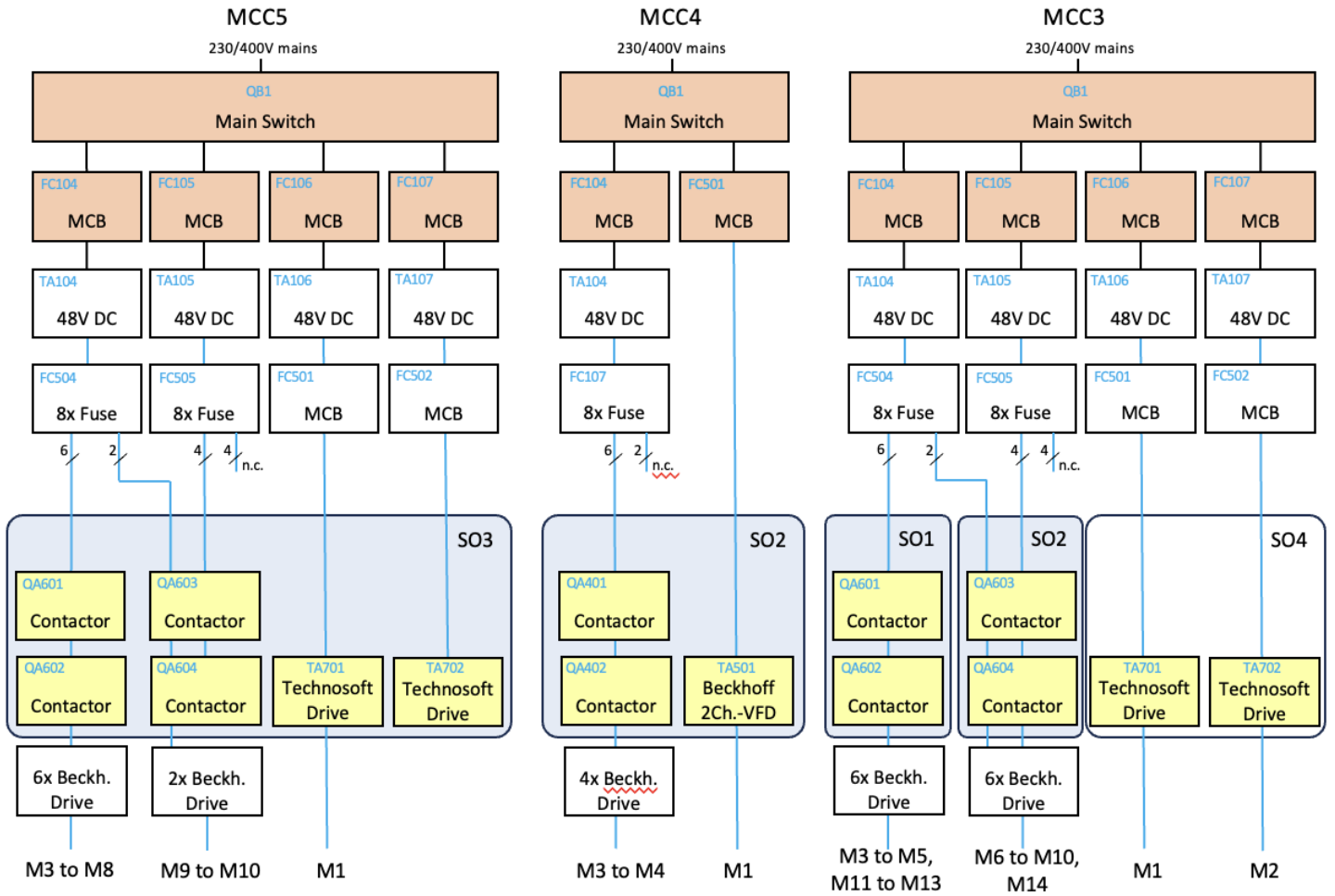


LOKI Motion Safety

Safety Output Groups (SO)

- SO1 (in cave):
  - Axes identified as non-hazardous for operational users (behind guards or inside (vacuum) housings etc.)
  - Special procedures for maintenance apply.
- SO2 (in cave):
  - Axes 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.
- SO3 (in detector tank):
  - No user access in operation, but more service-friendly solution for maintenance implemented.

LOKI Motion Safety System – Motive Power & Safety Output Groups **(SO)**



LOKI Motion Safety

Safety Output Groups (SO)

MCC3

SO1

QA601/2

Pin	ID	Axis Description
11	M3	In-Beam: Monitor M2 Halo
21	M4	In-Beam: Monitor M3 Trans.
31	M5	In-Beam: Laser Mirror
41	M11	Sample Cell Rotation
51	M12	Spare
81	M13	Spare

SO2

QA603/4

Pin	ID	Axis Description
11	M6	Sample Goniometer x
21	M7	Sample Goniometer y
31	M8	Sample Rotation Stage
41	M9	Linear Sample Changer
51	M10	Ancilliary axis 1 - Smple Area
81	M14	Spare

STO – SO4 in MCC2

Ch	ID	Axis Description
1	M1	Collimator Selector 1
2	M2	Collimator Selector 2

MCC4

SO2

STO

Drive	ID	Axis Description
1	M1	Sample stack linear z main
2	M2	Spare

QA401/2

Pin	ID	Axis Description
11	M3	Sample stack linear x
21	M4	Sample stack linear y
31	M5	Spare
41	M6	Spare
51		Not connected
81		Not connected

MCC5

SO3

STO

Drive	ID	Axis Description
1	M1	Detector Carriage
2	M2	Spare

QA601/2

Pin	ID	Axis Description
11	M3	Detector Beamstop x adjust
21	M4	Detector BmStop y adjust
31	M5	Detector BmStop 1 - M4
41	M6	Detector BmStop 2 - 20x25
51	M7	Detector BmStop 3 - 50x60
81	M8	Detector BmStop 4 - 65x75

QA603/4

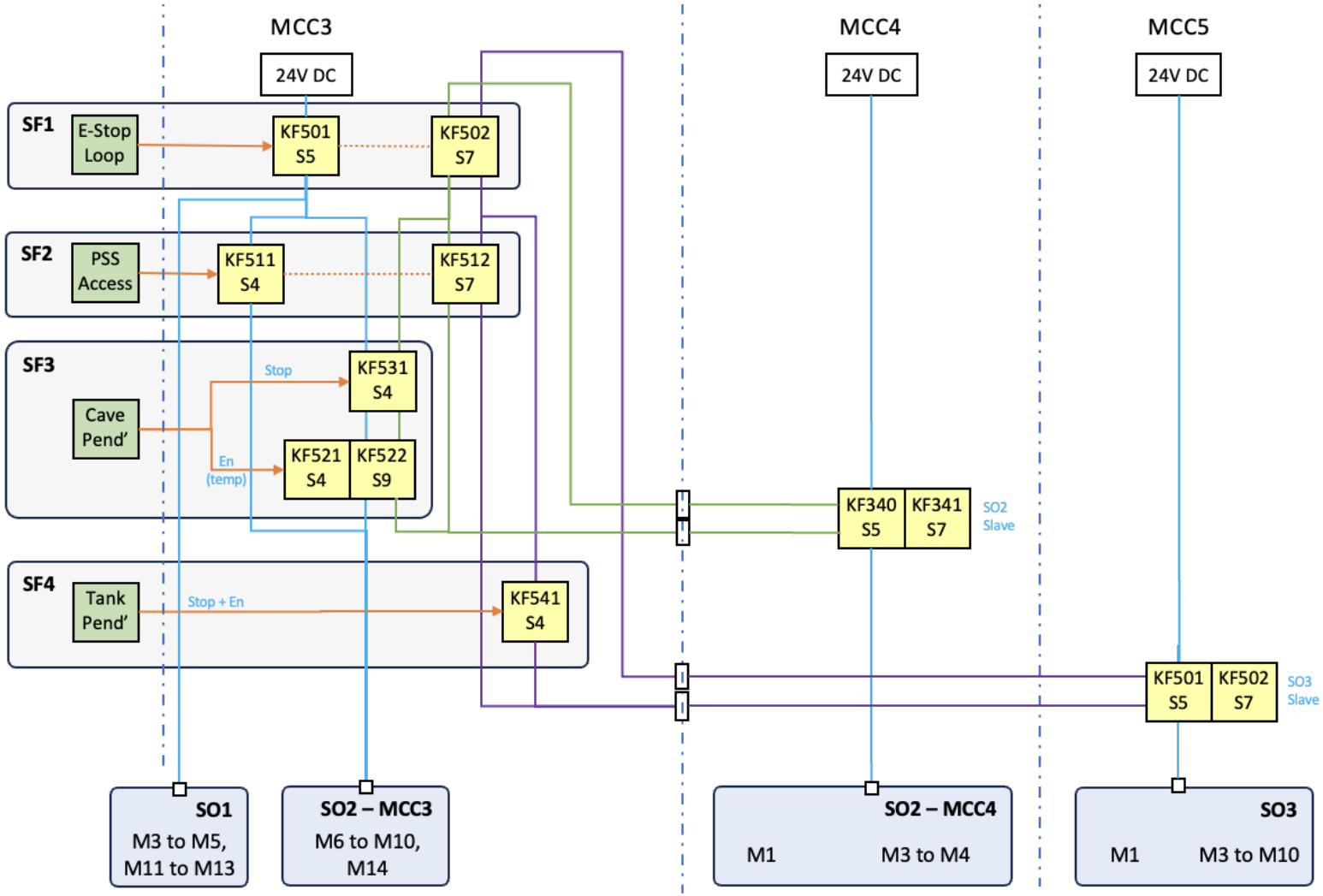
Pin	ID	Axis Description
11	M9	Detector BmStop 5-100x105
21	M10	Spare
31		Not connected
41		Not connected
51		Not connected
81		Not connected

Safety Function	SO1	SO2	SO3
SF1 – Motion E-Stop	X	X	X
SF2 – PSS Access		X	X
SF3 – Access Override Cave		X	
SF4– Access Override Tank			X

LOKI Motion Safety

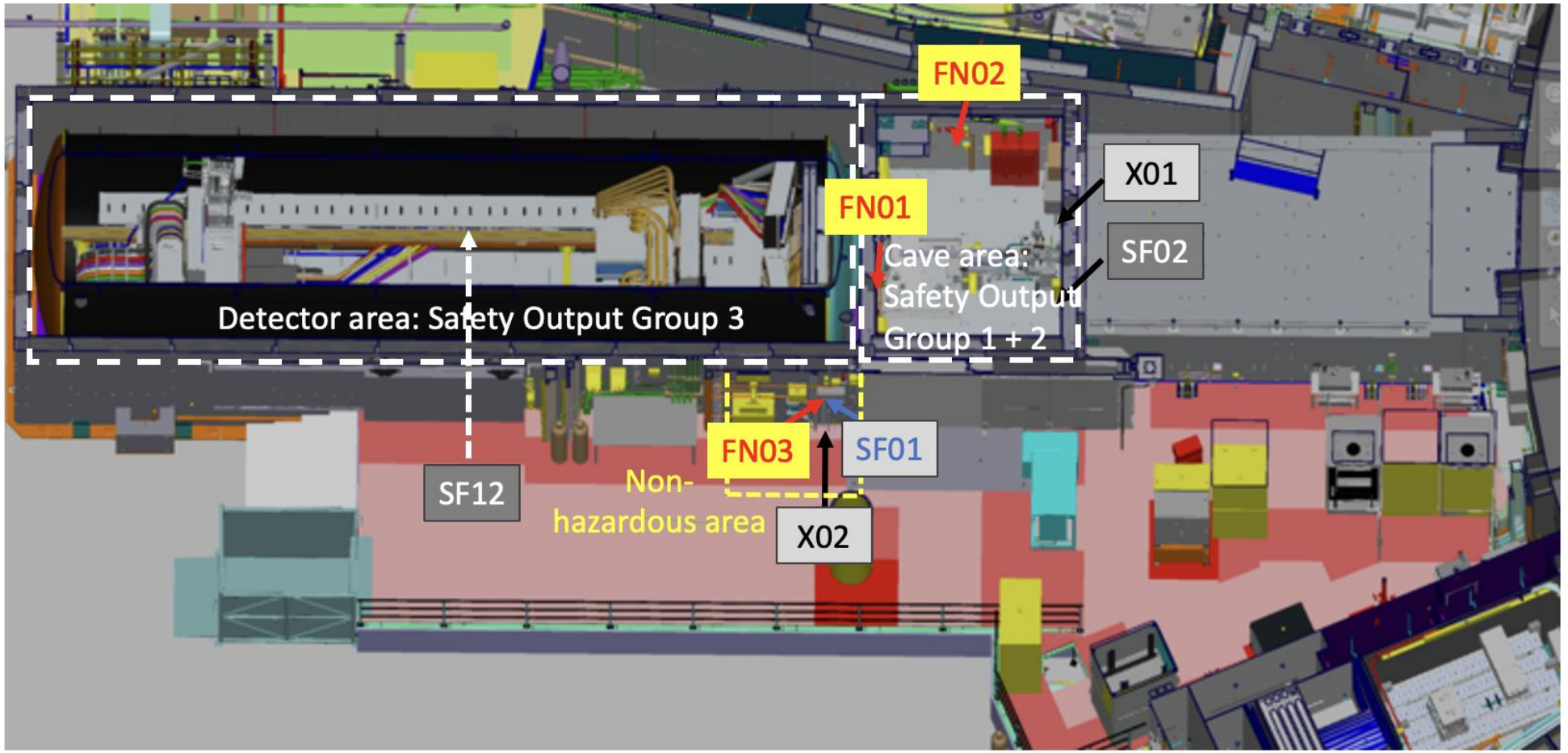
Safety Functions (SF)

- SF1: Motion E-Stop
  - Stops all axes in the cave and detector area.
- SF2: PSS Access
  - Stops all axes in the cave and detector area identified as hazardous and grouped in SO2 and SO3.
- SF3: Cave Pendant
  - Overrides SF2 and enables all axes in SO2 for a defined time (currently 2 min); re-triggerable
- SF4: Detector Tank Pendant
  - Same as SF3 but for SO3 in the tank, no timer.



LOKI Motion Safety

Implementation



E-Stop

FN01

Reset

SF01

Op-Control

SF02

Junction Box

X01

Validation

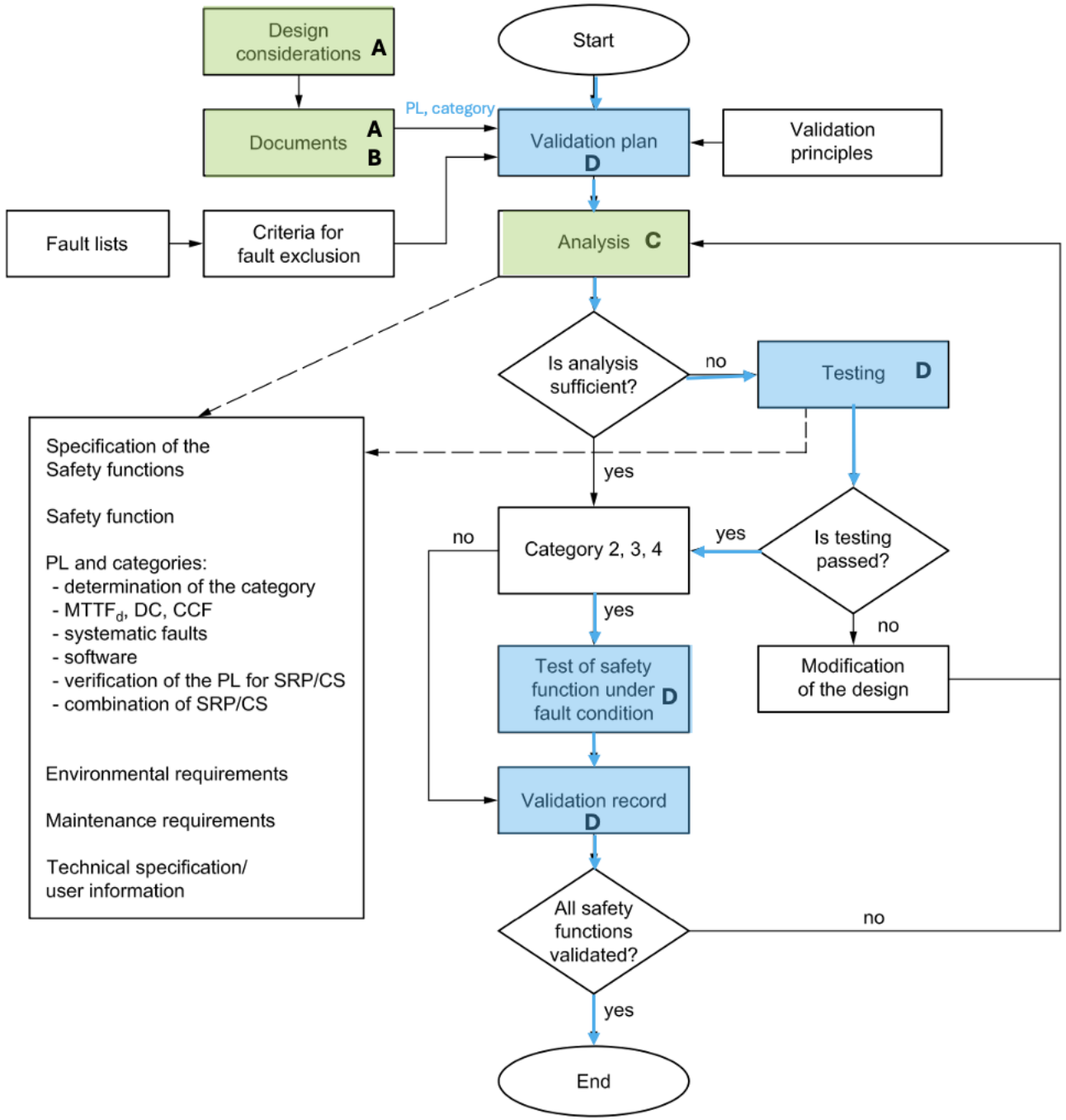
SS-EN ISO 13849-2

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

B. ESS-0114726 - LOKI ToM, Table-of-Motion, sheet 3

C. ESS-5944740 - Design Verification Calculation (SISTEMA) for LOKI Motion Safety

D. ESS-5944732 - Motion Safety Validation Plan for LOKI
ESS-5944738 - Motion Safety Validation Report for LOKI



LOKI Motion Safety

Validation Test Plan / Validation Test Report

Document Type: Validation Report
Document Number: ESS-5937539

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

8 FUNCTIONAL TESTS

Description	
The following tests prove the behaviour of the safety functions under normal operating conditions.	Fail
Requires temporary switch/bridging wires installed to simulate external signals.	Pass
If using jumper wires, be aware that "bouncing" while connecting the second channel may be detected as a fault.	N/A
No other special tools or wiring required.	
All devices are located in the field or inside MCC3 unless otherwise specified.	
Not all steps check all possible LEDs. Any listed indicators are important and must be checked.	

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	Other	Pass/Fail	Notes
0	Pre-Check	Ensure safety relays in initial state	Safety Relay indicators as per LED Chart			Pass	
1	Contactors	Confirm all contactors/ Relays are off/disabled		QA601-604 MCC4 KF340 MCC5 KF501		Pass	
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	

Validation test has been passed and approved.

Document Type: Validation Report
Document Number: ESS-5937539

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

TEST SUMMARY & APPROVAL

Validation Test Execution [X] Approved [ ] Rejected
Date: 2025-12-03 **Signature:** Kristina Jurišić
Comment:

Validation Approval [X] Approved [ ] Rejected
Date: 2025-12-03 **Signature:** Jacob Gillies
Comment:

Test Cases performed		Summary Findings					
		Pass	Fail	N/A	Signatures of testers	Date	Comments
1	Hardware Check	x			Kristina Jurišić	2025-12-03	
2	Output Tests MCC5	x			Kristina Jurišić Mohammed Addou Krai	2025-12-03	
3	Fault Tests MCC5	x			Kristina Jurišić Mohammed Addou Krai	2025-12-03	
4	Output Tests MCC4	x			Kristina Jurišić Mohammed Addou Krai	2025-12-03	
5	Fault Tests MCC4	x			Kristina Jurišić Mohammed Addou Krai	2025-12-03	
6	Output Tests MCC3	x			Kristina Jurišić Mohammed Addou Krai	2025-12-03	
7	Fault Tests MCC3	x			Kristina Jurišić Mohammed Addou Krai	2025-12-03	
8	Functional Tests	x			Kristina Jurišić Mohammed Addou Krai	2025-12-03	

LOKI Motion Safety

Exclusions

- MCC1:
  - Instrument Shutter (Pneumatics, in the bunker > access only for maintenance, trained personnel, LOTO, RAMS).
- MCC2:
  - Collimation Slit Sets and Changers (in a vacuum housing + behind shielding walls > access only for maintenance, trained personnel, LOTO, RAMS), provision to temporarily connect an operator stop.
- MCC3:
  - Window Guard (Pneumatics, in cave, accessible but shut down by PSS; operation only for maintenance, trained personnel, LOTO, RAMS).

LOKI Motion Safety

Left to do

- Current situation
  - Largest generic hazard is the “Unexpected Startup/Motion of Axes” while people are in the cave.
  - This is addressed by PSS Access and Override/Enable functions.
  - This is good and safe enough for skilled and trained users familiar with the system.
  - Setup of the cave with enclosures, boxes, shelves etc. is ongoing; not all subsystem options are installed yet.

- Final evaluation of the Cave for User Operation (ORR)
  - New evaluation and decisions on mitigations in the order proposed by SS-EN ISO 12100 / 13849:
    - Mechanical Measures (guards, fences etc.).
    - Implementations in the standard control system (if any).
    - Implementations in the SRP/CS (other than the ones already implemented).
    - Training, signs and procedures (to avoid for user operation).

- General Comment
  - Motion Safety System is currently a stand-alone system to cover the motion related hazards.
  - While doing the job for safety it is a little bit on the low side in showing status and warnings to the user.
  - For this it needs to be integrated with the other safety systems to not compete with them in labelling, indications or controls.

LOKI Motion Safety

Reference Documents

Analysis & Requirements

Design

Installation

Validation

Operation

- ESS-1084771 - LOKI Instrument Hazard Analysis (IHA)
- ESS-5467337 - Motion Risk Analysis of Neutron Instruments
- ESS-0114726 - LOKI ToM, Table-of-Motion, sheet 3
- ESS-5513696 - LOKI Motion Control System – System Block Diagram
- ESS-4924706 - LOKI Motion Control 3 ePlan
- ESS-4924707 - LOKI Motion Control 4 ePlan
- ESS-4924708 - LOKI Motion Control 5 ePlan
- ESS-5516371 - System Design Description - LOKI Motion Control System
- ESS-5944740 - Design Verification Calculation (SISTEMA) for LOKI Motion Safety System
- ESS-5629386 - Electrical inspection LOKI MC Cabinets
- ESS-5941611 - MCA Self-Inspection Report for LOKI Motion Control
- ESS-5513743 - Inspection and Test Report for LOKI Motion Control (Electrical)
- ESS-5944732 - Motion Safety Validation Plan for LOKI
- ESS-5944738 - Motion Safety Validation Report for LOKI
- ESS-5669198 - Operation Manual - MCU5001: 16Ax. Motion Control Cabinet
- ESS-5669199 - Operation Manual - MCU5002: Servo Motion Control Cabinet

LOKI Motion Safety

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

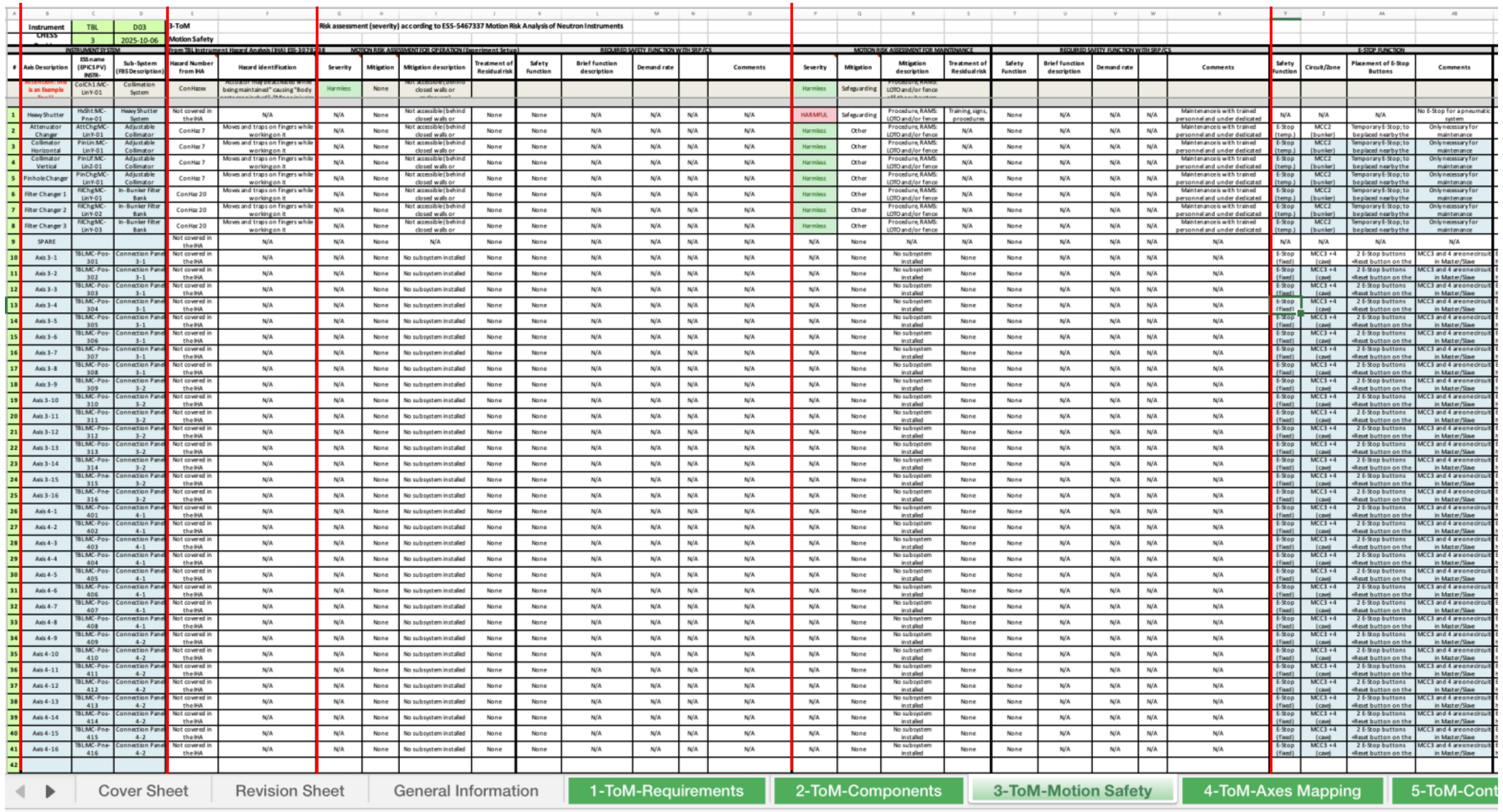
Table-of-Motion, Sheet 3

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

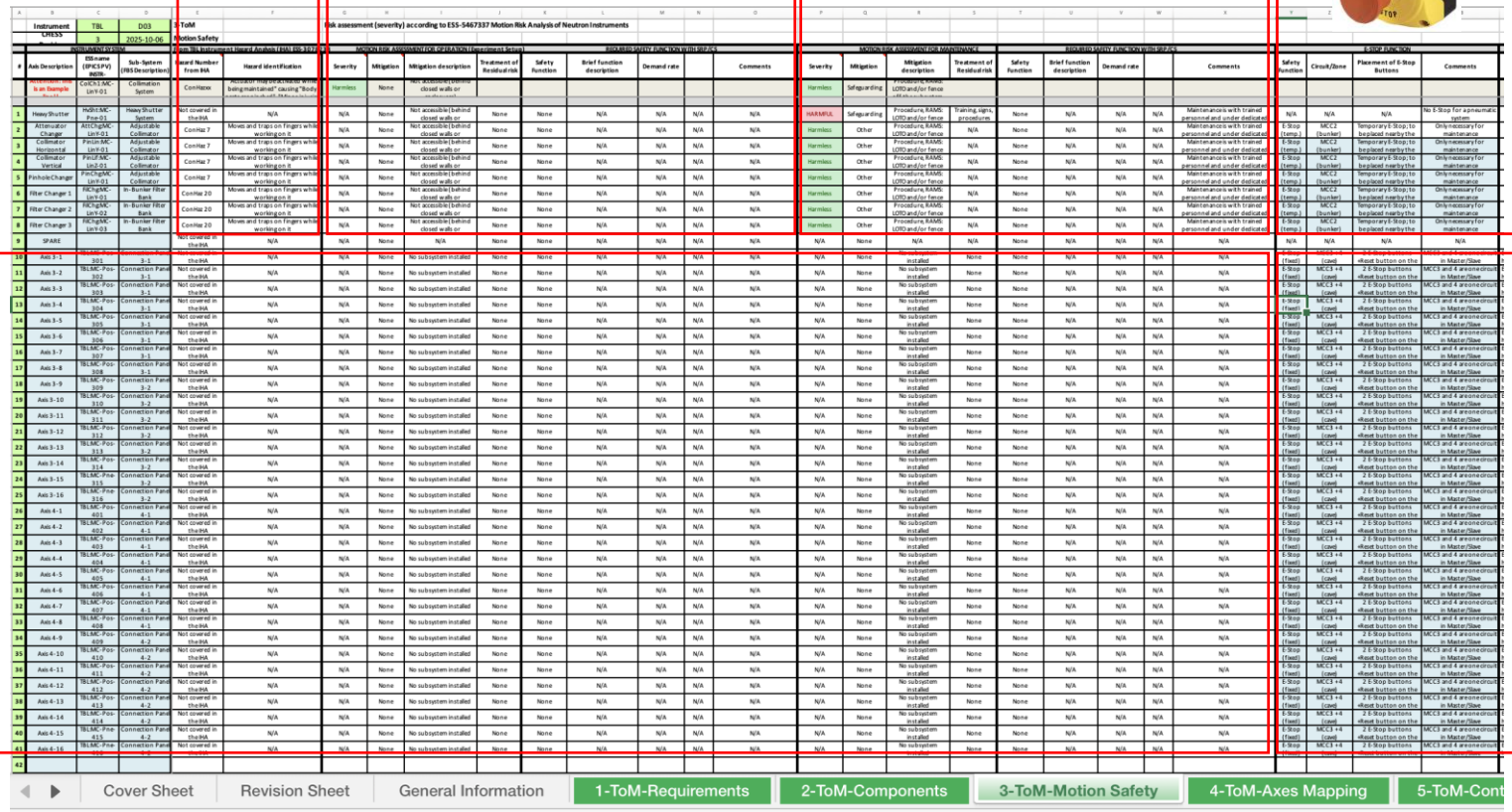
Circuit/Zone	Placement of E-Stop Buttons
MCC2 (bunker)	Temporary E-Stop; to be placed nearby the motion

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

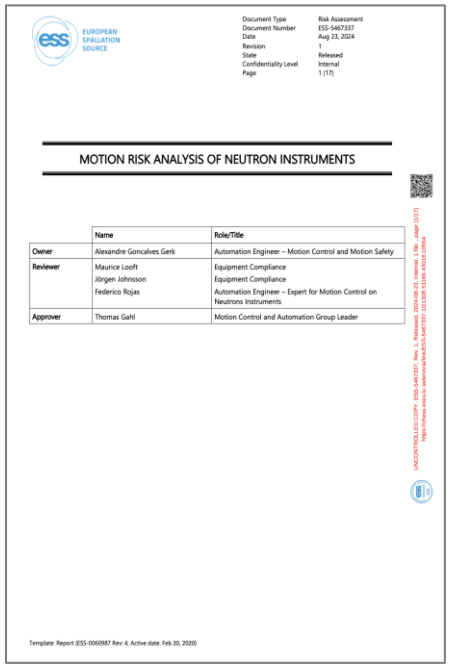


Risk Analysis & Treatment

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.

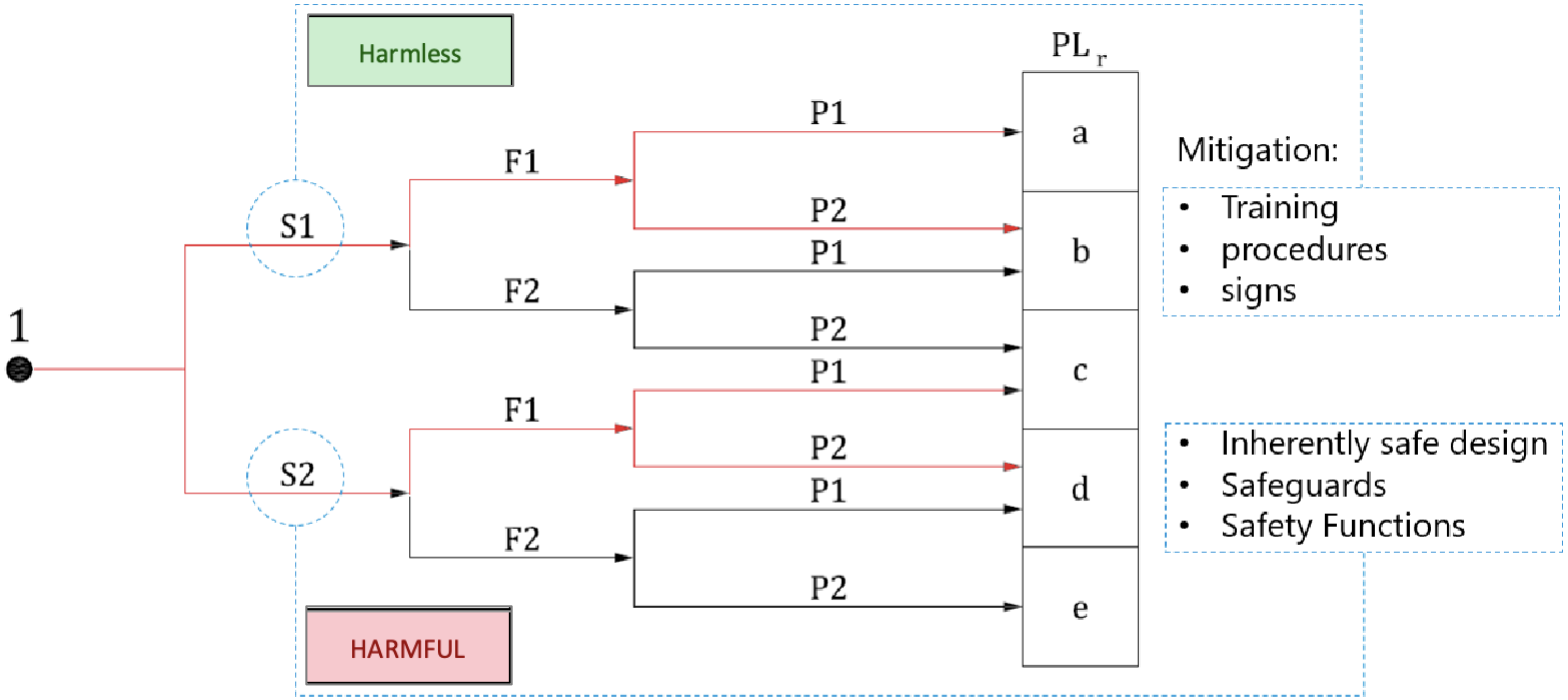
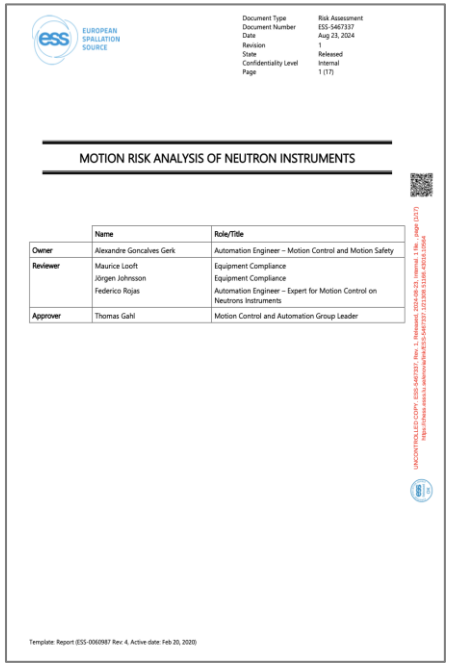


Figure 8 - Risk evaluation



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)

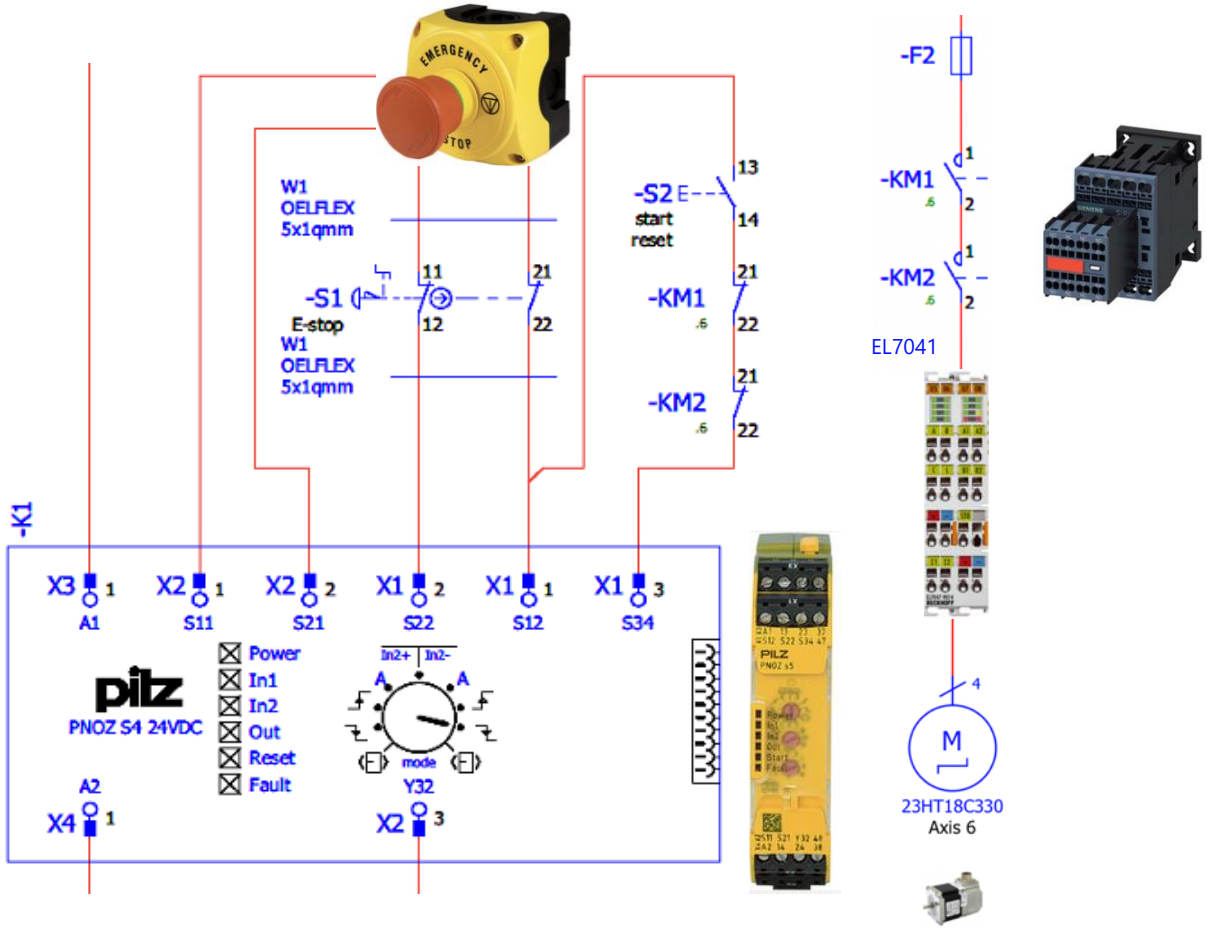
E-Stop Design

Design of E-Stop Circuit

Principle: Contactors are cutting power to the stepper motor drives

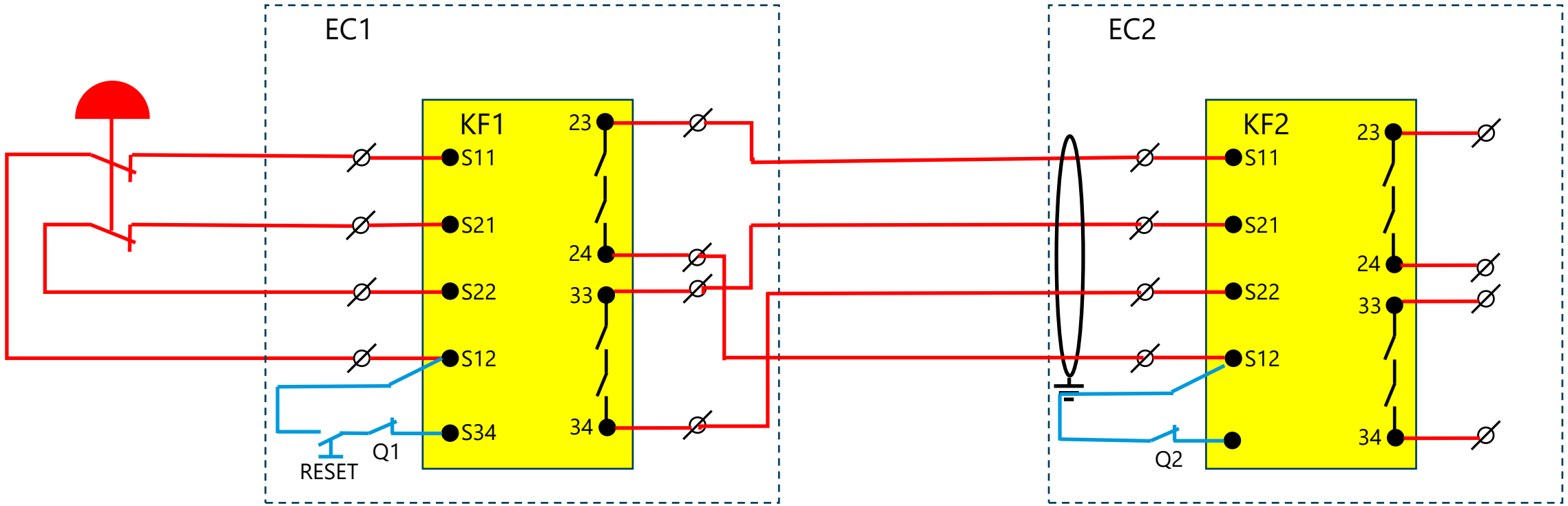
Performance Level d: How to achieve?

- 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

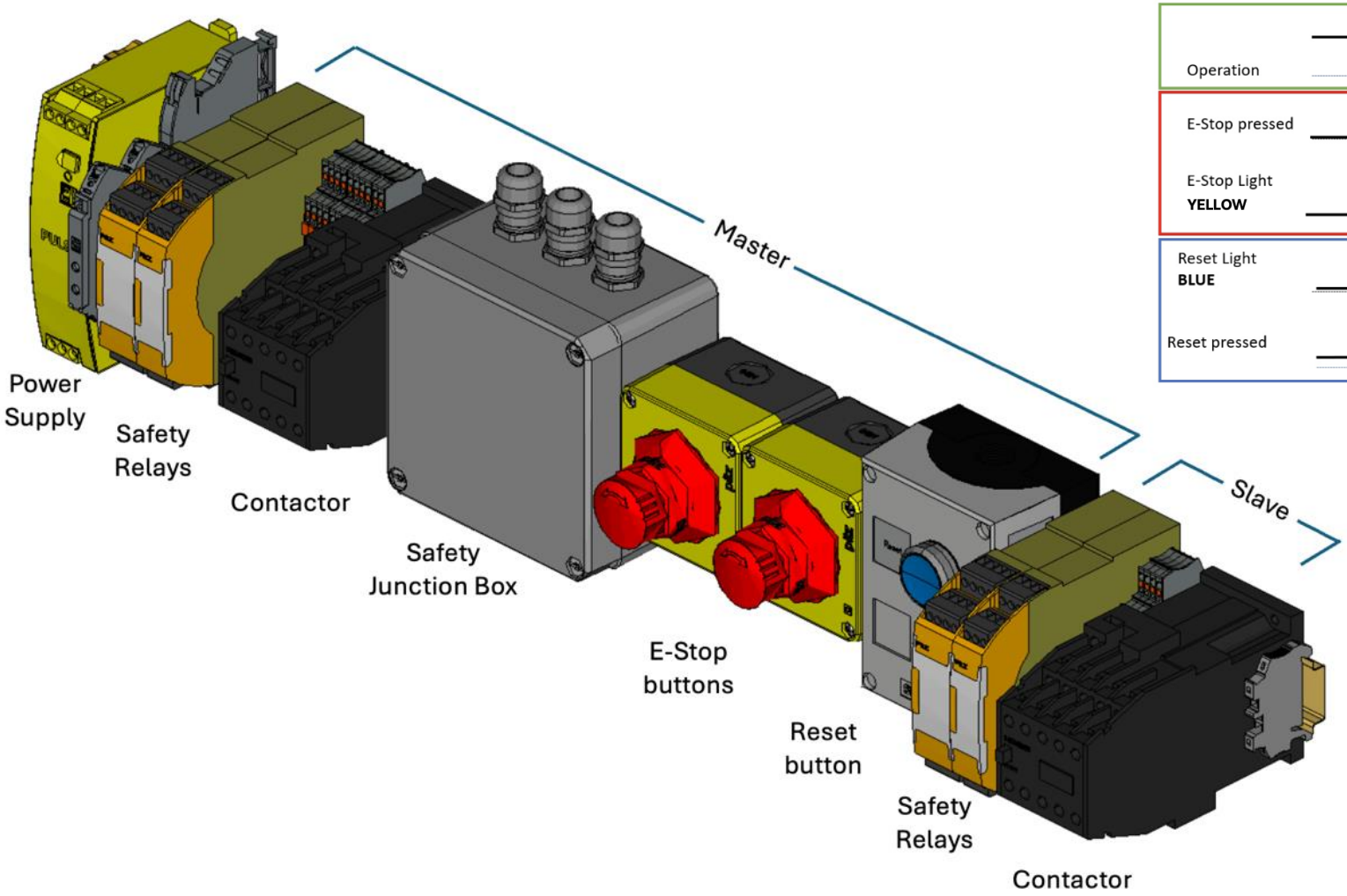
- Dual-channel operation with detection of shorts across contacts.
- Earth fault detection in circuit.
- Reset with falling edge

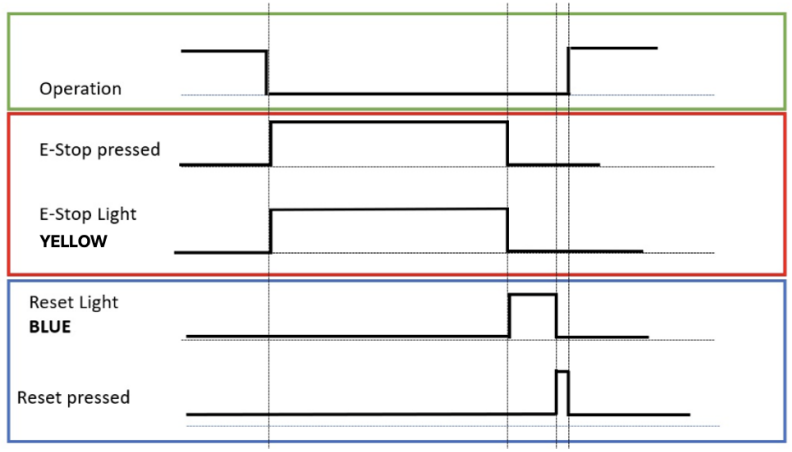
Slave input

- 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.