Safety Science of Servo Motor Systems

Tamás Tornai, László Gogolák, Igor Fürstner

Tamás Tornai, Doctoral School on Safety and Security Sciences, Obuda University, Népszínház utca 8., 1088 Budapest, Hungary, tam.tornai@stud.uni-obuda.hu

László Gogolák, Department of Mechatronics and Automation, Faculty of Engineering, University of Szeged, 6720 Szeged, Hungary, gogolak@mk.u-szeged.hu

Igor Fürstner, Obuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, József körút 6. , 1088 Budapest, Hungary, furstner.igor@bgk.uni-obuda.hu

Abstract: Servo motor system are key elements of modern industrial automation and robotics, playing an icreasingly complex role in achieving precision motion control and safety critical processes. From the perspective of safety science, the study of these systems covers several closely related areas: functional safety, cyber security, as well as system reliability and fault detection. The safety of servo motor systems is based not only on the presence of protective functions, but also on their integration, the reliability of communication protocols, and the capability of data driven decision making. In this investigation, the aim of safety science is to provide a comprehensive theoretical and practical framework for evaluating the operational integrity, vulnerability, and protection of automated systems.The purpose of this study is to give an overview of the security challenges of servo motor systems and to outline possible research directions at the intersection of mechatronics and safety science.

Keywords: Mechatronic systems ,Motion Control, Servo motor systems, Safety Engineering, System

1 Introduction

Servo motor systems are fundamental elements of modern industrial automation, providing precise positioning, high dynamic and reliable operation in applications ranging from production lines to robotics , logistisc system, CNC machines and even medical devices. The fast response capabilities and high power density of servo drives enable accurate and efficient motion control, while this high level of technical sophistication also means that their malfunction can potentially cause significant physical and material damage [1,2,3,4,5]. The safety science of servo motors is therefore primarily built on physical and functional safert. The hazard arising during the operation of servo systems include unexpected accelerations, overspeed, overloads, mechanical collisions, dangerous torque levels, faulty brakes or improperly managed emergency stops. To prevent these, modern servo drives are equipped with a wirde range of built in safety functions, such as Safe Torque Off (STO), Safe Stop ½ (SS1/SS2), Safe Limited Speed (SLS), Safe Maximum Speed (SMS), Safe Limited Torque (SLT) or Safe Brake Control (SBC) [6, 15,16,17]. The proper integration, validation and maintenance of these functions are essential to avoid accidents.

The operating environment of servo motor systems is extremely diverse it ranges from the high speed movements of industrial robot arms to submicron positioning accuracy on precision manufacturing lines. Ensuring functional safety in such a heterogeneous environment is a complex task, as it requires consideration of the mechanical loads, actuator behavior, control algorithms and human-machine interaction safety. Standerdized safety requrement such as IEC 61508, ISO 13849 or IEC 62061 provide a unified framework for identifying and reducing risks and for determining the necesarry safety integrity levels.

Although servo motor are increasingly becoming networked intelligent devices and thus form part of cyber-physical systems to some extent, cybersecurity in the safety science of servo systems plays a supporting rather than primary role. The communication protection mechanisms such as authenticated communication protocols, password management or basic network protection aim primarily at maintaining functional safety rather than classical information security. In the case of servo motors, the most critical risks still stem from physical failures, improper control or incorrect safety configuration.

The safety science of servo motor systems is therefore mainly a multidisciplinart engineering field, in which mechanical, electrical and control engineering disciplines are closely interconnected. In modern industrial applications, increasing emphasis is placed on real time condition monitoring, fault detection, diagnostics and predictive maintenance, wich enable early detection of failures and activation of safety functions when necessary.

The aim of this study is to provide a comprehensive overview of the physical and functional safety of servo motor systems. The article presents the main risk factors, the mechanical and control engineering solutions required for safe opreation, the relevant industrial standards, and the methods by which fault free and safe operation of servo systems can be ensured. In addition, it briefly addresses the cyber-physical aspects which, although they play a background role, still contribute to the reliable operation of the systems.

2 Safety requirement and challenges in servo drives

2.1 Physical hazards in servo motor systems

The physical risks associated with servo motor systems arise mainly from their high dynamic capabilities and the specific characteristics of electric drive technology. Servo motors are capable of rapid accelerations and highly precise positioning, which are beneficial in industrial applications but can also lead to severe hazards if the system behaves unexpectedly. Overspeed, uncontrolled acceleration, sudden direction changes or slipping may generate dangerous mechanical loads. Typical physical risks include drivetrain overload leading to overheating or mechanical damage, shaft torque shocks, resonance-induced vibrations and gradual bearing wear[3,4,5]. Brake malfunctions, particularly in vertically loaded axes, can result in falling accidents with serious consequences. Industrial experience shows that improperly configured or poorly maintained servo systems frequently exhibit irregular motion behaviour [2,14]. Incorrect parameter-isation, unsuitable acceleration profiles or missing limit stops may all contribute to unsafe operation. To mitigate such risks, modern industrial systems increasingly integrate automated diagnostic functions and real-time monitoring modules capable of detecting abnormal physical behaviour before hazardous conditions develop.

2.2 Functional safety and built-in safety functions

A core component of servo system safety is functional safety, which ensures that failures do not lead to dangerous behaviour and that the system transitions into a predefined safe state [6,7,8,9]. Modern servo drives implement a wide range of built-in safety functions defined by international standards. Among the most important are Safe Torque Off (STO), which prevents torque generation; Safe Stop 1 and 2 (SS1/SS2), which provide controlled or torque-free stopping; Safe Limited Speed (SLS), which restricts maximum speed; Safe Limited Torque (SLT), which constrains mechanical loading; Safe Maximum Speed (SMS), which enforces absolute speed boundaries; and Safe Brake Control (SBC), which ensures reliable brake actuation in critical lifting or vertical axes. These functions belong to the safety category defined in IEC 61800-5-2 and are supported natively by most industrial servo drives [6,7,8]. Functional safety, however, is not achieved merely by enabling drive-level functions. A reliable system requires an appropriate safety architecture, certified sensors, redundant measurement channels and validated control logic. Misconfiguration of safety parameters such as excessive speed limits or incorrect deceleration profiles may provide a false sense of security and fail to adequately protect operators or equipment [1,2,11]. Correct integration therefore requires validation procedures based on standards such as IEC 61508, IEC 62061 and ISO 13849, which define the required Safety Integrity Level (SIL) or Performance Level (PL) for the application.

2.3 Safety architectures and system level approach

Ensuring safety in servo systems requires a system-wide perspective [11,14,15,16,17]. Servo drives typically operate as part of larger automated machines or robotic cells, in which mechanical structures, sensors, communication networks and control logic must all contribute to safe operation. Safety PLCs coordinate safety functions and communicate with drives through protocols such as Safety over EtherCAT, PROFIsafe or CIP Safety [6,11,18]. Although some of these mechanisms include authentication or data-integrity checks, their main purpose is functional safety: ensuring deterministic behaviour and enabling rapid detection of faults.
The effectiveness of a safety system largely depends on its architecture. Redundant sensors, diagnostics-enabled encoders, multi-channel safety relays and validated brake logic enhance fault tolerance and allow the system to react quickly to abnormal conditions [2,11,15]. Simulation tools, including MATLAB/Simulink environments, increasingly play a key role in designing and validating safety functions before real deployment. Recent literature highlights the growing use of mathematical models and virtual prototyping to analyse servo behaviour under overspeed, overload or mechanical failure scenarios. The present study builds on these approaches by evaluating servo system behaviour in a simulation environment and analysing how predictive and machine-learning-based supervision layers can enhance safe operation.

3 Methodology

This section presents the modelling framework and the multi-layered safety supervision architecture developed to analyse and improve the safe operation of servo motor systems. The methodology combines classical control theory, functional safety mechanisms, predictive modelling techniques and machine laerning based decision support. All components were implemented and evaluated in a MATLAB based simulation environment to ensure reproducibility and precise parametric analysis [19,20].

3.1 Servo motor Dynamic Model

A simplified but dynamically accurate model of a permanenet magnet servo motor was adopted for the simulation. The mechanical dynamics are governed by:

$$J\frac{d\omega(t)}{dt} = r(t) - \tau(t) - \tau_L(t) - b\omega(t) \quad (1)$$

where J is the rotor inertia, b the viscous damping coefficient, $\omega(t)$ the angular velocity, $\tau(t)$ the motor torque, and $\tau_L(t)$ an external disturbance torque.The load torque was implemented as a time-varying disturbance, and small measurement noise was added to the speed feedback to emulate realistic encoder behaviour. The simulation was performed with a sampling time of 10^{-4} s, providing high-resolution dynamic analysis.

3.2 PI-Based Speed Control Layer

The core control layer is a classical PI (Proportional–Integral) regulator:

$$\tau_{PI}(t) = K_p e(t) + K_i \int e(t)dt, \qquad e(t) = \omega * (t) - \omega_m(t) \quad (2)$$

Saturation limits are applied:

$$\tau_{PI}(t) \in [-\tau_{max}, \tau_{max}] \quad (3)$$

with an anti windup mechanism that stops integral accumulation when the output saturates.
This PI controller represents the baseline industrial motion control behaviour, and its output serves as the starting point for both predicitve and safety oriented modifications.

3.3 Funcitonal Safety Layer: State Machine Architecture

A deterministic safety state machine was developed in accordance with the safety functions defined in IEC 61800-5-2. The architecture distinguishes four operational state: a Normal mode, in which no intervention is required, a SLS mode that restricts the maximum permissible speed, a SS1 modee thet performs a controlled deceleration and STO mode in which all torque generating functions of the drive are disabled.
Transitions between these states occur when predefined safety related conditions are violated. The controller moves the system toward a higher safety level whenever the measured speed exceeds allowed limits, the motor torque or current

approaches hazardous values, the observed acceleration indicates a tendency toward instability, or when any of the presctibed safety margins is breached. Through continuous monitoring and deterministic state evaulation, the safety state machine ensures that the servo drive enters the safety possible operational whenever potentionally dangerous behaviour is detected.

The safety state machine produces a corrected torque:

$$\tau_{safety}(t) = f_{SM}\big(\omega_m(t), \tau_{cmd}(t), i(t)\big) \tag{4}$$

which overrides all previous torque commands.
This block represents the reactive layer of functional safety.

3.4 Analytical Predictive Supervisor

To reduce unnecessary safety activations and smooth the system's behaviour, an analytical model-based supervisor was implemented. The short-horizon prediction of the angular velocity is obtained using:

$$\widehat{\omega}\big(t + T_{\text{pred}}\big) = \omega(t) + \frac{T_{\text{pred}}}{J}\big(\tau_{PI}(t) - \tau_L(t) - b\,\omega(t)\big) \tag{5}$$

If the predicted velocity approaches the SLS threshold, the supervisor reduces the PI torque before unsafe conditions occur. This layer provides a simple but effective proactive limitation and serves as the analytical baseline for the machine-learning supervisor.

3.5 Machine Learning Supervisor

The key contribution of this study is Random Forest (RF) based supervisor capable of learning optimal torque corrections directly from data.

3.5.1 Training Data Generation

A synthetic dataset cosisting of 5000 samples was generated under randomized operating conditions, in wich the motor speed was deliberately selected around the SLS boundary and the PI controller output as well as the external load torque were varied to represent divesre and realistic dynamic scenarios. For each operating point, the analytical predictive supervisor was applied to compute the corresponding ideal safe torque value, which served as the regression target for model training. In this way, the Random Forest model learned the mapping between the measured speed and th PI torque command, and the torque reduction necesarry to prevent approaching the safety limit. As a result, the RF supervisor approximates the function

$$\boldsymbol{\tau_{RF}} = \boldsymbol{f_{RF}}(\boldsymbol{\omega}, \boldsymbol{\tau_{PI}}) \quad (7)$$

capturing optimal preventive intervention without requiring any explicit knowledge of the underlying physical equations.

3.5.2 RF model Training

Listing 1 shows the MATLAB command used to train the bagged ensemble model with 20 trees.
Mdl = fitrensemble(X,Y,"Method","Bag","NumLearningCycles",20);
The model was compacted for real time use. Training time less than 0.5 seconds.

3.5.3 Runtime Integration

Every 100 simulation steps a new RF prediciton is computed:

$$\tau_{RF}(t) = f_{RF}\left(\omega_{m(t)}, \tau_{PI}(t)\right) \quad (8)$$

Then a smoothing filter is applied:

$$\tau_{RF}(t) = \alpha\tau_{RF}(t-1) + (1-\alpha)\tau_{ra\omega}(t) \quad (9)$$

with $\alpha = 0{,}9$ for actuator friendly smooth transitions. The RF supervisor replaces the PI torque if it predicts unsafe future motion.

3.6 Hierarchical Torque Command Selection

The command torque is determined through a hierarchical selection, where te PI output may be reduced by the analytical predictor, further refined the Random Forest supervisor, and the ultimately overridden by the safety state machine whenever required. This hierarchy, where safety overrides both supervisory layers and the PI controller, ensures stable operation and prevents hazardous conditions.

3.7 Simulation Scenarios

To evaluate the effectiveness of the proposed supervisory architecture, three simulation scenarios were carried out under identical operating conditions. In the first scenario, the system relied solely on the baseline PI speed controller combinde with the functonal safety state machine, representing the conventional industrial control structure without predictive capabilities. The second scenario incorporated the analytical predictive supervisor, which modified the PI torque output whenever the short term model based prediction indicated that the motor

speed might approach the SLS boundary. In the third scenario, the Random Forest based supervisort was activated, replacing the analytical prediction layer and providing a data driven torque limitation strategy trained to anticipate unsafe behaviour.
All three scenarios were executed using the same reference trajectory, mesarurement nouse characteristics and load disturbance profile to ensure a fair and cinsistent comparison. Throughtout each simulation, the system dynamisc were recorded, including the actual angular velocity, the PI and supercisory torque commands, the safety limited torque enforced by the state machine, the resulting motor current and the evolution of the safety state over time. Thes outputs collectively enable a detailed evaulation of how each supervisory method influences stability, overspeed prevention and the overall need for safety intervention.

4 Results

Four simulation scenarios were evaluated to compare the behaviour of the servo system under different supervisory strategies. All scenarios used indentical reference trajectories, distrubances and measurement noise, ensuring a strictly controlled one to one comparison. The evaluation focuses on velocity tracking, torque behaviour and the activation of safety mechanisms.

4.1 Forced Safety Activation

A dedicated validation scenario was used to verify the correctness of the safety state machine. The motor was deliberately driven beyond the SMS limit causing a deterministic transition through SLS and SS1 before reaching STO as illustrated in Figure 1. This configuration that the safety architecture behaves exactly as defined by IEC 61800-5-2 and provides a reliable final protective layer.

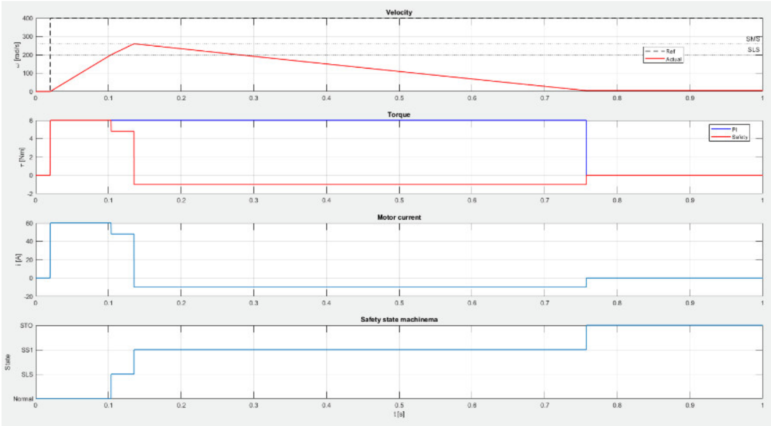

Figure 1
Safety state transitions during a forced overspeed event.

4.2 Baseline configuration

In the baseline configuration the PI controller drives the system towards the reference until the SLS threshold is approached (Figure 2.). Due to load disturbance and measurement noise, the PI output exhibits noticeable overshoot tendencies. As the motor nears the speed limit, the safety layer intervenes and limit the torque, stabilising the velocity but introducing abrupt transitions and elevated current peaks. The baseline case therefore represent safe but non optimal behaviour, dominated by reactive safety intervention.

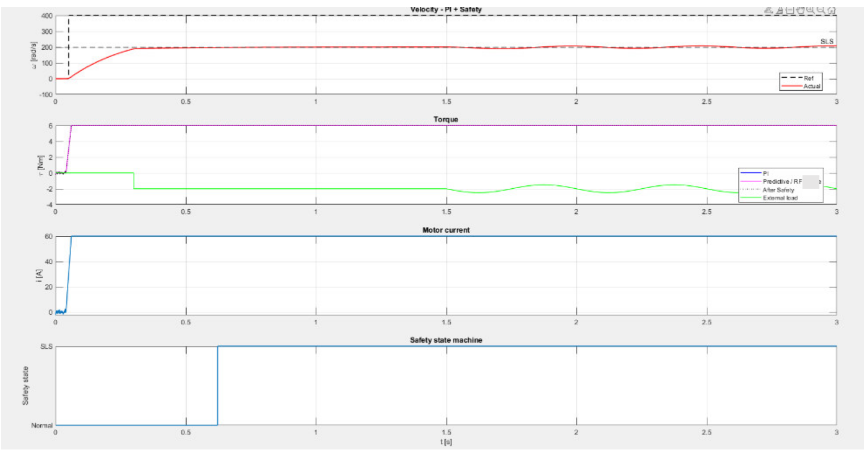

Figure 2
Baseline PI control with safety intervention (PI + Safety).

4.3 Analytical Predictive Supervisor

Introducing the analytical predictive supervisor sebstantially improves system behaviour (Figure 3.). By reducing the PI torque before the SLS boundary is reached, the predictive layer eliminates overshoot prevents safety intervention entirely. Torque and current signals become smoother, and the motor converges gradually to the desired speed. The model based supervisor thus provides a deterministic and conservative control action that efficiently mitigates overspeed tendencies under disturbance.

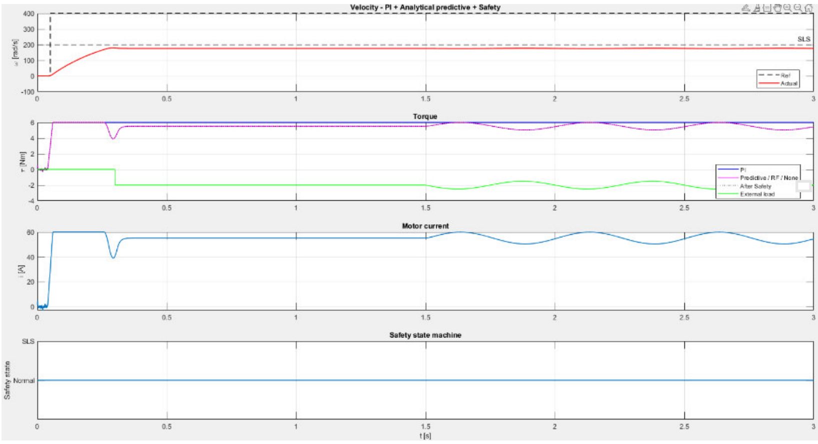

Figure 3

Servo Control with PI + Analytical predictive + Safety

4.4 Random Forest Supervisor

The RF supervisor reproduces the main effects of the analytical model despite having no explicit knowledge of the physical system (Figure 4.). It restricts torque proactively keeps velocity within safe limits and avoids activation of the safety state machine throughout the simulation. Although the RF output shows slightly higher variability, overall behaviour remains stable and safe. This confirms that a trained data driven model can serve as a lightweight surrogate for analytical prediction I real time applications.

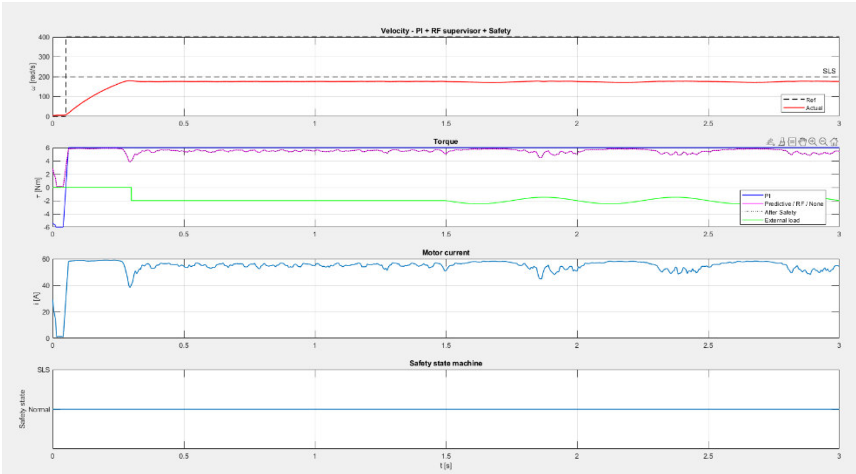

Figure 4
Servo Control with PI + RF Supervisor + Safety

5 Discussion

The simulation results demonstrate that the safety behaviour of servo motor systems can be significantly improved by incorporating supervisory layers above the conventional PI controller. The baseline PI + Safety configuration showed that the drive frequently approached the SLS boundary and required direct safety level torque clipping, indicating limited disturbance robustness. When the analytical predictive supervisor was applied, the system maintained smooth velocity tracking and stable torque behaviour even under varying load safety intervention was no longer required, confirming the effectiveness of model based proactive limitation. The Random Forest supervisor reproduced the analytical behaviour with only minor variability, despite having no explicit knowledge of the motor model. This confirms that data driven methods can internalise safety aware response patterns when trained with sufficiently rich synthetic data. Importantly, the RF based controller also prevented overspeed and maintained torque within safe limits, keeping the safety stat machine in its Normal state throuhout the run. The dedicated fault injection scenario further validated the correctness of the safety architecture, as the system transitioned deterministically through SLS and SS1 to STO, exactly defined by IEC 61800-5-2.
Overall, the results show that predictive and data driven supervisors can significantly reduce the reliance on safety level intervention and contribute to to smoother torque behaviour, while fully preserving the functional safety guarantees of the underlying safety layer.

6 Conslusion

This study introduced a multi layered safety oriented control architecture for servo motor systems, combining classical PI control, an analytical predictive supervisor, a machine learning based Random Forest supervisor and an IEC compliant safety state machine. The proposed framework successfully prevented overspeed, reduced torque peaks under load disturbances and ensured that the safety layer intervened only when strictly necessary. The data driven supervisor achieved performance close to the analytical method demonstrating that machine learning models can effectively replicate safety aware control behaviour without explicit system knowledge.
The architecture provides a practical pathway for integrating predictive and AI based techniques into into industrial servo drives while maintaining strict funcitonal safety requirements. Future work will focus on hardware in the loop validation, the integration of encoder level diagnostics and the extension of the machine learning model toward anomaly detection and predictive maintenance.

References

[1] Z. Dong, S. Chen, Z. Sun, B. Tang, and W. Wang, "A servo control algorithm based on explicit MPC and extended state observer," Actuators, vol. 14, no. 6, p. 281, 2025.
[2] F. Kraus and M. Yazdi, "Functional safety and condition monitoring in drive systems," IEEE Industrial Electronics Magazine, vol. 15, no. 3, pp. 18–30, 2021.
[3] M. Jafari and A. Nouri, "Dynamic modelling and hazard analysis of servo motor failures," ISA Transactions, vol. 132, pp. 44–58, 2023.
[4] H. Liu, X. Zhang, and P. Li, "Analysis of torque ripple, vibration and resonance in servo drive applications," Mechanical Systems and Signal Processing, vol. 201, p. 110480, 2023.
[5] K. Shibata, A. Yamazaki, and T. Sato, "Vibration propagation and mechanical hazard risk assessment in servo-driven axes," Precision Engineering, vol. 84, pp. 262–272, 2024.
[6] IEC 61800-5-2:2016, Adjustable speed electrical power drive systems Safety requirements Functional, IEC, 2016.
[7] IEC 61508, Functional safety of electrical/electronic/programmable systems, Parts 1–7, IEC, 2010.
[8] ISO 13849-1:2015, Safety of machinery – Safety-related parts of control systems, ISO, 2015.
[9] IEC 62061:2021, Safety of machinery – Functional safety of control systems, IEC, 2021.
[10] J. O. Krah and J. Holtz, "Safety-related architecture and redundancy concepts for low-cost drives," in Proc. SGRE Conf., 2024
[11] N. Brubaker et al., "INCONTROLLER: State-sponsored attack tools targeting industrial control systems," Google Mandiant, Threat Report, 2022.
[12] CISA, "ICSA-23-075-02: Siemens SINAMICS Drive vulnerabilities," U.S.

Dept. of Homeland Security, 2023.
[13] S. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security: A survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.
[14] N. Navet and H. Song, "Distributed safety monitoring for networked servo control systems," in Proc. IFAC World Congress, 2020.
[15] Rockwell Automation, Kinetix 5700: Safe Speed Monitoring, Publication MOTION-AT005A-EN-P, 2018.
[16] Siemens AG, SINAMICS S120 Safety Integrated Function Manual, 2017.
[17] Beckhoff Automation, TwinSAFE: Safety Technology Documentation, 2022.
[18] ISO 10218-1:2025, Robots and robotic devices Safety requirements for industrial robots ISO, 2025.
[19] MathWorks, *Developing Safe Industrial Equipment Using Simulation*, Webinar, 2025.
[20] H. Kato and T. Fujii, "Hardware-in-the-loop fault injection for servo drive safety validation," *Control Engineering Practice*, vol. 141, p. 105768, 2025.