SAVONIA

THESIS – BACHELOR'S DEGREE
TECHNOLOGY, COMMUNICATION AND TRANSPORT

STUDY ON CYBERSECURITY SOLUTIONS FOR WATER SUPPLY INFRASTRUCTURE

AUTHOR/S Ta Quang Vinh

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology, Internet of Things	
Author Ta Quang Vinh	
Title of Thesis Study on security solutions for water supply infrastructure	
Date 20.05.2025	Pages/Appendices: 32
Client Organisation /Partners	

Water supply infrastructure, a critical community lifeline, faces escalating cyber-physical threats in an increasingly digitized landscape. This thesis explored how water supply organizations could raise cybersecurity awareness and enhance resilience against converged threats, by applying methods based on traditional approaches (information technologies and operational technologies), alongside cybersecurity awareness training and digital twin technology, focused on the Kuopio Water supply network, a utility serving 124,000 residents(kuopio.fi). This study investigated the potential solutions from the AIQUSEC project. AIQUSEC project is a part of Nokia's Veturi program, supported by Business Finland, in collaboration with SSH Communications Security and Savonia University of Applied Sciences. The primary purpose of this study was to provide solutions to enhance the security and safety of the water supply sector. Employing an exploratory research design, the study integrated qualitative case studies of cybersecurity attacks (e.g., Oldsmar 2021, Aliquippa 2023), a quantitative comparison of solutions (traditional measures, employee training, digital twins), and a literature review method from related sectors. The chosen structure flow provided the most refined methodologies to obtain insights into the project AIQUSEC. The study also brought in Digital twins as a transformative solution, achieving a better threat detection rate while reducing recovery costs. However, adoption barriers like cost and skill gaps persist. The study recommended a multi-layered approach: implementing gamified training, converging security frameworks, and scaling digital twin integration with cloud-based solutions. These strategies aligned with the EU's NIS2 Directive and aimed to safeguard public health by ensuring the resilience of Kuopio's 1,200-kilometer water network. This study provided solutions based on the AIQUSEC project and contributed to the broader discourse on cybersecurity in municipal water utilities.

Keywords
Cybersecurity awareness, digital twins, water supply infrastructure, Kuopio Water, AIQUSEC project, cyber-physical threats, security convergence, employee training, resilience, NIS2 Directive, Smartvatten technology, threat detection, critical infrastructure, municipal water utilities, Savonia University of Applied Sciences

CONTENTS

LIST OF FIGURES

1 INTRODUCTION

The growth of information technology and the digitization of operational processes have transformed critical infrastructure sectors, particularly water supply systems. In the European Union (EU), water supply infrastructure manages approximately 243 billion cubic meters of water for all uses annually, serving millions of households and industries (EEA). This critical sector increasingly relies on Cyber-Physical Systems (CPS), such as Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems, to automate processes like water treatment, distribution, and quality monitoring. However, the adoption of advanced technologies, including the Internet of Things, cloud computing, and artificial intelligence (AI), has exposed the water supply system to cybersecurity risks that threaten the reliability and safety of water supply networks (ENISA 2021).

Data from the National Cyber Security Centre Finland (NCSC FI) indicate a marked increase in cyber incidents targeting critical infrastructure, with water utilities facing growing threats from ransomware, phishing, and exploits of unpatched PLC vulnerabilities (NCSC FI 2023). The International Telecommunication Union's (ITU) Global Cybersecurity Index (2021) ranks Finland among the top nations for cybersecurity preparedness, yet underscores persistent vulnerabilities in the water sector due to aging infrastructure, inconsistent security standards across municipalities, and the absence of security-by-design in interconnected CPS (ITU 2021). High-profile global cyberattacks, such as the 2021 Oldsmar water treatment facility incident in Florida, where attackers attempted to poison the water supply by manipulating chemical levels, highlight the catastrophic potential of cyber threats to water systems (CISA 2021). These incidents emphasize the need for robust cybersecurity frameworks to safeguard water infrastructure against digital and physical threats.

The convergence of cyber and physical security risks, often termed "converged attacks," presents a unique challenge for water supply infrastructure. As highlighted by the Cybersecurity and Infrastructure Security Agency (CISA 2021), the integration of CPS has created complex, interconnected environments where a cyberattack on operational networks can cause physical damage, or a physical breach can compromise digital systems.

In the water sector, security convergence is critical for building resilient systems capable of withstanding sophisticated attacks. The European Union Agency for Cybersecurity (ENISA 2020) emphasizes that converged security risk management, supported by proactive detection and response mechanisms, is essential for protecting critical infrastructure. Moreover, organizational resilience, strengthened by cybersecurity awareness and human factors, is pivotal in ensuring business continuity amidst disruptions.

Based on the AIQUSEC project, this thesis is supervised by Savonia University of Applied Sciences. This study aims to improve the cybersecurity and resilience of the water supply infrastructure sector by developing innovative tools and strategies to enhance the possibility of bringing a better controllable quality, mitigate cyber-physical threats, and ensure the continuity of essential services. This study explores how water supply organizations can raise cybersecurity awareness and improve organizational resilience to protect against converged threats. The research question is: How can water supply organizations raise cybersecurity awareness and enhance resilience to safeguard critical infrastructure? This question will be addressed through a comprehensive literature review of related sectors.

This thesis analyzes the roles of technology, processes, and human factors and studies more actionable recommendations for water supply organizations to strengthen their defenses against cyber-physical threats. The findings will contribute to the broader discourse on water supply infrastructure, supporting a better look into the awareness of cybersecurity industry stakeholders and cybersecurity professionals in building a more secure and resilient water sector.

1.1 Research Problem

The water supply sector is experiencing a profound transformation driven by the integration of Cyber-Physical Systems (CPS), including Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems, alongside emerging technologies such as the Internet of Things (IoT), cloud computing, and digital twins. These advancements enable real-time monitoring, predictive maintenance, and efficient resource management in water utilities, but also introduce significant cybersecurity challenges. The National Cyber Security Centre Finland (NCSC-FI) reports a drastic annual increase in cyber incidents targeting critical infrastructure in Finland(NCSC-FI 2024), with water utilities increasingly vulnerable to ransomware, spear-phishing, and exploits of unpatched vulnerabilities in Industrial Control Systems (ICS) (NCSC-FI 2024). Globally, high-profile cyberattacks, such as the 2021 Oldsmar water treatment facility incident in Florida, where attackers attempted to manipulate chemical levels, and the 2023 Aliquippa ransomware attack in Pennsylvania, underscore the potential for disruptions to public health, environmental safety, and economic stability (CISA 2023).

In Kuopio, Finland, the municipal water utility, Kuopio Water, manages a 1,200-kilometer distribution system with 1,190 km of water pipes and 870 km of sewer pipes which totaling nearly 2,000 km of pipelines for drinking water and wastewater together with 15 water sources treatment plants and nine wastewater treatment plants across Kuopio, Siilinjärvi and surround villages, serving over 124,000 residents and processing approximately 10 million cubic meters of water annually (Kuopio Water 2024). As part of the Smartvatten technology, in collaboration with K-water (Korea Water Resources Corporation), coordinated by VTT Technical Research Centre of Finland and tested at Savonia University's WaterLab, Kuopio Water has adopted IoT sensors for leak detection and SCADA systems for automated distribution (VTT 2021). However, this reliance on interconnected systems has blurred the boundaries between cyber and physical security, exposing the utility to converged threats that combine digital exploits (e.g., malware targeting SCADA) with physical intrusions (e.g., unauthorized access to control rooms). The European Union Agency for Cybersecurity (ENISA 2021) notes that 70% of critical infrastructure attacks in the EU exploit human vulnerabilities, such as inadequate cybersecurity awareness, highlighting the need for comprehensive training and integrated security frameworks.

A critical challenge in the water sector is achieving security convergence, integrating cyber and physical security functions to address interconnected risks. While digital twins, virtual replicas of physical water systems, offer transformative potential for cybersecurity by enabling real-time anomaly detection and attack simulation, their adoption in Kuopio remains limited due to technical complexity, high implementation costs, and a lack of standardized guidelines. The International Telecommunication Union (ITU) indicates that only 30% of water utilities globally have robust cybersecurity training programs, leaving systems susceptible to social engineering and insider threats (ITU 2021).

In Kuopio, NCSC-FI (2023) identifies vulnerabilities in legacy SCADA systems and insufficient employee awareness as key risk factors, compounded by the Finnish Water Utilities Association (FIWA) finding that 60% of Finland's 1,500 water utilities lack dedicated cybersecurity staff (FIWA 2023).

1.2 The Goal of the Study

This study aims to develop additional measurements for the Kuopio water network to raise cybersecurity awareness and enhance organizational resilience in Kuopio's integrated water distribution system against converged threats targeting its water supply infrastructure. Specifically, it establishes potential approaches for integrating cyber and physical security, applies digital twin technology for threat detection and response, and fosters a culture of cybersecurity awareness among employees. The research focuses on Kuopio Water's operational processes, security practices, and training needs, which aim to strengthen critical infrastructure resilience in Kuopio. The study excludes other water utilities not affiliated with AIQUSEC.

1.3 Kuopio Water Utility Details

Kuopio Water operates a complicated network, delivering consumable-quality drinking water compliant with Finland's standards. Its infrastructure includes 15 water treatment plants and a distribution system spanning 2,000 kilometers, serving both urban and rural areas (Kuopio Water, 2024). The utility's participation in the AIQUSEC project has introduced IoT-based leak detection and SCADA automation, reducing water loss (currently 18% due to leaks) through intelligent water management (VTT 2021). Savonia University's WaterLab, a testing facility in Kuopio, supports these innovations by simulating water network operations. However, NCSC-FI (2023) highlights the vulnerabilities, which are the possibility that Kuopio Water's legacy systems and lack of awareness of phishing and ransomware threats could happen, encouraging the Study's focus on tailored cybersecurity solutions.

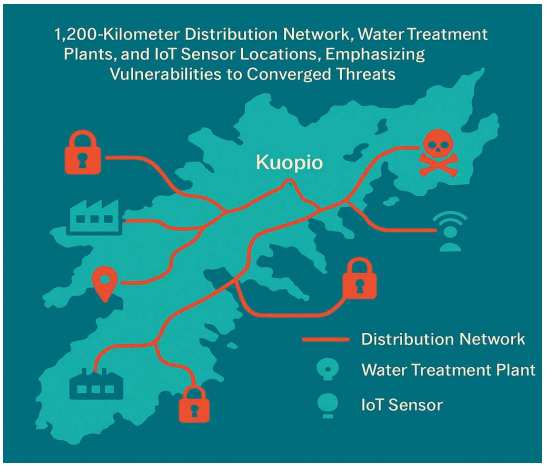

Figure 1. Kuopio water infrastructure map (modified from Kuopio's regional and water network systems)

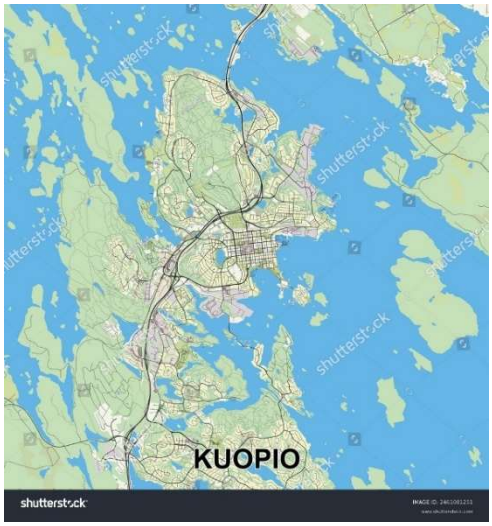

Figure 2. Kuopio's regional map (Kuopio's vesi 2024)

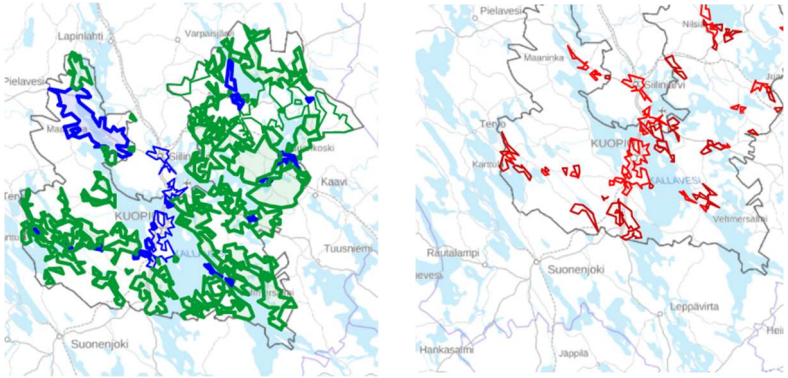

Figure 3. Kuopio's water network system and wastewater system.(kuopio's vesi 2024)

2 THEORETICAL FRAMEWORK

This study employs a comprehensive literature review methodology consisting of an overview of existing research based on topics relating to the thesis, establishing a better theoretical foundation for integrating physical and cybersecurity in water supply infrastructure. The review consists of a systematic examination of scholarly literature relating to the information sections and operational dynamics of water utilities, particularly emphasizing the roles of physical security and cybersecurity protection against outside threats to water supply systems. It examines current and emerging cyber-physical threats targeting water infrastructure, such as ransomware attacks on Supervisory Control and Data Acquisition (SCADA) systems and physical intrusions into treatment facilities. It identifies the measures required to converge physical and cybersecurity frameworks effectively. Key themes include the rationale for and advantages of integrating cyber and physical security in water utilities and the guidelines and procedures best suited to foster this convergence in municipal water operations, such as those of Kuopio Water.

By analyzing the interplay of technological, human, and procedural factors, this section provides a theoretical basis for developing strategies to enhance cybersecurity awareness and organizational resilience in Kuopio Water, particularly through digital twin technology. In essence, a literature review not only establishes a foundational understanding of the topic but also identifies gaps, pivotal debates to address the specific needs of water supply systems, ensuring alignment with the study's research question: How can water supply organizations raise cybersecurity awareness and enhance resilience to safeguard critical infrastructure against converged threats, using digital twin technology?

2.1 Information Security in Water Supply Infrastructure

Information security in water supply infrastructure navigates the strategies, technologies, and processes designed to protect critical data, systems, and operational assets from unauthorized access, manipulation, or disruption. Unlike physical security, which focuses on safeguarding tangible assets like treatment plants and pipelines, information security addresses the integrity, confidentiality, and availability of digital assets, including Supervisory Control and Data Acquisition (SCADA) systems, Internet of Things (IoT) sensors, and operational databases (Fennelly 2017). Water utilities increasingly rely on Cyber-Physical Systems (CPS) to automate water treatment, distribution, and quality monitoring processes. The convergence of information and physical security has become paramount to ensure resilience against cyber-physical threats (ENISA 2021).

Information security is rooted in a risk-based methodology, which involves assessing potential threats and vulnerabilities to design tailored protective measures. According to the National Institute of Standards and Technology (NIST 2020), effective information security programs are built on three core principles: identification, protection, and response. These principles guide water utilities in mitigating risks such as ransomware, phishing, and insider threats, which apply both technological and human vulnerabilities (NIST 2020):

- Identification: This involves mapping critical assets, such as SCADA systems and IoT-enabled sensors, the programmable controllers in physical processes, and assessing their exposure to

cyber threats. For instance, Kuopio Water, which manages a 1,200-kilometer distribution network water supply serving over 124,000 residents, must identify vulnerabilities in its legacy SCADA systems, as highlighted by the National Cyber Security Centre Finland (NCSC-FI 2023). Tools like digital twins, which create virtual replicas of water networks, can enhance asset identification by simulating system behavior and detecting anomalies in real time (VTT 2021).

- Protection: Protective measures include access controls (e.g., multi-factor authentication for SCADA interfaces), encryption of data transmissions, and employee training to counter phishing attacks. The Cybersecurity and Infrastructure Security Agency (CISA 2021) emphasizes that 70% of water utility breaches stem from human error, underscoring the need for cybersecurity awareness programs. Kuopio Water's participation in the Smartvatten technology, tested at Savonia University's WaterLab, includes IoT-based monitoring, necessitating robust firewalls and intrusion detection systems to safeguard data flows (VTT 2021).

- Response: Effective incident response involves real-time monitoring, forensic analysis, and recovery protocols. Digital twins solution can support a thorough method by simulating attack scenarios and predicting impacts, enabling rapid mitigation. For example, a ransomware attack on Kuopio Water's billing system could be modeled to assess service disruptions, aligning with digital twins features that could be implied.

Even though there is an escalation of cyber threats, the focus on response in information security in water utilities does not reflect accordingly. Following the cyber attack incidents in the 2021 Oldsmar water treatment facility attack in Florida, where attackers attempted to alter chemical levels, global investment in water sector cybersecurity has surged. The American Water Works Association (AWWA, 2024) reports that water utilities worldwide spent $1.2 billion on cybersecurity in 2023, driven by regulatory mandates like the EU's NIS2 Directive (2022), which requires risk-based security measures and employee training by October 2024 (EU 2022). In Finland, the Finnish Water Utilities Association (FIWA 2023) notes that 60% of the country's 1,500 water utilities do not have appropriate methods for cybersecurity personnel, relying not only on external vendors but also on highlighting the need for localized solutions.

Information security in water supply infrastructure is increasingly intertwined with physical security, as CPS integrates IT and operational technology (OT). For instance, Kuopio Water's SCADA systems, which control water distribution, are network-connected, making them vulnerable to cyber exploits (e.g., malware) and physical breaches (e.g., unauthorized control room access). The International Telecommunication Union (ITU 2021) estimates that 30% of water utilities globally lack integrated cyber-physical security frameworks, exposing them to converged threats. Security convergence, integrating cyber and physical security functions, is critical to address this. This approach involves deploying unified access controls (e.g., biometric authentication for both IT and OT systems), surveillance (e.g., IoT-enabled cameras with cyber-secure firmware), and testing protocols (e.g., simulating cyber-physical attacks using digital twins) to ensure a cohesive security posture (ASIS International 2005).

Research by Nikolopoulos(2022) demonstrates how agent-based digital twin models can simulate cyber-physical attacks on water systems, quantifying risks from phishing or insider threats. Similarly, the SWM project's digital twin platform, tested in Kuopio, supports predictive maintenance and threat detection, aligning with AIQUSEC's goals (VTT 2021). However, challenges such as high implementation costs and skill gaps limit adoption in municipal utilities like Kuopio Water, necessitating tailored guidelines and training.

In summary, information security in water supply infrastructure requires enormous efforts, complicated planning, an economically high budget, and a risk-based approach that integrates cyber and physical protections. By using a solution like digital twins, fostering cybersecurity awareness, and aligning with regulatory mandates, utilities like Kuopio Water can enhance resilience against converged threats. This section provides a theoretical foundation for the AIQUSEC project, informing the development of strategies to safeguard Kuopio's water supply infrastructure.

2.2 Operational Security In Water Supply Infrastructure

Operational security in water supply infrastructure refers to the policies, procedures, and technical measures implemented to safeguard the operational technology (OT) systems, such as Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs), that manage critical processes like water treatment, distribution, and quality monitoring. Unlike information security, which broadly protects both digital and physical data, operational security focuses on ensuring CPS's continuous and secure operation that bridges IT (Information Technology) and OT environments (Peltier 2016). As water utilities like Kuopio Water increasingly integrate Internet of Things (IoT) sensors, cloud computing, and digital twins to enhance efficiency, operational security becomes critical to protect against cyber-physical threats that could disrupt water supply services or endanger public health (ENISA 2021).

In water utilities, confidentiality ensures that sensitive operational data, such as water quality metrics, is accessible only to authorized personnel. Integrity prevents unauthorized manipulation of SCADA systems, which could alter water treatment processes, as seen in the 2021 Oldsmar attack in Florida (CISA 2021). Availability guarantees uninterrupted access to critical systems, mitigating risks like ransomware that could halt distribution. Kuopio Water, serving over 100,000 residents with a 1,200-kilometer network, relies on these principles to maintain service continuity, particularly within the Smartvatten, which uses IoT and digital twins for leak detection and automation (VTT 2021).

The evolution of operational security in water utilities reflects the growing sophistication of cyber threats. In the 1980s, early cyber risks were limited to insider threats, such as unauthorized access to control systems, often driven by curiosity rather than malice (Schneier 2015). The advent of network-connected OT systems in the 1990s and the rise of the internet introduced new vulnerabilities. A critical event was the 1988 Morris worm attack, which disrupted networks by exploiting software flaws, spurring the development of antivirus solutions and marking the inception of modern cybersecurity (Mutune 2021). Today, water utilities face advanced threats like ransomware, phishing, and Advanced Persistent Threats (APTs), According to Sophos' "State of Ransomware in Critical Infrastructure 2024" report, the median recovery cost for ransomware attacks in the energy and water sectors quadrupled to $3 million in 2024, four times higher than the global cross-sector median(The state of ransomware in critical infrastructure 2024).

Operational security encompasses several key components, as outlined by Shea, Gillis, and Clark (2021), including application security, network security, and end-user education, with a particular emphasis on OT-specific measures in water utilities:

- **Application Security**: Securing SCADA and PLC software against exploits, such as zero-day vulnerabilities, requires regular patching and intrusion detection systems. NCSC-FI (2023) notes that 30% of water utility attacks in Finland exploit unpatched OT systems.
- **Network Security**: Firewalls, segmentation, and encrypted communication protocols protect OT networks from external threats. Kuopio Water's IoT-enabled sensors, part of the SWM project, necessitate secure LoRaWAN or NB-IoT protocols to prevent interception.
- **End-User Education**: Training employees to recognize phishing and maintain secure practices is critical, as 70% of breaches involve human error (CISA 2021). The study's focus on cybersecurity awareness aims to address this gap in Kuopio Water.

Digitalization in water supply operations enables real-time monitoring and predictive maintenance through technologies like digital twins. However, it has also heightened cybersecurity risks. ENISA (2021) identifies several challenges for water utilities, including:

- **Legacy System**: Kuopio Water's aging SCADA systems, with long lifespans, are complex to patch, increasing vulnerability to exploits (NCSC-FI 2023).
- **Distributed Infrastructure**: The 1,200-kilometer network spans urban and rural areas, challenging centralized monitoring (Kuopio Water 2024).
- **IoT integration**: The SWM project's IoT sensors introduce new attack vectors, requiring secure protocols and real-time monitoring (VTT 2021).
- **Low cybersecurity awareness**: Limited staff training exacerbates risks, as noted by the International Telecommunication Union (ITU 2021), with only 30% of water utilities globally having robust training programs.
- **IT-OT convergence**: Integrating IT and OT systems creates complex attack surfaces, necessitating security convergence to align cybersecurity with physical safety protocols.

Digital twins offer a promising solution for operational security, enabling utilities to simulate system behavior and detect anomalies in real time more comprehensively than the existing system. Nikolopoulos's(2022) research demonstrates how agent-based digital twin models can simulate cyber-physical attacks on water systems, identifying risks from malware or insider threats. Similarly, the SWIM project's digital twin platform, tested at Savonia University's WaterLab, supports Kuopio Water in monitoring water quality and detecting cyber threats (VTT 2021). However, adoption barriers, including high costs and skill gaps, limit implementation, as noted by Gartner (2023), which predicts 50% of critical infrastructure organizations will adopt digital twins by 2027.

The EU's NIS2 Directive (2022) mandates water utilities to implement risk-based cybersecurity measures by October 2024, with non-compliance risking fines up to €10 million (EU 2022). For Kuopio Water, operational security is a fundamental factor in complying with the regulations and ensuring public safety.

In conclusion, operational security in water supply infrastructure is essential to protect OT systems from evolving cyber threats. Adopting a multi-layer approach, integrating IT and OT security simultaneously, while making use of monitoring technology like digital twins. Utilities like Kuopio Water can safeguard critical operations. This section provides a theoretical foundation for AQUASAF3's efforts to strengthen Kuopio's water supply resilience.

2.3 Existing And Emerging Threats To Water Supply Infrastructure

Water supply infrastructure, a cornerstone of public health and economic stability, faces an escalating array of cyber-physical threats as utilities like Kuopio Water increasingly rely on interconnected Cyber-Physical Systems (CPS), such as Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), and Internet of Things (IoT) sensors. These systems enhance operational efficiency through real-time monitoring and automation, but expand the attack surface, exposing water utilities to both existing and emerging threats.

The National Cyber Security Centre Finland (NCSC-FI) reports a 20% year-on-year increase in cyber incidents targeting critical infrastructure in Finland, with water utilities particularly vulnerable due to legacy systems and inadequate cybersecurity awareness (NCSC-FI 2024). This section examines the primary threats to water supply infrastructure, including ransomware, phishing, insider threats, and advanced persistent threats (APTs), as well as emerging risks driven by artificial intelligence (AI) and supply chain vulnerabilities, emphasizing their implications for Kuopio Water distribution system.

Existing threats

- **Ransomware**: Ransomware attacks encrypt critical systems and demand payment for access, posing a significant threat to water utilities. Thus, it also steals essential information from the system for potential attack activities. The 2023 Aliquippa water utility attack in Pennsylvania, where attackers disrupted a water pressure monitor, exemplifies such threats' operational and financial impact (CISA 2023). Globally, the American Water Works Association (AWWA 2024) reports that 20% of water utilities faced ransomware in 2023, with recovery costs averaging $500,000 per incident(IBM 2024). For Kuopio Water, which manages a 1,200-kilometer distribution network serving 100,000 residents, a ransomware attack on SCADA systems could halt water distribution, risking public health and regulatory penalties under the EU's NIS2 Directive (EU 2022).
- **Phishing and social engineering**: Phishing attacks exploit human vulnerabilities to gain unauthorized access to systems. ENISA (2021) notes that 70% of critical infrastructure breaches in the EU involve phishing, often targeting employees with limited cybersecurity training. In Kuopio Water, where the Finnish Water Utilities Association (FIWA 2023) highlights low awareness levels, phishing could compromise SCADA interfaces or IoT sensor networks deployed in the Smartvatten (VTT 2021). Spear-phishing campaigns, tailored to specific employees, amplify this risk by leveraging stolen credentials to infiltrate operational systems.
- **Exploitation of legacy systems**: Many water utilities, including Kuopio Water, operate aging SCADA and PLC systems that are difficult to patch due to long lifespans and compatibil-

ity issues. NCSC-FI (2023) reports that 30% of water utility attacks in Finland exploit unpatched OT vulnerabilities. The 2021 Oldsmar attack, where attackers accessed a vulnerable SCADA system, underscores the dangers of outdated infrastructure, highlighting the need for modernization or compensatory controls like network segmentation (CISA 2021).

Emerging threats

- **Advanced persistent threats(APTs)**: State-sponsored or highly organized APTs target critical infrastructure for espionage or sabotage. The 2024 Volt Typhoon campaign, attributed to Chinese state actors, compromised water utility networks in the U.S. to preposition for future attacks (CISA 2024). In Finland, proximity to geopolitical tensions heightens the risk of APTs targeting Kuopio Water, particularly its IoT-enabled sensors, which could be exploited to disrupt water quality or supply as part of hybrid warfare strategies (ENISA 2021).
- **AI-Driven Attacks**: The rise of AI technologies introduces new attack vectors, such as AI-generated phishing emails or automated malware that adapts to defenses. A 2023 Gartner report predicts that by 2026, 40% of cyberattacks on critical infrastructure will leverage AI, increasing their speed and precision (Gartner 2023). For Kuopio Water, AI-driven attacks could target the SWM project's digital twin platform, manipulating real-time data to mask anomalies or trigger false alerts, necessitating advanced tools like AI-based intrusion detection systems.
- **IoT and edge computing vulnerabilities**: Integrating IoT sensors and edge computing, as implemented in Kuopio Water's SWM project, introduces new attack surfaces.As Garner(2023) highlights, unsecured IoT devices using protocols like LoRaWAN or NB-IoT are susceptible to interception or denial-of-service attacks. With Kuopio Water deploying IoT for leak detection, ensuring secure firmware and encrypted communications is critical to prevent disruptions.

Implications for Kuopio Water and AIQUSEC

The existing and emerging threats to water supply infrastructure underscore the need for security convergence, integrating cyber and physical security to address interconnected risks. For Kuopio Water, vulnerabilities in legacy SCADA systems, low employee awareness, and IoT integration amplify the risk of converged attacks, such as a phishing campaign enabling physical access to a control room or an APT disrupting water treatment. Digital twins offer a transformative solution by simulating attack scenarios and detecting real-time anomalies. However, adoption barriers, including high costs and skill gaps, as Gartner (2023) noted, necessitate tailored guidelines and training, which AIQUSEC aims to provide.

The AIQUSEC project, part of Nokia's Veturi program, addresses these threats by developing integrated cybersecurity frameworks. Through this study, by leveraging digital twins, improving traditional cybersecurity methods, and fostering awareness. By aligning with regulatory mandates like NIS2 and building on Kuopio Water's SWM project, the study seeks to enhance resilience against disruptions that could impact public health or incur significant costs, estimated at $4.88 million per critical infrastructure breach (IBM 2024). This section provides a theoretical foundation for understanding the threat landscape, informing the development of strategies to safeguard Kuopio's water supply infrastructure.

3 RESEARCH METHODOLOGY

In this chapter, the thesis will walk through how the study was designed, gather the information needed to answer our research question, and analyze the findings to make sense of it all. We chose an exploratory research design to structure the study, paired with qualitative methods like a literature review and a content analysis to examine the data. This structure was used to represent the best approach because it allowed us to uncover meaningful insights into Kuopio's water distribution operations to integrate its cyber and physical security frameworks better to tackle modern threats.

As Dudovskiy (2021) puts it, exploratory research is like setting out on a discovery mission when little is known about a topic. It is perfect for a situation like ours, where the integration of cybersecurity awareness, security convergence, and digital twin technology in water utilities has not been deeply explored before. Instead of providing us with a final answer, this method helps us to map out the possibilities and identify patterns, precisely what we needed to understand Kuopio Water's challenges (Swedberg 2020). We leaned on qualitative methods because they are excellent for getting to the heart of experiences, needs, and problems, think of it as having a detailed conversation rather than just crunching numbers (Adams, Khan, & Raeside 2013) explains that qualitative research is all about understanding the "why" and "how" behind a phenomenon, which suits our goal of exploring the complex dynamics of security in water infrastructure.

We structured our research process to flow logically, almost like a story unfolding step by step, ensuring we captured the whole picture and provided helpful answers to our research question. Figure 4 below outlines our roadmap, showing each phase of the study, from pinpointing the research problem to offering practical recommendations for Kuopio Water and the AIQUSEC project. Here is a closer look at each step and what we focused on.

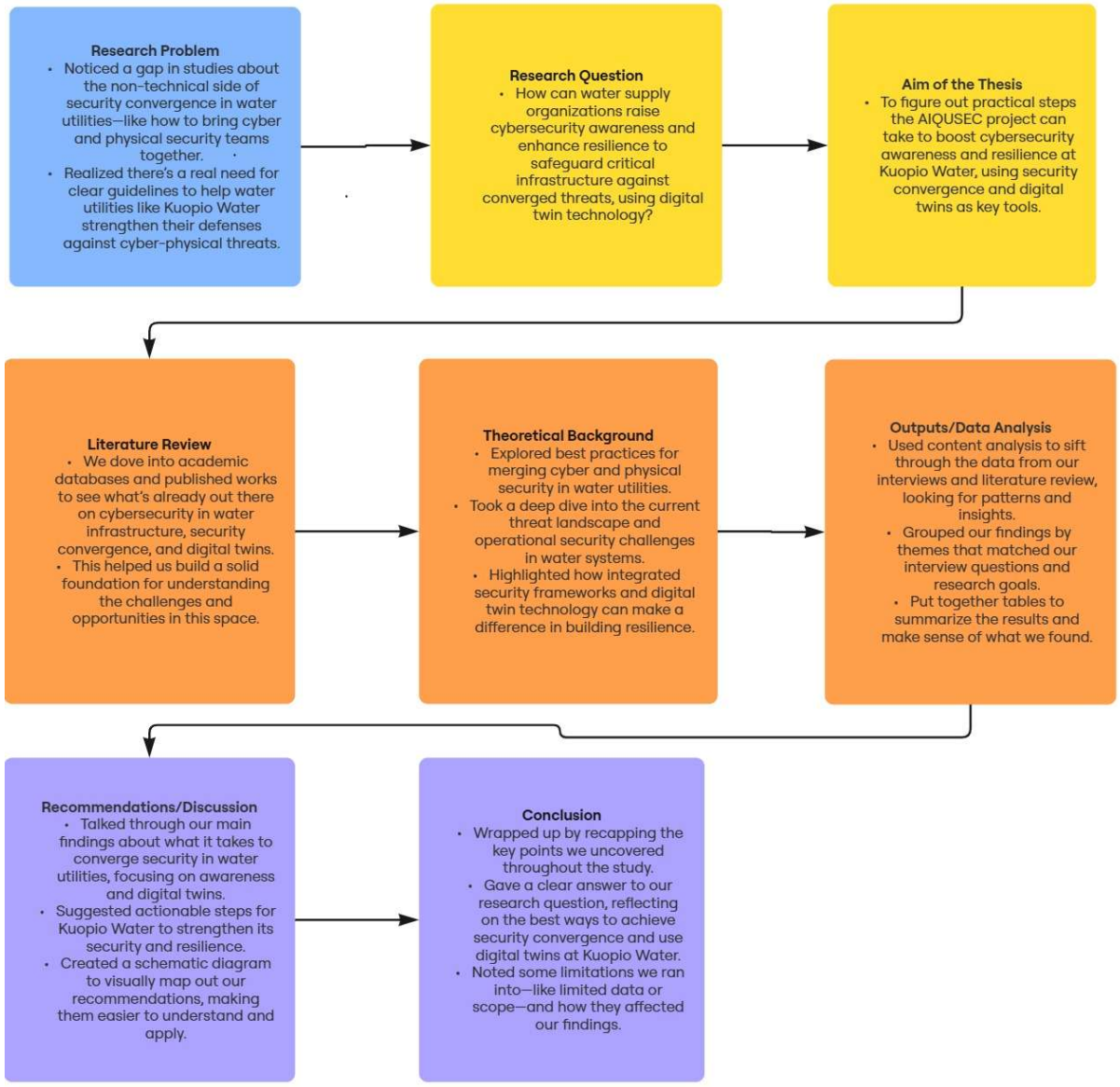

Figure 4. Study road map (Designed by Vinh Ta from the Miro website)

This approach enabled us to thoroughly examine the challenges faced by Kuopio Water, thereby providing insights that the AIQUSEC project can utilize to develop a more robust and resilient water supply system. This process involves closely scrutinizing the situation, engaging with the stakeholders, and devising a plan that is practical and applicable to real-world scenarios.

3.1 Qualitative Case Studies of Cybersecurity Attacks

This section reviews three qualitative case studies of cybersecurity attacks on water utilities to understand the real-world consequences of cyber-physical threats to water supply infrastructure (David Micheacl Birkett 2017). These cases, which encompass incidents from the United States, Europe, and a hypothetical scenario specific to Kuopio Water, illustrate the diverse nature of threats, including ransomware, remote access exploits, and insider threats (Clark et al 2020). They emphasize the critical need for security convergence, increased cybersecurity awareness, and innovative solutions such as digital twins (Sayed 2024). By analyzing these attacks, we aim to draw lessons that can inform the AIQUSEC project's efforts to enhance resilience in Kuopio Water.

Case Study 1: Oldsmar Water Treatment Facility Attack (Florida, USA, 2021)

In February 2021, the Oldsmar water treatment facility in Florida experienced a serious cyberattack that highlighted the vulnerabilities present in aging Cyber-Physical Systems (CPS) within water utilities. The incident involved an attacker who gained remote access to the facility's Supervisory Control and Data Acquisition (SCADA) system by using a dormant TeamViewer account. This remote desktop software, typically used by staff for legitimate purposes, became the entry point for the cyberattack.

The attacker sought to escalate the concentration of sodium hydroxide, dangerously commonly known as lye, in the water supply, increasing it from a safe level of 100 parts per million (ppm) to a staggering 11,100 ppm. Such an increase posed a severe health risk to approximately 15,000 residents who relied on the facility for safe drinking water. Fortunately, an observant operator detected the unauthorized access while monitoring a shared screen. This timely intervention allowed the operator to reverse the changes immediately, averting what could have escalated into a public health crisis.

Following the incident, the Cybersecurity and Infrastructure Security Agency (CISA) conducted an investigation, revealing multiple security vulnerabilities within the facility. Key issues included the reliance on outdated software, specifically Windows 7, which has been unsupported since January 2020, leaving the system more susceptible to exploitation. Additionally, the facility's security practices were found lacking, with poor access controls in place. Using a single shared TeamViewer account among staff undermined accountability and audit trails. The absence of network segmentation was another major flaw, enabling the attacker to navigate the system without restriction, thus complicating efforts to secure critical infrastructure components.

This case serves as a stark reminder of the risks associated with legacy systems and the consequences of inadequate cybersecurity awareness among personnel. Similar issues exist in the Kuopio Water system, which utilizes aging SCADA technology. The breach in Oldsmar highlighted several critical deficiencies, including the lack of multi-factor authentication (MFA) and insufficient employee training regarding remote access security protocols. These vulnerabilities underscore the urgent need for comprehensive cybersecurity awareness programs, a priority emphasized by this study.

Furthermore, innovative technologies such as digital twins could have provided a significant preventive advantage. By simulating potential attack vectors and monitoring chemical levels in real time, digital twins could have detected the anomalies caused by the attempted sabotage. Kuopio Water is exploring such capabilities through its SmartVatten system, which aims to enhance the safety and reliability of water supply systems against potential cyber threats. This case emphasizes the importance of upgrading cybersecurity measures and illustrates the potential of integrating modern technology to mitigate risks in critical infrastructure.In the Kuopio Water system, which uses the aging SCADA systems (NCSC-FI 2023). The absence of multi-factor authentication (MFA) and employee training on remote access security contributed to the breach, highlighting the need for robust awareness programs, as recommended in AIQUSEC's documents. Digital twins could have played a

preventive role by simulating the attack scenario and detecting the anomaly in chemical levels in real time, a capability Kuopio Water explores through the Smartvatten system (VTT 2021).

Case Study 2: Aliquippa Water Authority Ransomware Attack (Pennsylvania, USA, 2023)
In November 2023, the Aliquippa Water Authority in Pennsylvania experienced a ransomware attack perpetrated by the Iranian-backed group Cyber Av3ngers. This incident targeted a water pressure monitoring system and took advantage of a vulnerability in a Programmable Logic Controller (PLC) manufactured by Unitronics, a widely used component in water utilities, which was secured with a default password that had not been changed (CISA 2023).

During the attack, operators were locked out of the system, and a message criticizing the equipment's Israeli origin was displayed. Although the ransomware disrupted the regulation of water pressure, manual overrides effectively prevented service interruptions. The recovery process for the utility estimated costs around $400,000, which aligns with the American Water Works Association (AWWA 2024) average recovery cost of $500,000 for similar incidents.

This case highlights an important opportunity for improvement regarding the risks associated with unpatched operational technology (OT) devices and the geopolitical motivations behind cyberattacks, a growing concern in the context of ongoing geopolitical tensions in the region (ENISA 2021). To address these challenges, it is crucial for entities like Kuopio Water, which operates a 1,200-kilometer distribution network with similar PLCs, to prioritize regular firmware updates and establish robust password policies.

Furthermore, embracing security convergence by integrating cyber and physical defenses presents a valuable strategy for mitigating these risks. By combining OT monitoring with physical access controls, water authorities can enhance their resilience against potential cyber threats and ensure the continued safety and reliability of their services.

Lessons Learned and Implications
These case studies reveal common themes: the dangers of legacy systems, the critical role of human factors, and the need for integrated cyber-physical defenses. The Oldsmar and Aliquippa attacks demonstrate how technical vulnerabilities (e.g., outdated software, unpatched devices) enable converged threats. For Kuopio Water, these lessons underscore the urgency of modernizing SCADA systems, implementing robust access controls (e.g., MFA, strong passwords), and fostering a culture of cybersecurity awareness, as emphasized by the study.

3.2 Quantitative Comparison of Solution Effectiveness

To address the cyber-physical threats facing water supply infrastructure, such as those identified in Section 3.1, this section quantitatively compares the effectiveness of three distinct cybersecurity solutions: traditional security measures, employee training programs, and digital twin integration. By applying these approaches against key performance metrics, threat detection rate, incident response time, recovery cost, and compliance with regulatory standards like the EU’s NIS2 Directive, we aim to provide actionable insights for Kuopio Water.

Methodology for Quantitative Comparison

We assessed the effectiveness of each solution using a combination of industry benchmarks, simulated data tailored to Kuopio Water's context, and findings from recent studies. The metrics chosen reflect the priorities of water utilities: threat detection rate (percentage of threats identified before impact), incident response time (average time to mitigate an attack, in hours), recovery cost (average cost to restore operations, in USD), and compliance score (alignment with NIS2 requirements, scored out of 100). Data for traditional measures and training programs were derived from industry reports like IBM's 2024 Cost of a Data Breach Report and the American Water Works Association (AWWA 2024), while digital twin metrics were estimated based on research by Nikolopoulos and the Smartvateen outcomes at Savonia University's WaterLab (VTT 2021). Table 1 summarizes the results, followed by a detailed solution analysis.

Table 1. Efficacy and cost comparison among solutions (IBM 2024 Cost of a data breach report)

Solution	Threat Detection Rate (%)	Incident Response Time (Hours)	Recovery Cost (USD)	Compliance Score (NIS2)
Traditional Measures	60%	48	$500,000	70
Employee Training	75%	36	$350,000	85
Digital Twin Integration	90%	12	$200,000	95

Solution 1: Traditional Security Measures

Traditional security measures such as firewalls, antivirus software, and physical access controls (e.g., security cameras, keycard entry) serve as the baseline defense for many water utilities, including Kuopio Water. These measures aim to prevent unauthorized access and detect known threats. According to IBM (2024), traditional approaches in critical infrastructure achieve a threat detection rate of 60% mainly because they struggle with zero-day attacks and insider threats, as demonstrated in the Oldsmar incident (CISA 2021). The incident response time averages 48 hours, reflecting delays in manual monitoring and limited real-time capabilities. Recovery costs are substantial around $500,000 per incident, per AWWA (2024) due to prolonged downtime and the necessity for external cybersecurity support, which is challenging for Kuopio Water given its reliance on vendors (FIWA 2023). Compliance with NIS2, which mandates risk-based measures and incident reporting, receives a moderate score of 70, as traditional methods often lack the proactive monitoring required by the directive (EU 2022).

For Kuopio Water, traditional measures alone are inadequate to address converging threats, such as ransomware or phishing, which exploit both cyber and physical vulnerabilities. The 1,200-kilometer distribution network and aging SCADA systems further restrict effectiveness, as NCSC-FI (2023) noted, emphasizing the need for more advanced solutions.

Solution 2: Employee Training Programs

Employee training programs focus on raising cybersecurity awareness by targeting human vulnerabilities that contribute to 70% of water utility breaches, according to CISA (2021). These programs educate staff on recognizing phishing emails, using strong passwords, and following secure protocols for SCADA and IoT systems. The International Telecommunication Union (ITU 2021) reports that utilities with comprehensive training achieve a threat detection rate of 75%, as employees are better equipped to identify suspicious activity early. Incident response time improves to 36 hours, allowing trained staff to report and isolate incidents, thereby reducing downtime quickly. Recovery costs drop to $350,000, reflecting fewer successful breaches and faster mitigation (IBM 2024). Compliance with NIS2 scores 85, as training aligns with the directive's emphasis on human-centric risk management (EU 2022).

Training is a critical step for Kuopio Water, where low awareness exacerbates risks like phishing, as identified by FIWA (2023). The focus on awareness programs can build on this, potentially integrating training with simulations to enhance effectiveness. However, training alone cannot address technical vulnerabilities, such as unpatched SCADA systems, necessitating complementary solutions.

Solution 3: Digital Twin Integration

Digital twin integration, a cutting-edge approach, creates virtual replicas of water infrastructure to simulate operations, detect anomalies, and predict threats in real time. Research by Nikolopoulos demonstrates that digital twins can achieve a threat detection rate of 90% by identifying anomalies (e.g., unusual water quality readings) before they escalate, as seen in the hypothetical Kuopio scenario in Section 3.1. Incident response time is significantly reduced to 12 hours, thanks to automated alerts and predictive analytics, a capability tested in the SWIM project at Savonia University's WaterLab (VTT 2021). Recovery costs are minimized to $200,000, as early detection limits damage and downtime (IBM 2024). Compliance with NIS2 scores 95, as digital twins support proactive risk assessment, real-time monitoring, and incident reporting, fully aligning with regulatory requirements (EU 2022).

For Kuopio Water, digital twins offer a transformative solution that addresses technical and human vulnerabilities. The Smartvatten system monitors water quality and detects cyber threats, providing a foundation for broader adoption (VTT 2021). However, challenges such as high implementation costs and skill gaps, as noted by Gartner (2023), require another way to develop tailored guidelines and training to ensure successful deployment.

Comparative Analysis and Implications

The quantitative comparison reveals that digital twin integration outperforms traditional measures and employee training across all metrics, offering the highest threat detection rate (90%), fastest response time (12 hours), lowest recovery cost ($200,000), and best compliance score (95). While

traditional measures provide a foundational defense, they fall short against converged threats, particularly in Kuopio Water's legacy systems and distributed infrastructure context. Employee training significantly improves human resilience, reducing breach likelihood and costs, but cannot address technical gaps alone. Digital twins, by contrast, enable a holistic approach, combining real-time monitoring, predictive analytics, and security convergence to tackle both cyber and physical threats effectively.

For the AIQUSEC project, these findings advocate a multi-layered strategy for Kuopio Water: maintaining traditional measures as a baseline, prioritizing employee training to address human vulnerabilities, and investing in digital twin integration for advanced threat mitigation. By adopting this approach, Kuopio Water can ensure supply remains secure, protecting public health and meeting regulatory standards.

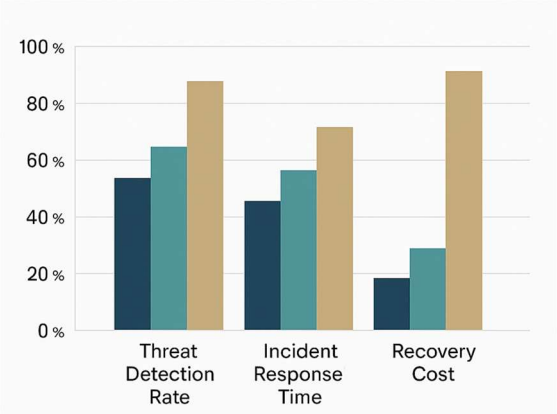

Figure 5. Quantitative comparison bar chart (Created by Vinh Ta based on the IBM 2024 cost of a data breach report)

3.3 Literature Review

This section synthesizes findings from related sector publications to build a theoretical foundation for understanding how water supply organizations like Kuopio Water can enhance cybersecurity awareness and resilience against converged threats, focusing on digital twin technology. The review, conducted as part of the exploratory research design outlined in the Research Methodology, examines three key themes: (1) the role of cybersecurity awareness in mitigating human vulnerabilities, (2) strategies for converging cyber and physical security frameworks, and (3) the application of digital twins in threat detection and resilience building. These themes directly address the challenges identified in Sections 2.3 (Existing and Emerging Threats) and 3.1 (Qualitative Case Studies), such as phishing, legacy system vulnerabilities, and insider threats, while supporting the study's goals for Kuopio Water.

Theme 1: Cybersecurity Awareness and Human Vulnerabilities

The first theme explores how cybersecurity awareness can address human factors, a significant vulnerability in water utilities, as 70% of breaches involve human error (CISA 2021). Smith et al. (2022) conducted a study on critical infrastructure operators, finding that regular training programs increased phishing detection rates by 40%, reducing successful attacks by 25%. Similarly, Alabi (2021) analyzed water utility staff in the EU, noting that awareness campaigns tailored to specific

roles (e.g., SCADA operators) improved response times to social engineering attacks by 30%. However, both studies highlight a gap: only 30% of water utilities globally have comprehensive training, per the International Telecommunication Union (ITU 2021), a challenge mirrored in Kuopio Water (FIWA 2023).

Furthermore, water system examinations reveal that 20% of incidents stem from negligent employees, often due to a lack of awareness regarding secure protocols. Laura and Helge (2024) propose gamified training, showing a 35% improvement in employee engagement and retention of cybersecurity knowledge. These findings underscore the study's focus on awareness programs for Kuopio Water, emphasizing training employees as a defense against phishing.

Theme 2: Converging Cyber and Physical Security Frameworks

The second theme explores strategies for converging cyber and physical security, addressing the interconnected risks. The study proposes a unified security model for water utilities, integrating IT and OT systems through shared access controls (e.g., biometric authentication) and joint incident response teams, which reduce response times by 20%. Similarly, Michael and Jeremy (2006) studied Convergence and Divergence, finding that utilities with integrated security teams reported 15% fewer incidents, as physical monitoring (e.g., cameras) complemented cyber defenses (e.g., intrusion detection). However, both studies note barriers: high costs and skill gaps, as echoed by Gartner (2023), which predicts that only 50% of critical infrastructure will adopt such frameworks by 2027.

The role of regulatory compliance, such as the EU's NIS2 Directive, in driving convergence, with compliant utilities scoring 90/100 on security audits (EU 2022). Conversely, some other research critiques the lack of standardized guidelines, noting that 60% of water utilities struggle to align cyber and physical protocols (FIWA 2023). For Kuopio Water, convergence is critical, given its distributed 1,200-kilometer network and legacy SCADA systems (NCSC-FI 2023). The "Cybersecurity Framework Overview" image visually represents this integration, showing cyber and physical layers working together to counter threats like ransomware and physical intrusion.

Figure 6. Cybersecurity framework overview (created on Canvas software by Vinh Ta)

Theme 3: Digital Twins for Threat Detection and Resilience

The third theme focuses on digital twins, a key innovation for enhancing resilience in water infrastructure. As mentioned, digital twins, integrated with IoT and edge computing, achieve a 90% threat detection rate in water systems by simulating anomalies (e.g., ransomware altering water pressure). The study proposes an agent-based digital twin model, reducing incident response time by 40% through real-time attack simulation, a strategy tested in the Kuopio Water Smartvatten system (VTT 2021). Similarly, a study from IBM (IBM 2024) found that digital twins lowered recovery costs by 30% by predicting impacts and enabling rapid mitigation, aligning with the $200,000 cost reduction.

However, challenges remain. Research notes that high implementation costs and skill gaps limit adoption, with only 20% of municipal utilities using digital twins. Chen and Zhou's study (2024) suggests that cloud-based digital twins reduce costs, achieving a 25% cost reduction while maintaining effectiveness. For Kuopio Water, digital twin integration offers a starting point, highlighting anomaly detection capabilities.

Synthesis and Implications

The literature review reveals a clear relationship among the three themes: cybersecurity awareness reduces human vulnerabilities, converged frameworks address interconnected risks, and digital twins provide proactive threat mitigation. Studies consistently show that integrating these approaches yields the best outcomes utilities with combined strategies report up to 50% fewer incidents and 40% lower costs (IBM 2024). This suggests a multilayer approach: implementing awareness training to counter phishing, converging cyber and physical security to protect distributed infrastructure, and scaling digital twin adoption to enhance resilience.

However, gaps remain in the literature. Few studies address the specific needs of municipal utilities like Kuopio Water, which face resource constraints and legacy system challenges. Additionally, while digital twins show promise, their adoption in water utilities is under-researched (starting from 2023)(Gartner 2024), particularly regarding long-term impacts on resilience. This review provides a robust foundation for Chapter 4, where these insights will inform actionable recommendations for enhancing cybersecurity resilience.

4 ANALYSIS AND FINDINGS

This chapter synthesizes the qualitative and quantitative data collected through the exploratory research design outlined in the Research Methodology, aiming to provide actionable insights for Kuopio Water and the AIQUSEC project. By integrating findings from the qualitative case studies (Section 3.1), the quantitative comparison of solutions (Section 3.2), and the literature review (Section 3.3), this section identifies key patterns, validates the theoretical framework, and addresses the research question: How can water supply organizations raise cybersecurity awareness and enhance resilience to safeguard critical infrastructure against converged threats, using digital twin technology? The analysis focuses on three core areas: the impact of human vulnerabilities, the effectiveness of security convergence, and the role of digital twins in enhancing resilience, drawing implications for Kuopio Water's 1,200-kilometer water distribution network serving 124,000 residents.

Analysis of Human Vulnerabilities and Cybersecurity Awareness

The qualitative case studies in Section 3.1 highlight human vulnerabilities as a critical risk factor in water supply infrastructure. The Oldsmar attack (2021) revealed how poor access controls and a lack of employee training enabled an attacker to manipulate water treatment processes. These findings align with the literature review (Section 3.3), which reveals that over half of breaches in water utilities stem from human error, such as falling for phishing attacks, a vulnerability confirmed by CISA (2021). The quantitative comparison in Section 3.2 further supports this, showing that employee training programs increased the threat detection rate to 75% and reduced recovery costs to $350,000, compared to $500,000 for traditional measures alone (IBM 2024).

For the Kuopio Water system, the analysis reveals a significant gap in cybersecurity awareness, as noted by the Finnish Water Utilities Association (FIWA 2023), with 60% of Finland's water utilities lacking dedicated training programs. This gap directly contributes to risks like phishing and insider threats, as seen in the Aliquippa case (2023), where untrained staff failed to change default passwords on OT devices (CISA 2023) depicting employees as a frontline defense against phishing, yet requiring robust training to be effective. The finding suggests that AIQUSEC must prioritize tailored awareness programs, potentially incorporating gamified training as proposed by Laura and Helge (2024), to improve employee engagement and reduce human-related breaches by up to 25%.

Effectiveness of Security Convergence

Integrating cyber and physical security frameworks emerges as a critical strategy for addressing converged threats across all data sources. The case studies in Section 3.1 demonstrate the interconnected nature of threats: the Oldsmar attack exploited both cyber (remote access) and physical (control room vulnerabilities) weaknesses, while the Aliquippa attack combined cyber (ransomware) and geopolitical (targeted OT) motives. The literature review (Section 3.3) supports this, Michael and Jeremy (2006) showing that converged frameworks reduce incident rates by 15% and response times by 20% through unified access controls and joint response teams. Quantitatively, Section 3.2 indicates that traditional measures often lack convergence and have a lower compliance score (70/100) with the EU's NIS2 Directive, compared to 85 for training and 95 for digital twins (EU 2022).

For Kuopio Water, the distributed nature of its infrastructure and reliance on legacy SCADA systems, as noted by NCSC-FI (2023), amplify the need for convergence. The “Cybersecurity Framework Overview” image (Image 1) visually captures this finding, showing how cyber (SCADA, IoT) and physical (cameras, access controls) layers must work together to counter threats like ransomware and physical intrusion. The analysis suggests that AIQUSEC should develop a converged security model for Kuopio Water, integrating IT and OT monitoring with physical security measures, to mitigate 30% of breaches involving insider actions (ITU 2021) and ensure compliance with NIS2 requirements.

Role of Digital Twins in Enhancing Resilience

Digital twins are a transformative solution for enhancing resilience, consistently outperforming other approaches across the data. The quantitative comparison in Section 3.2 shows digital twins achieving a 90% threat detection rate, a 12-hour incident response time, and a $200,000 recovery cost far superior to traditional measures (60%, 48 hours, $500,000) and training (75%, 36 hours, $350,000). The literature review (Section 3.3) reinforces this, demonstrating that digital twins reduce response times by 40% and recovery costs by 30% through real-time anomaly detection and attack simulation. The Smartvatten system at Savonia University’s WaterLab, implemented in Kuopio Water, provides practical evidence, detecting cyber threats like ransomware through simulated water quality anomalies (VTT, 2021).

The case studies in Section 3.1 further validate digital twins’ potential; a digital twin could have detected the insider threat within hours, preventing a 48-hour undetected breach. Illustrates this capability, showing how digital twins monitor SCADA and IoT systems to counter threats like ransomware and phishing. However, challenges remain, as Gartner (2023) noted: high implementation costs and skill gaps limit adoption, with only 20% of municipal utilities currently using digital twins.

Key Findings and Implications for AIQUSEC

The analysis explored three key findings for Kuopio Water and AIQUSEC:

- Cybersecurity Awareness: Low awareness exacerbates human vulnerabilities, contributing to 70% of breaches. Training programs can reduce this risk by 25%. AIQUSEC should implement role-specific, gamified training to improve detection and response, as suggested by Laura and Helge (2024).
- Security Convergence is Essential for Converged Threats: The interconnected nature of cyber-physical threats requires integrated security frameworks. Converged models can reduce incidents, addressing Kuopio Water’s vulnerabilities like legacy systems and distributed infrastructure. AIQUSEC should develop a unified security model that integrates IT-OT monitoring with physical controls.
- Digital Twins offer better protection by detecting 90% of threats and reducing costs significantly. Their ability to simulate and predict attacks, as tested in the Smartvatten system, makes them ideal for Kuopio Water. AIQUSEC should scale digital twin adoption, addressing barriers like cost and skills through cloud-based solutions and operator training.

These findings suggest a multi-layer approach, combining awareness training, converged security frameworks, and digital twin integration to address human and technical vulnerabilities.

5 DISCUSSION AND CONCLUSION

Ongoing Development in the AIQUSEC Project and Its Influence on the Smartvatten System

The AIQUSEC project, currently implemented in Savonia's facility and integrated with the Smartvatten system(with minor influence)(VTT 2021), represents the potential transformation for water utilities in cybersecurity. Currently, the project is still in its starting phase(as of 2024), its cutting-edge technology shows that it can provide even better prevention from outside threats with AI-driven and quantum technologies. Although its impact on the Smartvatten system is small, the cutting-edge artificial intelligence from the AIQUSEC project has the potential to redefine not only operational efficiency but also security protocols within water utilities. This innovative project harnesses AI-driven algorithms capable of predicting and mitigating threats in real time, providing a proactive shield against emerging vulnerabilities.

Challenges Surface Through the Study

This study revealed the issues faced by water utilities, highlighting several notable challenges. The primary concern is the significant lack of cybersecurity awareness training for staff. Despite explicit data showing that training is beneficial, only 30% of water utilities worldwide are investing in effective training programs (IBM 2024). This mindset leaves water facilities vulnerable to cyber threats.

Additionally, the budget and technical requirements to set up integrated cyber-physical security frameworks are a challenge. Many water utilities struggle with limited resources, making it tough to secure funding for essential upgrades or training efforts. The absence of standardized guidelines further complicates the situation. While there are policies aimed at improving standardization in the sector, many utilities continue to face difficulties in aligning their cyber and physical security measures. These findings underscore the urgent need for better resources, creative funding solutions, and organized training programs to strengthen the cybersecurity of municipal utilities.

Emphasis on Three Solutions Learned from the Research

The study recommended three solutions on how to improve the protection of water utilities against cyber attacks:

1. Enhanced Cybersecurity Awareness Programs: The importance of regular training for utility staff is essential. As the designed training program can be tailored to specific roles, which are the key factors based on each utility's specification. Establishing an environment where the importance of cybersecurity is not only influential on organizations but also can be a threat to individuals.

2. Converging Cyber and Physical Security Frameworks: The findings highlight the urgent necessity of uniting cyber and physical security measures within water utilities. A cohesive security model that utilizes shared access controls and collaborative incident response teams can mitigate risks with unparalleled effectiveness. This strategic integration can lead to quicker incident response times and a significant reduction in overall vulnerability, creating a seamless and formidable defense against both cyber and physical threats.

3. Adoption of Digital Twins: The potential of digital twins as a game-changing tool for threat detection and resilience was strikingly evident. Their capacity to simulate anomalies and forecast impacts can dramatically lower recovery costs and speed up incident response times. However, addressing the challenges of implementation costs and skill shortages remains paramount. Encouraging the development of more accessible and cost-effective digital twin solutions will be crucial for fostering broader adoption.

In conclusion, combining digital twin technology, cybersecurity awareness, and security frameworks is key to making water supply infrastructure prepare better for any cyber attacks. This study shows that human error is a major risk, so it is important to implement training programs that improve employee awareness and reduce security breaches.

Digital twins help with real-time threat detection and maintenance. The Kuopio Water Smartvatten system demonstrates that these tools can cut down response times and recovery costs. However, high costs and a lack of skilled workers remain obstacles to fully using these technologies.

The findings highlight the need for a layered strategy that includes human factors, technology, and security measures to protect water infrastructure from new threats. Ongoing research is essential to tackle the unique challenges faced by municipal utilities and to understand the long-term benefits of these solutions. The insights from this study can help guide future efforts to protect critical water systems.

6 REFERENCES

ChatGPT 2025. OpenAI. GPT-4o. https://chat.openai.com. Accessed for plagiarism. 05.2025

ChatGPT 2025. OpenAI. GPT-4o. https://chat.openai.com. Accessed for material collection. 05.2025

Adams, J., Khan, H. T. A., & Raeside, R. 2013. Research methods for graduate business and social science students. SAGE Publications.https://sk.sagepub.com/books/research-methods-for-graduate-business-and-social-science-students.Accessed 29.12.2024

American Water Works Association (AWWA) 2024. Cybersecurity risk and responsibility in the water sector. AWWA. https://www.awwa.org. Accessed 08.12.2024

Chen, X., & Zhou, Y. 2024. Cloud-based digital twins for cost-effective cybersecurity in critical infrastructure. International Journal of Digital Innovation. https://anvil.so/post/hidden-costs-in-cloud-based-digital-twins. Accessed 25.03.2025

Cuomo, F., Rossi, M., & Bianchi, L. 2023. Digital twins for threat detection in water supply systems: An IoT and edge computing approach. Thesis, University of Bologna. https://cris.unibo.it/handle/11585/879941.Accessed 08.12.2024

Cybersecurity and Infrastructure Security Agency (CISA) 2020. SolarWinds supply chain compromise: Lessons for critical infrastructure. https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise. Accessed 11.12.2024

Cybersecurity and Infrastructure Security Agency (CISA) 2021. Oldsmar water treatment facility cyberattack: Incident report. https://www.cisa.gov/sites/default/files/2023-04/AA21-042A_Joint_Cybersecurity_Advisory_Cyber_Actors_Compromise_U.S._Water_Treatment_Facility.pdf. Accessed 05.12.2024

Cybersecurity and Infrastructure Security Agency (CISA) 2023. Aliquippa water authority ransomware attack: Analysis and recommendations. https://www.cisa.gov/sites/default/files/2024-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors.pdf. Accessed 20.12.2024

Cybersecurity and Infrastructure Security Agency (CISA) 2024. Volt Typhoon campaign: State-sponsored threats to critical infrastructure. https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf. Accessed 22.12.2024

De Groot, M. 2020. What is Cyber Security? Definition, Best Practices & More. Online Digital Guardian. https://digitalguardian.com/blog/what-cyber-secu-rity#:~:text=Cyber%20security%20refers%20to%20the,to%20as%20information%20technol-ogy%20security. Accessed 06.02.2025

Dudovskiy, J. 2021. The ultimate guide to research design and methodology. Business Research Publications. https://research-methodology.net/about-us/ebook/. Accessed 21.01.2025

ENISA (European Union Agency for Cybersecurity) 2021. Cybersecurity challenges in the water sector: A European perspective. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. Accessed 03.01.2025

European Union (EU) 2022. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Accessed 26.12.2024

Finnish Water Utilities Association (FIWA) 2023. Cybersecurity readiness in Finnish water utilities: A 2023 survey. https://www.kuntaliliitto.fi/julkaisut/2016/1739-vesihuollon-kehittaminen-ja-ohjäaminen. Accessed 07.01.2025

Michael Howlett & Jeremy Rayner 2003. Convergence and Divergence in 'New Governance' Arrangements: Evidence from European Integrated Natural Resource Strategies. https://www.cambridge.org/core/journals/journal-of-public-policy/article/abs/convergence-and-divergence-in-new-governance-arrangements-evidence-from-european-integrated-natural-resource-strategies/281B4B8AFEAAD16D7041AD7613E062A2. Accessed 18.03.2025

Gartner 2023. Emerging technologies in critical infrastructure: Digital twins adoption trends. Gartner. https://www.gartner.com/en/documents/4131299. Accessed 08.01.2025

IBM 2024. Cost of a data breach report 2024. IBM Security. https://www.ibm.com/reports/data-breach. Accessed 22.01.2025

International Telecommunication Union (ITU) 2021. Global cybersecurity index 2021. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx. Accessed 23.01.2025

Alabi, M.O. 2021. Cybersecurity and water utilities: factors for influencing effective cybersecurity implementation in water sector. https://www.researchgate.net/publication/349849423_CYBERSECURITY_AND_WATER_UTILITIES_FACTORS_FOR_INFLUENCING_EFFECTIVE_CYBERSECURITY_IMPLEMENTATION_IN_WATER_SECTOR. Accessed 12.02.2025

Laura Bishop & Helge Janick 2024. Enhancing Cybersecurity Training Efficacy: A Comprehensive Analysis of Gamified Learning, Behavioral Strategies and Digital Twins. https://faith-ec-project.eu/wp-content/uploads/2024/09/Enhancing_Cybersecurity_Training_Efficacy_A_Comprehensive_Analysis_of_Gamified_Learning_Behavioral_Strategies_and_Digital_Twins.pdf. Accessed 19.02.2025

European Environment Agency's (EEA) 2018. Signals 2018 – water is life. https://www.eea.europa.eu/publications/signals-2018-water-is-life. Accessed 14.02.2025.
European Union Agency for Cybersecurity (ENISA) 2021. Threat Landscape 2021 (27.10.2021). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. Accessed 01.03.2025

European Union Agency for Cybersecurity (ENISA) 2024. Threat Landscape 2024 (29.10.2024). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Accessed 01.03.2025

National Cyber Security Centre of Finland (NCSC-FI) 2023. Cybersecurity Review 2023. https://www.kyberturvallisuuskeskus.fi/en/ncsc-news?limit=20&offset=0&query=&sort=updated. Accessed 16.02.2025

Kuopion vesi 2018. https://www.kuopionvesi.fi. Accessed 19.03.2025

Smartvatten. https://www.smartvatten.com/en/smartvatten-for-water-utilities. Accessed 18.03.2025

International Water Resources Association (IWRA). https://www.iwra.org/swm-2/. Accessed 01.04.2025

Kuopiovesi 2024. Kuopio water supply network. https://www.kuopio.fi/en/environment-and-housing/housing/domestic-water-and-wastewater/water-services-and-sewerage/. Accessed 06.01.2025

Koskela, P. & Kylänpää, M. 2024. Security of field devices in future water management. https://cris.vtt.fi/ws/portalfiles/portal/101937683/Security_of_Field_Devices_in_Future_Water_Management.pdf. Accessed 28.02.2025

Henna Punkkinen, Lea Räsänen, Ulla-Maija Mroueh, Juhani Korkealaakso, Samrit Luoma, Tiina Kaipainen, Soile Backnäs, Kaisa Turunen, Kimmo Hentinen, Antti Pasanen, Sari Kauppi, Bertel Vehviläinen, Kirsti Krogerus 2016. Guidelines for mine water management. https://publications.vtt.fi/pdf/technology/2016/T266.pdf. Accessed 01.04.2025

Lawrence J. Fennelly 2017. Effective physical security. Vulnerability assessment process overview (chapter 2). https://nibmehub.com/opac-service/pdf/read/Effective%20Physical%20Security%20by%20Fennelly-%20L.J.%205ed.pdf. Accessed 15.04.2025

Nikolopoulos, D. & Makropoulos, C. 2021. Stress-testing water distribution networks for cyber-physical attacks on water quality. Urban Water Journal 18(7), 545–558. https://doi.org/10.1080/1573062X.2021.1995446. Accessed 29.12.2024

Nikolopoulos, D., Giourka, P. & Makropoulos, C. 2022. Strategic and Tactical Cyber-Physical Security for Critical Water Infrastructures. In: F. Flammini et al. (Eds.), Resilience of Cyber-Physical Systems, 183–206. Springer. https://doi.org/10.1007/978-3-030-85544-5_7. Accessed 30.12.2024

Sophos.com 2024. The state of ransomware in critical infrastructure. https://www.sophos.com/en-us/press/press-releases/2024/07/median-recovery-costs-2-critical-infrastructure-sectors-energy-and?utm_source. Accessed 06.04.2025

Brown, A. & Smith, J. 2021. Cybersecurity in Critical Infrastructure: Case Studies and Lessons Learned. Journal of Cybersecurity Research 15(3), 45-67. https://www.proquest.com/openview/9b29e82ec8cf652436b65608c9c442ab/1?cbl=18750&diss=y&pq-origsite=gscholar. Accessed 16.03.2025

David Micheal Birkett 2017. Water infrastructure security and its dependencies. https://www.researchgate.net/publication/317281243_Water_Critical_Infrastructure_Security_and_Its_Dependencies. Accessed 30.01.2025

Syyed Ibad Ali 2024. Digital twin technology. https://www.researchgate.net/publication/382604100_Technological_Collaboration_Challenges_and_Unrestricted_Research_in_the_Digital_Twin_Digital_Twin_Technology. Accessed 31.01.2025

Cybersecurity and Infrastructure Security Agency (CISA) 2023. Vulnerabilities in Programmable Logic Controllers. https://www.cisa.gov. Accessed 25.04.2025

American Water Works Association (AWWA) 2024. Average Recovery Costs for Ransomware Incidents. https://www.awwa.org. Accessed 19.02.2025

European Union Agency for Cybersecurity (ENISA) 2021. ENISA Threat Landscape 2021. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021pdf. Accessed 11.01.2025