Research Article
Open Access

MJ Engineering Sciences

Available at: https://mjcellpress.com/article/mjes04/

A comprehensive hybrid mathematical, deep learning, and IoT framework for industrial IT risks anticipation

Ferdinand Fabrice Ayissi Zogo[1*], Jacques Matanga[1] and Jean François Essiben Dikoundou [1].

[1] National Higher Polytechnic School of Douala, University of Douala, P.O. Box 2701, Douala, Cameroon

[*]Corresponding author: fabriceayissi@gmail.com

Key words

IT risks anticipation, Hybrid framework, Mathematical optimization, Deep Neural Networks, IoT sensor networks, Industry 4.0, Cyberattacks.

Abstract

The fast digitalization of industrial systems, facilitated by Industry 4.0 technology, has created increasingly complex IT risks, such as cyberattacks, operational interruptions, and data breaches, all of which can have a negative impact on productivity, safety, and financial stability. Traditional risk assessment approaches frequently fall short of tackling these dynamic threats due to their reactive nature and inability to process vast amounts of real-time data. To bridge this gap, this study provides a Comprehensive Hybrid framework that combines mathematical modeling, deep learning, and IoT-driven analytics to enable proactive industrial IT risks anticipation. To evaluate possible vulnerabilities across interconnected industrial networks, the framework uses mathematical optimization techniques such as stochastic modeling, Bayesian risk assessment, and Game theory optimization. It uses Deep Neural Networks (DNN), such as Long Short-Term Memory (LSTM) and the Autoencoder for Unsupervised Anomaly identification, to analyze historical and real-time data for anomaly identification, predictive risk assessment, and adaptive threat forecasting. Additionally, distributed IoT sensor networks deliver continuous, high-resolution data streams from vital infrastructure, allowing for real-time monitoring. Through this synergistic integration, the framework improves IT risk prediction accuracy through multi-modal data fusion and adaptive learning, while maintaining data privacy via federated learning implementations. When tested on real-world datasets, the model outperformed current techniques.

Received:18.01.2025 Accepted: 26.07.2025 Published online: 11.08.2025

How to cite this article: Ayissi Zogo, F. F., Matanga, J., & Essiben Dikoundou, J. F. (2025). *A comprehensive hybrid mathematical, deep learning, and IoT framework for industrial IT risks anticipation*. *MJ Engineering Sciences*, 1(1), 48–67. https://doi.org/10.63156/mjes04

1. Introduction

Industrial ICT (Information and Communication Technology) systems are becoming increasingly vulnerable to a wide range of disruptions, including cyberattacks, sensor malfunctions, hardware degradation, and communication inefficiencies. The progressive integration of Industrial Internet of Things (IIoT) devices into legacy infrastructures has amplified exposure to sophisticated threats such as ransomware, Distributed Denial-of-Service (DDoS) attacks, and false data injection (Antonakakis et al., 2017). Additionally, sensor drift, aging hardware, and network latency further compound the reliability challenges inherent in these systems (Mo et al., 2012). Traditional risk assessment methods, which depend heavily on statistical models and rule-based anomaly detection, are often inadequate in capturing complex, dynamic threat patterns in real time.

Recent empirical research highlights the significance of these threats. In 2023, ransomware assaults in industrial sectors increased by 62%, with 75% of targeted organizations paying the ransom to avoid operational shutdowns (Dragos, 2024). According to IBM X-Force (2024) and ENISA (2024), 40–50% of industrial firms had DDoS incidents in 2024, with disruptions lasting three to six hours. False data injection attacks, including sensor spoofing, represented 18% of industrial control system (ICS) breaches and frequently bypassed conventional detection mechanisms (Dragos, 2023). According to Deloitte (2023), sensor failures alone were responsible for 23% of unscheduled industrial downtime, which led to losses of an estimated $260,000 per hour. These hazards are exacerbated by hardware deterioration in aged IIoT infrastructure, where components have an annual failure rate of 15–20% (IEEE, 2023a). Furthermore, 12% of process inefficiencies in industrial networks are caused by communication latency, which further reduces productivity (IEEE, 2023b).

In addition to technical failures, external disruptions such as power outages and natural disasters pose serious threats. Power grid failures cost the global economy approximately $150 billion annually, with industrial facilities averaging 8.5 hours of downtime per outage (World Bank, 2023). Natural disasters, especially extreme weather events, account for 40% of industrial disruptions and require an average of 72 hours for recovery (FEMA, 2023). Human error and software vulnerabilities also remain persistent risk factors; misconfigurations and unintentional data leaks cause 30% of ICS incidents (NIST, 2023), while 60% of system crashes result from unpatched firmware or software flaws (Siemens CERT, 2023).

These observations highlight significant gaps in current approaches. Traditional models, including Bayesian networks and legacy rule-based systems, fail to address the dynamic and multidimensional nature of modern threats. Notably, legacy systems are unable to detect 42% of zero-day attacks (Ponemon Institute, 2023), and existing statistical frameworks struggle with real-time adaptation in IIoT environments. To address these limitations, this research proposes a hybrid framework that integrates mathematical risk models—particularly stochastic processes—for quantifying uncertainty, deep learning architectures (LSTM/GNNs) for adaptive threat detection based on temporal sensor data, and distributed IoT analytics to facilitate real-time decision-making at the edge, thereby reducing reliance on centralized cloud systems.

The literature review underpinning this work was conducted using a systematic methodology. Key databases such as IEEE Xplore, ACM Digital Library, Scopus, and Web of Science were searched using relevant keywords. Studies were included based on their focus on deep learning and mathematical models, while purely theoretical works lacking experimental validation or those not directly applicable to industrial cybersecurity were excluded.

This paper introduces an integrated risk anticipation framework, featuring mathematical derivations for probabilistic risk assessment, including failure rate estimation and attack propagation modeling. It also provides architectural diagrams that illustrate the fusion of DNN-based anomaly detection with IoT edge computing strategies. The proposed approach is validated through case studies on industrial control systems. The structure of the paper is as follows: Section 2 presents a literature review on IT risk anticipation; Section 3 details the hybrid framework design and architecture; Section 4 describes the experimental validation; and Section 5 offers conclusions and future research directions.

2. Literature review on IT risk management

2.1 Defining Industrial ICT Risks

Industrial ICT risks encompass a wide spectrum of threats and vulnerabilities that can compromise the confidentiality, integrity, and availability of information and operational technology (OT) systems in industrial settings. These threats originate from various sources. Cybersecurity threats include malware, ransomware, phishing, denial-of-service (DoS) attacks, unauthorized access, data breaches, and insider threats. Operational failures involve hardware and software malfunctions, system errors, human mistakes, and obsolete technologies. Natural disasters, such as floods, fires, or earthquakes, can also interrupt IT/OT infrastructure. Compliance and regulatory risks stem from failing to meet industry standards and legal obligations, potentially resulting in financial penalties and reputational harm. Additionally, supply chain risks arise when third-party vendors or suppliers introduce vulnerabilities. The growing interconnectedness of IT and OT systems in modern industrial environments means that a disruption in one area can quickly cascade, resulting in physical damage, production halts, safety issues, and substantial financial losses.

2.2 The Value of Risk Prediction

Historically, industrial ICT risk management has largely been reactive, focusing on responding to events after they occur. However, due to the complex and evolving nature of these threats, a proactive and predictive approach has become essential (NIST SP 800-82, 2022). Anticipating risks allows organizations to prepare backup plans and implement mitigation strategies in advance (ISO/IEC 27001, 2022). It also enables better decision-making by prioritizing risks based on probability and impact, facilitating efficient resource allocation (Kaplan & Garrick 1981). This predictive approach enhances organizational resilience by fostering systems that can withstand and quickly recover from incidents (ENISA, 2021, 2025). Furthermore, it ensures regulatory compliance with frameworks such as the NIS Directive and GDPR (General Data Protection Regulation), and protects institutional reputation by minimizing exposure to situations that could damage public trust and competitive standing (PwC, 2023). Lastly, effective risk management supports innovation by giving organizations the confidence to pursue new technologies (World Economic Forum, 2023).

2.3 Industrial ICT Risks Taxonomy

This taxonomy organizes risks into primary categories and subcategories, based on their source, nature, and impact on industrial operations.

2.3.1 Technical Risks

Technical risks arise from vulnerabilities in the hardware, software, network infrastructure, and communication protocols used in industrial ICT systems. System and software vulnerabilities include unpatched known flaws, zero-day vulnerabilities without public patches, configuration weaknesses like default passwords or open ports, undocumented features or intentional backdoors (CISA, 2019), and programming errors such as buffer overflows or memory corruption. Network and communication protocol risks emerge from insecure legacy protocols lacking authentication or encryption (Modbus, 2012), inadequate network segmentation between IT and OT systems (IEC, 2013), vulnerabilities in wireless communication channels (ISA, 2018), denial-of-service attacks that overwhelm network resources (Dragos, 2024), and insecure remote access methods like VPNs or RDP. Hardware and device risks include physical tampering, firmware vulnerabilities that are difficult to patch, compromised hardware components from the supply chain, and devices that are end-of-life and no longer supported with security updates.

2.3.2 Operational Risks

Operational risks originate from human factors, procedures, and processes within industrial environments. Insider threats take several forms: malicious insiders intentionally sabotage systems, negligent insiders unintentionally

cause harm due to carelessness, and compromised insiders have their credentials or workstations hijacked by external actors.

2.4 Related Work

2.4.1 Threat Anticipation Techniques

Recent developments in predictive risk analysis for industrial environments have yielded several innovative techniques. Industrial threat intelligence utilizes machine learning for early detection of ICS attack patterns (Karnouskos et al., 2021). The concept of digital twins enables the simulation of cyber-physical system vulnerabilities before actual exploitation (Grieves, 2022). Attack graphs are another tool, modeling multi-stage network breaches in industrial systems (Wang et al., 2020).

2.4.2 Sector-Specific Implementations

Several sectors have adapted these predictive methods to their specific needs. In smart manufacturing, real-time anomaly detection is implemented using IIoT sensor data (Zheng et al., 2023). The energy sector applies probabilistic risk models to manage grid contingencies (Ten et al., 2021). In transportation, blockchain technologies are being used to mitigate supply chain risks (Petit et al., 2022).

2.4.3 Emerging Challenges

Despite progress, important research gaps remain. The convergence of IT and OT systems introduces unique vulnerabilities in Industry 4.0 architectures (Boyes, 2023). Human factors, particularly in operator decision-making, significantly influence system resilience (Carpenter et al., 2022). Regulatory compliance continues to be a dynamic challenge as cybersecurity standards evolve (ENISA, 2023, 2025).

2.5 Frameworks for Industrial ICT Risk Anticipation

2.5.1 ISO/IEC 27005:2022

ISO/IEC 27005:2022 stands out for its holistic integration with ISO 27001 controls (Cherdantseva Y. et al., 2016) and flexibility in supporting both qualitative and quantitative risk assessment methods (Beckers K., 2015). However, it faces limitations in practice. Small and medium-sized enterprises often struggle with its abstract and complex guidelines (Almeida R. et al., 2020), and the framework lacks mechanisms for real-time risk adaptation (Shedden P. et al., 2016).

2.5.2 ISO 31000

ISO 31000 provides a comprehensive approach to enterprise risk management, applicable across organizational types and sizes. It offers a structured process for identifying threats and opportunities, while improving resource allocation and helping organizations achieve strategic objectives (Tranchard 2018; Rampini et al. 2019). According to Solange G. (2022), it serves as a general reference for managing various types of risks based on its principles and guidelines.

2.5.3 ITIL

The IT Infrastructure Library (ITIL) framework focuses on key processes such as threat identification, vulnerability assessment, risk evaluation, and continuous monitoring. It provides a structured method for managing IT services and is widely used to establish systematic risk management practices (Wang et al., 2022).

2.5.4 OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) helps organizations identify critical IT assets and analyze associated threats and vulnerabilities. It provides a structured method for aligning risk awareness with operational objectives (Alberts and Dorofee, 2003; Caralli et al., 2007).

2.5.5 NIST Cybersecurity Framework (CSF)

The NIST CSF offers a high-level structure for cybersecurity activities through five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018, 2024). These functions help organizations align cybersecurity measures with business requirements.

2.5.6 COBIT

COBIT (Control Objectives for Information and Related Technologies), developed by ISACA, is a comprehensive IT governance framework. It ensures that IT supports business goals, delivers value, and manages associated risks effectively (ISACA, 2018).

2.5.7 FAIR

FAIR (Factor Analysis of Information Risk) is a quantitative model that enables organizations to assess and express information risk in financial terms. It complements qualitative frameworks and enhances decision-making (Jones and Freund, 2018; ISACA, 2021).

2.5.8 IEC 62443 Series

IEC 62443 is an international standard developed specifically for the security of industrial automation and control systems (IACS). It addresses secure system design, operational security, and various other facets of industrial cybersecurity (IEC, 2021; Stouffer et al., 2015, 2023).

2.6 Comparison of Current ICT Risk Management Standards

The table 1 presents a comparative overview of major ICT risk management frameworks, highlighting their key focus areas, advantages, limitations, and corresponding references. This synthesis aims to guide the selection or integration of appropriate standards based on organizational needs and industrial contexts.

Table 1: Comparison of Risk Management Frameworks

Framework/Key Focus	Advantages	Gaps/Limitations	Key References
COBIT 2019 IT governance & management	• Holistic alignment with business goals • Strong process controls • Integrates with other frameworks	• Less prescriptive on technical controls • Complex implementation • Requires customization	ISACA (2018). COBIT 2019 Framework
ISO/IEC 27005 Information security risk management	• Compatible with ISO 27001 • Structured risk assessment process • International standard	• Primarily qualitative • Requires industry customization • Less financial focus	ISO/IEC (2018). ISO/IEC 27005:2018
ITIL 4 IT service management	• Integrates risk into service lifecycle • Widely adopted standard • Practical implementation guidance	• Less financial quantification • Requires customization • Limited security detail	AXELOS (2019). ITIL 4 Foundation
OCTAVE Operational risk assessment	• Asset-centric approach • Practical threat modeling • Good for security issues	• Resource intensive • Less financial quantification • Limited scalability	Alberts & Dorofee (2002). OCTAVE Approach
FAIR Quantitative risk analysis	• Financial risk quantification • Prioritizes data-driven decisions • Strong for cyber risk	• Requires significant data • High setup effort • Limited adoption	The Open Group (2018). FAIR Standard
ISO 31000 Enterprise risk management	• Generic principles for all industries • Holistic integration with other standards • Aligns with wider stakeholder interests	• Lacks prescriptive methods • No specific implementation support	ISO (2018). ISO 31000:2018

IEC 62443 Industrial systems risk management	• Tailored for ICS (Industrial Control Systems) • Detailed security lifecycle guidance • Widely adopted in industry	• Limited outside ICS context • Complex implementation	IEC (2019). IEC 62443 Security Series
NIST CSF Cybersecurity framework	• Risk-based approach • Aligns with NIST SP 800-53 • Modular and flexible	• Voluntary implementation • Requires mapping to other standards	NIST (2018). Framework v1.1

2.7 The causes of ICT risks

The causes of ICT risks can vary depending on the specific context, but several common contributing factors are widely recognized across industries and systems.

2.7.1 Cyber security threats

Cybersecurity threats refer to malicious actions that compromise the availability, confidentiality, or integrity of ICT systems. These include malware such as viruses, worms, and ransomware, which are designed to disrupt or damage systems (Symantec, 2023). Phishing represents another significant threat, involving social engineering attacks that deceive users into disclosing sensitive information (Verizon, 2023). Denial-of-Service (DoS) attacks, which overwhelm systems with illegitimate traffic, render them inaccessible to legitimate users (Kaspersky, 2023). Insider threats—whether malicious or due to negligence—are also critical, stemming from employees, contractors, or partners with access to sensitive systems or data (CERT, 2022).

2.7.2 Human error

Human error is a major cause of ICT risks, often resulting from insufficient training, lack of awareness, or failure to follow best practices. Misconfiguration occurs when systems, networks, or applications are improperly configured, leaving them vulnerable to exploitation (Gartner, 2022). Weak passwords, such as easily guessable credentials or the reuse of passwords across accounts, further expose systems (NIST, 2020). Accidental data deletion, the unintended removal of critical information or files, is another form of human error (IBM Security, 2023). Noncompliance with protocols, such as neglecting to use multi-factor authentication or failing to encrypt sensitive data, also increases risk (ISO/IEC 27001, 2022).

2.7.3 Economic and Geopolitical Factors

External economic and geopolitical conditions significantly influence ICT risk landscapes. During financial crises, organizations may reduce budgets for cybersecurity and ICT maintenance, thereby increasing vulnerability (World Economic Forum, 2023). Geopolitical tensions often trigger a surge in cyberattacks, particularly during periods of instability or political conflict (FireEye, 2023). Additionally, global supply chain disruptions can delay or restrict access to critical ICT components, affecting system reliability (McKinsey, 2023).

2.7.4 Emerging Technologies

While the adoption of new technologies can offer numerous benefits, it may also introduce unforeseen risks. In cloud computing, for example, misconfigured services or reliance on third-party providers with weak security can lead to vulnerabilities (CSA, 2023). The Internet of Things (IoT) offers serious security concerns, as studies show most devices ship with insecure defaults (e.g., hardcoded credentials) and lack update mechanisms, making them perfect targets for botnets and network breaches (NIST, 2020). Artificial Intelligence (AI) systems, if based on flawed or biased algorithms, can lead to incorrect decisions with serious consequences (MIT Technology Review, 2023). Similarly, blockchain technology carries risks related to smart contract flaws and private key management (Nakamoto, 2008).

2.7.5 External Threats

External threats originate outside the organization and are often beyond direct control. Hackers, whether individuals or groups, exploit system vulnerabilities to gain unauthorized access to data and infrastructure (McAfee, 2023). Nation-state actors, including state-sponsored cyber espionage and sabotage units, pose significant risks to critical systems (FireEye, 2023). Natural disasters such as floods, earthquakes, or fires can severely damage infrastructure and disrupt operations (FEMA, 2022). Supply chain attacks involve compromising third-party vendors or service providers to infiltrate the target organization's systems (NIST, 2021).

2.7.6 Regulatory and Compliance Issues

Organizations that violate laws, regulations, or industry standards face legal, financial, and reputational consequences. Data privacy violations, such as failing to protect personal data in line with frameworks like GDPR or CCPA, expose firms to substantial penalties (GDPR.EU, 2023). A lack of auditing processes means organizations may fail to detect noncompliance with security policies (ISO/IEC 27001, 2022). Moreover, inadequate incident reporting—such as not informing regulatory authorities or affected users of breaches—can worsen the impact of security incidents (HIPAA, 2023).

2.7.7 Operational Failures

Operational failures stem from poor internal management or inadequate operational procedures. For instance, the absence of redundancy—i.e., failure to install backup systems—can result in complete service outages during system failures (AXELOS, 2021). Poor change management, such as deploying untested updates or modifications, may introduce new system vulnerabilities or disruptions (ISACA, 2022). Inadequate monitoring delays the detection of anomalies or intrusions, increasing the risk of prolonged exposure (SANS, 2023). Furthermore, resource constraints, such as limited budgets or staffing shortages, reduce an organization's ability to maintain and secure ICT systems (Gartner, 2023).

2.7.8 Technical Vulnerabilities

Technical vulnerabilities refer to flaws within software, hardware, or networks that can be exploited by attackers or lead to systemic failure. Software bugs—errors in programming—may result in crashes, data corruption, or security flaws (Anderson, 2020). Unpatched systems that lack timely updates remain exposed to known vulnerabilities (ENISA, 2022). Weak encryption protocols increase the risk of data interception or theft (Schneier, 2015). Legacy systems that are outdated and no longer supported amplify the risk of exploitation or failure (Ross et al., 2021).

2.7.9 Non-material sabotage

Non-material sabotage, especially intellectual sabotage, involves intentional alteration, corruption, or destruction of digital assets such as software programs, data, or backup files (Parker, 1998). The consequences can be just as, or even more, severe than physical sabotage, leading to prolonged downtime, financial loss, and reputational harm (Schneier, 2004). Forms of non-material sabotage include unauthorized program modifications that cause malfunctions or breaches (Pfleeger & Pfleeger, 2015). Trojan horses, disguised as legitimate applications, perform harmful actions unbeknownst to users (Cheswick, Bellovin, & Rubin, 2003). Logic bombs are malware triggered under specific conditions, often corrupting databases gradually and eluding detection until recovery becomes complex and costly (Bishop, 2005). Viruses and worms, which are self-replicating, can spread rapidly across networks and act like logic bombs with propagation mechanisms, especially via the internet and email (Zeltser, 2021). Spyware, installed without user knowledge from deceptive websites, steals sensitive data and is difficult to detect (Stallings & Brown, 2018).

2.7.10 Hijacking of software

Despite recent successes in prosecuting software piracy and the reduced attractiveness of illegal copying due to lower prices, the practice remains prevalent (BSA, 2023; Siwek, 2022). Companies caught using pirated software face serious penalties. These include being forced to purchase the missing licenses, pay compensation that may reach up to 200% of the license value (WIPO, 2021), and cover procedural costs such as court, bailiff, and expert witness fees (OECD, 2020).

2.7.11 Dismissals for operational reasons, strikes

Ensuring fair and respectful treatment of employees is essential, as mistreatment can fuel resentment and result in retaliatory actions, including breaches of the company's information system (Kelloway et al., 2022; Spector and Fox, 2005). The sudden unavailability of key personnel—due to strikes or dismissals—can also render systems inoperable, affecting the company's entire operational chain (Pfeffer, 2010; Herath and Rao, 2009).

2.8 The process of identifying an IT risk

IT risk identification is the systematic process of recognizing potential threats to an organization's information systems, data, and infrastructure. This process typically begins with asset inventory, which catalogs critical systems and data, followed by detailed threat and vulnerability assessments designed to identify potential attack vectors or weaknesses (Stoneburner et al., 2002; NIST SP 800-30). Risk frameworks such as ISO/IEC 27005 or COBIT are widely used to evaluate risks including cyberattacks, system failures, and data breaches (ISACA, 2018). The identification process is often complemented by stakeholder interviews, historical event analysis, and the use of risk matrices, which help prioritize risks based on their likelihood and potential impact (FAIR Institute, 2021). Continuous monitoring is also essential, ensuring that emerging threats, such as zero-day exploits or regulatory changes, are detected and managed in a timely manner.

2.8.1 ICT risk assessment

ICT risk assessment relies on various mathematical equations to quantify and evaluate potential risks. A fundamental expression, adopted by frameworks such as NIST SP 800-82 and IEC 62443, defines overall risk as:

$$Risk = Threat \times Vulnerability \times Impact \quad (1)$$

In this equation, Threat represents the likelihood of a cyberattack, Vulnerability indicates a weakness within the system, and Impact refers to the potential consequences of a successful attack.

Quantitative risk assessment models, as outlined in NIST SP 800-30 (2012), include the Annualized Loss Expectancy (ALE), which estimates expected annual losses based on two key factors:

$$ALE = ARO \times SLE \quad (2)$$

Here, SLE (Single Loss Expectancy) represents the financial cost of a single incident, while ARO (Annualized Rate of Occurrence) is the expected number of such incidents per year.

Threat likelihood estimation, as described in ISO/IEC 27005 (2022), is often performed using Bayesian networks. These probabilistic models calculate the likelihood of an attack based on evidence and prior probabilities. The Bayesian equation is expressed as:

$$P\,(Attack|Evidence) = \frac{P\,(Evidence|Attack)}{P\,(Attack)} \quad (3)$$

In this expression, *P(Attack)* represents the prior probability of an attack, while *P(Evidence|Attack)* is the likelihood of observing specific indicators if an attack has occurred. This approach enables adaptive and probabilistic estimation of threats based on current and historical information.

3 Innovative Hybrid Approach Addressing the Shortcomings of Existing Methods

This section introduces a hybrid approach designed to overcome the limitations of traditional risk assessment frameworks by combining mathematical modeling techniques with adaptive learning algorithms. It begins with mathematical foundations, including stochastic processes, Bayesian reasoning, and game-theoretic defense strategies to model, infer, and optimize cybersecurity decisions under uncertainty.

3.1 Mathematical Modeling

3.1.1 Stochastic Risk Assessment

Industrial ICT risks can be effectively represented using stochastic processes, where threat events occur at random over time. Let R(t) denote the total risk at time t, which can be modeled as a compound Poisson process, capturing both the random arrival of threats and the variability in their severity. This process is defined as:

$$R(t) = \sum_{l=1}^{N(t)} X_i \qquad (4)$$

Here, N(t) is a Poisson counting process that represents the number of threat arrivals up to time t, with rate λ, and X_i represents the random severity or impact of the i-th threat. The expected value of the risk over time is given by:

$$\mathbf{E}[R(t)] = \lambda t \mathbf{E}[X_i] \qquad (5)$$

3.1.2 Bayesian Risk Assessment

Bayesian modeling enables probabilistic reasoning under uncertainty by leveraging prior knowledge and observed data. The risk variables in a cyber-physical system can be represented through a joint distribution, which is factorized as (6):

$$P(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} P(X_i | P_a(X_i)) \qquad (6)$$

To compute the posterior probability P(Q|E) where Q is a query variable and E is observed evidence, the following steps are used:

1. Multiply conditional probability tables:

$$\phi = \prod_{i=1}^{n} P(X_i | P_a(X_i)) \qquad (7)$$

2. Marginalize hidden variables H:

$$\phi'(Q, E) = \sum_{l=1} \phi(Q, E, H) \qquad (8)$$

3. Normalize:

$$P(Q|E) = \frac{\phi'(Q,E)}{\sum_Q \phi'(Q,E)} \quad (9)$$

This inference process is mathematically rigorous but computationally intensive, with complexity exponential in the treewidth of the moralized graph associated with the Bayesian network. Nonetheless, it provides a powerful mechanism for incorporating real-time evidence into the assessment of cyber risk.

3.1.3 Game-Theoretic Defense Optimization

In the context of industrial cybersecurity, game-theoretic models offer a powerful framework for modeling interactions between attackers and defenders. One such approach is the Stackelberg game formulation, where strategic decisions are made sequentially. In

s model, the defender acts as the leader and selects a patching frequency δ, while the attacker, acting as the follower, chooses an exploit time τ in response.

The defender's utility function reflects the trade-off between patching costs and potential losses from successful attacks. It is defined as:

$$U_d(\delta,\tau) = -C_d\delta - L.\mathrm{I}(\tau < \delta^{-i}) \quad (10)$$

Here, c_d denotes the cost per unit of patching frequency, L represents the loss incurred if the attack occurs before the next patch, and I is the indicator function evaluating whether the condition $\tau < \delta^{-1}$ holds.

To determine the Nash equilibrium, the game is solved through backward induction. This involves two steps:

1. The attacker's best response is computed by minimizing their utility with respect to the defender's chosen strategy:

$$\tau^*(\delta) = argmin_\tau U_a(\delta,\tau) \quad (11)$$

2. The defender's optimal strategy is then found by maximizing their utility, considering the attacker's best response:

$$\delta^* = argmax_\delta U_d(\delta,\tau^*(\delta)) \quad (12)$$

In this setup, both players act rationally to optimize their respective outcomes. Under certain assumptions, a closed-form solution for the optimal patching frequency can be derived, given by:

$$\delta = \sqrt{\frac{C_a}{C_d}} \quad (13)$$

This expression balances the attacker's cost *ca* against the defender's patching cost *cd* offering a theoretically grounded guideline for optimal defense scheduling in adversarial settings.

3.2 Deep Neural Network (DNN) for Anomaly Detection

3.2.1 LSTM for Temporal Risk Prediction

Long Short-Term Memory (LSTM) networks are well-suited for capturing sequential dependencies in time-series data, such as sensor streams found in industrial ICT systems. These networks are particularly effective for temporal risk prediction because they retain long-term information and can selectively forget irrelevant inputs. The core operations of an LSTM cell are governed by a set of equations that control the flow of information through various gates and states.

The LSTM cell equations are defined as follows:

$$\begin{cases} f = \sigma(x_t U^f + s_{t-1} W^f) & (14) \\ i = \sigma\left(x_t U^i + s_{t-1} W^i\right) & (15) \\ o = \sigma(x_t U^o + s_{t-1} W^o) & (16) \\ g = \tanh(x_t U^g + s_{t-1} W^g) & (17) \\ c_t = c_{t-1} \circ f + g \circ i & (18) \\ s_t = \tanh(c_t) \circ o & (19) \\ y = softmax(V s_t) & (20) \end{cases}$$

where:

- f: Forget gate input, and output gates.
- i: input gate
- o: output gate
- g: self-recurrent
- c_t: Cell state.
- s_t: Hidden state (used for risk prediction).

3.2.2 Autoencoder for Unsupervised Anomaly Detection

An autoencoder is a type of neural network used to learn compressed representations of input data and reconstruct them with minimal error. An autoencoder reconstructs input x as $\hat{x}$, minimizing reconstruction error:

$$L = ||x - \hat{x}||_2^2 \quad (21)$$

An anomaly is flagged when when $L > \tau$ (threshold), indicating that the input deviates significantly from the learned normal patterns.

3.3 IoT Sensor Network Analytics

3.3.1 Graph-Based Risk Propagation

In industrial IoT systems, sensors and their interconnections can be modeled as a graph G = (V, E), where V represents the set of nodes (i.e., sensors) and E represents the edges corresponding to communication links

between them. Risk propagation across the network is governed by the adjacency matrix A, and the Laplacian matrix is defined as L = D − A, where D is the degree matrix.

The dynamics of risk diffusion over the network follow a partial differential equation that accounts for the influence of neighboring nodes and local risk. This diffusion is described by:

$$\frac{\partial R_i(t)}{\partial \mathrm{t}} = \alpha \sum_{j \in N(i)} A_{ij} \left(R_j(t) - R_i(t) \right) + \beta . Local\ Risk \qquad (22)$$

3.3.2 Federated Learning for Privacy-Preserving Risk Modeling

To preserve data privacy while still enabling collaborative learning, sensors can participate in federated learning. In this approach, each sensor trains a local deep neural network (DNN) model without sharing raw data. Instead, model updates are exchanged and aggregated to update a shared global model. Let W_t represent +the global model at round t; the update rule for the next round is:

$$W_{t+1} = W_t + \nu \sum_{k=1}^{K} \frac{\eta_k}{N} \nabla L_k(W_t) \qquad (23)$$

where:

• K: Number of sensors.
• L_k: Loss at sensor k.

3.4 Integration & Risk Prediction

The final risk score is computed by integrating multiple sources of information to produce a comprehensive and reliable assessment. Specifically, the integration combines three components: the stochastic risk component $R_{stoch}(t)$, which models random threat behavior over time; the DNN-based anomaly score $R_{DNN}(t)$ which captures temporal anomalies using deep learning; and the graph-based risk $R_{graph}(t)$, which reflects spatial propagation of risk across IoT sensor networks.

These three components are linearly combined into a single risk prediction model:

$$R_{final}(t) = \alpha R_{stoch}(t) + \beta R_{DNN}(t) + \gamma R_{graph}(t) \qquad (24)$$

The coefficients α, β, and γ are weights assigned to each risk source, and they are constrained such that α+β+γ=1. These weights are not arbitrarily chosen but are instead optimized using reinforcement learning techniques to improve the model's accuracy and adaptability.

3.5 Why an Innovative Hybrid Approach (Mathematical + Deep Learning + IoT) is Essential for Industrial IT Risk Anticipation?

3.5.1 The Hybrid Advantage

A hybrid approach that combines mathematical modeling, deep neural networks, and IoT integration offers complementary strengths that enhance industrial IT risk anticipation capabilities.

a) Mathematical Modeling

One of the main strengths of mathematical modeling is its ability to provide interpretable risk quantifications. These models can yield structured, explainable insights that are directly applicable in industrial contexts. Their formalism allows for rigorous reasoning about threats and vulnerabilities, which is essential for critical decision-making processes in industrial environments.

b) Deep Neural Networks

Deep neural networks excel in detecting unknown attack patterns within high-dimensional data. This capacity to identify previously unseen anomalies makes them particularly powerful for modern cybersecurity applications. Moreover, these models can also be applied in industrial settings where complex and voluminous sensor data are prevalent. Their strength lies in their adaptability and learning ability in the presence of dynamic threats. It is worth reiterating that their key advantage is the detection of unknown attack patterns in high-dimension data.

c) IoT Integration

IoT integration brings the ability to monitor the physical state of systems in real time. This capability is vital for anticipating risks that manifest through environmental or mechanical changes. Real-time data from IoT devices can be directly leveraged to prevent physical damages and react proactively. Such integration is feasible and practical within industrial infrastructures, especially for applications requiring immediate responses.

The practical benefit of this hybrid approach is illustrated in Figure 1, which shows how vibration sensors and an edge machine learning model are used to detect anomalies in real time. If an anomaly is detected, the system triggers a security protocol; otherwise, monitoring continues uninterrupted. This demonstrates the system's ability to prevent equipment damage by identifying malicious motor overloads as they happen.

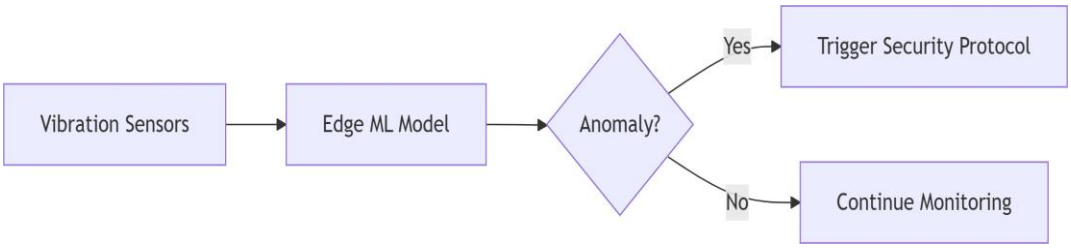

Figure 1: Prevented equip

ment damage by detecting malicious motor overloads in realtime

4. Experimental validation

4.1 Data Collection

The dataset used for simulation, titled *Cyber-Threat-Intelligence-Custom-Data_new_processed.CSV*, is a structured compilation of cybersecurity-related data. It likely includes critical features such as threat indicators, timestamps, attack types, and system logs, all of which are essential for analyzing and simulating industrial ICT risks.

The selection of this data source is justified on two grounds. First, in terms of real-world relevance, honeypots—used to generate parts of the dataset—are effective in capturing actual attack patterns observed in

industrial environments, as noted by Pa et al. (2016). This ensures that the simulated threats reflect realistic and practical conditions encountered in operational systems.

Second, the dataset addresses bias mitigation by incorporating synthetic data to supplement rare attack categories, such as false data injection. This inclusion helps prevent class imbalance during model training and evaluation, which is a common challenge in cybersecurity datasets with highly skewed class distributions. The integration of synthetic instances for underrepresented attacks is supported by the work of Torres et al. (2021), which highlights the value of such data augmentation strategies in improving model robustness.

4.2.1 DDoS Detection Performance

Below, we have the DDoS detection performance coding and figure (figure 2):

```
print('\n_DDoS_Detection_Performance_\n')
print(classification_report(y_test, y_pred, target_names=['Normal', 'DDoS']))
print(f'Optimal_Threshold:{optimal_threshold:.3f}')
print(f'AUG-ROC:{auc(fpr, tpr):.3f}')
```

As presented in figure 2, the classification report indicates that for the 'Normal' class, precision is 1.00, recall is 0.87, and the F1-score is 0.93, based on 121,541 samples. For the 'DDoS' class, precision is 0.91, recall is 0.91, and the F1-score is 0.82, across 287 samples. Overall accuracy is 0.87. The macro average scores are 0.51 (precision), 0.89 (recall), and 0.42 (F1-score), while the weighted averages are 1.00, 0.87, and 0.93. The optimal threshold is 0.265, and the AUC-ROC is 0.953.

```
                precision    recall  f1-score   support

       Normal       1.00      0.87      0.93    121541
         DDoS       0.01      0.91      0.02       207

     accuracy                           0.87    121748
    macro avg       0.51      0.89      0.48    121748
 weighted avg       1.00      0.87      0.93    121748

Optimal Threshold: 0.265
AUC-ROC: 0.953
```

Figure 2: DDoS Detection Performance.

4.2.2 Confusion Matrix

The confusion matrix for the DDoS detection model is presented using the following code and corresponding figure (figure 3):

```
# Confusion Matrix
plt.figure(figsize=(6,5))
sns.heatmap(confusion_matrix(y_test, y_pred),
        annot=True, fmt='d', cmap='Blues',
        xticklabels=['Pred_Normal', 'Pred_DDoS'],
        yticklabels=['True_Normal', 'True_DDoS'])
```

```
plt.title('Confusion Matrix')
plt.show()
```

The resulting matrix shows that out of the 121,541 normal instances, 105,982 were correctly classified and 15,559 were misclassified as DDoS. For the 207 DDoS instances, 188 were correctly detected, while 19 were misclassified as normal. These results are visualized in Figure 3.

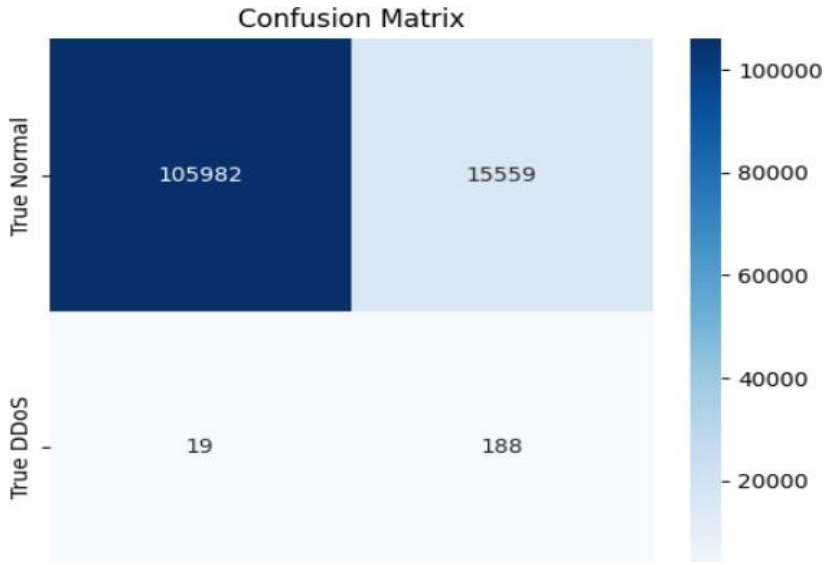

Figure 3: The confusion Matrix

4.2.3 The ROC Curve

Below is the code used to generate the ROC curve for DDoS detection, along with the corresponding figure (figure 4).

```
# ROC Curve code
plt.figure(figsize=(8,6))
plt.plot(fpr, tpr, color='darkorange', lw=2,
      label='ROC Curve (AUC={:.2f})'.format(auc(fpr, tpr)))
plt.plot([0, 1], [0, 1], color='navy', lw=2, linestyle='--')
plt.xlabel('False Positive Rate')
plt.ylabel('True Positive Rate')
plt.title('ROC_Curve_for_DDoS_Detection')
plt.legend(loc='lower right')
plt.show()
```

As shown in Figure 4, the ROC curve illustrates the model's ability to distinguish between normal and DDoS traffic. The curve bows significantly toward the upper-left corner, indicating strong performance. The area under the curve (AUC) is approximately 0.95, confirming high classification effectiveness.

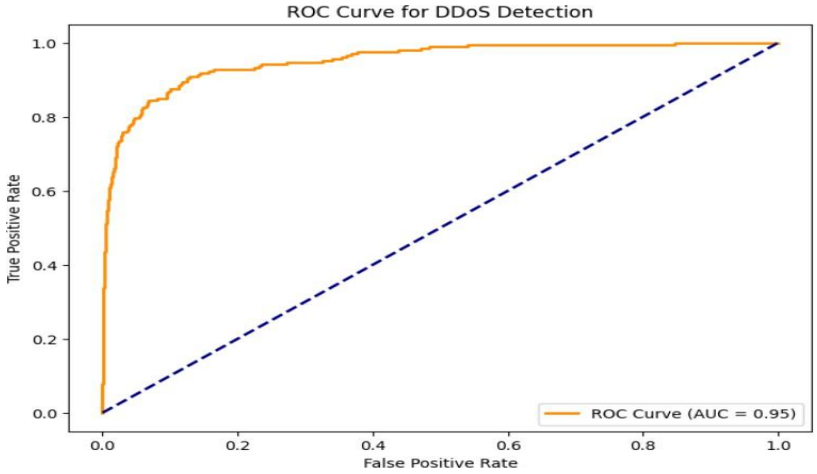

Figure 4: ROC Curve for DDOS detection

5 Conclusion and Future Perspectives

This paper has introduced a comprehensive hybrid framework that combines mathematical modeling, deep learning techniques, and IoT-edge computing to effectively address the pressing challenge of industrial ICT risk anticipation. By integrating these three dimensions, the proposed approach establishes a strong link between theoretical constructs and practical industrial applications. The resulting solution is scalable, adaptive, and well-suited for safeguarding Industry 4.0 infrastructures against evolving cyber-physical threats.

Looking ahead, several perspectives are envisaged to enhance the framework's robustness and applicability. One direction involves integrating interpretability modules to ensure compliance with regulatory standards, particularly in critical infrastructure sectors. Another avenue is the adoption of post-quantum cryptographic protocols, aligned with NIST recommendations, to counteract emerging computational threats. Additionally, privacy-preserving mechanisms for threat intelligence sharing can be developed using blockchain-secured federated learning, fostering secure collaboration among industrial stakeholders.

Financial supports

No funds, grants or other financial support was received to conduct this study or to prepare the manuscript.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Alberts, C., & Dorofee, A. (2003). *Managing information security risks: The OCTAVE approach*. Carnegie Mellon University, Software Engineering Institute.
2. Almeida, R., et al. (2020). *SME challenges in adopting ISO 27005*. *Journal of Information Security*.
3. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
4. Antonakakis, M., April, T., Bailey, M. D., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017, August). *Understanding the Mirai botnet*. In *Proceedings of the 26th USENIX Security Symposium* (pp. 1093–1110). USENIX Association.
5. AXELOS. (2019). *ITIL 4 foundation: ITIL 4 edition*. The Stationery Office.
6. AXELOS. (2021). *ITIL 4: High-velocity IT (HVIT)*. The Stationery Office.
7. Beckers, K. (2015). *Patterns for information security risk assessment*. Springer.
8. Bishop, M. (2005). *Introduction to computer security*. Addison-Wesley.
9. Boyes H (2023). Cybersecurity for industry 4.0. *Springer*.

10. BSA | The Software Alliance. (2023). *Global software survey: Security risks of unlicensed software*. https://www.bsa.org/reports/bsa-global-software-survey-the-compliance-gap
11. Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007, May 1). *Introducing OCTAVE Allegro: Improving the information security risk assessment process* (Technical Report CMU/SEI-2007-TR-012). Software Engineering Institute, Carnegie Mellon University. https://doi.org/10.1184/R1/6574790.v1
12. Carpenter, G., Woods, D. D., & Hollnagel, E. (2022). Human-centric cybersecurity for critical infrastructure.
13. CERT Division. (2022). *Insider threat guide for critical infrastructure*. Carnegie Mellon University.
14. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of information security risk management standards. *Computers & Security, 65*, 92–110. https://doi.org/10.1016/j.cose.2016.01.008
15. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker* (2e éd.). Addison-Wesley Professional. ISBN 978-0-201-63466-2
16. Cloud Security Alliance (CSA). (2023). *Top threats to cloud computing: The egregious 11*. CSA.
17. Cybersecurity and Infrastructure Security Agency (CISA). (2019). *Cybersecurity and Infrastructure Security Agency regulatory guidance*. Retrieved from https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/laws-and-regulations/cybersecurity-and-infrastructure-security-agency-guidance
18. Deloitte. (2023). *Industrial IoT downtime cost analysis: Sensor failures and operational impacts*.
19. Dragos, Inc. (2023). *Global ICS cyber threat report* [OT Cybersecurity Year in Review report]. Retrieved from https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/
20. Dragos. (2024). *2024 ICS/OT threat landscape report*. Dragos Inc.
21. ENISA. (2022). *Threat landscape for supply chain attacks*. European Union Agency for Cybersecurity.
22. ENISA. (2024). *Threat landscape for industrial automation systems: DDoS impact analysis*.
23. European Union Agency for Cybersecurity (ENISA). (2021, October). *ENISA Threat Landscape 2021: Analysis of cybersecurity threats across Europe from April 2020 to mid-July 2021*. ENISA. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
24. European Union Agency for Cybersecurity (ENISA). (2023). *Good practices for ICS security*. Publications Office of the European Union.
25. European Union Agency for Cybersecurity (ENISA). (2025). *NIS2 Technical Implementation Guidance: On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures* (Version 1.0). Publications Office of the European Union. ISBN 978-92-9204-704-7. https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
26. European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Official Journal of the EU.
27. FAIR Institute. (2021). *Factor Analysis of Information Risk (FAIR) overview*. FAIR Institute. Retrieved [date you accessed it], from https://www.fairinstitute.org/what-is-fair
28. Federal Emergency Management Agency (FEMA). (2022). *Natural hazards and disaster risk reduction*. U.S. Department of Homeland Security.
29. Federal Emergency Management Agency (FEMA). (2023). *Business disruption statistics report 2023 (FEMA P-214 7)*. U.S. Department of Homeland Security.
30. FireEye. (2023). *M-Trends 2023: State-sponsored cyber operations*. Mandiant.
31. Gartner. (2022). *Top security and risk management trends*.
32. Gartner. (2023). *Top security and risk management trends for OT*.
33. Grieves, M. (2022). *Digital twins: Bridging physical and cyber systems for threat modeling*. Springer Nature.
34. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6
35. IBM Security X-Force. (2024). *Threat intelligence index 2024: DDoS trends in critical infrastructure*. Retrieved from https://www.ibm.com/security/xforce/threat-intelligence
36. IBM Security. (2023). *Cost of a data breach report 2023: Critical infrastructure sector analysis*. IBM Security.
37. IEEE Internet of Things Journal. (2023a). *Hardware reliability in aging IIoT deployments: A longitudinal study*.
38. IEEE Internet of Things Journal. (2023b). *Latency-induced inefficiencies in industrial edge networks*.
39. International Electrotechnical Commission (IEC). (2013). *IEC 62443-3-3: Security for industrial automation and control systems*. International Electrotechnical Commission.
40. International Electrotechnical Commission (IEC). (2019). *IEC 62443 series: Industrial communication networks – Network and system security*.

41. International Electrotechnical Commission (IEC). (2021). *IEC 62443 series: Industrial communication networks – Network and system security*. IEC.
42. International Electrotechnical Commission. (2021). *IEC 62443 series: Industrial communication networks*. Carnegie Mellon University, Software Engineering Institute.
43. International Organization for Standardization & International Electrotechnical Commission. (2022, October). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection: Guidance on managing information security risks* (4e édition). ISO/IEC.
44. International Organization for Standardization & International Electrotechnical Commission (ISO/IEC). (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022)*. https://www.iso.org/standard/82875.html
45. International Organization for Standardization (ISO). (2018). *ISO 31000:2018 – Risk management – Guidelines*.
46. International Society of Automation & International Electrotechnical Commission (ISA/IEC). (2018). *ISA/IEC 62443-4-2: Technical security requirements for IACS components*.
47. IoT Security Foundation. (2023). *IoT security compliance framework*. IoTSF.
48. ISACA. (2018, November 14). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.
49. ISACA. (2021.). *COBIT 2019 and FAIR: Integrating risk management into IT governance*. ISACA.*https://www.isaca.org*.
50. ISACA. (2022). *COBIT 2019 framework: Governance and management objectives*. ISACA.
51. ISO/IEC. (2018). *ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management*. International Organization for Standardization.
52. Jones, J., & Freund, J. (2018). *Measuring and managing information risk: A FAIR approach*. Butterworth-Heinemann.
53. Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x
54. Karnouskos, S., et al. (2021). *AI-based cyber threat intelligence for industrial environments*. *Computers & Security, 103*, 102196.
55. Kaspersky. (2023). What is a DDoS attack? *Kaspersky Resource Center*. Retrieved from https://www.kaspersky.com/resource-center/threats/ddos-attacks
56. Kelloway, E. K., et al. (2022). Workplace revenge and its consequences. *Journal of Organizational Behavior, 43*(3), 345–361.
57. McAfee. (2023). *Cybercrime in 2023: The underground economy and emerging threats*. McAfee LLC.
58. McKinsey & Company. (2023). *Global supply chain decoupling: Risks and responses*. McKinsey.
59. MIT Technology Review. (2023). *The dark side of AI: Bias and unexplainability in machine learning*.
60. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012, January). *Cyber-Physical Security of a Smart Grid Infrastructure*. *Proceedings of the IEEE, 100*(1), 195–209. https://doi.org/10.1109/JPROC.2011.2161428
61. Modbus Organization. (2012). *Modbus Application Protocol Specification (MBAP)*. Retrieved from https://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf
62. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.org.
63. National Institute of Standards and Technology (NIST). (2012). *Guide for conducting risk assessments (SP 800-30 Rev. 1)*. NIST.
64. National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology.
65. National Institute of Standards and Technology (NIST). (2020). *NISTIR 8259: Foundational cybersecurity activities for IoT device manufacturers*. National Institute of Standards and Technology.
66. National Institute of Standards and Technology (NIST). (2021). *Cybersecurity supply chain risk management (NIST SP 800-161 Rev. 1)*.
67. National Institute of Standards and Technology. (2022). *Guide to Operational Technology (OT) security* (Draft of NIST SP 800-82 Rev. 3). NIST. (csrc.nist.gov)
68. National Institute of Standards and Technology. (2024). *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard* (Federal Information Processing Standard 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203
69. Netscout. (2024). *DDoS threat intelligence report 2024*. Netscout Systems, Inc. https://www.netscout.com/threatreport
70. Organisation for Economic Co-operation and Development. (2020). *Piracy and counterfeit goods trade: Economic and legal implications*. OECD Publishing. https://doi.org/10.1787/9789264252653-en

71. Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons.
72. Petit, J., Kubler, S., Le Traon, Y., & Främling, K. (2022). Blockchain-based solutions for mitigating risks in transportation supply chains: A systematic literature review. *Transportation Research Part E: Logistics and Transportation Review, 163*, 102747.
73. Pfeffer, J. (2010). *Power: Why some people have it—and others don't*. Harper Business.
74. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing* (5th ed.). Pearson.
75. Ponemon Institute. (2023). *The state of legacy system security in industrial environments*. Ponemon Institute LLC.
76. PwC. (2023). *Global digital trust insights 2023*. PricewaterhouseCoopers. Retrieved from https://www.pwc.ch/en/insights/cybersecurity/global-digital-trust-2023.html
77. Rampini, A. A., Viswanathan, S., & Vuillemey, G. (2019). Risk management in financial institutions. *The Journal of Finance, 74*(5), 2177-2219.
78. Ross, R., et al. (2021). *NIST SP 800-82 Rev. 3: Guide to industrial control systems (ICS) security*. NIST.
79. SANS Institute. (2023). *ICS monitoring: Detecting threats in critical infrastructure*. SANS.
80. Schneier, B. (2004). *Secrets and lies: Digital security in a networked world*. Wiley.
81. Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (20th Anniversary ed.). Wiley.
82. Shedden, P., et al. (2016). *Static vs. dynamic risk frameworks*. *ACM Computing Surveys*.
83. Siemens CERT. (2023). *Vulnerability statistics for industrial firmware and software (CERT Report 2023-042)*.
84. Siwek, S. E. (2022). *The true cost of software piracy to the global economy*. Institute for Policy Innovation. Retrieved from https://www.ipi.org/ipi_issues/detail/the-true-cost-of-copyright-industry-piracy-to-the-us-economy
85. Solange, G. (2022). Beyond compliance: Adaptive risk management using ISO 31000 in cyber-physical systems. *Journal of Risk Research, 25*(3), 287-305.
86. Spector, P. E., & Fox, S. (2005). The stressor-emotion model of counterproductive work behavior. In S. Fox & P. E. Spector (Eds.), *Counterproductive work behavior: Investigations of actors and targets* (pp. 151–174). American Psychological Association. https://doi.org/10.1037/10893-007
87. Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson..
88. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30
89. Stouffer, K. A., Pease, M., Tang, C. Y., Zimmerman, T., Pillitteri, V. Y., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023, September). *Guide to Operational Technology (OT) Security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3
90. Stouffer, K. A., Pillitteri, V. Y., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication 800-82 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2
91. Symantec. (2023). *Internet security threat report* (Vol. 28). Broadcom Inc.
92. Ten, X., et al. (2021). *Risk modeling for smart grid infrastructures*. *IEEE Transactions on Smart Grid, 12*(1), 115–126.
93. The Open Group. (2018). *FAIR™ standard – Version 2.0: Factor analysis of information risk.*
94. Tranchard, S. (2018). ISO 31000 risk management – Principles and guidelines. *ISO News*. Retrieved from https://www.iso.org/news/ref2263.html
95. U.S. Department of Health & Human Services (HHS). (2023). *HIPAA breach notification rule*.
96. Verizon. (2023). *Data breach investigations report (DBIR)*. Verizon Business.
97. Wang, D., Zhong, D., & Li, L. (2022). A comprehensive study of the role of cloud computing on the information technology infrastructure library (ITIL) processes. *Library Hi Tech, 40*(6), 1954-1975.
98. Wang, Y., Tian, Z., Zhang, H., & Zhang, Y. (2020). Modeling multi-stage attack graphs for industrial control systems using probabilistic risk assessment. *Computers & Security, 96*, 101899.
99. World Bank. (2023). *The economic impacts of power infrastructure failures: Global industrial sector analysis*.
100. World Economic Forum. (2023). *Global cybersecurity outlook 2023*. World Economic Forum.
101. World Intellectual Property Organization (WIPO). (2021). *Enforcing software copyrights: A guide for businesses*. WIPO.
102. Zeltser, L. (2021). *Malware analysis and detection engineering*. Apress.
103. Zheng, P., Wang, Z., Sang, Z., Zhong, R. Y., Liu, Y., Liu, C., & Xu, X. (2023). Smart manufacturing systems for real-time anomaly detection: An Industrial IoT data-driven approach. *IEEE/ASME Transactions on Mechatronics, 28*(1), 364-375.