GIORDANO LILLI

SAFETY-DRIVEN DESIGN OF AUTOMATION SYSTEMS IN NUCLEAR FACILITIES

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede and Ivo Pletikosić.

Università
degli Studi
di Padova

UNIVERSITY OF PADOVA
Department of Management and Engineering

Doctoral School in Mechatronics and Product Innovation Engineering
XXXVI CYCLE

SAFETY-DRIVEN DESIGN OF AUTOMATION SYSTEMS IN NUCLEAR FACILITIES

Coordinator:	Prof. Daria Battini
Supervisor:	Prof. Roberto Oboe
Co-supervisors:	Dr. Alberto Andrighetto Dr. Mattia Manzolaro

Ph.D. Candidate: Giordano Lilli

Academic year: 2022-2023

Giordano Lilli:
Safety-driven design of automation systems in nuclear facilities,

SUPERVISOR:
Prof. Roberto Oboe

CO-SUPERVISORS:
Dr. Alberto Andrighetto
Dr. Mattia Manzolaro

LOCATION:
Padova, Italy

To my Family

Always in motion is the future
— Yoda

ABSTRACT

Automation technologies employed in critical tasks within nuclear facilities provide clear advantages in reducing staff exposure, but they also involve reliability challenges and safety implications connected with potential failure scenarios during operation. Nuclear laboratories and industrial automation sectors exhibit quite distinct approaches to safety assessment and harmonization. This thesis aims to demonstrate how the early integration of safety in the design process might be advantageous for both reliability enhancement and risk reduction. The study takes advantage of the remote handling infrastructure that is currently being developed for the transport and storage of radioactive Target Ion Source (TIS) units within the Selective Production of Exotic Species (SPES) nuclear research facility. A semi-quantitative Probabilistic Risk Assessment (PRA) has been developed to assess severe failure scenarios that might occur during remote handling procedures. A hybrid methodology combining HAZard and OPerability analysis (HAZOP) and Layer Of Protection Analysis (LOPA) systematically investigated the various nodes, determining the likelihood of failure scenarios, and evaluating their consequences. Following the identification of criticalities, the PRA proposed a number of safeguards, recommendations, and design upgrades that would increase the robustness and maintainability of key components. The evaluation and optimization of maintenance activities have been recognized as key weaknesses. To face this shortcoming, some key essential Front-End assemblies experienced a thorough redesign leading to an improved maintenance and the introduction of backup actuation features. In addition, the most critical maintenance tasks have been evaluated in an extensive experimental campaign that allowed to optimize the interventions in accordance with the As Low As Reasonably Achievable (ALARA) principles and to estimate the time required for each specific activity. In the last section, safety of automation software is discussed. The control logic of the Horizontal Handling Machine (HHM), as a representative use case, has been completely redesigned based on the IEC 61499 standard. This process enabled the application of an integrated tool-chain to design, simulate, and formally verify the control software prior to its deployment. The provided example demonstrates how symbolic model checking tools can be integrated into the software development process enabling the formal verification of Linear Temporal Logic (LTL) properties. Overall, the adoption of the described techniques resulted in a significant increase in the level of safety of the facility's automation. The proposed approach can be easily extended to the design of safety-critical systems in other contexts.

SOMMARIO

L'impiego dell'automazione in operazioni critiche all'interno di impianti nucleari offre chiari vantaggi legati alla riduzione dell'esposizione del personale, ma porta con sé anche problematiche di affidabilità e di sicurezza connessi ai potenziali scenari di guasto. I settori dell'automazione industriale e quello nucleare affrontano la valutazione e l'integrazione della sicurezza in modo diverso. Questa tesi vuole dimostrare come l'integrazione precoce della sicurezza nelle fasi di progettazione possa portare dei vantaggi sia in termini di miglioramento dell'affidabilità, sia di riduzione del rischio. Lo studio sfrutta l'infrastruttura di gestione remota, attualmente in fase di sviluppo, dedicata al trasporto e stoccaggio delle unità Target Ion Source (TIS) radioattive del laboratorio di ricerca nucleare Selective Production of Exotic Species (SPES). Un'analisi del rischio semi-quantitativo di tipo PRA è stata sviluppata per valutare gli scenari gravi che possono insorgere durante le procedure automatiche. Questa metodologia ibrida, che combina le analisi HAZOP e LOPA, verifica sistematicamente i vari nodi, determina la probabilità di accadimento degli scenari di guasto e valuta le loro conseguenze. Oltre all'identificazione delle criticità, l'analisi ha proposto una serie di misure di sicurezza, di raccomandazioni e di migliorie al design che possono aumentare la robustezza e la manutentabilità dei componenti più critici. Tra i punti deboli del progetto, vi è la valutazione e l'ottimizzazione degli interventi di manutenzione. Per affrontare queste tematiche, alcuni sottosistemi del Front-End sono stati riprogettati al fine di migliorarne la manutenzione e di introdurre dei dispositivi di attuazione di riserva. Inoltre, gli interventi di manutenzione più critici sono stati valutati tramite un'ampia campagna sperimentale che ha permesso di ottimizzare le attività in accordo con i principi ALARA e di stimare il tempo necessario per lo svolgimento di ciascuna attività. Nell'ultima sezione viene discussa la sicurezza del software di automazione. La logica di controllo dell'Horizontal Handling Machine (HHM), utilizzata come caso rappresentativo, è stata riprogettata secondo lo standard IEC 61499. Questo ha permesso l'applicazione di una serie di strumenti integrati che consentono lo sviluppo, la simulazione e la verifica formale del software prima del suo rilascio. Il caso in esame ha dimostrato come sia possibile integrare nelle fasi di sviluppo degli strumenti di model checking che permettano la verifica formale di proprietà di tipo LTL. L'adozione delle tecniche qui presentate ha portato ad un incremento significativo del livello di sicurezza dell'automazione nell'impianto. L'approccio proposto può essere facilmente esteso alla progettazione di sistemi critici in altri contesti.

PUBLICATIONS

[I] **G. Lilli**, L. Centofante, M. Manzolaro, A. Monetti, R. Oboe, and A. Andrighetto. “Remote handling systems for the Selective Production of Exotic Species (SPES) facility.” In: *Nuclear Engineering and Technology* 55 (2023), pp. 378–390. doi: 10.1016/J.NET.2022.08.034.

[II] **G. Lilli**, A. Andrighetto, M. Ballan, L. Centofante, S. Corradetti, F. Gramegna, O. S. Khwairakpam, M. Manzolaro, T. Marchi, A. Monetti, R. Oboe, D. Rifuggiato, and D. Scarpa. “Remote handling of radioactive targets at the SPES facility.” In: *Il Nuovo Cimento C* 46.32 (2023). doi: 10.1393/ncc/i2023-23032-y.

[III] **G. Lilli**, A. Andrighetto, L. Centofante, M. Manzolaro, A. Monetti, and R. Oboe. “The SPES target ion source automated storage system.” In: *Journal of Physics: Conference Series* (Accepted) (2023).

[IV] **G. Lilli**, M. Sanavia, R. Oboe, C. Vianello, M. Manzolaro, L. P. De Ruvo, and A. Andrighetto. “A semi-quantitative risk assessment of remote handling operations on the SPES Front-End based on HAZOP-LOPA.” In: *Reliability Engineering & System Safety* 241 (2024), p. 109609. doi: 10.1016/j.ress.2023.109609.

[V] **G. Lilli**, M. Xavier, E. Le Priol, V. Perret, T. Liakh, R. Oboe, and V. Vyatkin. “Formal Verification of the Control Software of a Radioactive Material Remote Handling System, based on IEC 61499.” In: *IEEE Open Journal of the Industrial Electronics Society* (Accepted) (2023).

[VI] L. Centofante, A. Donzella, A. Zenoni, M. Ferrari, M. Ballan, S. Corradetti, F. D’Agostini, **G. Lilli**, M. Manzolaro, A. Monetti, L. Morselli, D. Scarpa, and A. Andrighetto. “Study of the radioactive contamination of the ion source complex in the Selective Production of Exotic Species (SPES) facility.” In: *Review of Scientific Instruments* 92.5 (2021), p. 53304. doi: 10.1063/5.0045063.

[VII] S. Corradetti, M. Manzolaro, S. Carturan, M. Ballan, L. Centofante, **G. Lilli**, A. Monetti, L. Morselli, D. Scarpa, A. Donzella, A. Zenoni, and A. Andrighetto. “The SPES target production and characterization.” In: *Nuclear Instruments and Methods in Physics Research, Section B: Beam Interactions with Materials and Atoms* 488 (2021), pp. 12–22. issn: 0168583X. doi: 10.1016/j.nimb.2020.12.003.

[VIII] D. Scarpa, E. Mariotti, O. S. Khwairakpam, V. Parenti, A. Buono, P. Nicolosi, M. Calderolla, A. Khanbekyan, M. Ballan, L. Centofante, S. Corradetti, **G. Lilli**, M. Manzolaro, A. Monetti, L. Morselli, and A. Andrighetto. "New solid state laser system for SPES: Selective Production of Exotic Species project at Laboratori Nazionali di Legnaro." In: *Review of Scientific Instruments* 93.8 (2022), p. 083001. ISSN: 0034-6748. DOI: 10.1063/5.0078913.

[IX] A Andrighetto, L Centofante, F Gramegna, A Monetti, M Ballan, A Zenoni, S Corradetti, **G. Lilli**, M Manzolaro, T Marchi, A Arzenton, O. S. Khwairakpam, D Scarpa, A Donzella, E Mariotti, G Meneghetti, P Colombo, L Biasetto, R Oboe, M Lunardon, and D Rifuggiato. "Low energy radioactive ion beams at SPES for nuclear physics and medical applications." In: *Nuclear Instruments and Methods in Physics Research B* 541 (2023), pp. 236–239. DOI: 10.1016/j.nimb.2023.05.044.

[X] M. Ballan et al. "Nuclear physics midterm plan at Legnaro National Laboratories (LNL)." In: *The European Physical Journal Plus 2023 138:8* 138.8 (2023), pp. 1–79. ISSN: 2190-5444. DOI: 10.1140/EPJP/S13360-023-04249-X.

ACKNOWLEDGMENTS

First and foremost I would like to express my sincere gratitude to my supervisor, Professor Roberto Oboe, who accepted the responsibility of guiding me through this journey, demonstrating his experience, knowledge, passion, and patience on every occasion. His approach to new challenges is an inspiration for me to follow, from both the professional and human standpoint.

This endeavor would not have been possible without the strong support of my co-supervisors, Dr. Alberto Andrighetto and Dr. Mattia Manzolaro. Their constant help, respect, trust and friendship have encouraged me during these three long years on a daily basis. Thank you very much.

My gratitude extends to Prof. Chiara Vianello from the Department of Industrial Engineering of Padua University, who, along with Luca De Ruvo from INFN and Matteo Sanavia shared their knowledge and expertise, substantially assisting my research activities.

Additionally, during my PhD I had the privilege of working under the supervision of Professor Valeriy Vyatkin from Aalto University in Finland and to collaborate with Midhun Xavier from Luleå University in Sweden. I am truly thankful for this opportunity, the collaboration has been incredibly rewarding, and played a pivotal role in the achievement of the results presented in this thesis.

I cannot forget mentioning Michele and Denis, the technicians that helped me in my project with their suggestions, skills and insights. In addition, I would like to thank my colleagues who volunteered their time to assist me as operators during the experimental campaigns.

A big thanks goes to my friends, Alberto, Lisa and Elizabeth. Four years ago I never thought I would have this experience. Everything started as a challenge, mainly with myself. I have spent the majority of my time with them, and I have always felt a deep understanding, willingness, empathy, and encouragement. Thanks for making me feel part of a family despite the ups and downs of this period.

The most important thanks goes to my wife Martina, who has always believed in me, who has instilled in me the strength to never give up, who has always been present to listen to my difficulties, and who has been a big support, especially during this final period. Thanks for your love, motivation, and patience.

Last but absolutely not least, few words to my son Gioele. Through this work, I sincerely wish to demonstrate that nothing is impossible and that it is never too late to get into the game. I love you, this thesis is for you.

CONTENTS

I Introduction

II Consolidation

III Optimization

v Conclusions

vi Appendix

LIST OF FIGURES

LIST OF TABLES

LISTINGS

ACRONYMS

ACS	Access Control System
AGM	Absorbed Glass Mat
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
ALARA	As Low As Reasonably Achievable
ALPI	Acceleratore Linear Per Ioni
ARIEL	Advanced Rare IsotopE Laboratory
ASM	Abstract State Machine
BDD	Binary Decision Diagram

BMC	Bounded Model Checking
CAN	Controlled Area Network
CAT	Composite Automation Type
CERN	European Organization for Nuclear Research
CM	Conditional Modifier
CTL	Computation Tree Logic
CPS	Cyber-Physical System
CPU	Central Processing Unit
DFTA	Dynamic Fault Tree Analysis
DoE	Design of Experiment
EC	Enabling Condition
ECC	Execution Control Chart
EEPS	Extraction Electrode Positioning System
EPICS	Experimental Physics and Industrial Control System
ER	Essential Requirement
ESS	European Spallation Source
EU	European Union
FAIR	Facility for Antiproton and Ion Research
FB	Function Block
FBD	Function Block Diagram
FBME	Function Blocks Modeling Environment
FEBIAD	Forced Electron Beam Induced Arc Discharge
FSM	Finite State Machine
FSoE	FailSafe over ErherCAT®
GANIL	Grand Accélérateur National d'Ions Lourds
GUI	Graphical User Interface
HAZOP	HAZard and OPerability analysis
HHM	Horizontal Handling Machine
HI	Hazard Identification
HMI	Human Machine Interface
HRI	Human-Robot Interface
HRIBF	Holifield Radioactive Ion Beam Facility
IAEA	International Atomic Energy Agency
iCPS	industrial Cyber-Physical System
ICRP	International Commission on Radiological Protection
IDE	Integrated Development Environment

IE	Initiating Event
IFMIF	International Fusion Materials Irradiation Facility
IP	Internet Protocol
IPL	Independent Protection Layer
INFN	Istituto Nazionale di Fisica Nucleare
ISAC	Isotope Separator and ACcelerator
ISOL	Isotope Separation On-Line
ISOLDE	Isotope Separator On-Line DEvice
ITER	International Thermonuclear Experimental Reactor
JET	Joint European Torus
LD	Ladder Diagram
LINAC	LINear particle ACcelerator
LOPA	Layer Of Protection Analysis
LNL	Laboratori Nazionali di Legnaro
LTL	Linear Temporal Logic
MAD	Material Access Door
MEDICIS	Medical Isotopes Collected from ISOLDE
MHM	Manual Handling Machine
MPS	Machine Protection System
NC	Normally Closed
NDT	Non-Deterministic Transition
NPP	Nuclear Power Plant
ORNL	Oak Ridge National Laboratories
PFD	Probability of Failure on Demand
PLC	Programmable Logic Controller
PPB	Primary Proton Beam
PPE	Personal Protective Equipment
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Analysis
PTZ	Pan Tilt Zoom
RAMS	Reliability, Availability, Maintainability and Safety
RH	Remote Handling
RHS	Remote Handling Supervisor
RIB	Radioactive Ion Beam
RILIS	Resonance Ionization Laser Ion Source
RP	Radiation Protection

SIL	Safety Integrity Level
SMV	Symbolic Model Verifier
SNS	Spallation Neutron Source
SP	Supply Point
SPN	Stochastic Petri Net
SPST	Single Pole Single Throw
ST	Structured Text
STPA	System Theoretic Process Analysis
RP	Radiation Protection
SCCS	Safety-Critical Control System
SIL	Safety Integrity Level
SSID	Service Set IDentifier
SSIS	SPES Surface Ion Source
SPES	Selective Production of Exotic Species
SPST	Single Pole Single Throw
TIS	Target Ion Source
TRIUMF	Canada's particle accelerator centre
TS	Technical Stop
TSS	Temporary Storage System
UPS	Uninterruptible Power Supply
VIF	Variance Inflation Factor
VLAN	Virtual Local Area Network
WDP	Work and Dose Planning
XML	eXtensible Markup Language

Part I

INTRODUCTION

1 INTRODUCTION

1.1 BACKGROUND AND SIGNIFICANCE

The integration of automation systems for process control and maintenance tasks in radioactive environments is commonly regarded as an effective strategy to reduce personnel exposure. Following the gradual spread and growing maturity of multipurpose robotic solutions over the past decades, Nuclear Power Plants (NPPs) have been identified as an ideal field of application. In particular, the employment of teleoperated systems is beneficial for carrying out regular maintenance activities as well as unanticipated interventions during plant operation [1]. The hazardous scenarios arising after a severe nuclear accident constitute another domain where employing robots can provide substantial advantages [2]. High radiation levels, physical constraints, along with toxic and flammable atmosphere, can limit personnel access in such situations. The Fukushima Daiichi NPP accident [3] has provided a significant demonstration of the actual potential of robotics in creating novel concepts specifically designed for the accomplishment of critical tasks such as inspections [4, 5], retrieval of fuel debris [6], aerial surveys [7], and monitoring of soil radioactive contamination [8]. Some examples are displayed in Fig. 1.1. Aside from accident events, trustworthy mobile robots and remote equipment play an important role in nuclear site decommissioning [9–12], where their use is justified by a significant reduction in cumulative doses received by project staff [13]. Typical applications include dismantling of nuclear equipment [14], replacement of exhausted filters [15], or decontamination [16]

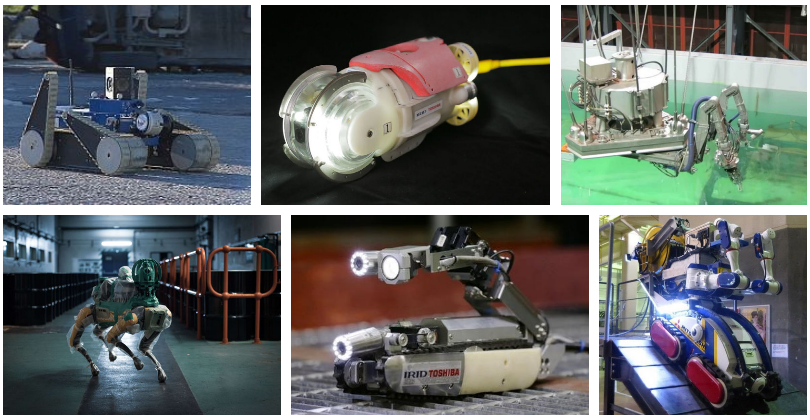


Figure 1.1: Examples of teleoperated robots used in inspection tasks in NPPs following a major accident.

In addition to NPPs, which constitute a consolidated, industrial field of application that makes extensive use of robotics, particle accelerators represent an alternative domain where Remote Handling (RH) maintenance procedures can provide significant benefits in addressing their distinctive safety challenges and mitigating the peculiar radiological conditions [17]. Designing, operating, and maintaining the equipment for new accelerator facilities is significantly impacted by the steady rise in beam energy and intensity. As radiation levels rises, Radiation Protection (RP) becomes progressively more important and demanding. In this scenario, RH emerges as a key technology to be deployed for the management of modern accelerator facilities. At CERN, teleoperated robots have been successfully employed in crucial interventions [18–20] and survey campaigns [21–23], some multi-purpose systems are visible in Fig. 1.2. In this context, 3D mixed reality Human-Robot Interface (HRI) [24–26] and vision algorithms [27, 28] provided an invaluable support to skilled operators carrying out remote safety-critical activities. Unique logistical constraints, harsh environment, severe radiological conditions and significant payloads are all contributing factors that are commonly experienced in other laboratories, strengthening the necessity for RH solutions. Meaningful examples are offered by the upcoming FAIR [29, 30], and research centers exploiting spallation processes, such as SNS [31, 32] and ESS [33]. RH tools, including servomanipulators and bridge cranes, are paired with dedicated Hot-Cells in the aforementioned installations to perform specific maintenance tasks.

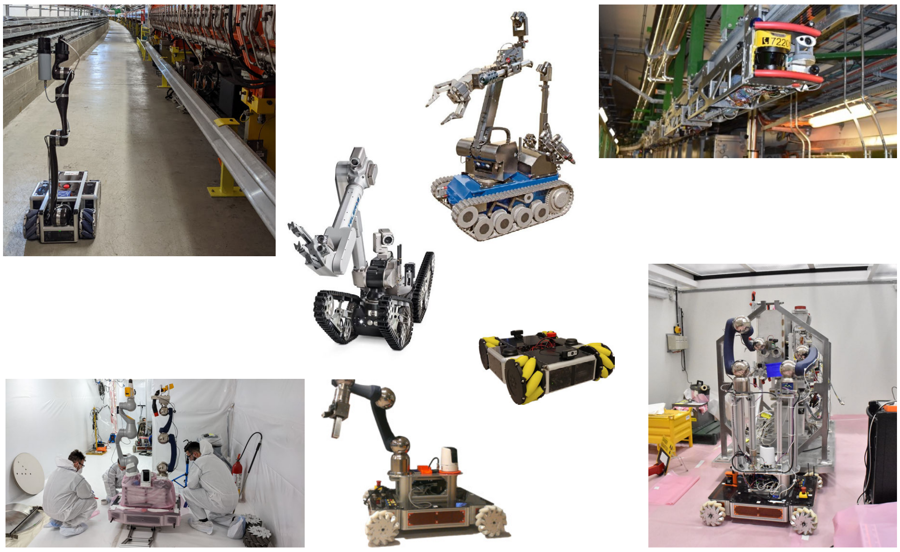


Figure 1.2: Robotic systems used at CERN for remote maintenance activities. Credit: CERN.

Fusion facilities, which represent the state-of-the-art in terms of RH implementation, have contributed significantly to the "Design for Maintenance" culture and to the development of methodologies for the design of such systems [34]. Specifically, RH has been recognized by the ITER project as the nominal (and the only viable) method for reactor maintenance. This approach enabled RH to be considered as part of the machine's early conception. The development of procedures, equipment and tools benefits from the operational feedbacks from Joint European Torus (JET) [35], where designers implemented a comprehensive RH framework that allowed for the successful execution of long-term maintenance campaigns in completely remote settings, as well as full remote recovery strategies from in-vessel failure. A RH maintenance robot inside the JET tokamak is visible in Fig. 1.3. The acquired experience emphasized the value of fine-tuning RH procedures in dedicated training facilities and the importance of monitoring the operation area through cameras. Additionally, the implemented tools and procedures contributed in understanding the operational challenges for future plants. Two parallel approaches are required for the successful implementation of the ITER remote maintenance framework. On one hand, the design of plant components and layout must adhere to rigorous RH requirements aimed at ensuring reliable, effective, and optimized remote maintenance throughout its operational life [36, 37]. Effective RH systems [38–40] and procedures [41], on the other hand, must be developed for the safe accomplishment of repair, replacement of parts, testing, and re-commissioning activities. The assessment of the radiation environment in which the RH systems will operate is a

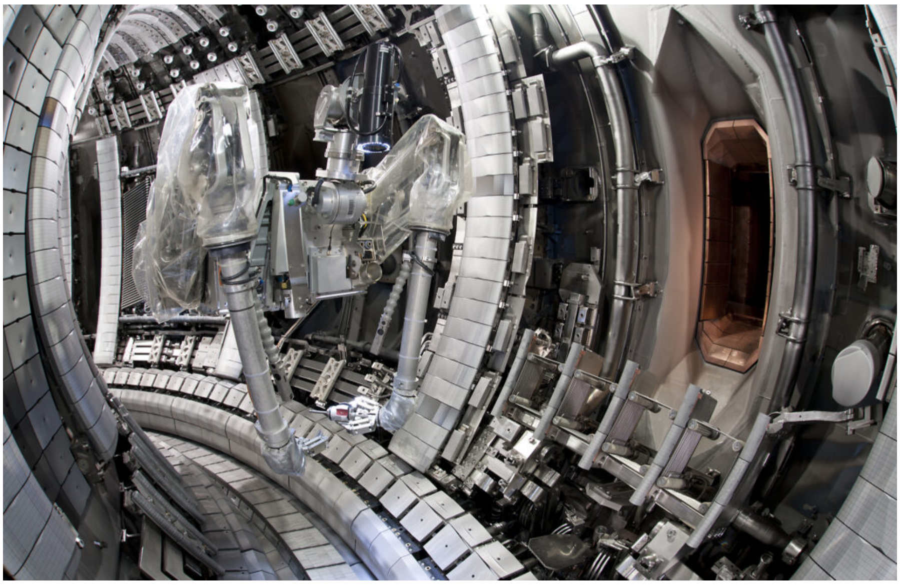


Figure 1.3: Remote handling system used in the JET nuclear reactor. Credit: UKAEA.

vital stage in the design of such equipment and methodologies [42]. This evaluation allows to optimize the shielding layout of critical regions and to develop reliable procedures which take into account the actual operating conditions [43]. The IFMIF RH development have significantly benefited from the best practices and the experiences gained at ITER [44, 45]. In this instance as well, a thorough process has been put in place for the development of specific tools [46], concepts [47] and procedures [48] for the execution of remote maintenance tasks. The design approach, in particular, was based on a specific methodology that was established to encompass all of the necessary aspects required for the accurate implementation and execution of remote operation within the facility [49].

In general, nuclear facility maintenance activities require careful consideration since they may directly or indirectly influence equipment reliability. Moreover, any later consequences triggered by maintenance problems can result in operational interruption, thus affecting the safety of the plant. [50] Still, the opportunity to decrease workers exposure, prevent human errors, increase tasks reliability and repeatability, and cope with risks are the primary driving reasons for the implementation of process automation solutions as well as remote maintenance strategies [51].

We should make a clear distinction between automation systems directly involved in the process and robotic solutions employed in remote maintenance operations. While the first category includes systems that are usually meant to perform predetermined, reliable and repetitive tasks, the second group encompasses flexible and reconfigurable equipment, typically teleoperated, for the execution of specific interventions within an unstructured environment [52].

Radioactive Ion Beam (RIB) facilities provide an interesting and appealing setting for the deployment of RH solutions since they combine these two domains. Indeed, while RH becomes increasingly important for automating key stages of the process, critical maintenance activities might benefit from robotics to reduce worker exposure [53] in accordance with As Low As Reasonably Achievable (ALARA) principles [54, 55]. The deep integration of RH systems within the process automation strongly differentiates RIB facilities from other types of applications, in which robotics is reserved for maintenance procedures. Significant examples of Isotope Separation On-Line (ISOL) facilities employing RH systems in the RIB production process can be found within ISOLDE [56] and MEDICIS [57] at CERN, see Fig. 1.4, or ISAC and ARIEL experiments at TRIUMF [58],

The design of reliable automation systems for the aforementioned nuclear contexts must deal with specific challenges posed by the peculiar operational environment. Notably, two distinct approaches can be pursued to mitigate the effects of radiations on system degradation: On one side, through robust design and the use of radiation-tolerant

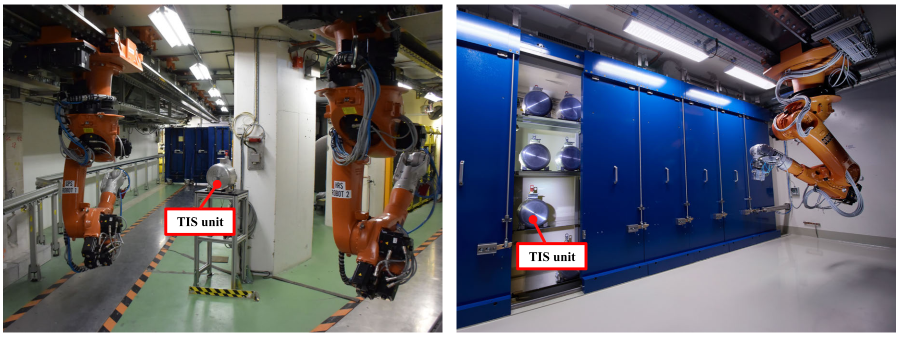


Figure 1.4: (left) ISOLDE and (right) MEDICIS remote handling robots.

materials [59], lubricants [60, 61], and electronics [62, 63], and simultaneously, through specific compensatory strategies such as the removal of sensitive components, the incorporation of hardware and software redundancies, or the implementation of correction algorithms [64].

The effective integration of automation technologies within nuclear facilities is the result of a comprehensive approach that includes both the design of RH systems and the development of RH-compliant experimental equipment. An example of a robot-friendly architecture is given in [65]. As mentioned earlier, even though the experience gained within NPPs, accelerator complexes, and fusion plants has resulted in an increasing availability of detailed design guidelines, best practices, and methodologies that have provided immeasurable advantages in the remote maintenance culture and the early integration of RH-compliant interfaces during the design stage of the plant, there is still a lack in the perception of how the design of both the plant and the RH system can affect personnel safety in failure scenarios. While there is no doubt about the positive impact of RH systems in reducing personnel exposure through the implementation of remote maintenance procedures, the potential recovery actions that would have to be planned in the event of RH equipment failure raise a serious concern in terms of RP and safety of workers.

The review of state-of-the-art methodologies and protocols for developing RH solutions in fusion facilities [49, 66] revealed that the safety evaluation of the entire system and the analysis of recovery scenarios are usually deferred to a final stage of the process. However, IAEA safety standards stress the advantages of carrying out the safety assessment during the design stage, or as early as feasible in the lifespan of activities that give rise to radiation risks [67]. This strategy supports in identifying and resolving plant vulnerabilities [68], offers insights into the safety aspects of facility design and operation, and provides plant designers an unbiased benchmark that can be utilized to rank the safety implications of different design options [69]. A further reference can be found in the industrial sector, where the hazard identification [70] and the introduction of inherently safe design measures during the engineering stage represent the primary means for reducing the risk associated with machinery [71, 72].

This open point was tackled in this thesis by taking advantage of the RH framework that is currently in development for the future Selective Production of Exotic Species (SPES) facility. A combined Probabilistic Risk Assessment (PRA) approach has been implemented during the design stage of both the SPES plant and the RH equipment. As specific challenge, the analysis focuses on the potential repercussions of RH failure conditions on personnel exposure during recovery maintenance operations. These actions are extremely critical since they are not intended to be performed remotely, but rather by skilled operators. The early evaluation of failure scenarios enables for the improvement of overall safety of the facility while providing a clear indication of the system's weaknesses. The analysis results are used to achieve two primary goals: reducing the need for hands-on interventions (through design upgrades and software verification) and, when unavoidable, optimizing maintenance activities. A preventive assessment of required maintenance tasks has been incorporated in the study as a direct and effective application of ALARA principles, with the goal of further minimizing their residual risk.

This work presents a safety-driven design approach for automation systems in nuclear facilities, aiming at investigating how early application of PRA techniques might improve the overall safety of the facility, optimize maintenance interventions and minimize personnel exposure. The study's findings are intended to provide support to the development of existing and future accelerator facilities [73–77].

1.2 RESEARCH OBJECTIVES

The aim of this thesis is to investigate the impact of a safety-driven design approach, applied to automation systems within nuclear facilities, on the predicted personnel exposure during planned and unexpected maintenance interventions. More precisely, the study's main goal is to demonstrate how safety assessments of key remote handling procedures, applied during the RH machines early design stage, have the potential to highlight system weaknesses and drive safety-oriented hardware, software and organizational design improvements with two specific objectives: implementing remote recovery solutions that do not require on-the-field human assistance, and minimizing personnel exposure during residual maintenance activities. The overall objectives of the Ph.D. project have been identified in accordance with the fundamental goals of the wider field of research, aiming at the development of effective methodologies and best practices for the design of safe automated systems operating in hazardous environments. The expected outcome of the study is to provide a significant contribution to the field of design and operation of reliable remote handling systems, by presenting the proposed design process as a general and meaningful strategy that can be implemented in different demanding applications, such as RIB facilities, particle accelerators or fusion reactors. The three fundamental goals of the thesis are discussed in further detail below.

Safety assessment

This procedure seeks to identify the primary sources of hazard and assess the likelihood of failure of crucial RH elements by applying specific PRA techniques during their preliminary design stage. As initial step, by means of a rigorous process aimed at detecting potentially hazardous conditions and operational issues, the analysis will look into the system's deviations from the behavior expected by design and evaluate the resulting failure scenarios that may lead to a risk for personnel or the environment. In the second phase the study will define a set of safeguards, as technological and organizational solutions, that will help in decreasing the need for personnel access by providing effective remote recovery alternatives, as well as minimizing the severity of mandatory physical maintenance activities. The effectiveness of the proposed protection layers in preventing the propagation of initial failure events to actual hazardous consequences is evaluated in the third stage. As the final result, the evaluation will highlight the missing safety measures and develop a roadmap with the milestones to accomplish in order to ensure that the systems operate in line with the specified requirements. The benefits of early application of PRA techniques for remote handling tasks and their impact on the improvement of key component design have been explored in [78].

Upgrade of the system

By incorporating safety principles during the design stage of automation systems in nuclear plants, it would be possible to limit, or at least optimize, the necessary maintenance activities that will be required at some point during the plant's life cycle. The enhancement process aims to upgrade two main aspects of RH systems.

From the hardware point of view, the redesign's goal is the implementation of technical solutions and inherently safe measures that will enable the execution of full remote recovery actions following a failure scenario specified by the risk assessment, hence avoiding the need for personal assistance. Nevertheless, if the operator presence is essential for specific types of interventions, the study focused on applying "Design for Maintenance" solutions that will optimize the effectiveness of tasks while minimizing worker exposure. The objective of the investigation in this phase is to showcase the positive effect of introducing backup actuation systems in the likelihood reduction of high-exposure risk maintenance procedures.

On the software side, the Ph.D. project aims at addressing the problem of Safety-Critical Control System (SCCS) testing by presenting an effective strategy for developing modular applications, implementing automatic verification procedures, and reducing system complexity through an automated tool-chain which takes advantage of the IEC 61499 standard [79]. The method's intent is to reduce the likelihood of failure scenarios by improving software reliability.

Maintenance review and optimization

The study's final mission is to illustrate the advantages of a proactive approach to maintenance interventions in the reduction of expected human exposure, given that on-site upkeep actions are sometimes unavoidable. The procedure is aimed at evaluating the various tasks to be carried out in a highly radioactive locations through a comprehensive maintenance assessment. Specifically, experimental tests will allow to estimate the time required for the execution of specific interventions and, provided the dose rate in the working location, the operator's absorbed dose. The ensuing statistical analysis will identify the most significant factors that may be adjusted to shorten their duration. In addition, the test campaign will attempt to spot any critical issue, standardize the intervention parameters, and define detailed procedures to assist operators.

1.3 OUTLINE OF THE THESIS

The dissertation consists of eight chapters, organized as follows:

Chapter 1 establishes the context for the study, clarifies the problem statements, highlights the research objectives and points out the significance of the work in relation to the existing body literature.

Chapter 2 introduces the thesis theoretical framework and describes the PRA methodologies as well as the automation software synthesis and analysis principles adopted in the study for the safety assessment and the formal verification of safety-critical software, respectively. The motivations behind the choice of the proposed research instruments are discussed providing references to prior studies in which the same techniques have been employed in similar and alternative contexts. The SPES facility is finally introduced, emphasizing its relevance as a use case for the demonstration of the benefits provided by safety-driven design methodologies applied to nuclear Remote Handling (RH) systems, in the reduction of personnel exposure.

Chapter 3 presents the SPES Remote Handling (RH) framework, describing the facility layout, the software architecture, the communication infrastructure, the functional requirements resulting from the Target Ion Source (TIS) unit life cycle, and the main RH systems: the Front-End, the Horizontal Handling Machine (HHM) and the Temporary Storage System (TSS). The chapter provides a clear comparison between the prototypes in their concept stage and the finalized machines following the integration of safety-driven design upgrades, radiation tolerance measures and availability principles.

Chapter 4 describes a semi-quantitative Probabilistic Risk Assessment (PRA) of RH procedures in the vicinity of the SPES Front-End. Using a blended approach based on two techniques, the likelihood of critical failure scenarios, their effects, and safety measures are assessed. In the first phase, a HAZard and OPerability analysis (HAZOP) analysis is applied as a qualitative risk assessment tool to systematically identify dangerous situations and operational problems that may arise from unexpected behavior of essential elements leading to potentially dangerous (unintended) repercussions. The second stage involves the use of Layer Of Protection Analysis (LOPA) to evaluate the positive changes in the system's risk level provided by the implementation of the recommended Independent Protection Layers (IPLs), as well as their ability to prevent hazardous situations, thus confirming the validity of the advised safeguards. The chapter finally outlines the key findings of the PRA and lays out a clear roadmap with the milestones that must be met prior to the facility's start-up in order to achieve the desired safety goals. This includes redesigning critical assemblies to incorporate backup actuation features, verifying control software and the completing partially implemented IPLs, such as establishing a preventive maintenance program and standardized operating procedures.

Chapter 5 builds upon the presented PRA discussing the redesign process of a crucial motion axis installed on the SPES Front-End: the Extraction Electrode Positioning System (EEPS). The iterative methodology aims at addressing the shortcomings highlighted by the HAZOP-LOPA analyses, mainly related to the lack of a backup motion interface and accessibility issues. The study presents three distinct system reviews aimed at the progressive resolution of the existing vulnerabilities. The proposed innovations are validated by field experiments which demonstrate the reduction in maintenance duration provided by the new system revision.

Chapter 6 extends the optimization of the maintenance activities through a comprehensive assessment focused on the mitigation of residual risk provided by on-site upkeep tasks. The presentation covers the methodology, the results, and the analysis of experimental maintenance tests designed to estimate the duration of various tasks. The outcomes of the study will represent a significant asset in the proactive estimation of personnel exposure prior to real interventions. The experimental sessions additionally provided the opportunity to identify potential vulnerabilities, establish standardized operating procedures, and acquire knowledge to develop an effective operator training program.

Chapter 7 completes the RH upgrade process describing the benefits provided by the migration of the IEC 61131-based software of the HHM to an IEC 61499 architecture, which enabled the implementation of offline and online software verification techniques. This chapter outlines the development of flexible and reconfigurable control software based on IEC 61499, as well as its formal verification using an integrated tool-chain. The presented findings support the tool-chain's validity by illustrating the benefits of formal system verification in detecting non-trivial software design flaws that may result in a failure event under particular conditions.

Chapter 8 reports a detailed summary of the research outcomes, outlines the significant contribution of the dissertation, and discusses the implications of the proposed design process on the development of novel automation systems operating in hazardous settings.

Figure 1.5 reports a graphical overview of the Ph.D. research project and the thesis outline.

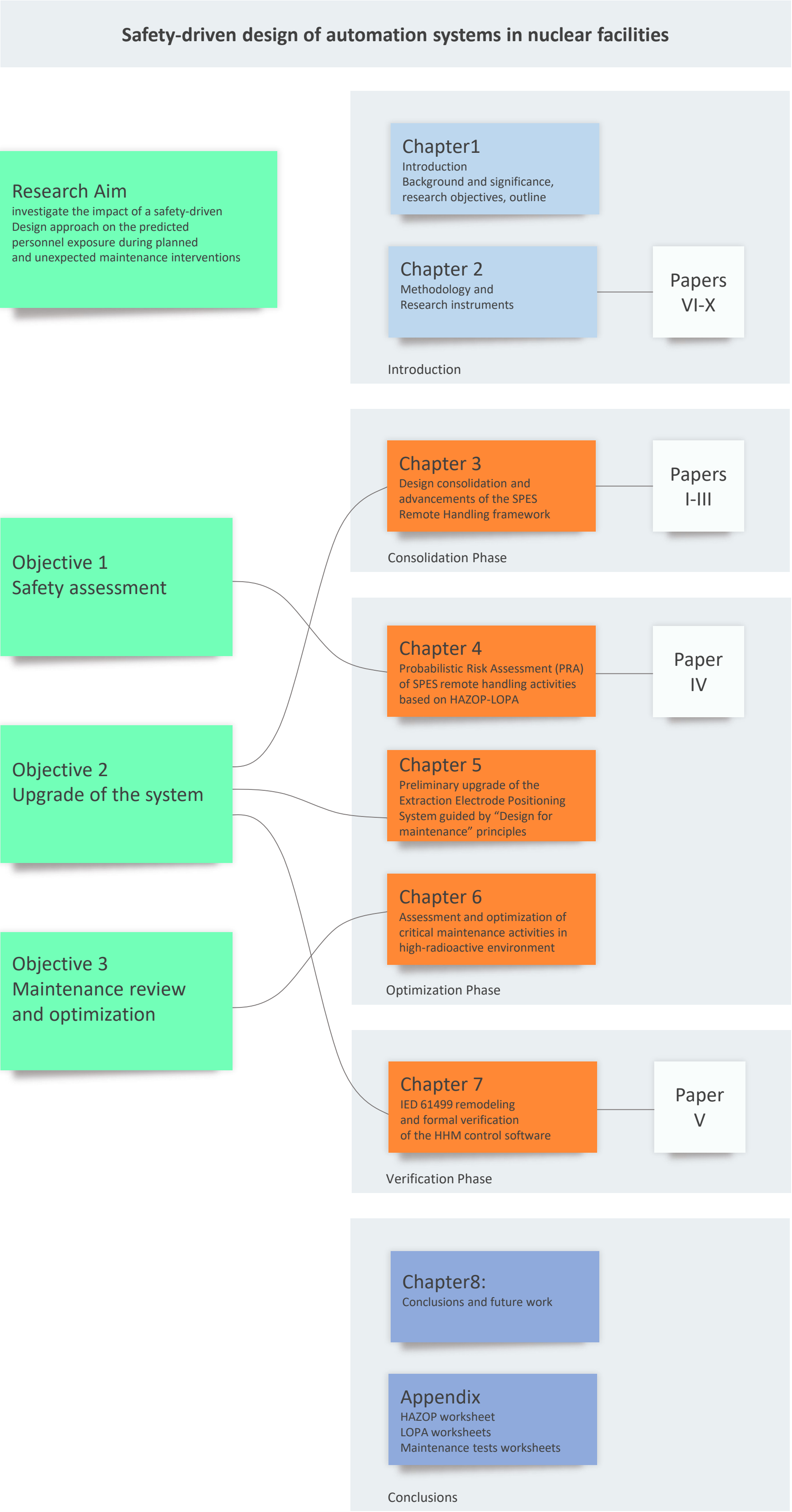

Safety-driven design of automation systems in nuclear facilities
Research Aim
investigate the impact of a safety-driven Design approach on the predicted personnel exposure during planned and unexpected maintenance interventions
Chapter1
Introduction
Background and significance, research objectives, outline
Chapter 2
Methodology and Research instruments
Papers VI-X
Introduction
Chapter 3
Design consolidation and advancements of the SPES Remote Handling framework
Papers I-III
Consolidation Phase
Objective 1
Safety assessment
Chapter 4
Probabilistic Risk Assessment (PRA) of SPES remote handling activities based on HAZOP-LOPA
Paper IV
Objective 2
Upgrade of the system
Chapter 5
Preliminary upgrade of the Extraction Electrode Positioning System guided by "Design for maintenance" principles
Chapter 6
Assessment and optimization of critical maintenance activities in high-radioactive environment
Objective 3
Maintenance review and optimization
Optimization Phase
Chapter 7
IED 61499 remodeling and formal verification of the HHM control software
Paper V
Verification Phase
Chapter8:
Conclusions and future work
Appendix
HAZOP worksheet
LOPA worksheets
Maintenance tests worksheets
Conclusions

Figure 1.5: Graphical representation of the Ph.D. project structure and the thesis outline.

2 METHODOLOGY AND RESEARCH INSTRUMENTS

2.1 CONVENTIONAL SAFETY AND RADIATION PROTECTION

Conventional safety within Italian industrial contexts is regulated by the Legislative Decree 81/2008 [80], which requires work equipment to comply with the safety requirements defined by the Machinery Directive 2006/42/CE [71, 81]. Directives are employed by the European Union (EU) to formulate general safety objectives on specific topics [82, 83]. The "presumption of conformity" with the Essential Requirements (ERs) of the directives (and the subsequent CE marking) can be achieved by adhering to European harmonised standards, which specify the minimum requirements for product design and assessment. Harmonised Standards are classified into three categories: A, B and C:

- Type A (general safety standards): contain basic concepts and general design principles that can be applied to machinery. An example is ISO 12100 [72], describing iterative risk assessment and reduction methodologies.
- Type B (safety standards common to groups): deal with specific safety aspect or a particular type of safeguard that can be applied on a variety of machinery. This category is further divided in B1 [84–87] and B2 [88, 89] standards.
- Type C (machine-related standards): contain the detailed safety requirements for a particular machine or group of machines [90].

An overview of the relationship between national laws and EU directives is outlined in Fig. 2.1

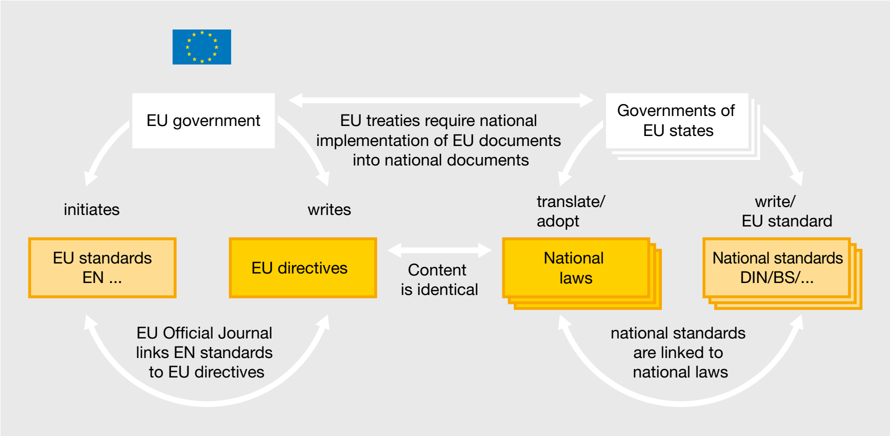

EU government
EU treaties require national implementation of EU documents into national documents
Governments of EU states
initiates
writes
translate/ adopt
write/ EU standard
EU standards EN ...
EU directives
Content is identical
National laws
National standards DIN/BS/...
EU Official Journal links EN standards to EU directives
national standards are linked to national laws

Figure 2.1: Harmonised standards and national laws.

The 2006/42/CE Directive defines a machinery as an assembly consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application. The recently issued Machinery Regulation (EU) 2023/1230 [91] has extended the scope of the Directive, encompassing digital components, such as the control software. The main goal of these directives is to ensure a common safety level in machinery placed on the European market. Specifically, the aim of risk assessment is to reduce risks as far as possible, identifying potential hazards, applying appropriate safeguards, and informing operators of the existing residual risks.

The Machinery Directive excludes from its scope the systems specially designed for nuclear purposes which, in the event of failure, may result in an emission of radioactivity. The reason may be found in the risk reduction approach provided by safety standards. Considering the mechanical risk as an example, the conventional strategy to avoid injuring operators is to stop any movements in the event of potentially harmful scenario. In the context of nuclear facilities, the approach intended to address this event can be slightly different. Indeed, an emergency stop procedure may result in a later recovery intervention with a high radiological impact. Conversely, a controlled sequence aimed at restoring the system safe configuration and minimize the overall dose contribution of the plant is definitely preferable. Still, the mechanical risk of the machinery may be addressed by an Access Control System (ACS) preventing the personnel access in the operating zones of automatic systems while they are in service.

Although not strictly required, the International Atomic Energy Agency (IAEA) emphasizes the benefits provided by the risk reduction approach adopted for conventional machinery in designing automation systems suited to nuclear applications [70]. Specifically, EN ISO 12100 [72] provides risk assessment and reduction principles to help designers in achieving safety of the machinery. The standard proposes the application of inherently safe design measures as first step of the risk reduction process, as outlined in Fig. 2.2. These measures are intended to achieve risk reduction directly from the design stage, by changing the design or operating characteristics of the machine without the use of guards or protective devices [92]. This goal can be achieved thanks to the early incorporation of risk assessment into the design stage of automation systems and considering the safety aspects directly within the engineering process. In this study, Chapter 4 presents the benefits provided by the application of a Probabilistic Risk Assessment (PRA) to critical remote handling scenarios, on the reduction of the likelihood of recovery interventions under severe radiological conditions. Additionally, Chapter 5 describes the mechanical redesign of a motion system aimed at improving its maintainability and operational safety.

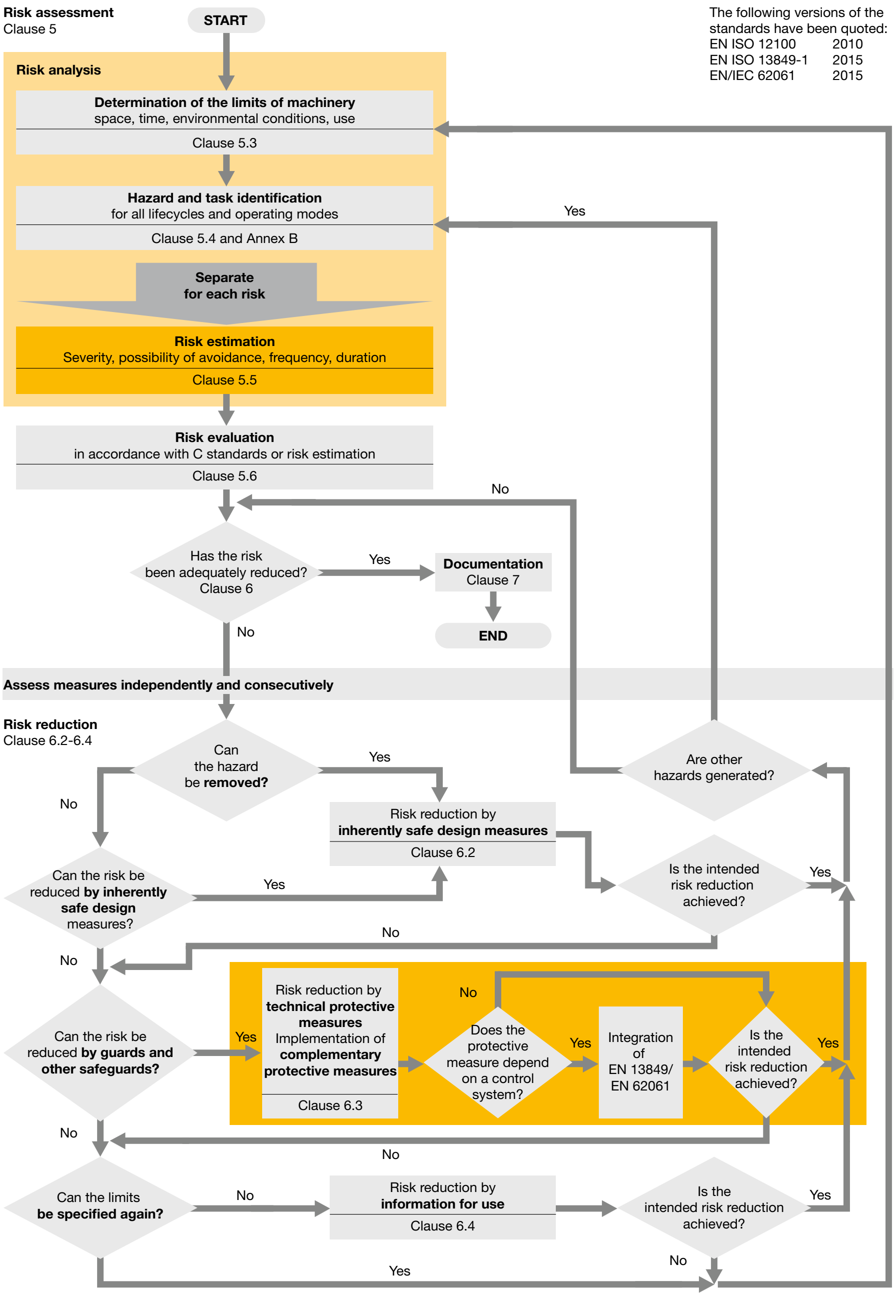

Risk assessment
Clause 5
START
The following versions of the standards have been quoted:
EN ISO 12100 2010
EN ISO 13849-1 2015
EN/IEC 62061 2015
Risk analysis
Determination of the limits of machinery
space, time, environmental conditions, use
Clause 5.3
Hazard and task identification
for all lifecycles and operating modes
Clause 5.4 and Annex B
Separate for each risk
Risk estimation
Severity, possibility of avoidance, frequency, duration
Clause 5.5
Risk evaluation
in accordance with C standards or risk estimation
Clause 5.6
Has the risk been adequately reduced? Clause 6
Documentation
Clause 7
END
Yes
No
Assess measures independently and consecutively
Risk reduction
Clause 6.2-6.4
Can the hazard be removed?
Risk reduction by inherently safe design measures
Clause 6.2
Are other hazards generated?
Is the intended risk reduction achieved?
Can the risk be reduced by inherently safe design measures?
Can the risk be reduced by guards and other safeguards?
Risk reduction by technical protective measures
Implementation of complementary protective measures
Clause 6.3
Does the protective measure depend on a control system?
Integration of EN 13849/ EN 62061
Is the intended risk reduction achieved?
Can the limits be specified again?
Risk reduction by information for use
Clause 6.4
Is the intended risk reduction achieved?

Figure 2.2: ISO 12100 risk assessment and reduction flowchart.

Following the risk reduction process, a residual risk is present. While conventional hazards can be mitigated through the implementation of safeguards, from the radiological perspective this may imply a risk of personnel exposure. The residual radiological risk provided by the use of Remote Handling (RH) systems is effectively addressed by Radiation Protection (RP), which aims at protecting people and the environment from the harmful effects of ionizing radiation. The annual limits of maximum effective dose for a professionally exposed workers are defined by national laws [93]. In addition, more conservative policies can be applied by different institutions.

According to the International Commission on Radiological Protection (ICRP) recommendation 60 [94], any exposure of people to ionizing radiation should be controlled and based on three fundamental principles:

- *justification:* any exposure of people to ionizing radiation must be justified;
- *limitation:* individual doses must not exceed legal restrictions;
- *optimization:* individual and collective doses must be kept As Low As Reasonably Achievable (ALARA).

In this study, ALARA principles [95, 96] have been incorporated in the mechanical redesign of a critical system, as described in Chapter 5, and in the optimization of maintenance activities, see Chapter 6.

2.2 PROBABILISTIC RISK ASSESSMENT

Probabilistic Risk Assessment (PRA) is a methodical and thorough procedure aimed at assessing risks of complex technical plants along their life-cycle. Risk is described as the potential consequence of an event subject to hazard(s). In PRA, risk is defined by two factors: the Severity (S) of the undesirable consequence that can result from the initiating event, and the Likelihood (L) of the analyzed failure event. A quantitative risk assessment categorizes consequences using a Severity score and expresses their Likelihoods as probabilities or frequencies.

PRA techniques are effectively employed in a variety of domains, including the marine sector [97–99], Natech events [100–102], and the process industry [103–110]. In nuclear applications, PRA has been extensively employed for the evaluation of complex plants, infrastructures and logistics. In recent years the analysis have been extended to Nuclear Power Plant (NPP) multi-unit accidents [111, 112]. In addition, the development of enhanced integrated methodologies has been beneficial for the assessment of nuclear batteries [113], nuclear fuel transfer [114], and critical infrastructures [115]. The continuous advances applied to risk-oriented reliability analysis led to the development of various optimization algorithms which have been investigated to mitigate the “state explosion” problem and limit the computational demands of dynamic PRA methodologies [116–119].

Autonomous robotic solution employed in complex scientific laboratories must comply with rigorous standards in terms of resilience [120, 121] and Reliability, Availability, Maintainability and Safety (RAMS) [122–124]. Indeed, despite providing undeniable advantages, their integration into such elaborated structures conveys peculiar issues that call for the use of specialized risk assessment techniques. In [125], System Theoretic Process Analysis (STPA) and Stochastic Petri Nets (SPNs) have been coupled to analyze the risk deriving by the use of multi-mobile robots operating in hazardous and dynamic environments, such as factories and laboratories, in the presence of people. Additionally, PRA methods may be used to evaluate the risk reduction offered by remote response mitigation solutions and enhance the confidence of emergency robots used in the event of NPP beyond-design-basis scenarios [126].

In comparison to standard NPPs, nuclear research installations and Isotope Separation On-Line (ISOL) facilities are frequently less organized, and their modeling is typically challenging due to their distinctive layout. Furthermore, as in the case of SPES, the employment of robotic equipment within an experimental area where severe radioactive exposure and contamination issues could potentially arise, necessitate a dedicated risk assessment approach.

In this study, a detailed safety and maintenance evaluation has been developed for the most critical RH tasks of the SPES facility. The analysis, which takes advantage of the HAZard and OPerability analysis (HAZOP) technique and Layer Of Protection Analysis (LOPA), aims at enhancing the hardware design, robustness, and reliability of the considered automation systems, along with their operational safety. HAZOP technique is a structured and systematic method aimed at identifying potential hazards and operability problems in a process or operation. In the presented research, this approach is used to list and evaluate the risk associated to the potential deviation of the SPES RH systems from their expected behavior. LOPA, on the other hand, is a semi-quantitative risk assessment tool used to evaluate the effectiveness of Independent Protection Layers (IPLs) in preventing dangerous events. The PRA study is described in Chapter 4.

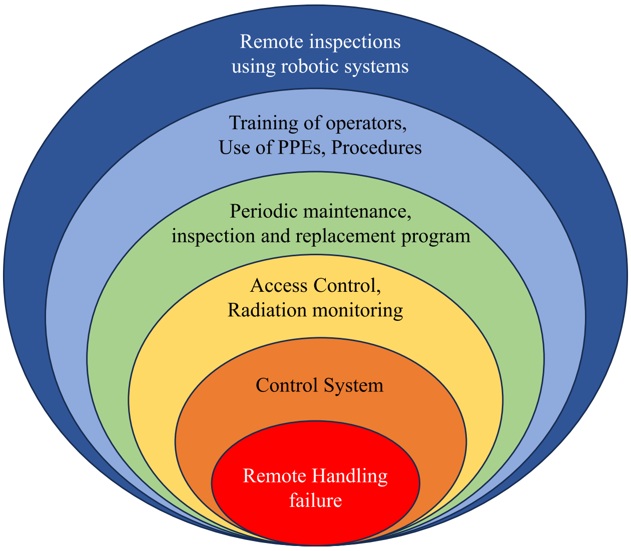


Figure 2.3: Independent Protection Layers (IPLs) for the Selective Production of Exotic Species (SPES) facility.

2.3 MAINTENANCE PLANNING AND OPTIMIZATION

According to the IAEA, nuclear facilities shall continuously work to enhance their operation and maintenance standards in order to preserve their safety. The main goal of maintenance activities is the improvement of the equipment (and plant) reliability. Specifically, maintenance, checking, monitoring and inspection share the common objective of ensuring that the plant is operated in line with the design assumptions and intent, as well as within the nominal operating limits and conditions. [128]. From the safety perspective a typical goal is to prevent issues, potentially leading to radiation exposure, through failure prediction. Furthermore, the early diagnosis of aging mechanisms represents a basic reliability objective.

Preventive and corrective actions are intended to guarantee that systems, components, and structures can operate according to their design specifications, this goal can be achieved through organizational and technical measures conceived to detect, stop and/or reduce the degradation of components, systems and structure [128].

Reorganization, repair and replacement of system components are the usual maintenance activities, which may include calibration, in-service inspections and verification tasks to improve the effectiveness of maintenance interventions. An overview of the different typologies of maintenance tasks is reported in Fig. 2.4.

Preventive maintenance plans have traditionally been based on recommendation on manufacturer advices on required inspection intervals, not taking into account the actual operating conditions and the availability factors [127]. In this case, activities are typically

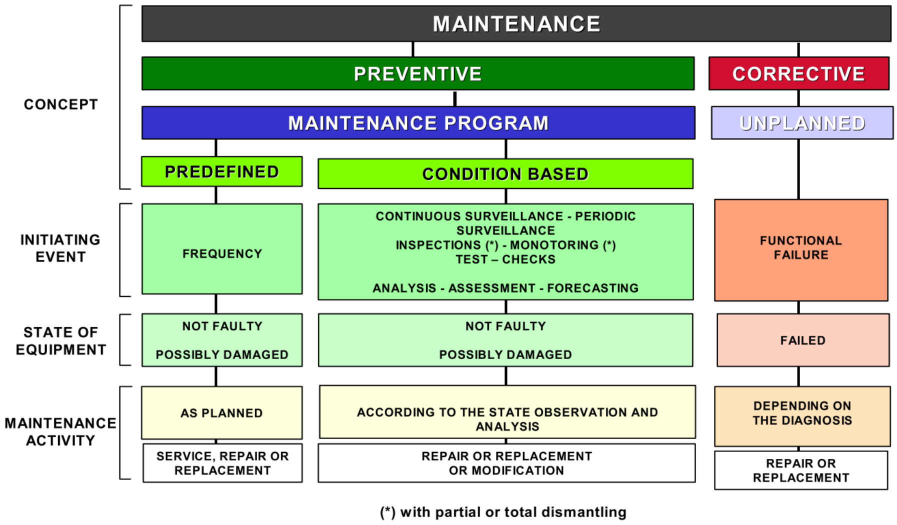

MAINTENANCE
PREVENTIVE
CORRECTIVE
CONCEPT
MAINTENANCE PROGRAM
UNPLANNED
PREDEFINED
CONDITION BASED
INITIATING EVENT
FREQUENCY
CONTINUOUS SURVEILLANCE - PERIODIC SURVEILLANCE
INSPECTIONS (*) - MONOTORING (*)
TEST – CHECKS
ANALYSIS - ASSESSMENT - FORECASTING
FUNCTIONAL FAILURE
STATE OF EQUIPMENT
NOT FAULTY
POSSIBLY DAMAGED
NOT FAULTY
POSSIBLY DAMAGED
FAILED
MAINTENANCE ACTIVITY
AS PLANNED
ACCORDING TO THE STATE OBSERVATION AND ANALYSIS
DEPENDING ON THE DIAGNOSIS
SERVICE, REPAIR OR REPLACEMENT
REPAIR OR REPLACEMENT OR MODIFICATION
REPAIR OR REPLACEMENT
(*) with partial or total dismantling

Figure 2.4: Strategic maintenance relationships [127].

scheduled at the planned time, in accordance with regulations and plant technical specifications [129].

Different optimization techniques have been developed over time with the aim of achieving various objectives, such as safety, reliability and cost [130, 131]. Specifically, development of maintenance plans can be based on clustering and system identification, followed by the risk assessment of critical components, in order to provide effective maintenance strategies [132, 133]. Within this process, multiple key factors should be considered, including:

- Safety and risk significance;
- Regulatory requirements;
- Reliability/Availability;
- Maintenance targets;
- Costs.

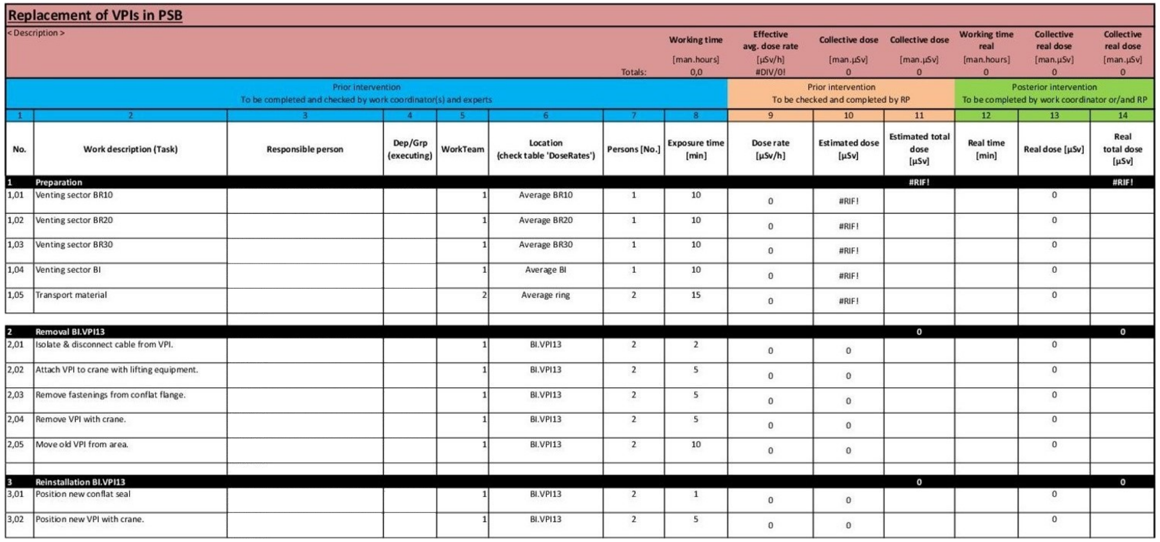
Maintenance optimization is an additional step, driven by different factors, such as reliability, aging or risk assessment [134]. Combined methodologies have been proposed to develop optimization approaches based on multiple parameters [135]. Moreover, RAMS analysis can provide a useful asset to design condition-based maintenance strategies [136, 137]. In this context, effectiveness (or performance) indicators can be used to evaluate the intrinsic advantages and disadvantages of the different approaches [138].

Recommendations from IAEA supports the organizations managing nuclear plants in the development of effective maintenance strategies [70, 128]. Specifically, the overall interventions performances can be improved through:

- the assessment of accident conditions and recovery actions;
- the development of detailed procedures for maintenance, testing and inspection tasks;
- the implementation of a comprehensive work planning and control system;
- the establishment of a training program and the use of mock-ups for operator rehearsal.

Additionally, the increasing availability of virtual and augmented reality can further assist operators during the training process [139]. In this study, maintenance has been incorporated following two parallel approaches. Chapter 5 presents the mechanical design review of critical components installed in highly radioactive locations, which have be been re-engineered following specific maintainability guidelines.

Moreover, a comprehensive assessment of safety-critical maintenance intervention is described in Chapter 6. In this research, the optimization of challenging interventions to be performed under severe radiological conditions has been possible thanks to an experimental campaign aimed at identifying potential vulnerabilities, developing and optimizing operating procedures, and training operators. The subsequent analysis of collected data also enabled the identification of design factors impacting the duration of maintenance tasks. The accurate estimation of the time required by the various interventions, as key study outcome, will be beneficial for the future development of reliable Work and Dose Planning (WDP). These tools can offer several benefits in the preparation of maintenance activities, an example of WDP is provided in Fig. 2.5.



Replacement of VPIs in PSB													
< Description >						Totals:	Working time [man.hours] 0,0	Effective avg. dose rate [µSv/h] #DIV/0!	Collective dose [man.µSv] 0	Collective dose [man.µSv] 0	Working time real [man.hours] 0	Collective real dose [man.µSv] 0	Collective real dose [man.µSv] 0
Prior intervention To be completed and checked by work coordinator(s) and experts								Prior intervention To be checked and completed by RP			Posterior intervention To be completed by work coordinator or/and RP		
1	2	3	4	5	6	7	8	9	10	11	12	13	14
No.	Work description (Task)	Responsible person	Dep/Grp (executing)	WorkTeam	Location (check table 'DoseRates')	Persons [No.]	Exposure time [min]	Dose rate [µSv/h]	Estimated dose [µSv]	Estimated total dose [µSv]	Real time [min]	Real dose [µSv]	Real total dose [µSv]
1	Preparation									#RIF!			#RIF!
1,01	Venting sector BR10			1	Average BR10	1	10	0	#RIF!			0	
1,02	Venting sector BR20			1	Average BR20	1	10	0	#RIF!			0	
1,03	Venting sector BR30			1	Average BR30	1	10	0	#RIF!			0	
1,04	Venting sector BI			1	Average BI	1	10	0	#RIF!			0	
1,05	Transport material			2	Average ring	2	15	0	#RIF!			0	
2	Removal BI.VPI13									0			0
2,01	Isolate & disconnect cable from VPI.			1	BI.VPI13	2	2	0	0			0	
2,02	Attach VPI to crane with lifting equipment.			1	BI.VPI13	2	5	0	0			0	
2,03	Remove fastenings from conflat flange.			1	BI.VPI13	2	5	0	0			0	
2,04	Remove VPI with crane.			1	BI.VPI13	2	5	0	0			0	
2,05	Move old VPI from area.			1	BI.VPI13	2	10	0	0			0	
3	Reinstallation BI.VPI13									0			0
3,01	Position new conflat seal			1	BI.VPI13	2	1	0	0			0	
3,02	Position new VPI with crane.			1	BI.VPI13	2	5	0	0			0	

Figure 2.5: Example of Work and Dose Planning (WDP) required by RP officers prior to high-risk maintenance interventions.

2.4 SAFETY-CRITICAL CONTROL SOFTWARE DESIGN AND VERIFICATION

The recent advances in technology and AI [140–143] enabled the incorporation of complex software solutions within nuclear facilities for the realization of safety functions [144], digital twins [145], testing [146] and diagnostic tasks [147]. In this context, cybersecurity plays an essential role in preserving the plant integrity [148–152]. Considering safety-critical applications, one of the most important requirements for industrial control software is reliability. The choice of the software design methodology is thus essential to provide flexible, portable, scalable and adaptable solutions.

IEC 61499 [79] is an increasingly used standard for modeling complex distributed systems in industrial automation [153]. The goal of IEC 61499, which was issued as a system-level architecture for distributed automation systems, was to enhance the software capabilities of the existing Programmable Logic Controllers (PLCs) based on the earlier IEC 61131-3 standard. The software model is realized through standardized Function Blocks (FBs) linked to Execution Control Charts (ECCs), a Moore type of Finite State Machine (FSM) [154]. When a state is entered, the associated algorithm is executed and an output event is returned. In complex distributed systems, the specific event-driven execution approach appeared to increase determinism and reduce integration and reconfiguration effort. Model-driven design methodologies supports the exploitation of the IEC 61499 potential, providing highly reusable and reconfigurable industrial Cyber-Physical System (iCPS) applications [155–159].

A further element that becomes essential in critical applications, such as nuclear laboratories, is control software safety. In these contexts, thorough testing is essential to reduce the danger of potentially disastrous problems that could result from even small mistakes. Different studies focused on the control software verification have been carried out since the early stages of the IEC 61499 development [160, 161]. In this regard, the inclusion of the plant in the closed-loop model enables the most effective verification [162].

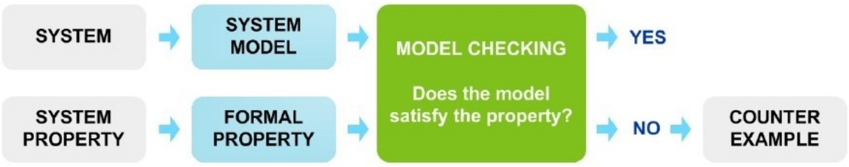


Figure 2.6: Model checking principle.

Boolean logic is not suitable for the verification of dynamic systems due to their inherent tendency to evolve over time and variable evaluations that may be dependent on the previous model states. Thanks to a set of temporal operators, Linear Temporal Logic (LTL) is able to overcome this limitation by adding time specifications over state sequences of a model (or model traces). Given two LTL expressions, φ_1 and φ_2, the most common operators are:

- $\mathbf{G}\varphi_1$: **G**lobally φ_1 has to hold on the entire subsequent path;
- $\mathbf{F}\varphi_1$: **F**inally: φ_1 eventually has to hold (somewhere on the subsequent path);
- $\varphi_1\mathbf{U}\varphi_2$: **U**ntil: φ_1 has to hold at least until φ_2 becomes true, which must hold at the current or a future position;
- $\mathbf{X}\varphi_1$: ne**X**t: φ_1 has to hold at the next state.

LTL formulas are interpreted over valid state sequences of the model. Each of them starts in a specific initial state of the model, and all the neighboring states throughout the sequence are part of the model's transition relation. If a LTL formula is met for every valid state sequence in the model, it is also satisfied for the entire model. Model checking entails determining whether a LTL formula is satisfied for the model and, if not, identifying a counterexample (or failure trace) indicating its violation.

Simulations are intended to play a crucial role in evaluating the behavior of the control system, supporting the virtual commissioning phases and validating the software compliance with expected outputs. Albeit useful for identifying errors, simulations are not enough to ensure the system's reliability. For this reason, formal verification methods have been proposed, as an interesting alternative for the automatic verification of the safety and integrity of automated machines.

In this regard, the integration of model-checking within the closed-loop verification process supports the identification of design vulnerabilities providing useful counterexamples [163]. Indeed, a closed-loop architecture is used to consider the overall behavior of the system, by including both the plant and the controller FBs [164–167]. Despite model-checking methodologies have been incorporated in a variety of domains, such as avionics [168, 169], automotive [170–172], and NPP [173–176] providing undeniable advantages on the software validation, a bottleneck in the spread of these techniques are the demanding computing requirements [177]. This weak point has been addressed in different studies, aiming at reduce their computational impact [178–180].

In this study, Chapter 7 presents a detailed formal verification process applied to a safety-critical RH system. The methodology includes three steps: the creation of a formal model of the existing solution, the definition of a set of LTL properties and the final symbolic model checking phase. The FB2SMV tool [181] is then used to convert FBs (in XML format) to SMV code by utilizing the Abstract State Machine (ASM) [182] semantic as an intermediary model. Within the described formal verification tool-chain, LTL specifications are verified with the NuSMV model checker [183] and then further investigated using tools specifically designed for analyzing counterexamples. The described workflow allows for the integration of the design, simulation and formal verification phases within a single tool-chain prior to the actual operation of the control software [184].

2.5 THE SPES PROJECT

The SPES project of INFN-LNL is developing a second-generation nuclear facility for the production of intense exotic beams, according to the ISOL technique, to be delivered to experimental users for interdisciplinary research [185]. The radioactive isotopes of interest are produced by the interaction of a multi-foil uranium carbide target with a high intensity (200 μA) Primary Proton Beam (PPB) with proton energies in the range of 30-70 MeV [186]. In these conditions, a nuclear fission reaction takes place, and ^{238}U fragments are produced at a rate of approximately 10^{13} fissions per second [187, 188]. The fission products, are ionized [189], extracted and accelerated by an electrostatic potential of 40 kV. Figure 2.7 (Left) shows the general layout of the SPES facility: the PPB generated by the SPES cyclotron is represented

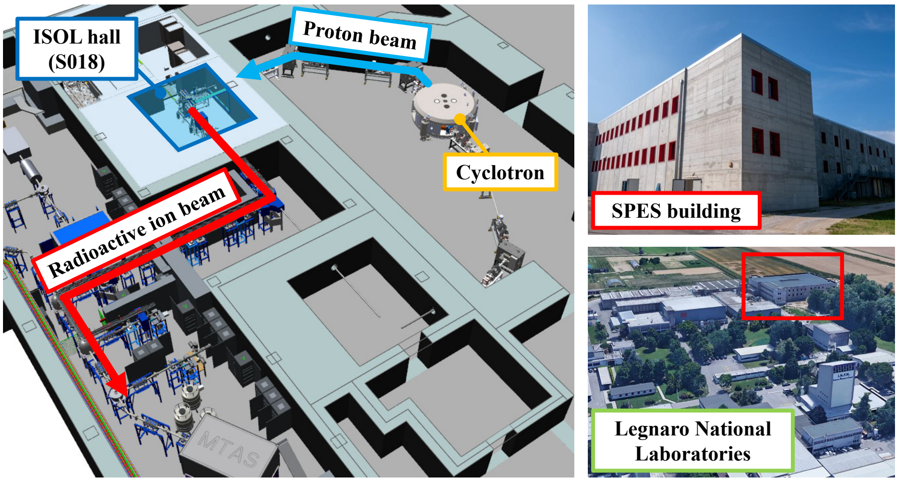


Figure 2.7: Left: General layout of the SPES proton (blue) and RIB (red) beam lines, Right: The SPES facility building (on the top), View of the INFN-LNL complex (on the bottom).

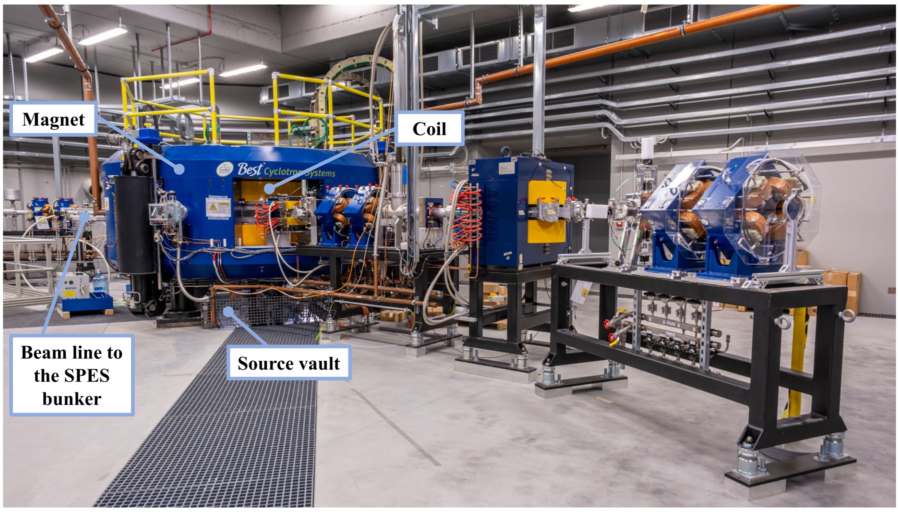


Figure 2.8: View of the Best® 70p cyclotron: the SPES primary driver.

by the blue arrow, while the red path indicates the Radioactive Ion Beam (RIB) line. As visible on the right, SPES building is currently in advanced construction phase at LNL.

The primary driver of SPES is a commercial cyclotron manufactured by Best Cyclotron Systems Inc®, visible in Fig. 2.8 [190]. A set of mass separation, tuning, focusing and charge breeding stages are implemented prior to the injection in the ALPI LINAC [191], where the reaccelerated beam will reach high-energy experimental areas. The structure and organization of the SPES laboratory is common to most of the ISOL facilities all over the world [192–194] for the production of RIBs. SPES aims at the production of first-class beams in terms of quality and intensity to perform forefront research in nuclear physics and astrophysics. Among low energy (non-reaccelerated) applications, the ISOLPHARM [195] project will exploit the radioactive beams produced in the SPES facility for the production of medically relevant radioisotopes.

The Target Ion Source (TIS) unit is the core of the SPES project, here the radioactive nuclei are stopped, extracted, ionized and accelerated to be delivered to specific experimental areas. The vacuum chamber features two flanges for the connection with the proton beam line and the RIB line. A graphite target container holds seven UCx disks (diam. 40 mm, thickness 0.8 mm) appropriately spaced to maximize the proton beam high-power deposition and improve the release capabilities with short diffusion paths through the target. Residual protons are absorbed by a graphite beam dump, while an additional disk called "window" has been designed to confine the produced isotopes within the container [196]. Figure 2.9 shows a section view of the TIS unit.

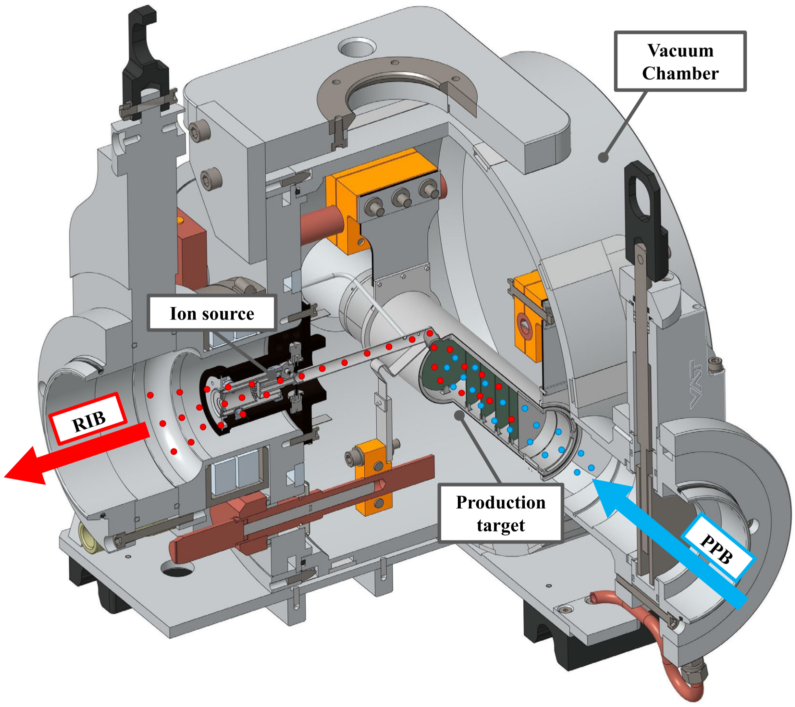


Figure 2.9: Section view of the SPES Target Ion Source (TIS) unit.

Additional composite targets, like SiC [197], TiC [198] or B4C [199], have been investigated. The target container is enveloped by a tantalum heater, visible in Fig. 2.10 designed to increase the disk temperature up to the maximum value of 2300 °C through ohmic heating. At this working point, the fission fragments' effusion rate is optimized, and the effusive-flow transport [200] through the target-vapor system within the container allows the produced isotopes to reach the tantalum transfer line, used to guide the ions towards the ion source. The target layout allows the efficient dissipation of the 8 kW power deposited during irradiation [201]. A dedicated evaluation campaign has been conducted during two low-power irradiation tests at HRIBF facility of the ORNL showing remarkable performances on the both the isotopes production and the thermal stability [202]. Moreover, a high power test, with a 4 kW 66 MeV proton beam, has been performed on a SiC target where the temperature distribution was measured, validating the implemented numerical models [203]. In this experimental campaign, the target activity calculations made with FLUKA [204–206] were benchmarked with the post-irradiation dose rate measurements, indicating a generally good agreement. Different types of ionization mechanisms are available. According to the required beam, three standard ion sources have been developed: the SPES Surface Ion Source (SSIS) [207], the SPES FEBIAD Ion Source [208], and the Resonance Ionization Laser Ion Source (RILIS) [209, 210]. The TIS unit needs to be replaced periodically due to the commonly ob-

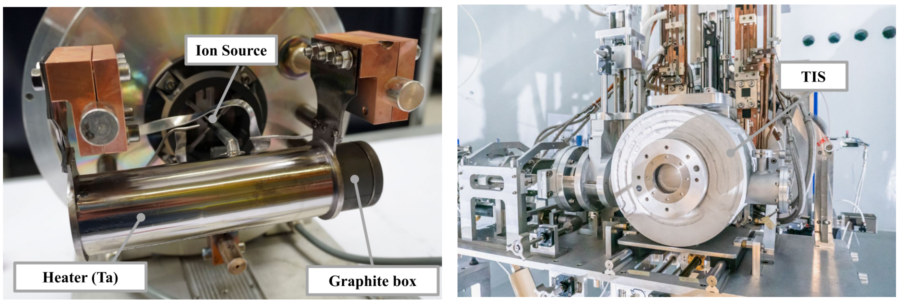


Figure 2.10: The actual TIS unit under test installed on the SPES Front-End (on the right), the target heating circuit (on the left).

served drop in performance of targets and ion sources, caused by many different mechanisms. These involve both targets (for example the onset of sintering [211] which has a detrimental effect on isotopes release) and ion sources (degradation due to embrittlement or insulator failures) [212].

The SPES run schedule is structured in four-week modules: in the first two weeks the TIS unit is impinged by the primary beam for physics experiments, while the following two weeks are used for the radioactive cooling of the unit before the replacement and setup of the new one for the next irradiation cycle. In this high radioactive environment, handling operations are entrusted to autonomous systems able to manipulate, transport and store the TIS unit without need of human intervention. For this reason, a dedicated Remote Handling (RH) framework is under development to fulfill the functional and safety requirements of the project.

Comprehensive surveys on RH technologies adopted in world-class particle accelerator laboratories have been presented in Refs. [30, 213, 214]. The design phase of the SPES RH framework profited from the expertise gained in other important ISOL facilities featuring automated system for the transport and management of radioactive material such as ISAC and ARIEL experiments at TRIUMF [58], ISOLDE [56] and MEDICIS [57] facilities at CERN as well as SPIRAL II [215] at GANIL.

The TIS unit life cycle drives the design of the SPES RH framework. After the target production phase in a dedicated laboratory [216], the TIS unit management shifts to the SPES RH framework, where a set of automated systems takes care of the unit installation on the SPES Front-End for irradiation, the subsequent retrieval and storage for radioactive decay, till the dismantling at the end of TIS life. The SPES facility will run on a cyclic operation scheme, based on two weeks irradiation followed by two weeks stop. The dose absorbed by the EPDM O-rings of the gate valve after the irradiation has been calculated with MCNPX, reaching the level of 300 kGy [59]. The replacement of the unit occurs on a specific moment at the end of this last period. Preliminary simulations [196] of the TIS unit total gamma

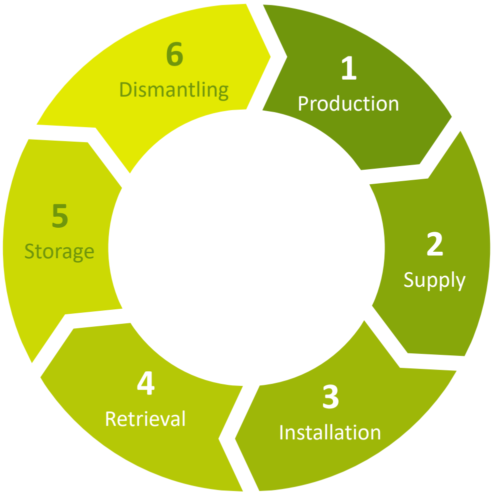


Figure 2.11: The Target Ion Source (TIS) unit life cycle.

dose after 14 days of irradiation (considering 40 MeV, 200 μA proton beam) and a cooling period of 14 days showed an equivalent dose of about 40 mSv/h at one meter from the unit. Immediately after the beam stop, the unit reaches the activity of about $3 \cdot 10^{13}$ Bq, and the equivalent dose is approximately 100 times higher. After this first steep decay, the TIS replacement operation takes place: the irradiated TIS unit is removed from the SPES Front-End and transferred to a dedicated location for long-term storage. The new TIS unit is then installed and coupled to the machine for a new irradiation cycle. Following a cooling period of about 5 years, the spent TIS units are dismantled in a dedicated Hot Cell and safely disposed of. A graphical representation of the TIS unit life cycle is displayed in Fig. 2.11.

The study presented in this thesis takes advantage of the SPES facility as illustrative use-case for the evaluation of novel RH design approaches. Specifically, Chapter 3 describes the comprehensive consolidation process of the SPES RH framework.

Part II

CONSOLIDATION

3 DESIGN CONSOLIDATION AND ADVANCEMENTS OF THE SPES REMOTE HANDLING FRAMEWORK

3.1 INTRODUCTION

The design of Remote Handling (RH) equipment employed in nuclear facilities should follow adaptability, flexibility, robustness and reliability principles to enhance their effectiveness as primary solution to perform safety-critical interventions [11]. Moreover, the overall performances of the RH systems within a specific plant can benefit from the early evaluation (during their engineering phase)of potential failure scenarios that may arise during operation, as well as optimization of plant interfaces based on robot-friendly design strategies [18].

In this chapter, a comprehensive overview of the SPES RH is presented. Specifically, the study focuses on the design consolidation process aiming at the improvement of the reliability and robustness of the various systems. The research follows two parallel approach: Section 3.2 describes the consolidation of the global framework architecture, while Sections 3.3 and 3.4 present the reliability-oriented upgrades of the RH machines. The proposed design upgrades have been implemented with the aim of optimizing the different systems as preliminary stage prior to the risk assessment presented in Chapter 4. A global view of the SPES target area, in which the RH systems operate, is depicted in Fig. 3.1.

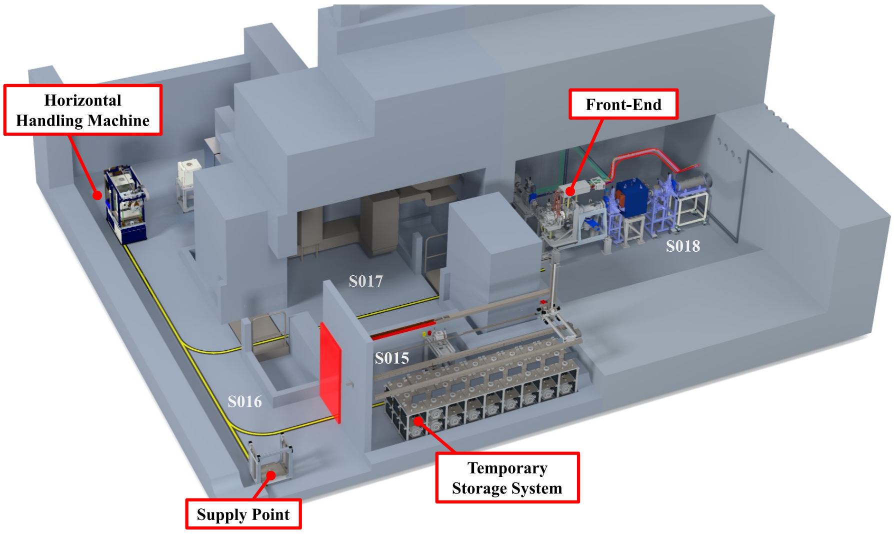


Figure 3.1: Overview of the SPES target area dedicated to the Remote Handling of irradiated TIS units during operation.

3.2 REMOTE HANDLING FRAMEWORK

The SPES RH framework consists of different machines designed to fulfil the specific requirements of each phase in the Target Ion Source (TIS) unit life cycle. This section presents the global consolidation strategies developed to enhance the safety and reliability of the architecture.

The SPES Front-End is the core of the Radioactive Ion Beam (RIB) production process. The system, visible in Fig. 3.2, enables the connection of a TIS unit with the Primary Proton Beam (PPB) line and the RIB for proton irradiation and the subsequent isotopes' extraction. The hazardous radiological conditions developed within the ISOL hall following the TIS unit irradiation demands for an automated approach in the design of the TIS unit replacement procedure. This requirement driven the development of two RH systems: the Horizontal Handling Machine (HHM), in charge of the TIS unit displacements within the SPES target area, and the Temporary Storage System (TSS), designed to take care of radioactive targets during the decay phase. A typical replacement procedure is divided in two main phases: first, the irradiated TIS unit is removed from the Front-End by the HHM and transferred to the TSS, and second, a new unit is installed on the Front-End and coupled with the beam lines for a new irradiation cycle. The mechanical and electrical design of the RH systems is based on the specific peculiarities of the operational scenarios: robustness, reliability and fault tolerances represent the key principles to ensure smooth and safe operation. In case of faults during a critical task execution, a set of backup systems and procedures have been developed to minimize the

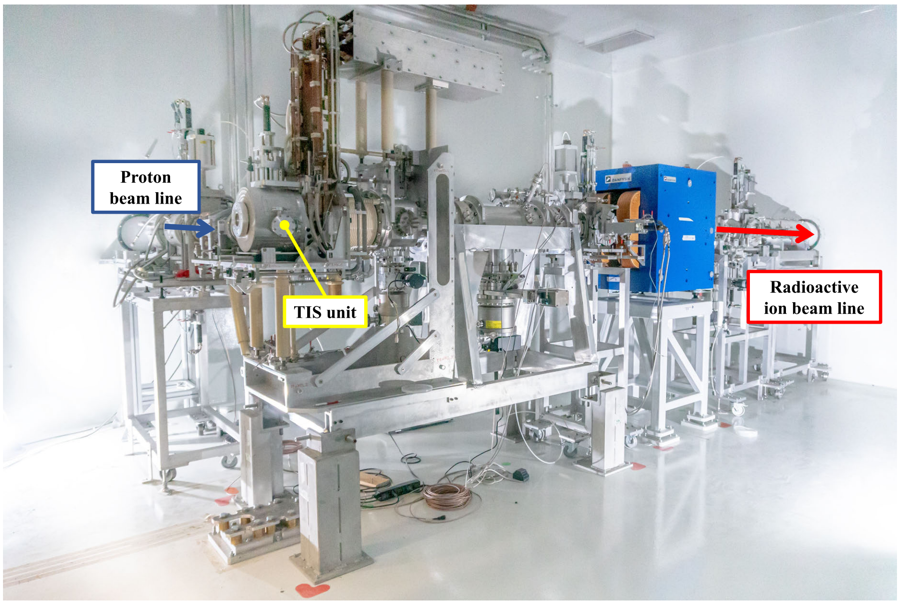


Figure 3.2: The SPES On-Line Front-End installed in the ISOL hall (S018).

personnel exposure during the subsequent maintenance intervention. The following paragraphs provide an overview of the consolidation of several aspects of the SPES RH framework in terms of general layout, control and safety architecture, communication infrastructure, and supervisory layer.

3.2.1 *Optimization of the general layout*

The definition of the SPES target area layout should be based on the analysis of the actual operating scenarios in order to optimize the tasks execution and minimize the risk associated with RH operation from the functional, safety, and Radiation Protection (RP) perspective. Figure 3.3 outlines the functional zones implemented in the proposed arrangement. The target area structure results from the definition of stations, zones and routes. Specifically, the following stations have been defined within the target area:

- the SPES Front-End, located within the ISOL hall (S018). Here TIS units are installed by the HHM and coupled with the PPB and RIB lines for proton irradiation. Activated units are removed after two weeks of beam and two weeks of cooling;
- the TSS, installed in a dedicated room (S041). The system receives irradiated TIS units coming from the Front-End, which are transported by the HHM and installed on a dedicated exchange point;

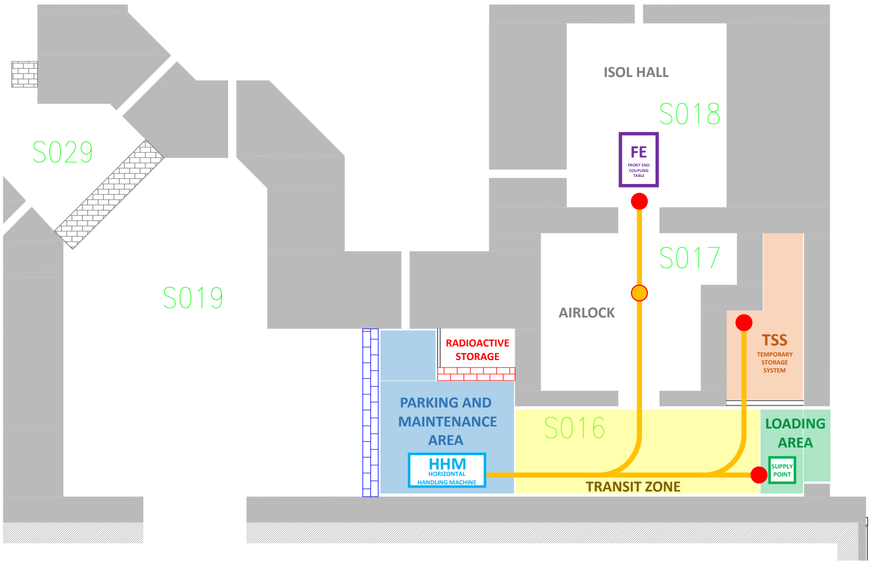


Figure 3.3: General plan of the operational routes and positions of the remote handling vehicles.

- the Supply Point (SP), located at the entrance of the target area (S016). On this station are installed new targets coming from the off-line production laboratories. The system serves as point of contact between the RH operating zone and the laboratory.

The HHM, an AGV-based vehicle, takes care of the TIS unit movements. Different zones have been defined within the target area:

- a parking and maintenance area, including an automated charging station, and providing a sheltered location in which off-line maintenance activities can be performed with a minimal radiological impact;
- a transit zone, which shall always remain clear to enable the HHM movement between different stations;
- a loading area, located at the entrance, used to supply new TIS units. These are manually installed on the SP to enable the subsequent automated loading on the HHM prior to the installation on the Front-End.

The HHM moves within the different areas following an optical path on the floor. The available routes are designed to connect the parking station with: the SPES Front-End, the TSS, and the SP. Both intermediate and working positions are identified through dedicated transponder and magnets. While operating locations are next to stations to enable the remote installation or retrieval of TIS units, service stops are usually located along the routes in specific positions required for diagnostic and technical purposes. An example is provided by the predetermined locations reached by the HHM used to send the shielding doors opening and closing commands avoiding potential mechanical collisions. The intermediate stops are also used to split global motion sequences in multiple sub-tasks. This strategy supports the modularity approach applied in the development of the RH control code.

A typical TIS unit removal procedure includes the following steps:

1. following the irradiation and the first decay period, the TIS unit is disconnected from the PPB and RIB lines.
2. the HHM leaves the parking zone and reaches the ISOL hall;
3. the HHM picks up the unit from the Front-End coupling table and places it within a closed shielding box during the transport;
4. the HHM quits the ISOL hall and access the TSS airlock;
5. the shielding box is opened, and the irradiated unit is installed on the TSS exchange point;
6. the HHM returns to the parking station;
7. the TSS manipulator stores the TIS unit in a dedicated location.

The subsequent installation of a new TIS unit is performed according to the procedure below:

1. a new TIS unit, coming from the off-line production laboratories, in manually placed on the SP located at the entrance of the target area through a Material Access Door (MAD);
2. the HHM leaves the parking zone and reaches the SP;
3. the HHM picks up the unit from the SP and places it within a closed shielding box during the transport;
4. the HHM quits the SP and access the ISOL hall;
5. the shielding box is opened, and the fresh unit is installed on the Front-End;
6. the HHM returns to the parking station;
7. the unit is coupled with the RIB and PPB lines on the Front-End.

The early development of operating procedures and the analysis of potential failure scenarios prompted a substantial revision of the target area layout. Figure 3.4 depicts the old layout of the SPES target area. In the original version, the parking area of the HHM was located at the entrance of the zone, and the routes were traveled in the opposite direction. Furthermore, because the current layout did not include the SP, the loading of the new TIS unit should have taken advantage of the TSS exchange point, on which the fresh target should have been manually installed.

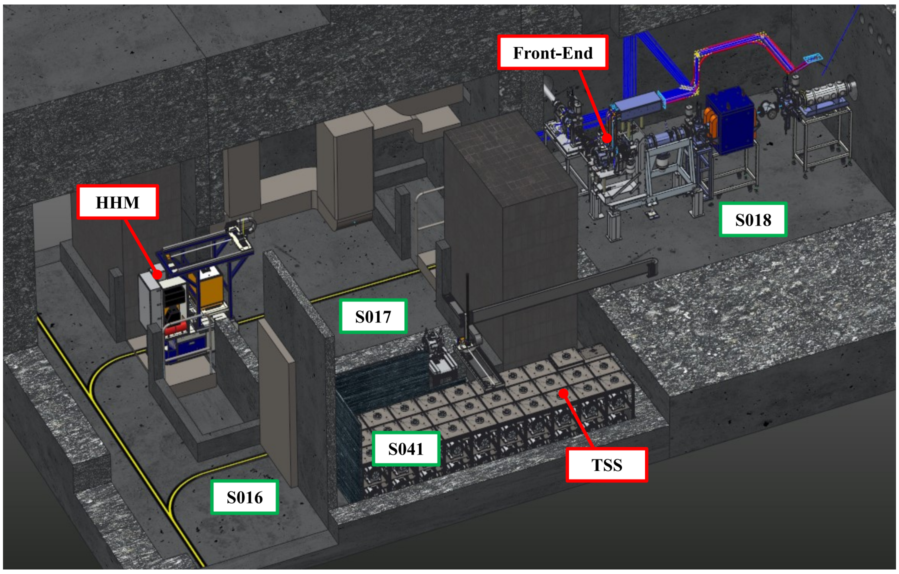


Figure 3.4: The old layout of the SPES target area, in which new TIS units are manually installed on the TSS exchange point.

The existing configuration presented different criticalities. As an example, the original layout required operators to cross the HHM pathways during the TIS unit supply procedure. From the RP perspective, this represents a problem since the HHM wheels can spread contamination coming from the ISOL hall. The new layout, conversely, enables for a clear division between areas with a risk of surface contamination, and generally accessible zones. While the risk still exists in case of personnel access during maintenance activities, the new layout makes it possible to minimize the contamination risk during routine operations.

An additional improvement provided by the revised layout concerns the patrol procedures. Indeed, for safety reasons, the facility Access Control System (ACS) requires an authorized operator to physically access the different zones to verify the absence of personnel and to "patrol" the rooms before the closure of the access door. The conclusion of this procedure enables the possibility to activate the "Operation" ACS mode, which removes all the beam interlocks and authorizes the TIS unit irradiation. Following the conclusion of both irradiation and RH procedure, provided that all the safety conditions are met, the ACS can be switched to the "access" mode and the target area can be entered again. During this phase, the opening of each access door breaks the patrol for the specific zone. The use of the TSS exchange point as loading bay for TIS units required a personnel access within the target area and thus the re-patrol of the zone during each TIS exchange. Conversely, the introduction of the new layout, together with the design of the SP and the introduction of a MAD allows to separate the material access from the personnel access, thus enabling the safe supply of new TIS units without affecting the ACS operating modes and the related procedures.

3.2.2 *Control and safety architecture design*

The proper execution of RH tasks requires strong coordination and interaction through hardware and software interlocks, adopted to ensure the safety of personnel and machines, respectively.

Starting from the original concept, where each single RH machine had its own control systems and had to communicate with other partners individually, a new layout based on a distributed architecture has been proposed. In this new approach, self-contained tasks not requiring interactions with other systems are autonomously executed on the local PLC, while a common controller known as Remote Handling Supervisor (RHS) takes care of the synchronization and interactions between different sub-systems during complex RH operations involving multiple machines, or third-party systems.

The synoptic in Fig. 3.5 shows a high-level overview of the SPES RH control system architecture. On one hand, the RHS supervises the mission execution of the HHM and TSS systems, on the other hand, it

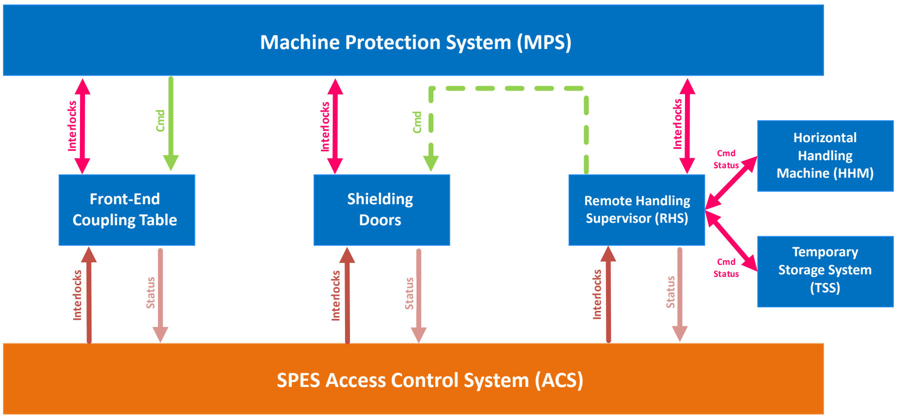

Machine Protection System (MPS)
Interlocks
Cmd
Interlocks
Cmd
Interlocks
Cmd
Status
Horizontal Handling Machine (HHM)
Front-End Coupling Table
Shielding Doors
Remote Handling Supervisor (RHS)
Cmd
Status
Temporary Storage System (TSS)
Interlocks
Status
Interlocks
Status
Interlocks
Status
SPES Access Control System (ACS)

Figure 3.5: Functional architecture of the SPES Remote Handling control and safety system.

acts as a unique communication partner with external systems, such as the SPES Machine Protection System (MPS). The MPS is responsible for the safety of the machine, avoiding dangerous states that could damage critical components. With this scope, it is interconnected with all the systems in the facility and permits the exchange of mutual software interlocks to preserve its global integrity. As an example, the HHM interacts with the MPS to request the opening or closing of the access door of the ISOL hall, or to get the status of the coupling procedure within the Front-End coupling table.

The physical architecture of the SPES RH control and safety network is outlined in Fig. 3.6. The blue dashed lines represent the links between standard control PLC for the mutual exchange of software interlocks, while the orange lines are related to the safety network. Standard control PLCs are reported on the left: the TSS PLC communicates on one side with the MPS via Modbus TCP/IP on a wired connection, on the other side with the HHM onboard PLC on Wi-Fi for the exchange of software interlocks (dashed lines). The safety network is represented on the right: the TSS Safety PLC (TSS-S) exchange double channel hardware interlocks with the ACS, while the communication between the HHM and the TSS safety PLC is realized through FailSafe over ErherCAT® (FSoE) certified protocol according to IEC 61784-3 [217]. In case of signal loss, a dedicated watchdog timer [218] will trigger a controlled stop of the system according to the status of the running task. Local wireless control panels equipped with an emergency stop are installed to perform maintenance activities.

System control logic runs on Schneider® M340 and M580 PLCs, exchange of information between different systems is based on field bus communication protocols such as Controlled Area Network (CAN) bus, CANopen and Modbus TCP/IP. In addition to the MPS, the remote handling devices are interlocked with the SPES ACS, which regulates personnel access to the SPES target area [219–221]. Controls and Safety

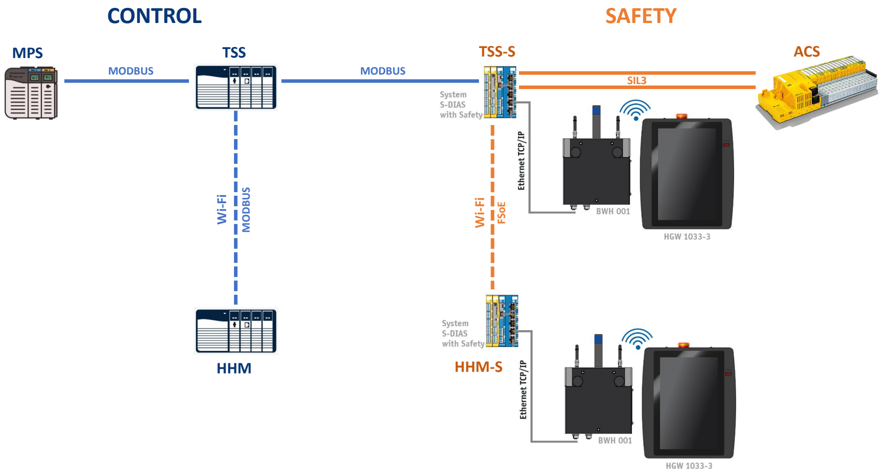


Figure 3.6: Synoptic of the SPES Remote Handling control and safety network architecture.

networks are logically and physically separated. Dedicated safety PLCs are installed on all the RH systems. Field signals are acquired through hard-wired safety sensors while the master PLC shares double-channel hardware interlocks with the ACS to implement safety functions up to IEC 62061 [222] Safety Integrity Level (SIL) 3. To reach this level, the safety controllers are based on the Sigmatek® SCP111 CPU and the safety logic is realized through built-in control blocks provided by Sigmatek® certified libraries.

Operational parameters, such for example the TIS units' pick-up coordinates (x, y, z), are stored in a centralized database which is accessed by field PLCs during the execution of remote handling sequences. In addition, the code running in the SPES CPUs is tracked and archived in an internal repository based on the Git version control system [223].

Before the start of the operation, a series of hardware, functional and dysfunctional acceptance tests will be performed to certify the entire SPES safety infrastructure.

3.2.3 *Wireless communication: infrastructure and logic*

Communication is a key aspect that needs to be addressed in safety-critical applications employing wireless machines. In the SPES case, the use of the HHM requires a specific analysis on the potential consequences that may derive from a communication issue. In this study, the minimization of potentially dangerous situations derived from lack of communication has been addressed by two parallel approaches, focused on both the software and hardware optimization.

On the software side, the control logic has been redesigned following a modular strategy in which global missions are executed by the RHS, whereas critical sequences are maintained at a local level to avoid any possible problem caused by communication issues. As an example, the set of tasks performed to remove an irradiated TIS unit from the SPES Front-End is executed locally as an atomic sequence by the onboard HHM PLC after the reception of the "start" command by the RHS. A potential communication breakdown will therefore not lead to a stop in the RH operation. Conversely, the local system will accomplish the critical sequence and wait for the restoration of the network under known and safe conditions. The local system signals the successful completion of each individual sequence, causing a transition in the global mission state machine managed by the RHS.

From the hardware point of view, a robust infrastructure based on a dedicated Wi-Fi radio network has been proposed as primary physical communication layer between the HHM and the RHS. The system is based on a dual-band (2.4 and 5 GHz) coaxial radiating cable laid along the HHM routes within the SPES target area. To mitigate the effects of radiations, the control electronics and sensitive components are installed in a sheltered location. The layout of the infrastructure is depicted in Fig. 3.7.

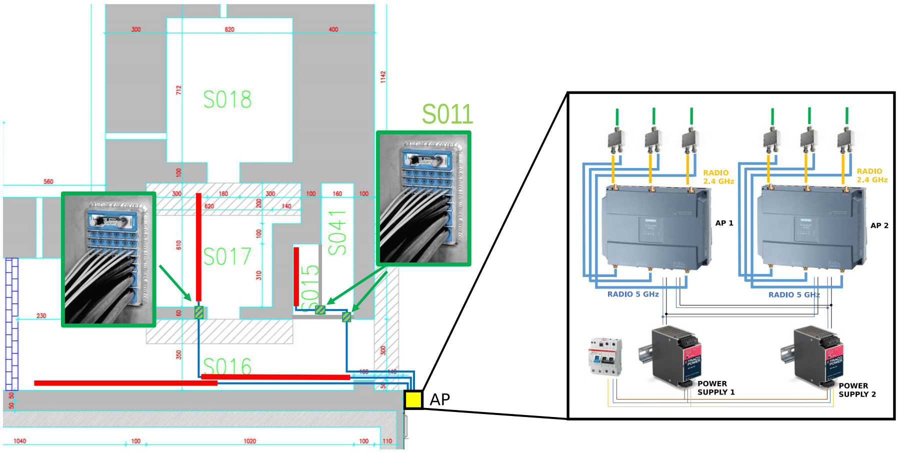


Figure 3.7: Layout of the SPES target area Wi-Fi infrastructure based on a coaxial radiating cable fed by two dual-band access points.

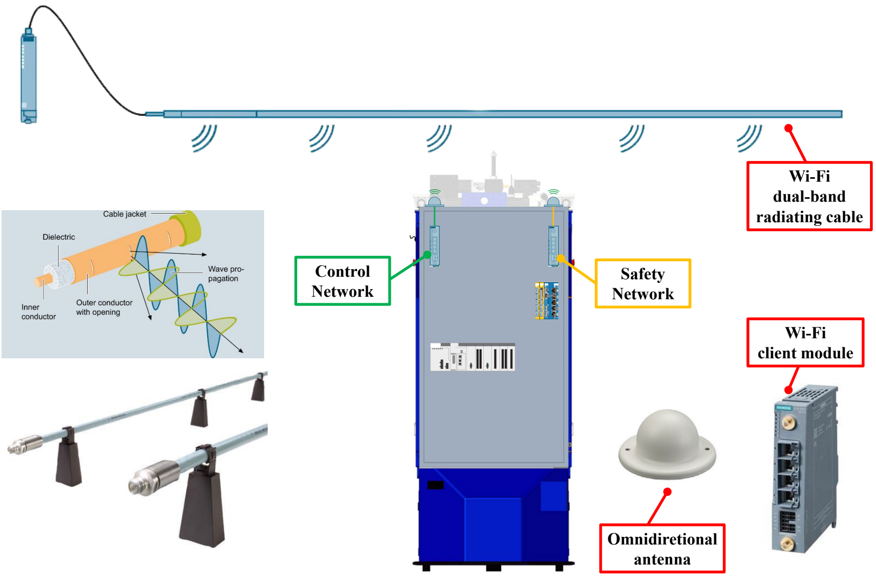


Figure 3.8: Concept view of main radio components employed in the SPES target area: the fixed Wi-Fi radiating cable and the onboard client modules and antennas.

The plant takes advantage of two redundant industrial access points (Scalance® W788-2), each of them combining the two radio interfaces on the same cable through a splitter. The HHM includes two Wi-Fi clients (Scalance® WUM763-1), each of them connected with an omnidirectional antenna. The proposed architecture provides a high degree of flexibility, which may support the requirement to maintain the control and safety networks separate, which connect with their ground partners via the Modbus TCP/IP and FSoE protocols, respectively. Indeed, the network layout enables to split the traffic at different levels, taking advantage of independent frequencies, channels, SSID. Control and safety signals are shared between the master PLCs and the onboard PLC through respectively standard and safety protocols on independent VLANs. The schematics in Fig. 3.8 outlines the described architecture in a simplified graphical representation.

From the hardware standpoint, the proposed solution overcomes the vulnerabilities of the original design, in which the communication was based on a single access point, collecting the traffic of both the control and safety network. Additionally, the initial design concept was planning to use conventional access points, which would have been damaged by radiations. On the software side, the original control logic maintained a significant data exchange with the external supervisor throughout the task execution, resulting in potential stops in unexpected configurations if communication problems emerged. This scenario is particularly critical, since the ensuing recovery actions must be carried out under unknown conditions.

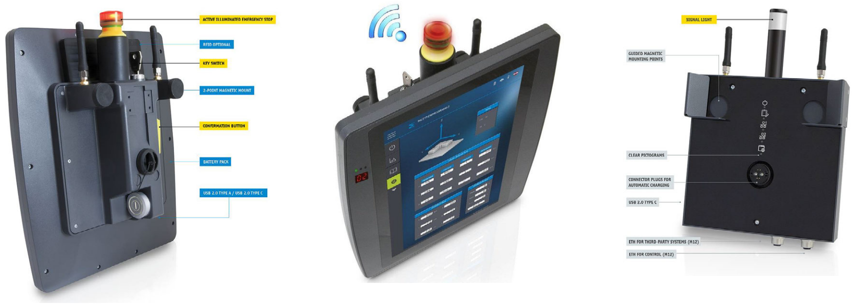
3.2.4 *Human-Machine Interfaces*

The multiple operating scenarios expected for the SPES RH systems demand for the design of tailored Human Machine Interfaces (HMIs) which can adapt to the specific user and task.

During standard procedures, operators launch automatic handling tasks from the SPES control room. Here a Graphical User Interface (GUI), based on the Experimental Physics and Industrial Control System (EPICS) framework [224], reports the status of the system and logs the significant information. In this operating mode, tasks are managed by the RHS and can be launched by inexperienced operators.

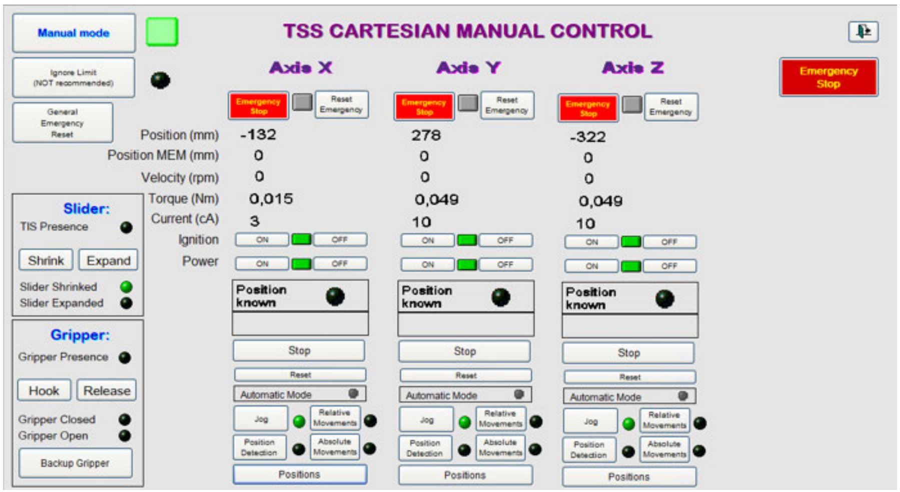
The GUI is base on a multi-user architecture. This enables the activation of different command pages according to the privileges of the logged-in user. While standard operators can launch predetermined sequences, experts will be able to execute specific sub-sequences and move the axes within a manual operation mode. Finally, administrator users have access to a whole set of diagnostic variables and can perform advanced settings on the different machines.

During the commissioning of the systems and specific maintenance tasks, operators must be physically located near to the RH system in order to have a visual feedback on the launched commands. For this reason, in the context of the RH consolidation, a portable touch-panel has been introduced as additional tool aiming at helping operators in the execution of manual adjustments or checks on the machines. Figure 3.9 shows the implemented solution, based on a mobile Wi-Fi touch panel (Sigmatek® HGW 1033). A specific HMI has been developed for the execution of step-by-step procedures on the field. The touch panel allows sending commands and to read the status of the different machines through a direct Wi-Fi link with a base station. Additionally, the device features three rotary encoder wheels used for the fine positioning of the motion axes and safety devices used to stop the machine: an emergency stop button and a three state confirmation command.


ACTIVE ILLUMINATED EMERGENCY STOP
RFID OPTIONAL
KEY SWITCH
2-POINT MAGNETIC MOUNT
CONFIRMATION BUTTON
BATTERY PACK
USB 2.0 TYPE A / USB 2.0 TYPE C
SIGNAL LIGHT
GUIDED MAGNETIC MOUNTING POINTS
CLEAR PICTOGRAMS
CONNECTOR PLUGS FOR AUTOMATIC CHARGING
USB 2.0 TYPE C
ETH FOR THIRD-PARTY SYSTEMS (M12)
ETH FOR CONTROL (M12)

(a) (b) (c)

Figure 3.9: The Sigmatek® HGW-1033 Mobile WLAN panel: (a) rear view, (b) front view, (c) base station (BWH 001).



TSS CARTESIAN MANUAL CONTROL

	Axis X	Axis Y	Axis Z
Position (mm)	-132	278	-322
Position MEM (mm)	0	0	0
Velocity (rpm)	0	0	0
Torque (Nm)	0,015	0,049	0,049
Current (cA)	3	10	10

Figure 3.10: Example of Schneider® Vijeo Citect HMI dedicated to the manual axis movement by an expert operator.

Figure 3.10 displays, as an example, a page of the RH operating GUI enabling the manual movements of the TSS axes. The GUI allows to access a centralized database where critical settings and absolute axes coordinates are stored and maintained. Additionally, the system takes care of real-time monitoring, data logging, and alerts/warnings notification. These features are extremely beneficial to trace back the status of the system prior to potential failure events.

3.2.5 *Supervision*

During standard operation, monitoring the execution of RH tasks through surveillance cameras represents an effective tool to provide real-time feedback to operators. Additionally, the video recording of safety-critical missions constitutes an invaluable asset in understating system dynamics prior to potential accident scenarios.

For the discussed reasons, a set of wall-mounted Pan Tilt Zoom (PTZ) IP cameras, featuring a 30x optical zoom, has been deployed throughout the SPES target area. In principle, two cameras are installed in each zone to monitor the HHM movements and actions, resulting in a set of 8 surveillance cameras. The installation position has been defined according to the expected radiation field during the beam, selecting most sheltered locations. The ability to move the cameras, together with the optical zoom, provides a significant support to the debugging of failure conditions while preserving personnel from undue radiation exposure during inspections.

As additional tools, both the HHM and the TSS have been equipped with onboard cameras installed on the motion axes and on the pneumatic gripper to monitor the TIS unit movements within the different

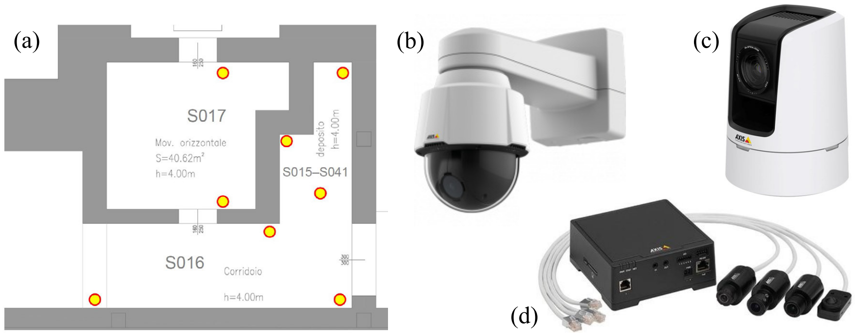


Figure 3.11: Synoptic of the SPES Remote Handling control and safety network architecture.

stations. Furthermore, a PTZ 30x optical zoom camera has been installed on the HHM to perform remote inspections within the SPES. This design upgrade can be extremely useful to visualize the status of the Front-End. Figure 3.11 details the key components of the supervision network installed with the SPES target area, specifically:

(a) the layout of the SPES target area and the position of fixed PTZ cameras;
(b) the wall-mounted AXIS® P5655-E PTZ cameras installed in fixed locations;
(c) the onboard AXIS® V5915 PTZ camera installed on the HHM;
(d) the onboard AXIS® F44 + F1005-E cameras installed on the HHM and the TSS.

3.3 THE HORIZONTAL HANDLING MACHINE

TIS unit movements within the SPES target area are entrusted to automated systems belonging to the SPES RH framework. The primary TIS unit transport vehicle is the Horizontal Handling Machine (HHM). During standard operation, the HHM is responsible for the transfer of new and activated TIS units between the different stations described in the previous paragraphs. The system, illustrated in Fig. 3.12, is based on an AGV following an optical path on the floor [225].

The navigation pattern, represented in Fig. 3.3 is composed of different routes, covered in accordance with the type of handling task, and it includes several transponders used to identify operational (red) and intermediate (orange) positions, while a set of magnets are used for the fine positioning of the vehicle in correspondence with the TIS unit pick or placement points. The vehicle parking position is located in room S016, where an automatic docking station recharges the batteries prior to operation. During access conditions, the HHM is confined in the parking position to avoid any mechanical risk for personnel, while throughout operation the system is authorized to transit within the SPES target area for remote handling tasks.

The payload of the AGV consists of a cartesian manipulator used to grab the TIS unit for removal or installation tasks. The system includes three motion axes: one on the longitudinal direction and two on the vertical direction. Two of them are dedicated to the grasping and positioning of the TIS unit through a pneumatic end effector described below, while the third axis is reserved for the vertical displacement of a shielded (25 mm lead + 10 mm steel) box used for the storage of the TIS unit during transport.

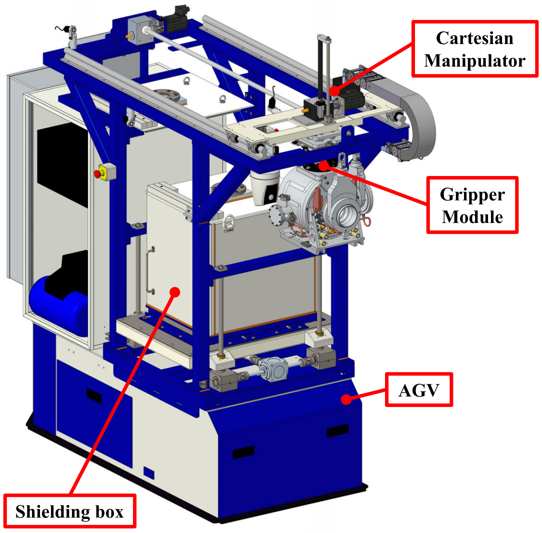


Figure 3.12: 3D model of the Horizontal Handling Machine (HHM) automated vehicle for the remote transfer of the SPES TIS unit.

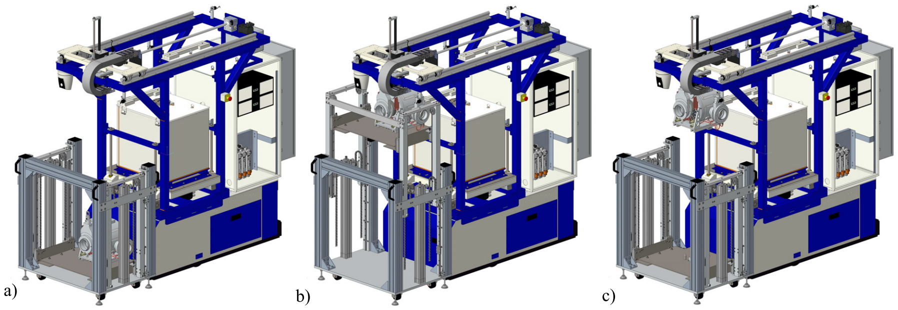


Figure 3.13: The TIS unit loading on the HHM using the Supply Point.

A typical operational cycle to replace a TIS unit on the SPES Front-End includes the subsequent execution of two remote handling missions:

- Retrieval of an irradiated TIS unit from the SPES Front-End and delivery to the TSS for long-term storage
- Pick up of a fresh TIS unit from the SP, see Fig. 3.13 and installation on the SPES Front-End for irradiation.

Both operations are completely automated and, for safety reasons, the TIS unit remains enclosed in the shielding box during transport. The entire TIS unit replacement process will take approximately one hour.

Due to historical reasons, the HHM has been developed as a prototype within an iterative process aimed at incorporating the different RH requirements. The essential role of the HHM in executing safety-critical tasks in highly radioactive environments suggested an in-depth consolidation of the existing design, which has been addressed in the context of this thesis as a preliminary stage prior to the risk assessment presented in Chapter 4. The proposed upgrades, related to the power management, the hardware design and the control logic are discussed in the following sections.

3.3.1 *Energy management*

As already mentioned, the HHM is composed of two machines, an AGV and a cartesian manipulator. In the original configuration, each of the two subsystems included their own batteries. Specifically, the AGV was equipped with a set of lead-acid batteries and an onboard battery charger, whereas the cartesian manipulator featured two redundant UPS used to power the motion axes drives and the control cabinet. The RH systems consolidation process highlighted a number of criticalities provided by the existing topology. First, in the original configuration, each of the three supply components (AGV batteries and 2 UPS) required to be manually charged prior to operation. This task was critical since it required multiple access in a zone featuring a contamination risk. In addition, the operator was given responsibility

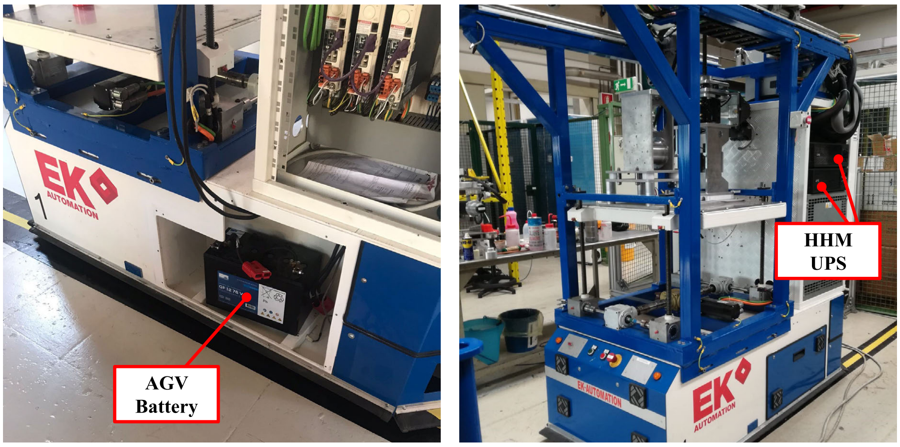


Figure 3.14: The HHM prior to the hardware upgrade: old AGV batteries (on the left), the HHM UPSs (on the right).

for checking the machine's charging condition. A second weakness was related to the type of batteries used for the AGV. On the one hand, lead-acid batteries features a significant risk of hydrogen release during charging phase (thus originating an explosion risk), on the other hand the battery type was mainly intended for rush applications than for traction vehicles, resulting in the early degradation of the system's performances. Figure 3.14 shows the existing power architecture of the HHM.

To overcome the discussed criticalities, a new power management architecture has been proposed. The AGV batteries have been replaced with a novel set of AGM batteries, featuring a minimized risk of hydrogen release and suitable for traction applications. In addition, the

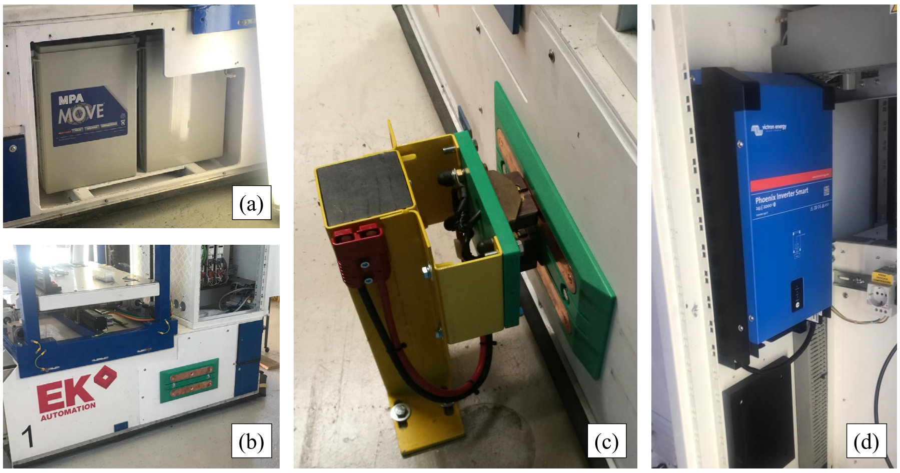


Figure 3.15: Power upgrades of the HHM: (a) the new traction batteries, (b) charging contacts on the AGV left side, (c) charging station, (d) main HHM inverter.

UPS have been removed, enabling the incorporation of 24 V/2000 VA Victron® inverter aimed at powering the whole HHM loads. Finally, the batteries power supply has been removed from the vehicle, and an automatic charging station has been implemented thanks to the introduction of charging contacts on the side of the HHM.

The proposed hardware upgrades, outlined in Fig. 3.15, enable the remodeling of the HHM batteries adopting a unified architecture, the implementation of automatic charging procedures, reducing unnecessary personnel access in contaminated areas, and the minimization of fire risk.

3.3.2 *Hardware consolidation*

The HHM is in charge of the manipulation and transport of highly radioactive TIS unit after irradiation. The RH consolidation process has proposed to improve the hardware design of the machine by incorporating fault-tolerant principles aiming at increasing the availability of the system. Specifically, the goal of the approach is to improve the HHM design to let it complete safety-critical tasks even if some hardware component fails. This approach is advantageous for the subsequent maintenance intervention since it allows for the reduction of overall personnel exposure by optimizing the radiological conditions of the maintenance work site.

In the following, the hardware design of the HHM is described. The adopted layout is based on the TSS hardware architecture, described in Section 3.4. The system has been tested in the actual operating conditions within the SPES target area, Figure 3.16 shows the HHM vehicle during RH procedures on the SPES Front-End..

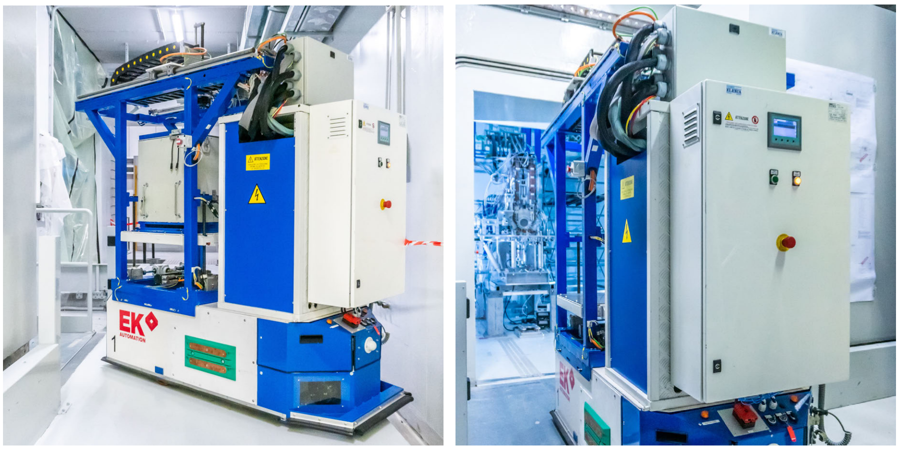


Figure 3.16: The Horizontal Handling Machine (HHM) during commissioning tests nearby the SPES Front-End.

The HHM manipulator is equipped with two fail-safe pneumatic end effectors (Schunk® Quick Change SWS) in a nested configuration for redundancy reasons. The gripper comes with two indexing pins, two inductive proximity switches for the closed/open state detection and a fail-safe actuator to lock the object during motion. A compensation module allows to comply with ±5 mm misalignment in all directions, while a series of mechanical end switches stop the motion in case of unexpected collisions. In such an event an alarm is triggered, and a RH operator can take over the control of the machine to remotely offset the gripper with the help of the onboard cameras. Two SPST-NC mechanical switches are located in the lower part of the tool to detect the TIS unit presence during motion. The main gripper is connected and powered by a backup unit. In case of fault of the main actuator during the positioning of a TIS unit, it is possible to release the backup gripper to complete the task and perform a maintenance intervention under safe conditions. Redundancies are implemented in different components of the HHM, such as the mechanical limit switches used to acknowledge the proper execution of RH tasks.

3.3.3 *Software architecture*

The HHM is equipped with a Schneider® M340 PLC for the supervision of the automated motion sequences. A complete TIS unit removal or installation mission includes several steps and the combined action of different systems such as the shielding doors, HHM and the SPES Front-End coupling table.

Given the original configuration, in which all the interactions between the different partners were managed internally by the onboard PLC, the consolidation process introduced a distributed architecture according to the design described in Section 3.2. In the new layout, the RHS takes care of the global execution, whereas the sub-missions are managed locally by the HHM. The control software is logically partitioned in modular sequences starting and finishing in predefined states. With this architecture, radio communications over a dedicated Wi-Fi network are minimized and limited to sending start commands and logging of data to avoid inconsistent states due to possible communication issues.

In addition to the fault tolerance features described in the previous section, the HHM will run an automatic test sequence prior to the execution of most critical tasks. Thanks to this procedure, early detection of most anomalies will be possible, avoiding undesired failure scenarios during operation.

A comprehensive revision of the HHM control code, taking advantage of modern standards and formal verification methods, is discussed in Chapter 7.

3.4 THE TEMPORARY STORAGE SYSTEM

Activated TIS units, at the end of the irradiation cycle, are stored in the SPES Temporary Storage System (TSS) for radioactive decay prior to dismantling. The TSS initial prototype has undergone an in-depth hardware and software consolidation process, aimed at improving its reliability and resilience, the final TSS concept is shown in Fig. 3.17.

Monte Carlo simulations performed with FLUKA and MCNPX code have reported that a single TIS unit stored after 15 days of cooling contributes to about 40% of the total TSS gamma source, while its gamma intensity is reduced to 1% of its original value after one year of storage [226]. The TSS features a special layout conceived to minimize the external dose contribution. Specifically, the foreseen H*(10) rate in the external transit corridor does not exceed 1 μSv/h, while in the entrance part of the TSS room, the maximum H*(10) rate is 25 μSv/h. Figure 3.18 outlines the TSS environmental dose rate.

Irradiated TIS units coming from the SPES Front-End are positioned on the TSS slider by the HHM, the unit subsequently hands over to the TSS cartesian manipulator and is stored in a predefined location within the storage rack. A ventilation duct over the TSS keeps a negative pressure of -80 Pa in the storage area, extracting possible volatile contaminants, namely Br, Kr, I, and Xe for the SPES case. The TSS airlock (room S015) is kept at -40 Pa and serves as buffer zone between the TSS storage rack and the non-classified zones. During TIS unit insertion, the slider movement requires the opening of a gate door. In this configuration the ventilation control system tolerates a transient equilibrium that will be restored once the slider is retracted, and the gate closed. After a cooling period of 2-5 years [39] exhausted TIS units can be removed from the TSS and transferred to a Hot Cell for dismantling.

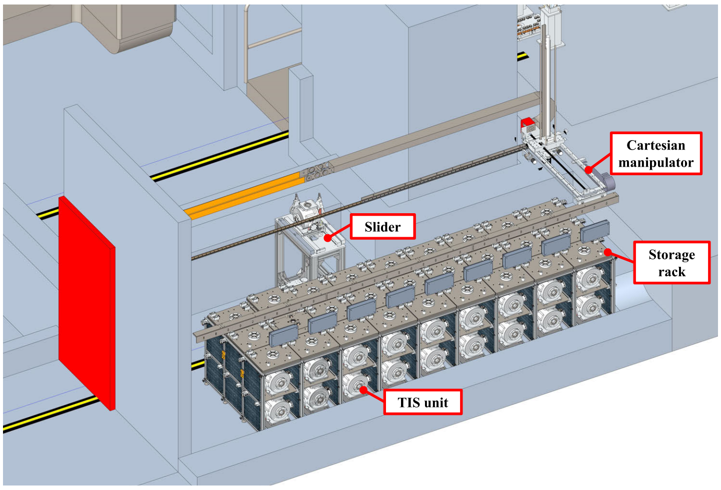


Figure 3.17: 3D view of the Temporary Storage System (TSS) installed in the SPES target area.

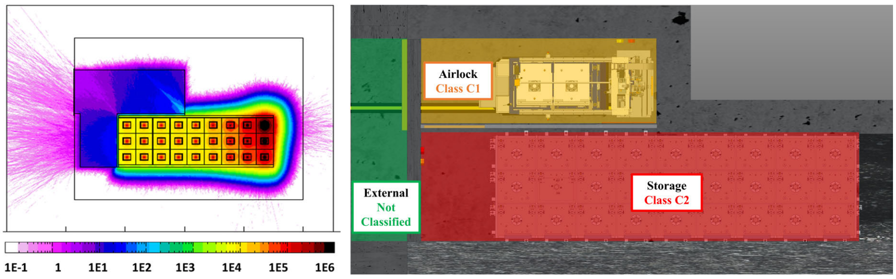


Figure 3.18: (Left) Top view of the TSS Monte Carlo model, the equivalent dose rate H*(10) rate values are expressed in [$\mu Sv/h$] [226]. (Right) The foreseen containment classes of the TSS area, according to ISO 17873, are represented by different colors. Namely, Not Classified in green, C1 (-60 Pa < p < -40 Pa) in orange, C2 (-100 Pa < p < -80 Pa) in red.

3.4.1 *Hardware design*

The TSS consists of three parts. Firstly, a storage rack is designed to host up to 54 TIS units, which correspond to more than five years of nominal SPES operation (considering ten production cycles per year). The structure, shown in Fig. 3.19 is composed of 9 modules, each of them is able to accommodate 6 units on 2 levels. The modules are shielded with lead layers to reduce the external environmental dose. Secondly, a cartesian manipulator takes care of the TIS unit handling and positioning within the storage rack. The system, visible in Fig. 3.20, moves above the modules to place the irradiated unit in a specific

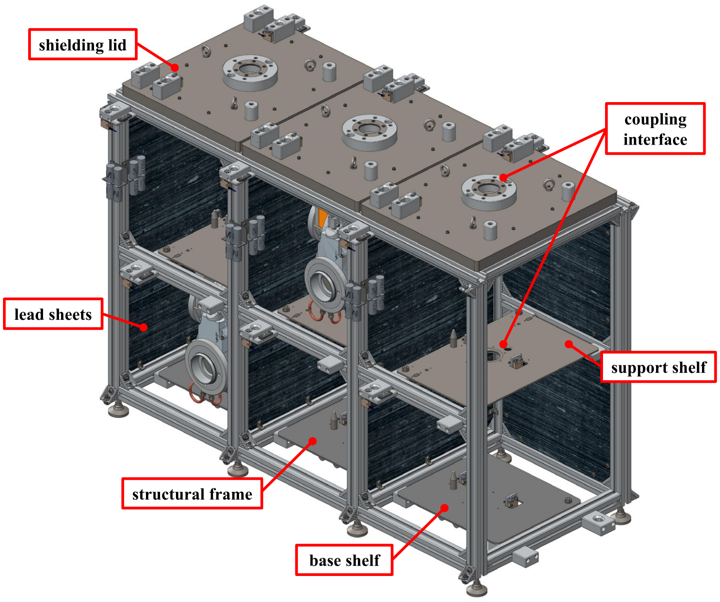


Figure 3.19: Basic functional unit of the TSS rack. Each storage module is designed to host 6 TIS units.

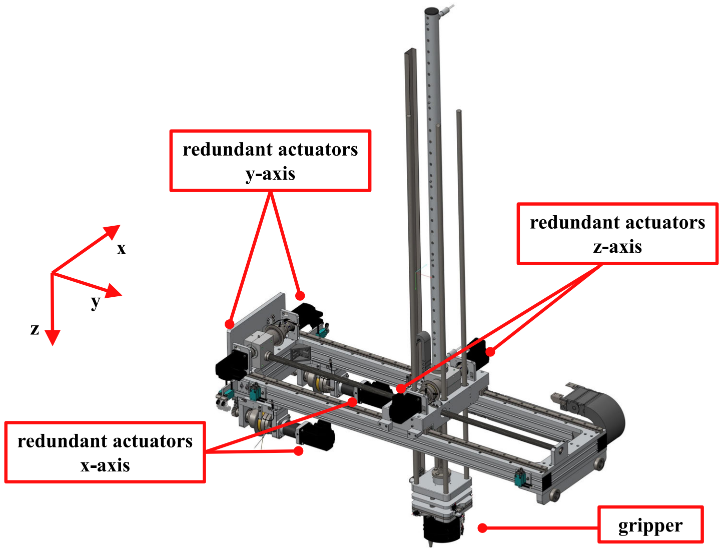


Figure 3.20: The TSS cartesian manipulator.

location with a vertical approach. Finally, a sliding table represents the point of interaction between HHM and the TSS cartesian manipulator. In this position the TIS unit coming from the Front-End is received and transferred to the operating area of the TSS manipulator, the whole procedure is outlined in Fig. 3.21.

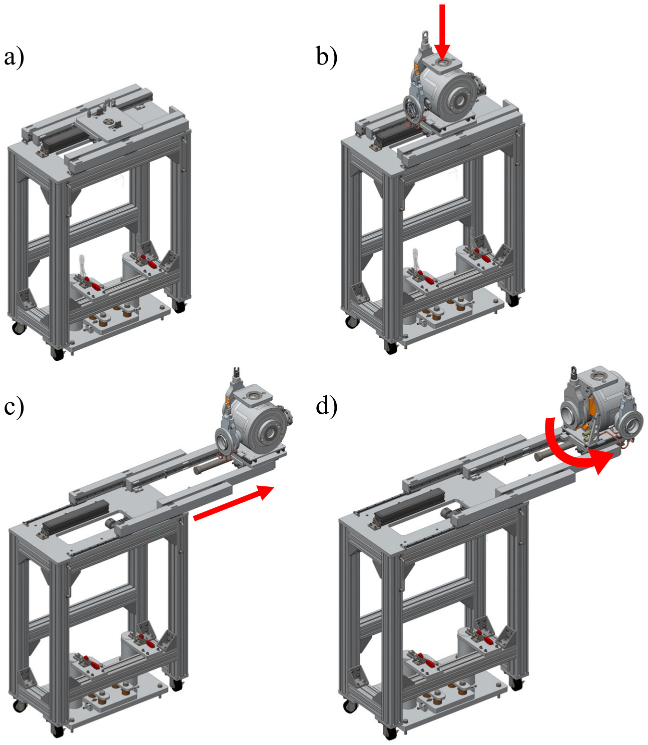


Figure 3.21: The TIS unit supply sequence on the TSS slider.

Within the storage rack, TIS units installed on the lower level are resting on the rack baseplate, while a set of removable intermediate supports allows the storage of the TIS units on the upper level. Each cell is enclosed with a shielding lid. Lids and intermediate supports feature a common gripping interface to be engaged by the TSS manipulator. To access the lower layer, they are firstly removed from their original location and then stacked on top of the lids of the neighboring modules. The storage rack is periodically rearranged: units with a lower dose are progressively shifted towards front positions, while highly radioactive ones are kept in the inner locations, far away from the transit zone S016. In this configuration the external ambient dose is minimized thanks to the distance increase and the interposition of the various shielding layers of front and middle storage modules.

The cartesian manipulator features a redundant pneumatic end effector, shown in Fig. 3.22. Exact positioning of the units within the rack is ensured by indexing pins, while redundant mechanical switches (Microprecision Electronics SA® MP321) are installed in all the storage locations to detect the TIS unit presence. Besides TIS unit reallocation, the manipulator handles the movement of storage rack shielding lids and intermediate supports during the unit insertion on a specific location. An absolute positioning control system allows to reach the desired coordinates by computing the difference between the target and the current position (obtained through an incremental encoder on each axis) and applying a predefined sequence of movements. Each motion axis is equipped with two brushless motors; in case of fault of the main one, the backup actuator can take over and complete the task.

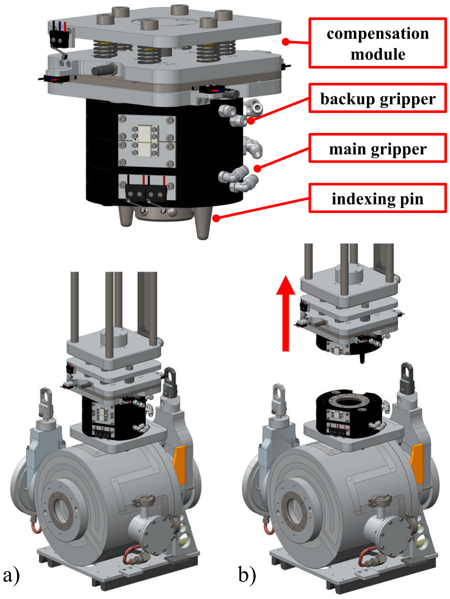


Figure 3.22: Example of disconnection of the TSS backup gripper in case of fault of the main unit.

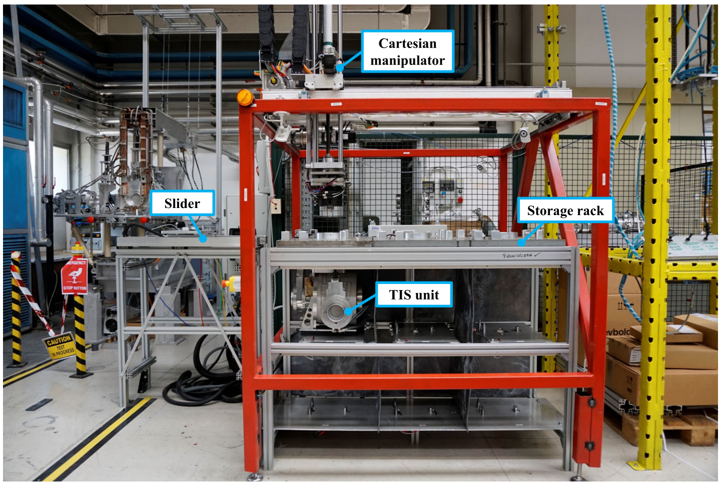


Figure 3.23: Temporary Storage System (TSS) prototype realized in the remote handling laboratory used for the validation of the mechanical and control design

The swapping between the two is made possible by electro-mechanical clutches able to couple/uncouple the actuators with the mechanical transmission. This fault-tolerant approach allows to restore the system safe conditions in order to minimize the personnel exposure during maintenance intervention.

The concept design of the TSS system has been validated in the remote handling laboratory thanks to a prototype shown in Fig. 3.23. The mockup reproduced one module of the rack featuring a reduced storage capacity, nevertheless the mechanical architecture, the cartesian manipulator, the sliding table and all the electronic components were equivalent to the final version. Following the design consolidation process, the full-scale system has been installed within the SPES target area, as shown in Fig. 3.24 and Fig. 3.25.

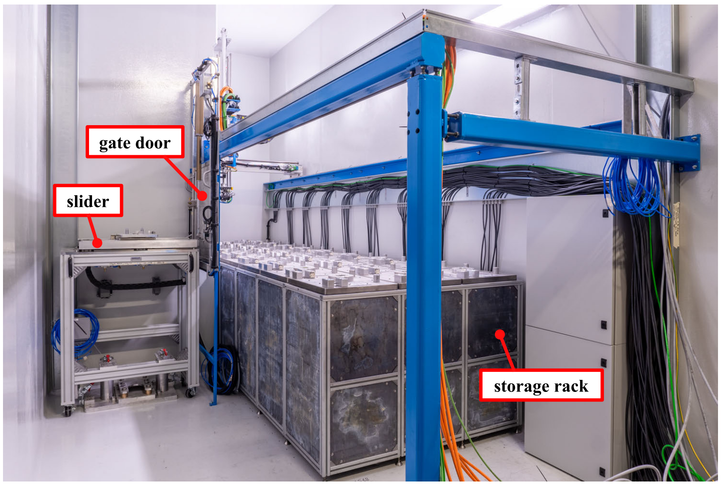


Figure 3.24: Side view of the TSS during installation at the SPES facility.

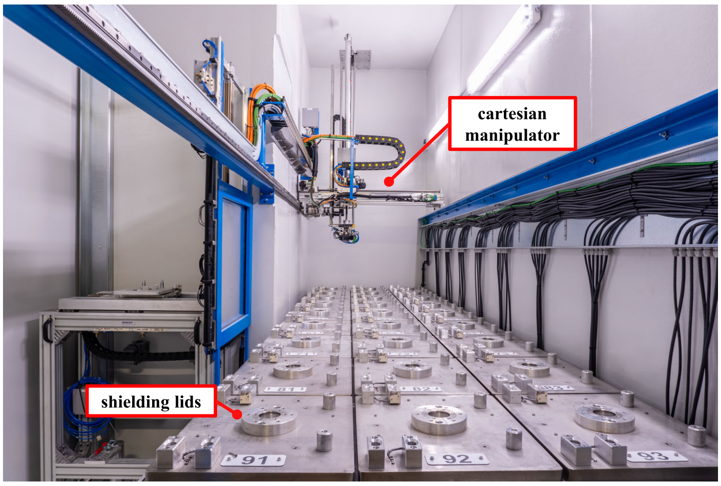


Figure 3.25: Top view of the TSS storage rack.

3.4.2 *Software architecture*

Each storage cell can be modeled by identifying six distinct cartesian positions (or levels) on the standard coupling interface of the various motion payloads within the storage rack. The TSS levels are outlined in Fig. 3.26. Each location, such as the shielding lids, support shelves, or TIS units, is described by a set of coordinates encoded by a unique identifier and stored in a dedicated database. The operator selects a pickup location and an available space within the rack to deposit a radioactive TIS unit for storage in the TSS. An automatic routine plans the required motion tasks to accomplish the storage sequence. The algorithm lists all the steps to free the trajectory from the TIS pickup location to the final storage destination. Thanks to a modular structure, the entire sequence can be divided into smaller tasks. Each

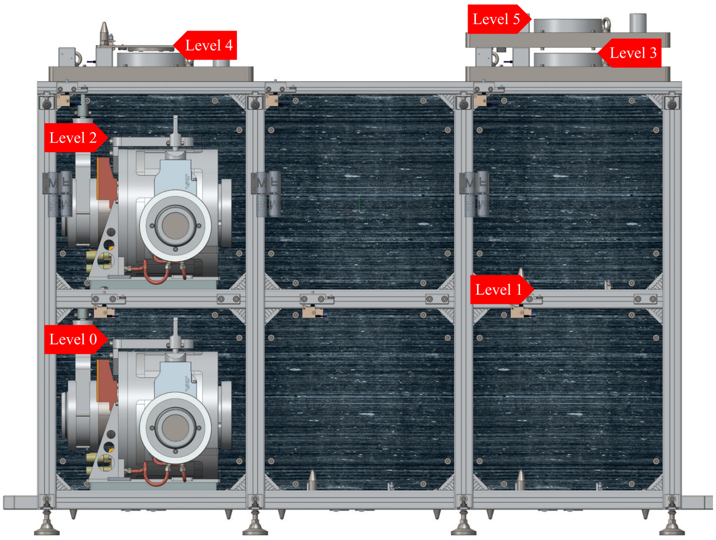


Figure 3.26: The Temporary Storage System positioning levels.

sub-task includes a start (pick) and a destination (drop) location. Every position that the TSS cartesian manipulator can access vertically is equipped with redundant presence switches. Once grasped, the gripper's sensing devices acknowledge the proper TIS unit engagement before moving it to the drop point. At this stage, the presence switches at the destination site detect the positioned item and authorize the TIS unit release. The process is completed by lifting the manipulator to the top position while waiting for the next sub-task. The motion planning software is based on two nested state machines: the inner loop controls the execution of sub-tasks, while the external layer manages trajectories and executes the complete sequence. The TSS control system acts as the supervisor for the other remote handling devices, gathering control, safety, and interlock signals. This setup provides a single interface for connecting to both the SPES ACS and the MPS. Two different PLCs govern the control and safety logic. The first device manages standard physical or fieldbus (Modbus TCP/IP) signals for system operation, whereas the second PLC exchanges double-channel signals with designated safety partners up to IEC 62061 [222] SIL 3.

Signals coming from the actual limit switches installed within the rack are organized in dedicated databases which are accessed during the task execution. According to the layout displayed in Fig. 3.27, the detection devices within the storage rack are codified using unique IDs. As an example, device T231B denotes the limit switch B, installed on the second row, third column, first level, dedicated to the detection of the TIS unit presence. The proposed architecture enables to automate the verification of safety conditions during task execution, such as controlling that the trajectory towards a defined storage location is free of intermediate shielding lids.

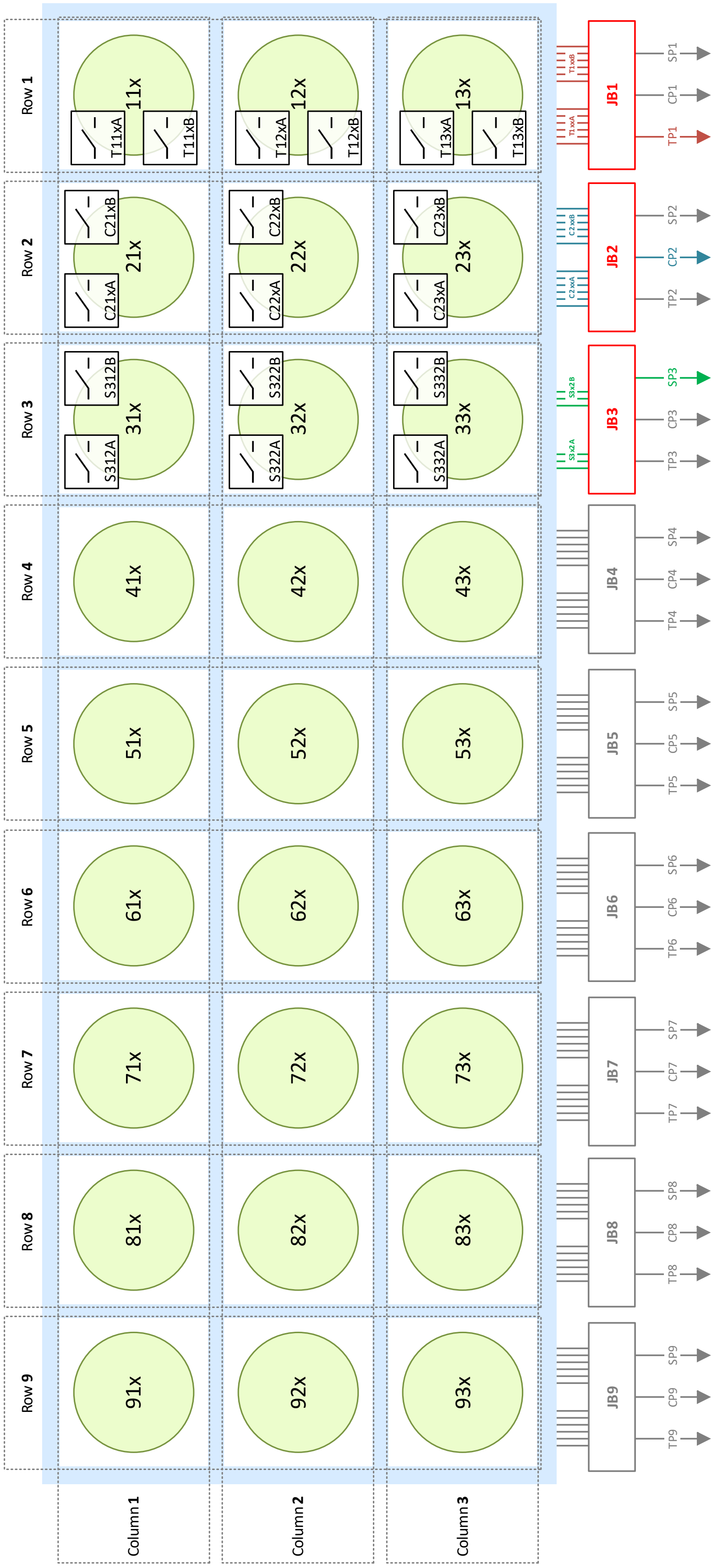


Figure 3.27: Cabling architecture of the Temporary Storage System storage rack.

3.5 DISCUSSION AND FINAL REMARKS

The essential contribution provided by the SPES RH systems in ensuring the safety of the facility, prompted the need for a thorough consolidation of the current architecture aimed at strengthening the systems' resilience and reliability. The design upgrades detailed in this chapter are intended to improve the fault-tolerance of RH machines and increase systems' availability even in the event of a fault. The consolidation process was pursued as part of the inherently safe design approach derived from industrial sectors and recommended in [72].

Consolidation methods have been implemented across two distinct domains. From the framework perspective, the research has proposed a general layout aimed at minimizing RP vulnerabilities, a distributed control and safety architecture intended at optimizing data exchange, a communication infrastructure and logic designed to minimize the risk of accidental interruptions and a supervision layer assisting operators in monitoring the execution of RH tasks. Additionally, the single RH machines' hardware and software architecture have undergone significant improvements, upgrading ing them from their prototype condition to a more robust design, aimed at a safe start of operation.

The findings in this chapter highlight the benefits offered by an optimized architecture and enhanced systems in comparison to the previous layout in terms of a decrease in the likelihood of failure events. The described process was carried out as a preliminary upgrade, with the goal of consolidating the overall framework and addressing the most evident criticalities prior to the actual risk assessment, which was proposed as key research objective.

The analysis of anticipated operational scenarios and the potential effects of failure conditions in a highly radioactive environment served as the foundation for the implemented hardware and software design enhancements. In this regard, the new architecture has a direct impact on systems' reliability, as well as minimizing maintenance activities under non-optimized radiological conditions, hence reducing personnel exposure to ionizing radiation.

The proposed improvements follow general design principles that can be applied to a variety of RH systems operating in other domains. This approach can be considered as a first step towards the early incorporation of safety principles into the RH design process.

As the next research step, Chapter 4 presents a comprehensive risk assessment focused on critical RH activities within the SPES target area, analyzing the potential deviation of the systems while already taking into account their consolidated design.

Part III

OPTIMIZATION

4 PROBABILISTIC RISK ASSESSMENT OF SPES REMOTE HANDLING ACTIVITIES BASED ON A HAZOP-LOPA COMBINED APPROACH

4.1 INTRODUCTION

A semi-quantitative Probabilistic Risk Assessment (PRA) focused on the remote handling activities in the vicinity of the SPES Front-End is presented in this chapter. The likelihood of significant failure scenarios, their effects, and safety precautions are evaluated using two combined methodologies. The study first implements a HAZard and OPerability analysis (HAZOP) analysis, as a qualitative risk assessment methodology for the systematic identification of dangerous conditions and operational issues that may occur from unexpected behavior of essential elements resulting in potentially dangerous (unintended) repercussions. A Layer Of Protection Analysis (LOPA) is then applied to evaluate improvements in the system's risk level obtained by the introduced Independent Protection Layers (IPLs), hence confirming the validity of the suggested safeguards. The chapter is structured as follows: Section 4.2 outlines the study's goal, while Section 4.3 provides a detailed overview of the key systems addressed by the risk assessment: the SPES Front-End and remote handling equipment. Section 4.4 describes the methodology adopted for this study: the HAZOP-LOPA analysis. Sections 4.5 and 4.6 present the main findings of the research and discuss their implications. Section 4.7 finally draws the conclusions and presents the next research steps.

4.2 RESEARCH OBJECTIVES AND APPROACH

The main goal of the investigation is the identification of the primary sources of hazard and the assessment of the likelihood of failure of essential elements to suggest the design of effective recovery solutions that will be adopted to decrease the demand of personnel access. The aims of the research have been further detailed as follows:

- Identify the system's deviations from the behavior foreseen in the design stage. Assess the failure scenarios that may result in a danger for humans or for the environment using a methodical procedure targeted at recognizing harmful conditions and operational problems.

- Assess the performance of the recommended protection layers (safeguards), through a specific comparison between the risk level of the system without any barrier and the risk level of the protected system employing a risk tolerance criterion.

- Optimize the system under analysis by putting in place safety measures meant to reduce the danger of access for staff members linked to maintenance interventions aimed at repairing the equipment after a failure in locations with a high risk of radioactivity.

The PRA methods outlined in this study, which are widely used in other contexts, are applied to the SPES risk scenarios while the facility is still in the construction stage. Considering Nuclear Power Plants (NPPs) as an example, Level 1 Probabilistic Safety Analysis (PSA) is used to support the process of identifying and resolving plant weaknesses during the design phase [68]. Similarly, the above strategy is extremely beneficial for the SPES facility, since it enables the upgrade of machines design, the development of effective safeguards, and the drafting of specific procedures aimed at the mitigation of the residual risk highlighted by the PRA outcomes. The advantages deriving from the application of HAZOP to the foreseen remote handling tasks in facilities that are still under construction, as well as their effects on the improvement of essential component design, have been observed in other fields such as nuclear fusion research centers [78].

4.3 FOCUS OF THE STUDY

At SPES, remote handling machines are intended to automate the TIS unit life cycle and minimize the need for hands-on interventions. Human involvement is still necessary, though, in the event of a failure, during maintenance activities. The hazardous operating conditions are provided, among the many possibilities, by maintenance tasks intended to correct a fault state that occurred inside the ISOL hall during the TIS unit automatic removal procedure. Human interventions in this area can result in severe radiation exposure, on top to the ordinary hazards triggered by the specific installation (which include mechanical risks, high-voltage, low light, and limited space). As a result, the focus of the study are failures that could impact the most crucial remote handling activities. The main systems engaged in this process are the SPES Front-End and the Horizontal Handling Machine (HHM), which are depicted in Fig. 4.1. A comprehensive description of these two machines, as primary focus of the PRA, is available in the following sections.

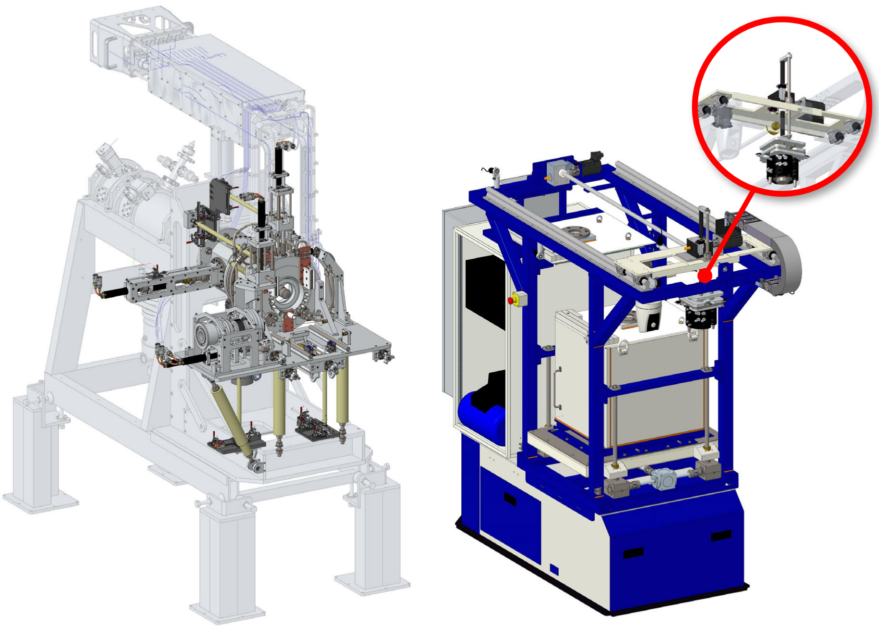


Figure 4.1: The remote handling systems analyzed in the study: the SPES Front-End (on the left), and the Horizontal Handling Machine (HHM) (on the right).

4.3.1 *Front-End*

The SPES On-Line Front-End, acts as interface between the PPB and RIB lines and the TIS unit, where the radioisotopes are produced following a fission reaction triggered by protons colliding with the UCx target disks.

4.3.1.1 *Operating modes*

Due to the deteriorating effects that are frequently seen on both the target and ion source, the TIS unit needs to be replaced on a regular basis. The SPES program has been developed in accordance with this requirement, providing a cyclic operation over four weeks, including two weeks of irradiation alternating with a two-week break. Following the cooling phase, the TIS unit exhibits a 100-fold drop in activity [196]. At this stage, a dedicated remote handling system called HHM takes care of its automatic replacement. From the functional standpoint, two distinct operating modes can be identified for the SPES Front-End: “setup” and “beam”. In the initial setup, the system’s purpose is to disconnect the radioactive TIS unit and connect a new unit to the beam lines. The switch to the “beam” mode is triggered by the TIS unit’s effective coupling and configuration. In this arrangement, the proton beam coming from the SPES cyclotron can impinge the target for isotopes production. A portion of the SPES Front-End, which includes the TIS unit, is maintained at high voltage (40 kV) during this phase. Simultaneously, ohmic heating keeps the target and ion source at the nominal working temperature of 2300 °C. Isotopes are extracted and accelerated in the direction of experimental stations thanks to a titanium electrode (at 0 V) on the RIB line. The SPES Front-End, located within the ISOL hall is visible in Fig. 4.2.

4.3.1.2 *Description*

The TIS unit's connection and disconnection from the PPB and RIB lines are handled by dedicated subsystems, as part of the SPES Front-End. The coupling process consists of four steps and begins when after the TIS has been installed on the Front-End by the HHM. The TIS unit is coupled with RIB line first, while the PPB line connects with the vacuum chamber in a second stage. The procedure ends with the TIS unit gate valves being opened. Four linear axes, each consisting of a lead-screw powered by a pneumatic motor, are intended to carry out the outlined motion sequence. The TIS unit is initially moved backwards or forwards in the RIB direction by a special nut pushing two mechanical stops at the unit baseplate. A telescopic bellows that connects the PPB line to a specific interface on the TIS unit can be extended and compressed by means of a second axis. The two additional vertical axes are supplied with a raising pin attached to the nut. The pins plug into the hooks at the top of the gate shafts after the unit coupling, allowing the valves to open and close. For each axis of motion, different sensors are provided to determine its exact position. Specifically, two limit switches (Omron® TZ-1GV22) and a linear potentiometer (Genge&Thoma® 13-032b) work together to deliver re-

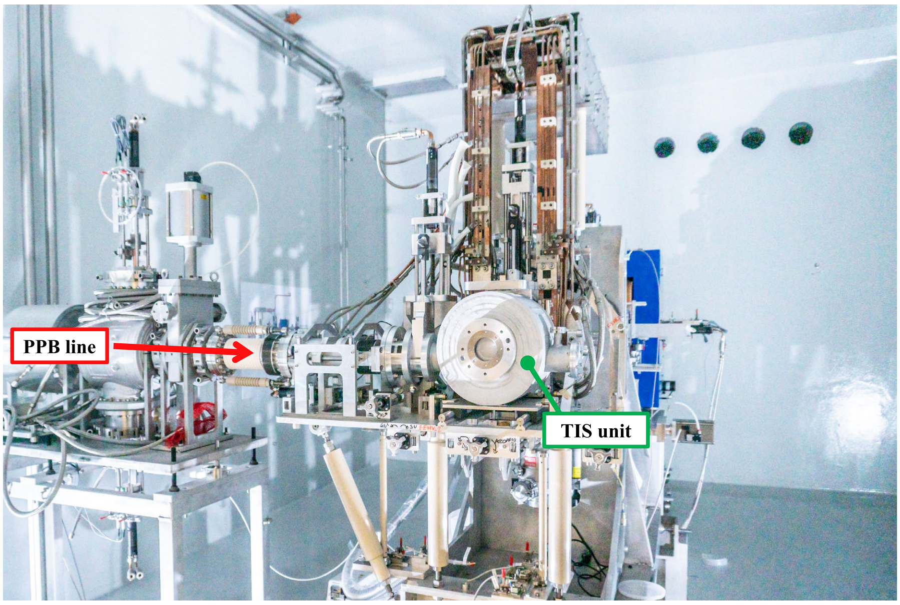


Figure 4.2: The SPES On-Line Front-End installed within the ISOL hall.

dundant feedback on the axis position. Thanks to this architecture, in the case that one of the components fails, the others can be used for recovering the lost system status information. Non-conductive driveshaft, realized in PEEK, are used to link the mechanical axes (located in the 40 kV portion of the Front-End) with the ground chassis where the sensing units are mounted. In order to overcome potential lacks of movement caused by a fault of the pneumatic actuator, a backup motion interface is directly attached to the lead-screw of each linear axis. Thanks to this feature, an external system can be connected to complete a partial coupling or decoupling task. A detailed view of the PPB motion axis is displayed in Fig. 4.3, showing the pneumatic actuator, the lead-screw mechanism, the telescopic bellows, and the backup motion interface. The four axes in charge of coupling and decoupling the TIS unit share the same kinematic and operational principles. Because of this, a generic motion axis is taken into account as a node in the HAZOP analysis discussed in Section 4.5.

On the SPES Front-End, an additional motion axis is committed to the motion of the extraction electrode, enabling its displacement along the RIB line. In this case the kinematic chain includes a pneumatic motor, a reduction gear, a magnetic rotary feed-through, and a rack-pinion coupling. Despite being more sophisticated, this axis employs the standardized coupler architecture, with the significant exception that the backup motion interface is not implemented in this specific case due to lack of space. The system is visible in Fig. 4.4.

The Front-End, after the TIS unit connection, performs its setup in preparation for the upcoming irradiation stage. Once coupled with

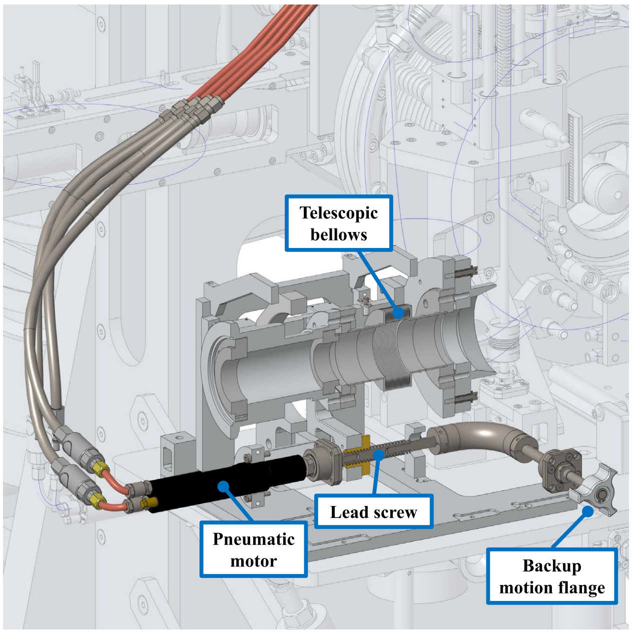


Figure 4.3: 3D view of the motion systems devoted to the TIS coupling with the PPB (a) and the RIB (b) channels on the SPES Front-End.

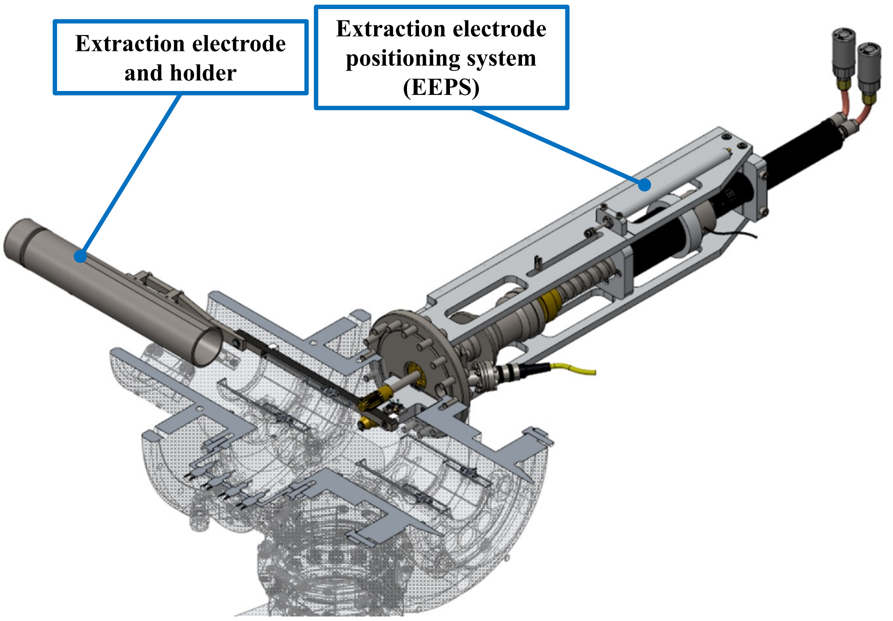

Extraction electrode and holder
Extraction electrode positioning system (EEPS)

Figure 4.4: Section view of the rib line and the Extraction Electrode Positioning System (EEPS). The actuation system features a rack-pinion mechanisms and two limit switches in vacuum. .

the PPB and RIB lines, multi-stage roots pumps and turbopumps work together to establish a high vacuum regime (10^{-6} mbar), while a series of multipurpose connectors supplies electrical power, water cooling, and gas, as well as being used to monitor sensitive parameters. During operation, the MPS supervises the system's behavior while seeking to prevent potentially harmful inconsistent conditions by exchanging hardware and software interlocks signals with experimental equipment on-site.

The ISOL hall is subjected to a composite radiation field which includes protons, neutrons, and photons as a consequence of the PPB collision with the UCx target and the consequent ^{238}U fission process. In this context, it is possible to distinguish between three main contributions: the TIS unit [196], the implantation of isotopes on the extraction electrode [227], and the residual activation of the Front-End machine [228].

With the help of the FLUKA [204, 206] and MCNPX [229] Monte Carlo codes, the equivalent dose rate in the ISOL hall has been estimated. Specifically, the equivalent gamma dose rate calculated at one meter from the TIS unit after a full-intensity irradiation cycle (two weeks, 40 MeV, 200 μA PPB) and a two-week decay period is around 40 mSv/h. When compared to the value obtained shortly after irradiation, where the TIS unit activity is about $3 \cdot 10^{13}$ Bq, the post-decay dose rate is reduced of approximately two orders of magnitude.

Maintenance activities are usually planned during yearly Technical Stops (TSs). In this case, following the removal of the TIS unit, the main contributions are due to the Front-End and the extraction electrode. The simulated ambient dose equivalent rate dH*(10)/dt after one year of operation (10 irradiation cycles) and 45 days of cooling, is approximately one order of magnitude lower than the contribution due to the isotope deposition on the ion extraction electrode tip in the same sampling position. Figure 4.5 reports the simulated ambient dose equivalent rate dH*(10)/dt due to photons emitted by the Front-End activated materials in the ISOL hall. The dose rate map does not take into account the potential contribution of surface contamination, which represent an additional risk for operators during regular and unplanned maintenance activities.

According to the As Low As Reasonably Achievable (ALARA) principles [95], most significant radioactive sources, consisting of the TIS unit and the extraction electrode, must be removed prior to the execution of these activities to reduce workers exposure. Since this safeguard is unattainable during regular operations, the severity rating of HAZOP deviations that may result in dangerous consequences accounts for a substantial environmental dose rate. A detailed discussion is available in Section 4.5.

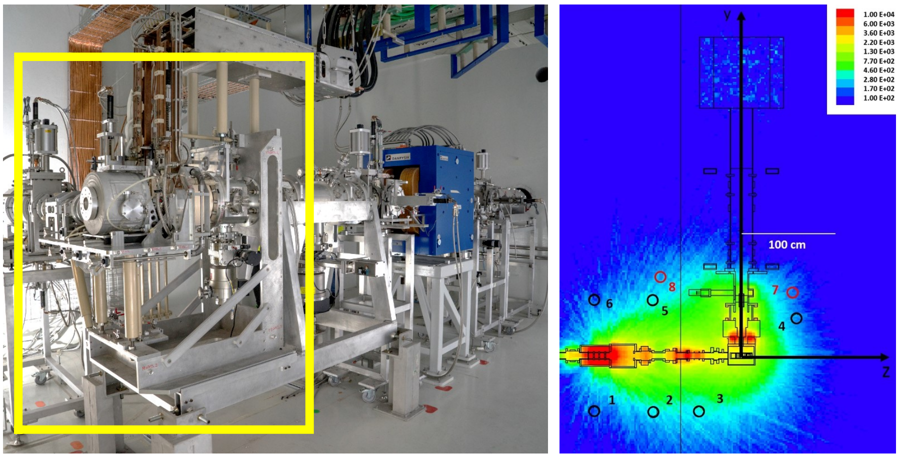


Figure 4.5: (left) the SPES ISOL hall, (right) MCNPX spatial mesh of the ambient dose equivalent rate dH*(10)/dt in the ISOL hall, the mesh is calculated on a horizontal plane crossing the center of the TIS unit [228].

4.3.2 *Horizontal Handling Machine (HHM)*

The HHM is the SPES primary remote handling system, based on an AGV, which is in charge of the manipulation and transport of the TIS unit within the irradiation zone of the facility. The study focuses, among the different scenarios, on the remote handling procedures aimed at replacing the TIS unit once it has been detached from the Front-End. During this operation, the HHM first moves toward the Front-End in order to retrieve the TIS unit. Subsequently, the cartesian manipulator picks it up and places it in a shielded box for the following transfer and storage within the TSS [212]. The described sequence represents the most crucial HHM procedure because it accomplishes remote handling duties with a high-activity TIS unit under severe dose rate environmental conditions. The HHM accessing the ISOL hall is visible in Fig. 4.6.

Aside from standard operation, the HHM can be employed as remote handling tool in the event of a malfunction to any of the Front-End motion axes associated with the connection (or disconnection) of the TIS unit. According to the description given in the previous section, a backup motion flange is available for each linear axis. Whenever required, the HHM can be equipped with a specific actuator aimed at coupling with the Front-End and controlling the faulty assembly.

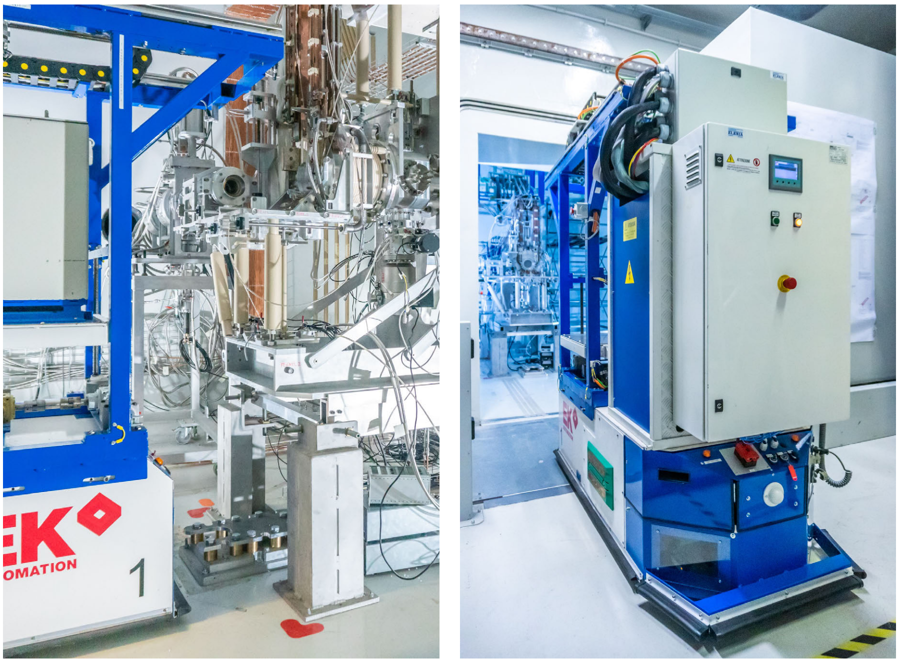


Figure 4.6: The HHM while removing the TIS unit from the SPES Front-End.

4.4 RISK ASSESSMENT TOOLS

From a safety point of view, the states of the SPES facility have been categorized depending on their frequency of occurrence, following the classification principles promoted by the International Atomic Energy Agency (IAEA) guidelines [230]. Table 4.1 categorizes the states into five levels and relates to them with their likelihood. Specifically, the "operational" states are denoted by levels A and B, while the "accident" situations are identified by levels C and D. Level E is reserved for unanticipated events that go beyond the plant design basis.

A single professionally exposed worker is allowed to receive a maximum annual effective dose of 20 mSv/year under Italian law (D. Lgs. 101/20) [93]. However, LNL's internal policies [227] indicate a conservative threshold of 5 mSv/year per worker. The severity levels in Table 4.2 are determined in respect to the population and personnel's potential exposure, and are presented as individual doses integrated over a one-year period. A maximum yearly effective dose corresponding to severity levels (S) I and II is considered to be tolerable for Cat. B employees, whereas severity levels (S) III and IV have relevance for Cat. A workers. The SPES risk acceptance criterion is used to determine the exposure ranges for non-exposed workers and the general population. The PRA presented in this chapter utilizes the risk matrix reported in Table 4.3. Among the three recognizable levels, acceptable risks are depicted in green, intermediate risks in yellow,

Level (L)	Likelihood	Description
A	L >1	*Normal Operation (NO):* operations within specified operating limits and conditions (starting, stopping)
B	10^{-2} <L <1	*Anticipated Operational (AE):* events that should occur during the useful life of the structure
C	10^{-4} <L <10^{-2}	*Unanticipated Operational (UE):* events that could occur during the life cycle of the facility
D	10^{-6} <L <10^{-4}	*Design basis accidents (DBA):* incidental conditions foreseen in the design phase
E	L <10^{-6}	*Beyond Design Basis Incidents (BDBA):* more serious accident conditions than an accident considered at the design level

Table 4.1: Likelihood levels (L), intervals are expressed in yr^{-1}.

Level (S)	Severity (Conventional)	Severity (Radiological)
I	Light wounds	Population <0.001 mSv Worker <0.5 mSv
II	Moderate wounds with medical attention	0.001 mSv <Population <0.01 mSv 0.5 mSv <Worker <6 mSv
III	Serious wounds with medical attention	0.01 mSv <Population <0.1 mSv 6 mSv <Worker <10 mSv
IV	Extensive injury or death	0.1 mSv <Population <1 mSv 10 mSv <Worker <20 mSv
V	Multiple deaths	Population >1 mSv Worker >20 mSv

Table 4.2: Severity levels [S] associated to national limits on the maximum annual effective dose for individuals.

and unacceptable risks are represented by red scores. Due to the specified risk acceptance condition, the risk matrix is not symmetrical. This chapter presents a blended PRA that combines HAZOP and LOPA. The HAZOP study, presented in Section 4.5, is an organized and methodical brainstorming methodology used as a qualitative risk assessment tool to identify potential hazards in a system [231]. LOPA, which is described in Section 4.6, is a semi-quantitative technique for estimating the magnitude of risk associated with the selected failure conditions by taking into account the frequency of Initiating Events (IEs), the impact of IPLs, as well as any possible repercussions [232].

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

Table 4.3: The SPES risk matrix. Risk levels are represented by different colors: Low (L) in green, Medium (M) in yellow, High (H) in red.

4.5 hazard and operability (hazop) analysis

4.5.1 *Introduction*

The HAZard and OPerability analysis (HAZOP) [233, 234] when applied to a system (or process) enable the identification, for the identified "nodes", of the potential deviations from intended behavior in the design stage with the aim of assessing the hazards associated with each pair cause-consequence leading to the deviation [235]. This method is typically used for proving the resilience of the design, process, and procedures of operating facilities through the evaluation of the possible failure scenarios, their transmission, consequences, and the implemented safety measures [78]. The identification of any predicted deviations or unwelcome circumstance is made possible by the systematic evaluation of the various nodes throughout each operational phase and the examination of the interactions across all the different elements [236]. A multidisciplinary team (HAZOP team) with an extensive understanding of the facility's design, operation, and maintenance develops the investigation during regular meetings [237]. Hazard Identification (HI) and PRA are combined with the assessment of failure events as essential phases of the safety management process. The semi-quantitative HAZOP analysis described in this chapter has been applied to the SPES facility during its design stage, prior to the actual operation, to highlight the most crucial malfunctioning conditions from the perspective of personnel safety that may occur during the execution of remote handling tasks including the HHM and the SPES Front-End.

4.5.2 *Material and Methods*

The HAZOP method has been combined with the risk matrix shown in Table 4.3 to quantify the risk scenarios associated with each deviation. The assessment was developed in accordance with the protocol displayed in Fig. 4.7. The procedure begins with the meticulous screening for potentially dangerous situations, i. e. operational issues that can originate from anomalies in system behavior and could result in unintentional (abnormal) effects [238]. The Likelihood (L) and Severity (S) levels associated with the given scenarios are evaluated in the following phase, according to the categories presented in Table 4.1 and Table 4.2, respectively. Following the formulation of safeguards and recommendations, the risk associated with each failure condition is compared before and after their introduction.

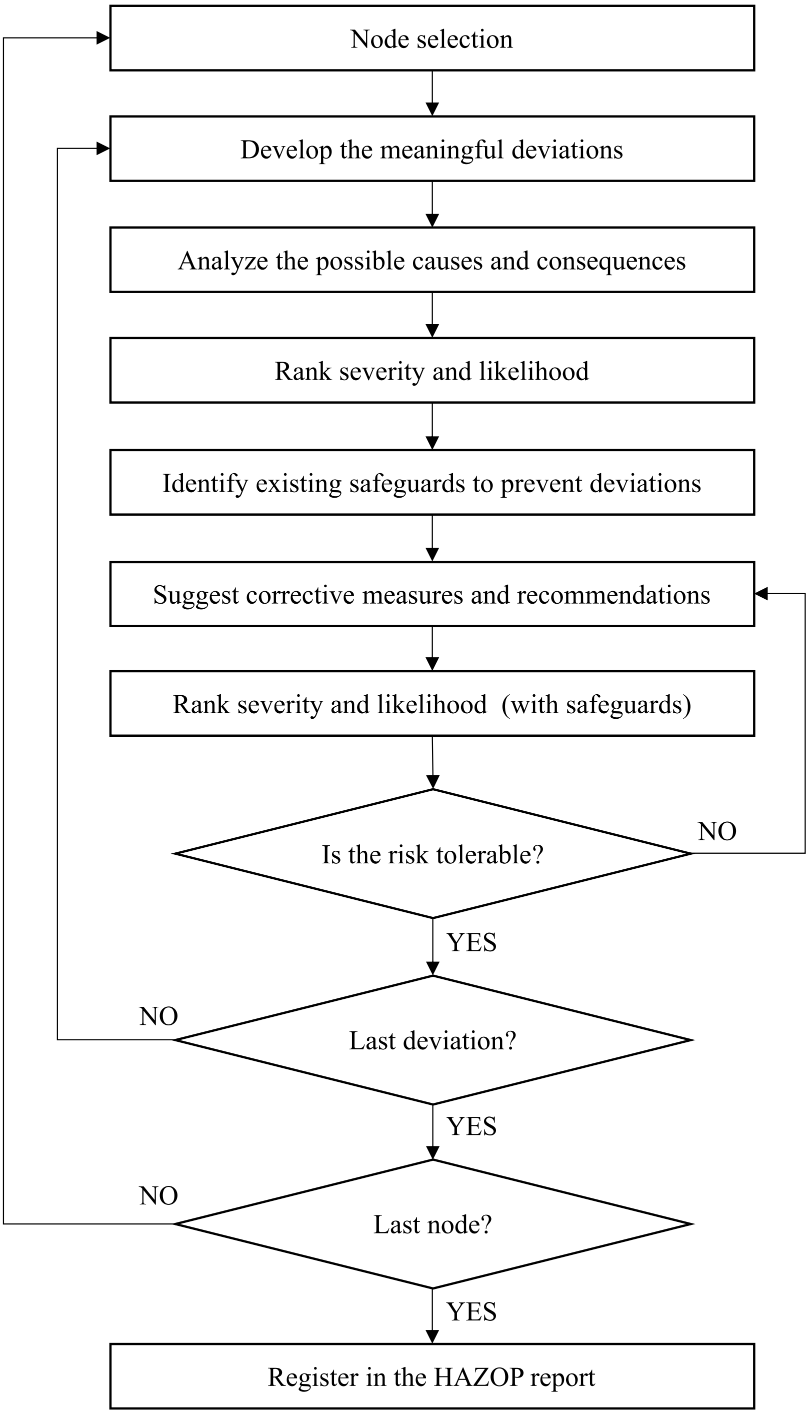

Node selection
Develop the meaningful deviations
Analyze the possible causes and consequences
Rank severity and likelihood
Identify existing safeguards to prevent deviations
Suggest corrective measures and recommendations
Rank severity and likelihood (with safeguards)
Is the risk tolerable?
NO
YES
NO
Last deviation?
YES
NO
Last node?
YES
Register in the HAZOP report

Figure 4.7: The HAZOP analysis flowchart.

The HAZOP study has been focused on the recovery actions to be performed in case of a failure under severe environmental conditions. As remarked by the ALARA principles, intervention shall be optimized in order to prevent or limit personnel access to high-risk areas. The study provided a set of safeguards, reported in Table 4.4, conceived to optimize the failure scenarios emerging from each deviation. Some of them have the goal of reducing the likelihood that the causes of the deviations will occur, while others have been introduced to minimize the severity of the consequence, e. g. the impact on workers.

Code	Safeguard
A	Diagnostics, Auto-test
B	Periodic replacement
C	Inspection and maintenance program
D	Backup actuators
E	Training of specialized operators
F	Use of PPEs
G	Operating procedures
H	Radiation monitoring
I	Personal dosimeters
J	Access Control System (ACS)
K	Body Scanner
L	Machine Protection System (MPS) override
M	Remote inspection using the Horizontal Handling Machine (HHM)

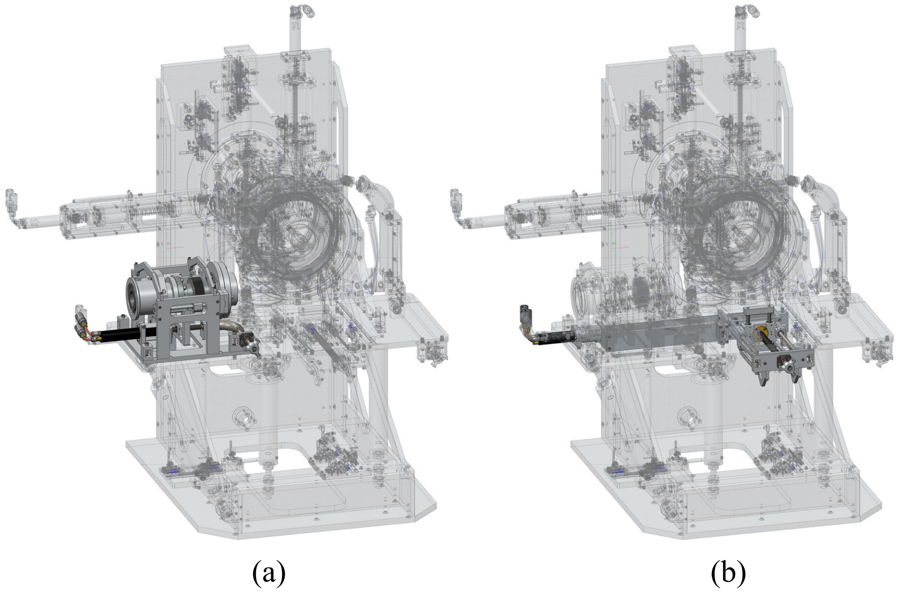
Table 4.4: The safeguards identified in the HAZOP analysis.

4.5.3 *Results*

The following sections provide a detailed description of the outcomes of the HAZOP analysis. The complete HAZOP worksheets can be found in Appendix. A. In the presented analysis, each cause-consequence pair is associated with the applicable safeguards to be implemented in order to mitigate the overall risk of the analyzed deviation.

4.5.3.1 *Proton & RIB channels*

The first HAZOP node is related to the motion axes devoted to the connection of the TIS unit with the PPB and RIB lines. The two systems are located on the Front-End coupling table as highlighted in Fig. 4.8. Despite recognizing that each of them features a unique design, from the risk assessment perspective they all share the same functional components: a main pneumatic motor supplied by a dedicated circuit, a mechanical transmission chain and a backup actuation flange. As a result, they have been aggregated into a single HAZOP node. The considered deviation for this node is the lack of movement of one of the two axes, resulting in a failure scenario in which an irradiated TIS unit gets stuck within the ISOL hall. The analyzed deviation could be the result of various anomalies that have been identified. The HAZOP worksheet for the PPB and RIB channel node is shown in Table 4.5. Based on how each potential cause of the observed deviation has an influence on either Business (B) or Safety (S), the identified consequences have been classified into two groups.



(a) (b)

Figure 4.8: 3D view of the motion systems devoted to the TIS unit coupling with the PPB (a) and the RIB (b) channels on the SPES Front-End.

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	

Table 4.5: HAZOP worksheet for the RIB channel node.

The Likelihood (L) assessment for each failure condition considers a variety of factors, such as design modifications aimed at preventing IEs or the beneficial effects of safeguards introduction. Examples from the first category in the context of pneumatic motors include employing radiation-tolerant lubricant or redesigning the impeller with PEEK material. Regarding the second group, it is important to stress the benefits of preventive maintenance. As the primary cause (1.1.1), a pneumatic motor failure has been proposed. This may be related to a problem with the lubricant, impeller, impurities or material deterioration. For this event, three possible failure recovery scenarios has been analyzed. In the first case the HHM is employed for the remote disconnection of the TIS unit exploiting the backup motion flange of the faulty axis. Thanks to this approach, the TIS unit may be removed from the area in order to strongly decrease the environmental dose and thus allowing to perform a subsequent maintenance intervention under optimized radiological conditions. Since this scenario does not imply any personnel exposure, the associated risk has been classified as low. The recovery approach employed in the first scenario is likewise used in the second (1.1.2); the difference in this instance is that the Manual Handling Machine (MHM) is used rather than the HHM. This distinct activity necessitates the involvement of an operator for the backup axis motion. In this case, the worker will approach the Front-End operating the MHM for the backup axis actuation keeping a 2 meters distance from the irradiated TIS unit. Both the limited duration of the intervention and the possibility to equip the MHM with a customized shielding has contributed in classifying the risk associated with this event as medium. The third scenario (1.1.3) examines the need for a maintenance intervention, aimed at the replacement of the damaged pneumatic motor, in the event that the TIS unit cannot be uncoupled from the Front-End and removed using automatic or manual handling devices. This recovery action exposes the operator to a significantly higher dose, hence it must be carefully evaluated through a dedicated Work and Dose Planning (WDP) that needs to be approved by the Facility's RP officers.

Failure of the pneumatic air supply is a potential second factor that could result in the axis being blocked. The recommended recovery actions are parallel to those considered in the previous case. In more detail, scenario 1.2.1 involves the use of the HHM for the remote actuation of the axis backup flange, whereas in case 1.2.2 the MHM is used to uncouple the TIS unit in a rapid intervention. Speaking about maintenance operations in presence of an irradiated TIS unit, a distinction should be made between interventions within the ISOL hall (S018) and interventions in the technical room (S017). When compared to 1.1.3, the risk associated with 1.2.3 can be categorized as medium due to the physical working position being located further away from the primary source of danger, the TIS unit. External interventions (1.2.4), on the other hand, don't pose any major radiological concerns and can be considered as low risk.

The third cause (1.3.1) includes all potential mechanical issues that can result in the blockage of the axis under examination. Since the backup flange is worthless in this situation, a maintenance operation in the vicinity of the TIS unit is required. Aside from the actual feasibility of this type of intervention, which is heavily dependent on the individual and collective dose estimated in accordance with the environmental conditions of the operating zone, the risk associated with this event has been categorized as high.

The evaluation of additional minor hardware malfunctions that may prevent the Front-End motion axes from moving completes the analysis of this node. This includes potential electrovalves failure in room S017 (1.4.1) or problems with the control system in room 1017 (1.5.1). In both situations, the working area is not dangerous and the risk associated with the intervention is low.

4.5.3.2 *PPB & RIB gates*

The motion axes in charge of the operation of the TIS unit gate valves are taken into account by the HAZOP analysis as a second node. The two systems, which are a part of the Front-End coupling table, are intended to latch onto two specific hooks on the TIS unit to open or close the valves in the PPB and RIB directions. Due to their similarities, the two motion axes, highlighted in Fig. 4.9 can be considered as a single HAZOP node. Table 4.6 reports a summary of the results, where the risk associated to each pair cause-consequences has been color coded according to the SPES risk matrix presented in Tab. 4.3. The complete HAZOP analysis is available in Appendix A.

The analyzed deviation for this node is attributed to a lack of movement of one of two axes, leading the TIS unit to become stuck on the Front-End with one of the gate valves entirely or partially open.

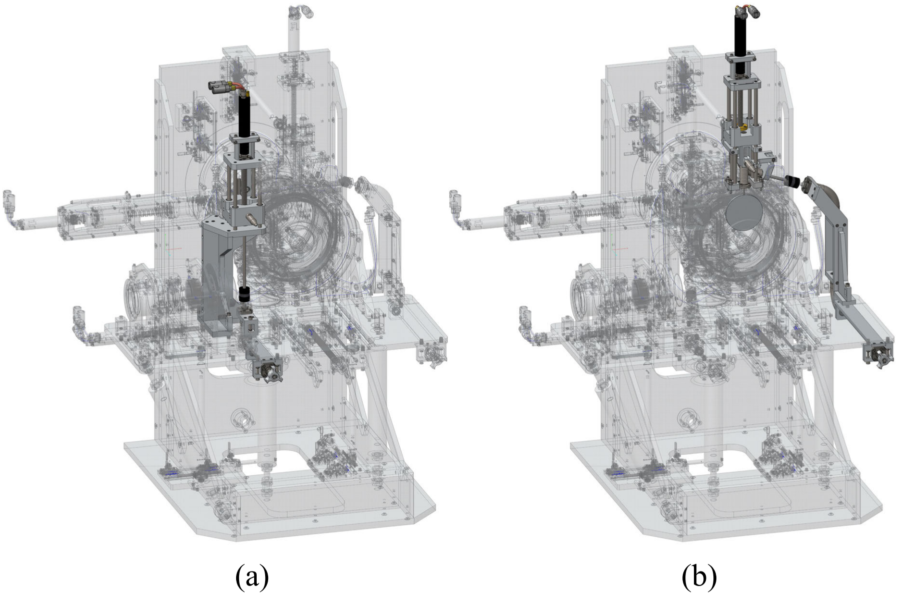


Figure 4.9: 3D view of the motion systems devoted to the opening and closing of the TIS unit PPB (a) and RIB (b) gate valves on the SPES Front-End.

ID	Cause	Consequence
2.1.1	Gate valve failure, open pos.	Forced disconnection (MHM)
2.1.2	Gate valve failure, open pos.	Maintenance intervention (S018)

Table 4.6: Summary of HAZOP ID 2: PPB and RIB gates.

It is possible to distinguish between several scenarios. For example, if the TIS unit gate valve can be closed using either the HHM or the MHM acting on the backup motion flange, the case can be linked to the failure recovery techniques evaluated for node 1.

Conversely, there will be two solutions available if the failure prevents a remote recovery. In the first case (2.1.1), if the configuration of the gate valves within the TIS unit is compatible with its remote transport and storage, an option could be to bypass some specific MPS interlocks enabling the TIS unit disconnection from the PPB and RIB lines with the gate valves partially open. By using this approach, later maintenance interventions may be accomplished with a reduced environmental dose. In the second scenario (2.1.2), the only available recovery option would be to carry out a maintenance intervention with the TIS unit installed on the Front-End in order to address the primary issue. In all cases, there is a risk of potential contamination in addition to the possibility for high gamma dose exposure, which qualifies these situations as high risk.

4.5.3.3 *PPB and RIB diagnostic*

The HAZOP study, as third node, focuses on the diagnostic components used for the monitoring the status of the Front-End coupling table. Each linear motion axis features two limit switches and a linear potentiometer. While the first are utilized to identify the axis's status (open or closed), the second is used for calibration and redundancy. Figure 4.10 displays the diagnostic modules for the four primary motion axes devoted to the TIS unit coupling to the PPB and RIB lines. Table 4.7 briefly summarizes the analyzed scenarios, more details are available in Appendix A. The missing detection of the axis position has been recognized as the key deviation for this node. Two potential causes have been identified in this context: either a breakdown of an electric component like a limit switch or potentiometer (3.1.1), or a mechanical misalignment in the position detection chain (3.2.1). In both cases, the status of the system can be evaluated through alternative methods

ID	Cause	Consequence
3.1.1	Switch/pot. hardware failure	Maintenance intervention (S018)
3.2.1	Mechanical misalignments	Maintenance intervention (S018)

Table 4.7: Summary of HAZOP ID 3: PPB and RIB diagnostic.

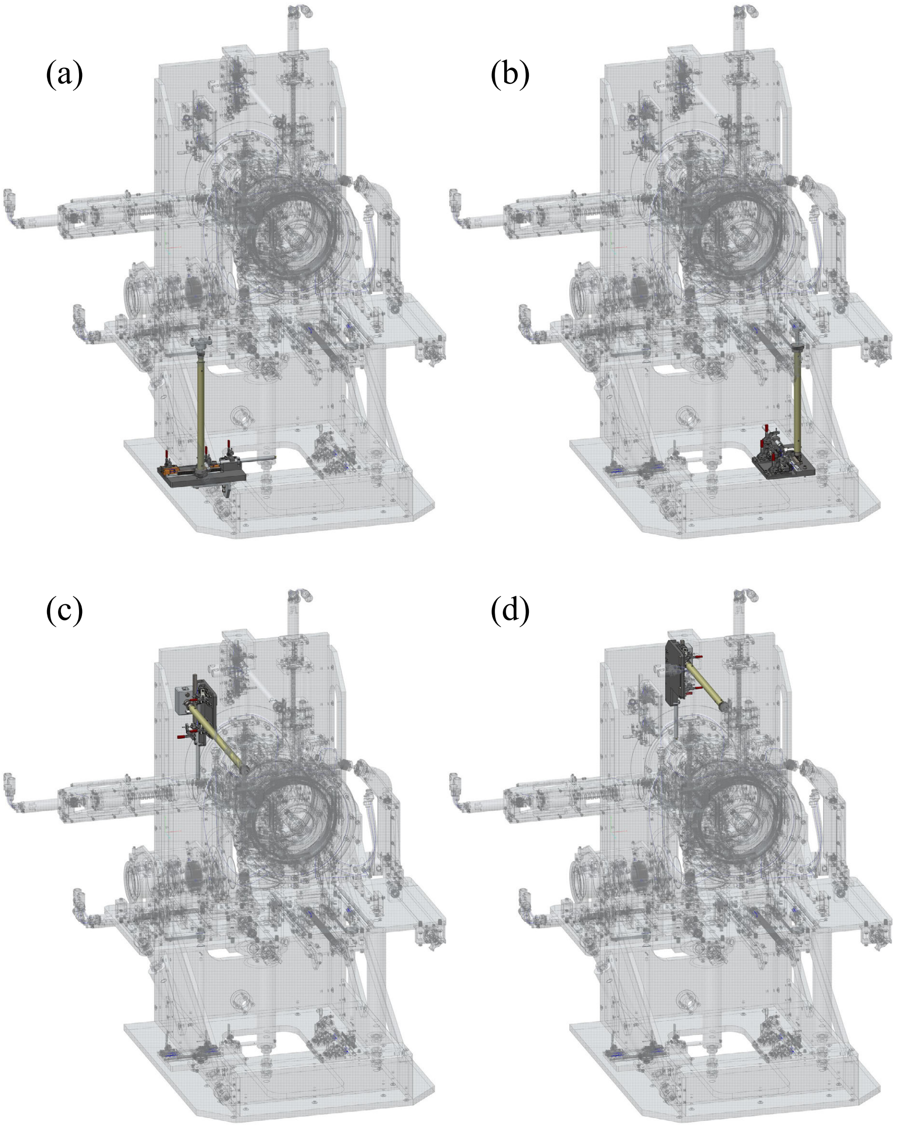


Figure 4.10: 3D view of the diagnostic devices (potentiometers and limit switches) dedicated to the position detection of PPB channel (a), RIB channel (b), PPB gate valve (c), RIB gate valve (d) motion axes on the SPES Front-End.

such as surveillance cameras, remote inspections using the HHM or redundant detection devices. Following a thorough inspection and verification of the system status, the bypass of specific MPS conditions would allow to ignore the interlock and complete the TIS unit removal sequence. Because of this strategy, the maintenance intervention envisioned in cases 3.1.1 and 3.2.1 to restore the right detection chain would be carried out in a site devoid of the TIS unit. For this reason, the associated risk has been evaluated as medium.

4.5.3.4 *Extraction Electrode Positioning System (EEPS)*

Because of its distinct features, the Extraction Electrode Positioning System (EEPS) visible in Fig. 4.11 has been considered as an independent node in the HAZOP study. Being unable of moving the extraction electrode along the RIB line was identified as main deviation. This scenario is critical because it may prevent the RIB gate from closing, inhibiting the TIS unit from being uncoupled and removed. The analyzed failure scenarios are summarized in Tab. 4.8, whereas a more in-depth assessment is available in Appendix A.

The main pneumatic motor malfunctioning has been identified as the primary reason (4.1.1) of the extraction electrode not moving in the examination of the various cause-consequence pairs. Unfortunately, because the backup motion flange is missing on the EEPS, the remote procedures suggested for the failure recovery of the other Front-End motion axes are not applicable in this scenario. As a result, replacing the motor during a maintenance intervention with the irradiated TIS unit still placed on the Front-End would be the only method to restore movement. This event has been classified as high risk due to the significant estimated personnel exposure. A demanding maintenance intervention is expected as well in the event of mechanical troubles on either the transmission chain components placed in atmosphere or in vacuum. In both circumstances, an operator must enter the ISOL hall with a significant ambient dose. Furthermore, the access to in-vacuum

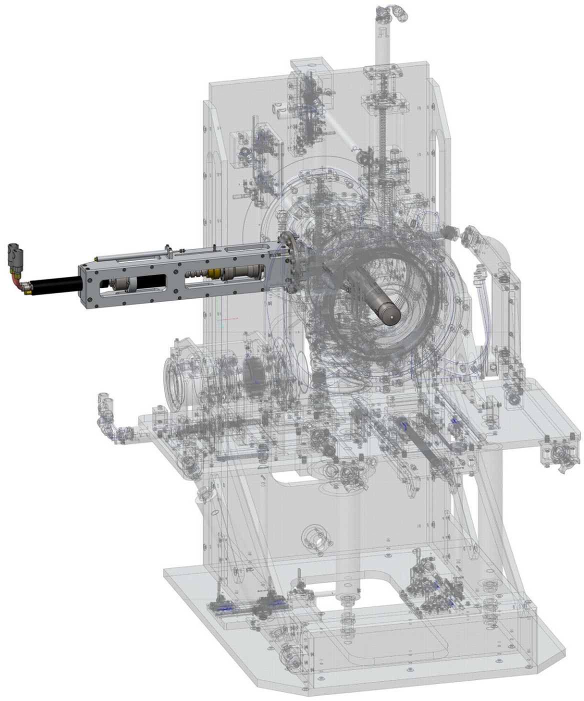


Figure 4.11: 3D view of the motion systems in charge of the positioning of the Front-End extraction electrode along the RIB line.

ID	Cause	Consequence
4.1.1	Pneumatic motor failure	Maintenance intervention (S018)
4.2.1	Mechanical problems (atm.)	Maintenance intervention (S018)
4.3.1	Mechanical problems (vac.)	Maintenance intervention (S018)
4.4.1	Pneumatic supply failure	Maintenance intervention (S018)
4.4.2	Pneumatic supply failure	Maintenance intervention (S017)
4.5.1	Electrovalve hardware failure	Maintenance intervention (S017)
4.6.1	PLC hardware failure	Maintenance intervention (1017)

Table 4.8: Summary of HAZOP ID 4: EEPS.

components would expose the personnel to potential contamination. As a result, the risks associated with scenarios 4.2.1 and 4.3.1 have been classified as high.

The remaining failure situations match the ones that were mentioned for node 1 in Tab. 4.5. In fact, cases 4.4.1 and 4.4.2 are related to a potential fault in the pneumatic supply circuit, requiring a maintenance intervention in either the ISOL hall (S018), with a medium risk, or the technical room (S017) with a low risk. Additional minor faults such as electrovalves malfunctioning (4.5.1) or PLC electrical issues (4.6.1), may cause the axis to get stopped, but the corresponding maintenance interventions have been classified as low risk since these procedures take place in areas with negligible radiological risk.

4.5.3.5 *EEPS diagnostic*

The EEPS diagnostic equipment has been studied as a separated HAZOP node, the components of interest are shown in Fig. 4.4. This decision is motivated by the specific effects that could result from a failure condition in this assembly. The missed detection was regarded as the primary deviation. The hardware malfunctioning of electrical components (both placed in atmosphere or in vacuum) and potential mechanical misalignment are included in the failure scenarios that were studied. As reported by the summary in Table 4.9, HAZOP ID 5.1.1 addresses the possible failure of two sensing devices placed in the atmosphere: a linear potentiometer and a resolver. The associated risk has been rated as medium because, while this problem does not prevent the TIS unit from being uncoupled and removed, the

ID	Cause	Consequence
5.1.1	Hardware failure (atm.)	Maintenance intervention (S018)
5.2.1	Hardware failure (vac.)	Maintenance intervention (S018)
5.3.1	Mechanical misalignments	Maintenance intervention (S018)

Table 4.9: Summary of HAZOP ID 5: EEPS diagnostic.

maintenance intervention dedicated to the replacement of the defective component is nonetheless difficult due to the assembly's specific location within the ISOL hall (S018).

Maintenance interventions aimed at replacing critical components installed in vacuum, such as limit switches, following an electrical hardware failure have been categorized as high risk, see 5.2.1. This is motivated by the potential risk of contamination that may arise while accessing the elements along the RIB line. Conversely, possible mechanical misalignment (5.3.1) may be fixed through medium risks interventions since they not require the direct exposure to potentially contaminated parts. The complete HAZOP analysis is available in Appendix A.

4.5.3.6 *TIS unit connections*

Following the evaluation of all the moving elements on the SPES Front-End, the HAZOP analysis identified the connection plate on the coupling table as an extra node. This assembly, which is placed in the RIB direction and is seen in Fig. 4.12, enables the provision of electrical power, water cooling, gas, and signals to the TIS unit. The panel is particularly critical as a potential problem, such as misalignment, stickiness, usury, or aging of the connectors, may hinder the TIS unit from coupling with the RIB channel or, in the worst case scenario, prevent its decoupling after irradiation. The recovery measures planned in response to this second case, which is the most pertinent given the

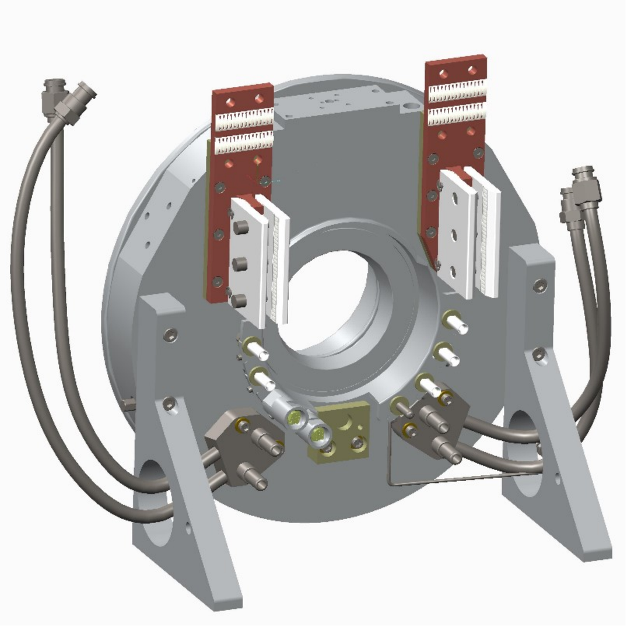


Figure 4.12: 3D view of the SPES Front-End connection plate dedicated to the electrical power, water cooling, gas supply and signal exchange with the TIS unit.

ID	Cause	Consequence
6.1.1	Mechanical problems	Maintenance intervention (S018)
6.1.2	Mechanical problems	Maintenance intervention (S018)

Table 4.10: Summary of HAZOP ID 6: TIS unit connections.

high dose contribution provided by the hot TIS unit, are outlined in Tab. 4.10. A mechanical issue with the connection plate, preventing the TIS unit from being decoupled, hence is the deviation that has been examined. The complete HAZOP analysis is available in Appendix A.

According to the investigation, a maintenance intervention must be performed to fix a mechanical issue that prevents the TIS unit from detaching. The first scenario (6.1.1) focuses on inspection and maintenance tasks with the goal of determining the exact cause of the problem and addressing the situation to restore the possibility of remote removal of the irradiated TIS unit. Inevitably, the event must be considered high risk due to its proximity to the source. In the second instance, the study also discusses the maintenance activities that must be done following the removal of the TIS unit in order to resolve the connection issue. Although Scenario 6.2.1 is less concerning, it is still rated as medium risk.

4.5.3.7 *HHM compensation module*

The final section of the HAZOP study focuses on failure scenarios that might arise during remote handling tasks that involve the HHM. The study focused primarily on the HHM gripping module as the most important assembly interacting with the TIS unit during transportation; the system is represented in Fig. 4.13. Table 4.11 lists the cause-consequence pairs addressed for the HHM compensation module. The examined deviation in this instance is a lack of stability or difficult positioning of the TIS unit due to a problem with this critical assembly. Scenario 7.1.1 examines a potential electrical/mechanical hardware failure of a HHM compensation module component, such as limit switches or signal feedthrough, as the primary cause of the deviation. Case 7.2.1, on the other hand, attributes the malfunction to potential mechanical misalignment. In both situations, the selected recovery strategy calls for a maintenance intervention to be carried out on the HHM at its parking position (S016). Because of the limited

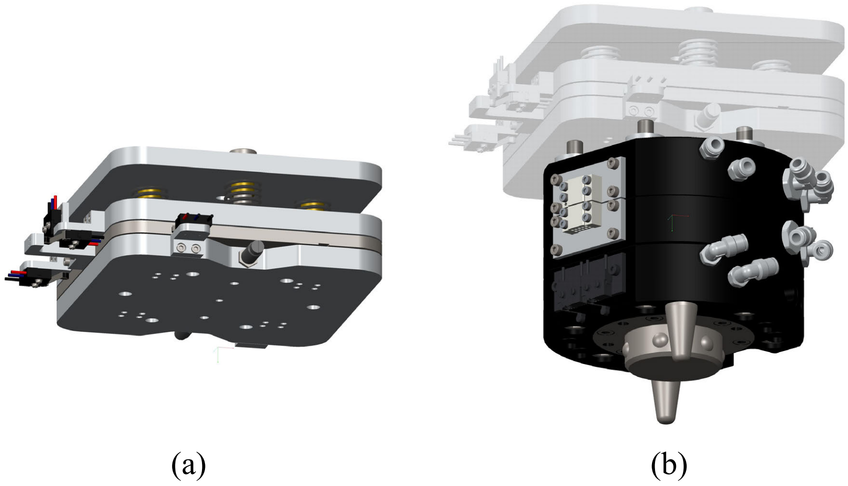
ID	Cause	Consequence
7.1.1	Hardware failure	Maintenance intervention (S016)
7.2.1	Mechanical misalignments	Maintenance intervention (S016)

Table 4.11: Summary of HAZOP ID 7: HHM compensation module.

radiological impact of the intervention within this specific location, the risk associated with this activity is low.

4.5.3.8 *HHM gripper*

The HAZOP analysis takes into account potential failure scenarios associated with the HHM gripper, which is displayed in Fig. 4.13, evaluating multiple deviations. The recommended recovery plan for the vast majority of them is represented by a maintenance intervention within the HHM parking position. This is located in a sheltered area and poses a minimal radiological concern, resulting in a low-risk classification. The full study is accessible in Appendix A, whereas Tab. 4.12 presents a condensed list of the potential causes that could result in the TIS unit release during the transport from Front-End to TSS as the most critical deviation. In more detail, this failure scenario can be caused by a variety of factors, ranging from an erroneous command to mechanical or electrical issues. In any case, the loss of an irradiated TIS unit during transport is an extremely unfavorable scenario due to the potential repercussions and the challenging recovery procedures. As previously mentioned, if a TIS unit drops from the HHM gripper, a number of issues could arise. First, the TIS unit might experience damage and ultimately distribute contaminants throughout the surroundings. Second, as it falls, other parts of equipment like the HHM or the Front-End may be damaged (or contaminated). However, the most crucial aspect is the recovery process because the lost TIS unit's physical position and orientation are unknown and most likely incompatible with conventional remote handling systems. For this reason, the planning of an automated recovery intervention must include specific robotic solutions which are typically employed in



(a)

(b)

Figure 4.13: 3D view of the compensation module (a) and the pneumatic gripper (b) installed on the HHM for the TIS unit manipulation.

ID	Cause	Consequence
11.1.1	Mechanical hardware failure	Remote inspection and recovery
11.2.1	Pneumatic supply failure	Remote inspection and recovery
11.3.1	Wrong command	Remote inspection and recovery
11.4.1	Electrical failure	Remote inspection and recovery
11.5.1	Generic failure	Manual inspection and recovery

Table 4.12: Summary of HAZOP ID 11: HHM gripper.

inspection tasks in unexpected environmental conditions in order to perform a preliminary visual and radiological survey. In a subsequent phase, they can be exploited to manipulate the TIS unit so that it can be relocated in an orientation that is compatible with the facility's standard remote handling machines. Despite the overall challenges of such a robotic recovery procedure, the associated risk can be rated as low if the procedure does not entail any personnel exposure. The choice is motivated by the assumption that in such an unexplored environment, the exposure and contamination risks can be so relevant that any human activity is essentially unfeasible.

Despite the above considerations, the HAZOP analysis also assessed a possible recovery scenario (11.5.1) in which an operator may physically inspect the area and manually recover the TIS unit. It is evident that the event might take place only with the preventive authorization of the RP officers, meaning that the anticipated worker exposure falls within the permitted range. Still, the risk raised by this intervention has been graded as high due to the complexity of the task and potential contamination hazards.

4.6 LAYER OF PROTECTION ANALYSIS (LOPA)

4.6.1 *Introduction*

Deviations identified through the HAZOP analysis in Section 4.5 are further investigated in the second stage of the PRA using LOPA [239, 240]. This method can be used to assess the capacity of IPLs in minimizing or avoiding dangerous outcomes that may arise from process anomalies. The distinctive characteristic of these safety measures relies on their ability to prevent failure event from developing into an actual hazardous condition while remaining unaffected by the impact of the IE or other IPLs [241].

4.6.2 *Material and Methods*

From the LOPA perspective, the HAZOP deviations result in harmful outcomes only when coupled with concurrent factors, also known as Enabling Conditions (ECs), which are separate from the IEs [242]. In the presented study, the focus is restricted to potentially hazardous scenarios. As a result, having the facility configured in maintenance mode has been identified as an enabling condition.

4.6.2.1 *Enabling Conditions*

The scope of the LOPA analysis was initially determined considering the scenarios assessed in the HAZOP study. The evaluation was subsequently restricted to those linked to unacceptable risks (which correspond to red regions in the SPES Risk Matrix, see Tab. 4.3), or, in a broader sense, those requiring a human intervention. Since the selected subset implies the ability to physically access the emote handling area, an Enabling Condition (EC) related to the possibility of having the SPES facility configured in maintenance mode has been integrated in the LOPA analysis. According to the SPES operational schedule, its frequency has been set to 0.25, as shown in Tab. 4.13. This assumption is based on the likelihood that one of the IPLs, the Access Control System (ACS) may fail. This is considerably larger while in "access" mode, since only one badge reader is required for this safety measure to be effective.

Enabling Conditions (EC)	PFD
Facility under maintenance	0.25

Table 4.13: Enabling Conditions (EC).

4.6.2.2 *Conditional Modifiers*

Conditional Modifier (CM) are used to introduce conditions other than IPLs which may have an effect in the reduction of the mitigated frequency for a specific event. As reported in Tab. 4.14, three conditions have been considered: first, since the operator's presence has been considered in every scenario, the corresponding frequency is always 1. Second, as previously mentioned, the necessity for personnel access under severe radioactive conditions can be reduced through the use of backup actuation systems to address different types of motion chain malfunctions. Indeed, a backup motion interface is available for each motion axis of the SPES Front-End, as outlined in Section 4.2. With the assistance of an external motor mounted on purpose on the HHM, this feature enables the conclusion of the TIS unit detachment and removal sequence in case of fault of the related pneumatic motor. For this CM, the related Probability of Failure on Demand (PFD) has been set to 0.1. The MPS override is the final strategy under consideration that could reduce the necessity for a high-risk maintenance intervention. Following meticulous evaluation, it was discovered that this possibility might actually allow the system to force the motion completion even when not all the required signals are present, thus overcoming specific error conditions. With the help of this method, which require a careful evaluation by remote handling specialists, the TIS unit separation procedure can be accomplished without the need for human interaction. This will make it possible to carry out the following maintenance tasks with a reduced ambient dose rate. In the LOPA analysis, the value 0.1 has been assigned to the correspondent PFD as well.

Conditional Modifiers	PFD
Operator Presence	1
Backup actuation systems	0.1
MPS override	0.1

Table 4.14: Conditional Modifiers (CM).

4.6.2.3 *Independent Protection Layers*

Starting from the safeguards identified in the HAZOP analysis, listed in Tab. 4.4, LOPA seeks to assess the performance of those who operate independently of the others. To achieve the propagation of the failure condition from the IE to the actual consequence, all of these safety measures must fail at the same time. The definition and validation of the Independent Protection Layers (IPLs) is one of the most significant goals and achievements of LOPA. On the one hand, the assessment

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

Table 4.15: Independent Protection Layers (IPLs).

allows for the verification of whether the suggested safeguards are adequate to meet the intended target frequencies. On the other hand, it highlights which measures must be compulsory implemented, assisting the designer in the prioritization of the compulsory actions aimed at the facility's commissioning. Among the identified safeguards, IPLs shall meet the following characteristics:

- be effective in the prevention of potential harmful consequences;
- be independent of the IE and with the other IPLs identified for the same scenario;
- be measurable: their effectiveness shall be validated using specific methodologies (e. g. review, testing, documentation, etc.)

The IPL qualification of a safeguard, implies its effectiveness in avoiding the consequence originated by the IE. Different considerations may help the analyst, or the team, in the evaluation process. As an example, a first question can relate the safeguard ability to identify the situation that calls for it to take action. This could be an alarm, a process variable, etc. A safety measure is not an IPL if it cannot always identify the condition and trigger a certain action. An additional question can be if the safety measure identify the issue in time to take the necessary remedial action to avert the undesirable outcome. The required amount of time must account for the time it takes to detect the problem, gather information, evaluate the options, make a decision and wait for the action to take effect. The introduced considerations are summarized in the IEC 61511-3 [242], which states that each IPL must be independent, unique, and physically isolated from other IPLs. Additionally, they shall not share common points of failure, be highly available and be auditable in order to be verified. The list of IPLs that have been selected for the SPES facility is included in Tab. 4.15.

Control systems and MPS are two components of the first layer. These tools typically include dedicated software interlocks and automatic testing procedures that may prevent risk scenarios resulting from hardware failures under ordinary operating conditions. The two systems are physically independent of any other IPL and their reaction to system changes is driven by measurable process properties or physical signals. The PFD of the first IPL is set to 0.1, the impact of this layer is in the reduction of the likelihood of the IE.

The second IPL encompasses all the steps that can be taken to optimize maintenance interventions, such as training of specialized operators, selection of the most appropriate Personal Protective Equipments (PPEs), and implementation of detailed operational procedures. These measures will have a significant impact on both the intervention time and the risk of errors or, in the worst-case scenario, injury. Because of its significance and effectiveness in reducing the severity of the recovery scenario, the PFD has been estimated at 0.01.

Activities that could prevent hardware failure from happening and extend the lifespan of critical components are included in the third IPL. As reported in Tab. 4.15 they are described as: periodic maintenance, inspection, and replacement program. With a global PFD of 0.1, those actions have an effect in decreasing the IE likelihood. This IPL is auditable and independent of the IE event and the components of any other IPLs identified for the same failure condition.

The radiation monitoring infrastructure, the personal dosimeters, and the ACS are all part of the fourth set of measures. These safeguards are used to protect the operator from being exposed to high dose rates, thus decreasing the severity of the recovery actions. In defining the PFD level, we assumed that the SPES facility might primarily be configured in an operational or maintenance state. While in the first case the SPES (SIL 2) ACS will make entrance to the zone nearly impossible in presence of elevated gamma dose rates, in the second operating mode the effectiveness of this protection layer is committed to a badge reader, which allows authorized operators access to the zone. The related PFD in this instance is 0.1.

As last IPL, the benefits of employing the HHM for remote inspections have been considered. This opportunity is highly beneficial for reducing personnel exposure and optimizing maintenance activities. The IPL appears to be independent of the other IPLs and its operation and effectiveness may be confirmed. In conclusion, from the LOPA perspective, it enables a reduction in the severity of the effects that result from the IE, the PFD in this case is 0.1.

4.6.2.4 *Flowchart*

The LOPA analysis determines if the available IPLs are adequate to satisfy the desired target frequency for each failure conditions. The process starts with the identification of risk scenarios. In this study, the considered failure conditions are the one related to intermediate and unacceptable risk requiring a personnel access in high-radioactive areas, see the SPES risk matrix in Tab. 4.3. The mitigated target frequency in this situation has been set to $1.00E - 6$. The analysis is then carried on by selecting the frequency of occurrence for the specific IE, which is then multiplied by the PFDs of the applicable EC, CMs, and IPLs. The mitigated frequency is finally compared with the desired target frequency. Two mitigated frequencies have been taken into account in the study. The first one considers all relevant IPLs, while the second one only takes into account those that are currently implemented. The LOPA flowchart has been reported in Fig. 4.14.

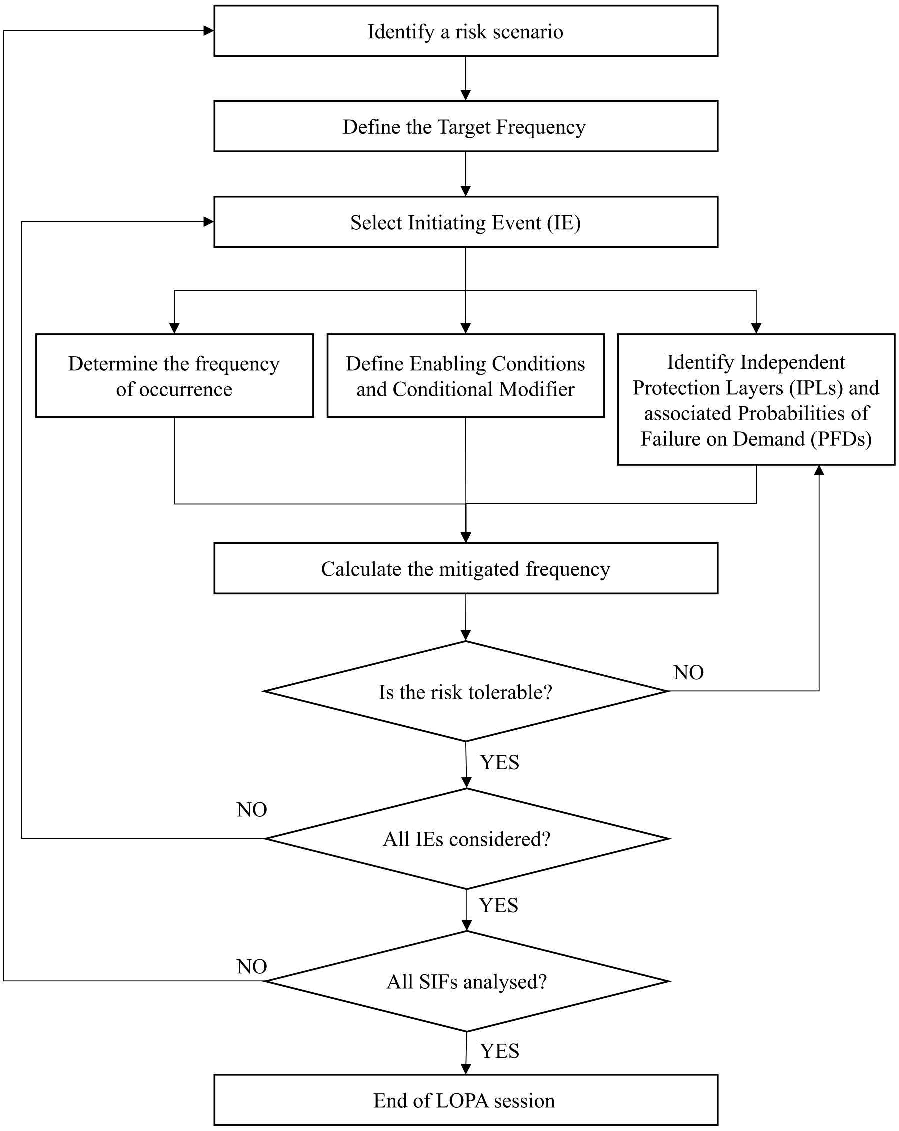

Identify a risk scenario
Define the Target Frequency
Select Initiating Event (IE)
Determine the frequency of occurrence
Define Enabling Conditions and Conditional Modifier
Identify Independent Protection Layers (IPLs) and associated Probabilities of Failure on Demand (PFDs)
Calculate the mitigated frequency
Is the risk tolerable?
NO
YES
NO
All IEs considered?
YES
NO
All SIFs analysed?
YES
End of LOPA session

Figure 4.14: The LOPA flowchart.

4.6.3 *Results*

In this study, LOPA was focused on HAZOP scenarios involving human action, identified with medium to high risk, with a focus on those leading to major consequences. An example of the LOPA focused on the RIB channel is displayed in Table 4.16. A star (*) appears next to the PFD of IPLs that are still being completed. Taking into consideration all IEs for each node, the cumulative mitigated frequency is computed.

Node: PPB and RIB channels													
Deviation: 1. Motion blocked													
		Inital frequency [yr^{-1}]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr^{-1}]	Mitigated frequency with partial IPLs implemented [yr^{-1}]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
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

Table 4.16: LOPA worksheet for the RIB channel node.

The complete analysis is available in Appendix B, while Tab. 4.17 summarizes the most important findings. The third column reports the Frequency Base Target for the analyzed failure scenarios. Since in this assessment has been focused only on the high-risk events emerged from the HAZOP analysis, the corresponding frequency has been set at $1.00E-6$. The last two columns report the mitigated frequency. While the left one takes into account all the applicable IPLs, the right column computes only the ones already implemented and currently available. If the target frequency for a particular LOPA ID is met, the mitigated frequency is indicated in green. Alternatively, if the target value is not achieved due to incomplete IPLs, the mitigated frequency is marked in red. A star (*) appears when merely the order of magnitude is satisfied and additional optimization must be performed to ensure the necessary safety level.

			Mitigated Frequency	
LOPA ID	Hazard scenario	Frequency Base Target	Final frequency with all IPLs implemented	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: EEPS. Operator intervention required. Direct exposure to high levels of radiation.	$1.00e-6$	$2.88e-6^*$	$6.25e-3$
5	Diagnostic fault: EEPS. 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.	$1.00e-6$	$1.25e-6^*$	$1.25e-2$

Table 4.17: LOPA results.

LOPA ID 1, considering as IE the lack of motion of the PPB or RIB axes, assess the possibility of a human maintenance intervention within the ISOL hall. In this case, as already discussed in Section 4.5, the opportunity to take advantage of backup actuation interfaces allows for a remote or semi-automatic recovery procedure. When, for different reasons, this strategy is not viable a traditional maintenance intervention is required. At this point, the conventional IPLs mitigate the frequency of occurrence of a severe personnel exposure essentially preventing any personnel access in high environmental dose rate areas. The mitigated frequency, when all IPLs will be operational, is adequate to meet the target frequency, while at the moment this is not the case.

In LOPA ID 2 have been assessed the failure scenarios deriving from a lack of motion in the PPB or RIB gate valves. As in the previous case, the additional motion flanges are beneficial in the reduction of the need for a human intervention, since they enable alternative recovery procedures that present a minimal radiological impact. Nevertheless, when such strategies cannot be pursued, a traditional intervention is required. Even in this case, the applicable CMs and IPLs contribute in satisfying the target frequency for this scenario. Unfortunately, at the moment the available IPLs are not enough.

Analogous consideration can be applied to LOPA ID 3, where recovery interventions in response to faults to the PPB or RIB motion axes diagnostics are evaluated. The possibility to bypass some MPS conditions and the other applicable CMs and IPLs make the mitigated frequency of occurrence of this specific scenario below the target value. As in the previous cases, the currently implemented protection layers are not sufficient to ensure the desired safety level.

In LOPA ID 4 are evaluated the potential effects of failures in the motion chain devoted to the positioning of the Front-End extraction electrode. As reported in Tab. 4.17, the mitigated frequency of this scenario does not satisfy the target frequency. Despite the order of magnitude is reached, the lack of a backup motion flange has a significant effect in the prevention of maintenance activities with a potential high exposure. The missing CM has an impact in the final mitigated frequency, since each hardware failure will require a personnel access in the ISOL hall.

LOPA ID 5, similarly to the previous scenario, focuses on the impact of hardware breakdown of the EEPS diagnostic components on the subsequent recovery actions. Also in this case, the lack of backup motion interfaces and the difficulty to perform remote inspections in such inaccessible location result in a mitigated frequency higher than the target one for this specific event. Possible improvements of the system aimed at complying with the desired safety level of the facility include the application of an additional CM such as the introduction of a backup actuation flange.

Maintenance interventions following a mechanical problem with the TIS unit connections on the coupling table are assessed by LOPA ID 6. In this case, even if a personnel access is always required, the possibility to perform remote periodic inspections on the Front-End, together with offline coupling tests will reduce the frequency of the event till a level within the desired limits.

LOPA ID 7 analyzes the consequences of a TIS unit drop along the HHM route within the SPES target area. Among the potential recovery strategies listed in the HAZOP study, the analysis focuses on manual interventions aimed at relocating the unit in a position compatible with its remote manipulation. In the analyzed scenario the lack of a dedicated inspection tool such as a multipurpose robot, used for the prior estimation of the personnel exposure and for the accurate planning of the intervention, results in a higher mitigated frequency, which does not meet the target value, except for its order of magnitude.

4.6.4 *Discussion*

The potential effects of failure scenarios to recovery actions are assessed in Section 4.5 for the various nodes, while Section 4.6 examines the impact of the suggested safeguards on risk reduction. This section provides an overview and discussion of the most important study's findings. Section 4.6 have presented the LOPA results applied to the most critical recovery scenarios highlighted by the HAZOP analysis. For those events, linked to an unacceptable risk in the SPES risk matrix, (see Tab. 4.3), a desired target frequency of 1.00 E-6 has been selected. From the analysis emerged that both CMs and IPLs play a critical role in maintaining the final frequency of occurrence of a failure scenario within the target limits. The study confirmed that overall, the proposed mitigation strategies are adequate to fulfill with the facility's desired safety level and that the final frequencies satisfy the target frequency for every hazard scenario, at least the order of magnitude. Nevertheless, since target frequencies are not currently satisfied, several actions need to be completed to implement the proposed measures.

The initial observation highlighted by the analysis's findings concerns the usefulness of the proposed conditional factors. Specifically, the main considerations related to the CMs are reported below:

- **Redundancy:** the LOPA confirmed that, among the CMs, backup actuation system allow to reduce the probability of human interventions. For this reason, where not available it is critical to introduce this feature. A significant example is the EEPS, where the expected frequency of maintenance interventions aimed at restoing a failure condition is increased due to the missing opportunity to address the lack of motion through remote strategies. As first remark, the LOPA strongly suggest the design and implementation of a backup actuation system for the EEPS.

- **MPS override:** from the LOPA it is evident that, in specific hardware failure scenarios, bypassing critical MPS conditions will enable to remove the TIS unit under a specific surveillance and thus improving the radiological background of the subsequent maintenance activity's location. Thus, it is suggested to carefully evaluate this option, together with the required procedures and regulations, in order to exploit this feature in case of need.

The LOPA results, presented in Table 4.17, indicate that the proposed IPLs are appropriate to reach the target frequency in the majority of the examined circumstances. Failures involving the EEPS or the HHM gripper constitute the only exceptions. Although the desired frequency order of magnitude is met for such equipment, adding an extra IPL is advised to further lower the risk of personnel exposure coming from maintenance interventions under unfavorable radiological settings. The addition of a backup motion flange or being able to perform remote inspections are two examples. The study's unambiguous conclusion is that, as a result of incomplete IPLs, target frequencies are presently unsatisfied. In particular, the analysis highlighted the current gaps in operating procedures, the need for a robust training program, and a preventative maintenance strategy. A list of the numerous actions that must be accomplished is provided below:

- **Training program:** development of a specific training facility, resembling the online setup in terms of footprint, interferences, and overall dimensions, where operators can train to gain expertise and save time during the actual maintenance activities.

- **Procedures:** drafting of specific procedures providing the step-by-step description of the maintenance task, detailed pictures of the required actions, the layout of the area and the operating position highlighted in the 3D view, the list of the required tools and PPEs, and the instructions on what to do in case of unexpected events or an emergency. An example is the desired behavior in case of fall of a screw or a tool during the intervention: from the RP perspective, it can be preferable to quit the zone and plan another intervention instead of trying to search and catch up the missing item in a radiological environment.

- **Preventive maintenance program:** introduction of periodic inspection, maintenance and replacement actions followed by an independent testing and certification phase. The two phases needs to be performed by two (or more) different operators. The first step aims at verifying the status of the most critical components (the ones with most critical recovery interventions in case of hardware failure) anticipating their replacement during programmed TS or performing maintenance activities aimed at enhancing their lifespan (greasing, cleaning, etc.) During the second phase, an independent inspector will verify the proper execution of the foreseen maintenance activities performing visual inspections, mechanical and functional tests through a standardized checklist.

- **Remote inspections:** upgrade of the HHM to incorporate remote inspection features through a dedicated PTZ camera and specific actuators able to couple with the Front-End backup actuation flanges to overcome the lack of motion of a specific axis in case of hardware failure during operation. These two features enable remote inspections and recovery procedures without any foreseeable personnel exposure to ionizing radiations.
- **Software:** assess the compliance of the control software with the facility's specifications and safety requirements through dedicated tests. Adoption of most reliable standards and best practices with a specific focus on the management of signal coherence, task priorities, information integrity, user permissions, etc. Implementation of data logging, warning and alerts notifications to trace the system behavior prior to a fault condition. Development of automatic test routines to be executed in order to test all the sensors and actuators prior to actual operation.

The analysis evaluated the potential consequences of a hardware malfunction in over 20 crucial components located in the ISOL hall. The HAZOP study, outlined in Section 4.5 performed an in-depth assessment of 38 failure scenarios over 8 nodes, which were chosen to represent key subsystems of SPES Front-End and remote handling systems. The research proposes 13 safety measures, presented in Table 4.4, including both organizational (B, C, E, F, and G) and technical (A, D, H, I, J, K, L, M) solutions. The ensuing LOPA then organizes the available safeguards into five independent families, or IPLs, as shown in Table 4.15. The study, which is detailed in Section 4.6, takes into account 14 IEs related to HAZOP deviations resulting in moderate or unacceptable risks, i.e., those that call workers to access high-exposure areas. On the one hand, the presented research provides significant technological options that could be applied to enhance the safety of the plant. On the other hand, it will lay out a strategy to develop successful organizational measures, such as creating a preventive maintenance program and operational procedures, that are essential for starting facility operations in conformity with the desired requirements.

4.7 CONCLUSIONS

This chapter has described an integrated PRA aimed at improving the design of the SPES facility's essential parts and reducing worker exposure to ionizing radiation as they carry out maintenance duties. To accomplish these objectives, HAZOP-LOPA methods have been combined to examine the worst-case scenarios that might arise while performing remote handling tasks on the SPES Front-End and to determine the most appropriate safety measures. According to the LOPA results, all of the proposed IPLs, with the exception of the EEPS and the HHM gripper, are suitable to reach the desired safety level each risk scenario. Indeed, despite the order of magnitude is satisfied, these two nodes require an extra IPL. Implementing remote inspection techniques preceding maintenance activities could be a feasible solution.

The analysis unequivocally demonstrates how ineffective IPLs in the current facility's development phase prevent target frequencies from being met. The key steps towards the accomplishment of the intended safety objectives have been identified as a result of the evaluation process. Consequently, future steps will be devoted to the implementation of safeguards listed in Table 4.4 throughout the facility. Among the described facility's weaknesses and criticalities it is possible to highlight three main aspects which, up to now, have not been assessed. Those items are analyzed in detail as next research steps, they are:

- Design of EEPS backup systems;
- Development and optimization of maintenance activities;
- Safety improvement of the control software.

4.7.1 *Design for maintenance*

While IPLs represent key assets to achieve target frequencies, the relevance of CM in lowering the probability associated with specific recovery scenarios was also underlined by LOPA. According to the study's outcomes, where backup motion interfaces are not available, additional improvements will have to be incorporated into the system to facilitate remote disengagement of the TIS unit in the event that the primary actuators fail, preventing the need for staff access.

"Design for maintenance" encompasses all activities targeted at improving the design of systems or parts installed in critical locations with the goal to ease the maintenance process by improving the accessibility, ergonomics and ease of maintenance. In this work this approach has been applied to critical components installed on the SPES Front-End and, as suggested by the PRA outcomes, has been applied in the review of the design of the EEPS described in Chapter 5.

4.7.2 *Maintenance assessment*

The arbitrary, but plausible prediction of severity represents a shortcoming of this investigation. Indeed, the absence of information describing the operator's exact working position and the time required for the execution of the maintenance interventions is the cause of this uncertainty. It is important to emphasize that, programmed maintenance activities, extraordinary interventions poses several concerns in terms of radioprotection. Indeed, while the first ones are usually scheduled during the facility's TS, the second ones may occur in an unexpected moment, usually during operation.

Hence, a detailed maintenance assessment, described in Section 6, has been developed as next research step to address the described bottleneck. The study's objective is the collection of accurate experimental data on the intervention durations for selected maintenance interventions reflecting established protocols. On one hand, given the intrinsic hazard of the zone an overall optimization of maintenance interventions is always beneficial. On the other hand, the possibility to estimate the personnel exposure for a specific activity represent an extremely useful tool to assess the feasibility of the intervention during standard operation. Additionally, by integrating the simulated ambient dose rate at the working position, it will be possible to base the severity level estimation on accurate personnel exposure models, thus fine-tuning the PRA. As last step, the study's outcomes will be beneficial for the completion of partially implemented IPLs, such as:

- development of a training program;
- definition of standardized operating procedures, featuring cockpit style checklists;
- establishment of a preventive maintenance program, with periodic inspections and independent testing/certification.

4.7.3 *Formal software verification*

Software safety in critical contexts results as important as hardware safety. The wrong handling of unforeseen conditions may result in unexpected behavior and potentially dangerous failure scenarios. Chapter 7 describes the implementation of a specific workflow that allow, through an integrated tool-chain to take advantage of most recent standards for PLC programming in order to assess the safety of the control software prior to its deployment.

In addition to the described improvements, the following steps should be addressed to guarantee the success of the identified IPLs:

- installation of a reliable radiation dose monitoring system;
- integration of dedicated actuators on the HHM to enable the remote actuation of Front-End motion axes;
- study of the potential bypass of MPS interlocks under specific circumstances.

5 PRELIMINARY UPGRADE OF THE EXTRACTION ELECTRODE POSITIONING SYSTEM GUIDED BY "DESIGN FOR MAINTENANCE" PRINCIPLES

5.1 INTRODUCTION

Among the available techniques for reducing the severity of maintenance activities in highly radioactive areas, the optimization of the design of safety-critical systems represents an effective approach, just as much as safeguards and IPLs are.

In this chapter, a preliminary study aimed at the hardware upgrade of crucial components is presented. The feasibility analysis is applied to the Extraction Electrode Positioning System (EEPS) with the goal of addressing the criticalities reported by the PRA in Section 4. As highlighted by the LOPA, in this node the target frequency of the assessed failure scenarios is not reached due to a missing CM or IPL. The following sections describe three distinct design reviews intended to correct the system vulnerabilities and improve its overall architecture. On top of the weaknesses of the EEPS, the extraction electrode itself represent an extremely sensitive component. Its role during operation is to extract and accelerate the radioactive ions coming from the TIS unit along the RIB line. The operational feedbacks provided by different RIB facilities have shown how the challenging operating conditions make this component constantly exposed to significant thermal stresses, potential high-voltage electric discharges and surface contamination issues. Figure 5.1 depicts the described effects on real extraction electrodes after one or more years of operation.

The significant dose contribution provided by the extraction electrode contamination [227] requires its removal prior to any scheduled

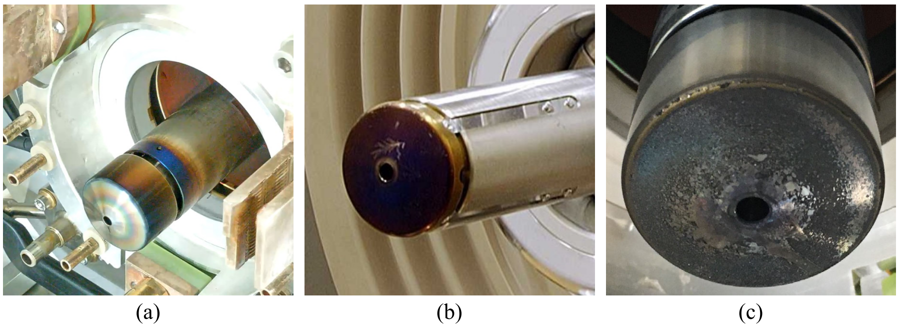

(a) (b) (c)

Figure 5.1: Real world effects on the extraction electrode: (a) thermal stresses, (b) high-voltage electrical discharges, (c) surface contamination. Courtesy of CERN.

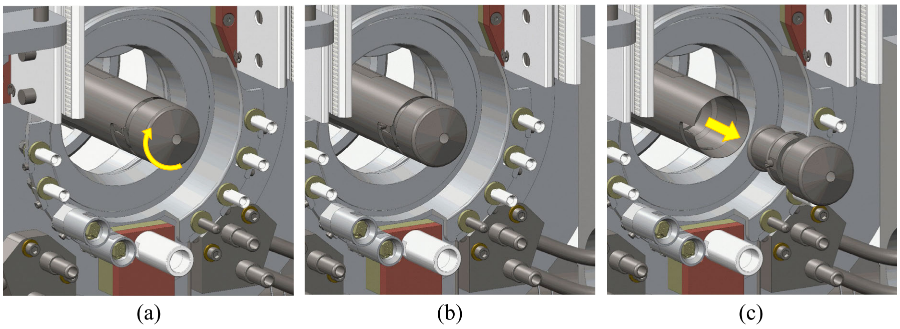


Figure 5.2: SPES extraction electrode disconnection procedure: (a) clockwise rotation, (b) pin aligned, (c) pull out of the electrode.

maintenance activities within the ISOL hall during Technical Stops (TSs). This specific maintenance task can be performed through specific manual tools or with RH equipment. The electrode disconnection procedure is depicted in Fig. 5.2. The EEPS thus constitutes an extremely compelling case study to demonstrate the benefits of design optimization on the potential personnel exposure during maintenance and recovery interventions.

5.2 OBJECTIVES AND METHODOLOGY

The identification of hazards of RH systems in the early design stage constitutes a valuable asset in the reduction of operational and maintenance risk for personnel [243]. The goal of this study is to provide a clear demonstration of how "maintenance-oriented" design upgrades of safety critical systems triggered by early safety assessment [244, 245] can represent a valid strategy for the reduction of personnel exposure, in accordance with ALARA principles [246].

In this chapter, the design upgrade of the EEPS is carried out with two main goals in mind: first, to reduce the necessity for personnel access by incorporating remote actuation features, and second, to optimize the residual hands-on interventions applying "design for maintenance" principles aiming at reducing the duration of the interventions and the possibility of human error.

Generally speaking, the experience gained in different nuclear applications promoted the development of specific guidelines to support the design of equipment installed in dangerous location subject to remote maintenance. These include, as an example, the implementation of robot-friendly features, such as the adoption of standardized gripping interfaces and universal connectors to help teleoperated upkeep activities, given the limited capabilities of robots [37]. Along with the aforementioned strategies, which are taken into account for the design of remote recovery features, the study aims at improving the design of the equipment to optimize the manual maintenance activities performed by operators. In this context, the research takes advantage of specific maintainability guidelines that have been successfully applied to the redesign of other critical components installed at SPES, such as the linear potentiometer used in the Front-End motion axes [247].

Figure 5.3 depicts some key principles that may support the engineering of equipment installed in high-risk locations. Specifically, a "maintenance-oriented" design requires few and simple actions for the replacement of critical components. This goal is achieved by introducing tool-free connection mechanisms that can be operated with one hand and does not require the manipulation of small components. From the ergonomics point of view, heavy components or elements installed in complex settings should be installed with the help of trolleys and lifting devices, while in case of reduced visibility the use of portable lights would help the operator throughout the task execution. Additional factors that should be considered in the design of new components are related to the use of moving parts. Considering fastening clamps as an example, even if they provide an interesting alternative to traditional locking methods, special attention should be posed on the potential effect of vibrations (sometimes induced by the beam) on loosing these components. Furthermore, from the RP standpoint, a trade-off shall be found between the reduction of intervention duration and the increase of mass (that might get activated) introduced by new system's design.

The following section presents the preliminary redesign of the Front-End EEPS based on the described maintainability guidelines.

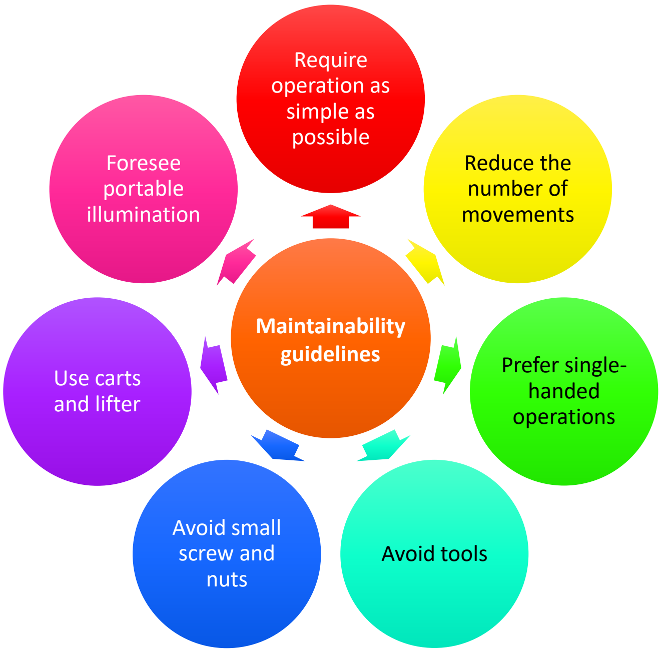

Maintainability guidelines
Require operation as simple as possible
Reduce the number of movements
Prefer single-handed operations
Avoid tools
Avoid small screw and nuts
Use carts and lifter
Foresee portable illumination

Figure 5.3: Maintainability guidelines.

5.3 EXTRACTION ELECTRODE POSITIONING SYSTEM REDESIGN

The PRA presented in Section 4 highlighted the advantages of backup actuation strategies as effective CMs that can reduce the likelihood of high-exposure risk maintenance interventions. Among the Front-End motion systems used during RH tasks within the ISOL hall, the study identified the Extraction Electrode Positioning System (EEPS) as the most critical one. Indeed, the LOPA revealed that the available CMs and IPLs are not enough to reach the target frequency in the analyzed recovery scenarios. Specifically, the main weakness of the assembly, depicted in Fig. 5.4, is the missing backup actuation flange, which leads to the need for hands-on maintenance activities following each failure event. The overall list of the identified vulnerabilities is reported below.

1. Position: difficult to reach, operator shall cross the PPB line
2. Components in atmosphere (motor, gearbox): locking clamps, 2-6 screws
3. Components in vacuum: standard CF flange, 16+ screws
4. Maximum breakaway torque of magnetic rotary feedthrough: 4 Nm
5. Backup motion flange: not available

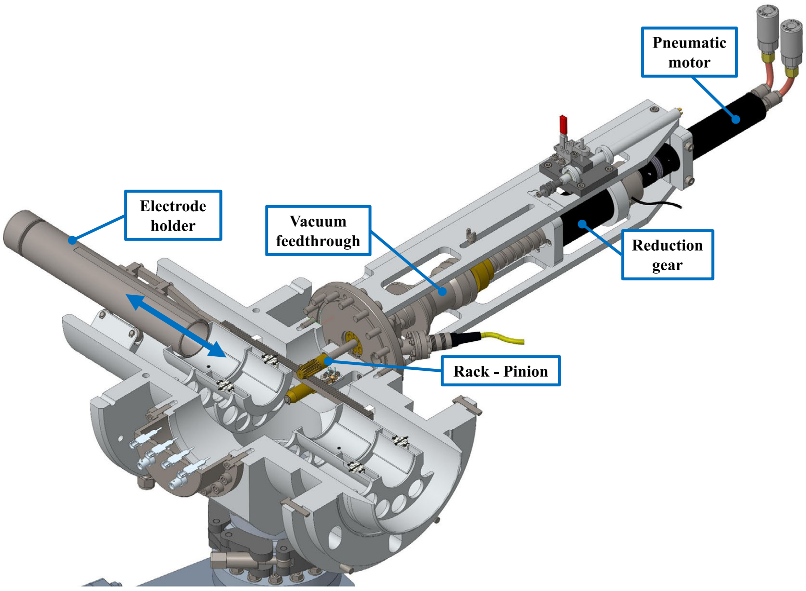
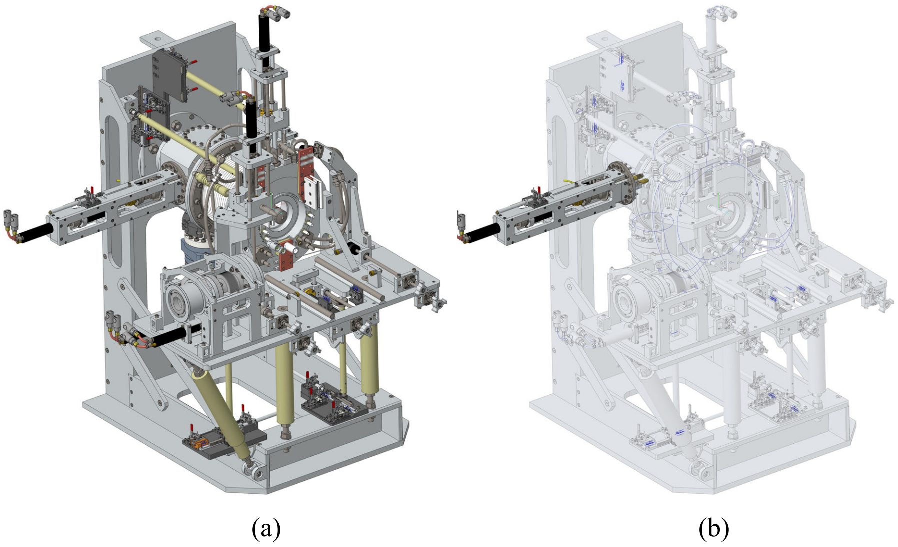


Figure 5.4: Section view of the SPES Front-End showing the old design of the EEPS.



(a)

(b)

Figure 5.5: (a) Global view of the SPES Front-End, (b) Focus on the EEPS *rev. 1.0*.

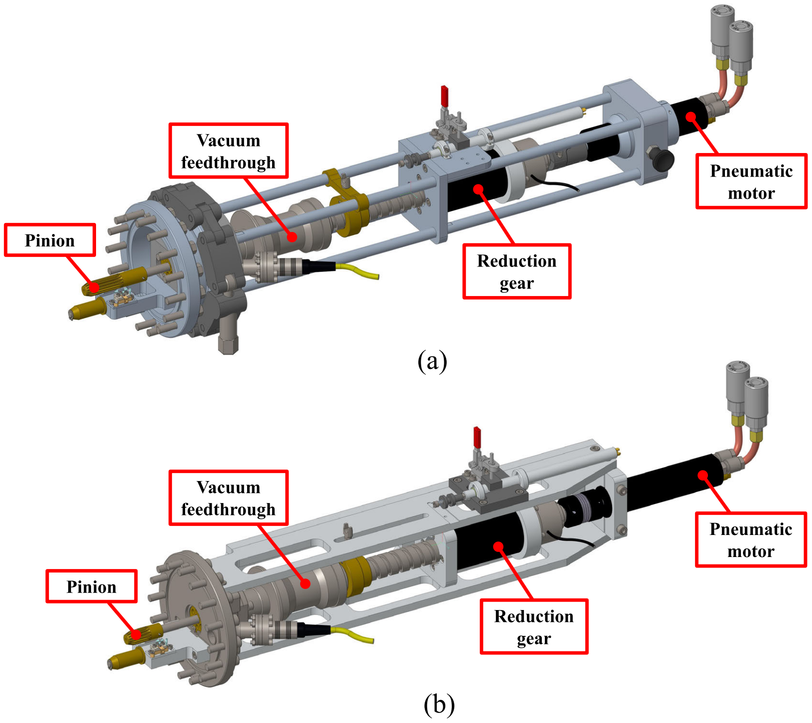
The motion assembly is divided in two main subsystems: the driving section is operating in atmosphere, while driven elements are installed in vacuum along the RIB line. The first subsystem features a radiation-tolerant pneumatic motor as main actuator, a reduction gearbox ($i = 60$) and a magnetic rotary feedthrough used to transfer the motion to the extraction electrode holder by a rack-pinion coupling. A resolver and a linear potentiometer provide accurate position feedback before and after the gearbox, respectively. A pair of limit switches are installed in vacuum to detect the end of the electrode holder's stroke. The driven subsystem includes the sliding electrode holder, which is supported by dedicated bearings and connected to a linear rack. Figure 5.5 depicts the existing EEPS installed on the SPES Front-End. The following sections describe the redesign process of the EEPS aimed at addressing the vulnerabilities identified by the LOPA.

5.3.1 *EEPS design revision 2.0*

The list of EEPS weaknesses discussed in the previous section remarks the impact of non-optimized fastening methods on the duration of maintenance activities, see points no. 2 and 3. According to the maintainability guidelines discussed in Section 5.1, the use of tool-free fastening strategies allows to optimize the maintenance process by decreasing the likelihood of potential errors and the time required for the task execution. In the SPES case the preferred maintenance strategy is, whenever possible, to quickly replace faulty components. Another option is to remove the whole motion assembly to repair or replace critical elements in a safe area. In the current configuration, the pneumatic motor is kept in position by a clamp tightened with 2 screws, while the entire EEPS is fastened to the main RIB line by 16 screws.

The EEPS has undergone a comprehensive redesign process, aiming at the improvement of the described system vulnerabilities. In particular, EEPS revision 2.0 aims at reducing the time required for the replacement of critical components, such as the pneumatic motor and the in-vacuum limit switches. The redesigned EEPS features the same commercial components of the previous version, while upgrading the mechanical structure used for their installation. Figure 5.6 compares the existing EEPS (a) with the redesigned system (b).

The main criticality is represented by the CF flange used to connect the EEPS with the Front-End RIB line. As visible in Fig. 5.4, accessing in-vacuum components requires the removal of 16 screws, and this task can take a significant amount of time. For this reason, in the new design, the Front-End has been equipped with a conical transition stage, where the EEPS can be connected using quick chain clamp. The final stage of the old EEPS replacement procedure requires two people: one holding the assembly and one to remove the last screws. The redesigned system still need an additional operator to maintain the EEPS while the second one looses the two tensioning knobs. However, the removal of the new EEPS can take just few seconds and does not require any tool. The experimental tests of the EEPS removal are



(a)

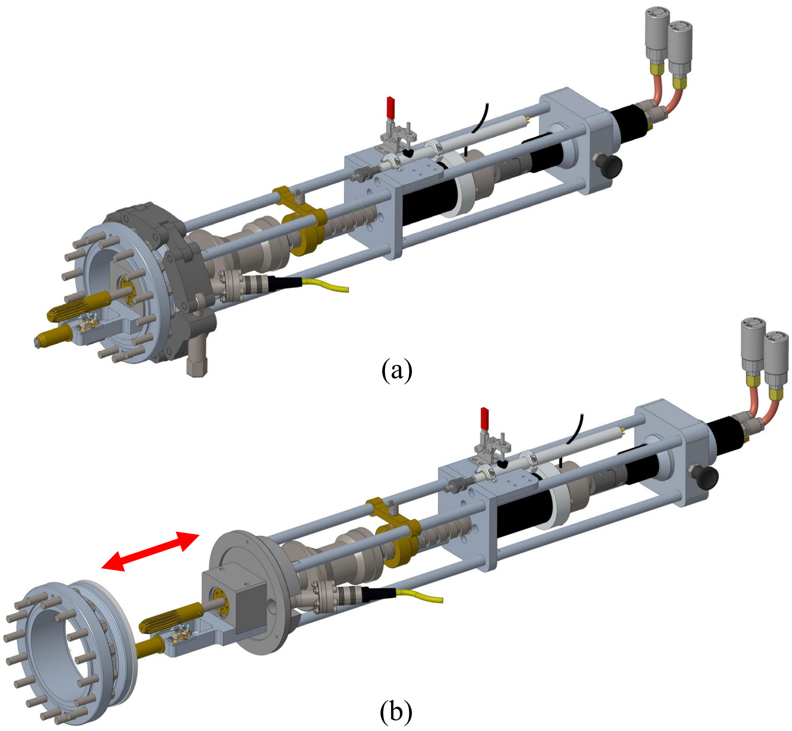
(b)

Figure 5.6: Comparison between (a) the EEPS *rev 2.0* and (b) the original EEPS.

discussed in Section 6.4.2. A potential improvement of the proposed design could be the development of a supporting structure to keep the EEPS in place while the operator tightens the clamp chain. This solution could enable the execution of the replacement task by a single operator, reducing the collective dose. A detailed view of the disconnection procedure implemented in the EEPS *rev. 2.0* is visible in Fig. 5.7.

The second upgrade implemented in the redesigned EEPS is related to the pneumatic motor fastening method. The conventional technique used throughout the Front-End motion axes makes use of an aluminum clamp tightened on the motor body by two screws. Conversely, in the EEPS *rev. 2.0* the motor is enveloped on a self centering shell. The unit is then inserted within a conical flange and held in place through an indexing plunger. Basically, thanks to this system, the release of the motor during critical maintenance interventions does not require any tool, but just the pulling of the pin handle. On the other hand, the installation of a new motor can be even easier, since the unit is self-locking. Figure 5.8 depicts the redesigned motor housing.

The mass of the EEPS *rev. 2.0* is approximately 13.4 kg, whereas the existing assembly weights 12.9 kg. Taking the transition and the chain clamp into account, the new EEPS adds 2.5 kg to the original configuration. Since more material can be activated during operation, this can be seen as a limitation of the proposed design. However, the advantages


(a)

(b)

Figure 5.7: Quick connection flange of the new EEPS. (a) EEPS coupled with the RIB line, (b) EEPS disconnected.

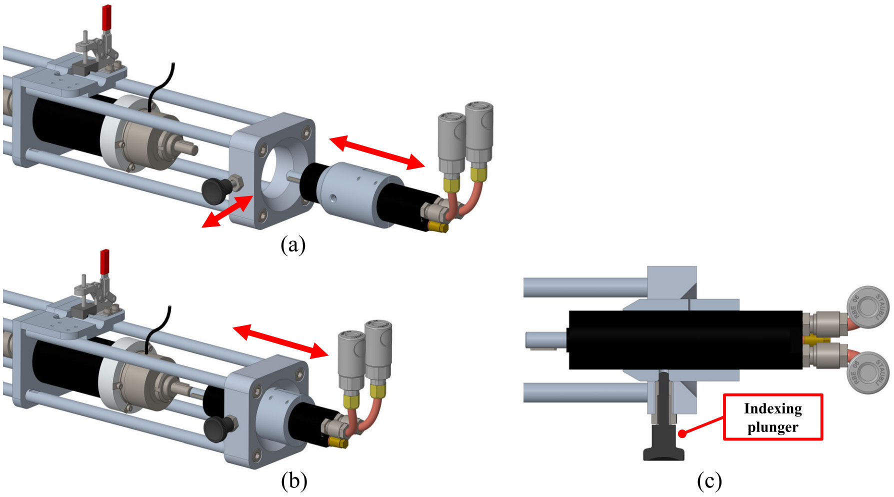


Figure 5.8: Quick release housing of the EEPS pneumatic motor. (a) motor coupled, (b) motor disconnected, (c) indexing plunger.

provided by the introduction of the rapid disconnection flange during maintenance activities justify the redesign process. Indeed, despite a slightly higher environmental dose rate, the replacement time is dramatically reduced, resulting in an overall reduction of personnel exposure. The 0.5 kg increment in the detachable EEPS section, does not influence the maintenance outcome. A global view of the SPES Front-End equipped with the new EEPS is shown in Fig. 5.9.

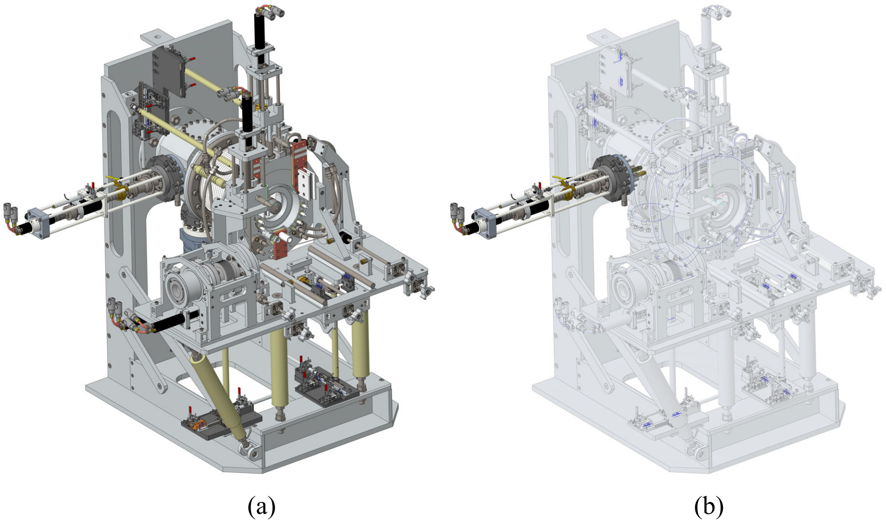


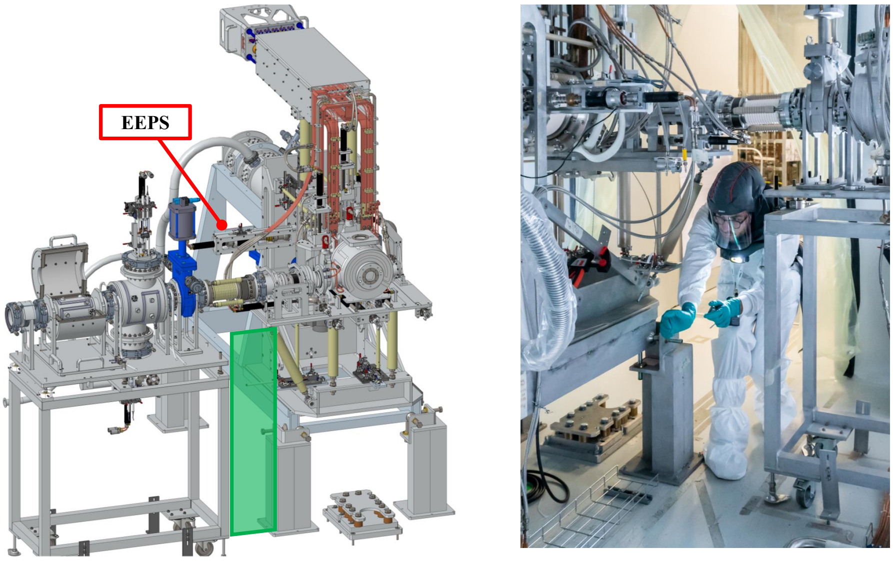
Figure 5.9: (a) Global view of the SPES Front-End, (b) Focus on the EEPS *rev. 2.0*.

5.3.2 *EEPS design revision 2.1*

The duration of EEPS maintenance activities within the ISOL hall is influenced by various factors. A detailed discussion on the impact of the position of various components and the repercussions of beam crossing on the duration of interventions is available in Chapter 6. Specifically, the experimental tests presented in Chapter 6, proved how the EEPS position is difficult to access. Indeed, as outlined by Fig. 5.10, an operator aiming at replacing a component on the EEPS is required to cross the PPB line passing through a narrow pathway, the overall dimensions are: 40 cm wide by 130 cm high. This phase is extremely critical since it poses different risks: from a mechanical point of view the location is characterized by a confined space and the chance of impacting with beam line components. Furthermore, from a radiological perspective, if the operator's bodysuit gets damaged during the crossing, a risk of skin contamination arises.

Aiming at addressing the described issues, the study investigated the viability of mirroring the system. Figure 5.11 compares the existing layout (already upgraded to *rev. 2.0*) with the mirrored version.

The installation of the EEPS on the right side of the RIB line is technically feasible, despite requiring some "minor" upgrades. The first modification is the rotation and re-assembly of the *steerers* block. This component, used for beam positioning, constitutes the first beam optic element along the RIB line. Additionally, the electrode holder needs to be redesigned to fit the rack rail on the opposite side.



(a)

(b)

Figure 5.10: The SPES Front-End. (a) The narrow pathway passage underneath the PPB line s highlighted in green. (b) An operator crossing the beam line during maintenance activities.

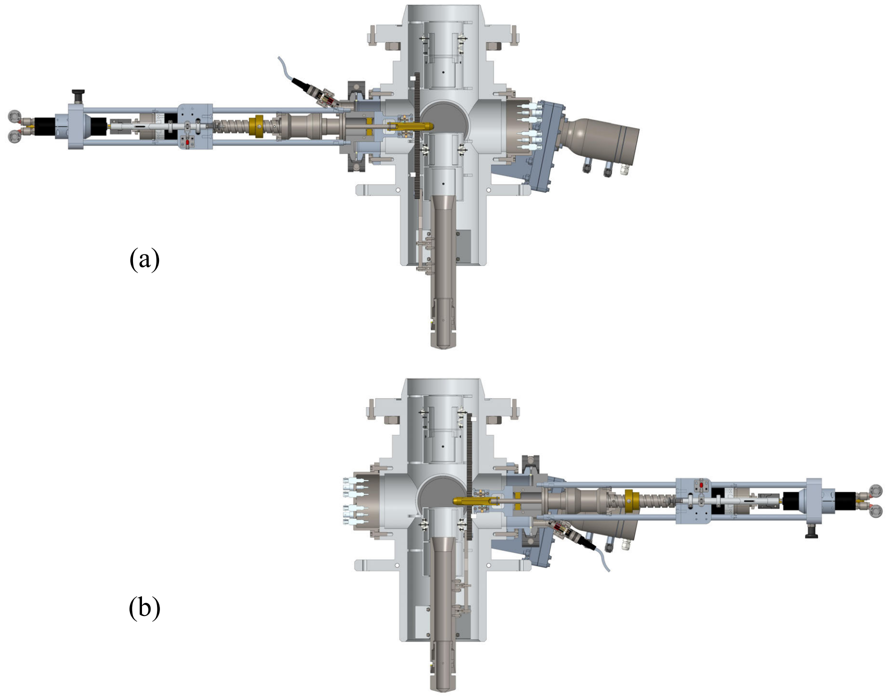


Figure 5.11: (a) The EEPS in its original position, (b) the mirrored EEPS.

Figure 5.12 provides a summary of the Front-End upgrades that must be implemented in order to mirror the EEPS.

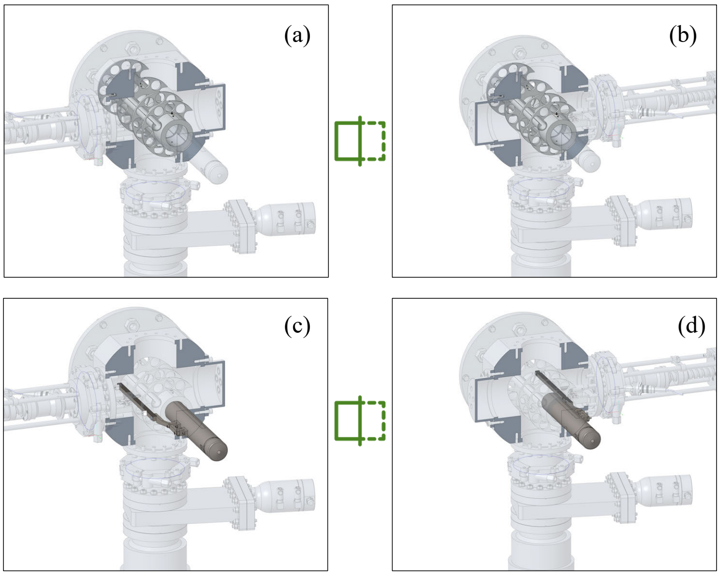


Figure 5.12: Overview of the Front-End components to modify for the upgrade of the system to the EEPS *rev. 2.1*. (a) and (b) show the mirroring of the steerers block. (c) and (d) outline the mirroring of the electrode holder tube and the driving rack.

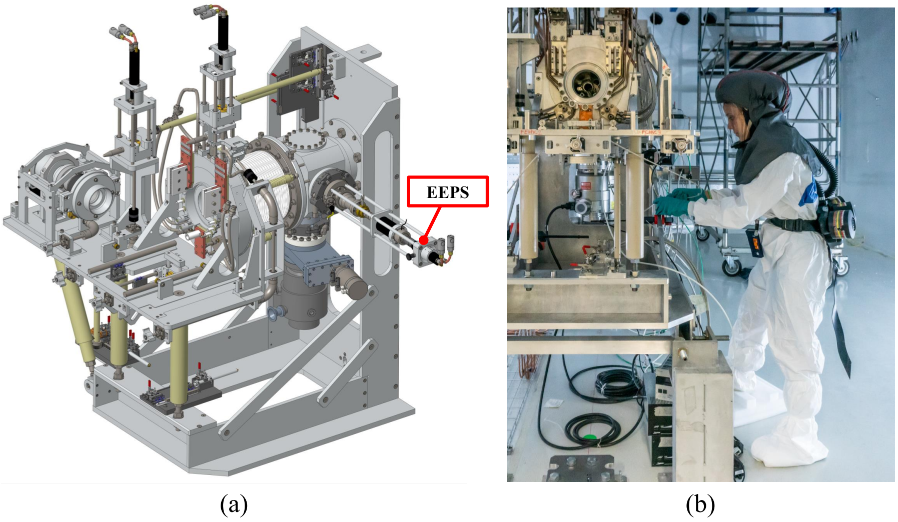


Figure 5.13: (a) Global view of the SPES Front-End, equipped with the EEPS *rev. 2.1*, (b) an operator performing a maintenance task on the righ side of the RIB line.

The new EEPS positioning of *rev. 2.1* is totally transparent from the functional perspective. Still, it represents a huge step forward in the optimization of accessibility, ergonomics, safety and maintainability of this component. The accessibility on the RIB right side is highly improved, resulting in an overall reduction of the intervention duration and in a minimization of the contamination risk. Chapter 6 presents a detailed assessment of maintenance tasks in the proposed configuration, in comparison with the existing design. The EEPS *rev. 2.1* installed on the Front-End is depicted in Fig. 5.13

5.4 CONCEPT DESIGN OF NEXT-GENERATION EEPS

On the SPES Front-End, backup motion flanges are available for the four main motion axes to enable the TIS unit disconnection in case of failure of the main actuation devices. The procedure, as outlined in Fig. 5.14, takes advantage of an auxiliary manual handling system as key recovery method.

Despite the undeniable benefits introduced in the redesigned versions, the main vulnerability of the EEPS is still an open point since, as highlighted in Chapter 4, the EEPS does not include any backup motion flanges. The impact of this critical weakness on predicted personnel exposure, as assessed by the PRA, has driven a comprehensive redesign of the EEPS to evaluate the potential inclusion of external motion interfaces. Instead of the direct coupling between the driving components and the magnetic rotary feedthrough, the new release evaluated the implementation of a single actuation shaft coupled with both the main actuator and the backup flange. Since the actuation of

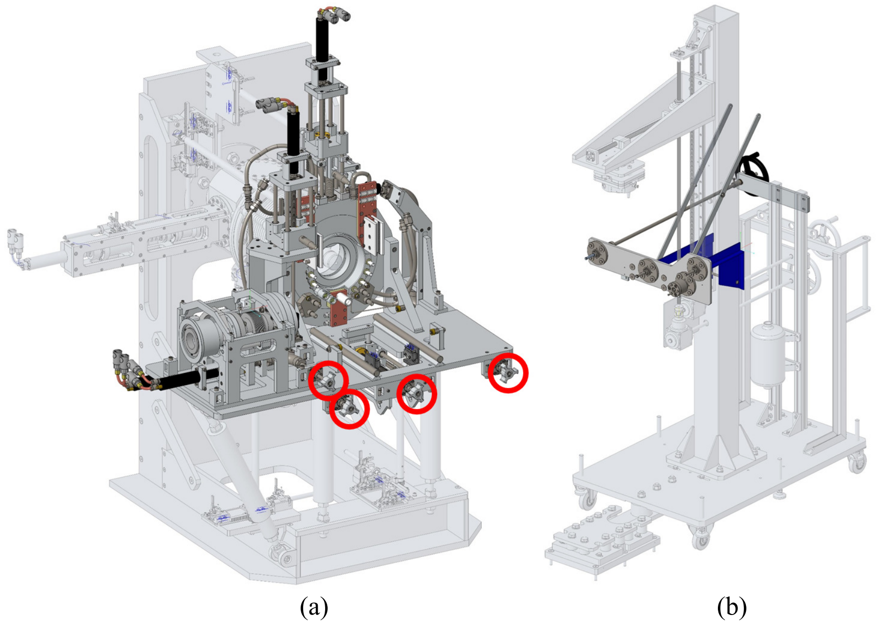


Figure 5.14: (a) focus on the backup actuation flanges of the Front-End motion axes, (b) the external motion actuator provided by the Manual Handling Machine (MHM).

the backup flange should be easy, the required torque should be maintained within reasonable limits, this requirement essentially precludes the use of a planetary gear. Indeed, the reduction ratio $i = 60$ prevents any type of manual, or electric, actuation on the backup flange without the use of a gearbox. In addition, given the non-negligible length of the transmission shaft (1 m), and the size required to sustain the nominal torque, this approach is not the preferred one. Conversely, the idea was to connect the backup flange directly with the pneumatic motor, which normally operates under negligible load conditions, almost at the no-load speed. This approach will require to actuate the backup flange through an external driver, e. g. an electric screwdriver during manual interventions or a dedicated electrical motor installed on the HHM. The proposed strategy requires to align the two actuation ports. On one hand the backup motion flange position should be compatible with the HHM footprint. On the other hand the main actuator shall be accessible, to ease its replacement during maintenance interventions, avoiding any type of interference with the existing Front-End elements such as gate valves, turbo pumps, frames, etc.

A further restriction concerns the introduction of additional bevel gearboxes or reduction stages. Aside from increasing the complexity of the system, this approach will add more components that may fail during operation, require a constant maintenance, will be activated and increase the mass of the radiological waste during the decommissioning. Moreover, a reduction stage will require lubricants, which are not always radiation compatible.

The discussed factors led to the development of a novel hardware architecture, in which the number of components is reduced. Indeed, the EEPS concept design exploits a different type of reduction mechanism, based on the worm-gear coupling. Taking advantage of its intrinsic non reversibility and the high gear ratio, this transmission system provides an effective solution to the described requirements.

The experience gathered in other facilities shown that the EEPS can incur in various types of stresses. Specifically, looking ad different failures happened to the extraction electrode of the ISOLDE and MEDICIS Front-Ends, it can be seen that the effect of spurius high-voltage electrical discharges may result in the local sticking/welding of electrode holder tube with the bearings. This failure condition can block the electrode movement and thus the TIS unit decoupling. Examples of discharge traces can be seen in Fig. 5.1. The maximum available torque is thus a critical factor in the recovery of a failure event. In the SPES case the bottleneck is the value of the magnetic rotary feedthrough (VACGEN® cod. ZMRD6) maximum breakaway torque, which is 4 Nm. Following an extensive market research an alternative model has been identified: UHVD® cod. MD40TX000Z, see Fig. 5.15. The following factors influenced the choice:

- The maximum break-away torque is 9 Nm;
- The unit can be customized with an integrated driving pulley;
- The conventional lubricant can be replaced with a radiation-tolerant one [61].

The provided benefits perfectly match with the worm-gear coupling. Indeed, given a specific module, it will be possible to test different transmission ratios varying the number of teeth of the wheel installed on the rotary thimble.

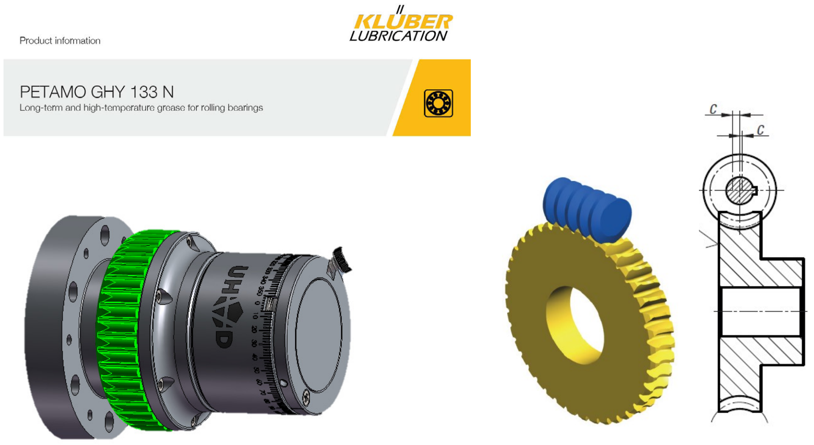


Figure 5.15: Focus on the magnetic rotary feedthrough and the worm-gear concept.

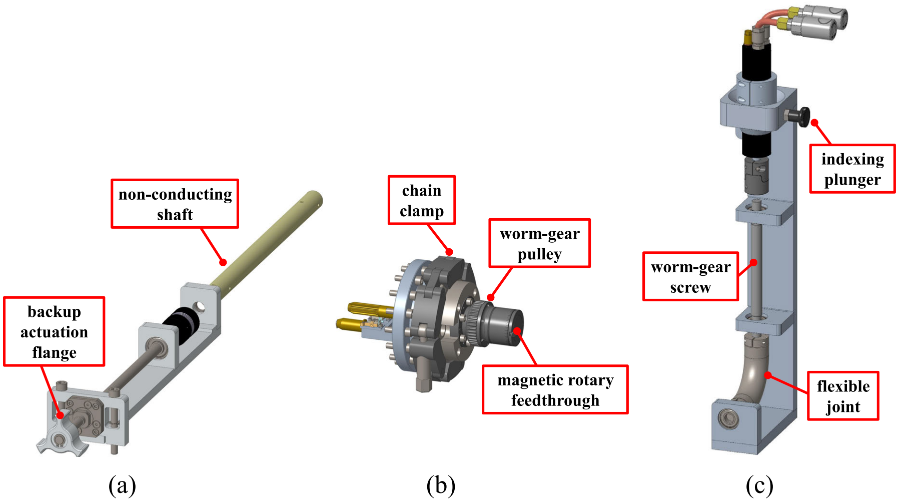


Figure 5.16: Detail view of (a) the EEPS backup actuation flange, (b) the magnetic feedthrough, and (c) the worm-gear driving unit.

As a result of the abovementioned considerations, a novel concept design of the EEPS has been proposed. The motion system is essentially divided into three parts, displayed in Fig.5.16: the backup actuation flange, the magnetic rotary feedthrough, and the worm-gear driving unit. In case of breakdowns the different subsystems can be replaced rapidly and independently.

The backup flange is mounted on the high-voltage section of the coupling table, as outlined in Fig. 5.17. The system body includes pre-assembled brackets, bearings, flanges, shafts, etc. The Front-End baseplate features a dedicated milled housing for precise positioning, ensured by three self retaining locking screws. The unit can thus be pre-assembled externally before installation on the coupling table.

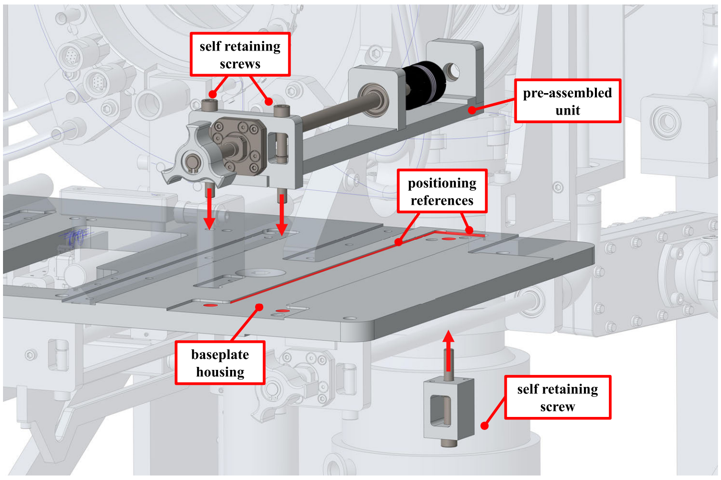
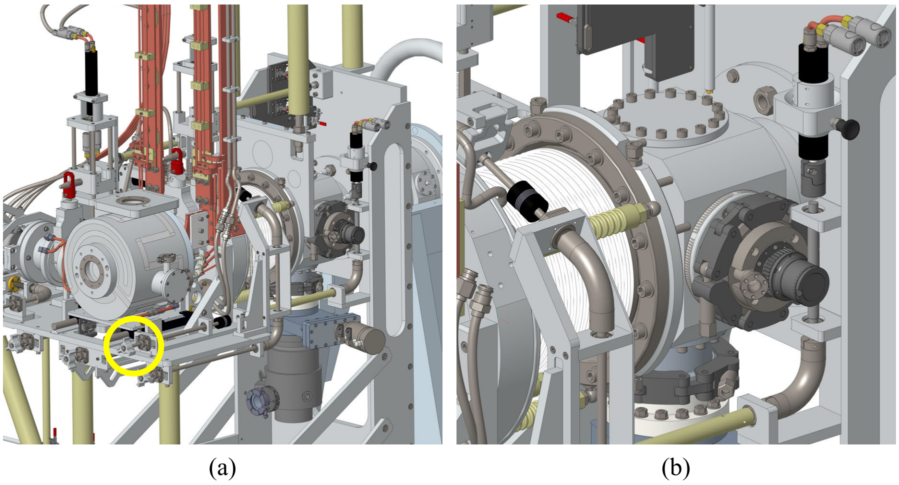


Figure 5.17: Detail view of the backup actuation unit.

The magnetic rotary feedthrough is part of an assembly that includes a quick release vacuum flange, a limit switch support, an electric connector, and the mechanical shaft/pinion. Taking advantage of the developments proposed by the EEPS *rev 2.0*, the flange features a conical edge and three indexing pins that allow its fast positioning or removal through a quick clamp chain. The driving unit is installed on the Front-End back right frame. The assembly, which is conceived as a whole, includes the pneumatic motor, the worm gear screw, a 90° flexible joint used for the connection with the backup actuation system and all the required holders, bearings, etc. As for the previous subsystems, even in this case a dedicated housing has been milled in the Front-End frame, while three screw holders have been used to maintain the fastening screws in position during the installation or removal phase. This strategy allows to pre-assemble the system offline and then install it against the references with a rapid intervention. The system includes the design improvements proposed in EEPS *rev 2.0*, such as the rapid alignment and disconnection flange for the pneumatic motor based on the spring-loaded indexing plunger. The assembly is coupled with two elements. On the upper side the leading screw matches the worm wheel of the rotary feedthrough, on the lower side a rapid jaw joint is used for the connection with the backup actuation flange. The high-voltage (40 kV) difference between the coupling table and the frame requires the use of a non-conducting shaft. In this case the PEEK material has been selected because of its radiation tolerance and the high insulation properties. Two slotted holes enable the side shifting of the system. In this way it is possible to release it from both the worm gear pulley of the rotary feedthrough and from the transmission shaft. A detail view of the system is available in Fig. 5.18.



(a)

(b)

Figure 5.18: Detail view of (a) the new EEPS backup actuation flange, (b) the magnetic feedthrough driven by the worm-gear mechanism.

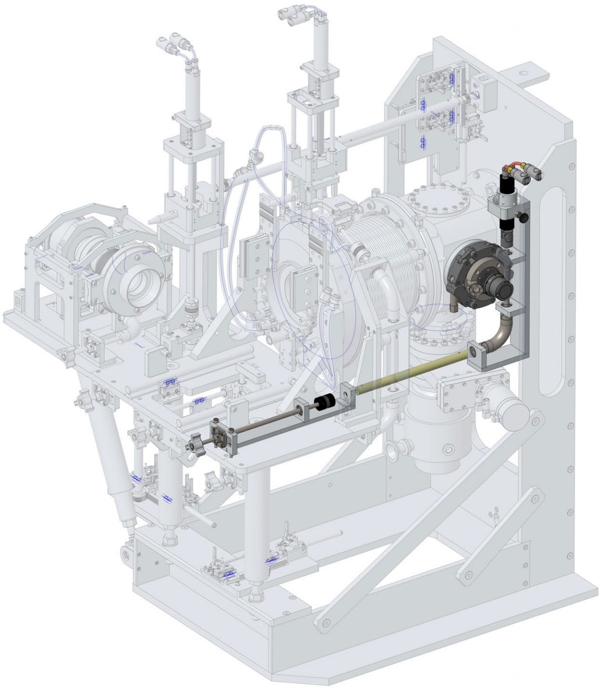


Figure 5.19: Concept design of next-generation EEPS.

The global system can bee seen in Fig. 5.19. In comparison with the original version, the system mass does not increase significantly, and the possibility to dismount the different subsystems independently further mitigates this issue. Additionally, in the new EEPS concept the previously installed planetary gearbox has been removed. The assembly positioning on the RIB right side is motivated by the lack of space for the installation of the backup flange on the left side due to the presence of the PPB motion bellows, providing benefits in terms of improved accessibility and significant reduction of mechanical/radiological risks for the operators during maintenance activities.

5.5 DISCUSSION AND CONCLUSIONS

The redesign study presented in this section was carried out according to the thesis objective aimed at upgrading RH systems by incorporating "design for maintenance" principles within an iterative process.

The three major reviews progressively overcome the weak points highlighted in PRA. Of course, the new proposed designs have a different impact on the facility. In particular, the integration of *rev. 2.0* is quite straightforward. Its implementation simply requires the dismounting of the existing motion axis, the introduction of the rapid disconnection transition and the installation of the new version.

Moving to *rev. 2.1*, its implementation is subject to the reconfiguration of the *steerers* block of the SPES Front-End, in particular this involves the complete dismounting of the central section of the Front-End RIB line, the rotation of the *steerers* block, the electrical re-cabling and the replacement of the electrode holder tube. This task, even if possible, requires a significant effort and it may be considered in a second stage of the facility lifetime, most likely after the first low-energy run, during the TS that anticipates the high-energy operation.

The last concept design requires the machining of two Front-End elements (the coupling table baseplate and the side of the main frame) to house the EEPS subsystems. Even if these modifications are minimal, they cannot be performed on the already installed on-line machine. For this reason, the next generation of SPES Front-End is already in production in the SPES offline laboratory, including these modifications. This will enable an in-depth test campaign on the new design aimed at assess its reliability, spot possible problems and train operators for future maintenance activities.

A weakness of the study is, of course, the preliminary nature of the EEPS concept design, which should be considered as a feasibility assessment rather than an executive engineering process. The actual implementation of the proposed architecture will require, as future research step, a thorough evaluation aimed at the sizing of the different components and the assessment of mechanical stresses through simulations and experimental tests.

Despite its limitations, the study helped in demonstrating how the early integration of a PRA within the design process of safety-critical systems allows to improve the overall safety of RH operation. Indeed, the proposed methodology takes into account recovery and maintainability aspects, as an extension to the conventional approach, where the design is driven by functional specifications. The introduced features assist in reducing the impact of failure events on personnel exposure during recovery actions, thereby minimizing the severity of HAZOP deviations, see Chapter 4.

The preliminary experimental results showing the advantages provided by the redesign of the EEPS to maintenance activities, see Section 6.4.2, support the validity of the proposed approach and the significance of the methodology in the context of the existing body of literature focused on the development of effective protocols for the design of safe and robust RH solutions for nuclear applications.

Future research activities will take advantage of the guidelines presented in this work, potentially including some of the proposed design concepts to other critical components within the SPES facility.

6 ASSESSMENT AND OPTIMIZATION OF CRITICAL MAINTENANCE ACTIVITIES IN HIGH-RADIOACTIVE ENVIRONMENT

6.1 INTRODUCTION

Despite the growing availability of RH tools able to perform remote maintenance tasks in dangerous environments, human interventions are nowadays still required for multiple challenging tasks or for robot repair. The mission of maintenance activities in nuclear facilities is to ensure the reliable operation of critical components and to face potential equipment breakdowns through an organized and safe approach. In this respect, maintenance proactive planning plays an essential role in guaranteeing the plant's safety level [50]. The periodicity of interventions can be linked to the risk associated with failure scenarios evaluated through a PRA or, in other instances, to the integrated dose received by the components, measured through dedicated radiation monitoring devices [248–251].

According to the PRA findings, presented in Chapter 4, the primary risk reduction strategy is intended to reduce the likelihood of failure events through different approaches, such as the implementation of a preventive maintenance and inspection plan, or the optimization of the design of crucial components to enable remote recovery strategies, see Chapter 5. Nevertheless, since a residual risk still exists, planned and unplanned interventions in highly radioactive areas requires an in-depth analysis. As a result, this chapter presents a comprehensive assessment and review of critical maintenance activities within the ISOL hall, aiming at improving the operator's safety. As remarked

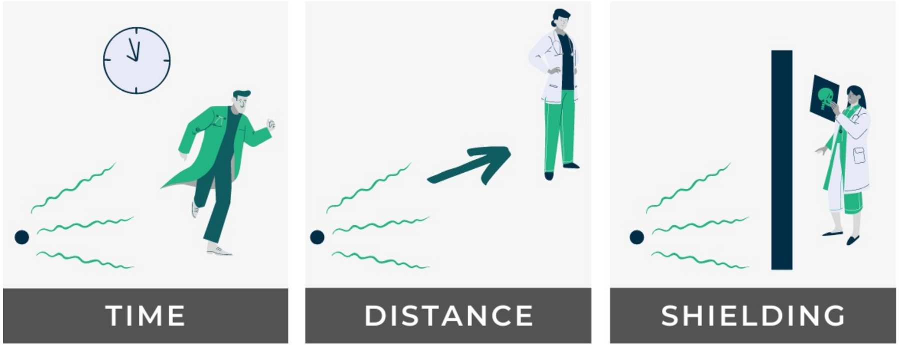


Figure 6.1: Application of ALARA principles: time reduction, distance increase and use of shielding.

by the PRA, this type of analysis and optimization can significantly contribute to improve the effectiveness of the identified IPLs within the SPES facility. The maintenance assessment, as an extension of the aforementioned study, is focused on the standardization, optimization and validation of safety-critical maintenance activities in dangerous locations including both the exposure and contamination risks.

The ALARA principles, summarized in Fig. 6.1, indicates the key strategies to pursue in order to minimize the personnel exposure during maintenance activities: limit the amount of time spent near the radiation source, increase the distance from the hot-spots, and make use of a shielding to protect the operator during the intervention [96]. Unfortunately, in the SPES case, the implementation of barriers between the worker and the source is frequently not a realistic option due to the configuration of the intervention site, whereas the operator distance from the hot-spots represents a predetermined design constraint. As a result, the main parameter that can be tuned to minimize the personnel exposure is the task's duration. In this study a comprehensive experimental campaign has been carried out to assess the impact of different optimization strategies, such as design changes, procedures, and tools, on the duration of SPES maintenance interventions.

6.1.1 *Background*

The evaluation of SPES maintenance activities were first investigated in a previous study [252], which examined the different tasks from an ergonomics perspective, providing a set of maintainability guidelines which drove the re-engineering of the fastening mechanisms of some crucial components, such as the Front-End potentiometers and limit switches [247]. In this thesis, the comprehensive redesign of the EEPS, presented in Chapter 5, has extended the aforementioned studies by providing additional optimizations based on the suggested maintainability principles. The SPES Front-End redesign process is extended and supported by the maintenance assessment presented in this chapter, which aims at providing a solid statistical foundation to validate the benefits introduced by the described optimizations.

A series of experiments meant to collect information on intervention length are presented in the following sections. The conventional approach adopted in other facilities is to plan this type of blank tests only following an actual breakdown condition requiring a physical intervention. The trials are usually intended to estimate the individual and collective dose associated with the maintenance activity. In contrast, this study is intended to develop a preventive approach which takes advantage of the construction stage of the facility, to validate and propose effective optimization methods leading to a considerable reduction of the foreseen personnel exposure.

6.1.2 *Aim of the research*

The maintenance assessment presented in this chapter is intended to support the mitigation of the residual risk resulting from on-site maintenance tasks. The main objectives of the research are:

- Identify potential vulnerabilities that may represent a source of errors or waste of time during the task execution;
- Standardize the intervention parameters, determining the required tools, PPEs, and defining the best working position in order to provide homogeneous operating conditions;
- Define detailed step-by-step operating procedures, collect visual material (photos and videos) supporting the development of an effective operator training program;
- Validate experimentally hardware design changes leading to a reduction of the maintenance tasks duration;
- Suggest potential system optimization aimed at shortening the interventions, minimizing the potential error sources (small components, positioning, cabling, etc.) and reducing the complexity (and thus the skill level of the operator);
- Identify the most significant factors affecting the task duration;
- Collect reliable estimates of the task duration, including multiple operators, different skill level and characteristics, to be used as a significant asset in the proactive estimation of personnel exposure prior to real interventions.

The study ultimately seeks to demonstrate how a proactive approach to the assessment of maintenance interventions can provide a substantial beneficial effect on the minimization of predicted personnel exposure during residual hands-on interventions.

6.2 experiment design

An experiment is a test, or a series of tests, where purposeful changes are made to input variables of a process or system in order to observe and identify changes in the output response. This section describes the datasets and the implemented procedures of different experimental tests aimed at the evaluation of the effect of various parameters on the duration of maintenance tasks, which has been considered as response variable. The time required for the interventions has been measured on a random sample of maintenance tasks (i. e. experimental units), in which the factors' levels are changed simultaneously. In spite of varying the factors one by one, this approach enables the study of the interactions among different factors.

6.2.1 *Factors*

The input factors analyzed in the study, which can be continuous variables or categorical variables, have been classified as operator-related and task-related. Operator-related factors are:

- ID
- Run
- Age
- Sex
- Operator height
- Skill level: Beginner, Competent, Expert

Besides obvious information used for classification, such as ID, Age, and Sex, the operator height and skill level have been considered due to their expected impact on the task duration.
The task-related factors are listed below.

- Assembly: extraction ELectrode (EL), Proton Channel (PC), RIB channel (RC), Proton gate (PG), RIB gate (RG)
- Component: Motor (M), Potentiometer (P), limit Switch (S)
- Task: Mounting (M), Dismounting (D)
- Design: Old (O), New (N)
- Tool: A, B
- Distance
- Height
- Side: Left side of the RIB line (L), Right side of the RIB line (R)
- Beam crossing: Yes (Y), No (N)
- Weight
- Number of fixing screws (Screws)

The same task type can be composed of different actions depending on the Front-End component. Moreover, the assemblies are installed in different locations, which have been detailed through the indication of the component distance from the operator's starting location, its height, the installation side, and whether or not the operator must cross the PPB line to reach the intervention place. Additional factors are the component weight and the number of fastening screws.

6.2.2 *Design principles*

The experimental tests described in this chapter have been designed according to the basic principles of DoE:

- **Blocking** is a technique used to mitigate the effects of known and controllable nuisance factors [253] through the development of homogeneous blocks in which the nuisance variables remain constant while the factor of interest varies. In this study, blocking principle has been applied carrying out the tests in the same environmental conditions, from a fixed starting location, and with the same instrumentation.
- **Randomization** is a common technique used to balance the effect of uncontrollable factors that may impact the results of an experiment [254]. This method ensures that the statistical assumptions needed for generalizable results are met. In the experiment, each operator performed a randomized set of runs among different tasks, components and assemblies.
- **Replication** in statistics is the non-consecutive running of the experimental design multiple times [254]. It is essential to differentiate between replicates and repeated measures: they are both multiple response measures performed at the same combination of factor settings, but repeat measurements are produced during a single run or a series of runs, whereas replicate measurements are taken during a series of identical but distinct runs, which are frequently randomized. At least two replicates were used in each run of the sessions described in the following sections.

6.2.3 *Sessions*

Maintenance tests have been organized in different sessions, linked to distinct research objectives.

6.2.3.1 *Screening session*

The experimental phase started with some pilot runs in the context of a first screening session aimed at clarify the test protocols, identify

Feature	Description
Operators	5
Repetitions	2
Components	12 (3 components on 4 assemblies)
Tasks	Mounting, Dismounting

Table 6.1: Screening session dataset.

potential hardware vulnerabilities, and standardize the task execution. This includes the identification of the exact operator working position, the evaluation of most suitable toola, and the definition of detailed procedures. The screening session dataset is described in Table 6.1.

6.2.4 *Comparison session*

This experimental campaign aims at evaluating the impact of various design or organizational improvements by comparing the same maintenance task in two (or more) configurations. The comparison session dataset is described in Table 6.2. Approximately 380 maintenance tests make up the whole sample size.

Feature	Description
Operators	6-10
Repetitions	2-3
Components	5
Tasks	Mounting, Dismounting

Table 6.2: Comparison session dataset.

6.2.4.1 *Survey session*

The goal of the last experimental session is the collection of reliable and accurate data on the maintenance tasks duration for the most crucial components installed on the SPES Front-End. The survey session dataset is described in Table 6.3. The total sample size is around 600 maintenance tests.

Feature	Description
Operators	10
Repetitions	2
Components	15
Tasks	Mounting, Dismounting

Table 6.3: Survey session dataset.

6.3 MATERIAL AND METHODS

The goal of the experimental campaign is to collect realistic data on the interventions' duration. To improve the accuracy of the estimation, the operators have carried out the experimental tests wearing all the PPEs that will be required during operation. Additionally, the ambient lighting has been switched off to simulate the actual operating scenarios.

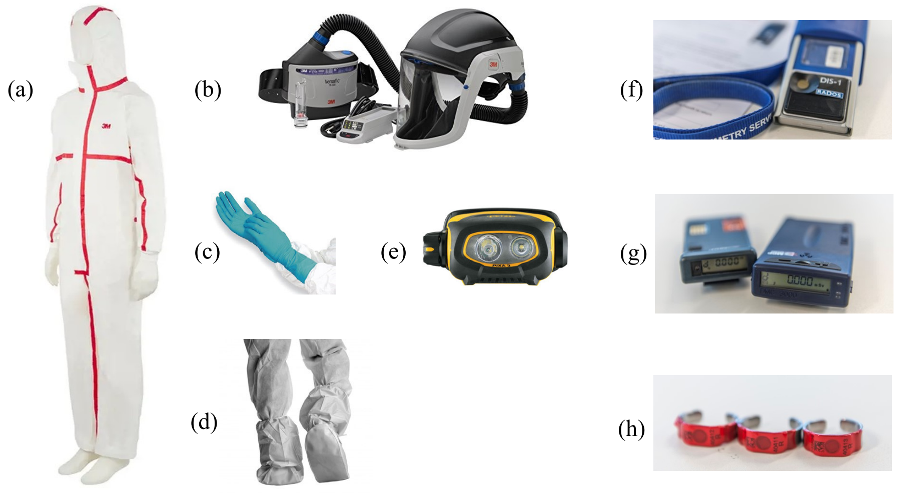


Figure 6.2: Personnel Protective Equipment (PPE) required during SPES Front-End maintenance activities.

Because the test conditions had never been evaluated before, the screening session allowed for the identification of the PPEs required for the safe execution of maintenance activities. The following list details the selected measures, which are summarized in Fig. 6.2.

(a) Type 4/5/6 protective coverall with tape sealed seams resistant to radioactive particulate (EN 10732);
(b) Integrated helmet and mask providing head (EN397), eye and face (EN166 medium energy impact) protection, combined with a battery powered air respirator unit and particulate filters;
(c) 2 pairs of gloves;
(d) Overboot covers;
(e) Headlamp;
(f) Passive dosimeter for the measurement of gamma, beta and neutron radiations;
(g) Active dosimeter featuring a direct dose display, audible indication of the radiation level and alarm functions;
(h) Extremity dosimeter (thermoluminescence-based finger ring).

The different experimental tests have been executed adopting a standardized protocol. There are two main types of interventions: Dismounting (D) and Mounting (M) tasks, which can be executed on different components, installed in various assemblies. In all the runs, the operator starts from a fixed location, enters the ISOL hall, reaches the working position, executes the task and exits. As already mentioned, the runs have been randomized and two operators were taking turns along each experimental session. Figure 6.3 displays an operator fully dressed for the intervention.

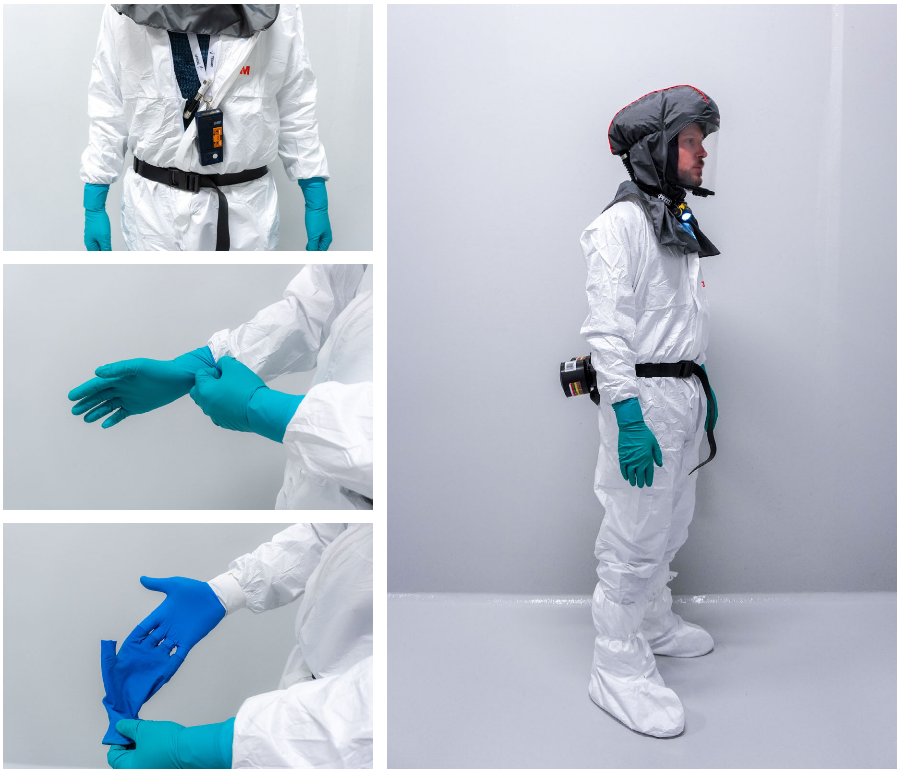


Figure 6.3: PPEs worn by operators during maintenance tests.

6.4 RESULTS AND DISCUSSION

The data collected during the three described experimental campaigns, as well as a light statistical analysis are presented in the following sections.

6.4.1 *Screening session*

The screening session played an important role in the definition of the test protocols and in the standardization of the experimental conditions. Performing homogeneous trials enables the subsequent data analysis to be based on a solid dataset. Additionally, it allows for a reliable estimate of the time required by different interventions and for the comparison between different experimental conditions.

One of the parameter that have been standardized is the operator working position for each maintenance task. Among the potential locations, the position providing the best ergonomic access to the analyzed component has been selected. This approach becomes highly beneficial for the future estimation of the predicted personnel exposure for a specific activity. Indeed, given the measured task duration, the evaluation of the dose rate in a specified position will allow to accurately predict the individual dose contribution of the intervention.

6.4.1.1 *Optimizations*

Visibility

The screening sessions represented a useful opportunity to address real-world issues that may lead to operational errors during maintenance activities. An interesting example is provided by the pneumatic connection of the Front-End motors. In the original configuration, visible in Fig. 6.4 (left), the two supply pipes were not marked. The first experimental trials showed that operators spent a non-negligible amount of time in understanding the right connection pairing. In this context, a clear identification, as displayed in Fig. 6.4 (right), allows saving time and reducing the potential source of connection errors.

Connectors

The components installed on the SPES Front-End, such as potentiometers and limit switches, are equipped with a cable-mounted electrical connector to enable their rapid replacement during maintenance tasks. Following the positioning of the device, during the mounting process, the connector is coupled with its female counterpart on the Front-End. In the original version, the ground connections on the system were using multiple cables, each one terminated with a female cable-mounted socket. The first pilot runs of the screening session showed that operators spent a significant amount of time searching for the correct cable, which could eventually move, to connect the two elements together. To overcome this issue, as design optimization, the use of panel mounted socket connections is suggested. This improvement, along with a clear identification of the socket ID, allows saving time during maintenance interventions.

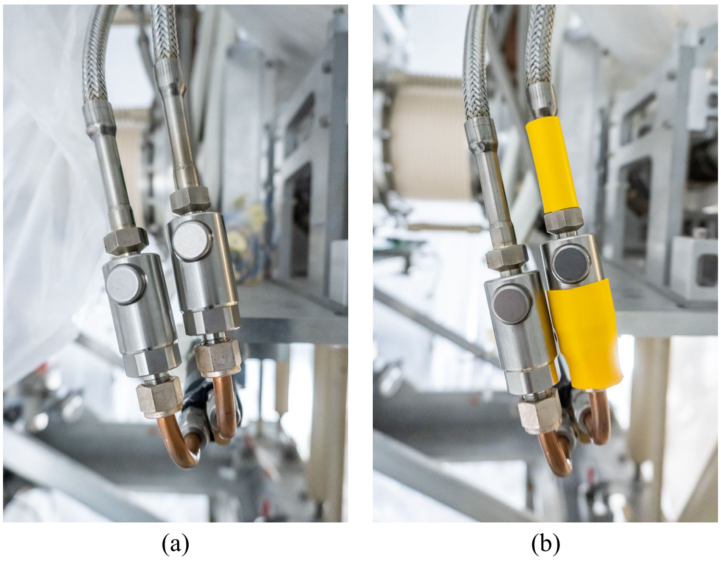

(a) (b)

Figure 6.4: Pneumatic connectors (left), high visibility marking (right).

Preliminary actions

Both the limit switches and the potentiometers installed on the Front-End are linked to a rack-pinion system used to detect each axis position. The operational feedback showed that the axis position influences the possibility to replace the component. Specifically, when the system is located at one stroke end, the corresponding cam makes contact with the switch's lever, making removal challenging. For this reason, the Front-End motion axes should be arranged in a specific configuration (usually at the stroke mid-point) to ease the maintenance activities prior to the actual intervention.

6.4.1.2 *Procedures*

From the experimental test standpoint, standardized operating procedures enable the comparison between different interventions. On the other side, during real operation, they provide a useful tool which supports the operator in both the training and the task execution. During the screening session, harmonized procedures have been defined for the different analyzed tasks taking advantage of operational feedbacks. An example is provided by the pneumatic motor mounting task: the fastening clamp used to block the motor position allows for multiple component orientations. During the screening session an operator inadvertently mounted the motor in the wrong orientation, preventing the pneumatic pipes from being coupled with the motor connectors. This potential issue has been taken into account in the drafting of the procedure, which now requires to insert the motor within the clamp, connect the supply pipes and, as last step, secure the position with the two screws. This modification ensures that the motor orientation is correct, thus avoiding redundant corrective actions.

Each maintenance activity should start with a briefing in which the maintenance team discuss the key intervention steps. The operator

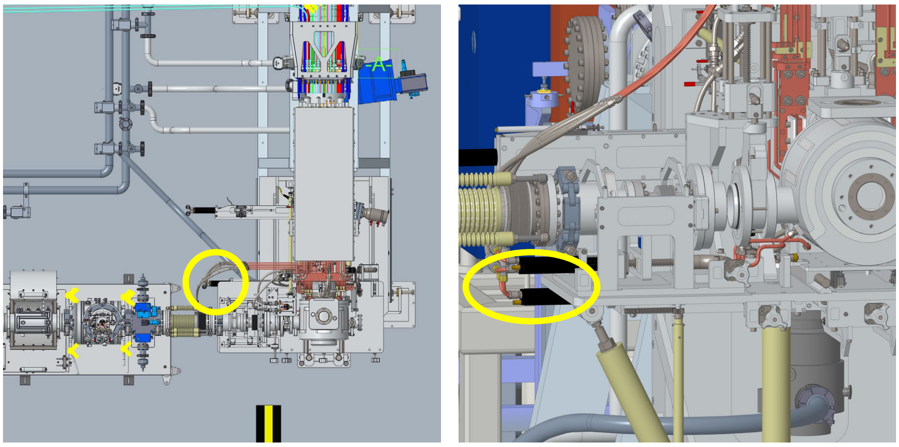


Figure 6.5: 2D (left) and 3D (right) maps of the SPES ISOL hall used to identify the component position prior to maintenance activities.

subsequently takes advantage of a cockpit-style checklist to verify the availability of all the required tools, hardware components, and PPEs.

A 2D map and a 3D view, see Fig. 6.5, are then studied to identify the component location and the corresponding working position. The last step prior to the actual task execution is the review of the exact list of actions with the help of an illustrated procedure, which also includes the desired operator behavior in case of unexpected events.

The experience acquired during the screening session underlined the importance of including visual and manual checks providing a direct feedback to the operator on the correct execution of the maintenance activity. Figure 6.6 provides an example of the illustrated sequence of actions for the execution of the extraction electrode dismounting task.

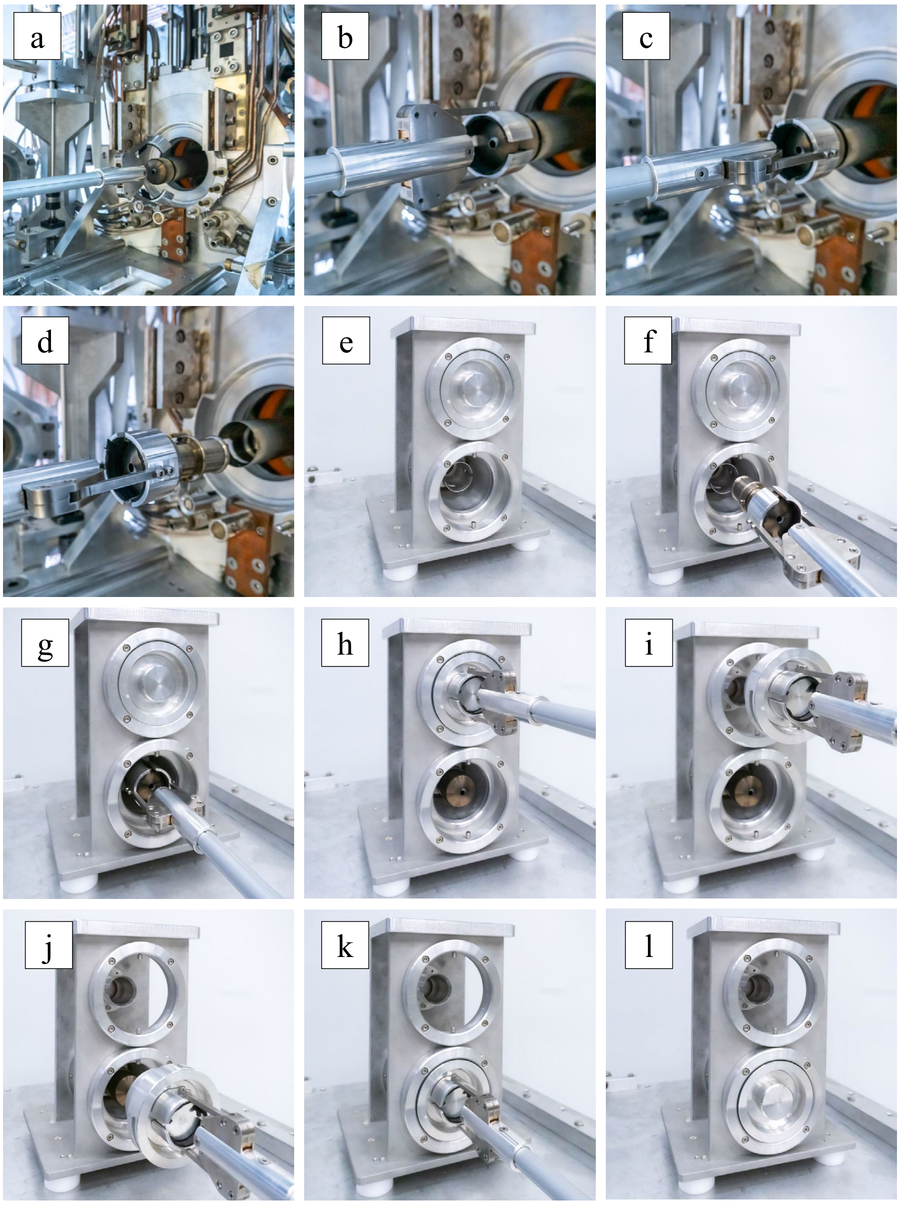


Figure 6.6: Example of illustrated procedure for the removal and storage of the SPES extraction electrode.

6.4.2 *Comparison session*

This section presents the primary outcomes of the experimental campaign aimed at the comparison between different operating conditions in order to evaluate their impact on the overall duration of maintenance activities. Figure 6.7 includes some pictures taken during the experiments. The maintenance tests have been carried out following a common protocol: for each comparison, two non-consecutive trials are executed for each task in the two configurations. Specifically, the analyzed scenarios are:

- Pneumatic motor fastening method: clamp design vs quick release design;
- Vacuum flange: standard CF flange vs conycal flange design;
- Potentiometer fastening method: screwed version vs toggle clamp;
- Limit switch fastening method: screwed version vs toggle clamp;
- Pneumatic motor disconnection procedure: comparison between different tools.

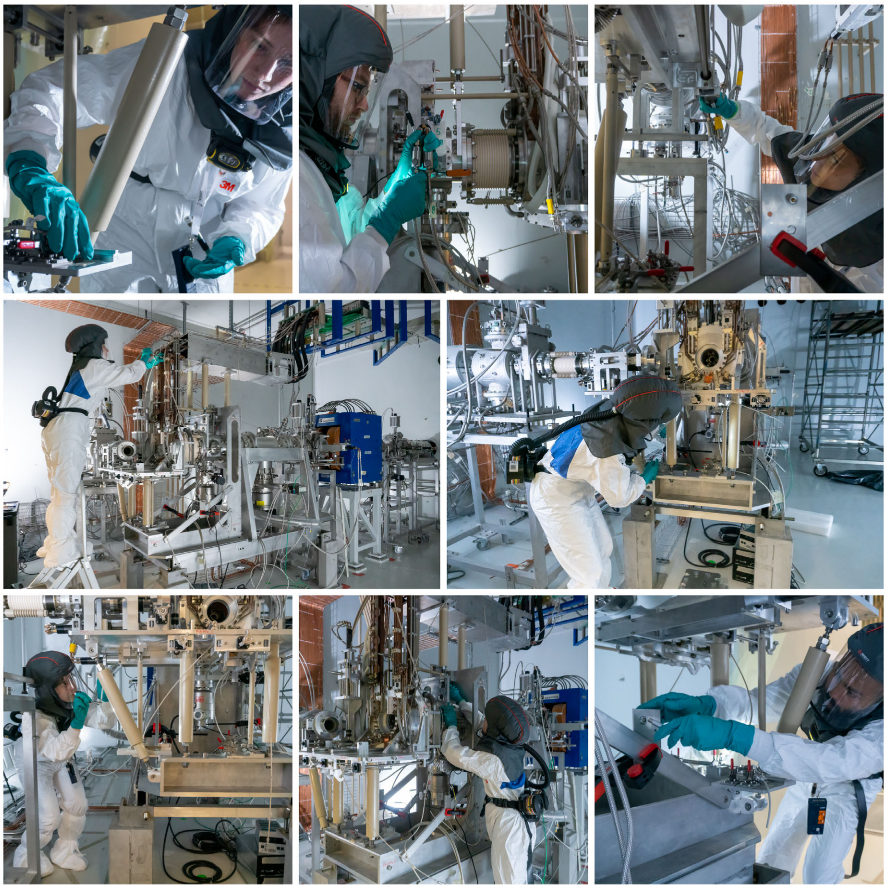


Figure 6.7: Different examples of SPES Front-End maintenance tests.

Following the experimental sessions, the collected data are analyzed to determine if a statistically meaningful difference exists between the mean of the samples in the two configurations. In this process, the prior application of the Levene's test helps to verify the hypothesis of homogeneity of variances. As second step, the two-sample t test enables the validation of the existing difference with a confidence interval of 95%. This testing process has been applied for both the validation of proposed design optimizations, or to evaluate operational alternatives, such as the choice of the most suitable tool, prior to the definition of final intervention procedures.

6.4.2.1 *Impact of optimized design: pneumatic motor*

As first comparison test, the pneumatic motor fastening mechanism is considered. The purpose of this experiment is to assess the impact of the EEPS pneumatic motor optimized fastening mechanism on the reduction of the replacement task duration in comparison with the existing design. Specifically, the benchmark aims at evaluating the design presented in Section 5.3.1, including a self-centering flange and an indexing plunger with the existing securing technique based on a conventional clamp tightened by two screws. The two mounting mechanisms, which are displayed in Fig. 6.8, have been tested on the assembly, the EEPS, under the same environmental settings.

During the experiment, the EEPS motor dismounting and mounting tasks have been carried out in three different configurations:

- Old connection design located on the Left RIB side (OL);
- New connection mechanism located on the Left RIB side (NL);
- New connection mechanism located on the Right RIB side (NR).

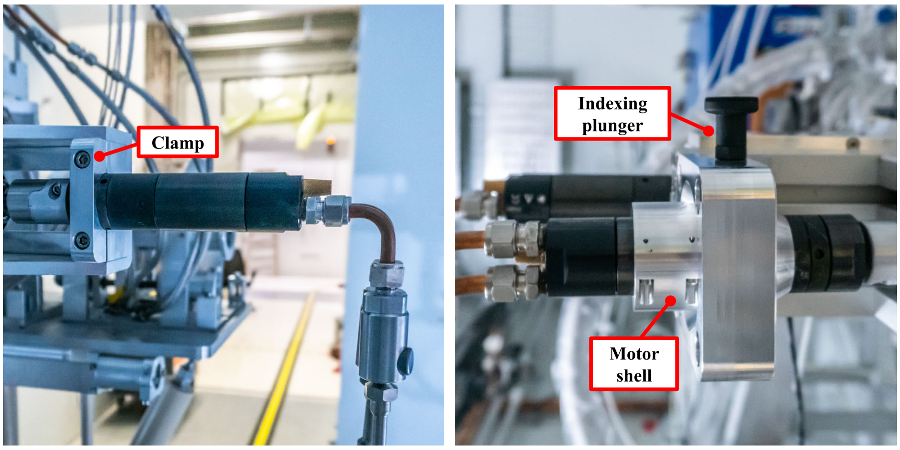


Figure 6.8: The pneumatic motor fastening mechanisms: old design based on a clamp (left), new design featuring an indexing plunger (right).

Design	N	Mean	SE Mean	StDev	Variance	Minimum	Median	Maximum	Range
OL	20	31,05	1,69	7,54	56,89	25,00	29,00	59,00	34,00
NL	20	19,00	0,53	2,36	5,58	15,00	19,00	23,00	8,00
NR	20	13,70	0,30	1,34	1,80	11,00	13,50	16,00	5,00

Table 6.4: Descriptive statistics of dismounting task on the EEPS motor using the old and new connection mechanisms. Time is given in [s].

Table 6.4 summarizes the descriptive statistics of the time required by the EEPS motor dismounting task in the three different configurations, whereas Table 6.5 describes the mounting tasks' duration. The complete test reports are available in Appendix C. A graphical representation of the experimental results is displayed by means of the boxplots in Fig. 6.9 and Fig. 6.10, which are related to the dismounting and mounting tasks, respectively. The beneficial effect of the optimized fastening design for the EEPS pneumatic motor is evident in both experimental scenarios. The "OL" and "NL" datasets have been analyzed with the Levene's test, which confirmed the homogeneity of variances. Subsequently, the two-sample t test, individually applied on the dismounting and mounting tasks, acknowledged the observed difference in the mean of the two samples. This result supports the validity of the redesigned mechanism.

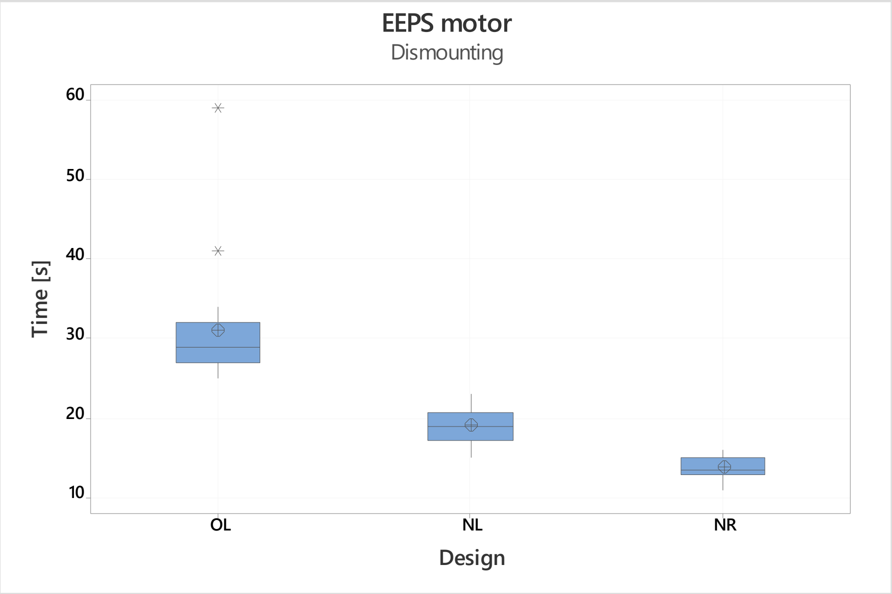


Figure 6.9: Boxplot comparing the duration of dismounting task on the EEPS motor using the old and new connection mechanisms. (OL) denotes the Old design on the Left RIB side, (NL) stands for New design on the Left RIB side, (NR) describes the New design on the Right RIB side.

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

Table 6.5: Descriptive statistics of mounting task on the EEPS motor using the old and new connection mechanisms. Time is given in [s].

In a second phase, the two-sample t test have been applied to the "NL" and "NR" samples, assuming equal variances. The obtained *p*-value confirmed the statistical difference between the two means, thereby demonstrating the beneficial effect of the relocation of the EEPS motor on the right side of the RIB line, where the accessibility is improved. The test outcome provides a strong justification to the design proposal aimed at the mirroring of the system, presented in Section 5.3.2 Considering the mounting task, the introduction of a quick connection flange for the EEPS pneumatic motor provides a reduction of the intervention time by approximately 40%. Moreover, the installation of the assembly on the RIB right side enables for an extra 30% reduction in task duration.

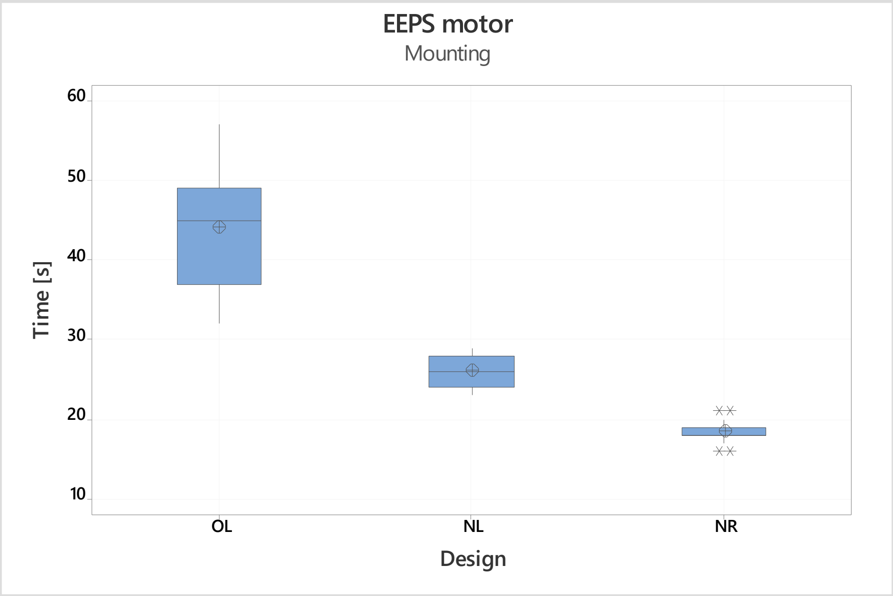


Figure 6.10: Boxplot comparing the duration of mounting task on the EEPS motor using the old and new connection mechanisms. (OL) denotes the Old design on the Left RIB side, (NL) stands for New design on the Left RIB side, (NR) describes the New design on the Right RIB side.

6.4.2.2 *Impact of optimized design: vacuum flange*

This section presents the Front-End maintenance tests focused on the dismounting and mounting of the EEPS vacuum flange. As described in Section 5.3.1, this element needs to be dismounted to access components installed in vacuum along the RIB line. A typical example is provided by the rad-hard limit switches used to detect the stroke ends of the extraction electrode holder rack-pinion transmission mechanism. The experiment aims at evaluating the advantages introduced by the optimized connection design proposed in Section 5.3.1, benchmarking the obtained results with the existing layout. Figure 6.11 shows the vacuum flange connection mechanisms available for the EEPS: the old version (on the left) is based on a standard CF flange secured by 16 screws, whereas the new design (on the right) makes use of a quick release chain clamp. Due to the length of the replacement task with the standard design, the two samples does not have the same number of observations. Nevertheless, the beneficial effect introduced by the optimized coupling method is pretty obvious.

Table 6.6 summarizes the descriptive statistics of the time required by the EEPS vacuum flange Dismounting (D) and Mounting (M) tasks with the two designs. The complete test reports are available in Appendix C. This specific intervention requires two operators during the last part of the dismounting task and the initial part of the mounting task. The second operator is required to hold the EEPS system while the first worker completes the connection (or disconnection) of the flange. For the sake of comparison, the time spent by the second operator has been added to the duration of the first operator task. The beneficial effect of the design optimization of the EEPS vacuum flange on the time required for dismounting (left) and mounting (right) tasks are shown in Fig. 6.12. In both the mounting and dismounting tasks,

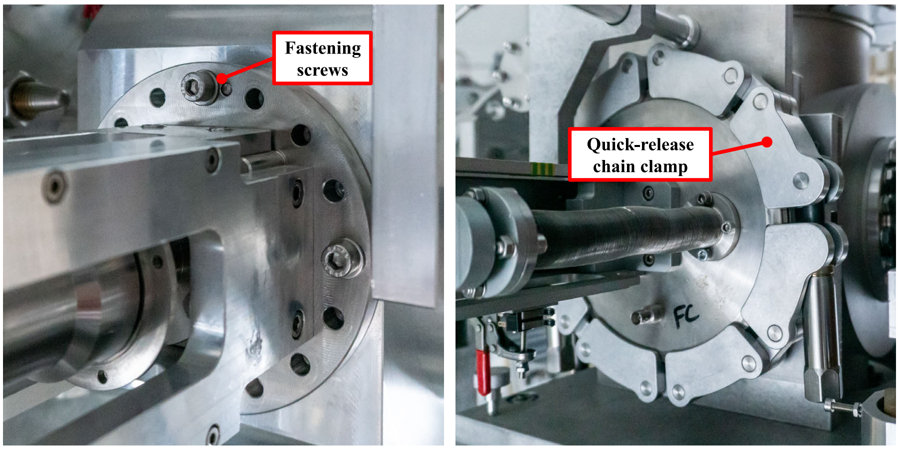


Figure 6.11: The vacuum flange sealing mechanisms: old design based on standard CF flange (left), new design using a chain clamp (right).

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

Table 6.6: Descriptive statistics of the Dismounting (D) and Mounting (M) tasks on the EEPS vacuum flange with the old and new design. Time is given in [s].

the quick release design of the vacuum flange, based on two conical flanges and a chain clamp mechanism, provides a reduction of the intervention duration of more than 80%. The "old" and "new" datasets have been analyzed with the Levene's test. Given the significant result, equal variances are not assumed. The two-sample t test, have then been individually applied on the dismounting and mounting tasks, confirming the difference in the mean of the two samples. This result supports the validity of the redesigned flange.

An additional consideration concerns the required skills and ability to mount the CF flange. The non-negligible stress state during task execution can lead to a wrong fixation of the 16 screws, potentially necessitating a corrective intervention. Conversely, the chain clamp removes several degrees of freedom in the fastening method, thereby reducing the task complexity and the possible mounting errors.

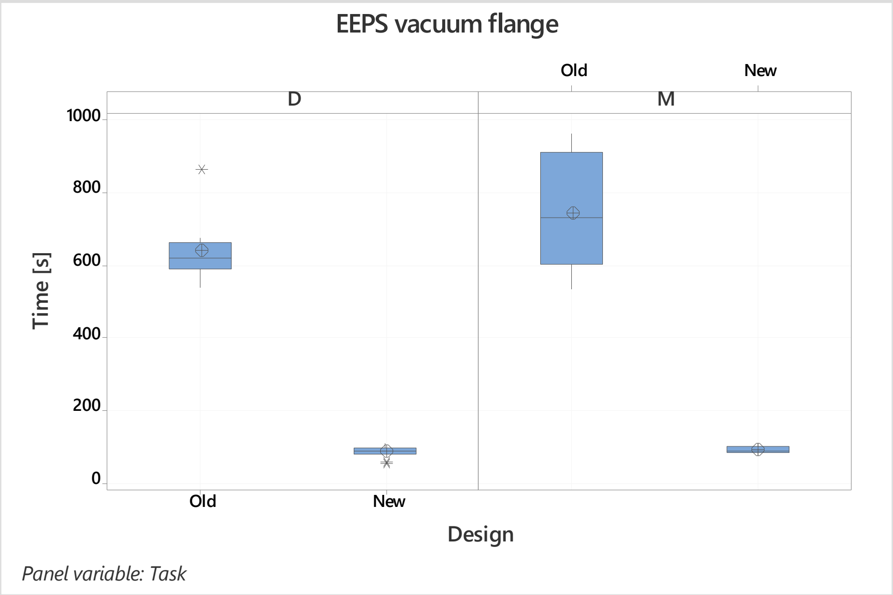


Figure 6.12: Boxplot comparing the duration of maintenance interventions on the EEPS vacuum flange using the old and new connection mechanisms: dismounting task (left), mounting task (right).

6.4.2.3 *Impact of optimized design: linear potentiometer*

The experimental tests discussed in this section are intended at measuring the advantages, in terms of time reduction, introduced by an optimized design of the linear potentiometer fastening method. This component is installed on the different motion axes of the SPES Front-End as diagnostic device used to detect their actual position. A recent study [247] has proposed an optimized fastening design, based on an alignment ring and a toggle clamp that should shorten its replacement time. A detailed comparison between the proposed solution with the existing layout has been implemented thanks to experimental tests on the dismounting and mounting tasks. The trials have been carried out on the same assembly, the PPB gate diagnostic, measuring the required replacement time in the two configurations. Figure 6.13 shows the linear potentiometer connection mechanisms available for the PPB gate: the old version (on the left) is based on M3 screws, whereas the new design (on the right) features a quick release toggle clamp.

Table 6.7 summarizes the descriptive statistics of the time required by the PPB gate potentiometer Dismounting (D) and Mounting (M) tasks with the two designs. The complete test reports are available in Appendix C. The beneficial effect of the design optimization of the PPB gate potentiometer connection mechanism on the time required for dismounting (left) and mounting (right) tasks are shown in Fig. 6.14. Besides the evident benefits offered by the redesigned fastening method, in terms of reduction of the intervention time, the toggle-clamp mechanism overcomes potential issues linked with the manipulation of small components, such as the challenging positioning and the potential risk of fall.

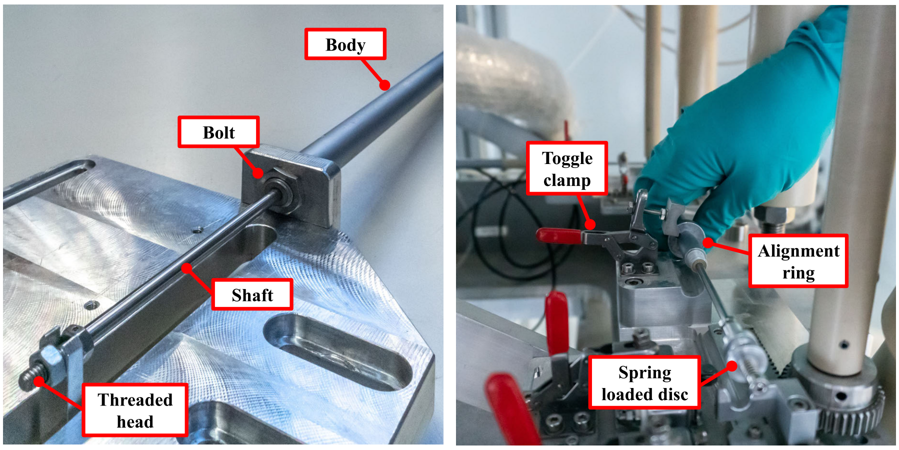


Figure 6.13: The linear potentiometer fastening mechanisms: old design based on M3 screws (left), new design featuring a toggle clamp (right).

Task	Design	N	Mean	SE Mean	StDev	Variance	Minimum	Median	Maximum	Range
D	Old	18	70,83	3,70	15,71	246,74	47,00	66,50	98,00	51,00
	New	18	21,00	0,62	2,64	6,94	17,00	21,00	28,00	11,00
M	Old	18	88,56	3,42	14,52	210,73	69,00	87,00	116,00	47,00
	New	18	29,22	0,70	2,96	8,77	25,00	29,00	37,00	12,00

Table 6.7: Descriptive statistics of the Dismounting (D) and Mounting (M) tasks on the proton gate potentiometer with the old and new design. Time is given in [s].

As additional remark, the experiments confirmed the preliminary observations emerged during the screening session: the connection of the potentiometer cable to the Front-End is easier and quicker when the socket is panel mounted. The electrical connectors used for the tests feature a push-pull mechanism designed to reduce the connection time. The datasets associated to the "old" and "new" fastening method have been analyzed with the Levene's test. Given the significant result, equal variances are not assumed. Additionally, the two-sample t test, have then been individually applied on the dismounting and mounting tasks, confirming the difference in the mean of the two samples. Taking into account the dismounting task, the time of the intervention with the new design is roughly one-third the one required by the old version. The significance of the obtained time reduction supports the validity of the redesigned fastening mechanism and the usefulness of the maintainability guidelines proposed in [252].

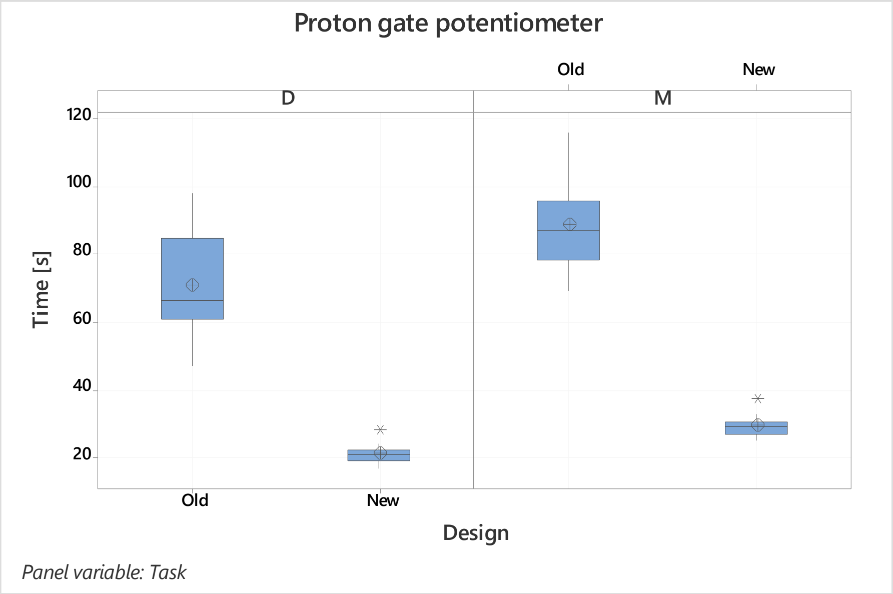


Figure 6.14: Boxplot comparing the duration of maintenance interventions on the PPB gate potentiometer using the old and new connection mechanisms: dismounting task (left), mounting task (right).

6.4.2.4 *Impact of optimized design: limit switch*

The fastening method used to secure the Front-End limit switches has also undergone a comprehensive design review. These components are installed, in parallel to the potentiometer, on the motion axes diagnostics. The switch is triggered by a cam installed in the rack-pinion transmission mechanism linked to the actual mechanical axis. In its original configuration, the limit switch was fastened directly to the baseplate. A new design, proposed in [247], introduced a locking mechanism featuring a toggle clamp and a self alignment plate. The impact of this design change has been assessed through experimental tests aimed at evaluating the duration of dismounting and mounting tasks of this component in the original and revised layout. The tests have been carried out on the same assembly: the RIB channel. Figure 6.15 shows the limit switch connection mechanisms available for the RIB channel: the old version (on the left) is based on M3 screws, whereas the new design (on the right) features a quick release toggle clamp.

Table 6.8 summarizes the descriptive statistics of the time required by the RIB channel limit switch dismounting and mounting tasks with the two designs. The complete test reports are available in Appendix C. The beneficial effect of the design optimization of the RIB channel limit switch connection mechanism on the time required for dismounting (left) and mounting (right) tasks are shown in Fig. 6.16.

As for the potentiometer, the benefits of the proposed design review go beyond the simple reduction of the replacement time. Indeed, the possibility to align the system off-line, along with the quick release clamp not requiring the manipulation of small screws makes this solution ideal to prevent potential installation errors. As clearly shown by the boxplot in Fig. 6.16, another positive impact of this fastening

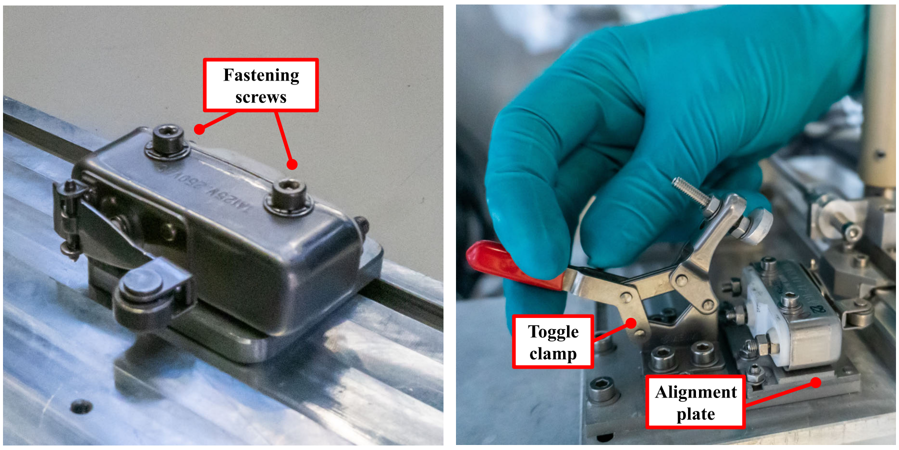


Figure 6.15: The limit switch fastening mechanisms: old design based on M3 screws (left), new design featuring a toggle clamp (right).

Task	Design	N	Mean	SE Mean	StDev	Variance	Minimum	Median	Maximum	Range
D	Old	18	28,56	1,09	4,60	21,20	20,00	29,50	37,00	17,00
	New	18	13,39	0,34	1,42	2,02	11,00	13,00	16,00	5,00
M	Old	18	42,78	2,42	10,28	105,59	25,00	43,50	67,00	42,00
	New	18	20,33	0,71	3,01	9,06	15,00	20,00	26,00	11,00

Table 6.8: Descriptive statistics of the Dismounting (D) and Mounting (M) tasks on the RIB channel limit switch with the old and new design. Time is given in [s].

method is the reduction of the variance of the samples. This is motivated by the decrease of the task complexity, in contrast with the existing procedure which is operator-dependent. The "old" and "new" datasets have been analyzed with the Levene's test. Given the significant result, equal variances are not assumed. The two-sample t test, have then been individually applied on the dismounting and mounting tasks, confirming the difference in the mean of the two samples. Overall, the revised mechanism enables the halving of the intervention time in both the mounting and dismounting task. In addition, the tool-free locking method prevents any potential mistakes in the positioning and securing of the limit switch on the Front-End. The obtained experimental results, and the subsequent statistical validation, supports the quality of the redesigned fastening mechanism.

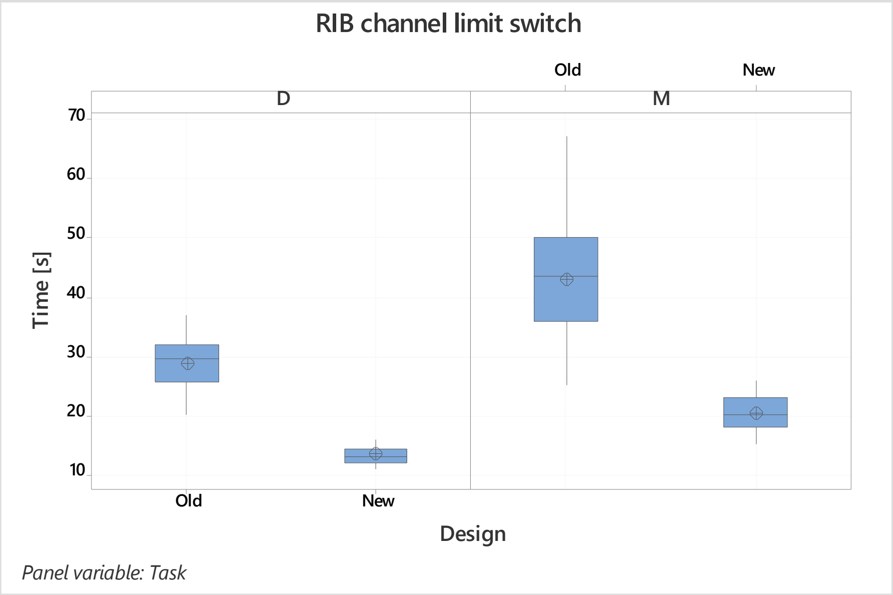


Figure 6.16: Boxplot comparing the duration of maintenance interventions on the PPB gate potentiometer using the old and new connection mechanisms: dismounting task (left), mounting task (right).

6.4.2.5 *Tool selection: pneumatic motor*

As an extension to the presented results, which are mainly related to the benefits provided by an optimization of the system design, this section describes a set of experimental tests devoted to the evaluation of the effect of using different tools to perform the same maintenance activity. In this experiment, the replacement of the PPB channel pneumatic motor has been considered as representative use case for the comparison between two different tools. Figure 6.17 shows the tools employed for the test: tool A (on the left) is a conventional hex key, whereas tool B (on the right) is a ratcheting hex driver. The test assembly has been selected among the Front-End motion axes due to its intrinsic layout. Indeed, the mechanical components surrounding the motor fastening clamp prevent the free rotation of a conventional hex key, requiring a series of additional screwing movements not required in other locations. In this case, the benefit of a ratcheting driver is especially evident since, once positioned, this tool will remain engaged for the duration of the operation. In contrast, the hex key must be constantly relocated.

Table 6.9 summarizes the descriptive statistics of the time required by the PPB channel motor dismounting and mounting tasks with the two tools. The complete test reports are available in Appendix C. Figure 6.18 shows the impact of the two tools on the duration of dismounting (left) and mounting (right) tasks for the PPB channel motor. Even if the difference between the two means is less evident than in the last experiment, it still represents an improvement of the working conditions. Indeed, the aim of the test was not to drastically reduced the intervention duration. Instead, the experiment was focused to show that the prior evaluation of the best operating conditions, including tools, working location, procedure, and so on, delivers measurable

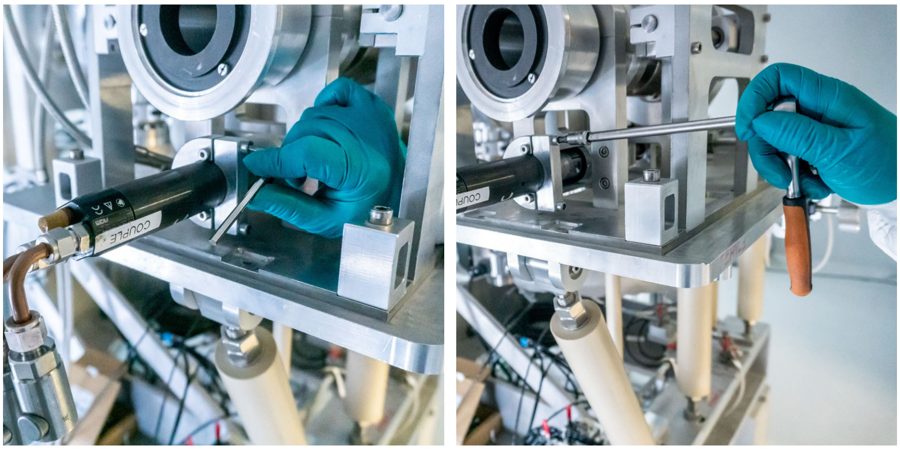


Figure 6.17: The tools that can be used to replace the PPB channel motor: (left) hex key, (right) ratcheting driver.

Task	Tool	N	Mean	SE Mean	StDev	Variance	Minimum	Median	Maximum	Range
D	A	18	28,56	1,21	5,11	26,14	23,00	27,00	40,00	17,00
	B	18	22,28	1,36	5,77	33,27	17,00	21,00	38,00	21,00
M	A	18	44,22	2,57	10,91	119,01	34,00	41,00	74,00	40,00
	B	18	31,22	1,73	7,34	53,95	23,00	28,00	50,00	27,00

Table 6.9: Descriptive statistics of the Dismounting (D) and Mounting (M) tasks on the PPB channel motor with tools A and B. Time is given in [s].

benefits in terms of reducing expected personnel exposure. In this regard, a further recommendation provided by operational feedbacks is to tape the driver bit to the key extension, this precaution actually prevents the bit from detaching during the intervention.

The "Tool A" and "Tool B" datasets have been analyzed with the Levene's test. Given the significant result, equal variances are not assumed. The two-sample t test, have then been individually applied on the dismounting and mounting tasks, confirming the difference in the mean of the two samples. This result, supports the choice of tool B as most suitable. Moreover, the analysis further emphasizes the important provided by the selection of the most suitable tools for the execution of a specific task during the definition of tailored maintenance procedures. As already mentioned, the decision-making process should take into account the constraints imposed by the specific operational site, along with the type of the intervention.

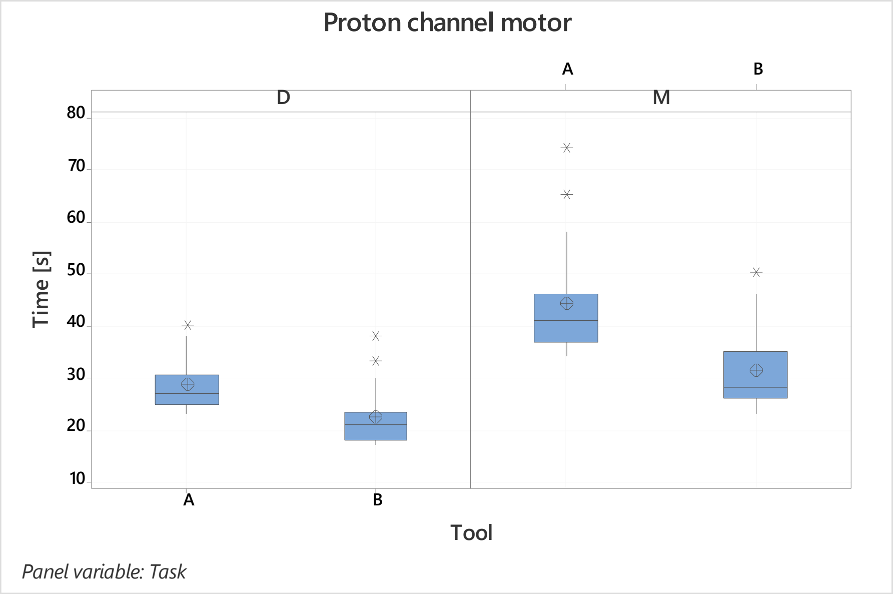


Figure 6.18: Boxplot comparing the duration of maintenance interventions on the PPB channel motor performed using tools A and B: dismounting task (left), mounting task (right).

6.4.3 *Survey session*

This section describes the collected data and key findings of a comprehensive experimental campaign designed to accurately estimate the duration of a selection of safety-critical maintenance tasks carried out on the SPES Front-End under severe radiological conditions. The components considered during the maintenance tests are the pneumatic motors, linear potentiometers and limit switches installed on the five Front-End motion axes, namely:

- Proton Channel (PC)
- RIB Channel (RC)
- Proton Gate (PG)
- RIB Gate (RG)
- extraction ELectrode positioning system (EL)

The operators performed a randomized set of trials in which the component type, assembly and type of task are mixed to prevent any potential bias on the collected data. Each of the analyzed tasks (dismounting or mounting) has been replicated two times.

In the following, the experiments are grouped according to the component type. Following the experimental tests, the collected data are analyzed to identify the key factors affecting the task duration. Since, for a specific pair task-component, the intervention procedure is the same, any difference in the execution time can be attributed to environmental conditions linked to the specific assembly in which the component is installed. In the presented statistical analysis a linear regression model has been applied for each class of component. Considering the intervention duration as response variables, the terms of the model have been selected among the different continuous and categorical predictors, including interactions up to order 2. The identified linear regression model has been calculated considering a 95% confidence interval. Significant model terms are selected through a stepwise backward elimination process (α to remove: 0.05). The standardized effects of the different terms have been evaluated thanks to the Pareto chart. Finally, residual plots have been analyzed to confirm the fulfillment of the linear model assumption, i. e.:

- Linearity: the relationship between X and the mean of Y is linear;
- Independence: observations are independent of each other;
- Normality: for any fixed value of X, Y is normally distributed;
- Homoscedasticity: the variance of residual is the same for any value of X.

6.4.3.1 *Pneumatic motors*

The first component considered in the experimental tests is the pneumatic motor in charge of the positioning of the different Front-End motion axes. The campaign involved 10 operators, performing Mounting (M) and Dismounting (M) tasks on pneumatic motors installed in 5 assemblies. Each test has been replicated twice. A pneumatic motor installed on the SPES Front-End is depicted in Fig. 6.19.

Considering the mounting task as an example, the operator enters the ISOL hall grabbing the motor and the appropriate tool (a ratcheting driver). Once reached the working location, the motor is positioned on the assembly and properly oriented. The supply pipes are then coupled with motor connectors, and the fastening clamp screws are tightened before the operator can quit the area. Table 6.10 summarizes the descriptive statistics of the time required by the pneumatic motor mounting task throughout the different subsystems on the SPES Front-End, whereas a graphical comparison of the task duration across the Front-End motion axes is provided by the boxplot in Figure 6.20.

In the dismounting task the sequence of actions is reversed: the operator first disconnects the supply pipes and then opens the clamp, removing the motor and quitting the area. The descriptive statistics of motor dismounting tasks duration throughout the different Front-End assemblies are reported in Table 6.11. Additionally, a visual overview of the differences between the interventions is provided by the boxplot in Fig. 6.21. As clearly visible, the dismounting task is briefer than the mounting process in every considered assembly. This result is motivated by the simplified procedure, which does not include the motor correct orientation. Additionally, during the mounting intervention, the operator has to look for flexible pipes, which are not always positioned properly.

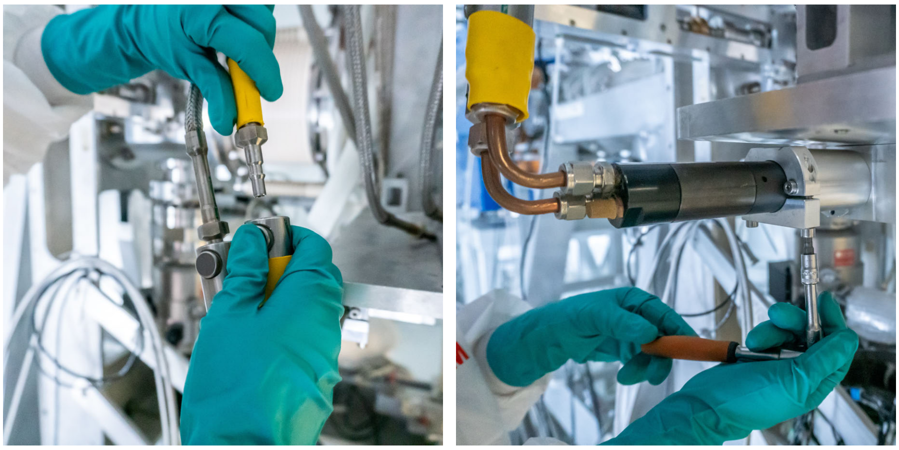


Figure 6.19: Pneumatic motor installed on the SPES Front-End; (left) unplugging of the pneumatic connections, (right) opening of the fastening clamp.

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

Table 6.10: Descriptive statistics of mounting tasks duration of the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG) pneumatic motors. Time is given in [s].

A linear regression model has been applied to the complete dataset related to motor dismounting and mounting tasks. As preliminary operation, the few included outliers have been excluded from the sample. Subsequently, independent continuous and categorical predictors have been included as potential model terms considering also the interactions up to order 2. The stepwise backward elimination of terms allowed for the narrowing of the model considering only the most significant relationship, the α to remove is 0.05. The identified model features a 95% confidence interval. On the Pareto chart showed in Fig. 6.22, bars that cross the reference line (at 1.97) represent the statistically significant terms of the model.

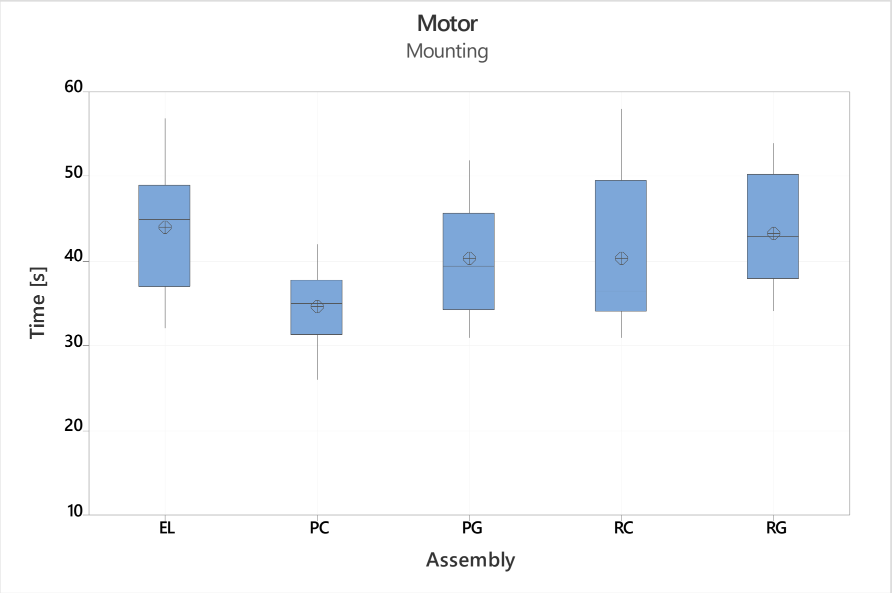


Figure 6.20: Boxplot of the time required for the pneumatic motor mounting on the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG)

Assembly	N	Mean	SE Mean	St Dev	Variance	Min.	Median	Max.	Range
EL	20	31.05	1.69	7.54	56.89	25.00	29.00	59.00	34.00
PC	20	23.40	0.85	3.82	14.57	17.00	22.50	32.00	15.00
PG	20	31.00	1.26	5.62	31.58	22.00	30.50	43.00	21.00
RC	20	30.30	1.59	7.12	50.75	22.00	29.00	49.00	27.00
RG	20	35.60	1.59	7.10	50.36	23.00	34.50	47.00	24.00

Table 6.11: Descriptive statistics of dismounting tasks duration of the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG) pneumatic motors. Time is given in [s].

The residuals plot displayed in Fig. 6.23 confirms the assumption of the linear regression model, namely: linearity, statistically independence, normal distribution and homogeneity of residuals variance.

Because the Pareto chart displays the absolute value of the effects, this tool can be used to determine which effects are larger. Aside from the task type, which represent an obvious term of the model, the second higher magnitude in Fig. 6.22 is provided by the component *Height*. This outcome is related to specific motion axes necessitating a ladder to let the operator reach the pneumatic motor installed at a 2.2 m height, see Fig. 6.24 (left). Since ladder opening, closing and climbing are time-consuming operations, whenever possible, components should be positioned at the standing reach level.

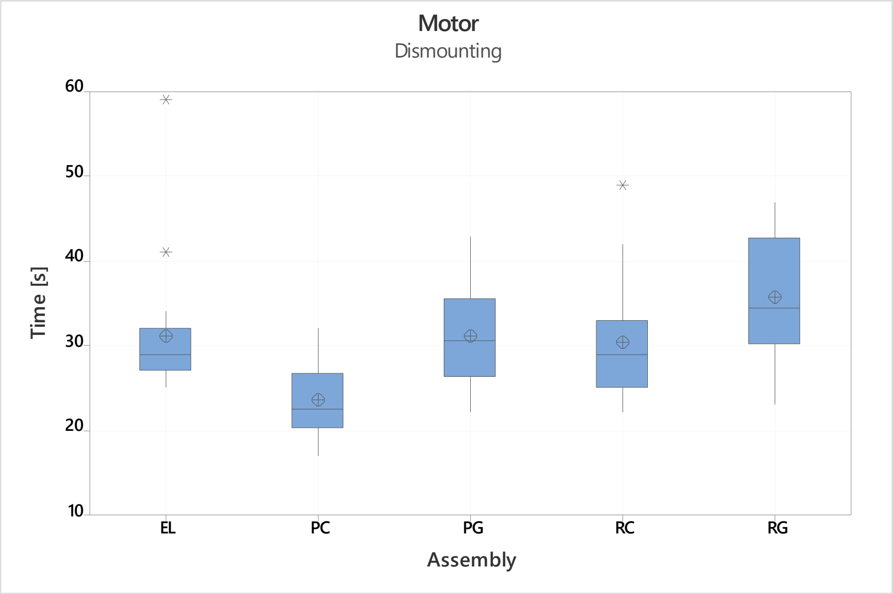


Figure 6.21: Boxplot of the time required for the pneumatic motor dismounting on the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG).

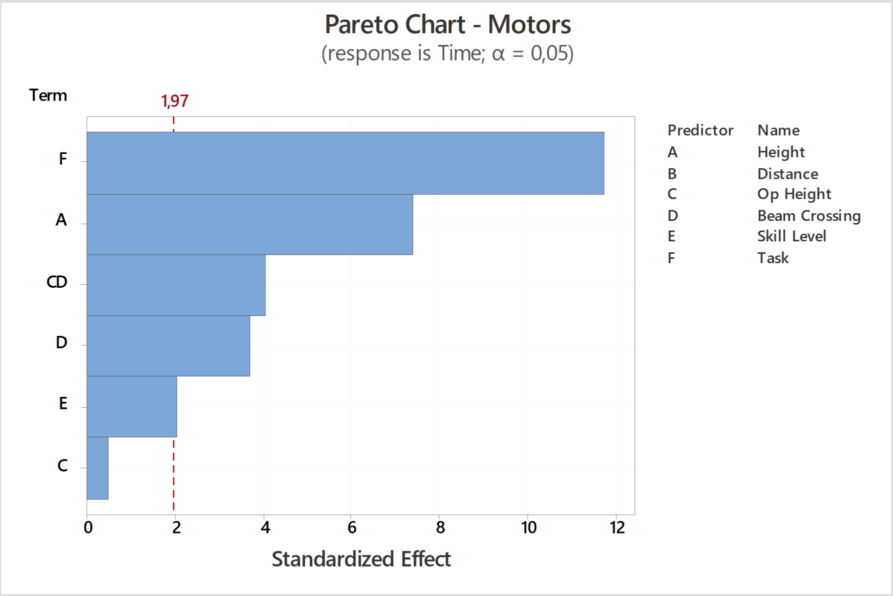


Figure 6.22: Pareto chart of the pneumatic motor replacement tasks: dismounting and mounting.

The *Beam Crossing* term represents the need, for a specific task, to cross the PPB line by passing through a narrow gap on the left side of the SPES Front-End. Despite being identified as a relevant term, the Variance Inflation Factor (VIF) shows a significant correlation with at least another independent variable. It is the case of the *Operator Height*. While this term is not relevant when considered alone, it provides a statistically relevant contribution when combined with

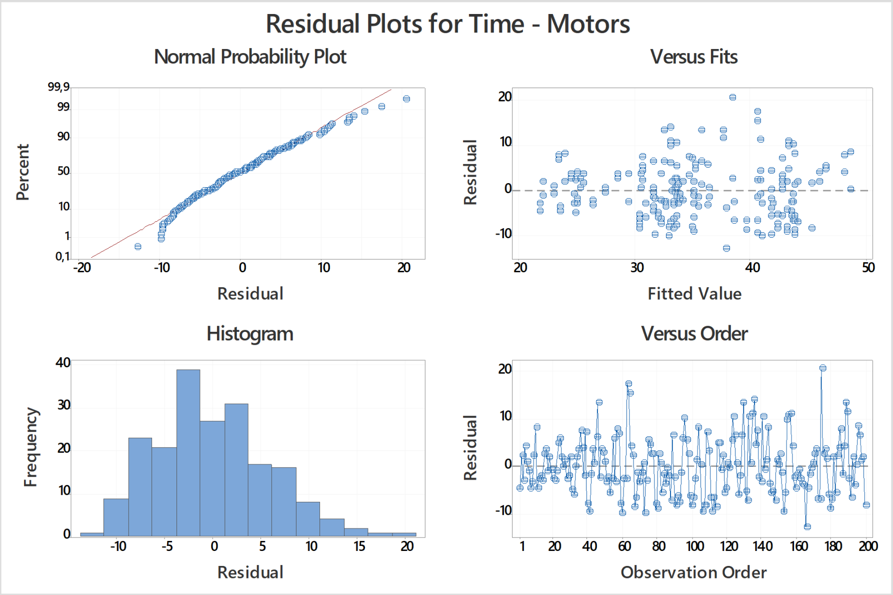


Figure 6.23: Residual plots of the pneumatic motor replacement tasks: dismounting and mounting.

the *Beam Crossing* factor. Experimentally, this correlation was evident by the difficulty of taller operators in passing through the narrow space below the PPB line, see Fig. 6.24 (right). This important finding strongly support the need for the components to be installed on the right side of the RIB line, where the accessibility is improved. Although this indication becomes useful for future design optimizations, it can also be considered as additional experimental evidence in favor of the design revision of the EEPS presented in Section 5.3.2 aimed at the mirroring of the motion axis layout.

The last significant factor which affects the pneumatic motor replacement duration is the operator *Skill Level*. An in-depth analysis shown that, while there is no significant difference between the *Beginner* and *Competent* levels, interventions performed by *Expert* operators are generally shorter. Indeed, the motor replacement tasks include some manual activities (e. g. screwing) which are operator-dependent. This result further emphasizes the importance of establishing a comprehensive training program that allows operators to practice on dedicated (and realistic) mock-ups.

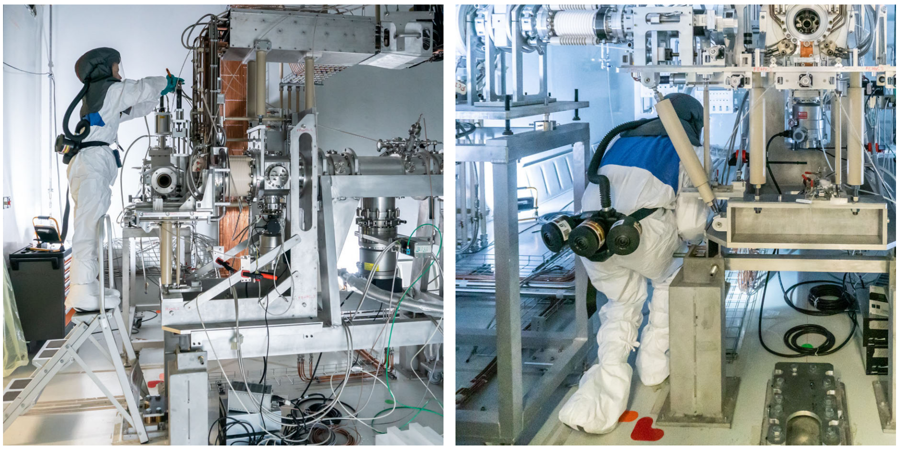


Figure 6.24: An operator using a ladder to reach the RIB gate pneumatic motor (left), an operator crossing the PPB line to reach the components installed on the left RIB side (right).

6.4.3.2 *Potentiometers*

As second component under examination, the experimental tests have been focused on the linear potentiometers installed on the Front-End motion axis diagnostics to detect the actual system position, the component is visible in Fig. 6.25. As in the previous case, the experiment has been performed testing the Dismounting (D) and Mounting (M) tasks on 5 assemblies employing 10 operators replicating each test for two times in a randomized order.

In the mounting activity, the operator enters the ISOL hall, reaches the working position, and install the component on the specific motion assembly. Following the proper positioning of both the potentiometer body and the shaft tip, the locking of a toggle clamp secures the component. The last step to perform is the connection of the potentiometer cable by inserting the connector on the specific panel-mounted socket. At this point, the operator quits the area. Table 6.12 summarizes the descriptive statistics of the time required by the potentiometer mounting task throughout the different subsystems on the SPES Front-End, whereas a graphical comparison of the task duration across the Front-End motion axes is provided by the boxplot in Fig. 6.26

In the dismounting task the sequence of actions is reversed: the operator first decouples the signal connectors and then releases the toggle-clamp, removing the potentiometer and quitting the area. The descriptive statistics of potentiometer dismounting tasks duration throughout the different Front-End assemblies are reported in Table 6.13. Additionally, a visual overview of the differences between the interventions is provided by the boxplot in Fig. 6.27. The prior experiment showed that the pneumatic motor dismounting task was significantly shorter than the mounting task. The difference is less pronounced, but still noticeable, for the potentiometer.

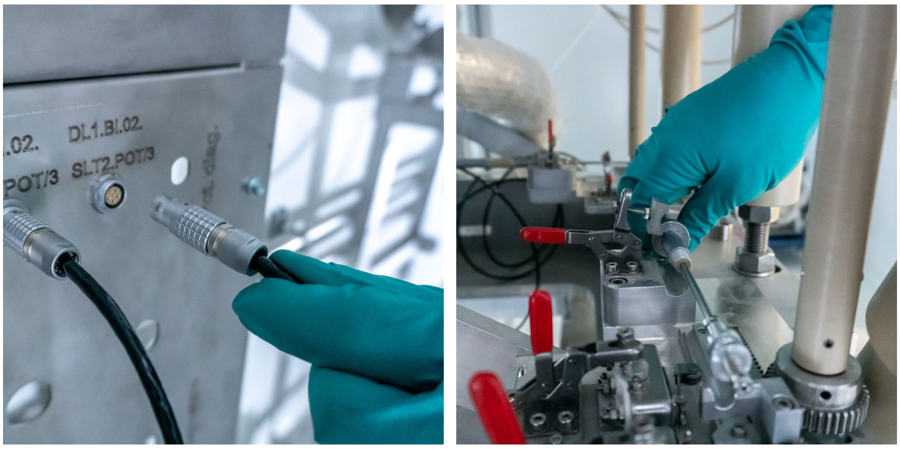


Figure 6.25: Linear potentiometer installed on the SPES Front-End; (left) unplugging of the electrical connector, (right) releasing of the toggle clamp.

Assembly	N	Mean	SE Mean	St Dev	Variance	Min.	Median	Max.	Range
EL	20.00	26.20	0.96	4.31	18.59	21.00	25.00	37.00	16.00
PC	20.00	19.70	0.71	3.18	10.12	14.00	19.50	26.00	12.00
PG	20.00	29.80	1.48	6.60	43.54	23.00	27.00	53.00	30.00
RC	20.00	19.75	0.67	2.99	8.93	16.00	19.00	28.00	12.00
RG	20.00	28.40	1.38	6.16	37.94	20.00	28.00	40.00	20.00

Table 6.12: Descriptive statistics of mounting tasks duration of the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG) potentiometers. Time is given in [s].

A linear regression model has been applied to the complete dataset related to potentiometer dismounting and mounting tasks. As preliminary operation, the existing outliers have been excluded from the sample. In a second phase, continuous and categorical predictors have been included as independent model variables, considering interactions up to order 2. A stepwise backward elimination of terms (α to remove: 0.05) has then enabled the reduction of the model terms taking into account only the most meaningful relationship resulting in a 95% confidence interval. The Pareto chart in Fig. 6.28 shows the statistically significant model terms as the bars that cross the reference line (at 1.97). The residuals plot in Fig. 6.29 confirms the fulfillment of the linear regression model assumptions: linearity, statistically independence, normal distribution and homogeneity of residuals variance.

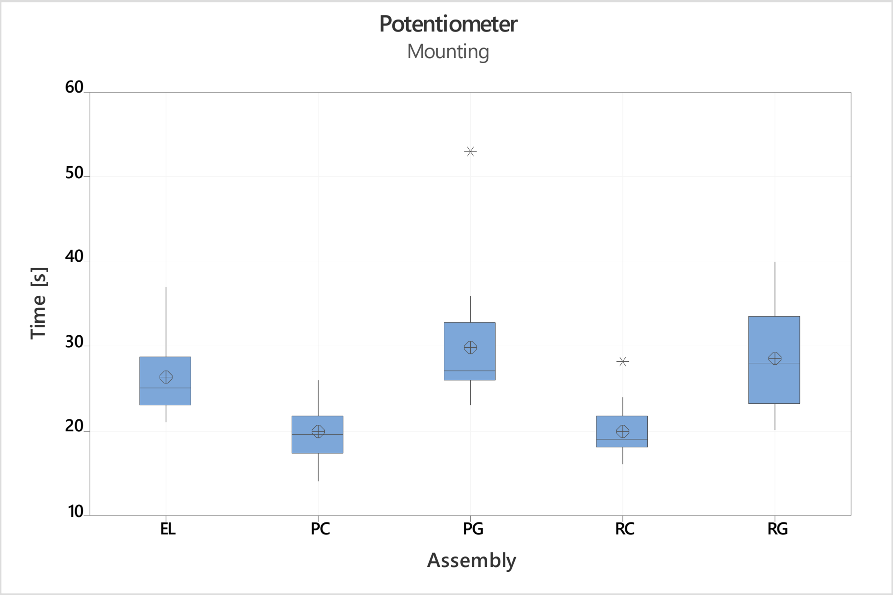


Figure 6.26: Boxplot of the time required for the potentiometer mounting on the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG).

Assembly	N	Mean	SE Mean	St Dev	Variance	Min.	Median	Max.	Range
EL	20.00	26.50	2.17	9.70	94.16	17.00	26.00	59.00	42.00
PC	20.00	14.00	0.33	1.49	2.21	12.00	13.50	17.00	5.00
PG	20.00	22.35	0.88	3.95	15.61	16.00	23.00	32.00	16.00
RC	20.00	14.20	0.56	2.53	6.38	10.00	14.00	21.00	11.00
RG	20.00	17.80	0.58	2.61	6.80	12.00	18.00	22.00	10.00

Table 6.13: Descriptive statistics of dismounting tasks duration of the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG) potentiometers. Time is given in [s].

As in the previous case, the *Task* impact on the intervention duration is pretty evident. Still, the *Distance* term assumes a statistical relevance when considering the potentiometer replacement. This effect is due to the overall briefness of the interventions compared with the motor mounting and dismounting tasks.

The *Beam Crossing* and *Operator Height* terms provide, also in this case, a non-negligible impact on the task duration. Again, the second term itself is not enough to cross the threshold. Conversely, it becomes significant when combined with the need for crossing the PPB line.

On the SPES Front-End all the potentiometers are installed below the height of 2 m, this means that their replacement can be performed without the use of a ladder.

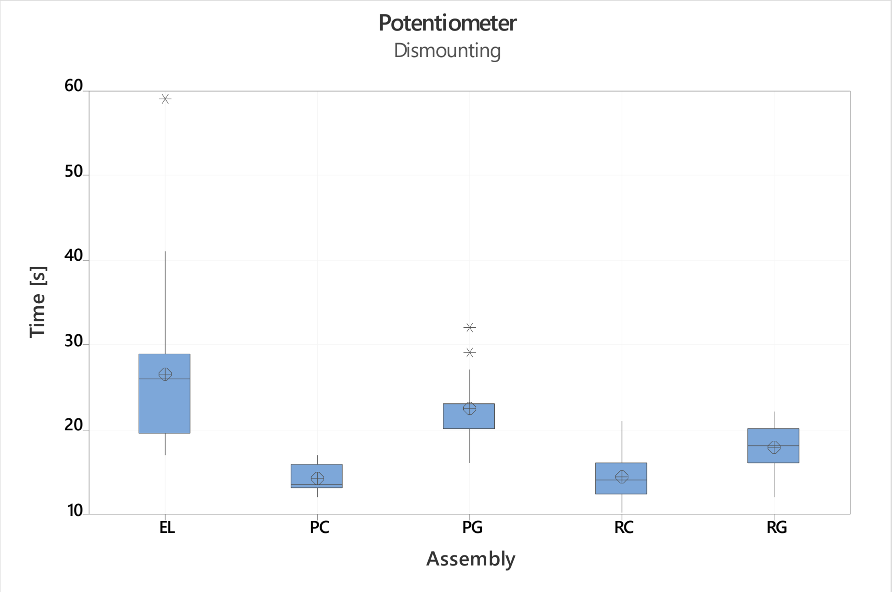


Figure 6.27: Boxplot of the time required for the potentiometer dismounting on the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG).

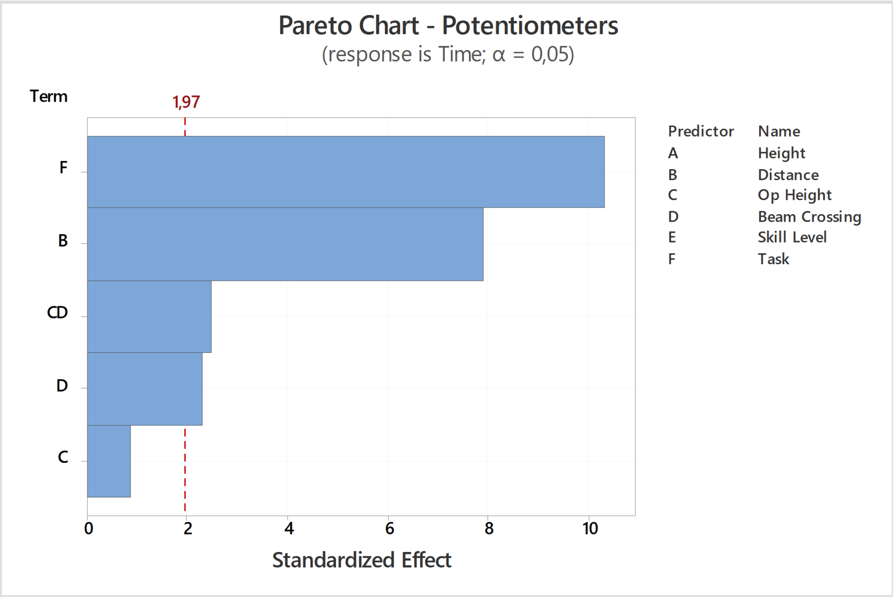


Figure 6.28: Pareto chart of the potentiometer replacement tasks: dismounting and mounting.

Looking at Fig. 6.28, this aspect is confirmed by the absence of the component *Height* among the significant terms of the model.

One last consideration is related to the *Skill level* factor, which is not included among the significant terms of the linear regression model. This specific finding strongly confirms the goodness of the redesigned potentiometer fastening mechanism proposed in [247] as an effective tool which simplifies the task execution and reduces the task variance.

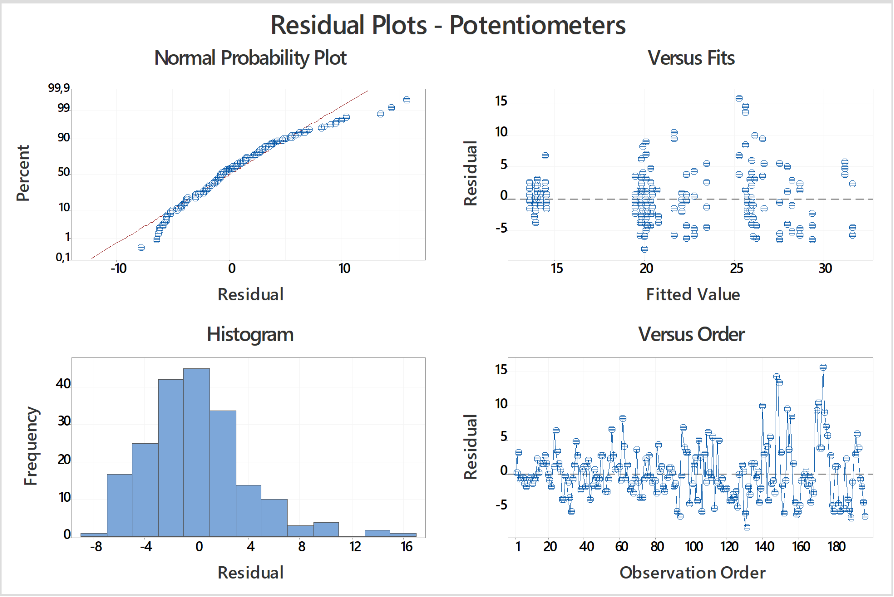


Figure 6.29: Residual plots of the potentiometer replacement tasks: dismounting and mounting.

6.4.3.3 *Limit switches*

The Front-End limit switches have been considered as the focus of a third experimental test, aimed at collecting the Dismounting (D) and Mounting (M) task duration for these components, which are used as diagnostic devices to detect the stroke ends of the motion axes dedicated to the TIS unit coupling and decoupling. The experiments involved 10 operators, repeating the tasks for two non-consecutive replicates among 4 assemblies within a randomized set of runs. In this case, the EEPS has not been considered due to the different type of implemented installation. An example of limit switch installed on the SPES Front-End is depicted in Fig. 6.30.

During the mounting activity, the operator approaches the Front-End and reaches the working site. The first step is the positioning of the limit switch on the specific motion assembly, the switch is already pre-mounted on a self alignment plate. The device is then secured using by locking a toggle clamp. Subsequently, the limit switch cable is connected to the corresponding signal connector and the operator can quit the zone. Table 6.14 summarizes the descriptive statistics of the time required by the limit switch mounting task throughout the different subsystems on the SPES Front-End, whereas a graphical comparison of the task duration across the Front-End motion axes is provided by the boxplot in Figure 6.31.

The dismounting task procedure requires carrying out the actions in reverse order. Specifically, the cable-mounted limit switch connector needs to be disconnected first, and then, in a second phase, the limit switch can be retrieved by releasing the locking clamp. The descriptive statistics of limit switch dismounting tasks duration throughout the different Front-End assemblies are reported in Table 6.15. Moreover, a clear visualization of the differences between the two interventions is provided by the boxplot in Fig. 6.32.

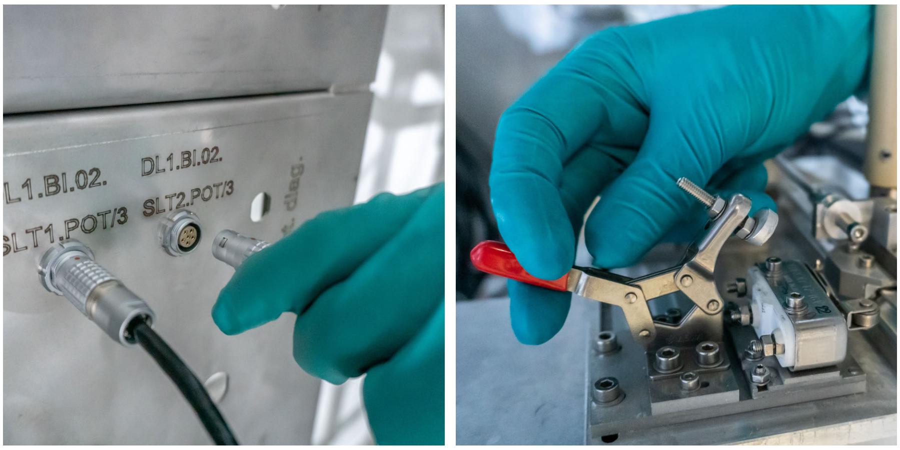


Figure 6.30: Limit switch installed on the SPES Front-End; (left) unplugging of the electrical connector, (right) releasing of the toggle clamp.

Assembly	N	Mean	SE Mean	St Dev	Variance	Min.	Median	Max.	Range
PC	20.00	18.05	0.75	3.36	11.31	14.00	17.50	28.00	14.00
PG	20.00	28.00	1.43	6.42	41.16	21.00	26.50	46.00	25.00
RC	20.00	16.40	0.61	2.72	7.41	13.00	16.00	23.00	10.00
RG	20.00	24.45	1.21	5.43	29.52	19.00	23.50	43.00	24.00

Table 6.14: Descriptive statistics of mounting tasks duration of the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG) limit switches. Time is given in [s].

Following the experimental phase, a linear regression model has been applied to the complete dataset related to limit switches dismounting and mounting tasks. As preliminary operation, outliers have been eliminated from the sample. Then, a set of independent variables have been included as potential model terms considering also the interactions up to order 2. The stepwise backward elimination of terms (α to remove is 0.05) enabled an optimization of the model which takes into account only the most significant relationship featuring a 95% confidence interval. Figure 6.33 shows the Pareto Chart of Limit Switches. Factors crossing the reference line (at 1.98) constitutes the model's terms with a statistical significance.

Figure 6.34 displays the residuals plot of the identified linear regression model. Through a graphical analysis it is possible to confirm the validity of the model assumptions in terms of linearity, independence, normality and homoscedasticity of residuals.

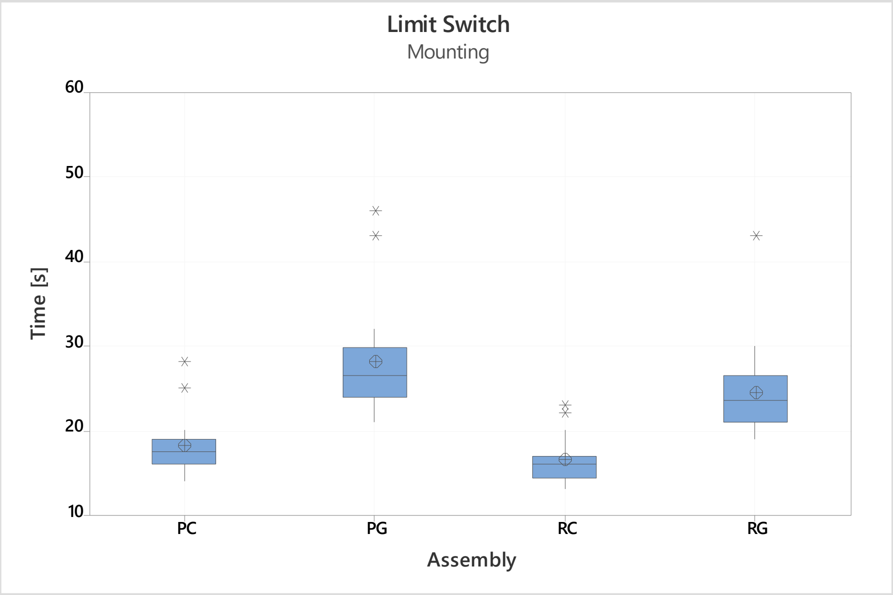


Figure 6.31: Boxplot of the time required for the limit switch mounting on the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG).

Assembly	N	Mean	SE Mean	St Dev	Variance	Min.	Median	Max.	Range
PC	20.00	13.75	0.43	1.92	3.67	11.00	13.50	18.00	7.00
PG	20.00	21.35	0.80	3.57	12.77	17.00	20.50	31.00	14.00
RC	20.00	12.65	0.27	1.23	1.50	10.00	13.00	15.00	5.00
RG	20.00	14.80	0.43	1.94	3.75	12.00	15.00	18.00	6.00

Table 6.15: Descriptive statistics of dismounting tasks duration of the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG) limit switches. Time is given in [s].

The primary significant term of the regression model, as in the other examples, is the *Task* type. This result can be directly related to the different procedural steps in the mounting and dismounting activities.

As second term, the combined effect of *Beam Crossing* and *Operator Height* provides a relevant contribution to the task length. As already discussed, passing through the narrow space below the PPB line represents a challenging task for tall operators.

The boxplots outlined in Fig. 6.31 and Fig. 6.32 clearly show how the limit switch mounting and dismounting tasks are rapid activities. Since the on-site task duration is reduced, as in the potentiometer case, the *Distance* of the assembly from the operator starting position emerges as a statistically significant term within the linear regression model.

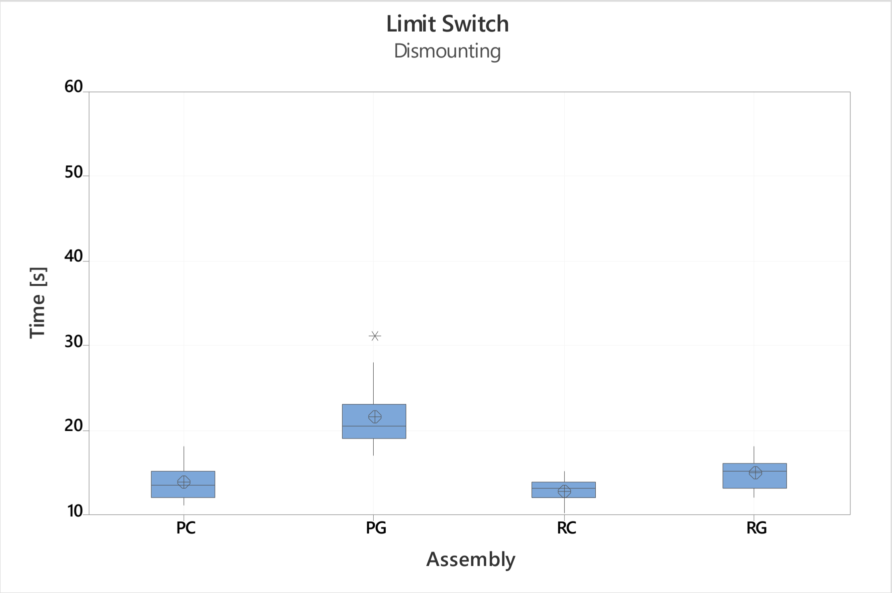


Figure 6.32: Boxplot of the time required for the limit switch dismounting on the Extraction Electrode (EL), Proton Channel (PC), Proton Gate (PG), RIB Channel (RC), RIB gate (RG).

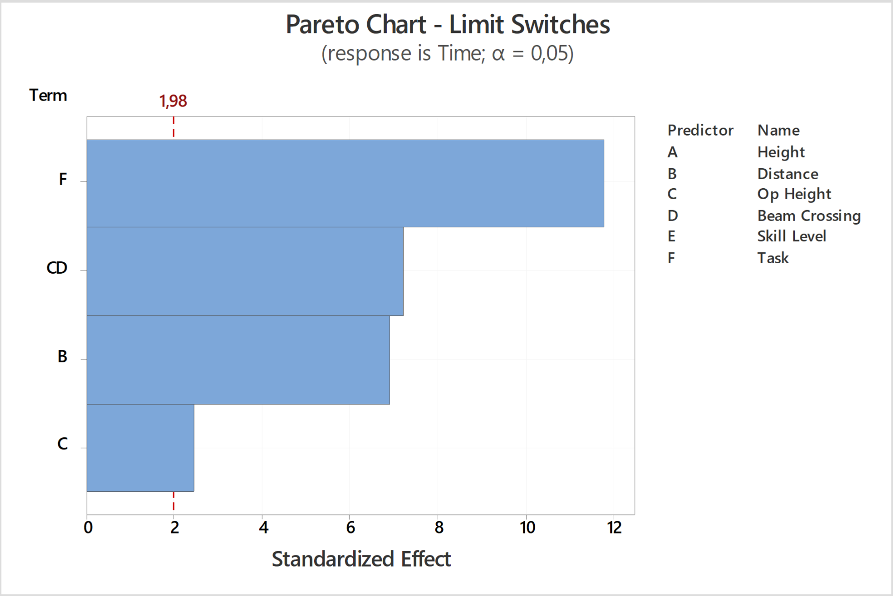


Figure 6.33: Pareto chart of the limit switch replacement tasks: dismounting and mounting.

Last but not least, since the RG and PG limit switches are installed at a height of 1.9 m and the components position is not so accessible, the duration of the interventions of some operators may be affected. This aspect is reflected by the term component *Height*. Indeed, the rapid nature of the task further emphasize the other terms, which are less relevant in more complex activities.

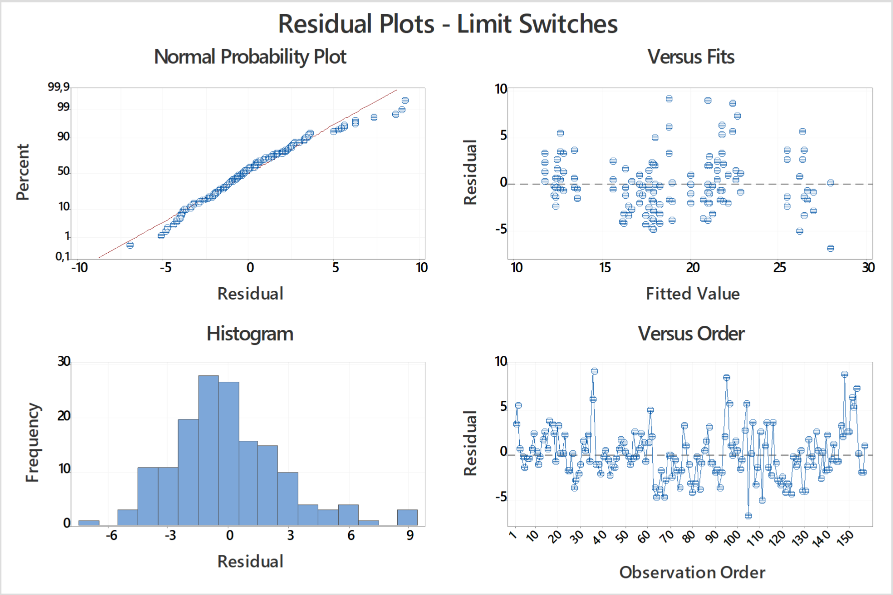


Figure 6.34: Residual plots of the limit switch replacement tasks: dismounting and mounting.

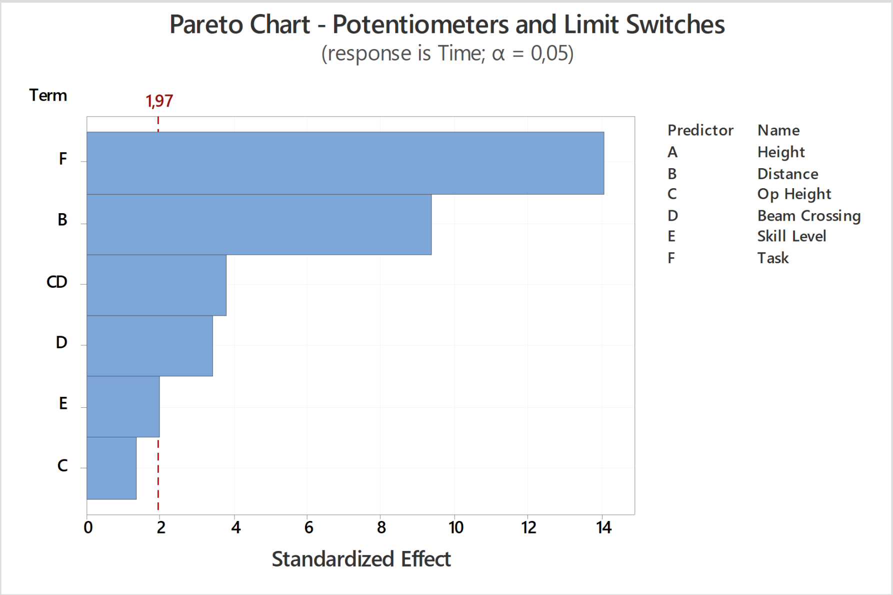


Figure 6.35: Pareto chart of the potentiometer and limit switch replacement tasks: dismounting and mounting.

Since the limit switches and the linear potentiometers feature the same type of mechanical and electrical connection strategy, a linear regression model has been implemented on a combined dataset which includes experiments on both components. From the analysis of Pareto Chart in Fig. 6.35 and of residuals plot in Fig. 6.36 it can be seen that the abovementioned considerations can be generalized. Specifically, the study shows how the fastening mechanism design optimization,

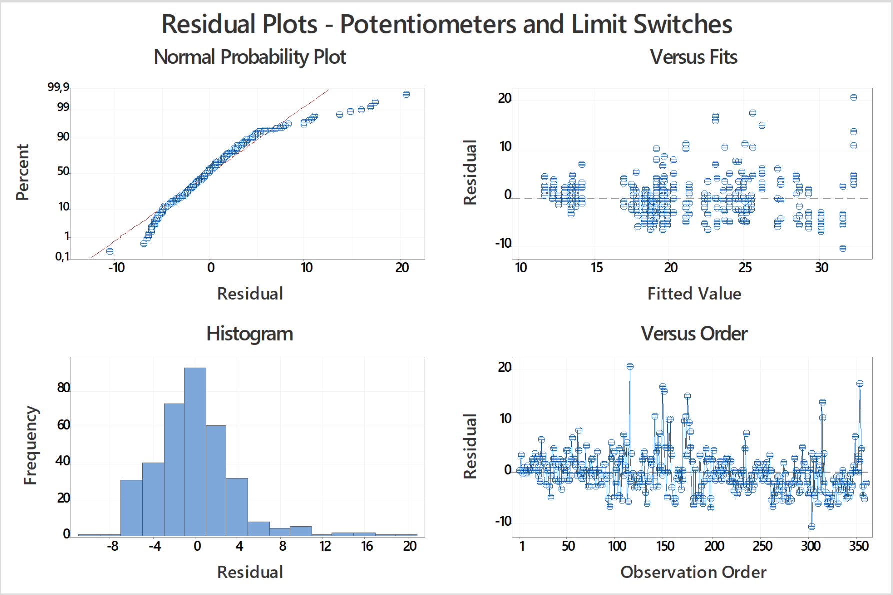


Figure 6.36: Residual plots of the potentiometer and limit switch replacement tasks: dismounting and mounting.

based on a tool-free approach, allows to minimize the dependency of maintenance activities duration from the operator skill level. Moreover, installing hardware components within the standing reach limit has the advantage of avoiding the use of ladder, which has been shown to be a time-consuming additional operation.

6.4.3.4 *Extraction electrode*

The last maintenance activities evaluated during the survey session are related to the dismounting and mounting of the extraction electrode. The replacement of this component, unlike previous case, shall take into account the significant radiological impact of this element [227]. For this reason, specific tools have been designed to mitigate the risk of the operation. The Dismounting (D) and Mounting (M) tasks have been performed by 10 operators with two randomized replicates.

The extraction electrode is located along the RIB line, facing the TIS unit. A custom gripping tool has been designed to enable the removal of the component, which is connected to the Front-End through a bayonet fitting, while maintaining a distance from the source of about 2 m. Figure 6.37 depicts the tools and the procedure implemented for the extraction electrode removal.

To remove the extraction electrode, the RIB shutter should be opened and the EEPS should move out the holder till the end position. Following this preliminary stage, the operator disconnect the extraction electrode from the holder using the manual gripping tool. In a second step, the exhausted electrode is secured within a shielded storage box. Finally, using the same gripping tool, the box is closed with a shield. The complete disconnection procedure is reported in Fig. 6.6.

When SPES will be in operation, planned maintenance activities will be performed during yearly Technical Stops (TSs). The ALARA principles requires to minimize the environmental dose rate prior

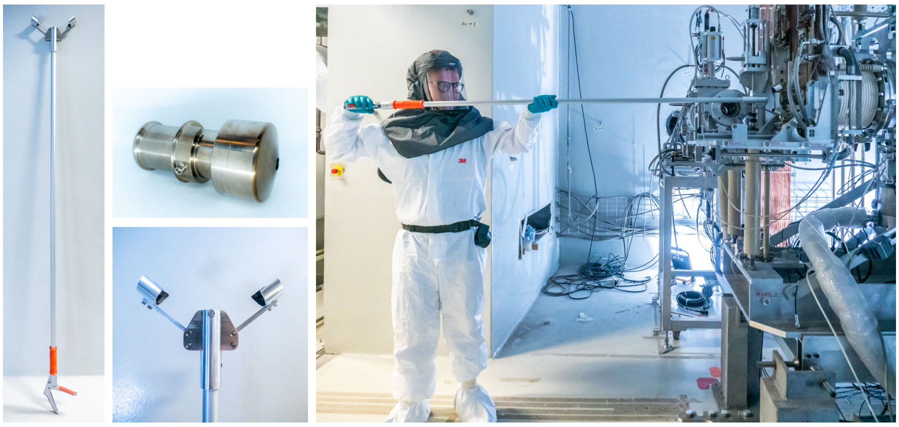


Figure 6.37: The extraction electrode manual gripper (left), an operator removing the electrode during the Front-End maintenance tests (right).

Task	N	Mean	SE Mean	St Dev	Variance	Min.	Median	Max.	Range
D	20	29,950	0,933	4,174	17,418	20,000	30,000	36,000	16,000
M	20	21,900	0,764	3,417	11,674	14,000	22,000	29,000	15,000

Table 6.16: Descriptive statistics of extraction electrode dismounting and mounting tasks. Time is given in [s].

to any intervention. To reach this goal, the two primary radioactive source within the ISOL hall should be displaced. Specifically, while the TIS unit is removed by the HHM, the extraction electrode should be taken away and properly stored following the described procedure.

The experimental tests also included the mounting task, which is performed with a similar procedure: the operator grasp a clean electrode with the gripping tool and install it on the Front-End electrode holder keeping a 2 m distance from the machine. Table 6.16 summarizes the descriptive statistics of the time required by extraction electrode Dismounting (D) and Mounting (M) tasks on the SPES Front-End, whereas Fig. 6.38 compares the boxplot of the tasks duration.

As clearly visible, the mounting task is shorter than the dismounting operation. This is motivated by the additional storage closing phase which is required after the electrode removal but not for the clean electrode installation. Despite the employment of optimized tools and procedures provides significant benefits on the limitation of the task duration, a completely automatic RH solution is currently under development. This additional option will be tested and compared with the manual procedure as a future research step.

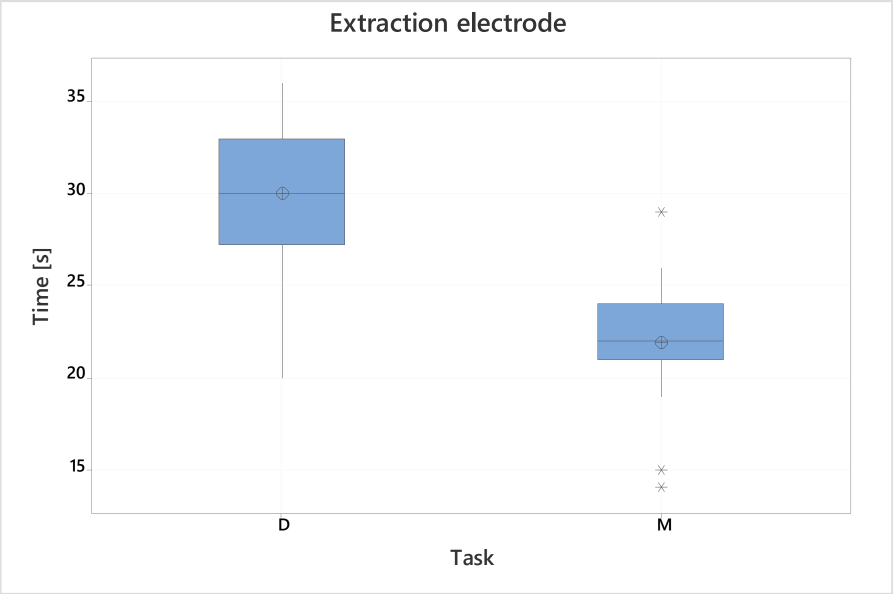


Figure 6.38: Boxplot of the time required for the extraction electrode Dismounting (D) and Mounting (M) tasks.

6.5 CONCLUSIONS

In this chapter, a comprehensive assessment of the SPES Front-End maintenance activities has been presented. The study enabled the review of the upkeep tasks with a significant expected radiological impact and the evaluation of potential design optimizations aimed at mitigate the residual risk introduced by hands-on interventions.

In relation to the objectives outlined in Section 6.1, the analysis delivered a set of significant results, such as:

- the identification and correction of system vulnerabilities according to operational feedbacks;
- the definition of standardized operating procedures aimed at prevent potential errors and help the operators during the task execution;
- the validation of different design optimization through dedicated comparison experiments, which confirmed the statistical impact of the introduced review;
- the identification of most significant factors which influence the maintenance tasks duration, in order to provide clear guidelines for future re-engineering of critical components;
- the collection of intervention data for the estimation of task duration.

The study's outcomes enrich and update earlier research. Specifically, the correction of design weaknesses extends the RH systems consolidation process discussed in Chapter 3. Moreover, the development of standard protocols and the collection of visual material are fundamental steps towards the establishment of a solid operator training program, as suggested by the PRA in Chapter 4. Finally, the experimental validation of novel design concepts and the identification of the factors impacting the intervention duration represent valuable assets for the optimization of the design of critical components, as the one discussed in Chapter 6. Indeed, the study highlighted how improved fastening techniques can reduce task duration variance, resulting in a more accurate estimation of the intervention's time.

A limitation of the research is the missing integration of the time duration and working position data with the environmental dose rate estimated in different configurations. Future research steps will address this challenge, allowing for the development of accurate Work and Dose Plannings (WDPs) for each maintenance intervention taking advantage of the collected data. The dose estimation would provide several benefits, serving as a useful tool for maintenance organization, enabling a more accurate estimation of the severity associated with HAZOP failure scenarios, and permitting a quantitative assessment of the design optimization effects in terms of saved personnel dose. An alternative research domain might focus on incorporating other components installed in the SPES ISOL hall within the maintenance assessment, likely including a wider range of runs and operators to enrich the sample size. Lastly, while this study focused on conventional maintenance procedures, forthcoming investigations would also examine the manual recovery scenarios proposed in Chapter 4.

In addition to the evident advantages provided for the development of the SPES plant, the described process successfully illustrates the positive impact that a proactive approach to maintenance activities in radioactive environments has on reducing personnel exposure during residual hands-on interventions. This general result can support the early integration of maintenance assessment studies in other facilities as an alternative to the traditional on-demand strategy.

Part IV

VERIFICATION

7 IEC 61499 REMODELING AND FORMAL VERIFICATION OF THE HHM CONTROL SOFTWARE

7.1 INTRODUCTION

Automation systems in nuclear laboratories must comply with strict safety requirements to avoid any potential risk to personnel or equipment. The critical operating environment generally discourages innovation in the design of control software, leading to an old-fashioned approach still today in the Industry 4.0 era. However, the introduction of distributed control systems based on modern standards would be advantageous for operational and safety challenges. This paradigm shift will lead to the development of smarter systems based on flexible and reconfigurable automation architectures. In this context, the evolution from applications based on IEC 61131-3 [255] towards IEC 61499 [79, 256] solutions would provide key tools to face the design and verification challenges typical of complex distributed control systems. The main advantages of this migration include:

- Flexible, reconfigurable, and scalable architecture;
- Modular design, standardized Function Blocks;
- Simulations, offline and online verification;
- Formal model-checking techniques.

Since its conception as a safety-critical automation system, the HHM hardware architecture has been designed using a safety-driven approach. A comprehensive overview is available in Chapter 3, while the system is depicted in Fig. 7.1. From the operational perspective, the most dangerous remote handling failures conditions have been assessed in a dedicated PRA, described in Chapter 4. The study enabled the identification and validation of the IPLs required to meet the desired safety standards for the SPES facility. Specifically, safety, reliability, and robustness have been highlighted as key requirements of the control software of Safety-Critical Control System (SCCS) [122]. In this context, software formal verification can reduce the risk of system failures, potentially leading to unintended maintenance interventions within high-radiation areas.

The SPES facility can be considered an attractive use case to demonstrate the advantages of implementing SCCS based on IEC 61499. Indeed, RH systems involved in the TIS unit replacement procedure face an intense radiation field.

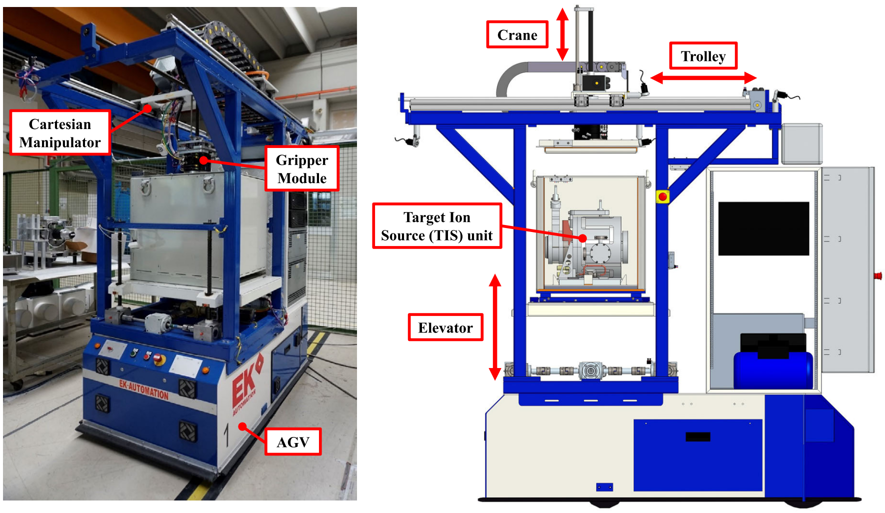


Figure 7.1: (left) the actual HHM, (right) view of the HHM motion axes.

Operational safety is the outcome of an integrated strategy that combines the formal verification of control software with the deployment of inherently safe design principles to the hardware. This chapter describes the development of flexible and reconfigurable control software based on IEC 61499, along with its formal verification through an integrated tool-chain. The study focuses on the most critical remote handling task: the automated removal of a radioactive TIS unit from the SPES Front-End using the HHM.

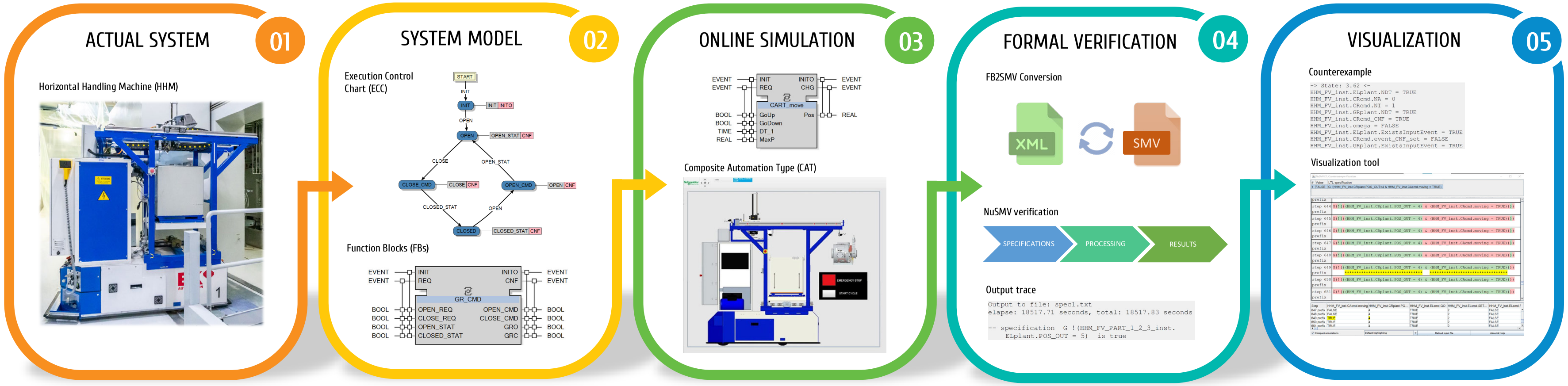
The proposed methodology addresses the challenge of verifying and analyzing Function Blocks (FBs) implemented in the IEC 61499 standard by providing a tool-chain that supports continuous development and testing of distributed control systems, including formal verification tools within the design process. Additionally, the selective incorporation of Non-Deterministic Transitions (NDTs) in formal verification allow the enhancement of model's realism while limiting complexity. The chapter is structured as follows: Section 7.2 discusses the study's objectives and the adopted approach. Section 7.3 details the IEC 61499 redesign of the HHM control software. Sections 7.4 and 7.5 describe the implementation of online simulations and formal verification, respectively. Section 7.6 presents the main results of the work, whereas Section 7.7 outlines the conclusions and future goals.

7.2 RESEARCH OBJECTIVES AND APPROACH

Despite the undeniable benefits introduced by the IEC 61499 standard, which provides a reference architecture and models for distributed control system development, the integration of the aforementioned technologies into real industrial applications might be challenging due to the actual complexity of the solution and the time required for both the Cyber-Physical System (CPS) implementation and verification. Indeed, while some examples for basic systems are provided in [184], it is still not clear whether the described techniques can be applied to complex CPS. The main objectives of the study are to demonstrate the benefits of the migration of IEC 61131-based software to an IEC 61499 architecture in enabling software verification using a meaningful example. Once consolidated, the strategy may be extended to other critical RH systems. Furthermore, the investigation aims at providing real-world strategies for developing modular applications, implementing automatic verification procedures, and reducing system complexity. This chapter showcases how the described techniques can be applied in the refactoring and verification of a SCCS, the HHM.

The proposed approach, illustrated in Fig. 7.2, makes use of a comprehensive tool-chain enabling the design, simulation and formal verification of the automation software prior to its deployment [184]. The framework consists of a number of tools, including the IEC 61499-compliant IDE EcoStruxure™ Automation Expert by Schneider Electric®, the FB2SMV tool [181] used to convert Function Blocks (in XML format) to SMV code, and the NuSMV symbolic model checker [183].

The process starts with the remodeling of the existing HHM control software in a new, modular and flexible architecture based on the IEC 61499 standard. This migration provides two distinct advantages: first, the optimization of the software logic, second, the generation of the XML model of the control solution. While online simulations can be executed directly within the IDE, formal verification is accomplished using an external tool. FB2SMV is in charge of the conversion from the XML output to a SMV model using the Abstract State Machine (ASM) [182] semantic as an intermediary model. Subsequently, NuSMV is employed to verify specific Linear Temporal Logic (LTL) expressions within the state space of the application. In case one of them is not satisfied, it additionally provides a counterexample trace that can be visualized using specific tools. In this context, NDTs are incorporated in the model to improve the system's realism. The development of a modular and portable system model, the reduction of verification complexity through the partial incorporation of NDTs, and the implementation of an automatic verification procedure are the fundamental novelties of the proposed solution.



```
-> State: 3.62 <-
HHM_FV_inst.ELplant.NDT = TRUE
HHM_FV_inst.CRcmd.NA = 0
HHM_FV_inst.CRcmd.NI = 1
HHM_FV_inst.GRplant.NDT = TRUE
HHM_FV_inst.CRcmd_CNF = TRUE
HHM_FV_inst.omega = FALSE
HHM_FV_inst.ELplant.ExistsInputEvent = TRUE
HHM_FV_inst.CRcmd.event_CNF_set = FALSE
HHM_FV_inst.GRplant.ExistsInputEvent = TRUE
```

```
Output to file: spec1.txt
elapse: 18517.71 seconds, total: 18517.83 seconds

-- specification  G !(HHM_FV_PART_1_2_3_inst.
     ELplant.POS_OUT = 5)  is true
```

#	Value	LTL specification
1	FALSE	G !(HHM_FV_inst.CRplant.POS_OUT=4 & HHM_FV_inst.CAcmd.moving = TRUE)

Figure 7.2: Proposed workflow for the validation of safety-critical automation systems.

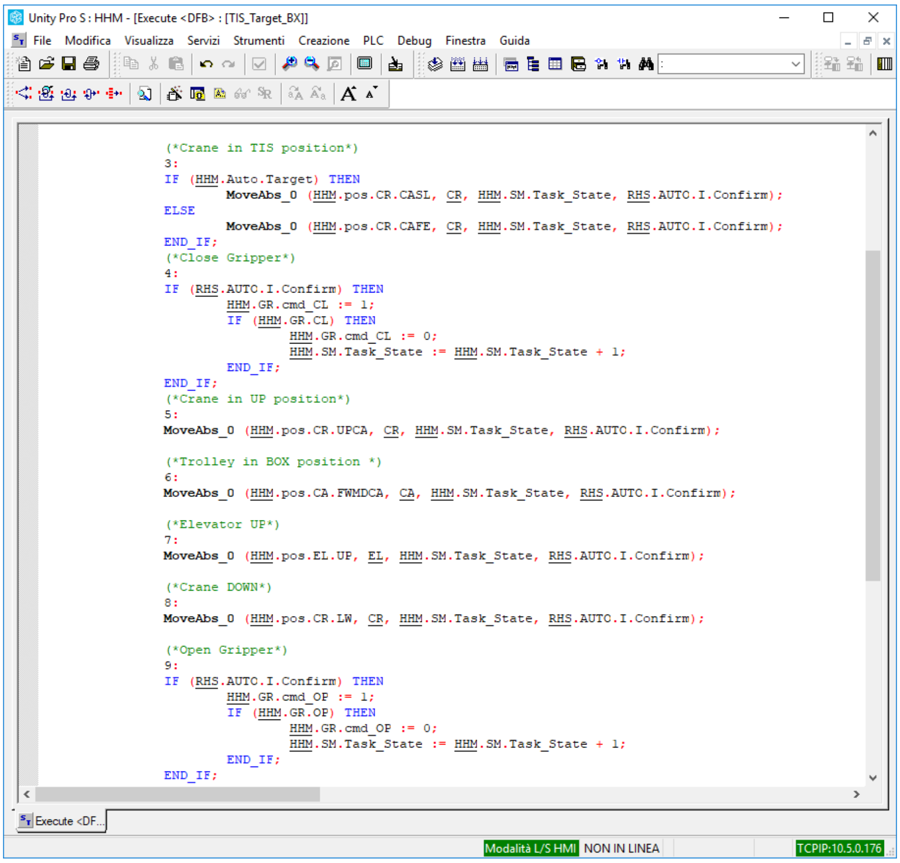
7.3 IEC 61499 SOFTWARE REDESIGN

An illustrative example is used to describe the entire formal verification process of the HHM control software. The proposed method includes the IEC 61499 software remodeling, the symbolic model checking, and the visualization of counterexamples. NDTs are progressively incorporated within the model to simulate an overall realistic behavior. In this work, the refactoring of an IEC 61131 control software with a new flexible and reconfigurable architecture based on IEC 61499 is presented. Additionally, formal modeling and verification tools have been incorporated to validate the effectiveness of the designed solution.

The HHM onboard PLC (Schneider Electric® M340) controls the sequence execution, which includes the axes movements, the pneumatic gripper actuation, and the reading of the various hard-wired signals from the limit switches demanded to detect the proper positioning of the radioactive TIS unit. The system is in charge of the management of RH sequences aimed at the exploitation of critical tasks in hazardous settings. The code is executed locally to avoid any potential incoherence resulting from communication issues. The HHM software logic supports multiple operating modes and motion sequences based on the type of remote handling task. Among the existing operational procedures, we focused on the most critical task: the removal of an irradiated TIS unit and subsequent storage inside the shielding box during transport. During this procedure, the HHM is facing the SPES Front-End and all actions are carried out by the cartesian manipulator. This motion sequence has been considered as critical since a potential fault during the execution would necessitate a maintenance intervention under severe radiological conditions, leading to a significant personnel exposure. The described RH procedure matches the risk scenarios discussed in Chapter 4.

7.3.1 *The existing HHM IEC 61131-3 software*

The original HHM control software was designed in accordance with the IEC 61131-3 standard. The project is based on multiple state machines, each of them associated with a specific motion sequence. The status of the process is described by specific global variables, which are read and written in different code sections throughout the execution. The *elevator*, *trolley*, and *crane* axes commands and status signals are forwarded to the actual motion drives by dedicated FB using the *CanOPEN* protocol. On the other hand, the *gripper* electrovalves are actuated via physical relays. The existing control software makes use of Structured Text (ST), Function Block Diagram (FBD) and Ladder Diagram (LD) languages.


Unity Pro S : HHM - [Execute <DFB> : [TIS_Target_BX]]
File Modifica Visualizza Servizi Strumenti Creazione PLC Debug Finestra Guida
Execute <DF...
Modalità L/S HMI
NON IN LINEA
TCPIP:10.5.0.176

```
(*Crane in TIS position*)
3:
IF (HHM.Auto.Target) THEN
        MoveAbs_0 (HHM.pos.CR.CASL, CR, HHM.SM.Task_State, RHS.AUTO.I.Confirm);
ELSE
        MoveAbs_0 (HHM.pos.CR.CAFE, CR, HHM.SM.Task_State, RHS.AUTO.I.Confirm);
END_IF;
(*Close Gripper*)
4:
IF (RHS.AUTO.I.Confirm) THEN
        HHM.GR.cmd_CL := 1;
        IF (HHM.GR.CL) THEN
                HHM.GR.cmd_CL := 0;
                HHM.SM.Task_State := HHM.SM.Task_State + 1;
        END_IF;
END_IF;
(*Crane in UP position*)
5:
MoveAbs_0 (HHM.pos.CR.UPCA, CR, HHM.SM.Task_State, RHS.AUTO.I.Confirm);

(*Trolley in BOX position *)
6:
MoveAbs_0 (HHM.pos.CA.FWMDCA, CA, HHM.SM.Task_State, RHS.AUTO.I.Confirm);

(*Elevator UP*)
7:
MoveAbs_0 (HHM.pos.EL.UP, EL, HHM.SM.Task_State, RHS.AUTO.I.Confirm);

(*Crane DOWN*)
8:
MoveAbs_0 (HHM.pos.CR.LW, CR, HHM.SM.Task_State, RHS.AUTO.I.Confirm);

(*Open Gripper*)
9:
IF (RHS.AUTO.I.Confirm) THEN
        HHM.GR.cmd_OP := 1;
        IF (HHM.GR.OP) THEN
                HHM.GR.cmd_OP := 0;
                HHM.SM.Task_State := HHM.SM.Task_State + 1;
        END_IF;
END_IF;
```

Figure 7.3: The original HHM control program, based on IEC 61131-3.

An overview of the software section dedicated to the TIS unit pick-up sequence is reported in Fig. 7.3. The algorithm is implemented as a ST switch *case*, including the sequential states of the RH procedure.

7.3.2 *Design of the correspondent Finite State Machine (FSM)*

Starting from the existing IEC 61131-3 program, the functional specifications of the process have been formulated as a Finite State Machine (FSM). The algorithm indicates, for each state, the actions to execute and the signals required for moving to the next step. Usually, transition conditions are based on the status of the different limit switches installed on the machine. These are devoted, as an example, at the detection of the gripper state, or at recognizing the TIS unit correct positioning within the shielding box. Actions, on the other hand, include the opening and closing of the gripper, or the command to a linear motion axes towards a predetermined position. The TIS unit pick-up procedure consists of the following steps:

- the *trolley* initially moves ahead to pick up the TIS unit;
- the *crane* descends, engages the TIS unit, and rises to the top position;

- the *trolley* moves to the middle position on top of the open shield box while holding the TIS unit;
- the *crane* lowers the TIS unit while the *elevator* rises the box. Once in position, the *gripper* releases the payload;
- the manipulator finally closes the box with the lid.

The Finite State Machine (FSM) is depicted in Fig. 7.4.

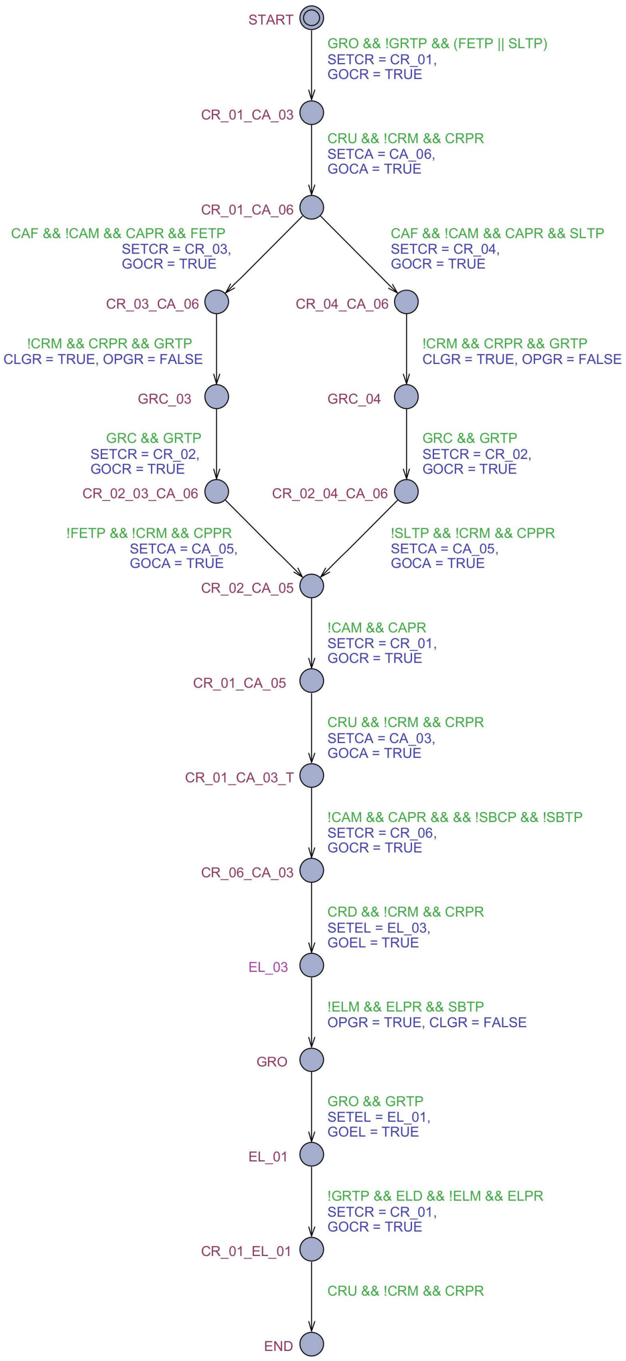


Figure 7.4: The TIS unit pick-up sequence's Finite State Machine (FSM).

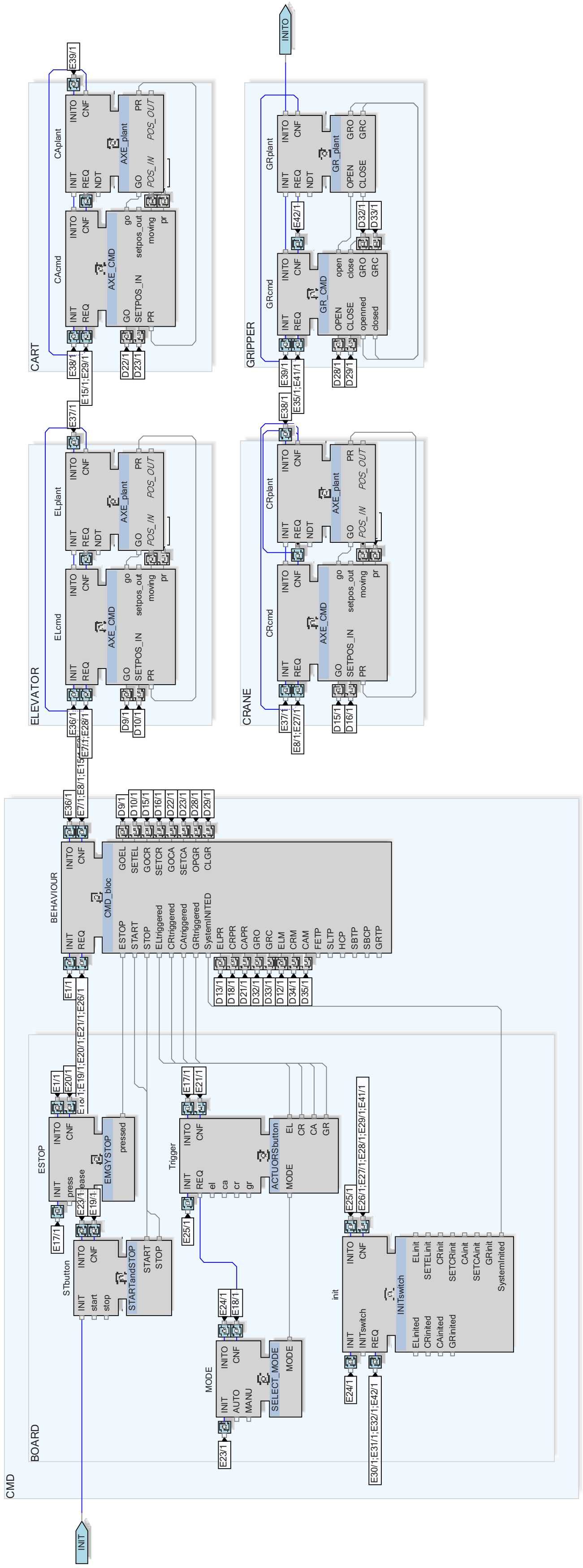


Figure 7.5: The IEC 61499 global composite Function Block of the HHM model.

7.3.3 The IEC 61499 implementation

One of the many benefits provided by the IEC 61499 refactoring, aside from supporting formal verification, is the introduction of a modular, standardized, and reusable architecture for the development of FBs. This strategy results in improved code organization and the potential to "certify" the behavior of the FBs, thus reducing the verification complexity in subsequent applications. Additionally, the existing IEC 61131 design, which is based on Structured Text (ST), incorporates global variables within the program to track the program execution. Since the software's behavior is not always evident this poses a serious concern. In contrast, IEC 61499 provides for the explicit specification of the dependencies and interactions between different FBs. The remodeled application of the HHM control logic was developed using the EcoStruxure™ Automation Expert tool. The software architecture is built on FBs linked to Moore-type finite state machines known as Execution Control Chart (ECC) [154]. An overview of the global composite FB model is available in Fig. 7.5.

The *elevator*, *trolley*, *crane*, and *gripper* are the key actuation groups employed in this application. Each of these mechatronic systems, which work together to securely encase the TIS unit in the shielding box, is supervised by a dedicated controller. The following sections provide a detailed description of the main Function Blocks (FBs).

7.3.3.1 Linear motion axes

A standardized pair of controller and plant FB can be used to conceptually model the three linear axes. Using a modular and reusable strategy, the development work can be significantly decreased. Additionally, it makes it possible for the system to be easily reconfigured in order to achieve alternative capabilities in the future. The core FB AXE_CMD, which implements an absolute positioning control system,

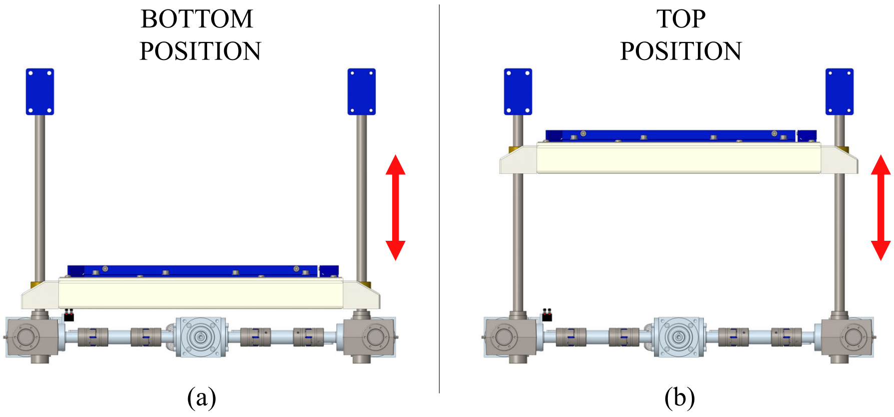
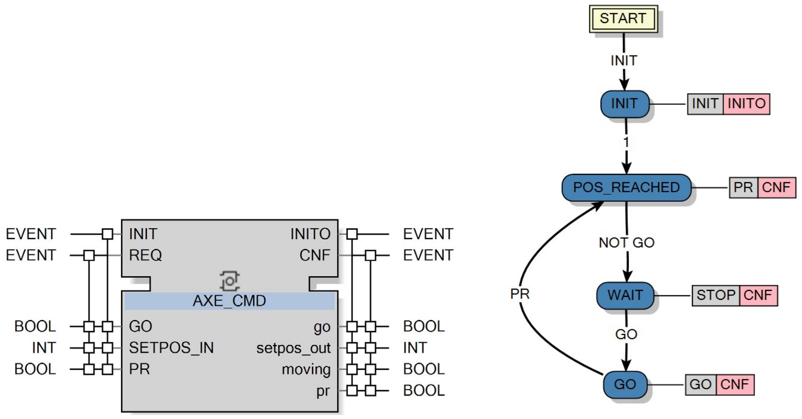


Figure 7.6: Visual representation of the elevator linear motion axis: (a) bottom position, (b) top position.



(a) (b)

Figure 7.7: Overview of the controllers dedicated to the HHM linear motion axes. (a) The AXE_CMD FB, (b) the AXE_CMD ECC.

is shared by the three linear axes. The FB and the corresponding ECC are displayed in Fig. 7.7. The plant FB precisely sets the axis according to the destination coordinates and provides the `POS_REACHED` signal to the controller once the motion is completed. The given target position directs the `AXE_CMD` to the preset coordinates. The FB acknowledges its arrival and stops it once it reaches the designated spot. A visual representation of the *elevator* linear motion axis is reported as an example in Fig. 7.6.

7.3.3.2 *Gripper*

The operating mode of the HHM pneumatic *gripper* differs from the above-mentioned systems due to its inherent discrete logic. *Gripper* `CLOSE` or `OPEN` commands are processed when the `REQ` event is triggered. The FB provides two output signals to indicate when the relevant "closed" or "open" state has been reached.

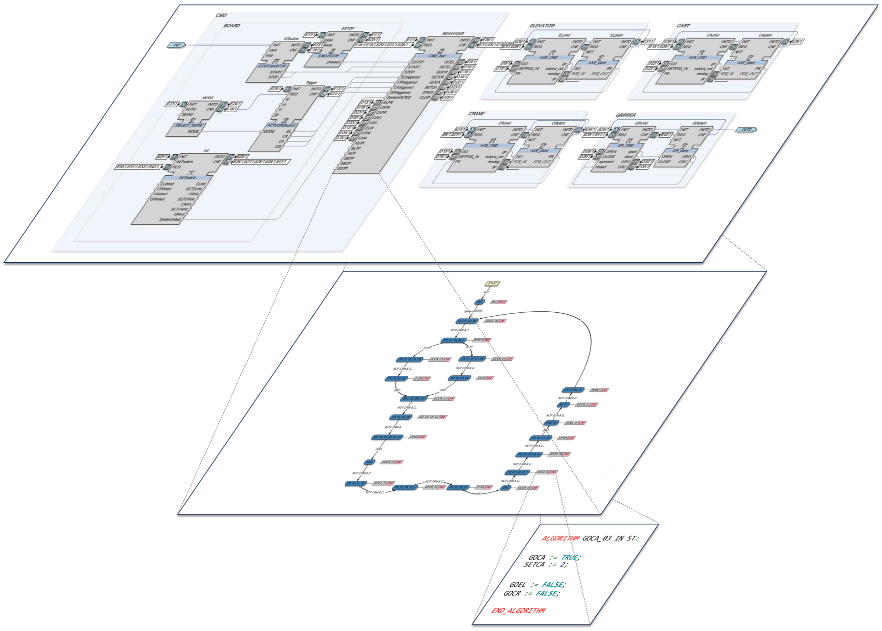
7.3.3.3 *Sequence Controller*

The `SEQUENCE` FB manages the integration of the various subsystems and the overall HHM behavior throughout the execution of the remote handling sequence. The precise list of tasks is defined within the correspondent ECC. Each FSM state is associated with a set of actions carried out by a specific algorithm. Motion actions are started by setting the desired position for a specific axis and sending the `GO` command to the appropriate controller. The reception of the `POS_REACHED` command from the plant FB causes the transition to the next state. In our case study, the sequence controller FB implements a state machine that refers to a single HHM task: the TIS unit pick-up sequence. This sequence has been examined as a representative example. The system's adaptable architecture will make it possible to incorporate more motion sequences in the future by updating a single FB.

7.3.3.4 *Support Function Blocks*

The `INIT` FB initializes the system and prepares it to perform the desired procedure at the start of software execution. The user can then choose between manual and automatic HHM operating modes by using the `TRIGGER` and `MODE_SELECTION` FBs. While the first allows the user to direct the HHM behavior, the automatic mode forces the system to stick to the Sequence controller's state machine logic. The `ESTOP` FB, as the last support FB, offers the ability to stop the execution at any time. This feature protects the system from internal or external failure caused by unfavorable conditions.

The IEC 61499 composite FB is visible in the top layer of Fig. 7.8. The model includes the different FBs devoted to the axes and gripper control, support functions and overall sequence management. Execution Control Charts (ECCs) aim at describing the behavior of each FB as Finite State Machines (FSMs). The Sequence controller ECC is outlined in the middle layer of Fig. 7.8. Actions to be performed throughout the different states are detailed in specific algorithms, similar to the one shown in the bottom layer.



```
ALGORITHM GOCA_03 IN ST:

GOCA  := TRUE;
SETCA := 2;

GOEL  := FALSE;
GOCR  := FALSE;

END_ALGORITHM
```

Figure 7.8: Layer view of the IEC 61499 application. (top layer) function blocks, (middle layer) execution control charts, (bottom layer) algorithms.

7.4 SIMULATION MODEL

IEC 61499 applications can typically be tested using dynamic (online) or static (offline) techniques. In order to assure safety in a system that has already been deployed and is in use, the first group of techniques seeks to monitor it in its operating state. Conversely, offline safety measures are meant to reduce fault risk at the design stage and test the system before use [257]. In our work, we focused on offline verification methods aimed at fault removal. This process can be accomplished at the designed stage using formal verification tools or online testing techniques. Software simulation involves feeding the program with input sequences that replicate the behavior of the actual system and determining whether or not the program's outputs comply with specific requirements. The adopted development suite includes a native HMI, which may be used as a command center and to simulate system execution. Composite Automation Types (CATs) were used to model a range of mechatronic components for the simulated plant. This feature facilitates testing of the system's simulation behavior in a common environment because CATs can be directly linked to both HMI objects and FBs. Inputs were used to link the controller FBs to the relevant CAT blocks, replicating the real-world behavior of the mechatronic components in the system. The HHM representation implemented in the HMI is shown in Fig. 7.10, where the three linear motion axes are linked to distinct CAT blocks. Each axis plant FB is connected to a dedicated `AXE_CMD` controller, which selects the desired position set-point from a predefined pool of coordinates and triggers the motion request. In response to the controller's inputs, the plant block validates the

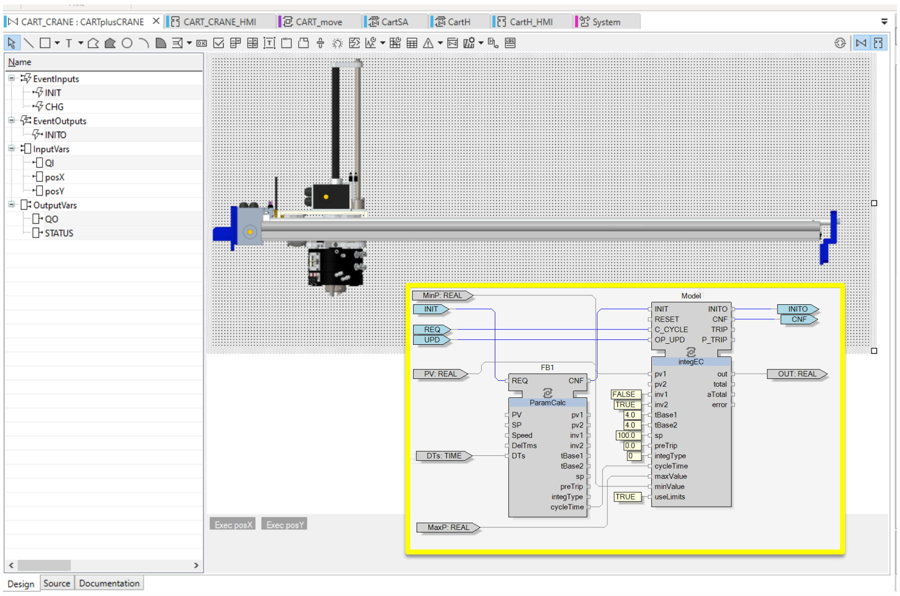


Figure 7.9: The *trolley* Composite Automation Type (CAT) and the corresponding FB.

coordinates, performs the movement, and acknowledges its arrival at the predetermined location. The axis motion may be stopped at any time by activating a STOP input event. The GR_CMD FB opens or closes the clamp based on the input signal from the controller. In order to interlock the option of releasing the payload only in particular positions, the GR_CMD FB is provided with the axes' actual positions.

We should emphasize that the HMI CATs offer a more accurate representation of the system behavior when compared to the axis plant FBs discussed in Section 7.3. While in the basic implementation, the plant FB will only trigger the POS_REACHED signal after an arbitrary time, here an integrator simulates the linear axis movement and sends the actual position coordinates to the correspondent object in the HMI allowing the user to follow the motion while it is being executed. Further debugging tools, such as runtime monitoring blocks, can be also employed to detect specific critical conditions. The software's modularity allows for the independent and concurrent development of the controller and plant FBs. Each FB will be initially tested and debugged with the aid of custom mock-up blocks. As they reach maturity, they can then be interconnected to run the simulation. After the verification, the final stage will be to replace the simulation's plant FB with the actual system.

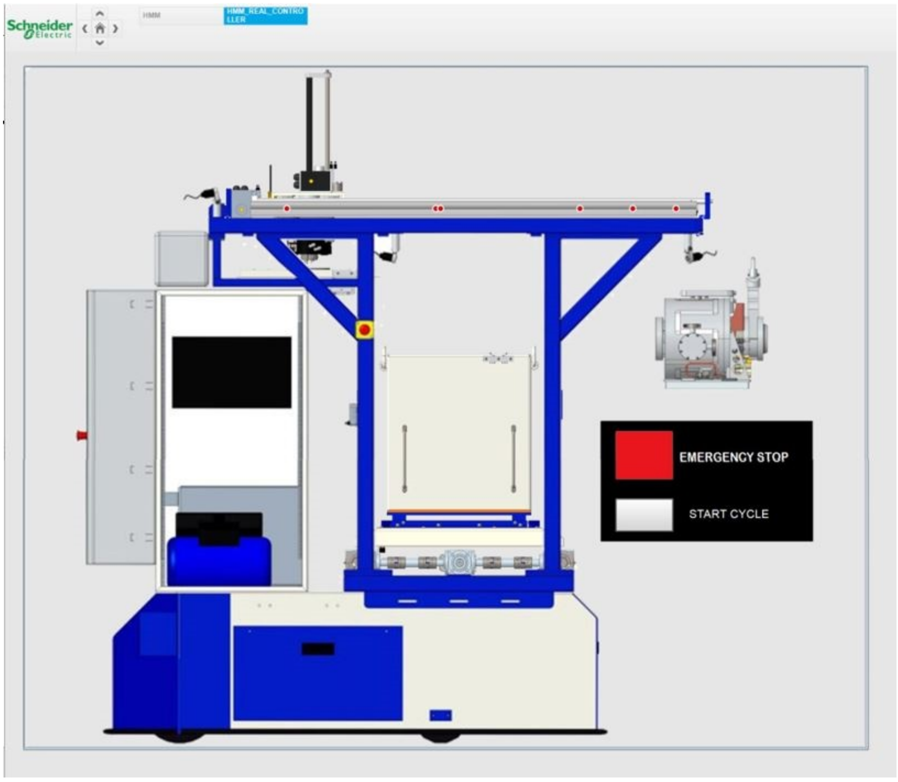


Figure 7.10: Graphical representation of the global HHM CAT used in the Human Machine Interface (HMI) for online monitoring and simulations.

Unfortunately, simulations often cannot explore all possible paths due to the huge size of state automata representing industrial control software. This bottleneck makes them insufficient as an exhaustive verification method since it prevents conclusive verification of program behavior in a reasonable amount of time. Furthermore, the quality of the output is also influenced by the automation engineer's knowledge and experience in selecting pertinent testing sequences that may correspond to typical dangerous circumstances of the controlled process [258]. To address these problems, formal verification techniques have been established, which provide methods for closed-loop (plant and controller) model checking able to analyze a program in its entirety.

7.5 FORMAL VERIFICATION

The formal verification of finite state systems, such as closed-loop control algorithms, has been effectively accomplished in the last ten years thanks to symbolic model checking based on Binary Decision Diagrams (BDDs) These tools have been developed in the past to overcome the state explosion problem in finite automata [180]. Model checking is the process of exploring the reachable states of a model, which is described as a Finite State Machine (FSM), in order to validate temporal logic specifications. When a property is violated, the tool provides a counterexample in the form of a sequence of states [179]. As previously mentioned, the most well-known open-source model detection tools among the available solutions are NuSMV and SPIN. In particular, because of its extensive core capabilities and good scalability, NuSMV is frequently used for reliability and security verification of industrial designs [259]. This tool supports the representation of synchronous and asynchronous finite state systems and it allows for the verification of both Linear Temporal Logic (LTL) and Computation Tree Logic (CTL) specifications using implicit methods. In more detail, it compares a model against a property using a symbolic representation of the specification [260].

In this study the HHM control software, redesigned according to IEC 61499, has been converted to a SMV model, enabling its subsequent symbolic model checking exploiting NuSMV. The goal of this methodology is to identify potential failure conditions that may happen only following specific paths within the state space of the model. The difficult reproducibility of the error causes makes this approach more effective at detecting failure when compared with conventional simulation techniques. Accurate modeling of the real system is essential in order to validate the intended behavior of the device and detect potentially undesirable states. This enables simulation and verification of the apparatus prior to its actual operation. Since the model is an abstraction, it may not include all relevant characteristics of the real-world system or the context in which it is embedded. Hence, a condensed version of the plant FB can be used to create a reduced formal model, which can then be verified utilizing symbolic model checking techniques thanks to the NuSMV tool. As an illustration, in the presented use case, the `AXE_CMD` FB only takes into account the beginning, intermediate, and final states rather than the motion dynamic considered in the real system. This approximation is still acceptable because the goal at this stage is to assess the possible blockage within two locations instead of the specific stop positioning.

7.5.1 *LTL expressions*

Table 7.1 describes a collection of LTL expressions that have been developed to identify potential critical problems. Specifications no. 1-3 are meant to ensure that none of the three linear motion axes enters the error state during system execution. On the other hand, requirements no. 4 and 5 deal with potential collision detection. More in detail, the first verify that *trolley* movements are inhibited when the *crane* is not fully raised, and the second focuses on the system configuration occurring while positioning the TIS unit within the shielding box. Similarly to the last scenario, the *trolley* must not move while the *elevator* is raised and the *crane* is lowered. Specification no. 6 aims to confirm that the *gripper* only opens in a specific location: when the TIS unit is lowered within the box (*elevator* up and *crane* down).

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.

Table 7.1: Description of the LTL specifications verified with NuSMV in the HHM model.

A batch script, detailed in Listing 7.1, has been developed to examine all the aforementioned requirements with NuSMV and log data.

```
time
read_model -i HHM_FV_PART_1.smv
flatten_hierarchy
encode_variables
build_model
time
check_ltlspec -p "G !(HHM_FV_PART_1_inst.ELplant.POS_
   OUT = 5)" -o spec1.txt
time
check_ltlspec -p "G !(HHM_FV_PART_1_inst.CAplant.POS_
   OUT = 5)" -o spec2.txt
time
check_ltlspec -p "G !(HHM_FV_PART_1_inst.CRplant.POS_
   OUT = 5)" -o spec3.txt
time
check_ltlspec -p "G  !(HHM_FV_PART_1_inst.CRplant.POS
   _OUT in (2..4) & HHM_FV_PART_1_inst.CAcmd.moving =
    TRUE)" -o spec4.txt
time
check_ltlspec -p "G  !(HHM_FV_PART_1_inst.ELplant.POS
   _OUT = 2 & HHM_FV_PART_1 _inst.CRplant.POS_OUT = 4
    & HHM_FV_PART_1_inst.CAcmd.moving = TRUE)" -o
   spec5.txt
time
check_ltlspec -p "G  !(HHM_FV_PART_1_inst.ELplant.POS
   _OUT = 1 & HHM_FV_PART_1_inst.CRplant.POS_OUT = 4
   & HHM_FV_PART_1_inst.GRplant.GRO = TRUE)" -o spec
   6.txt
time
```

Listing 7.1: Batch script used to check the LTL specifications with NuSMV

7.5.2 *Test scenarios*

The proposed formal verification process aims at offering unique performance in terms of detection of critical error scenarios. In the presented work, the LTL specifications outlined in Tab. 7.1 have been evaluated in two different scenarios to test the formal verification effectiveness and reliability. Specifically, the main HHM sequence controller ECC has been modified from the original version to incorporate a potential source of error that may lead to a mechanical collision.

As described in Section 7.3, the `SEQUENCE` FB implements a FSM where the HHM axes movements are executed sequentially to prevent any potential collision that may occur during the insertion of an irradiated TIS unit within the HHM shielding box. If we specifically consider state GRC_03_GRC_04 in Fig. 7.11, which corresponds to the TIS unit picked up by the HHM cartesian manipulator, the subsequent path towards the shielding box shall be carried out in three distinct steps: (1) backward movement of the *trolley* axis, (2) lowering of the *crane* axis, and (3) rising of the *elevator*. The described motion sequence and the correspondent states are visible in Fig. 7.11. In the research, a design flaw in the HHM control software has been deliberately introduced to determine the NuSMV ability to identify it.

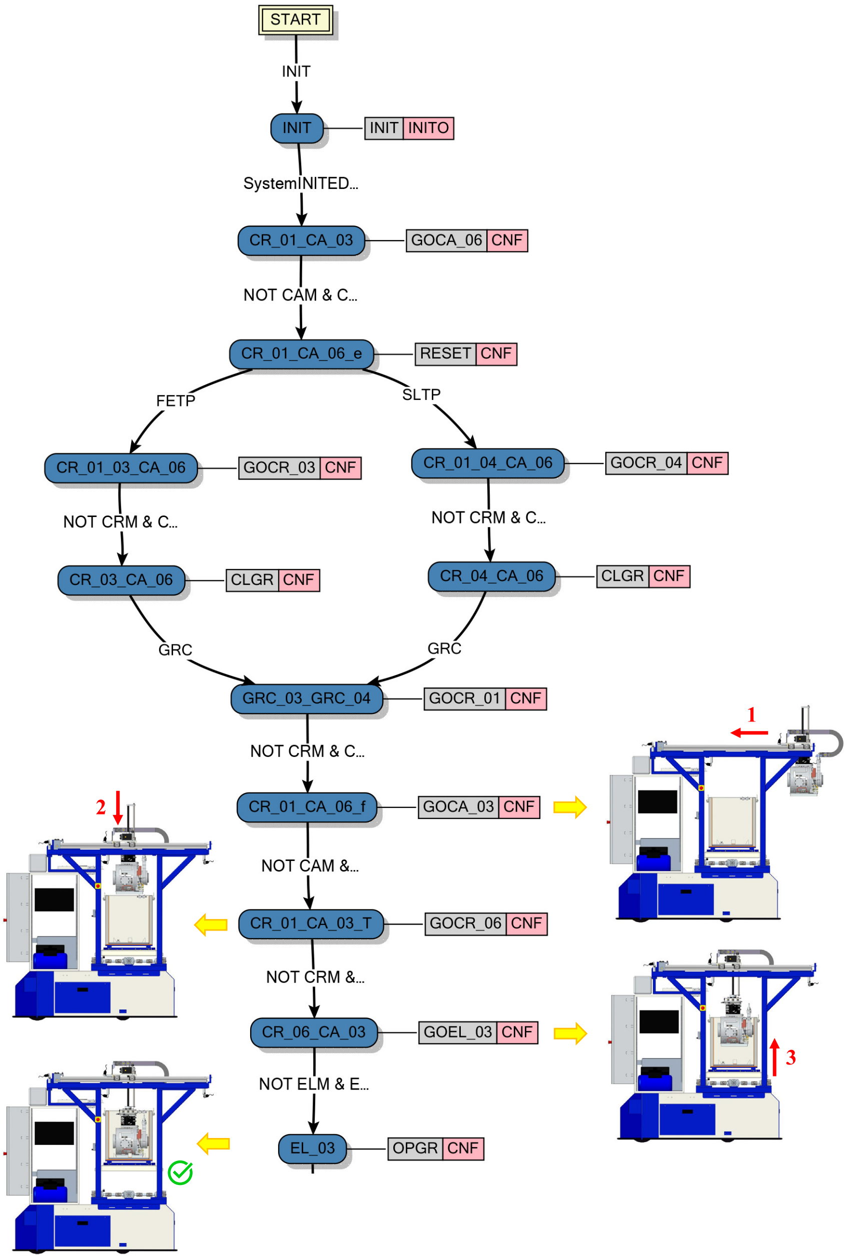


Figure 7.11: First investigated control sequences. ECC of the Controller FB implementing the sequential movement of the three linear axes.

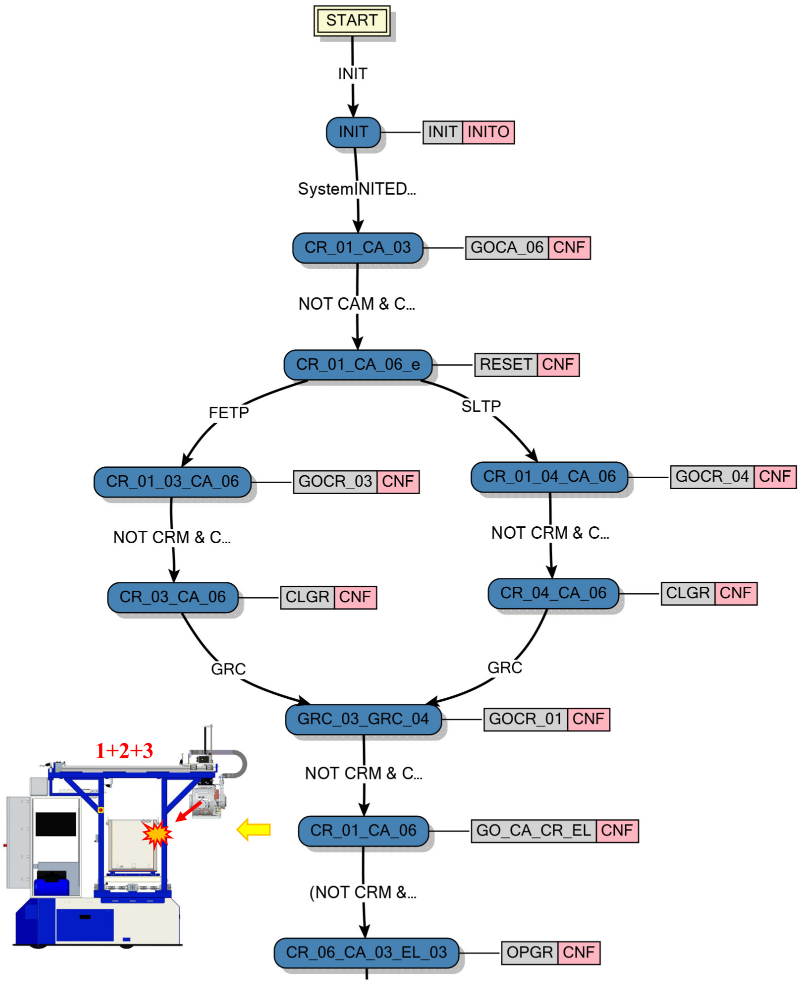


Figure 7.12: Second investigated control sequences. ECC of the Controller FB implementing the parallel movement of the three linear axes.

More in detail, the ECC linked to the `SEQUENCE` FB has been updated to launch the previously mentioned actions in a parallel execution, with the three motion axes moving simultaneously, as shown in Fig. 7.12. This type of design flaws is particularly challenging to identify through conventional simulations techniques, as it does not always result in a fault condition. The relative motion axes speeds do, in fact, affect the likelihood of a collision. This implies that we may be able to perform multiple simulations without observing any failure event. The following section discusses how adding non-determinism to the model can make it more realistic by taking into account the impact of real world non-idealities and enabling the early identification of potential system defects. With regard to the test under discussion, NDTs within axes plant FBs seek to change the amount of time required to get the `POS_REACHED` signal, directly impacting the relative speed between concurrent axis movements. A potential mechanical collision is detected by the violation of LTL property no. 5 in Table 7.1.

7.5.3 *Discrete State Plant Modelling in Function Blocks with Non-Deterministic Transitions*

Generally speaking, the IEC 61499 applications developed for visualization and online verification purposes, need to include different elements required to improve the accuracy of CATs used in the EcoStruxure™ Automation Expert HMI. Conversely, the model developed for the formal verification, should be simplified and reduced prior to its conversion to SMV code. For this reason, the *elevator*, *trolley*, and *crane* components were modeled in this study by simplified FBs that embody the intended behavior of the actual system while omitting the features used for visualization. Thus, by discretizing the plant model's FB while maintaining its functional capabilities, the original complex model can be reduced to a simpler representation. The AXE_PLANT component features two data inputs (GO and POS_IN) and two data outputs (POS_REACHED and POS_OUT). The system may simulate real-world behavior using the NDT event's random signal emission, which enables the discovery of previously undetected faults using CTL or LTL specifications. As an example, Fig. 7.13 depicts a potential scenario in which a NDT has been introduced in the ECC associated with *elevator* plant FB. In this case the plant enters the GO state upon receiving the controller's GO signal and following the NDT event, it reaches the END state. The physical meaning of this NDT is that the transition between the GO and END states, i.e. the axis motion towards a given position, might take an unspecified amount of time. If a NOT_GO signal is generated while the plant is in the GO state, it enters the STOP state and remains there until another GO signal is activated. In the END state, the plant notifies the controller that the task has

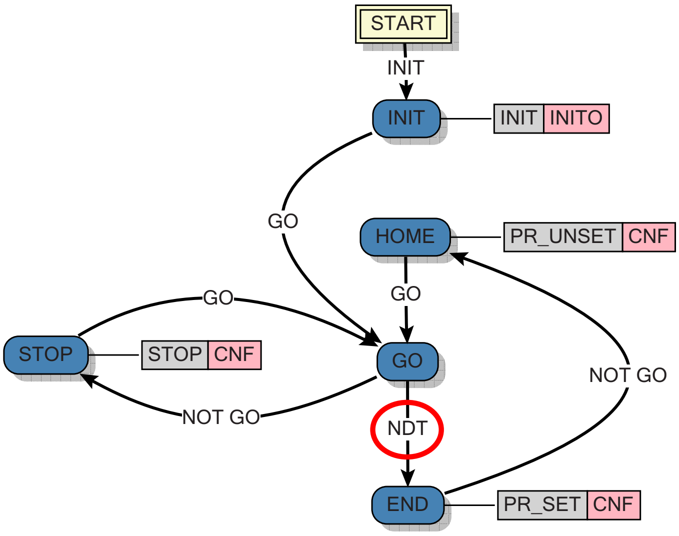


Figure 7.13: Example of injection of a Non-Deterministic Transition (NDT) within the elevator plant model.

No.	Scenario
1	NDT in *elevator* plant
2	NDT in *trolley* plant
3	NDT in *crane* plant
4	NDT in *gripper* plant
5	NDT in *elevator* and *trolley* plants
6	NDT in *elevator*, *trolley* and *crane* plants
7	NDT in *elevator*, *trolley*, *crane* and *gripper* plants

Table 7.2: Non-Deterministic Transition (NDT) scenarios analyzed in the study: NDTs are progressively included in the model.

been completed by setting the value of POS_REACHED signal to TRUE. Following the deactivation of the GO signal, the plant returns to the HOME state. The *gripper* plant model features two data inputs, OPEN and CLOSE, and two data outputs, GRO and GRC. The model initially enters the OPENING state when the controller sets OPEN to TRUE. Second, it switches to the OPEN state in response to a NDT signal. Similarly, when the controller sets CLOSE to TRUE, the plant reaches the CLOSING state and, following a random time delay caused by the NDT, enters the CLOSED state. If the CLOSE command is activated during the OPENING state, the model transitions to the CLOSING state. If the OPEN command is activated during the CLOSING state, the plant returns to the OPENING state and awaits for the emission of the NDT signal.

The discrete state model of the HHM was converted into a SMV model using the FB2SMV tool. Subsequently, the verification has been carried out by NuSMV, using an Intel® core™ i7-10510U CPU@1.80 GHz 2.30 GHz with 32 Gb RAM. In an effort to mitigate the state space explosion problem, NDTs have gradually been introduced into different sections of the model according to the scenarios in Table 7.2. The progressive integration of NDTs might be viewed as a feature of the proposed tool-chain. While it is true that critical faults might occur as a result of multiple non-deterministic conditions acting simultaneously, in a first verification stage, distinct blocks can be assessed independently while maintaining the execution time within reasonable limits.

7.6 results and discussion

The initial phase of the project, which followed the software remodeling based on IEC 61499, was devoted to validating the model by launching various simulations directly within the EcoStruxure™ Automation Expert suite. This was achieved through the use of CATs, which allow FBs to be directly linked to HMI objects.

The application model and the HMI have been developed independently. Once sufficiently stable, the HMI plant FB was connected to the controller FBs, replacing the existing simplified version of plant FBs. Launching the online simulation, the user can monitor the sequence execution. The software will begin in the initial state, progress through specific checkpoints, and eventually reach the final state. Unfortunately, even if the simulation doesn't report any errors, this merely indicates that there exists a path where it crosses all the checkpoints. Hence, using symbolic model checking tools will provide a more thorough level of investigation. Prior to the verification procedure, it is crucial to verify the accuracy of the formal model. This can be accomplished by simulating the model in NuSMV, where various paths and random states are explored. The simulation assists in demonstrating that the model properly covers all the ECC states of the behavioral FB by tracing the path of ECC states. It also helps to confirm that the generated formal model behaves in accordance with the discrete state model by providing information about the values of all the variables in each state.

The NuSMV simulation technique can detect changes in the ECC and their impact on system behavior. Initially, using this method it will be possible to confirm that all paths leading from the beginning to the end will pass through the crucial checkpoint. As the second step, this assertion needs to be proven even in the presence of non-determinism. Indeed, the introduction of NDTs may have resulted in the inclusion of certain additional pathways in the application, and this is reflected in a larger state space with multiple routes. In contrast to simulation, where we can test only one scenario, NDTs allow us to evaluate several possibilities. The evidence that the given specifications are validated in all of these paths will thus extend the results of the online simulation. The six formulated properties have been checked using a batch script that reads the supplied SMV model and performs the verification, logging both the execution time and result for each specification. The quantity of memory needed to store and manipulate BDDs is the primary limitation of model checking methods. In light of this, the proposed implementation allows for the gradual integration of NDTs into the model. This stepwise approach provides better control over the model and allows for faster specification analysis. The time required for NuSMV to execute the formal verification of all the described LTL specifications while altering the number of NDTs is depicted in

Fig. 7.14. It is evident that the gradual inclusion of NDTs resulted in a global increase in execution time. Because of the ample state space, it is feasible that with a larger number of NDTs, global verification of all pathways will fail.

Reducing the number of NDT points in this situation may be a viable option for squeezing the state space to a tolerable size and then gradually increasing it. Bounded Model Checking (BMC) is an alternate strategy that searches for a counterexample in executions whose length is constrained by some number k. If no bug is discovered, k is increased until either a bug is discovered, the problem becomes unmanageable, or some predetermined upper bound is reached [179]. A key feature of the described engineering framework is the ability to govern non-determinism. Indeed, NDTs can be injected into specific locations to perform formal verification in a particular configuration. This method allows us to validate the automation system under particular stress conditions. As discussed in Section 7.5, the IEC 61499 application was formally verified following the purposeful introduction of a design fault that might potentially lead to a collision occurrence.

Despite the difficulties in identifying this failure condition using conventional simulations, NuSMV was able to successfully accomplish this task, thus providing a counterexample which demonstrates the violation of LTL property no. 5 in Table 7.1. In the case under study, the amount of time needed for the formal verification was comparable with what was required for the same LTL expression in Scenario no. 7 (see Fig. 7.14). However, it is difficult to formulate a generic statement because the duration depends on the particular paths that lead to the failure conditions. The evidence of the violation is provided by NuSMV in the form of a failure trace, which depicts a state sequence of system model transitions where the specification is not met. Figure 7.15 shows how, through the use of specific visualization tools [261] it would be possible to decode the output trace and examine the path that led to the violation. This result is of great significance as it showcases how the presented set of tools can be employed in the verification of complex safety-critical control systems, enabling the early detection of potential failure conditions that would be extremely difficult to spot through traditional simulation and testing techniques.

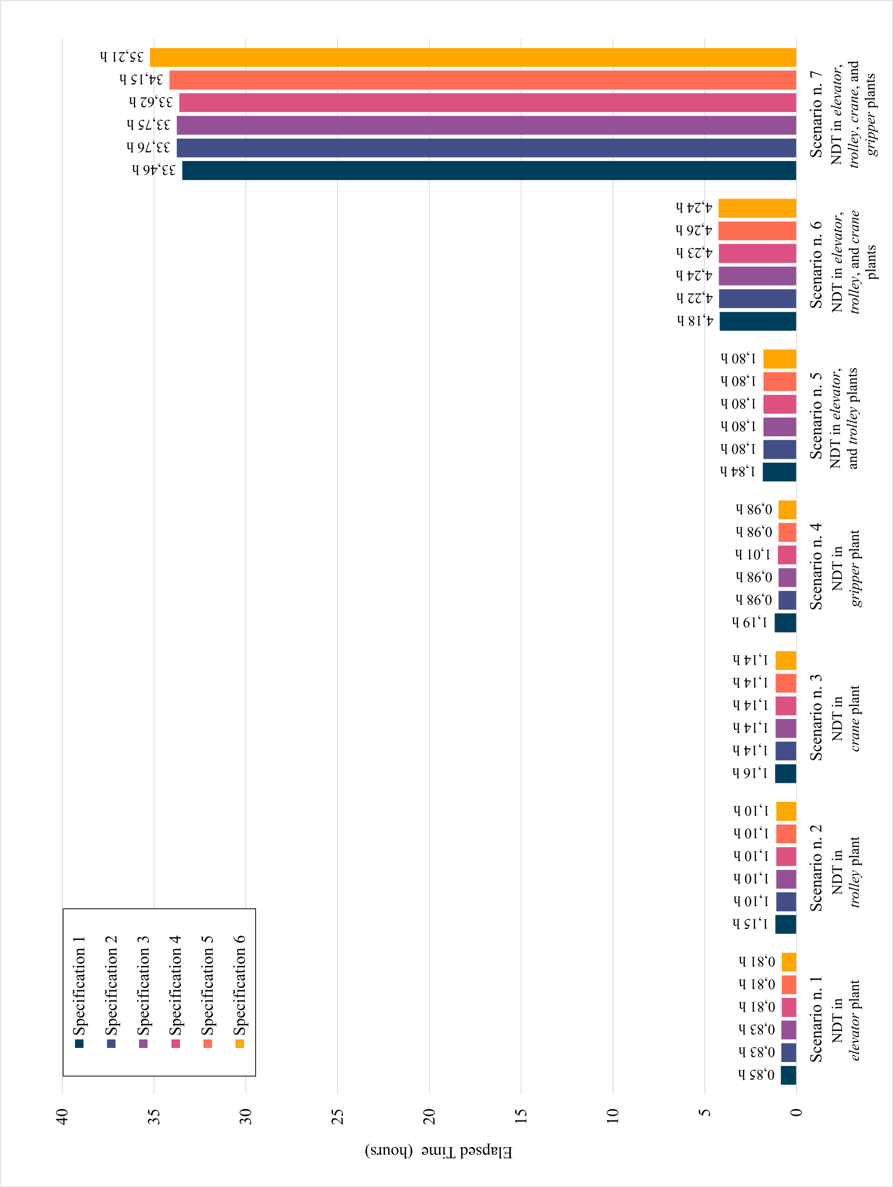
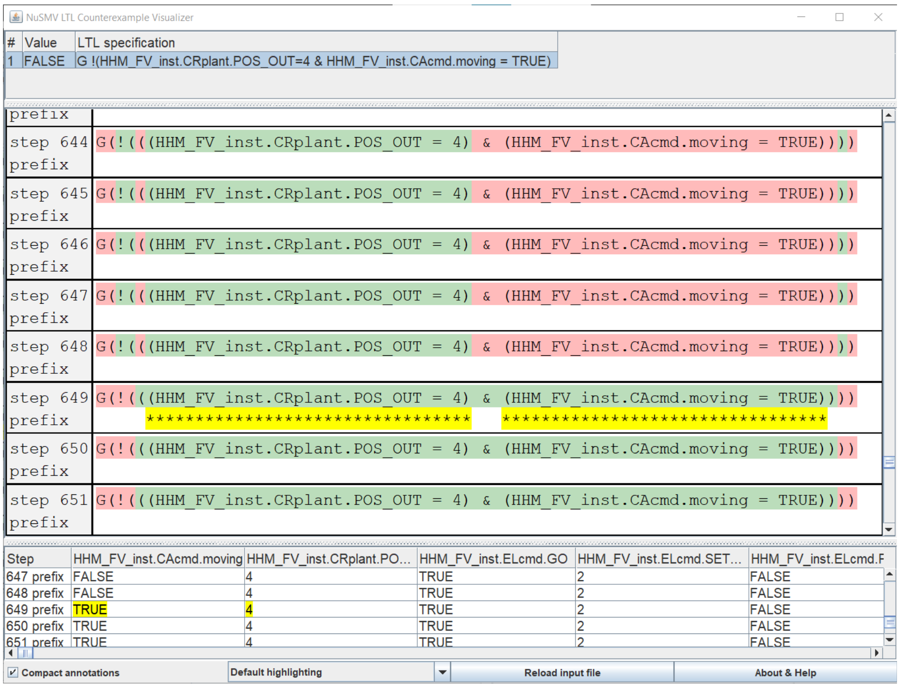


Figure 7.14: Execution time required by NuSMV in different NDTs configuration.



NuSMV LTL Counterexample Visualizer

#	Value	LTL specification
1	FALSE	G !(HHM_FV_inst.CRplant.POS_OUT=4 & HHM_FV_inst.CAcmd.moving = TRUE)

```
prefix
step 644 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix
step 645 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix
step 646 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix
step 647 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix
step 648 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix
step 649 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix        *********************************    *********************************
step 650 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix
step 651 G(!(((HHM_FV_inst.CRplant.POS_OUT = 4) & (HHM_FV_inst.CAcmd.moving = TRUE))))
prefix
```

Step	HHM_FV_inst.CAcmd.moving	HHM_FV_inst.CRplant.PO...	HHM_FV_inst.ELcmd.GO	HHM_FV_inst.ELcmd.SET...	HHM_FV_inst.ELcmd.F
647 prefix	FALSE	4	TRUE	2	FALSE
648 prefix	FALSE	4	TRUE	2	FALSE
649 prefix	TRUE	4	TRUE	2	FALSE
650 prefix	TRUE	4	TRUE	2	FALSE
651 prefix	TRUE	4	TRUE	2	FALSE

Figure 7.15: Graphical visualization of the counterexample trace produced by NuSMV when a LTL specification is violated.

7.7 CONCLUSIONS AND FUTURE WORK

In this chapter, we've shown how to use an integrated tool-chain for the analysis and verification of the control software for a real, safety-critical automated system employed in the transport and storage of radioactive material in a nuclear research facility. The provided use case was intended to demonstrate the actual feasibility of integrating the phases of modeling, simulation, verification, and analysis in a complex system using an automatic procedure. The study benefited from the software redesign based on the IEC 61499 standard for several kinds of reasons. First, it enabled the optimization of code structure by defining standardized, modular, and reusable FBs based on specific ECCs. Second, it allowed for the explicit specification of the relationships and dependencies between FBs while eliminating the incorporation of global variables. Third, it supported the translation of the code into an SMV model, thereby enabling formal verification of LTL safety specifications. Finally, the incorporation of NDTs within different FBs facilitated the simulation of sequence execution under realistic conditions. The developed IEC 61499 solution's portability promotes the system to be integrated into various tool-chains. In the proposed example, we investigated this feature by combining it with FB2SMV and FBME for the verification of a set of LTL safety specifications. While the first tool is used to extract the software formal model, model verification is subsequently carried out using NuSMV. FBME, on the other hand, is a comprehensive tool, capable of automating the entire verification process by incorporating automatic model generation, NuSMV verification, visualization, and analysis of counterexample trace. The suggested tool-chain can be instrumental in the early identification of design flaws that could result in potential mechanical collisions. The presented results emphasize the validity of the tool-chain by demonstrating the benefits of formal system verification in detecting non-trivial design errors that may result in a failure event under specific circumstances. A key feature of the proposed solution, in addition to modularity and portability, is the deep control over localized NDT introduction. This capability can be effective in reducing the process complexity, permitting independent testing of specific FBs, and keeping the time required by model checking within reasonable limits. One limitation of the presented methodology resides in the accuracy with which the IEC 61499 model represents the actual system. Indeed, the necessity for mitigating the state explosion problem ultimately led to the adoption of a simplified design, especially with regard to plant FBs. Ensuring a high level of accuracy between the model and its real-world equivalent is crucial during this phase. Furthermore, in the provided use case we investigated a single, albeit critically important, remote handling procedure. Further developments will allow the software model to be expanded to include more system motion sequences and plant details, thus finalizing the development of a digital twin of the primary SPES RH system.

Part V

CONCLUSIONS

8 CONCLUSIONS AND FUTURE WORK

In-depth integration of automation systems in nuclear applications represents an increasingly prominent strategy to reduce personnel exposure to ionizing radiations. The implementation of RH techniques in process automation and remote maintenance is currently taking place in different domains, including NPPs, particle accelerators and fusion reactors. Effective RH design methodologies are necessary to address the distinctive challenges of the working environment. In this context, early safety assessment throughout the design phase may represent a valuable asset to detect potential criticalities and optimize maintenance activities.

The main contribution of this thesis consists in the development of a safety-driven design approach for automation systems within the SPES facility. The preliminary consolidation of the RH framework, presented in Chapter 3, served as a baseline for the process. The impact of safety-driven design on the necessity for personnel access to dangerous locations is discussed using specific optimization examples applied to the target area layout, control system architecture, communication infrastructure, energy management logic, and procedures.

A semi-quantitative PRA based on HAZOP-LOPA was then applied to automated processes on the SPES Front-End to evaluate major failure scenarios that may arise during RH tasks and their implications for manual recovery actions. The study, discussed in Chapter 4, identified specific safeguards aimed at decreasing the likelihood of failure events and, as result, the number of hands-on upkeep tasks. Additionally, a set of IPLs has been presented and validated as an effective tool to guarantee the required degree of operational safety. Key outcomes of the PRA assisted in the establishment of an explicit plan aimed at the implementation of the suggested safeguards, including the safety-driven redesign of critical systems, the control software validation and the maintenance tasks analysis and optimization.

The design of a crucial Front-End assembly has undergone a significant revision, outlined in Chapter 5, to address the shortcomings revealed by the PRA. The described process effectively incorporated "Design for Maintenance" concepts intended to introduce full-remote recovery functionalities while also optimizing residual maintenance tasks. Experimental results demonstrated the reduction of maintenance duration introduced by the proposed design.

Maintenance activities are assessed in Chapter 6 through an extensive test campaign. The collected data enabled the estimation of the expected intervention time, under realistic conditions, for the most critical tasks. The subsequent analysis highlighted the leading factors that influence the duration of the interventions, such as component location and fixing method. This knowledge contributes to the design process targeted at optimizing maintenance. Additional benefits of the assessment are the validation of proposed design upgrades, the experimental testing of the most effective intervention tools, the identification of potential sources of human errors, the collection of training material and the definition of standardized operating procedures.

A use case intended to demonstrate the potential offered by formal verification techniques to Safety-Critical Control System (SCCS) is finally presented in Chapter 7. The IEC 61499 upgrade of the HHM control software enabled the review of the architecture using a modular approach based on standardized FBs. The presented application aims at providing a real-world example of how an integrated tool-chain may become beneficial for the symbolic model checking of specific properties in the state space of the model. The study showcases how this technique is able to detect non-obvious design flaws, which might be extremely challenging to spot using conventional simulations.

According to the research objectives in Chapter 1, this thesis provides a significant example on how the early incorporation of a PRA in the design stage of safety-critical RH systems can be beneficial for the reduction of personnel exposure during potential recovery scenarios. The study's outcomes, supported by specific experimental results, further emphasize the significance of the approach as an extension of the currently available design protocols in nuclear applications.

One of the research's limitation is the missing integration of the collected data on maintenance tasks duration with the estimated dose rate in the working position. As a future investigation, a comprehensive simulation taking into account the different dose contributions within the SPES ISOL hall at various cooling times will provide an extremely useful asset in the planning of maintenance interventions. In addition, it will enable the HAZOP severity scores adjustment, and thus a more accurate analysis.

Additional room for improvement is available on the evaluation of the PFD of the IEs assessed during the LOPA study. Dynamic Fault Tree Analysiss (DFTAs) in this context would provide a more realistic estimation of the life span of critical components, taking into account additional effects such as the impact of radiations in the aging of materials. Future results will support the development of more focused preventive maintenance plans.

The HHM control software, as last open challenge, will require a further enhancement aimed at improved accuracy. Indeed, while the presented model includes the key elements of the actual system, the introduction of the axes dynamic behavior will help in the creation of a digital-twin of the SPES primary RH system.

Part VI

APPENDIX

A HAZOP WORKSHEETS

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	

Table A.1: HAZOP node: PPB and RIB channels.

Node: PPB and RIB gates							
Deviation: 2. TIS stucked							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		

1. Gate valve failure, open position	1. Remote disconnection of the TIS unit with the gate valve opened.	B/S	C	IV	H	A, B, C, L, M	Improve components' reliability;
							Radiation survey prior to the intervention;
							Work and Dose Planning;
							Maintenance intervention optimization;

	2. Maintenance intervention: repair the equipment (room S018)	B/S	C	V	H	A, B, C, E, F, G, H, I, J, K, M	

Table A.2: HAZOP node: PPB and RIB gates.

Node: PPB and RIB diagnostic							
Deviation: 3. Missing detection							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		

1. Limit switch or potentiometer hardware failure	1. Maintenance intervention: replace the component after the TIS unit removal (room S018)	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K, L, M	Radiation survey prior to the intervention;
							Work and Dose Planning;
							Maintenance intervention optimization;

2. Mechanical misalignments	1. Maintenance intervention: repair the equipment after the TIS unit removal (room S018)	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K, L, M	

Table A.3: HAZOP node: PPB and RIB diagnostic.

Node: Extraction Electrode Positioning System (EEPS)							
Deviation: 4. Motion blocked							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		

1. Pneumatic motor failure	1. Maintenance intervention: motor replacement (room S018)	B/S	C	IV	H	A, B, C, E, F, G, H, I, J, K	Backup actuation interface
							Radiation survey prior to the intervention;
							Work and Dose Planning;
							Maintenance intervention optimization;

2. Mechanical problems (atm.): drive, screw, rotary feedthrough, etc.	1. Maintenance intervention: replacement of the component (room S018)	B/S	C	IV	H	A, B, C, E, F, G, H, I, J, K	
3. Mechanical problems (vac.): rack, pinion, etc.	1. Maintenance intervention: replacement of the component (room S018)	B/S	C	V	H	A, B, C, E, F, G, H, I, J, K	
4. Pneumatic supply failure	1. Maintenance intervention: repair the equipment (room S018)	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K	
	2. Maintenance intervention: repair the equipment (room S017)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	
5. 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	
6. PLC hardware failure	1. Maintenance intervention: repair the equipment (room 1017)	B	C	I	L	A, B, C, G	

Table A.4: HAZOP node: Extraction electrode.

Node: Extraction Electrode Positioning System (EEPS) diagnostic							
Deviation: 5. Missing detection							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		

1. Potentiometer or resolver hardware failure	1. Maintenance intervention: replace the component after the TIS unit removal (room S018)	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K, L, M	Radiation survey prior to the intervention;
							Work and Dose Planning;
							Maintenance intervention optimization;

2. Limit switch hardware failure (vac.)	1. Maintenance intervention: replace the component after the TIS unit removal (room S018)	B/S	C	IV	H	A, B, C, E, F, G, H, I, J, K, L, M	
3. Mechanical misalignments	1. Maintenance intervention: repair the equipment after the TIS unit removal (room S018)	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K, L, M	

Table A.5: HAZOP node: Extraction electrode diagnostic.

Node: TIS unit connections							
Deviation: 6. TIS stucked							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		

1. Mechanical problems: connections failure	1. Maintenance intervention: repair the equipment (room S018)	B/S	C	IV	H	A, B, C, E, F, G, H, I, J, K, L, M	Radiation survey prior to the intervention;
							Work and Dose Planning;
							Maintenance intervention optimization;

	2. Maintenance intervention: repair the equipment after the TIS unit removal (room S018)	B/S	C	III	M	A, B, C, E, F, G, H, I, J, K, L, M	

Table A.6: HAZOP node: TIS unit connections.

Node: HHM compensation module							
Deviation: 7. Leak of gripper positioning/stability							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		

1. Hardware failure	1. Maintenance intervention: repair the equipment (room S016)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	Improve components' reliability;
							Radiation survey prior to the intervention;
							Work and Dose Planning;
							Maintenance intervention optimization;

2. Mechanical misalignments	1. Maintenance intervention: repair the equipment (room S016)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	

Table A.7: HAZOP node: HHM compensation module.

Node: HHM gripper							
Deviation: 8. Gripper doesn't close, TIS unit grasp not possible							
Causes	Consequences	Category	Risk Matrix			Safeguards	Recommendations
			L	S	R		

1. Pneumatic supply failure	1. Maintenance intervention: repair the equipment (room S016)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	Improve components' reliability;
							Radiation survey prior to the intervention;
							Work and Dose Planning;
							Maintenance intervention optimization;
							Development of recovery plans;
							Use of fail-safe gripper;
							Assessment of human reliability;

2. Mechanical hardware failure	1. Maintenance intervention: repair the equipment (room S016)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	
Deviation: 9. Missing compressed air							
1. Compressor, electrovalve, or PLC hardware failure	1. Maintenance intervention: repair the equipment (room S016)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	
Deviation: 10. Gripper doesn't open, TIS unit release not possible							
1. Pneumatic supply failure	1. Maintenance intervention: repair the equipment (room S016)	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K	
2. Mechanical hardware failure	1. Maintenance intervention: repair the equipment (room S016), release through the backup gripper	B/S	C	I	L	A, B, C, D, E, F, G, H, I, J, K	
Deviation: 11. TIS unit release during the transport from Front-End to Temporary Storage System							
1. Mechanical hardware failure	1. Remote insepction and recovery with a dedicated robotic system	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K, M	
2. Pneumatic supply failure	1. Remote insepction and recovery with a dedicated robotic system	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K, M	
3. Wrong command	1. Remote insepction and recovery with a dedicated robotic system	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K, M	
4. Electrical failure	1. Remote insepction and recovery with a dedicated robotic system	B/S	C	I	L	A, B, C, E, F, G, H, I, J, K, M	
5. Generic failure	1. Personnel inspection and manual recovery	B/S	C	V	H	A, B, C, E, F, G, H, I, J, K, M	

Table A.8: HAZOP node: HHM gripper.

B

LOPA WORKSHEETS

Node: PPB and RIB channels													
Deviation: 1. Motion blocked													
		Initial frequency [yr $^{-1}$]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr $^{-1}$]	Mitigated frequency with partial IPLs implemented [yr $^{-1}$]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
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

Table B.1: LOPA ID 1: PPB and RIB channels.

Node: PPB and RIB gates													
Deviation: 2. TIS stucked													
		Initial frequency [yr^{-1}]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr^{-1}]	Mitigated frequency with partial IPLs implemented [yr^{-1}]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
1. Gate valve failure, open position	2. Maintenance intervention: repair the equipment (room S018)	0.01	0.25	-	0.01*	-	0.1	0.1	1	-	-	2.50E-07	2.50E-05
											Total:	2.50E-07	2.50E-05

Table B.2: LOPA ID 2: PPB and RIB gates.

Node: PPB and RIB diagnostic												
Deviation: 3. Missing detection												
		Initial frequency [yr^{-1}]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr^{-1}]	Mitigated frequency with partial IPLs implemented [yr^{-1}]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
1. Limit switch or potentiometer hardware failure	1. Maintenance intervention: replace the component after the TIS unit removal (room S018)	0.2	0.25	0.1*	0.01*	0.1*	0.1	0.1	1	-	0.1*	5.00E-09	5.00E-04
2. Mechanical misalignments	1. Maintenance intervention: repair the equipment after the TIS unit removal (room S018)	0.1	0.25	0.1*	0.01*	-	0.1	0.1	1	-	-	2.50E-07	2.50E-04
											Total:	2.55E-07	7.50E-04

Table B.3: LOPA ID 3: PPB and RIB diagnostic.

Node: Extraction Electrode Positioning System (EEPS)													
Deviation: 4. Motion blocked													
		Initial frequency [yr^{-1}]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr^{-1}]	Mitigated frequency with partial IPLs implemented [yr^{-1}]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
1. Pneumatic motor failure	1. Maintenance intervention: motor replacement (room S018)	0.1	0.25	0.1*	0.01*	0.1*	0.1	-	1	-	-	2.50E-07	2.50E-03
2. Mechanical problems (atm.): drive, screw, rotary feed., etc.	1. Maintenance intervention: replacement of the component (room S018)	0.1	0.25	-	0.01*	0.1*	0.1	-	1	-	-	2.50E-06	2.50E-03
4. Pneumatic supply failure	1. Maintenance intervention: inspection and repair (room S018)	0.1	0.25	0.1*	0.01*	0.1*	0.1	0.1	1	-	-	1.25E-07	1.25E-03
											Total:	2.88E-06*	6.25E-03

Table B.4: LOPA ID 4: Extraction Electrode Positioning System (EEPS).

Node: Extraction Electrode Positioning System (EEPS) diagnostic													
Deviation: 5. Missing detection													
		Initial frequency [yr^{-1}]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr^{-1}]	Mitigated frequency with partial IPLs implemented [yr^{-1}]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
1. Potentiometer or resolver hardware failure	1. Maintenance intervention: replace the component after the TIS unit removal (room S018)	0.2	0.25	0.1*	0.01*	-	0.1	-	1	-	0.1*	5.00E-07	5.00E-03
3. Mechanical misalignments	1. Maintenance intervention: repair the equipment after the TIS unit removal (room S018)	0.1	0.25	0.1*	0.01*	-	0.1	-	1	-	-	2.50E-06	2.50E-03
											Total:	3.00E-06*	7.50E-03

Table B.5: LOPA ID 5: Extraction Electrode Positioning System (EEPS) diagnostic.

Node: TIS unit connections													
Deviation: 6. TIS stucked													
		Initial frequency [yr^{-1}]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr^{-1}]	Mitigated frequency with partial IPLs implemented [yr^{-1}]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
1. Mechanical problems: connections failure	1. Maintenance intervention: repair the equipment (room S018)	0.2	0.25	0.1*	0.01*	0.1*	0.1	-	1	-	-	5.00E-07	5.00E-03
1. Mechanical problems: connections failure	2. Maintenance intervention: repair the equipment after the TIS unit removal (room S018)	0.5	0.25	0.1*	0.01*	0.1*	0.1	0.1	1	-	-	1.25E-07	1.25E-03
											Total:	6.25E-07	6.25E-03

Table B.6: LOPA ID 6: TIS unit connections.

Node: HHM gripper													
Deviation: 11. TIS unit release during the transport from Front-End to Temporary Storage System													
		Initial frequency [yr^{-1}]	ECs	IPLs					CMs			Mitigated frequency with all IPLs implemented [yr^{-1}]	Mitigated frequency with partial IPLs implemented [yr^{-1}]
Initiating Event:	Consequence		Facility under maintenance	Control System, MPS, Autotest	Training of specialized operators, Use of PPEs, Procedures	Periodic maintenance, inspection and replacement program	Access Control System (ACS), Radiation monitoring, Personal dosimeters	Remote inspections using the Horizontal Handling Machine (HHM)	Operator Presence	Backup actuation systems	MPS override		
5. Generic failure	1. Personnel inspection and manual recovery	0.5	0.25	0.1*	0.01*	0.1*	0.1	-	1	-	-	1.25E-06	1.25E-02
											Total:	1.25E-06*	1.25E-02

Table B.7: LOPA ID 11: HHM gripper.

C

MAINTENANCE TESTS WORKSHEETS

COMPARISON SESSION

Node: Extraction Electrode																
Component: Motor																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	32 s
1	2	24	F	1.70 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	33 s
2	1	33	F	1.67 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	30 s
2	2	33	F	1.67 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	29 s
3	1	33	M	1.83 m	Competent	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	34 s
3	2	33	M	1.83 m	Competent	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	25 s
4	1	27	M	1.68 m	Competent	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	27 s
4	2	27	M	1.68 m	Competent	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	30 s
5	1	31	F	1.58 m	Competent	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	27 s
5	2	31	F	1.58 m	Competent	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	28 s
6	1	35	M	1.65 m	Expert	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	31 s
6	2	35	M	1.65 m	Expert	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	32 s
7	1	23	F	1.68 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	26 s
7	2	23	F	1.68 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	26 s
8	1	29	M	1.81 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	59 s
8	2	29	M	1.81 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	41 s
9	1	32	F	1.58 m	Expert	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	29 s
9	2	32	F	1.58 m	Expert	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	27 s
10	1	28	M	1.73 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	29 s
10	2	28	M	1.73 m	Beginner	EL	M	D	O	5.0 m	1.6 m	L	Y	1.4 kg	2	26 s
1	1	24	F	1.70 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s
1	2	24	F	1.70 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	46 s
2	1	33	F	1.67 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s
2	2	33	F	1.67 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	45 s
3	1	33	M	1.83 m	Competent	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	52 s
3	2	33	M	1.83 m	Competent	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	56 s
4	1	27	M	1.68 m	Competent	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	40 s
4	2	27	M	1.68 m	Competent	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	46 s
5	1	31	F	1.58 m	Competent	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	51 s
5	2	31	F	1.58 m	Competent	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	49 s
6	1	35	M	1.65 m	Expert	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	36 s
6	2	35	M	1.65 m	Expert	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	32 s
7	1	23	F	1.68 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	45 s
7	2	23	F	1.68 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	39 s
8	1	29	M	1.81 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	49 s
8	2	29	M	1.81 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	57 s
9	1	32	F	1.58 m	Expert	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	42 s
9	2	32	F	1.58 m	Expert	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s
10	1	28	M	1.73 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	47 s
10	2	28	M	1.73 m	Beginner	EL	M	M	O	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s

Table C.1: EEPS motor replacement test worksheet, old design, left side.

Node: Extraction Electrode																
Component: Motor																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	21 s
1	2	24	F	1.70 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	20 s
2	1	33	F	1.67 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	16 s
2	2	33	F	1.67 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	15 s
3	1	33	M	1.83 m	Competent	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	23 s
3	2	33	M	1.83 m	Competent	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	23 s
4	1	27	M	1.68 m	Competent	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	17 s
4	2	27	M	1.68 m	Competent	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	18 s
5	1	31	F	1.58 m	Competent	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	18 s
5	2	31	F	1.58 m	Competent	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	20 s
6	1	35	M	1.65 m	Expert	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	18 s
6	2	35	M	1.65 m	Expert	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	17 s
7	1	23	F	1.68 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	20 s
7	2	23	F	1.68 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	19 s
8	1	29	M	1.81 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	21 s
8	2	29	M	1.81 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	20 s
9	1	32	F	1.58 m	Expert	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	22 s
9	2	32	F	1.58 m	Expert	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	19 s
10	1	28	M	1.73 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	18 s
10	2	28	M	1.73 m	Beginner	EL	M	D	N	5.0 m	1.6 m	L	Y	1.4 kg	0	15 s
1	1	24	F	1.70 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	24 s
1	2	24	F	1.70 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	25 s
2	1	33	F	1.67 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	29 s
2	2	33	F	1.67 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	28 s
3	1	33	M	1.83 m	Competent	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	27 s
3	2	33	M	1.83 m	Competent	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	28 s
4	1	27	M	1.68 m	Competent	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	24 s
4	2	27	M	1.68 m	Competent	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	24 s
5	1	31	F	1.58 m	Competent	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	26 s
5	2	31	F	1.58 m	Competent	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	24 s
6	1	35	M	1.65 m	Expert	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	24 s
6	2	35	M	1.65 m	Expert	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	23 s
7	1	23	F	1.68 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	26 s
7	2	23	F	1.68 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	25 s
8	1	29	M	1.81 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	28 s
8	2	29	M	1.81 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	27 s
9	1	32	F	1.58 m	Expert	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	29 s
9	2	32	F	1.58 m	Expert	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	27 s
10	1	28	M	1.73 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	25 s
10	2	28	M	1.73 m	Beginner	EL	M	M	N	5.0 m	1.6 m	L	Y	1.4 kg	0	28 s

Table C.2: EEPS motor replacement test worksheet, new design, left side.

Node: Extraction Electrode																
Component: Motor																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	15 s
1	2	24	F	1.70 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	14 s
2	1	33	F	1.67 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	12 s
2	2	33	F	1.67 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	13 s
3	1	33	M	1.83 m	Competent	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	14 s
3	2	33	M	1.83 m	Competent	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	13 s
4	1	27	M	1.68 m	Competent	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	13 s
4	2	27	M	1.68 m	Competent	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	13 s
5	1	31	F	1.58 m	Competent	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	15 s
5	2	31	F	1.58 m	Competent	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	16 s
6	1	35	M	1.65 m	Expert	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	12 s
6	2	35	M	1.65 m	Expert	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	11 s
7	1	23	F	1.68 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	14 s
7	2	23	F	1.68 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	15 s
8	1	29	M	1.81 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	13 s
8	2	29	M	1.81 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	14 s
9	1	32	F	1.58 m	Expert	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	16 s
9	2	32	F	1.58 m	Expert	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	15 s
10	1	28	M	1.73 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	13 s
10	2	28	M	1.73 m	Beginner	EL	M	D	N	5.0 m	1.6 m	R	N	1.4 kg	0	13 s
1	1	24	F	1.70 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
1	2	24	F	1.70 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
2	1	33	F	1.67 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	19 s
2	2	33	F	1.67 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	21 s
3	1	33	M	1.83 m	Competent	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
3	2	33	M	1.83 m	Competent	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	19 s
4	1	27	M	1.68 m	Competent	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	17 s
4	2	27	M	1.68 m	Competent	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
5	1	31	F	1.58 m	Competent	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
5	2	31	F	1.58 m	Competent	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
6	1	35	M	1.65 m	Expert	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
6	2	35	M	1.65 m	Expert	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	16 s
7	1	23	F	1.68 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
7	2	23	F	1.68 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	19 s
8	1	29	M	1.81 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
8	2	29	M	1.81 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	16 s
9	1	32	F	1.58 m	Expert	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	21 s
9	2	32	F	1.58 m	Expert	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	20 s
10	1	28	M	1.73 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	18 s
10	2	28	M	1.73 m	Beginner	EL	M	M	N	5.0 m	1.6 m	R	N	1.4 kg	0	20 s

Table C.3: EEPS motor replacement test worksheet, new design, right side.

Node: Extraction Electrode																
Component: Flange																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
2	1	33	F	1.67 m	Beginner	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	862 s
3	1	33	M	1.83 m	Competent	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	627 s
4	1	27	M	1.68 m	Competent	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	603 s
5	1	31	F	1.58 m	Competent	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	673 s
6	1	35	M	1.65 m	Expert	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	623 s
8	1	29	M	1.81 m	Beginner	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	583 s
9	1	32	F	1.58 m	Expert	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	535 s
10	1	28	M	1.73 m	Beginner	EL	F	D	O	5.0 m	1.6 m	L	Y	12.9 kg	16	610 s
2	1	33	F	1.67 m	Beginner	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	778 s
3	1	33	M	1.83 m	Competent	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	768 s
4	1	27	M	1.68 m	Competent	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	533 s
5	1	31	F	1.58 m	Competent	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	694 s
6	1	35	M	1.65 m	Expert	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	960 s
8	1	29	M	1.81 m	Beginner	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	952 s
9	1	32	F	1.58 m	Expert	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	640 s
10	1	28	M	1.73 m	Beginner	EL	F	M	O	5.0 m	1.6 m	L	Y	12.9 kg	16	588 s

Table C.4: EEPS flange replacement test worksheet, old design.

Node: Extraction Electrode																
Component: Flange																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	90 s
1	2	24	F	1.70 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	78 s
2	1	33	F	1.67 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	108 s
2	2	33	F	1.67 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	92 s
3	1	33	M	1.83 m	Competent	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	78 s
3	2	33	M	1.83 m	Competent	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	84 s
4	1	27	M	1.68 m	Competent	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	94 s
4	2	27	M	1.68 m	Competent	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	82 s
5	1	31	F	1.58 m	Competent	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	98 s
5	2	31	F	1.58 m	Competent	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	106 s
6	1	35	M	1.65 m	Expert	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	50 s
6	2	35	M	1.65 m	Expert	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	54 s
7	1	23	F	1.68 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	74 s
7	2	23	F	1.68 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	80 s
8	1	29	M	1.81 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	86 s
8	2	29	M	1.81 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	82 s
9	1	32	F	1.58 m	Expert	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	100 s
9	2	32	F	1.58 m	Expert	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	76 s
10	1	28	M	1.73 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	86 s
10	2	28	M	1.73 m	Beginner	EL	F	D	N	5.0 m	1.6 m	L	Y	13.4 kg	0	92 s
1	1	24	F	1.70 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	88 s
1	2	24	F	1.70 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	83 s
2	1	33	F	1.67 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	83 s
2	2	33	F	1.67 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	78 s
3	1	33	M	1.83 m	Competent	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	82 s
3	2	33	M	1.83 m	Competent	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	84 s
4	1	27	M	1.68 m	Competent	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	96 s
4	2	27	M	1.68 m	Competent	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	76 s
5	1	31	F	1.58 m	Competent	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	102 s
5	2	31	F	1.58 m	Competent	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	95 s
6	1	35	M	1.65 m	Expert	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	110 s
6	2	35	M	1.65 m	Expert	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	77 s
7	1	23	F	1.68 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	104 s
7	2	23	F	1.68 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	86 s
8	1	29	M	1.81 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	100 s
8	2	29	M	1.81 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	94 s
9	1	32	F	1.58 m	Expert	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	107 s
9	2	32	F	1.58 m	Expert	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	85 s
10	1	28	M	1.73 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	84 s
10	2	28	M	1.73 m	Beginner	EL	F	M	N	5.0 m	1.6 m	L	Y	13.4 kg	0	90 s

Table C.5: EEPS flange replacement test worksheet, new design.

Node: Proton Gate																
Component: Potentiometer																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	32	M	1.84 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	61 s
1	2	32	M	1.84 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	65 s
1	3	32	M	1.84 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	58 s
2	1	27	M	1.68 m	Competent	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	74 s
2	2	27	M	1.68 m	Competent	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	68 s
2	3	27	M	1.68 m	Competent	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	73 s
3	1	32	F	1.58 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	61 s
3	2	32	F	1.58 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	61 s
3	3	32	F	1.58 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	61 s
4	1	35	M	1.65 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	50 s
4	2	35	M	1.65 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	63 s
4	3	35	M	1.65 m	Expert	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	47 s
5	1	31	F	1.58 m	Beginner	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	82 s
5	2	31	F	1.58 m	Beginner	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	70 s
5	3	31	F	1.58 m	Beginner	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	93 s
6	1	33	F	1.67 m	Beginner	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	98 s
6	2	33	F	1.67 m	Beginner	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	95 s
6	3	33	F	1.67 m	Beginner	PG	P	D	O	5.0 m	1.9 m	L	Y	0.1 kg	2	95 s
1	1	32	M	1.84 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	91 s
1	2	32	M	1.84 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	81 s
1	3	32	M	1.84 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	74 s
2	1	27	M	1.68 m	Competent	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	89 s
2	2	27	M	1.68 m	Competent	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	90 s
2	3	27	M	1.68 m	Competent	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	89 s
3	1	32	F	1.58 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	80 s
3	2	32	F	1.58 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	73 s
3	3	32	F	1.58 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	69 s
4	1	35	M	1.65 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	90 s
4	2	35	M	1.65 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	81 s
4	3	35	M	1.65 m	Expert	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	109 s
5	1	31	F	1.58 m	Beginner	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	85 s
5	2	31	F	1.58 m	Beginner	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	81 s
5	3	31	F	1.58 m	Beginner	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	73 s
6	1	33	F	1.67 m	Beginner	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	109 s
6	2	33	F	1.67 m	Beginner	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	114 s
6	3	33	F	1.67 m	Beginner	PG	P	M	O	5.0 m	1.9 m	L	Y	0.1 kg	2	116 s

Table C.6: Proton gate potentiometer replacement test worksheet, old design.

Node: Proton Gate																
Component: Potentiometer																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	32	M	1.84 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
1	2	32	M	1.84 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
1	3	32	M	1.84 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
2	1	27	M	1.68 m	Competent	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	24 s
2	2	27	M	1.68 m	Competent	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
2	3	27	M	1.68 m	Competent	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	20 s
3	1	32	F	1.58 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
3	2	32	F	1.58 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	22 s
3	3	32	F	1.58 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
4	1	35	M	1.65 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
4	2	35	M	1.65 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	17 s
4	3	35	M	1.65 m	Expert	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
5	1	31	F	1.58 m	Beginner	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	28 s
5	2	31	F	1.58 m	Beginner	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	22 s
5	3	31	F	1.58 m	Beginner	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
6	1	33	F	1.67 m	Beginner	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	22 s
6	2	33	F	1.67 m	Beginner	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	17 s
6	3	33	F	1.67 m	Beginner	PG	P	D	N	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
1	1	32	M	1.84 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	29 s
1	2	32	M	1.84 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	26 s
1	3	32	M	1.84 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	28 s
2	1	27	M	1.68 m	Competent	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	29 s
2	2	27	M	1.68 m	Competent	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	26 s
2	3	27	M	1.68 m	Competent	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s
3	1	32	F	1.58 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	37 s
3	2	32	F	1.58 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	28 s
3	3	32	F	1.58 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	25 s
4	1	35	M	1.65 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	30 s
4	2	35	M	1.65 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	30 s
4	3	35	M	1.65 m	Expert	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	32 s
5	1	31	F	1.58 m	Beginner	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	29 s
5	2	31	F	1.58 m	Beginner	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	30 s
5	3	31	F	1.58 m	Beginner	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	32 s
6	1	33	F	1.67 m	Beginner	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	29 s
6	2	33	F	1.67 m	Beginner	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	26 s
6	3	33	F	1.67 m	Beginner	PG	P	M	N	5.0 m	1.9 m	L	Y	0.1 kg	0	33 s

Table C.7: Proton gate potentiometer replacement test worksheet, new design.

Node: RIB Channel																
Component: Limit Switch																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	32	M	1.84 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	32 s
1	2	32	M	1.84 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	33 s
1	3	32	M	1.84 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	33 s
2	1	27	M	1.68 m	Competent	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	31 s
2	2	27	M	1.68 m	Competent	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	26 s
2	3	27	M	1.68 m	Competent	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	27 s
3	1	32	F	1.58 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	27 s
3	2	32	F	1.58 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	21 s
3	3	32	F	1.58 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	20 s
4	1	35	M	1.65 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	37 s
4	2	35	M	1.65 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	30 s
4	3	35	M	1.65 m	Expert	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	31 s
5	1	31	F	1.58 m	Beginner	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	24 s
5	2	31	F	1.58 m	Beginner	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	26 s
5	3	31	F	1.58 m	Beginner	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	23 s
6	1	33	F	1.67 m	Beginner	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	32 s
6	2	33	F	1.67 m	Beginner	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	29 s
6	3	33	F	1.67 m	Beginner	RC	S	D	O	3.8 m	0.9 m	R	N	0.1 kg	2	32 s
1	1	32	M	1.84 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	55 s
1	2	32	M	1.84 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	46 s
1	3	32	M	1.84 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	50 s
2	1	27	M	1.68 m	Competent	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	43 s
2	2	27	M	1.68 m	Competent	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	51 s
2	3	27	M	1.68 m	Competent	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	44 s
3	1	32	F	1.58 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	32 s
3	2	32	F	1.58 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	29 s
3	3	32	F	1.58 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	25 s
4	1	35	M	1.65 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	35 s
4	2	35	M	1.65 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	37 s
4	3	35	M	1.65 m	Expert	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	37 s
5	1	31	F	1.58 m	Beginner	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	50 s
5	2	31	F	1.58 m	Beginner	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	67 s
5	3	31	F	1.58 m	Beginner	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	38 s
6	1	33	F	1.67 m	Beginner	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	50 s
6	2	33	F	1.67 m	Beginner	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	36 s
6	3	33	F	1.67 m	Beginner	RC	S	M	O	3.8 m	0.9 m	R	N	0.1 kg	2	45 s

Table C.8: RIB channel limit switch replacement test worksheet, old design.

Node: RIB Channel																
Component: Limit Switch																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Design	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	32	M	1.84 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
1	2	32	M	1.84 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
1	3	32	M	1.84 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
2	1	27	M	1.68 m	Competent	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
2	2	27	M	1.68 m	Competent	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
2	3	27	M	1.68 m	Competent	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
3	1	32	F	1.58 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
3	2	32	F	1.58 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
3	3	32	F	1.58 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
4	1	35	M	1.65 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
4	2	35	M	1.65 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
4	3	35	M	1.65 m	Expert	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
5	1	31	F	1.58 m	Beginner	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
5	2	31	F	1.58 m	Beginner	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
5	3	31	F	1.58 m	Beginner	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
6	1	33	F	1.67 m	Beginner	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
6	2	33	F	1.67 m	Beginner	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
6	3	33	F	1.67 m	Beginner	RC	S	D	N	3.8 m	0.9 m	R	N	0.1 kg	0	11 s
1	1	32	M	1.84 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	24 s
1	2	32	M	1.84 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	23 s
1	3	32	M	1.84 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	23 s
2	1	27	M	1.68 m	Competent	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	18 s
2	2	27	M	1.68 m	Competent	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	20 s
2	3	27	M	1.68 m	Competent	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	18 s
3	1	32	F	1.58 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	22 s
3	2	32	F	1.58 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	18 s
3	3	32	F	1.58 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
4	1	35	M	1.65 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	20 s
4	2	35	M	1.65 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	19 s
4	3	35	M	1.65 m	Expert	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
5	1	31	F	1.58 m	Beginner	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	26 s
5	2	31	F	1.58 m	Beginner	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	20 s
5	3	31	F	1.58 m	Beginner	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	21 s
6	1	33	F	1.67 m	Beginner	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	23 s
6	2	33	F	1.67 m	Beginner	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	23 s
6	3	33	F	1.67 m	Beginner	RC	S	M	N	3.8 m	0.9 m	R	N	0.1 kg	0	15 s

Table C.9: RIB channel limit switch replacement test worksheet, new design.

Node: Proton Channel																
Component: Motor																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Tool	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	32	M	1.84 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
1	2	32	M	1.84 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	25 s
1	3	32	M	1.84 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	27 s
2	1	27	M	1.68 m	Competent	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	25 s
2	2	27	M	1.68 m	Competent	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
2	3	27	M	1.68 m	Competent	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	23 s
3	1	32	F	1.58 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	29 s
3	2	32	F	1.58 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	27 s
3	3	32	F	1.58 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	24 s
4	1	35	M	1.65 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	32 s
4	2	35	M	1.65 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	38 s
4	3	35	M	1.65 m	Expert	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	23 s
5	1	31	F	1.58 m	Beginner	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	40 s
5	2	31	F	1.58 m	Beginner	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	37 s
5	3	31	F	1.58 m	Beginner	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	29 s
6	1	33	F	1.67 m	Beginner	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	25 s
6	2	33	F	1.67 m	Beginner	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	30 s
6	3	33	F	1.67 m	Beginner	PC	M	D	A	3.8 m	1.4 m	L	N	1.4 kg	2	28 s
1	1	32	M	1.84 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	35 s
1	2	32	M	1.84 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	34 s
1	3	32	M	1.84 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	38 s
2	1	27	M	1.68 m	Competent	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	45 s
2	2	27	M	1.68 m	Competent	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	37 s
2	3	27	M	1.68 m	Competent	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	41 s
3	1	32	F	1.58 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	40 s
3	2	32	F	1.58 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	36 s
3	3	32	F	1.58 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	36 s
4	1	35	M	1.65 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	39 s
4	2	35	M	1.65 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	41 s
4	3	35	M	1.65 m	Expert	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	49 s
5	1	31	F	1.58 m	Beginner	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	74 s
5	2	31	F	1.58 m	Beginner	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	58 s
5	3	31	F	1.58 m	Beginner	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	65 s
6	1	33	F	1.67 m	Beginner	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	44 s
6	2	33	F	1.67 m	Beginner	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	42 s
6	3	33	F	1.67 m	Beginner	PC	M	M	A	3.8 m	1.4 m	L	N	1.4 kg	2	42 s

Table C.10: Proton channel limit switch replacement test worksheet, tool A.

Node: Proton Channel																
Component: Motor																
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Tool	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	32	M	1.84 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	19 s
1	2	32	M	1.84 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	18 s
1	3	32	M	1.84 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	21 s
2	1	27	M	1.68 m	Competent	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	18 s
2	2	27	M	1.68 m	Competent	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	18 s
2	3	27	M	1.68 m	Competent	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	18 s
3	1	32	F	1.58 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	25 s
3	2	32	F	1.58 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	23 s
3	3	32	F	1.58 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	19 s
4	1	35	M	1.65 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	17 s
4	2	35	M	1.65 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	21 s
4	3	35	M	1.65 m	Expert	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	21 s
5	1	31	F	1.58 m	Beginner	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	38 s
5	2	31	F	1.58 m	Beginner	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	33 s
5	3	31	F	1.58 m	Beginner	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	30 s
6	1	33	F	1.67 m	Beginner	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	20 s
6	2	33	F	1.67 m	Beginner	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	21 s
6	3	33	F	1.67 m	Beginner	PC	M	D	B	3.8 m	1.4 m	L	N	1.4 kg	2	21 s
1	1	32	M	1.84 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	28 s
1	2	32	M	1.84 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
1	3	32	M	1.84 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	24 s
2	1	27	M	1.68 m	Competent	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	28 s
2	2	27	M	1.68 m	Competent	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	27 s
2	3	27	M	1.68 m	Competent	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	23 s
3	1	32	F	1.58 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	36 s
3	2	32	F	1.58 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	34 s
3	3	32	F	1.58 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
4	1	35	M	1.65 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	35 s
4	2	35	M	1.65 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
4	3	35	M	1.65 m	Expert	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	28 s
5	1	31	F	1.58 m	Beginner	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	46 s
5	2	31	F	1.58 m	Beginner	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	50 s
5	3	31	F	1.58 m	Beginner	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	35 s
6	1	33	F	1.67 m	Beginner	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
6	2	33	F	1.67 m	Beginner	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	30 s
6	3	33	F	1.67 m	Beginner	PC	M	M	B	3.8 m	1.4 m	L	N	1.4 kg	2	34 s

Table C.11: Proton channel limit switch replacement test worksheet, tool B.

SURVEY SESSION

Node: Proton Channel															
Component: Motor															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	20 s
1	2	24	F	1.70 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	27 s
2	1	33	F	1.67 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	22 s
2	2	33	F	1.67 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	29 s
3	1	33	M	1.83 m	Competent	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	24 s
3	2	33	M	1.83 m	Competent	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	22 s
4	1	27	M	1.68 m	Competent	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	19 s
4	2	27	M	1.68 m	Competent	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	20 s
5	1	31	F	1.58 m	Competent	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
5	2	31	F	1.58 m	Competent	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	32 s
6	1	35	M	1.65 m	Expert	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	17 s
6	2	35	M	1.65 m	Expert	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	19 s
7	1	23	F	1.68 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	23 s
7	2	23	F	1.68 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	22 s
8	1	29	M	1.81 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	27 s
8	2	29	M	1.81 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	28 s
9	1	32	F	1.58 m	Expert	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	21 s
9	2	32	F	1.58 m	Expert	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	24 s
10	1	28	M	1.73 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	24 s
10	2	28	M	1.73 m	Beginner	PC	M	D	3.8 m	1.4 m	L	N	1.4 kg	2	22 s
1	1	24	F	1.70 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	32 s
1	2	24	F	1.70 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	34 s
2	1	33	F	1.67 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	40 s
2	2	33	F	1.67 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	41 s
3	1	33	M	1.83 m	Competent	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	35 s
3	2	33	M	1.83 m	Competent	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	33 s
4	1	27	M	1.68 m	Competent	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	35 s
4	2	27	M	1.68 m	Competent	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	31 s
5	1	31	F	1.58 m	Competent	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	32 s
5	2	31	F	1.58 m	Competent	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	36 s
6	1	35	M	1.65 m	Expert	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	27 s
6	2	35	M	1.65 m	Expert	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	26 s
7	1	23	F	1.68 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	35 s
7	2	23	F	1.68 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	37 s
8	1	29	M	1.81 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	38 s
8	2	29	M	1.81 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	42 s
9	1	32	F	1.58 m	Expert	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	36 s
9	2	32	F	1.58 m	Expert	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	30 s
10	1	28	M	1.73 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	42 s
10	2	28	M	1.73 m	Beginner	PC	M	M	3.8 m	1.4 m	L	N	1.4 kg	2	27 s

Table C.12: Proton channel motor replacement test worksheet.

Node: RIB Channel															
Component: Motor															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	22 s
1	2	24	F	1.70 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	30 s
2	1	33	F	1.67 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	34 s
2	2	33	F	1.67 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	31 s
3	1	33	M	1.83 m	Competent	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	42 s
3	2	33	M	1.83 m	Competent	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	49 s
4	1	27	M	1.68 m	Competent	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	27 s
4	2	27	M	1.68 m	Competent	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	33 s
5	1	31	F	1.58 m	Competent	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	28 s
5	2	31	F	1.58 m	Competent	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	26 s
6	1	35	M	1.65 m	Expert	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	23 s
6	2	35	M	1.65 m	Expert	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	24 s
7	1	23	F	1.68 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	25 s
7	2	23	F	1.68 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	28 s
8	1	29	M	1.81 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	42 s
8	2	29	M	1.81 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	33 s
9	1	32	F	1.58 m	Expert	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	31 s
9	2	32	F	1.58 m	Expert	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	30 s
10	1	28	M	1.73 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	25 s
10	2	28	M	1.73 m	Beginner	RC	M	D	3.8 m	1.4 m	L	Y	1.4 kg	2	23 s
1	1	24	F	1.70 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	39 s
1	2	24	F	1.70 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	39 s
2	1	33	F	1.67 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	58 s
2	2	33	F	1.67 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	56 s
3	1	33	M	1.83 m	Competent	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	50 s
3	2	33	M	1.83 m	Competent	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	48 s
4	1	27	M	1.68 m	Competent	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	31 s
4	2	27	M	1.68 m	Competent	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	33 s
5	1	31	F	1.58 m	Competent	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	34 s
5	2	31	F	1.58 m	Competent	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	32 s
6	1	35	M	1.65 m	Expert	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	35 s
6	2	35	M	1.65 m	Expert	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	37 s
7	1	23	F	1.68 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	31 s
7	2	23	F	1.68 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	38 s
8	1	29	M	1.81 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	52 s
8	2	29	M	1.81 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	51 s
9	1	32	F	1.58 m	Expert	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	36 s
9	2	32	F	1.58 m	Expert	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	36 s
10	1	28	M	1.73 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	35 s
10	2	28	M	1.73 m	Beginner	RC	M	M	3.8 m	1.4 m	L	Y	1.4 kg	2	34 s

Table C.13: RIB channel motor replacement test worksheet.

Node: Proton Gate															
Component: Motor															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	36 s
1	2	24	F	1.70 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	34 s
2	1	33	F	1.67 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	28 s
2	2	33	F	1.67 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	32 s
3	1	33	M	1.83 m	Competent	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	28 s
3	2	33	M	1.83 m	Competent	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	31 s
4	1	27	M	1.68 m	Competent	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	30 s
4	2	27	M	1.68 m	Competent	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	25 s
5	1	31	F	1.58 m	Competent	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	39 s
5	2	31	F	1.58 m	Competent	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	30 s
6	1	35	M	1.65 m	Expert	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	22 s
6	2	35	M	1.65 m	Expert	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	24 s
7	1	23	F	1.68 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	26 s
7	2	23	F	1.68 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	32 s
8	1	29	M	1.81 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	39 s
8	2	29	M	1.81 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	43 s
9	1	32	F	1.58 m	Expert	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	36 s
9	2	32	F	1.58 m	Expert	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	33 s
10	1	28	M	1.73 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	27 s
10	2	28	M	1.73 m	Beginner	PG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	25 s
1	1	24	F	1.70 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	37 s
1	2	24	F	1.70 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	41 s
2	1	33	F	1.67 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	45 s
2	2	33	F	1.67 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	52 s
3	1	33	M	1.83 m	Competent	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	42 s
3	2	33	M	1.83 m	Competent	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	32 s
4	1	27	M	1.68 m	Competent	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	34 s
4	2	27	M	1.68 m	Competent	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	34 s
5	1	31	F	1.58 m	Competent	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	50 s
5	2	31	F	1.58 m	Competent	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	46 s
6	1	35	M	1.65 m	Expert	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	34 s
6	2	35	M	1.65 m	Expert	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	31 s
7	1	23	F	1.68 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	37 s
7	2	23	F	1.68 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	35 s
8	1	29	M	1.81 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	48 s
8	2	29	M	1.81 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	48 s
9	1	32	F	1.58 m	Expert	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	40 s
9	2	32	F	1.58 m	Expert	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	43 s
10	1	28	M	1.73 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	38 s
10	2	28	M	1.73 m	Beginner	PG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	39 s

Table C.14: Proton gate motor replacement test worksheet.

Node: RIB Gate															
Component: Motor															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	34 s
1	2	24	F	1.70 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	33 s
2	1	33	F	1.67 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	39 s
2	2	33	F	1.67 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	44 s
3	1	33	M	1.83 m	Competent	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	38 s
3	2	33	M	1.83 m	Competent	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	32 s
4	1	27	M	1.68 m	Competent	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	26 s
4	2	27	M	1.68 m	Competent	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	30 s
5	1	31	F	1.58 m	Competent	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	39 s
5	2	31	F	1.58 m	Competent	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	46 s
6	1	35	M	1.65 m	Expert	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	25 s
6	2	35	M	1.65 m	Expert	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	23 s
7	1	23	F	1.68 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	44 s
7	2	23	F	1.68 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	34 s
8	1	29	M	1.81 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	44 s
8	2	29	M	1.81 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	47 s
9	1	32	F	1.58 m	Expert	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	35 s
9	2	32	F	1.58 m	Expert	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	38 s
10	1	28	M	1.73 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	31 s
10	2	28	M	1.73 m	Beginner	RG	M	D	3.8 m	2.2 m	L	N	1.4 kg	2	30 s
1	1	24	F	1.70 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	54 s
1	2	24	F	1.70 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	43 s
2	1	33	F	1.67 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	45 s
2	2	33	F	1.67 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	52 s
3	1	33	M	1.83 m	Competent	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	38 s
3	2	33	M	1.83 m	Competent	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	36 s
4	1	27	M	1.68 m	Competent	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	37 s
4	2	27	M	1.68 m	Competent	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	35 s
5	1	31	F	1.58 m	Competent	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	44 s
5	2	31	F	1.58 m	Competent	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	43 s
6	1	35	M	1.65 m	Expert	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	43 s
6	2	35	M	1.65 m	Expert	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	39 s
7	1	23	F	1.68 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	34 s
7	2	23	F	1.68 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	38 s
8	1	29	M	1.81 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	53 s
8	2	29	M	1.81 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	54 s
9	1	32	F	1.58 m	Expert	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	52 s
9	2	32	F	1.58 m	Expert	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	45 s
10	1	28	M	1.73 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	41 s
10	2	28	M	1.73 m	Beginner	RG	M	M	3.8 m	2.2 m	L	N	1.4 kg	2	39 s

Table C.15: RIB gate motor replacement test worksheet.

Node: Extraction Electrode															
Component: Motor															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	32 s
1	2	24	F	1.70 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	33 s
2	1	33	F	1.67 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	30 s
2	2	33	F	1.67 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	29 s
3	1	33	M	1.83 m	Competent	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	34 s
3	2	33	M	1.83 m	Competent	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	25 s
4	1	27	M	1.68 m	Competent	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	27 s
4	2	27	M	1.68 m	Competent	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	30 s
5	1	31	F	1.58 m	Competent	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	27 s
5	2	31	F	1.58 m	Competent	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	28 s
6	1	35	M	1.65 m	Expert	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	31 s
6	2	35	M	1.65 m	Expert	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	32 s
7	1	23	F	1.68 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	26 s
7	2	23	F	1.68 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	26 s
8	1	29	M	1.81 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	59 s
8	2	29	M	1.81 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	41 s
9	1	32	F	1.58 m	Expert	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	29 s
9	2	32	F	1.58 m	Expert	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	27 s
10	1	28	M	1.73 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	29 s
10	2	28	M	1.73 m	Beginner	EL	M	D	5.0 m	1.6 m	L	Y	1.4 kg	2	26 s
1	1	24	F	1.70 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s
1	2	24	F	1.70 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	46 s
2	1	33	F	1.67 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s
2	2	33	F	1.67 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	45 s
3	1	33	M	1.83 m	Competent	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	52 s
3	2	33	M	1.83 m	Competent	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	56 s
4	1	27	M	1.68 m	Competent	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	40 s
4	2	27	M	1.68 m	Competent	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	46 s
5	1	31	F	1.58 m	Competent	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	51 s
5	2	31	F	1.58 m	Competent	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	49 s
6	1	35	M	1.65 m	Expert	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	36 s
6	2	35	M	1.65 m	Expert	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	32 s
7	1	23	F	1.68 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	45 s
7	2	23	F	1.68 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	39 s
8	1	29	M	1.81 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	49 s
8	2	29	M	1.81 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	57 s
9	1	32	F	1.58 m	Expert	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	42 s
9	2	32	F	1.58 m	Expert	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s
10	1	28	M	1.73 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	47 s
10	2	28	M	1.73 m	Beginner	EL	M	M	5.0 m	1.6 m	L	Y	1.4 kg	2	37 s

Table C.16: Extraction electrode motor replacement test worksheet.

Node: Proton Channel															
Component: Potentiometer															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
1	2	24	F	1.70 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	17 s
2	1	33	F	1.67 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
2	2	33	F	1.67 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
3	1	33	M	1.83 m	Competent	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
3	2	33	M	1.83 m	Competent	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
4	1	27	M	1.68 m	Competent	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
4	2	27	M	1.68 m	Competent	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
5	1	31	F	1.58 m	Competent	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
5	2	31	F	1.58 m	Competent	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
6	1	35	M	1.65 m	Expert	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
6	2	35	M	1.65 m	Expert	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
7	1	23	F	1.68 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
7	2	23	F	1.68 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
8	1	29	M	1.81 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
8	2	29	M	1.81 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
9	1	32	F	1.58 m	Expert	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
9	2	32	F	1.58 m	Expert	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	15 s
10	1	28	M	1.73 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
10	2	28	M	1.73 m	Beginner	PC	P	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
1	1	24	F	1.70 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	18 s
1	2	24	F	1.70 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	21 s
2	1	33	F	1.67 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	26 s
2	2	33	F	1.67 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	23 s
3	1	33	M	1.83 m	Competent	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	22 s
3	2	33	M	1.83 m	Competent	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	21 s
4	1	27	M	1.68 m	Competent	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
4	2	27	M	1.68 m	Competent	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
5	1	31	F	1.58 m	Competent	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	19 s
5	2	31	F	1.58 m	Competent	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	18 s
6	1	35	M	1.65 m	Expert	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
6	2	35	M	1.65 m	Expert	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
7	1	23	F	1.68 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	19 s
7	2	23	F	1.68 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	21 s
8	1	29	M	1.81 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	25 s
8	2	29	M	1.81 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	23 s
9	1	32	F	1.58 m	Expert	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	17 s
9	2	32	F	1.58 m	Expert	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	20 s
10	1	28	M	1.73 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	21 s
10	2	28	M	1.73 m	Beginner	PC	P	M	3.8 m	0.9 m	L	N	0.1 kg	0	18 s

Table C.17: Proton channel potentiometer replacement test worksheet.

Node: RIB Channel															
Component: Potentiometer															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
1	2	24	F	1.70 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
2	1	33	F	1.67 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	10 s
2	2	33	F	1.67 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
3	1	33	M	1.83 m	Competent	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
3	2	33	M	1.83 m	Competent	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
4	1	27	M	1.68 m	Competent	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
4	2	27	M	1.68 m	Competent	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
5	1	31	F	1.58 m	Competent	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
5	2	31	F	1.58 m	Competent	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
6	1	35	M	1.65 m	Expert	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	11 s
6	2	35	M	1.65 m	Expert	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	11 s
7	1	23	F	1.68 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
7	2	23	F	1.68 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
8	1	29	M	1.81 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	21 s
8	2	29	M	1.81 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
9	1	32	F	1.58 m	Expert	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
9	2	32	F	1.58 m	Expert	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
10	1	28	M	1.73 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
10	2	28	M	1.73 m	Beginner	RC	P	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
1	1	24	F	1.70 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	28 s
1	2	24	F	1.70 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	24 s
2	1	33	F	1.67 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	19 s
2	2	33	F	1.67 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	21 s
3	1	33	M	1.83 m	Competent	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	18 s
3	2	33	M	1.83 m	Competent	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	19 s
4	1	27	M	1.68 m	Competent	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
4	2	27	M	1.68 m	Competent	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	19 s
5	1	31	F	1.58 m	Competent	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	23 s
5	2	31	F	1.58 m	Competent	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	18 s
6	1	35	M	1.65 m	Expert	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
6	2	35	M	1.65 m	Expert	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
7	1	23	F	1.68 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	19 s
7	2	23	F	1.68 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	22 s
8	1	29	M	1.81 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	20 s
8	2	29	M	1.81 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	23 s
9	1	32	F	1.58 m	Expert	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	19 s
9	2	32	F	1.58 m	Expert	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	18 s
10	1	28	M	1.73 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	19 s
10	2	28	M	1.73 m	Beginner	RC	P	M	3.8 m	0.9 m	R	N	0.1 kg	0	17 s

Table C.18: RIB channel potentiometer replacement test worksheet.

Node: Proton Gate															
Component: Potentiometer															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s
1	2	24	F	1.70 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
2	1	33	F	1.67 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
2	2	33	F	1.67 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	20 s
3	1	33	M	1.83 m	Competent	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
3	2	33	M	1.83 m	Competent	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	25 s
4	1	27	M	1.68 m	Competent	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
4	2	27	M	1.68 m	Competent	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
5	1	31	F	1.58 m	Competent	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	20 s
5	2	31	F	1.58 m	Competent	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	18 s
6	1	35	M	1.65 m	Expert	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	20 s
6	2	35	M	1.65 m	Expert	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	16 s
7	1	23	F	1.68 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	16 s
7	2	23	F	1.68 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	22 s
8	1	29	M	1.81 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	32 s
8	2	29	M	1.81 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	29 s
9	1	32	F	1.58 m	Expert	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
9	2	32	F	1.58 m	Expert	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
10	1	28	M	1.73 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
10	2	28	M	1.73 m	Beginner	PG	P	D	5.0 m	1.9 m	L	Y	0.1 kg	0	22 s
1	1	24	F	1.70 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	30 s
1	2	24	F	1.70 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	31 s
2	1	33	F	1.67 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	24 s
2	2	33	F	1.67 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	33 s
3	1	33	M	1.83 m	Competent	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	34 s
3	2	33	M	1.83 m	Competent	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	26 s
4	1	27	M	1.68 m	Competent	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	31 s
4	2	27	M	1.68 m	Competent	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s
5	1	31	F	1.58 m	Competent	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	32 s
5	2	31	F	1.58 m	Competent	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	26 s
6	1	35	M	1.65 m	Expert	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s
6	2	35	M	1.65 m	Expert	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	33 s
7	1	23	F	1.68 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
7	2	23	F	1.68 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s
8	1	29	M	1.81 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	53 s
8	2	29	M	1.81 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	36 s
9	1	32	F	1.58 m	Expert	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	24 s
9	2	32	F	1.58 m	Expert	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	25 s
10	1	28	M	1.73 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s
10	2	28	M	1.73 m	Beginner	PG	P	M	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s

Table C.19: Proton gate potentiometer replacement test worksheet.

Node: RIB Gate															
Component: Potentiometer															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	18 s
1	2	24	F	1.70 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	16 s
2	1	33	F	1.67 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	16 s
2	2	33	F	1.67 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	17 s
3	1	33	M	1.83 m	Competent	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	17 s
3	2	33	M	1.83 m	Competent	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	18 s
4	1	27	M	1.68 m	Competent	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	15 s
4	2	27	M	1.68 m	Competent	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	20 s
5	1	31	F	1.58 m	Competent	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	21 s
5	2	31	F	1.58 m	Competent	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	20 s
6	1	35	M	1.65 m	Expert	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	14 s
6	2	35	M	1.65 m	Expert	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	12 s
7	1	23	F	1.68 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	18 s
7	2	23	F	1.68 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	17 s
8	1	29	M	1.81 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	22 s
8	2	29	M	1.81 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	22 s
9	1	32	F	1.58 m	Expert	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	19 s
9	2	32	F	1.58 m	Expert	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	20 s
10	1	28	M	1.73 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	16 s
10	2	28	M	1.73 m	Beginner	RG	P	D	5.0 m	1.9 m	R	N	0.1 kg	0	18 s
1	1	24	F	1.70 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	36 s
1	2	24	F	1.70 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	29 s
2	1	33	F	1.67 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	30 s
2	2	33	F	1.67 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	22 s
3	1	33	M	1.83 m	Competent	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	32 s
3	2	33	M	1.83 m	Competent	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	25 s
4	1	27	M	1.68 m	Competent	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	25 s
4	2	27	M	1.68 m	Competent	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	23 s
5	1	31	F	1.58 m	Competent	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	40 s
5	2	31	F	1.58 m	Competent	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	39 s
6	1	35	M	1.65 m	Expert	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	29 s
6	2	35	M	1.65 m	Expert	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	24 s
7	1	23	F	1.68 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	20 s
7	2	23	F	1.68 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	25 s
8	1	29	M	1.81 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	36 s
8	2	29	M	1.81 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	30 s
9	1	32	F	1.58 m	Expert	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	34 s
9	2	32	F	1.58 m	Expert	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	27 s
10	1	28	M	1.73 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	22 s
10	2	28	M	1.73 m	Beginner	RG	P	M	5.0 m	1.9 m	R	N	0.1 kg	0	20 s

Table C.20: RIB gate potentiometer replacement test worksheet.

Node: Extraction Electrode															
Component: Potentiometer															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	17 s
1	2	24	F	1.70 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	18 s
2	1	33	F	1.67 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	21 s
2	2	33	F	1.67 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	22 s
3	1	33	M	1.83 m	Competent	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	26 s
3	2	33	M	1.83 m	Competent	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	24 s
4	1	27	M	1.68 m	Competent	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	22 s
4	2	27	M	1.68 m	Competent	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	18 s
5	1	31	F	1.58 m	Competent	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	19 s
5	2	31	F	1.58 m	Competent	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	17 s
6	1	35	M	1.65 m	Expert	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	31 s
6	2	35	M	1.65 m	Expert	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	32 s
7	1	23	F	1.68 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	26 s
7	2	23	F	1.68 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	26 s
8	1	29	M	1.81 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	59 s
8	2	29	M	1.81 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	41 s
9	1	32	F	1.58 m	Expert	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	29 s
9	2	32	F	1.58 m	Expert	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	27 s
10	1	28	M	1.73 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	29 s
10	2	28	M	1.73 m	Beginner	EL	P	D	5.0 m	1.6 m	L	Y	0.1 kg	0	26 s
1	1	24	F	1.70 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	24 s
1	2	24	F	1.70 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	23 s
2	1	33	F	1.67 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	29 s
2	2	33	F	1.67 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	29 s
3	1	33	M	1.83 m	Competent	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	27 s
3	2	33	M	1.83 m	Competent	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	26 s
4	1	27	M	1.68 m	Competent	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	23 s
4	2	27	M	1.68 m	Competent	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	23 s
5	1	31	F	1.58 m	Competent	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	28 s
5	2	31	F	1.58 m	Competent	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	22 s
6	1	35	M	1.65 m	Expert	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	22 s
6	2	35	M	1.65 m	Expert	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	21 s
7	1	23	F	1.68 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	27 s
7	2	23	F	1.68 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	31 s
8	1	29	M	1.81 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	37 s
8	2	29	M	1.81 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	35 s
9	1	32	F	1.58 m	Expert	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	25 s
9	2	32	F	1.58 m	Expert	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	24 s
10	1	28	M	1.73 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	25 s
10	2	28	M	1.73 m	Beginner	EL	P	M	5.0 m	1.6 m	L	Y	0.1 kg	0	23 s

Table C.21: Extraction electrode potentiometer replacement test worksheet.

Node: Proton Channel															
Component: Limit Switch															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
1	2	24	F	1.70 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	18 s
2	1	33	F	1.67 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
2	2	33	F	1.67 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
3	1	33	M	1.83 m	Competent	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
3	2	33	M	1.83 m	Competent	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
4	1	27	M	1.68 m	Competent	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
4	2	27	M	1.68 m	Competent	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	13 s
5	1	31	F	1.58 m	Competent	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
5	2	31	F	1.58 m	Competent	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
6	1	35	M	1.65 m	Expert	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	11 s
6	2	35	M	1.65 m	Expert	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
7	1	23	F	1.68 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
7	2	23	F	1.68 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	15 s
8	1	29	M	1.81 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
8	2	29	M	1.81 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	17 s
9	1	32	F	1.58 m	Expert	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	15 s
9	2	32	F	1.58 m	Expert	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
10	1	28	M	1.73 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	12 s
10	2	28	M	1.73 m	Beginner	PC	S	D	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
1	1	24	F	1.70 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	18 s
1	2	24	F	1.70 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	18 s
2	1	33	F	1.67 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	20 s
2	2	33	F	1.67 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
3	1	33	M	1.83 m	Competent	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	17 s
3	2	33	M	1.83 m	Competent	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	19 s
4	1	27	M	1.68 m	Competent	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	14 s
4	2	27	M	1.68 m	Competent	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	15 s
5	1	31	F	1.58 m	Competent	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	15 s
5	2	31	F	1.58 m	Competent	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
6	1	35	M	1.65 m	Expert	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	19 s
6	2	35	M	1.65 m	Expert	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	18 s
7	1	23	F	1.68 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	20 s
7	2	23	F	1.68 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	17 s
8	1	29	M	1.81 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	25 s
8	2	29	M	1.81 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	28 s
9	1	32	F	1.58 m	Expert	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
9	2	32	F	1.58 m	Expert	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
10	1	28	M	1.73 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	16 s
10	2	28	M	1.73 m	Beginner	PC	S	M	3.8 m	0.9 m	L	N	0.1 kg	0	18 s

Table C.22: Proton channel limit switch replacement test worksheet.

Node: RIB Channel															
Component: Limit Switch															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
1	2	24	F	1.70 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
2	1	33	F	1.67 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	10 s
2	2	33	F	1.67 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	11 s
3	1	33	M	1.83 m	Competent	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
3	2	33	M	1.83 m	Competent	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
4	1	27	M	1.68 m	Competent	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
4	2	27	M	1.68 m	Competent	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
5	1	31	F	1.58 m	Competent	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
5	2	31	F	1.58 m	Competent	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
6	1	35	M	1.65 m	Expert	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
6	2	35	M	1.65 m	Expert	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	11 s
7	1	23	F	1.68 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
7	2	23	F	1.68 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
8	1	29	M	1.81 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
8	2	29	M	1.81 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
9	1	32	F	1.58 m	Expert	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
9	2	32	F	1.58 m	Expert	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
10	1	28	M	1.73 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	12 s
10	2	28	M	1.73 m	Beginner	RC	S	D	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
1	1	24	F	1.70 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	23 s
1	2	24	F	1.70 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	20 s
2	1	33	F	1.67 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
2	2	33	F	1.67 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
3	1	33	M	1.83 m	Competent	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
3	2	33	M	1.83 m	Competent	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
4	1	27	M	1.68 m	Competent	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	13 s
4	2	27	M	1.68 m	Competent	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
5	1	31	F	1.58 m	Competent	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
5	2	31	F	1.58 m	Competent	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
6	1	35	M	1.65 m	Expert	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
6	2	35	M	1.65 m	Expert	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
7	1	23	F	1.68 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
7	2	23	F	1.68 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	14 s
8	1	29	M	1.81 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	17 s
8	2	29	M	1.81 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	22 s
9	1	32	F	1.58 m	Expert	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	18 s
9	2	32	F	1.58 m	Expert	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	16 s
10	1	28	M	1.73 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	15 s
10	2	28	M	1.73 m	Beginner	RC	S	M	3.8 m	0.9 m	R	N	0.1 kg	0	14 s

Table C.23: RIB channel limit switch replacement test worksheet.

Node: Proton Gate															
Component: Limit Switch															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	18 s
1	2	24	F	1.70 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
2	1	33	F	1.67 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	17 s
2	2	33	F	1.67 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	20 s
3	1	33	M	1.83 m	Competent	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
3	2	33	M	1.83 m	Competent	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	24 s
4	1	27	M	1.68 m	Competent	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	24 s
4	2	27	M	1.68 m	Competent	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	20 s
5	1	31	F	1.58 m	Competent	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
5	2	31	F	1.58 m	Competent	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	18 s
6	1	35	M	1.65 m	Expert	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
6	2	35	M	1.65 m	Expert	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	17 s
7	1	23	F	1.68 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	19 s
7	2	23	F	1.68 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
8	1	29	M	1.81 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	31 s
8	2	29	M	1.81 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	28 s
9	1	32	F	1.58 m	Expert	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
9	2	32	F	1.58 m	Expert	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	20 s
10	1	28	M	1.73 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
10	2	28	M	1.73 m	Beginner	PG	S	D	5.0 m	1.9 m	L	Y	0.1 kg	0	22 s
1	1	24	F	1.70 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	25 s
1	2	24	F	1.70 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	26 s
2	1	33	F	1.67 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	29 s
2	2	33	F	1.67 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	32 s
3	1	33	M	1.83 m	Competent	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
3	2	33	M	1.83 m	Competent	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	28 s
4	1	27	M	1.68 m	Competent	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	30 s
4	2	27	M	1.68 m	Competent	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
5	1	31	F	1.58 m	Competent	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	24 s
5	2	31	F	1.58 m	Competent	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	28 s
6	1	35	M	1.65 m	Expert	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	21 s
6	2	35	M	1.65 m	Expert	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	27 s
7	1	23	F	1.68 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	30 s
7	2	23	F	1.68 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	25 s
8	1	29	M	1.81 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	46 s
8	2	29	M	1.81 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	43 s
9	1	32	F	1.58 m	Expert	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	23 s
9	2	32	F	1.58 m	Expert	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	29 s
10	1	28	M	1.73 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	26 s
10	2	28	M	1.73 m	Beginner	PG	S	M	5.0 m	1.9 m	L	Y	0.1 kg	0	24 s

Table C.24: Proton gate limit switch replacement test worksheet.

Node: RIB Gate															
Component: Limit Switch															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	13 s
1	2	24	F	1.70 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	14 s
2	1	33	F	1.67 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	12 s
2	2	33	F	1.67 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	13 s
3	1	33	M	1.83 m	Competent	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	14 s
3	2	33	M	1.83 m	Competent	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	13 s
4	1	27	M	1.68 m	Competent	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	16 s
4	2	27	M	1.68 m	Competent	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	15 s
5	1	31	F	1.58 m	Competent	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	15 s
5	2	31	F	1.58 m	Competent	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	16 s
6	1	35	M	1.65 m	Expert	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	12 s
6	2	35	M	1.65 m	Expert	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	12 s
7	1	23	F	1.68 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	15 s
7	2	23	F	1.68 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	18 s
8	1	29	M	1.81 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	17 s
8	2	29	M	1.81 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	16 s
9	1	32	F	1.58 m	Expert	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	18 s
9	2	32	F	1.58 m	Expert	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	16 s
10	1	28	M	1.73 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	14 s
10	2	28	M	1.73 m	Beginner	RG	S	D	5.0 m	1.9 m	R	N	0.1 kg	0	17 s
1	1	24	F	1.70 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	20 s
1	2	24	F	1.70 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	24 s
2	1	33	F	1.67 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	20 s
2	2	33	F	1.67 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	21 s
3	1	33	M	1.83 m	Competent	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	24 s
3	2	33	M	1.83 m	Competent	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	22 s
4	1	27	M	1.68 m	Competent	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	21 s
4	2	27	M	1.68 m	Competent	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	25 s
5	1	31	F	1.58 m	Competent	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	23 s
5	2	31	F	1.58 m	Competent	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	30 s
6	1	35	M	1.65 m	Expert	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	24 s
6	2	35	M	1.65 m	Expert	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	24 s
7	1	23	F	1.68 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	28 s
7	2	23	F	1.68 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	27 s
8	1	29	M	1.81 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	43 s
8	2	29	M	1.81 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	30 s
9	1	32	F	1.58 m	Expert	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	21 s
9	2	32	F	1.58 m	Expert	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	19 s
10	1	28	M	1.73 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	20 s
10	2	28	M	1.73 m	Beginner	RG	S	M	5.0 m	1.9 m	R	N	0.1 kg	0	23 s

Table C.25: RIB gate limit switch replacement test worksheet.

Node: Extraction Electrode															
Component: Electrode															
Operator	Run	Age	Sex	Op. Height	Skill Level	Assembly	Component	Task	Distance	Height	Side	Beam Crossing	Weight	Screws	Time
1	1	24	F	1.70 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	27 s
1	2	24	F	1.70 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	25 s
2	1	33	F	1.67 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	36 s
2	2	33	F	1.67 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	32 s
3	1	33	M	1.83 m	Competent	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	36 s
3	2	33	M	1.83 m	Competent	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	33 s
4	1	27	M	1.68 m	Competent	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	29 s
4	2	27	M	1.68 m	Competent	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	28 s
5	1	31	F	1.58 m	Competent	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	33 s
5	2	31	F	1.58 m	Competent	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	34 s
6	1	35	M	1.65 m	Expert	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	26 s
6	2	35	M	1.65 m	Expert	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	20 s
7	1	23	F	1.68 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	24 s
7	2	23	F	1.68 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	30 s
8	1	29	M	1.81 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	29 s
8	2	29	M	1.81 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	30 s
9	1	32	F	1.58 m	Expert	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	35 s
9	2	32	F	1.58 m	Expert	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	30 s
10	1	28	M	1.73 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	32 s
10	2	28	M	1.73 m	Beginner	EL	E	D	3.8 m	1.5 m	R	N	0.9 kg	0	30 s
1	1	24	F	1.70 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	24 s
1	2	24	F	1.70 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	22 s
2	1	33	F	1.67 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	25 s
2	2	33	F	1.67 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	23 s
3	1	33	M	1.83 m	Competent	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	25 s
3	2	33	M	1.83 m	Competent	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	22 s
4	1	27	M	1.68 m	Competent	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	21 s
4	2	27	M	1.68 m	Competent	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	19 s
5	1	31	F	1.58 m	Competent	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	29 s
5	2	31	F	1.58 m	Competent	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	24 s
6	1	35	M	1.65 m	Expert	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	14 s
6	2	35	M	1.65 m	Expert	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	15 s
7	1	23	F	1.68 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	21 s
7	2	23	F	1.68 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	22 s
8	1	29	M	1.81 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	22 s
8	2	29	M	1.81 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	26 s
9	1	32	F	1.58 m	Expert	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	22 s
9	2	32	F	1.58 m	Expert	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	20 s
10	1	28	M	1.73 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	21 s
10	2	28	M	1.73 m	Beginner	EL	E	M	3.8 m	1.5 m	R	N	0.9 kg	0	21 s

Table C.26: Extraction electrode replacement test worksheet.

BIBLIOGRAPHY

[1] A. Iborra, J. A. Pastor, B. Álvarez, C. Fernández, and J. M. Fernández Meroño. "Robots in Radioactive Environments." In: *IEEE Robotics and Automation Magazine* 10.4 (2003), pp. 12–22. ISSN: 10709932. DOI: 10.1109/MRA.2003.1256294.

[2] I. Tsitsimpelis, C. J. Taylor, B. Lennox, and M. J. Joyce. "A review of ground-based robotic systems for the characterization of nuclear environments." In: *Progress in Nuclear Energy* 111 (2019), pp. 109–124. ISSN: 0149-1970. DOI: 10.1016/J.PNUCENE.2018.10.023.

[3] A. Ono. "Fukushima Daiichi decontamination and decommissioning: current status and challenges." In: *Annals of the ICRP* 50.1 (2021), pp. 24–30. ISSN: 1872969X. DOI: 10.1177/01466453211010865.

[4] T. Yoshida, K. Nagatani, S. Tadokoro, T. Nishimura, and E. Koyanagi. "Improvements to the rescue robot quince toward future indoor surveillance missions in the Fukushima Daiichi nuclear power plant." In: *Springer Tracts in Advanced Robotics* 92 (2014), pp. 19–32. ISSN: 16107438. DOI: 10.1007/978-3-642-40686-7_2/COVER.

[5] Y. Kobayashi, S. Kanai, C. Kikumoto, and K. Sakoda. "Design and Fabricate of Reconnaissance Robots for Nuclear Power Plants that Underwent Accidents." In: *Journal of Robotics and Mechatronics* 34.3 (2022), pp. 523–526. ISSN: 18838049. DOI: 10.20965/JRM.2022.P0523.

[6] S. Suzuki, H. Toba, T. Takeda, Y. Togashi, and T. Akao. "Development of Robot Simulating Fuel Debris Retrieval." In: *Journal of Robotics and Mechatronics* 34.3 (2022), pp. 537–543. ISSN: 18838049. DOI: 10.20965/JRM.2022.P0537.

[7] W. Yim, A. Barzilov, and G. Friesmuth. "Development of autonomous robotic monitoring vehicle (ARMV) for aerial radiation monitoring." In: *2013 10th International Conference on Ubiquitous Robots and Ambient Intelligence, URAI 2013* (2013), pp. 687–688. DOI: 10.1109/URAI.2013.6677454.

[8] M. Tanigaki, Y. Inoue, S. Momota, T. Saito, T. Nemoto, T. Ono, A. Wada, M. Ohashi, K. Tsuno, M. Kano, T. Matsuura, T. Yasuoka, H. Hanai, and K. Arakawa. "Development of a robot for the measurement of radioactive contamination and fertility of the soil in Farmland." In: *Radiation Protection Dosimetry* 198.13-15 (2022), pp. 964–970. ISSN: 17423406. DOI: 10.1093/RPD/NCAC020.

[9] G. L. Kim, H. Kim, H. W. Seo, J. H. Yu, and J. W. Son. "Classification and consideration for the risk management in the planning phase of NPP decommissioning project." In: *Nuclear Engineering and Technology* 54.12 (2022), pp. 4809–4818. ISSN: 2234358X. DOI: 10.1016/J.NET.2022.07.022.

[10] K. Park, S. Son, J. Oh, and S. Kim. "Sustainable Decommissioning Strategies for Nuclear Power Plants: A Systematic Literature Review." In: *Sustainability (Switzerland)* 14.10 (2022). ISSN: 20711050. DOI: 10.3390/SU14105947.

[11] International Atomic Energy Agency. *Application of Remotely Operated Handling Equipment in the Decommissioning of Nuclear Facilities*. Vienna: IAEA Technical Report Series No. 348, IAEA, 1993.

[12] International Atomic Energy Agency. *Decommissioning by Design: How Advanced Reactors are Designed with Disposal in Mind | IAEA*. Vienna: IAEA Bulletin, IAEA, 2023.

[13] R. Borchardt, L. Denissen, P. Desbats, M. Jeanjacques, J.-G. Nokhamzon, P. Valentin, S. Slater, L. Valencia, S. Wittenauer, T. Yamauchi, and B. Burton. "Remote handling techniques in decommissioning - A report of the NEA Co-operative Programme on Decommissioning (CPD) project." In: *NEA-RWM-R–2011-2* (2011).

[14] L. Vargovčík, R. Holcer, and J. Medveď. "Mobile Robotic Systems for Fragmentation of Nuclear Equipment." In: *Applied Mechanics and Materials* 282 (2013), pp. 116–122. ISSN: 1662-7482. DOI: 10.4028/WWW.SCIENTIFIC.NET/AMM.282.116.

[15] Y. Ge, Y. Lin, H. Xie, and J. Yang. "Design and Development of Intelligent Replacement Robot for Radioactive Spent Filter Element in NPP and Its Performance Validation." In: *International Conference on Nuclear Engineering, Proceedings, ICONE* 12 (2022). DOI: 10.1115/ICONE29-93482.

[16] P. Santos, J. Recknagel, M. Knuth, K. Steinbacher, M. Ritz, B. Wassmann, and D. Fellner. "ROBBE - Robot-aided processing of assemblies during the dismantling of nuclear power plants." In: *EPJ Nuclear Sciences and Technologies* 8 (2022). ISSN: 24919292. DOI: 10.1051/EPJN/2022016.

[17] T. Otto. "Safety for Particle Accelerators." In: Particle Acceleration and Detection (2021). DOI: 10.1007/978-3-030-57031-6.

[18] K. Kershaw, B. Feral, J. L. Grenard, T. Feniet, S. De Man, C. Hazelaar-Bal, C. Bertone, and R. Ingo. "Remote Inspection, Measurement and Handling for Maintenance and Operation at CERN." English. In: *International Journal of Advanced Robotic Systems* 10 (2013). ISSN: 1729-8806. DOI: 10.5772/56849.

[19] C. P. Sesmero, L. R. Buonocore, and M. Di Castro. "Omnidirectional robotic platform for surveillance of particle accelerator environments with limited space areas." In: *Applied Sciences (Switzerland)* 11.14 (2021). ISSN: 20763417. DOI: 10.3390/APP11146631.

[20] C. Gentile, G. Lunghi, L. R. Buonocore, F. Cordella, M. Di Castro, A. Masi, and L. Zollo. "Manipulation Tasks in Hazardous Environments Using a Teleoperated Robot: A Case Study at CERN." In: *Sensors* 23.4 (2023). ISSN: 14248220. DOI: 10.3390/S23041979.

[21] L. Attard, C. J. Debono, G. Valentino, M. D. Castro, and M. Di Castro. "Vision-based change detection for inspection of tunnel liners." In: *Automation in Construction* 91 (2018), pp. 142–154. ISSN: 0926-5805. DOI: 10.1016/j.autcon.2018.03.020.

[22] L. Attard, C. J. Debono, G. Valentino, M. Di Castro, A. Masi, and L. Scibile. "Automatic crack detection using mask R-CNN." In: *International Symposium on Image and Signal Processing and Analysis, ISPA* 2019-September (2019), pp. 152–157. ISSN: 18492266. DOI: 10.1109/ISPA.2019.8868619.

[23] L. Attard, C. J. Debono, G. Valentino, and M. Di Castro. "Vision-Based Tunnel Lining Health Monitoring via Bi-Temporal Image Comparison and Decision-Level Fusion of Change Maps." In: *Sensors (Basel, Switzerland)* 21.12 (2021). ISSN: 14248220. DOI: 10.3390/S21124040.

[24] K. A. Szczurek, R. M. Prades, E. Matheson, J. Rodiguez-Nogueira, and M. Di Castro. "Mixed Reality Human-Robot Interface with Adaptive Communications Congestion Control for the Teleoperation of Mobile Redundant Manipulators in Hazardous Environments." In: *IEEE Access* (2022). ISSN: 21693536. DOI: 10.1109/ACCESS.2022.3198984.

[25] K. A. Szczurek, R. Cittadini, R. M. Prades, E. Matheson, and M. Di Castro. "Enhanced Human-Robot Interface with Operator Physiological Parameters Monitoring and 3D Mixed Reality." In: *IEEE Access* (2023). ISSN: 21693536. DOI: 10.1109/ACCESS.2023.3268986.

[26] K. A. Szczurek, R. M. Prades, E. Matheson, J. Rodriguez-Nogueira, and M. D. Castro. "Multimodal Multi-User Mixed Reality Human-Robot Interface for Remote Operations in Hazardous Environments." In: *IEEE Access* 11 (2023), pp. 17305–17333. ISSN: 21693536. DOI: 10.1109/ACCESS.2023.3245833.

[27] C. V. Almagro, M. Di Castro, G. Lunghi, R. M. Prades, P. J. S. Valero, M. F. Pérez, and A. Masi. "Monocular Robust Depth Estimation Vision System for Robotic Tasks Interventions in

Metallic Targets." In: *Sensors 2019* 19.14 (2019), p. 3220. ISSN: 1424-8220. DOI: 10.3390/S19143220.

[28] C. Veiga Almagro, R. A. Muñoz Orrego, Á. García González, E. Matheson, R. Marín Prades, M. Di Castro, and M. Ferre Pérez. "(MARGOT) Monocular Camera-Based Robot Grasping Strategy for Metallic Objects." In: *Sensors 2023, Vol. 23, Page 5344* 23.11 (2023), p. 5344. ISSN: 1424-8220. DOI: 10.3390/S23115344.

[29] L. M. Orona, H. Weick, J. Mattila, F. Amjad, E. Kozlova, C. Karagiannis, K. H. Behr, and M. Winkler. "Super-FRS target area remote handling: Scenario and development." In: *International Journal of Advanced Robotic Systems* 10 (2013). ISSN: 17298806. DOI: 10.5772/57073.

[30] F. Amjad, H. Weick, J. Mattila, L. Orona, E. Kozlova, M. Winkler, K. H. Behr, and C. Karagiannis. "Survey on remote handling logistics for super-FRS." In: *International Journal of Advanced Robotic Systems* 10 (2013). ISSN: 17298806. DOI: 10.5772/56848.

[31] T. McManamy and J. Forester. "SNS Target Systems initial operating experience." In: *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 600.1 (2009), pp. 25–27. ISSN: 0168-9002. DOI: 10.1016/J.NIMA.2008.11.015.

[32] J. R. Haines, T. J. McManamy, T. A. Gabriel, R. E. Battle, K. K. Chipley, J. A. Crabtree, L. L. Jacobs, D. C. Lousteau, M. J. Rennich, and B. W. Riemer. "Spallation neutron source target station design, development, and commissioning." In: *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 764 (2014), pp. 94–115. ISSN: 0168-9002. DOI: 10.1016/J.NIMA.2014.03.068.

[33] M. Göhran, L. Åström, P. Erterius, S. Vareskic, and E. Mukovic. "Status update on the design and construction of the Active Cells Facility and Remote Handling Systems." In: *Journal of Physics: Conference Series* 1021.1 (2018). ISSN: 17426596. DOI: 10.1088/1742-6596/1021/1/012068.

[34] R. Buckingham and A. Loving. "Remote-handling challenges in fusion research and beyond." In: *Nature Physics* 12.5 (2016), pp. 391–393. ISSN: 1745-2481. DOI: 10.1038/nphys3755.

[35] O. David, A. B. Loving, J. D. Palmer, S. Ciattaglia, and J. P. Friconneau. "Operational experience feedback in JET Remote Handling." In: *Fusion Engineering and Design* 75-79.SUPPL. (2005), pp. 519–523. ISSN: 0920-3796. DOI: 10.1016/J.FUSENGDES.2005.06.161.

[36] S. Sanders, A. Rolfe, S. F. Mills, and A. Tesini. "Application of remote handling compatibility on ITER plant." In: *Fusion Engineering and Design* 86.9-11 (2011), pp. 1989–1992. ISSN: 0920-3796. DOI: 10.1016/J.FUSENGDES.2011.03.057.

[37] International Atomic Energy Agency. *Safety Aspects of Nuclear Power Plant Automation and Robotics*. Vienna: IAEA TECDOC-672, IAEA, 1992.

[38] R. Shuff, M. Van Uffelen, C. Damiani, A. Tesini, C.-H. H. Choi, and R. Meek. "Progress in the design of the ITER Neutral Beam cell Remote Handling System." In: *Fusion Engineering and Design* 89.9-10 (2014), pp. 2378–2382. ISSN: 0920-3796. DOI: 10.1016/j.fusengdes.2014.01.043.

[39] J. P. Friconneau, V. Beaudoin, A. Dammann, C. Dremel, J. P. Martins, and C. S. Pitcher. "ITER hot Cell—Remote handling system maintenance overview." In: *Fusion Engineering and Design* 124 (2017), pp. 673–676. ISSN: 0920-3796. DOI: 10.1016/J.FUSENGDES.2017.01.005.

[40] C. H. Choi, S. Shi, T. Yokoyama, C. Hall, K. Keogh, and P. Talbot. "Concept of operation of the remote handling system for the ITER vacuum vessel pressure suppression system." In: *Fusion Engineering and Design* 173 (2021), p. 112875. ISSN: 0920-3796. DOI: 10.1016/J.FUSENGDES.2021.112875.

[41] D. M. Ronden, M. De Baar, R. Chavan, B. S. Elzendoorn, G. Grossetti, C. J. Heemskerk, J. F. Koning, J.-D. D. Landis, P. Spaeh, and D. Strauss. "The ITER EC H&CD Upper Launcher: Maintenance concepts." In: *Fusion Engineering and Design* 88.9-10 (2013), pp. 1982–1986. ISSN: 0920-3796. DOI: 10.1016/j.fusengdes.2012.12.031.

[42] P Martínez-Albertos, P Sauvan, M. J. Loughlin, Y Le Tonqueze, and &. R. Juárez. "Assessment of ITER radiation environment during the remote-handling operation of In-Vessel components with D1SUNED." In: *Scientific Reports* 13.1 (2023), p. 3544. DOI: 10.1038/s41598-023-30534-x.

[43] R. Villari, D. Nagy, L. Bertalot, A. Colangeli, D. Flammini, N. Fonnesu, G. Mariano, F. Moro, and E. Polunovskiy. "Nuclear Analyses of ITER Diagnostics Lower Ports." In: *IEEE Transactions on Plasma Science* 50.11 (2022), pp. 4533–4538. ISSN: 19399375. DOI: 10.1109/TPS.2022.3184338.

[44] O. David, G. Miccichè, A. Ibarra, J.-P. Friconneau, and G. Piazza. "Overview of the preliminary remote handling handbook for IFMIF." In: *Fusion Engineering and Design* 84 (2009), pp. 660–664. DOI: 10.1016/j.fusengdes.2009.01.089.

[45] G. Miccichè, M. Ascott, A. Bakic, D. Bernardi, J. Brenosa, S. Coloma, O. Crofts, G. Di Gironimo, M. Ferre, G. Fischer, T. Tadic, T. Matyas, A. Ibarra, A. Karap, I. G. Kiss, C. Kunert, L. Lorenzelli, G. Mitchell, M. Mittwollen, P. Pagani, S. Papa, G. Porempovics, T. Tadic, and T. Matyas. "The remote handling system of IFMIF-DONES." In: *Fusion Engineering and Design* 146 (2019), pp. 2786–2790. ISSN: 0920-3796. DOI: 10.1016/j.fusengdes.2019.01.112.

[46] F. Arranz, O. Nomen, B. Brañas, J. Castellanos, J. Molla, and D. Gutierrez. "Remote disconnection system for the beam dump of the LIPAc accelerator." In: *Fusion Engineering and Design* 125 (2017), pp. 123–126. ISSN: 0920-3796. DOI: 10.1016/j.fusengdes.2017.10.010.

[47] T. Lehmann, F. Rauscher, J. Oellerich, G. Fischer, and J. Zapata. "Modular transportation concept for application in DEMO Oriented Neutron Source (DONES)." In: *Fusion Engineering and Design* 164 (2021), p. 112199. ISSN: 0920-3796. DOI: 10.1016/j.fusengdes.2020.112199.

[48] S. Coloma, M. Ferre, F. Arranz, G. Miccichè, D. Sánchez-Herranz, O. Nomen, and J. M. J. Cogollor. "Remote handling maintenance of beam dump in IFMIF-DONES." In: *Fusion Engineering and Design* 165 (2021), p. 112216. ISSN: 0920-3796. DOI: 10.1016/j.fusengdes.2020.112216.

[49] S. Coloma, M. Ferre, J. M. J. Cogollor, and G. Miccichè. "Methodology for Remote Handling Operations in IFMIF-DONES." In: *Fusion Engineering and Design* 146 (2019), pp. 1334–1337. ISSN: 0920-3796. DOI: 10.1016/j.fusengdes.2019.02.070.

[50] International Atomic Energy Agency. *Safety Culture in the Maintenance of Nuclear Power Plants*. Vienna: IAEA Safety Reportts Series No. 42, IAEA, 2005. ISBN: 92–0–112404–X.

[51] International Atomic Energy Agency. *Radioisotope Handling Facilities and Automation of Radioisotope Production*. Viena: IAEA TECDOC-1430, IAEA, 2004. ISBN: 92-0-116104-2.

[52] International Atomic Energy Agency. *Remote Technology Related to the Handling, Storage and Disposal of Spent Fuel*. Vienna: IAEA-TECDOC-842, IAEA, 1995.

[53] Y. Yang, Y. Su, W. Li, W. Yan, L. Sheng, Y. Li, B. Yang, W. Mao, and L. Wang. "Radiation protection considerations in radioactive ion beam facilities." In: *Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms* 455 (2019), pp. 96–107. ISSN: 0168-583X. DOI: 10.1016/J.NIMB.2019.06.031.

[54] International Atomic Energy Agency. *Radiation Protection Aspects of Design for Nuclear Power Plants*. Vienna: IAEA Safety Standards Series No. NS-G-1.13, IAEA, 2005. ISBN: 92-0-107905-2.

[55] International Atomic Energy Agency. *Occupational Radiation Protection*. Vienna: IAEA Safety Standards Series No. GSG-7, IAEA, 2018. ISBN: 978-92-0-102917-1.

[56] R Catherall, W Andreazza, M Breitenfeldt, A Dorsival, G. J. Focker, T. P. Gharsa, T. J. Giles, J.-L. Grenard, F Locci, P Martins, S Marzari, J Schipper, A Shornikov, and T Stora. "The ISOLDE facility." In: *Journal of Physics G: Nuclear and Particle Physics* 44.9 (2017). DOI: 10.1088/1361-6471/aa7eba.

[57] C. Duchemin et al. "CERN-MEDICIS: A Review Since Commissioning in 2017." In: *Frontiers in Medicine* 8 (2021). ISSN: 2296-858X. DOI: 10.3389/fmed.2021.693682.

[58] G. Minor, J. Kapalka, C. Fisher, W. Paley, K. Chen, M. Kinakin, I. Earle, B. Moss, P. Bricault, and A. Gottberg. "Remote handling systems for the ISAC and ARIEL high-power fission and spallation ISOL target facilities at TRIUMF." In: *Nuclear Engineering and Technology* 53.4 (2021), pp. 1378–1389. ISSN: 2234358X. DOI: 10.1016/j.net.2020.09.024.

[59] D. Battini, G. Donzella, A. Avanzini, A. Zenoni, M. Ferrari, A. Donzella, S. Pandini, F. Bignotti, A. Andrighetto, and A. Monetti. "Experimental testing and numerical simulations for life prediction of gate valve O-rings exposed to mixed neutron and gamma fields." In: *Materials & Design* 156 (2018), pp. 514–527. ISSN: 0264-1275. DOI: 10.1016/J.MATDES.2018.07.020.

[60] V. N. Bliznyuk, J. Smith, T. Guin, C. Verst, J. Folkert, K. McDonald, G. Larsen, and T. A. DeVol. "Photoluminescence Induced in Mineral Oil by Ionizing Radiation." In: *Lubricants* 11.7 (2023), p. 287. ISSN: 20754442. DOI: 10.3390/LUBRICANTS11070287/S1.

[61] M. Ferrari, A. Zenoni, M. Hartl, Y. Lee, A. Andrighetto, A. Monetti, A. Salvini, and F. Zelaschi. "Experimental study of consistency degradation of different greases in mixed neutron and gamma radiation." In: *Heliyon* 5.9 (2019), e02489. ISSN: 2405-8440. DOI: 10.1016/J.HELIYON.2019.E02489.

[62] A. Coronetti, R. G. Alia, J. Budroweit, T. Rajkowski, I. D. Costa Lopes, K. Niskanen, D. Soderstrom, C. Cazzaniga, R. Ferraro, S. Danzeca, J. Mekki, F. Manni, D. Dangla, C. Virmontois, N. Kerboub, A. Koelpin, F. Saigne, P. Wang, V. Pouget, A. Touboul, A. Javanainen, H. Kettunen, and R. C. Germanicus. "Radiation Hardness Assurance through System-Level Testing: Risk Acceptance, Facility Requirements, Test Methodology, and Data Exploitation." In: *IEEE Transactions on Nuclear Science* 68.5

(2021), pp. 958–969. ISSN: 15581578. DOI: 10.1109/TNS.2021.3061197.

[63] L. Weninger, R. Clerc, M. Ferrari, A. Morana, T. Allanche, R. Pecorella, A. Boukenter, Y. Ouerdane, E. Marin, O. Duhamel, M. Gaillardin, P. Paillet, and S. Girard. “Gamma Ray Effects on Multi-Colored Commercial Light-Emitting Diodes at MGy Level.” In: *Electronics* 12.1 (2022), p. 81. ISSN: 2079-9292. DOI: 10.3390/ELECTRONICS12010081.

[64] E. S. Lee, G. Loianno, D. Thakur, and V. Kumar. “Experimental evaluation and characterization of radioactive source effects on robot visual localization and mapping.” In: *IEEE Robotics and Automation Letters* 5.2 (2020), pp. 3259–3266. ISSN: 23773766. DOI: 10.1109/LRA.2020.2975723.

[65] M. Ferrari, D. Senajova, O. Aberle, Y. Q. Aguiar, D. Baillard, M. Barbagallo, A. P. Bernardes, L. Buonocore, M. Cecchetto, V. Clerc, M. Di Castro, R. Garcia Alia, S. Girod, J. L. Grenard, K. Kershaw, G. Lerner, M. M. Maeder, A. Makovec, A. Mengoni, M. Perez Ornedo, F. Pozzi, C. V. Almagro, and M. Calviani. “Design development and implementation of an irradiation station at the neutron time-of-flight facility at CERN.” In: *Physical Review Accelerators and Beams* 25.10 (2022). ISSN: 24699888. DOI: 10.1103/PHYSREVACCELBEAMS.25.103001.

[66] A. Tesini and A. C. Rolfe. “The ITER Remote Maintenance Management System.” In: *Fusion Engineering and Design* 84 (2009), pp. 236–241. DOI: 10.1016/j.fusengdes.2008.11.029.

[67] International Atomic Energy Agency. *Safety Assessment for Facilities and Activities*. Vienna: IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, 2016. ISBN: 978-92-0-109115-4.

[68] International Atomic Energy Agency. *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*. Vienna: IAEA Safety Standards Series No. SSG-3, IAEA, 2010. ISBN: 978-92-0-114509-3.

[69] International Atomic Energy Agency. *Procedures for Conducting Probabilistic Safety Assessment for Non-Reactor Nuclear Facilities*. Vienna: IAEA TECDOC-1267, IAEA, 2002.

[70] International Atomic Energy Agency. *Industrial Safety Guidelines for Nuclear Facilities*. Vienna: IAEA Nuclear Energy Series No NP-T-3.3, IAEA, 2018. ISBN: 978-92-0-101617-1.

[71] *Machinery Directive (MD) 2006/42/EC*. 2006.

[72] *EN ISO 1200:2010. Safety of machinery - General principles for design - Risk assessment and risk reduction*. 2010.

[73] P. Anger, V. Cingal, J.-C. Pacary, S. Perret-Gatel, and A. Savalle. "Safety System for the Respect of Nuclear Requirements of SPIRAL2 Facility." In: *JACoW* IPAC2020 (2020), pp. 57–60. DOI: 10.18429/JACOW-IPAC2020-WEVIR11.

[74] G. F. Steyn et al. "Development of new target stations for the south african isotope facility." In: *Instruments* 2.4 (2018). ISSN: 2410390X. DOI: 10.3390/INSTRUMENTS2040029.

[75] J. Lee, H. J. Yim, T. Hashimoto, Y. H. Park, W. Hwang, S. J. Park, J. W. Jeong, S. Heo, K. H. Yoo, Y. H. Yeon, D. J. Park, J. Kim, B. H. Kang, J. Y. Moon, and T. Shin. "Recent progress of ISOL facility at RAON." In: *Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms* 542 (2023), pp. 17–21. ISSN: 0168-583X. DOI: 10.1016/J.NIMB.2023.05.045.

[76] S. Hurier, K. Rijpstra, P. Creemers, J. P. Ramos, L. Popescu, and T. E. Cocolios. "Design and thermal simulations towards a high intensity radioactive ion source for ISOL@MYRRHA." In: *Journal of Physics: Conference Series* 2244.1 (2022). ISSN: 17426596. DOI: 10.1088/1742-6596/2244/1/012065.

[77] E. Kozlova, A. Sokolov, T. Radon, R. Lang, I. Conrad, G. Fehrenbacher, H. Weick, M. Winkler, E. Kozlova, A. Sokolov, T. Radon, R. Lang, I. Conrad, G. Fehrenbacher, H. Weick, and M. Winkler. "Radiation protection design for the Super-FRS and SIS100 at the international FAIR facility." In: *EPJWC* 153 (2017), p. 03003. ISSN: 2100014X. DOI: 10.1051/EPJCONF/201715303003.

[78] L. P. Duisings, S. Van Til, A. J. Magielsen, D. M. Ronden, B. S. Elzendoorn, and C. J. Heemskerk. "Applying HAZOP analysis in assessing remote handling compatibility of ITER port plugs." In: *Fusion Engineering and Design* 88.9-10 (2013), pp. 2688–2693. ISSN: 0920-3796. DOI: 10.1016/J.FUSENGDES.2012.12.002.

[79] *IEC 61499. Function blocks-Part 1: architecture, Second Edition*. 2012.

[80] *Decreto Legislativo 9 aprile 2008, n.81, Testo unico sulla salute e sicurezza sul lavoro*. 2008.

[81] *Decreto Legislativo 27 gennaio 2010, n.17, Attuazione della direttiva 2006/42/CE, relativa alle macchine e che modifica la direttiva 95/16/CE relativa agli ascensori.* 2010.

[82] *Electromagnetic Compatibility (EMC) Directive 2014/30/EU*. 2014.

[83] *Low-Voltage Directive (LVD) 2014/35/EU*. 2014.

[84] *EN IEC 62061:2021. Safety of machinery - Functional safety of safety-related control systems*. 2021.

[85] *EN IEC 60204-1:2018. Safety of machinery - Electrical equipment of machines - Part 1: General requirements*. 2018.

[86] *EN ISO 13849-1:2015. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design*. 2015.

[87] *EN ISO 13849-2:2012. Safety of machinery - Safety- related parts of control systems - Part 2: Validation*. 2012.

[88] *EN ISO 13850:2015. Safety of machinery - Emergency stop function - Principles for design*. 2015.

[89] *EN ISO 14119:2013. Safety of machinery - Interlocking devices associated with guards - Principles for design and selection*. 2013.

[90] *EN ISO 23125:2015. Machine tools - Safety - Turning machines*. 2015.

[91] *Machinery Regulation (EU) 2023/1230*. 2023.

[92] *ISO/TR 14121-2:2012. Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods*. 2012.

[93] *Decreto Legislativo 31 luglio 2020, n.101, Attuazione della direttiva 2013/59/Euratom, che stabilisce norme fondamentali di sicurezza relative alla protezione contro i pericoli derivanti dall'esposizione alle radiazioni ionizzanti*. 2020.

[94] International Commission on Radiological Protection. *1990 Recommendations of the International Commission on Radiological Protection*. ICRP Publi. Oxford: Pergamon, 1991.

[95] D. F. Wirth, S. Roesler, M. Silari, M. Streit-Bianchi, C. Theis, H. H. Vincke, and H. H. Vincke. "Radiation protection at CERN." In: *CERN Accelerator School: High Power Hadron Machines, CAS 2011 - Proceedings* (2013), pp. 415–436. DOI: 10.5170/CERN-2013-001.415.

[96] International Atomic Energy Agency. *Frequently Asked Questions on ALARA: optimization of doses for occupational exposure*. Vienna: IAEA consultancy meeting, IAEA, 2010.

[97] D. Dinis, A. P. Teixeira, and C. Guedes Soares. "Probabilistic approach for characterising the static risk of ships using Bayesian networks." In: *Reliability Engineering and System Safety* 203 (2020), p. 107073. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2020.107073.

[98] H. Li, X. Ren, and Z. Yang. "Data-driven Bayesian network for risk analysis of global maritime accidents." In: *Reliability Engineering and System Safety* 230 (2023), p. 108938. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2022.108938.

[99] X. Huang, Y. Wen, F. Zhang, H. Han, Y. Huang, and Z. Sui. "A review on risk assessment methods for maritime transport." In: *Ocean Engineering* 279 (2023), p. 114577. DOI: 10.1016/j.oceaneng.2023.114577.

[100] A. Misuri, G. Landucci, and V. Cozzani. “Assessment of risk modification due to safety barrier performance degradation in Natech events.” In: *Reliability Engineering and System Safety* 212 (2021), p. 107634. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2021.107634.

[101] V. Caratozzolo, A. Misuri, and V. Cozzani. “A generalized equipment vulnerability model for the quantitative risk assessment of horizontal vessels involved in Natech scenarios triggered by floods.” In: *Reliability Engineering and System Safety* 223 (2022), p. 108504. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2022.108504.

[102] A. Misuri, F. Ricci, R. Sorichetti, and V. Cozzani. “The Effect of Safety Barrier Degradation on the Severity of Primary Natech Scenarios.” In: *Reliability Engineering and System Safety* 235 (2023), p. 109272. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2023.109272.

[103] X. Wu, H. Huang, J. Xie, M. Lu, S. Wang, W. Li, Y. Huang, W. Yu, and X. Sun. “A novel dynamic risk assessment method for the petrochemical industry using bow-tie analysis and Bayesian network analysis method based on the methodological framework of ARAMIS project.” In: *Reliability Engineering and System Safety* 237 (2023), p. 109397. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2023.109397.

[104] M. Iaiani, A. Tugnoli, P. Macini, and V. Cozzani. “Outage and asset damage triggered by malicious manipulation of the control system in process plants.” In: *Reliability Engineering and System Safety* 213 (2021), p. 107685. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2021.107685.

[105] R. G. Maidana, T. Parhizkar, A. Gomola, I. B. Utne, and A. Mosleh. “Supervised dynamic probabilistic risk assessment: Review and comparison of methods.” In: *Reliability Engineering and System Safety* 230 (2023), p. 108889. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2022.108889.

[106] V. Casson Moreno, G. Marroni, and G. Landucci. “Probabilistic assessment aimed at the evaluation of escalating scenarios in process facilities combining safety and security barriers.” In: *Reliability Engineering and System Safety* 228 (2022), p. 108762. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2022.108762.

[107] R. He, J. Zhu, G. Chen, and Z. Tian. “A real-time probabilistic risk assessment method for the petrochemical industry based on data monitoring.” In: *Reliability Engineering and System Safety* 226 (2022), p. 108700. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2022.108700.

[108] H.-J. Liaw. "Improved management practice and process hazard analysis techniques for minimizing likelihood of process safety incidents in Taiwan." In: *Journal of Loss Prevention in the Process Industries* 81 (2023), p. 104966. DOI: 10.1016/j.jlp.2022.104966.

[109] W. Pu, A. Aziz, A. Raman, M. D. Hamid, X. Gao, and A. Buthiyappan. "Inherent safety concept based proactive risk reduction strategies: A review." In: *Journal of Loss Prevention in the Process Industries* 84.2 (2023), pp. 950–4230. DOI: 10.1016/j.jlp.2023.105133.

[110] P. Mocellin and L. Pilenghi. "Semi-quantitative approach to prioritize risk in industrial chemical plants aggregating safety, economics and ageing: A case study." In: *Reliability Engineering and System Safety* 237 (2023), p. 109355. DOI: 10.1016/j.ress.2023.109355.

[111] T. Zhou, M. Modarres, and E. L. Droguett. "Multi-unit nuclear power plant probabilistic risk assessment: A comprehensive survey." In: *Reliability Engineering and System Safety* 213 (2021). ISSN: 09518320. DOI: 10.1016/J.RESS.2021.107782.

[112] J. DeJesus Segarra, M. Bensi, and M. Modarres. "Multi-unit seismic probabilistic risk assessment: A Bayesian network perspective." In: *Reliability Engineering and System Safety* 234 (2023). ISSN: 09518320. DOI: 10.1016/J.RESS.2023.109169.

[113] F. Antonello, J. Buongiorno, and E. Zio. "A methodology to perform dynamic risk assessment using system theory and modeling and simulation: Application to nuclear batteries." In: *Reliability Engineering and System Safety* 228 (2022), p. 108769. DOI: 10.1016/j.ress.2022.108769.

[114] L. Tao, L. Chen, D. Ge, Y. Yao, F. Ruan, J. Wu, and J. Yu. "An integrated probabilistic risk assessment methodology for maritime transportation of spent nuclear fuel based on event tree and hydrodynamic model." In: *Reliability Engineering and System Safety* 227 (2022). ISSN: 09518320. DOI: 10.1016/J.RESS.2022.108726.

[115] C. A. Johnson, R. Flage, and S. D. Guikema. "Feasibility study of PRA for critical infrastructure risk analysis." In: *Reliability Engineering and System Safety* 212 (2021), p. 107643. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2021.107643.

[116] A. Kumar, A. Saxena, and M. Ram. "Multi-State Reliability Measures Analysis of Nuclear Power Plant (NPP) System." In: *International Journal of Reliability, Quality and Safety Engineering* 27.2 (2020). ISSN: 02185393. DOI: 10.1142/S0218539320400070.

[117] T. Parhizkar, J. E. Vinnem, I. B. Utne, and A. Mosleh. "Supervised Dynamic Probabilistic Risk Assessment of Complex Systems, Part 1: General Overview." In: *Reliability Engineering and System Safety* 208 (2021). ISSN: 09518320. DOI: 10.1016/J.RESS.2020.107406.

[118] C. Jiang, Z. He, F. Li, F. Xie, L. Zheng, J. Yang, and M. Yang. "A hybrid computing framework for risk-oriented reliability analysis in dynamic PSA context: A case study." In: *Quality and Reliability Engineering International* (2022). ISSN: 10991638. DOI: 10.1002/QRE.3196.

[119] X. Zheng, H. Tamaki, T. Sugiyama, and Y. Maruyama. "Dynamic probabilistic risk assessment of nuclear power plants using multi-fidelity simulations." In: *Reliability Engineering and System Safety* 223 (2022), p. 108503. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2022.108503.

[120] R. Yan, S. Tolo, S. Dunnett, J. Andrews, and E. Patelli. "Resilience in the context of nuclear safety engineering." In: *Proceedings - Annual Reliability and Maintainability Symposium* 2020-Janua (2020). ISSN: 0149144X. DOI: 10.1109/RAMS48030.2020.9153717.

[121] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez. "A review of definitions and measures of system resilience." In: *Reliability Engineering and System Safety* 145 (2016), pp. 47–61. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2015.08.006.

[122] D. Imran Khan, S. Virtanen, P. Bonnal, and A. K. Verma. "Functional failure modes cause-consequence logic suited for mobile robots used at scientific facilities." In: *Reliability Engineering and System Safety* 129 (2014), pp. 10–18. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2014.03.012.

[123] P. Kumar, L. K. Singh, and C. Kumar. "An optimized technique for reliability analysis of safety-critical systems: A case study of nuclear power plant." In: *Quality and Reliability Engineering International* 35.1 (2019), pp. 461–469. ISSN: 10991638. DOI: 10.1002/QRE.2340.

[124] P. Kumar, L. K. Singh, and C. Kumar. "Software reliability analysis for safety-critical and control systems." In: *Quality and Reliability Engineering International* 36.1 (2020), pp. 340–353. ISSN: 10991638. DOI: 10.1002/QRE.2577.

[125] C. Bensaci, Y. Zennir, D. Pomorski, F. Innal, and M. A. Lundteigen. "Collision hazard modeling and analysis in a multi-mobile robots system transportation task with STPA and SPN." In: *Reliability Engineering and System Safety* 234 (2023). ISSN: 09518320. DOI: 10.1016/J.RESS.2023.109138.

[126] I. S. Kim, Y. Choi, and K. M. Jeong. "A new approach to quantify safety benefits of disaster robots." In: *Nuclear Engineering and Technology* 49.7 (2017), pp. 1414–1422. ISSN: 2234358X. DOI: 10.1016/J.NET.2017.06.008.

[127] International Atomic Energy Agency. *Guidance for optimizing nuclear power plant maintenance programmes*. Vienna: IAEA-TECDOC-1383, IAEA, 2003.

[128] International Atomic Energy Agency. *Maintenance, Testing, Surveillance and Inspection in Nuclear Power Plants*. Vienna: IAEA Safety Standards Series No. SSG-74, IAEA, 2022.

[129] M. Du, S. Zhang, and Y. F. Li. "Integrated Scheduling of Maintenance Workers and Activities for Nuclear Power Plant Subsystem." In: *Proceedings - 12th International Conference on Reliability, Maintainability, and Safety, ICRMS 2018* (2018), pp. 442–447. DOI: 10.1109/ICRMS.2018.00088.

[130] E. Bismut, M. D. Pandey, and D. Straub. "Reliability-based inspection and maintenance planning of a nuclear feeder piping system." In: *Reliability Engineering and System Safety* 224 (2022), p. 108521. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2022.108521.

[131] F. Zhang, H. Liao, J. Shen, and Y. Ma. "Optimal Maintenance of a System With Multiple Deteriorating Components Served by Dedicated Teams." In: *IEEE Transactions on Reliability* (2022). ISSN: 15581721. DOI: 10.1109/TR.2022.3190274.

[132] I. Wayan Ngarayana, T. M. D. Do, K. Murakami, and M. Suzuki. "Nuclear Power Plant Maintenance Optimisation: Models, Methods & Strategies." In: *Journal of Physics: Conference Series* 1198.2 (2019), p. 022005. ISSN: 1742-6596. DOI: 10.1088/1742-6596/1198/2/022005.

[133] S. Perez-Canto and J. C. Rubio-Romero. "A model for the preventive maintenance scheduling of power plants including wind farms." In: *Reliability Engineering and System Safety* 119 (2013), pp. 67–75. ISSN: 09518320. DOI: 10.1016/J.RESS.2013.04.005.

[134] International Atomic Energy Agency. *Maintenance Optimization Programme for Nuclear Power Plants*. Vienna: IAEA Nuclear Energy Series No. NP-T-3.8, IAEA, 2018.

[135] S. Martorell, A. Sánchez, S. Carlos, and V. Serradell. "Comparing effectiveness and efficiency in technical specifications and maintenance optimization." In: *Reliability Engineering and System Safety* 77.3 (2002), pp. 281–289. ISSN: 09518320. DOI: 10.1016/S0951-8320(02)00061-3.

[136] H. P. Jagtap, A. K. Bewoor, R. Kumar, M. H. Ahmadi, M. El Haj Assad, and M. Sharifpur. "RAM analysis and availability optimization of thermal power plant water circulation system using PSO." In: *Energy Reports* 7 (2021), pp. 1133–1153. ISSN: 23524847. DOI: 10.1016/J.EGYR.2020.12.025.

[137] J. Alanen, J. Linnosmaa, T. Malm, N. Papakonstantinou, T. Ahonen, E. Heikkilä, and R. Tiusanen. "Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems." In: *Reliability Engineering and System Safety* 220 (2022). ISSN: 09518320. DOI: 10.1016/J.RESS.2021.108270.

[138] P. Contri, I. Kuzmina, and B. Elsing. "Maintenance optimization and nuclear power plant life management - A proposal for an integrated set of maintenance effectiveness indicators." In: *Journal of Pressure Vessel Technology, Transactions of the ASME* 134.3 (2012). ISSN: 00949930. DOI: 10.1115/1.4005809.

[139] S. Gazzotti, F. Ferlay, L. Meunier, P. Viudes, K. Huc, A. Derkazarian, J. P. Friconneau, B. Peluso, and J. P. Martins. "Virtual and Augmented Reality Use Cases for Fusion Design Engineering." In: *Fusion Engineering and Design* 172 (2021). ISSN: 09203796. DOI: 10.1016/J.FUSENGDES.2021.112780.

[140] J. Kim, D. Lee, J. Yang, and S. Lee. "Conceptual design of autonomous emergency operation system for nuclear power plants and its prototype." In: *Nuclear Engineering and Technology* 52.2 (2020), pp. 308–322. ISSN: 1738-5733. DOI: 10.1016/J.NET.2019.09.016.

[141] C. Lu, J. Lyu, L. Zhang, A. Gong, Y. Fan, J. Yan, and X. Li. "Nuclear power plants with artificial intelligence in industry 4.0 era: Top-level design and current applications—a systemic review." In: *IEEE Access* 8 (2020), pp. 194315–194332. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3032529.

[142] T. Zhang, T. Wan, W. Pan, and S. Liu. "Prospects of Nuclear Power Plant Operation and Maintenance Technology in the Era of Artificial Intelligence." In: *ACM International Conference Proceeding Series* (2022), pp. 34–42. DOI: 10.1145/3529763.3529769.

[143] D. L. Van Bossuyt, N. Papakonstantinou, B. Hale, J. Salonen, and B. O'Halloran. "Model Based Resilience Engineering for Design and Assessment of Mission Critical Systems Containing Artificial Intelligence Components." In: *Artificial Intelligence and Cybersecurity: Theory and Applications* (2022), pp. 47–66. DOI: 10.1007/978-3-031-15030-2_3/COVER.

[144] E. P. Jharko. “Safety functions in the software quality assurance of NPP safety important systems.” In: *2019 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2019* (2019). DOI: 10.1109/ICIEAM.2019.8742945.

[145] E. Jharko. “Digital Twin of Npps: Simulation Systems and Verification.” In: *Proceedings - 2021 International Russian Automation Conference, RusAutoCon 2021* (2021), pp. 852–857. DOI: 10.1109/RUSAUTOCON52004.2021.9537546.

[146] V. Kemkin, B. Doroshenko, K. Sakharov, I. Salov, J. Salova, and A. Chernyaev. “Application of a systematic approach to the analysis of requirements and testing of NPP automated process control systems in the field of information security using specialized software.” In: *Proceedings - ICOECS 2021: 2021 International Conference on Electrotechnical Complexes and Systems* (2021), pp. 580–583. DOI: 10.1109/ICOECS52783.2021.9657321.

[147] E. Jharko and K. Chernyshov. “Diagnostic Tasks in Human-Machine Control Systems of Nuclear Power Plants.” In: *Proceedings - 2022 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2022* (2022), pp. 563–571. DOI: 10.1109/ICIEAM54945.2022.9787283.

[148] E. Jharko. “Systems Important for NPP Safety: Software Verification and Cybersecurity.” In: *Lecture Notes in Electrical Engineering* 729 LNEE (2021), pp. 90–98. ISSN: 18761119. DOI: 10.1007/978-3-030-71119-1_10.

[149] O. Lobanok, V. Promyslov, and K. Semenkov. “Safety-Driven Approach for Security Audit of I&C Systems of Nuclear Power Plants.” In: *Proceedings - 2022 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2022* (2022), pp. 545–550. DOI: 10.1109/ICIEAM54945.2022.9787237.

[150] D. Tripathi, L. K. Singh, A. K. Tripathi, and A. Chaturvedi. “Model based security verification of Cyber-Physical System based on Petrinet: A case study of Nuclear power plant.” In: *Annals of Nuclear Energy* 159 (2021). ISSN: 18732100. DOI: 10.1016/J.ANUCENE.2021.108306.

[151] International Atomic Energy Agency. *Defence in Depth in Nuclear Safety*. Vienna: IAEA INSAG-10, IAEA, 1996. ISBN: 92-0-102596-3.

[152] International Atomic Energy Agency. *Computer Security for Nuclear Security*. Vienna: IAEA Nuclear Security Series No. 42-G, IAEA, 2021. ISBN: 978-92-0-121120-0.

[153] D. Drozdov, V. Dubinin, S. Patil, and V. Vyatkin. “A formal model of IEC 61499-based industrial automation architecture supporting time-aware computations.” In: *IEEE Open Journal*

of the Industrial Electronics Society 2 (2021), pp. 169–183. ISSN: 26441284. DOI: 10.1109/OJIES.2021.3056400.

[154] E. A. Lee and S. A. Seshia. *Introduction to Embedded Systems - A Cyber-Physical Systems Approach*. MIT Press, 2017, pp. 1–519. ISBN: 978-0-262-53381-2.

[155] M. Bonfè, C. Fantuzzi, and C. Secchi. "Design patterns for model-based automation software design and implementation." In: *Control Engineering Practice* 21.11 (2013), pp. 1608–1619. ISSN: 0967-0661. DOI: 10.1016/J.CONENGPRAC.2012.03.017.

[156] L. Sonnleithner, B. Wiesmayr, V. Ashiwal, and A. Zoitl. "IEC 61499 Distributed Design Patterns." In: *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA* (2021). ISSN: 19460759. DOI: 10.1109/ETFA45728.2021.9613569.

[157] G. Čengić, O. Ljungkrantz, and K. Åkesson. "A framework for component based distributed control software development using IEC 61499." In: *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA* (2006), pp. 782–789. DOI: 10.1109/ETFA.2006.355186.

[158] V. Vyatkin, S. Karras, and T. Pfeiffer. "Architecture for automation system development based on IEC61499 standard." In: *2005 3rd IEEE International Conference on Industrial Informatics, INDIN* 2005 (2005), pp. 13–18. DOI: 10.1109/INDIN.2005.1560345.

[159] R. Hametner, A. Zoitl, and M. Semo. "Automation component architecture for the efficient development of industrial automation systems." In: *2010 IEEE International Conference on Automation Science and Engineering, CASE 2010* (2010), pp. 156–161. DOI: 10.1109/COASE.2010.5584013.

[160] V. Vyatkin and H. M. Hanisch. "A modeling approach for verification of IEC1499 function blocks using net condition/event systems." In: *IEEE Symposium on Emerging Technologies and Factory Automation, ETFA* 1 (1999), pp. 261–270. DOI: 10.1109/ETFA.1999.815365.

[161] H. M. Hanisch, M. Hirsch, D. Missal, S. Preuße, and C. Gerber. "One Decade of IEC 61499 Modeling and Verification - Results and Open Issues." In: *IFAC Proceedings Volumes* 42.4 (2009), pp. 211–216. ISSN: 1474-6670. DOI: 10.3182/20090603-3-RU-2001.0306.

[162] V. Vyatkin, H. M. Hanisch, C. Pang, and C. H. Yang. "Closed-loop modeling in future automation system engineering and validation." In: *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews* 39.1 (2009), pp. 17–28. ISSN: 10946977. DOI: 10.1109/TSMCC.2008.2005785.

[163] M. Xavier, S. Patil, V. Dubinin, and V. Vyatkin. "Formal Modelling, Analysis, and Synthesis of Modular Industrial Systems Inspired by Net Condition/Event Systems." In: *International Conference on Applications and Theory of Petri Nets and Concurrency*. Springer, Cham, 2023, pp. 16–33. DOI: 10.1007/978-3-031-33620-1_2.

[164] R. Sinha, S. Patil, L. Gomes, and V. Vyatkin. "A Survey of Static Formal Methods for Building Dependable Industrial Automation Systems." In: *IEEE Transactions on Industrial Informatics* 15.7 (2019), pp. 3772–3783. ISSN: 19410050. DOI: 10.1109/TII.2019.2908665.

[165] E. M. Clarke, O. Grumberg, D. Kroening, D. Peled, and H. Veith. *Model Checking*. MIT Press, 1999. ISBN: 9780262038836.

[166] K. Schneider. *Verification of Reactive Systems, Formal Methods and Algorithms*. Springer Berlin, Heidelberg, 2004, p. 602. ISBN: 978-3-642-05555-3. DOI: 10.1007/978-3-662-10778-2.

[167] C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008. ISBN: 978-0-262-02649-9.

[168] G. E. Gelman, K. M. Feigh, and J. Rushby. "Example of a complementary use of model checking and agent-based simulation." In: *2013 IEEE International Conference on Systems, Man, and Cybernetics* (2013). DOI: 10.1109/SMC.2013.158.

[169] H. Wang, D. Zhong, and T. Zhao. "Avionics system failure analysis and verification based on model checking." In: *Engineering Failure Analysis* 105 (2019), pp. 373–385. ISSN: 13506307. DOI: 10.1016/J.ENGFAILANAL.2019.06.020.

[170] V. Todorov, F. Boulanger, and S. Taha. "Formal verification of automotive embedded software." In: *6th International FME Workshop on Formal Methods in Software Engineering (FormaliSE)* (2018). DOI: 10.1145/3193992.3194003.

[171] J. H. Kim, K. G. Larsen, B. Nielsen, M. Mikučionis, and P. Olsen. "Formal analysis and testing of real-time automotive systems using UPPAAL tools." In: *Lecture Notes in Computer Science* 9128 (2015), pp. 47–61. ISSN: 16113349. DOI: 10.1007/978-3-319-19458-5_4/COVER.

[172] P. Filipovikj, N. Mahmud, R. Marinescu, C. Seceleanu, O. Ljungkrantz, and H. Lönn. "Simulink to UPPAAL statistical model checker: analyzing automotive industrial systems." In: *Lecture Notes in Computer Science* 9995 LNCS (2016), pp. 748–756. ISSN: 16113349. DOI: 10.1007/978-3-319-48989-6_46.

[173] A. Pakonen, I. Buzhinsky, and K. Björkman. "Model checking reveals design issues leading to spurious actuation of nuclear instrumentation and control systems." In: *Reliability Engineering and System Safety* 205 (2021), p. 107237. ISSN: 0951-8320. DOI: 10.1016/J.RESS.2020.107237.

[174] E. Jee, S. Jeon, S. Cha, K. Koh, J. Yoo, G. Park, and P. Seong. "FBDverifier: interactive and visual analysis of counterexample in formal verification of function block diagram." In: *Journal of Research and Practice in Information Technology* 42.3 (2010), pp. 171–188. ISSN: 1443-458X.

[175] E. Németh and T. Bartha. "Formal verification of safety functions by reinterpretation of functional block based specifications." In: *Lecture Notes in Computer Science* 5596 LNCS (2009), pp. 199–214. ISSN: 03029743. DOI: 10.1007/978-3-642-03240-0_17/COVER.

[176] B. F. Adiego, D. Darvas, E. B. Viñuela, J. C. Tournier, S. Bliudze, J. O. Blech, and V. M. G. Suárez. "Applying model checking to industrial-sized PLC programs." In: *IEEE Transactions on Industrial Informatics* 11.6 (2015), pp. 1400–1410. ISSN: 15513203. DOI: 10.1109/TII.2015.2489184.

[177] I. Buzhinsky and A. Pakonen. "Symmetry breaking in model checking of fault-tolerant nuclear instrumentation and control systems." In: *IEEE Access* 8 (2020), pp. 197684–197694. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.3034799.

[178] A. Cimatti and A. Griggio. "Software model checking via IC3." In: *Lecture Notes in Computer Science* 7358 LNCS (2012), pp. 277–293. ISSN: 03029743. DOI: 10.1007/978-3-642-31424-7_23.

[179] A. Biere, A. Cimatti, E. M. Clarke, O. Strichman, and Y. Zhu. "Bounded Model Checking." In: *Advances in Computers* 58 (2003). DOI: 10.1016/S0065-2458(03)58003-2.

[180] J. R. Burch, E. M. Clarke, K. L. McMillan, D. L. Dill, and L. J. Hwang. "Symbolic model checking: 1020 states and beyond." In: *Information and Computation* 98.2 (1992), pp. 142–170. ISSN: 0890-5401. DOI: 10.1016/0890-5401(92)90017-A.

[181] D. Drozdov. "fb2smv: IEC 61499 function blocks XML code to SMV converter." In: *https://github.com/dmitrydrozdov/fb2smv* (2014).

[182] Y. Gurevich. "Evolving Algebras 1993: Lipari Guide." In: *Specification and Validation Methods* 40 (1995), pp. 231–243. DOI: 10.48550/arxiv.1808.06255.

[183] A. Cimatti, E. Clarke, E. Giunchiglia, F. Giunchiglia, M. Pistore, M. Roveri, R. Sebastiani, and A. Tacchella. "NuSMV 2: An opensource tool for symbolic model checking." In: *Lecture Notes in Computer Science* 2404 (2002), pp. 359–364. ISSN: 16113349. DOI: 10.1007/3-540-45657-0_29/COVER.

[184] M. Xavier, S. Patil, and V. Vyatkin. *Cyber-physical automation systems modelling with IEC 61499 for their formal verification*. 2021. DOI: 10.1109/INDIN45523.2021.9557416.

[185] A. Andrighetto, M. Manzolaro, S. Corradetti, D. Scarpa, A. Monetti, M. Rossignoli, M. Ballan, F. Borgna, F. D'Agostini, F. Gramegna, G. Prete, G. Meneghetti, M. Ferrari, and A. Zenoni. "Spes: an intense source of neutron-rich radioactive beams at Legnaro." In: *Journal of Physics: Conference Series* 966.1 (2018). DOI: 10.1088/1742-6596/966/1/012028.

[186] F. Gramegna. "SPES, the LNL exotic beam ISOL facility." In: *Nuovo Cimento della Societa Italiana di Fisica C* 42.2-3 (2019). DOI: 10.1393/NCC/I2019-19061-6.

[187] A. Andrighetto, L. Biasetto, M. Manzolaro, M. Barbui, G. Bisoffi, S. Carturan, M. Cinausero, F. Gramegna, G. Prete, V. Rizzi, C. Antonucci, S. Cevolani, C. Petrovich, P. Colombo, G. Meneghetti, P. Di Bernardo, P. Zanonato, I. Cristofolini, V. Fontanari, B. Monelli, and R. Oboe. "The SPES multi-foil direct target." In: *Nuclear Instruments and Methods in Physics Research, Section B: Beam Interactions with Materials and Atoms* 266.19-20 (2008), pp. 4257–4260. DOI: 10.1016/J.NIMB.2008.05.134.

[188] A. Andrighetto, S. Corradetti, M. Ballan, F. Borgna, M. Manzolaro, D. Scarpa, A. Monetti, M. Rossignoli, R. Silingardi, A. Mozzi, A. Zenoni, and G. Prete. "The SPES High Power ISOL production target." In: *Nuovo Cimento della Societa Italiana di Fisica C* 38.6 (2015). DOI: 10.1393/ncc/i2015-15194-x.

[189] M. Manzolaro, G. Meneghetti, A. Andrighetto, G. Vivian, and F. D'Agostini. "Thermal-electric coupled-field finite element modeling and experimental testing of high-temperature ion sources for the production of radioactive ion beams." In: *Review of Scientific Instruments* 87.2 (2016). ISSN: 10897623. DOI: 10.1063/1.4933081.

[190] T Marchi et al. "The SPES facility at Legnaro National Laboratories." In: *Journal of Physics: Conference Series* 1643.1 (2020), p. 12036. ISSN: 17426596. DOI: 10.1088/1742-6596/1643/1/012036.

[191] G. Bisoffi, G. Bassato, A. Battistella, J. Bermudez, D. Bortolato, S. Canella, B. Chalykh, M. Comunian, A. Facco, E. Fagotti, A. Galatà, M. Giacchini, F. Gramegna, T. Lamy, P. Modanese, A. Palmieri, R. Pengo, A. Pisent, M. Poggi, A. Porcellato, C.

Roncolato, and D. Scarpa. "ALPI setup as the SPES accelerator of exotic beams." In: *EPJ Web of Conferences* 66 (2014). ISSN: 21016275. DOI: 10.1051/EPJCONF/20146611003.

[192] J Bagger, R Laxdal, Y Bylinski, O Kester, A Gottberg, P Schaffer, K Hayashi, S Koscielniak, M Marchetto, and F Ames. "TRIUMF in the ARIEL era." In: *IPAC2018 Proc* (2018). DOI: doi:10.18429/JACoW-IPAC2018-MOXGB2.

[193] D. Stracener, J. Beene, D. Dowling, R. Juras, Y. Liu, M. Meigs, A. Mendez, P. Mueller, J. Sinclair, and B. Tatum. "Holifield Radioactive Ion Beam Facility Status." In: *Particle Accelerator Conference (PAC 09)*. 2010, FR5REP122.

[194] T. Nilsson. "European RIB facilities - Status and future." In: *Nuclear Instruments and Methods in Physics Research, Section B: Beam Interactions with Materials and Atoms* 317.PART B (2013), pp. 194–200. DOI: 10.1016/J.NIMB.2013.06.037.

[195] A. Andrighetto, M. Tosato, M. Ballan, S. Corradetti, F. Borgna, V. Di Marco, G. Marzaro, and N. Realdon. "The ISOLPHARM project: ISOL-based production of radionuclides for medical applications." In: *Journal of Radioanalytical and Nuclear Chemistry* 322.1 (2019), pp. 73–77. ISSN: 15882780. DOI: 10.1007/S10967-019-06698-0.

[196] A. Monetti, A. Andrighetto, C. Petrovich, M. Manzolaro, S. Corradetti, D. Scarpa, F. Rossetto, F. Martinez Dominguez, J. Vasquez, M. Rossignoli, M. Calderolla, R. Silingardi, A. Mozzi, F. Borgna, G. Vivian, E. Boratto, M. Ballan, G. Prete, and G. Meneghetti. "The RIB production target for the SPES project." In: *European Physical Journal A* 51.10 (2015). DOI: 10.1140/EPJA/I2015-15128-6.

[197] M. Manzolaro, S. Corradetti, M. Ballan, R. Salomoni, A. Andrighetto, and G. Meneghetti. "Thermal and mechanical characterization of carbides for high temperature nuclear applications." In: *Materials* 14.10 (2021), p. 2689. ISSN: 1996-1944. DOI: 10.3390/MA14102689.

[198] S. Corradetti, S. M. Carturan, G. Maggioni, G. Franchin, P. Colombo, and A. Andrighetto. "Nanocrystalline titanium carbide/carbon composites as irradiation targets for isotopes production." In: *Ceramics International* 46.7 (2020), pp. 9596–9605. ISSN: 0272-8842. DOI: 10.1016/J.CERAMINT.2019.12.225.

[199] S. Corradetti, S. Carturan, L. Biasetto, A. Andrighetto, and P. Colombo. "Boron carbide as a target for the SPES project." In: *Journal of Nuclear Materials* 432.1-3 (2013), pp. 212–221. ISSN: 0022-3115. DOI: 10.1016/J.JNUCMAT.2012.08.024.

[200] Y. Zhang, I. Remec, G. D. Alton, and Z. Liu. "Simulation of rare isotope release from ISOL target." In: *Nuclear Instruments and Methods in Physics Research, Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 620.2-3 (2010), pp. 142–146. ISSN: 01689002. DOI: 10.1016/J.NIMA.2010.04.015.

[201] S. Corradetti, A. Andrighetto, M. Manzolaro, D. Scarpa, J. Vasquez, M. Rossignoli, A. Monetti, M. Calderolla, and G. Prete. "Research and development on materials for the SPES target." In: *EPJ Web of Conferences* 66 (2014). DOI: 10.1051/EPJCONF/20146611009.

[202] D. Scarpa, L. Biasetto, S. Corradetti, M. Manzolaro, A. Andrighetto, S. Carturan, G. Prete, P. Zanonato, and D. W. Stracener. "Neutron-rich isotope production using the uranium carbide multi-foil SPES target prototype." In: *European Physical Journal A* 47.3 (2011), pp. 1–7. DOI: 10.1140/EPJA/I2011-11032-5.

[203] A. Monetti, R. A. Bark, A. Andrighetto, P. Beukes, J. L. Conradie, S. Corradetti, D. Fourie, C. Lussi, M. Manzolaro, G. Meneghetti, G. Prete, M. Rossignoli, D. Scarpa, P. Van Schalkwyk, N. Stoddart, and J. Vasquez. "On-line test using multi-foil SiC target at iThemba LABS." In: *The European Physical Journal A* 52.6 (2016), pp. 1–10. ISSN: 1434-601X. DOI: 10.1140/EPJA/I2016-16168-0.

[204] A. Ferrari, P. Sala, A. Fasso, and J. Ranft. "FLUKA: A Multi-Particle Transport Code." In: *CERN-2005-10, INFN TC05/11, SLAC-R-733* (2005). DOI: 10.2172/877507.

[205] G. Battistoni, F. Cerutti, A. Fassò, A. Ferrari, S. Muraro, J. Ranft, S. Roesler, and P. R. Sala. "The FLUKA code: description and benchmarking." In: *AIP Conference Proceedings* 896.1 (2007), p. 31. ISSN: 0094-243X. DOI: 10.1063/1.2720455.

[206] T. T. Böhlen, F. Cerutti, M. P. Chin, A. Fassò, A. Ferrari, P. G. Ortega, A. Mairani, P. R. Sala, G. Smirnov, and V. Vlachoudis. "The FLUKA Code: Developments and Challenges for High Energy and Medical Applications." In: *Nuclear Data Sheets* 120 (2014), pp. 211–214. ISSN: 0090-3752. DOI: 10.1016/J.NDS.2014.07.049.

[207] M. Manzolaro, F. D'Agostini, A. Monetti, and A. Andrighetto. "The SPES surface ionization source." In: *Review of Scientific Instruments* 88.9 (2017). DOI: 10.1063/1.4998246.

[208] M. Manzolaro, A. Andrighetto, G. Meneghetti, A. Monetti, D. Scarpa, M. Rossignoli, J. Vasquez, S. Corradetti, M. Calderolla, and G. Prete. "Ongoing characterization of the forced electron beam induced arc discharge ion source for the selective production of exotic species facility." In: *Review of Scientific Instruments* 85.2 (2014). ISSN: 0034-6748. DOI: 10.1063/1.4857175.

[209] D. Scarpa, J. Vasquez, A. Tomaselli, D. Grassi, L. Biasetto, A. Cavazza, S. Corradetti, M. Manzolaro, J. Montano, A. Andrighetto, and G. Prete. “Studies for aluminum photoionization in hot cavity for the selective production of exotic species project.” In: *Review of Scientific Instruments* 83.2 (2012). DOI: 10.1063/1.3673628.

[210] D. Scarpa, E. Mariotti, O. S. Khwairakpam, V. Parenti, A. Buono, P. Nicolosi, M. Calderolla, A. Khanbekyan, M. Ballan, L. Centofante, S. Corradetti, G. Lilli, M. Manzolaro, A. Monetti, L. Morselli, and A. Andrighetto. “New solid state laser system for SPES: Selective Production of Exotic Species project at Laboratori Nazionali di Legnaro.” In: *Review of Scientific Instruments* 93.8 (2022), p. 083001. ISSN: 0034-6748. DOI: 10.1063/5.0078913.

[211] J. P. Ramos. “Thick solid targets for the production and online release of radioisotopes: The importance of the material characteristics – A review.” In: *Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms* 463 (2020), pp. 201–210. ISSN: 0168-583X. DOI: 10.1016/J.NIMB.2019.05.045.

[212] G. Lilli, L. Centofante, M. Manzolaro, A. Monetti, R. Oboe, and A. Andrighetto. “Remote handling systems for the Selective Production of Exotic Species (SPES) facility.” In: *Nuclear Engineering and Technology* 55 (2023), pp. 378–390. ISSN: 1738-5733. DOI: 10.1016/J.NET.2022.08.034.

[213] M. T. Wilson. “Remote handling and accelerators.” In: *IEEE Transactions on Nuclear Science* 30.4 (1983), pp. 2138–2141. DOI: 10.1109/TNS.1983.4332741.

[214] G Murdoch. “Remote Handling in High-Power Proton Facilities.” In: 2005, pp. 174–178. ISBN: 0-7803-8859-3. DOI: 10.1109/PAC.2005.1590390.

[215] M. Lewitowicz. “The SPIRAL2 project and experiments with high-intensity rare isotope beams.” In: *J.Phys.Conf.Ser.* 312.SECTION 5 (2011). ISSN: 17426596. DOI: 10.1088/1742-6596/312/5/052014.

[216] S. Corradetti, M. Manzolaro, S. M. Carturan, M. Ballan, L. Centofante, G. Lilli, A. Monetti, L. Morselli, D. Scarpa, A. Donzella, A. Zenoni, and A. Andrighetto. “The SPES target production and characterization.” In: *Nuclear Instruments and Methods in Physics Research, Section B: Beam Interactions with Materials and Atoms* 488 (2021), pp. 12–22. ISSN: 0168583X. DOI: 10.1016/j.nimb.2020.12.003.

[217] *IEC 61784-3:2021. Industrial communication networks - Part 3: Functional safety fieldbuses*. International Electrotechnical Commission, 2021.

[218] G. Peserico, A. Morato, F. Tramarin, and S. Vitturi. "Functional Safety Networks and Protocols in the Industrial Internet of Things Era." In: *Sensors 2021, Vol. 21, Page 6073* 21.18 (2021), p. 6073. ISSN: 1424-8220. DOI: 10.3390/S21186073.

[219] D. Benini, M. L. Allegrini, P. L. de Ruvo, G. Prete, L. Sarchiapone, and D. Zafiropoulos. "The SPES Access Control System." In: *LNL Annual Report 2018* 258 (2019). ISSN: 1828-8561.

[220] P. L. de Ruvo, M. L. Allegrini, D. Benini, and G. Prete. "Functional Architecture of SPES Safety System." In: *LNL Annual Report 2019* 259 (2020). ISSN: 1828-8561.

[221] D. Benini, M. L. Allegrini, P. L. de Ruvo, and G. Prete. "Security Procedures for the SPES Building Access Control System." In: *LNL Annual Report 2019* 259 (2020). ISSN: 1828-8561.

[222] *IEC 62061:2021. Safety of machinery - Functional safety of safety-related control systems*. International Electrotechnical Commission, 2021.

[223] B. Chacon, Scott and Straub. *Pro git*. Apress, 2014.

[224] L. R. Dalesio, J. O. Hill, M. Kraimer, S. Lewis, D. Murray, S. Hunt, W. Watson, M. Clausen, and J. Dalesio. "The experimental physics and industrial control system architecture: past, present, and future." In: *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 352.1-2 (1994), pp. 179–184. ISSN: 0168-9002. DOI: 10.1016/0168-9002(94)91493-1.

[225] J. Vasquez, R. Oboe, A. Andrighetto, I. Cristofolini, M. Guerzoni, A. Margotti, G. Meneghetti, D. Scarpa, M. Bertocco, and G. Prete. "The SPES target chamber remote handling system." In: *2013 IEEE International Conference on Mechatronics, ICM 2013* (2013), pp. 356–360. DOI: 10.1109/ICMECH.2013.6518562.

[226] A. Donzella, A. Zenoni, M. Ferrari, A. Andrighetto, M. Ballan, F. Borgna, S. Corradetti, F. D'Agostini, M. Manzolaro, A. Monetti, M. Rossignoli, D. Scarpa, D. Turcato, and A. Zanettin. "Shielding analysis of the SPES targets handling system and storage area using the Monte Carlo code FLUKA." In: *Nuclear Instruments and Methods in Physics Research, Section B: Beam Interactions with Materials and Atoms* 463 (2020), pp. 169–172. ISSN: 0168583X. DOI: 10.1016/j.nimb.2019.05.069.

[227] L. Centofante, A. Donzella, A. Zenoni, M. Ferrari, M. Ballan, S. Corradetti, F. D'Agostini, G. Lilli, M. Manzolaro, A. Monetti, L. Morselli, D. Scarpa, and A. Andrighetto. "Study of the radioactive contamination of the ion source complex in the Selective Production of Exotic Species (SPES) facility." In: *Review of Scientific Instruments* 92.5 (2021), p. 53304. DOI: 10.1063/5.0045063.

[228] A. Donzella, M. Ferrari, A. Zenoni, D. Paderno, I. Bodini, V. Villa, M. Ballan, L. Centofante, A. Monetti, C. Petrovich, L. Zangrando, and A. Andrighetto. "Residual activation of the SPES Front-End system: a comparative study between the MCNPX and FLUKA codes." In: *European Physical Journal A* 56.2 (2020). ISSN: 1434601X. DOI: 10.1140/epja/s10050-020-00068-1.

[229] D. B. Pelowitz, J. W. Durkee, J. S. Elson, M. L. Fensin, J. S. Hendricks, M. R. James, R. C. Johns, G. W. Mckinney, S. G. Mashnik, J. M. Verbeke, L. S. Waters, and T. A. Wilcox. "MCNPX User's Manual. Version 2.7.0." In: *Los Alamos National Laboratory, LA-CP-11-00438* (2011).

[230] CORDEL. *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties*. Tech. rep. World NuclearAssociation, 2020.

[231] C. Xie, L. Huang, R. Wang, J. Deng, Y. Y. Shu, and D. Jiang. "Research on quantitative risk assessment of fuel leak of LNG-fuelled ship during lock transition process." In: *Reliability Engineering and System Safety* 221 (2022), p. 108368. ISSN: 0951-8320. DOI: 10.1016/j.ress.2022.108368.

[232] *Layer of protection analysis : simplified process risk assessment.* CCPS concept book. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2001. ISBN: 1591244455.

[233] *Methods for determining and processing probabilities, Red Book*. English. Arnhem: CPR12E, 2005. ISBN: 9012085438 9789012085434.

[234] C. A. Ericson. *Hazard analysis techniques for system safety*. English. Hoboken, NJ: Wiley-InterScience, 2016. ISBN: 9781118940389 1118940385.

[235] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos. "Hazard and operability (HAZOP) analysis. A literature review." In: *Journal of Hazardous Materials* 173.1-3 (2010), pp. 19–32. ISSN: 03043894. DOI: 10.1016/J.JHAZMAT.2009.08.076.

[236] *IEC 31010:2019. Risk management - Risk assessment techniques.* International Electrotechnical Commission, 2019. ISBN: 978 0 580 95443 6.

[237] J. L. Fuentes-Bargues, M. C. González-Cruz, C. González-Gaya, and M. P. Baixauli-Pérez. "Risk Analysis of a Fuel Storage Terminal Using HAZOP and FTA." In: *International Journal of Environmental Research and Public Health 2017, Vol. 14, Page 705* 14.7 (2017), p. 705. ISSN: 1660-4601. DOI: 10.3390/IJERPH14070705.

[238] *IEC 61882:2016. Hazard and operability studies (HAZOP studies) — Application guide*. International Electrotechnical Commission, 2016. ISBN: 978 0 580 87354 6.

[239] A. M. Dowell. "Layer of protection analysis for determining safety integrity level." In: *ISA Transactions* 37.3 (1998), pp. 155–165. ISSN: 00190578. DOI: 10.1016/S0019-0578(98)00018-4.

[240] A. M. Dowell. "Layer of Protection Analysis and Inherently Safer Processes." In: *Process Safety Progress* 18.4 (1999), pp. 214–220. ISSN: 10668527. DOI: 10.1002/PRS.680180409.

[241] R. J. Willey. "Layer of protection analysis." In: *Procedia Engineering* 84 (2014), pp. 12–22. ISSN: 18777058. DOI: 10.1016/J.PROENG.2014.10.405.

[242] *IEC 61511-3:2016. Functional safety — Safety instrumented systems for the process industry sector*. International Electrotechnical Commission, 2016. ISBN: 978 0 580 79125 3.

[243] J. Guiochet. "Hazard analysis of human–robot interactions with HAZOP–UML." In: *Safety Science* 84 (2016), pp. 225–237. ISSN: 18791042. DOI: 10.1016/j.ssci.2015.12.017. arXiv: 1602.03139.

[244] N. Papakonstantinou, J. Linnosmaa, J. Alanen, A. Z. Bashir, B. O'Halloran, and D. L. Van Bossuyt. "Early hybrid safety and security risk assessment based on interdisciplinary dependency models." In: *Proceedings - Annual Reliability and Maintainability Symposium* 2019-January (2019). ISSN: 0149144X. DOI: 10.1109/RAMS.2019.8768943.

[245] N. Papakonstantinou, J. Linnosmaa, A. Z. Bashir, T. Malm, and D. L. Van Bossuyt. "Early combined safety-security defense in depth assessment of complex systems." In: *Proceedings - Annual Reliability and Maintainability Symposium* 2020-January (2020). ISSN: 0149144X. DOI: 10.1109/RAMS48030.2020.9153599.

[246] K. S. Jeong, D. G. Lee, K. W. Lee, and H. K. Lim. "A qualitative identification and analysis of hazards, risks and operating procedures for a decommissioning safety assessment of a nuclear research reactor." In: *Annals of Nuclear Energy* 35.10 (2008), pp. 1954–1962. ISSN: 0306-4549. DOI: 10.1016/J.ANUCENE.2008.05.008.

[247] D. Paderno, I. Bodini, A. Zenoni, A. Donzella, L. Centofante, and V. Villa. "Proof of Concept Experience in the SPES Experiment: First Solutions for Potentiometers Replacement in System Maintenance." In: *Lecture Notes in Mechanical Engineering* (2021), pp. 301–306. ISSN: 21954364. DOI: 10.1007/978-3-030-70566-4_48.

[248] D. Pramberger, Y. Q. Aguiar, J. Trummer, and H. Vincke. "Characterization of Radio-Photo-Luminescence (RPL) Dosimeters as Radiation Monitors in the CERN Accelerator Complex." In: *IEEE Transactions on Nuclear Science* 69.7 (2022), pp. 1618–1624. ISSN: 15581578. DOI: 10.1109/TNS.2022.3174784.

[249] A. Zimmaro, R. Ferraro, J. Boch, F. Saigne, R. G. Alia, M. Brucoli, A. Masi, and S. Danzeca. "Testing and Validation Methodology for a Radiation Monitoring System for Electronics in Particle Accelerators." In: *IEEE Transactions on Nuclear Science* 69.7 (2022), pp. 1642–1650. ISSN: 15581578. DOI: 10.1109/TNS.2022.3158527.

[250] M. Marzo, R. G. Alia, A. Infantino, M. Brucoli, and S. Danzeca. "Impact of neutrons on the RadFET dose response when exposed to mixed-fields." In: *Radiation Physics and Chemistry* 179 (2021), p. 108062. ISSN: 0969-806X. DOI: 10.1016/J.RADPHYSCHEM.2018.11.016.

[251] I. Mateu, M. Glaser, G. Gorine, M. Moll, G. Pezzullo, and F. Ravotti. "ReadMON: A portable readout system for the CERN PH-RADMON Sensors." In: *IEEE Transactions on Nuclear Science* 65.8 (2018), pp. 1700–1707. ISSN: 00189499. DOI: 10.1109/TNS.2017.2784684.

[252] L. Centofante. *Study of a new Target-Ion Source unit and beam line for an energy and power upgrade of the SPES project at INFN LNL*. PhD Thesis. University of Brescia, 2022.

[253] R. A. Fisher. *The design of experiments*. Oxford, England: Oliver & Boyd, 1935.

[254] D. C. Montgomery. *Design and Analysis of Experiments, 8th Edition*. John Wiley & Sons, Incorporated, 2012. ISBN: 9781118214718.

[255] *IEC 61131-3:2013. Programmable Controllers. Part 3: Programming Languages*. International Electrotechnical Commission, 2013.

[256] A. Zoitl and R. Lewis. *Modelling Control Systems Using IEC 61499, 2nd Edition*. Vol. 95. Institution of Engineering and Technology, 2014. ISBN: 9781849197601. DOI: 10.1049/PBCE095E.

[257] P Ovsiannikova and V Vyatkin. "Towards user-friendly model checking of IEC 61499 systems with counterexample explanation." In: *ETFA* (2021). DOI: 10.1109/ETFA45728.2021.9613491.

[258] C. Schnakenbourg, J. M. Faure, and J. J. Lesage. "Towards IEC 61499 function blocks diagrams verification." In: *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics* 3 (2002), pp. 210–215. ISSN: 08843627. DOI: 10.1109/ICSMC.2002.1176038.

[259] Z. Xu, D. Zhong, W. Li, H. Huang, and Y. Sun. "Formal verification of dynamic hybrid systems: a NuSMV-based model checking approach." In: *ITM Web of Conferences* 17 (2018). DOI: 10.1051/itmconf/20181703026.

[260] M. Frappier, B. Fraikin, R. Chossart, R. Chane-Yack-Fa, and M. Ouenzar. "Comparison of model checking tools for information systems." In: *Lecture Notes in Computer Science* 6447 LNCS (2010), pp. 581–596. ISSN: 03029743. DOI: 10.1007/978-3-642-16901-4_38.

[261] A. Pakonen, I. Buzhinsky, and V. Vyatkin. "Counterexample visualization and explanation for function block diagrams." In: *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)* (2018), pp. 747–753. DOI: 10.1109/INDIN.2018.8472025.