


Article

Cybersecurity Requirements for Industrial Machine Control Systems

Leszek Kasprzyczak ¹, Anna Manowska ^{1,*}  and Marek Dźwiarek ²

¹ Faculty of Mining, Safety Engineering and Industrial Automation, Silesian University of Technology, 44-100 Gliwice, Poland; leszek.kasprzyczak@polsl.pl

² Central Institute for Labour Protection—National Research Institute, 00-701 Warszawa, Poland; madzw@poczta.onet.pl

* Correspondence: anna.manowska@polsl.pl

Abstract: The first part of this paper discusses the research context, taking a closer look at the development of Industry 4.0 and the growing importance of the IIoT, which entails new cybersecurity challenges. The issue of cyber threats and the need to increase the level of protection in machine control systems, which are particularly vulnerable to attacks due to their connection to the network, is also presented. The Introduction concludes with a presentation of the article's objective, which is to analyze the requirements of security levels (SLs) and the implementation of relevant international standards. The next section reviews the current research on cybersecurity in machine control systems. This section also points out the research gaps that the article aims to fill. The next section presents the risk assessment used to ensure safety during machine operations based on ISO 12100. The article describes safety functions implemented in machine control systems, including the SIL (safety integrity level) and PL (performance level) specifications. An important part of the article is the creation of a relationship between PL and SL, showing how the safety functions of systems are related to protection against cyber threats. The last part of the article gives a case study in the form of examples of machines and their control systems performing safety functions, which require various SLs depending on the PLs.

Keywords: cybersecurity; machinery control systems; performance levels; PLs; security levels; SLs



check for updates

Academic Editors: Fabrizio Marozzo and Cristina Stolojescu-Crisan

Received: 24 December 2024

Revised: 23 January 2025

Accepted: 24 January 2025

Published: 26 January 2025

Citation: Kasprzyczak, L.; Manowska, A.; Dźwiarek, M. Cybersecurity Requirements for Industrial Machine Control Systems. *Appl. Sci.* **2025**, *15*, 1267. <https://doi.org/10.3390/app15031267>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The effective cybersecurity of industrial systems requires the cooperation of both manufacturers and machine users. Remote access and password monitoring should not be a coincidence, as negligence can result in the appearance of cyber-attacks, for example, by former employees on both the manufacturer's and user's side, as well as other external parties.

Cyber-attacks are primarily associated with attacks via the Internet; however, one should also take into account the unintentional infection of the system by connecting a virus-ridden data carrier, such as a portable memory stick, or deliberate sabotage associated with unrestricted access by an internal company employee to programmable devices on production lines.

Cyber-attacks can cause, among other things, the following:

- Halting production or reducing production;
- Loss of quality of manufactured workpieces, which may not be easy to detect quickly and exposes the company to financial losses;

- Loss of data—encryption by blackmailers demanding ransom;
- Falsification of documentation and the introduction of chaos in various departments of the company;
- Emission of hazardous substances into the environment—contamination of the environment and danger to local residents or the wider area;
- Loss of safety functions in machine control systems, which can directly expose employees to mechanical hazards, hazards associated with the emission of hazardous substances, and many others.

It is therefore important to implement appropriate protections in terms of cybersecurity with expenditures commensurate with the potential consequences caused by cybercrime. A company should have a policy in place related to cybersecurity, which should be constantly improved due to the fact that cyber criminals are constantly looking for opportunities to attack through the vulnerabilities they discover.

Policies related to cybersecurity should address, among other things, the management of passwords for programmable devices, such as the following:

- Rules for creating passwords for newly acquired PLCs/microcontrollers/machine computers;
- How often they should be changed (e.g., due to employee turnover);
- Where they should be stored (on the local computer's disc/on the network on a server, whether in encrypted form; consider that such a computer can also be attacked, resulting in the loss of stored passwords; another solution is to store passwords written on paper);
- Who should have access to stored passwords;
- Rules for supervising compliance with the policy (checking that passwords are not written, for example, with a marker on the controller or on the door of the control cabinet or on electrical diagrams, etc.).

It is also important to deliberately assign permissions and formulate requirements for remote machine operation as follows:

- Encrypted connections required;
- Access only within a certain pool of IP addresses;
- Degree of password complexity;
- Temporary access rather than unlimited time;
- Read-only connection, if sufficient;
- Generation of a post-intervention checksum;
- Recording the date, time, and personal data of the modifier.

Experience shows that as programmable devices are used, vulnerabilities in their software become apparent. This therefore requires the constant monitoring of software updates. This issue is often neglected, giving cyber criminals more freedom of action.

The purpose of this study is to analyze cybersecurity requirements for industrial machine control systems, focusing on their integration with safety levels (SLs) and performance levels (PLs). The study aims to fill the gap in the literature by providing a comprehensive framework for linking safety and security requirements in industrial systems, addressing both hardware and network-level vulnerabilities. The remainder of this article will mainly analyze the aspect concerning the loss of safety functions (SFs) in machine control systems due to a cyber-attack, which can result in hazards to employees. Hazards can result in slight or severe injuries and even the death of a single person caused by a machine. The article does not consider catastrophes (the death of many people as a result of a danger event).

2. Analysis of Cyber Threats in the Industry

With the increasing digitization of industrial processes and the development of IoT and IIoT technologies, the cybersecurity of machine and production line control systems has become a key issue in securing critical infrastructure and industrial automation. Research in this field focuses on analyzing and optimizing measures to protect against cyber-attacks and implementing effective strategies to safeguard against security breaches in control systems. The sources of cyberattacks can be divided into two groups, namely external threats and internal threats. External threats often include cybercriminal organizations or independent hackers who use tools such as phishing, ransomware, and denial-of-service attacks to exploit system vulnerabilities. Internal threats, on the other hand, can result from malicious or negligent actions by employees or others with access to the network [1]. Identifying these sources is crucial to implementing tailored security measures.

Tanveer et al. in [2] describe methods for designing industrial automation applications that are secure against attacks while ensuring the high availability of systems. This work is a key contribution to the issue of security integration in IoT/IIoT applications. Lesi et al. in [3] analyze the issue of distributed security in industrial automation, specifically focusing on IoT vulnerabilities and threats that require multi-layer security in high-risk environments.

Duque Anton et al. in [4] conduct an extensive analysis of the vulnerability of control systems to cyber threats around the world. The findings reveal significant security vulnerabilities that can pose a direct danger to the safety of operators. On the other hand, Buczkowski et al. in [5] introduce the CySec-Tool, which allows for security optimization based on probabilistic attack models. Analysis based on the attack model enables the identification of vulnerabilities in automation and control systems.

Boyes in [6] emphasizes the importance of applying protection standards for industrial networks and the control of industrial systems. This research takes into account the specific principles of designing systems that are resilient to cyber-attacks, which is crucial for managing risk in industrial networks.

An important aspect in cybersecurity research for automation systems is the topic of detecting and defending against malicious activities. A hierarchical approach to managing system complexity and security was discussed by Mesarovic (1970), providing foundational insights into multi-level control systems [7]. Liu et al. in [8] describe scenarios of attacks based on data falsification in power grids, which indicates the need for advanced methods to detect integrity violations. Slay and Miller in [9] detail an incident involving an attack on a water management system, which provides an important case study of the consequences of a lack of cybersecurity in critical infrastructure.

In the context of security certification and compliance assurance, the work of Chen et al. [10] and Gajek et al. [11] take a closer look at the topic of so-called property-based attestation and the TLS (transport layer security) model. These studies bring important aspects to the development of secure communication protocols and protection against attacks.

In the area of key exchange and encryption, the work of Manowska et al. [12] points to new methods of defending against key compromise in key exchange protocols, which provides the foundation for protecting against unauthorized access to machine control systems.

The topic of privacy and security in control systems was addressed by Cutillo et al. in [13]. Their research includes mechanisms for discovering common contacts and protecting user privacy, which can be applied in the context of the remote monitoring of industrial systems.

The article [14] addresses current problems of risk analysis and probabilistic modelling for functional safety management in the life cycle of safety-related systems. Some methodological aspects of the functional safety assessment are outlined that include the

modelling of dependent failures or cybersecurity and verifying the safety integrity level (SIL) under uncertainty.

In the article [15], the author identifies typical mistakes of machinery safety-related control systems and mentions the cybersecurity requirements that will be imposed by Machinery Regulation 2023/1230/EU [16] in 2027.

All of the above work underscores the growing need to implement protective measures against cyber threats, but there remains a research gap in the integration of IEC 62443 group of standards on the security for industrial automation and control systems with the safety levels of machine control systems' safety functions. In particular, there is a lack of unambiguous cybersecurity guidelines for machine safety systems within Industry 4.0. This article fills these gaps by proposing the implementation of security standards for machine control systems, taking into account security levels (SLs) and their relationship to the safety functions implemented by machine control systems, providing greater protection against unwanted incidents and increasing the resilience of industrial infrastructure against cyber-attacks.

3. Machine Safety Requirements

3.1. Risk Assessment and Reduction

According to ISO 12100 [17], a risk assessment should be performed as early as at the machine design stage. The risk assessment consists of risk analysis and risk evaluation. The risk analysis consists of the three following steps:

- Defining machine limitations;
- Identifying hazards (e.g., mechanical, electrical, security threats);
- Risk estimation.

For each individual hazard, a risk estimation is performed, which can take several levels, from negligible through low, medium, significant, or high. The higher the risk, the more severe the injury possibly is and/or there is a higher probability of a hazardous event. Thus, the higher the risk, the more reliable and therefore expensive measures must be taken to minimize the risk to an acceptable level.

Also, the Machinery Regulation 2023/1230/EU [16], which will take effect in 2027, requires the use of protections against intrusion with particular attention to the safety functions performed by machine control systems. In the Annex III on Essential Health and Safety Requirements, Section 1.1.9 requires a machine or related product to record the evidence of authorized or unauthorized tampering with respect to that component of hardware when it relates to connecting to or accessing software that is essential to the machine's or related product's compliance.

Thus, depending on the estimated risk that may arise from cyber threats, appropriate measures should be adopted to reduce the risk from that hazard. To estimate the risk from cyber threats, we will use the proposed relationship between PLs and SLs in the next chapters.

3.2. Safety Functions

Risks from certain hazards are minimized with safety-related control systems. A given control system can then implement a single or multiple safety functions.

The requirement specification for safety functions consists of functional requirements and safety integrity. Functional requirements are most often specified as a formulation, such as "Stop the dangerous movement of the machine when the interlocking guard is opened and prevent it from starting until the guard is closed".

The ranking of system state parameters is based on their relative impact on the overall safety and security of the system. Parameters were evaluated using a weighted scoring

system, considering criteria such as the frequency of occurrence, severity of potential consequences, and the likelihood of detection. The methodology follows established risk assessment frameworks, including ISO 12100 and ISO 13849-1 [18], which recommend prioritizing parameters based on their contribution to system vulnerability and resilience. This approach ensures that critical parameters are given higher weight in the analysis, reflecting their importance in mitigating cyber and operational risks.

Typically, the safety function is realized with three elements, a sensor that detects the hazard (opening the guard), a logic unit that processes the signals from the sensor, and an actuator connected to the logic unit (e.g., a contactor that shuts down the drive under consideration or a valve that shuts off the operating medium). These elements form an SCS (safety-related control system) according to IEC 62061 [19] or SRP/CS (safety-related part of a control system) according to ISO 13849-1. Due to the greater popularity of ISO 13849 in the industry, we will focus on its requirements in the remainder of this article.

3.2.1. Determination of the Required Level of Safety Integrity

To determine the required performance level (PLr) of a given safety function implemented in the control system, the graph in Figure 1 can be used based on Annex A of ISO 13849-1 [18].

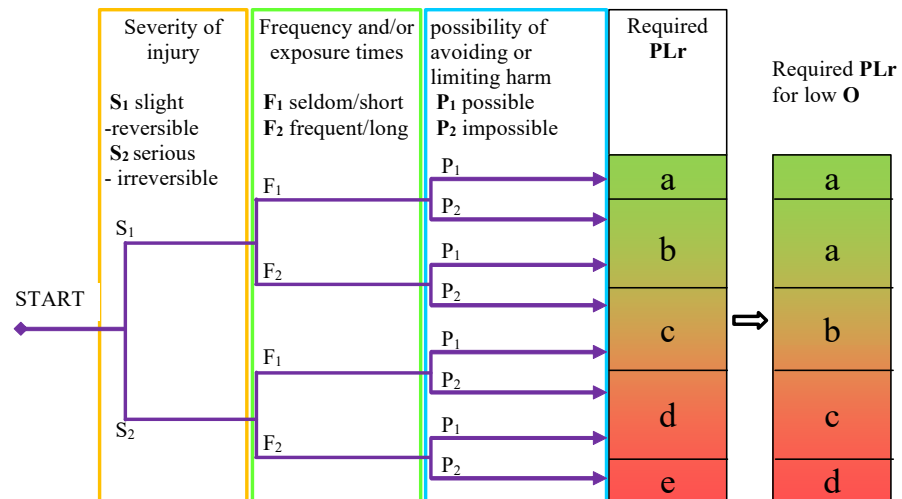


Figure 1. Graph for determining the PLr (own elaboration).

In the graph, path choices are made consisting of the following:

- The severity of the injury (S);
- The frequency of exposure and/or its duration (F);
- The possibility of avoiding or limiting harm (P).

The standard allows for a reduction in one level in the required PLr if the low probability of a hazardous occurrence (O) can be justified.

3.2.2. Achieved PLs and SILs

A given safety function is implemented from safety-related hardware and software elements. The individual subsystems are characterized by the safety parameters required by ISO 13849-1 and/or IEC 62061. On the basis of appropriate formulas or simplified methods, the frequency of dangerous failure per hour PFH_d of the entire safety chain must be determined and on this basis, the achieved PL and/or SIL of the safety function under consideration is obtained—see Table 1. It can be seen from this table that the higher the SIL/PL, the lower the frequency of dangerous failure per hour of the system implementing the safety function in question. In addition, the more elements there are in the safety chain,

the greater the sum of their PFH_d will be and therefore, the resulting SIL/PL will be lower, which may result in failure to achieve the target integrity.

Table 1. Determination of SILs and PLs of the system based on PFH_d .

PFHd	SIL	PL
$\geq 10^{-5}$ to $< 10^{-4}$	-	a
$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1	b
$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1	c
$\geq 10^{-7}$ to $< 10^{-6}$	2	d
$\geq 10^{-8}$ to $< 10^{-7}$	3	e

In case the PL is not known for all subsystems, it is necessary to determine the performance level of such subsystems by itself. The determination of the performance level, PL, for the subsystem is determined based off the following:

- The architecture of the system (categories B, 1, 2, 3, 4);
- The value of the mean time to dangerous failure ($MTTF_d$);
- Diagnostic coverage (DC);
- Common cause failure tolerance (CCF).

We will not discuss all the factors mentioned here, and we refer the interested reader to the analysis of the standard [18] or the publication [20]. In the following, we will focus on explaining the categories of systems related to system architecture, as they are an important part in the subsequent analysis.

3.2.3. System Architecture—Categories

According to [16], there are five safety categories, which are B, 1, 2, 3, and 4. Single-channel systems include categories B, 1, and 2. They differ from each other in that category 1 uses well-tried components (e.g., parts used in the past in similar applications with positive results) and well-tried safety principles (e.g., oversized components), so the probability of failure is lower than in the “weakest” category B. Category 2 additionally includes fault detection in subsystems. Categories 3 and 4 apply to two-channel systems (Figures 2–5). Table 2 compares the different categories.



Figure 2. Architecture of the single-channel systems for categories B and 1 (own elaboration).

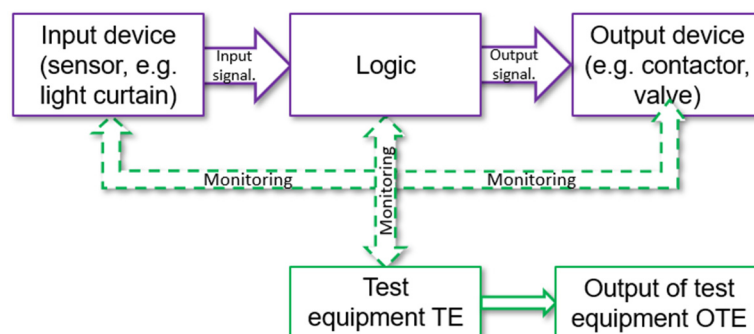


Figure 3. Architecture of systems with monitoring equipment for category 2 (own elaboration).

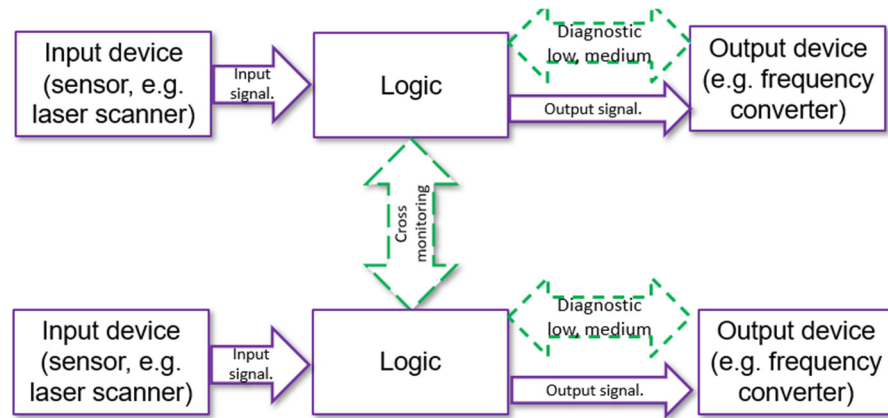


Figure 4. Architecture of redundant systems for category 3 (own elaboration).

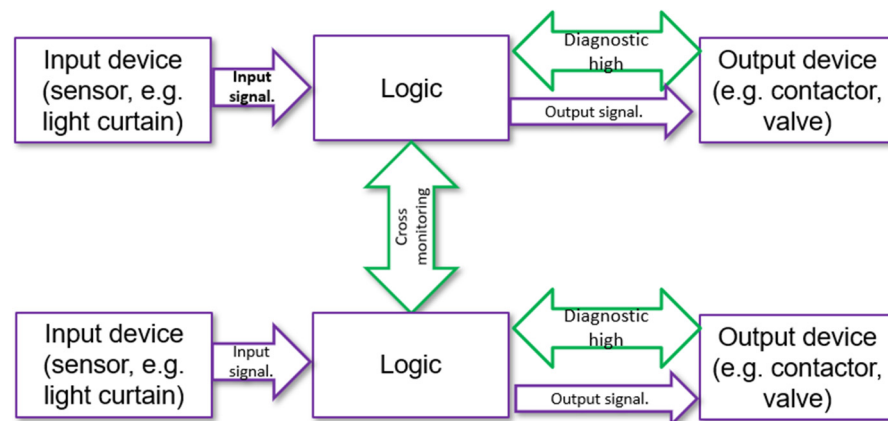


Figure 5. Architecture of redundant systems with the highest diagnostic coverage for category 4 (own elaboration).

Table 2. Comparison of safety categories based on ISO 13849-1.

Category	Features	
B	Use of elements that comply with standards and basic safety principles, withstanding expected exposures. Occurrence of failure may result in loss of safety function (single-channel system)	<div style="display: flex; flex-direction: column; align-items: center; justify-content: center;"> <div style="writing-mode: vertical-rl; transform: rotate(180deg);">well-tried safety principles</div> <div style="writing-mode: vertical-rl; transform: rotate(180deg);">Failures detection</div> <div style="writing-mode: vertical-rl; transform: rotate(180deg);">Redundancy</div> </div>
1	As in B, well-tried components and well-tried safety principles are used. The occurrence of a failure may cause a loss of safety function, but the probability of this is lower than in category B (single-channel system)	
2	As in B, well-tried safety principles are used. The safety function is checked by the control system. The occurrence of a fault may cause the loss of the safety function between checks (single-channel system)	
3	As in B, well-tried safety principles are applied. The two-channel structure is tolerant to a single fault. Low-to-medium diagnostic coverage of 60 to 99%	
4	As in B, well-tried safety principles are applied. The two-channel structure is tolerant of single failure or cumulative failures. High diagnostic coverage $\geq 99\%$	

4. Relationship Between Safety Categories and PLs and Security Levels

As mentioned in the Introduction, one of the potential targets of cyber criminals can become the machine’s safety systems. A real danger then arises for an operator and maintenance service if they undertake work in machine zones that pose a risk, which should be protected by the control system (e.g., ensuring low speeds to avoid danger;

stopping when a light curtain zone is violated; controlling process parameters such as temperature or liquid level). It is therefore important to link safety-related machine control system requirements with cybersecurity requirements.

However, the stability and cybersecurity of the entire hierarchical infrastructure, which includes interconnected hardware, software, and network components, also plays a crucial role. This hierarchy often comprises multiple layers, from local control systems to enterprise-level networks and cloud-based solutions. Each layer introduces specific vulnerabilities and requires tailored security measures. For example, while the network layer may be prone to denial-of-service attacks, the application layer could be susceptible to data breaches. Analyzing the interdependencies and failure propagation within this hierarchy is essential to ensure not only the safety of individual machines but also the resilience of the entire infrastructure. Future studies should incorporate multi-layered risk assessment frameworks, such as those outlined in IEC 62443 group of standards and ISO/IEC 27001 [21], to address these challenges.

The technical specification IEC TS 62443-1-1 [22] Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models recommends at least three SLs (Security Levels 1, 2, 3)—Table 3—while IEC 62443-4-2:2019 [23] Security for industrial automation and control systems—Part 4-2: Technical security requirements for IACS components (industrial automation and control system(s)) gives four SLs (Security Levels 1, 2, 3, 4).

Table 3. Security levels according to IEC TS 62433-1-1 [22].

SL	Qualitative Description
1	Low
2	Medium
3	High

Informative Annex A of IEC 62443-3-2 [24] states that IEC 62443-4-2 [23] defines SLs at four different levels (1, 2, 3, and 4). The higher the SL, the greater the level of security. SL 0 indicates that there are no requirements in this area.

- SL 1—protection against casual or coincidental violation.
- SL 2—protection against intentional violation using simple means with low resources, generic skills, and low motivation.
- SL 3—protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.
- SL 4—protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation.

We are considering three levels of machine security because SL4 takes into account sophisticated measures with expanded resources and high motivation, which can be undertaken mainly by highly skilled and equipped special forces teams that are not considered to be involved in attacking industrial machines. SL4 can be considered in the protection of power plants, nuclear power plants, and chemical plants, which if attacked can cause catastrophes.

Moreover, three types of SLs are specified as follows:

- Target, SL-T (required);
- Capability, SL-C;
- Achieved, SL-A.

Type SL-T defines the required effectiveness of countermeasures, devices, and systems that should be implemented to prevent cyber-attacks.

Type SL-A is the actual SL achieved by the actual system. The achieved SL-A level should be greater than or equal to the required SL-T level.

Type SL-C means that the device in question has the ability to provide a given SL when properly configured and integrated.

There is a need to establish a direct relationship between the PL safety level according to ISO 13849-1 and the SL according to IEC TS 62443-1-1 [22]. It can be deduced that the higher the PL is, the higher the risk is reduced by the safety-related control system; therefore, the higher the PL is, the higher the SL should be against cyber-attacks so that the considered safety function is not lost.

The relationship between PL/category and SL can be determined from Figures 6 and 7. Cybersecurity in a four-level system must encompass a wide range of tasks to ensure comprehensive protection and operational efficiency. This includes the following:

- Developing a clear understanding of the system's architecture, vulnerabilities, and potential attack vectors across all levels, from local devices to cloud-based services.
- Implementing synchronized protocols for real-time threat detection and response. This ensures that actions taken at one level (e.g., local control) align with strategies at higher levels (e.g., enterprise management).
- Securing both the physical and virtual components of the system. This includes robust firewalls, encryption methods, and redundancy measures to prevent unauthorized access and ensure data integrity in the network of data exchange.
- Recognizing the human factor in system security, such as errors in judgement, fatigue, or lack of training and mitigating these risks through regular training programmes, ergonomic interfaces, and automated alerts to support decision-making processes.

A fully integrated approach, leveraging group of standards such as IEC 62443 and ISO 27001 [21], is essential to address these diverse tasks. Additionally, advanced tools like AI-driven anomaly detection can enhance the system's ability to identify and counteract threats dynamically.

It is important to note that the analysis presented in this article focuses on specific aspects of cybersecurity, particularly on protection mechanisms at the lower levels of the hierarchy, such as machine control systems and local networks. However, protection at the bottom of the hierarchy does not ensure the cybersecurity of the entire system. A comprehensive approach requires addressing vulnerabilities across all layers, from local control systems to enterprise-level networks and cloud infrastructure. Future research should expand on this work by analyzing the interdependencies and security strategies necessary for ensuring system-wide resilience.

With the assumption that machine control systems are connected to the communications network and may be vulnerable to cyber-attacks, the following guidelines were proposed for the PLr column with the parameter $O = 100\%$ (O —the probability of occurrence of a hazardous event):

Category B

Category B allows us to obtain safety levels PLa or PLb. An SF with PLa/b level reduces the risk with a low level (S1, F1, P1/P2; S1, F2, P1).

Category B can be realized as a one-channel electromechanical or programmable system, for example, based on a standard PLC.

In the case of a system built based on electromechanical parts, there is no possibility of a cyber-attack, so SL-T 0 (no protection) is assumed.

In the case of a system built based on programmable components (e.g., a standard PLC), there is a possibility of a cyber-attack, but the risk minimized by the function is low (at the PLa/b level), so SL-T 1 (low level) is assumed.

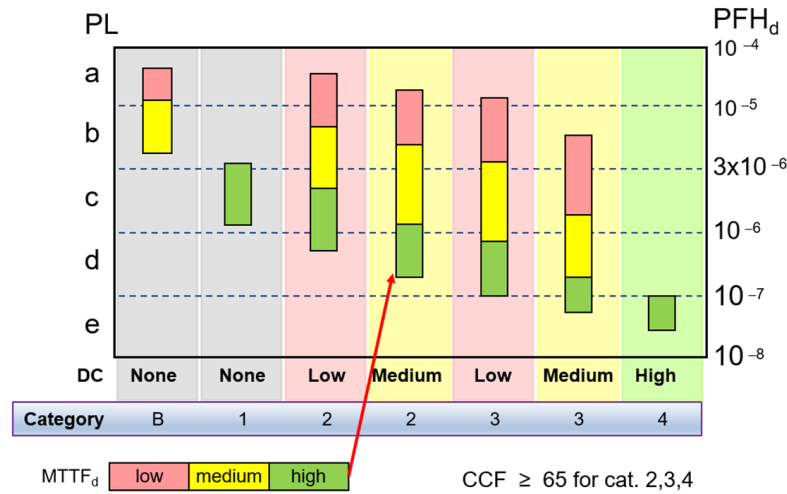


Figure 6. Auxiliary graph for determining the relationship between PL/Cat and SL—determination of the achieved PL, among others, using categories (own elaboration).

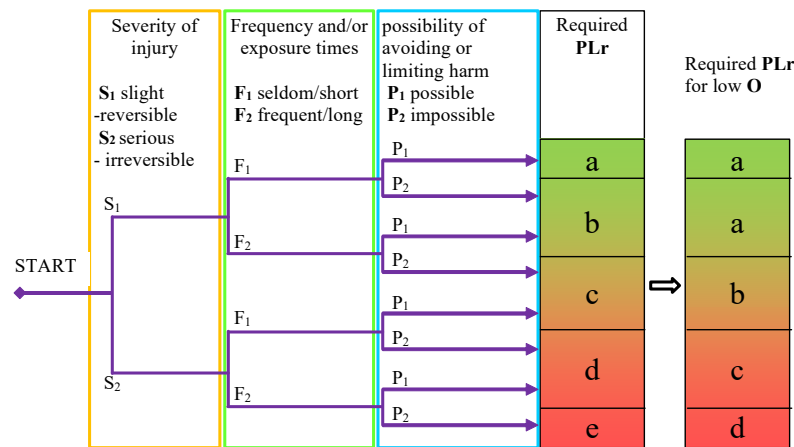


Figure 7. Auxiliary graph for determining the relationship between PL/Cat and SL—parameters S, F, and P for determining the PLr (own elaboration).

Category 1

Category 1 achieves safety levels of PLb or PLc and is mainly applied at the PLc level. An SF with PLc level reduces the risk with a medium level (S1, F2, P2; S2, F1, P1).

Category 1 is implemented as a one-channel system based on well-tried components, which according to ISO 13849-2 [25] includes electromechanical parts. Programmable electronic circuits are not used, as they are not classified as well-tried ones.

In the case of a system built based on well-tried components (electromechanical components), there is no possibility of a cyber-attack, so SL-T 0 (no protection) is assumed.

Category 2

Category 2 achieves safety levels from PLa to PLd, with the most common use for the PLc level, and usage is less common for PLd level. An SF with a PLc level reduces risk with a medium level (S1, F2, P2; S2, F1, P1), while one with a PLd level reduces risk with a higher level (S2, F1, P2; S2, F2, P1).

Category 2 is implemented as a one-channel electronic system with monitoring, so there may be a loss of an SF between testing and the result of not detecting all faults. Category 2 is typically used for safety systems containing a type 2 light curtain according to IEC 61496-1 [26], which is tested by a programmable module.

In the case of a system built with programmable elements, there is the possibility of a cyber-attack. When the minimized risk is low, which corresponds to PLa/b, then SL-T 1

(low level) is assumed. When the minimized risk is medium (at PLc level) and high (at PLd level), SL-T 2 (medium level) and SL-T 3 (high level) are used, respectively.

Category 3

Category 3 allows for safety levels from PLa to PLe, with the most common use for the PLd level. An SF with a PLd level reduces risk with a high level (S2, F1, P2; S2, F2, P1).

Category 3 is implemented as a redundant two-channel system with low- or medium-level diagnostics, so there may be a loss of SF as a result of not detecting all faults. Category 3 is often implemented from two different channels, namely programmable (stopping machine actuators) and electromechanical (cutting off electrical/pneumatic/hydraulic power). However, its typical application is also inverter drives with an STO (safe torque off—see ISO 13850 [27]) stop function, characterized by PLd and category 3.

For systems realizing PLb/c levels and built on the basis of one programmable channel and another electromechanical channel, SL-T 2 (medium level) is adopted. For high-risk minimization (at PLd level), SL-T 3 (high level) is adopted.

Category 4

Category 4 allows for PLe levels of safety. An SF with a PLe level reduces the risk with the highest level (S2, F2, P2).

Category 4 is implemented as a two-channel system with high-level fault detection diagnostics. High diagnostics are provided by programmable electronic systems.

In the case of a system built with programmable components, there is the possibility of a cyber-attack. In this case, the highest risk (at PLe level) is minimized, so SL-T 3 (high level) is adopted.

In the case of using the PLr column with the parameter $O \ll 100\%$, it is possible to mitigate the security protection requirements with the reasoning outlined above.

5. Case Study—Examples of Determining SLs of Safety Functions Implemented in Machine Safety Systems

In the next section of the paper, examples of machines equipped with safety-related control systems performing specific safety categories according to ISO 13849 are presented. This assumes that control systems containing programmable devices may be connected to a communication network and therefore may be susceptible to cyber-attacks.

5.1. Example 1—Machine Control System: Category B, PLa; Cybersecurity SL-T 0

In many industrial sectors, tank or barrel mixers are used. Such a mixer performs a slow rotary motion, which implies that the hazard can be avoided (parameter P1). No crush and shear zone is created inside a tank of its size. Thus, the potential injury may be light (parameter S1), for example, a bump, abrasion, or cut. The user on average opens the machine several times a day (parameter F1). Taking into account the aforementioned characteristics, the required level is $PLr = a$.

The safety system is realized with standard parts (not necessarily well tried and tested; see the proximity sensor B1 performing the locking function—Figure 8). Programmable devices and coupling to a communication network are not present.

For a circuit implementing the interlocking function shown in Figure 8, under the assumptions described above, no protection against cyber-attack is required. Thus, SL-T 0 (no protection) is assumed.

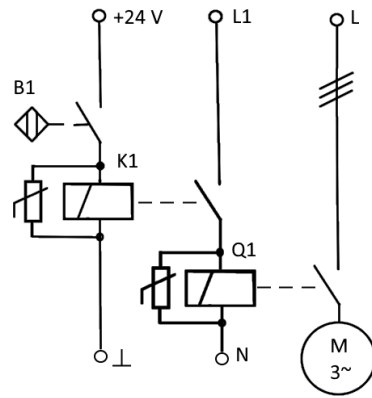


Figure 8. Example of a mixer control system to achieve PLa (own elaboration).

5.2. Example 2—Machine Control System: Category B, PLb; Cybersecurity SL-T 1

Let us consider a bakery machine for kneading dough. Such a machine performs slow rotations (which implies that a hazard can be avoided (parameter P1)) inside a container with smooth walls and dimensions that prevent the formation of crush and shear zones. Thus, it is assumed that potential injuries may be light (parameter S1), such as abrasion. The user has frequent contact with the machine (dough loading/unloading, cleaning) about 20% of the time during the shift (parameter F2). Taking into account the aforementioned characteristics, PLr = b is required.

The safety system is implemented with standard components (not necessarily well tried; see the NO limit switch acting as an interlock and the standard PLC—Figure 9). Basic safety principles are met, i.e., the use of a suppressor on the contactor coil. The machine is equipped with a programmable system that can be coupled to a communication network.

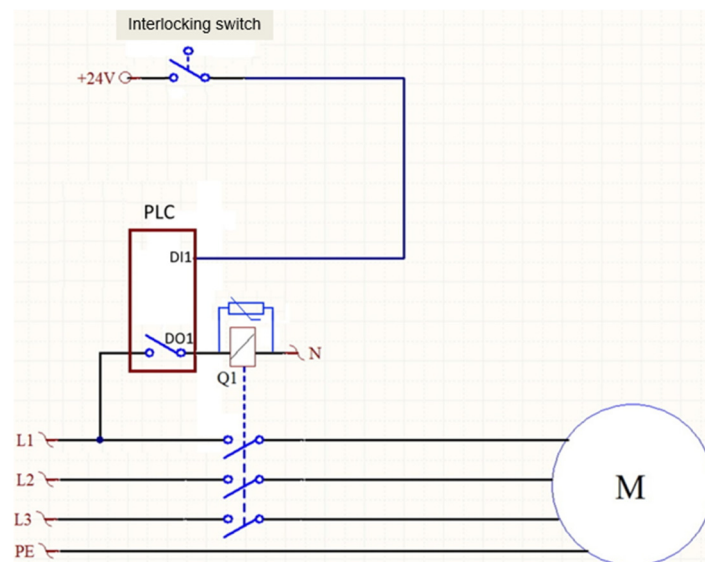


Figure 9. Example of a mixer control system to achieve PLb level (own elaboration).

For the circuit implementing the presented interlocking function in Figure 9 with the assumptions described above, protection against cyber-attack is required. The required protection level is assumed to be SL-T 1 (low level).

5.3. Example 3—Machine Control System: Category 1, PLc; Cybersecurity SL-T 0

Let us consider an SF implementing an emergency stop function, such as a turning machine (conventional lathe). According to ISO 13850 [27], the emergency stop function

(E-Stop) is required to meet at least PLc/Cat. 1. According to ISO 13849-1 [18], category 1 implies the use of well-tried components and well-tried safety principles. According to ISO 13849-2 [25], electromechanical components with a positive opening are considered as well-tried components (see the E-Stop button in Figure 10—the arrow symbol in a circle indicates positive opening). The standard in question also gives a list of well-tried safety principles, including oversizing the contactor's switching current, separating functional circuits from safety circuits. Figure 10 shows separate circuits for the starting and operational stopping of a machine and a separate circuit for the emergency stop. The drawing was simplified by omitting basic safety principles (e.g., the use of surge suppressors on inductive components). The circuit implementing the considered SF does not contain programmable circuits and coupling to the communication network.

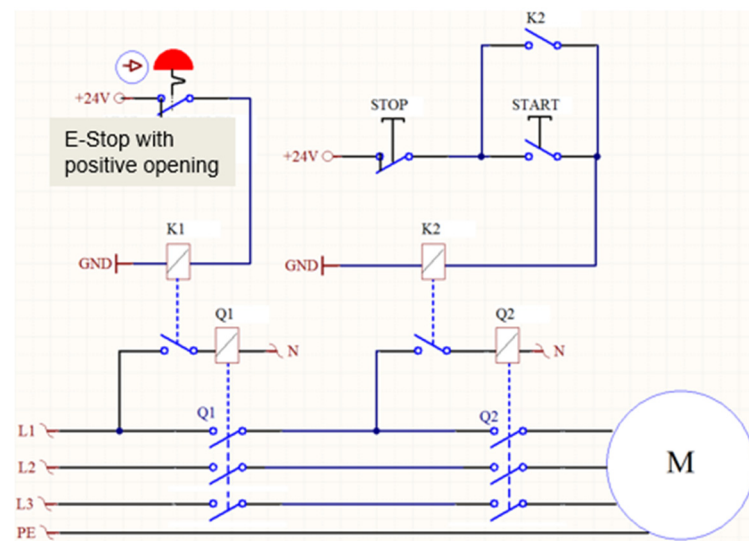


Figure 10. Example of circuits implementing the process operations of the machine and the safety system responsible for the emergency stop to ensure that the PLc level is achieved (own elaboration).

For the circuit implementing the emergency stop function shown in Figure 10, with the assumptions described above, no protection against cyber-attack is required. Thus, SL-T 0 (no protection) is assumed.

5.4. Example 4—Machine Control System: Category 2, PLc; Cybersecurity SL-T 2

Figure 11 shows a turntable protected by a type 2 light curtain according to IEC 61496-1 [26]. The machine makes slow rotary movements (which implies that the danger can be avoided (parameter P1)). The rotary movements create shear points, with the implication that potential injuries could be severe (parameter S2). The user enters the danger zone several times per shift. This implies the F1 parameter is used. Taking into account the aforementioned characteristics, $PLr = c$ is required.

The light curtain is connected to a programmable safety unit (Figure 12) and is cyclically tested by it. However, not all faults can be detected. Therefore, the highest diagnostic DC cannot be achieved. The auxiliary contactor Q1 is included in the feedback loop. The main and auxiliary contacts of the contactor are mechanically connected. When a fault occurs and is detected, the programmable safety relay is able to indicate the fault with a red lamp.

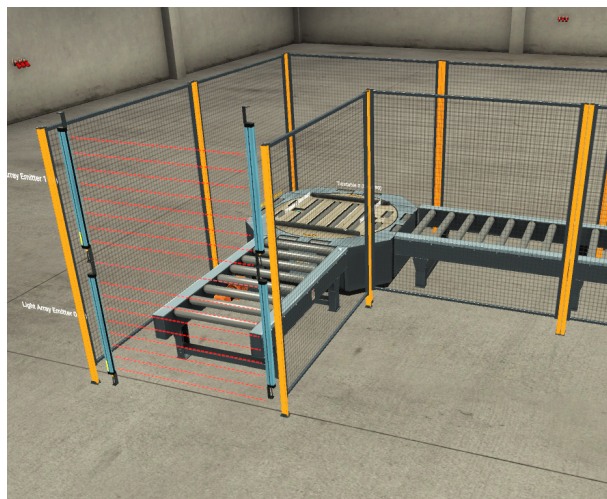


Figure 11. Turntable danger zone protected by type 2 light curtain (own elaboration).

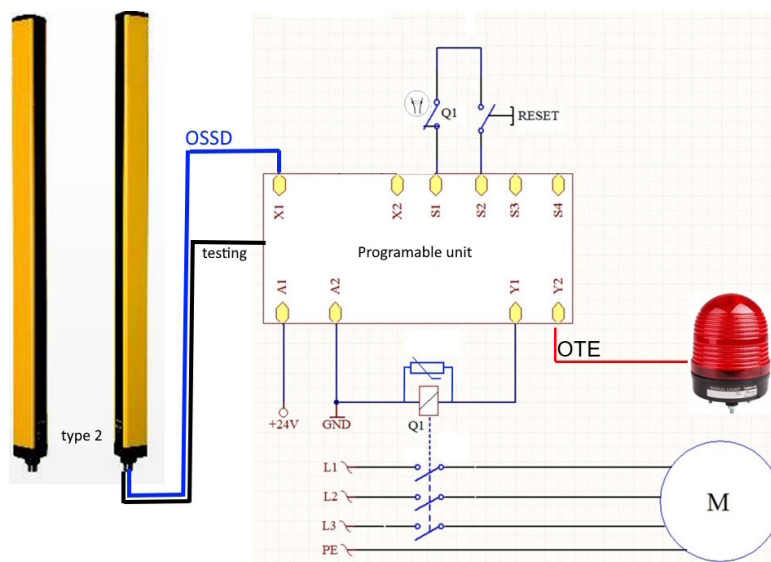


Figure 12. Machine control system to achieve PLC level (own elaboration). OSSD—output signal switching device.

For the circuit implementing the presented function of detecting the violation of the danger zone from Figure 12 with the assumptions described above, protection against cyber-attack is required. The required security level takes SL-T 2 (medium level).

5.5. Example 5—Machine Control System: Category 2, PLd; Cybersecurity SL-T 3

Figure 13 shows a packaging machine. The machine performs rapid rotational movements (which implies that it is unlikely to avoid danger (parameter P2)). Dynamic movements can cause severe impacts or entrapment (suffocation) of a person with the plastic film. Thus, it is assumed that potential injuries may be severe (parameter S2). The user opens the side interlocking guard infrequently, only once or twice per shift during jam removal. This implies the F1 parameter is used. Given the aforementioned characteristics, the required level is PLr = d.



Figure 13. The danger zone of a machine (behind the door) protected by, among other things, an interlocking guard (own elaboration).

The door interlocking sensor is connected to a programmable safety unit (Figure 14). The NC contact of the interlocking sensor is tested, e.g., with test pulses from the programmable unit, which makes it possible to detect short circuits to the ground and short circuits to the positive pole of the supply. However, not all types of faults can be detected. Therefore, the highest DC cannot be achieved. The auxiliary contactor contact Q1 is included in the feedback loop. The main and auxiliary contacts of the contactor are mechanically linked. If a fault occurs, the programmable safety unit is able to indicate the fault with a red lamp and disconnect the master contactor Q2 in the master switchgear.

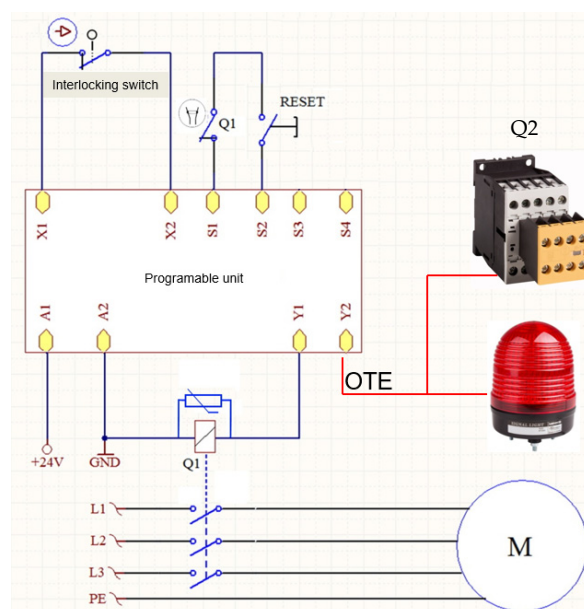


Figure 14. Machine control system to achieve PLd level (own elaboration).

For a circuit implementing the depicted interlocking function of Figure 14 under the assumptions described above, protection against cyber-attack is required. The required security level adopts SL-T 3 (high level).

5.6. Example 6—Machine Control System: Category 3, PLd; Cybersecurity SL-T 3

Figure 15 shows a robotic cell. The robot moves quickly along different trajectories (which implies that the danger (parameter P2) cannot be avoided). Dynamic movements can cause strong impacts to humans, such as to the head, which can lead to death. Thus, it is assumed that potential injuries could be severe (parameter S2). The user enters the cell by violating the protective zone monitored by the laser scanner to pick up the pallet (they do not stay there long). This implies the F1 parameter is used. Based on the graph, the required level is PLr = d. Robotic cells should be designed according to the requirements of ISO 10218-2 [28], which requires the use of the PLr = d level and category 3.

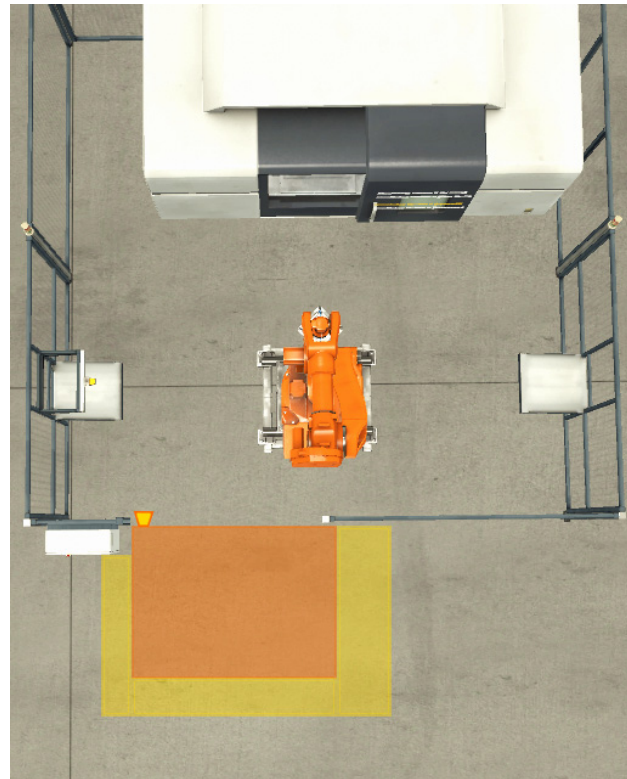


Figure 15. Hazardous zone in a robotic cell protected by a laser scanner (own elaboration).

The laser scanner (typically rated at PLd/Kat.3 level) is connected to a robot controller (typically rated at PLd/Kat.3) equipped with safety functions for stopping the robot drives (Figure 16).

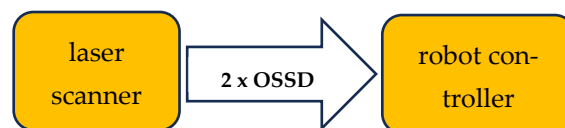


Figure 16. Safety system consisting of laser scanner (PLd/Cat.3) and robot controller (PLd/Cat.3) to achieve PLd/Cat.3 level (own elaboration).

For the circuit implementing the depicted function of detecting the violation of the danger zone of Figure 16 with the assumptions described above, protection against cyber-attack is required. The required protection level is assumed to be SL-T 3 (high level).

5.7. Example 7—Machine Control System: Category 4, PLe; Cybersecurity SL-T 3

Let us consider a hydraulic press. The movement of the press actuator is fast, which implies that danger cannot be avoided (parameter P2). The sliding motion can crush a

person or a body part. So, the potential injury is assumed to be severe (parameter S2). The operator inserts and removes the workpiece from the press every few minutes, violating the protective zone monitored by the light curtain type 4 according to IEC 61496-1. This implies parameter F2 is used. Based on the graph, the level $PLr = e$ is required. Hydraulic presses should be designed in accordance with the requirements of ISO 16092-3 [29], which requires a $PLr = e$ level and category 4 for the SF under consideration.

The light curtain (Type 4, PLe/Kat.4) is connected to a programmable safety unit, the outputs of which are connected to redundant electromechanical components with fault monitoring (electrohydraulic valves or contactors) that stop the dangerous movement of the actuator (Figure 17).

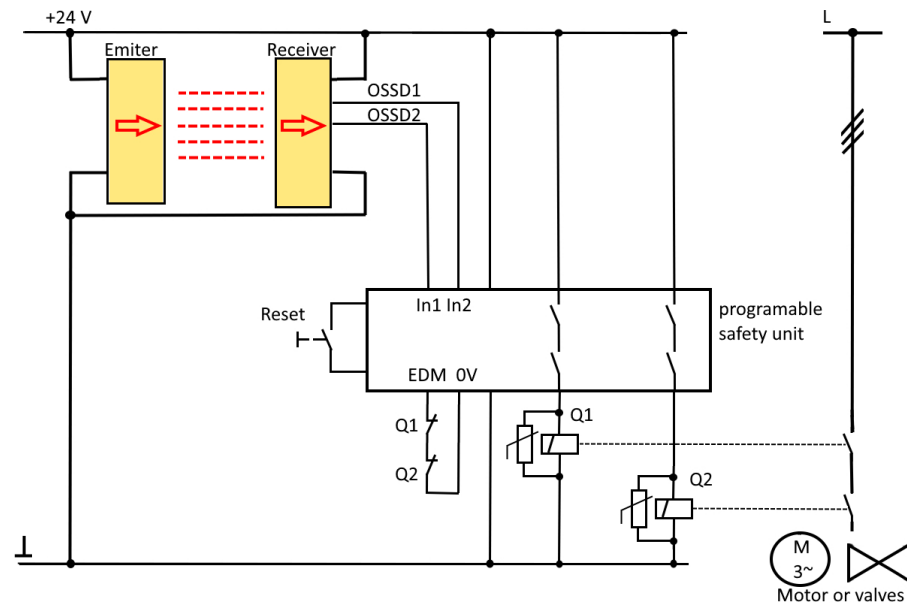


Figure 17. Control system to achieve PLe (own elaboration).

For the circuit implementing the depicted function of detecting the violation of the danger zone from Figure 17 with the assumptions described above, protection against cyber-attack is required. The required protection level is assumed to be SL-T 3 (high level).

6. Summary and Conclusions

This paper presents a proposal for linking PL safety levels of safety functions with SLs. Seven representative examples of various machines and safety functions realized in their control systems were provided. The analysis resulted in the required SL-T cybersecurity levels for each safety function. The next step should be the implementation of appropriate hardware, software, and methods to achieve appropriate SL-A levels based on the required SL-T.

On principle, the cybersecurity objectives should not conflict with safety-related control systems and production efficiency.

Periodic audits related to the effectiveness of the security measures in place are recommended. Countermeasures against cyber-attacks may be audited as needed, and if necessary, controlled cyber-attacks may be conducted to detect existing security vulnerabilities.

Furthermore, the manufacturer should communicate in the form of instructions the requirements for the necessary skills of maintenance services and the necessary training and equipment for ensuring cybersecurity.

The authors suggest further research and recommend implementation of the IEC 62443 series of standards to enhance protection against cyber threats to machine control

systems. Currently, the manufacturers provide some technical means, such as configurable industrial security devices that allow for monitoring network traffic and setting certain access rules (e.g., IP pool). These devices can be used to protect certain machines, e.g., robot cells to prevent unauthorized access to the robot controller. Another interesting solution is equipment with RFID keys and a reader that can be used against sabotage directly at the machine. RFID keys give different permissions for different employees to access more or less advanced functions of the machine control system and its ports e.g., USB ports. Thus, collecting new experiences with the implementation of this kind of equipment will be the next activity in cybersecurity research and development.

Author Contributions: “Introduction”, L.K. and A.M.; “Analysis of cyber hazards in industry”, A.M.; “Safety requirements for machinery”, L.K. and M.D.; “Relationship between safety categories and PLs and SLs”, M.D. and L.K.; “Case study—examples of determining SLs of safety functions implemented in machine safety systems”, L.K. and M.D.; “References”, A.M., L.K. and M.D.; supervision, development, and administration of the project, M.D. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is published and based on the results of a research task carried out within the scope of the fifth stage of the National Programme “Improvement of safety and working conditions” supported by the resources of the National Centre for Research and Development, task no. II.PB.18 entitled “Development of a method of risk analysis conducted by machine designers with cybersecurity aspects in view” and the statutory research BK-271/RG1/2024.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Stallings, W. *Network Security Essentials: Applications and Standards*; Pearson: Boston, MA, USA, 2020.
2. Tanveer, A.; Sinha, R.; MacDonell, S.G.; Leitao, P.; Vyatkin, V. Designing Actively Secure, Highly Available Industrial Automation Applications. *arXiv* **2021**, arXiv:2101.01856.
3. Lesi, V.; Jakovljevic, Z.; Pajic, M. Security Analysis for Distributed IoT-Based Industrial Automation. *arXiv* **2020**, arXiv:2006.00044. Available online: <https://arxiv.org/abs/2006.00044> (accessed on 25 September 2024). [CrossRef]
4. Duque Anton, S.D.; Fraunholz, D.; Krohmer, D.; Reti, D.; Schneider, D.; Schotten, H.D. The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World. *arXiv* **2021**, arXiv:2111.13862. Available online: <https://arxiv.org/abs/2111.13862> (accessed on 25 September 2024).
5. Buczkowski, P.; Malacaria, P.; Hankin, C.; Fielder, A. Optimal Security Hardening over a Probabilistic Attack Graph: A Case Study of an Industrial Control System using the CySecTool Tool. *arXiv* **2022**, arXiv:2204.11707. Available online: <https://arxiv.org/abs/2204.11707> (accessed on 20 September 2024).
6. Boyes, W. *Instrumentation Reference Book*; Butterworth-Heinemann: Oxford, UK, 2010. Available online: <https://www.sciencedirect.com/science/article/pii/B9780750683081000577> (accessed on 25 September 2024).
7. Mesarovic, M.D.; Takahara, Y. *Theory of Multi-Level Hierarchical Systems*; Academic Press: New York, NY, USA, 1970.
8. Liu, Y.; Ning, P.; Reiter, M.K. False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2011**, *14*, 1–33. [CrossRef]
9. Slay, J.; Miller, M. Lessons Learned from the Maroochy Water Breach. In *International Conference on Critical Infrastructure Protection*; Springer: Boston, MA, USA, 2007; pp. 73–82. [CrossRef]
10. Chen, L.; Löhr, H.; Manulis, M.; Sadeghi, A.R. Property-Based Attestation without a Trusted Third Party. *Inf. Secur. Conf. ISC* **2008**, 5222, 277–284.
11. Gajek, S.; Manulis, M.; Pereira, O.; Sadeghi, A.R.; Schwenk, J. Universally Composable Security Analysis of TLS. In *Provable Security. ProvSec 2008*; Baek, J., Bao, F., Chen, K., Lai, X., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5324. [CrossRef]

12. Manowska, A.; Boros, M.; Hassan, M.W.; Bluszcz, A.; Tobór-Osadnik, K. A Modern Approach to Securing Critical Infrastructure in Energy Transmission Networks: Integration of Cryptographic Mechanisms and Biometric Data. *Electronics* **2024**, *13*, 2849. [[CrossRef](#)]
13. Cutillo, L.A.; Mark, M.; Thorsten, S. Security and Privacy in Online Social Networks. *Handbook of Social Network Technologies*. 2010. Available online: <https://api.semanticscholar.org/CorpusID:19873542> (accessed on 23 January 2025).
14. Śliwiński, M.; Piesik, E. Designing control and protection systems with regard to integrated functional safety and cybersecurity aspects. *Energies* **2021**, *14*, 2227. [[CrossRef](#)]
15. Kasprzyczak, L. Common errors in machine safety-related control systems and methods of their elimination. *J. KONBiN* **2023**, *53*, 141–151. [[CrossRef](#)]
16. Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC. Available online: <https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng> (accessed on 23 January 2025).
17. *ISO 12100:2010*; Safety of Machinery. General Principles for Design. Risk Assessment and Risk Reduction. ISO: Geneva, Switzerland, 2010.
18. *ISO 13849-1:2023*; Safety of Machinery. Safety-Related Parts of Control Systems—General Principles for Design. ISO: Geneva, Switzerland, 2023.
19. *IEC 62061:2021+A1:2024*; Safety of Machinery. Functional Safety of Safety-Related Control Systems. IEC: Geneva, Switzerland, 2024.
20. Dźwiarek, M.; Hryniewicz, O. Periodical inspection frequency of safety related control systems of machinery—Practical recommendations for the determination. In *Advances in Safety, Reliability and Risk Management*; Grall, B., Soares, G., Eds.; Taylor & Francis Group: London, UK, 2011; pp. 495–502, ISBN 978-0-415-68379-1.
21. *ISO/IEC 27001:2022*; Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO: Geneva, Switzerland, 2022.
22. *IEC TS 62443-1-1:2009*; Industrial communication networks - Network and system security—Part 1-1: Terminology, Concepts and Models. IEC: Geneva, Switzerland, 2009.
23. *IEC 62443-4-2:2019*; Industrial Communication Networks—Network and System Security—Part 1-1: Terminology, Concepts and Models. IEC: Geneva, Switzerland, 2019.
24. *IEC 62443-3-2:2020*; Security for Industrial Automation And Control Systems—Part 3-2: Security Risk Assessment for System Design. IEC: Geneva, Switzerland, 2020.
25. *ISO 13849-2:2012*; Safety of Machinery—Safety-Related Parts of Control Systems Part 2: Validation. ISO: Geneva, Switzerland, 2012.
26. *IEC 61496-1:2020*; Safety of Machinery—Electro-Sensitive Protective Equipment—Part 1: General Requirements and Tests. IEC: Geneva, Switzerland, 2020.
27. *ISO 13850:2015*; Safety of Machinery—Emergency Stop Function—Principles for Design. ISO: Geneva, Switzerland, 2015.
28. *ISO 10218-2:2011*; Robots and Robotic Devices—Safety Requirements for Industrial Robots Part 2: Robot Systems and Integration. ISO: Geneva, Switzerland, 2011.
29. *ISO 16092-3:2017*; Machine Tools Safety—Presses Part 3: Safety Requirements for Hydraulic Presses. ISO: Geneva, Switzerland, 2017.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.