Open Access Research Journal of
Multidisciplinary Studies
Journals home page: https://oarjpublication/journals/oarjms/
ISSN: 2783-0268 (Online)

(REVIEW ARTICLE)

Check for updates

Innovative approaches to enhancing functional safety in Distributed Control Systems (DCS) and Safety Instrumented Systems (SIS) for Oil and Gas Applications

Fidelis Othuke Onyeke [1,*], Oladipo Odujobi [2], Friday Emmanuel Adikwu [3] and Tari Yvonne Elete [1]

[1] *Shell Petroleum and Development Company (SPDC), Port Harcourt Nigeria.*
[2] *Tomba Resources, Warri, Nigeria.*
[3] *Waltersmith Refining and Petrochemical Company Ltd, Lagos, Nigeria.*

Open Access Research Journal of Multidisciplinary Studies, 2022, 03(01), 106–112

Publication history: Received on 01 January 2022; revised on 11 February 2022; accepted on 14 February 2022

Article DOI: https://doi.org/10.53022/oarjms.2022.3.1.0027

Abstract

Functional safety in Distributed Control Systems (DCS) and Safety Instrumented Systems (SIS) is vital for ensuring operational integrity and mitigating risks in the oil and gas industry. These systems face numerous challenges, including high-risk processes, gaps in existing safety frameworks, and emerging threats such as cybersecurity vulnerabilities and aging infrastructure. This paper explores innovative approaches to enhancing functional safety by adopting advanced technologies, including artificial intelligence, machine learning, digital twins, and predictive maintenance. The integration of robust cybersecurity measures is emphasized as a critical component of modern safety practices. Key design principles, such as redundancy, fail-safe mechanisms, and lifecycle management, are outlined alongside best practices for training, certification, and adherence to international standards. The paper concludes with actionable recommendations for operators, engineers, policymakers, and industry leaders to foster a culture of safety, innovation, and continuous improvement, ensuring the resilience and sustainability of oil and gas operations in an increasingly complex environment.

Keywords: Functional Safety; Distributed Control Systems (DCS; Safety Instrumented Systems (SIS; Cybersecurity; Predictive Maintenance; Oil and Gas Industry

1. Introduction

Distributed Control Systems (DCS) and Safety Instrumented Systems (SIS) are foundational technologies in the oil and gas sector, where operational efficiency, safety, and reliability are critical (Catelani, Ciani, & Patrizi, 2022). A DCS is a centralized system that supervises and controls industrial processes, ensuring seamless operation by monitoring variables such as pressure, temperature, and flow rates. By distributing control across various subsystems, a DCS enhances scalability, reduces risks of single-point failures, and provides operators with real-time data for decision-making (Q. Zhou et al., 2020). In contrast, SIS is explicitly designed to prevent hazardous events by taking corrective actions when predefined safety thresholds are breached. These systems work independently of the primary control systems, adding a vital layer of protection in high-risk environments such as oil refineries, offshore platforms, and gas processing plants (K. Kosmowski & Gołębiewski, 2019).

Integrating DCS and SIS enables efficient management of routine operations and emergency scenarios. While DCS ensures optimal production and process quality, SIS focuses on safeguarding personnel, assets, and the environment. Together, these systems address the complex interplay of operational demands and safety requirements inherent in the oil and gas industry, where even minor deviations can lead to catastrophic consequences (Ashraf et al., 2022).

Functional safety is a critical concept in the design and operation of DCS and SIS. It refers to the ability of these systems to detect, respond to, and mitigate failures that could result in unsafe conditions. In the oil and gas industry, functional

* Corresponding author: Fidelis Othuke Onyekwe.

safety ensures that industrial processes operate within safe limits, reducing the likelihood of incidents such as explosions, fires, or toxic gas releases.

The relevance of functional safety extends beyond compliance with regulatory standards; it is central to operational integrity and risk management. Effective functional safety systems minimize downtime caused by accidents, enhance reliability, and protect workers and nearby communities. Additionally, the financial implications of safety are significant, as robust systems prevent costly disruptions, legal liabilities, and reputational damage (Smith & Simpson, 2020).

Modern standards like IEC 61508 and IEC 61511 provide comprehensive guidelines for implementing functional safety in industrial processes. These standards emphasize a lifecycle approach, covering everything from design and installation to maintenance and decommissioning. Adherence to such standards ensures that DCS and SIS are compliant and resilient against evolving risks, such as cybersecurity threats targeting industrial control systems (Smith & Simpson, 2020).

This paper explores innovative approaches to enhancing functional safety in DCS and SIS for oil and gas applications. While effective, traditional methods are often limited in addressing emerging challenges such as increased process complexity, aging infrastructure, and heightened cybersecurity risks. The oil and gas sector requires adaptive and forward-looking strategies to ensure that safety systems keep pace with technological advancements and operational demands (K. T. Kosmowski, 2021).

The primary objective of this study is to analyze how new technologies, such as artificial intelligence (AI), machine learning (ML), and digital twins, can transform functional safety in DCS and SIS. By leveraging predictive analytics and real-time monitoring, these innovations offer the potential to preemptively address system failures and optimize performance. Furthermore, integrating advanced cybersecurity measures is explored to protect safety systems from digital threats, which have become increasingly prevalent with the adoption of industrial Internet of Things (IoT) devices.

The paper also aims to bridge the gap between theoretical concepts and practical applications by proposing best practices and design principles tailored to the oil and gas industry. These include redundancy mechanisms, fail-safe designs, and compliance with international safety standards. By highlighting both challenges and opportunities, the study seeks to guide industry stakeholders—including engineers, operators, and policymakers—in implementing robust functional safety frameworks that align with future trends.

2. Current Challenges in Functional Safety for DCS and SIS

2.1. Typical Safety Challenges in Oil and Gas Environments

The oil and gas industry operates in high-risk environments, where safety is paramount. A key challenge is managing the potential hazards associated with high-pressure systems, flammable materials, and volatile chemical processes. Minor deviations in operational parameters can lead to catastrophic outcomes, including explosions, fires, and environmental disasters. Distributed Control Systems and Safety Instrumented Systems are tasked with mitigating these risks, but their effectvarious challenges can hinder their effectiveness (Idris, 2022).

System failures are a significant concern. Hardware and software malfunctions in DCS and SIS can disrupt critical operations, leading to unsafe conditions. Failures may result from manufacturing defects, improper maintenance, or external factors such as extreme environmental conditions. Even a brief malfunction can escalate into a severe incident in safety-critical scenarios (Aydin & Sertbaş, 2022). Human factors also play a pivotal role in safety challenges. Operator errors, misjudgments, and insufficient training can compromise the reliability of functional safety systems. For instance, delayed or incorrect responses to alarms can exacerbate hazardous situations. Additionally, poorly designed user interfaces in DCS and SIS can lead to misinterpretation of data, further increasing the likelihood of errors (Ansari, Naghdy, & Du, 2022).

2.2. Gaps in Existing Functional Safety Frameworks and Standards

While international standards such as IEC 61508 and IEC 61511 provide robust guidelines for implementing functional safety, gaps remain in their application and enforcement. These standards emphasize a systematic approach to safety, encompassing the entire lifecycle of safety systems from design to decommissioning. However, adherence to these frameworks can be inconsistent across organizations, particularly in regions with limited regulatory oversight.

One significant gap lies in interpreting and customizing these standards for specific applications. The generic nature of the guidelines often leaves room for ambiguity, making it challenging to address unique operational scenarios in the oil and gas sector. Additionally, the implementation of safety standards can be resource-intensive, requiring substantial investments in technology, personnel training, and periodic system reviews. Many organizations, especially smaller operators, may lack the resources or expertise to fully comply with these requirements (Liaropoulos, Sapountzaki, & Nivolianitou, 2019).

Another limitation of existing frameworks is their ability to address rapidly evolving threats. While the standards provide foundational principles, they may not adequately account for emerging challenges, such as cybersecurity risks, that directly impact the reliability of functional safety systems. This gap underscores the need for continuous updates to align safety practices with modern technological advancements (Bommasani et al., 2021).

2.3. Emerging Threats to Functional Safety Systems

The oil and gas industry faces a growing array of emerging threats that challenge the reliability of DCS and SIS. Cybersecurity risks have become critical as these systems increasingly rely on interconnected digital technologies. Cyberattacks targeting industrial control systems (ICS) can disrupt operations, manipulate safety parameters, or disable critical systems altogether. The integration of Industrial Internet of Things (IIoT) devices, while enhancing operational efficiency, has introduced new vulnerabilities that attackers can exploit (Miller, Staves, Maesschalck, Sturdee, & Green, 2021).

Aging infrastructure presents another significant threat. Many oil and gas facilities continue relying on legacy systems not designed to meet modern safety requirements. These outdated systems often lack the robustness and resilience of newer technologies, making them more susceptible to failures. Additionally, maintaining and upgrading aging equipment can be challenging, as spare parts may no longer be available, and technical expertise for obsolete systems may be limited (Ersdal, Sharp, & Stacey, 2019).

Process complexities further exacerbate safety challenges. The associated processes become more intricate as oil and gas operations expand to include unconventional resources and deeper offshore reserves. Managing these complexities requires advanced safety systems capable of real-time monitoring, diagnostics, and automated responses. However, integrating these capabilities into existing DCS and SIS can be technically and financially demanding.

Another emerging issue is the human-machine interface (HMI) in safety systems. While technological advancements have improved the capabilities of DCS and SIS, they have also increased their complexity. Operators often struggle to interpret vast amounts of data generated by modern systems, leading to delays in critical decision-making. Poorly designed interfaces can overwhelm operators, reducing the effectiveness of functional safety systems during emergencies (Bengler, Rettenmaier, Fritz, & Feierle, 2020).

3. Innovative Approaches to Enhancing Functional Safety

3.1. Modern Advancements in Technology

Technological innovation is transforming how functional safety is approached in Distributed Control Systems (DCS) and Safety Instrumented Systems (SIS). Among these advancements, artificial intelligence (AI) and machine learning (ML) have emerged as game changers. These technologies enhance safety systems' predictive and analytical capabilities, enabling them to identify anomalies and potential failures before they escalate into hazardous conditions (Carreras Guzman, Wied, Kozine, & Lundteigen, 2020).

AI-driven algorithms can analyze large volumes of operational data to detect subtle patterns that may indicate a developing issue. For instance, changes in pressure or temperature trends that might go unnoticed by human operators can be flagged by AI for further inspection. Similarly, ML models can continuously learn from historical data to improve their accuracy in predicting system behavior, making them invaluable for risk assessment and failure prevention (Shaikh, Rasool, & Lone, 2022).

Advanced diagnostics is another significant innovation. Modern diagnostic tools provide deeper insights into the health of safety-critical components, such as sensors, valves, and actuators. By leveraging these tools, maintenance teams can detect and address issues like wear and tear, calibration errors, or degraded performance, thereby ensuring that safety systems operate at peak efficiency. These diagnostic capabilities, often integrated into DCS and SIS, help reduce unplanned downtime and enhance the overall reliability of safety systems (Khan et al., 2021).

3.2. The Role of Digital Twins, Predictive Maintenance, and Real-Time Monitoring

Digital twins have revolutionized the way functional safety is managed in complex industrial environments. A digital twin is a virtual replica of a physical system that mirrors its real-time behavior and conditions. In DCS and SIS, digital twins enable operators and engineers to simulate, monitor, and optimize processes without disrupting actual operations (Jiang, Yin, Li, Luo, & Kaynak, 2021).

By using digital twins, safety scenarios can be tested under various conditions to evaluate system responses and identify vulnerabilities. For instance, operators can simulate emergency shutdowns or process deviations to determine how the system would react, providing critical insights into the robustness of safety mechanisms. This proactive approach minimizes risks and ensures that safety systems are well-prepared for real-world challenges (Mihai et al., 2022).

Predictive maintenance is another key innovation that aligns with functional safety objectives. Traditional maintenance schedules are often based on fixed intervals, which can lead to either unnecessary servicing or delayed intervention. Predictive maintenance, powered by AI and IoT-enabled sensors, uses real-time data to assess the condition of equipment and predict when maintenance is required. This approach reduces the likelihood of equipment failures that could compromise safety while optimizing maintenance resources (Zonta et al., 2020).

Real-time monitoring, facilitated by advanced sensors and IoT connectivity, is crucial in improving system reliability. Modern DCS and SIS can collect and analyze data in real-time, providing operators with up-to-date information on process conditions and equipment status. Alerts and alarms generated by these systems allow for swift action to prevent unsafe conditions. Moreover, real-time monitoring enables continuous compliance with safety standards, as deviations from prescribed limits can be immediately detected and addressed (Vodyaho, Osipov, Zhukova, & Chernokulsky, 2020).

3.3. Integration of Cybersecurity Measures

As DCS and SIS become increasingly digital and interconnected, they are exposed to a growing number of cybersecurity threats. Cyberattacks targeting industrial control systems (ICS) can have devastating consequences, ranging from operational disruptions to compromised safety functions. Therefore, integrating robust cybersecurity measures into DCS and SIS is critical for maintaining functional safety.

One approach is the implementation of defense-in-depth strategies, which involve multiple layers of security to protect critical systems. These layers include firewalls, intrusion detection systems, and secure communication protocols that prevent unauthorized access to DCS and SIS. Additionally, regular software updates and patches are essential to address vulnerabilities in system components (C. Zhou et al., 2020).

Another key measure is network segmentation, which isolates safety-critical systems from non-essential networks. Organizations can reduce the risk of cyber threats spreading across the network by creating secure zones for DCS and SIS. Access control mechanisms, such as role-based permissions and multi-factor authentication, further enhance the security of these systems by limiting who can interact with safety-critical components.

Cybersecurity training and awareness programs for personnel are equally important. Human errors, such as falling victim to phishing attacks or using weak passwords, remain a significant vulnerability. By educating staff on cybersecurity best practices, organizations can reduce the risk of breaches that could compromise functional safety. Advanced technologies, such as AI-driven threat detection, are also being integrated into cybersecurity strategies for DCS and SIS. These systems can monitor network traffic and identify suspicious activities, enabling faster responses to potential attacks. For example, anomaly detection algorithms can flag unusual communication patterns that may indicate an ongoing cyberattack, allowing for immediate mitigation measures (Perwej, Abbas, Dixit, Akhtar, & Jaiswal, 2021).

4. Design Principles and Best Practices for Enhanced Functional Safety

4.1. Key Design Principles for Robust DCS and SIS

Implementing robust Distributed Control Systems and Safety Instrumented Systems in the oil and gas industry begins with adherence to core design principles prioritizing safety, reliability, and resilience. These principles are crucial for managing the inherent risks associated with high-pressure processes, flammable materials, and complex operations. One foundational principle is inherent safety by design. This involves eliminating hazards wherever possible or reducing them to a minimum at the design stage. For example, selecting materials and equipment that can withstand

the harsh environmental conditions typical of oil and gas facilities reduces the risk of failure under extreme circumstances.

Another critical principle is the segregation of safety and control functions. DCS, which focuses on process control, and SIS, which is responsible for safety-critical interventions, must remain independent to avoid common cause failures. This segregation ensures that if the DCS experiences a failure, the SIS remains unaffected and capable of taking necessary actions, such as initiating emergency shutdowns. System scalability and flexibility also play a vital role in design. As oil and gas operations expand or adapt to new challenges, the control and safety systems must accommodate these changes without compromising performance. This requires modular designs that can integrate new technologies, sensors, and processes seamlessly.

4.2. Best Practices for Enhanced Functional Safety

Redundancy is a cornerstone of functional safety in oil and gas settings. Incorporating multiple layers of protection ensures that system failures do not lead to catastrophic outcomes. For instance, redundant sensors, actuators, and processors provide backup capabilities if primary components fail. In critical applications, systems often use triple modular redundancy (TMR), where three parallel units continuously monitor operations, and the majority decision determines the system's actions. This reduces the likelihood of errors and enhances reliability (Richardson, Lemoine, Stephens, & Waller, 2020).

Fail-safe mechanisms are designed to default to a safe state in the event of system malfunctions. For example, valves in SIS are often configured to close automatically in case of power loss, preventing the release of hazardous substances. Similarly, systems are programmed to initiate controlled shutdowns when abnormal conditions are detected, ensuring that operations halt safely and orderly (Wolf & Serpanos, 2020).

Effective lifecycle management of DCS and SIS is crucial for maintaining their reliability and compliance with safety standards. This involves regular assessments and updates throughout the systems' operational lifecycle. The process begins with hazard and risk analysis during the design phase, followed by thorough verification and validation of system functionality before deployment. Once operational, systems require ongoing maintenance, testing, and inspections to ensure they continue to meet safety requirements. This includes periodic proof testing of SIS components to confirm their reliability under real-world conditions. When systems approach the end of their lifecycle, decommissioning and replacement plans must prioritize safety to prevent legacy issues from compromising operations (K. Kosmowski & Gołębiewski, 2019).

4.3. Importance of Training, Certification, and Compliance

4.3.1. Training and Certification

Human factors remain a significant determinant of functional safety. Even the most advanced DCS and SIS are ineffective without skilled operators and engineers capable of managing them. Comprehensive training programs are essential to familiarize personnel with the complexities of these systems, including interpreting data, responding to alarms, and executing emergency protocols.

Certification programs, such as those offered by TÜV Rheinland or Exida, ensure that professionals meet global competency standards in functional safety. Certified personnel bring an added layer of assurance, as they are trained to design, implement, and maintain safety systems following industry best practices.

4.3.2. Compliance with International Safety Standards

Adherence to international safety standards is a non-negotiable aspect of functional safety in the oil and gas sector. Standards such as IEC 61508 (functional safety of electrical/electronic systems) and IEC 61511 (safety instrumented systems for the process industry) provide comprehensive guidelines for achieving and maintaining safety (Smith & Simpson, 2020).

Compliance begins with a systematic approach to safety lifecycle management, encompassing risk assessment, design, implementation, operation, and maintenance. Audits and inspections conducted by certified bodies ensure that systems remain aligned with these standards. Furthermore, many regulatory frameworks mandate compliance with these standards, making it both a legal and operational imperative for organizations. Compliance also promotes uniformity and interoperability across systems, particularly in multinational operations. By aligning with recognized standards,

companies ensure that their safety practices meet global benchmarks, fostering trust among stakeholders and regulators.

5. Conclusion

Distributed Control Systems (DCS) and Safety Instrumented Systems (SIS) are critical pillars of operational integrity in the oil and gas industry. This paper has highlighted these systems' pressing challenges, including the complex and hazardous nature of oil and gas operations, gaps in existing safety standards, and the emerging threats posed by cybersecurity risks and aging infrastructure. These challenges underscore the urgency of adopting innovative approaches to functional safety.

Technological advancements, such as artificial intelligence, machine learning, digital twins, and predictive maintenance, offer unprecedented opportunities to enhance the reliability and efficiency of DCS and SIS. Additionally, integrating robust cybersecurity measures is essential to safeguard these systems against evolving digital threats. Design principles, including redundancy, fail-safe mechanisms, and lifecycle management, form the foundation for resilient systems. Coupled with rigorous training and compliance with international standards, these measures ensure the effective deployment and maintenance of safety systems in high-risk environments.

Operators and engineers must prioritize the adoption of modern technologies to address current safety challenges. Investing in advanced diagnostic tools, real-time monitoring systems, and AI-driven analytics can significantly improve the detection and mitigation of potential risks. For instance, integrating predictive maintenance systems enables operators to identify and address component failures before they escalate into critical incidents. Regular training and certification are equally important. Engineers and operators should pursue professional development programs to stay updated on the latest advancements in functional safety and cybersecurity. Certified training ensures that personnel are well-equipped to design, implement, and maintain complex systems in compliance with global standards.

Policymakers play a vital role in fostering innovation and ensuring compliance across the industry. Governments and regulatory bodies should encourage the adoption of advanced safety technologies by providing incentives such as tax benefits or subsidies for organizations that implement state-of-the-art systems. Policymakers should also focus on strengthening and updating existing safety standards like IEC 61508 and IEC 61511 to address emerging threats, including cybersecurity. Mandating regular audits and safety inspections can ensure that companies adhere to these enhanced standards. Additionally, fostering collaboration between industry stakeholders, technology providers, and regulatory agencies can drive innovation and improve the implementation of functional safety practices.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ansari, S., Naghdy, F., & Du, H. (2022). Human-machine shared driving: Challenges and future directions. *IEEE Transactions on Intelligent Vehicles, 7*(3), 499-519.

[2] Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2677-2690.

[3] Aydin, H., & Sertbaş, A. (2022). Cyber security in Industrial Control Systems (ics): a survey of rowhammer vulnerability. *Applied Computer Science, 18*(2).

[4] Bengler, K., Rettenmaier, M., Fritz, N., & Feierle, A. (2020). From HMI to HMIs: Towards an HMI framework for automated driving. *Information, 11*(2), 61.

[5] Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., . . . Brunskill, E. (2021). On the opportunities and risks of foundation models. *arXiv preprint arXiv:2108.07258*.

[6] Carreras Guzman, N. H., Wied, M., Kozine, I., & Lundteigen, M. A. (2020). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering, 23*(2), 189-210.

[7] Catelani, M., Ciani, L., & Patrizi, G. (2022). Logic Solver Diagnostics in Safety Instrumented Systems for Oil and Gas Applications. *Safety, 8*(1), 15.

[8] Ersdal, G., Sharp, J. V., & Stacey, A. (2019). *Ageing and life extension of offshore structures: the challenge of managing structural integrity*: John Wiley & Sons.

[9] Idris, M. N. (2022). Safety Evaluation of Petroleum Tank Farm: An Analytical Study of NNPCL Maiduguri Depot Plant. *African Journal of Engineering and Environment Research Vol, 4*(1).

[10] Jiang, Y., Yin, S., Li, K., Luo, H., & Kaynak, O. (2021). Industrial applications of digital twins. *Philosophical Transactions of the Royal Society A, 379*(2207), 20200360.

[11] Khan, K., Sohaib, M., Rashid, A., Ali, S., Akbar, H., Basit, A., & Ahmad, T. (2021). Recent trends and challenges in predictive maintenance of aircraft's engine and hydraulic system. *Journal of the Brazilian Society of Mechanical Sciences and Engineering, 43*, 1-17.

[12] Kosmowski, K., & Gołębiewski, D. (2019). Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance. *Journal of Polish Safety and Reliability Association, 10*.

[13] Kosmowski, K. T. (2021). Functional safety and cybersecurity analysis and management in smart manufacturing systems. *Handbook of Advanced Performability Engineering*, 61-87.

[14] Liaropoulos, A., Sapountzaki, K., & Nivolianitou, Z. (2019). Adopting risk governance in the offshore oil industry and in diverse cultural and geopolitical context: North Sea vs Eastern Mediterranean countries. *Safety Science, 120*, 471-483.

[15] Mihai, S., Yaqoob, M., Hung, D. V., Davis, W., Towakel, P., Raza, M., . . . Prasad, R. V. (2022). Digital twins: A survey on enabling technologies, challenges, trends and future prospects. *IEEE Communications Surveys & Tutorials, 24*(4), 2255-2291.

[16] Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection, 35*, 100464.

[17] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management, 9*(12), 669-710.

[18] Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning, 27*(2), 23-39.

[19] Shaikh, T. A., Rasool, T., & Lone, F. R. (2022). Towards leveraging the role of machine learning and artificial intelligence in precision agriculture and smart farming. *Computers and Electronics in Agriculture, 198*, 107119.

[20] Smith, D. J., & Simpson, K. G. (2020). *The safety critical systems handbook: a straightforward guide to functional safety: IEC 61508 (2010 Edition), IEC 61511 (2015 edition) and related guidance*: Butterworth-Heinemann.

[21] Vodyaho, A., Osipov, V., Zhukova, N., & Chernokulsky, V. (2020). Data collection technology for ambient intelligence systems in internet of things. *Electronics, 9*(11), 1846.

[22] Wolf, M., & Serpanos, D. (2020). *Safe and secure cyber-physical systems and internet-of-things systems*: Springer.

[23] Zhou, C., Hu, B., Shi, Y., Tian, Y.-C., Li, X., & Zhao, Y. (2020). A unified architectural approach for cyberattack-resilient industrial control systems. *Proceedings of the IEEE, 109*(4), 517-541.

[24] Zhou, Q., Shahidehpour, M., Paaso, A., Bahramirad, S., Alabdulwahab, A., & Abusorrah, A. (2020). Distributed control and communication strategies in networked microgrids. *IEEE Communications Surveys & Tutorials, 22*(4), 2586-2633.

[25] Zonta, T., Da Costa, C. A., da Rosa Righi, R., de Lima, M. J., da Trindade, E. S., & Li, G. P. (2020). Predictive maintenance in the Industry 4.0: A systematic literature review. *Computers & Industrial Engineering, 150*, 106889.