ESTIA Motion Safety System
- Implementation and Left to Do

Instrument Safety Readiness Review ESTIA

PRESENTED BY JACOB GILLIES
(ON BEHALF OF THE MOTION CONTROL & AUTOMATION GROUP)

2026-06-16

ESTIA Motion Safety

Instrument Hazard Analysis & Handover to Motion Safety

			Accident description				Normal Operation				Maintenance		
Hazard number	Instrument Area	Instrument Sub-area	Haz ID	Initiating event	Accident description	Consequence Severity	Level_of_Risk:		Controls to mitigate risk	Consequence severity	Level of Risk		Controls to mitigate risk
ConHaz14	Bunker	Chpper Pit	13.XH14	VS motion during maintenance and commissioning	Hands get squeezed during maintenance & commissioning of the VS without the Vacuum Chamber in place	C - Injuries requiring support of emergency services	CX3	Tolerable	Not applicable during operation	C - Injuries requiring support of emergency services	CX3	Tolerable	Task RAMS must be performed to ensure safety for the individual tests
ConHaz29	primary spectrometer	Selene Guide 1&2	13.XH29	Metrology Cart and Alignment Robot operation (motorized in safe mode) during maintenance with maintenance door open and with poor illumination inside the vacuum chamber	Limbs are squeezed	C - Injuries requiring support of emergency services	CX5	Acceptable	Not applicable during operation	B - Injuries requiring professional treatment, includes LTIs	BX5	Acceptable	Handover to motion safety (common MCA)
ConHaz30	primary spectrometer	Selene Guide 1&2	13.XH30	Mover operation during maintenance	Limbs are squeezed	C - Injuries requiring support of emergency services	CX5	Acceptable	Not applicable during operation	A - Minor injuries or discomfort, can be treated with first aid kit	AX4	Acceptable	Handover to motion safety (common MCA)
ConHaz48	secondary spectrometer	Sample Stage and Detector Arm	13.XH48	Trapped body parts	Axes drive into positions where bodyparts are pinched	C - Injuries requiring support of emergency services	CX4	Tolerable	Handover to motion safety (common MCA)	B - Injuries requiring professional treatment, includes LTIs	BX2	Tolerable	Handover to motion safety (common MCA)
ConHaz67	primary spectrometer	Middle Focus	13.XH65	Trapped body parts	Axes drive into positions where bodyparts are pinched	C - Injuries requiring support of emergency services	CX4	Tolerable	Handover to motion safety (common MCA)	B - Injuries requiring professional treatment, includes LTIs	BX3	Tolerable	Handover to motion safety (common MCA)
ConHaz70	secondary spectrometer	Instrument cave	13.XH70	Motion of SE equipment, such as Solid-liquid cell sample changer or Room temperature sample changer	Axes drive into positions where bodyparts are pinched	C - Injuries requiring support of emergency services	CX4	Tolerable	Handover to motion safety (common MCA)	C - Injuries requiring support of emergency services	CX5	Acceptable	Handover to motion safety (common MCA)
ConHaz71	secondary spectrometer	Instrument cave	13.XH71	Motion of SE equipment, such as Solid-liquid cell sample changer or Room temperature sample changer	Axes drive into positions where bodyparts are pinched	C - Injuries requiring support of emergency services	CX4	Tolerable	Handover to motion safety (common MCA)	C - Injuries requiring support of emergency services	CX5	Acceptable	Handover to motion safety (common MCA)

- 1 Bunker risk: See Exclusions
- 2 Selene Guide maintenance risks: Mitigated by stopping functions
- 4 Operation risks: Mitigated by enabling functions

ESTIA Motion Safety

Exclusions

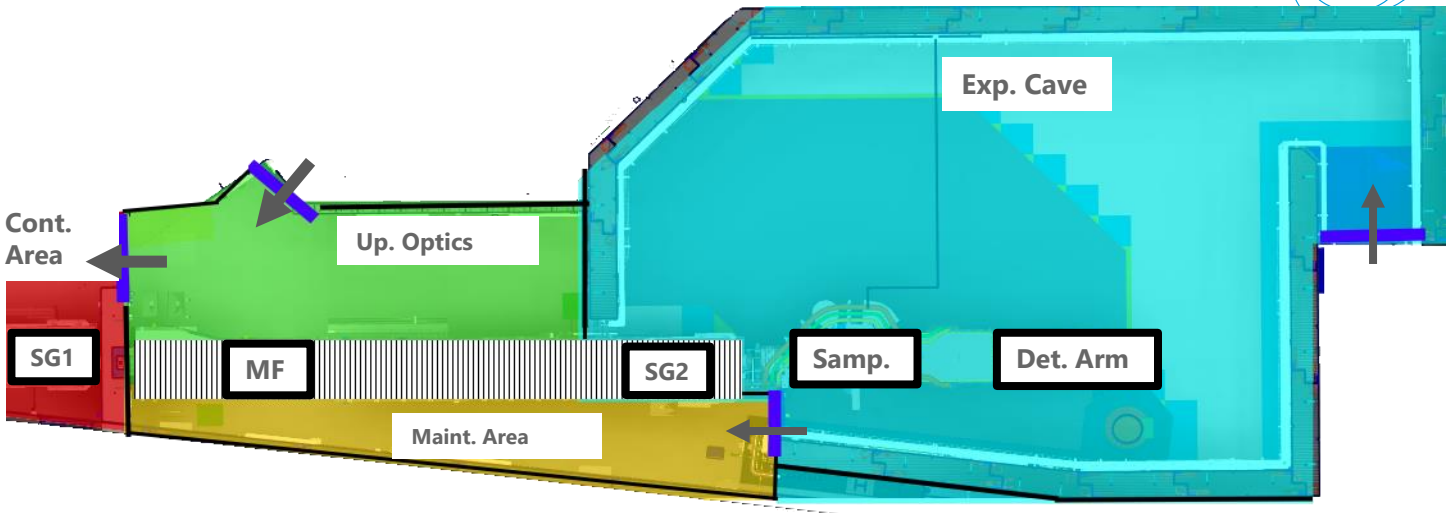
- MCC1 (In-bunker Virtual Source):
  - Access only for maintenance, trained personnel, LOTO, RAMS; provision to temporarily connect an operator stop (Motor only).

- MCC2 (Selene Guide 1):
  - Within a radiation-controlled zone.
  - Access only for maintenance, trained personnel, LOTO, RAMS; provision to temporarily connect an operator stop.
  - Investigate connection to common E-Stop, in cave connection point before operation.

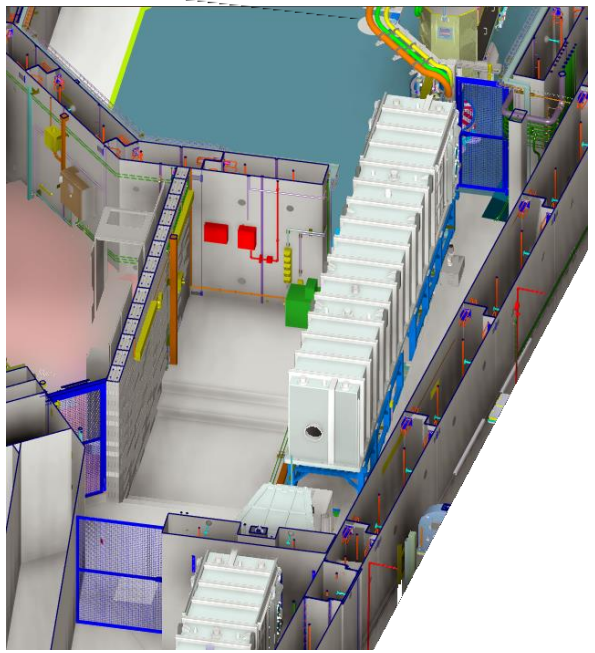
ESTIA Motion Safety

Areas

- Selene Guide 1:
  - Locked door to Controlled area; access only for maintenance. See Exclusions
- Upstream Optical Cave:
  - PSS Sensed manual Door
  - Access to Middle Focus (MF)
- Experimental Cave:
  - PSS Sensed manual Door
  - Access to Sample Area, Detector Arm and Selene Guide 2 (SG2)
- Maintenance Area:
  - PSS Sensed Manual Door via Experimental cave
  - Access to MF and SG2.

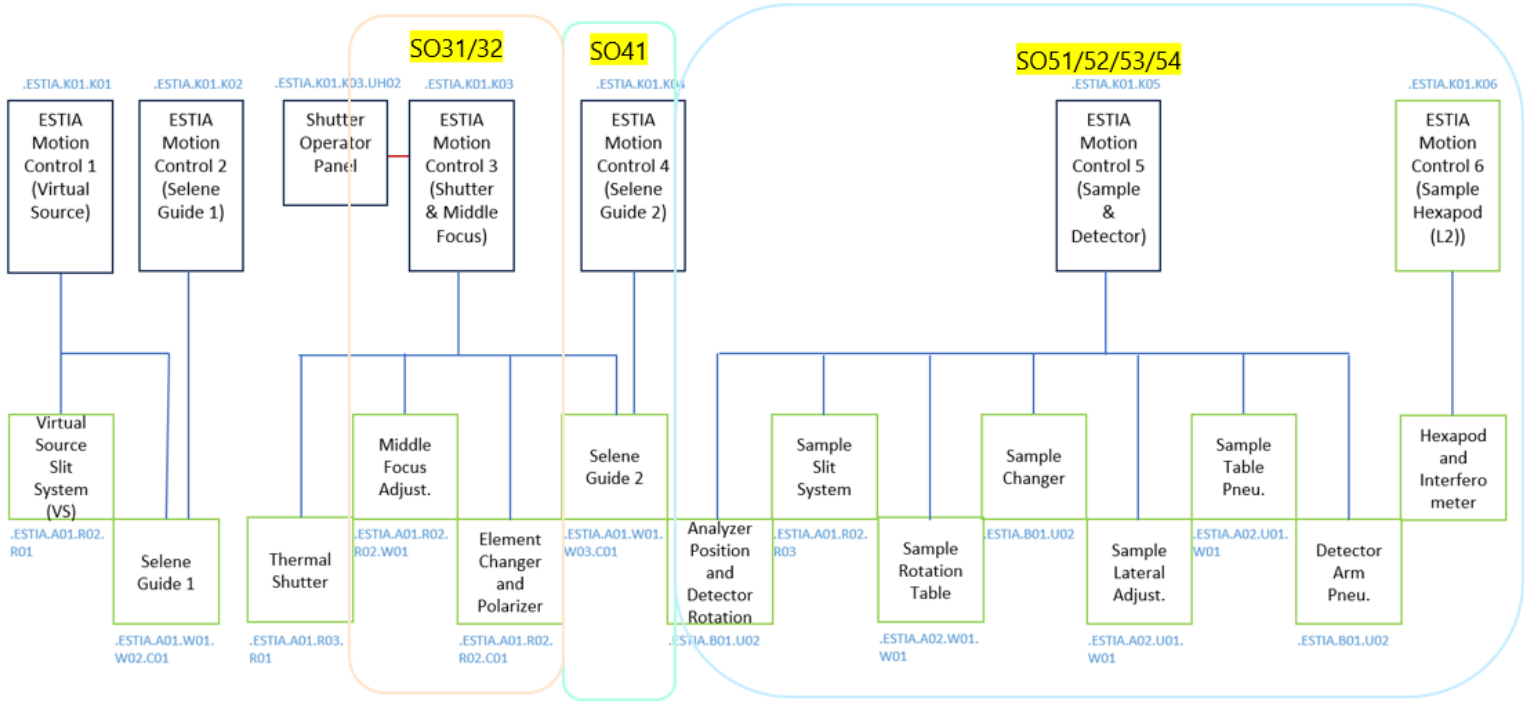


- PSS monitors 3 zones
  - Single "All locked" bit
- SG2 spans 2 zones
  - E-Stop logic complexity



ESTIA Motion Safety

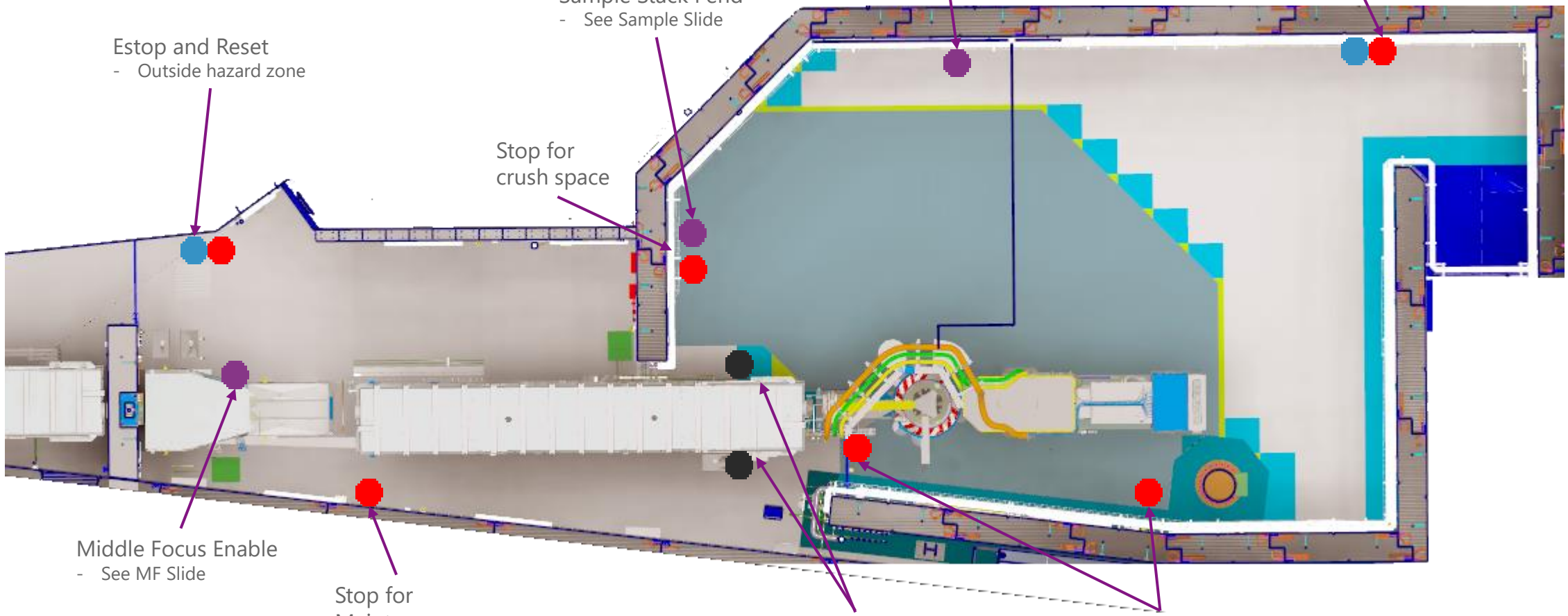
Safe Output Groups



SO	Axes	Control (+ E-Stop)
31	Middle Focus Axes exc. In-Beam Changer	Operator Stop MF Door
32	In-Beam Rotary Changer	Operator Stop MF Door MF Jog
41	Selene Guide 2	Operator Stop
51	Sample stack E-Stop Only (Sample Slits)	E-Stop Only
52	Sample stack (including SE patch panel)	Operator Stop Samp. Enable
53	Detector Arm Rotation	Enable Grip Grip Detection
54	Hexapod	Operator Stop Samp. Enable

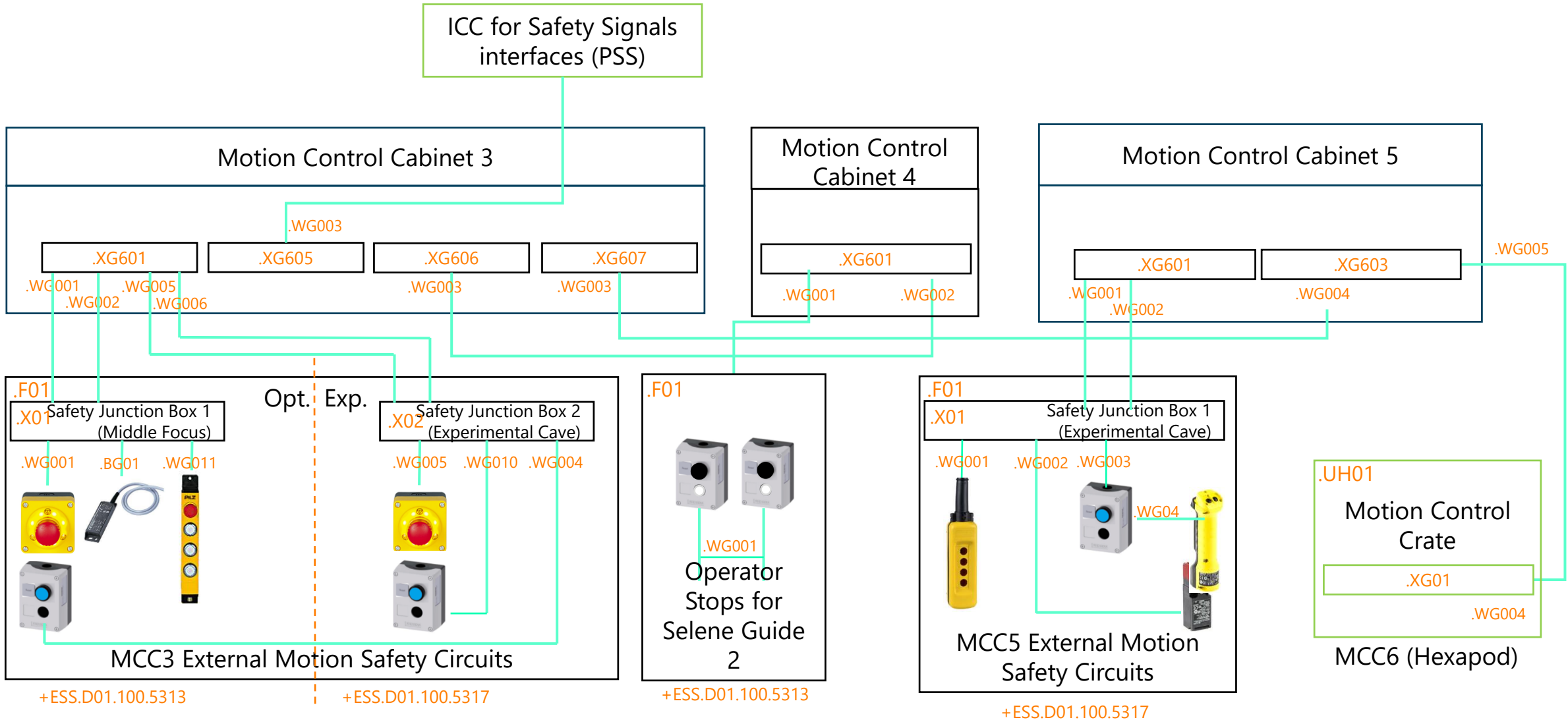
ESTIA Motion Safety

Implementation



ESTIA Motion Safety

Cabling



ESTIA Motion Safety

Safety Functions (SF)

Safety Functions				
ID	Name	Description	Axes	PLr
SF31 SF41 SF51	E-Stop	Remove power from all safe output subsystems	All	PLd
SF32	Access – Cave	Remove power from select axes unless PSS “Safe to operate” is present	Sample Table/ Detector	PLe
SF33	Restart Exp	Bypass SF2 as required	Sample Table	PLd
SF34	Restart Opt	For Maintenance, Stop motion in controlled area	Selene Guide 2	PLd
SF35	Stop – Middle Focus	Remove power from Middle Focus when MF Stop Pressed	Middle Focus axes	PLd
SF36	Enable – Middle Focus	Enabling based on MF Door state and Enabling controls	Middle Focus axes	PLd
SF42	Isolate – Selene Guide	For Maintenance, Stop motion in controlled area	Selene Guide 2	PLd
SF52	Stop – Sample Stack	Remove power from Sample Stack SO52	Sample Table	PLd
SF53	Enable – Sample Stack	Enabling based on PSS Access and Enabling controls	Sample Table	PLd
SF54	Isolate – Detector Power	Isolate Motion to Detector Rotation	Detector Rotation	PLe
SF55	Enable – Detector Rotation	Enable detector arm rotation axis	Detector Rotation	PLd

ESTIA Motion Safety

SF54 Isolate Detector

Description:
Arm is suspended on Air Pads for motion. Has a centre rotation and series of locking bolts

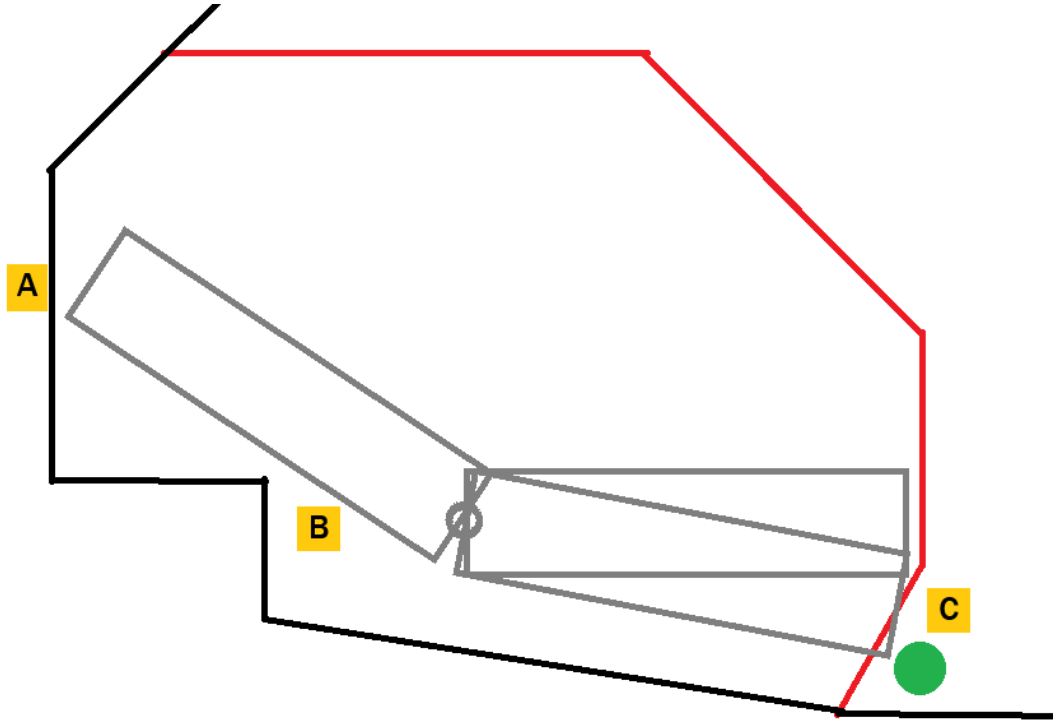
Maintenance:
this motion is free, across the polished floor.

Some risk of collision or crushing with a wall, but activities rely on trained people, bumpers, and the device is reasonably easy to push for a physically capable adult.

User Operation:
Arm is secured at one end and driven in an Arc. Either end of the arc presents a crushing hazard

Crushing hazards present at A, B and C.

C is a walkway and presents a continuous Hazard (More information and analysis available)



ESTIA Motion Safety

SF54 Isolate Detector

Factor	Assessment
1. use of the machine by	B - unskilled person[a]
2. speed of the part of the machine	A, but could be B: medium to low speed event: Max speed is ~200mm/s which is under 250mm, but depending on positioning hazard can present within 3 seconds. Typical programmed speed is ~80mm/s
3. spatial possibility to escape from the hazard	A: Mostly possible to avoid, only when the arm is in the extremes, or a person in on the ground doing maintenance that escape is reduced
4. possibility of recog-nition/awareness of the hazard (e.g. hot/cold surface, non-ionising radiation etc.)	A or B: Axis is quiet, and moved slow enough some times to be not noticed. Some audible aware-ness of Air engaging, but "normalcy" of proximity to hazard reduces recognition. Introduction of Audible/Visual alarms when air may support A
5. complexity of the operations	B - medium complexity: Hold to Run, co-ordinating multiple people in the space, monitoring of alignment instruments. Multiple different subsystems in the same space.

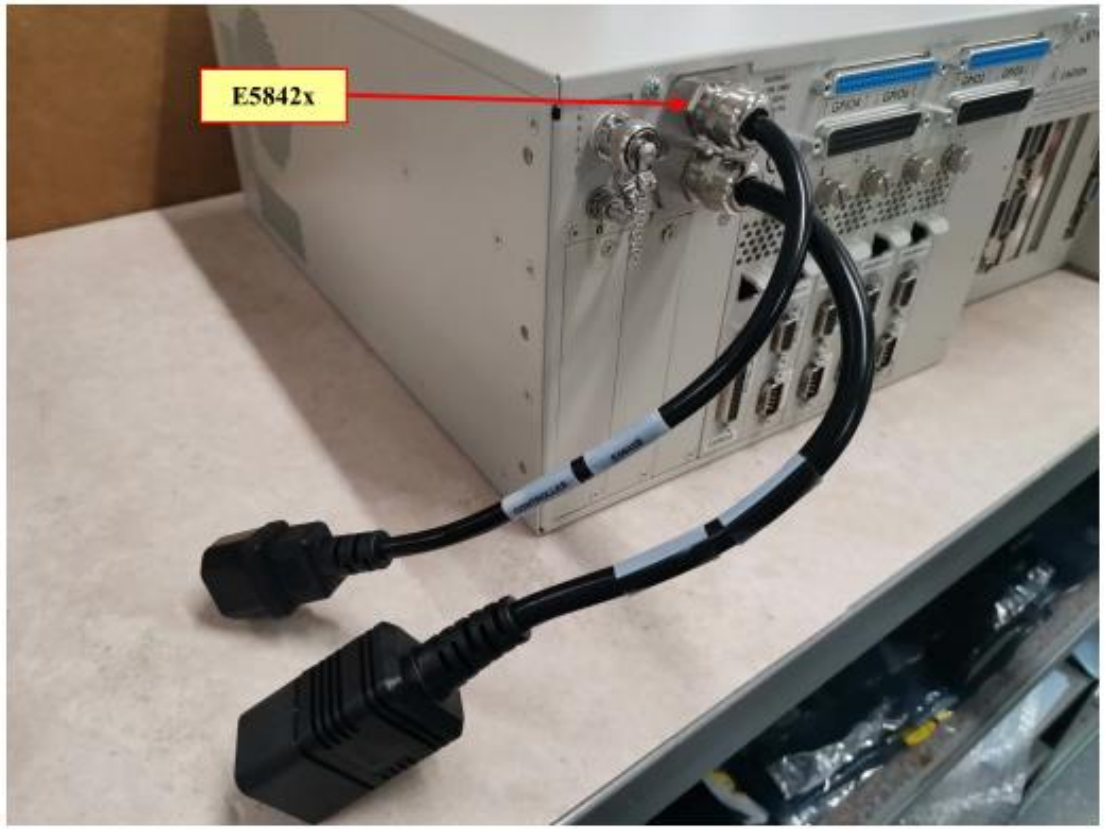
Table A.2 — Selection of parameter P1 or P2

Overall score		Parameter "P"
one or more "C"		P2
no "C", three or more "B"		P2
no "C", two "B", the rest "A"		P1 or P2 depending on the specific situation
no "C", one or no "B", the rest "A"		P1

"When a hazardous event occurs, P1 should only be selected if there is a realistic possibility of avoiding or significantly reducing harm. Otherwise, P2 should be selected"

ESTIA Motion Safety

NIT - Hexapod



- Power isolation requires full reboot of controller
- Split power version is available, but controller must be sent to factory
- Cost ~2000Euro
- New controller with upgrade ~18000 Euro

Validation Workflow

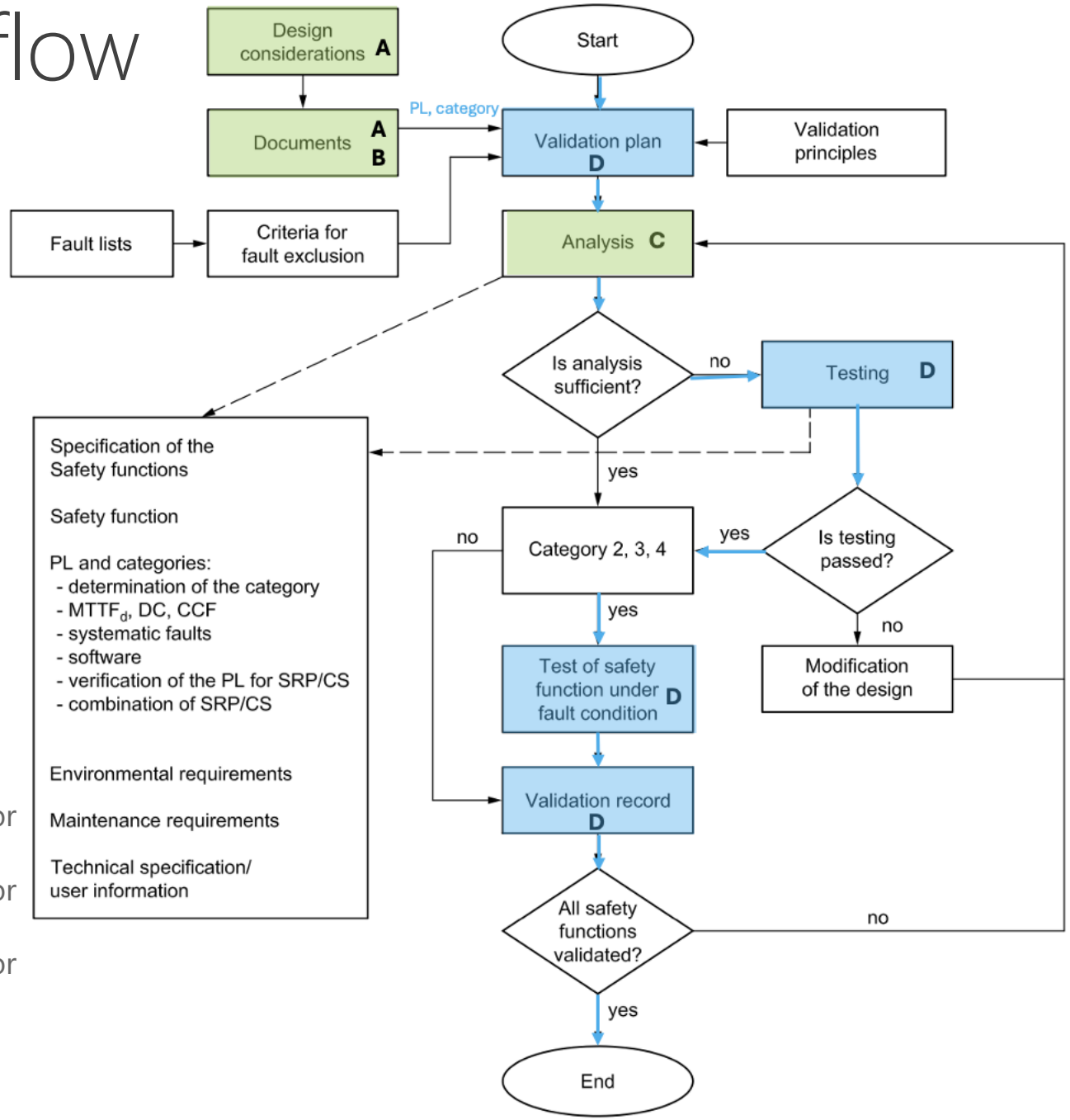
SS-EN ISO 13849-2

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

B. ESS-0366533 - ESTIA Table-of-Motion, sheet 3

C. ESS-6094789 - Design Verification Calculation (SISTEMA) for ESTIA Motion Safety

D. ESS-6091016 - Motion Safety Validation Plan for ESTIA MCC3
   ESS-6091017 - Motion Safety Validation Plan for ESTIA MCC4
   ESS-6091018 - Motion Safety Validation Plan for ESTIA MCC5
   ESS-6094315 - Motion Safety Validation Report for ESTIA MCC3
   ESS-6094316 - Motion Safety Validation Report for ESTIA MCC4
   ESS-6094317 - Motion Safety Validation Report for ESTIA MCC5



ESTIA Motion Safety

Validation Status

- Validation in progress
- MCC3 and MCC4 Validated
- Required change has been identified in MCC5 and modification is underway
  - Expected completion of MCC5 Validation on Wednesday 17Th June
- Document approval process ongoing

ESTIA Motion Safety

Left to do

- Current situation
  - System has been installed and functional behaviour of the safety system has been tested
    - Rework of one output system in progress
  - Validation documentation still in the approval pipeline
  - The most “Operationally complete” installation to date
  - This is good and safe enough for next phase (trial operation = hot commissioning) with skilled and trained users familiar with the system, once all referenced documents are released

- Next steps
  - Support the hot commissioning phase for troubleshooting and continuous improvement.
  - Get feedback from the users of the acceptance and the user-friendliness of the system.
  - Collate notes and design documents into formal documentation required for Operation

- Improvements:
  - Assess Residual risks and questions

ESTIA Motion Safety

NITs

The following NITs will be created:

ID	Name	Description
	MCC5 Validation	If MCC5 Validation is not completed by the end of the week, it will become an NIT
	Hexapod	Hexapod split supply to be investigated. Further validation of Inhibit signal required
	User improvements	Improve recovery during mode switching and restart, remove unnecessary extra resets. Timing improvements for enabling functions and LED feedback. Other minor issues as they are identified
	Operator Stops	Black operator stops, especially pendant, fails to switch both contacts correctly. Investigate contacts, replace button.

ESTIA Motion Safety

Residual Risks and Questions before Operation

ID	Name	Description	Notes
Res1	Risk Mitigation conflicts and Gap analysis	The hazard zone contains multiple discrete systems with separate stopping functions. MCA Motion analysis and E-Stop system strictly interacts with MCA motion elements Adjacent Stop buttons require personnel to read labelling to understand the effect of a button.	ESS Global Quality task
Res2	Unexpected motion	MCA Safety system requires user interaction to enable power when the cave is open. Once power is enabled, there is no restriction on the source of motion commands.	Recommend measures are implemented at the software level to restrict sources of control when cave access is granted.
Res3	Access logic	PSS access includes the Detector tank/Roof and cave in a single signal, Safe to operate . If a single door is open, removing safe to operate, all cave/detector axes are controlled by their operator function	Note this behaviour in operational training and risk management documentation. Investigate splitting signal
Res4	MCC3 Critical to operation	E-Stop logic needs to be combined (MCC3). Result is no motion if MCC3 is off or faulted. Should safety master be an isolated cabinet? Should IPCs/Safety have a separate always on 24V source?	Review for future improvement
Res5	Selene Guide 1 E-Stop	Should SG1 be included on the E-Stop bus?	Review for Operation
Res6	Sample Area User control	The pendant solution is fine for maintenance use, but is it the right solution for daily use	Review for Operation
Res7	E-Stop Indication	How to provide users with clear indication of E-Stop status	Requires ESS/NSS wider solution as part of Res1

ESTIA Motion Safety

Reference Documents

Analysis & Requirements	ESS-0318496 - ESTIA Instrument Hazard Analysis (IHA) ESS-5467337 - Motion Risk Analysis of Neutron Instruments ESS-0366533 - ESTIA Table-of-Motion, sheet 3
Design	ESS-5513695 - System Block Diagram for ESTIA Motion Control ESS-5337419 - ESTIA Motion Control 3 ePlan ESS-5337420- ESTIA Motion Control 4 ePlan ESS-5337421 - ESTIA Motion Control 5 ePlan ESS-5516370 - System Design Description - ESTIA Motion Control System ESS- - Design Verification Calculation (SISTEMA) for ESTIA Motion Safety
Installation	ESS- - Electrical inspection ESTIA MC Cabinets ESS- - MCA Self-Inspection Report for ESTIA Motion Control ESS- - Inspection and Test Report for ESTIA Motion Control
Validation	See Validation Page
Operation	ESS-5669198 - Operation Manual - MCU5001: 16Ax. Motion Control Cabinet ESS-5669200 - Operation Manual - MCU5003: Piezo Motion Control Cabinet ESS-5166392 - Motion Control Risk Assessment (RAMS)

ESTIA 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!
2026-06-16

10

Additional Information

Safety Requirements Specification

Table-of-Motion, Sheet 3

Safety Requirements Specification

Evaluation

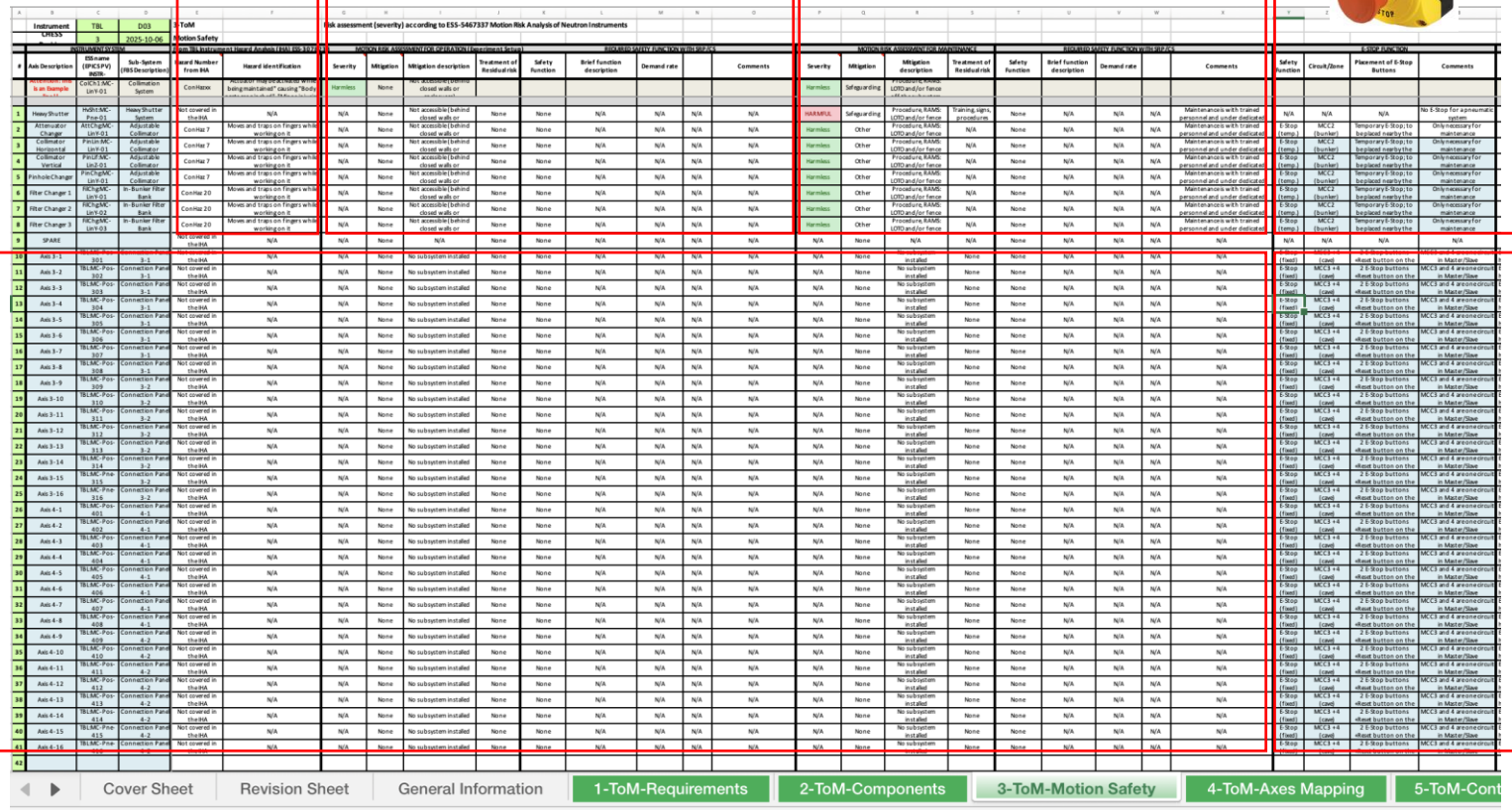
Mitigation	Mitigation description
None	Not accessible (behind closed walls or enclosures)

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

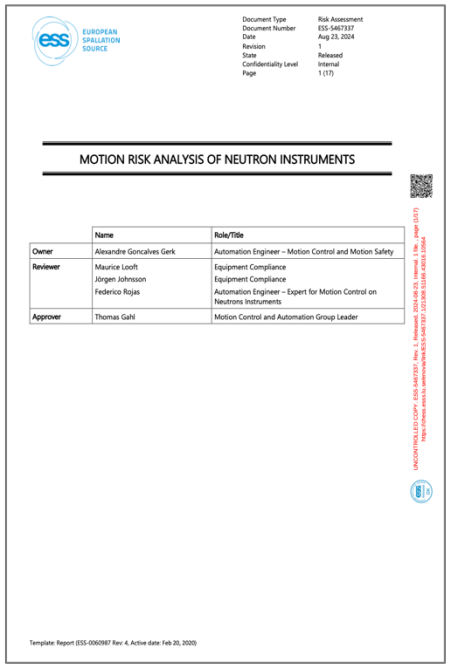
Circuit/Zone	Placement of E-Stop Buttons
MCC3 + 4 (cave)	2 E-Stop buttons +Reset button on the cave table

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



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.

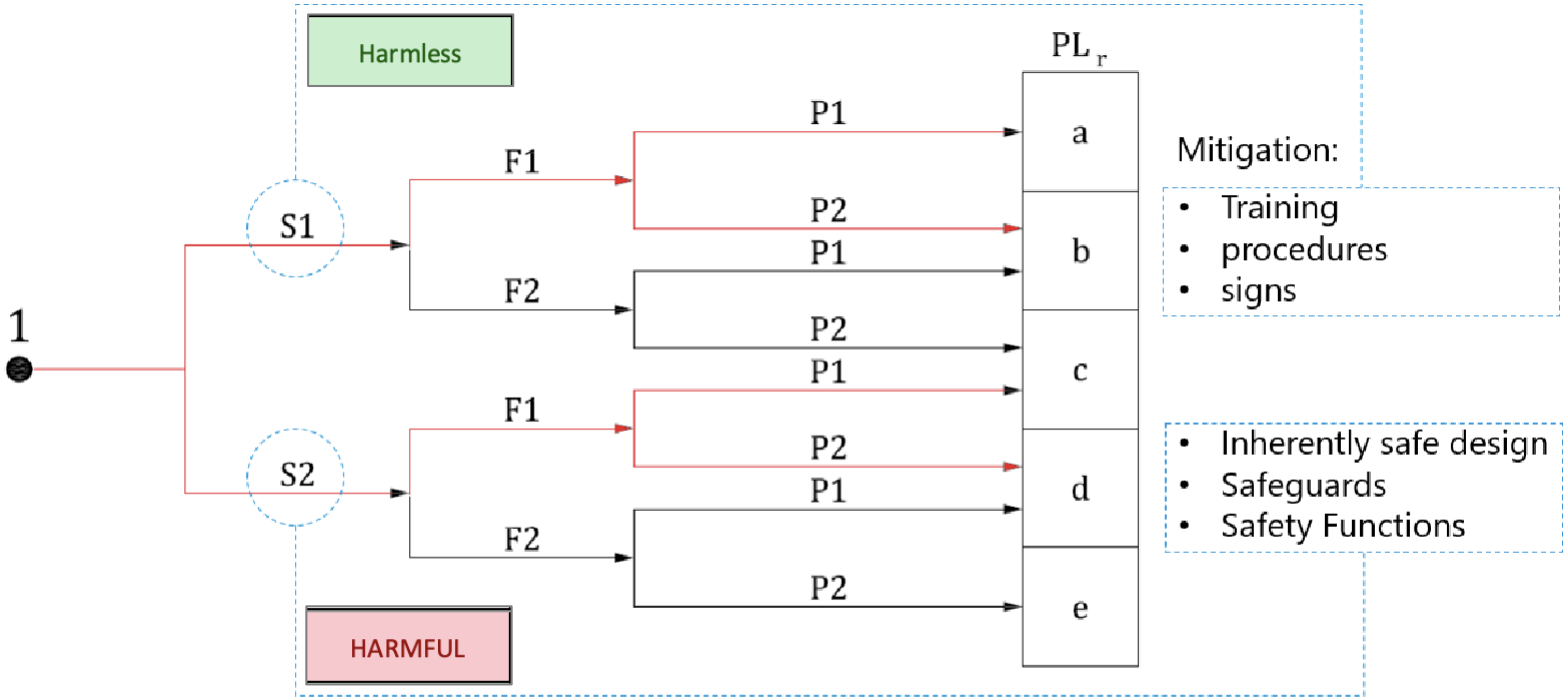
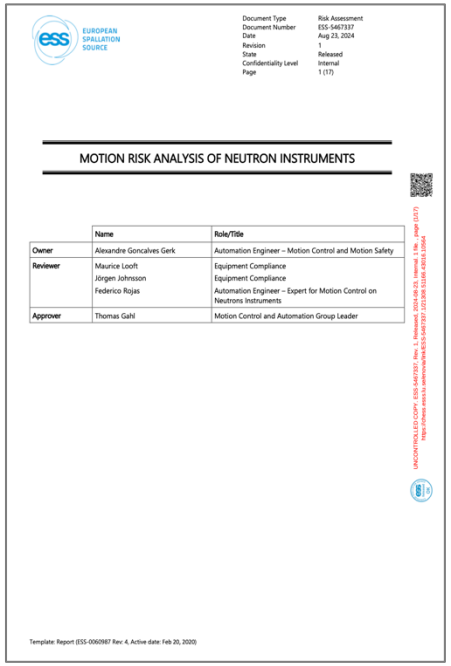


Figure 8 - Risk evaluation


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)

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.