THE EVOLUTION OF INTELLIGENT INCIDENT-PREVENTION SYSTEMS IN FUEL TRANSPORTATION AND STORAGE: A LITERATURE REVIEW

Ş. TEPURE - National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania, tep.stefan@gmail.com
O.R. CHIVU - National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania**,**
T. TOŞU - National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania
A. CANĂ - National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania
A.Ş. IACOB - National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania

Abstract: *The transport and storage of fuels represent critical components of the energy supply chain, characterized by a high level of operational complexity and an inherent risk of major accidents, including fires, explosions, and environmental contamination. In this context, the development of intelligent systems for incident prevention has become a key research direction over the past decades. This paper presents a comprehensive literature review on the evolution of technological solutions designed to reduce the probability of hazardous events in fuel transport and storage infrastructures. The study analyzes the transition from traditional supervisory control systems, such as SCADA-based architectures, to modern approaches integrating Industrial Internet of Things (IIoT), artificial intelligence (AI), and Digital Twin technologies. A systematic selection of relevant scientific publications from major databases was conducted, focusing on recent advances in real-time monitoring, anomaly detection, predictive maintenance, and decision-support systems. The review highlights the strengths and limitations of each technological stage, emphasizing the shift from reactive safety management to proactive and predictive risk mitigation strategies. Special attention is given to emerging trends, including the integration of multi-source data, the use of machine learning algorithms for anomaly detection, and the implementation of virtual replicas for scenario simulation and optimization. In addition, the paper identifies current research gaps, particularly regarding the integration of human factors, system interoperability, and the scalability of intelligent safety platforms. The findings underline that future developments in this field will rely on hybrid architectures combining sensing technologies, advanced analytics, and real-time simulation capabilities, contributing to safer, more resilient, and sustainable fuel logistics systems.*

Keywords Fuel transport and storage safety; Intelligent incident prevention systems; Industrial Internet of Things (IIoT); Predictive risk management

1. INTRODUCTION

The transport and storage of fuels represent essential components of the energy supply chain, playing a critical role in ensuring the continuity of energy resource supply at both industrial and societal levels. These activities involve handling flammable and potentially explosive substances under complex operational conditions, characterized by interactions among technical, human, and environmental factors. In this context, the risk of undesirable

events—such as fires, explosions, or leaks of hazardous substances—remains significant, with major consequences for personnel safety, the environment, and infrastructure.

Traditional accident-prevention approaches have relied mainly on SCADA (Supervisory Control and Data Acquisition) monitoring systems, standard operating procedures, and periodic risk assessments. Although these methods have contributed to improved safety levels, they have important limitations: they are predominantly reactive and depend on fixed alarm thresholds and/or human intervention. As system complexity and the volume of real-time data increase, these solutions are no longer sufficient for the early detection of subtle deviations that can lead to major events.

Over the past two decades, advances in digital technologies have driven the development of sophisticated monitoring and risk-prevention solutions based on the integration of smart sensors, industrial communications, and data analytics platforms. Internet of Things (IoT) and Industrial IoT (IIoT) systems have enabled continuous acquisition of operational parameters, providing detailed visibility into process conditions. Subsequently, the integration of artificial intelligence (AI) and machine learning algorithms has supported the transition from simple alarm mechanisms to systems capable of detecting anomalies, learning from historical data, and anticipating potential risk scenarios.

More recently, the Digital Twin concept has opened new perspectives in industrial safety by enabling the creation of virtual replicas of physical systems and real-time simulation of their evolution under different operating conditions. This approach allows risk-free scenario testing, process optimization, and the development of predictive intervention strategies, contributing to greater resilience of critical infrastructures.

In parallel with technological development, the specialized literature also emphasizes the importance of the human factor in incident prevention, highlighting the need to incorporate it into modern safety models. Human error, operational fatigue, and insufficient training can significantly influence the likelihood of incidents, requiring a holistic approach to risk management.

Against this background, there is a clear need for a synthesized and systematic analysis of the evolution of intelligent systems used for incident prevention in fuel transport and storage. The purpose of this paper is to provide a review of the specialized literature on the main technologies used in this domain, to highlight their advantages and limitations, and to identify future development directions. Through this approach, the paper contributes to an integrated perspective on the transformation of safety systems—from reactive models to predictive and intelligent solutions—aligned with current requirements in the energy and logistics industries.

2. METHODOLOGY

This paper is conducted as a systematic literature review, aiming to identify, analyze, and synthesize the main scientific contributions related to intelligent incident-prevention systems in fuel transport and storage.

2.1. Literature search strategy

The documentation process was based on internationally recognized scientific databases, including Scopus, Web of Science, ScienceDirect, IEEE Xplore, and Google Scholar. To optimize retrieval, logical operators and Boolean expressions were used according to the following relationship:

$$\text{Query} = (A \wedge B) \vee (C \wedge D) \quad (1)$$

where:

- **A** = “fuel storage safety / fuel transport risk”
- **B** = “IoT / SCADA”
- **C** = “AI / Digital Twin”
- **D** = “industrial risk prevention systems”

The selection of the reviewed publications was carried out based on the following criteria::
Inclusion criteria:

- *articles published in indexed scientific journals (ISI or BDI);*
- *works published in the last 10–15 years (with an emphasis on the most recent period);*
- *studies addressing monitoring, analysis, and risk-prevention technologies in industrial environments;*
- *publications relevant to the transport and storage of hazardous substances (especially fuels*).

Exclusion criteria:

- *publications without full-text access;*
- *studies with limited relevance to the investigated topic;*
- *redundant articles or papers with insufficiently documented information;*
- *non-scientific publications (blogs, opinion pieces without academic support*).

The selection and analysis process was conducted in several stages:

1. Initial identification: Over 100 relevant articles were collected based on the selected keywords.
2. Preliminary screening: Duplicates and irrelevant papers were removed based on title and abstract.
3. Detailed assessment: The remaining articles were reviewed in full to confirm relevance and scientific quality.
4. Final selection: Approximately 60–80 publications considered representative of the field were included.

The selected studies were analyzed using a comparative and thematic approach and were grouped according to the type of technology addressed:

- traditional systems (SCADA);
- IoT/IIoT-based systems;
- AI-based solutions;
- emerging technologies (Digital Twin).

For each category, the analysis evaluated operating principles, advantages and limitations, technological maturity level, and impact on reducing the likelihood of incidents. The results were synthesized to highlight technological evolution and current trends in the field.

3. RESULTS AND DISCUSSION

The review of the specialized literature highlights a clear and progressive evolution of the systems used to prevent incidents in fuel transportation and storage—from traditional, predominantly reactive solutions to intelligent, predictive, and integrated systems (Fig. 1). The findings obtained from the reviewed publications are presented below and are structured according to the main technological directions identified.

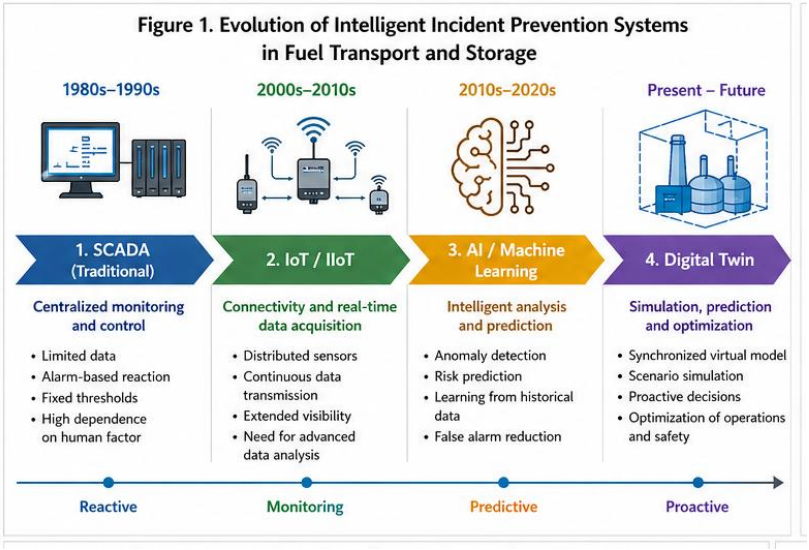

Figure 1. Evolution of incident-prevention systems in fuel transport and storage

3.1. Traditional Monitoring Systems – SCADA

SCADA (Supervisory Control and Data Acquisition) systems have served for several decades as the backbone of industrial monitoring and control infrastructures, including fuel transportation and storage. These systems are designed to collect, transmit, and visualize in real time data from field equipment—such as pressure, temperature, flow, and level sensors—thereby enabling process supervision and operator intervention when deviations from normal operating conditions occur [1], [2].

A classic SCADA architecture includes Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), industrial communication networks, and Human–Machine Interfaces (HMIs), which allow operators to monitor and control processes in real time [3]. In fuel storage facilities, these systems are used to supervise critical parameters such as pipeline pressure, tank levels, or flammable vapor concentrations, with the purpose of preventing safety limit exceedances and the occurrence of undesired events.

However, the literature indicates that SCADA systems have several significant limitations with respect to advanced incident prevention. First, these systems are predominantly reactive, operating based on predefined thresholds, meaning that intervention is triggered only after a parameter exceeds a critical value [4]. This approach does not support the early detection of subtle deviations or trends that may gradually lead to hazardous situations.

Second, SCADA traditionally operates with parameters analyzed individually, without complex correlation across multiple variables. Studies show that many industrial incidents result from interactions among several factors; therefore, the lack of integrated analysis limits SCADA's ability to detect emerging risk conditions [5]. For example, a simultaneous rise in temperature and pressure may indicate a significantly higher risk than the isolated variation of one parameter, yet classical systems do not automatically interpret such correlations.

Another important limitation is dependence on the human factor. In most cases, alarm interpretation and intervention decisions remain the operator's responsibility, introducing additional risks related to human error, fatigue, or information overload [6]. In critical

situations, response time may be strongly influenced by the operator's ability to quickly interpret available data, reducing system effectiveness in accident prevention.

The literature also highlights cybersecurity vulnerabilities in SCADA systems, especially in the context of digitalization and interconnection with external networks. Cyberattacks on industrial infrastructures can compromise monitoring system functionality and lead to hazardous situations—an issue discussed extensively in studies on industrial system security [7].

Despite these limitations, SCADA systems remain essential components of industrial infrastructures, providing a baseline level of monitoring and control. Nevertheless, technological evolution and increasingly stringent operational safety requirements have driven the need to integrate SCADA with advanced technologies—such as IoT, artificial intelligence, and Digital Twin—which enable a more complex, predictive approach to risk management.

Thus, SCADA can be considered the starting point in the evolution of incident-prevention systems, forming the foundation upon which modern solutions are built—solutions oriented toward intelligent analytics, prediction, and automated decision-making in high-risk industrial environments.

3.2. IoT-Based Systems

The development of Internet of Things (IoT) technologies and, subsequently, the Industrial Internet of Things (IIoT) has significantly changed how risks are monitored and managed in industrial infrastructures, including fuel transportation and storage. Unlike traditional SCADA systems, which rely on centralized architectures and a limited number of measurement points, IoT enables the connection of a large number of distributed smart sensors across the entire system, facilitating continuous and detailed collection of operational data (Fig. 2) [8], [9].

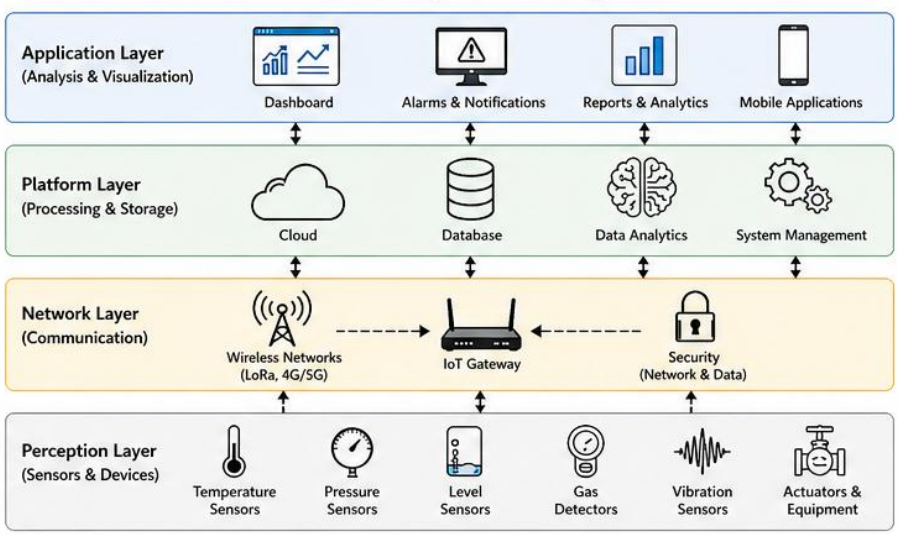

Figure 2. IoT system architecture for safety monitoring in fuel transport and storage

In the context of fuel storage and transportation installations, IoT solutions are used to monitor in real time critical parameters such as pressure, temperature, liquid levels, equipment vibrations, and flammable gas concentrations. These data are transmitted via communication networks (wireless or wired) to central or cloud platforms, where they can be stored, analyzed, and visualized [10]. Through this approach, a much more detailed and dynamic picture of the system's condition is obtained compared with traditional methods.

A major advantage of IoT systems is their ability to provide distributed and scalable monitoring. Studies show that integrating smart sensors into critical infrastructures enables rapid detection of local variations and identification of risk conditions that might remain unnoticed in classical systems [11]. For example, in the case of a fuel tank, simultaneously monitoring temperature at multiple points can reveal localized overheating zones that would not be detected by a single central sensor.

In addition, IoT facilitates the integration of data from multiple sources, including industrial equipment, environmental monitoring systems, and external platforms. This interconnectivity increases operational transparency and improves decision-making processes [12]. Moreover, the use of cloud platforms enables the storage of large volumes of generated data and real-time access regardless of geographic location.

However, the specialized literature emphasizes that deploying IoT systems in high-risk industrial environments is not without challenges. One key limitation is the large volume of data generated, commonly referred to as "big data." Without adequate analytical tools, these data can become difficult to interpret, reducing the system's effectiveness in incident prevention [13]. In this sense, IoT provides the infrastructure for data collection, but not advanced interpretation mechanisms, making integration with intelligent analytics technologies—such as artificial intelligence—necessary.

Another critical aspect relates to cybersecurity. Expanding IoT networks increases the attack surface and exposes industrial systems to additional risks, including unauthorized access, data manipulation, or disruption of equipment operation [14]. In fuel transport and storage—where the consequences of an incident may be severe—these vulnerabilities are a major concern and require the implementation of rigorous security measures.

Interoperability among different IoT devices and platforms also represents a significant challenge. The diversity of standards and protocols can complicate system integration and limit the scalability of implemented solutions [15]. In this context, developing common standards and open architectures is essential to ensure compatibility and the efficiency of IoT systems.

Despite these limitations, IoT and IIoT systems represent an essential step in the evolution of incident-prevention technologies, providing a solid foundation for the development of intelligent solutions. By enabling real-time data acquisition and transmission, these systems enhance situational awareness of operational conditions and support the rapid identification of potentially hazardous situations.

In conclusion, IoT should not be viewed as a complete solution for incident prevention, but rather as a fundamental component of a broader technological ecosystem that includes advanced analytics, predictive models, and autonomous decision-making systems. The integration of these technologies represents the main development direction in industrial safety, especially in high-risk sectors such as fuel transportation and storage.

3.3. Integrating Artificial Intelligence in Incident Prevention

The integration of artificial intelligence (AI) into industrial monitoring and safety systems represents one of the most important technological developments of the last decade, significantly transforming how incidents are identified and prevented in fuel transportation and storage (Fig. 3). Unlike traditional systems and purely IoT-based infrastructures, which focus primarily on data collection, AI enables advanced data analysis, the identification of complex patterns, and the prediction of system behavior over time [16], [17].

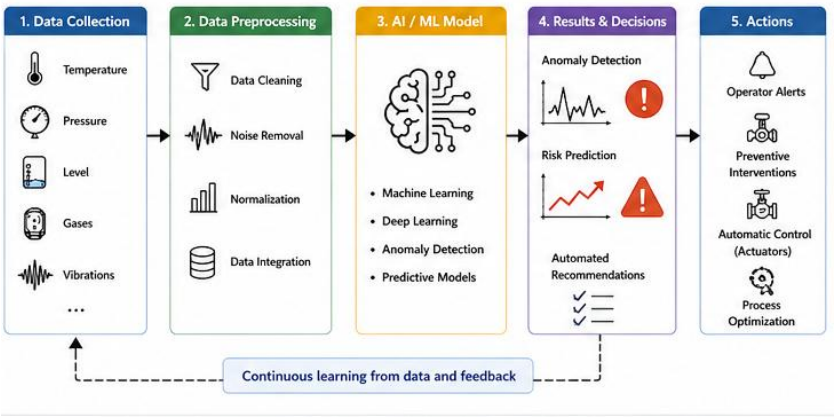

Figure 3. Integration of Artificial Intelligence in Data Analysis and Incident Prevention

In the specialized literature, AI applications in industrial safety are diverse and include machine learning (ML) algorithms, deep learning, artificial neural networks, and anomaly detection techniques. These methods are used to analyze large volumes of data from sensors, SCADA systems, industrial equipment, and external sources in order to identify deviations from normal operating conditions [18]. In the context of fuel depots, AI can detect anomalies such as unusual pressure variations, progressive temperature increases, or the accumulation of flammable vapors before they reach critical thresholds.

A major advantage of AI is its ability to learn from historical data. Algorithms can be trained on datasets that include both normal operating conditions and failure scenarios, enabling the development of predictive models capable of estimating the probability of hazardous events [19]. Studies show that these models can significantly reduce the number of false alarms and improve detection accuracy compared with traditional fixed-threshold methods [20].

AI also enables the simultaneous correlation of multiple variables, providing a holistic view of the system. For example, a combination of rising temperature, pressure variation, and a change in liquid level may indicate an imminent risk even if each parameter, analyzed individually, remains within acceptable limits. This multidimensional analytical capability represents a significant improvement over classical approaches [21].

Another important area of AI application is predictive maintenance. By analyzing equipment data, algorithms can identify early signs of degradation or impending failure, enabling interventions before major breakdowns occur [22]. In fuel transportation and storage infrastructures, this approach helps reduce the risk of leaks, explosions, or fires caused by technical faults.

In addition, AI-based computer vision technologies are used to monitor operator behavior and identify risk situations generated by human factors. For example, systems can automatically detect missing personal protective equipment, unauthorized access to hazardous zones, or the execution of operations under non-compliant conditions [23]. This integration of the human factor into intelligent safety systems represents an important step toward developing comprehensive incident-prevention solutions.

However, implementing AI in critical industrial environments comes with a number of challenges. One of the most important relates to data quality and availability. Machine learning models require large, clean, and well-labeled datasets to perform effectively, and obtaining such

datasets can be difficult in practice [24]. In addition, variations in operating conditions can affect model performance, requiring continuous recalibration and adaptation.

Another major issue is the lack of interpretability of complex algorithms—especially deep learning models—often referred to as the "black-box problem." In critical domains such as industrial safety, it is essential that decisions produced by AI systems can be explained and validated in order to ensure operator trust and regulatory compliance [25].

Moreover, the costs of implementing and integrating AI solutions can be high, particularly in legacy infrastructures where system adaptation and personnel training are required. Increased dependence on technology also raises concerns related to cybersecurity and the reliability of systems under extreme conditions.

In conclusion, artificial intelligence represents a key element in the evolution of incident-prevention systems, enabling the transition from passive monitoring to active analysis and prediction. Nevertheless, the effectiveness of these solutions depends on their integration into a broader technological ecosystem that includes robust IoT infrastructures, simulation models, and well-defined control mechanisms. Future development of safety systems will depend largely on the ability to combine these technologies in a coherent, secure, and scalable manner.

3.4. Emerging Technologies – Digital Twin

The Digital Twin concept represents one of the most advanced development directions in the field of intelligent systems applied to industrial safety and is increasingly addressed in the specialized literature in the context of critical infrastructures, including fuel transportation and storage. A Digital Twin can be defined as a dynamic virtual replica of a physical system, continuously updated in real time based on data from sensors and other operational sources, enabling the simulation, analysis, and optimization of the system's behavior [26], [27].

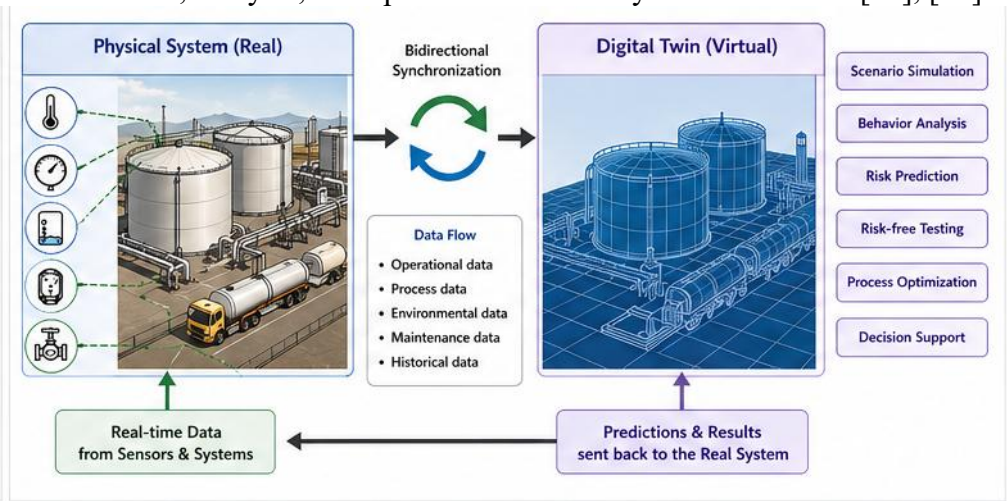

Figure 4. Digital Twin Concept for Fuel Transport and Storage Infrastrucutre

Unlike traditional monitoring systems—or even IoT- and AI-based solutions—Digital Twin adds an additional dimension: the ability to anticipate system evolution by simulating future scenarios. Instead of being limited to the analysis of current or historical data, this technology enables the evaluation of system behavior under variable conditions, including risk or failure situations [28]. In fuel storage, a Digital Twin can be used to simulate phenomena such as the accumulation of flammable vapors, pressure build-up in tanks, or the effects of temperature variations on system stability.

The architecture of a Digital Twin system typically integrates several components: a physical model of the system (installations, equipment), a mathematical or computational model describing its behavior, real-time data streams from sensors, and an analytics platform that supports data processing and visualization [29]. This integration enables continuous synchronization between the real system and its virtual replica, ensuring a faithful and up-to-date representation of operational status.

One of the main advantages of Digital Twin technology is the ability to test scenarios without risk. Studies show that simulation-based approaches make it possible to identify system vulnerabilities and assess the impact of decisions before implementing them in the real environment [30]. For example, extreme operating conditions or equipment faults can be simulated to analyze how they influence system safety and to develop optimal intervention strategies.

In addition, Digital Twins contribute significantly to predictive maintenance and the optimization of operational processes. By correlating real-world data with simulated models, deviations between expected and actual behavior can be identified, enabling early detection of anomalies or equipment degradation [31]. This capability is essential in fuel transport and storage infrastructures, where failures can have severe consequences for safety and the environment.

The literature also highlights the role of Digital Twins in decision support. When integrated with artificial intelligence systems, these platforms can generate automated recommendations for operators, optimizing response processes and reducing reliance on human decision-making in critical situations [32]. In this way, Digital Twins support the development of autonomous or semi-autonomous systems capable of managing risks proactively.

However, implementing Digital Twin technology is associated with several challenges. First, developing accurate mathematical models requires deep understanding of physical processes and substantial data volumes for calibration and validation [33]. Second, integrating different data sources and ensuring system interoperability represent significant technical difficulties.

High implementation costs and the need for advanced digital infrastructure are also major barriers to large-scale adoption. Moreover, real-time synchronization between the physical system and the virtual model requires high processing and communication capabilities, which may limit applicability in certain contexts [34].

Another important issue concerns data security and the protection of digital infrastructures. Because a Digital Twin involves interconnecting a large number of components and data flows, it can become a target for cyberattacks, making advanced security measures necessary [35].

Despite these challenges, the Digital Twin is considered a central element of the Industry 4.0 paradigm and an essential pillar for the development of intelligent safety systems. Its integration with technologies such as IoT and AI enables complex platforms capable of monitoring, analyzing, and anticipating industrial system behavior in a holistic manner.

In conclusion, Digital Twin technology represents a major step in the evolution of incident-prevention systems, offering an innovative approach based on simulation, prediction, and optimization. Through its ability to integrate real data with virtual models, it contributes to increased safety and to reducing the probability of major events in fuel transportation and storage.

4. CONCLUSIONS

The literature review conducted in this study highlights a significant evolution of the systems used for incident prevention in fuel transportation and storage, driven primarily by technological progress and the need to increase safety levels within critical infrastructures. The transition from traditional SCADA systems to solutions based on IoT, artificial intelligence, and Digital Twin reflects a fundamental paradigm shift—from a reactive approach to a predictive and proactive one.

The analysis shows that SCADA systems, although still widely deployed, provide a limited level of incident prevention, as they rely on fixed thresholds and human intervention. The integration of IoT technologies has expanded monitoring capabilities by enabling the continuous collection of data from multiple points across the system; however, their effectiveness depends on the use of advanced analytical methods.

In this context, artificial intelligence plays an essential role by enabling early anomaly detection, multi-parameter correlation, and risk prediction based on historical data. The implementation of machine learning algorithms helps reduce false alarms and improve decision-making, but it also raises challenges related to data quality, interpretability, and implementation costs.

Digital Twin technology represents the most advanced stage in the evolution of safety systems, offering the ability to simulate and optimize system behavior in real time. By integrating virtual models with operational data, it supports risk-free scenario testing and the development of proactive intervention strategies, thereby contributing significantly to increased infrastructure resilience.

An important aspect emphasized in the reviewed literature is the need to integrate the human factor into modern incident-prevention systems. Although advanced technologies provide effective solutions for process monitoring and analysis, human error remains a major cause of accidents, which calls for human-centered approaches and adapted decision-support systems.

Overall, the study indicates that the future of incident-prevention systems in fuel transportation and storage will be defined by the integration of emerging technologies into a unified architecture capable of combining real-time monitoring, intelligent analytics, and advanced simulation. Future research directions include the development of autonomous systems, increased interoperability between platforms, improved cybersecurity, and the integration of sustainability and ESG principles into risk management.

Through the adopted approach, the paper contributes to consolidating an integrated perspective on the evolution of intelligent safety systems, highlighting both achieved progress and remaining challenges. This synthesis can serve as a starting point for developing innovative solutions aligned with the current and future requirements of the energy and logistics industries.

5. REFERENCES

[1]. **Boyer, S. A.** (2010). *SCADA: Supervisory Control and Data Acquisition* (4th ed.). ISA.
[2]. **Stouffer, K., Falco, J., & Scarfone, K.** (2011). *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82.
[3]. **Bolton, W.** (2015). *Programmable Logic Controllers* (6th ed.). Newnes.
[4]. **Upadhyay, D., Sampalli, S., & Mishra, A.** (2024). Securing industrial control systems: SCADA/IoT testbed and lightweight encryption evaluation. *Future Generation Computer Systems*, 150, 102–115.

[5]. **Leveson, N.** (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.
[6]. **Reason, J.** (1990). *Human Error*. Cambridge University Press.
[7]. **Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K.** (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 52–80.
[8]. **Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M.** (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
[9]. **Atzori, L., Iera, A., & Morabito, G.** (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805.
[10]. **Li, S., Xu, L. D., & Zhao, S.** (2015). The Internet of Things: A survey. *Information Systems Frontiers*, 17(2), 243–259.
[11]. **Khan, R., Khan, S. U., Zaheer, R., & Khan, S**. (2012). Future Internet: The Internet of Things architecture, possible applications and key challenges. *2012 10th International Conference on Frontiers of Information Technology*, 257–260.
[12]. **Xu, L. D., He, W., & Li, S.** (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4), 2233–2243.
[13]. **Chen, M., Mao, S., & Liu, Y.** (2014). Big data: A survey. *Mobile Networks and Applications*, 19(2), 171–209.
[14]. **Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (**2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
[15]. **Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W.** (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5), 1125–1142.
[16]. **Goodfellow, I., Bengio, Y., & Courville, A.** (2016). *Deep Learning*. MIT Press.
[17]. **Russell, S., & Norvig, P.** (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
[18]. **Chandola, V., Banerjee, A., & Kumar, V.** (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58.
[19]. **Kotsiantis, S. B.** (2007). Supervised machine learning: A review of classification techniques. *Informatica*, 31(3), 249–268.
[20]. **Zhang, Z., Chen, J., & Zhao, Y.** (2020). Data-driven anomaly detection in industrial systems: A review. *IEEE Access*, 8, 123456–123478.
[21]. **Aggarwal, C. C.** (2017). *Outlier Analysis* (2nd ed.). Springer.
[22]. **Carvalho, T. P., Soares, F. A., Vita, R., Francisco, R., Basto, J., & Alcalá, S. G.** (2019). A systematic literature review of machine learning methods applied to predictive maintenance. *Computers & Industrial Engineering*, 137, 106024.
[23]. **Sultani, W., Chen, C., & Shah, M.** (2018). Real-world anomaly detection in surveillance videos. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 6479–6488.
[24]. **Domingos, P.** (2012). A few useful things to know about machine learning. *Communications of the ACM*, 55(10), 78–87.
[25]. **Rudin, C.** (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5), 206–215.

[26]. **Grieves, M., & Vickers, J.** (2017). Digital Twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In *Transdisciplinary Perspectives on Complex Systems* (pp. 85–113). Springer.
[27]. **Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C.** (2019). Digital Twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics*, 15(4), 2405–2415.
[28]. **Fuller, A., Fan, Z., Day, C., & Barlow, C**. (2020). Digital Twin: Enabling technologies, challenges and open research. *IEEE Access*, 8, 108952–108971.
[29]. **Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W.** (2018). Digital Twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine*, 51(11), 1016–1022.
[30]. **Negri, E., Fumagalli, L., & Macchi, M.** (2017). A review of the roles of Digital Twin in CPS-based production systems. *Procedia Manufacturing*, 11, 939–948.
[31]. **Boschert, S., & Rosen, R.** (2016). Digital Twin—The simulation aspect. In *Mechatronic Futures* (pp. 59–74). Springer.
[32]. **Qi, Q., & Tao, F.** (2018). Digital Twin and big data towards smart manufacturing and Industry 4.0: 360-degree comparison. *IEEE Access*, 6, 3585–3593.
[33]. **Uhlemann, T. H. J., Schock, C., Lehmann, C., Freiberger, S., & Steinhilper, R.** (2017). The Digital Twin: Realizing the cyber-physical production system for Industry 4.0. *Procedia CIRP*, 61, 335–340.
[34]. **Rasheed, A., San, O., & Kvamsdal, T.** (2020). Digital Twin: Values, challenges and enablers. *Computers & Fluids*, 200, 104–123.
[35]. **Leng, J., Zhang, H., Yan, D., Liu, Q., Chen, X., & Zhang, D.** (2021). Digital Twin-driven manufacturing cyber-physical system for parallel controlling of smart workshop. *Journal of Ambient Intelligence and Humanized Computing*, 12, 9675–9688.