A Virtual Digital Twin Approach for Safety-Centric Risk Management for Extreme Light Infrastructure – Nuclear Physics (ELI-NP)

Aurelian Ionescu, Cicerone Laurentiu Popa, Radu Constantin Parpala, Lidia Florentina Parpala, and Costel Emil Cotet*

Department of Robots and Manufacturing Systems, Faculty of Industrial Engineering and Robotics, University Politehnica of Bucharest, 060042 Bucharest, Romania
Email: aurelian.ionescu85@stud.fiir.upb.ro (A.I.); laurentiu.popa@upb.ro (C.L.P.); radu.parpala@upb.ro (R.C.P.); lidia.parpala@upb.ro (L.F.P.); costel.cotet@upb.ro (C.E.C.)
Manuscript received July 3, 2025; accepted October 5, 2025; published November 5, 2025.

***Abstract*—High-risk industrial environments, such as particle accelerator facilities, require rigorous validation of safety interlocks, yet testing these systems under real operational conditions poses significant challenges. This paper presents a safety-focused digital twin framework designed to integrate real PLC hardware implementing Machine Protection System (MPS) and Personnel Protection System (PPS) logic. The framework connects partially to the facility's control infrastructure (EPICS) and to the simulation platform via OPC UA and supports Hardware-in-the-Loop (HIL) testing to assess safety system performance in realistic but risk-free conditions. Initial validation focused on interlock response time and failure mode analysis, with test results confirming beam shutdown triggers within 1−5 ms across twelve simulated fault scenarios. A structured Failure Modes and Effects Analysis (FMEA) quantified the criticality and detection coverage of potential faults, guiding design improvements and operational priorities. Although full-scale digital twin simulation is planned for deployment once the facility becomes fully operational, the current implementation already supports early-stage verification and risk assessment. Contributions include the demonstrations of real-time safety interlock performance using actual PLC code in tight coupling with MPS and PPS hardware architecture and method. This framework lays the foundation for proactive, simulation-driven validation in high-risk infrastructure for the Extreme Light Infrastructure – Nuclear Physics (ELI-NP) VEGA linear accelerator in Magurele, Romania.**

***Keywords*—digital twin, Linear Accelerator (LINAC), machine protection system, personnel protection system, simulation, OPC Unified Architecture (OPC UA), Failure Mode and Effects Analysis (FMEA), risk analysis**

I. Introduction

High-risk industrial facilities, such as particle accelerator installations, demand robust safety architectures and predictive risk assessment. Traditional safety methods-based on statistic hazard studies or post-incident reviews – fail to reflect dynamic, real-time operational conditions. A critical challenge lies in validating safety interlocks before commissioning, particularly for fast-reacting systems such as Machine Protection System (MPS) and Personnel Protection System (PPS), where live testing may be impractical or unsafe. Digital twin technology, which creates a real-time virtual replica of the physical system, offers a viable solution. A digital twin mirrors process states via Programmable Logic Controller (PLC) data and support scenario-driven simulation to evaluate fault responses, verify protection logic, and enable operator training. The present research focuses on developing a digital twin framework connected to real PLC hardware through OPC UA, enabling Hardware-in-the-Loop (HIL) testing of safety logic. The scope includes integration of MPS/PPS safety systems, real-time fault injection, and evaluate interlock responses. Application of Failure Modes and Effects Analysis (FMEA) complements the validation process by identifying critical faults and mitigation strategies [1].

This work illustrates how a digital twin can transform industrial safety management from reactive to proactive by enabling rehearsal of dangerous incidents and verification of protection systems in a virtual environment.

II. Methodology

A. Digital Twin Architecture and Data Sources

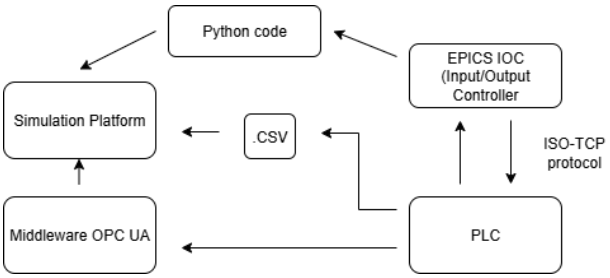

Fig. 1. Methods of integration with simulation platform.

As a first step, the block diagram–based system architecture is established, providing the structural framework required for subsequent model calibration and validation against empirical data. Operational parameters (processing times, PV, failure rates, personnel walking routes, etc.) are gathered from facility records, real-time tests and expert input. The model will be validated by comparing simulated output against normal plant behavior, ensuring it behaves like the actual system in fault-free operation. Concurrently, the Safety Interlock Logic (MPS/PPS) is captured from the PLC programs. Conceptually, the interlock logic is represented in the simulator by event-triggered mechanisms. Physically, the real PLCs (CPU1512SP-1 PN, Siemens S7-1500 series) are integrated in *hardware-in-the-loop* mode. The PLCs are configured as OPC UA server (via Siemens TIA Portal), exposing their internal I/O variables. In this architecture, if the PLC detects a hardware fault (or if the simulator triggers a fault condition),

the PLC outputs change state and those changes will be immediately mirrored in the simulation. This bidirectional linkage ensures actions in the virtual model and the actual control logic remain coherent in real time [2] (see Fig. 1).

B. Safety Interlock Systems

Safety Interlock Systems (the MPS and PPS) are essential pillars of industrial risk mitigation. They continuously monitor critical parameters and automatically intervene to prevent accidents when thresholds are exceeded. International standards (IEC 61508/61511) prescribe that such systems be highly reliable, redundant, and "fail-safe", ensuring that any detected hazard leads to an immediate and predictable shutdown of hazardous. In accelerator facilities, hardware relays or PLC interlocks will, for example, cut power to beam devices or insert beam shutters if radiation levels rise above safe limits or if an access door is opened. In other industries (e.g., manufacturing robots), similar systems (light curtains, emergency stop circuits) halt motion instantly if a worker breaches a protected zone. In our study, the MPS protects equipment by sensing instrument faults (e.g., magnet quench, vacuum loss) and dumping the beam, while the PPS protects personnel by controlling access and enforcing safe shutdown if people are in danger. These interlocks are designed according to safety standards and operate at high speeds and priority, providing the safety "front line" for the facility [3] (see Fig. 2).

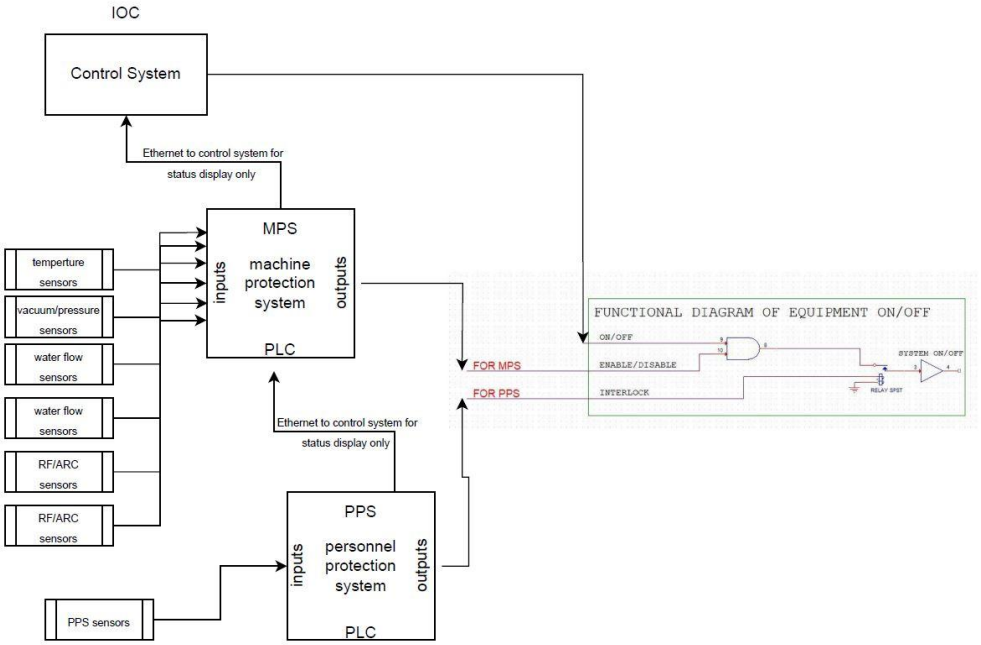

Fig. 2. MPS/PPS PLC logic diagram.

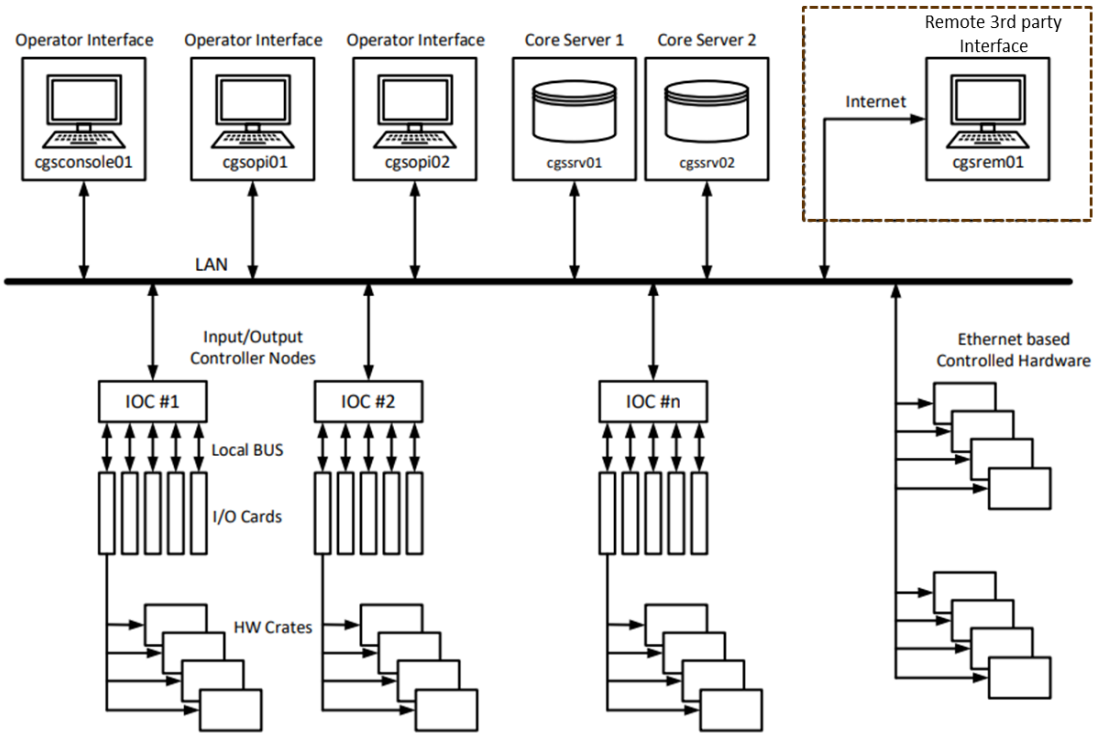

Fig. 3. Software control system block diagram.

C. PLC Architecture and Control System Integration

The core of the digital twin's control logic is the real industrial PLC-based safety system. Each PLC module has galvanically isolated inputs and outputs. This isolation prevents electrical cross-talk: a sensor contact at 0 V is interpreted as a fault, whereas 24 V indicates a normal (no fault) condition. In practice, this active-low logic means any open-circuit or loss of power to a safety sensor immediately signals a fault. The PLC modules are modular and expandable: new modules can be added to monitor additional equipment or zones without redesigning the entire system. Each module performs specific monitoring tasks (e.g., one handles radiation detectors, another monitors temperature sensors) and they communicate via standard fieldbus protocols (e.g., PROFINET) for coordination. The ladder logic programmed into the PLC reflects the facility's safety architecture: various fault inputs (such as temperature fault, vacuum fault, radiation alarm, door open) are logically OR'd to one or more interlock outputs. When any critical input goes bad, the PLC triggers an immediate shutdown of the beam or power to the accelerator, ensuring rapid response to hazards [4] (see Fig. 3).

This one-to-one mapping of safety signals between the PLC hardware and the virtual environment is what enables realistic hardware-in-the-loop testing of the interlock systems.

D. Facility Layout and Access Control

The physical facility layout is divided into three exclusion zones for the LINAC. Zone 1 corresponds to the LINAC vault (room E-P-10). Zone 2 comprises adjacent areas (rooms E-P-09 and E-P-08) on the accelerator floor. Zone 3 covers the experimental hall (E7) where beams and targets are located. Each zone has entry doors and emergency exits, and all entrances to radiation areas are interlocked. To protect personnel, an Access Control System (ACS) is implemented as part of the PPS [5]. The ACS is a standalone safety subsystem (separate from the main EPICS control network) that enforces the following requirements: it prevents any person from being inside a hazardous zone when the beam is active; it blocks beam operation if any door is not fully closed; it enforces mandatory search procedures before start-up; and it provides visual/audible warnings prior to beam enablement. The ACS hardware is redundant and fail-safe: for instance, if a door switch fails or no one responds to the evacuation tone, the system will automatically inhibit beam production [6] (see Fig. 4).

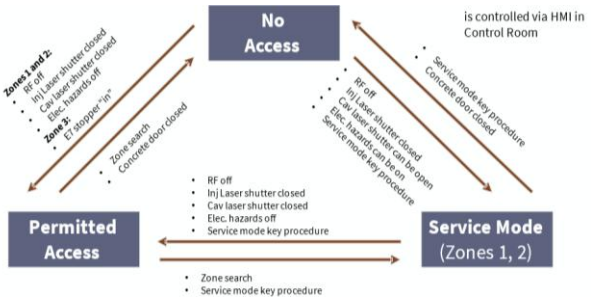

Fig. 4. Transition between access states.

E. Hardware-in-the-Loop Integration

A central element of this work is the **HIL integration** between the virtual model and the real control hardware. The Siemens S7-1500 PLC running the MPS/PPS logic is configured as an OPC UA server that publishes it's I/O tags. On the simulation side, two integration methods are implemented:

OPC UA coupling: The simulation tool (or an external client software) connects as an OPC UA, UA Expert client to the PLC's exposed variables. Process variables, door states, beam-permit signals, etc., are exchanged in real-time. In one architecture, an OPC DataHub intermediary can be used: the PLC writes I/O to the DataHub, and the simulator reads them from the hub (and vice versa). This live data exchange makes the digital twin "read" the PLC status and act through actual I/O wiring (see Fig. 5).

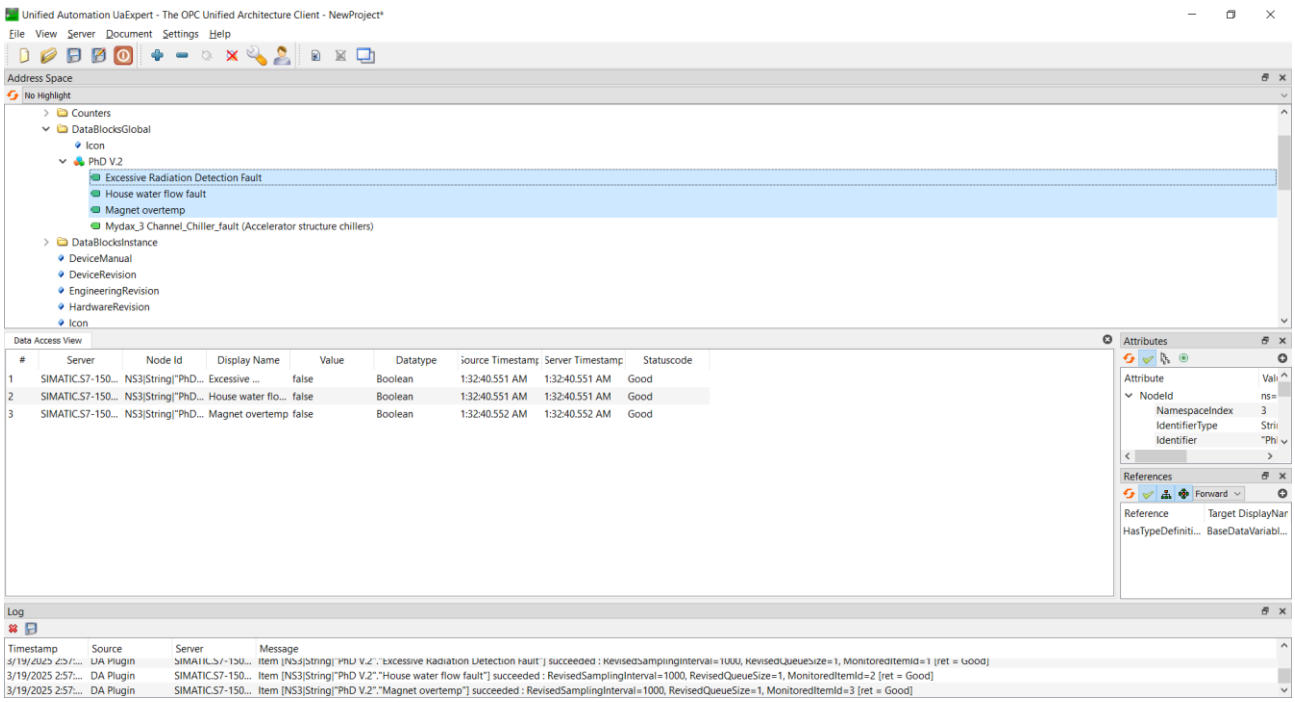

Fig. 5. UA expert coupling with PLC server.

Fig. 6. Cycle time statistics.

File-based exchange: As an alternative or fallback, the PLC can periodically export its relevant variables to a DataLogger CSV file (via a script or SCADA HMI routine). The simulation platform imports this CSV on-the-fly to update initial conditions or ongoing parameters. Conversely, the simulation can write outputs (fault notes, timing information) to a file that the PLC host reads. This batch-mode approach enables integration even if continuous OPC UA connectivity is not available [7] (see Fig. 6).

III. Results and Discussion

Interlock response verification: The combined PLC-testing setup demonstrated that the modeled MPS and PPS systems are capable of meeting strict reaction-time requirements.

This is in line with expectations for hardware interlocks and far faster than any human operator could respond. For perspective, by the time a technician notices a radiation alarm visually, the MPS/PPS have already cut the beam. This underscores the necessity of automated protection: the digital twin shows quantitatively that the safety automation reacts in time to prevent damage, and that operator intervention cannot substitute for it under fast-fault conditions. However, the simulations also highlight the need for operator training: once an interlock trips, staff must follow correct procedures to safely reset the system and resume operation (see Table 1).

Table 1. Summary of key quantitative results

Metric	Quantitative Result	Notes/Remarks
Average Interlock Response Time	1-5 ms	Time from fault trigger to beam shutdown
Shortest Recorded Response Time	1.019 ms	Recorded via Siemens TIA Portal diagnostics
Longest Recorded Response Time	4.099 ms	Occurred during simulated faults
Number of Tested Failure Scenarios	16	Includes magnet overheating, vacuum loss, radiation alarm

Table 2. FMEA

Failure Mode	Cause(s)	Effect(s)	Severity	Occurrence	Detection method and ratings	RPN	PLC response	Mitigation/improvements actions
Magnet Over-Temperature Fault	Cooling failure or overcurrent in solenoids, bends, quads, sextupoles	Magnet damage, beam mis-steering, downtime	before	before	Thermal switch sensors (>70°C) trigger fault before/after	before 72-moderate after **48** low	Disable electron beam, cut magnet power, log event to EPICS	Redundant thermal sensors, predictive analytics, manual reset required.
			8	3				
			after	after				
			8	3				
					3 **2**			
House Water Flow Fault	Flow rate drops below 50 m³/h or temp deviates from 19±1°C	Overheating of LINAC components, shutdown	before	before	Flow meters and temperature sensors on PLC I/O before/after	before 160 high risk after **72**-moderate	Disable electron beam and secondary equipment, log to EPICS	Circulate pumps alternative, added flow/ **Δ**p trending and alarm rationalisation, preventive maintenance.
			8	5				
			after	after				
			8	3				
					4 **3**			

OPC UA Reliability and Cybersecurity: The OPC UA integration in the safety-critical HIL simulation is specifically designed for reliability and robust cybersecurity. Critical OPC UA failure modes, such as certificate expiration and communication interruptions, are proactively managed using manual certificate management and a runtime license with no functional limitations through UA Expert, ensuring valid, authenticated sessions. Cybersecurity threats, including Man-in-the-Middle (MITM) and Denial-of-Service (DoS) attacks, are mitigated following IEC 62443 guidelines. Network resilience is ensured through a dedicated isolated subnet utilizing a single mode fiber-optic ring topology with redundant switches. Additional security layers include physical tamper detection on IT racks, comprehensive CCTV surveillance, and stringent access control measures, further safeguarding the network and the devices from unauthorized interference [8].

Incident impact assessment: The model will allow evaluating how different incident types affect operations. For example, a brief beam trip caused by a minor equipment fault

(a few-second shutdown) has negligible impact if rare-operations recover quickly, and losses are minimal. In contrast, a major event requiring a multi-hour evacuation (such as a high-radiation alarm triggered by a leak) can significantly delay experiments and require costly requalification tests after restart.

FMEA Process Summary: The methodology employed a structured FMEA scoring system – assigning severity, occurrence, detection methods and ratings – to quantify each identified failure mode, yielding a Risk Priority Number (RPN) that highlights the most critical risk. Failure mode was rated on three 1−10 scales (S, O, D). The RPN was then calculated as RPN = S × O × D, yielding values from 1 to 1000. Risk thresholds were defined as: RPN ≥ 150 (high risk, immediate action), 100-149 (moderate, near-term improvement), and <100 (low, monitor and maintain). For instance, a water-flow fault initially scored RPN = 160; mitigation measures such as improved flow monitoring and a backup pump reduced this to RPN = 72.

This integration of FMEA with simulation in the future will also facilitate safety logic refinement, as virtual tests under various fault scenarios can reveal where the automated safety logic required adjustment to better detect and mitigate emerging risks. Table 2 presents a significant excerpt from this analysis, including relevant failure modes [9].

Applicability to other high-risk industries: The virtual digital twin methodology with OPC UA-linked Hardware-in-the-Loop (HIL) safety simulation, can be extended to other high-risk industries such as chemical plants and oil&gas operations. In chemical plant, this method could simulate critical scenarios such as hazardous chemical spills, pressure vessel ruptures, or unexpected temperature fluctuations, allowing validation of emergency shutdown procedures triggered via OPC UA-linked PLCs. Similarly, for oil&gas installations, digital twin could model pipeline ruptures, wellhead pressure spikes, or gas leaks, rigorously testing the automated responses of critical safety equipment like emergency shutdown valves, blowout preventers, and fire suppression systems in real-time HIL environments.

IV. Case Study and Similar Applications

Several prior examples in the accelerator field demonstrate the benefits of digital twin strategies:

CERN LHC 2008 incident: On 19 September 2008, during commissioning of the Large Hadron Collider, a faulty electrical connection between two magnets in Sector 3–4 melted, causing a massive helium leak and damaging 53 magnets. This resulted in over a year of downtime and costs on the order of tens of millions of dollars. The root causes were later identified as a poor weld and the lack of online monitoring of busbar voltage. In response, CERN installed thousands of voltage sensors and improved quality control. A digital twin of the LHC sector could have predicted such a quench scenario, potentially revealing the design weakness beforehand. This case highlights how real-time diagnostics and simulation (as available in a digital twin) are crucial in preventing long, expensive outages [10].

SPARC_LAB (INFN, Italy): Researchers developed a digital twin of the SPARC_LAB plasma accelerator using machine learning. They trained neural networks (autoencoders and PCA models) on real beam data to predict the transverse beam profile without firing the accelerator. The twin's predictions matched real measurements closely, and ran almost *200,000 times faster* than the detailed physics simulation it replaced. This "virtual diagnostic" twin allowed rapid tuning and fault analysis without beam time, minimizing downtime. It illustrates that even in complex accelerators, surrogate models can form part of a twin for real-time decision support [11].

Each of these cases demonstrates that virtual models can enhance safety and performance by enabling pre-testing, real-time diagnostics, and operator training. Our work builds on these lessons by creating a unified simulation environment that not only optimizes beam performance but also actively evaluates and verifies the facility's safety interlocks and evacuation procedures.

V. Related Work

Recent digital twin frameworks emphasize interoperability, fidelity, and lifecycle integration. Schleich *et al.*'s "Shaping the Digital Twin for Design and Production Engineering" [12] outlines scalable and synchronized virtual-physical systems. The UA Expert Client (OPC UA-based integration) implemented in this context aligns with these principles by enabling real-time HIL testing and virtual safety verification for critical infrastructure. Furthermore, Al-Ali *et al.* highlight in their study on LLMs and UML modeling the influence of instruction-tuned models on task alignment [13], while Alsobeh *et al.* [14] demonstrate that metadata-aware LLMs contribute to improved real-time observability in safety-critical environments. Trends in blockchain developments reveal a shift toward integration with intelligent technologies, forming hybrid architectures for enhanced security, scalability, and decision making. Technologies such as Machine Learning (ML), Deep Learning (DL), and federated learning are increasingly combined with blockchain to support decentralized intelligence, especially in domains requiring data trust and resilience [14]. For instance, Khan et. al. proposed a BDLT-IoMT framework integrating blockchain with Support Vector Machine (SVM) learning for secure and efficient processing in medical IoT applications, illustrating how such paradigms can enhance robustness in distributed cyber-physical systems [15].

VI. Conclusion

This study has developed a digital twin framework model for a high-risk accelerator facility, integrating operational flows with the critical MPS and PPS protection systems. The virtual environment, coupled via OPC UA to the real PLC logic and the EPICS control system, will reproduce both workflows and safety events in a virtual setting. The main achievements and lessons learned are:

Hardware-in-the-Loop PLC integration: Enables the real-time linking of a physical PLC with an external/virtual platform. This approach allows the exact MPS/PPS control code to be tested under realistic conditions, ensuring proper safety logic before commissioning and supporting further PLC validation.

Virtual training and verification: The digital twin represents a valuable tool for personnel training.

For example, evacuation drills could be carried out in the simulator using the real control interface, giving operators a realistic practice environment. The model also can verify that all alarms and indicators behave as intended, increasing confidence in the safety procedures.

Identification of optimizations: Experimenting with the twin enables the identification of possible system improvements. These include adding predictive warnings (e.g., trending radiation levels), tuning interlock thresholds for optimal balance between safety and availability, and refining recovery protocols (e.g., reducing restart time after a fault).

Initial validation focused on evaluating interlock performance and system robustness. Twelve simulated fault scenarios triggered beam shutdowns within 1–5 milliseconds, confirming the system's fast response capability. A structured Failure Modes and Effects Analysis (FMEA) identified critical failure paths and detection gaps, guiding early-stage design optimizations and operational focus.

This implementation supports early verification of safety logic prior to full facility operation and demonstrates how simulation-driven approaches can proactively manage risk. The platform establishes a foundation for expanded digital twin functionality, including full beam dynamics simulation and AI-based fault prediction, aligning with Industry 4.0 principles.

By enabling rigorous, reproducible testing of real interlock hardware, the framework offers a model for enhancing safety assurance in particle accelerators and other high-risk infrastructure.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Aurelian Ionescu: Conceptualization, methodology, development of the digital twin architecture, execution of simulations, data analysis, and writing—original draft preparation; Cicerone Laurentiu Popa and Radu Constantin Parpala: Contribution to system integration design, validation of experimental results, and technical supervision; Lidia Florentina Parpala: Data curation, documentation preparation, and manuscript review; Costel Emil Cotet: Conceptual supervision, methodological oversight, and project coordination; all authors had approved the final version.

Acknowledgment

This research was supported by UNSTPB and ELI-NP/IFIN-HH.

References

[1] Variable Energy Gamma System (VEGA System). [Online]. Available: https://www.i-tech.si/wp-content/uploads/2024/04/C.C.pdf

[2] A. G. Siemens. SIMATIC S7-1500/ET 200 MP-system manual. [Online]. Available: https://cache.industry.siemens.com/dl/files/792/59191792/att_895925/v4/s71500_et200mp_system_manual_en-US_en-US.pdf

[3] IEC 61511-1:2016, "Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements," *International Electrotechnical Commission*, 2016.

[4] IEC 61508-1:2010, "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements," I*nternational Electrotechnical Commissio*n, 2010.

[5] CNCAN, "NSR-01:2000 – Fundamental radiological safety norms," *Romanian National Commission for Nuclear Activities Control*, no. 14, 2000.

[6] ANSI/HPS N43.1-2011, "Radiation safety for the design and operation of particle accelerators," American National Standards Institute/Health Physics Society, 2011.

[7] Skkynet Corporation. Reading from an OPC UA server and converting data to OPC DA (Training Video). [Online]. Available: https://cogentdatahub.com/training-videos

[8] H. Rahman, T. Wuest, and M. Shafae, "Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use case of cyberattack taxonomies," *Journal of Manufacturing Systems*, vol. 68, 2023.

[9] IEC 60812:2018, "Failure modes and effects analysis," *International Electrotechnical Commission*, 2018.

[10] *CERN Press Office, Incident in LHC Sector 3–4*, Press Release, Sept. 20, 2008.

[11] G. Latini *et al*., "Design of machine-learning-based algorithms for virtual diagnostics of the electron Beam at SPARC_LAB," *Photonics*, vol. 11, no. 6, art. 516, 2024.

[12] B. Schleich, N. Anwer, L. Mathieu, and S. Wartzack, "Shaping the digital twin for design and production engineering," *CIRP Annals*, vol. 66, no. 1, pp. 141–144, 2017.

[13] A. R. A. Ali, R. Gupta, T. Z. Batool, T. Landolsi, F. Aloul, and A. A. Nabulsi, "Digital twin conceptual model within the context of internet of things," *Future Internet*, vol. 12, no. 10, art. 163, 2020.

[14] B. A. Ahmad, A. Alsobeh, O. Meqdadi, and N. A. Shaikh, "Student-centric evaluation survey to explore the impact of LLMs on UML modeling," *Information*, vol. 16, no. 565, 2025.

[15] A. A. Khan *et al.*, "BDLT-IoMT — A novel architecture: SVM machine learning for robust and secure data processing in internet of medical things with blockchain cybersecurity," *The Journal of Supercomputing*, vol. 81, no. 271, 2025.