SAFETY-DRIVEN DESIGN OF AUTOMATION SYSTEMS IN NUCLEAR FACILITIES

PHD PROGRAM IN MECHATRONICS AND PRODUCT INNOVATION ENGINEERING

COLLEGIO DEGLI INGEGNERI DELLA PROVINCIA DI VENEZIA, 12 APRILE 2025

Ph.D. Candidate: Giordano Lilli

Supervisor: Prof. Roberto Oboe

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI TECNICA E GESTIONE DEI SISTEMI INDUSTRIALI (DTG)

Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali di Legnaro

Background and Motivation

Automation systems in radioactive environments:

Nuclear Power Plants (NPPs)

- Teleoperated maintenance activities
- Rescue robots, inspections
- Decommissioning

Particle accelerators

- Inspections, RP surveys, crack monitoring
- Teleoperated maintenance activities

Fusion Reactors

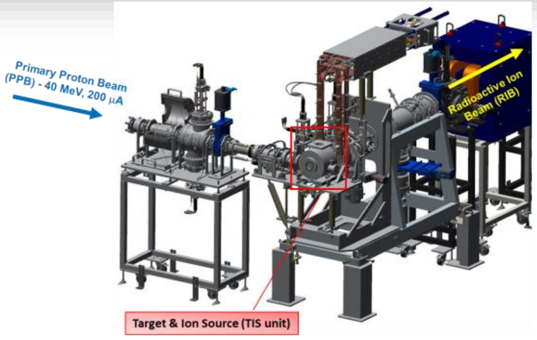
- Full-remote handling approach
- R&D, protocols, best practices

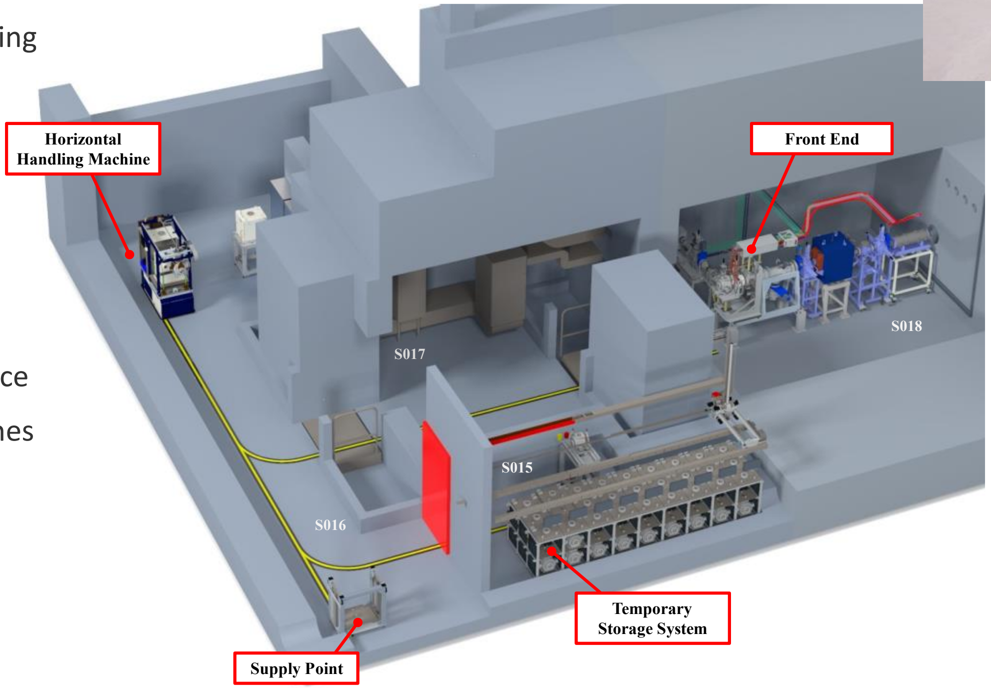
Radioactive Ion Beam (RIB) facilities

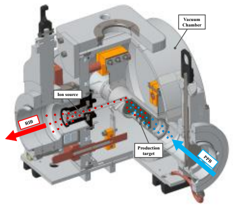
- Automation of process and maintenance
- Common problems, different approaches

The SPES facility

- Emerging RIB facility
- Advanced construction stage
- Illustrative use-case







Università degli Studi di Padova

Research Objectives

Research Aim

investigate the impact of a safety-driven remote handling design approach on the predicted personnel exposure during planned and unexpected maintenance interventions

Objectives

1. Safety assessment
2. Upgrade of the system
3. Maintenance review and optimization

The SPES Remote Handling framework
Design consolidation and advancements

Methodology

Two parallel approaches:

- Consolidation of the global architecture
- Consolidation of the machines

Architecture:

- Consolidation of the SPES target area layout
- Definition of HHM paths, intermediate points, operating stations
- Definition of the MPS interlocks with Front-End, shielding doors, etc.
- Definition of the ACS (Access Control System) interlocks

Communication:

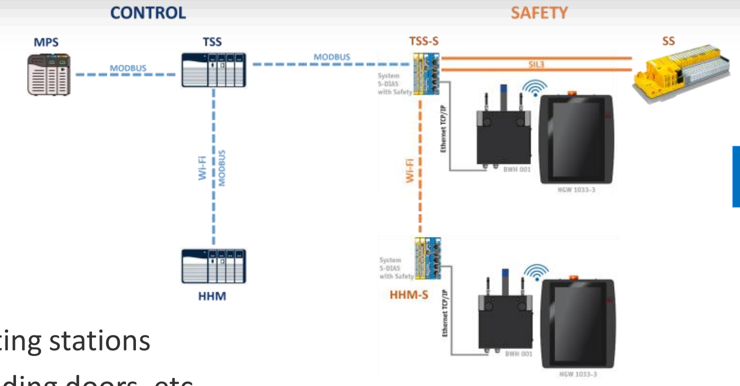
- Wi-Fi dual band radiating cable

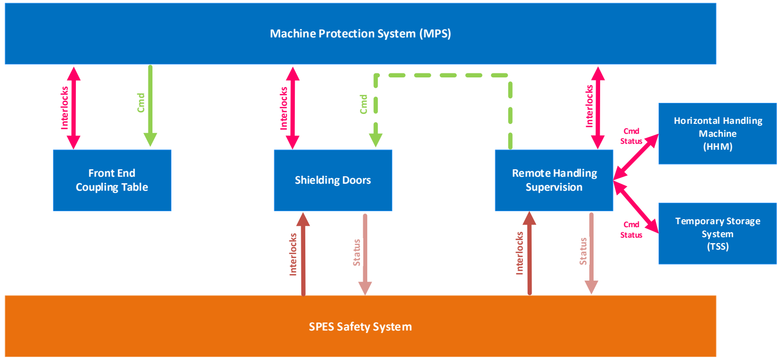
Supervision:

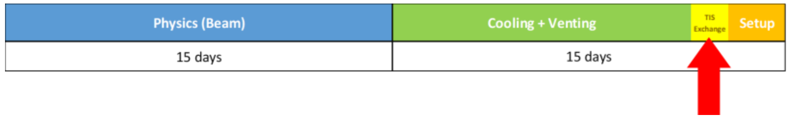
- Set of Pan Tilt Zoom (PTZ) 30x optical zoom cameras

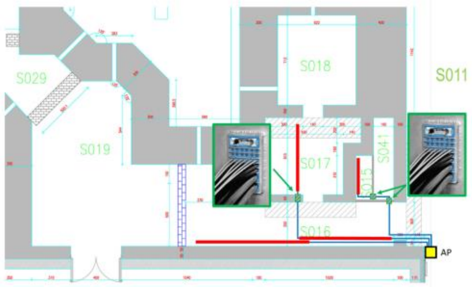
Control:

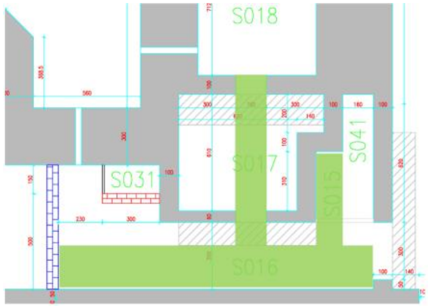
- Definition of the Remote Handling Supervisor (RHS) architecture

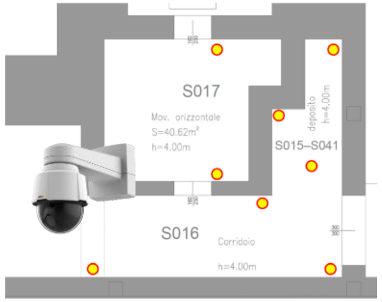


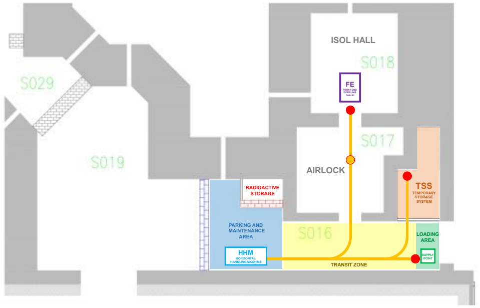


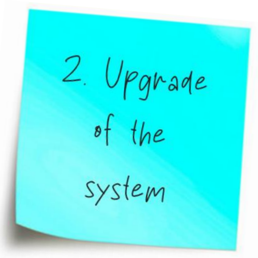












The SPES Remote Handling framework
Design consolidation and advancements

Università degli Studi di Padova

Horizontal Handling Machine (HHM)

Software:

- Modular architecture, atomic sequences
- Optimization of the interactions with the supervisor
- Minimization of the wi-fi data exchange dependency. Critical sequences are executed locally by the onboard PLC.

Energy management:

- Remodulation of HHM batteries: unified AGM battery units coupled with onboard inverter to power the rack
- Automatic charging procedure through a dedicated charging station, no more need for personnel access.

Hardware consolidation:

- Mechanical and cabling consolidation

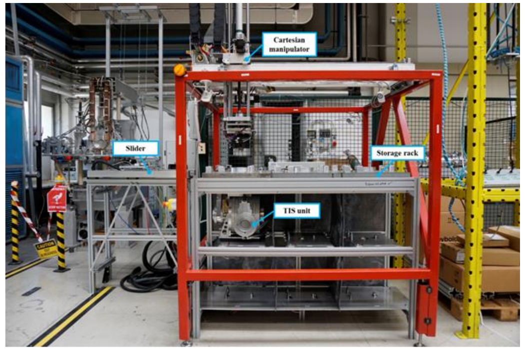
Temporary Storage System (TSS)

Hardware design:

- Redundant actuation for all the motion axes
- Fault-tolerant design

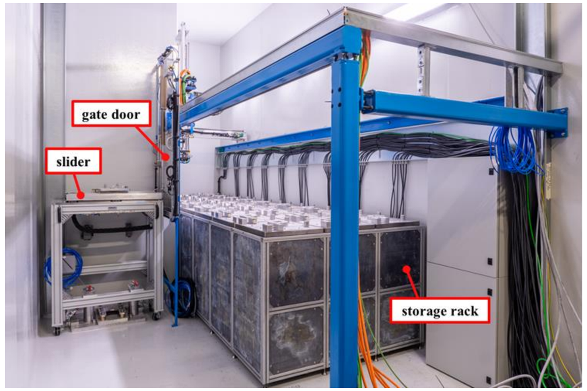
Software:

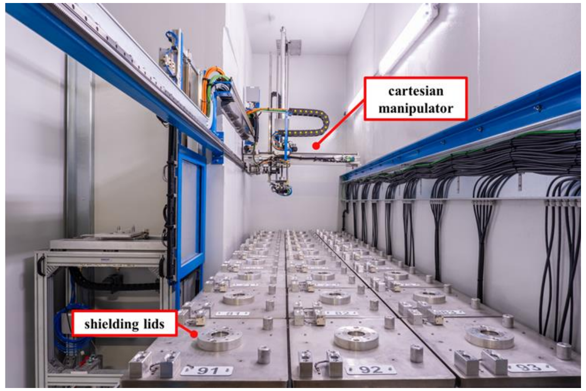
- Scalable architecture, state machine based
- Hardware abstraction layer



FROM PROTOTYPE

TO FINAL SYSTEM





Probabilistic Risk Assessment (PRA)
of SPES remote handling activities

Methodology: combined approach

HAZOP - LOPA analysis: semi-quantitative risk assessment tools usually implemented in the process industry

Focus:

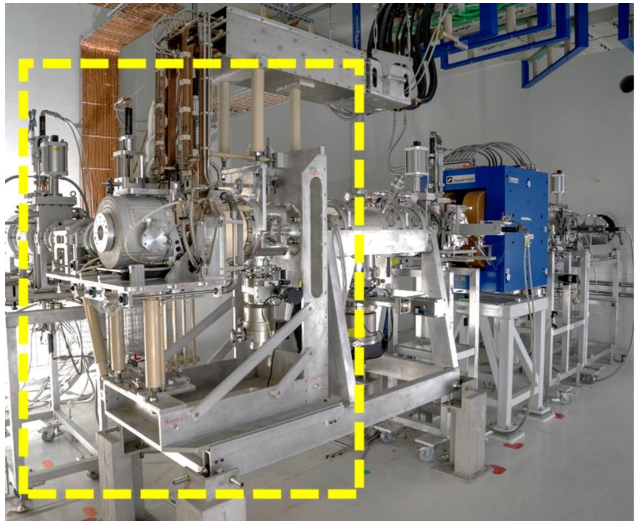
Remote handling activities on the SPES Front-End

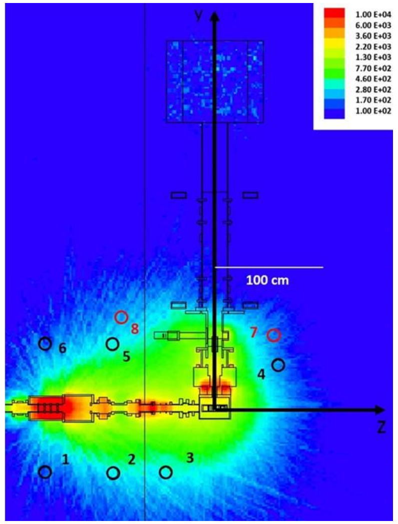
Goals:

- Identification of critical failure scenarios
- Improvement of the system
- Validation of the proposed safety measures

Risk Matrix

Risk Classification Matrix		Likelihood				
		A	B	C	D	E
Severities	V	H	H	H	H	M
	IV	H	H	H	M	M
	III	H	M	M	M	L
	II	M	M	M	L	L
	I	M	M	L	L	L



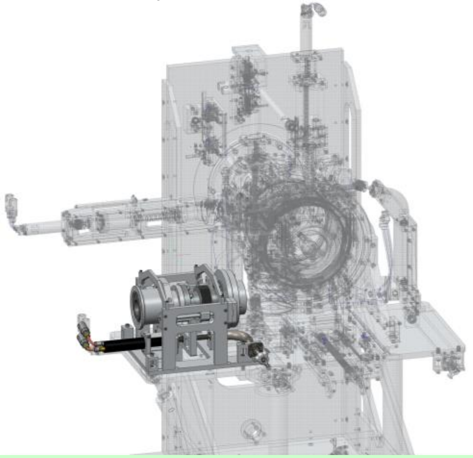


1. Safety assessment

Hazard and Operability (HAZOP) Study:

Qualitative risk assessment tool

- Example **deviation**: lack of movement



Node: PPB and RIB channels							
Deviation: 1. Motion Blocked							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		
1. Pneumatic motor failure	1. Remote recovery: finalize the motion using the backup actuator provided by HHM	B	C	I	L	A, B, C, D	Installation of air filters. Radiation survey prior to the intervention; Work and Dose Planning; Maintenance intervention optimization;
	2. Manual recovery: finalize the motion using auxiliary handling systems	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K	
	3. Maintenance intervention: motor replacement (room S018)	B/S	C	IV	H	A, B, C, E, F, G, H, I, J, K, M	
2. Pneumatic supply failure	1. Remote recovery: finalize the motion using the backup actuator provided by HHM	B	C	I	L	A, B, C, D	
	2. Manual recovery: finalize the motion using auxiliary handling systems	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K	
	3. Maintenance intervention: repair the equipment (room S018)	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K, M	
	4. Maintenance intervention: repair the equipment (room S017)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	
3. Mechanical problems	1. Maintenance intervention: inspection and repair (room S018)	B/S	C	IV	H	A, B, C, E, F, G, H, I, J, K, M	
4. Electrovalve hardware failure	1. Maintenance intervention: repair the equipment (room S017)	B	C	I	L	A, B, C, E, F, G, H, I, J, K	
5. PLC hardware failure	1. Maintenance intervention: repair the equipment (room 1017)	B	C	I	L	A, B, C, G	

Safeguards

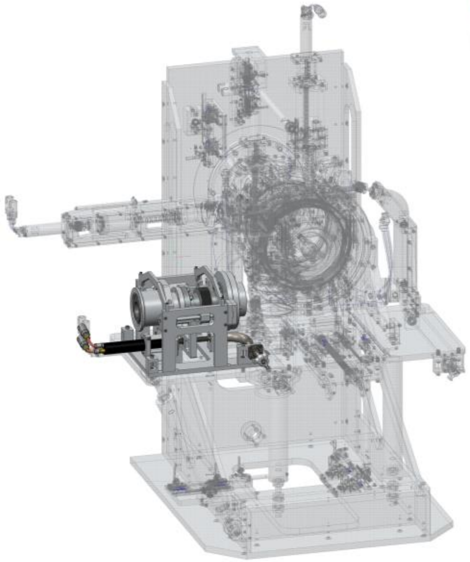
- Periodic replacement of the pneumatic motor
- Diagnostics: check pressure switches, power supply, etc.
- Periodic maintenance and inspection program
- Periodic functional checks
- Backup handling systems
- Operator training and training, use of PPE

Probabilistic Risk Assessment (PRA)
of SPES remote handling activities

Layer of Protection Analysis (LOPA)

Semi-quantitative risk assessment tool

- Probability of Failure on Demand (**PFD**):
  - Enabling Conditions (**ECs**)
  - Independent Protection Layers (**IPLs**)
  - Conditional Modifiers (**CMs**)
- Risk acceptability criterion.
  - **Target** frequency: **1.00E-06 yr^{-1}**



Node: PPB and RIB channels

Deviation: 1. Motion Blocked

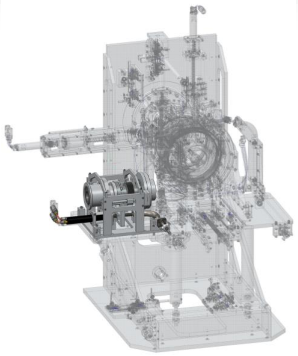
Initiating Event:	Consequence	Inital frequency [yr^{-1}]	ECs: Facility under maintenance	IPLs: Control System, MPS, Autotest	IPLs: Training of specialized operators, Use of PPEs, Procedures	IPLs: Periodic maintenance, inspection and replacement program	IPLs: Access Control System (ACS), Radiation monitoring, Personal dosimeters	IPLs: Remote inspections using the Horizontal Handling Machine (HHM)	CMs: Operator Presence	CMs: Backup actuation systems	CMs: MPS override	FUTURE Mitigated frequency with all IPLs implemented [yr^{-1}]	NOW Mitigated frequency with partial IPLs implemented [yr^{-1}]
1. Pneumatic motor failure	3. Maintenance intervention: motor replacement (room S018)	0.1	0.25	0.1*	0.01*	0.1*	0.1	-	1	0.1	-	2.50E-08	2.50E-04
2. Pneumatic supply failure	3. Maintenance intervention: repair the equipment (room S018)	0.5	0.25	0.1*	0.01*	0.1*	0.1	0.1*	1	0.1	-	1.25E-08	1.25E-04
3. Mechanical problems	1. Maintenance intervention: inspection and repair (room S018)	0.1	0.25	-	0.01*	0.1*	0.1	0.1*	1	-	-	2.50E-07	2.50E-04
											Total:	2.88E-07	6.25E-04

Probabilistic Risk Assessment (PRA)
of SPES remote handling activities

Results

Analysis highlights:

- 20 hardware components
- 38 failure scenarios over 8 nodes
- 13 safeguards: organizational/technical solutions
- 5 Independent Protection Layers



Outcomes:

- Validation of the proposed **Independent Protection Layers**
- Validation of the **Conditional Modifiers**
- **Roadmap** with next commissioning milestones
  - Design upgrade: backup actuation systems
  - Maintenance assessment, training program, procedures, etc.
  - Software verification
- **Identification** of nodes with missing IPLs

LOPA ID	Hazard scenario	Frequency Base Target	Mitigated Frequency: Final frequency with all IPLs implemented	Mitigated Frequency: Current frequency with partial IPLs implemented
1	Motion Blocked: PPB or RIB line. Operator intervention required. Direct exposure to high levels of radiation.	1.00e − 6	2.88e − 7	6.25e − 4
2	Motion Blocked: PPB or RIB gate valve. Operator intervention required. Direct exposure to high levels of radiation.	1.00e − 6	2.50e − 7	2.50e − 5
3	Diagnostic fault: PPB or RIB motion axis. Operator intervention required. Direct exposure to high levels of radiation.	1.00e − 6	2.55e − 7	7.50e − 4
4	Motion Blocked: extraction electrode. Operator intervention required. Direct exposure to high levels of radiation.	1.00e − 6	2.88e − 6*	6.25e − 3
5	Diagnostic fault: extraction electrode. Operator intervention required. Direct exposure to high levels of radiation.	1.00e − 6	3.00e − 6*	7.50e − 3
6	Motion Blocked: connections. Operator intervention required. Direct exposure to high levels of radiation.	1.00e − 6	6.25e − 7	6.25e − 3
7	TIS drop along route S018-S015: HHM gripper.	1.00e − 6	1.25e − 6*	1.25e − 2

Independent Protection Layer (IPL)	PFD
Control System, MPS, Autotest	0.1
Training of specialized operators, Use of PPEs, Procedures	0.01
Periodic maintenance, inspection and replacement program	0.1
Access Control System (ACS), Radiation monitoring, Personal dosimeters	0.1
Remote inspections using the Horizontal Handling Machine (HHM)	0.1

UNIVERSITÀ DEGLI STUDI DI PADOVA

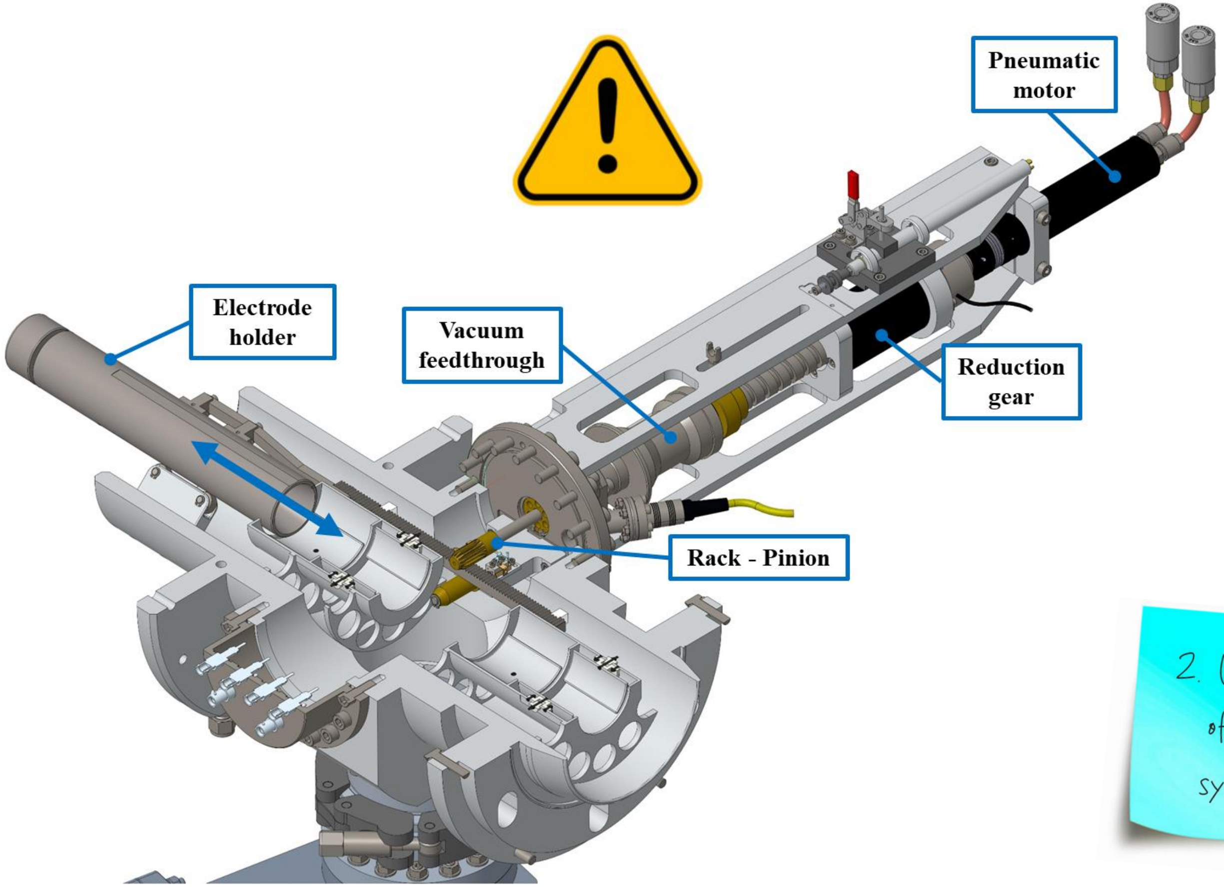
The Extraction Electrode Positioning System
preliminary design upgrade

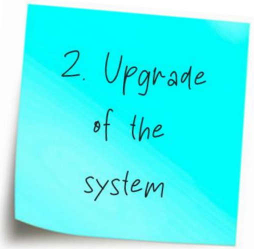
Methodology: Design for maintenance

Vulnerabilities of the existing system:

- Position:
  - **difficult to reach**, operator crosses the beams line
- Mechanical design:
  - Motor: **2 screws**
  - Limit switches: vacuum CF flange, **16 screws**
- Transmission (magnetic rotary feedtrough)
  - Maximum breakaway torque **4 Nm**
- Backup motion interface:
  - **not available**

Maintainability guidelines



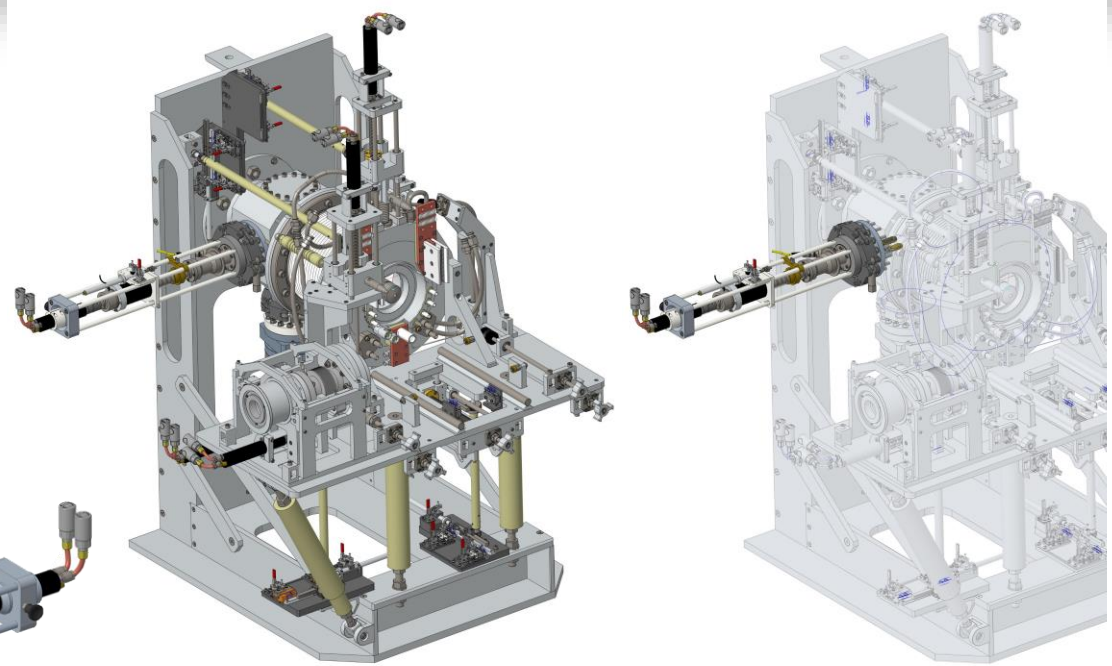


The Extraction Electrode Positioning System
preliminary design upgrade

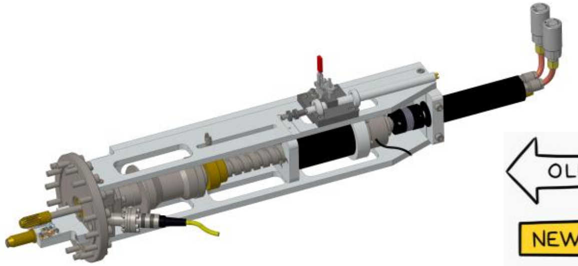
Methodology: Design for maintenance

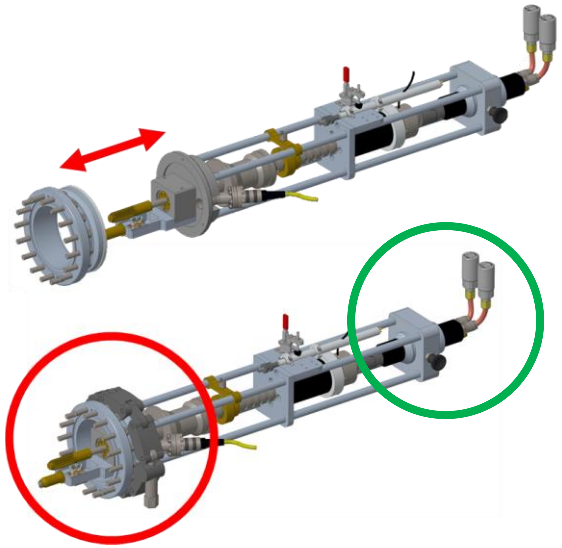
Upgrade – rev 2.0:

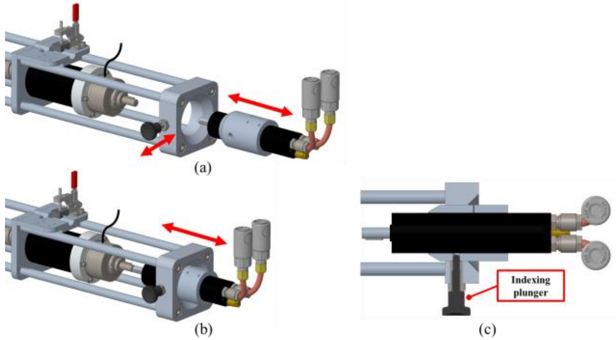
- Position:
  - **difficult to reach**, operator crosses the beams line
- Mechanical design:
  - Motor: **rapid disconnection**
  - Limit switches: **chain clamp (no screws)**
- Transmission (magnetic rotary feedtrough)
  - Maximum breakaway torque **4 Nm**
- Backup motion interface:
  - **not available**



Comparison





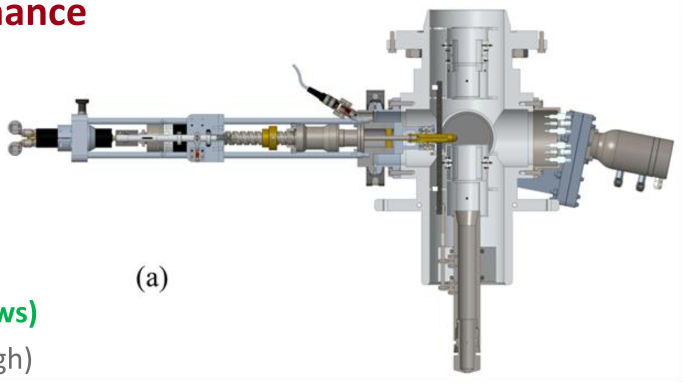


The Extraction Electrode Positioning System
preliminary design upgrade

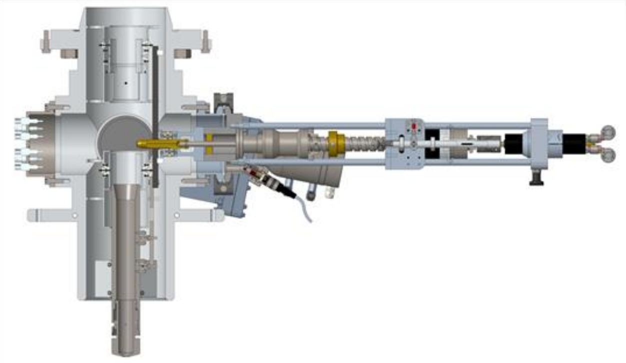
Methodology: Design for maintenance

Upgrade – rev 2.1:

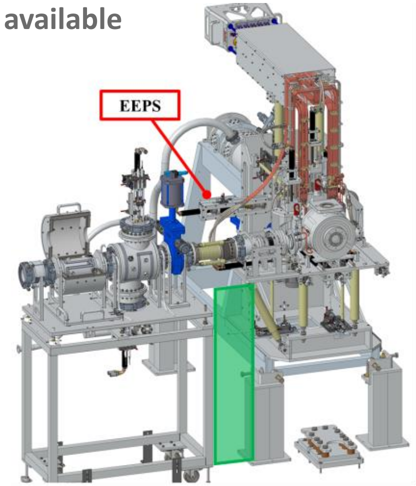
- Position:
  - **Mirrored layout**, RIB right side
- Mechanical design:
  - Motor: **rapid disconnection**
  - Limit switches: **chain clamp (no screws)**
- Transmission (magnetic rotary feedtrough)
  - Maximum breakaway torque **4 Nm**
- Backup motion interface:
  - **not available**



(a)

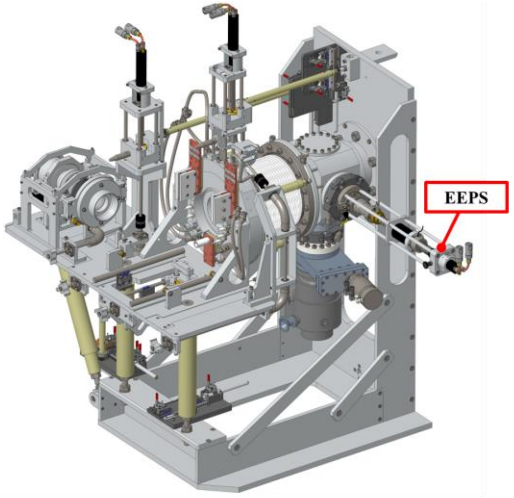


Comparison



(a)

(b)

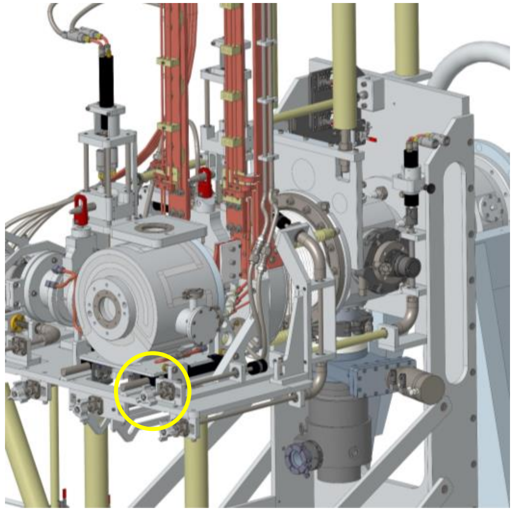


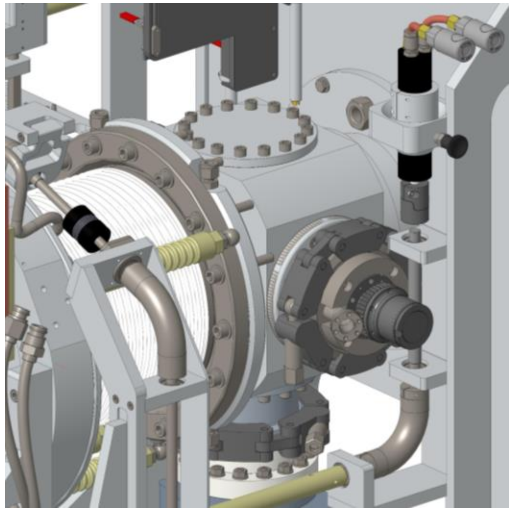
(a)

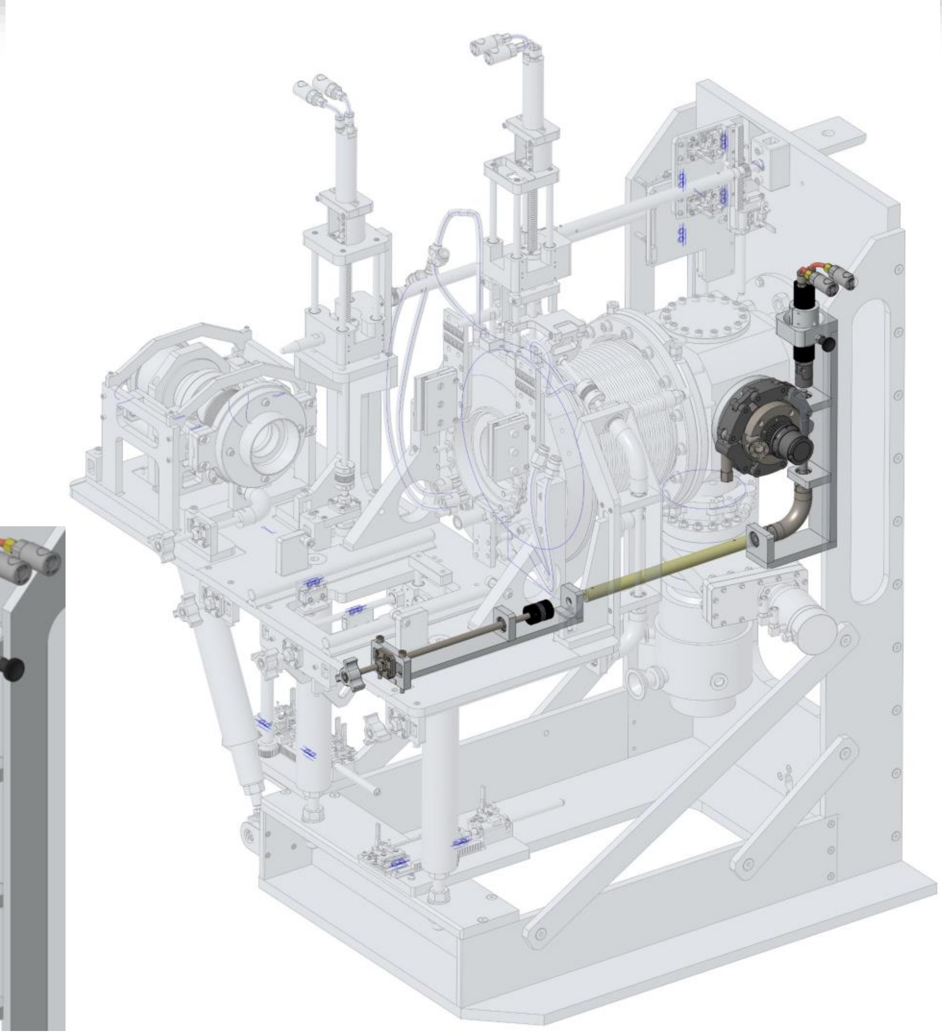
Methodology: Design for maintenance

Concept design – rev 3.0:

- Position:
  - **Mirrored layout**, RIB right side
- Mechanical design:
  - Motor: **rapid disconnection**
  - Limit switches: **chain clamp (no screws)**
- Transmission (magnetic rotary feedtrough)
  - Maximum breakaway torque 4 Nm -> **9 Nm**
- Backup motion interface:
  - **implemented**







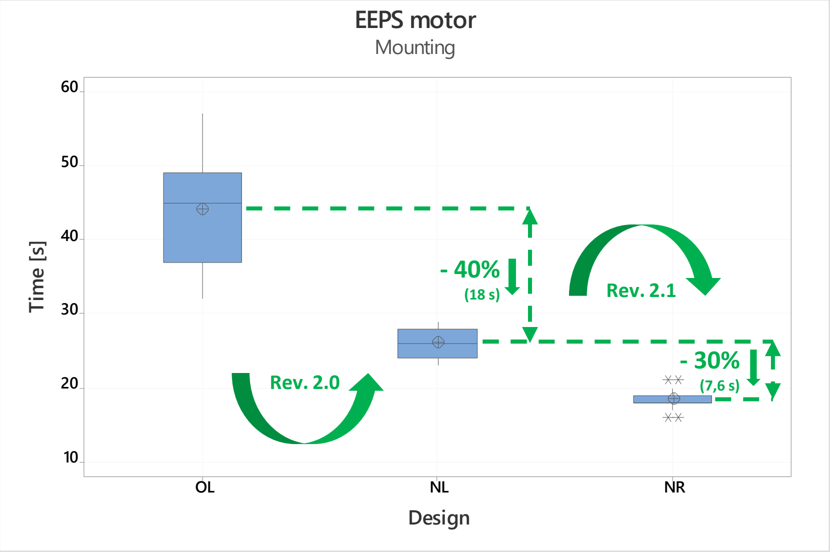
The Extraction Electrode Positioning System
preliminary design upgrade

Results

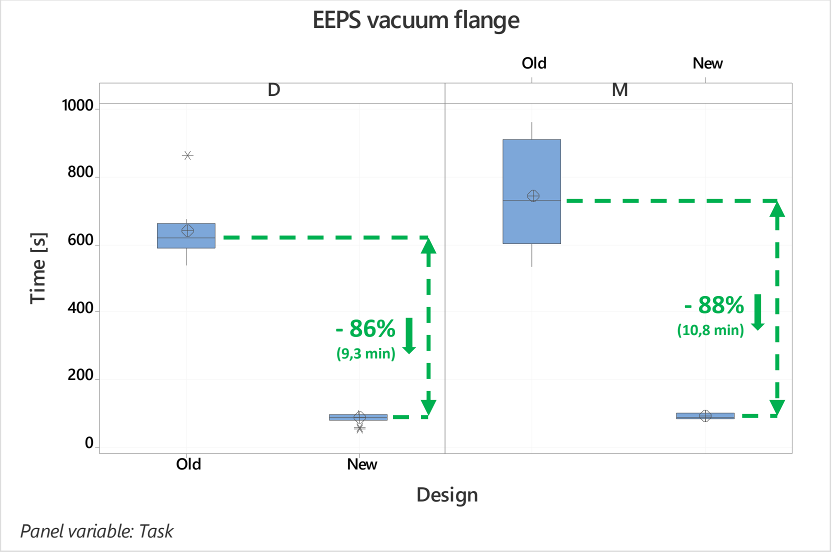
Maintenance-oriented design upgrade

- Revision 2.0 and 2.1 are currently under construction,
- The benefits introduced by the proposed design have been validated experimentally

Experimental results:



Design	N	Mean	SE Mean	StDev	Variance	Minimum	Median	Maximum	Range
OL	20	44,00	1,58	7,05	49,68	32,00	45,00	57,00	25,00
NL	20	26,05	0,43	1,91	3,63	23,00	26,00	29,00	6,00
NR	20	18,40	0,30	1,35	1,83	16,00	18,00	21,00	5,00



Task	Design	N	Mean	SE Mean	StDev	Variance	Minimum	Median	Maximum	Range
D	Old	8	639,5	34,7	98,1	9624,6	535,0	616,5	862,0	327,0
	New	20	84,50	3,28	14,68	215,53	50,00	85,00	108,00	58,00
M	Old	8	739,1	55,7	157,5	24805,0	533,0	731,0	960,0	427,0
	New	20	90,20	2,29	10,24	104,91	76,00	87,00	110,00	34,00

Methodology

Experimental campaign

Screening session

Survey session

- 500+ maintenance tests:
  - 10 operators
  - 14 components (pneumatic motors, limit switches, potentiometers)
  - 2 tasks: mounting and dismounting
  - 2 runs
- Time estimation
- Factorial analysis

Comparison session

- **Tool A** vs **Tool B**
- **Old** design vs **New** design

Definition of procedures

Identification of operational issues

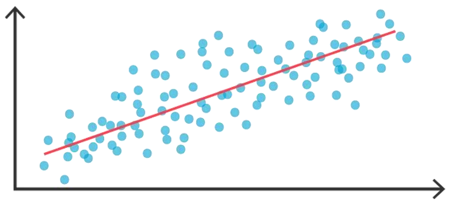
Maintenance Assessment
optimization of critical activities in high-radioactive environment

Results

Survey Session

Regression analysis

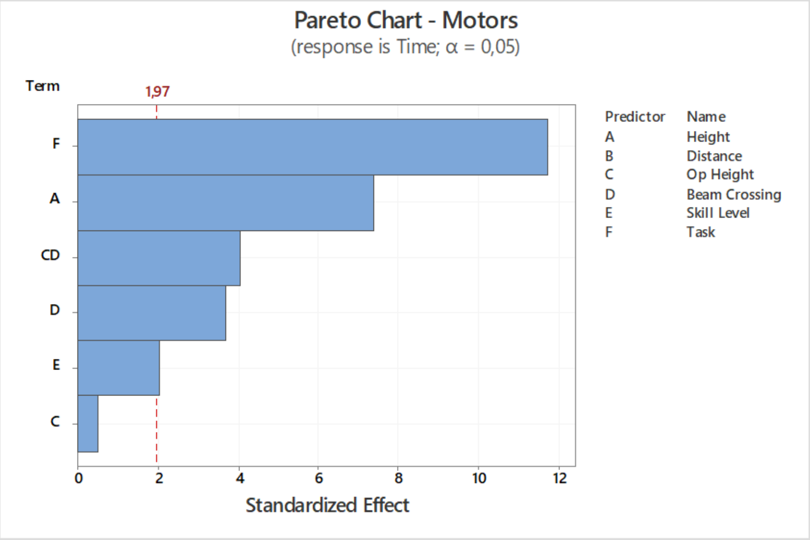
- Component height
- Operator height
- Beam crossing
- Skill level

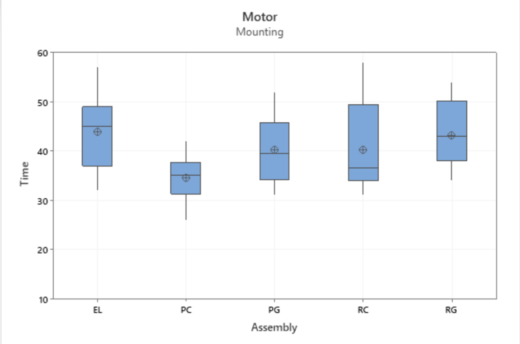


Comparison session

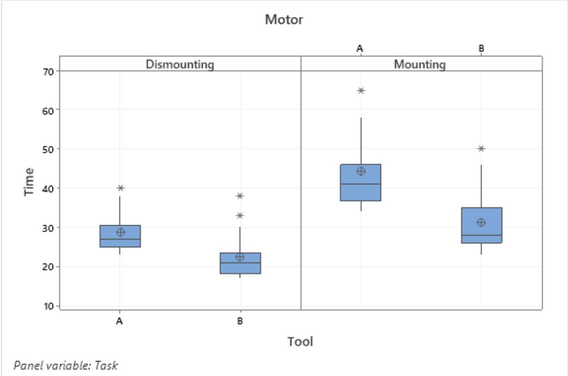
2-sample t test

- Statistical difference in datasets:
  - Tool A vs Tool B
  - Old design vs New design
- Design upgrade validation

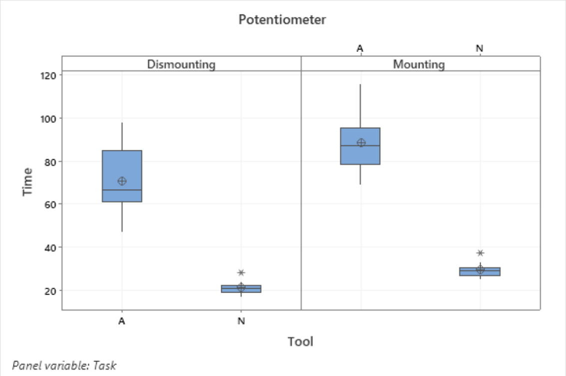




Assembly	N	Mean	SE Mean	St Dev	Variance	Min.	Median	Max.	Range
EL	20	44.00	1.58	7.05	49.68	32.00	45.00	57.00	25.00
PC	20	34.45	1.08	4.82	23.21	26.00	35.00	42.00	16.00
PG	20	40.30	1.40	6.27	39.27	31.00	39.50	52.00	21.00
RC	20	40.25	1.95	8.74	76.41	31.00	36.50	58.00	27.00
RG	20	43.25	1.48	6.60	43.57	34.00	43.00	54.00	20.00



Tool A vs Tool B

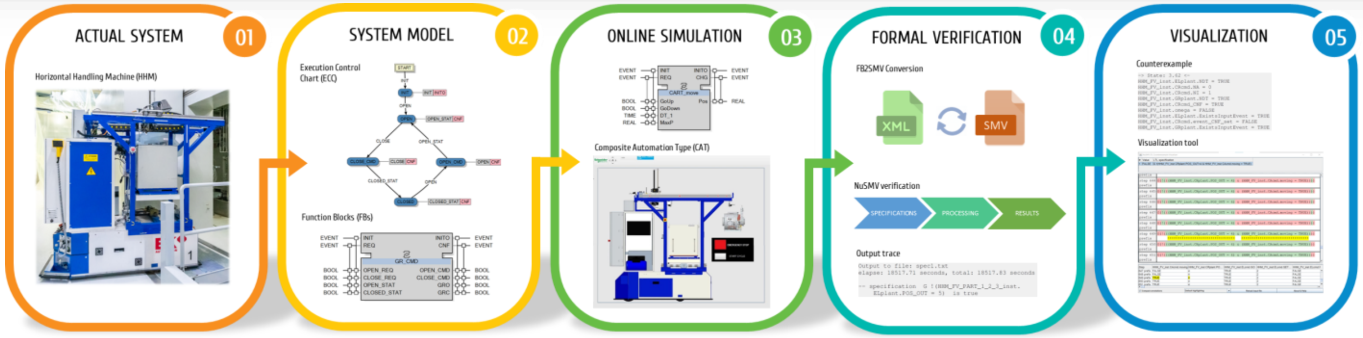


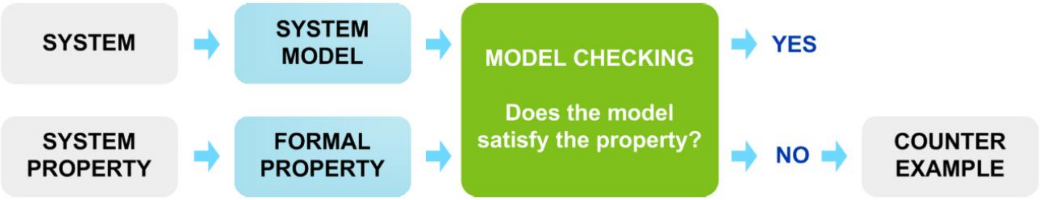
Old design vs New design

Methodology

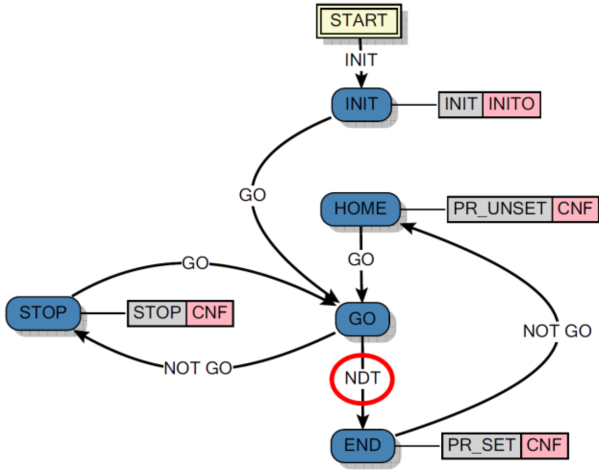
Formal verification

- Conversion of Function Blocks (XML) to **SMV** code
- Linear Temporal Logic (LTL) specifications
- **NuSMV** model checker
- Effect of introduction of **NDTs**





No	Property	Comment
1	`G !(ELplant.POS_OUT = 5)`	The *elevator* plant Function Block must never reach the *error* state in any of the sequence elements.
2	`G !(CAplant.POS_OUT = 5)`	The *trolley* plant Function Block must never reach the *error* state in any of the sequence elements.
3	`G !(CRplant.POS_OUT = 5)`	The *crane* plant Function Block must never reach the *error* state in any of the sequence elements.
4	`G !(CRplant.POS_OUT in (2..4) & CAcmd.moving = TRUE)`	The *crane* must always be in the top position while the *trolley* is moving to prevent mechanical collisions.
5	`G !(ELplant.POS_OUT = 2 & CRplant.POS_OUT = 4 & CAcmd.moving = TRUE)`	To avoid mechanical collisions, the *trolley* must not move while the HHM is lowering the TIS unit inside the HHM shielding box.
6	`G !(ELplant.POS_OUT = 1 & CRplant.POS_OUT = 4 & GRplant.GRO = TRUE)`	The pneumatic *gripper* shouldn't open until the *elevator* is not in the top position, even if the *crane* is in the lower position.

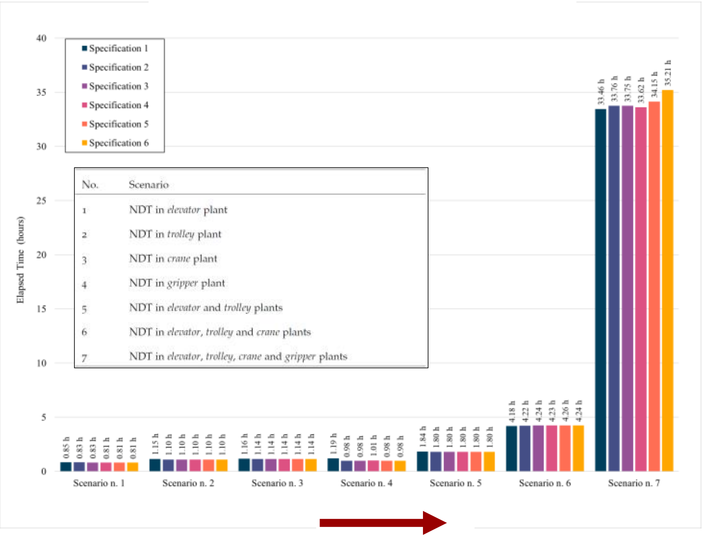


Results

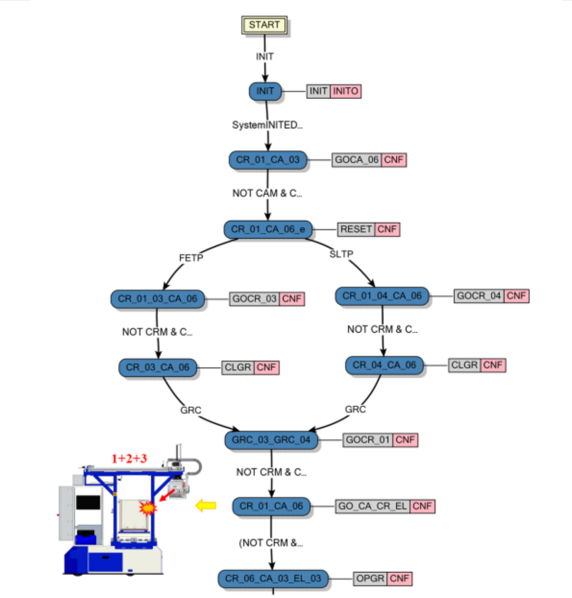
Formal verification

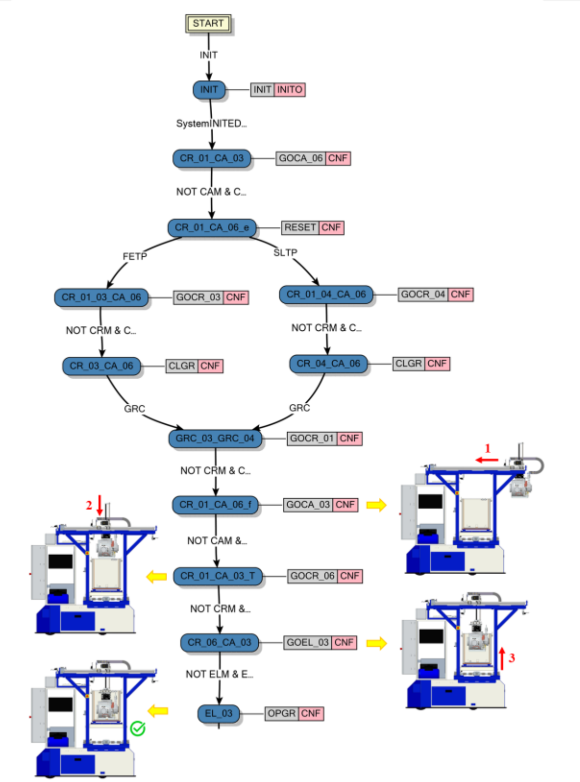
- LTL properties **verified**
- **Challenge:** spot potential collisions due to parallel execution of movements
- Counterexample visualization
- State explosion problem

NuSMV execution time



NDTs





Results and Discussion

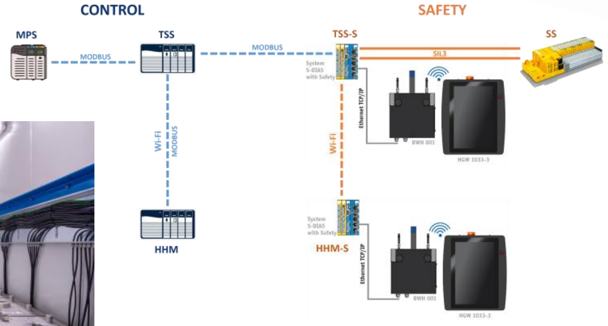
Motivation:

Remote Handling design protocols are increasingly important, conventional approaches are based on functional specification.

Contribution of the presented study:

SPES constitutes an illustrative use-case that can be used to demonstrate the advantages of:

- Remote handling consolidation
- Probabilistic Risk Assessment
- Maintenance-oriented design upgrade
- Assessment and optimization of maintenance activities
- Formal software verification



Research limitations:

- Missing integration of collected data on maintenance tasks duration with the estimated dose rate in the working position
- The Probability of Failure on Demand (PFD) does not take into account radiation effects
- Accuracy of the IEC 61499 formal verification model of the Horizontal Handling Machine (HHM)

Conclusions and future work

Main outcome

Early incorporation of **Probabilistic Risk Assessment (PRA)** techniques during the design process of automation systems in nuclear facilities can provide **substantial benefits** to the reduction of personnel **exposure**

Next research steps

- Monte-carlo simulation of the environmental dose rate to finetune the severity estimation
- Dynamic Fault-Tree Analysis (DFTA) to better estimate the likelihood of failure events
- Engineering of the novel concept design of the Extraction Electrode Positioning System
- Enrichment of the IEC 61499 formal verification model, creation of a digital-twin of safety-critical remote handling systems.

Thank you!