OPEN ACCESS
Engineering Science & Technology Journal
P-ISSN: 2708-8944, E-ISSN: 2708-8952
Volume 5, Issue 3, P.No. 995-1007, March 2024
DOI: 10.51594/estj/v5i3.953
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/estj

THEORETICAL INSIGHTS INTO SECURING REMOTE MONITORING SYSTEMS IN WATER DISTRIBUTION NETWORKS: LESSONS LEARNED FROM AFRICA-US PROJECTS

Fatai Adeshina Adelani[1], Enyinaya Stefano Okafor[2], Boma Sonimiteim Jacks[3,] & Olakunle Abayomi Ajala[4]

[1]Lagos Water Corporation, Lagos, Nigeria
[2]Independent Researcher, Phoenix, Arizona, USA
[3]Independent Researcher, Nigeria
[4]Indiana Wesleyan University, USA

*Corresponding Author: Fatai Adeshina Adelani
Corresponding Author Email: fadelani@gmail.com

Article Received: 10-01-24 **Accepted:** 21-02-24 **Published:** 24-03-24

ABSTRACT

This review paper delves into the critical realm of securing remote monitoring systems within water distribution networks, illuminating theoretical insights and practical lessons gleaned from collaborative projects between Africa and the United States. Given the pivotal role of water distribution networks in public health and safety, integrating remote monitoring systems offers substantial benefits in operational efficiency and resource management. However, this integration also introduces significant security vulnerabilities that pose risks to critical infrastructure data's integrity, availability, and confidentiality. Through a comprehensive analysis, this paper explores the multifaceted security challenges inherent in these systems, underscores the importance of robust theoretical frameworks for cybersecurity, and highlights effective security practices derived from international collaboration projects. It proposes principles for designing, implementing, and managing secure systems, emphasizing the

necessity of defence-in-depth strategies, the principle of least privilege, and the critical role of continuous monitoring and adaptive response mechanisms. Furthermore, it identifies ongoing challenges and future directions for research, stressing the dynamic nature of cybersecurity threats and the potential of emerging technologies to fortify security measures. The paper advocates for sustained collaborative efforts and research to navigate the evolving landscape of security challenges in water distribution networks, ensuring their resilience against threats.

Keywords: Remote Monitoring Systems, Water Distribution Security, Cybersecurity Frameworks.

INTRODUCTION

Water distribution networks are critical infrastructures in ensuring public health, economic stability, and societal well-being. These networks, comprising treatment facilities, storage tanks, pipelines, and distribution centres, deliver clean and safe water to communities, industries, and agricultural sectors (Katina & Keating, 2015; Sänger, Heinzel, & Sandholz, 2021). The complexity and vastness of these systems necessitate the adoption of advanced technologies for monitoring and management to maintain efficiency, reliability, and resilience against disruptions (Dargin & Mostafavi, 2020).

In recent years, integrating remote monitoring systems into water distribution networks has emerged as a game-changer (Harshadeep & Young, 2020). These systems employ sensors, actuators, and communication technologies to collect real-time data on water quality, flow rates, pressure levels, and other critical parameters. This continuous data stream enables operators to detect leaks, predict system failures, optimize water distribution, and ensure compliance with regulatory standards (Glasgow, Burkholder, Reed, Lewitus, & Kleinman, 2004; Park, Kim, & Lee, 2020). Moreover, remote monitoring facilitates the implementation of smart water management practices, leading to enhanced operational efficiency and resource conservation (Nova, 2023; Sun & Scanlon, 2019).

However, the reliance on digital technologies and networked systems introduces new vulnerabilities and security challenges. Cyber-attacks, unauthorized access, and data breaches can compromise the integrity, confidentiality, and availability of critical operational data, potentially leading to service disruptions, public health crises, and loss of public trust (Lehto, 2022). The consequences of security incidents in water distribution networks can be far-reaching, affecting the immediate operational capabilities and the long-term sustainability and safety of water resources (Gunduz & Das, 2020).

The necessity for robust security measures in remote monitoring systems is, therefore, paramount (Ge, Zhang, Meqdad, & Chen, 2023). Ensuring the security of these systems involves a multifaceted approach, encompassing the protection of physical assets, safeguarding of data communications, and implementation of cybersecurity protocols to deter, detect, and respond to threats. The challenge lies in developing and maintaining resilient security practices in the face of evolving threats, adaptable to technological advancements, and scalable across diverse and geographically dispersed water distribution infrastructures (Berkeley, Wallace, & Coo, 2010; Chaterji et al., 2019; Mehvar et al., 2021).

This review paper aims to shed light on the theoretical insights into securing remote monitoring systems in water distribution networks, drawing lessons from collaborative projects between Africa and the US. By focusing on theoretical frameworks, security challenges, and principles

guiding the development and implementation of secure systems, this paper seeks to contribute to the knowledge on enhancing water distribution networks' security and reliability. It synthesizes and analyzes the overarching themes, strategies, and best practices that have emerged from cross-continental collaborations. The purpose is to provide a comprehensive overview that can inform future research, policy-making, and implementation efforts to secure the critical infrastructure of water distribution against the backdrop of increasing cyber-physical threats.

The Importance of Securing Remote Monitoring Systems

Remote monitoring systems in water distribution networks represent a crucial technological advancement that has transformed how water utilities manage and operate their infrastructures (Geels, 2005). These systems integrate a wide array of sensors, meters, and devices connected through wireless or wired networks to continuously collect data on various aspects of the water distribution process. This data includes water quality indicators (such as pH, turbidity, and contaminant levels), flow rates, pressure readings, and the status of critical components. By enabling real-time visibility into the network's performance, remote monitoring systems facilitate proactive maintenance, leak detection, pressure management, and efficient water quality management. They also support decision-making processes, allowing operators to swiftly respond to anomalies, optimize resource allocation, and ensure compliance with regulatory standards (Aisopou, Stoianov, & Graham, 2012; Raich, 2013).

Despite their significant benefits, remote monitoring systems introduce various risks and vulnerabilities that can compromise the security and functionality of water distribution networks. Some of these vulnerabilities arise from:

- **Cybersecurity Threats:** As digital and networked solutions, remote monitoring systems are susceptible to cyber-attacks, including malware, ransomware, phishing, and denial of service (DoS) attacks. Attackers can exploit software, firmware, or network protocol weaknesses to gain unauthorized access, manipulate data, or disrupt system operations (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin, 2023; Eian, Yong, Li, Qi, & Fatima, 2020).
- **Physical Security Risks:** The physical components of remote monitoring systems, such as sensors and communication devices installed across the network, can be targets for tampering, theft, or vandalism. Such incidents can lead to data loss, system downtime, and compromised water quality monitoring.
- **Data Privacy and Integrity Issues:** The vast amount of data collected and transmitted by remote monitoring systems requires stringent measures to ensure data privacy, integrity, and authenticity. Without robust encryption and authentication mechanisms, sensitive information could be intercepted, altered, or falsified (Nandy et al., 2019; Ratha, Connell, & Bolle, 2001).
- **System Complexity and Interconnectivity:** The complexity and interconnectivity of remote monitoring systems with other IT and operational technology (OT) systems increase the difficulty of securing these networks. Vulnerabilities in one system can potentially be exploited to gain access to or disrupt other systems within the utility's operational framework.

The implications of security breaches in remote monitoring systems extend beyond immediate operational disruptions. The potential impacts include:

- **Public Health Risks:** Compromise of water quality monitoring systems can lead to undetected contamination events, posing serious risks to public health. Failure to promptly identify and address water quality issues can result in waterborne disease outbreaks and long-term health effects.
- **Safety Concerns:** Security breaches that affect the control mechanisms of water distribution can lead to over-pressurization or under-pressurization incidents, risking infrastructure damage and posing safety hazards to the public and utility workers.
- **Loss of Public Trust:** Incidents that compromise the security and reliability of water distribution networks can erode public trust in utility providers. Restoring confidence after a security breach can be challenging and costly, requiring significant efforts to reinforce system security and engage transparently with the community.
- **Economic and Regulatory Repercussions:** Security breaches can also have economic implications, including the costs associated with system recovery, regulatory fines for non-compliance with water quality standards, and potential litigation. Utilities may face increased insurance premiums and the need for significant investment in security enhancements.

Securing remote monitoring systems is not just a technical necessity but a critical component of ensuring public health, safety, and trust. It requires a comprehensive approach that addresses cybersecurity, physical security, data protection, and system resilience to safeguard against the diverse range of threats water distribution networks face.

Theoretical Frameworks for Security

The security of remote monitoring systems in water distribution networks is paramount to ensuring water services' safe and efficient delivery. This section delves into various theoretical frameworks underpinning these systems' security, including cybersecurity frameworks, risk management models, and the principles of encryption, authentication, and data integrity. It also explores how these theoretical concepts are applied in the context of remote monitoring for water distribution, highlighting the complexities and unique challenges faced by this critical infrastructure.

Cybersecurity Frameworks

Cybersecurity frameworks provide structured approaches for managing and mitigating cybersecurity risks. They offer a set of guidelines, best practices, and standards designed to protect the integrity, confidentiality, and availability of information systems (Trim & Lee, 2016). In the context of remote monitoring systems for water distribution, these frameworks are crucial for establishing a comprehensive security strategy. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a prominent example, which outlines five core functions: Identify, Protect, Detect, Respond, and Recover. This framework helps water utilities identify critical assets and vulnerabilities, implement protective measures, detect and respond to cybersecurity events, and recover from incidents to ensure continuous service delivery (Krumay, Bernroider, & Walser, 2018; Mylrea, Gourisetti, & Nicholls, 2017).

Risk Management Models

Risk management models are essential for assessing and managing the risks associated with remote monitoring systems. These models involve identifying potential threats, assessing vulnerabilities, determining the likelihood and impact of security breaches, and implementing measures to mitigate risks. The ISO 31000 standard provides guidelines for risk management,

emphasizing a systematic, transparent, and reliable process. In the water distribution sector, applying these models helps utilities prioritize resources and focus on high-risk areas, ensuring that security measures are effective and cost-efficient (Björnsdóttir, Jensson, de Boer, & Thorsteinsson, 2022; Hutchins, 2018).

Encryption, Authentication, and Data Integrity Measures

The theoretical underpinnings of encryption, authentication, and data integrity are fundamental to securing remote monitoring systems. Encryption algorithms ensure that data transmitted between sensors, control units, and central monitoring stations is unreadable to unauthorized parties. Authentication mechanisms verify the identity of users and devices, preventing unauthorized access to the system. Data integrity measures, such as cryptographic hash functions and digital signatures, ensure that data has not been tampered with during transmission or storage.

- Encryption is critical in protecting the confidentiality of sensitive information, including water quality parameters and system operation data. Advanced encryption standards (AES) and public-key infrastructure (PKI) are commonly used to secure communications in remote monitoring systems (Mousavi & Ghaffari, 2021; Prasath, Jayakumar, & Karthikeyan, 2019).
- Authentication involves techniques such as two-factor authentication (2FA), digital certificates, and biometric verification to ensure that only authorized personnel and devices can access the system.
- Data integrity measures are essential for maintaining trust in the system's data, ensuring that the information used for decision-making is accurate and reliable.

Application in Water Distribution

Applying these theoretical frameworks and security measures to remote monitoring systems in water distribution networks involves addressing unique challenges. The dispersed nature of these networks and the criticality of uninterrupted water supply necessitate robust security measures resilient to cyber and physical threats. Implementing encryption and authentication requires careful consideration of the system's operational requirements and constraints, such as the need for real-time data processing and the limitations of low-power sensor networks (Granjal, Monteiro, & Silva, 2015).

The integration of these theoretical insights into practical security strategies ensures that remote monitoring systems are not only protected against current threats but are also adaptable to future challenges. By applying these frameworks, water utilities can enhance the security of their infrastructure, safeguard public health, and maintain the trust of the communities they serve. This theoretical foundation supports the development of secure, resilient, and reliable water distribution systems that can withstand the evolving landscape of cybersecurity threats (Ifinedo, 2012).

Security Challenges in Water Distribution Networks

Securing water distribution networks, especially those equipped with remote monitoring technologies, presents unique challenges. Integrating Information and Communication Technology (ICT) into these critical infrastructures has revolutionized how they are operated and managed. However, it has also introduced complexities that necessitate a reevaluation of security strategies. This section delves into the unique security challenges faced by the water distribution sector, the complexities introduced by remote monitoring technologies, and the interplay between physical security and cybersecurity within this context.

Unique Security Challenges in the Water Distribution Sector

a) Wide Geographic Spread: Water distribution networks cover vast areas, often spanning remote and inaccessible regions. This wide geographic spread makes it difficult to monitor and protect all network components physically. Remote monitoring systems help bridge this gap by providing real-time data from across the network. However, this reliance on digital connectivity opens up new avenues for cyber-attacks.
b) Complexity of Systems: The inherent complexity of water distribution networks, with their interconnected and interdependent components, adds another layer of difficulty. A security breach in one part of the system can have cascading effects, potentially compromising the entire network. The challenge lies in securing a complex, dynamically changing environment without hindering its operational efficiency.
c) Legacy Systems and Integration Issues: Many water distribution networks have evolved over decades, incorporating a mix of old and new technologies. Integrating remote monitoring systems with legacy infrastructure often requires custom solutions, which can introduce vulnerabilities if not properly secured. The heterogeneity of these systems complicates the implementation of uniform security measures.
d) Limited Resources: Water utilities, especially in developing regions, often operate with limited resources, both in terms of funding and technical expertise. Allocating sufficient resources for cybersecurity can be challenging, making these systems more vulnerable to attacks.

Complexities Introduced by Remote Monitoring Technologies

Remote monitoring technologies, while providing numerous benefits, also introduce several complexities:

a) Data Security and Privacy: These systems generate and transmit vast amounts of sensitive data. Ensuring the confidentiality, integrity, and availability of this data is paramount. Cyber-attacks targeting data in transit or at rest can lead to data breaches, compromising personal information and operational secrets.
b) Dependency on Communication Networks: Remote monitoring relies heavily on communication networks. Disruptions to these networks, whether through cyber-attacks such as Denial of Service (DoS) or physical infrastructure damage, can render remote monitoring systems inoperative, leaving the water distribution network blind to real-time conditions.
c) Software Vulnerabilities: Remote monitoring systems are software-driven. Software vulnerabilities, if exploited, can provide attackers access to control systems, allowing them to manipulate the distribution process, alter water treatment protocols, or shut down critical components.

The security of water distribution networks is no longer just about guarding physical assets against unauthorized access or tampering. The interplay between physical security and cybersecurity is critical in remote monitoring technologies. Cyber-physical attacks, where cyber breaches have direct physical consequences, are a real threat. For example, a cyber-attack that takes control of valve operations can lead to physical damage, service disruptions, or even

catastrophic failures in the distribution system (Ashibani & Mahmoud, 2017; Ryu, Kim, & Um, 2009).

Addressing these security challenges requires a holistic approach encompassing physical and cyber dimensions. It involves protecting the digital interfaces and data and ensuring the resilience of physical components against cyber-induced manipulations. This dual focus is essential for maintaining the integrity, reliability, and trust in water distribution networks equipped with remote monitoring technologies. The interconnectivity between physical and cyber systems demands integrated security strategies that can pre-empt, withstand, and quickly recover from all attacks, ensuring a continuous and safe water supply to all users.

Lessons Learned from Africa-US Projects

The collaboration between African countries and the United States in enhancing the security of remote monitoring systems in water distribution networks has yielded valuable insights and practical strategies. These projects have served as real-world laboratories for testing and refining theoretical concepts, confronting security challenges, and developing effective practices for safeguarding critical water infrastructure. This section synthesizes the lessons learned from these collaborative efforts, highlighting the theoretical insights gained, the strategies employed to address security challenges, and the key takeaways for securing remote monitoring systems.

Synthesis of Theoretical Insights

Collaborative projects between Africa and the US have underscored the importance of a multi-layered theoretical approach to security, integrating concepts from cybersecurity frameworks, risk management models, and physical security principles. These projects have demonstrated that effective security in remote monitoring systems is not solely about applying the latest technologies but also about understanding and implementing foundational security principles. Encryption, authentication, and data integrity measures are crucial underpinnings for protecting data in transit and at rest. Moreover, the application of risk management models has guided the identification, assessment, and prioritization of threats, enabling targeted and efficient allocation of resources to mitigate risks.

Addressing Security Challenges

The unique security challenges in the water distribution sector, such as the need to protect against both cyber and physical threats, have been a focal point of Africa-US collaborative projects. These initiatives have highlighted the complexities introduced by remote monitoring technologies, including the increased attack surface and the potential for sophisticated cyber-attacks that can manipulate data or disrupt operations. Projects have tackled these challenges by developing and implementing comprehensive security strategies that encompass both cyber and physical dimensions. This includes the deployment of intrusion detection systems, the establishment of secure communication channels, and the physical hardening of critical infrastructure components.

Effective Strategies and Practices

Several key strategies and practices for securing remote monitoring systems have emerged from Africa-US collaborative projects:

- Integrated Security Approach: Successful projects have adopted an integrated approach to security, treating cyber and physical security as interconnected components rather than

separate entities. This holistic view has facilitated the development of comprehensive security measures that address the full spectrum of potential vulnerabilities.

- Community Engagement and Training: Engaging local communities and training personnel in security best practices have been crucial in enhancing the resilience of water distribution systems. Projects have shown that well-informed and vigilant operators and users can act as a first line of defence against potential threats.
- Adoption of International Standards: The application of international cybersecurity standards and best practices has helped harmonize security efforts across different jurisdictions. This alignment has been particularly beneficial in projects spanning multiple countries, ensuring a consistent and high level of security across all participating nations.
- Continuous Monitoring and Incident Response: Implementing systems for continuous monitoring of network activity and having a robust incident response plan in place has been key to early detection and swift mitigation of security incidents. Projects have demonstrated the importance of preparedness and the ability to react quickly to potential breaches.

Key Takeaways

The collaboration between Africa and the US in securing remote monitoring systems in water distribution networks has highlighted several key takeaways:

- The necessity of adopting a multi-disciplinary approach to security, integrating theoretical insights and practical considerations.
- The importance of flexibility and adaptability in security practices to address the evolving landscape of threats and vulnerabilities.
- The value of international collaboration and knowledge sharing in fostering innovation and enhancing the effectiveness of security measures.

These lessons learned underscore the complexity of securing remote monitoring systems in water distribution networks and the need for ongoing collaboration, research, and innovation to address these challenges effectively.

Principles of Effective Security Practices

Developing and implementing secure remote monitoring systems in water distribution networks requires adherence to a set of fundamental principles derived from theoretical insights and practical lessons learned. These principles serve as guidelines for effectively designing, implementing, and managing security measures. They consider the need for scalability, adaptability, and sustainability in security practices, ensuring that the systems remain resilient against evolving threats while supporting the critical operations of water distribution networks.

A) Principle 1: Defense in Depth

Defence in depth is a strategy that employs multiple layers of security controls throughout the information system. Derived from military strategy, this principle applies to securing remote monitoring systems by integrating various defensive mechanisms at different layers. It includes physical security measures, network security controls, application security, and data encryption, ensuring that if one layer is breached, others still provide protection.

B) Principle 2: Least Privilege

The least privilege principle requires that users and systems are granted the minimum levels of access—or permissions—needed to perform their functions. This principle minimizes the potential impact of a security breach by restricting access to sensitive information and critical system functionalities to only those entities that absolutely require it. In remote monitoring

systems, implementing the least privilege can prevent unauthorized access and limit the damage from insider threats.

C) Principle 3: Segmentation and Isolation

Segmentation and isolation involve dividing network resources into separate zones and applying controls to limit access between them. This approach is crucial for protecting critical parts of the network, such as the operational technology (OT) networks used in water distribution systems, from vulnerabilities in less secure areas, like corporate IT networks. Segmentation helps in containing security breaches, making it harder for attackers to move laterally within the network.

D) Principle 4: Continuous Monitoring and Response

Effective security practices entail continuously monitoring network activity and implementing a proactive incident response plan. Continuous monitoring allows for the early detection of anomalies and potential security incidents, enabling timely interventions. An established incident response plan ensures that the organization can quickly contain and mitigate the impact of security breaches, minimizing downtime and operational disruption.

E) Principle 5: Security by Design

Security by design emphasizes the integration of security measures from the earliest stages of system development rather than as an afterthought. This principle advocates for the inclusion of security considerations in the design, development, and deployment phases of remote monitoring systems. Prioritizing security from the start can identify and mitigate vulnerabilities early, leading to more robust and resilient systems.

F) Principle 6: Scalability and Flexibility

Security solutions must be scalable and flexible to accommodate water distribution networks' growth and changing needs. As networks expand or incorporate new technologies, security systems should be capable of scaling up without significant redesigns. Flexibility is also crucial to adapt to the evolving threat landscape, allowing for integrating new security technologies and practices as they become available.

G) Principle 7: Sustainability and Maintainability

Sustainability and maintainability are critical for the long-term effectiveness of security measures. This principle focuses on designing systems that are both environmentally sustainable and maintainable with reasonable effort and cost. Security practices should include regular updates, patches, and reviews to ensure they remain effective against new threats. Additionally, consideration of energy-efficient technologies contributes to the system's sustainability as a whole.

H) Principle 8: Stakeholder Engagement and Training

Engaging stakeholders and providing continuous training are essential for maintaining security awareness and preparedness. This includes educating system operators, users, and management on the importance of security practices and their roles in maintaining them. Training programs should be updated regularly to reflect the latest security trends and threats.

Incorporating these principles into the design, implementation, and management of remote monitoring systems ensures a comprehensive approach to security. By considering scalability, adaptability, and sustainability, these practices protect against current threats and provide a foundation for responding to future challenges in securing water distribution networks.

Challenges and Future Directions

Securing remote monitoring systems in water distribution networks presents ongoing challenges that require continuous attention and adaptation. As these systems become increasingly integral to managing and operating water distribution networks, their security implications become more complex and critical. This section explores the current challenges, the role of emerging technologies and theoretical developments, and future research directions to enhance security measures.

One of the primary challenges in securing remote monitoring systems is the evolving nature of cyber threats. Attackers continually develop new methods and tools to exploit vulnerabilities, making it difficult for security measures to remain effective over time. Additionally, integrating these systems with existing infrastructure often involves legacy technologies that may not have been designed with modern security threats in mind, creating potential weak points in the network. The vast and distributed nature of water distribution networks also complicates security efforts. Ensuring consistent security practices across different locations and systems can be challenging, especially in regions with limited resources and expertise. Furthermore, balancing security with operational efficiency and user accessibility adds a layer of complexity to designing and implementing effective security measures.

Emerging technologies, such as artificial intelligence (AI) and blockchain, offer promising avenues for enhancing the security of remote monitoring systems. AI can be used to detect anomalies and potential security threats in real time, improving the responsiveness of security measures. With its decentralized and tamper-resistant ledger, blockchain technology offers a new approach to ensuring data integrity and traceability, which are crucial for the reliable operation of water distribution networks. Theoretical developments in cybersecurity, risk management, and system resilience also play a critical role in shaping future security practices. Advances in these areas can provide a deeper understanding of the threat landscape and inform the development of more robust and adaptive security frameworks. Incorporating these theoretical insights into practical security strategies can enhance the effectiveness of measures designed to protect remote monitoring systems.

Future research should focus on developing holistic and adaptive security frameworks that can evolve in response to new threats and technological advancements. This includes exploring the use of machine learning algorithms for predictive threat analysis, investigating the potential of blockchain for secure data management, and developing standardized security protocols that can be easily implemented across different systems and regions.

There is also a need for research into cost-effective security solutions that can be deployed in resource-constrained environments. Ensuring the accessibility of advanced security technologies to all parts of the world is crucial for the global resilience of water distribution networks.

CONCLUSION

The review of theoretical insights and lessons learned from Africa-US projects underscores the importance of a comprehensive approach to securing remote monitoring systems in water distribution networks. These insights highlight the necessity of integrating theoretical frameworks with practical experiences to develop security measures that are both effective and adaptable to changing conditions.

The collaboration between countries and across disciplines has been instrumental in advancing our understanding of the security challenges and opportunities presented by remote monitoring

systems. However, as threats continue to evolve and new technologies emerge, the need for continued collaboration and research becomes ever more critical. By working together, stakeholders can develop innovative solutions and strategies to address the complex security challenges facing water distribution networks, ensuring their reliability and safety for years to come.

This call to action emphasizes the ongoing journey towards securing critical water infrastructure. It is a collective effort that requires the engagement of researchers, practitioners, policymakers, and the global community to safeguard one of our most vital resources.

References

Aisopou, A., Stoianov, I., & Graham, N. J. (2012). In-pipe water quality monitoring in water supply systems under steady and unsteady state flow conditions: A quantitative assessment. *Water Research, 46*(1), 235-246.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68*, 81-97.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333.

Berkeley, A. R., Wallace, M., & Coo, C. (2010). A framework for establishing critical infrastructure resilience goals. *Final report and recommendations by the council, national infrastructure advisory council*, 18-21.

Björnsdóttir, S. H., Jensson, P., de Boer, R. J., & Thorsteinsson, S. E. (2022). The Importance of Risk Management: What is Missing in ISO Standards? *Risk Analysis, 42*(4), 659-691.

Chaterji, S., Naghizadeh, P., Alam, M. A., Bagchi, S., Chiang, M., Corman, D., . . . Mou, S. (2019). Resilient cyberphysical systems and their application drivers: A technology roadmap. *arXiv preprint arXiv:2001.00090*.

Dargin, J. S., & Mostafavi, A. (2020). Human-centric infrastructure resilience: Uncovering well-being risk disparity due to infrastructure disruptions in disasters. *PloS One, 15*(6), e0234381.

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber attacks in the era of covid-19 and possible solution domains.

Ge, Y., Zhang, G., Meqdad, M. N., & Chen, S. (2023). A systematic and comprehensive review and investigation of intelligent IoT-based healthcare systems in rural societies and governments. *Artificial Intelligence in Medicine*, 102702.

Geels, F. (2005). Co-evolution of technology and society: The transition in water supply and personal hygiene in the Netherlands (1850–1930)—a case study in multi-level perspective. *Technology in Society, 27*(3), 363-397.

Glasgow, H. B., Burkholder, J. M., Reed, R. E., Lewitus, A. J., & Kleinman, J. E. (2004). Real-time remote monitoring of water quality: a review of current applications, and advancements in sensor, telemetry, and computing technologies. *Journal of Experimental Marine Biology and Ecology, 300*(1-2), 409-448.

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey. *Ad Hoc Networks, 24*, 264-287.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks, 169*, 107094.

Harshadeep, N. R., & Young, W. (2020). Disruptive technologies for improving water security in large river basins. *Water, 12*(10), 2783.

Hutchins, G. (2018). *ISO 31000: 2018 enterprise risk management*: Greg Hutchins.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Katina, P. F., & Keating, C. B. (2015). Critical infrastructures: A perspective from systems of systems. *International Journal of Critical Infrastructures, 11*(4), 316-344.

Krumay, B., Bernroider, E. W., & Walser, R. (2018). *Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework.* Paper presented at the Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber Security: Critical Infrastructure Protection* (pp. 3-42): Springer.

Mehvar, S., Wijnberg, K., Borsje, B., Kerle, N., Schraagen, J. M., Vinke-de Kruijf, J., . . . Hulscher, S. (2021). Towards resilient vital infrastructure systems–challenges, opportunities, and future research agenda. *Natural Hazards and Earth System Sciences, 21*(5), 1383-1407.

Mousavi, S. K., & Ghaffari, A. (2021). Data cryptography in the Internet of Things using the artificial bee colony algorithm in a smart irrigation system. *Journal of Information Security and Applications, 61*, 102945.

Mylrea, M., Gourisetti, S. N. G., & Nicholls, A. (2017). *An introduction to buildings cybersecurity framework.* Paper presented at the 2017 IEEE symposium series on computational intelligence (SSCI).

Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., . . . Bhattacharyya, S. (2019). Review on security of internet of things authentication mechanism. *IEEE Access, 7*, 151054-151089.

Nova, K. (2023). AI-enabled water management systems: an analysis of system components and interdependencies for water conservation. *Eigenpub Review of Science and Technology, 7*(1), 105-124.

Park, J., Kim, K. T., & Lee, W. H. (2020). Recent advances in information and communications technology (ICT) and sensor technology for monitoring water quality. *Water, 12*(2), 510.

Prasath, J., Jayakumar, S., & Karthikeyan, K. (2019). Real-time implementation for secure monitoring of wastewater treatment plants using internet of things. *International Journal of Innovative Technology and Exploring Engineering, 9*(1), 2997-3002.

Raich, J. (2013). Review of sensors to monitor water quality. *European reference network for critical infrastructure protection (ERNCIP) project*.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal, 40*(3), 614-634.

Ryu, D. H., Kim, H., & Um, K. (2009). Reducing security vulnerabilities for critical infrastructure. *Journal of Loss Prevention in the Process Industries, 22*(6), 1020-1024.

Sänger, N., Heinzel, C., & Sandholz, S. (2021). Advancing resilience of critical health infrastructures to cascading impacts of water supply outages—insights from a systematic literature review. *Infrastructures, 6*(12), 177.

Sun, A. Y., & Scanlon, B. R. (2019). How can Big Data and machine learning benefit environment and water management: a survey of methods, applications, and future directions. *Environmental Research Letters, 14*(7), 073001.

Trim, P., & Lee, Y.-I. (2016). *Cyber security management: a governance, risk and compliance framework*: Routledge.