Enhancing business continuity planning through AHP-based physical security control prioritization*

Nataliya Zagorodna[1,*,†], Ruslan Kozak[1,†], Taras Lechachenko[1,†], Yuriy Skorenkyy[1,†], and Oleksandr Revniuk[1,†]

[1] *Ternopil Ivan Puluj National Technical University, 56 Ruska str., 46001 Ternopil, Ukraine*

Abstract

This paper presents an approach for prioritizing physical security controls for manufacturing SMEs in accordance with ISO/IEC 27001:2022. It combines Business Impact Analysis, attack tree modeling, and the Analytic Hierarchy Process to support business continuity planning under limited resources. The study shows that weaknesses in physical security can enable cyber-physical attacks, particularly in Industry 5.0 environments. Expert-based AHP results identify equipment protection, facility securing, and environmental protection as the most critical controls.

Keywords

explainable artificial intelligence, XAI, self-organizing map. SOM, network traffic anomaly detection, cyber influence modeling, intelligent intrusion detection, critical feature analysis, cyber threats, unsupervised learning.

1. Introduction

Information security management standard ISO/IEC 27001 provides organizations with a structured framework for safeguarding information assets through an Information Security Management System (ISMS), encompassing risk assessment, risk management, and continuous improvement [1, 2]. The implementation of standard requires thorough risk assessment and careful prioritization of security controls, consolidated in Annex A of the latest ISO/IEC 27001:2022 edition, which comprises 93 controls organized into four categories: organizational, people, physical, and technological [1].

As European green and digital transition policies drive small and medium enterprises (SMEs) toward digitization of production and management processes [3, 4], organizational resilience and business continuity have emerged as requirements of paramount importance. The EU's NIS2 Directive (2022/2555) requires robust cybersecurity risk management and business continuity planning, particularly for entities in critical sectors including manufacturing [5], while the Recovery and Resilience Facility allocates substantial resources to support SMEs in their twin digital and green transitions [6]. Industry 5.0 offers the most promising framework to address contemporary challenges facing SMEs in smart manufacturing. This paradigm integrates extensive digitization and automation — leveraging Internet of Things (IoT) devices, artificial intelligence, and industrial analytics — with human-centric innovations such as collaborative robots (cobots) and immersive virtual environments [7, 8]. By synergizing human creativity with advanced technological capabilities, Industry 5.0 enables mass customization while ensuring sustainability, resilience, and enhanced workforce wellbeing [9]. However, resource-constrained SMEs require robust methodologies for information security controls prioritization to achieve ISO/IEC 27001 compliance while managing limited budgets and technical expertise [10].

* *CSDP'2026: Cyber Security and Data Protection, May 7, 2026, Lviv, Ukraine*
* Corresponding author.
† These authors contributed equally.
zagorodna_n@tntu.edu.ua (N. Zagorodna); ruslan.o.kozak@gmail.com (R. Kozak); taras5a@ukr.net (T. Lechachenko); skorenkyy@tntu.edu.ua (Y. Skorenkyy); revo0708@gmail.com (O. Revniuk)
0000-0002-1808-835X (N. Zagorodna); 0000-0003-1323-6448 (R. Kozak); 0000-0003-1185-6448 (T. Lechachenko); 0000-0002-4809-9025 (Y. Skorenkyy); 0009-0005-0511-5354 (O. Revniuk)

Business impact analysis (BIA), as a foundational component of business continuity planning (BCP) and disaster recovery (DR) strategies, directly influences organizational priorities for physical and organizational security controls [11, 12]. BIA enables organizations to identify and prioritize critical business functions, information assets, and physical locations based on their significance to operational continuity and business success [13]. Without rigorous BIA, organizations risk the paradox of over-protecting low-impact areas while leaving mission-critical assets vulnerable to disruption. In manufacturing environments, unauthorized intrusions and security breaches can precipitate multiple severe consequences: loss of proprietary industrial data and intellectual property, interruption of production operations with cascading supply chain effects, degradation of product quality threatening customer relationships, and — most critically — tangible physical hazards to personnel operating machinery and production equipment [6, 14].

Among the 93 information security controls referenced in ISO/IEC 27001:2022 Annex A, organizational controls (37 controls addressing policies, compliance, and business processes) and physical controls (14 controls covering facility security, environmental protection, and physical access management) are frequently underestimated in implementation strategies [15, 16]. This oversight creates a critical vulnerability in organizational information protection, as physical security breaches can circumvent even the most sophisticated technological safeguards, while inadequate organizational controls undermine the governance structure essential for sustained security posture [17, 18]. The integration of Industry 5.0 technologies — particularly IoT sensors, AR interfaces, and collaborative robotics — further extends the attack surface, making systematic prioritization of physical and organizational controls imperative for comprehensive cyber-physical security [19, 20].

This research addresses this gap by developing a methodology for systematic prioritization of ISO/IEC 27001 physical controls, specifically tailored for Industry 5.0 manufacturing SMEs, considered in previous works [21, 22], which complements previously developed procedures regarding cybersecurity measures [23, 24] and allows to streamline the business continuity planning of an enterprise.

2. Related Works

Analytical hierarchy process [25] is a technique to solve the complex, unstructured problems by breaking them down into small components, reorganizing these components into hierarchic positioning, synthesizing the final judgment to evaluate which alternative has the highest-ranking, and also to influence the output of the situation. It utilizes a hierarchical structure to extract, deteriorate, compose, and control the complexity of the decision including numerous attributes, and it utilizes judgment or the decision maker's opinion to gauge the relative worth or commitment of these characteristics. In AHP, pairwise comparisons are developed to reduce complicated decisions, and synthetization of the results are also taken. Furthermore, the AHP also assists in taking subjective and objective types of the decision. In the AHP model, weights are given to the decision makers. During the decision-making process, the alternatives are compared with each other by assigning that weight. AHP has been widely used [2] to prioritize ISO/IEC 27002:2013 information security controls, utilizing criteria such as implementation time, effectiveness, risk, budgetary constraints, exploitation time, maintenance cost, and mitigation time, etc. Fuzzy AHP is shown to be the most appropriate for prioritizing information security controls due to its ability to handle ambiguity, support hierarchical processes, and validate results through consistency indices. Recent research has combined Spherical Fuzzy AHP with TODIM methods for digital maturity assessment [26] to tackle the problem of subjective judgments of experts. Application of Multi Criteria Decision Making (MCDM) based on fuzzy logic for the qualitative assessment of information security risks has been done in [27]. AHP based ranking of information security risks has been done in [28], for banking and construction sectors. MCDM and AHP for

information security risk assessment with Bayesian prioritization procedure to overcome incompleteness of the available information have been used in [29].

Worth noting, the latest edition of the ISO/IEC 27001 standard has not been used as a basis for AHP-powered decision making and vulnerabilities of Industry 5.0-specific critical assets (IoT sensors, immersive interfaces, digital twins) were not adequately addressed in traditional frameworks. A few research questions are worth special attention, namely what criteria should be prioritized when evaluating security controls for Industry 5.0 SMEs and how can AHP framework account for the extended attack surface introduced by personal devices and IoT sensors in industrial environments.

3. Modeling approach

BIA identifies critical processes and assets, i.e. premises, equipment and physical locations which are the most important to the business, and defines what the consequences of their destruction, interference, shutdown, etc. may be. Let's consider a scenario, in which a medium-sized company or manufacturer, for example, has production facilities, a logistics center and an office with a small on-site data center, where sensitive data are processed. In this case the following steps can be taken to identify priority controls:

1. Specify physical infrastructure.
2. Identify critical business processes and supporting physical assets.
3. Analyze attack scenarios for critical processes and assets.
4. Select physical security controls to treat attack scenarios.
5. Prioritize security controls to protect critical assets.

Many assessment criteria and alternatives were discussed [30] and this helps in the selection of the most appropriate set. Figure 1 represents a hierarchy structure for the evaluation of physical controls utilizing the AHP method.

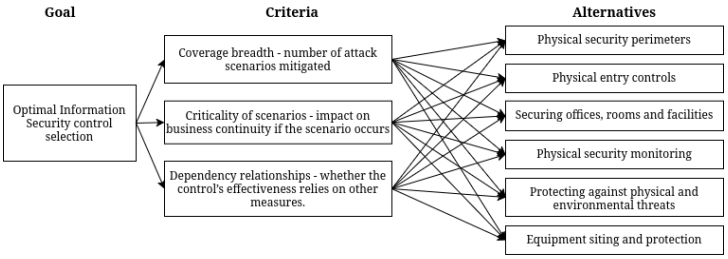

Figure 1: Hierarchy structure for the evaluation of physical controls in AHP.

Detailed description of the selected physical controls according to ISO/IEC 27001:2022 is given in the Table 1 below. This set of controls corresponds to specifics of SMEs being in focus of papers [21, 22] and may be adopted for the Statement of Applicability (SoA), required by the ISO/IEC 27001:2022 standard.

3.1. Business impact analysis

A systematic Business Impact Analysis (BIA) serves as the cornerstone for identifying and prioritizing mission-critical business processes according to their contribution to organizational continuity and competitive positioning [31]. Within manufacturing SME contexts, production operations constitute the primary critical function, characterized by dependencies on manufacturing equipment, electrical infrastructure, and industrial control systems. Disruption to production capabilities leads to immediate cessation of output, causing a chain of consequences, including loss of revenue, unfulfilled customer commitments, and reputational deterioration [14]. Given the severity of potential operational and financial impacts, the Recovery Time Objective (RTO) for production operations is established at less than 24 hours, reflecting industry standards for critical manufacturing processes [11].

Table 1
Selected physical security controls of ISO/IEC 27001:2022

Control Number	Control Name	Control Objective	Description
A.7.1	Physical security perimeters	Prevent unauthorized physical access to company facilities.	Establishing secure perimeters, such as fences, gates, and security checkpoints, to restrict entry.
A.7.2	Physical entry	Control and monitor access to buildings, offices, and data centers.	Implementing access control systems (e.g., keycards, biometric scanners, and security guards) to regulate entry.
A.7.3	Securing offices, rooms, and facilities	Ensure that only authorized personnel can enter sensitive areas.	Using locks, restricted zones, and security protocols to prevent unauthorized access.
A.7.4	Physical Security Monitoring	Requires organisations to implement appropriate surveillance tools	Monitoring access- restricted areas to protect from data theft, malware infection of IT assets, etc.
A.7.5	Protecting against physical and environmental threats	Reduce risks from natural disasters, fire, and power failures.	Implementing climate control, fire suppression systems, and backup power solutions.
A.7.8	Equipment siting and protection	Protect IT equipment from unauthorized access or damage.	Securing workstations, servers, and networking devices with locks, cages, and surveillance

The secondary level of criticality encompasses logistics and distribution operations, which depend upon warehouse management systems, transportation scheduling platforms, and enterprise resource planning (ERP) integration. Interruptions within this operational domain generate supply chain propagation effects, manifesting as delivery delays, contractual penalties, and customer satisfaction degradation. Contemporary research demonstrates that supply chain disruptions in manufacturing SMEs create cascading impacts across multiple organizational tiers, with particular vulnerability in resource-constrained environments. Consequently, the RTO for logistics and distribution functions is defined as less than 48 hours, balancing operational criticality against resource availability constraints. Supporting business processes, including administrative functions (human resources, financial operations) and non-critical information technology services (electronic mail, intranet platforms), maintain organizational functionality yet exhibit reduced temporal sensitivity. These processes are assigned RTOs of approximately 72 hours, reflecting their contributory rather than mission-critical status [13]. This hierarchical prioritization framework ensures optimal allocation of business continuity resources toward safeguarding functions demonstrating the highest correlation with organizational survival and competitive performance [32].

3.2. Physical infrastructure of manufacturing SME

The subject of this study is a medium-sized manufacturing company that combines administrative, production, and logistics functions within a single operational ecosystem. The company's infrastructure can be described as a set of interconnected units:

1. Office Building: Reception, employee workstations, and meeting rooms.
2. Production Facilities: Assembly lines, workshops, and raw material storage.
3. Data Center: Server racks, cooling systems, UPS, and networking equipment.
4. Logistics Center: Warehousing, packaging areas, and loading docks.

The office building serves as the organizational hub, accommodating reception, HR, finance, and management activities. It is the nerve center for decision-making and coordination, ensuring that strategic and administrative processes align with operational needs. Adjacent to this lies the

production facility, which houses assembly lines, specialized machinery, and raw material storage. This area represents the company's core value creation, where raw inputs are transformed into finished goods. The facility also includes workshops for maintenance, underscoring the importance of keeping machinery operational and minimizing downtime. Supporting these functions is a small on-site data center, a critical technological asset that hosts ERP systems, production control software, and logistics databases. Despite its modest size, the data center is vital for synchronizing production schedules, monitoring supply chains, and ensuring that digital systems underpinning physical operations remain resilient. Finally, the logistics center provides the bridge between production and customers. With warehousing, packaging areas, and loading docks, it ensures that finished goods are stored securely, packaged efficiently, and dispatched on time. Together, these facilities form a tightly integrated ecosystem where physical and digital assets converge to sustain business continuity.

The organizational facility infrastructure comprises distinct functional zones that collectively constitute the cyber-physical security perimeter. The administrative complex serves as the organizational nerve center, integrating reception services, human resources management, financial operations, and executive decision-making functions. This zone represents the locus of strategic coordination, ensuring alignment between administrative protocols and operational requirements while maintaining the organizational governance framework essential for sustained business continuity [33]. Proximate to the administrative complex, the manufacturing facility encompasses assembly operations, specialized production equipment, and raw material repositories. This domain constitutes the primary value-creation infrastructure, wherein material inputs undergo systematic transformation into finished products through controlled industrial processes. The facility incorporates dedicated maintenance workshops, underscoring the criticality of preventive and corrective maintenance protocols in minimizing production downtime and ensuring continuous operational capability. A dedicated on-site data center, despite its modest physical footprint, represents a mission-critical technological asset hosting integrated enterprise systems including enterprise resource planning (ERP) platforms, production control applications, and supply chain management databases [34, 35]. Contemporary manufacturing environments increasingly depend on such integrated digital infrastructure to synchronize production schedules, monitor supply chain dynamics, and ensure operational resilience of cyber-physical systems underpinning production operations [36]. The convergence of physical manufacturing assets with digital control systems necessitates comprehensive security frameworks that address both technological vulnerabilities and physical access controls in accordance with ISO/IEC 27001:2022 requirements for physical and environmental security. The logistics center provides the operational interface between production completion and customer fulfillment, incorporating warehousing infrastructure, packaging operations, and loading facilities. This functional domain ensures secure storage of finished goods inventory, efficient packaging processes, and timely dispatch operations that maintain supply chain continuity and customer satisfaction metrics. These interdependent facilities constitute an integrated ecosystem wherein physical infrastructure and digital assets converge to sustain organizational business continuity and operational resilience [11, 13].

3.3. Critical assets of manufacturing SME

From this analysis, several assets emerge as indispensable to the company's resilience. Production machinery and control systems, including CNC machines, PLCs, and ERP integration, form the backbone of manufacturing operations. The data center servers, which host ERP and logistics databases, are equally critical, as they provide the digital infrastructure [37] that coordinates production and distribution.

The warehouse inventory and transport systems represent the physical manifestation of logistics, ensuring that goods are stored, tracked, and dispatched efficiently. Supporting all of these are power supply and environmental controls, such as UPS units and HVAC systems, which safeguard against outages and environmental fluctuations. Finally, access control mechanisms such

as badges, CCTV, and locks, provide the first line of defense against unauthorized entry and physical threats. Taken together, these assets illustrate the company's reliance on both physical and digital systems. Their protection is not merely a matter of operational efficiency but of organizational survival, making them the focal point for subsequent security analysis.

3.4. Threats to production operations

Production operations form the company's most vital process, directly tied to revenue generation and customer satisfaction. Adversaries seeking to disrupt this domain may exploit both physical and digital vulnerabilities. The attack surface includes machinery, control systems, and supporting infrastructure such as power supply and environmental controls.

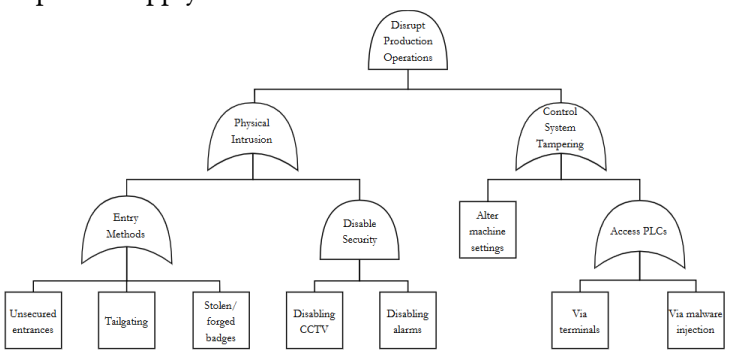

Figure 2: Attack tree for production operations.

Potential attack scenarios (Figure 2) include:

1. Unauthorized physical access to production areas, enabling sabotage or theft of machinery components.
2. Tampering with control systems (e. g., PLCs or ERP integration) to halt or misconfigure production lines.
3. Disruption of utilities, such as cutting power or interfering with HVAC systems, leading to downtime or equipment damage.
4. Insider threats, where employees misuse legitimate access to alter production schedules or damage equipment.

3.5. Threats to logistics and distribution

Logistics and distribution represent the second critical process, ensuring that finished goods reach customers on time. Adversaries may target this domain to cause delays, financial losses, or reputational harm. The logistics center, with its warehouses, transport systems, and ERP integration, is particularly vulnerable to physical intrusion and disruption. Potential attack scenarios (Figure 3) include:

- Theft or tampering with inventory, leading to financial loss and supply chain disruption.
- Blocking or delaying shipments by interfering with loading docks or transport scheduling systems.
- Sabotaging warehouse systems, such as disabling barcode scanners or altering inventory records.
- Environmental disruption, such as arson or flooding, to damage stored goods.

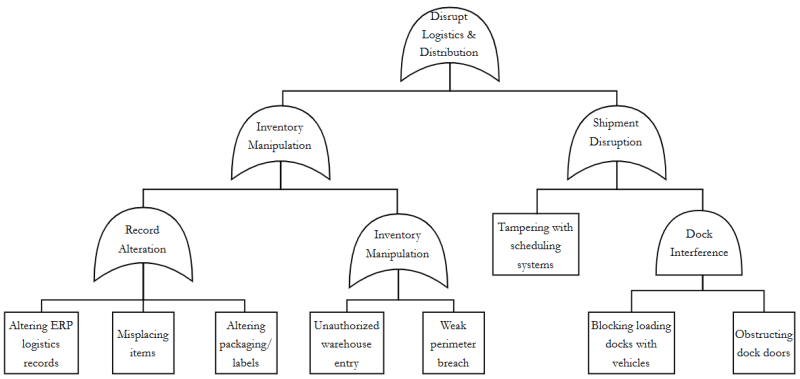

Figure 3: Attack tree for logistics and distribution.

4. Mapping physical security controls to attack scenarios

4.1. Production operations attack tree analysis

Attack trees illustrate how adversaries may pursue multiple paths to achieve disruption. Each branch represents a potential scenario, ranging from low-sophistication physical intrusions to more advanced manipulations of control systems. Importantly, the trees highlight the interdependence between physical and digital assets: a breach in physical security often enables subsequent exploitation of IT systems, amplifying the impact. The attack tree for production operations reveals multiple ways adversaries might disrupt manufacturing. ISO 27001 Annex A provides a structured set of physical security controls that directly counter these threats.

1. Tailgating into production areas can be prevented through A.7.2 Physical entry controls, which mandate secure entry systems such as mantraps, badge readers, or biometric authentication. By enforcing strict entry procedures, the company ensures that only authorized personnel gain access.
2. Stolen or forged badges are mitigated by combining A.7.2 Physical entry controls with A.7.4 Physical security monitoring. Regular monitoring of CCTV footage and automated badge deactivation policies reduce the risk of unauthorized use.
3. Attempts to disable CCTV or alarms are countered by A.7.4 Physical security monitoring, which requires tamper-resistant surveillance systems and redundant monitoring. This ensures that even if one system is compromised, another continues to provide oversight.
4. Exploiting unsecured entrances is addressed by A.7.1 Physical security perimeters, which emphasizes secure boundaries, locked doors, and controlled access points.
5. Direct sabotage of machinery, whether through physical damage, altering settings, or removing components, is mitigated by A.7.8 Equipment siting and protection. This control requires protective enclosures, restricted access to control panels, and authorization for equipment changes.
6. Manipulating control systems such as PLCs or ERP terminals is prevented by A.7.3 Securing offices, rooms, and facilities, which ensures that sensitive areas like server rooms and control stations are locked and monitored.
7. Disruptions to utilities, cutting power, disabling UPS, or interfering with HVAC, are addressed by A.7.5 Protecting against physical and environmental threats. This control requires securing power panels, generator rooms, and environmental systems to maintain operational continuity.

Together, these controls form a layered defense, ensuring that production operations remain resilient against both opportunistic and deliberate attacks. By aligning each leaf node with ISO 27001 controls, organizations can systematically address vulnerabilities identified in attack trees, ensuring that both production and logistics remain resilient against adversarial threats.

4.2. Logistics and distribution attack tree analysis

The logistics attack tree highlighted vulnerabilities in warehousing, transport, and inventory systems. ISO 27001 controls provide targeted safeguards against each identified threat:

1. Weak perimeter security around warehouses is mitigated by A.7.1 Physical security perimeters, which requires fencing, barriers, and controlled vehicle access.
2. Tailgating delivery personnel is countered by A.7.2 Physical entry controls, supported by escort policies and anti-tailgating doors.
3. Attempts to disable entry controls are addressed by redundancy and audit requirements under A.7.2, ensuring that failures are detected and corrected quickly.
4. Theft or tampering with inventory is mitigated through A.7.8 Equipment siting and protection, which requires secure storage, CCTV monitoring, and automated inventory tracking.
5. Altering packaging or labels is prevented by restricting access to packaging areas under A.7.8, combined with quality assurance checks.
6. Hiding or misplacing items is countered by automated inventory systems and segregation of duties, also mandated under A.7.8.
7. Blocking loading docks with unauthorized vehicles is prevented by A.7.1 Physical security perimeters, which enforces vehicle access controls and monitored dock areas.
8. Delaying trucks via false scheduling is mitigated by A.7.3 Securing offices, rooms, and facilities, ensuring that logistics scheduling systems are physically protected from tampering.
9. Damaging vehicles is addressed by securing fleet parking areas under A.7.8, supported by surveillance and restricted access.
10. Disabling barcode scanners or shutting down warehouse IT systems is prevented by A.7.8 Equipment security and A.7.3, which require secure handling of IT equipment and restricted access to terminals.
11. Altering ERP logistics records is mitigated by A.7.3, which ensures that ERP terminals are physically secured and monitored.

These controls collectively safeguard the logistics chain, ensuring that goods are stored, tracked, and dispatched without disruption. By mapping each leaf node of the attack trees to specific ISO 27001 Annex A controls, the organization gains a clear roadmap for defense. The controls are not abstract requirements but practical countermeasures: perimeter security stops intruders before they enter, entry controls prevent unauthorized access, monitoring detects tampering, environmental protections safeguard utilities, and equipment security ensures machinery and IT systems remain intact.

This layered approach demonstrates how ISO 27001 can be operationalized to protect both production and logistics, the company's most critical processes, against adversarial threats.

4.3. Consolidated matrix of security controls

The following consolidated matrix (Table 2) reveals control overlap and coverage density:

1. A.7.8 Equipment security emerges as the most comprehensive, mitigating threats across both production and logistics. It covers sabotage, theft, tampering, and IT equipment misuse.
2. A.7.2 Physical entry controls and A.7.1 Physical security perimeter provide strong defenses against unauthorized access, both at the perimeter and entry points.
3. A.7.3 Securing offices, rooms, facilities is critical for protecting IT systems and logistics scheduling, bridging the gap between physical and digital threats.
4. A.7.5 Protecting against environmental threats is narrower but essential for production continuity, as it addresses power and HVAC disruptions.
5. A.7.4 Physical security monitoring provides oversight but is dependent on the effectiveness of other controls (perimeter and entry).

Table 2
ISO 27001 Annex A Controls vs. Attack Scenarios

ISO 27001 Control	Attack Scenarios Mitigated	Coverage Scope
A.7.1 Physical security perimeters	- Unsecured entrances (Production) - Weak warehouse perimeter (Logistics) - Blocking loading docks with vehicles (Logistics) - Obstructing dock doors (Logistics)	Strong coverage of external intrusion and perimeter threats
A.7.2 Physical entry	- Tailgating (Production & Logistics) - Stolen/forged badges (Production) - Disabling entry controls (Logistics) - Unauthorized warehouse entry (Logistics)	High coverage of access-related threats
A.7.3 Securing offices, rooms, facilities	- Accessing PLCs via terminals (Production) - Introducing malware via ERP terminals (Production) - Altering ERP logistics records (Logistics) - Shutting down warehouse IT systems (Logistics) - Tampering with scheduling systems (Logistics).	Broad coverage of IT/operational facility protection
A.7.4 Physical Security Monitoring	- Disabling CCTV/alarms (Production) - Detecting badge misuse (Production) - Monitoring unauthorized entry attempts (Logistics)	Monitoring access- restricted areas to protect from data theft, malware infection of IT assets, etc.
A.7.5 Protecting against physical and environmental threats	- Cutting power supply (Production) - Preventing generator activation (Production) - Disabling UPS (Production) - Interfering with HVAC (Production)	Focused coverage of surveillance and monitoring
A.7.8 Equipment siting and protection	- Sabotaging machinery (Production) - Removing components (Production) - Altering machine settings (Production) - Theft of goods (Logistics) - Altering packaging/labels (Logistics) - Misplacing items (Logistics) - Damaging vehicles (Logistics) - Disabling barcode scanners (Logistics)	Specialized coverage of environmental and utility disruptions

The above matrix was used as input to the Analytic Hierarchy Process (AHP), evaluating each control against a combined criterion: coverage breadth (number of attack scenarios mitigated) together with scenario criticality (impact on business continuity if the scenario occurs). Such a structured approach allows to assign weights and derive a prioritized list of controls, ensuring that resources are allocated to measures with the greatest impact on resilience. This hierarchy allows decision-makers to perform pairwise comparisons across criteria and alternatives. For example, equipment security (A.7.8) may score highest in coverage breadth, while environmental protection (A.7.5) may rank lower in breadth but higher in criticality for production continuity. The AHP process will yield a weighted prioritization, guiding resource allocation toward the most impactful controls.

5. Selection and comparison of alternatives

Given the specific nature of the processes, assets and security risks characteristic for manufacturing SMEs [21, 22] physical controls that meet the requirements of SoA in accordance with ISO/IEC 27001:2022, detailed in tables 1 and 2, were chosen as alternatives. These alternatives represent key physical and environmental security controls defined in ISO/IEC 27001/27002 and address different layers of physical protection.

The alternatives were evaluated and compared using the AHP methodology [38]. The comparison was conducted with respect to the three evaluation criteria, represented on figure 1.

The suggested method derives priority weights from expert judgments and provides a mechanism for verifying the consistency of judgments and their aggregation.

The calculation formulas are presented as described in [38] and are consistent with the standard AHP methodology.

Let $A=(a_{ij})$ be a pairwise comparison matrix of size $n \times n$ where a_{ij} represents the relative importance of element *i* over element *j*.

The priority vector

$$w=(w_1, w_2, \ldots, w_n) \tag{1}$$

is obtained using the eigenvector method and is normalized:

$$\sum_{i=1}^{n} w_i = 1. \tag{2}$$

The weighted sum vector is calculated as:

$$(Aw)_i = \sum_{j=1}^{n} a_{ij} w_j. \tag{3}$$

The consistency vector is then obtained by dividing each component of the weighted sum vector by the corresponding priority weight:

$$\lambda_i = \frac{(Aw)_i}{w_i}. \tag{4}$$

The maximum eigenvalue λ_{max} is estimated as the average of the consistency vector:

$$\lambda_{max} = \frac{1}{n} \sum_{i=1}^{n} \lambda_i \tag{5}$$

To evaluate the consistency of the pairwise comparison matrix, the Consistency Index (CI) is calculated as:

$$CI = \frac{\lambda_{max} - n}{n-1} \tag{6}$$

According to AHP, the Consistency Ratio ($CR = \frac{CI}{RI}$) should be less than 0.10 to indicate an acceptable level of consistency of the pairwise comparison judgments. In [39] expert opinions were aggregated using fuzzy logic system. When using AHP the individual expert judgments are more appropriate to aggregate in group judgment matrix using the geometric mean [40]. This ensures that the reciprocal property of the AHP pairwise comparison matrix is preserved and provides a consensual representation of the experts' perspectives.

$$a_{ij}^{group} = \left(\prod_{l=1}^{k} a_{ij}^{(l)} \right)^{\frac{1}{k}}, \tag{7}$$

where a_{ij}^{group} denotes the pairwise comparison value between criteria *i* and *j* provided by the *l*-th expert, where *k* is the total number of experts.

At the beginning three experts with a minimum of five years of professional experience in cybersecurity were chosen. Then they were suggested to do AHP pairwise comparison of three criteria represented in figure 1. At the next step, experts were required to carry out pairwise comparison of selected alternatives by each of criterion. The Consistency Index (CI) and Consistency Ratio (CR), as the standard metrics of AHP method, were used to measure the logical

consistency of pairwise comparison matrices, ensuring judgments are rational. The aggregation of experts opinions was made using geometric mean, computed by formula (7).

The example of the pairwise comparison of the selected alternatives by second criterion "Criticality of scenarios" based on three experts evaluations is presented in Table 3.

Table 3
The results of the pairwise comparison of the alternatives by second criterion

Expert 1		Expert 2		Expert 3	
A.7.8	0.39	A.7.5	0.32	A.7.3	0.30
A.7.3	0.21	A.7.8	0.26	A.7.8	0.26
A.7.5	0.17	A.7.3	0.21	A.7.5	0.16
A.7.1	0.11	A.7.2	0.08	A.7.1	0.14
A.7.2	0.06	A.7.1	0.06	A.7.2	0.07
A.7.4	0.03	A.7.4	0.04	A.7.4	0.04

The Consistency Index (CI) and Consistency Ratio (CR) were calculated for the pairwise comparison matrices of each expert, and the resulting values are presented below (Table 4). Following the Random Index (RI) values suggested by [2], the RI for a pairwise comparison matrix of size six was chosen to be 1.25.

Table 4
Consistency Index and Consistency Ratio of pairwise comparison matrices

Number of expert	Consistency Index (CI)	Consistency Ratio (CR)
Expert 1	0.09	0.07
Expert 2	0.05	0.04
Expert 3	0.03	0.02

Based on formula (7), an aggregated pairwise comparison matrix (Table 5) is constructed from the individual expert matrices. The aggregated results of pairwise comparisons are then used to compute the priority weights, as well as the Consistency Index (CI) and the Consistency Ratio (CR) for the aggregated matrix.

Table 5
Aggregated pairwise comparison matrix

Alternatives	A.7.1	A.7.2	A.7.3	A.7.4	A.7.5	A.7.8
A.7.1	1	1.65	0.25	2.62	0.69	0.34
A.7.2	0.60	1	0.27	2.62	0.25	0.25
A.7.3	3.91	3.63	1	5.31	1	0.55
A.7.4	0.38	0.38	0.18	1	0.20	0.17
A.7.5	1.44	3.91	1	4.93	1	0.69
A.7.8	2.88	3.91	1.81	5.59	1.44	1

The Consistency Index (CI) and the Consistency Ratio (CR) for the aggregated pairwise comparison matrix equal to CI = 0.03 and CR = 0.02, respectively.

The global criterion for each alternative was calculated as weighted average of obtained normalized values of eigen vectors based on aggregated pairwise comparison matrices for criteria and aggregated pairwise comparison matrices for alternatives by each of criteria. The final results obtained from the aggregated pairwise comparison matrices are given in Figure 4.

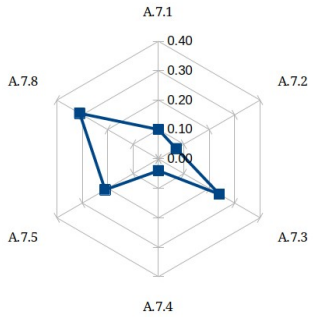

Figure 4: The final results of ISO 27001:2022 physical controls prioritization for SME.

This net diagram visualizes priorities of the physical controls specified by the ISO/IEC 27001:2022 standard and mandates choice of the controls to be included into the company's Statement of Applicability. Such prioritization also simplifies allocation of limited resources of SMEs in the most efficient way. Use of AHP as the methodology for selection of the most appropriate controls reduces ambiguities of individual assessments and allows periodic re-assessments to be conducted according to well documented, formal and transparent procedure, as required by the standard.

6. Conclusions

This research developed a systematic methodology for prioritizing physical security controls in manufacturing SMEs implementing ISO/IEC 27001:2022, addressing a critical gap in business continuity planning for resource-constrained organizations. By integrating Business Impact Analysis with attack tree modeling and Analytic Hierarchy Process evaluation, the study provides a structured framework for allocating limited security resources to controls that most effectively mitigate threats to mission-critical operations.

The attack tree analysis revealed that production operations and logistics/distribution functions face interconnected physical and cyber-physical threats, where breaches in physical security often enable subsequent exploitation of digital systems. The consolidated control-scenario matrix demonstrated that among the six evaluated ISO 27001 Annex A physical controls, A.7.8 Equipment siting and protection provides the broadest coverage, mitigating distinct attack scenarios across both production and logistics domains. The aggregated AHP results from three cybersecurity experts confirmed this assessment, assigning A.7.8 the highest priority weight (0.31), followed by A.7.3 Securing offices, rooms, and facilities at 0.24, and A.7.5 Protecting against physical and environmental threats at 0.21.

These findings demonstrate that equipment protection and facility securing constitute foundational investments for manufacturing SMEs, as they address both physical sabotage and unauthorized access to control systems — threats that directly impact production continuity and organizational survival. The relatively lower priority assigned to A.7.4 Physical security monitoring (0.04) suggests that while surveillance is important, it functions primarily as a complementary control rather than a primary defense mechanism.

The methodology's consistency ratios validate the reliability of the prioritization framework. This approach enables SMEs to systematically develop Statement of Applicability documents aligned with ISO/IEC 27001:2022 requirements while optimizing resource allocation based on business impact criticality. Future research should extend this framework to incorporate Industry 5.0-specific assets such as collaborative robots, IoT sensors, and augmented reality interfaces, which introduce novel attack surfaces requiring specialized physical protection strategies, into the ISO/IEC 27001:2022 based prioritization scheme.

Declaration on Generative AI

During the preparation of this work, the authors used Claude Sonnet 4.5 in order to improve writing style as well as for formatting assistance. After using this AI tool, the content was reviewed and edited by authors, who therefore take full responsibility for the publication's content.

References

[1] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Int. Organ. Stand., 2022.

[2] M. Tariq, et al., Evaluation and Prioritization of Information Security Controls of ISO/IEC 27002:2013 for SMEs Through Fuzzy TOPSIS, In Advances in Intelligent Data Analysis and Applications, vol. 253, Springer, Singap., 2022. doi:10.1007/978-981-16-5036-9_27.

[3] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An SME Strategy for a sustainable and digital Europe, COM(2020), 2020.

[4] X. Gao, The EU's twin transitions towards sustainability and digital leadership: a coherent or fragmented policy field?, Reg. Stud., 2024. doi:10.1080/00343404.2024.2360053.

[5] European Parliament and Council, Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), Off. J. Eur. Union L 333, 2022.

[6] European Commission, Regulation (EU) 2021/241 of the European Parliament and of the Council establishing the Recovery and Resilience Facility, Off. J. Eur. Union L 57, 2021.

[7] X. Xu, Y. Lu, B. Vogel-Heuser, L. Wang, Industry 4.0 and Industry 5.0 — Inception, conception and perception, J. Manuf. Syst., 61, 2021, 530-535. doi:10.1016/j.jmsy.2021.10.006.

[8] P. Maddikunta, et al., Industry 5.0: A survey on enabling technologies and potential applications, J. Ind. Inf. Integr., 26 (2022), 100257. doi:10.1016/j.jii.2021.100257.

[9] S. Nahavandi, Industry 5.0 — A human-centric solution, Sustainability, 11 (2019). doi:10.3390/su11164371.

[10] E. Carayannis, J. Morawska-Jancelewicz, The Futures of Europe: Society 5.0 and Industry 5.0 as Driving Forces of Future Universities, J. Knowl. Econ., 13 (2022) 3445-3471. doi:10.1007/s13132-021-00854-2.

[11] ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements, Int. Organ. Stand., 2019.

[12] G. Zsidisin, M. Henke (Eds.), Revisiting Supply Chain Risk, Springer Ser. Supply Chain Manag., Springer 7 (2019). doi:10.1007/978-3-030-03813-7.

[13] B. Herbane, Rethinking organizational resilience and strategic renewal in SMEs, Entrep. & Reg. Dev., 31 (2019), 476-495. doi:10.1080/08985626.2018.1541594.

[14] A. Corallo, M. Lazoi, M. Lezzi, P. Pontrandolfo, Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level, IEEE Trans. Eng. Manag., 70 (2023), 3745-3765. doi:10.1109/TEM.2021.3084687.

[15] A. Tawileh, J. Hilton, S. McIntosh, Managing Information Security in Small and Medium Sized Enterprises: A holistic approach, In: 2007 IEEE International Conference on Information Reuse and Integration, 2007, 341-346. doi:10.1109/IRI.2007.4296638.

[16] S. Sharma, H. Sharma, A multi-criteria intelligent framework for selecting an information security management system standard using fuzzy AHP and TOPSIS methods, J. Inf. Secur. Appl., 73 (2023), 103422. doi:10.1016/j.jisa.2023.103422.

[17] M. Whitman, H. Mattord, Management of Information Security, 6th. ed., Cengage Learn., 2018.

[18] Z. Soomro, M. Shah, J. Ahmed, Information security management needs more holistic approach: A literature review, Int. J. Inf. Manag., 36 (2016), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009.

[19] N. Tuptuk, S. Hailes, Security of smart manufacturing systems, J. Manuf. Syst., 47 (2018), 93-106. doi:10.1016/j.jmsy.2018.04.007.
[20] M. Nankya, R. Chataut, R. Akl, Securing Industrial Control Systems: Components, Cyber Threat. Mach. Learn. Def. Strateg., Sensors 23 (2023). doi:10.3390/s23218840.
[21] Y. Skorenkyy, et al., Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices, CEUR Workshop Proc., 3468 (2023), 12-23.
[22] S. Fedak, Y. Skorenkyy, M. Dautaj, R. Zolotyy, O. Kramar, Digital Twins for Optimisation of Industry 5.0 Smart Manufacturing Facilities, CEUR Workshop Proc., 3628 (2023), 344-349.
[23] T. Lechachenko, Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model, CEUR Workshop Proc., 3628 (2023), 325-329.
[24] R. Kozak, et al, Cybersecurity provisioning for Industry 4.0 digital twin with AR components, CEUR Workshop Proc., 4057 (2025), 166-178.
[25] T. Saaty, What is the analytic hierarchy process?, In: Mathematical Models for Decision Support, Springer, Berlin/Heidelberg, Germany, 1988, 109-121.
[26] E. Nebati, B. Ayvaz, A. Kusakci, Digital transformation in the defense industry: A maturity model combining SF-AHP and SF-TODIM approaches, Appl. Soft Comput., 132 (2023), 109896. doi:10.1016/j.asoc.2022.109896.
[27] A. Shameli-Sendi, Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment, Open Cybern. Syst. J., 6 (2012), 26-37. doi:10.2174/1874110X01206010026.
[28] H. Gharaee, M. Agha, Designing of Multi Criteria Decision Making Model for Improve Ranking of Information Security Risks, Signal Data Process., 2 (2015), 3-14.
[29] Z. Eren-Dogu, C. Celikoglu, Information Security Risk Assessment: Bayesian Prioritization for AHP Group Decision Making, Int. J. Innov. Comput. Inf. Control. 8 (2012), 8001-8018.
[30] A. Patil, Fuzzy AHP Methodology and its sole applications, Int. J. Manag. Res. Rev. 8 (2018), 24-32.
[31] J. Krahulec, M. Jurenka, Business Impact Analysis in the Process of Business Continuity Management, Secur. Def. Q., 6 (2015), 29-36. doi:10.5604/23008741.1152450.
[32] V. Dakic, K. Premuzic, R. Petrunic, Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), In: Proceedings of the 35th DAAAM International Symposium, 2024. doi:10.2507/35th.daaam.proceedings.007.
[33] M. Whitman, H. Mattord, Principles of Information Security, 3rd. ed., Thomson Course Technol., Boston, MA, 2007.
[34] L.-E. Anica-Popa, M. Vrîncianu, I. Pugna, D.-M. Boldeanu, Addressing Cybersecurity Issues in ERP Systems — Emerging Trends, In: Proceedings of the 18th International Conference on Business Excellence, 2024, 1306-1323. doi:10.2478/picbe-2024-0108.
[35] R. Mehta, Strategic Integration of ERP and Manufacturing Information Systems: Overcoming Implementation Challenges and Driving Digital Transformation, J. Inf. Syst. Eng. Manag., 10 (2025), 835-845. doi:10.52783/jisem.v10i45s.9034.
[36] L. Wells, J. Camelio, C. Williams, J. White, Cyber-physical security challenges in manufacturing systems, Manuf. Lett. 2 (2014), 74-77. doi:10.1016/j.mfglet.2014.01.005.
[37] R. Kozak, et al., Cybersecurity issues related to incorporation of VR components into Industry 5.0 human-machine interfaces, Procedia Comput. Sci., 276 (2026), 176-184. doi:10.1016/j.procs.2026.02.022.
[38] T. Saaty, How to make a decision: The analytic hierarchy process, Eur. J. Oper. Res., 48 (1990), 9-26.
[39] M. Karpinski, O. Revniuk, D. Tymoshchuk, R. Kozak, A. Tokkuliyeva, Fuzzy logic system as a component of the web application security information system. Ceur Workshop Proc., 4042 (2025), 308-315.
[40] T. Saaty, L. Vargas, Models, Methods, Concepts & Applications of the Analytic Hierarchy Process, 2nd. ed., Springer, New York, NY (2012). doi:10.1007/978-1-4614-3597-6.