TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Isaac Osang Ewa 184630IASM

ENABLING TRUSTED CYBER-PHYSICAL SYSTEMS ARCHITECTURES WITH BLOCKCHAIN TECHNOLOGY IN WATER-SUPPLY SYSTEMS

Master's thesis

Supervisor: Alexander Norta
PhD
Co-Supervisor Chibuzor Udokwu
MSc

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Isaac Osang Ewa 184630IASM

BLOCKCHAIN-TEHNOLOOGIAEGA TURVALISTE KÜÜMIS-FÜÜSIKALISTE SÜSTEEMIDE ARHITEKTUURIDE LUBAMINE VEDEVARUSTUSSÜSTEEMIDES

magistritöö

Juhendaja: Alexander Norta

PhD

Kaasjuhendaja Chibuzor Udokwu MSc

MSc

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Isaac Osang Ewa

05.08.2020

Abstract

Water is important to human life, therefore it important that is available whenever and wherever it is people need it as safe and clean. The water sectors across the globe have been leveraging on the pervasiveness of cyber-physical systems (CPS) which has also attracted cyberattacks to the water systems. The water sector is critical infrastructure, it ought to be well protected against malicious cyber activities.

Water CPS is a growing paradigm, but very limited studies have been conducted in terms of carrying out a source-to-consumer risk analysis for the water-supply systems CPS architecture, and even less have been done in securing these infrastructures with blockchain technology.

This thesis proposes to carry out an end-to-end (source-to-consumer) security threat analysis of the cyber-physical systems architecture of the water-supply system and implementing blockchain technology in the security treatment process.

The approach to solving this problem is in three steps by applying a risk management framework for the analysis. The first step is to identify the CPS assets that are involved in the communication network. Secondly, determine the risks by analyzing the threats and threat agents. Then finally apply security requirements and security controls using blockchain technology to mitigate the risk.

The last part of this thesis presents the proposed models for the blockchain security controls and an evaluation of the results.

This thesis is written in English and is 103 pages long, including 7 chapters, 15 figures, and 23 tables.

Annotatsioon

[Thesis title in Estonian]

Vesi on inimese elus oluline, seetõttu on oluline, et see oleks kättesaadav igal pool ja igal pool, kus inimesed seda vajavad. Kogu maailma veesektorid on võimendanud küberfüüsikaliste süsteemide ulatuslikkust, mis on veesüsteemidele meelitanud ka küberrünnakuid. Veesektor on elutähtis infrastruktuur, see peaks olema hästi kaitstud pahatahtliku kübertegevuse eest.

vee küberfüüsikalised süsteemid on kasvav paradigma, kuid veevarustussüsteemide CPS-i arhitektuuri jaoks tarbijale allikatest lähtuva riskianalüüsi osas on tehtud väga vähe uuringuid ja veelgi vähem on tehtud nende infrastruktuuride turvamisel blockchain tehnoloogia.

See lõputöö teeb ettepaneku viia läbi veevarustussüsteemi küberfüüsikaliste süsteemide arhitektuuri otsest (lähteallikast tarbijani) turvaohu analüüs ja rakendada blockchain tehnoloogia turbeprotsessis.

Selle probleemi lahendamiseks kasutatakse kolme sammu, rakendades analüüsis riskijuhtimise raamistikku. Esimene samm on tuvastada CPS-i varad, mis on sidevõrgus kaasatud. Teiseks määrake riskid, analüüsides ohte ja ohuagente. Seejärel rakendage riski maandamiseks lõpuks turvanõudeid ja turvakontrolli, kasutades blockchain-tehnoloogiat.

Lõputöö viimases osas on esitatud pakutud ahela turvakontrolli mudelid ja hinnang tulemustele.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 103 leheküljel, 7 peatükki, 15 joonist, 23 tabelit.

List of abbreviations and terms

CPS	Cyber-physical Systems
CI	Critical infrastructure
WSS	Water-supply system
SCADA	Supervisory Control and Data Acquisition
ICS	Intelligent Control System
WSN	Wireless Sensor Network
ISR	Information Science research
PLC	Programmable Logic controller
IoT	Internet of things
PKI	Public Key infrastructure
PoW	Proof-of-Work
IS	Information Security
ISSRM	The Information System Security Risk Management
ISO	International Standard Organization
PBFT	Practical Byzantine Fault Tolerance
BPMN	Business Process Model and Notation
DSR	Design-science Research

Table of contents

List of figures

List of tables

1. Introduction

Water is essential to life; therefore, critical infrastructures in water-supply systems must be well secured. Water systems infrastructures are being faced with an increasing number of attacks against the system being reported globally. The water sector has endured several forms of attacks, ranging from interfering with Industrial control systems, ransomware, manipulation of valves and flow operations, treatment chemicals tampering, and several others. In recent years, there have been reports of cyber-attacks on water facility some of which have been investigated by reputable institutions and government agencies [1]. Recently, in May 2020, there was a report of an attempted cyberattack on Israel's water supply aimed at disrupting the industrial computers that support the country's water facilities.[1]

Today, the water sectors in many countries are applying Cyber-physical systems (CPS) in urban water distribution critical infrastructures (CI). Cyber-physical systems are networked systems with a tight combination of physical and cyber objects. The emergence of CPS in water supply management and control allows for persistent monitoring of vulnerable areas, immediate reporting of abnormal operating conditions, and the drastic reduction of regular patrol and visiting of sites for inspection. Despite its impressive advantages, the CPS components have become the entry points for hackers and other malicious activities. The impact of a successful attack in critical water facilities could have major social and financial consequences, so the protection of this is important and should not be ignored.

To ensure secure and trusted interactions between CPS entities, blockchain technology has been adopted in CPS architectures in recent years. Blockchain has an inherent ability

[1] Link to attempted cyberattack on Israeli water system https://www.cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna/, Accessed 27/07/2020

to provide new foundations for distributed systems by establishing trust efficiently enabling trusted interactions among nodes. Blockchain is a secure digital ledger of transactions that can be made to record transactions not only in the financial world but also in other sectors where the need to maintain historical activities is important [2]. Some of the features of blockchain are: it is decentralized, no single regulating authority, it is immutable and auditable [3], making data entered to be verifiable. There are two types of blockchain and this categorization is based on how nodes are added to the blockchain. The two types are permissioned and permissionless. The exponential growth of blockchain technology has caused it to spread into various fields and application and it has supported several applications [4].

This thesis seeks to analyze the threats and vulnerabilities of the CPS entities in the water supply sector and propose blockchain technology as a preferred measure of protection against cyberattacks and malicious activities in the water supply sector.

1.1 Existing Body of Knowledge

The following sections provide an overview of the existing body of knowledge and the stat-of-the-art in the water supply security systems. Section 1.1.1 defines water-supply systems and introduces the recent advancements in the water sector. Section 1.1.2 Introduces the various cyberattack incidents in the water-supply system. Section 1.1.3 describes the role of Cyber-physical systems in Water-supply systems. The final section 1.1.5 Describes the adoption of blockchain in CPS technology in several domains.

1.1.1. Water-supply system

Water-supply systems (WSS) are systems whose edges and nodes include, pressure pipes, junction pipes, water sources, and end-users. With the sole aim to provide portable water to end-users enough pressure level [5]. Water-supply systems include several sub-systems that combine sequentially to ensure clean and safe water is made available for the end-users or consumers. This makes WSS a system-of-systems. The sub-systems include water sourcing, water treatment, and water distribution. Series of activities are carried out by experts of different disciplines ensuring continuous availability and flow of water for the end-users.

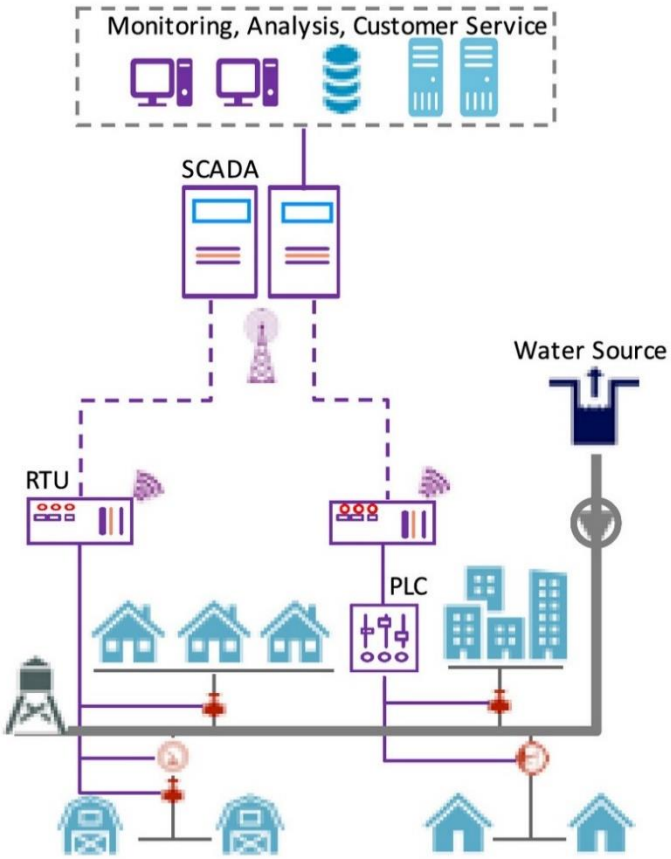

Figure 1:Typical architecture of a water-supply system (Source [6])

A typical water-supply system includes a treatment plant where the water collected from the various water sources are treated and purified for consumption or industrial purpose. Water sources these days are classified into groundwater, surface water, rainwater, and sometimes sewage. Due to the scope of this thesis, these sources will not be explored. The sourced water is then subjected to purification at the water treatment plant. The various equipment at the treatment plant as well as the distribution network is connected to a Supervisory Control and Data Acquisition (SCADA) systems that are used for the monitoring and control of WSS as shown in Figure 1, through Programmable Logic controllers (PLCs) and Real-time Units(RTUs). The communication mode between the RTUs and PLCs to the central control and monitoring unit could be via the Internet, wireless networks, wired networks, and telephone network.

Purified water is transported to the end-user through a network of pressure pipes, pumps, reservoirs controlled, and monitored to deliver water at the designated destination with

sufficient pressure, healthy for consumption, and safe to the network. The distribution networks are equipped with sensors and actuators in real-time communication with the control and monitoring center.

1.1.2. Incidents in Water Sectors

In recent times, there have reports of cyberattacks and attempted attacks on water infrastructures. The water sector has been classified among the most targeted critical sector in the United States [7]. Attacks on Industrial control systems have high implications, some of which can long-lasting impacts on the health and social life of a country. In this section, we shall be highlighting some cyberattacks on water infrastructures within the last decade captured in the peer-reviewed article by Hassanzadeh et al published in 2020 [1].

Table 1: List of recent cyber-attacks in the water sector

S/N	Facility	Year of occurrence	Incident description	Impact on Infrastructure
1	Key Largo Wastewater Treatment District, US	2012	Former senior employee illegally accessing computer and downloading emails and personal documents	No consequence
2	Bowman Avenue Dam, US	2013	hackers obtained unauthorized remote access to the SCADA system	$30,000 remediation cost but no critical consequence on infrastructure.
3	Five Water Utilities, across three US states	2014	A sacked employee of the company that manufactures smart meters illegally accessed a protected computer, changed passwords,	inaccurate water bills and the deactivation of the tower gateway base stations (TGBs)

			modifying radio frequency and overwriting computer scripts	
4.	Kemuri Water Company (Pseudonym), US	2016	The exploitation of the internet-facing payment application server and manipulation of utility valves and flow control application	exfiltration of 2.5 million unique records and manipulation of chemicals and flow rates
5	Regional Water Supplier, UK	2017	Changing of clients' details online including their bank account details by hacker resulting in refunds meant for customers being diverted to hacker's account in collaboration with an insider employee	A total of £500,000 was diverted and never recovered.
6	European Water Utility.	2018	Strange IP address discovered to be using facility infrastructure for crypto mining, with 40% of operations relating to mining operations.	Resulted in a 60% surge in overall bandwidth consumption.

7	Onslow Water and Sewer Authority, US	2018	Cybercriminals inflicted ransomware viruses on the facility IT system by locking out employees and encrypting databases and other files. With cybercriminals demanding payment to decrypt files.	Loss of entire IT facility to criminals.
8	Fort Collins Loveland Water District, US	2019	Hackers inflicted ransomware on facility causing employees not to access critical files	District declined to pay the ransom

Attacks on ICS in water-supply systems can be very significant, although its significance depends largely on the type of the attack and the location attacked. This is, therefore, pointing to the need for the research and design of secure architectures that are more resilient to cyber-attacks. [8]

Some of the popular attacks against water supply include [9]: (1) Attacking the Physical layers – involves the compromising of sensors and actuators. (2) Attacking the Datalink layers – involves attacks on the links between devices. (3) SCADA layer – directs attacks on the entire SCADA system

1.1.3. CPS Architecture in Water-supply systems

Cyber-physical systems (CPS) is a pervasive concept in the field of embedded systems and the Internet-of-things (IoT). It involves physical entities with computational capacity and communication core. The interconnection between the physical and the cyber network is the key factor in a CPS architecture. It is a system where the physical system is extended with cyber components, where the capabilities of each component are dependent on the other. In other words, CPS can be generally described as “physical and engineered systems whose operations are monitored, controlled, coordinated, and integrated by a computing and communicating core” [10].

CPSs are replacing existing infrastructures in various domains due to their improved performance as a result of advanced design and high level of abstraction. CPSs has several advantages: they offer superior service and safe, individual entities can work together forming complex systems with new features [9]

The major purpose of cyber-physical systems in the water supply is to monitor and control physical processes within the system in a very efficient manner.

1.1.4. Blockchain-Enabled CPS

Blockchain was originally utilized specifically for the protection of financial transactions, but its benefits were later realized by other applications and domains of CPS mentioned in section 1.1.3 as it became obvious that the efficiency of these systems can be enhanced by adopting blockchain. [2]. Currently, researchers and scientists are still looking for more applications where blockchain technology can still be applied.

Blockchain provides a powerful and efficient technique for the data generated by the physical resources in a distributed network to interact in a trusted or even trust-less and verifiable way. The survey of blockchain-enabled cyber-physical systems, Rathore et al researched some emerging blockchain-enabled CPS as follows [2]

- Implantable devices: for patient monitoring and immutable information collection for medical intelligence

- Industrial control system: maintaining historical records of usage and performance, enhancing the secure connection between components and control.

- Transportation: blockchain in transportation systems and autonomous vehicles are used to set up verified, trusted, and independent smart transport systems.

- Smart grid systems: blockchain is used for preserving privacy, providing energy consumption pattern for users, enhancing fairness in electricity distribution, and enabling peers to negotiate energy prices anonymously and transact securely.

The CPS architectural paradigm is providing numerous advantages to the economy and the society, and when coupled with the robust features of blockchain technology as a security-service makes it all together reliable, secured, and trustworthy. Despite the

multiple benefits of adopting blockchain in CPS, there are yet many challenges, such as scalability, latency, throughput, complex consensus algorithms, heterogeneity, storage, and so on.

1.4. Gap Detection and Contribution

Despite the recent advancement in technologies to secure the water-supply system with traditional SCADA technology and even with the emergence of distributed CPS implementation on water-supply networks, there are still several growing reports of cyber-attacks on critical water infrastructures. This, therefore, calls for a more secure system that can provide end-to-end protection for the system in a verifiable, trusted, and secured manner, where each node(CPS device) independently stores its data and at the same time shares the similar data with the entire network. Secondly, with the traditional SCADA industrial control system, an attack on each component could lead possible lead to the collapse of the entire system especially if the malicious entry point is at the control center.

With blockchain technology, members of the network are independent, and information appended into the blockchain are immutable and are verified through consensus by all members of the network, an attack a malicious or authorized entry from a member will not be verified and may not affect the data on other nodes.

This thesis focuses on analyzing threats to the CPS infrastructures of the water-supply systems. This thesis aims to apply a security framework for analyzing and managing the risks generated in the interactions of CPS devices using the water supply sector as a case study. This work seeks to propose blockchain technology as a superior trusted and secured solution for CPS in the water service sector by proposing models for blockchain-based security control in the water-supply system network and evaluating its performance thereof.

1.5. Research Methodology

In information system research (ISR) discipline, there are two paradigms: behavioral science and design science. The behavioral science on one hand seeks to develop and verify theories that explain or predict human or organizational behavior, while design science on the other seeks to extend the boundaries of human and organizational

capabilities by creating new and innovative artifacts [11]. The research methodology applied in this thesis is Design Science Research (DSR). The research scope of this thesis is to develop a solution that enables trusted CPS architectures with blockchain that cut across the data layers and the node interaction layers, hence the object of the study is an artifact in context, and two main efforts are designing and investigating this artifact in context.

1.1.5. Design Science Research Methodology

Design science is fundamentally a problem-solving paradigm, it creates and evaluates IT artifacts intended to solve identified organizational problem [11]. Such artifacts according to Denning [12] and Tsichritzi [13] represent ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and use of information systems can be effectively and efficiently accomplished. Figure 1 shows the conceptual framework which according to *Hevner et al* [11] it is used for understanding, executing, and evaluating information system research combining behavioral science and design science.

Based on this thesis, the design science framework instantiation is described in Figure 2. The left column represents the environment, which is the problem space where the artifact is needed. The environment consists of people, organizations, business processes, and strategies. On the right column is the knowledge base, which imparts the basic resources in terms of information and methodologies applied in the artifact. The created artifact eventually becomes applicable to the environment to meet its need and make useful additions to the knowledge base.

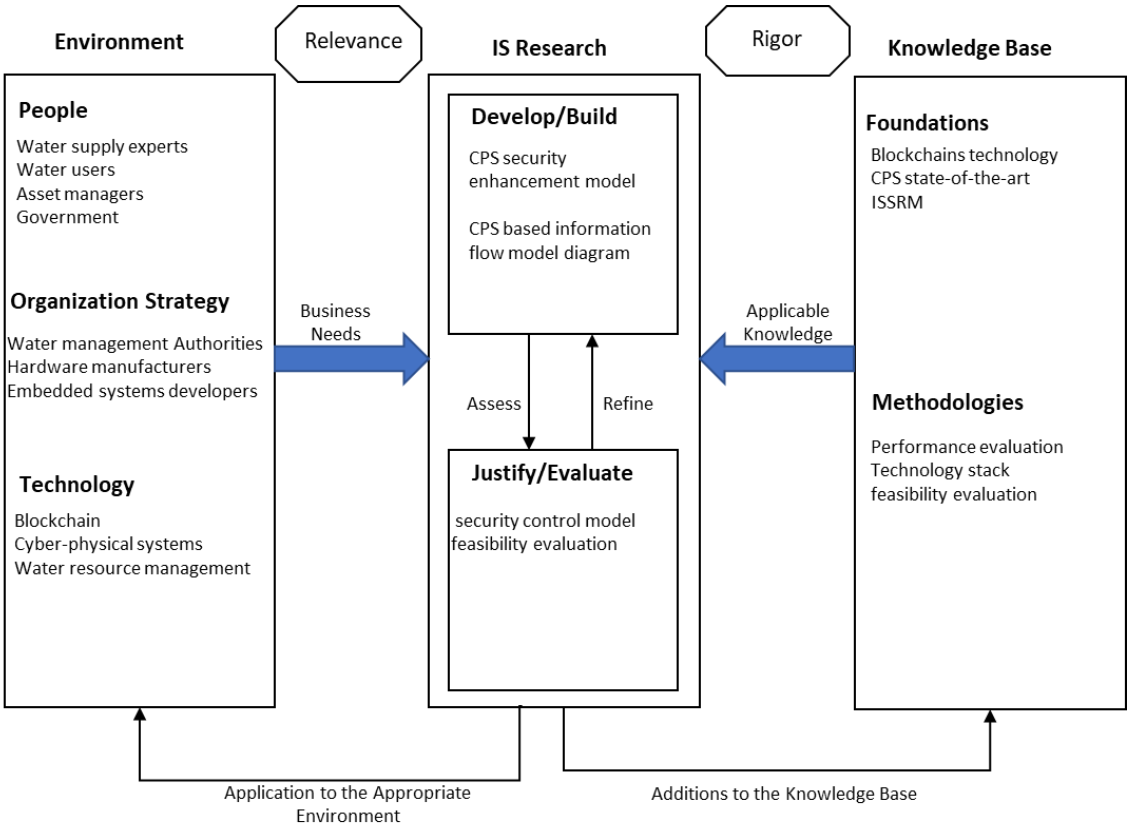

Figure 2: Information systems research framework (Source: [14])

Hevner et al.[14], also introduced introduce seven principal Design Science Research (DSR) guidelines (Table 1) that are adhered to in this thesis. The following sections discuss the application of guidelines as it applies to this thesis and within the context of design science research.

Table 2: Design-Science Research Guidelines (Source [11])

Guideline	**Description**
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.

Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contribution	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Design as an Artifact

The artifact of this thesis is aimed at bridging the gap in Section 1.2 is a security framework for the water-supply system using blockchain technology. Answers to the research questions are applied in developing security controls and requirement models for trusted CPS interactions in the water supply sector.

Problem Relevance

The current CPS based architectures in water supply networks still possess subtle vulnerable points that can penetrable by hackers. The aim of this research is work is to use risk-oriented patterns on CPS based water-supply system flow process to develop new security requirements for CPS

Design Evaluation

Table 2 presents the design science research evaluation methods. Evaluation methods must demonstrate the utility, quality, and efficiency of design artifacts rigorously [15]. Experimental evaluation is used in this thesis: Controlled experiments and simulation are used to present the artifact for this thesis.

Table 3: Design Science Evaluation Methods (Source: [11])

Evaluation Method	**Method Description**
Observational	Case Study: Study artifacts in-depth in the business environment
	Field Study: Monitor use of artifact in multiple projects
Analytical	Static Analysis: Examine the structure of artifact for static qualities (e.g., complexity)
	Architecture Analysis: Study t of artifact into IS architecture
	Optimization: Demonstrate inherent properties of the artifact or provide optimality bounds on the artifact
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
Experimental	Controlled Experiment: Study artifact in a controlled environment for qualities (e.g., usability)
	Simulation: Execute artifact with artificial data
Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects

	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility
	Scenarios: Construct detailed scenarios around the artifact

Research Contributions

This thesis enhances the security of CPS networks in water-supply systems by implementing blockchain technology on the infrastructure and applying domain model for infrastructural risk management in analyzing security threats in the water-supply system.

Design as a Rigor

In design-science research, rigor is gotten from using knowledge base effectively, as in theoretical backgrounds and research methodologies, such that it is used in the right manner to justify a theory or evaluate the artifact [11]. In this thesis, to identify the various asset in the system, intense data analysis will be done to determine the assets that are affected in information exchange. Secondly, different security patterns will be used to establish a trusted CPS architecture.

Design as a search

Design-science uses an iterative process to determine the best solution and, does so by breaking down complex problems into smaller ones. The main goal of this thesis is to propose blockchain as a more secured and trusted architecture for CPS components in the water supply sector. This goal is decomposed into three smaller problems: identification of CPS assets in the system, Risk analysis of existing systems, and application of security controls and risk evaluation.

Communication of research*:*

This thesis has been written as a pre-requisite requirement for the award of a master's degree in computer and systems engineering. The analysis made in the thesis will be made available for all interested audiences both technical and non-technical including business analyst, water resource experts, cybersecurity consultants, etc. and in the university portal for academic purposes

1.6. Research Questions

The main research question for this thesis is as follows:

How to enhance trusted communication among CPS entities in water-supply system architecture

To answer the main question, it is further divided into the following hierarchy of sub-questions:

- **RQ-1: How to identify relevant information exchanges between CPS nodes in WSS?**
    - What are the relevant entities involved in data transmission and communication?
    - What information is exchanged?
- **RQ-2: How to identify the security threats that exist in information exchange?**
    - What are the threat agents?
    - What are the vulnerabilities within the system?
    - What are the risk impacts?
- **RQ-3 How to use blockchain technology to mitigate the trust issues that affect the CPS infrastructure?**
    - What are the blockchain qualities that enable security?

- What are the security requirements in the water-supply system CPS architecture?

- What are the blockchain security controls that implement the security requirements?

RQ-1 Helps to identify the important resources as well as the shared data among communicating devices within the system. The identification of the interacting CPS devices one can understand the nature of the information exchanged between the decentralized devices.

RQ-2 with its sub-questions, we shall be able to diagnose the weaknesses and the risk factors within the system. It also exposes the vulnerabilities for attacks within the system and the possible impacts.

RQ-3 the requirements for establishing a trusted infrastructure in CPS to mitigate the security challenges are explored. To mitigate risks, security patterns are to be investigated which introduces security requirements for future data [16].

1.7. Thesis Structure

The rest of the thesis is structured in the following way: In Chapter 2, a running case is set by providing the need for trusted and secured CPS in the water-supply system, describing a typical water-supply system and its sub-systems, blockchain as a technology of trust and discussing the several risk management techniques. In Chapter 3, the Identification of Assets in the water-supply system network resulting in an understanding of the information exchanged within the system. The Risk analysis of the assets in the water-supply System is conducted in Chapter 4. The use of blockchain-based security control for implementing security requirements on assets performed in Chapter 5. In Chapter 6 the development of models for blockchain-based security control in water infrastructure CPS, evaluation of the proposed models with expert reviews. And finally, a summary of the thesis, by answering the research questions, limitations, and future work is determined in Chapter 7

2. Presuppositions

This chapter introduces the main objectives of this thesis by explaining the concepts that are used and improved upon in this thesis. Section 2.1 provides the running case for the thesis with an argument for the need for this thesis. Section 2.2 introduces the background concepts and technologies explored in the development of the artifact. The following Section 2.3 provides information about the risk and threat assessment methods, this concept is beneficial for the justification to adopt blockchain on the water supply infrastructures for improved security and reliability.

2.1. Running Case

Water is important to life; it is, therefore, expedient for governments and water supply companies across the globe to ensure it is clean for consumption and available in sufficient quantity whenever and wherever it is needed. As a result of increasing population, climate change, and changes in people's lifestyles, it is expected that shortly, water demand is expected to rise [17]. In recent times, the incorporation of technology is the water industry has been increasingly developing. The use of smart devices such as sensors, actuators, and water meters is spreading fast also. Due to the pervasiveness of wireless sensor networks, technology experts are improving the traditional SCADA water-supply system by incorporating the potentials of cyber-physical systems. SCADA for water supply has its drawbacks such as flexibility, real-time constraints, issues with managing large amounts of data, and it is relatively not safe and secure.

A paradigm of CPS, that combines computing, communication and storage abilities with monitoring and control of physical entities and can do so in a dependable, secured, efficient way and in real-time could be an appropriate perspective for the new SCADA water-supply system [9]. Although CPS has improved the overall capabilities of the modern-day SCADA water-supply system, studies have revealed its vulnerabilities to cyberattacks. There have been several reports of water infrastructures being attacked by malicious hackers such as the examples highlighted in Section 1.1.2.

This thesis, therefore, seeks to identify vulnerabilities of the systems and proposes a blockchain-based approach to ensure a trusted and secure CPS architecture for the water-supply system. In this work, we shall explore the entire water supply communication

infrastructure, carry out a risk assessment, and development of blockchain-based security control models that establishes superior security for water CPS.

2.2. Background

This section provides background information that is related to the running case in terms of the sector of interest- the water-supply system in Section 2.2.1 and a base knowledge that describes water cyber-physical systems in Section 2.2.2. There is also a background knowledge regarding blockchain technology in Section 2.2.3. Then a presentation of threat assessment methods as threat assessment methods, this knowledge background is important in the later parts of the thesis for assessing the threats to the water-supply system.

2.2.1. Water-supply systems

The water-supply system refers to the system that collects, transmits, treats, stores, and distributes water for the source points to the consumers for domestic, industrial, agricultural, or public use. The water-supply system. The water-supply system contains infrastructures that collect, treat, store, and distribute water between water sources and the end-user. With the increase in the world population and the development of urban cities, the distance between the water sources and consumers has increased. World water consumption has increased by a multiple of four in the past 5 decades and it is expected to continue to increase [18]. The purpose of the water-supply system is incomplete until portable water gets to the consumer in sufficient quantity and at the right pressure.

A basic water-supply system involves a series of activities or subsystems, they are Water Collection, Water treatment, water distribution/supply, and consumer [19]. In some cases, wastewater treatment is included.

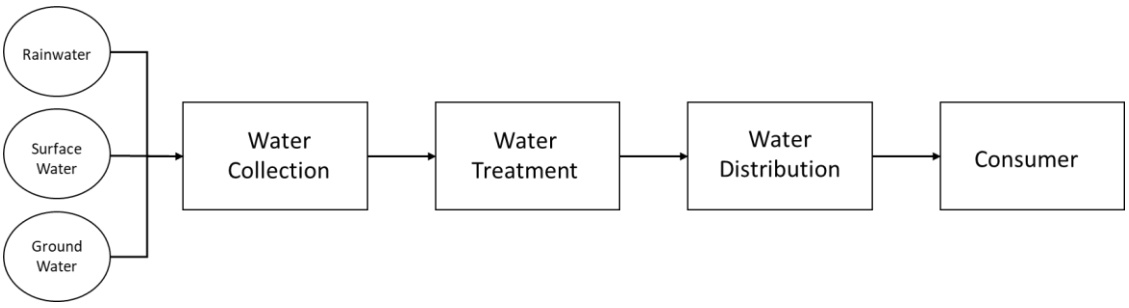

Figure 3: Basic diagram of a water-supply system

Water Collection

The water collection involves the sourcing of water from different sources, depending on the kind of water source. Water sources could be underground water, surface water which includes rivers, streams, and lakes, and rainwater.

Water treatment

Water treatment combines a series of actions – coagulation. Sedimentation, filtration, and disinfection- to provide clean, safe water for drinking. The water treatment process of recent time protects the consumers from waterborne disease. The treatment plant is the place where water treatment is carried out. With the spread of industrial control systems (ICS), modern water treatment plants leverage various technologies to ensure water is safe before distribution.

Water Distribution System

The distribution system is the total facilities that are used to supply water between the source point to the place where it is used. The system's main goal is to ensure water is delivered to end-users with acceptable quality, quantity, and pressure.

2.2.2. Water Cyber-Physical Systems

Cyber-physical systems are systems that combine computational and physical capabilities and can interact with the physical environment through computation, communication, and control. Water CPS in this context describes the CPS devices and nodes deployed in the water supply network. Typical water CPS can measure the water quality status in real-time and detect when water is contaminated quickly. The application of CPS in water-supply systems could increase the efficiency, reliability, security, and integrity of the system [20]. To implement CPS for water or water CPS the following will be needed (1) sensing, communication, and networking technologies to enhance flexible, reliable, and high performing decentralized networks within the CPS. (2) other computing technologies such as data management, machine learning, etc. (3) adaptive and predictive hierarchical hybrid control technologies are critical to achieving tightly coordinated and synchronized actions and interactions in a water CPS that is intrinsically synchronous, distributed. [20]

The Networking and Information Technology Research and Development (NITRD) CPS vision publication suggested the information in Table 4 as a summary of the critical technologies needed for developing water CPS.

Table 4: key technologies to develop water CPS (Source: [20])

Key technologies	Role
Distributed sensing, ommunications and perception	Enable time-aware and time-critical func-tionality
Adaptive and predictive hierarchical hybrid control	Achieve tightly coordinated and synchronized actions and interactions in water CPS that is intrinsically synchronous, distributed, and noisy
Diagnostics and prognostics	Identify, predict, and prevent or recover from faults
Autonomy and human interaction	Facilitate model-based design of reactive water CPS that is used by humans
Validation, verification, and certification	Ensure high confidence in system safety and functionality
Abstractions, modularity, and composability	Enable water CPS system elements to be combined and reused while retaining safety, security, and reliability
Systems-engineering based architectures and standards	Enable efficient design and development of reliability systems while ensuring interoperability and integration with legacy systems
Integration of multi-physics models and models of software	Enable co-design of physical engineered and computational elements with predictable system behaviors
Cyber-security	Guarantee safety by guarding against malicious attacks

2.2.3. Blockchain technology

Blockchain is a persistent, transparent, public, append-only ledger, using a mechanism of creating consensus between distributed parties whereby that rather than trusting each other they trust the mechanism by which the consensus is arrived at. Blockchain was first introduced as the background technology for bitcoin [21] a decentralized payment method and other cryptocurrencies and has since been used for other non-financial applications.

The addition of a new block to the chain requires that participant nodes provide evidence of being better qualified to add the block than the other nodes. Thus the need for a consensus mechanism. Proof-of-work (PoW) for bitcoin [21] was the first consensus mechanism, other consensus mechanisms are Proof-of-Stake from ethereum, Proof-of-Elapsed-Time [22], Proof-of-Authority, etc. The participants manage the blockchain through consensus mechanisms like Proof-of-work (PoW) for bitcoin, Proof-of-Stake (PoS), or Proof-of-elapsed-Time (PoET) [23] and others.

Blockchain Basic Operation

The basic operation of the blockchain includes validation transaction, gathering of the transactions for a block, broadcasting the ballot transactions in the block, and consensus on the next block creation, and chaining the blocks to form an immutable record. A participant in the blockchain initiates a transaction, then specific participants called miners to perform work to verify the transaction, broadcast the transaction, then claim the right to add the transaction to a block. Transaction validation is done by all miners independently, invalid transacts will be discarded and are not added to the chain.

The verification of the identity of the participant is done by the system using what is known as digital signatures which are the Public key and Private key of the participant to verify the participant. This help to maintain the integrity of the system

A blockchain is a series of blocks, that sequentially linked to each other like in a chain-like form. Each block includes validated transactions. An example of a top-level blockchain is shown in Figure 5.

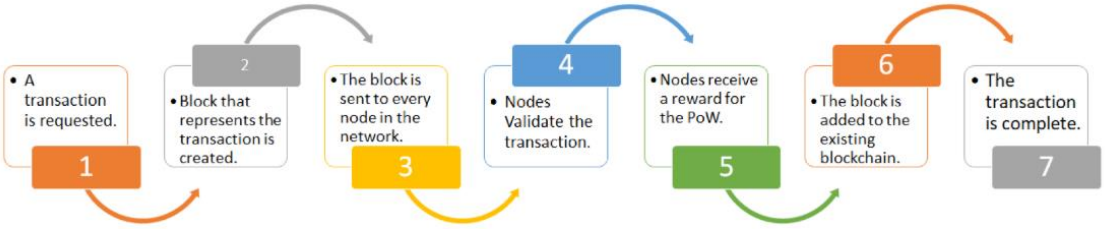

Figure 4: Blockchain process (Source [2])

Once a transaction is requested, it is distributed to all participant nodes in the network. The nodes must perform the verification before the transaction can be added to the block. Once the verification is complete, the nodes are rewarded for the PoW. Each node

confirms the block for correctness, the block is then added to the blockchain in every node.

2.2.4. Water Treatment Plant

At the water treatment plant, different forms of CPS entities are embedded in the water treatment process to ensure cleans and safe water is supplied to consumers. The different asset receives or transmits physical quantities and are transferred through the cyber environment. The value of the information sent or received is different depending on the type of device and the position in the treatment plant where it is deployed. Information exchange in the treatment plant is important to the entire system as any wrong data can have a significant implication on the entire water-supply system.

Table 5: Asset identification table for the treatment plant

	Asset Category	**Asset**	**Asset Description**	**Information Exchanged**
1	Field Devices	Control Valves	Deployed at several points in the plant. Opens or close to control water flow Actuated from the control center	Commands and acknowledgments
2		Pressure Transmitter	Measures water pressure which informs the control unit about the water pressure	Measurements and Configurations
3		Flow Meter	Measures flow rate and transmit to control	Measurements and Configurations
4		Level transmitter	Measures water level and sends to control	Measurements and Configurations

5		Pressure Pump	Pumps water based on pressure value received from the control center.	Commands and acknowledgments
6		Air blower	Blows air into the filtration chamber, it is activated by control commands	Commands and acknowledgments
7		Water quality analyzers	Checks chemical composition of water such as PH, turbidity, conductivity, ORP and chlorine level	Measurements and Configurations
8		Programmable Logic Controller (PLC)		
9	People	Operators	people working in the treatment plant	

2.3. Risk Management / Threat Assessment

We are going to discuss risk management assessment frameworks in this section. First, we are going to introduce the basic concept, some common risk assessment frameworks and then we further expatiate on the ISSRM which will be used in enabling trusted cyber-physical systems architecture with blockchain technology in the water-supply system. This section is further divided into two Subsections, 2.3.1 and 2.3.2.

2.3.1. Risk Management Frameworks

According to the International Standard Organization (ISO), information security risk is defined as the possibility that vulnerabilities of an asset, or group of assets will be

exploited by a particular threat, subsequently leading to a variety of harms in an organization [23].

2.3.2 Information Security Risk Management Framework

Information security risk management can be said to be a continually recurring activity, involving the pointing out and fixing of information security risks [24]. This framework generally involves the identification, description, and management of IS risks in a structured manner.

Some other popular methods such as ISO risk management method, ISSP, and Cyra have been innovated for the management of information security risks.

1. Integrated Safety, Security, and Privacy (ISSP) Risk Assessment Framework.

The use of the ISSP framework as a risk assessment framework is common when dealing with risk assessment in medical devices [25]. Key steps present in this framework are shown and elaborated subsequently;

A. Device Characterization

- In this step, the intended functions and technical characteristics of the devices are specified. Here the emphasis is particularly laid on the sensitivity of data.

B. Identification of Vulnerabilities, Threats, and Hazards

- In this section, events that could initiate threats and dangers are identified. Mainly the algorithm design's intrinsic flaws whose nature can be of security and safety concerns.

- Firstly, all security flaws or vulnerabilities found in the device program design and are listed using the Common Vulnerability Scoring System (CVSS) [20]. After this is done, all dangerous events that would later cause harm to the patient are then identified.

C. Control Analysis

- In the previous step, the identification of the flaws and vulnerability is identified. In this subsequent step, we will now analyze the available controls that are necessary for the approval of the device by the regulatory associations.

D. Vulnerability/Threat Likelihood Determination

- What this step is about is the calculation of the likelihood of the identified threat of the device in question. These threats are usually of cybersecurity concerns.

E. Hazard Likelihood Determination

The likelihood of hazardous events caused by system loss of integrity taking place is calculated using the Bayesian theorem. Secondly, this value is used by this framework to the possibility of a hazard caused by security flaws also.

F. Impact Valuation

- In this step, the effect of the hazard on the patient's health and the device is calculated.

G. Risk Determination

- Here, the risk will be estimated based on the values gotten from the preceding step.

$$Risk\ (Safety, security) = DI(d) * Hi(h, v) - CE(d) (4)$$

Where;

- DI represents the impact of the device's hazard on the patient's life.

- HO represents the possibility of the hazard happening from security flaws and algorithm related issues.

- CE represents the efficiency of existing controls of the equipment

H. Controls

- Safety and security controls will be incorporated in the equipment depending on the class of risk.

I. Monitoring and Patch Management

Lastly, since this framework is usually used for medical devices that are usually of utmost criticality, it is important to incorporate a monitoring mechanism and patch management routine.

2. Information System Security Risk Management Domain Model

The Information System Security Risk Management (ISSRM) Domain Model which gives the basis for the assessment of security-**oriented** models is a **conceptual** model represented as a Unified Modeling Language (UML) class diagram[26]. It gives an approach for the analyses, evaluation, and quantitative measurement of information security risks.

Table 6: ISSRM Domain Model Concepts (Source: [27])

Types	Concepts	Names
Asset-related concept	1	Asset
	2	Business asset
	3	IS asset
	4	Security Criterion
Risk-related concepts	5	Risk
	6	Event
	7	Impact
	8	Threat
	9	Vulnerability
	10	Threat agent
	11	Attack method

Risk treatment-related concepts	12	Risk treatment
	13	Security requirement
	14	Control

We have the following as the sections of concepts present in this framework;

- Assets related concepts,
- Risk related concepts and
- Risk-treatment related concepts

Now, we shall elaborate further on these concepts subsequently.

Assets related concepts

Here, we group assets as either business or information system assets, and then we specify security **criteria** (integrity, confidentiality, and availability) related to the businesses that will be specified.

Risk Related Concepts

Under this concept, we define the risk related modules and the risks itself as shown below;

- **Impact**: This can be said to be the potential unpleasant effects of the risk to an establishment.
- **Vulnerability**: properties of the IS asset that **constitutes** security loopholes.
- **Threat agent:** An agent that could probably cause damage to our system.
- **Threat**: this is a probable assault done by an agent, and it has the possibility of causing damage to our asset.
- **Event**: this is what we obtain when a threat is combined with a vulnerability or more.
- **Attack method**: the method used in attacking by an attack agent.

Risk Treatment-related concepts

In the risk treatment concept section, the **decision** on the treatment of risk satisfying the security risk will be explained. The handling of a possible danger can be done by risk prevention, risk transfer, risk reduction, and risk retention.

Security requirement: stipulates criteria that attained or met before the security standards are met.

Control:

These are systems, policies, and procedures designed to enhance safety as defined by the safety requirement.

Figure 6 shows a UML class diagram of the ISSRM domain model describing the relationship between the concepts already explained earlier. This shows how different components of the risk are connected methodically.

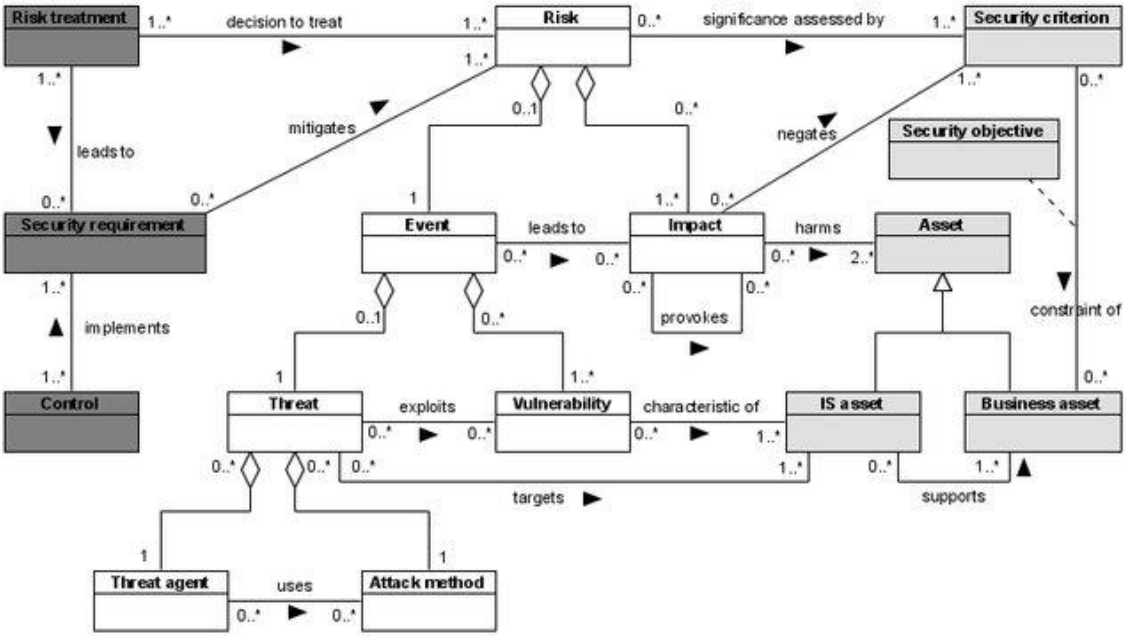

Figure 5: ISSRM Domain Model (Source [28])

3. CyRA

Cyra (Cyber Risk Assessment), which is a real-time risk-based security assessment framework has the following elements; Nested-Industrial control system (ICS) security

architecture, secure registration protocol, and risk-based multi-factor authentication protocol [25]**.**

- **Nested-Industrial control system (ICS) security architecture** Organizes ICS-based components according to their authentication and authorization criteria to resolve any possible cyber-attack threats and to implement countermeasures

- **secure registration protocol:** The secure registration protocol ensures that all components are registered before they are made available in the ICS. Each component has a digitally signed identity with encoded secrets or passwords. The ICS group enables the component to have access to other components in its group.

- **secure registration protocol and risk-based multi-factor authentication protocol** Applies real-time protection measures to the component identity confirmation process before a shared session key is formed for secure interaction and data exchange [25]. Below, such security measures are briefly discussed and a flowchart of the security measures are also shown in figure 7

i) **Threat Management (TM):** The mechanism is used to identify and communicate threats;

ii) **Vulnerability Identification (VI):** This is a method of finding vulnerabilities in security

iii) **Consequence Analysis** (CA): This is a mechanism that characterizes the seriousness of the ICS threat and vulnerability

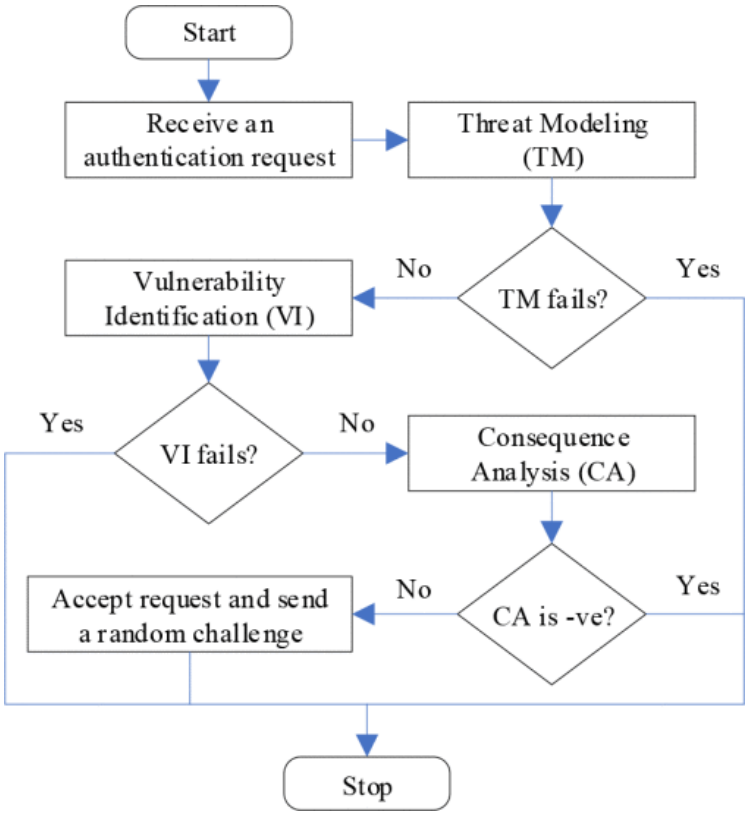

Figure 6: Security measure flowchart for CyRA (Source: [29]).

3. Cyber-physical Systems Assets in Water-supply system

The following chapter deals with the identification of cyber-physical assets in the entire water supply operation. There is an evaluation of the water supply system mode of operation in Section 3.2 on how there is inter-connectivity between various levels of the network. Afterward, the CPS assets in the network are identified as it applies to the scope of this research in section 3.3.

3.1. Introduction

The objective of Chapter 3 is to answer the RQ-1 research question - **How to identify relevant information exchanges between CPS nodes in WSS?** In this case, two sub-research questions were derived to answer the main research question as follows:

> **RQ1.1 -What are the relevant entities involved in data transmission and communication?**
>
> **RQ 1.2 - What information is exchanged in the network?**

The first sub-question RQ1.1 is answered in section 3.2 that discusses water supply communication flow. The focus of this thesis is on the CPS network of the system. Thus, specific attention is directed towards CPS interactions within the network.

The second research question is answered in section 3.3. The Water supply network is described in detail, with specific CPS assets identified and the information exchange that takes place in them.

3.2. Water-supply system Communication Flow

The water sector as explained in Chapter 2 consist of several independent sub-systems integrated to provide water to the end-user either for domestic use, industrial use, or even for fire-fighting purpose. The water supply network shows a sequence of workflows for the water supply scheme [30]. The following industrial areas include; water source, water treatment, and water distribution. The scope of this thesis is limited to the information technology (IT) and operation technology (OT) communication with the water-supply system. The following communication levels are therefore considered- water treatment plant, water distribution network, customer management, and consumer site.

Modern-day water supply infrastructures are designed with systems that allow for robust data/events, dependable, flexible, reconfigurable. This technical requirement has morphed to the integration of CPS in water-supply systems for monitoring and control [9].

The process flow diagram in Figure 7 shows the various levels of the water supply network and how communication of data and events is exchanged between the various agents.

3.2.1. Treatment Plant

This level involves the collection of water from the various sources - depending on the facility's preferred source – and the preparation of the collected water for consumption. The treatment plant is installed with several sensors sensing various physical quantities such as flow rate, pressure, water level, and chemical compositions in the water. There there are actuators that are controlled via software commands to alter some physical actions. These sensors and actuators that are capable of both physical and cyber characteristics are embedded in the various control valves, flow meters, level transmitters, pressure pumps, air blowers, agitators, and on/off valves.

3.2.2. Monitoring and Control Center

This is most times a remote room or location apart from the water treatment entities but is linked through wired or wireless internet protocols. Presently, many devices and sensors in the water utility sector are not connected to the internet [17], thus the need for CPS based architectures.

At the control and monitoring center, the activities of the treatment plant are monitored and controlled distribution network control as well. At this level, there are Computing devices with specific software installed to manage the various activities described in Figure 8. Sensor data are received and processed, actuator commands are sent to perform specific actions, conditions of transmission lines are monitored for leakages, damaged pumps, or contaminated water through the several flow meters and pressure valves and water quality testing equipment and logs of all activities are stored in a database.

3.2.3. Water Distribution Network

This is the network that delivers water at the appropriate pressure for plumbing. The distribution network is equipped with several CPS devices that perform different actions. These devices are connected via the internet to the control center. On the distribution network just like at the treatment plant, real-time water quality monitoring is carried out, but it is such that is extended to remote locations within the water distribution system. The CPS devices monitor water conditions such that a slight change in the parameters of the water quality triggers a contamination warning [20].

Some of the devices such as flow meters – that measures flow rates and helps to discover leakage, allow the control center to know how water is consumed in a particular location for future planning, pressure pumps, control valves, reservoir tank level transmitters, water quality testing equipment.

3.2.4. Customer Management

Customer management the level where the customer or consumer-related matters are handled. This department is collaborating with the control center and the customers as well. They prepare invoices for the consumers, authorize cut off for defaulting customers, take and process customer complaints, and keep customer records. This is a very import section of the water supply section as it involves both internal and external collaborations. In this section, there are computing devices where agents remotely fetch data from the control and monitoring units using applications and through the internet.

3.2.5. Consumer Site

This is the last end of the water supply network, albeit wastewater collected from consumers can be channeled back to the treatment plant for recycling in some urban city systems. On the consumer side, there are assets such as control valves and nowadays smart meters are being introduced to manage water supply efficiently. Smart meters allow customers to be billed according to their consumption, without having employees of the utility company visiting the customer's premises for manual meter reading [31]. Secondly, the customer can communicate via e-mail or web applications with the water utility company to either lodge complaints or even demand for specific services.

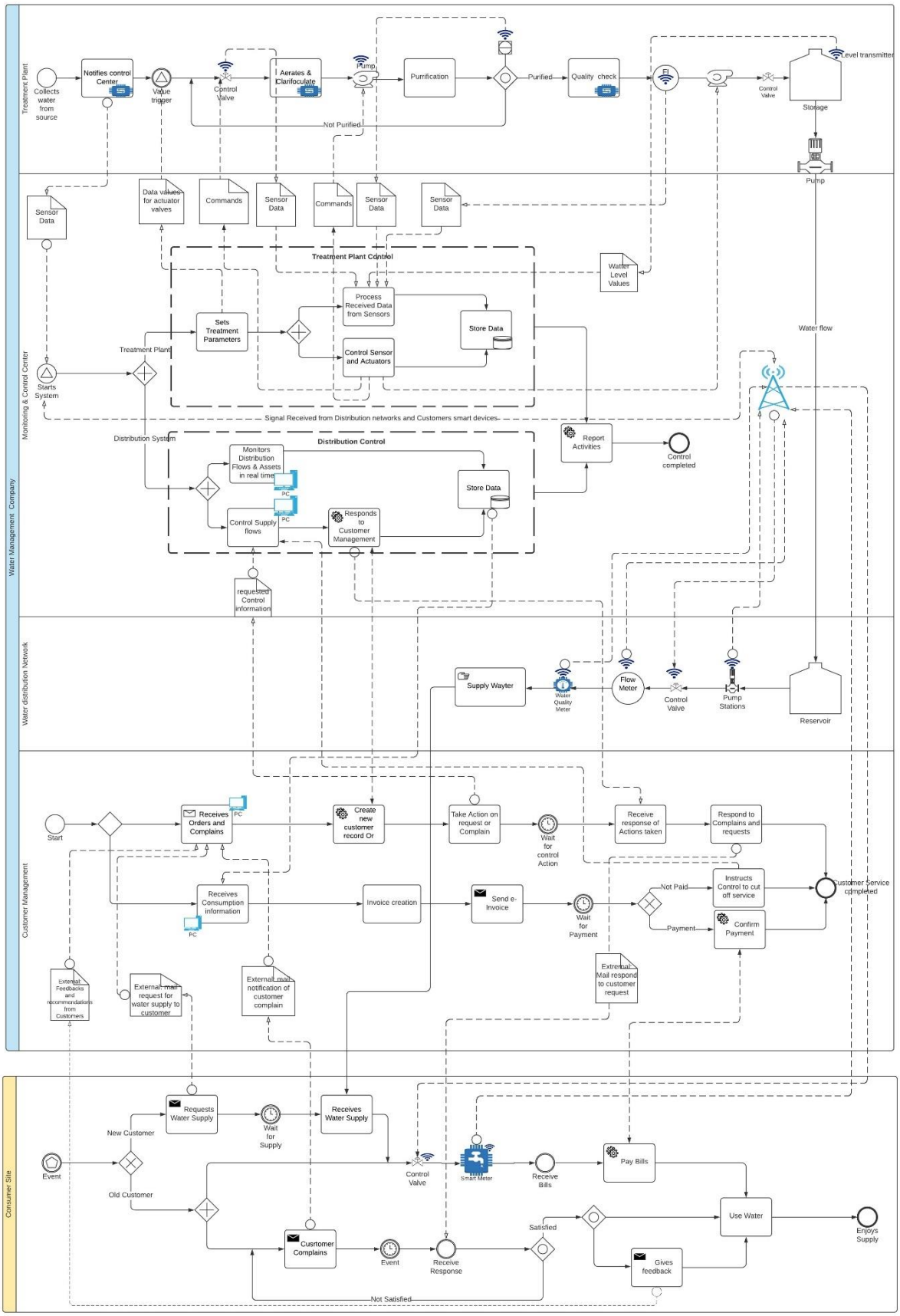

Figure 7:Water supply system information flow model

3.3. CPS Assets Identification and Data Exchanged

The water utility system information flow model is described in Figure 8, it contains the following interaction levels – treatment plant, control and monitoring center, customer management which are within the utility company, and consumer site that is external to the company. Each CPS asset generates specific data objects that can be for either internal or external communication and can also initiate further activities.

Assets are tangible or intangible entities that are valuable to a business or organization and that needs to be protected [20]. The identification of relevant entities or assets begins by determining the hardware entities involved in data exchanges in each compartment of the water-supply system. Identifying assets and putting a value on the assets is an important step in risk management. Assets could also be people, services, facilities, or processes [26].

The CPS entities in water supply technology are systems where sensors, actuators, and embedded systems are networked to sense, monitor, and control the physical environment by leveraging on the pervasiveness of wireless sensor networks (WSNs) which is an important component of the CPS [32]. WSNs are deployed at the physical interface where signals or data are transferred to the cyber environment or at the cyber environment interface from where instructions are sent to the physical environment [33].

Each process flow level has several similar CPS devices that perform similar actions but acting independently at different parts of the flow thus exchanging different data. In this thesis, we have decided to group the assets based on the nature of the devices and the form of data they exchange.

The CPS device for each asset category in the process flow is shown in the asset tables. The Information exchanged for each asset identified are also stated in the asset identification tables.

3.3.1. Monitoring and Control Center

The monitoring and control unit is the backbone of the entire network. At this stage, signals from other CP devices are processed, instructions/events are sent out. The CPS

devices in the Con troll center are majorly computing devices that may be on-premise or mobile but are connected to the network through the specific technologies or the internet.

Table 7: Asset identification table for the control center

	Asset	**Asset Description**	**Information Exchanged**
1	Computing Devices	Processing sensor data from all sensors on the network sends instructions to actuators.	Receives Sensor data from the treatment plant and distribution lines. Send activation Communicates with Customer management
2	Operators and Users	People operating and using the SCADA application software	

3.3.2. Distribution Network

CPS Devices deployed on the distribution network are remotely linked from the control center through several means. The CPS devices on the distribution lines include water quality analyzers, pressure transmitters, automatic valves for closure to stop water from flowing to sections with broken pipes,

Table 8: Asset identification table for the distribution network

	Asset	**Asset Description**	**Information Exchanged**
1	Control Valves	Close or open for water flow to specific parts of the network	Actuation instructions

2	Flow Meter	Provides real-time data of water flow rate	Measurements and Configurations
3	Pressure Pump	Endure continuous flow of water to areas where needed for distribution	Commands and acknowledgments
4	Water quality analyzers	Detecting intentional or unintentional contamination events within the system.	Measurements and Configurations

3.3.3. Customer Management

Customer management involves collaboration with customers, receiving and responding to complaints, keep customer personal details, and provide general utility services. Communication is also exchanged with the control center via email or other web-enabled means, collects utility records and reports from control databases also.

Table 9: Asset identification table at the customer management center

	Asset	**Asset Description**	**Information Exchanged**
1	Computing devices	For collaboration with customers and control center	Email (internal and external), customer data, web data
2	Support Agents	People responsible for supporting and responding to customers	Emails, phone calls

3.3.4. Consumer Site

Table 10: Asset identification table at the consumer site

	Asset	**Asset Description**	**Information Exchanged**

1	Smart meter	Tracks precise consumption data, can be monitored by customer and utility service providers.	Measurements and Configurations
2	Valves	Opens or closes to control authorized and unauthorized water flow to customer premises	Commands and acknowledgments
3	Consumer		

3.4. Assets Identification for CPS Architectures

Unlike other IT systems, assets in CPS architectures are identified differently mainly because the CPS assets interact with other systems. A CPS asset can be a physical asset, cyber asset, and interactions with other systems [34]. The asset identification should include all tangible and non-tangible assets in the water-supply system. Therefore, we shall further summarize the already identified assets into the table below to aid our threat identification and risk analysis in Chapter 4.

Table 11: Assets identification for CPS

Asset	**Component**
Field devices	Control Valves
	Automated Pumps
	Level Transmitter
	Air blower
	Water sensors
	Water quality analyzers

	Programmable Logic Controller (PLC)
	Flowmeter
Smart Devices	Smart Meter
Computing devices	Supervisory Computers
Communication and Network	WAN, LAN, Ethernet,
People	IT personnel, Customer Support Agents, Security advisers, Developers, operators
SCADA Application Software	Human-Machine Interface (HMI), Office tools, web application

3.5. Conclusion

This chapter is focused on identifying the CPS assets participating in the water-supply system. The process workflow presents different data exchanges at various levels of the system. The process involved in information exchange was explained, the CPS Assets for the various subsystems were identified and the data that are being exchanged was identified.

The analyses performed in this chapter are based on information exchange activities identified in the water-supply system process flow. The subsystems identified for analysis are treatment plant, control and monitoring, distribution network, customer management, and consumer site. The relevant CPS entities involved in the processes were identified and grouped based on their functionality and nature of information exchanged.

4. Risk Analysis of CPS Assets in Water-supply system

This chapter aims to apply the ISSRM domain model in analyzing the security risks identified in the water-supply system CPS architecture.

The analysis shall be providing answers to research question two: **How to identify the security threats that exist in information exchange?**

The research question is further broken down into the following sub-questions:

RQ2.1. What are the threat agents?

RQ2.2: What are the vulnerabilities within the system?

RQ2.3: What are the risk impacts?

Answers to the research questions RQ2.1 is provided in section 4.1 where the threats in CPS are stated. In Section 4.2, answers to RQ2.2, and RQ2.3 are provided by analyzing the assets identified in Chapter 3. For each asset identified, two possible risk scenarios are evaluated. The risk components - threat agent, threat, vulnerability, event, and impact are systematically derived from the process description of the identified assets

4.1. Security Threats of Cyber-physical Systems

Brauch in [26] defined threats as a possible danger that that is capable of exploiting the vulnerabilities in a system to cause potential harm. The CPS architecture can be considered at various levels, these levels include the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and the application layer according to ISO/OSI model [35] depending on the field of application. The threats to the CPS can be on any of these layers and so need to be protected. These threats are targeted at the assets in CPS identified in section 3.4.

Figure 8: Tree diagram of attacks and threats on CPS (Source [36])

Previous research on CPS security has proposed a tree of attacks and threats based on the functional model of CPS [28]. In Figure 2, the tree branches include attacks on the sensors, computing devices, communication networks, and feedback systems.

4.1.1. CPS Threat Agents, Motivations and Capabilities

This section presents the classification of possible intruders or attackers of CPS and their motivations and capabilities. Bugeja et al [36], presented a taxonomy of CPS threat agents, their motivations, and capabilities. The following section shall expound the classification. This is relevant to the main objective of this thesis which is to analyze digital security threats in a CPS network.

Threat Agents

Threat agent refers to an individual or group that can manifest a threat [17], Bugeja et al referred to the scheme of classification of threat agent by Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to develop a list of agent classes in the order of most capable to list capable: nations states, terrorist, competitors or organized criminals, hacktivist, thieves, and hackers.

Motivations

According to Bugeja et al, the threat agent is motivated by different things and the reason for their motivations could be: curiosity, personal gain, terrorism, and national interest.

Capabilities

The capabilities of the threat agents are what distinguishes them as threats to CPS architectures. The capabilities of the threat agents can be classified as low, moderate, and high.

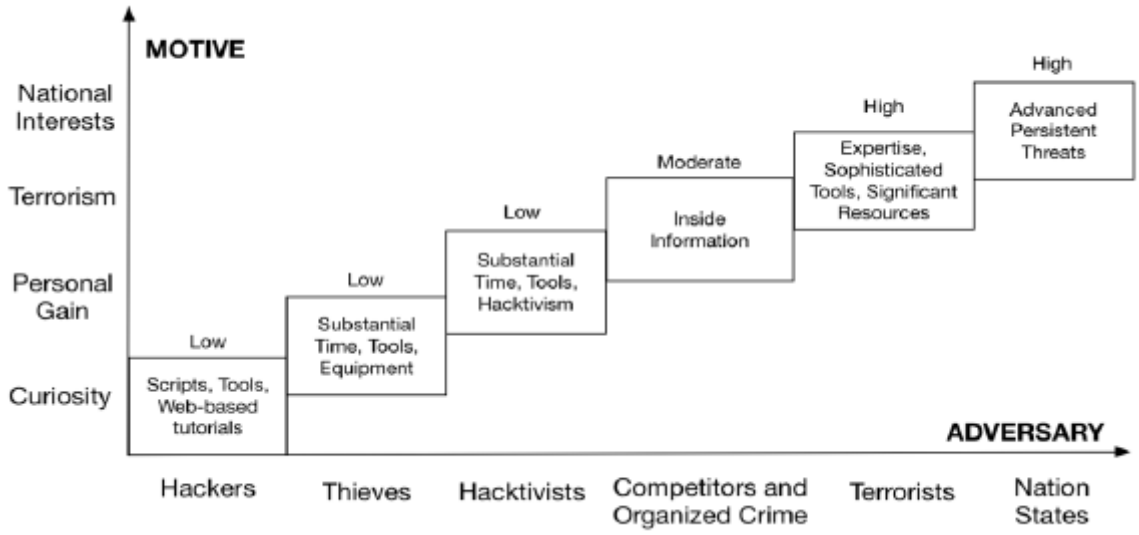

Figure 9: Typical CPS hostile threat agent with their capabilities and likely primary motivation (Source [36])

4.2. Risk Analysis of the CPS Assets in Water-supply Systems

In this section, we shall be conducting the risk analysis of all identified assets. Two possible scenarios are evaluated for each situation.

4.2.1. Field Device Risk Analysis

Two possible attack scenarios are described for the field devices asset. Each of the attacks has its owns threat agent. Table 12 describes each of the threat agent, the event, and risk components of the Field device.

Table 12 – Field Devices risk and threat analysis

Threat Agent	Nation-state Motivation: Terrorism, need to inflict violence Capabilities: high expertise, Sophisticated tools, Significant resources	Hacker Motivation: Curiosity, to experiment Capabilities: Low expertise
Threat	Attack on the actuator pump	Manipulation of sensor reading
Vulnerability	Weak firewall	Unprotected sensor device from electromagnetic waves
Event	An attack on the pump causing it to malfunction	An attacker using acoustic or electromagnetic wave to manipulate the physical properties of the sensor
Impact	Loss of control of the water treatment process	Physical damage of sensor device which could be cost-intensive
Risk	Unsafe water distributed to consumers	Transmission of wrong data to the command-and-control server

The analysis identifies two potential threat agents– a nation-state attacker and a hacker. For the first agent, his motivation is to terrorize another nation by causing fear and inflicting harm on the citizens of the enemy nation. For the hacker, his motivation is just out of curiosity for experimental purposes. Both attackers know the target field device and its functionality. The table describes the events of the attacks, the vulnerability in the first case could be because of poor defense systems on the network while in the second case it may be because the field device is not well shielded from electromagnetic wave signals.

Both attacks will negatively impact the water-supply system. The attacks could lead to a total loss of control of the water treatment system in the first case, while in the second case it may cause physical destruction of the could eventually result in more complex situations depending on the location of the field device.

4.2.2. Smart Device Risk Analysis

Two possible attack scenarios are described for the field devices asset. Each of the attacks has its owns threat agent. Table 2 describes each of the threat agent, the event, and risk components of a Smart water meter

Table 13 – Smart water meter risk and threat analysis

Threat Agent	Thief Motivation: Personal gain, Capabilities: Substantial expertise	Hacker Motivation: Personal gain, need to steal information Capabilities: substantial expertise
Threat	Manipulation of the smart water meter	Stealing of customer information
Vulnerability	Encryption method(s) are not properly implemented	Lack of network security at the edge, a potential entry point for malware

Event	Hacker trying to hack a smart water meter to cheat the utility and reduce their water bill	Privacy Compromise of end-user, the release of user personal information and home activities
Impact	Loss of revenue for the utility company	Loss of system integrity
Risk	Loss of control of smart meter by the utility company	Exposing user information to an unauthorized group

The scenarios in this smart water meter analysis present two equally capable threat agents – a thief and a hacker. The thief's motive is personal gain as he intends to manipulate the smart meter to avoid paying the appropriate utility bill. The hacker's motivation too was for personal gain, as he tries to gain access to the premise of the smart meter user and spying into the activities of the user as well as stealing the personal information of the user. The table also describes the vulnerabilities that may have allowed the cyber-attacks. In the case of the thief, a possible lack of security measures in the smart devices could allow a moderately expert hacker to manipulate the meter. In the hacker's case, the lack of network security at the edge device (smart water meter) could become a potential entry point for malware.

The water utility company is therefore at the risk of losing control of the smart meter that would impact the company's revenue adversely. They could also be at the risk of unauthorized exposure of customer's information which could impact the integrity of the utility company and could lead to serious legal disputes.

4.2.3. Computing Devices Risk Analysis

Two possible attack scenarios are described for the field devices asset. Each of the attacks has its owns threat agent. Table 3 describes each of the threat agent, the event, and risk components of a computing device

Table 14: Computing Devices risk and threat analysis

Threat Agent	Hacker Motivation: Personal gain, need to steal information Capabilities: substantial expertise	Thief Motivation: Personal gain, Capabilities: Low expertise
Threat	Computer virus on a laptop computer of an employee.	Unverified login to the computer
Vulnerability	Poor network separation for administrative and SCADA systems	Absence of multi-factor authentication
Event	Hackers placed a computer virus on the laptop of an employee. Then used the infected laptop as an entry point, and installed malicious software on the plant's computer system	Former employee illegally accessed computer system to download emails and other personal documents. He performed these actions using the credentials of other employees after the district did not renew his contract
Impact	Illegal distribution of emails and other information	Loss of valuable emails and document
Risk	Adversary penetration	Unverified user access

The motivation of the attacks in this table is similar for both cases – personal gains. The hacker, in this case, has substantial expertise who was able to place a computer virus on an insider's laptop and from there was able to run the malware on the computer and

impacted on the plant's control system and distributing illegal emails and gaining access to other information. The vulnerability, in this case, was as a result of the administrative computers being on the same network as the control systems.

The second scenario is the case of an aggrieved former employee who gained illegal access to a computer system and carted away with emails and documents by using the credentials of other employees. Though the thief is of low expertise because the system is vulnerable in that it does not allow for multi-factor authentication, which places the company at the risk of having unverified users accessing their network. In this case, the negative impact on the company was such that valuable information in the form of email and document was released to the wrong hands.

4.2.4. Communication and Network Risk Analysis

Two possible attack scenarios are described for the field devices asset. Each of the attacks has its owns threat agent. Table 2 describes each of the threat agent, the event, and risk components of the communication and network components of the CPS

Table 15: Communication and network risk and threat analysis

Threat Agent	Terrorist Motivation: Terrorism, inflict fear Capabilities: high expertise, Sophisticated tools, Significant resources	Organized Criminal Motivation: Personal gain Capabilities: moderate expertise, with inside information
Threat	The hijacking of the system.	Unauthorized user in the network
Vulnerability	- Weak password - Weak firewall	Lack of authorization and authentication

Event	The attacker gains access through a remote access point exploiting the weak password and firewall. The attacker was able to disrupt communications, access critical data, and inject malicious control commands as well as forge false data into the control center.	Cybercriminals can launch ransomware attacks, locking devices and encrypting files, then request money in exchange for unlocking and decrypting the devices and files respectively.
Impact	Control center failure	Loss of vital document and a possible loss of fund to decrypt files
Risk	Loss of control of the entire system	Loss of business-critical information and files

The analysis identifies two potential threat agents– a terrorist and an organized criminal. For the first agent, his motivation is to terrorize by disrupting the water supply. For the criminal, his motivation is for personal gains. Both attackers are familiar with communication and network infrastructure. The table describes the events of the attacks, the vulnerability in the first case is due to weak passwords and firewalls while in the second case it is because of lack of authentication and authorizations in the communication systems.

Both attacks will negatively impact the water-supply system. The attacks could lead to a total loss of control of the water treatment system in the first case, while in the second case it may lead to the destruction of vital documents and a possible loss of funds to decrypt infected files.

4.2.5. Operators and User-Risk Analysis

Two possible attack scenarios are described for the field devices asset. Each of the attacks has its owns threat agent. Table 2 describes each of the threat agent, the event, and risk components of the activities of an operator or user

Table 16: Operator and user risk and threat analysis

Threat Agent	Hacker, operator Motivation: Curiosity, to experiment Capabilities: Low expertise	Hacker, Motivation: personal gain Capabilities: Low expertise
Threat	System usage error	Illegal processing of data
Vulnerability	Insufficient security training	Lack of monitoring mechanisms
Event	An untrained operator modifying the security configuration of the security system erroneously left the network exposed for a cyberattack which led to the malfunctioning of the distributing network	A customer agent clicked a malicious link in an external email that made the agent download and executes a program which is, in fact, a virus. This led to the corruption of several files on the user's computer alone.
Impact	A partial or total shutdown of the treatment plant	Loss of files on the user computer
Risk	Firewall and defense breakdown	Phishing attack

The analysis identifies two potential threat agents both being insiders – the operator and a hacker through a customer agent. For the first agent, his motivation is curiosity, while for the hacker, his motivation was for personal gain. The first agent is an untrained operator whose experimental actions expose the system to potential cyber-attacks. The second is an ignorant user falling for phishing activities from an external hacker. The vulnerabilities observed in both cases are an untrained operator and a lack of monitoring activities in the network for malicious activities.

Both attacks will negatively impact the water-supply system. The attacks could lead to a total or partial shutdown of the treatment plant, while in the second case it may cause loss of important documents in the user's computer

4.2.6. SCADA System Risk Analysis

Two possible attack scenarios are described for the field devices asset. Each of the attacks has its owns threat agent. Table 2 describes each of the threat agent, the event, and risk components of the SCADA system.

Table 17: SCADA system risk and threat analysis

Threat Agent	Terrorist, a former employee Motivation: Terrorism, inflict fear Capabilities: high expertise, Sophisticated tools, Significant resources	Hacktivist Motivation: personal gain Capabilities: high expertise, Sophisticated tools, Significant resources
Threat	Unauthorized access to the SCADA system	unauthorized use of a computing resource
Vulnerability	Poor contract monitoring system for employees	Lack of monitoring mechanisms

Event	Aggrieved third-party contractor enabled remote control and monitoring of the pumps through a SCADA system and altered configuration of pumping stations	Hacker using SCADA network resources for crypto mining which triggered several alerts
Impact	Release raw sewage into the surrounding environment	slow response times, and overheating of the system
Risk	Loss of communication and pump control capabilities	Loss of computer resources due to cryptojacking activity

The analysis identifies two potential threat agents– A terrorist, who is a former employee and a hacktivist. For the first agent, his motivation is to terrorize another nation by causing fear. For the hacker, his motivation was for personal gain. Both have reasonably high expertise and possess significant resources. The table describes the events of the attacks, the vulnerability in the first case was the non-termination of access rights of the former while in the second case it was due to the lack of monitoring mechanism being put in place.

Both attacks will negatively impact the functionality of the system. The attacks could lead to a total loss of control of the control pumps leading to wasted water resources in the first case, while in the second case it may cause the system to respond slowly and lead to overheating of the processing units.

4.3. Conclusion

In this chapter, the security threats in CPS were determined which further confirms the identified assets identified in chapter 3. Also, the Assets were analyzed to determine the security risks on each of them. In the determination of the risks on these assets, the risk

components of the assets were identified. The risk components are – threat agent, threat, vulnerability, risk event, and impact. The risks were derived by systematically combining the risk components of each asset.

The tables in this chapter presented two possible scenarios. As a result, two possible risks were derived from each of the identified assets. The risk analyses were performed based on the risk components by systematically identifying all risk components from the process described in Chapter 4.

5. Blockchain-based Security Controls for implementing Security Requirement on Assets

The objective of this chapter is to apply blockchain-based security controls to mitigate the threats identified in Chapter 4. This implementation shall be providing answers to research question three: **How to use blockchain technology to mitigate trust issues that affect the water infrastructure CPS?**

The research question is further broken down into the following sub-questions:

RQ3.1. What are the blockchain qualities that enable security?

RQ232. What are the security requirements in the water-supply system CPS architecture?

RQ3.3: What are the blockchain security controls that implement the security requirements?

Answers to the research questions RQ3.1 is provided in section 5.1 where the qualities of blockchain that enable trust are explained. In section 5.2, answers to RQ3.2, and RQ3 are provided.

5.1. Blockchain Security Control Concepts

This section introduces the blockchain tools and concepts that form the security controls and enable trust and security in blockchain technology. These concepts include public key infrastructures, consensus mechanism, decentralized nodes, digital identity, and smart contracts. These concepts will be applied in Section 5.2 to address the security threats identified in Chapter 4.

5.1.1. Public Key Encryption

Public key encryption or public key infrastructure (PKI) is a cryptographic methodology that applies a pair of keys called public/private key pairs, a private key that is secretly kept, and a publicly available public key on the network. In the blockchain ecosystem, the public key can be used as addresses, account numbers, Identity numbers, etc. that can

be shared or broadcasted on a network [37]. Through advanced cryptographic techniques, PKI helps to ensure the authenticity and integrity of a message.

To achieve trust, blockchain uses public-key encryption alongside hash function and both are pivotal to the security and functionality of the blockchain environment. With public-key encryption; messages can be encrypted so that they deliver only to the intended destination, digital signatures are generated to prove the identity of the sender, and the digital signatures are used to verify a message was not altered during its transit.

5.1.2. Consensus Mechanism

The consensus mechanism is the component of the blockchain network that ensures each participant agrees about the state of the network in a trustless environment. It also controls the other operations in the network such as introducing new transactions and incentivizing the participants [38]. It is appropriate to say that a consensus mechanism is used to achieve agreement among the decentralized nodes in the blockchain network. Whenever a new transaction is requested, the various nodes perform some work to verify the authenticity and integrity of the network in which the entire system agrees to the correctness then it is added to the blockchain and this transaction is replicated on all the participating nodes. Today, there are various methods of finding consensus in a blockchain network depending on the blockchain network in which it is used: Practical Byzantine Fault Tolerance (PBFT), Proof of Work (PoW), Proof of Stake (PoS) and many others [39], [40].

Proof of Work

Proof-of-Work is the consensus system that is used in Bitcoin. In PoW the proving participant reveals to the verifier nodes that he has done a certain amount of computational work within a given time interval [41]. Proof of work may be used to prevent denial of service attacks and other misuses of the network, it also guarantees that the next block in a blockchain is the only true version. PoW has been generally criticized that it wastes energy because it requires a large amount of computational power [42]. PoW is the most commonly used consensus algorithm

Practical Byzantine Fault Tolerance (PBFT)

Byzantine fault tolerance is the characteristics used to describe the ability of a distributed system to reach an agreement or consensus despite having malicious or faulty nodes within the network The idea for BFT is to prevent system failure in the event failing nodes [43]. Whereas PBFT is an algorithm that protects against byzantine faults. PBFT is currently being used in some blockchain platforms especially in hyperledger fabric - a private blockchain.

Proof of Stake (PoS)

Proof of stake is a common energy-saving substitute for proof of work. In this type of consensus mechanism rather than investing expensive computer resources, the participants stake coins in the system. The participants' stakes determine their chances of discovering the next block. In proof of stake, the process of arriving at consensus is like that of PoW whereby the fork with the highest stake is selected as the main chain [42].

5.1.3. Digital Identity

According to Buccafurri et al [3], defined digital identity as the information of an entity that is used by a computer system that distinguishes an external agent that could be a person, an application, or a device. Identity management and verification is an important feature of blockchain technology, such that when a file is added to the blockchain system, its information's authenticity is guaranteed by all the nodes maintaining the network. Blockchain uses a public/private key pair to verify the identity of an entity. Users can create and manage their identities with blockchain through a decentralized identifier, identity management, and embedded encryption[1]. Blockchain overcomes issues related to data insecurity, fraud, and inaccessibility by its identity management features.

[1] Blockchain in Digital identity - Consensys , Accessed 3/08/2020.

5.1.4. Decentralized Nodes

With blockchain being a decentralized distributed ledger, it discards the concept of having a central control point or trusted third party (TTP). Instead, it depends on a peer-to-peer network system where every participant contributes to managing the network. Each participant or node has similar records in what can be referred to as a massively replicated ledger [48]. Concerning the scope of this thesis, the independent CPS devices are nodes which in a blockchain network will function as decentralized entities with the system.

5.1.5. Smart Contracts

A smart contract is a computer program that is capable of automatically facilitating, validating, or enforcing the negotiations or performance of a contract. It allows the execution of a contract code without the influence of a third party. Smart contracts execute the agreements in a contract either in part or in full and it is stored on the blockchain. The data in the blockchain is immutable, which makes the deployed smart contract unalterable.

Smart contracts leverage three blockchain features namely: tamper-proofing, permanent operation, and data transparency [44].

5.2. Security Control on Assets

In this section, the risks identified in Chapter 4 will be managed by the application of security requirements and security controls. By applying the security requirements and control, the risk is eliminated, or its effect is reduced. For this work, blockchain security control shall be applied. The risk treatment shall be based on the assets identified in the water-supply system CPS architecture.

5.2.1. Risk Treatment for Field Devices

Scenario 1: Malicious attack on the actuator pump (node device) to take over control of its function. The vulnerability detected was a weak firewall. The following table presents the security requirement and blockchain control applicable.

Table 18: Security control on field devices -Scenario 1

Asset	Risk	Vulnerability	Security requirement	Blockchain security controls
Field devices and control application	Unsafe water distribution due to loss of plant control	Weak firewall	Secure access to the network	Blockchain access control based public key infrastructure.
Explanation	Blockchain provides a public key encryption system. Signing all the data by each CPS sensor with their private key may prevent this type of threat.			

A recent review on the use of blockchain to mitigate cyberattacks in IoTs, blockchain helps to guarantee confidentiality, data integrity, and availability (CIA), with the use of the public/private key pair feature of blockchain [45]. Blockchain uses PKI to validate and authenticate the integrity of the information being transmitted on the blockchain.

5.2.2. Risk treatment for smart device

Scenario 2: Hacker with a reasonable level of expertise breaking through the smart water meter to steal and gain access to user personal information. The vulnerability detected is a lack of network security at the edge. The following table presents the security requirement and blockchain control applicable

Table 19: Security control on a smart meter, Scenario 2

Assets	Risk	Vulnerability	Security requirement	Blockchain security controls
Smart devices and user data	Exposing user information to an unauthorized group	Encryption methods are not properly implemented	Access control on user data	Blockchain access control based on

				public-key encryption
Explanation	encrypting user's information with their public keys and granting access only to the specific users			

In a research conducted by Wang et al in [46], User-information can be secured with blockchain public key infrastructure (PKI) which implements strong authentication, by allowing only authorized users with the right public/private key pair combination to access the customer's personal information. They introduced a framework whereby the owner is capable of distributing secret keys and encrypt shared data by specifying access guidelines on a smart contract. According to K*foury and Khoury* in [47], blockchain PKI overcomes trust concerns and eliminates the complexity of user protection.

5.2.3. Risk Treatment for Computing Device

Scenario 3: A former employee illegally accessed the computer system to download emails and other personal documents. He performed these actions using the credentials of other employees (who are unaware) after the district did not renew his contract. The following table presents the security requirement and blockchain control applicable.

Table 20: Security control of computing devices -Scenario 3

Assets	Risk	Vulnerability	Security requirement	Blockchain security controls
Computing device	Unverified user access	Absence of multi-factor authentication	Provide verifiable authentication system for user log in	Apply blockchain decentralized digital identity to for logging into enterprise computers.

Explanation	Using blockchain, all the CPS nodes can be assigned a digital identity and access can be assigned only to specific users. Digital identity provides strong authentication and data encryption.

Blockchain-based digital identity provides privacy and control, whereby the user is to have exclusive access to their assets such that encrypted data can only be signed with keys that are in the user's control [48]. To ensure access is given to the right user, the blockchain used digital identifiers (DID) where the user is verified by providing a proof of ownership, which requires that the user signs with his private key that belongs to the DID. If the keys match, then the user is granted access.

5.2.4. Risk Treatment of Communication Network

Scenario 4: A cybercriminal with moderate expertise launches ransomware attacks and locking devices and encrypting files in exchange for cash. The following table presents the security requirement and blockchain control applicable.

Table 21: Security control on communication network – scenario 4

Assets	Risk R_4	Vulnerability	Security requirement	Blockchain security controls
System Network	Loss of business-critical information and files	lack of authorization and authentication	Improve network security strategy	Decentralized blockchain network to monitor and control activities at the nodes.
Explanation	A decentralized CPS for water management based on blockchain is not susceptible to this type of attack since the system is not centralized. The network can choose to ignore data coming from a specific node if it is determined that the node is compromised, and it is transmitting incorrect information. With distributed blockchain consensus, only correct data can be processed by the network.			

Normally, the blockchain is fault-tolerant, that is because of the in-built redundancy. In [49], Kim stated that having many nodes renders the blockchain network resilient, even when some of the nodes are infected with a virus or are attacked, the blockchain is still accurate and accessible by all its healthy nodes.

5.2.5. Risk Treatment of Operators and Users

Scenario 5: An untrained operator modifying the security configuration of the security system, erroneously left the network exposed for a cyberattack which led to the malfunctioning of the distribution network

Table 22: Security control on operators and users – Scenario 5

Assets	Risk R_5	Vulnerability	Security requirement	Blockchain security controls
User	Firewall and defense breakdown	Insufficient security training	Access network and improve failure isolation system	Blockchain distributed nodes
Explanation	There is no single point of failure in the blockchain network. All the nodes are capable of verifying information and processing only correct data.			

Salman et al [60], while describing the properties of blockchain established that blockchain solves the problem of centralized decision making and eliminates the possibility of a single failure point. For blockchain to guarantee a more reliable system there must be a consensus among all nodes. Identical information is stored across the network.

5.2.6. Risk Treatment of SCADA system

Scenario 6: Aggrieved third-party contractor enabled remote control and monitoring of the pumps through a SCADA system and altered configuration of pumping stations

Table 23: Security control on SCADA system – scenario 6

Assets	Risk R_6	Vulnerability	Security requirement	Blockchain security controls
SCADA system	Loss of communication and pump control capabilities	Poor contract monitoring system for employees	Control authorized remote access	Implement blockchain smart contracts
Explanation	Insider attacks can be addressed by blockchain using smart contracts. For instance, all the possible functions executable by a contractor or staff will be outlined in a smart contract. Therefore, no user can execute any function outside what is described in a smart contract			

With a smart contract, a scheme is designed in [50] to prevent server impersonation attacks and create a secure way to verify the service periods. Also, the activities of operators can be subjected to a role-based access control mechanism using smart contracts [51], which restricts the extent of activities or configurations that can be down by users.

5.3. Conclusion

In this chapter, we have presented the blockchain security controls for water CPS: public-key encryption, consensus algorithms such as PoS and PoW, digital identity smart contracts, and decentralized node in Section 5.1. Then in Section 5.2 provided security requirements and our proposed blockchain security controls for the various scenarios presented in chapter 4 which eliminates or reduces the impacts of the risks.

6. Blockchain-based Risk Security Control Model and Evaluation

The goal of this chapter is to first, present the model for the blockchain security controls to the risks identified in Section 5.2. The goal of the model is to present how the implementation of blockchain security protocols can mitigate the risks and secure the assets. Secondly to evaluate the validity of the models proposed. The Evaluation was carried according to design-science research evaluation by case study and expert interviews. Finally, Section 6.3 presents the paper-based deployment-feasibility evaluation that considers existing and planned blockchain-technology focused projects.

6.1. Blockchain-based Risk Security Control

In Section 5.1, we discussed some blockchain concepts that enhance trust and security in cyber-physical systems. These concepts and protocols have been employed in creating a model for the control of the security risks with blockchain. The goal of this thesis is to apply blockchain security features on the cyber-physical assets of the water supply system to ensure security and guarantee trusted communications. The following sections shall present the model designed for each of the scenarios and analyzed them appropriately. The risk analysis in this thesis is based only on the CPS devices that are applicable in the water supply systems. We have grouped these assets based on their area of functionality and the roles they played in the CPS domain.

6.1.1. Risk Treatment for Field Devices

Field devices according to Table 11, are the assets that operate far away from the control systems, they can also be considered as edge devices. To carry out risk security control on these devices, we came up with a scenario that involves a field device. The scenario presented a situation where the field device was compromised.

Scenario 1

Asset: Field devices and control application

Risk: Unsafe water distribution due to loss of plant control

Vulnerability detected: Weak firewall

Security Requirement: Secure access to the network

Blockchain security control: blockchain-based access control based on public key infrastructure.

Model Description

To implement the blockchain security control, the model BPMN diagram has been developed in Figure 10.

Normal Operation: To control a pump (field device), The control center generates appropriate commands for control which is sent across the network (wired or wireless) to the actuator device without any interference. The actuator receives the signal and acknowledges the receipt by sending a response signal back to the control system, then the pump will be actuated.

Attack Condition: When the actuator is attacked by a hacker since it is a CPS component with the capability of combining physical activities and the computational process, it may be exposed and vulnerable to attack. In this scenario, the attack on the actuator will either cause to receive malicious signals or send false feedbacks to the control system, which will eventually result in the loss control of the actuator by the control system/

Blockchain-based Security Control: To the kind of situation above of the field device, we propose a blockchain-based security control system, and this approach is modeled in Figure 10. Blockchain uses public key infrastructures to verify, validate, and authenticate a transaction thereby eliminating the chances of transmitting false and invalid data across its network. By implementing blockchain on the network described in the scenario, at the instant of sending the control command, the command signal is encrypted with the public key (address) of the destination node before it is sent. Only the receiving node has the private key that can decrypt the signal sent it. Even if it is interrupted by any malicious activated it cannot be decrypted by another node or activity. On receiving the encrypted signal, the actuator decrypts it, process the signal, executes the directed command. The actuator must send an acknowledgment message to the control system. This message too must be encrypted in such a way that only the control system can decrypt it. If the pump

is compromised, because of the PKI no harm will be done to the overall system. The proposed model describes this risk of security control for the pump as a field device.

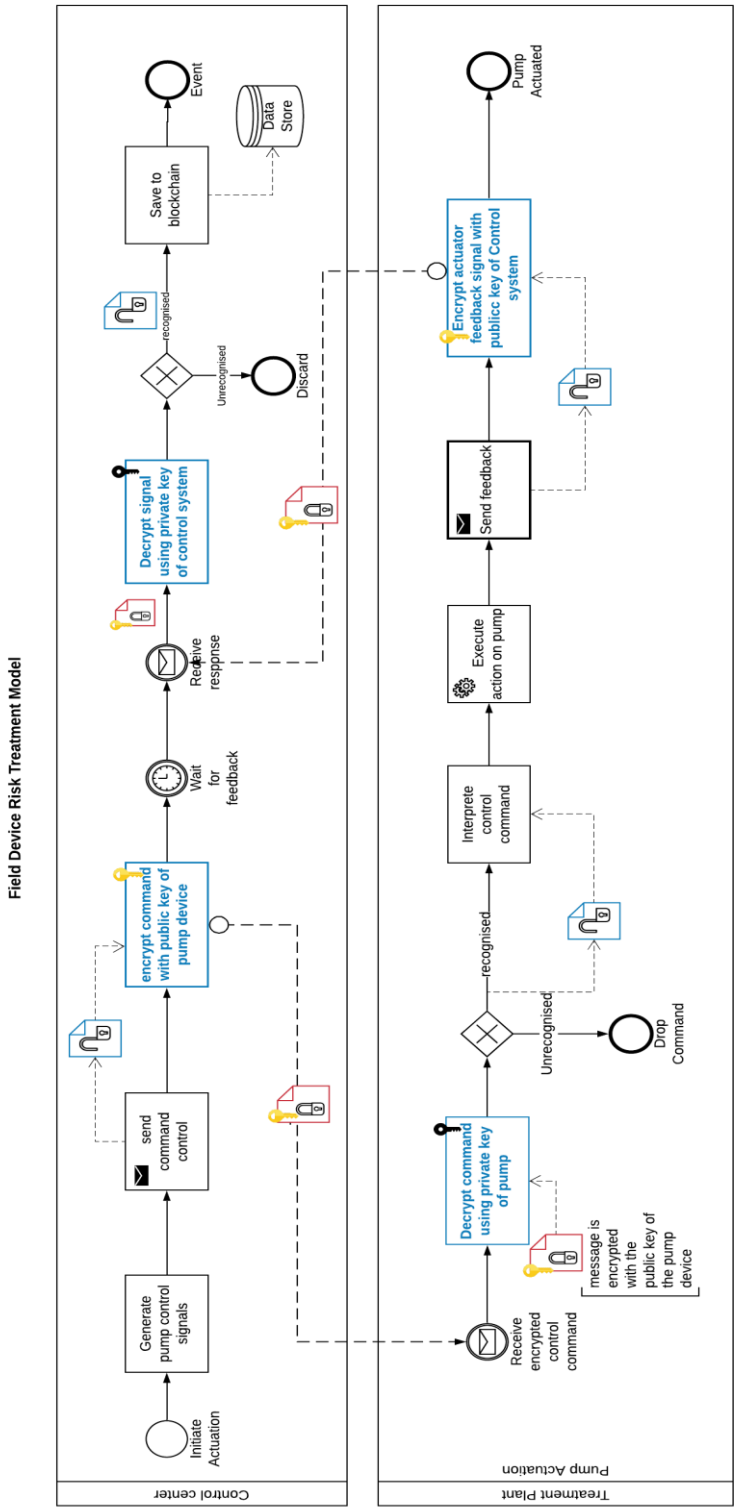

Figure 10: Field device risk treatment model

6.1.2. Risk Treatment for Smart Device

Smart water meter is a CPS asset identified in the water supply system network architecture. To carry out risk security control on this device, we came up with a scenario that involves a smart water meter. The scenario presented a situation where the smart water meter was compromised

Scenario 2

Asset: Smart device and user data

Risk: Exposing user information to unauthorized parties

Vulnerability detected: Lack of network security at the edge.

Security Requirement: Secure access to the network

Blockchain security control: blockchain-based access control based on public-key encryption.

Model Description

To implement the blockchain security control, the model BPMN diagram has been developed in Figure 11.

Normal Operation: The smart water meter communicates with the utility service control system occasionally, based on the design of most smart meters, they periodically make contact with the control server to consistently sync their data. In normal working conditions, this communication should be seamless, provided the meter is not compromised nor is the data that is sent or received interrupted.

Attack Condition: In this scenario, the hacker maliciously gained access to the smart meter and obtain the smart device user's personal information. The attacker will intercept the communication line between the device and the control system such that, a

Blockchain-based security control: The smart contract periodically sends and receives data to and from the utility service company. To prevent unauthorized access to the device the blockchain public key infrastructure is employed and to further protect the personal information of the sender, a smart contract is included in the security control to provide

both encryption/decryption purposes and verifying the authenticity of the message sender. When the smart device sends data, the smart contract is automatically executed to check the identity of the sender, if the sender is the legal owner, the message is then encrypted using the destination public key to prevent the message from being intercepted while in transit. The encrypted message is then first received by the service provider server, which is then decrypted before the message is used. The reverse process applies when the service server sends a return message to the smart device. To ensure the message is only accessible to the right owner it is encrypted with the smart device's public key and the smart contract executes on receiving a message to decrypt and check the sender before it is read. In any case, if the message does not conform to the policies in the contract, the message will be discarded.

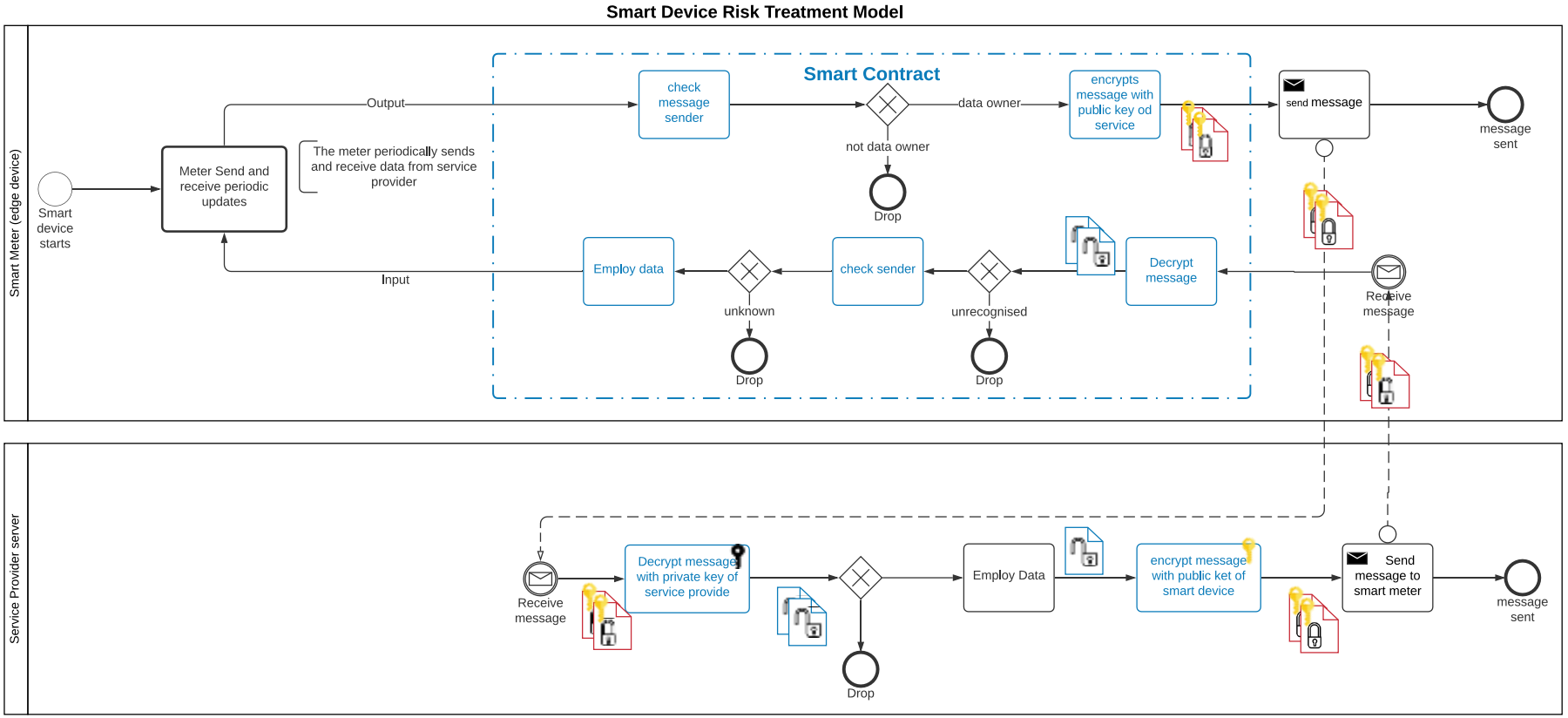

Figure 11: Smart device treatment model

6.1.3. Risk Treatment for Computing Device

The computing device in the water supply CPS architecture includes laptops, desktops, and other similar devices. To carry out risk security control on this device, we came up with a scenario that involves a computing device being illegally accessed. The scenario presented a situation where the computing device is compromised.

Scenario 3

Asset: Computing device and user information

Risk: Unverified user access

Vulnerability detected: Absence of multi-factor authentication

Security Requirement: Provide verifiable authentication system for user log in

Blockchain security control: Apply blockchain decentralized digital identity to for logging into enterprise computers.

Model Description

To implement the blockchain security control, the model BPMN diagram has been developed in Figure 12.

Normal Operation: Current employee logs into their respective computer with basic credentials- usernames and passwords. In an ideal situation is good, but it is not enough,

Attack Condition: An attacker got the login credentials of another user, the attacker could steal files, delete files, or perform other harmful activities. The attacker can get the file through various means even without the owner being aware.

Blockchain-based security control: Blockchain provides several security techniques to ensure only authorized and authenticated users get access to critical information. In this scenario, blockchain digital identity or decentralized identifier (DID) which allows for verifiable digital identities. The DIDs are links to some document which contains a set of public keys related to the user, timestamp, signature, set of service endpoints, and authentication method. All these enable verifiable-login and prevent unauthorized access to the system. In the model in figure 12, the employee provides the login credentials, then

as a second level authentication, the user is linked to the DID document to provide specific information before access is granted. A fraudulent user will not be able to provide the right set of information for login to the computer com.

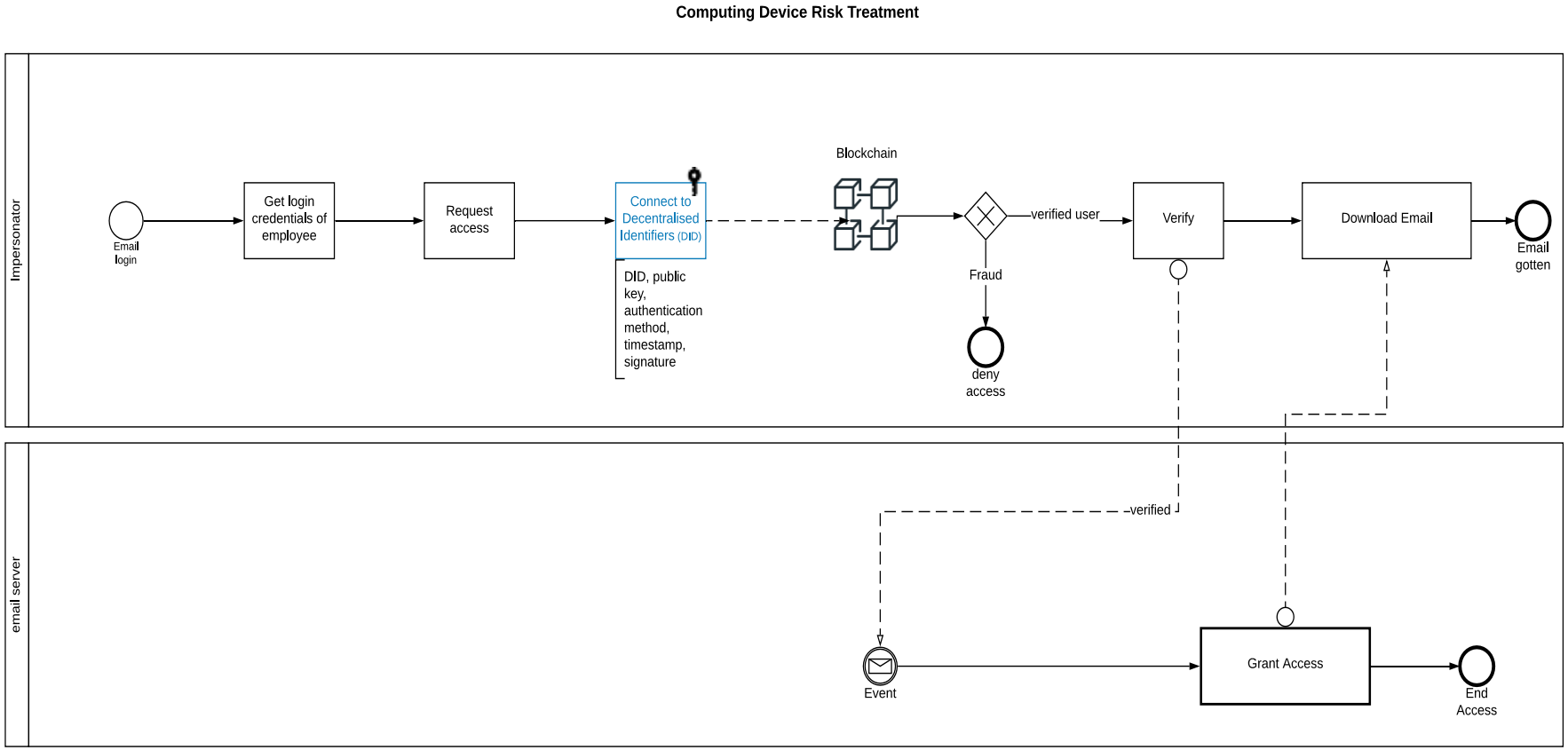

Figure 12: Computing device risk treatment

6.1.4. Risk Treatment for Communication and Network

The communication lines and networks are a very important CPS aspect of the water supply system. To carry out risk security control on this device, we came up with a scenario that involves a network-related attack. The scenario presented a situation where the network is compromised.

Scenario 2

Asset: Systems network

Risk: Loss of business-critical information and files

Vulnerability detected: lack of authorization and authentication

Security Requirement: Improve network security strategy

Blockchain security control: Decentralized blockchain network to monitor and control activities at the nodes.

Model Description

To implement the blockchain security control, the model BPMN diagram has been developed in Figure 13.

Normal Operation: Network is functioning properly as the interconnectivity of CPS devices is unhindered by any activities.

Attack Condition: In the event where the network is lacking strict rules for authentication and authorization as captured in the vulnerability of the scenario, an attacker will be able to penetrate the network and carry out malicious activities. In the event where the malware is introduced to one point of the network, there is a high tendency it could spread to other parts of the network.

Blockchain-based security control: To mitigate such challenge, blockchain can be employed to provide security, in the network. A decentralized CPS for water management based on blockchain is not susceptible to this type of attack since the system is not centralized. The network can choose to ignore data coming from a specific node if it is determined that the node is compromised, and it is transmitting incorrect information.

With distributed blockchain consensus, only correct data can be processed by the network. The model describes how the blockchain detects and isolates faulty and infected nodes and rather than affecting the network, the node is isolated.

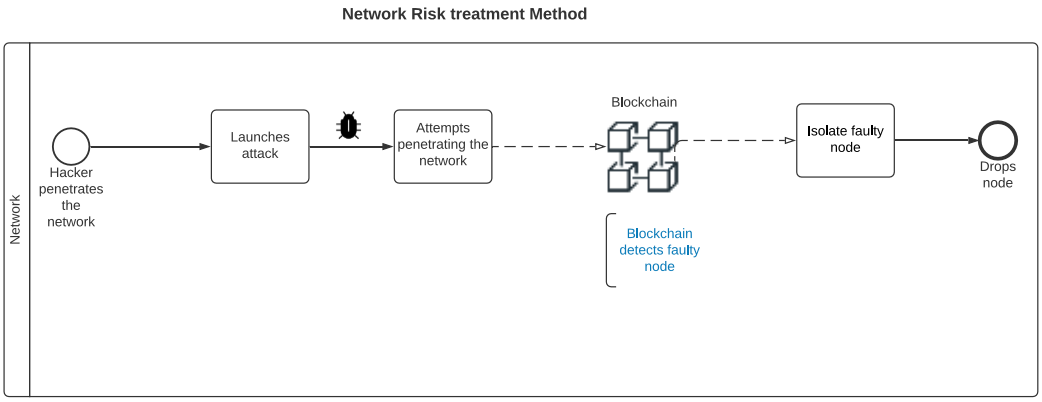

Figure 13: Blockchain risk security control on faulty nodes in the network

6.1.5. Risk Treatment Operators and User

In a CPS environment, people are considered assets because they interact with theses CPS components. People can influence both the physical and the computing capabilities of the CPS devices. To carry out risk security control in this case where an attack can occur as a result of human activities, we came up with a scenario that involves an operator of the SCADA system erroneously made changes in the system.

Scenario 5

Asset: User

Risk: Firewall and defense breakdown

Vulnerability detected: Insufficient security training

Security Requirement: Access network and improve failure isolation system

Blockchain security control: Decentralized blockchain network to monitor and control activities at the nodes

Model Description

To implement the blockchain security control, the model BPMN diagram has been developed in Figure 14.

Normal Operation: In a normal condition, the configuration of the SCADA system is done only by skilled operators to prevent causing damage to the entire network system and the control system

Attack Condition: In the instance where an operator without knowledge tries to configure the system and ends up exposing the system, an attacker can take advantage of the loopholes created and penetrate the system. And once the attacker penetrates the system,

Blockchain-based security control: Blockchain provides consensus mechanisms that make it easier to detect faulty nodes for them not to have any significant impact on the entire network. For the situation in this scenario, this kind of failure can be eliminated with blockchain implementation on water CPS. The entire systems within the network store and share similar information. Whenever there is a new update to the network, all the nodes in the network must agree (create consensus) to the fact that the information is valid and not malicious before it is added, else it will not be added. The illustration of the model in Figure 14, simplifies the activity of forming consensus before the configuration from a node is added to the chain of configurations (transaction) if the configurations are wrong and do not agree with the one already in the other nodes, such configuration will be rejected.

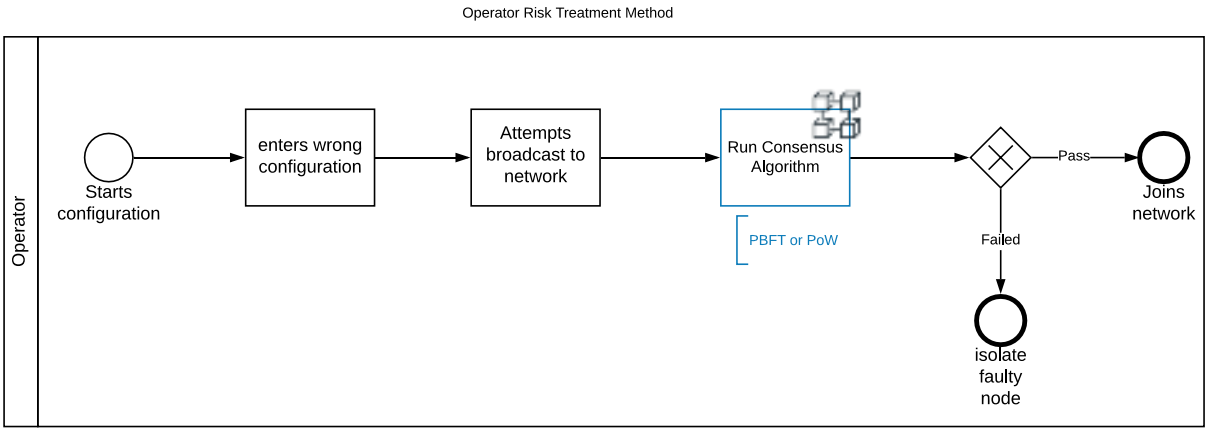

Figure 14: Blockchain risk security control on operator activities

6.1.6. Risk Treatment for SCADA systems

The scenario presented a situation where the computing device is compromised.

Scenario 6

Asset: SCADA system

Risk: Loss of communication and control pump capabilities

Vulnerability detected: Poor contract monitoring system for employees

Security Requirement: Control authorized remote access

Blockchain security control: Implement blockchain smart contracts with policies for contract duration management.

Model Description

To implement the blockchain security control, the model BPMN diagram has been developed in Figure 15.

Normal Operation: The system allows remote access into the SCADA system and contractors can access the same and make necessary configurations. Contractors' accesses are manually disabled at the expiration of their contracts. But this may not be efficient since it is a manual activity

Attack Condition: A former contractor whose accesses to remote sign-in has not been revoked after the expiration of the contract, enters login credentials and enters the system. This individual is capable of manipulating the activities at the entire plant.

Blockchain-based security control: To mitigate such occurrence, blockchain's smart contract protocol can be employed to check for such actions. A smart contract is a computer program that is capable of executing agreement terms with runs on the blockchain with the influence of a third party. A smart contract will be written that check certain information of people and applied to function at the point of remote login.

The proposed model blow presents the process flow when blockchain and smart contract is adopted into the system. The contractor requests to log in provide his login credentials, the login credential is taken and checked against the

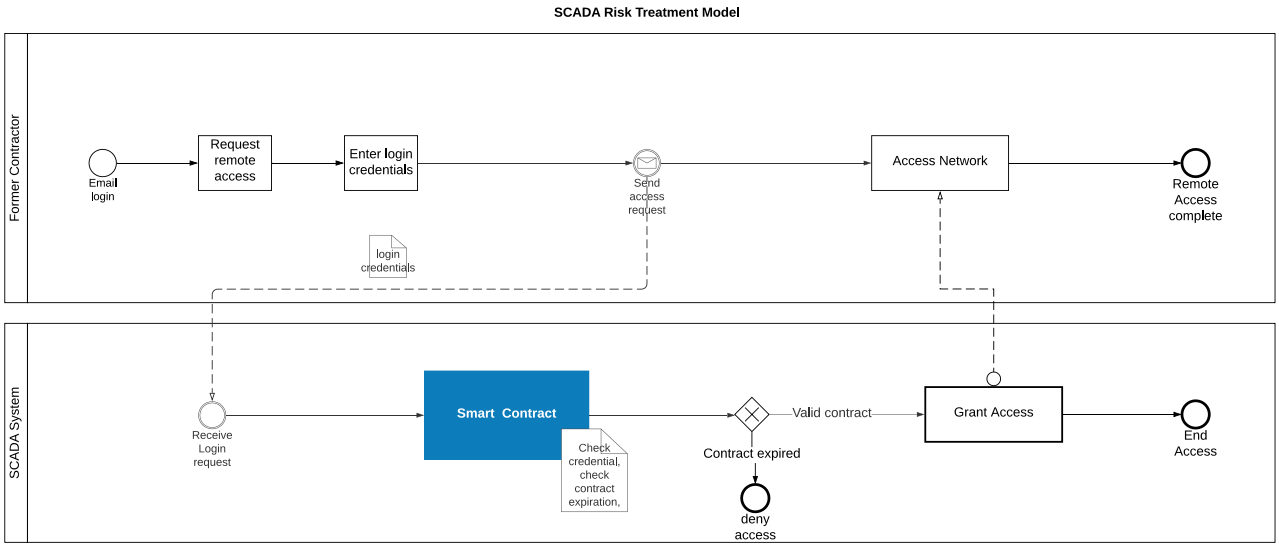

Figure 15: Blockchain risk security control on the SCADA system

6.2. Evaluation

This Section closes the evaluation statement in design-science research main concept for artifacts which is to build and then evaluate [11]. This section discusses the evaluation procedure by expert analysis for the thesis work. The section discusses the expert backgrounds, a description of the evaluation procedure, and the feedbacks of the various experts based on the questions presented.

6.2.1. Expert Background

Experts were selected based on their experience with the concept of risk management, information security, and blockchain technologies. Due to the experts' experience and familiarity with the concepts of this thesis, it was expected that valuable responses will be given. A total of three (3) were interviewed for the evaluation of the research. The experts were cybersecurity experts (2) and blockchain technology expert (1) backgrounds.

The experience of the professionals are as follows;

Expert 1: Management information lead, 8+ years in cybersecurity and system engineering, specializes in digital forensics

Expert 2: Vulnerability Management Team Lead, 4.5 years cybersecurity management, Ph.D. candidate – Security risk management on IoT systems.

Expert 3: Software engineer, 6+ years of experience in software development, Ph.D. candidate, and Junior research scientist at the University of Tartu. Research area in Information security, the security of blockchain-based applications and security engineering

6.2.2. Description of Evaluation Process

The participants were contacted via phone calls to participate in the evaluation of the research work, explaining the thesis goal and the methodologies and procedures. Interviews were conducted by different means for each of the experts. Interview with expert 1 was conducted via phone conversation and with the permission of the expert, the call was recorded. Expert 2, the interview was carried out via skype meeting which

allowed for a detailed conversation and elaborate feedback. Expert 3, questions, were sent via email, and the response was gotten accordingly.

The interviews were directed at Chapters 3, 4, 5, and Section 6.1 to access its structure and comprehensibility. The following questions were presented:

For security experts:

- Do you agree with the assets, vulnerability, and threats identified?
- Do you agree with the models for the security controls? Are the proposed models clear and easy to understand?
- How does the security control models address the risks identified in water CPS?
- Do you agree with the relevance and usefulness of the proposed solution?

Specifically, to the blockchain expert, the following questions were presented

- What is the feasibility of implementing blockchain on CPS?
- What is the cost implication of implementing blockchain on water CPS?
- What is the availability of blockchain technology for such implementations?

Notes were taken during the interview, concerning recommendations, suggestions, and personal opinions. Changes were made to the areas that were necessary and found to be inconsistent. The need for the changes was to accommodate the experts' views to ensure accuracy.

6.2.3. Results of Evaluation Procedure

This section contains the expert evaluation on each area of interest covered in this thesis from the asset-related concepts to the blockchain security control and then to the models proposed.

Evaluation of assets, vulnerabilities, and threats

The concept relating to asset identification in Chapter 3 and about the threats and vulnerabilities in the scenarios highlighted in chapter 4. The questions were asked, and the respondent agreed that though CPS assets in the water sector were not familiar to

them, agreed with the assets concerning the thesis goal as only system assets were of interest. Expert 2 stating *that "proper format for the asset identification should present both business and system assets"* but later agreed when it was explained that the scope of the thesis was CPS only toward CPS related assets, Expert 3 made a similar observation. In the area of the threats, all three experts agreed on validating the method of identifying threats presented in the thesis. Expert 1 insisted affirmed that "*that the threat agents were properly categorized*". The concept of stating vulnerabilities was for the various scenarios was corrected for some of the cases. Expert 2 expressed that "*the vulnerability statement should be elaborate enough to give the reader good insights but not ambiguous*" Expert 3 suggested changes to some vulnerabilities specific vulnerabilities be considered separate and the changes were affected immediately.

Evaluation of proposed model

The proposed models were considered one after the order by the experts, it was agreed by expert 1 and 2 to be correct according to the BPMN concepts. Although Expert 2 said, "*some of the symbols included were not standard BPMN symbols but for explanatory purposes, they can be acceptable*". It was agreed that the proposed models are clear and easy to understand. Some inconsistencies noted and made obviously, the changes were implemented immediately and were validated. The risk controls revealed in the models validated with scenarios 1,2,3 getting the approval of all the experts. Expert 1 said, "*an explanation would have been needed to understand the models 4 and 5 had it not been changed*".

Evaluation of risk mitigation with the proposed model

Evaluating the risk mitigation, it was agreed that blockchain provides high-level security, it was agreed by the experts that the security controls address the risks identified in the various scenarios. Expert 1 said "*blockchain is quite promising when it comes to security, integrity, and privacy. And those are the factors highlighted in the various scenarios presented".* Expert 3 proposed that the blockchain platform used should be indicated in the models citing the example where a smart contract was employed.

Evaluation of the relevance and usefulness of the solution

Expert 2 was conservative with the affirmation stating that *"model representation of the risk treatment for the specified risks have potentials to addressing the specified risks. However, since this is not an actual implementation, evaluation of its usefulness has to be based on the security requirements and controls formed from the analyzed risks. Controls seem effective to remediate the security risks*". Expert 1 was however affirmative about the relevance stating that "from *the surface point of view, the solution will be useful, but the actual implementation may reveal a different fact, but I agree it is relevant*".

Blockchain specific evaluation

Specific questions about the practical applicability of the model were directed to Expert 3, the blockchain expert. About the feasibility of implementing blockchain om water CPS, it was evaluated as very feasible, citing other domains containing more heterogeneous CPS components as proof that the implementation of water CPS is feasible. Expert 3 presented a question stating that "*what security platform is being spoken of in the thesis*" but was made to understand the thesis does not particularly consider a specific platform but taking the technology as a whole. On the cost implication of implementing blockchain, Expert 3 could not give a specific cost implication but said *"blockchain implementation could be normally cost-intensive*". Expert 2 also commented about the difficulty of implementation stating that "*There are costs associated with implementing public-key encryption on blockchain. However, the depths of these costs are unknown to me*". Concerning the availability, it was agreed that a lot of things are believed to be possible with blockchain but are yet to be implemented in practice.

General conclusion

In conclusion, the interviewers made suggestions and recommendations some of which have been affected by the thesis. Overall, it was agreed by all the experts that the models produced in this thesis are valid. The general result of the interview shows the security control model is useful in preventing the risks. Lastly, It was agreed that the costs aspect of the implementation of public-key encryption for CPS components could limit the feasibility of the proposed model.

6.3. Blockchain Technology Stack for Implementing Digital Identity Management and Access Control on Assets

In this section, we shall be performing a paper-based feasibility evaluation by considering existing and planned blockchain-technology based projects that employ the blockchain concepts considered in the development of the artifact in this thesis. Section 6.3.1

6.3.1. Digital Identity Management

Identity management has been a long persistent field and blockchain has enhanced its spread as more efficient solutions and projects by the day. To further evaluate the proposal in the model, the following projects contribute to the feasibility evaluation for this thesis.

A. uPort

Uport is a safe, user-friendly, self-sovereign identity that is built on Ethereum blockchain. According to the Uport whitepaper [55], Uport allows uses to own and control their identities, assets, reputation, and access digital services without using passwords, sign documents digitally, and many other things. Using the blockchain digital identity security control.

B. Sovrin

Like Uport is a blockchain-based digital identification solution it builds a user identity overtime. The sovrin whitepaper [56], describes extensively how user reputation is built with usage, sovrin is an extensive digital identification solution that leverages on the blockchain self-sovereign identity.

Other digital identity management solutions include: ShoCard [57], BitID[58] and IdchainZ [59]

C. MedRec - an electronic health record (EHR)

MedRec is a novel, decentralized record management system to handle EHRs, using blockchain technology [52]. As patients go to different hospitals for treatment, their health records are scattered across different data silos. This results in the patient losing easy access to past health records. Also, data sharing between hospitals might be a problem due to interoperability challenges. MedRec

addresses the issues highlighted above: fragmented health records, loss of easy access to health records, and interoperability challenges. MedRec also provides the means for responsible access to more medical records for research purposes.

MedRec leverages the concept of smart contracts on the Ethereum blockchain to log patient-provider relationships that associate a medical record with viewing permissions and data retrieval instructions for execution on external databases[52].

6.3.2. Access control on Assets

Access control systems' purpose is to regulate the access to valuable resources according to specific security and privacy requirements. Blockchain offers options for access control.

A. Blockchain-Based Access Control Service [60]

Presents access control service built on blockchain, exploits policy language of Ethereum, uses an attribute-based access control model.

With blockchain-based access control, owners and users accessing a resource can verify how policies have been evaluated for each access. Users can browse the blockchain to control their access requests.

B. Recording electricity usage using the blockchain platform

The project discussed below shows how electricity usage by IoT devices can be recorded using Ethereum[54]. A smartphone and three Raspberry Pi's are used to implement the prototype. The three Raspberry Pi's are treated as meters to keep track of electricity usage. The smartphone is used to set some policies, for example, to turn on energy-saving mode when electricity usage reaches a certain threshold, say 150 KW. The data is sent to the Ethereum network. Meanwhile, a device such as a lightbulb is retrieving values of the policy periodically from Ethereum. The meter tracks electricity usage and sends the updates to Ethereum.

Other projects on access control include BlendCAC [61], SCARAB [62]

6.4. Conclusion

In this chapter, we have proposed blockchain-based risk security controls and developed several control models for six (6) random risks using BPMN annotations. Explanations of each model and the scenario they address were addressed in this chapter. In Section 6.2, the models proposed have also been evaluated by experts and the documentation of the evaluation results that follow the expert evaluation based on the questions presented has been reported. Section 6.3 provided feasibility evaluation that considered existing and planned blockchain-technology projects that employed the technologies considered in this thesis.

7. Conclusion

This chapter presents a summary of the research carried out in this thesis work. Section 7.1 presents the general conclusions; Section 7.2 provides the answers to all research questions for this work. Finally, Section 7.3 presents the research ideas and areas for future work.

7.1. General conclusion

In this thesis security issues that affect cyber-physical systems in the water-supply systems are analyzed using the water supply sector as a case study. The water supply system presents a good example point for the cyber-physical system.

The result performed in this thesis is a security risk control for mitigating the cyber-attack risks in water CPS. The security requirement and controls mitigate the risks identified, evaluations performed shows the risk will be mitigated significantly or even eliminated.

The Blockchain features used in security risk control are Public key infrastructure, Digital Identity management, and Smart contracts.

7.2. Answer to research Question

The answers to the research questions in this thesis have been provided as follows:

How to enhance trusted communication among CPS entities in water-supply system architecture

To answer the main question, it is further divided into the following hierarchy of sub-questions:

7.2.1. RQ-1: How to identify relevant information exchanges between CPS nodes in WSS?

The relevant information exchanges between the CPS nodes were identified in WSS were identified by describing and modeling typical water supply system CPS bodes information communication flow. A BPMN model was used to describe the entire communication flow and was presented. The water supply system consists of several CPS

components at the different stages of the water supply system. The WSS CPS communication workflow includes the treatment plant, control center, distribution network, customer management, and the consumer site.

RQ1.1: What are the relevant entities involved in data transmission and communication?

The relevant entities involved in data transmission in water supply data transmission flow can also be described as assets, which can be described as Information System assets. These entities help in the exchange of signals and data within the systems.

The assets were identified and later categorized as follows: field devices, computing devices, smart devices, SCADA application software, communication and network, and people.

RQ1.2. What information is exchanged?

The identified assets exchange various kinds of information among themselves depending on the function of the location in the network of the asset. The information exchanged between the assets are as follows:

Field devices: The actuator devices exchanges response acknowledgments for actuation commands from the control system, the sensor devices exchange physical measurement values in terms of signals for calibration values from the control.

Computing devices: emails, configuration, customer data, web data

Smart Devices: exchanges measurement values, software updates

People: email, configuration commands, critical business information

SCADA software: control signals and configuration values.

7.2.2. RQ-2: How to identify the security threats that exist in information exchange?

The threats that exist in the information exchange were gotten by conducting a risk assessment on the various CPS assets based on scenarios that were created. The various risk and analysis table in Section 4 identified some of the threats that exist in water CPS information exchange.

RQ2.1: What are the threat agents?

With water CPS being a critical infrastructure, many threat agents could be identified, the security threat agents for CPS infrastructures were therefore classified based on their motivations and level of the adversary. The threat agents identified were hackers, thieves, competitors, and organized criminals, terrorists, and nation-states.

RQ2.2: What are the vulnerabilities within the system?

The complexity of the entire system makes it vulnerable the different points due to different reasons. Two failure scenarios were then created for each asset and various vulnerabilities were detected depending on the type of failure that occurred. This was covered in Section 4.2

RQ2.3: What are the risk impacts?

The risk impacts were identified based on the vulnerabilities detected and the kind of threat identified. Conducting the risk analysis in Section 4.2 provided several risk impacts depending on the scenario.

7.2.3. RQ-3 How to use blockchain technology to mitigate the trust issues that affect the CPS infrastructure?

To use blockchain technology to mitigate risk, it started with identifying the security requirements a risk requires, then the appropriate blockchain quality that mitigates the risk is considered. Then the security protocol is implemented as a security control means.

RQ3.1. What are the blockchain qualities that enable security?

The blockchain qualities that enable security are the decentralized public key infrastructure (PKI), consensus mechanism, digital identity, and decentralized nodes.

RQ3.2. What are the security requirements in the water-supply system CPS architecture?

The security requirements which are the criteria that to be attained or met before the security standards are met. Section 5security requirements for the various scenarios which varied considerably based on the scenario's failure.

RQ3.3. What are the blockchain security controls that implement the security requirements?

Different security controls were implemented in Chapter 5 that applied to the failure and the threats identified. Several blockchain security controls were considered such as PKI in situations where the authenticity of data is required, decentralized digital identity, and smart contracts.

7.3. Future Works

In the course of this master's thesis, some issues were identified as a proposal for future work. These issues will be introduced and background to provide future academic work shall be reopened

This research work was not implemented and on real-life, CPS device, or neither was the security control measures simulated. A useful area for future research will be to simulate the security control models proposed in this research work and if possible build a physical prototype implementing the scenarios highlighted.

Also, this thesis work was limited to the water sector, another future academic work could cover the risk analysis of the cyber-physical systems architecture of other sectors such as agriculture and implementing blockchain for security control.

References

[1] A. Hassanzadeh *et al.*, "A review of cybersecurity incidents in the water sector," *Journal of Environmental Engineering*, vol. 146, no. 5, p. 03120003, 2020.

[2] H. Rathore, A. Mohamed, and M. Guizani, "A Survey of Blockchain Enabled Cyber-Physical Systems," *Sensors*, vol. 20, no. 1, p. 282, 2020.

[3] F. Buccafurri, G. Lax, A. Russo, and G. Zunino, "Integrating digital identity and blockchain," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, 2018, pp. 568–585.

[4] W. Leea, T. Chen, W. Sun, and K. I.- Ho, "An S/Key-like One-Time Password Authentication Scheme Using Smart Cards for Smart Meter," in *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, 2014, pp. 281–286.

[5] P. Franchin and F. Cavalieri, "Seismic vulnerability analysis of a complex interconnected civil infrastructure," in *Handbook of seismic risk analysis and management of civil infrastructure systems*, Elsevier, 2013, pp. 465–514e.

[6] F. Hu *et al.*, "Robust cyber–physical systems: Concept, models, and implementation," *Future generation computer systems*, vol. 56, pp. 449–475, 2016.

[7] WhiteHouse, "Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure," 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure.

[8] S. Adepu, V. R. Palleti, G. Mishra, and A. Mathur, "Investigation of cyber attacks on a water distribution system," *arXiv preprint arXiv:1906.02279*, 2019.

[9] T. Sanislav, L. Miclea, and P. Prinetto, "Improving the Dependability of a Water Supply System via a Multi-Agent based CPS," *Proceedings of EWDTS*, pp. 425–431, 2012.

[10] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Design automation conference*, 2010, pp. 731–736.

[11] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[12] P. J. Denning, "A new social contract for research," *Communications of the ACM*, vol. 40, no. 2, pp. 132–134, 1997.

[13] D. Tsichritzis, "The Dynamics of Innovation," in *Beyond Calculation*, Springer New York, 1997, pp. 259–265.

[14] A. P. N. Automation, "TURNKEY AUTOMATION FOR WATER & WASTE WATER TREATMENT." http://www.gnbwebserver.godrej.com/apnaautomation/WaterTreatment.html.

[15] J. Venable, J. Pries-Heje, and R. Baskerville, "FEDS: a framework for evaluation in design science research," *European journal of information systems*, vol. 25, no. 1, pp. 77–89, 2016.

[16] N. Ahmed and R. Matulevičius, "Securing business processes using security risk-oriented patterns," *Computer Standards & Interfaces*, vol. 36, no. 4, pp. 723–733, 2014.

[17] C. Turcu, C. Turcu, and V. Gaitan, “An internet of things oriented approach for water utility monitoring and control,” *arXiv preprint arXiv:1811.12807*, 2018.
[18] N. Vakilifard, M. Anda, P. A. Bahri, and G. Ho, “The role of water-energy nexus in optimising water supply systems–Review of techniques and approaches,” *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 1424–1432, 2018.
[19] S. Byeon, G. Choi, S. Maeng, and P. Gourbesville, “Sustainable water distribution strategy with smart water grid,” *Sustainability*, vol. 7, no. 4, pp. 4240–4259, 2015.
[20] Z. Wang *et al.*, “Cyber-physical systems for water sustainability: challenges and opportunities,” *IEEE Communications Magazine*, vol. 53, no. 5, pp. 216–222, 2015.
[21] S. Nakamoto, “Bitcoin whitepaper,” *URL: https://bitcoin. org/bitcoin. pdf-(Дата обращения: 17.07. 2019)*, 2008.
[22] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, “A trust architecture for blockchain in IoT,” in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2019, pp. 190–199.
[23] “Information technology - Security techniques - Information security risk management. International Organization for Standardization (LEFM) approach,” International Organization for Standardization, Geneva, CH, Standard, 2008.
[24] C. J. Alberts and A. J. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional, 2003.
[25] T. Yaqoob, H. Abbas, and N. Shafqat, “Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices,” *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 6, pp. 1752–1761, Jun. 2020, doi: 10.1109/JBHI.2019.2952906.
[26] H. I. Kure, S. Islam, and M. A. Razzaque, “An integrated cyber security risk management approach for a cyber-physical system,” *Applied Sciences*, vol. 8, no. 6, p. 898, 2018.
[27] N. Mayer, “Model-based management of information system security risk,” PhD Thesis, 2009.
[28] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, “An integrated conceptual model for information system security risk management supported by enterprise architecture management,” *Software & Systems Modeling*, vol. 18, no. 3, pp. 2285–2312, 2019.
[29] A. S. Sani *et al.*, “CyRA: A Real-Time Risk-Based Security Assessment Framework for Cyber Attacks Prevention in Industrial Control Systems,” in *2019 IEEE Power Energy Society General Meeting (PESGM)*, Aug. 2019, pp. 1–5, doi: 10.1109/PESGM40551.2019.8973948.
[30] D. B. Paneria and B. V. Bhatt, “Modernization in water distribution system,” 2017.
[31] M. J. Mudumbe and A. M. Abu-Mahfouz, “Smart water meter system for user-centric consumption measurement,” in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, 2015, pp. 993–998.
[32] C.-Y. Lin, S. Zeadally, T.-S. Chen, and C.-Y. Chang, “Enabling cyber physical systems with wireless sensor networking technologies,” *International Journal of Distributed Sensor Networks*, vol. 8, no. 5, p. 489794, 2012.
[33] N. Jabeur, N. Sahli, and S. Zeadally, “Enabling cyber physical systems with wireless sensor networking technologies, multiagent system paradigm, and natural ecosystems,” *Mobile Information Systems*, vol. 2015, 2015.

[34] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, “Cyber-physical system risk assessment,” in *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2013, pp. 442–447.
[35] A. Koubâa and B. Andersson, “A vision of cyber-physical internet,” 2009.
[36] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, “Cyber-physical systems and their security issues,” *Computers in Industry*, vol. 100, pp. 212–223, 2018.
[37] M. Aydar, S. C. Cetin, S. Ayvaz, and B. Aygun, “Private key encryption and recovery in blockchain,” *arXiv preprint arXiv:1907.04156*, 2019.
[38] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, “Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities,” *IEEE Access*, vol. 7, pp. 85727–85745, 2019.
[39] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme, “Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency,” in *The Economics of Information Security and Privacy*, Springer Berlin Heidelberg, 2013, pp. 135–156.
[40] P. Gaži, A. Kiayias, and A. Russell, “Stake-Bleeding Attacks on Proof-of-Stake Blockchains,” in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, pp. 85–92.
[41] M. Jakobsson and A. Juels, “Proofs of work and bread pudding protocols,” in *Secure information networks*, Springer, 1999, pp. 258–272.
[42] Q. He, N. Guan, M. Lv, and W. Yi, “On the consensus mechanisms of blockchain/dlt for internet of things,” in *2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES)*, 2018, pp. 1–10.
[43] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery,” *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002, doi: 10.1145/571637.571640.
[44] Y. Liu *et al.*, “Blockchain-based identity management systems: A review,” *Journal of Network and Computer Applications*, p. 102731, 2020.
[45] B. Alotaibi, “Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review,” *IEEE Sensors Journal*, vol. 19, no. 23, pp. 10953–10971, 2019.
[46] S. Wang, Y. Zhang, and Y. Zhang, “A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems,” *IEEE Access*, vol. 6, pp. 38437–38450, 2018.
[47] E. Kfoury and D. Khoury, “Distributed Public Key Infrastructure and PSK Exchange Based on Blockchain Technology,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1116–1120.
[48] G. Wolfond, “A blockchain ecosystem for digital identity: improving service delivery in Canada’s public and private sectors,” *Technology Innovation Management Review*, vol. 7, no. 10, 2017.
[49] S. Kim, “Blockchain for a trust network among intelligent vehicles,” in *Advances in Computers*, vol. 111, Elsevier, 2018, pp. 43–68.
[50] J. P. Cruz, Y. Kaji, and N. Yanai, “RBAC-SC: Role-Based Access Control Using Smart Contract,” *IEEE Access*, vol. 6, pp. 12240–12251, 2018.
[51] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[52] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” in *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[53] Bitnation, “Bitnation Pangea,” *Bitnation Pangea*. https://tse.bitnation.co/ (accessed Aug. 05, 2020).

[54] S. Huh, S. Cho, and S. Kim, “Managing IoT devices using blockchain platform,” in *2017 19th international conference on advanced communication technology (ICACT)*, 2017, pp. 464–467.

[55] Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., & Sena, M. (2017). Uport: A platform for self-sovereign identity. URL: https://whitepaper. uport. me/uPort_ whitepaper_DRAFT20170221. pdf.

[56] Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. The Sovrin Foundation, 29(2016).

[57] El Haddouti, Samia, and Mohamed Dâfir Ech-Cherif El Kettani. "Analysis of Identity Management Systems Using Blockchain Technology." CommNet. 2019.

[58] Zhang, Tengxiang, et al. "BitID: Easily add battery-free wireless sensors to everyday objects." 2017 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, 2017.

[59] van Bokkem, Dirk, et al. "Self-sovereign identity solutions: The necessity of blockchain technology." arXiv preprint arXiv:1904.12816 (2019).

[60] D. Di Francesco Maesa, P. Mori and L. Ricci, "Blockchain Based Access Control Services," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1379-1386, doi: 10.1109/Cybermatics_2018.2018.00237.

[61] Xu, Ronghua, et al. "Blendcac: A blockchain-enabled decentralized capability-based access control for iots." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.

[62] Kokoris-Kogias, Eleftherios, et al. "Hidden in Plain Sight: Storing and Managing Secrets on a Public Ledger." IACR Cryptol. ePrint Arch. 2018 (2018): 20