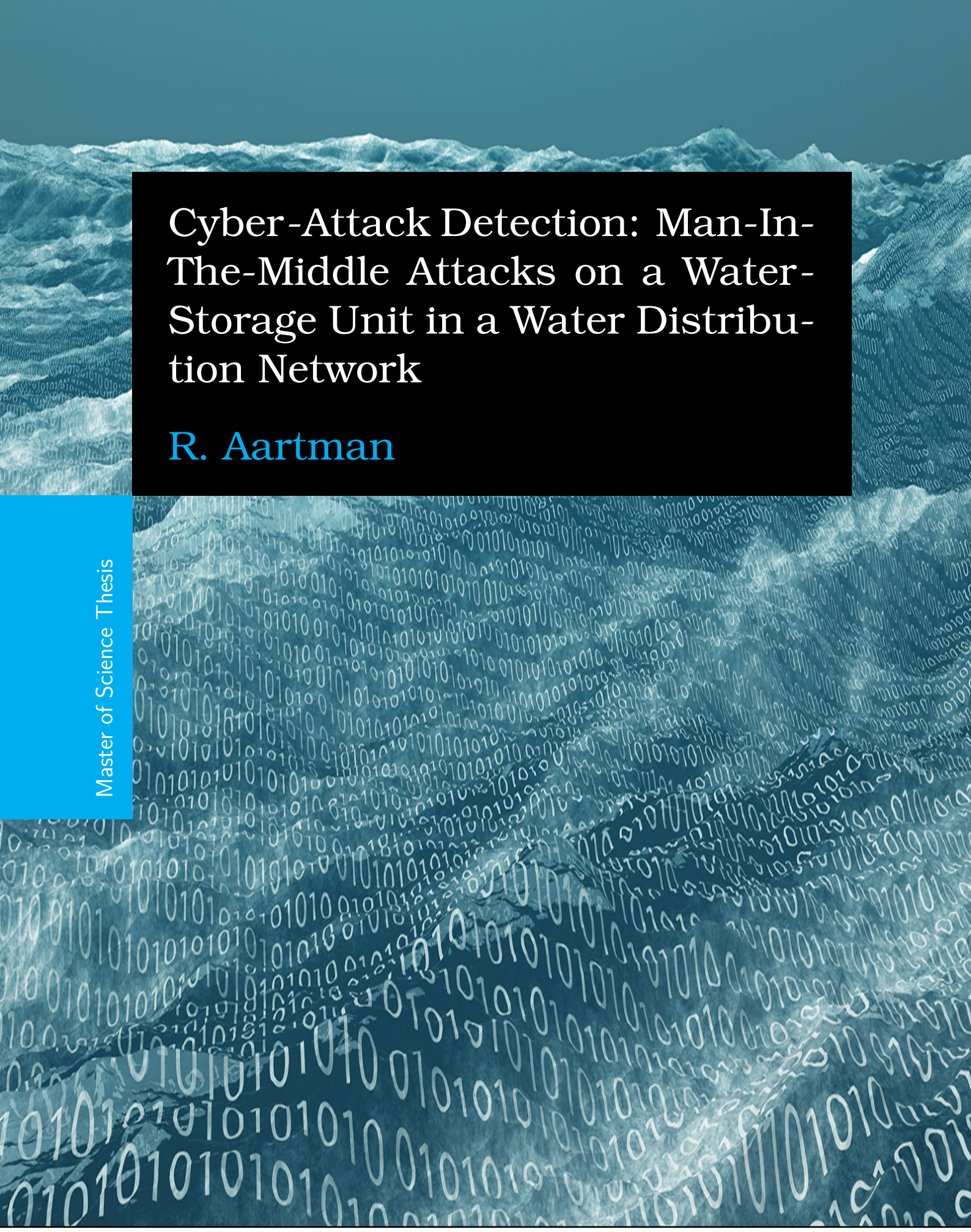


Cyber-Attack Detection: Man-In-The-Middle Attacks on a Water-Storage Unit in a Water Distribution Network

R. Aartman

Master of Science Thesis

TU Delft Delft University of Technology

Delft Center for Systems and Control

Cyber-Attack Detection: Man-In-The-Middle Attacks on a Water-Storage Unit in a Water Distribution Network

Master of Science Thesis

For the degree of Master of Science in Systems and Control at Delft University of Technology

R. Aartman

September 3, 2024

Faculty of Mechanical Engineering (ME) · Delft University of Technology

The work in this thesis was supported by Batenburg Magion. Their cooperation is hereby gratefully acknowledged.

Abstract

To detect cyber-physical attacks targeted at a water storage unit part of the Water Distribution Network (WDN), this thesis investigates the use of process data provided by Dunea, a Dutch drinking water production company, for this purpose.

In order to achieve this, a model-based anomaly detection method is employed. This consists of deriving an accurate model that represents the nominal dynamics of the system, computing the residual between the estimation and the measurement and evaluating the residual using the Non-Parametric Cumulative Sum (NP-CUSUM). Additionally, cyber-physical attacks are designed to expose the water storage unit, during its draining and replenishing, to the most extreme attacks that could potentially impact the WDN.

Results show that all designed attacks initiated during the reservoir's replenishing are detected within this mode of operation. Regarding the attacks initiated during the reservoir's draining, various attacks are detected within this mode, and some attacks are detected afterwards when the system operates in the replenishing mode. The model-based anomaly detection method implemented using the process data can detect all the designed and simulated cyber-physical attacks against the water storage unit.

This thesis's contributions include developing a benchmark for implementing potential future anomaly detection methods for Dunea's and other drinking water production companies' water storage units. Additionally, given the provided process data, a nonlinear hybrid automaton is created to describe the nominal behaviour of the water storage unit. Lastly, multiple attack profiles are studied, including their impact on the physical system and effectiveness in evading detection.

Table of Contents

Preface

Significant developments have been made in IT cybersecurity over the past years. However, work still needs to be done concerning cyber-security in the industrial domain. When Dr. R.M.G. Ferrari proposed I pursue an Industrial thesis in collaboration with the industrial cybersecurity division at Magion, I eagerly embraced the opportunity. It is crucial to protect critical industries that are vital to our existence as human beings. Therefore, I developed a cyber-attack detection mechanism for a water distribution company. Concerning cybersecurity in the industrial setting, we can utilise the existing theorems to enhance the detection mechanisms. Throughout my thesis, I had the opportunity to present my research at Wiccon, a cybersecurity conference that puts women's technical achievements in the spotlight, and at the High-Security Delta Café. There, I showcased the potential of leveraging knowledge of physical system dynamics to enhance resilience against cyber-physical attacks.

I want to thank my head supervisor, Dr. R.M.G. Ferrari, for his guidance and for making time in his busy schedule. I also want to express my appreciation to Ir. I. van Straalen, my daily supervisor for the last months. He was always able to discuss challenges and provide constructive feedback. Furthermore, I would like to thank Rob Verseijden en Ard Roelvink of Magion. They showed me the fundamentals of industrial cybersecurity and supported me throughout this project. Also, I would like to thank Thijs Aanhane and Dennis Zuiderwijk, operators at Dunea, for offering valuable insights into Dunea's process and providing the essential data. Last but not least, I want to express my gratitude to my family and friends who were there when I needed them the most, providing kind and encouraging words and support during this journey.

"All change is not growth, as all movement is not forward."
— *Ellen Glasgow*

Chapter 1

Introduction

Industrial Control Systems (ICSs) are crucial components of critical infrastructures that monitor and control industries such as water and power distribution, manufacturing, and transportation. They are essential for society's functioning, and a failure could have catastrophic consequences. Incorporating information and communication technology into ICSs has enhanced their efficiency and performance, exposing these systems to new vulnerabilities and threats. According to the British Standards Institution, there has been a noted increase in the following threats since 2019 [24]:

- Malware infections through internet and intranet channels
- Software and hardware vulnerabilities in supply chain
- Risks associated with internet-connected control components
- Intrusion points through remote maintenance access
- Compromise of extranet and cloud components

Ensuring the safety of ICSs is paramount, as any harmful threats imposed on these systems can potentially impact people's lives, the environment and the economy. A survey by IBM found that manufacturing accounted for the highest share of cyber-attacks worldwide, with nearly 25% in 2022 and 28% in 2023 [32], [33]. The Center for Strategic and International Studies tracks major cyber incidents, focusing on attacks against various industrial sectors [15]. Notable attacks they tracked include:

- In December 2023, Ukrainian state hackers targeted Russia's largest water utility plant.
- In February 2022, several oil terminals in major ports across Belgium and Germany were targeted by a cyber-attack.
- In April 2022, hackers attempted to shut down electrical substations in a Ukrainian energy facility.

In 2016, the European Union (EU) introduced the Network and Information Security (NIS) directive to ensure a high level of cybersecurity across Member States [49]. Apart from the regulations companies operating within the European Union must comply with, additional measures are available to strengthen cybersecurity. One such measure is the introduction National Institute of Standards and Technology (NIST) cybersecurity framework, which is globally recognised and used to manage and minimise cybersecurity risks. This framework comprises five core functions: identification, protection, detection, response, and recovery from cyber-attacks [47].

The examples presented above indicate that it is not a matter of whether your industry will be targeted but rather when. To effectively mitigate these attacks, detection is necessary. Therefore, this thesis aims to investigate the detection of cyber-physical attacks aimed at critical industrial control systems, with a focus on the production and distribution of drinking water. The importance of this sector arises from its crucial role in human existence, increasing water scarcity and essentiality for various industrial processes [64].

Detection methods have proven to successfully detect cyber-physical attacks on simulated medium-sized Water Distribution Networks (WDNs) and scaled-down versions in real-life testbeds ([2] - [5], [19], [28] - [30], [38], [41], [44], [46], [48], [52], [55], [57], [59] - [61], [63], [65]). However, to the best of the author's knowledge, the development of cyber-attack detection methods with regard to real-life WDNs is underrepresented in currently available literature. This led to the formulation of the following research question:

"Can cyber-physical attacks targeted against a real-life Water Distribution Network be detected by employing a model-based anomaly detection method?"

To answer this research question, three sub-questions are formulated:

1. *How can real-time process data be used to create a model representing the nominal dynamical behaviour of the WDN accurately?*
2. *How can one develop cyber-physical attacks and evaluate their influence on the WDN?*
3. *What anomaly detection method could be implemented to detect cyber-physical attacks?*

Dunea, a Dutch drinking water company responsible for producing and distributing drinking water to a large region of the South of Holland, kindly provided its process data for this research to answer these questions. Dunea should be prepared against unexpected cyber-physical attacks impacting daily operations. Therefore, it is crucial to simulate these attacks and develop detection mechanisms to identify and avert such attacks' catastrophic consequences.

This research will contribute to developing a detection method for practical application in a real-life water distribution network. In order to create this detection method, a non-linear hybrid automaton will be derived to describe these dynamics. Subsequently, the designed anomaly detector will be evaluated by simulating attacks with various attack profiles on the WDN to determine its effectiveness in detecting anomalies.

The outline of this report is structured as follows: in chapter 2 background information on Industrial Control Systems (ICSs), cyber-physical attacks and detection methods are provided.

Furthermore, it presents related work concerning detecting cyber-attacks in Water Distribution Networks (WDNs). In chapter 3, a process description of the WDN is presented, along with a detailed derivation of the mathematical model describing the nominal dynamics of the water storage unit. In chapter 4, the design and simulation of the cyber-physical attacks and the implementation of the anomaly detector are denoted. In chapter 5, the results of the detection of the simulated cyber-physical attacks are evaluated. Lastly, chapter 6 offers a definite conclusion of this study, answers the research question and provides recommendations for future research.

Chapter 2

Cyber-attacks in industrial control systems

This chapter aims to present comprehensive background information on Industrial Control Systems (ICSs), cyber-physical attacks, anomaly detection methods, and the relevant literature on cyber-attack detection within Water Distribution Networks (WDNs). In section 2-1, literature on ICS is discussed, including the dominant architecture, main components, and commonly used communication protocols. The vulnerabilities introduced by these developments, alongside their benefits, are emphasised. In section 2-2, the three primary resources an attack could exploit and potential areas vulnerable to attacks are outlined. Lastly, section 2-3 presents the current landscape of intrusion detection systems and discusses the literature regarding the implementation of anomaly detection methods used to identify cyber-physical attacks within WDNs.

2-1 Industrial control systems

In the last 50 years, the rise of digital control devices has increased communication between various components in ICSs. Due to the safety aspects and availability of control operations, it is necessary to segmentate components within ICSs. A standardised architecture is used as a framework in the industry to structure these components and their communication. This architecture, its main components and communication protocols will be described, such as supervisory control components, Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs) and fieldbus protocols. Unfortunately, ICSs have vulnerabilities such as access critical components, unencrypted communication protocols, and wireless access points. Malicious attackers can abuse these vulnerabilities, as was seen over the last 10 years with an increase in malicious cyber-attacks. This section aims to provide dominant architecture and communication protocols utilised, while highlighting the benefits and drawbacks of the adaptations that have been made.

2-1-1 Dominant architecture

This section will provide a more detailed understanding of the complex design of ICSs. The segmentation employed to structure ICSs and Information Technology (IT) networks, along with a detailed description of the primary components of the ICS, is given.

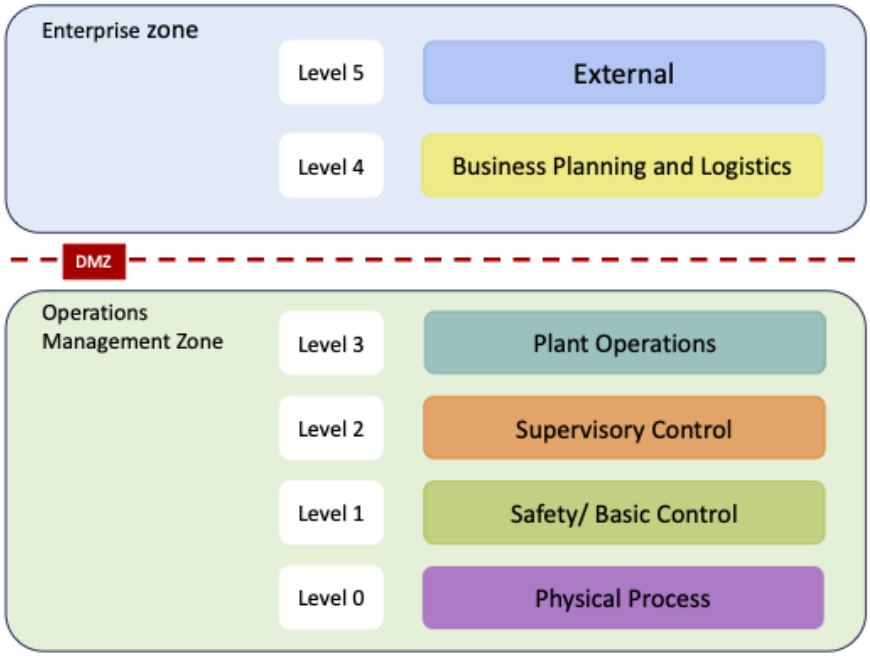


Figure 2-1: PERA levels [36]

PERA model

The growing number of components integrated into ICSs and their ability to interconnect both with each other and with the IT domain has significantly elevated the complexity of industrial architecture. Therefore, Theodore J. Williams and members of the Industry-Purdue University developed the Purdue framework for architecture in industrial automation in the 1990s [8]. The model creates a standard for segmentation and hierarchical structure of data-flows within the network of the ICS. The Purdue Enterprise Reference Architecture (PERA) model, as shown in Figure 2-1, consists of five levels, ranging from 0 to 4, as in the international standard, ISA 95 [36]. The PERA levels denote the criticality levels of components within an industrial enterprise, with level 0 being the most critical and essential for the production process and safety. The absence of level 3 should not disturb production on its own. Any levels higher than 3 should not impact the production process.

The framework consists of the enterprise zone, denoted by levels 4 and 5, a Demilitarised Zone (DMZ) and the manufacturing zone, denoted by levels 0-3. The DMZ establishes a distinct boundary between the two domains by overseeing traffic and creating a controlled space for exchanging process data [27]. The enterprise zone is subdivided into two levels: the enterprise layer for business planning and logistics and the external environment, which

is often the Internet. The manufacturing zone contains levels 0-3, level 0 being the physical process, level 1 containing the basic control devices, level 2 providing supervisory control, and level 3 containing devices for operating management. In Figure 2-2, a detailed representation of the components within the framework is shown. In the following section, a clear description of the main components of the manufacturing zone will be given. It is noted to the reader that this is a generalised topology description, and not all industrial control systems will necessarily have this architecture.

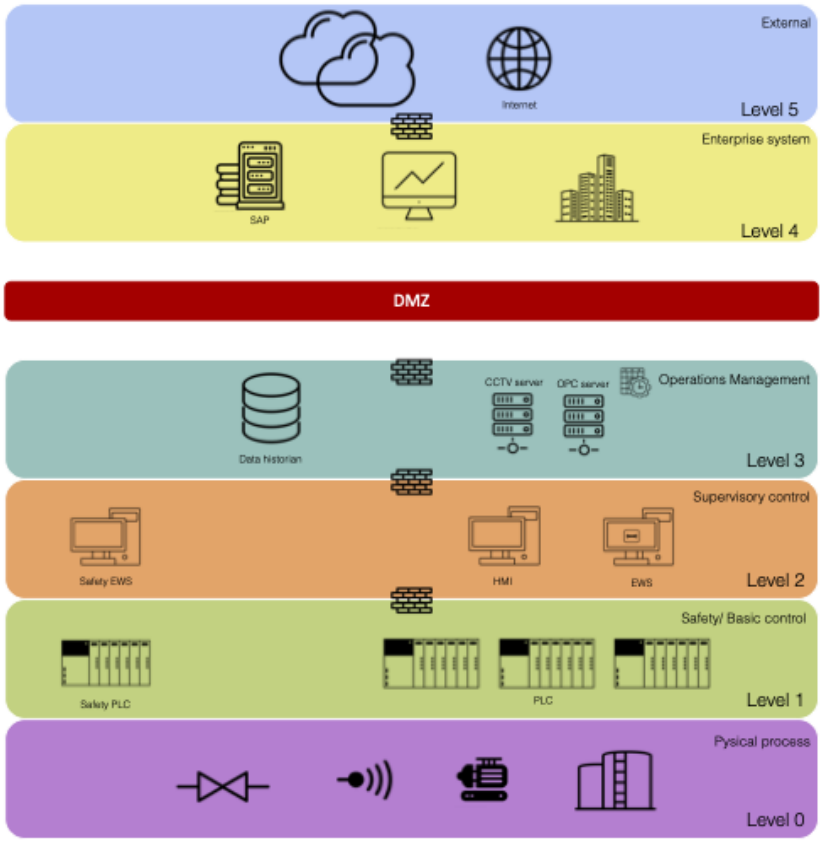


Figure 2-2: Detailed PERA architecture

Main components

The manufacturing zone comprises all essential devices and additional supporting equipment required for the manufacturing process. Levels 0-2 include critical devices to the overall manufacturing process. To provide a comprehensive understanding of these devices, a detailed description of the components at each level will be given.

Level 0 - Physical process Field devices, including sensors, transducers and actuators, use an industrial protocol such as Modbus or Process Field Bus (PROFIBUS) to communicate directly with a controller. These sensors measure various parameters such as temperature,

pressure, vibration and humidity. In contrast, actuators such as valves, pumps, turbines, burners and compressors influence the process [14].

Level 1 - Safety/ Basic control The primary control components employed in various ICSs are PLCs and DCSs.

PLCs

Originally, PLCs were designed to replace the electromechanical relays as switching or logic elements. The PLCs are programmed in ladder logic, which looks like a schematic diagram of relay logic [8]. A typical PLC consists of a power supply, Central Processing Unit (CPU), communication interface and Input/Output (I/O) modules(s) [14]. Modern PLCs can perform binary and analogue I/O and implement Proportional, Integral and Derivative (PID) control loops [22]. The processor-based system takes inputs from data generation devices, such as sensors, communicates them with the production via DCS or Supervisory Control and Data Acquisition (SCADA) devices, and presents the output to Human Machine Interface (HMI) [39]. The control logic of the PLC is accessible via a programming interface at an engineering workstation [56].

DCSs

Large, high-value, safety-critical process industries, such as oil refineries, drinking water treatment plants, chemical manufacturing plants and pharmaceutical processing facilities, commonly use DCSs [8], [56]. DCSs are control systems in which pre-programmed control actions mainly occur centrally within the DCS controllers rather than locally near the process. These functions of the DCS are typically implemented redundantly. However, for functions that require a very fast response time or autonomy, such as safety systems, local PLCs are still used, which have a lower computational time than a DCS. Using a HMI in combination with the DCS allows for live process values to be displayed and set points to be adjusted [22].

Level 2 - Supervisory control HMIs are used in combination with Supervisory Control and Data Acquisition (SCADA) devices and engineering working stations to perform supervisory control. In the supervisory control level, components, such as HMIs, are combined with Supervisory Control and Data Acquisition (SCADA) devices to provide operators with necessary process data and enable supervisory control if required. Furthermore, engineering working stations can be employed to modify the control law of specific control devices.

SCADA

SCADA is a vital component of ICS, it collects data from control hardware, such as Remote Terminal Units (RTUs), typically a type of PLC. The data is then transferred to a central computer facility, where it can be displayed to the operator in either a graphical or textual format [56]. The SCADA system allows the control system to operate remotely, which is useful when multiple local control systems are in place. The SCADA system can adjust local setpoints from a centralised control room [8]. However, it's important to note that the local control systems are not dependent on the SCADA system. The local control system will continue to function if the SCADA system fails. In summary, SCADA plays a critical role in collecting and transferring data from control hardware to a central location, where it can be displayed to the operator. While the SCADA system enables remote operation, the local control systems can function independently of it.

HMI

The HMI is a technology that enables humans to interact with machines or systems. It serves as a bridge between the user and the machine, allowing the exchange of information and control commands. The main purpose of this interface is to facilitate effective communication and control. An HMI typically displays plant processes, providing status information such as temperature, flow rate, and tank levels [14].

Engineering stations

The engineering workstation is commonly a desktop computer or server hosting the programming software for controllers, like PLC, RTU and applications. This platform can change the controller logic and industrial applications [14].

2-1-2 Communication protocols

For ICSs to function properly, it's crucial that devices can communicate with each other. Traditional wired communication technologies have been paramount in industrial monitoring and control networks. However, this communication was usually carried out over point-to-point wired systems. These systems required a huge amount of wiring, which, in turn, introduced a large number of physical points of failure, such as connectors and wire harnesses. To overcome these drawbacks, point-to-point systems were replaced with advanced industrial communication technologies. This section highlights the major communication technologies utilised in industrial control networks.

Fieldbuses

Originally, information was transferred to the controller analogously. Most analogue instruments used analogue currents within the range of 4 mA to 20 mA or analogue voltage between 0 V to 10 V. For example, in a dimmer switch, 4mA represents off, and 20mA represents on. The arrival of digital signals in the 1960s introduced digital controllers, transmitting signals containing binary values [18]. Therefore, it enabled the replacement of multiple analogue control loops with one single digital controller [22]. This necessitated the development of new communication protocols that would comply with the digital transition.

The International Electrotechnical Commission (IEC) established Fieldbus communication protocols in their IEC standard 61158 [35]. Since 1978, the industry has developed endless fieldbus protocols, including Foundation Fieldbus H1, ContronNet, PROFIBUS, and Modbus. RS-232, RS-485, and Modbus are the serial communication protocols launched around the 1980s. RS-232 and Modbus were developed and applied to be used for the connection of PLCs to industrial devices. RS-485 is used within industrial and commercial networks because it can communicate over longer distances and with multiple devices [8]. In 1986, Siemens launched PROFIBUS, the first fully digital protocol for powering field devices and supports communication speeds up to 12 Mbps and 126 addresses/nodes.

While initially designed to replace communication protocols for traditional analogue signals used at the lowest level of an industrial control system, fieldbus technology has since evolved significantly. This evolution has introduced additional functionality that can be used across various levels of the control hierarchy. Consequently, Ethernet has gained prominence with

connecting fieldbuses to PERA levels two and three devices [8], [22]. Ethernet can connect thousands of devices to the network, whereas most fieldbuses support communication for only up to 250 devices.

Industrial Ethernet

Ethernet is a communication technology widely used in both Local Area Network (LAN) and Wide Area Network (WAN). A LAN is a network of computer routers, switches and firewalls that covers a limited area, such as the office domain, whereas a WAN is a collection of LANs or other communication networks [8].

The introduction of switched networks was a significant development that enabled using Ethernet for industrial purposes. In traditional hub-based networks, signals were transmitted from one port to all other ports, causing congestion on the physical medium. However, switched networks only transmit data received on a port in the direction in which the recipient of the data is located, resulting in a more efficient data transmission process.

For industrial applications such as ICSs Industrial Ethernet (IE) is used, which involves special cable connectors, making it more reliable when compared to standard Ethernet. The commonly used IE protocols are PROFINET, EtherNet/IP, EtherCAT, SERCOS III, CC-Link IE, Modbus TCP/IP and Powerlink [8].

2-1-3 Vulnerabilities

In ICSs, vulnerabilities appear on different levels, posing significant challenges to the availability and integrity of industrial processes. At the system and component design level, network design level, and within security policy, culture, and technical operations, vulnerabilities introduce potential points of exploitation [1]. For the purpose of this thesis, the focus will be exclusively on the system and component design level and the network design level.

Devices positioned within PERA level one, as illustrated in Figure 2-2, are basic control components such as a PLC, RTU and Intelligent Electronic Devices (IEDs). These components are commonly connected through fieldbus protocols, such as Modbus and PROFIBUS DP, utilising a client/server communication model. In this model, a client initiates a data request to a server, which then responds with the requested data. Importantly, bidirectional communication allows clients to modify server data. Inconveniently, Modbus and PROFIBUS DP communication protocols lack essential security features such as encryption and authentication [31]. This vulnerability allows potential malicious actors to gain unauthorised access to sensitive information by exploiting vulnerabilities in communication cables, posing a serious threat to the confidentiality and integrity of industrial processes. Moreover, suppose PLCs or sensors that are part of the safety control system are compromised by malware, hackers, or human-made errors. In that case, it can lead to potentially catastrophic consequences.

As discussed in subsection 2-1-1 PLCs, SCADA systems, and DCS systems frequently communicate via an Ethernet communication protocol. Despite the efficiency gains associated with remote access to field devices, many devices within this network, including switches, routers, and engineering stations, were not originally designed with cybersecurity in mind. The reliance on Ethernet communication introduces a potential gateway for attackers to compromise

these vulnerable devices. Unauthorised access to and control over these critical devices could result in catastrophic consequences for industrial processes.

Moreover, companies often seek integration within network design between the ICS network and the office IT network, typically achieved using Ethernet. Wireless physical standards are also emerging to enhance the integration between Operational Technology (OT) and IT networks. Using TCP/IP, HTTP, and XML standards has blurred the line between enterprise and industrial networking [22].

In summary, the existence of multiple vulnerabilities within industrial control systems necessitates the implementation of comprehensive security measures. Safeguarding data availability, integrity, and confidentiality is paramount to mitigate the potential risks associated with unauthorised access and control over critical industrial components. As the integration between OT and IT networks continues to evolve, the need for addressing vulnerabilities becomes an ongoing challenge. This demands continuous adaptation and improvement of security protocols and practices, especially in the OT domain, which involves the physical world and the safety of humans and the environment.

2-2 Cyber-physical attacks

Companies implementing ICSs enclose two domains: the IT network and the OT network, with the intermediary DMZ that separates them. The target of a cyber-attack can be a component in one of these two domains. However, in most reported ICS incidents, the attackers gain access through the IT domain, then move to OT infrastructure, and influence the physical process through the communication infrastructure [26]. These attacks are known as Cyber-Physical Attacks (CPAs), and launching multiple attacks on OT assets can affect the physical behaviour of the system.

CPAs and faults can be modelled as an external signal influencing the system's dynamics [21]. However, there is a significant difference between them. Faults do not have a specific objective to fulfil, in contrast to CPAs that hold a malicious purpose, as pointed out by Teixeira et al. in [61]. Also, faults are generally considered random, while attacks are usually planned over time and result from calculations [50][61]. This chapter discusses the different types of CPAs that ICSs can be subjected to, along with the areas targeted by these attacks.

2-2-1 Categorisation

Cyber-Physical Attacks (CPAs) can be divided into three categories: disclosure, deception and disruption attacks [17], which can compromise the traditional security goals of integrity, availability and confidentiality [13].

Disclosure attacks
Disclosure attacks refer to the attempts to gain unauthorised access to sensitive information, thereby violating data confidentiality [13], [17]. This could involve eavesdropping to obtain sensory data and control inputs to gain knowledge of the system's transfer function [61]. It is important to note that the objective of disclosure attacks is to remain unseen and not disrupt

the system's normal operation.

Deception attacks
Deception attacks, often referred to as False Data Injection (FDI), occur when signals deviate from their actual value. The lack of integrity, i.e. the trustworthiness of data or resources, will result in deception [42]. Examples include introducing incorrect sensor measurement or control input or altering the control law [17]. Launching these attacks by compromising the integrity of sensor and actuator data [48] or by obtaining the secret keys by the sending devices [6]. It should be noted that deception attacks do not hold any disclosure capabilities [61].

Disruption attacks
Disruption attacks involve tampering with information, such as Denial of Service (DoS) or jamming attacks [17]. Attempting to disrupt the nominal functioning of a system and its ability to remain accessible and usable upon demand [23]. For instance, if a critical physical process is open-loop unstable and a DoS attack occurs, the absence of sensor data leads to an open-loop control problem, which could cause damage to the system and entities around it [13], [61].

2-2-2 Areas of attack

CPAs can occur at targeted components, such as devices in the physical layer, the PLC or the SCADA system. Moreover, the attacks can also aim for the communication link between devices, like the link between a PLC and the physical layer, or the link between PLCs, or the communication between PLC and SCADA. The multiple attacks are shown in Figure 2-3.

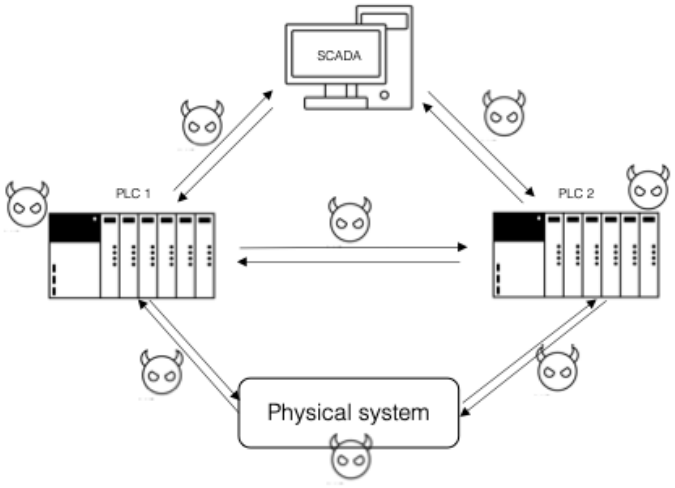


Figure 2-3: Graphical representation of the attack locations.

Figure 2-4 provides a more detailed illustration of potential attacks on the basic control level. Deception attacks can influence the integrity of the communicated values by injecting biased

data and creating $\tilde{u}$ and $\tilde{y}$. Disruption attacks can disable the communication between the actuators and the controller. In addition, the control law of the PLC can be rewritten, or physical damage can be inflicted on components such as pumps or valves.

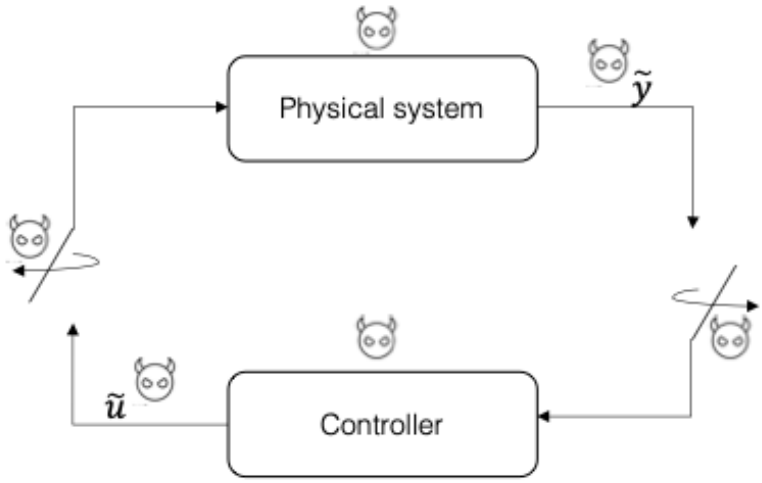


Figure 2-4: Graphical representation of attack on basic control level

2-2-3 Man In The Middle attack

Man In The Middle (MITM) attacks are performed at the SCADA client server device endpoint due to their communication protocol giving an easy way in. In this attack, the attacker can capture the traffic passing through the network, including data transmitted by the targets. To achieve this, the adversary gains access to a machine connected to a span port or tricking the switch into becoming a span port [43]. A replay attack is an example of a MITM attack. A replay attack lies within the plane of disclosure and disruption resources. In replay attacks, a finite data horizon is recorded during normal conditions and then retransmitted to the HMI monitors of the operator. This can occur while field devices are either disrupted or operated at a different setpoint. Another example of a MITM involves injecting false data into communication signals received while simultaneously jamming other field devices.

2-3 Intrusion detection systems

This section will elaborate on the various intrusion detection methods used to detect cyber-physical attacks in ICSs. Intrusion Detection System (IDS) are commonly used to identify malicious attacks against information systems by analysing network protocols and traffic data [30]. However, in ICSs, data confidentiality is not the highest priority. Instead, the emphasis is on enforcing security measures that are practical and compatible with the specific operational needs of the industrial setting [51].

Compared to conventional information technology, the security protocol applications of ICSs are simple and do not support encryption. Therefore, the traditional information security field methods can not be directly applied to industrial control systems security [72]. Additionally, ICSs differ from traditional information systems as they are directly connected to the physical world. This makes it challenging for traditional IDS designed for information to identify attacks against physical processes that do not cause abnormal network traffic or violate protocol specifications [30].

To address this challenge, anomaly-based intrusion detection can be employed. This involves defining normal behaviour and flagging any visible deviation from it as either unintentional faults or intentional attacks. Firstly, the existing fault diagnosis methods are outlined and then their application to anomaly detection methods for detecting cyber-physical attacks detection in related work is discussed.

2-3-1 Fault Diagnosis

Fault diagnosis is a process that involves detecting, isolating, identifying and estimating faults in a system at a given time, assuming knowledge of possible faults [37]. Fault detection determines the presence of a fault in a given system at a given time, testing the null hypothesis: $\mathcal{H}_0$: the system behaves nominally. Fault isolation evaluates i faulty hypotheses, $\mathcal{H}_i$: the system behaves as if the i-th fault is present at a given time. In case $\mathcal{H}_0$ and all but one $\mathcal{H}_i$ hypotheses are falsified, then the fault parameters are estimated. If $\mathcal{H}_0$ and all $\mathcal{H}_i$ are falsified, then a model of a new fault should be identified.

Change detection methods are utilised to test the null hypothesis, which can be divided into deterministic and probabilistic tests. An example of a deterministic test is the limit check of scalar variables, where the minimum and maximum allowed values are known $z_{min} < z(k) < z_{max}$ [37]. However, this method only applies in steady-state, and in some cases, the deterministic limit is unknown. A probabilistic change detection method commonly used is the Chi-squared test. This test is used to determine if there is a change in the variance σ of a normal distributed random variable. It evaluates N samples with a known covariance σ_0 and estimates $\hat{\sigma}_1$ from samples, described in the following equation:

$$\chi^2 = \frac{(N-1)\hat{\sigma}_1^2}{\sigma_0^2}. \tag{2-1}$$

Change detection methods such as limit value check and Chi-squared only focus on separately evaluating individual measurements or data sets. The previous test does not influence the next one. Furthermore, the Chi-squared test requires many samples before and after the change to verify or falsify the null hypothesis with sufficient significance. This leads to a delay in the detection of anomalies. On the other hand, stateful detection methods employ the history of the measurements. An example of a likelihood-based methods is the Cumulative Sum (CUSUM), which uses the log-likelihood ratio of an observation $z(i)$:

$$s(z) = \ln \frac{p_{\theta_1}(z)}{p_{\theta_0}(z)} \tag{2-2}$$

Where $z(i)$ is a sequence of independent random variables, the probability density function p_{θ_0} denotes the healthy normal distribution of signal and p_θ represents the probability distribution for the attack regarding the hypothesis $\mathcal{H}_1$. The CUSUM of the log-likelihood ratio is described as follows [12]:

$$S(k) = \sum_{i=1}^{k} (s(z(i)) = \sum_{i=1}^{k} \ln \frac{p_{\theta_1}(z(i))}{p_{\theta_0}(z(i))}. \tag{2-3}$$

The CUSUM experiences negative drift before the change and positive change after. The above-mentioned detection methods are signal-based methods that evaluate the signal $z(k)$ in the presence of a fault. In contrast, model-based detection methods rely on creating a nominal model rather than nominal features of a system. These methods rely on measurements and an observer to derive state estimations and compose a residual for analysis. The dynamics of the physical system can be described by:

$$\begin{aligned} x(k+1) &= f(x(k), u(k)) + \eta(x(k), u(k), k) \\ y(k) &= x(k) + \zeta(k), \end{aligned}$$

where $\eta(k)$ is the model uncertainty and $\zeta(k)$ measurement noise. The observer introduced to compute the residual is denoted as the following:

$$\begin{aligned} \hat{x}(k+1) &= f(y(k), u(k)) + \Lambda|\hat{x}(k) - y(k)| \\ \hat{y}(k) &= \hat{x}(k) \\ r(k) &\triangleq y(k) - \hat{y}(k), \end{aligned}$$

where Λ is the observer gain that dampens out the output error. If the residual $r(k)$ exceeds a predefined threshold, a fault is detected [20].

Although fault diagnosis and attack detection in cyber security are related to detecting anomalies, a subtle difference exists. The classical control-theoretic approaches from anomaly detection deal with independent disturbances, and faults and do not consider colluding malicious cyber-attacks where multiple variables can be tempered to hide attacks. This is done by mimicking physical disturbances and faults [54]. Furthermore, model-based detectors are primarily focused on detecting and isolating faults with a specific known structure. This poses challenges when dealing with adaptive intruders within the system, particularly intelligent adversarial attackers whose attack signature is unknown [45].

Despite the abovementioned differences, many researchers have applied conventional detection methods to cyber-physical attack detection. The next section will describe the related work regarding the development of anomaly detection methods to detect cyber-physical attacks in WDN.

2-3-2 Anomaly detection methods

As previously stated, the anomaly detection problem can be divided into three parts. Firstly, the representation of the physical system must be used to predict or estimate the system's outputs. A mathematical model can be derived using historical data and system identification methods, such as the auto-regressive integrated moving average and linear dynamical state-space, ARIMA model [30], or the sub-space identification method.

Next, an observer-based method estimates the output and calculates the difference between the measurement and the estimated output, known as the residual. In research, different methods have been studied for this purpose.

Amin et al. [7] uses an Unknown Input Observer (UIO) and direct system identification. On the other hand, Ahmed et al. [3] and Azzam et al. [11] employ a sub-space identification technique for Linear Time-Invariant (LTI) systems [66] to derive a Kalman filter to estimate the evolution of the system dynamics. Conversely, Jia and Zhang [38] utilise a Luenberger observer gain, while Amin et al. [6] employ a bank of Luenberger observers. The dynamical model of a LTI system can be obtained as a discrete-time state-space model of the form:

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + v_k, \\ y_k &= Cx_k + \eta_k, \end{aligned} \tag{2-4}$$

where $k \in \mathbb{N}$ is the discrete time index, $x_k \in \mathbb{R}^n$ is the state, $y_k \in \mathbb{R}^m$ are the measurement output, $u \in \mathbb{R}^p$ denotes the inputs, v_k the model uncertainty, and η_k the measurement noise, assumed to be Gaussian with zero mean and covariances Q and R respectively.

To estimate the state of the system based on the available output y_k, a linear filter can be used with the following structure:

$$\hat{x}(k+1) = A\hat{x}_k + Bu_k + L_k(y_k - C\hat{x}_k), \tag{2-5}$$

with the estimated state $\hat{x}_k \in \mathbb{R}^n$ and observer gain matrix $L_k \in \mathbb{R}^{n \times m}$. Defining the estimation error $e_k := x_k - \hat{x}_k$. The estimation error will behave according to the following equation

$$e_{k+1} = (A - L_k C)e_k - L_k\eta_k + v_k. \tag{2-6}$$

In contrast to the Luenberger observer, which is determined such that the estimation error converges to zero asymptotically $\lim_{k\to\infty} e_k = 0$, in the Kalman filter, the matrix L is designed to minimise the covariance matrix $P_k = \mathbb{E}[e_k e_k^T]$ [10]. Verifying that $R + CPC^T$ is positive definite, the estimator gain is

$$L_k := PC^T(CPC^T + R)^{-1}. \tag{2-7}$$

This leads to a minimal state covariance matrix P, with P given by the solution of the algebraic Riccati equation:

$$P = APA^T - APC^T\left(CPC^T + R\right)^{-1}CPA^T + Q. \tag{2-8}$$

The last part of the anomaly detection problem is analysing the residuals. This involves composing a null hypothesis for the nominal model where no attacks are present and an alternative hypothesis for the faulty model where an attack has occurred. Hypothesis testing is then conducted based on the residual statistics, which are tested using the methods described in the previous section. Related work uses static algorithms like chi-squared and limit-checks to evaluate the residual [3], [11], [38], [60], [69]. [11] uses chi-squared metric: $z(k) = r^T(k)\Sigma^{-1}r(k)$ and compares it with a threshold τ. Where $r(k)$ is the residual, Σ is the covariance matrix of the residual under normal conditions, and τ is set according to a desired false alarm rate. In contrast to Chi-squared, CUSUM also considers the previous measurements. Therefore CUSUM is broadly used in the literature [6], [16], [44], [48], [65]. Since this method depends on the probability distribution of the considered attack scenario state, non-parametric evaluation methods are used, such as the Non-Parametric Cumulative Sum (NP-CUSUM) and F-test. Research shows that the implementation of the NP-CUSUM independent of the statistics of the model of the attack succeeds in detecting attacks to the WDN [9], [16] and [30].

Conventional anomaly detection methods only evaluate the magnitude of residuals. In contrast, Hu et al. explore other residue characteristics in [29] and [30] to detect stealthy attacks. In their 2020 paper, [29], they propose a method that uses the permutation entropy to characterise the regularities in the prediction residuals generated during stealthy attacks. This helps in distinguishing the nonrandom residual series from a random one and identifying the occurrence of an attack. On the other hand, in their 2019 paper, [30], they compute the skewness coefficient of the residual. During a false data injection attack, a small portion of residuals are replaced with average residuals, and the residual distribution becomes right-skewed or left-skewed. However, these methods still depend on manually setting and tuning the algorithm parameters, such as detection threshold and residual length, for testing.

Within the studied literature, most model-based detection methods use an observer-based method. However, Housh [28] proposes a demand estimation method based on the records of water measurements. They use this as input to simulate the hydraulic laws, calculating and classifying the errors between the SCADA readings and simulated values. Additionally to the threshold on the residual, Housh proposes a multilevel approach to record the thresholds using three moving average filters with lags between 0 and 2. The classification errors include one outlier vector from each moving average filter and two components that must violate the threshold.

These methods are model-based approaches. Most industrial control systems, such as power grids and water distribution networks, are large, complex, distributed control networks. Due to the complexity and possible nonlinear behaviour, identifying such a system can be challenging. They often simplify and linearise the system for a given operating point [3], [60].

These conventional detection techniques cannot handle the complex multivariate data streams generated by modern Cyber-Physical Systems (CPSs). This is because the model-based methods rely on an accurate representation of the physical system, which can be difficult to achieve due to the dynamic nature of CPSs. Furthermore, model parameters, such as pipe roughness, can change over time in real-life applications. In response to these challenges, researchers have advanced beyond traditional specification or signature-based approaches and turned to the utilisation of machine learning techniques to leverage the copious amounts of data produced by these systems. This shift has been exemplified in studies such as [41] and [52].

2-3-3 Performance metrics

To assess the performance of the methods, the following metrics are often utilised, namely, Time To Detection (TTD) and Single Classification Rate (SCR) [58].

$$TTD = t_0 - t_d, \tag{2-9}$$

Where t_0 denotes the time an attack is detected, and t_d stands for the time at which the attack was initiated.

To quantify the accuracy of the algorithm True Positive Rate (TPR) and True Negative Rate (TNR) are computed based on the elements of the confusion matrix [58]. Both rates combined represent the SCR.

$$TPR = \frac{TP}{TP + FN} \tag{2-10}$$

$$TNR = \frac{TN}{TN + FP} \tag{2-11}$$

$$SCR = \frac{TPR + TNR}{2} \tag{2-12}$$

TP and TN represent the numbers of true positive and true negative time instants, respectively, while FP and FN are the numbers of false positive and false negative instances.

On the other hand, a hypothesis can be falsified incorrectly by enclosing a false positive or a false negative. The False Alarm Rate (FAR) can be used to tune the parameters for the anomaly detection methods. This approach was, for example, used in [3] by Ahmed et al., where a specified FAR was used to calibrate the detector parameters. The FAR denotes the ratio of false positives on the total test.

Chapter 3

Model of the water storage unit

As described in the previous chapter, model-based anomaly detection methods rely on a representative model and knowledge of the system in healthy conditions. Since the Water Distribution Network (WDN) is an extensive, complex network in section 3-1, a description of the distribution system is provided, and the boundaries of the subsystem of the WDN studied in this research are specified. The model describing the nominal system dynamics will be based on the laws of physics regarding fluid mechanical systems. In section 3-2 and section 3-3, the equations of motion for the different modes of operation are derived. Using the provided process data by Dunea and these equations of motion, the system parameters are identified in section 3-4 using multiple optimisation methods. Lastly, in section 3-5, the parameters for the final model are chosen, and a hybrid automaton is used to describe the system dynamics.

3-1 Fundamentals of the Water Distribution Network

Before a model can be created, it is essential to gain a comprehensive understanding of the distribution network and the associated processes. This section provides an overview of the automated process involved in the supply of the produced drinking water to consumers. Furthermore, a detailed description of the components at the water storage unit of the Leyweg is presented, along with the data provided by Dunea. Lastly, the fundamentals of fluid mechanics are provided to lay the groundwork for creating a model to describe the dynamics of the nominal behaviour of the water storage unit at the Leyweg.

3-1-1 Automated process

Dunea produces drinking water at three production sites in the western region of the South of Holland: Monster, Scheveningen, and Katwijk. Where the naturally filtered dune water is pumped out of the soil and post-processed to produce drinking water. Each site has its designated supply area. This thesis will focus on the supply area Zuid of the production

site at Scheveningen. To ensure a high quality of drinking water, the objective is to keep the pumping stations' production as constant as possible. However, water demand fluctuates throughout the day as most individuals follow a particular pattern. Therefore, water storage units are distributed strategically within the supply area to account for changes in consumer demand.

The pump station's setpoint is calculated using the capacity of the replenishment reservoirs, historical demand, the weather forecast, and other inputs. This calculation considers that every replenishment reservoir is filled and drained within 24 hours.

The reservoirs are drained to supply water during high-demand periods and replenished during periods of excess produced drinking water. This process is controlled through an automated operation method called "The Carousel" within Dunea, which can be seen as a centralised control system.

From 06:00 until 22:00, the temporarily stored drinking water is distributed to the consumers and visualised in blue in Figure 3-1, where A, B, C and D are the four replenishment reservoirs in the supply area. In the case of the supply area Zuid, these will be located at Leyweg, Zoetermeer, Trekvliet, and Bergsenhoek. The following actions are in order during this time window:

- If $Q_{out} - Q_{in} > 500\,m^3/h$ for a time span greater than 120 seconds, a pump at the water storage unit with the replenishment reservoir containing the highest nominal volume is turned on.

- If $Q_{out} < Q_{in}$ for a time span greater than 120 seconds, a pump of the replenishment reservoir with the lowest nominal volume is turned off.

- If the number of pumps in operation exceeds zero at 22:00, the pumps are stopped gradually.

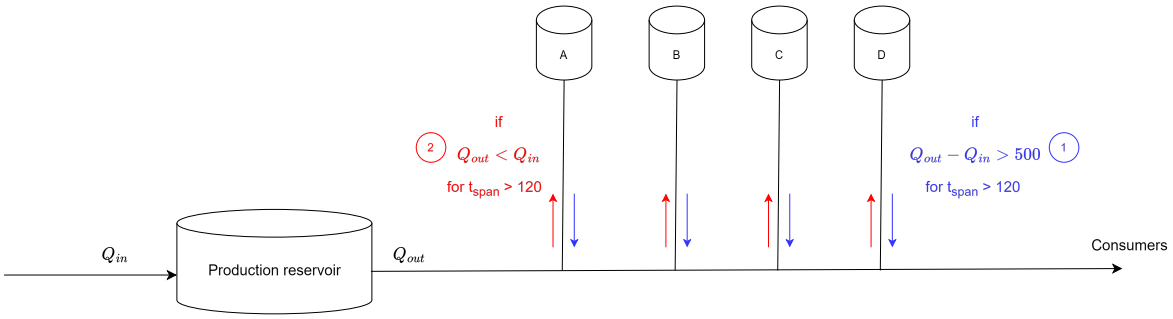


Figure 3-1: The automated process of the utilisation of the replenishment reservoir. The condition for the initialisation of the draining is visualised in blue, and the condition for the initialisation replenishing and increments of the flow rate is denoted in red.

From 22:00 until 06:00, the excess produced drinking water is stored in the reservoir, and the following actions are in order during this time window:

- If $Q_{out} < Q_{in}$ for some time greater than 120 seconds, the replenishment of the reservoir with the lowest capacity is increased by $250\,m^3/h$ until the maximum flow rate is reached.

- If the reservoir has reached its maximum capacity, the replenishment of that specific reservoir is stopped.

- If not all reservoirs are full at 06:00, the replenishment of the reservoirs is stopped gradually

This indicates that within the carousel, there are three modes of operation: conserving water, replenishing, and draining the reservoirs. As a result, the control of the water storage units and the communication of their capacity are paramount for the supply of drinking water to the industry and thousands of households in the South of Holland, as evidenced by this automated process. Therefore, this thesis will focus on modelling the water storage unit at the Leyweg to enhance cyber-security against cyber-physical attacks. The following section will describe the components located at the water storage unit to comprise an adequate model describing the different modes of operation of the water storage unit.

3-1-2 Water storage unit Leyweg

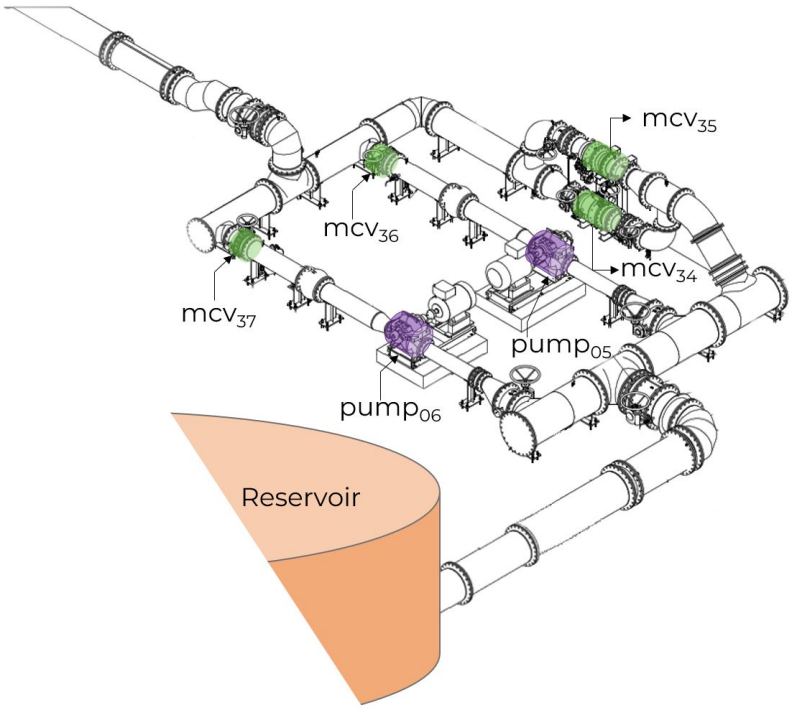


Figure 3-2: Schematic overview pipework water storage unit Leyweg

The water storage unit Leyweg consists of the following main components

- Reservoir
- Pump_{05} and Pump_{06}
- Motor-Controlled Valve $(\text{MCV})_{36}$ and MCV_{37}
- Flow Controlled Valves (FCVs): MCV_{34} and MCV_{35}
- Flow sensor
- Pressure sensor
- Level indicators
- Pipelines

The pipelines at the Leyweg water storage unit have multiple cross-sections. In Table 3-1, an overview of the pipes with the various cross-sections is given. Additionally, in Figure 3-2, it can be seen that the pipeworks are connected via tees, elbows, and cone-shaped pipes to connect pipes with different cross-sections.

Pipe diameter (mm)	Cross-section (m^2)
406	0.134
610	0.290
813	0.519

Table 3-1: Cross-sections of the various pipes in the water storage unit

Two centrifugal pumps can be used to drain the reservoir. Both pumps are the KSB-Omega 250-370 centrifugal pump, which is on/off regulated and operates at a fixed rotational speed. To replenish the reservoir, FCVs regulate the flow rate. The FCVs are MCVs, which have a valve angle setpoint that varies based on the desired flow rate, which can be increased with steps of $\approx 250\,m^3/h$ and will at most be $2500\,m^3/h$. The MCVs are butterfly valves with a diameter of 406 mm, but the vendor of the butterfly valves is unknown. The MCVs are automatically actuated. In case of any malfunctioning, they can be switched to manual actuation. MCV_{34} and MCV_{35} are utilised for the replenishment of the reservoir. MCV_{36} and MCV_{37} function as gate valves between the pumps and the connection to the consumer network, open to 90 degrees during the draining of the reservoir and delivery to the consumer network and close to 0 degrees when the draining is stopped.

To summarise, the centrifugal pump, MCV_{36} and MCV_{36} are used during the draining of the reservoir. MCV_{34} and MCV_{35} are utilised to regulate the replenishing flow rate. Additionally, there are flow rate, pressure, and level sensors to monitor the process.

Data provided by Dunea

There are two resources from which Dunea can extract process data, specifically the data historian and the Distributed Control System (DCS) system.

Dunea stores the process data within their data historian with a sampling time of five minutes. Additionally, they can export the data from the DCS system up to eight weeks back with a sampling time of one minute and up to one day with a sampling time of one second.

The data historian consists of the reservoir volume and flow rate during the draining and replenishing. The data within the DCS systems contains additional data on the valve angles, the status of the pumps, pressure and the angle setpoint of the FCVs. It is noted to the reader that no input signals to the pumps or MCVs are stored.

3-1-3 Basic fluid mechanics

This section explains the fundamental physics concerning fluids in mechanical systems, which lay the foundation for the dynamics describing the draining and replenishing of the reservoir at the water storage unit.

The Bernoulli equation, provided in the equation below, is a momentum analysis describing the relation between pressure, velocity and elevation in a frictionless flow, given the assumptions that there is a steady, incompressible and single-streamlined flow [70].

$$\frac{p_1}{\rho g} + \frac{V_1^2}{2g} + z_1 = \frac{p_2}{\rho g} + \frac{V_2^2}{2g} + z_2 = \text{constant}, \tag{3-1}$$

where p denotes the pressure in Pascal, V the velocity in m/s, ρ the densitiy in kg/m^3, g the gravitational constant and z the level in m.

In most mechanical systems, there is no frictionless flow, and pumps and/or turbines are often included in the system. Therefore, the Bernoulli equation can be extended to the Steady Flow Energy Equation (SFEE) to describe an open system's total energy and flows.

$$\left(\frac{p_1}{\rho g} + \frac{V_1^2}{2g} + z_1\right)_{in} = \left(\frac{p_2}{\rho g} + \frac{V_2^2}{2g} + z_2\right)_{out} + h_{friction} + h_{pump} - h_{turbine}, \tag{3-2}$$

where $h_{friction}$ is the head loss due to wall friction, h_{pump} is the head added to the system by the pump, and $h_{turbine}$ is the head extracted from the system. $h_{friction}$, h_{pump}, and $h_{turbine}$ are denoted in meters.

The head loss due to wall friction is approximately proportional to V^2 and can be described by Equation (6.10) in [70]:

$$h_{friction} = f\frac{L}{d}\frac{V^2}{2g} \quad \text{where } f = k(Re_d, \frac{\epsilon}{d}). \tag{3-3}$$

The dimensionless parameter f is called the Darcy friction factor, ϵ is the wall roughness, d is the pipe diameter, L the pipe length, and Re_d is the Reynolds number. The function k describing the friction factor depends on the stability of the flow.

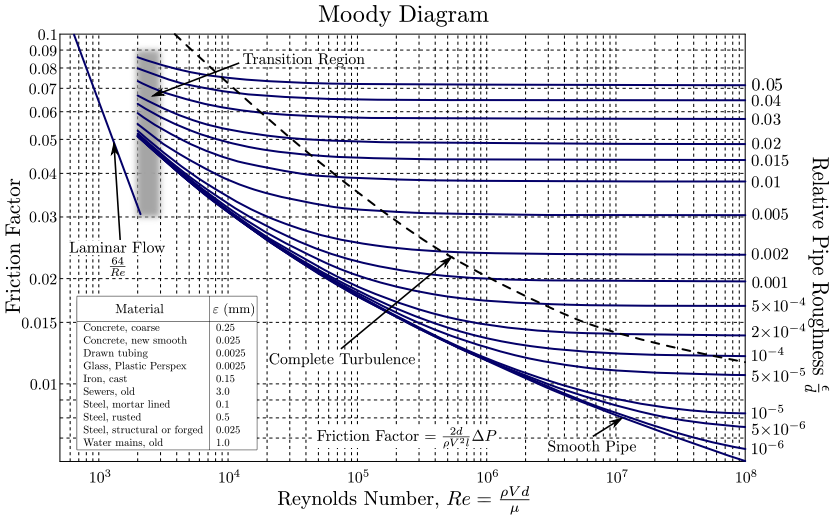


Figure 3-3: Moody chart [53]

The friction factor increases as the roughness of the pipe increases. The formula in Equation 3-4 for turbulent friction was plotted by Moody into what is now called the moody chart for pipe friction, shown in Figure 3-3.

$$\frac{1}{f^{1/2}} = -2.0\log\left(\frac{\epsilon/d}{3.5} + \frac{2.51}{Re_d \cdot f^{1/2}}\right) \tag{3-4}$$

$$Re_d = \frac{\rho V d}{\mu}, \tag{3-5}$$

where ρ is the fluid density in kg/m^3, V is the velocity, d is the pipe diameter, and μ is the absolute viscosity. For laminar flow, the friction factor can be described by: $f = \frac{Re}{64}$. The laminar parabolic flow profile becomes unstable at a Reynolds number of approximately 2300 [70].

In any pipe system, minor or local losses must be considered in addition to the friction loss calculated for the length of the pipe. These losses occur due to various factors such as pipe entrance or exit, sudden expansion or contraction of the pipe cross-section, bends, elbows, tees, and other fittings, valves, whether they are open or partially closed, and gradual expansions or contractions of the pipe cross-section. The contribution of minor loss to the overall head loss within a system can be quantified by using the loss coefficient K and can be described by Equation (6.75) in [70]:

$$K = \frac{h_m}{V^2/(2g)}. \tag{3-6}$$

A single pipe system can have multiple corners, tees, and valves, contributing to various minor losses. If the pipes have a constant diameter, these loss coefficients can be summed up into a total head loss:

$$h_{fricion} + \sum h_m = \frac{V^2}{2g}\left(f\frac{L}{d} + \sum K\right). \tag{3-7}$$

Adding Equation 3-7 to Equation 3-2 this will give the following equation:

$$\left(\frac{p_1}{\rho g} + \frac{V_1^2}{2g} + z_1\right)_{in} = \left(\frac{p_2}{\rho g} + \frac{V_2^2}{2g} + z_2\right)_{out} + h_{friction} + h_{pump} - h_{turbine} + \sum h_m. \tag{3-8}$$

In summary, the description of the automated process of the WDN conveyed insights into the regulation of the draining and replenishing of the reservoirs at the water storage unit. The water storage units play a pivotal role in ensuring the availability of drinking water. Therefore, the water storage unit at Leyweg will be the focus of this study. The water storage unit has three distinct operational modes: the idle state, replenishing, and draining the reservoir. The provided list of components and their contribution to these modes of operations, coupled with an understanding of the fundamental fluid mechanics principles, establishes the foundation for developing a mathematical model to represent the nominal behaviour of the water storage unit. In the following two sections, the models for the draining mode and the replenishing mode will be derived.

3-2 Model of the draining mode

As described in subsection 3-1-1, when the reservoir is drained, this can be done by either one pump or two pumps. Initially, the reservoir is drained employing a single pump, with the option to subsequently augment the flow rate throughout the day by activating an additional pump. These pumps operate in parallel, as illustrated in Figure 3-4. Moreover, if the demand decreases, the number of pumps in operation can be reduced from two to one, or both pumps can be sequentially shut down at a five-minute interval.

Each pump utilised at the Leyweg follows a set of operational procedures: increasing the rotational speed, maintaining constant rotational speed and decreasing the rotational speed. In subsection 3-2-1, the dynamics of the draining process are described, given the pump is operating at a constant rotational speed. In subsection 3-2-2, the dynamics of the draining process are discussed while the pump is in operation with varying rotational speeds.

3-2-1 Constant rotational speed

This section defines the system dynamics during the constant rotational speed operation of the pump. Initially, the fluid mechanics described in subsection 3-1-3 are applied to the water storage unit, followed by a description of pump dynamics. Finally, the equations of motion are formulated to characterise the system dynamics during pump operation at a constant rotational speed.

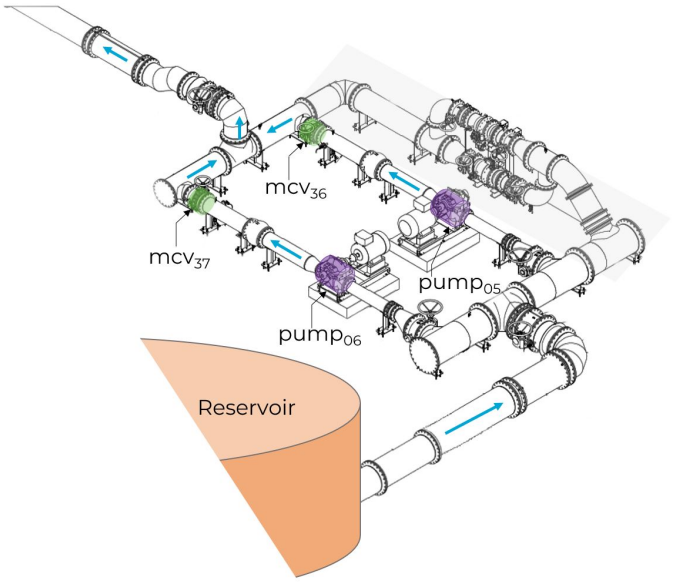


Figure 3-4: Overview components of the water storage unit involved in the delivery of temporarily stored drinking water

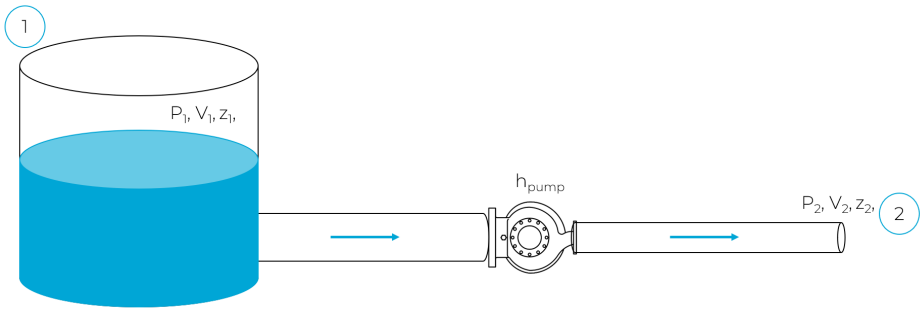


Figure 3-5: Simplified schematic representation of the pipework system utilised in the draining of the reservoir

Fluid mechanics

Considering a simplified schematic of the pipeworks as illustrated in Figure 3-5, the SFEE can be described as follows:

$$\left(\frac{p_1}{\rho g}+\frac{V_1^2}{2g}+z_1\right)_{in}=\left(\frac{p_2}{\rho g}+\frac{V_2^2}{2g}+z_2\right)_{out}+h_f+\sum h_m+h_{pump}. \tag{3-9}$$

Due to the continuity of mass and because water is considered an incompressible fluid, the continuity equation becomes:

$$V_1A_1=V_2A_2,$$

where $A_1 >> A_2$ and therefore $V_1 << V_2$ thus V_1 can be neglected.

The pipesworks of the water storage unit contain three different diameters, i.e. 406 mm, 610 mm and 813 mm. The cross-sections of the pipes will be denoted by $A_{0.4}$, $A_{0.6}$ and $A_{0.8}$ accordingly. Assuming $V_1 = 0$, continuity of mass:

$$Q = A_{0.8} \cdot V_{0.8} = A_{0.6} \cdot V_{0.6} = A_{0.4} \cdot V_{0.4} \tag{3-10}$$

and substituting Equation 3-7 in Equation 3-9 leads to the following equation:

$$\frac{p_1}{\rho g} + z_1 = \frac{p_2}{\rho g} + z_2 + \frac{Q^2}{2g}\Big(\frac{1}{A_{0.6}^2} + f_{0.8}(Q)\frac{L_{0.8}}{D_{0.8}}\frac{1}{A_{0.8}^2} + f_{0.6}(Q)\frac{L_{0.6}}{D_{0.6}}\frac{1}{A_{0.6}^2} + f_{0.4}(Q)\frac{L_{0.4}}{D_{0.4}}\frac{1}{A_{0.4}^2} + ... \\ \sum K_{0.8}\frac{1}{A_{0.8}^2} + \sum K_{0.6}\frac{1}{A_{0.6}^2} + \sum K_{0.4}\frac{1}{A_{0.4}^2}\Big) + h_{pump}, \tag{3-11}$$

where $L_{0.8}$, $D_{0.8}$, $f_{0.8}$, $K_{0.8}$ represent the total pipe length, pipe diameter, friction factor and minor loss coefficients regarding the pipes with a diameter of 813 mm. The same applies to the other pipe diameters.

Considering the different cross-sections within the water storage network, for each pipe diameter, the transition velocity from stable to unstable flow is determined for $Re_{d,crit} \approx 2300$ [70]. Given the fluid properties of water at a temperature of 20° Celsius, the fluid's dynamic viscosity μ will be $1 \cdot 10^{-3} Pa \cdot s$. The critical velocity at which the laminar flow becomes unstable at the different cross-sections is calculated using Equation 3-5 and denoted in Table 3-2. The average velocities in the various pipes are computed for one pump and two pumps in operation. These threshold velocities are lower than the average velocities, indicating turbulent flow within the pipes.

	Unstable flow (m/s)	V_{avg} one pump (m/s)	V_{avg} two pumps (m/s)
$A_{0.4}$	0.0057	1.96	3.92
$A_{0.6}$	0.00379	0.86	1.72
$A_{0.8}$	0.00283	0.48	0.963

Table 3-2: Transient velocity for turbulent flow and average velocities within the pipelines in the system

Given the turbulent flow, the friction factors can be calculated using Equation 3-4. The friction factors for the different cross-sections given one pump and two pumps in operations are calculated for the absolute roughness for commercial steel: $\epsilon = 5 \cdot 10^{-4} m$ [70]. Additionally, the head loss due to pipe friction is calculated using Equation 3-3 and presented in Table 3-3. From these calculations, it becomes evident that the friction factors do not differ significantly. When assuming a friction factor $f = 0.019$ for all cases, the updated head loss does not change significantly, as shown in Table 3-3. Therefore, one friction factor will be used throughout the modelling of draining the water storage unit.

Assuming a single friction factor for all pipes, the following equation describes the system's head that the pump is required to generate to achieve a desired flow rate.

	$0.25\,m^3/s$			$0.5\,m^3/s$		
A	f	h_f	$h_{f\_updated}$	f	h_f	$h_{f\_updated}$
$A_{0.4}$	0.0217	0.00086	0.00076	0.0216	0.00345	0.00303
$A_{0.6}$	0.0197	0.00026	0.0002	0.0196	0.00103	0.001
$A_{0.8}$	0.0185	$8.7 \cdot 10^{-5}$	$8.9 \cdot 10{-}5$	0.0184	$3.5 \cdot 10^{-4}$	$3.6 \cdot 10^{-4}$

Table 3-3: Friction factors for the various pipe cross-sections given the average flow rates and the corresponding head loss and the head loss given a constant friction factor

$$H_{sys} = \frac{p_2 - p_1}{\rho g} + z_2 - z_1 + \frac{Q^2}{2g}\left[\frac{1}{A_{0.6}^2} + f\left(\frac{L_{0.8}}{D_{0.8}}\frac{1}{A_{0.8}^2} + \frac{L_{0.6}}{D_{0.6}}\frac{1}{A_{0.6}^2} + \frac{L_{0.4}}{D_{0.4}}\frac{1}{A_{0.4}^2}\right) + \sum K_{0.8}\frac{1}{A_{0.8}^2} + \sum K_{0.6}\frac{1}{A_{0.6}^2} + \sum K_{0.4}\frac{1}{A_{0.4}^2}\right] \tag{3-12}$$

Since the flow in the system is turbulent, there will be random, rapidly varying fluctuations within the velocity and pressure. It is impossible to handle such instantaneous fluctuating variables with mathematics [70]. Therefore, the average pressure level will be identified using measurement data.

Assuming there is a constant pressure p_2 during the dynamics of the pump being at constant rotational speed, the equation for H_{sys} can be simplified to:

$$H_{sys} = a_1 - z_1 + a_2 \cdot Q^2, \tag{3-13}$$

where

$$a_1 = \frac{p_2 - p_1}{\rho g} + z_2,$$
$$a_2 = \frac{1}{2g}\left(\frac{1}{A_{0.6}^2} + f\left(\frac{L_{0.8}}{D_{0.8}}\frac{1}{A_{0.8}^2} + \frac{L_{0.6}}{D_{0.6}}\frac{1}{A_{0.6}^2} + \frac{L_{0.4}}{D_{0.4}}\frac{1}{A_{0.4}^2}\right) + \sum K_{0.8}\frac{1}{A_{0.8}^2} + \sum K_{0.6}\frac{1}{A_{0.6}^2} + \sum K_{0.4}\frac{1}{A_{0.4}^2}\right)$$

Pump dynamics

The pump curve can describe the delivered head of a pump to a corresponding flow rate. The pump has a specific characteristic pump curve for each number of rotations per minute. The intersection of the pump curve and the head demanded of the system expressed by the flow rate will be the operating point. In Figure 3-6, this is illustrated with H_s being the head demanded by the system and H_{pump} the head the pump can generate. Centrifugal pumps have a certain efficiency, and each pump has its specific pump curve for each number of rotations. Manufacturers often provide pump curves for different rotational speeds. However, the available chart only displays an operating range for a different rotational speed than the ones used by the pumps. Therefore, the shape of the pump curve should be estimated using measurement data.

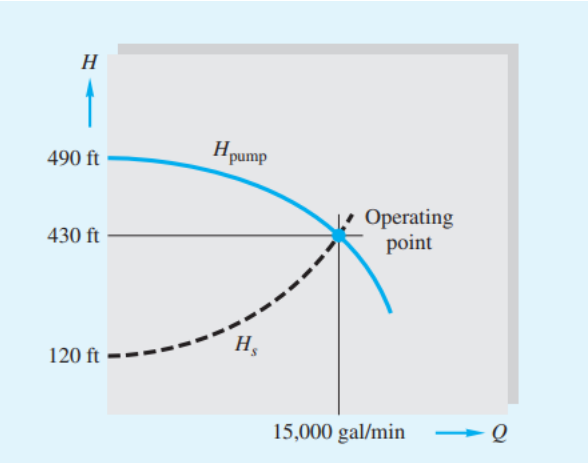


Figure 3-6: Operation point single pump [70]

Considering the pump curve can be described by:

$$H_{pump} = b_1 + b_2 \cdot Q^2. \tag{3-14}$$

It is important to consider that each pump's efficiency is affected by wear and tear. As a result, it is necessary to identify the parameters $b1$ and b_2 separately for pumps 5 and 6 operating at constant rotational speed.

Pumps 5 or 6 can operate singularly or simultaneously throughout the draining of the reservoir. When both pumps are on simultaneously, the pumps operate in parallel. The pressure drop over each branch will be the same, and the resulting flows can be added. Figure 3-7 illustrates that when two pumps are combined in parallel, the operating point will shift to a higher flow rate. It is important to note that when two pumps are operating, the shape of H_{sys} will be different compared to when only one pump operates. This is due to the differences in pipeline length and the number of turns, which result in additional losses caused by flow diverging and converging.

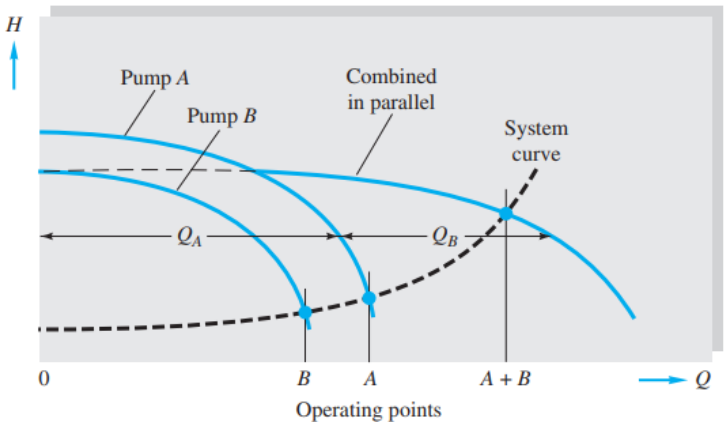


Figure 3-7: Operation point pumps in parallel [70]

Equations of motion

Given the system description of the water storage unit and the previously made assumptions. The following differential-algebraic equation describes the dynamics of draining mode with pump(s) operating at a constant rotational speed.

$$\dot{x}_1 = -\frac{x_2}{A_{res}} \tag{3-15}$$

$$g(x_1, x_2) := (a_2 - b_2) \cdot x_2^2 - x_1 + a_1 - b_1 = 0 \tag{3-16}$$

$$y = C \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = I_2 \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \tag{3-17}$$

where the differential state x_1 is the water level in m, algebraic state x_2 is the flow rate in m^3/s, and A_{res} is the cross-section of the reservoir in m^2.

Using real-time process data of the pumps in operation, the parameters a_1, a_2, b_1, and b_2 need to be identified for pumps 5 and 6 in operation singularly and for the pumps in parallel operation.

3-2-2 Changing rotational speed

If the centralised control system initiates the draining process, the pump's rotational speed is increased to its fixed nominal rotational speed. As the number of operational pumps decreases, the rotational speed of the pump decreases from its constant rotational speed to zero. Valves are positioned behind the pumps within the pipeworks of the water storage unit to prevent air from entering the pump. The specific locations of these valves can be seen in Figure 3-4. MCV_{36} opens and closes the exit of pump 5 and MCV_{37} of pump 6.

The following process describes the increase and decrease in the number of pumps in operation provided by Dunea.

Increasing number of pumps in operation:	**Decreasing number of pumps in operation:**
• Opening MCV to 10%	• Closing MCV to 40%
• Starting pump	• Stopping pump
• Opening MCV to 100%	• Close MCV to 0%

In Figure 3-8, the increasing flow rate and valve angle are shown. From this figure, it is observable that there is a delay between the pump's starting point and the first nonzero measured flow rate. This can be explained by the distance between the pump and the flow sensor and the time needed for the pump to get the rotors moving due to the moment of inertia. Figure 3-9 shows the decreasing flow rate and valve angle. From this figure, notably, the closing of the valve influences the flow rate due to increased losses. This shows that the changing valve angles and the rotational speed of the centrifugal pumps influence the flow

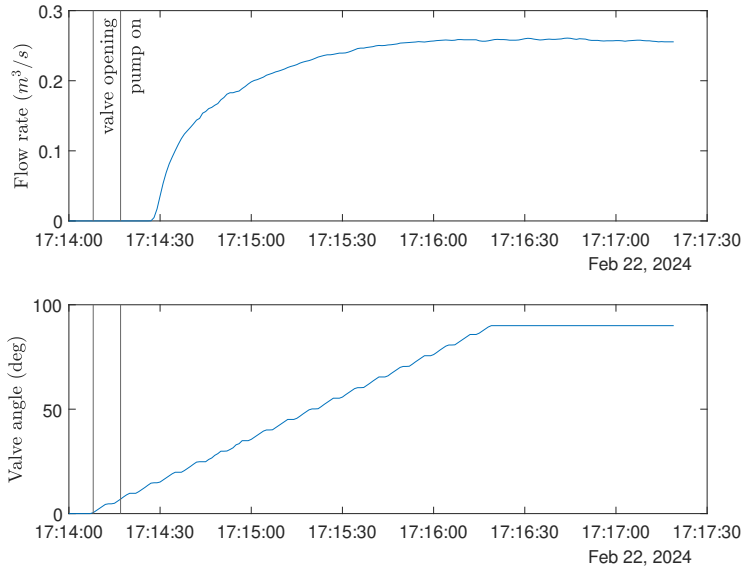


Figure 3-8: Starting draining of the reservoir. The top graph illustrates the increasing flow rate, and the bottom graph shows the valve angle. The left vertical line indicates the time instate at which the valves are opening, and the right line the first moment the pump status is on.

rate during these processes. The closing valves cause head losses in the system, leading to a decrease in flow rate. MCV_{36} and MCV_{37} are butterfly valves, and the following equation can describe the loss caused by the valve as described in the fluid mechanics by White in [70]:

$$h_{valve} = K_{valve}(\theta)\frac{Q^2}{2g \cdot A^2}, \tag{3-18}$$

where K_{valve} is the loss coefficient of the butterfly valve correlated to the valve angles θ. To help understand this correlation, in Figure 3-10, a graph with the loss coefficients of three butterfly valve vendors is provided. Here, 0 degrees indicates a closed valve and 90 degrees signifies an open valve. This graph demonstrates that the loss caused by the valve's angle increases when the angle decreases and the valve closes. Additionally, in Figure 3-11, the pump curve and H_{sys} for various valve angles are shown. Should the valve angle decrease, the operating point will shift to the left, leading to an increase in the generated pump head and a reduction in the flow rate.

For a comprehensive estimation of the impact of the valve loss coefficients on the flow rate, it is necessary to first obtain a good estimation of the system parameters under the conditions where the valves are fully open and the pump is operating at a constant rotational speed.

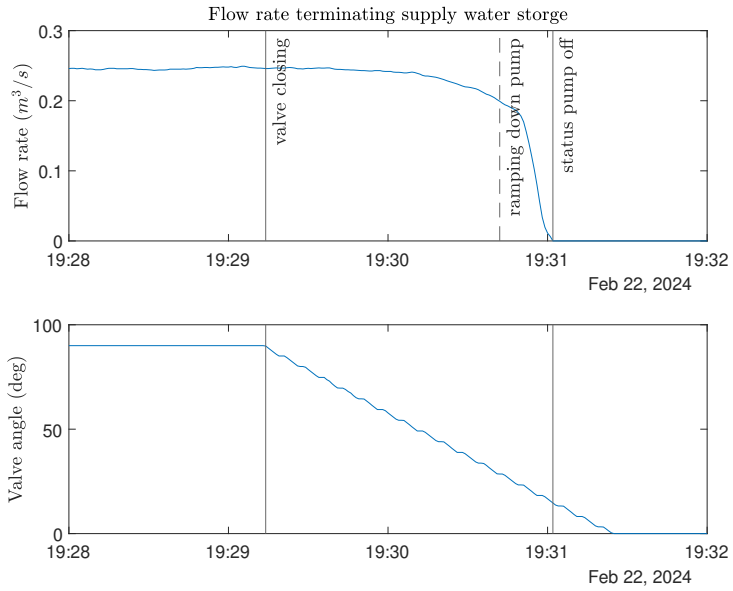


Figure 3-9: Terminating draining of the reservoir. The top graph illustrates the decreasing flow rate and the bottom graph shows the valve angle. The left continuous vertical line indicates the time the valves are closing, and the right continuous vertical line marks the first moment the pump status is off. The dashed vertical line displays the moment the pump is ramping and starting to decrease its rotational speed

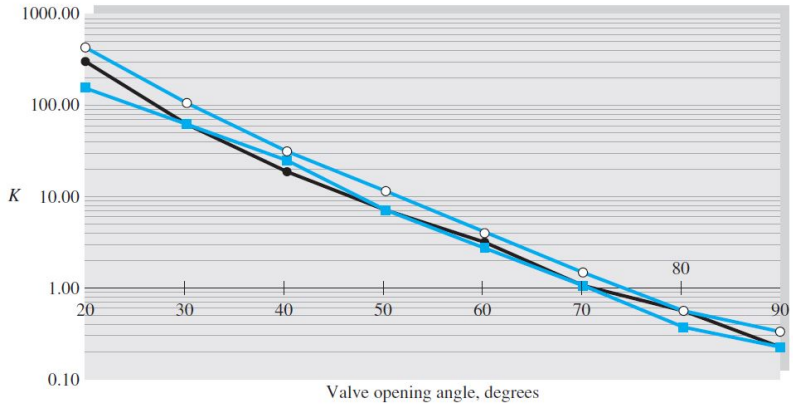


Figure 3-10: Loss coefficients butterfly valves for three different manufacturers [70]

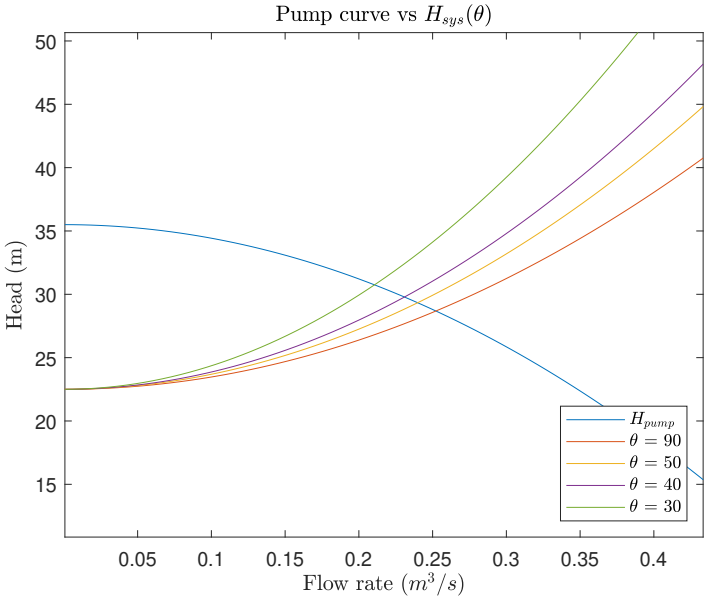


Figure 3-11: Operating point with closing valve

In subsection 3-2-1, the pump dynamics are described for a constant rotational speed. Each pump has its characteristics at specific rotational speeds. In Figure 3-12, the varying pump curves correlated to the pump's rotational speed are illustrated. This shows that when the pump's rotational speed increases, the operation point will move to the right, and the flow rate will increase.

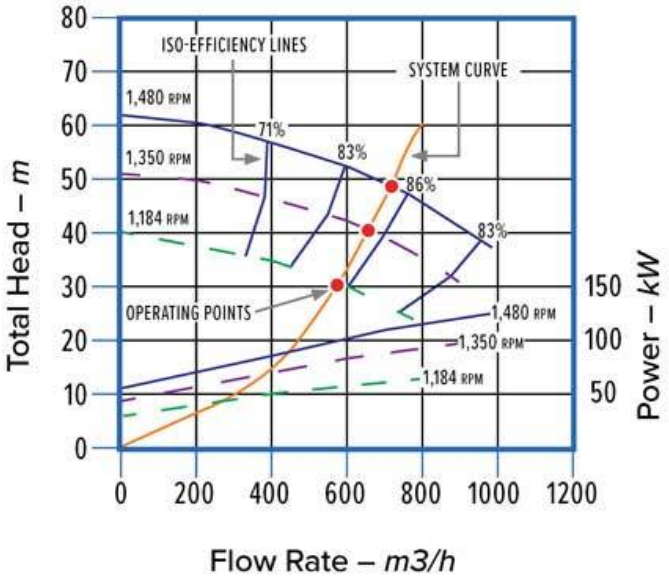


Figure 3-12: Centrifugal pump operating points at various rotational speeds [34]

In the ideal scenario, the dynamics will be modelled such that the rotational speed is the input of the draining mode. Then, the correlated pump curve will be utilised to estimate the resulting flow rate. When the signal to start the pump is given, the pump's rotational speed will increase accordingly, leading to an increase in the estimated flow rate.

Since these pump curves are not provided, estimating these functions using measurement data becomes necessary. However, this presents a complex problem for modelling dynamics of a two-minute time span within the overall average four-hour duration of the draining. Additionally, when the second pump is turned on, there is a transition from the pump characteristics of the single pump in operation to the pump curve of the pumps operating in parallel. Moreover, the shape of the H_{sys} curve is also changing due to the increase in the length of pipelines and their associated losses.

Hence, based on the available data and information, an ad hoc approach is used to model the pump dynamics when the rotational speed changes. This approach will be defined in the following section.

Equations of motion

During the initiation and termination of the reservoir drainage, the flow rate in the water storage unit is primarily influenced by the pump's rotational speed and the valves' angle.

Adding the losses caused by the butterfly valves to the SFEE described in Equation 3-9, the equation of motion will be

$$\left(\frac{p_1}{\rho g} + \frac{V_1^2}{2g} + z_1\right)_{in} = \left(\frac{p_2}{\rho g} + \frac{V_2^2}{2g} + z_2\right)_{out} + h_f + \sum h_m + h_{pump} + h_{valve}, \tag{3-19}$$

where

$$h_{valve} = K_{valve}(\theta)\frac{Q^2}{2g \cdot A_{0.4}^2}. \tag{3-20}$$

It is noted to the reader that in Equation 3-9, the minor losses of the open butterfly valve are incorporated within the term $\sum h_m$. Therefore, the loss coefficients to be identified will be the difference between the loss coefficients of the current angle and the open valve.

The dynamics of the angles of the valve whilst opening can be modelled as:

$$\theta(t) = \begin{cases} a_{\text{open}} \cdot t, & \text{for } t \leq \frac{90}{a_{\text{open}}} \\ 0, & \text{for } t > \frac{90}{a_{\text{open}}} \end{cases}, \tag{3-21}$$

where a_{open} represents the slope at which the valve is opening. The dynamics of the angles of the valve whilst closing can be modelled as follows:

$$\theta(t) = \begin{cases} 90 - a_{\text{close}} \cdot t, & \text{for } t \leq \frac{90}{a_{\text{close}}} \\ 0, & \text{for } t > \frac{90}{a_{\text{close}}} \end{cases}, \tag{3-22}$$

where a_{close} represents the slope at which the valve is closing.

Changing rpm With the absence of the pump curves at different rotational speeds, an ad hoc solution is constructed to estimate the flow rate during the change in the rotational speed of the pumps. Considering the ramping up of the pump's rotational speed, the increase in the rotational speed will increase the generated head, causing the flow rate to increase.

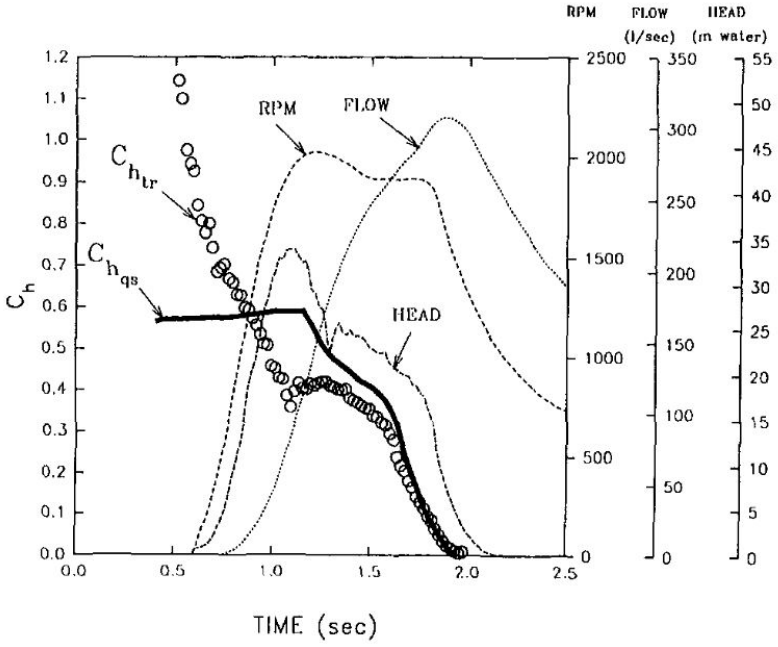


Figure 3-13: Hydrodynamic performance during low acceleration transient [40]

The increase in rotational speed can exhibit behaviour characteristics of a first-order system, as illustrated in Figure 3-13. This has an impact on the resultant flow rate as the generated pump head increases. The resulting flow rate follows the characteristics of a first-order time delay function at a lower response rate than the increase of the rotational speed. The exact response rate is dependent on the system specifications. Another possible function to describe the resulting ramping up of the rotational speed is a time-shifted sigmoid function due to the slowly increasing slope at the start of the function. This function's behaviour will mimic the behaviour of the soft starters used to start the pumps, reducing the inrush current.

However, using these functions to describe the dynamics of the increasing flow rate caused by the increasing pump head is incomplete due to the MCVs that are opening whilst the pump head is increasing. Therefore, the following equation is proposed:

$$H_{increase} = a_1 + a_2 \cdot r(t)^2 - z_1 \tag{3-23}$$

$$H_{sys} = a_1 + (a_2 + h_{valve}(\theta)) \cdot Q^2 - z_1 \tag{3-24}$$

$$H_{sys} - H_{increase} = 0, \tag{3-25}$$

where $r(t)$ is a function describing the increasing dynamical behaviour of the generated head of the pump, the function $r(t)$ can be described by a first-order time delay or a sigmoid function, the parameters of which will be identified in the next section.

The same will follow for the decrease in rotational speed. However, the decrease in the pump's rotational speed will happen when the valve angle is around a specific angle, as described by Dunea. This will probably be internally controlled at the water storage unit. However, there are no input signals available for this. Therefore, the angle at which the decrease in the pump's rotational speed is initiated will be estimated and utilised as an input signal to start the decrease in rotational speed.

To summarise, two models are derived representing the dynamics of the reservoir's draining. Considering the pump operating at constant rotational speed, the parameters will need to be identified for the pumps operating singularly and in parallel. Regarding the dynamics of the changing rotational speed, the function $r(t)$ will need to be identified and combined with the loss coefficients of the valves and the angle at which the decrease in the pump's rotational speed is initiated.

3-3 Model of the replenishing mode

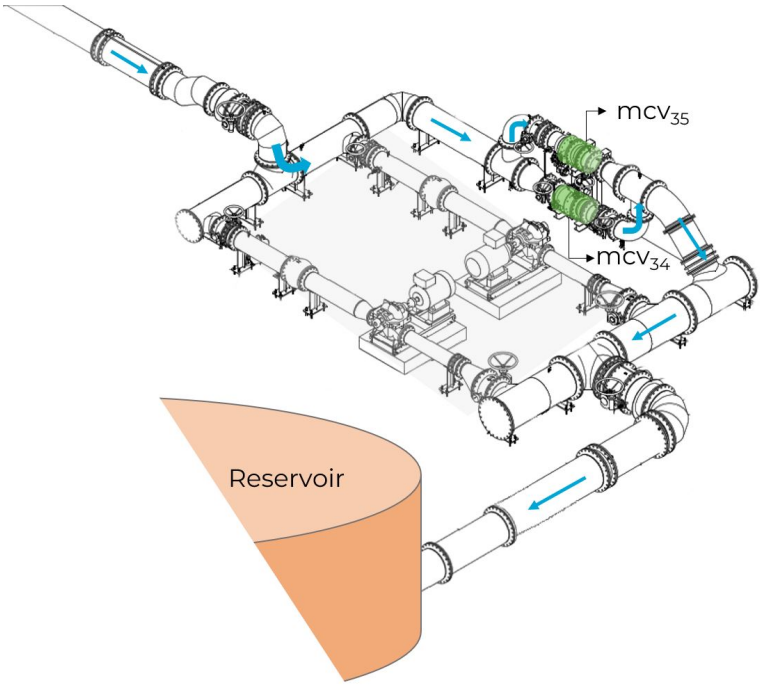


Figure 3-14: Overview components of the water storage unit involved in the replenishment of the reservoir

After characterising the equations of motions governing the draining process, the remaining mode to be modelled is the replenishing mode. Between 22:00 - 06:00, the flow rate increases with increments of approximately $250\,m^3/h$ during reservoir replenishment by increasing the angles of MCV_{36} and MCV_{37}, as shown in Figure 3-14. These processes are automated and controlled by the method of the previously described carousel. Consequently, the reservoir with the lowest volume is targeted for the next increase in flow rate. As a result, daily

variations in flow rate measurements occur, as depicted in Figure 3-15. Therefore, accurate modelling of this process is essential.

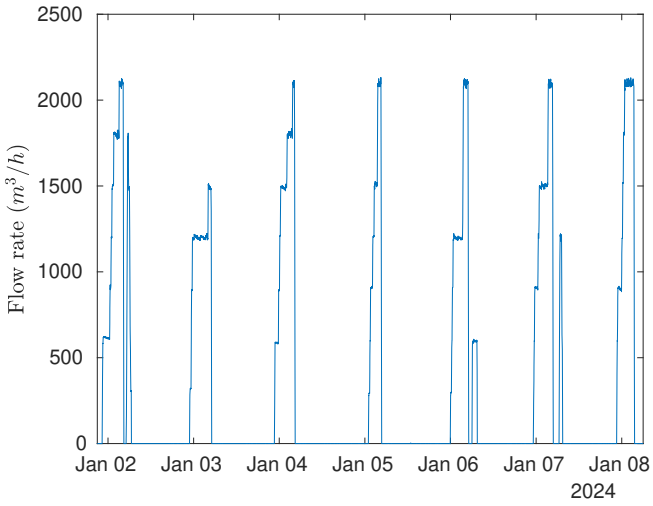


Figure 3-15: Measured flow rate of the replenishment of the reservoir.

3-3-1 Equations of motion

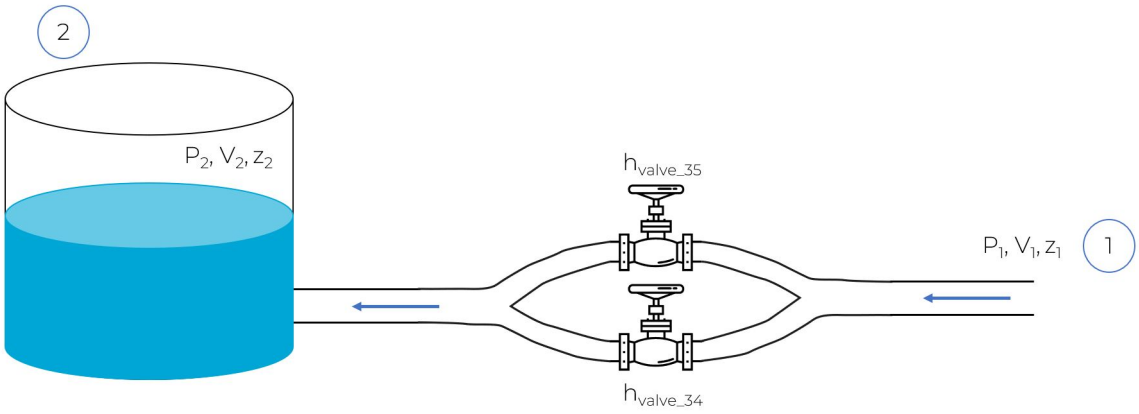


Figure 3-16: Simplified schematic representation of the pipework system utilised in the replenishment of the reservoir

Considering a simplified schematic of the pipeworks as illustrated in Figure 3-16, the SFEE can be described as follows :

$$\left(\frac{p_1}{\rho g}+\frac{V_1^2}{2g}+z_1\right)_{in}=\left(\frac{p_2}{\rho g}+\frac{V_2^2}{2g}+z_2\right)_{out}+h_f+\sum h_m+h_{valve\_34}+h_{valve\_35}. \quad (3\text{-}26)$$

Taking into account the various cross-sectional values of the pipes mentioned earlier and substituting Equation 3-7 in Equation 3-26 leads to the following equation:

$$\frac{p_1}{\rho g} + z_1 = \frac{p_2}{\rho g} + z_2 + \frac{Q^2}{2g}\Big(\frac{1}{A_{0.6}^2} + f_{0.8}(Q)\frac{L_{0.8}}{D_{0.8}}\frac{1}{A_{0.8}^2} + f_{0.6}(Q)\frac{L_{0.6}}{D_{0.6}}\frac{1}{A_{0.6}^2} + \frac{1}{4}f_{0.4}(Q)\frac{L_{0.4}}{D_{0.4}}\frac{1}{A_{0.4}^2}... + \sum K_{0.8}\frac{1}{A_{0.8}^2} + \sum K_{0.6}\frac{1}{A_{0.6}^2} + \frac{1}{4}\sum K_{0.4}\frac{1}{A_{0.4}^2}\Big) + h_{valve\_34} + h_{valve\_35}. \tag{3-27}$$

Based on the parallel positioning and equal valve angles, it is presumed that the flow is evenly distributed, as evidenced by the measurement data and illustrated in Figure 3-18. Any deviation from this assumption is expected to be minimal, with a maximum variance of only two degrees. The pipes with a diameter of 406 mm are connected to the valves, with half the flow rate passing through. As a result, a factor of $\frac{1}{4}$ is utilised to adjust the friction loss and the minor losses for this specific section.

The minimum flow present during the intake process is $250\,m^3/h \approx 0.0694\,m^3/s$. The fluid velocity within the pipe with the largest cross-section will be $0.134\,m/s$. Referring to Table 3-3, this means that within every pipe, the flow is turbulent, and Equation 3-4 can be used to calculate the friction factor. Because of the wide range of velocity the fluid will have during the intake process, the friction factor needs to be calculated for each time instant and for every pipe cross-section.

The head loss caused by the butterfly valves MCV_{34} and MCV_{35}, can be described by the following equation:

$$h_{valve} = \frac{1}{4}K_{valve}(\theta)\frac{(Q)^2}{2g \cdot A_{0.4}^2} \tag{3-28}$$

Where the loss coefficient $K_{valve}(\theta)$ increases if the valve angle θ decreases, as is shown in Figure 3-10 in subsection 3-2-2.

The parameters that should be determined are the height of the flow sensor z_1, the pipe wall roughness, ϵ, utilised in Equation 3-4 to calculate the friction factor, the total lengths of the pipes: $L_{0.4}, L_{0.6}, L_{0.8}$, the minor loss coefficients: $K_{0.4}, K_{0.6}, K_{0.8}$ and the loss coefficients of the butterfly valves MCV_{34} MCV_{35}.

3-3-2 Setpoint influence

The replenishment model takes the setpoint of the FCVs as input. The valves MCV_{34} and MCV_{35} are flow-controlled valves, receiving setpoints labelled as ams_{34} and ams_{35} from the centralised control unit. As clearly illustrated in Figure 3-17, the setpoints for both valves are identical. Based on the setpoints, the valve angles increase and decrease by 0.99 degrees per time step. Figure 3-18 illustrates the setpoints and the valve behaviour, while Figure 3-19 displays the measured angles of MCV_{34} showing a constant step size, except for the first step.

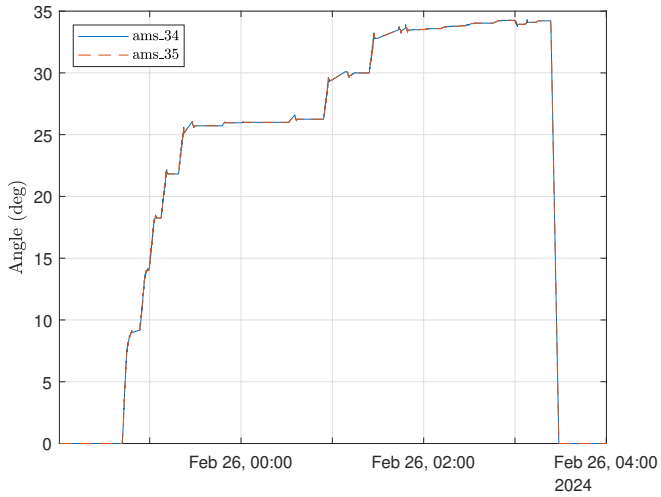


Figure 3-17: The setpoint ams_{34} of MCV_{34} is plotted in blue and ams_{35} of MCV_{35} in red.

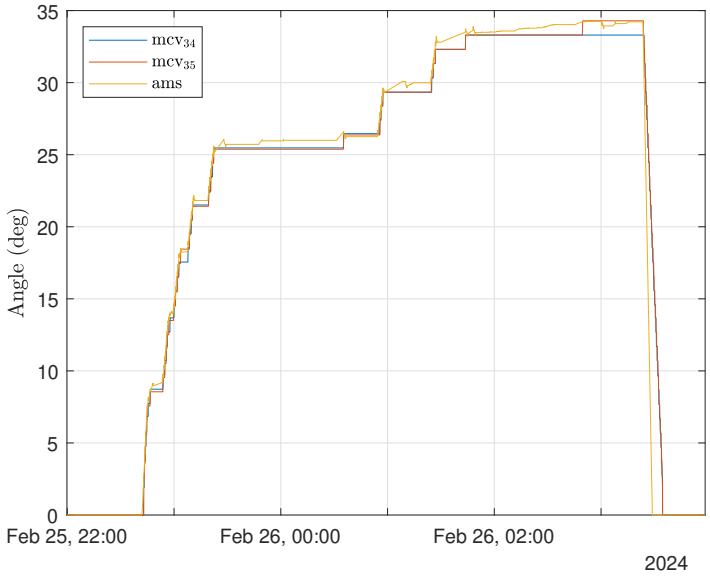


Figure 3-18: The setpoint of the valves is shown in yellow, and the corresponding valve angles are shown in blue and red for MCV_{34} and MCV_{35}.

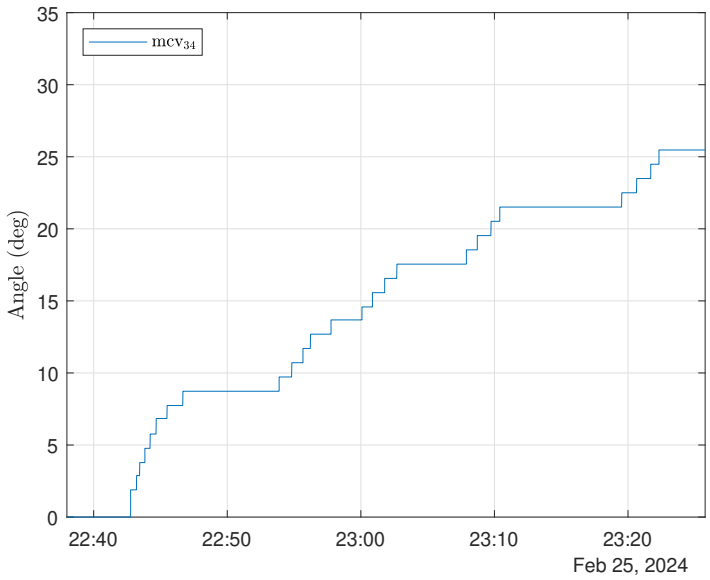


Figure 3-19: Valve angle of MCV_{34}

In Figure 3-20, it is notable that the setpoint of the valve is decreasing at a higher rate than the valves actually close.

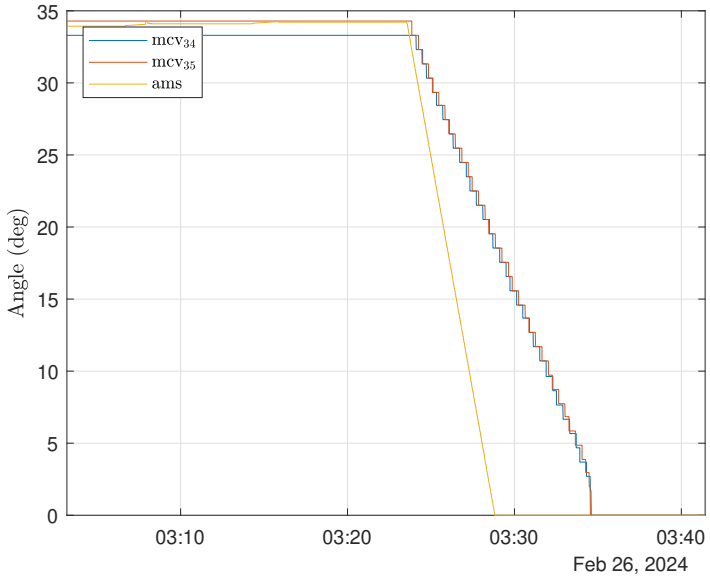


Figure 3-20: Closing the valve with a decreasing setpoint visualised in yellow and the measured valve angles in red and blue regarding MCV_{34} and MCV_{35}

The graphs above are created using data with a sampling time of 1 second. Eventually, the intake dynamics will be modelled with data with a sampling time of 1 minute. Therefore, the valve angle could increase with two steps of 0.99 degrees within a minute. Considering the

closing of the valves, the angle decreases with approximately three steps of 0.99 degrees within a minute, thus 2.97 degrees per minute. Given these observations, the following dynamics are derived to estimate the valve angles of MCV_{34} and MCV_{35}.

$$\theta(t) = \begin{cases} \theta(t-1) + 0.99, & \text{if } r(t) - (\theta(t-1) + 0.99) > -0.1 \\ \theta(t-1) + 1.98, & \text{if } r(t) - (\theta(t-1) + 1.98) > 0 \\ \theta(t-1) - 2.97, & \text{if } r(t) - r(t-1) < 4 \ \wedge \ r(t) - (\theta(t-1) - 2.97) < 0 \\ 0, & \text{if } r(t) - r(t-1) < 4 \vee r(t) = 0 \ \wedge \ \theta(t) < 6 \\ \theta(t-1), & \text{else} \end{cases} \tag{3-29}$$

Employing the dynamics described in Equation 3-29, the estimated valve angles given the setpoint with a sampling time of 60 seconds are shown in Figure 3-21. It can be observed from the graph that the estimated valve angles approximate the measurements successfully. However, at higher angles, there is a noticeable time lag in the increase of valve angles between the two measured valve angles. In contrast, the estimated angles increase almost simultaneously due to the small difference in the initial valve angle.

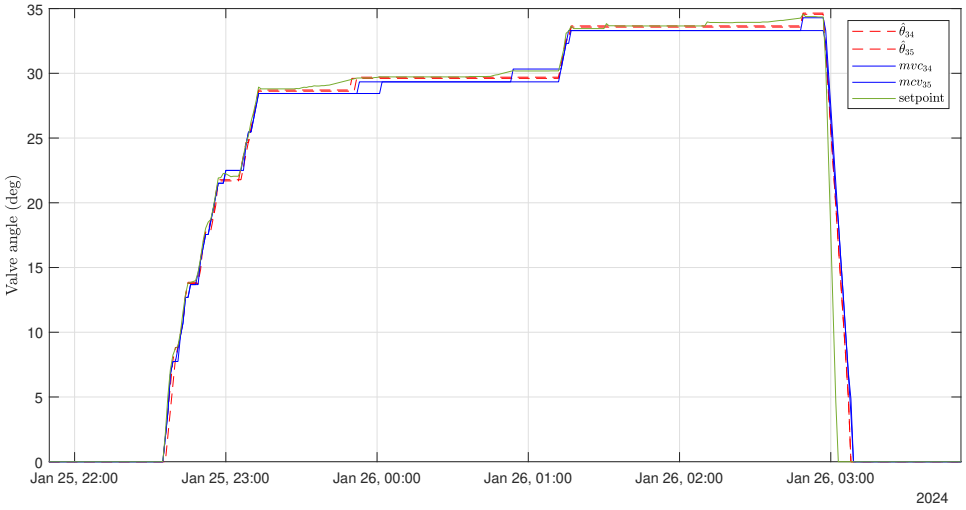


Figure 3-21: Simulation estimated valve angles given the valve setpoints. The setpoint is illustrated in green. The estimated valve angles are shown in red and the measured ones in blue.

3-4 System identification

The dynamics of the water storage unit can be described by three distinct modes: the idle state, replenishing, and draining of the reservoir. Each mode has its own set of equations of motion, derived along with the system parameters to be identified. This section outlines the data and methods used to identify these parameters. The sequential identification process ensures that the identified parameters can be utilised for subsequent identification tasks.

Initially, the parameters of the pumps operating at a constant rotational speed during the draining mode are identified. These obtained parameters are then used to identify the loss coefficients associated with the closing valves while the pumps operate at constant rotational speed. Following this, parameters characterising the effects of decreasing rotational speed and closing of the valves are identified. Thereafter, the parameters of the lower valve angles during the valve opening and the characteristics of the increasing flow rate due to increasing pump head are identified. Finally, parameters for the replenishing mode are identified, using the obtained loss coefficients for the butterfly valves as an initial guess. The performance of simulations using the identified system parameters will be assessed using performance metrics such as Variance Accounted For (VAF) and Mean Squared Error (MSE), as described in Equation 3-30:

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2, \quad \text{VAF} = \left(1 - \frac{var(y_i - \hat{y}_i)}{var(y_i)}\right) \cdot 100\%, \tag{3-30}$$

where n is the number of samples, y_i is the i-th measurement and $\hat{y}_i$ the corresponding estimation.

3-4-1 Data for system identification and validation

The volume and flow rate measurements are used to identify the dynamics in the draining mode while the pump is operating at constant rotational speed. The data utilised for the training and validation contains a sampling time of 5 minutes. In Table A-1 in the Appendix, the specific data set utilised is listed. Regarding the data utilised for the identification and validation of the pumps in operation, singularly, only data is used where no additional pump has been on within that same period of draining. The available data has been split up such that there are seven moments for the training data where pumps 5 is on singularly and six for pump 6. For the validation, there are five and four instants regarding pumps 5 and 6, respectively. With regards to the data for the pumps operating in parallel, this split has been made approximately 50% for training and 50% for validation. Providing a balance to train on a representative sample of data and also validating the identified parameters against a sizable set. In Figure 3-22, the data used to identify the dynamics of the system parameters when pump 5 is singularly in operation is shown. The measured flow rate and reservoir volume correlation are shown in Figure 3-23. The data used for pump 6 singularly and the pumps in parallel are shown in Appendix A-2-1.

The data used for the system identification of the dynamics in the draining mode while the pump's rotational speed is changing are the volume measurements, flow rate and valve angles of MCV_{36} and MCV_{37}. Since the duration of the dynamics operating in this mode has a maximum length of three minutes, the data with a sampling time of one second chosen to be used for the identification of this part of the dynamics. Dunea kindly provided five data sets that capture the 24-hour dynamics of the water storage unit. Since the DCS data has a sampling time of one second, it is important to note that only the most recent 24 hours of data are available. Regarding the increasing and decreasing rotational speed of the pump, with the exception of pump 5's speed increase, two data sets are utilised for the training and one for the validation. In the case of pump 5's speed increase, three data sets are utilised. In Appendix A-2-2, the employed training data is depicted.

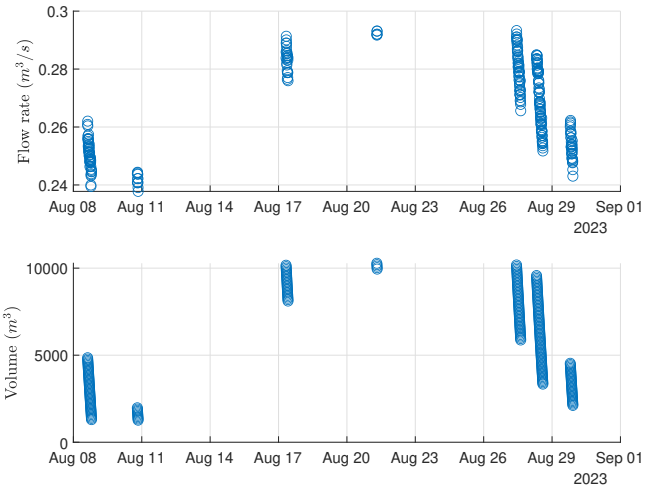


Figure 3-22: Identification data pump 5

The data employed for the system identification of the dynamics in the replenishing mode are the volume, flow rate, angles of MCV_{34} and MCV_{35} and the pressure measurements. The data is sampled every minute, which is preferred over the sampling interval of 5 minutes. Because the setpoints of the MCVs can change rapidly within 5 minutes, the data with one-minute time intervals contains more information. The training data of the flow rate and valve angles used for the identification is visualised in Figure 3-24. To clarify the behaviour of various parameters, the data for a specific period is shown in Appendix A-2-3 for the flow rate, valve angles, volume and pressure. Regarding the training and validation of the replenishing dynamics, two data sets with approximately the same amount of data points were utilised for both training and validation. Both data sets consist of multiple weeks of process data and provide various patterns in valve angles for the training and validation of the parameters.

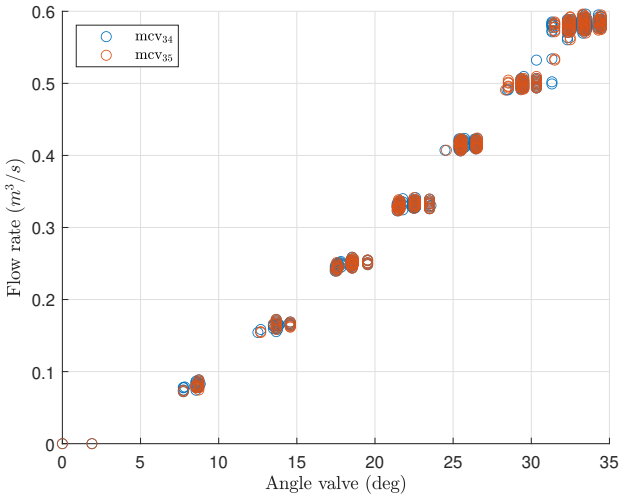


Figure 3-24: Training data steady-state flow plotted versus the valve angles of MCV_{34} in blue and MCV_{35} in red

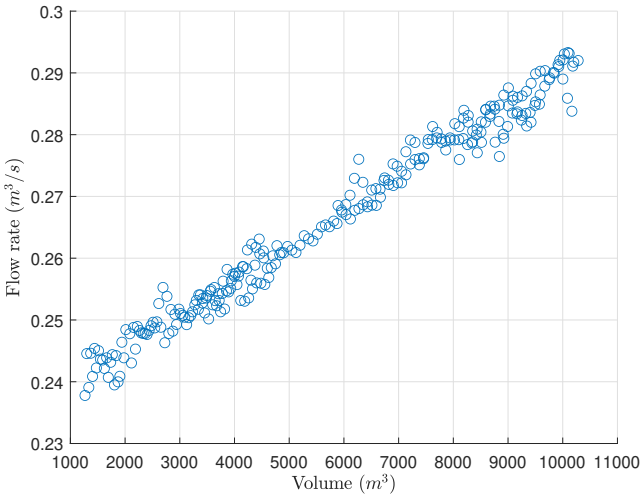


Figure 3-23: Correlation volume and flow training data pump 5

Data pre-processing

The data provided by Dunea must undergo unit changes in order to be incorporated into the model. The following unit changes are used:

- Angle from percentages to degrees
- Reservoir volume to water level, taking the bottom of the reservoir as level 0
- Flow rate from m^3/h to m^3/s
- Pressure from m water column to Pa

The data for the training of the draining at constant rpm with the pumps operating at parallel is selected by first collecting all the paired indices where the flow rate exceeds $0.33\,m^3/s$. Subsequently, the beginning of the constant rpm dataset is indicated when the slope falls below $5.55 \cdot 10^{-3}$. Analysis of the measurement data reveals that the slope increases by approximately 0.037 when the rotational speed is increased. Due to the turbulent flow, the flow rate can have a minor increase when operating at constant rotational speed; therefore, the value is chosen to be a positive number and not zero. Lastly, the end of the constant rpm data set is indicated when the slope exceeds the value of 0.014. Where the decrease in flow rate during the constant rational speed is approximately between 0 and 0.0055, and the decrease in flow rate when the pumps decrease their rotational speed is approximately 0.022.

In order to create a training data set with steady state data for the replenishing mode, it has been chosen to select the data based on the flow measurements. Because the change in valve angle can delay the measured flow rate, and in the case of higher flow rates, where the volume of the reservoir is higher, the valve angles are changed to maintain the same flow rate. The training data set is created by selecting the flow rate measurements based from the provided process data on whether the slope is less than 0.0055 between two data points, taking into account fluctuations due to the turbulent flow studied in the measurement data. Moreover,

the flow rate difference with the data point 5 minutes prior should not exceed $0.014\,m^3/s$, as this would indicate an increase in flow rate caused by the change in setpoint.

3-4-2 Identification methods

Identifying the system parameters can be seen as a grey box system identification problem. Since fluid mechanics knowledge provides information on the model structure, only the magnitude of specific parameters needs to be identified. Two algorithms are used to solve this optimisation problem and estimate the system parameters. One of them is nonlinear least-squares using the Interior Point (IP) algorithm solving nonlinear least-squares curve fitting problem, which can be formulated as:

$$\min_{\theta} ||f(x,\theta)||_2^2 = \min_{\theta} \sum_{i=1}^{n} (y_i - \hat{y}_i(x,\theta))^2 \tag{3-31}$$

Additionally, the MATLAB function `fmin` is used to find the minimum of the following objective function:

$$\min_{\theta} f(x) = \frac{1}{N} \sum_{i=1}^{N} ||y_i - \hat{y}_i(x,\theta)||^2, \tag{3-32}$$

where $\hat{y}(x,\theta)$ is the estimated output given the optimised parameters θ. The minimisation problem is solved using the Quasi-Newton numerical optimisation algorithm for the draining dynamics at constant rotational speed. For the draining dynamics at changing rotational speed and the replenishment dynamics, the Sequential Quadratic Programming (SQP) optimisation method is used because it is an iterative and constrained nonlinear optimisation method.

The loss coefficients of the MCVs are identified for the angles ranging from 0 to 80 degrees with intervals of 10. This process involves interpolation to find the loss coefficient corresponding to the given angle. The commonly used interpolation methods are linear, spline cubic and modified Akima piecewise cubic Hermite interpolation methods (Makima). The latter two methods are capable of handling non-linearities.

As the valve angles increase within the specified interval, the loss coefficients exhibit a decreasing trend. Therefore, it is essential to ensure that the interpolated loss coefficient values do not increase with the valve angle. To address this, linear and Makima interpolations are utilised to determine the system parameters.

Makima is selected alongside linear interpolation due to their differing characteristics. The aim is to evaluate various interpolation techniques to determine the most accurate approximation for modelling the system's nominal dynamics.

3-4-3 Draining mode

Given the derived equations of motion and the provided process data from the water storage unit of the Leyweg, this section is dedicated to identifying the parameters for the draining mode. Firstly, the parameters for the dynamics at constant rotational speed need to be

determined for pumps 5 and 6, both individually and in parallel. Secondly, the ramping down of the pump will be determined, considering the effect of closing the valves before the pump is shut down, and subsequently identifying the characteristics of the decreasing rotational speed. Lastly, the dynamics of the increasing rotational speed will be determined.

Constant rotational speed

Utilising the volume, the flow rate will be estimated, and subsequently, given the flow rate measurements and estimation, the cost function will be minimised. For all the cases of the constant rotational speed, the parameters $\mathbf{x} = \begin{bmatrix} a_1, & a_2, & b_1, & b_2 \end{bmatrix}$ are estimated to optimise the cost function to represent the dynamics proposed in Equation 3-15.

The initial parameters utilised are: $\mathbf{x}_0 = \begin{bmatrix} 20, & -10, & 5, & 10 \end{bmatrix}$, such that given the range of the water level, the intersection of the pump curve and H_{sys} will be around $0.25\,m^3/s$.

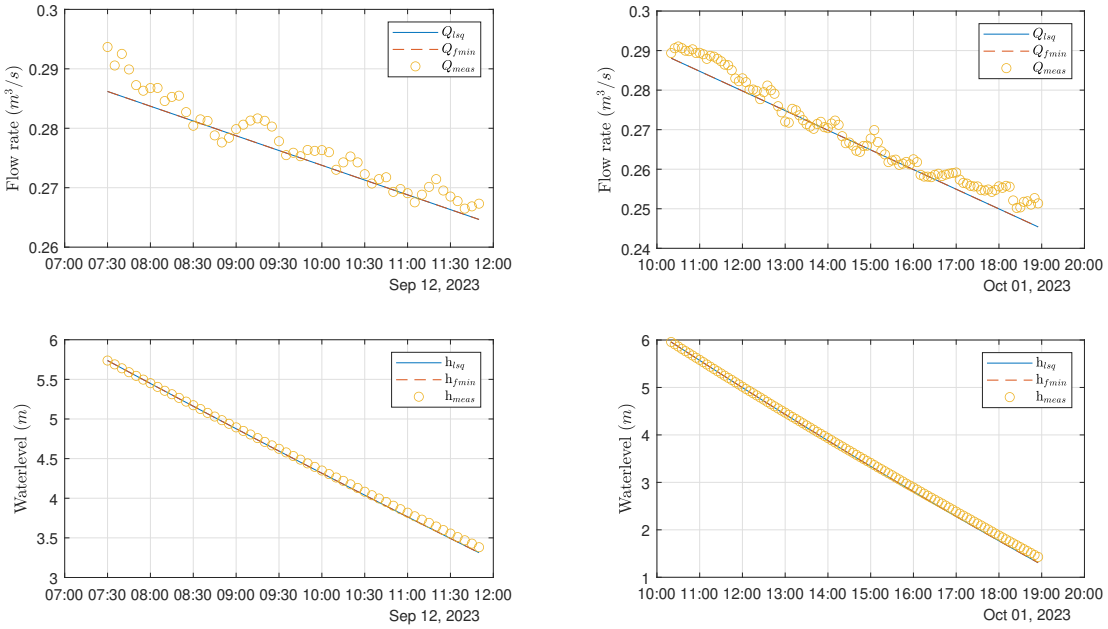
Obtained parameters The obtained parameters using multiple optimisation algorithms for the different scenarios are presented in Table 3-4.

Scenario	a_1	a_2	b_1	b_2
Pump_005 QN	-97.50	87.50	34.95	25.05
Pump_005 IP	-95.43	89.56	38.80	28.90
Pump_006 QN	$-1.07 \cdot 10^2$	97.18	35.497	24.496
Pump_006 IP	$-1.07 \cdot 10^2$	97.18	35.501	24.499
Parallel QN	-18.36	28.36	32.11	22.89
Parallel IP	-4.77	41.96	53.98	44.77

Table 3-4: Obtained system parameters pump dynamics constant rotational speed

Validation The pump dynamics and the reservoir's water level decay given the initial measured volume as in Equation 3-15 with the identified parameters are simulated, and a magnitude plot is shown in Figure 3-25a, Figure 3-25b and Figure 3-26 for the pumps 5 and 6 singly and combined in parallel, respectively. In Table 3-5, the performance of the estimated flow rate Q and water level h is provided.

Based on the measurement data and the fundamentals of fluid mechanics, it is evident that the flow decreases proportionally with the water level. Moreover, the flow rate measurements exhibit fluctuations due to the turbulent flow, characterised by rapid and random variations in velocity and pressure. The Figures illustrate that the estimations accurately align with the average measurements, confirming that the average pressure p_2 is accurately identified. This is evident in the estimation performance for each case and optimisation method, where the % VAF is significantly high. The estimations utilising the identified parameters with the two distinct optimisation methods show the same performance, indicating that both methods have successfully achieved an optimum solution. This lays the foundation for identifying the remaining dynamics of the draining mode.



(a) Pump 5 **(b)** Pump 6

Figure 3-25: Validation pump dynamics at constant rotational speed for the pump's operation singularly. The top graphs show the flow rate, and the bottom graphs show the water level. The measurements are scattered in yellow. The simulated values using the identified parameters using IP are denoted in blue, and the parameters using Quasi Newton (QN) are in the red dashed line.

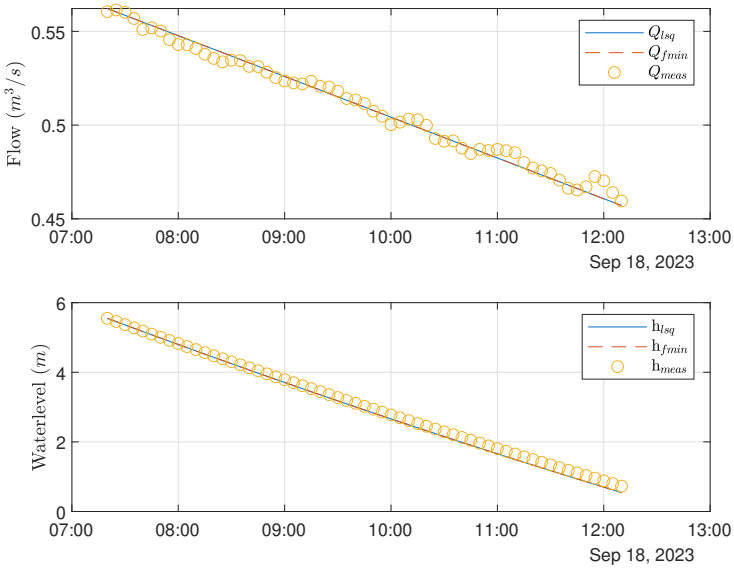


Figure 3-26: Validation pump dynamics combined in parallel. The top graph shows the flow rate, and the bottom graph shows the water level. The measurements are scattered in yellow. The simulated values using the identified parameters using IP are denoted in blue, and the parameters using QN are in the red dashed line.

	VAF Q	MSE Q	VAF h	MSE h
Pump_005 QN	95.56 %	$9.81{\cdot}10^{-6}$	99.95 %	0.0024
Pump_005 IP	95.56 %	$9.81{\cdot}10^{-6}$	99.95 %	0.0024
Pump_006 QN	97.22 %	$6.15{\cdot}10^{-6}$	99.92 %	0.0062
Pump_006 IP	97.22 %	$6.15{\cdot}10^{-6}$	99.92 %	0.0062
Parallel QN	95.92 %	$3.05{\cdot}10^{-5}$	99.87 %	0.0073
Parallel IP	95.92 %	$3.05{\cdot}10^{-5}$	99.87 %	0.0073

Table 3-5: Performance flow estimation and water level estimation pump operating at constant rotational speed.

Decreasing rotational speed

During the termination of the pump's draining, the valve first starts to close, and when the valve reaches a specific yet-to-be-identified angle, the rotational speed of the pump starts decreasing. As described in section 3-2-2, two different functions are used to estimate the decrease in pump head as a response to the changing behaviour of the pump's rotational speed. Regarding the decrease of the pump head, the following two equations are used for the time-delayed sigmoid function and first-order time-delayed function, respectively and are illustrated in Figure 3-27:

$$r(t) = K\left(1 - \exp\frac{t - t_{pump\_off} - \delta \cdot \tau}{\tau}\right) \tag{3-33}$$

$$r(t) = K \cdot \exp\left(\frac{-(t - t_{pump\_off})}{\tau}\right), \tag{3-34}$$

where the parameter δ in the sigmoid function denotes the shift of the function and is determined as $\delta = 8$, such that $r(0) < 1 \cdot 10^{-6}$ and $r(0.1) > 1 \cdot 10^{-4}$. Furthermore, the parameter K is determined by the flow rate at the start of the transition from constant to changing rotational speed. Additionally, t_{pump_off} refers to the time instant where $\theta(t) < \theta_{off}$ holds for the first time.

For the identification, the measurement data of the valve angles, flow rate and volume sampled at one second are used. Firstly, the loss coefficients of the valves while the pump is operating at constant rotational speed are identified. Consequently, the loss coefficients of the lower valve angles and the parameters describing $r(t)$ are identified. The following equation denotes the estimation of the closing of the MCVs:

$$\theta(t) = \begin{cases} 90 - a \cdot t, & \text{for } t \leq \frac{90}{a} \\ 0, & \text{for } t > \frac{90}{a} \end{cases}. \tag{3-35}$$

Estimation loss coefficients constant rmp The parameter K_{valve} in Equation 3-28 is identified regarding the estimation of the loss coefficients whilst the pump is in full operation. The loss coefficients for an array of valve angles are identified, namely:
$\theta = \begin{bmatrix} 0, & 10, & 20, & 30, & 40, & 50, & 60, & 70, & 80 \end{bmatrix}^T$.

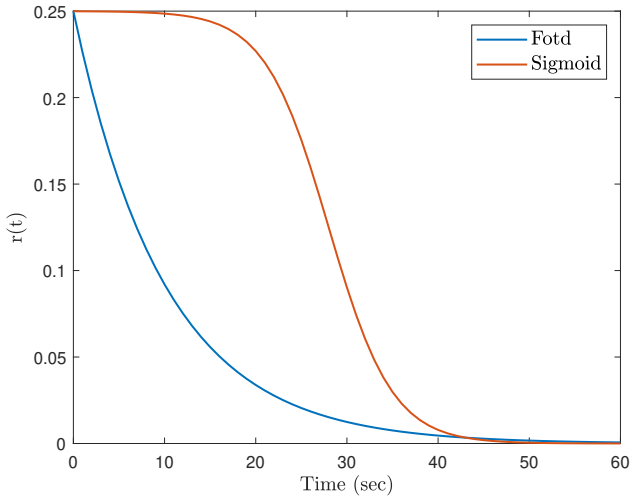


Figure 3-27: The function $r(t)$ for the decreasing pump head modelled as a first-order response denoted in blue and a sigmoid function in red

The current loss coefficients are estimated using linear interpolation and Makima as an interpolation option. Resulting in the following parameters are being optimised for:
$\mathbf{x} = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & K_{50}, & K_{60}, & K_{70}, & K_{80} \end{bmatrix}^T$.

For each parameter x_i, the bounds are specified as $x_{\text{lb},i} \leq x_i \leq x_{\text{ub},i}$ The lower and upper bounds are denoted by:

$\mathbf{x}_{\text{lb}} = \begin{bmatrix} 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0 \end{bmatrix}^T$,

$\mathbf{x}_{\text{ub}} = \begin{bmatrix} 6000, & 6000, & 6000, & 6000, & 6000, & 6000, & 6000, & 1000, & 50 \end{bmatrix}^T$.

The following constraints are applied to the optimisation problem to ensure the loss coefficients decrease as the valve angles increase:

$$\begin{bmatrix} x_1 \geq x_2, & x_2 \geq x_3, & x_3 \geq x_4, & x_4 \geq x_5, & x_5 \geq x_6, & x_6 \geq x_7, & x_7 \geq x_8, & x_8 \geq x_9 \end{bmatrix}^T.$$

The parameters are optimised using non-linear least squares with the optimisation algorithm IP, using the identified system and pump curve parameters optimised by the same algorithm in the previous section. The other optimisation method is SQP with the MATLAB function `fmincon`, using the identified system and pump curve parameters optimised by the Quasi-Newton optimisation method. Both methods use the same constraints, bounds and initial guess. The initial guess is:

$\mathbf{x}_0 = \begin{bmatrix} 1000, & 300, & 80, & 48, & 30, & 15, & 4, & 1.5, & 0.5 \end{bmatrix}^T$.

The initial guesses of the loss coefficients are chosen by the loss coefficients defined in Figure 3-10.

Estimation ramping down rotational speed For the estimation of the ramping down process of the pump dynamics, only the loss coefficients of the lower valve angles are identified,

together with τ representing the speed of decrease and θ_{off} the estimated angle at which the pump will be shut down. The identified loss coefficients for the higher valve angles will be part of the dynamics. The following parameters will be identified:

$$\mathbf{x} = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & \tau, & \theta_{off} \end{bmatrix}^T.$$

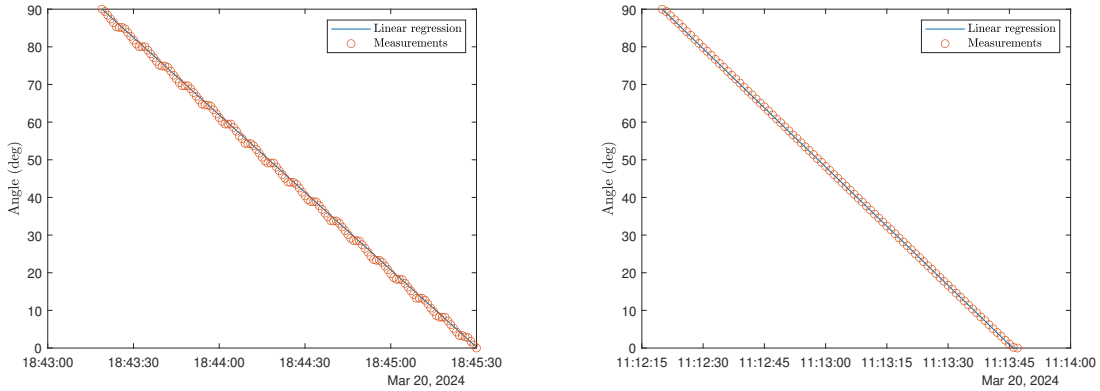
For each parameter x_i, the bounds are specified as $x_{\text{lb},i} \leq x_i \leq x_{\text{ub},i}$ The lower and upper bounds are denoted by:

$$\mathbf{x}_{\text{lb}} = \begin{bmatrix} 0, & 0, & 0, & 0, & 0, & 0, & 10 \end{bmatrix}^T,$$
$$\mathbf{x}_{\text{ub}} = \begin{bmatrix} 6000, & 6000, & 6000, & 6000, & 6000, & 1000, & 50 \end{bmatrix}^T,$$

with the constraints: $\begin{bmatrix} x_1 \geq x_2 \\ x_2 \geq x_3 \\ x_3 \geq x_4 \\ x_4 \geq x_5 \\ x_5 \geq K_{50} \end{bmatrix}$.

The obtained parameters for K_0, K_{10}, K_{20}, K_{30}, K_{40} for each optimisation algorithm are used as initial guesses. For the identification of the characteristics of $r(t)$, the following initial parameters are used: $\begin{bmatrix} \tau_0, & \theta_{off\_0} \end{bmatrix}^T = \begin{bmatrix} 1.5, & 29 \end{bmatrix}^T$, where τ_0 is determined by the decreasing flow rate.

Obtained parameters Utilising linear regression, the obtained parameters for the dynamics of the MCVs are $a = 0.6852$ and $a = 1.0482$ for MCV_{36} and MCV_{37} respectively. The validation of the obtained parameters is illustrated in Figure 3-28. Notably, for MCV_{36}, there is still some unmodelled behaviour of the valve since the valve closes stepwise. This results in a relatively higher MSE than for MCV_{37}, which can be seen in Table 3-6



(a) MCV_{36} **(b)** MCV_{37}

Figure 3-28: Validation slope closing MCVs with the measurements denoted in red circles and the estimated valve angle obtained by linear regression in blue.

	MCV_{36}				MCV_{37}			
	SQP_l	IP_l	SQP_m	IP_m	SQP_l	IP_l	SQP_m	IP_m
K_0	1000	1001	1000	1001	1000	1000	1000	999.98
K_{10}	300	300.17	299.98	300.15	300	300.10	299.99	300.91
K_{20}	80	80.95	80.63	81.63	80	80.56	80.18	45.02
K_{30}	24.05	24.05	24.78	24.79	37.93	29.19	40.07	29.40
K_{40}	10	10.01	10.60	10.60	10.08	12.98	10.90	13.77
K_{50}	2.53	2.53	2.82	2.82	6.13	7.11	7.38	7.25
K_{60}	0.38	0.38	0.58	0.28	4.96	3.74	3.44	3.98
K_{70}	$7.59{\cdot}10^{-13}$	$1.20{\cdot}10^{-7}$	$6.31{\cdot}10^{-13}$	$1.26{\cdot}10^{-5}$	1.61	2.62	2.16	2.55
K_{80}	$4.06{\cdot}10^{-14}$	$3.81{\cdot}10^{-8}$	$4.06{\cdot}10^{-14}$	$3.32{\cdot}10^{-6}$	1.54	2.15	1.83	2.10

Table 3-7: Obtained parameters identification loss coefficients butterfly valves during constant rotational pump speed. Here, l denotes linear interpolation, and m denotes maxima interpolation for the valve's loss coefficients.

	VAF	MSE
a_{36}	99.97 %	$4.98{\cdot}10^{-1}$
a_{37}	100 %	$4.15{\cdot}10^{-2}$

Table 3-6: Performance validation slope closing MCV_{36} and MCV_{37}

The obtained parameters for the two optimisation algorithms and two interpolation options for both MCV_{36} and MCV_{37} are denoted in Table 3-7. From Table 3-8 and the obtained parameters, it becomes evident that there is no significant difference in performance between the Makima and linear interpolation methods. Therefore, only linear interpolation will be used to identify the remaining parameters of the dynamics describing the rotational speed of the pumps.

	MCV_{36}		MCV_{37}	
	VAF	MSE	VAF	MSE
SQP_lin	99.05 %	$4.42{\cdot}10^{-6}$	96.34 %	$1.05{\cdot}10^{-5}$
IP_lin	99.05 %	$4.42{\cdot}10^{-6}$	99.08 %	$3.66{\cdot}10^{-6}$
SQP_mak	98.94 %	$5.51{\cdot}10^{-6}$	96.58 %	$9.74{\cdot}10^{-6}$
IP_mak	99.05 %	$4.38{\cdot}10^{-6}$	99.13 %	$3.39{\cdot}10^{-6}$

Table 3-8: Performance validation loss coefficients butterfly valves during constant rotational speed.

The obtained parameters regarding the loss coefficients for the angles between 0 and 40 degrees using linear interpolations and $r(t)$ for the decreasing pump head modelled as a first-order time delay response are shown in Table 3-9. The obtained parameters regarding the loss coefficients for the angles between 0 and 40 degrees using linear interpolations and $r(t)$ for the decreasing pump head modelled as a sigmoid function are shown in Table 3-10.

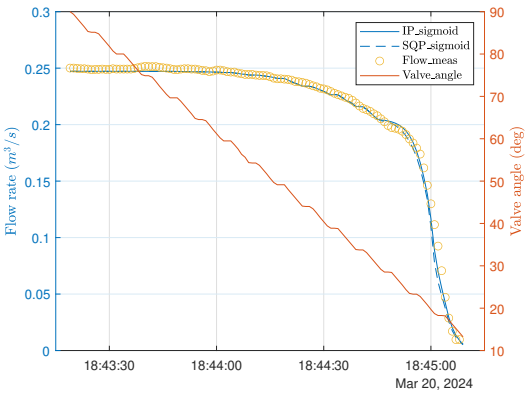
	MCV_{36}		MCV_{37}	
	SQP	IP	SQP	IP
K_0	1000	1021	1000	6000
K_{10}	307.03	1021	312.10	311.06
K_{20}	49.48	14.89	12.45	18.36
K_{30}	10.01	14.89	12.45	18.36
K_{40}	10.01	11.97	12.45	15.63
τ	134.15	36.47	51.45	45.02
θ_{off}	35	31.05	35	32.08

Table 3-9: Obtained parameters identification loss coefficients low angles and parameters for $r(t)$ as first-order time delay.

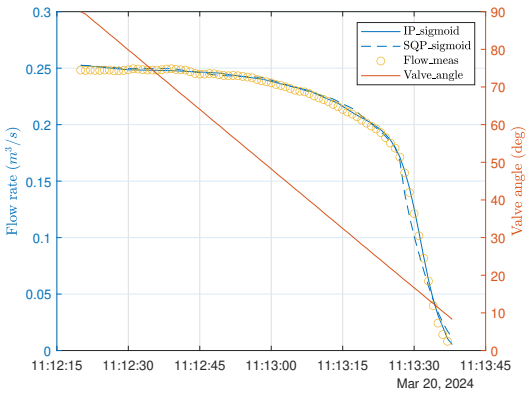
	MCV_{36}		MCV_{37}	
	SQP	IP	SQP	IP
K_0	1000	1002	1000	1002
K_{10}	300.96	165.29	298.47	52.92
K_{20}	26.11	24.00	40.36	37.85
K_{30}	22.90	23.98	23.36	26.71
K_{40}	10.02	10.01	14.18	13.56
τ	2.88	2.75	2.57	2.20
θ_{off}	35	34.36	35	34.26

Table 3-10: Obtained parameters identification loss coefficients low angles and parameters $r(t)$ as sigmoid time delay.

The loss coefficients identified with the provided valve angles and volume, along with the simulated decrease in pump output using the sigmoid function, are shown for pumps 5 and 6 in Figure 3-29a and Figure 3-29b respectively. Similarly, the identified loss coefficients simulated with the provided valve angles and volume, along with the simulated decrease in pump output using the first-order time delay function, can be seen for pumps 5 and 6 in Figure 3-30

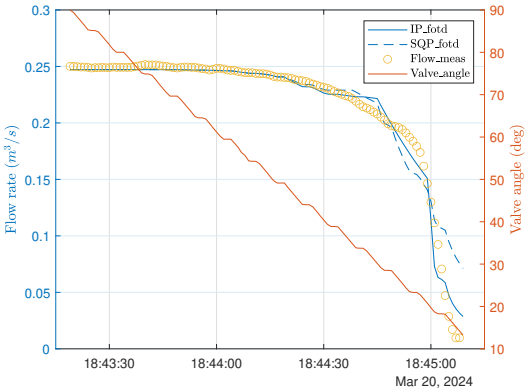


(a) Estimation flow rate pump 5 using the identified loss coefficients of MCV_{36}.

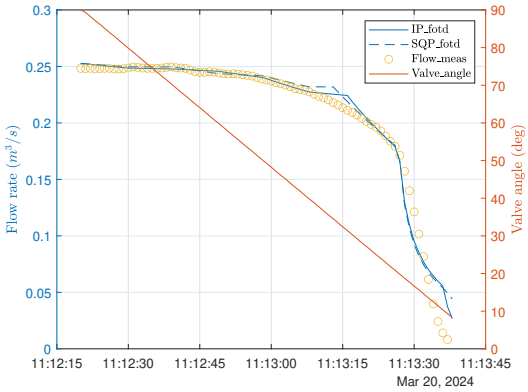


(b) Estimation flow rate pump 6 using the identified loss coefficients of MCV_{37}.

Figure 3-29: Result flow rate estimation by simulating $r(t)$ as sigmoid function using linear interpolation for the loss coefficients of MCVs. The left y-axis denotes the flow rate. The continuous blue line represents the estimated flow rate utilising IP-optimised parameters, while the dashed blue line represents the estimated flow rate using SQP-optimised parameters. Yellow circles visually represent the measurements. The right y-axis denotes the valve angle, with orange the measured valve angle is illustrated.



(a) Estimation flow rate pump 5 using the identified loss coefficients of MCV_{36}.



(b) Estimation flow rate for pump 6 using the identified loss coefficients of MCV_{37}.

Figure 3-30: Result flow rate estimation by simulating $r(t)$ as first-order time delayed function using linear interpolation for the loss coefficients of MCVs. The left y-axis denotes the flow rate. The continuous blue line represents the estimated flow rate utilising IP-optimised parameters, while the dashed blue line represents the estimated flow rate using SQP-optimised parameters. Yellow circles visually represent the measurements. The right y-axis denotes the valve angle, with orange the measured valve angle is illustrated.

The results in Table 3-11 and Table 3-12 show that the IP optimisation method obtains a higher % VAF in all the cases. Furthermore, the sigmoid function outperforms the first-order time delay function, as evidenced by both performance metrics and the above figures. The sigmoid function better fits the data because it accounts for unmodeled dynamics in the decrease of flow rate. This could be due to the large volume of fluid moving at high velocity,

	MCV_{36}		MCV_{37}	
	VAF	MSE	VAF	MSE
SQP	92.63 %	$3.11{\cdot}10^{-4}$	97.38 %	$1.44{\cdot}10^{-4}$
IP	98.58 %	$7.54{\cdot}10^{-5}$	97.94 %	$1.10{\cdot}10^{-4}$

Table 3-11: Performance validation flow rate estimation using $r(t)$ as first-order time delay.

	MCV_{36}		MCV_{37}	
	VAF	MSE	VAF	MSE
SQP	99.18 %	$3.75{\cdot}10^{-5}$	99.53 %	$3.03{\cdot}10^{-5}$
IP	99.64 %	$1.96{\cdot}10^{-5}$	99.95 %	$5.97{\cdot}10^{-6}$

Table 3-12: Performance validation flow rate estimation using $r(t)$ as sigmoid function.

which causes a delay in the reduction of flow rate. Additionally, there are approximately 10 meters of pipeline between the pump and the flow sensor, which further contributes to the delayed effect of the decreasing pump head (h_{pump})

Increasing rotational speed

Regarding the case of increasing rotational speed, the following two equations are used to model the change in the generated pump head: a first-order time-delay function and a sigmoid function. The equations are denoted below and illustrated in Figure 3-31.

$$r(t) = K\left(1 - \exp\left(\frac{-(t - t_{delay})}{\tau}\right)\right) \tag{3-36}$$

$$r(t) = K \exp\left(\frac{t - t_{delay} - \delta \cdot \tau}{\tau}\right), \tag{3-37}$$

where $\delta = 8$, K is the flow rate if the pump would be operating at constant rotational speed for the current volume, and t_{delay} is the delay in the flow rate measurement given the pump and flow rate sensor are approximately withing 10-meter distance of each other.

For the estimation of the ramping-up process of the pump dynamics, only the loss coefficients of the lower valve angles are identified, together with τ representing the response to the input and t_{delay} the time delay for the volume of the water to get into motion. The cost function will be optimised by estimating the following parameters:

$\mathbf{x} = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & \tau, & t_{delay} \end{bmatrix}^T$.

For each parameter x_i, the bounds are specified as $x_{\mathrm{lb},i} \leq x_i \leq x_{\mathrm{ub},i}$. The lower and upper bounds are denoted by:

$\mathbf{x}_{\mathrm{lb}} = \begin{bmatrix} 0, & 0, & 0, & 0, & 0, & 0.001, & 0 \end{bmatrix}^T$,

$\mathbf{x}_{\mathrm{ub}} = \begin{bmatrix} 6000, & 6000, & 6000, & 6000, & 6000, & 10, & 60 \end{bmatrix}^T$, with the constraints: $\begin{bmatrix} x_1 \geq x_2 \\ x_2 \geq x_3 \\ x_3 \geq x_4 \\ x_4 \geq x_5 \\ x_5 \geq K_{50} \end{bmatrix}$.

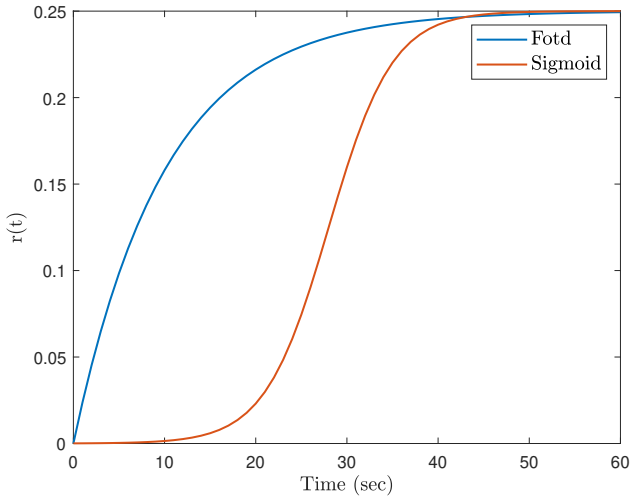


Figure 3-31: The function $r(t)$ for the increasing pump head modelled as a first-order response denoted in blue and a sigmoid in red.

Both methods use the same constraints and bounds. The initial guesses are:

$$\mathbf{x}_{0\_\text{sigmoid}} = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & 1.5, & 0.02 \end{bmatrix}^T,$$
$$\mathbf{x}_{0\_\text{first-order}} = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & 3, & 10 \end{bmatrix}^T,$$

where the parameters for the loss coefficients are denoted in Table 3-7 for the specific optimisation method and MCV, the following equation denotes the estimation of the opening of the MCVs:

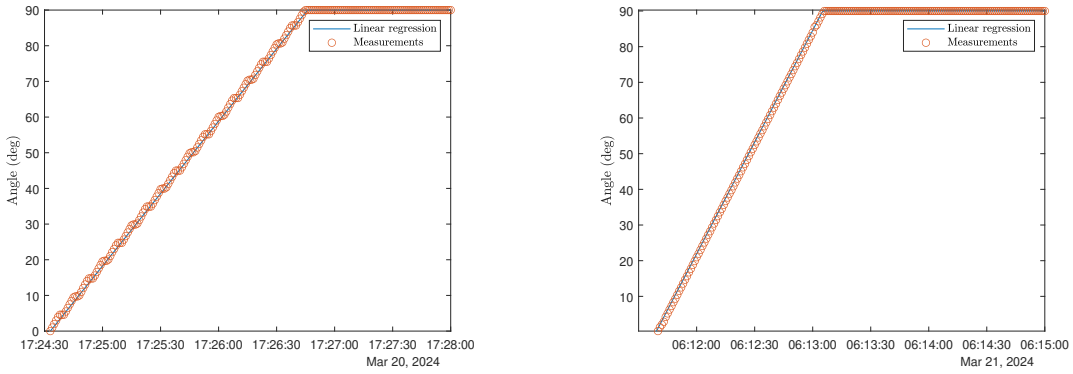
$$\theta(t) = \begin{cases} a \cdot t, & \text{for } t \leq \frac{90}{a} \\ 90, & \text{for } t > \frac{90}{a} \end{cases}, \tag{3-38}$$

where the obtained parameter $a = 0.6764$ for MCV_{36} and $a = 1.0443$ for MCV_{37} using linear regression.

Simulating the obtained parameters with the validation data for MCV_{36} and MCV_{37} the results are shown in Figure 3-32a and Figure 3-32b respectively. The performance of the identified slope during valve opening is indicated in Table 3-13. The values for calculating the performance are up to the first data point where the angle reaches 90. The VAF and the graphs show that the slopes are estimated accurately. Additionally, the optimised slopes are very similar to the slopes of the closing valves.

	VAF	MSE
a_{36}	99.98 %	$4.59{\cdot}10^1$
a_{37}	99.99 %	$7.22{\cdot}10^1$

Table 3-13: Performance slope opening MCV_{36} and MCV_{37}



(a) MCV_{36} **(b)** MCV_{37}

Figure 3-32: Validation slope opening MCVs with the measurements denoted in red circles and the estimated valve angle obtained by linear regression in blue.

Obtained parameters The obtained parameters for the two optimisation algorithms and modelling $r(t)$ as a first-order time delay response are shown in Table 3-14. The obtained parameters for the two optimisation methods algorithms and modelling $r(t)$ as a time-delayed sigmoid function are indicated in Table 3-15.

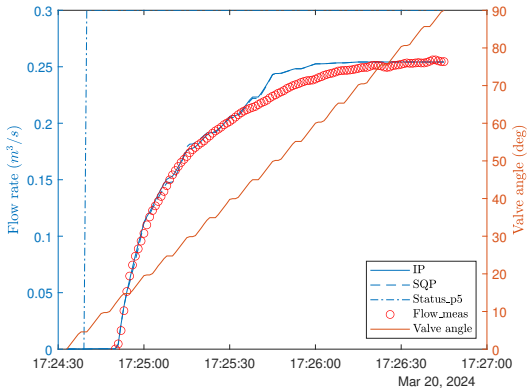
	MCV_{36}		MCV_{37}	
	SQP	IP	SQP	IP
K_0	1000.00	868.44	1000	1000
K_{10}	300.00	126.69	300	300.10
K_{20}	79.93	59.16	80	80.58
K_{30}	26.82	28.65	37.93	29.59
K_{40}	15.37	14.91	10.08	14.45
τ	4.01	6.19	3.00	6.28
t_{delay}	10.82	10.75	10	9.90

Table 3-14: Obtained parameters identification loss coefficients low angles and parameter for $r(t)$ as a first-order time delay to simulate the increasing rotational speed of the pump.

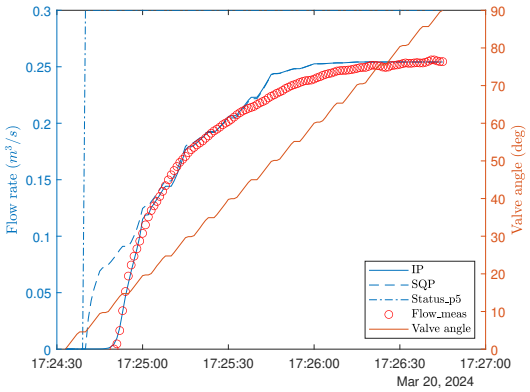
	MCV_{36}		MCV_{37}	
	SQP	IP	SQP	IP
K_0	1000.00	999.92	1000	1000
K_{10}	300.01	539.01	300	300.10
K_{20}	80.65	91.88	80	80.57
K_{30}	26.84	29.13	37.92	29.22
K_{40}	15.55	15.13	10.08	13.07
τ	1.40	1.28	1.46	1.48
t_{delay}	0.02	0.02	0.02	0.02

Table 3-15: Obtained parameters identification loss coefficients low angles and parameter for $r(t)$ as time delayed sigmoid to simulate the increasing rotational speed of the pump.

In Figure 3-33, the validation of the flow rate estimation and the increase in pump head for pump 5 is modelled as a first-order time delay and as a sigmoid function is indicated. This graph shows that the loss coefficients of the high angles are too low to follow the measurements correctly. While in Figure 3-34, the validation of ramping up of pump 6 is shown, the graphs follow the measurements correctly. Hence, the coefficients were optimised accurately. This is also notable in the identified parameters shown in Table 3-7 for the higher angles, where the values are approximately 0 for the angles 70 and 80 degrees. Thus, the loss coefficients for all the angles of MCV_{36} will be identified together with the parameters for ramping up the pump's rotational speed.



(a) Simulating $r(t)$ for pump 5 as time-delayed first-order response.



(b) Simulating $r(t)$ for pump 5 as a sigmoid function.

Figure 3-33: Validation estimation increasing flow rate as a result of the initialisation of pump 5. The left y-axis denotes the flow rate, the continuous blue line represents the estimated flow rate utilising IP-optimised parameters, while the dashed blue line represents the estimated flow rate using SQP-optimised parameters. Yellow circles visually represent the measurements. The right y-axis denotes the valve angle, with orange the measured valve angle is illustrated.

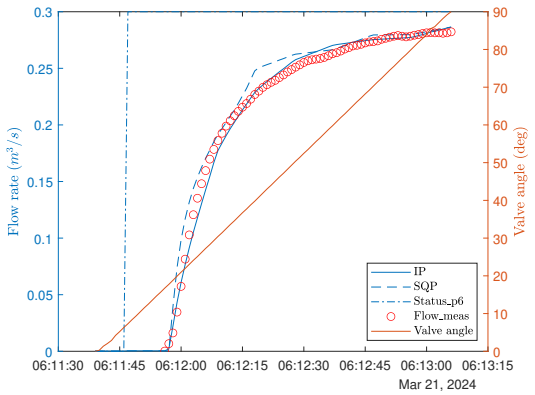
For the identification of the loss coefficients for all the angles, the following parameters are considered: $x = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & K_{50}, & K_{60}, & K_{70}, & K_{80}, & \tau, & t_{delay} \end{bmatrix}$,

with the constraints: $\begin{bmatrix} x_1 \geq x_2 \\ x_2 \geq x_3 \\ x_3 \geq x_4 \\ x_4 \geq x_5 \\ x_5 \geq x_6 \\ x_6 \geq x_7 \\ x_7 \geq x_8 \\ x_8 \geq x_9 \end{bmatrix}$.

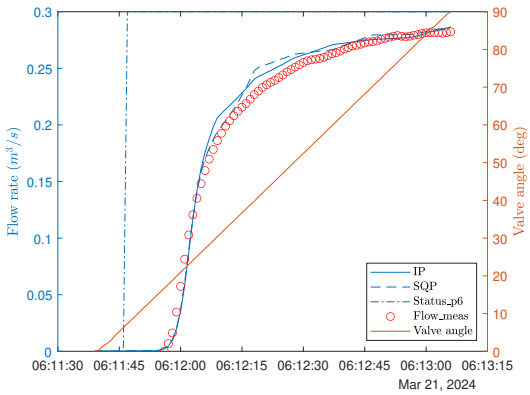
For each parameter x_i, the bounds are specified as $x_{\text{lb},i} \leq x_i \leq x_{\text{ub},i}$ The lower and upper bounds are denoted by:

$$\mathbf{x}_{\text{lb}} = \begin{bmatrix} 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0 \end{bmatrix}^T,$$

$$\mathbf{x}_{\text{ub}} = \begin{bmatrix} 6000, & 6000, & 6000, & 6000, & 6000, & 6000, & 6000, & 6000, & 6000, & 6000, & 60, & 50 \end{bmatrix}^T.$$



(a) Simulating $r(t)$ for pump 6 as time-delayed first-order response.



(b) Simulating $r(t)$ for pump 6 as a sigmoid function.

Figure 3-34: Validation estimation increasing flow rate as a result of the initialisation of pump 6. The left y-axis denotes the flow rate. The continuous blue line represents the estimated flow rate utilising IP-optimised parameters, while the dashed blue line represents the estimated flow rate using SQP-optimised parameters. Yellow circles visually represent the measurements. The right y-axis denotes the valve angle, with orange the measured valve angle is illustrated.

Using the initial guess:

$$\mathbf{x}_{0\_\text{sigmoid}} = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & K_{50}, & K_{60}, & K_{70}, & K_{80}, & 1.5, & 0.02 \end{bmatrix}^T,$$

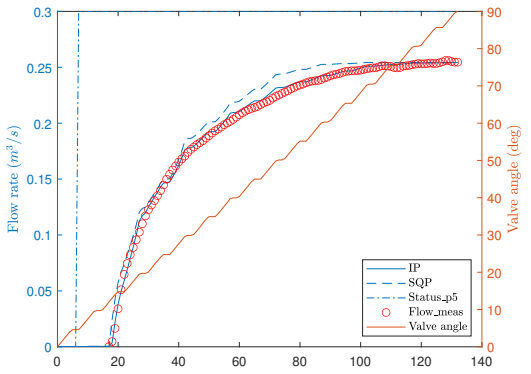
$$\mathbf{x}_{0\_\text{first-order}} = \begin{bmatrix} K_0, & K_{10}, & K_{20}, & K_{30}, & K_{40}, & K_{50}, & K_{60}, & K_{70}, & K_{80}, & 3, & 10 \end{bmatrix}^T,$$

where the initial values used for the loss coefficients are denoted in Table 3-7 for the specific optimisation methods and MCV. The obtained parameter values are presented in Table 3-16.

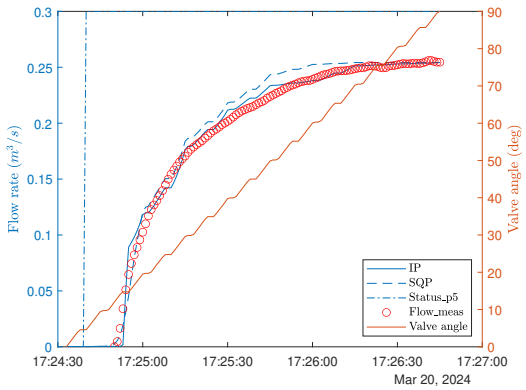
	FOTD		Sigmoid	
	SQP	IP	SQP	IP
K_0	1000	1001	1000	1000
K_{10}	300	300.20	300	303.38
K_{20}	80	80.91	80	97.05
K_{30}	24.04	29.82	24.04	29
K_{40}	10	13.79	10.01	12.67
K_{50}	2.53	5.99	2.53	5.35
K_{60}	0.38	2.99	300	4.15
K_{70}	$4.13 \cdot 10^{-6}$	0.79	$4.13 \cdot 10^{-6}$	0.71
K_{80}	0	0.12	0	0.30
τ	3	4.05	1.49	0.24
t_{delay}	10	10.84	0.02	9.0

Table 3-16: Obtained parameters identification loss coefficients low angles and parameter for $r(t)$ as a first-order time delay and sigmoid function

In Figure 3-35, the estimated increasing flow rate using the obtained parameters for the loss coefficients across the entire range is presented for $r(t)$ as sigmoid and FOTD.



(a) Simulating $r(t)$ as a time-delayed first order response



(b) Simulating $r(t)$ as a sigmoid function

Figure 3-35: Validation estimation increasing flow rate due to the initialisation of pump 5 utilising the obtained loss coefficients whole range of angles of MCV_{36}. The left y-axis denotes the flow rate. The continuous blue line represents the estimated flow rate utilising parameters obtained by the IP algorithm. The dashed blue line represents the estimated flow rate using SQP-optimised parameters. Yellow circles visually represent the measurements. The right y-axis denotes the valve angle. With orange, the measured valve angle is illustrated.

The performance of optimising the loss coefficients for the lower angles and the simulation of the ramping up is presented in Table 3-17. The performance of optimising the higher valve angles for MCV_{36} are denoted in Table 3-18. These tables show that the performance of the parameters optimised by the SQP algorithm was enhanced when all the loss coefficients were optimised. Overall, there is no significant difference between the performance of the first-order response and the sigmoid function. This can be explained by the fact that the functions seem to have similar dynamics since the first-order response has an average identified time delay of 10 seconds, and the sigmoid function itself only starts increasing after a certain amount of time and, in the beginning, will encounter some high losses due to the low valve angles.

	MCV_{36}		MCV_{37}	
	VAF	MSE	VAF	MSE
SQP_fotd	99.7 %	$4.77{\cdot}10^{-5}$	99.36 %	$1.32{\cdot}10^{-4}$
IP_fotd	99.69 %	$4.84{\cdot}10^{-5}$	99.86 %	$7.15{\cdot}10^{-5}$
SQP_sigmoid	95.42 %	$5.12{\cdot}10^{-5}$	99.72 %	$3.42{\cdot}10^{-5}$
IP_sigmoid	99.69 %	$5.02{\cdot}10^{-5}$	99.70 %	$7.65{\cdot}10^{-5}$

Table 3-17: Performance validation flow rate loss coefficients low angles.

To conclude, a mathematical model is developed to describe the dynamics of the water storage unit's draining mode, utilising the available data, fluid mechanics, and system identification. Despite the pump and valve input signals not being available and limited information on the pump curves, parameter correlations were leveraged to construct a model capable of accurately capturing the draining mode's nominal behaviour.

	MCV_{36}	
	VAF	MSE
SQP_fotd	99.51 %	$1.00 \cdot 10^{-4}$
IP_fotd	99.95 %	$9.77 \cdot 10^{-5}$
SQP_sigmoid	99.55 %	$9.35 \cdot 10 - 5$
IP_sigmoid	99.68 %	$4.01 \cdot 10^{-5}$

Table 3-18: Performance validation flow rate using the obtained loss coefficients for the whole range of valve angles.

3-4-4 Replenishing mode

The dynamics of the replenishing mode are identified in this section, utilising the equations of motions in Equation 3-27 along with measurement data of the pressure, volume, valve angles and flow rate.

To identify the system parameters, the previously mentioned two algorithms, namely SQP and IP, are used to optimise the system parameters. Concerning the valve angles, it is notable from Figure 3-24 that the valve angles never exceed 40 degrees. Therefore, the loss coefficients will only be identified up to 40 degrees: $\theta = \begin{bmatrix} 0, & 10, & 20, & 30, & 40 \end{bmatrix}$.
The parameters to be optimised and their initial guesses are presented in Table 3-19. Where the length of the pipes and the height of the inlet are guessed based on the provided pipeworks overview by Dunea. The minor losses and the roughness are based on Tables 6.1 and 6.5 and Figures 6.20, 6.21 and 6.23 in [70]. Lastly, the guesses for the loss coefficients are based on the results of the identification in the previous section, and the loss coefficients of the lower angels are increased, ensuring a low flow rate.

x	x_0
z_1	-0.99
$L_{0.4}$	4.01
$L_{0.6}$	17.93
$L_{0.8}$	16.19
$K_{m\_0.4}$	4.17
$K_{m\_0.6}$	4.50
$K_{m\_0.8}$	3.23
ϵ	0.09
K_{34_0}	$1.05 \cdot 10^4$
K_{34_10}	1500
K_{34_20}	220
K_{34_30}	80
K_{34_40}	25
K_{35_0}	$1.05 \cdot 10^4$
K_{35_10}	1500
K_{35_20}	220
K_{35_30}	80
K_{35_40}	25

Table 3-19: Initial guess system parameters replenishing mode

For each parameter x_i, the bounds are specified as $x_{\text{lb},i} \leq x_i \leq x_{\text{ub},i}$. Let $\mathbf{y}_z$ denote a row vector of size z containing all values of y. The lower and upper bounds are denoted by:

$$\mathbf{x}_{\text{lb}} = \begin{bmatrix} -1, & 3, & 16, & 12, & 0, & 0, & 0, & 1 \cdot 10^{-10}, & \mathbf{0}_{10} \end{bmatrix}^T,$$
$$\mathbf{x}_{\text{ub}} = \begin{bmatrix} 1, & 8, & 20, & 20, & 5, & 5, & 5, & 0.1, & 60000 \cdot \mathbf{1}_{10} \end{bmatrix}^T,$$

with the constraints: $\begin{bmatrix} x_9 \geq x_{10} \\ x_{10} \geq x_{11} \\ x_{11} \geq x_{12} \\ x_{12} \geq x_{13} \\ x_{14} \geq x_{15} \\ x_{15} \geq x_{16} \\ x_{16} \geq x_{17} \\ x_{17} \geq x_{18} \end{bmatrix}$.

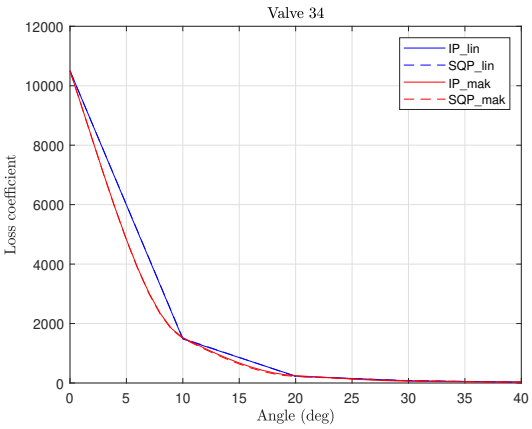
Obtained parameters

The obtained parameters for the different optimisation algorithms and the two interpolation methods are presented in Table 3-20.

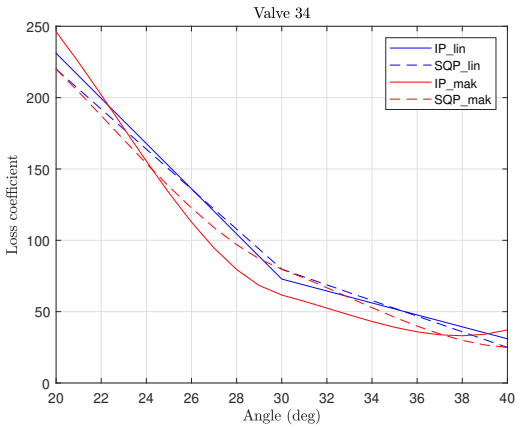
	IP_lin	SQP_lin	IP_mak	SQP_mak
z_1	0.983	1	-0.987	0.29
$L_{0.4}$	3.68	3.96	4.16	3.97
$L_{0.6}$	18.96	17.92	16.30	17.92
$L_{0.8}$	15.98	16.19	14.79	16.19
$K_{m\_0.4}$	0.50	3.80	1.91	3.85
$K_{m\_0.6}$	0.68	4.21	1.25	4.25
$K_{m\_0.8}$	1.01	3.14	4.83	3.15
ϵ	0.0011	$1 \cdot 10^{-10}$	0.013	$1 \cdot 10^{-10}$
K_{34_0}	$1.05 \cdot 10^4$	$1.05 \cdot 10^4$	$1.05 \cdot 10^4$	$1.05 \cdot 10^4$
K_{34_10}	1480	1500	1525.7	1500
K_{34_20}	231.07	219.98	246.23	220.02
K_{34_30}	72.84	79.74	61.67	79.74
K_{34_40}	30.97	24.91	37.22	24.93
K_{35_0}	$1.05 \cdot 10^4$	$1.05 \cdot 10^4$	$1.05 \cdot 10^4$	$1.05 \cdot 10^4$
K_{35_10}	1481.7	1500	1522.9	1500
K_{35_20}	225.51	219.98	232.33	220.02
K_{35_30}	77.77	79.75	83.52	79.74
K_{35_40}	29.87	24.91	32.16	24.92

Table 3-20: Obtained parameters using multiple optimisation algorithms and interpolation methods

The identified loss coefficients are displayed in Figure 3-36 and Figure 3-37 for MCV_{34} and MCV_{35} respectively. For the angles below 20 degrees, the coefficients exhibit negligible differences. However, for angles above 20 degrees, the obtained coefficients for both valves demonstrate variance. Furthermore, the coefficients for the Makima interpolation display more pronounced disparities compared to those for the linear interpolation. Additionally, it is worth noting that the coefficients for MCV_{35} hold minimal discrepancies between the optimisation algorithms.

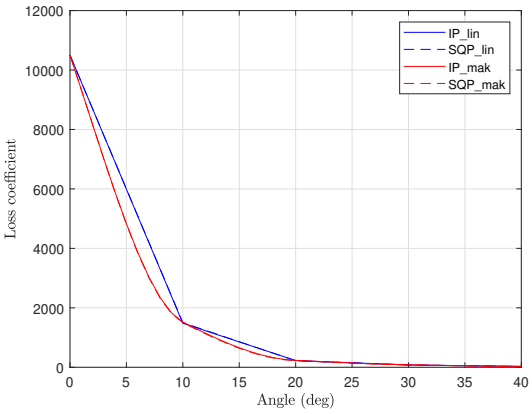


(a) Identified loss coefficients for MCV_{34}

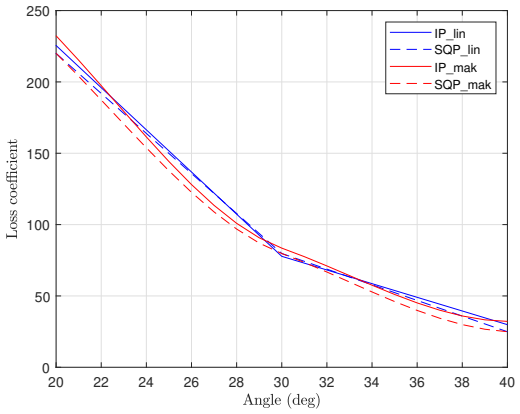


(b) Identified loss coefficients for MCV_{34} enhanced on $20 \leq \theta \leq 40$

Figure 3-36: Identified loss coefficients for the valve angles of MCV_{34}, where the coefficients with linear interpolation are shown in blue and with Makima in red. The optimisation method is illustrated by the continuous line using IP, while SQP is represented by the dashed line.



(a) MCV_{35}



(b) MCV_{35} enhanced on $20 \leq \theta \leq 40$

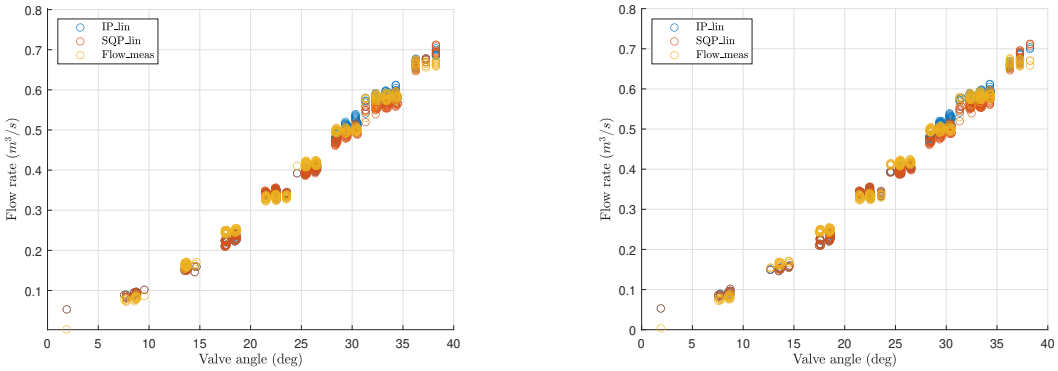
Figure 3-37: Identified loss coefficients for the valve angles of MCV_{35}, where the coefficients with linear interpolation are shown in blue and with Makima in red. The optimisation method is illustrated by the continuous line using IP, while SQP is represented by the dashed line.

Validation flow rate steady-state data

This section estimates the flow rate using Equation 3-39 with the water level, $z_2(t)$, pressure $p_1(t)$ and valve angles as input data and the identified parameters $\hat{z}_1$, $\hat{\epsilon}$, $\hat{K}_{34(\theta),35(\theta)}$, $\hat{K}_{m\_0.4,0.6,0.8}$, and $\hat{L}_{0.4,0.6,0.8}$ denoted in Table 3-20. Only data points where steady-state flow rates are measured are considered for the input data.

$$m(Q) := \frac{p_1(t) - p_2}{\rho \cdot g} + \frac{1}{2g \cdot A_6^2} \cdot Q^2 - z_2(t) + \hat{z}_1 - h_f(Q, \hat{\epsilon}, \hat{L}_{0.4,0.6,0.8}) - ... \\ \sum h_m(Q, \hat{K}_{m\_0.4,0.6,0.8}) - h_{valves}(Q, \theta(t), \hat{K}_{34(\theta),35(\theta)}) = 0 \tag{3-39}$$

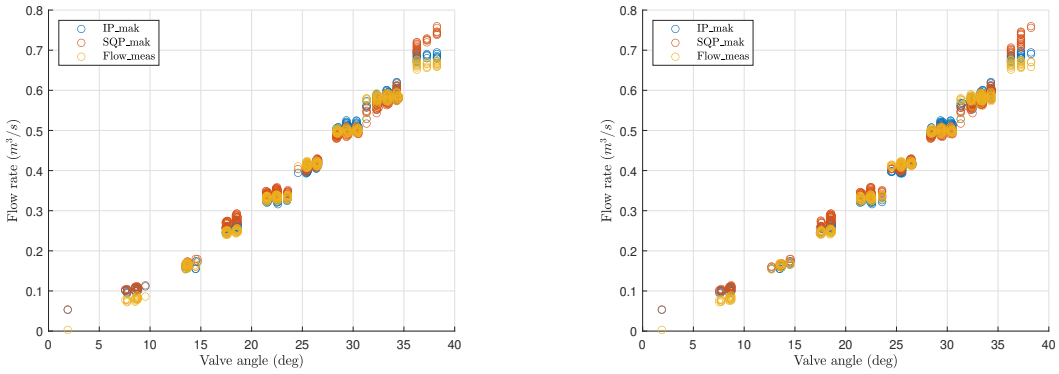
The results of the estimated flow rate utilising the obtained parameters with linear interpolation of the identified loss coefficients are shown in Figure 3-38 for the valve angles of MCV_{34} and MCV_{35}. From these plots, it can be observed that the estimated flow rates all lie within the same region as the measurements. Additionally, for the angles between 28 and 35 degrees, the IP algorithm results in a higher flow rate than the SQP algorithm. The flow rate per degree valve angle can vary for measurements and estimations. This can be explained by the fact that the volumes can differ, the pressure p_1 fluctuates, and the flow rate will have small deviations due to the turbulent flow.



(a) MCV_{34} **(b)** MCV_{35}

Figure 3-38: The validation of the flow rate estimated by linearly interpolating the loss coefficients of the valves. The estimation is shown in blue using obtained parameters with the IP algorithm, while parameters obtained by the SQP algorithm are shown in red. Scattered yellow dots represent steady-state flow measurements.

The results of the estimated flow rate with Makima interpolation of the identified loss coefficients are shown in Figure 3-39 for the valve angles of MCV_{34} and MCV_{35}. For both optimisation algorithms, up to 20 degrees, the flow rate is estimated to be higher than the measured flow rate, and for angles above 35 degrees. For the valve angles between zero and 10 degrees, this can be explained by the fact that due to the pressure of p_1 and the low volume of the reservoir at the starting point of the intake process, the flow rate is estimated higher since it does not consider that the water is increasing from zero velocity.

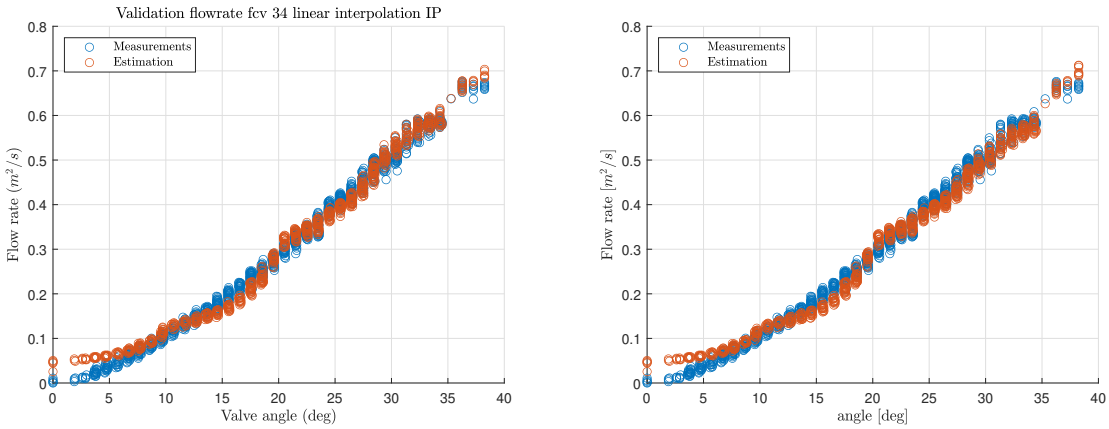


(a) MCV_{34} **(b)** MCV_{35}

Figure 3-39: The validation of the flow rate estimated by Makima interpolating the loss coefficients of the valves. The estimation is shown in blue using the parameters obtained by the IP algorithm, while parameters optimised by the SQP algorithm are shown in red. Scattered yellow dots represent steady-state flow measurements.

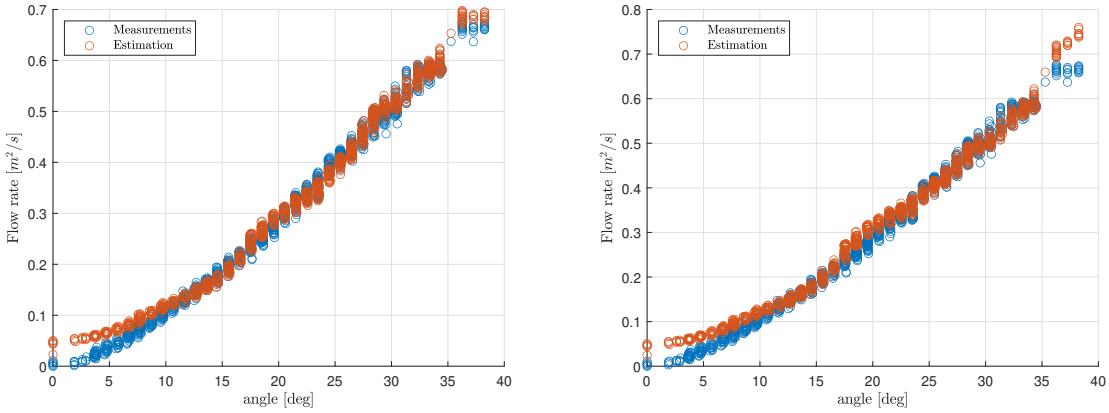
Validation flow rate estimation

This section discusses the validation of the estimation of the flow rate using Equation 3-39 with the water level $z_z(t)$ and pressure at $p_1(t)$ as input for the valve angles for the whole range of valve angles gives the following results. Based on the previous graphs, it is evident that the angles of the valves and the resulting flow rate show minimal differences. Hence, in order to enhance clarity, each flow estimation using the identified parameter is only plotted against the angles of MCV_{34}. The estimated flow rate given the linear interpolation of the loss coefficients and the system parameters obtained by the IP and SQP methods are shown in Figure 3-40. The estimated flow rate given the Makima interpolation of the loss coefficients and the system parameters obtained by the IP and SQP methods are shown in Figure 3-41. The performances of the estimations are displayed in Table 3-21. The graphs demonstrate that the estimations using the obtained parameters follow the measurement accurately between the angles of 5 and 35 degrees. Besides the previously mentioned, some distinctions are worth mentioning: the sudden increase around the angle of 20 degrees using the linear interpolation compared to the smooth transition using the Makima interpolation. The characteristics of the interpolation methods can explain this. Furthermore, estimations using linear interpolation show lower flow rate estimations between the angles of 10 and 20 degrees compared to the Makima interpolation.



(a) Optimisation employing IP **(b)** Optimisation employing SQP

Figure 3-40: The validation of the flow rate using the estimated loss coefficients for linear interpolation and system parameters with respect to the angles of MCV_{34}.



(a) Optimisation employing IP **(b)** Optimisation employing SQP

Figure 3-41: The validation of the flow rate using the estimated loss coefficients for Makima interpolation and system parameters with respect to the angles of MCV_{34}.

	VAF	MSE
IP_lin	99.67 %	$2.36 \cdot 10^4$
SQP_lin	99.75 %	$3.18 \cdot 10^4$
IP_mak	99.67 %	$1.58 \cdot 10^4$
SQP_mak	99.54 %	$2.59 \cdot 10^4$

Table 3-21: Performance simulating flow rate given volume measurements

Validation replenishing dynamics water storage unit

This section validates the simulation of the water storage unit's replenishment dynamics. The following differential-algebraic equations are used to describe the replenishing dynamics:

$$\dot{x}_1 = -\frac{x_2}{A_{res}} \tag{3-40}$$

$$m(x) := \frac{p_1(t) - p_2}{\rho \cdot g} + \frac{1}{2g \cdot A_6^2} \cdot x_2^2 + \hat{z}_1 - x_1 - h_f(x_2, \hat{\epsilon}, \hat{L}_{0.4,0.6,0.8}) - ... \\ \sum h_m(x_2, \hat{K}_{m\_0.4,0.6,0.8}) - h_{valves}(x_2, \theta(t), \hat{K}_{34(\theta),35(\theta)}) = 0 \tag{3-41}$$

$$y = Cx = I_2 \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \tag{3-42}$$

where the differential state x_1 is the water level of the reservoir in m and the algebraic state x_2 is the flow rate at the inlet in m^3/s, visualised at location 1 in Figure 3-16. A_{res} is the cross-section of the reservoir, $p_1(t)$ the pressure at the inlet and p_2 the atmospheric pressure, A_6 the cross-section of the pipe at the location of the flow sensor, $\hat{z}_1$ the level of the pipe at the flow sensor, $\theta(t)$ the angle of valves MCV_{34} and MCV_{35}. p_2 is atmospheric pressure, g gravitation ρ the density of water at a temperature of 20 °Celsius, $\hat{\epsilon}$ the identified pipe roughness, the loss coefficients of the pipes $\hat{K}_{34(\theta),35(\theta)}$, the minor losses relative to the different pipe cross-sections located at the water storage unit $\hat{K}_{m\_0.4,0.6,0.8}$, and the total lengths of the pipes with the different cross sections $\hat{L}_{0.4,0.6,0.8}$.

The performance of both the estimation of the flow rate and the estimation of the water level are shown in Table 3-22. From these metrics, it becomes evident that the estimation of the flow rate and the water level both have a high %VAF. The MSE of the water level using makima interpolation combined with both optimisation methods is higher than the linear interpolation estimations. This can be explained by the fact that the estimations of the flow rate are similar to or higher than the measurements for the angles up to 20 degrees, as shown in Figure 3-41.

	Flow rate		Water level	
	VAF	MSE	VAF	MSE
IP_lin	99.68 %	$2.32 \cdot 10^{-4}$	99.79 %	0.0066
SQP_lin	99.74 %	$3.20 \cdot 10{-}4$	99.92 %	0.0024
IP_mak	99.76 %	$1.54 \cdot 10^{-4}$	99.78 %	0.0101
SQP_mak	99.56 %	$2.59 \cdot 10^{-4}$	99.77 %	0.0129

Table 3-22: Performance estimation replenishment dynamics

Two cases have been highlighted in the following graphs to show the result of simulating the dynamics of the intake process of the replenishment reservoir.

In Figure 3-42, Figure 3-43 and Figure 3-44, the simulated flow rate and water level and the input valve angles are displayed for the night of January 23rd and January 24th. Overall, the flow rate estimations follow the measurement properly, resulting in a fair estimation of the water level. One thing to point out is the increased water level started to deviate around 02:00; for estimating the water level using the obtained parameters using the Makima interpolation. The flow rate estimated using this method was the overall highest estimated flow rate during the run.

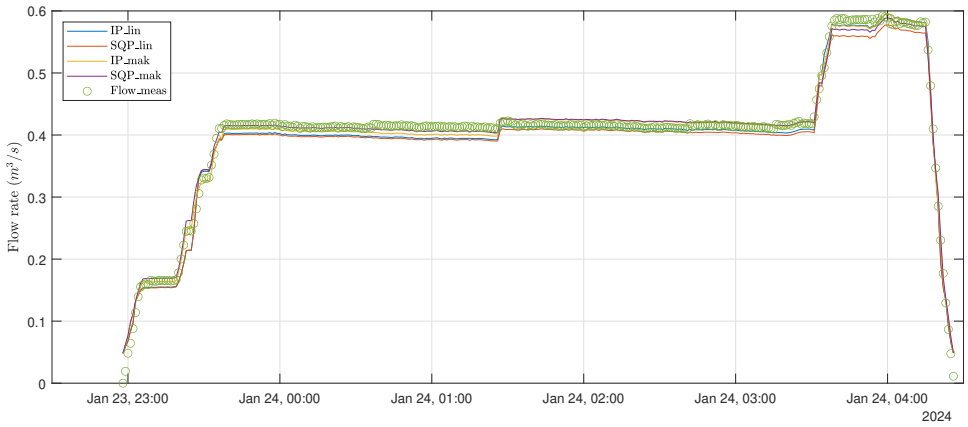


Figure 3-42: Validation flow rate estimation simulating the intake dynamics of the replenishment reservoir. The estimation using the optimised parameters with IP and linear interpolation for the valve loss coefficients is in blue. In red, the estimation using the optimised parameters with SQPtogether with linear interpolation for the valve loss coefficients. The estimation using the optimised parameters with IP and Makima interpolation for the valve loss coefficients is in yellow. In purple, the estimation using the optimised parameters with SQP and Makima interpolation for the valve loss coefficients. Additionally, the flow measurements are scattered in green.

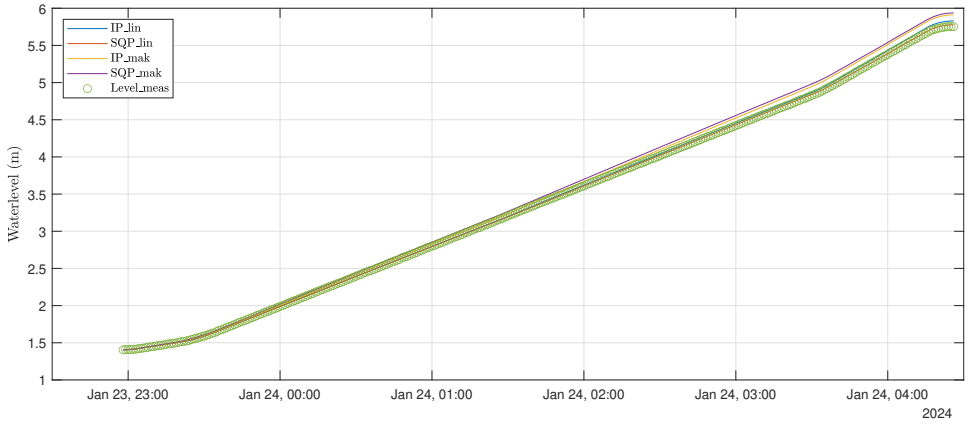


Figure 3-43: Validation water level estimation simulating the intake dynamics of the replenishment reservoir. The estimation using the optimised parameters with IP and linear interpolation for the valve loss coefficients is in blue. In red, the estimation using the optimised parameters with SQPtogether with linear interpolation for the valve loss coefficients. The estimation using the optimised parameters with IP and Makima interpolation for the valve loss coefficients is plotted in yellow. In purple, the estimation using the optimised parameters with SQP and Makima interpolation for the valve loss coefficients. Additionally, the flow measurements are scattered in green.

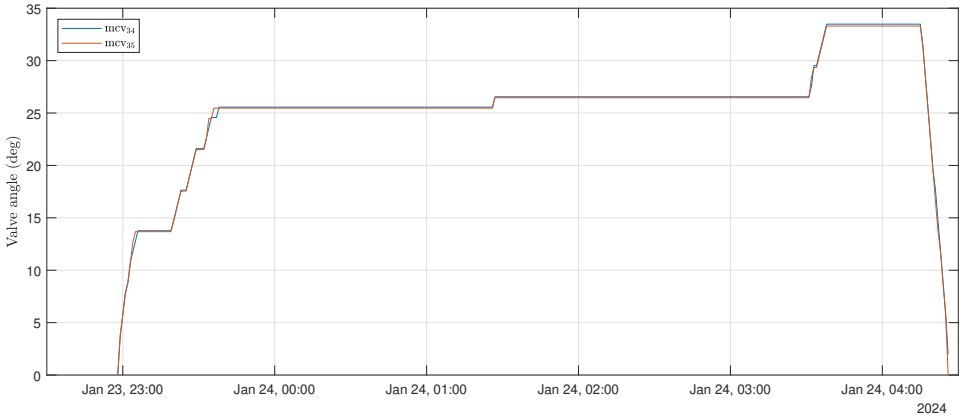


Figure 3-44: Valve angle data for MCV_{34} and MCV_{35} are used as input for intake dynamics simulation. The angles are shown in blue and red, respectively.

In Figure 3-42, Figure 3-43 and Figure 3-44, the simulated flow rate and water level and the input valve angles are displayed for the night of January 22nd and January 23rd. Also, in this case, the flow rate estimations follow the measurement suitably. Resulting in an accurate estimation of the water level. The estimated flow rate for the valve angles around 25 degrees, between 00:30 and 03:30, is estimated below the measured data for all methods, where the estimation using the parameters of SQP_makima performs the best. All parameters optimised using the different methods have satisfactory performance for the estimation of the flow rate and water level. However, when considering the combined performance of these parameters, it is evident that the IP_lin method outperforms the others.

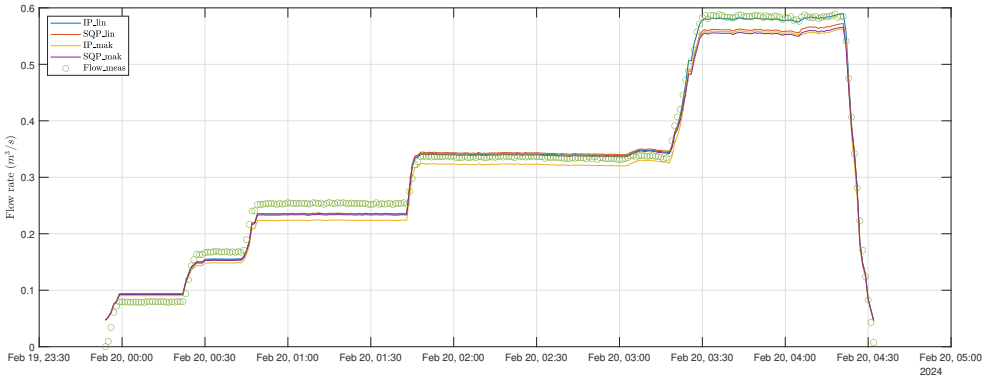


Figure 3-45: Validation flow rate estimation simulating the intake dynamics of the replenishment reservoir. The estimation using the optimised parameters with IP and linear interpolation for the valve loss coefficients is in blue. In red, the estimation using the optimised parameters with SQPtogether with linear interpolation for the valve loss coefficients. In yellow is the estimation using the optimised parameters with IP and Makima interpolation for the valve loss coefficients. In purple, the estimation using the optimised parameters with SQP and Makima interpolation for the valve loss coefficients. Additionally, the flow measurements are scattered in green.

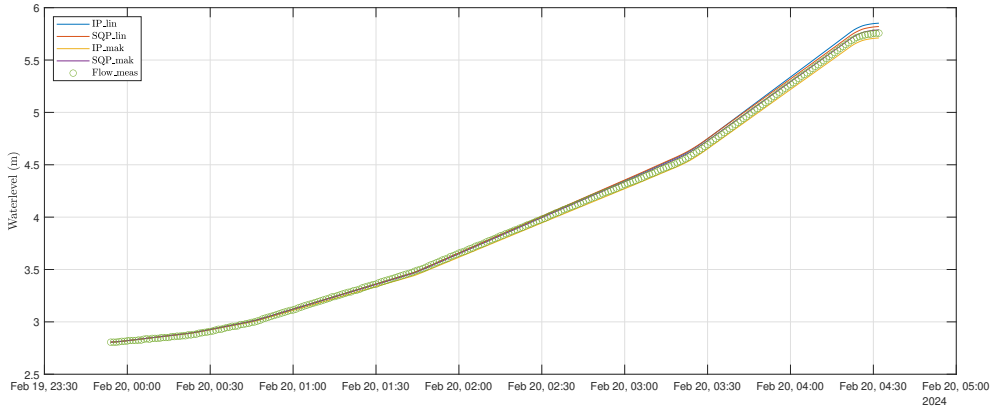


Figure 3-46: Validation water level estimation simulating the intake dynamics of the replenishment reservoir. The estimation using the optimised parameters with IP and linear interpolation for the valve loss coefficients is in blue. In red, the estimation using the optimised parameters with SQPtogether with linear interpolation for the valve loss coefficients. The estimation using the optimised parameters with IP and Makima interpolation for the valve loss coefficients is plotted in yellow. In purple, the estimation using the optimised parameters with SQP and Makima interpolation for the valve loss coefficients. Additionally, the flow measurements are scattered in green.

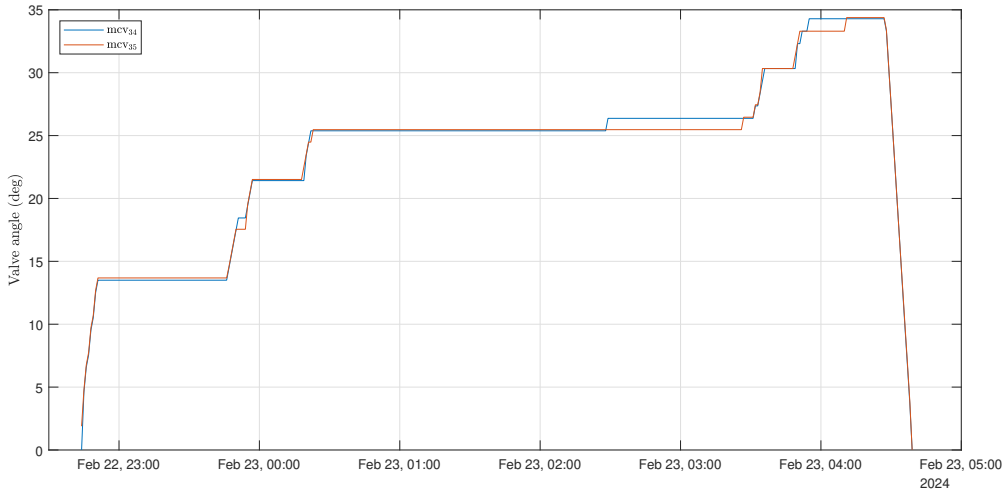


Figure 3-47: Valve angle data for MCV_{34} and MCV_{35} are used as input for intake dynamics simulation. The angles are shown in blue and red, respectively

Utilising measurement data and the principles of fluid mechanics, the estimation of the flow rate during the replenishment shows good performance when simulated with the valve measurements. The final model will employ the setpoints of the FCVs as input. Estimating the influence of the setpoint on the angles of the valves and utilising this as input to the Differential-Algebraic Equation (DAE) with the derived system parameters as a cascade interconnection.

3-5 Final model

In the previous sections, the mathematical descriptions and parameters necessary to characterise the nominal behaviour of the water storage unit have been provided. The dynamics describing the replenishing mode are derived, and for the draining mode, the dynamics of the pumps at constant rotational speed singularly and in parallel also have been specified. Furthermore, the dynamics change when the pump's rotational speed increases or decreases. However, this is only considered when the pumps are on singularly. Thus, remaining with the last modes of operation to establish a comprehensive model describing the dynamics. These modes involve the case that one pump operates at constant rotational speed and a second pump is started, as well as two pumps operating at constant rotational speed and one pump is stopped and are described in subsection 3-5-1.

Multiple identification methods have been used together with different types of interpolation to identify the system parameters regarding the various modes of operation. In subsection 3-5-2, the determination regarding the identified parameters in the final model will be made.

Given that all the modes have been modelled and the final parameters have been chosen, the final model can be described as a hybrid automaton. A graphical representation of this automaton is visualised in subsection 3-5-3.

3-5-1 Initialisation and termination of the second pump

When there is an increasing demand by the consumer net compared to the production output, the number of pumps in operation can be expanded, and the draining flow rate of the reservoir will be increased. When there is a decrease in demand compared to the production offset, and two pumps are up and running, the second pump can be terminated. In these cases, the equations of motion described in Equation 3-23 and the functions for $r(t)$ defined in Equation 3-34 Equation 3-33 for termination and Equation 3-36 and Equation 3-37 for initialisation can be used to describe the dynamics of the system.

At the initialisation of the second pump the parameter for K in $r(t)$ will be defined by K_{diff} which is calculated as follows:

$$g_2(x_1, K_{ss\_parallel}, \gamma_{par}) = 0 \tag{3-43}$$
$$K_{init} = x_2(k-1) \tag{3-44}$$
$$K_{diff} = K_{ss\_parallel} - K_{init}, \tag{3-45}$$
$$\tag{3-46}$$

where γ_{par} indicates the identified parameters for the pumps operating in parallel, as presented in Table 3-4, to solve $g_2(\cdot) = 0$ and estimate $K_{ss\_parallel}$, which denotes flow rate while the pumps operate in parallel at a constant rotational speed. Furthermore, a third state will be introduced to solve for the contribution of the increase in flow rate caused by the increasing head of the additional pump. The equations of motion for the initialisation of the second pump are denoted by the following:

$$\dot{x}_1 = -\frac{x_2}{A_{res}} \tag{3-47}$$

$$x_2 = x_3 + K_{init} \tag{3-48}$$

$$g_1(x_1, x_3, \theta) := H_{pump\_1}(K_{diff}, x_1, \gamma_2) - H_{sys}(x_1, x_3, \theta, \gamma_2) = 0, \tag{3-49}$$

where γ_2 presents the system parameters for the pump increasing its rotational speed, as presented in Table 3-16 and $H_{pump\_1}(\cdot)$ denotes the function of the increasing pump head as described in Equation 3-23 with the corresponding functions Equation 3-36 and Equation 3-37 for $r(t)$.

At the termination of the second pump, the parameter for K in $r(t)$ will be defined by K_{diff} which is calculated as follows:

$$g_2(x_1, K_{ss\_one}, \gamma_1) = 0 \tag{3-50}$$

$$K_{init} = x_2(k-1) \tag{3-51}$$

$$K_{diff} = K_{init} - K_{ss\_one}, \tag{3-52}$$

where K_{ss_one} is calculated using γ_1, which indicates the parameters for the pump that remains at constant rotational speed, as presented in Table 3-4 and solve for $g_2(\cdot) = 0$. When $\theta > \theta_{off}$ the following equation holds:

$$\dot{x}_1 = -\frac{x_2}{A_{res}} \tag{3-53}$$

$$x_2 = x_3 + K_{diff} \tag{3-54}$$

$$g_2(x_1, x_3, \theta) := H_{pump\_2}(x_1, x_3, \gamma_2) - H_{sys}(x_1, x_3, \theta, \gamma_2) = 0, \tag{3-55}$$

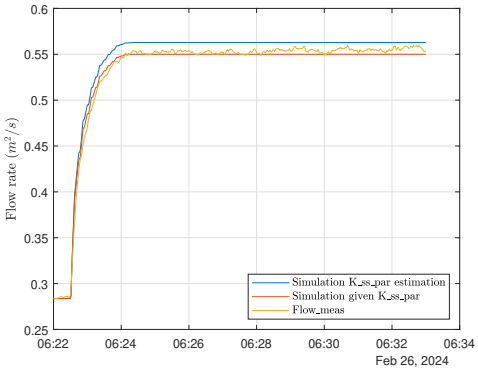
where $H_{pump\_2}(\cdot)$ is the identified pump curve for the pump operating at constant rotational speed and γ_2 indicate the constant rotational speed parameters of the pump that will ramp down, as presented in Table 3-4. This changes to the following when $\theta \leq \theta_{off}$ where $H_{pump\_3}(\cdot)$ is the function for the decreasing pump head as denoted in Equation 3-23:

$$g_3(x_1, x_3, \theta) := H_{pump\_3}(K_{diff}, x_1, \gamma_2) - H_{sys}(x_1, x_3, \theta, \gamma_2) = 0, \tag{3-56}$$

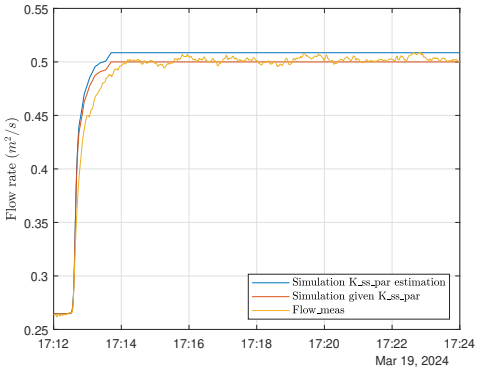
where γ_2 indicate the parameters of the pump ramping down, as presented in Table 3-7.

In Figure 3-48a, the result of simulating the addition of pump 5 to the pumps in operation is shown. The graphs show that the estimated flow rate for the pumps operating in parallel is higher than the measured flow rate. However, when using the average measured flow rate for $K_{ss\_parallel}$ it is evident that the estimated flow rate follows the trend of the measured flow rate well. In Figure 3-48b, the result of simulating the addition of pump 6 to the pumps in operation is shown. Similarly, the estimated steady-state flow rate is higher than the measured flow rate for the pumps operating in parallel. For the estimations of the flow rate, it is notable that when the flow rate reaches the value of the constant rotational pump speed, a jump is present. A possible explanation could be the higher loss coefficients for the butterfly valve at the higher angles. When comparing the values estimated for MCV_{36} in Table 3-16 with the

values estimated for MCV_{37} in Table 3-7 it shows that the loss coefficients for MCV_{36} are significantly smaller. This results in a smoother transition to the reference flow rate when the valves are open at 90 degrees.



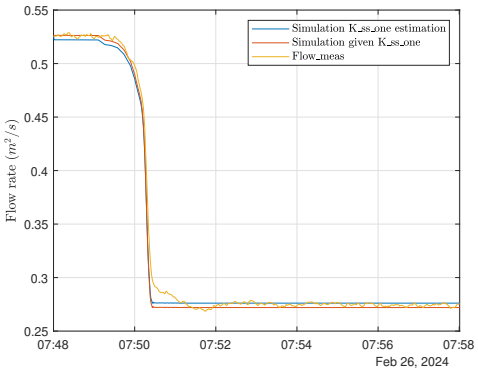
(a) Ramping up pump 5 as the additional pump.



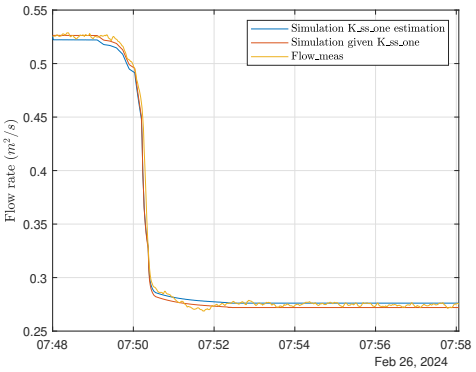
(b) Ramping up pump 6 as the additional pump.

Figure 3-48: Ramping up the additional pump using the parameters optimised using the IP algorithm and $r(t)$ simulated as First Order Time Delay (FOTD). In blue, the flow rate is shown where the steady-state flow for the pumps in parallel is estimated, and in red, the steady-state flow is provided using the average of the measurement data. In yellow, the measured flow rate is presented.

Using the identified parameters for ramping down the pump's rotational speed in section 3-4-3 and the provided dynamics above, the transition from two pumps in operation to one pump in operation is modelled. In Figure 3-49a and Figure 3-49b, the estimation of the ramping down of pump 6 whilst pump 5 is at constant rotational speed with first order time delay and sigmoid function as $r(t)$ are shown respectively. From Figure 3-49b, it is notable that the sigmoid function follows the smooth transition of the decreasing flow rate to the flow provided by the single pump significantly well due to its characteristics.



(a) Transition from two pumps operating in parallel to one using FOTD for $r(t)$.



(b) Transition from two pumps operating in parallel to one using sigmoid for $r(t)$

Figure 3-49: Transition from two pumps operating in parallel to pump 5 in operation by ramping down the rotational speed of pump 6. The estimated flow rate with $K_{ss\_parallel}$ and K_{ss_one} estimated is shown in blue. In red, the estimated flow rate given the measurements for $K_{ss\_parallel}$ and K_{ss_one} estimated is shown. In yellow, the measured flow rate is presented

At this point, a mathematical expression is derived for each sub-mode of the draining process to describe how the reservoir is drained under normal conditions. Combined with the dynamics for the replenishing mode it is possible to simulate how the water storage unit at Leyweg behaves over time.

3-5-2 Final model parameters

In section 3-4, the parameters necessary to describe the dynamics for the replenishing and the draining mode are identified. For the draining mode, the three sub-modes are considered: increasing rotational speed, constant rotational speed, and decreasing rotational speed.

In all operating modes, a decision must be made regarding the parameters identified by the various optimisation methods. The parameters chosen will be utilised in the final mode. Additionally, the interpolation method for the valve loss coefficients needs to be determined for the replenishing mode. In relation to the changing rotational speed, a decision has to be made regarding the function used for $r(t)$. It is possible that different types of functions are used for increasing and decreasing rotational speeds. This can be substantiated by the use of a physical component, specifically a soft starter, which reduces the inrush current at the start of the pump.

To summarise, for the draining mode, a decision should be made about the parameters identified and the functions $r(t)$ within the increasing and decreasing modes. For the replenishing mode, a decision should be made about the parameters identified and the interpolation methods used.

A systematic approach determines the best combination for each mode by calculating the total VAF and MSE scores. In the constant rotational speed sub-mode of the draining mode, there is no significant difference in the performance between the two optimisation methods as shown in Table 3-5. Thus, it has been decided that each VAF score will be equally weighted in the total calculation.

When considering the draining mode, the parameters identified using the SQP algorithm with the FOTD and sigmoid function for $r(t)$ during the increasing and decreasing modes are chosen respectively, taking into account the VAF and MSE. The parameters identified using the IP algorithm with the Makima interpolation method are selected for the replenishing mode.

The final parameters used in the model to represent the nominal behaviour of the water storage unit are denoted in Table A-2 in the Appendix.

3-5-3 Hybrid automaton

The dynamics of the water storage unit can be described by a hybrid automata featuring three main continuous modes: idle, replenishing, and draining. These modes are depicted in Figure 3-50 and the transition between them is triggered by the input signals from the carousel, which serves as the centralised control system.

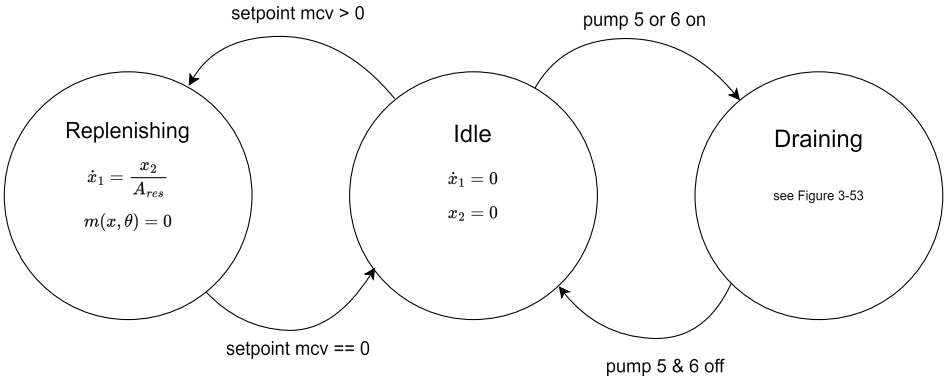


Figure 3-50: Hybrid automaton dynamics water storage unit

In Figure 3-51, a simplified description of the draining mode and its sub-modes is presented. Where increasing and decreasing rotational speeds are presented only for a single pump to show the transitions. The input signal u_1 initiates the draining process when one and terminates the draining by the pump when going from one to zero. In the final model, this model is extended with the increasing and decreasing modes for pumps 5 and 6 separately, the increasing mode when one pump is already on and the decreasing mode when two pumps are on. Furthermore, a mode for two pumps operating at constant rotation is present.

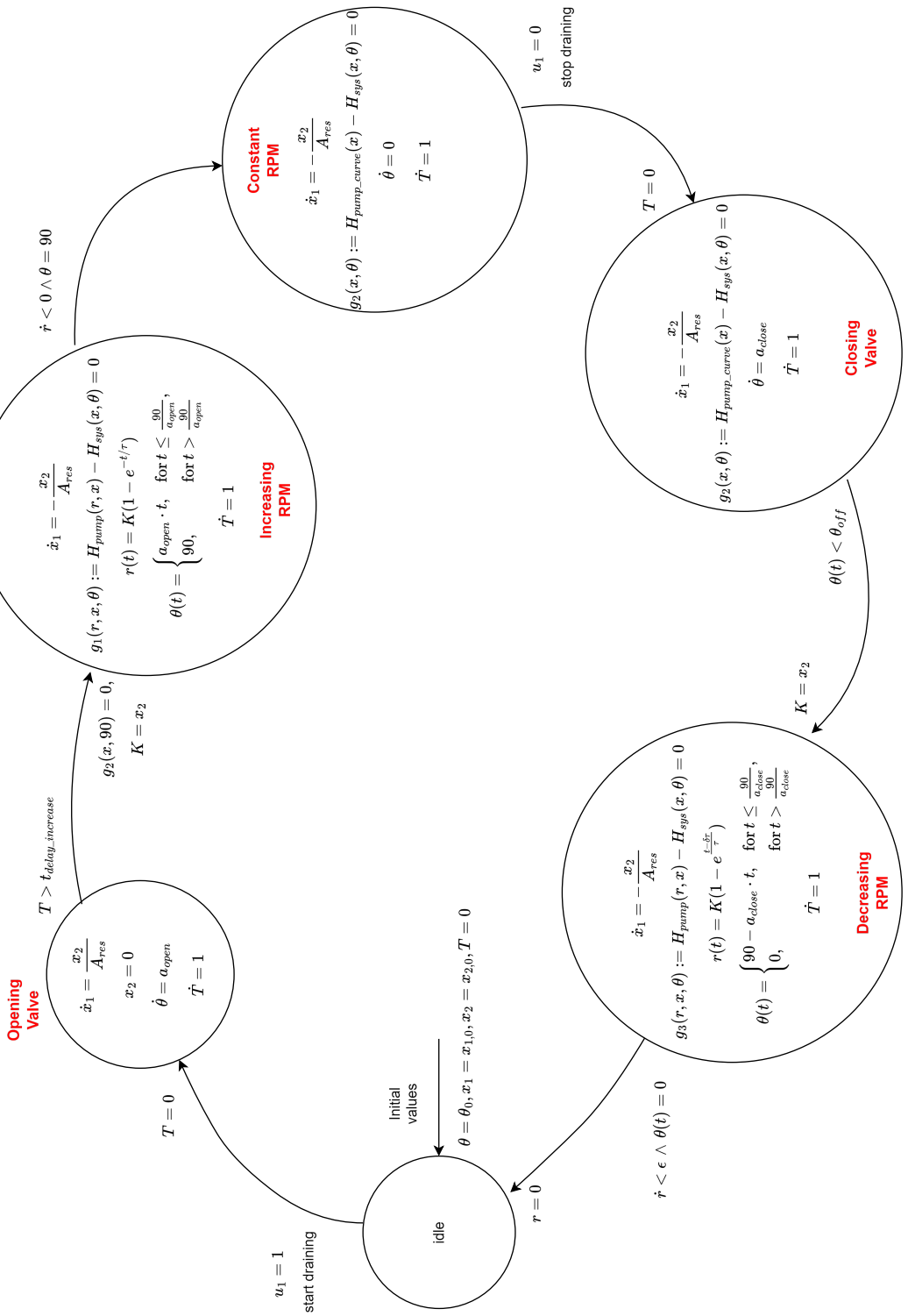


Figure 3-51: Simplified draining mode

Chapter 4

Anomaly Detection and Cyber-Physical Attack Strategies

Identifying anomalies involves observing system behaviour and highlighting any unexpected deviations as anomalies. Faulty components, human errors, or malicious attacks can cause these anomalies. This chapter employs a model-based detection approach to detect cyber-physical attacks targeted at the water storage unit. Potential cyber-physical attacks on the water storage unit are created and simulated to assess the performance of the detection method.

4-1 Anomaly detection model

In section 2-3, signal-based and model-based anomaly detection methods are described. When detecting cyber-physical attacks designed to evade detection, a model-based detection method is more effective than a signal-based detection method. For example, in the case of a replay attack, where prerecorded process data will be replayed, a signal-based anomaly detection method will not detect this as an anomaly as the measurements will show nominal behaviour. Therefore, this study will implement a model-based approach to detect potential cyber-physical attacks. As mentioned in section 2-3, model-based detection involves three main components: state estimation, which employs a mathematical model to describe the nominal behaviour of the system; residual computation, which involves calculating the difference between the state estimation and measurements; and residual evaluation to detect anomalies finally. This section introduces the mathematical formulation of the state estimation and the residual computation, which is discussed in subsection 4-1-1. Furthermore, the method utilised for residual evaluation, and its implementation are detailed in subsection 4-1-2.

4-1-1 State estimations and residual computation

The states of the nominal physical behaviour can be estimated by employing an observer. The observer will correct the state estimates if the output estimations deviate from the measure-

ments. Commonly employed techniques for state estimations in Linear Time-Invariant (LTI) systems include the Luenberger observer and the Kalman filter. In contrast to the Luenberger observer, the Kalman filter can be utilised to compute state estimates for systems that involve process and measurement noise by integrating the statistical model of the noise. Since the measurements include noise, the Kalman filter will be used for the state estimations.

First, the mathematical notation and the conditions of how the Kalman filter ensures convergence are provided. Thereafter, the practical implementation of the Kalman filter in relation to the dynamics of the water storage unit is described.

Considering the following LTI system with the state space model:

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k, & w_k &\sim \mathcal{N}(0, Q) \\ y_k &= Cx_k + Du_k + v_k, & v_k &\sim \mathcal{N}(0, R) \end{aligned} \tag{4-1}$$

Where $x_k \in \mathbb{R}^n$ is the state, u_k the control input, $w_k \in \mathbb{R}^n$ the process noise, which is assumed to be Gaussian with zero mean and a covariance Q, $y_k \in \mathbb{R}^m$ the measurement, and $v_k \in \mathbb{R}^m$ the measurement noise, a Gaussian random variable with zero mean and a covariance R. It is important to note that of the covariance matrices Q and R, at least one should be positive-definite and the other at least positive semi-definite. The linear system should be detectable to reconstruct the states, which holds if and only if the unobservable modes are stable [73].

Given the system's state space model in Equation 4-1, the Kalman filter performs two steps: the time update and the measurement update [67]. The time update is denoted by:

$$\begin{aligned} \hat{x}_{k+1|k} &= A\hat{x}_{k|k} + Bu_k \\ P_{k+1|k} &= AP_{k|k}A^T + Q, \end{aligned} \tag{4-2}$$

where $\hat{x}_k \in \mathbb{R}^n$ is the state estimate, and $P_k \in \mathbb{R}^{n \times n}$ is the covariance matrix of the state estimate. The measurement update with K_k being the Kalman gain is represented by the following:

$$\begin{aligned} K_k &= P_{k|k-1}C^T \left(CP_{k|k-1}C^T + R\right)^{-1} \\ \hat{x}_{k|k} &= \hat{x}_{k|k-1} + K_k(y_k - C\hat{x}_{k|k-1}) \\ P_{k|k} &= P_{k|k-1} - P_{k|k-1}C^T(CP_{k|k-1}C^T + R)^{-1}CP_{k|k-1}. \end{aligned} \tag{4-3}$$

The Kalman filter is unbiased and has a minimum variance, which means that the Kalman gain minimises the estimate's covariance. Given proper system dynamics and noise characteristics, the estimation will converge to the true state over time.

After providing the theoretical foundations of the Kalman filter, including the mathematical equations utilised and the conditions for which the filter ensures convergence, the next step is to apply the Kalman filter to the water storage unit model.

Measurements

One of the Kalman filter's assumptions is that the measurement noise must be zero mean. However, in the case of the volume measurements, there is non-zero mean noise.

When looking at the open-loop simulation of the volume dynamics, there is an increasing distance between the estimated and measured volumes. This can be seen in Figure 4-1, where the volume is estimated to be constant when the reservoir is not drained or replenished.

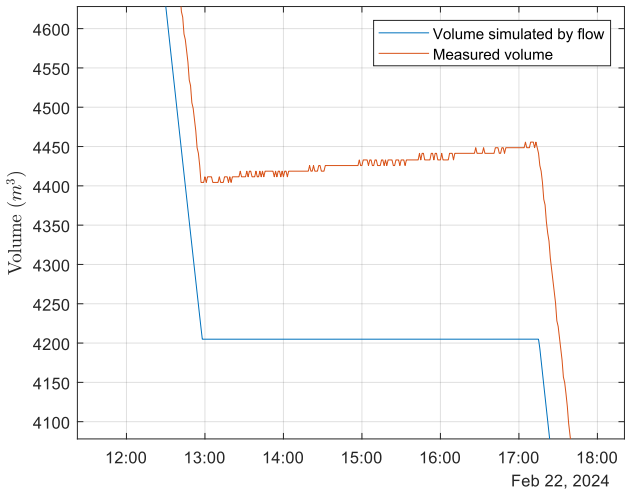


Figure 4-1: Estimated volume in blue and measured volume in red

A possible explanation for the increase in volume could be the backflow of the water in the pipes after the draining is stopped. The inertia of the water will be high when the draining is stopped, meaning that water will move out of the reservoir but is being blocked by the closing valves. However, when estimating the total volume of the pipes between the reservoir and the valves, this does not add up to the increase in volume. Another explanation could be that the water's surface is not homogeneously distributed, especially during draining. This means that when this process is stopped, there will be some change on the water surface. If this were visible in the sensor readings, fluctuations with a constant mean would be expected, and after an hour of draining, the amplitude of the oscillations would be dampened out. Since these potential physical causes of backflow are negated, it could be that the sensor is undergoing some systematic error. Ageing and environmental factors can lead to sensors producing measurement errors. Measurement errors can be categorised as random errors, such as noise and systematic errors. Systematic errors can be drifting or fixed biases [71]. Drifting refers to the dynamic difference between the measured value of the sensor and the true values, often caused by changing ambient temperature and time [62]. Since the volume measurements contain a drift, this drift causing the non-zero mean of the noise must be estimated since the Kalman filter assumes zero mean noise. Furthermore, by estimating the drift, the volume estimation will be corrected using an approximation of the actual volume measurement.

Application of the Kalman Filter

The differential state will be augmented with the state d_k to estimate the drift in the sensor's measurements and ensure better convergence of the volume estimation. As previously stated, the dynamics of the water storage unit can be described by a semi-explicit differential algebraic

equation. Therefore, when applying the Kalman filter to create the state estimations of the water storage unit, the time update step described in Equation 4-2 will include an algebraic equation: $g(\cdot) = 0$, to estimate the flow rate, which then used as an input for the differential equation.

These adaptations lead to the following expression for the time update:

$$\begin{aligned} g(\hat{x}_{k|k}, \hat{z}_{k|k}, \theta_k) &= 0 \\ \begin{bmatrix} \hat{x}_{k+1|k} \\ \hat{d}_{k+1|k} \end{bmatrix} &= \tilde{A} \begin{bmatrix} \hat{x}_{k|k} \\ \hat{d}_{k|k} \end{bmatrix} + \tilde{B}\hat{z}_{k|k} \\ g(\hat{x}_{k+1|k}, \hat{z}_{k+1|k}, \theta_k) &= 0 \\ P_{k+1|k} &= \tilde{A}P_{k|k}\tilde{A}^T + Q \end{aligned} \tag{4-4}$$

Where $\tilde{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\tilde{B} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\tilde{C} = \begin{bmatrix} 1 & 1 \end{bmatrix}$, θ_k is the valve angle, $\hat{z}_k$ is the algebraic state defined by solving the equation $g(\hat{x}_k, \hat{z}_k, \theta_k) = 0$. Various expressions exist for the function of $g(\cdot)$ and the definition of $\hat{z}_k$, considering the different operational modes described in chapter 3. The measurement update step will be implemented with the augmented state vector as denoted in Equation 4-3.

The augmented state space is unobservable since the observability matrix does not have full column rank. Since the eigenvalue of the unobservable state is one, this does not ensure stability and, thus, detectability. Nevertheless, the drift state is modelled to be constant, showing marginal stability. Thus, it will not exhibit unbounded growth, implying instability nor asymptotic stability. To ensure convergence of the error dynamics, it is crucial to appropriately set the initial conditions for the Kalman filter, and the system model must precisely capture the noise characteristics. Estimating the covariance matrix of the process noise typically involves utilising the system model and comparing it to the actual state measurements. However, in this specific scenario, it is known there is a drift in the measurements, inducing the actual state measurements to be unknown. Nonetheless, an estimation of the process noise covariance is made in both states. The reservoir has a cross-section of 1772 m^2, and given the flow measurements, the volume change can be neglected compared to the outflow of the outlet. Therefore, the process noise covariance will be small, the initial guess is $1 \cdot 10^{-4}$, and the drift covariance is estimated to be $1 \cdot 10^{-3}$.

Due to the drift in the volume measurements, it is unlikely to obtain an accurate estimation for the measurement noise by estimating the covariance of the difference between the measurements and the estimate. Therefore, an initial guess of a covariance of 30 is used. Given the initial guess for the Kalman filter, the states are estimated and compared with the volume measurements, composing the residual, which has a covariance of 180. Given the higher measurement covariance, the Q matrix is updated accordingly to $Q = \begin{bmatrix} 1 \cdot 10^{-3} & 0 \\ 0 & 1 \cdot 10^{-2} \end{bmatrix}$. Q is positive semi-definite, and R is positive definite.

The estimated output and volume measurements are shown in Figure 4-2 using the measured flow rate as input and the designed Kalman filter. The model parameters are estimated using a sampling time of one second. Since the measurements are sampled in one minute, the update step is only computed every minute. After interpolating the estimated values to a sampling

time of one minute, the observer error is calculated and shown in Figure 4-3. These figures show that the Kalman filter could reconstruct the state estimates, including the marginal stable unobservable state, and converge the estimated output to the volume measurement.

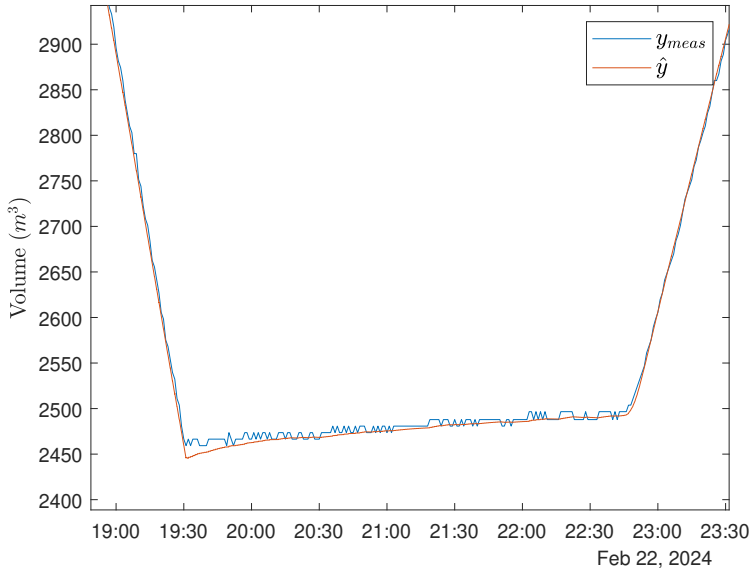


Figure 4-2: Measured volume is denoted in blue, and the updated estimated volume using the Kalman filter is shown in red.

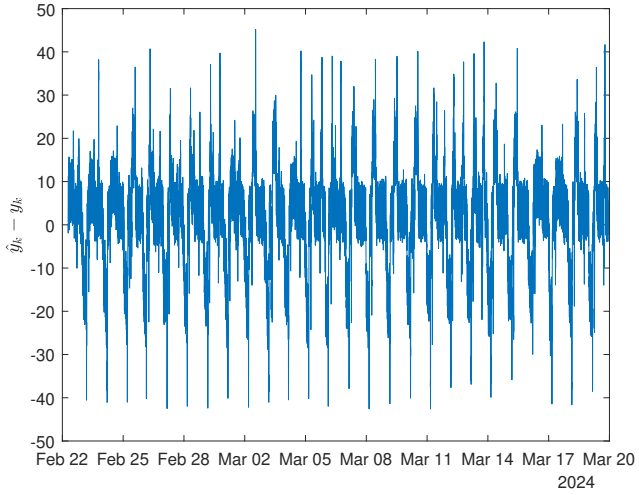


Figure 4-3: Observer error

The Kalman filter is applied to estimate the volume and the drift present in the volume measurement to ensure optimal convergence of the state estimates. Combined with the flow rate estimates by solving the algebraic equation each time step, the water storage unit's volume and flow rate residuals can be computed as the following:

$$\begin{aligned} r_1(k) &= y(k) - \hat{y}(k) \\ r_2(k) &= z(k) - \hat{z}(k), \end{aligned} \tag{4-5}$$

where $r_2(k)$ is a vector containing the residual of the replenishing and the draining flow rate.

4-1-2 Residual evaluation method

After the residual computation in the previous section, residual evaluation represents the final step essential for detecting potential attacks. As described in section 2-3, change detection methods can be deterministic or probabilistic. Deterministic methods, like limit checks, are straightforward to evaluate and define. However, they only consider the residual at a specific instant and rely on predefined limits. On the other hand, probabilistic tests, such as t-test or Chi-squared, utilise the probability distribution of a random variable to detect changes in mean and variance [25]. The drawback is that many samples are necessary before and after the change to verify the null hypothesis with good significance, causing a delay in detection. Detecting cyber-physical attacks within a water distribution network requires minimising the time needed for detection as much as possible.

Another commonly utilised method for probabilistic change detection is the CUSUM method [12]. It involves calculating the cumulative sum of the log-likelihood of observations. This approach enables the detection of change in a shorter period of time compared to methods such as the chi-squared probability test, making it suitable for detecting cyber-physical attacks where rapid detection is critical for effective mitigation. The statistical foundation on which the method is based will be elaborated in the next part.

Considering a sequence of independent random variables $z(i)$, $i = 1, 2, ..., k$ with the probability density function $p_\theta(z)$ dependent on θ. To illustrate the theorem, θ is the mean of a Gaussian distribution. Before an unknown change instant θ is equal to θ_0, after which the parameter will change to θ_1, with their corresponding probability distributions $p_{\theta_0}(z)$ and $p_{\theta_1}(z)$ [12]. Given that, for example, p_{θ_0} and p_{θ_1} are two probability density functions of the Gaussian distributions with the mean $\mu_0 = 0$ and $\mu_1 = 2$, and with the same variance $\sigma^2 = 1$. Take a random sample $z = -0.2$, the realisation is most often in the neighbourhood of μ_0, leading to $\frac{p_{\theta_0}}{p_{\theta_1}} < 1$ and therefore the natural logarithm is negative. The log-likelihood ratio $s(z)$ of an observation z has the following fundamental statistical property that the CUSUM exploits:

$$\begin{aligned} s(z) &= \ln \frac{p_{\theta_1}(z)}{p_{\theta_0}(z)}, \\ E_{\theta_0}(s) &= \int_{-\infty}^{\infty} s(z) p_{\theta_0}(z) dz < 0, \\ E_{\theta_1}(s) &= \int_{-\infty}^{\infty} s(z) p_{\theta_1}(z) dz > 0. \end{aligned} \tag{4-6}$$

The CUSUM is denoted by the following equation, as previously described in Equation 2-3:

$$S(k) = \sum_{i=1}^{k} s(z(i)) = \sum_{i=1}^{k} \ln \frac{p_{\theta_1}(z(i))}{p_{\theta_0}(z(i))}.$$

According to the statistical properties described in Equation 4-6, $S(k)$ is expected to exhibit a negative drift before the change and a positive drift after the change from θ_0 to θ_1.

The probability distribution of the abnormality should be known to implement the CUSUM. However, in the case of the cyber-physical attack, with an adaptive adversary possessing system knowledge, there will likely be a non-stationary residual $z(k)$. Additionally, if there is a focus on several predefined anomalies, there is a possibility that the attack will remain undetected. Therefore, in research, a Non-Parametric Cumulative Sum (NP-CUSUM) independent of the statistical model of a specific anomaly is utilised successfully to detect cyber-physical attacks on the Water Distribution Network (WDN) [9], [16], [30]. Thus, this non-parametric change detection method is implemented to detect cyber-physical attacks against the WDN within this research. The following section describes the mathematical derivation of the NP-CUSUM and its application with regard to the water storage unit dynamics.

Non-parametric CUSUM

The NP-CUSUM method exploits the fundamental statistical property of the CUSUM as described in Equation 4-6. Adapting it such that it is independent of the probability p_θ. The expected value of the random process $z_i(k)$, is required to be less than zero i.e. $\mathbb{E}_0[z_i(k)] < 0$ under the null-hypothesis H_0, and under H_1, it will be greater than zero, i.e., $\mathbb{E}_1[z_i(k)] > 0$. To ensure the constraint on the expected value of the null hypothesis holds for the system under healthy conditions, a small positive parameter b_i is introduced such that:

$$\mathbb{E}_0\left[n_i(k)\right] < 0, \quad \text{where} \quad n_i(k) = |\tilde{y}_i(k) - \hat{y}_i(k)| - b_i. \tag{4-7}$$

The NP-CUSUM statistic for each sensor i will be:

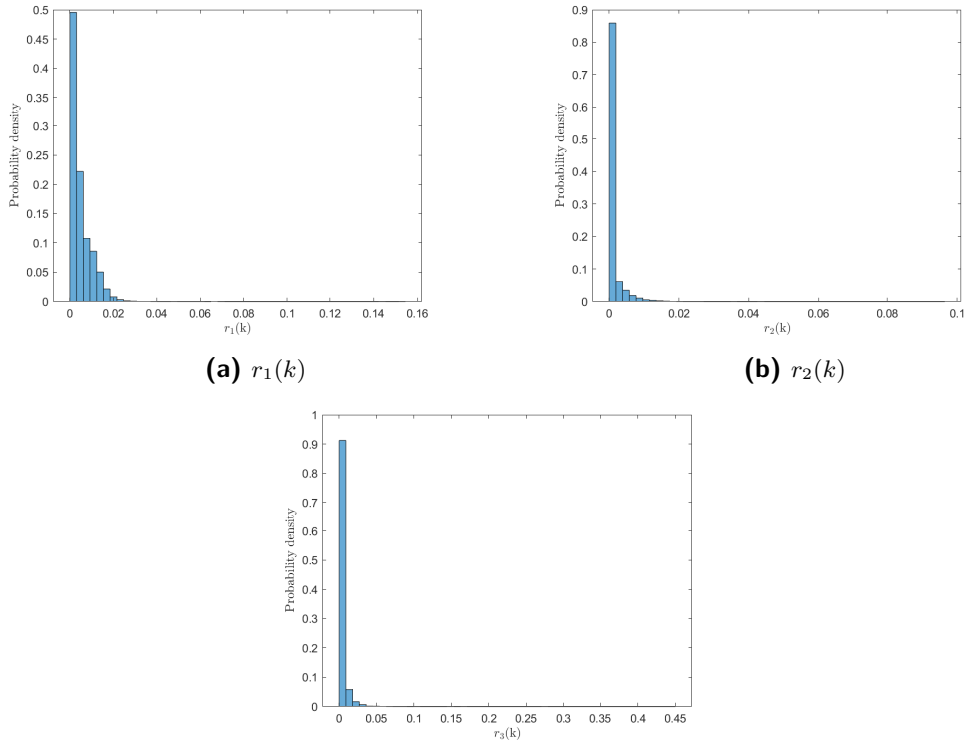
$$S_i(k) = \left(S_i(k-1) + n_i(k)\right)^+, S_i(0) = 0, \tag{4-8}$$

within the equation, the "+" in the upper right of $(a)^+$ indicates that when $a > 0$, $(a)^+ = a$; when $a \leq 0$, $(a)^+ = 0$. The corresponding decision rule is the following:

$$d_{N,i} \equiv d_\tau\left(S_i(k)\right) = \begin{cases} H_1 & \text{if } S_i(k) > \tau_i \\ H_0 & \text{otherwise ,} \end{cases} \tag{4-9}$$

where τ_i is the detection threshold, the probability distribution of the residuals is evaluated to determine the values b_i for each parameter. The residuals are denoted $r_i = |y_i(k) - \hat{y}_i(k)|$, the probability distribution of the residuals corresponding to the volume, draining and replenishing flow rate estimations, using the data set listed in the Appendix, are depicted in Figure 4-4. The probability distribution is visualised using a histogram, and the bin size is determined by setting the number of bins to 50 for each parameter.

The values for b_i are determined by the right endpoint of the bin with the highest probability. The bin with the highest probability of both flow rate residuals has a probability between 0.8 and 0.9, while the bin with the highest probability of the volume residual has a probability of 0.5. The expected value for n_1, corresponding to the volume, is higher than the expected value for $n_i(k)$ for the flow rates. Therefore, b_1 is increased to 0.006, allowing higher residuals



(a) $r_1(k)$ **(b)** $r_2(k)$

(c) $r_3(k)$

Figure 4-4: Probability distribution of $r_i(k)$

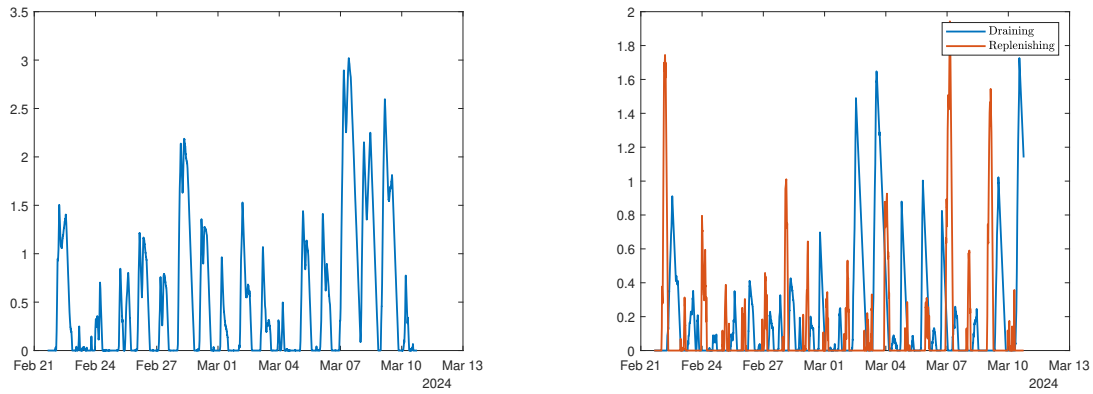
and an expected value of -0.0061. The values for b_i and the corresponding expected values for $n_i(k)$ are shown in Table 5-1. With the determined values for $b_i, i = 1, 2, 3$, the constraint stated in Equation 4-7 will hold.

	b_i	$\mathbb{E}_0[\lvert y_i(k) - \hat{y}_i(k)\rvert - b_i]$
i = 1	0.006	-0.0061
i = 2	0.002	-0.0012
i = 3	0.009	-0.0066

Table 4-1: Parameters for b_i and the corresponding expected value of n_i. Where $i = 1$ represents the volume, and $i = 2$ and $i = 3$ the draining and replenishing flow rates.

Figure 4-5 displays the result of the NP-CUSUM using data describing nominal behaviour. The NP-CUSUM shows non-zero values in the case of healthy dynamics, which can be attributed to unmodelled dynamics and model uncertainty. Therefore, a threshold should be determined below which the NP-CUSUM indicated healthy behaviour and beyond which an anomaly is detected. In the next chapter, the magnitude of the thresholds will be derived.

Together with the state estimations obtained by the Kalman filter and measurements, the residuals for the volume and the flow rates are computed. Subsequently, the NP-CUSUM is applied to evaluate the residuals and detect possible abnormalities. The probability of the residuals is utilised to determine the values for b_i, ensuring that the expected value of n_i is below zero.



(a) Nominal volume measurements

(b) Nominal draining flow measurements in blue, and nominal replenishing flow measurements in red.

Figure 4-5: NP-CUSUM using measurements of a healthy system

In summary, with state estimations, residual computation and the implementation of the NP-CUSUM, a model-based anomaly detection method is developed to detect cyber-physical attacks targeted at the water storage unit.

4-2 Design of cyber-physical attacks

The design of a cyber-physical attack should consider the specific location of the attack and the intended objective. Considering these factors, it is possible to determine the type of attack that should be developed to achieve the desired goals. In this research, multiple levels of an attacker's effort are explored. The first level involves a replay attack, which can be carried out without additional system knowledge. This could, for example, be executed by a random hacker. The second level comprises a more sophisticated attacker that actively leverages system knowledge to evade detection. As described in chapter 1, it is imperative to subject the designed detection mechanisms to sophisticated attacks aimed at evading detection and inflicting harm upon the system. This section depicts the attack specifications and the algorithms employed to simulate the attacks. It also describes how the physical impact of the designed cyber-physical attacks is assessed.

Two separate data sets are used to collect input data and replay data for the attacks when implementing cyber-physical attacks. Both data sets cover at least seven days of data covering the different demands during the week. The exact data sets used are listed in Table A-1 in the Appendix.

4-2-1 Attack location

When examining the Industrial Control System (ICS) of Dunea's WDN, the centralised control system, referred to as the carousel, serves as the supervisory level control level. It provides control inputs to switch modes of operation for the water storage units where additional

controllers are distributed to control the Motor-Controlled Valves (MCVs) and control the shutdown of the pump when the reservoir is full.

Cyber-physical attacks that could be executed include changing the control logic of a controller, closing a valve, damaging a pump or destroying a sensor. However, physical access to the water storage unit is needed to carry out these proposed attacks. Another possible location for an attack is the communication between the supervisory control level and the water storage unit.

The communication between the supervisory control level and the water storage unit will presumably be provided via level 2 communication protocols such as Ethernet/IP or Modbus/IP protocols. While these protocols have enabled communication between level 2 and 3 devices, they have vulnerabilities. The components, such as switches and routers used in these applications, are also vulnerable. When a malicious attacker has gained access to the enterprise network, it can exploit these vulnerabilities, leading to possible disclosure, disruption and deception attacks targeted at the physical system.

The attack location is selected between the supervisory control system and the Intelligent Electronic Devices (IEDs) at the water storage unit. The existing communication architecture enables communication between control components and field devices once access is gained, which can be accomplished from any location worldwide. This eliminates the necessity for physical access to the system and makes it a more likely and convenient target for an attack.

Given the attack location, the attack will be executed as a Man In The Middle (MITM) attack. Since MITM attacks are performed at the Supervisory Control and Data Acquisition (SCADA) client server device endpoint due to their communication protocol giving an easy way in. In this attack, the attacker can capture communication traffic passing through the network, including data transmitted by the targets [43]. Even though the control within the WDN is regulated utilising Distributed Control System (DCS) components, the MITM attack can be exploited in the same manner as described above because the vulnerabilities of the TCP/IP communication protocols between the DCS devices and the Input/Output (I/O) devices distributed throughout the field can be manipulated as a MITM attack.

4-2-2 Attack objective

The designed anomaly detector should be evaluated against potential cyber-physical attacks on the water storage unit. The defined attack objectives should cover extreme cases that could significantly impact the WDN due to the attacks targeted at the water storage unit.

In collaboration with the operators of Dunea, the following two attack objectives are formed:

- Ensuring none to limited water in the reservoir a high demand
- A full reservoir when there is excess produced drinking water

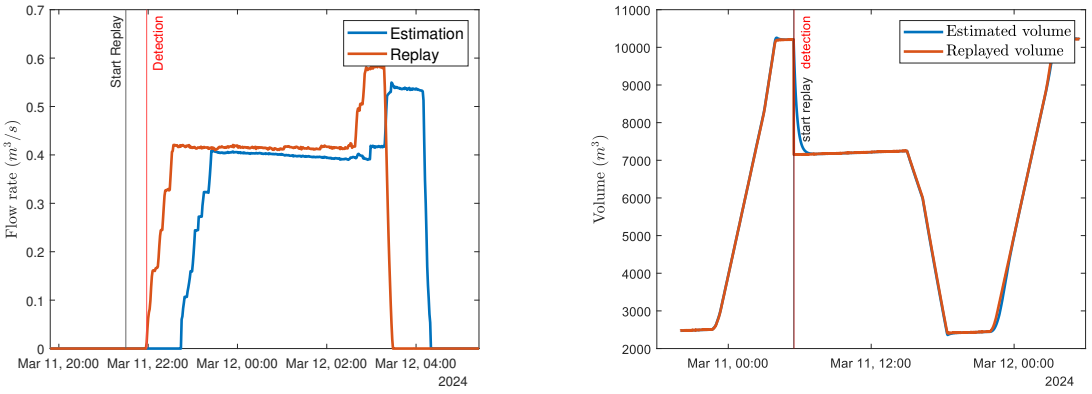
4-2-3 Replay attack

These attack objectives will be carried out through full and empty reservoir attacks as MITM attacks. An example of a MITM attack is a replay attack, which will be considered the

first to develop. The replay attack collects a finite horizon of communication data under normal conditions. After that, the recorded data is transmitted to the Human Machine Interface (HMI) monitors of the operator, while field devices can be jammed or operated at a different setpoint. This shows that no prior knowledge of the system is necessary for the replay attack, matching the first attacker profile.

In terms of the input signals, the full reservoir attack aims to disrupt the communication signal of the pump initialisation, thereby preventing the reservoir from draining. Conversely, the empty reservoir attack aims to disrupt the nonzero setpoints of the MCVs communicated by the centralised control system, thereby preventing the reservoir from replenishing. No additional logic is needed for the output signals, as the prerecorded measurement data of the draining and replenishing flow rate, volume, pressure, and valve angles can be replayed at the start of the attack.

If Dunea had a simple logical data validation system that uses process knowledge, this could entail validating a flow rate between 0.2 and 0.3 m^3/s if one pump is on and a flow rate between 0.45 and 0.58 m^3/s if two pumps are on. Moreover, there is no flow rate when the pumps are off and the valves are closed, and the flow rate is between the range of $0.065\,m^3/s$ and $0.7\,m^3/s$ when the Flow Controlled Valves (FCVs) are open. Additional logic can be derived for the volume change. Then, if this data validation is in place, the MITM attack replaying measurements will be easily discovered.



(a) Flow rate empty reservoir attack.

(b) Volume full reservoir attack

Figure 4-6: Replayed volume is denoted in red, and the estimated volume is in blue. The black vertical line indicates the start of the attack and the red vertical line indicates the instant the attack is detected by data validation.

From Figure 4-6a, it is notable that shortly after the start of the replay, the attack is detected by a simple logic check, as the setpoint to the FCVs is zero. The full reservoir is detected instantly since there is a significant difference between the replayed volume and the estimated volume, as shown in Figure 4-6b.

4-2-4 Advanced MITM attack

Considering the replay attack can easily be detected by simple logical implementations of data validation and limit checks, an advanced MITM attack is designed to remain undetected

whilst accomplishing its objectives and causing as much damage as possible. Due to unknown control logic, such as the carousel, and the impact of the attack on the water distribution network, it is not possible to analyse the influence of the water distribution network only on the water storage unit itself. This means that only an estimation of the time to detection can be made as other parameters are affected, and changes in control input to the water storage unit can not be considered. In this section, the design of the advanced MITM attacks is described, followed by the algorithms developed to create these cyber-attacks.

The design of the attacks

The attack consists of two parts. The first is the disruption of the input signal from the centralised control system to the water storage unit concerning turning on the pumps or changing the setpoint of the MCV for the replenishment to a nonzero value.

The second part is where the objective of the attack is obtained and the input signals are not disrupted any more. As shown in subsection 4-2-3, if the volume estimate deviates significantly from the measurements, the designed anomaly detector will detect the attack immediately. However, if false data replace the volume measurements, the physical effect of the attack can be exploited even further and detection avoided.

In the case of a full reservoir attack, the reservoir will flood, increasing the water level in the cellar at the water storage unit. Regarding the empty reservoir attack, less water in the system may cause a pressure drop during the period after. A decrease in pressure drop can impact the water quality. Due to the varying changes in the setpoint of the MCVs, the chance of being detected because of the replayed data deviating from the estimated flow rate is higher than because of the deviation caused by the water pressure due to the high-water level of the reservoir.

Therefore, for the second part of the attack false data of the volume measurements is calculated by the real-time flow rate and injected to remain undetected for as long as possible and increase the damage to the system beyond the attack objective.

Given this design, the following attacks will be launched at the communication of the measurements of the water storage unit to the centralised control system:

- False data injection of the volume measurements
- Replay of the pressure when the system is non-idle
- Replay of the flow rate when the input communication signal is disrupted
- Replay of the valve angle measurements when the input communication signal is disrupted

The replay data is collected via a disclosure attack, where the attacker can eavesdrop and obtain sensor data. For the water storage unit in draining mode, measurement data of the draining flow rate is selected in case one pump is on and two pumps are on.

In section A-4, Algorithm 1 describes the algorithm used to simulate the full reservoir attack. Where u_5, u_6 are the input signals from the centralised control system, zero off and one on.

The flags for the pumps are used to indicate which pumps are on. Since the valve angles of MCV_{36} and MCV_{37} are not 0 or 90 the first minute of the dynamics of the pumps being only in this case the valve measurement is inserted, for the remaining just the value of 90 is used. Additionally, prevent valve angle insertion below 90 if the replay data set is smaller than when the pumps are on.

In section A-4, Algorithm 2 describes the algorithm used to simulate the empty reservoir attack.

To summarise, the replay attack can be executed by eavesdropping the communicated signals without additional resources. However, these attacks can easily be detected, and the attack objectives will not be obtained. Therefore, an advanced attack is developed where process knowledge is utilised, and the attack is dependent on the system's current dynamics.

4-2-5 Physical impact

The real volume is constant during the disruption of the input signals. Afterwards, when the input signals are not disrupted any more, the model derived in chapter 3 is used to estimate the system's dynamics. However, this is an estimation of the dynamics since the disruption of the input signals may have led to a change in pressure, and the volume of the other reservoirs may be different thereby, the control inputs by the carousel could be different as well. The actual volume is simulated using the estimated flow rates.

The reservoir's overflow is estimated at 14000 m^3, and an internal safety mechanism will stop the pumps when the reservoir reaches a specified low level, which is estimated at 0.9-meter water level, resulting in $\approx 1600\, m^3$.

Chapter 5

Cyber-Attack Detection Results

This chapter presents the result of implementing the anomaly detector designed in section 4-1 to detect the advanced cyber-physical attacks developed in section 4-2. In section 5-1, the determination of the thresholds for the Non-Parametric Cumulative Sum (NP-CUSUM) for each parameter is described. Subsequently, the detection results of the full reservoir and empty reservoir are depicted in section 5-2 and section 5-3. Lastly, the results are summarised in section 5-4.

5-1 NP-CUSUM thresholds

The determination of the threshold τ will be a trade-off between the False Alarm Rate (FAR) and the Time To Detection (TTD), described in subsection 2-3-3. For the magnitudes of τ, a FAR of 1% is allowed and calculated using a new data set, different from the data used for determining b_i. The dynamics of the water storage unit are simulated utilising a data set of 18 days as this was the maximum amount of data available. However, in the future, when larger datasets are obtained, these same thresholds can result in a different FAR. Increasing the simulation time increases the likelihood of more and higher peaks. However, because the length of the data set increases, these spikes will not significantly contribute to the whole data set, making the presence of the spikes less likely. Therefore, the threshold can probably be lowered to obtain a 1% FAR. To estimate these thresholds for a 1% FAR, the data sets are extended by repeating parts of the original data set to create a data set of three months and six months. The corresponding thresholds are shown in Table 5-1 together with the parameters for b_i.

	b_i	τ_i 18 days	τ_i 3 months	τ_i 6 months
i = 1	0.006	2.94	2.84	2.76
i = 2	0.00195	1.58	1.49	1.46
i = 3	0.009	1.68	1.56	1.51

Table 5-1: Parameters for the NP-CUSUM with 1% FAR

The results are evaluated for each threshold defined in Table 5-1. The graphs display the results using the NP-CUSUM with the thresholds τ_i defined for a FAR of 1% corresponding to a data set spanning six months.

5-2 Full reservoir attack

The full reservoir attack is launched for the following three cases: (i) with only one pump turned on, (ii) a varying number of pumps on, and (iii) with two pumps turned on. To illustrate the effect of the full reservoir attack, the estimated volume, tampered volume measurements, and the actual volume of the attack in case (iii), two pumps turned on are depicted in Figure 5-1. The reader is referred to Appendix A-5 for the figures showing the attack's impact under the other cases. These figures show that the estimated volume follows the tampered volume measurements accurately. Furthermore, the actual volume remains constant from the start of the attack until the reservoir is replenished, leading to an overflow at 01:04, resulting in the spillage of 200 m^3 of water.

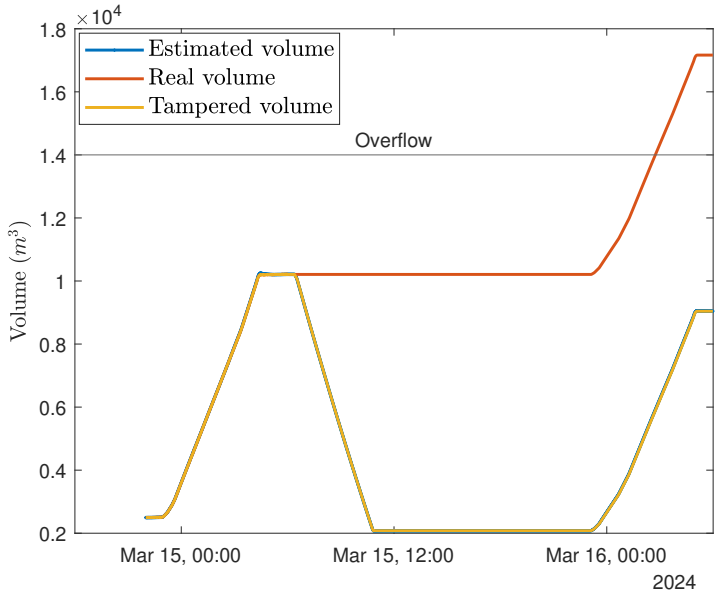


Figure 5-1: Physical impact of the full reservoir attack, in the case the two pumps are on. The estimated volume is indicated in blue, the actual volume is in red, and the tempered volume measurement is in yellow.

In regard to case (i), where a single pump is active, the measured and estimated flow rate is shown in Figure 5-2. It is important to note the distinction between the measured and replayed flow rates, emphasising that only the flow rate during the draining process is replayed. However, the anomaly detector treats both values as measurement data across all the cases.

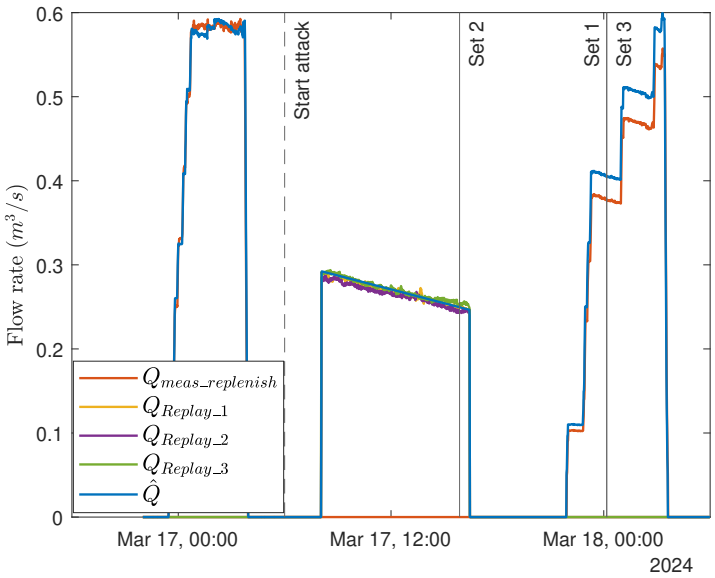


Figure 5-2: Flow rates during the full reservoir attack simulated while one pump is on during the reservoir drainage. The measured replenishment flow rate is indicated in red, the replayed data sets during the reservoir draining are in yellow, purple and green, respectively, and the estimated flow rate is in blue. The vertical dashed line indicates the start of the attack, and the continuous black line indicates the detection of the corresponding replay set.

Figure 5-3 and Figure 5-4 show the NP-CUSUM for the draining flow rate, the volume and the replenishment flow rate, respectively. From these figures it can be observed that the replay sets that were not detected during the draining were subsequently detected within a two-hour time frame during the replenishment phase. For each case, anomalies were detected during replenishment if not previously identified during draining because the estimated flow rate is higher than the measured replenishing flow rate. The difference between the real volume and the estimated volume can explain this. Consequently, a lower volume reduces counterpressure, resulting in a higher flow rate.

The results of the NP-CUSUM regarding the replenishing flow rate and the volume regarding the other cases can be found in Appendix section A-5.

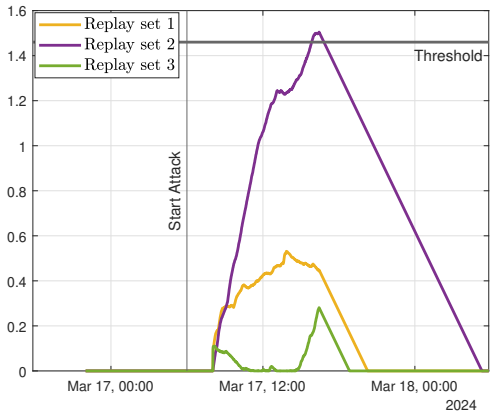
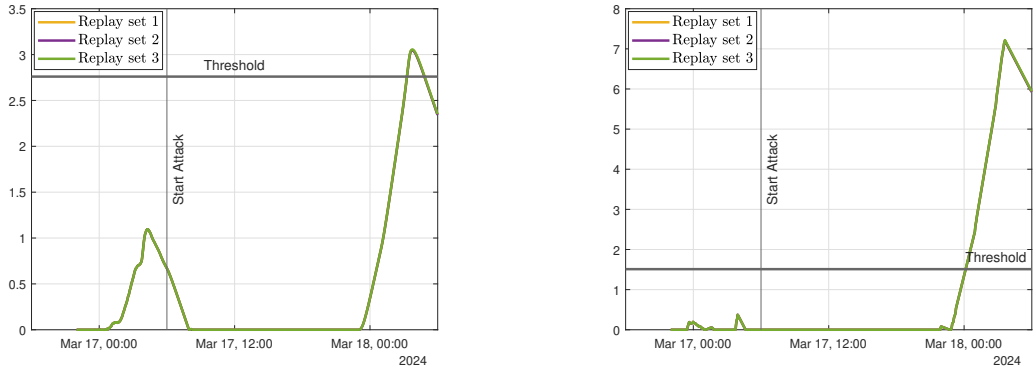


Figure 5-3: NP-CUSUM draining flow rate of the full reservoir attack with one pump on while draining. The threshold indicated in blue, the NP-CUSUM of the replay sets 1, 2 and three are in yellow, purple and green, respectively.

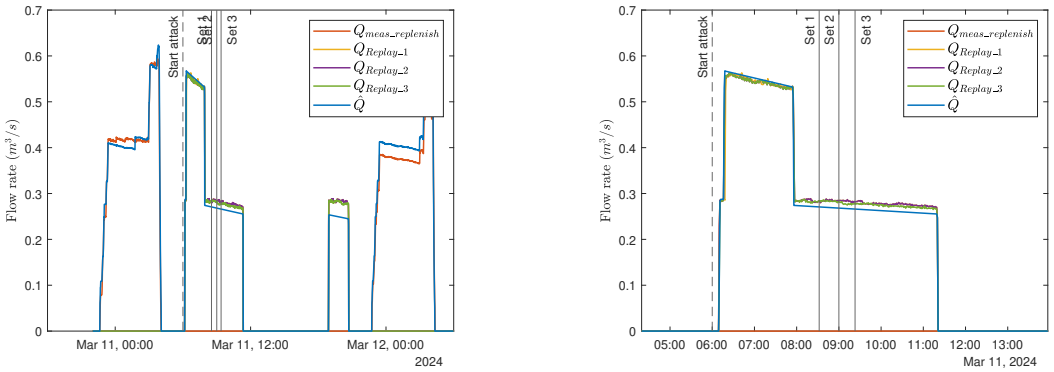


(a) NP-CUSUM volume

(b) NP-CUSUM replenishing flow rate

Figure 5-4: NP-CUSUM of the volume and replenishing flow rate. The NP-CUSUM of the replay sets 1, 2 and three are in indicated yellow, purple and green, respectively.

For the case (ii), a varying number of pumps being on, the flow rates are shown in Figure 5-5 and the result of the NP-CUSUM can be seen in Figure 5-6. These figures show that when the number of pumps is reduced to one pump after draining the reservoir with two pumps, all three of the replay data sets are detected as the estimated flow rate is significantly lower than the replayed flow rates. All replay sets are detected within less than an hour's difference.



(a) Flow rate with varying pumps during the full reservoir attack.

(b) Flow rate with a varying number of pumps zoomed in on the draining flow rate.

Figure 5-5: The measured replenishment flow rate is indicated in red, the replayed data sets during the reservoir draining are in yellow, purple and green, and the estimated flow rate is in blue. The vertical dashed line indicates the start of the attack, and the continuous black line indicates the detection of the corresponding replay set.

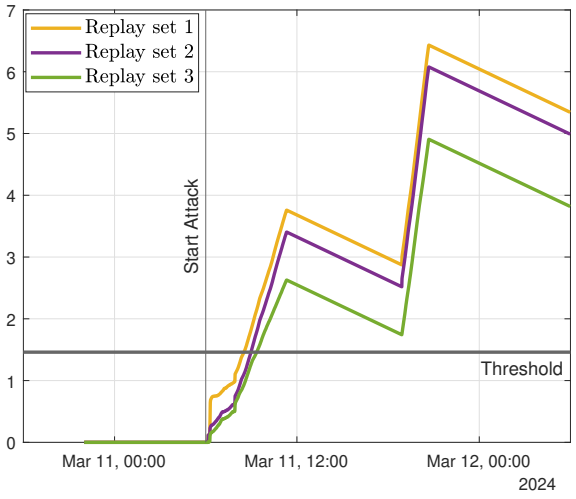


Figure 5-6: NP-CUSUM draining flow rate of the full reservoir attack with a varying number of pumps on while draining. The NP-CUSUM of the replay sets 1, 2 and three are indicated in yellow, purple and green, respectively.

For the case (iii), two pumps being on while draining the reservoir, the flow rates are shown in Figure 5-7, and the result of the NP-CUSUM evaluating the draining can be seen in Figure 5-8. From these figures, it can be observed that the replay data sets do not differ significantly from the estimated flow rates and, therefore do not exceed the threshold. The anomaly is detected after the disruption of the draining input, leading to an overflow of the reservoir when entering the replenishing mode.

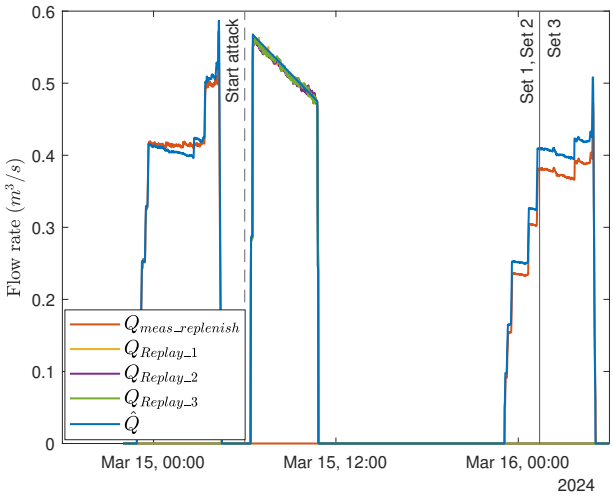


Figure 5-7: Flow rate with two pumps on while draining during the full reservoir attack. The measured replenishment flow rate is indicated in red. The replayed data sets during the reservoir draining are in yellow, purple and green. The estimated flow rate is in blue. The vertical dashed line indicates the start of the attack, and the continuous black line indicates the detection of the corresponding replay set.

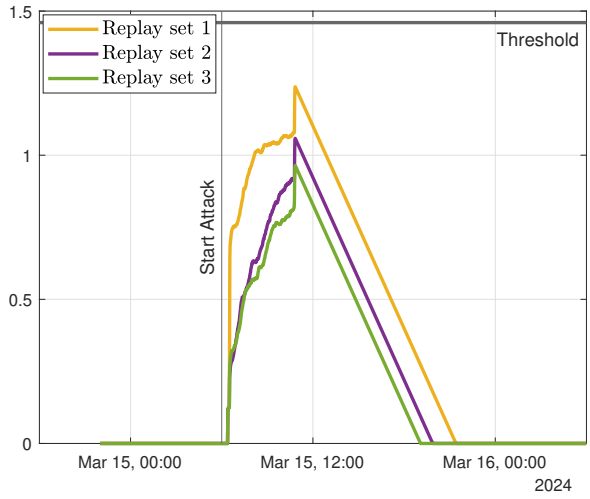


Figure 5-8: NP-CUSUM draining flow rate of the full reservoir attack with two pumps on while draining. The threshold indicated in blue, the NP-CUSUM of the replay sets 1, 2 and three are in yellow, purple and green, respectively.

The TTD for each case and the various replay sets considered are denoted in Table 5-2 evaluated by the three different values of the thresholds. From this table, it can be noticed that the lower values of the thresholds lead to the detection of one of the replay sets concerning the case of one pump turned on. Furthermore, the lowering of the threshold results in a reduction of the TTD with a maximum of 9 minutes. The TTD for the cases where two pumps are turned on, and one pump is turned on, except for replay set number two, varies

based on the post-draining mode event. In these scenarios, the attack detection occurs upon entry into the replenishing mode. If this would have occurred three hours later, the TTD would have been approximately 360 minutes longer.

τ :	18 days			3 months			6 months		
Replay set:	1	2	3	1	2	3	1	2	3
Input case:									
One	1100	1100	1100	1093	604	1093	1091	593	1091
Varying	164	189	216	157	183	207	153	181	204
Two	1174	1174	1174	1168	1168	1168	1165	1165	1165

Table 5-2: TTD in minutes for the various cases of the numbers of pumps on during the draining mode for the three distinct thresholds τ defined in Table 5-1.

5-3 Empty reservoir attack

The empty reservoir attack is simulated by utilising three distinct input signals collected from the data set, which will be disrupted by the Man In The Middle (MITM) attack. Additionally, four replay sets are employed on the output side to conceal the attack.

To illustrate the effect of the empty reservoir attack, Figure 5-9 shows the volume during the attack for one of the days. This figure shows that the reservoir is drained to its lowest level after disrupting the input signal to replenish it. Consequently, the local control system stops the draining process. The designed attack reaches the empty reservoir in all three input scenarios. The graphs of the other two scenarios are displayed in Figure A-17 and Figure A-18 in Appendix section A-5.

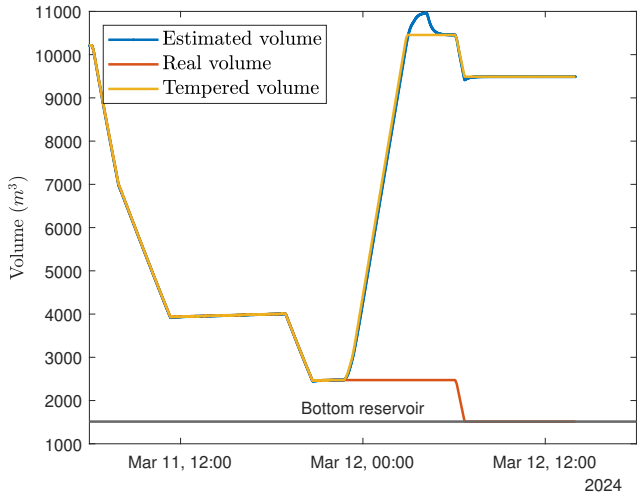
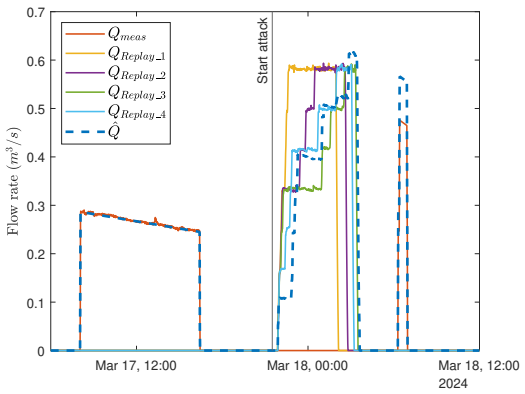
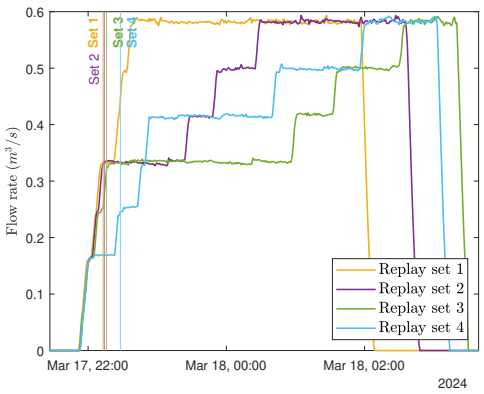


Figure 5-9: Physical impact of the empty reservoir attack simulated by the input data set starting March 16th. The estimated volume is indicated in blue, the actual volume is in red, and the tempered volume measurement is in yellow.



(a) Total overview empty reservoir attack



(b) Replayed replenishing flow rates with the vertical lines indicating the detection of the attack.

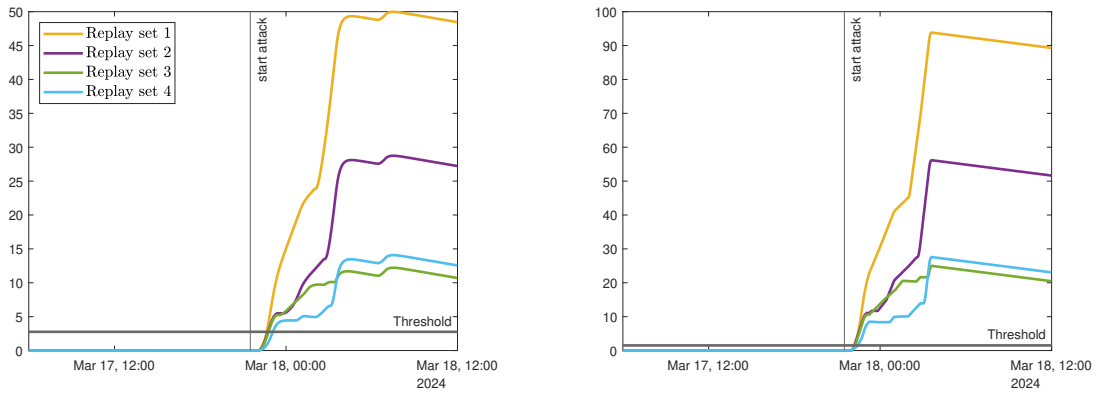
Figure 5-10: Flow rates during empty reservoir attack simulated by the input data set starting March 17th. The measured replenishment flow rate is indicated in red, the replayed data sets during the reservoir replenishment are in yellow, purple, green and light blue, and the estimated flow rate is dashed in dark blue.

The corresponding results of the NP-CUSUM detector are illustrated in Figure 5-11 for the volume and the replenishing flow rate. These graphs and the results in Figure 5-10b show that the anomaly detector can detect the designed empty reservoir attacks. Furthermore, the detector can detect all the attacks in the three selected input data sets. The corresponding graphs for the remaining input data sets depicting the NP-CUSUM results for the volume and flow rate are shown in Appendix section A-5. The time to detection for each input scenario and the various replay sets considered are denoted in Table 5-3 evaluated for the different threshold values.

In contrast to the full reservoir attack, lowering the thresholds does not significantly impact the TTD. This can be explained by the fact that when the estimated flow rate deviates from the replayed flow rate, the significant difference leads to a steep slope in the NP-CUSUM. Additionally, replay set 3 is detected last, considering input cases 1 and 2, and replay set 4 is detected last, regarding input case 3. Notably, in all of the cases, the detection times are close to each other, with some outliers. This can be explained by the fact that the replay sets start deviating after fifteen minutes, and sets 1, 2 and 3 follow approximately the same pattern for another twenty minutes.

τ :	18 days				3 months				6 months			
Replay set:	1	2	3	4	1	2	3	4	1	2	3	4
Input case:												
March 11th	45	46	48	60	44	45	48	59	44	45	47	59
March 15th	114	118	144	125	112	116	142	123	111	115	142	123
March 17th	79	91	99	79	76	89	97	77	74	89	97	77

Table 5-3: TTD in minutes for the attacks considering various input signal scenarios and the multiple replay sets analysed by the detector with three distinct thresholds τ defined in Table 5-1.



(a) Volume **(b)** Replenishing flow rate

Figure 5-11: NP-CUSUM of the volume and the replenishing flow rate during the attack simulated by the input dataset starting March 17th. The NP-CUSUM of the replay sets 1, 2, 3 and 4 are in yellow, purple, green and light blue, respectively.

5-4 Summary

To summarise the results of the NP-CUSUM detecting the designed cyber-physical attacks against the water storage unit. Regarding the full reservoir attack, the NP-CUSUM detected the attacks during the draining mode where various pumps are on. However, in the attacks where there is only one pump on, only one of the replay attacks is detected, and in the case where there are two pumps turned on, none of the replay sets were detected. Although the NP-CUSUM could not detect these attacks during the draining mode, it succeeded in detecting them when the system operates in the replenishing mode.

Regarding the empty reservoir attack, the implemented NP-CUSUM detector can detect the designed attacks regarding the various replay sets and input sets within a range between 44 and 144 minutes. Overall, the designed NP-CUSUM shows promising results for future implementation for detecting cyber-physical attacks and other anomalies at the water storage unit.

Chapter 6

Conclusions and Recommendations

6-1 Conclusion

In this research, a non-linear hybrid automaton is developed to describe the nominal dynamical behaviour of one of Dunea's water storage units. This is achieved by utilising real-time process data, process descriptions, and fluid mechanics principles. Despite unavailable input signals to the pumps and limited information on the pump specifics, a representative model was successfully derived. This model serves as a foundation for equivalent systems and offers a systematic approach to creating similar models for different systems.

Subsequently, this model was utilised to implement a model-based anomaly detection method to detect cyber-physical attacks. Implementing the Non-Parametric Cumulative Sum (NP-CUSUM) using the expected nominal behaviour to derive a ground truth for the null hypothesis. When this hypothesis is falsified, it indicates the presence of an anomaly.

The performance of the anomaly detector is evaluated by simulating multiple Man In The Middle (MITM) attacks. These attacks involved disrupting input signals to the water storage unit and tampering with output signals to deceive operators. Two specific attack scenarios were considered: one aimed at maintaining a full reservoir when there is excess drinking water and another intended to obtain an empty reservoir when there is a high consumer demand. These attacks were carried out with two distinct attacker profiles in mind: a hacker who has been informed to record and replay measurement data while disrupting the input and a more sophisticated attacker aiming to remain undetected by actively understanding the system dynamics.

The results show that the NP-CUSUM anomaly detector detected all simulated attacks during the replenishing mode of operation, demonstrating its potential for detecting cyber-physical attacks. However, the detection of attacks launched during the draining of the reservoir draining was inconsistent compared to the attacks starting during the replenishing, although these attacks were eventually detected as the system was operating in the replenishing mode.

A point for discussion is the impact of the designed cyber-physical attacks on the Water Distribution Network (WDN). This study only assesses the impact on the storage unit, and

potential effects on the carousel and subsequent control inputs remain unknown. Furthermore, in the case of a successful empty reservoir attack, Dunea may be unable to meet the consumers' demand, leading to a decrease in pressure in the network. However, this would be detectable before reaching critical levels compromising water quality. Dunea has strategically placed boosters to address pressure decline. Moreover, in the case of the case of a successful full reservoir attack, excess water in the system can raise pressure to damaging levels. However, this can be mitigated by flooding the reservoirs and the production reservoir and lowering the production rate. But to do so, there is a need for interference by the operators, meaning they first need to be aware of the problem.

The research conducted in this thesis aimed to investigate the detection of cyber-physical attacks on a real-life water storage unit part of the WDN of Dunea through the utilisation of real-time process data. The research question addressed is the following:

"Can cyber-physical attacks targeted against a real-life Water Distribution Network be detected by employing a model-based anomaly detection method?"

The results depicted that the NP-CUSUM anomaly detector effectively detected all simulated attacks during the replenishing mode. The attacks initiated during reservoir draining were not all detected during this mode, though they were eventually detected as the system entered the replenishing phase. In conclusion, real-time process data can be utilised to create a model-based anomaly detector to detect the designed cyber-physical attacks targeted on the water storage unit, which forms a part of the WDN of Dunea.

6-2 Recommendations

Several recommendations for future research have been identified based on the research conducted and the conclusions reached.

Attack profiles
In this thesis, two MITM attack profiles are considered. The first one involves disrupting the input signals of the pump and starting previously recorded data at 06:00. The second one replays measurement data of the flow rate and pressure only at the time instant when disrupting the input signals and for the whole duration of the attack injecting false data of the volume measurements. Considering the second attack profile, the results show that some replay sets were detected during the reservoir draining. This could be explained by the fact that the replay sets were collected when the reservoir volume was significantly lower or higher than the volume at the moment of the attack. Therefore, in future research, if the attack profiles are extended and attacks enhanced to remain undetected, an improvement would be to decide which flow rate data set to replay based on the initial volume at the initiation of the pump.

Concerning detection during the replenishing mode, this may not be effective because the main reason these attacks are being detected is the difference in valve angles of the replayed data. Therefore, further research in designing new advanced attacks would have to involve full knowledge of the system and fluid mechanics to create an attack that will remain undetected for a longer duration. Future strategies for advanced attacks may involve false data injection

of flow rate measurements instead of replayed measurements. The attack flow rate would then be calculated similarly to how the flow rate is estimated right now for the anomaly detector. Considering the model that is used for this anomaly detector is mainly based on measurement data, it would be possible for an attacker to exploit it as well. To summarise, to prolong the duration of remaining undetected, it would be advantageous to continuously inject false flow rate data during the replenishing and replay flow rate from a substantial set of pre-recorded data during the reservoir draining.

Increasing detectibility
The anomaly detector is designed to rely on measurement signals to reconstruct the input signals to the draining mode, as the direct input signals are not available. If an attack disrupts the input signal to the pump without concealing the attack through data replay, the anomaly detector may not detect this attack. However, operators would potentially notice such an occurrence. If these signals become accessible in the future, the detector could potentially detect these attacks.

The results in chapter 5 indicate that some cyber-attacks initiated to disrupt the pump input signals while concealing their actions through the replaying pre-recorded measurement data remained undetected. The passive anomaly detection approach employed to identify these cyber-physical attacks can be classified as a method that operates in an observable manner. Conversely, active detection methods increase detectability by introducing an excitation signal to the system. Watermarking is an active detection method that adds a watermark to authenticate the communication signals. In future research, this could be applied to enhance the integrity of the communicated signal, as has been done in [4]. In this work, Ahmed et al. introduced a physical watermark to the control signals of the WADI testbed, successfully detecting replay attacks targeted at the WADI testbed.

Anomaly detection
In this thesis, anomaly-based detection methods have been studied for their ability to detect cyber-physical attacks. An anomaly-based detection method is used to detect every anomaly in the system, encompassing both faults and cyber-physical attacks. The proposed anomaly detection would serve as an alarming mechanism in a practical implementation. To act upon these alarms, a distinct course of action is necessary for each anomaly, and therefore, faults should be identified accordingly. Possible system faults can be engineered for future applications to formulate multiple realistic fault models, as demonstrated in a previous study by Vrachimis et al. in [68]. If the null hypothesis is falsified and none of the other hypotheses is falsified, this could indicate a cyber-attack or other underlying issue.

Adaptability
Over time, system parameters within the modelled water storage unit might change. These changes could be attributed to factors such as the replacement of valves, decreased efficiency of pumps, and the relative roughness of the pipes decrease. As a result, it is necessary to update the model to maintain an accurate anomaly detector. Updating the model would require preprocessing the measurement data and optimising all system parameters in the same sequence as utilised in the thesis. The data preprocessing can be automated, and the parameter identification codes can be pipelined, thereby minimising the workload involved.

If Dunea intends to create an additional anomaly detector for one of the remaining four water storage units, the methods outlined in this thesis can be applied, provided that all necessary input signals and process data are available. To establish a model, it would be necessary

to identify the system parameters, as the pipework layout may vary, and different types of pumps could be in use.

From this thesis, it becomes evident that after gaining knowledge of the laws of physics involved in the Industrial Control System (ICS) and a comprehensive understanding of the processes and all components involved, an inventory must be made with all the required data and system specifications needed to derive a representative model. When information is absent, assumptions or simplified solutions can be employed with system identification. All the input data to the system is required to model the nominal behaviour of a WDN. Even though this research demonstrated the possibility of modelling the system dynamics accurately using ad-hoc solutions, this approach is not ideal.

Appendix A

Appendix

A-1 Provided process data

Data set	Employed for:
07 August 2023 to 05 October 2023 (5 min)	Training and validation draining dynamics at constant rotational speed
24-hour data (1 sec): 22, 23, 26 February 2024 and 19 and 20 March 2024	Draining dynamics while changing rotational speed
29 December 2023 to 23 February 2024	Replenishing dynamics
22 January 2024 to 21 February 2024	b_i parameter NP-CUSUM
22 February 2024 to 10 March 2024	Threshold NP-CUSUM
22 February 2024 to 20 March 2024	Kalman filter
10 March 2024 to 19 March 2024	Input signals attack design
20 March 2024 to 17 April 2024	Replay signals attack design

Table A-1: Provided process data by Duna. The data provided is sampled at 1 min intervals unless it is stated otherwise.

A-2 System Identification data

A-2-1 Draining mode | Contant rotational speed

In Figure A-1 and Figure A-3 the flow rate and volume measurements utilised for the training of pump 6 and pumps in parallel operating at constant rotational speed are presented respectively. In Figure A-2 and Figure A-4, the correlation between the flow rate and the volume measurements regarding pump 6 and both pumps operating at constant rotational speed are depicted, respectively.

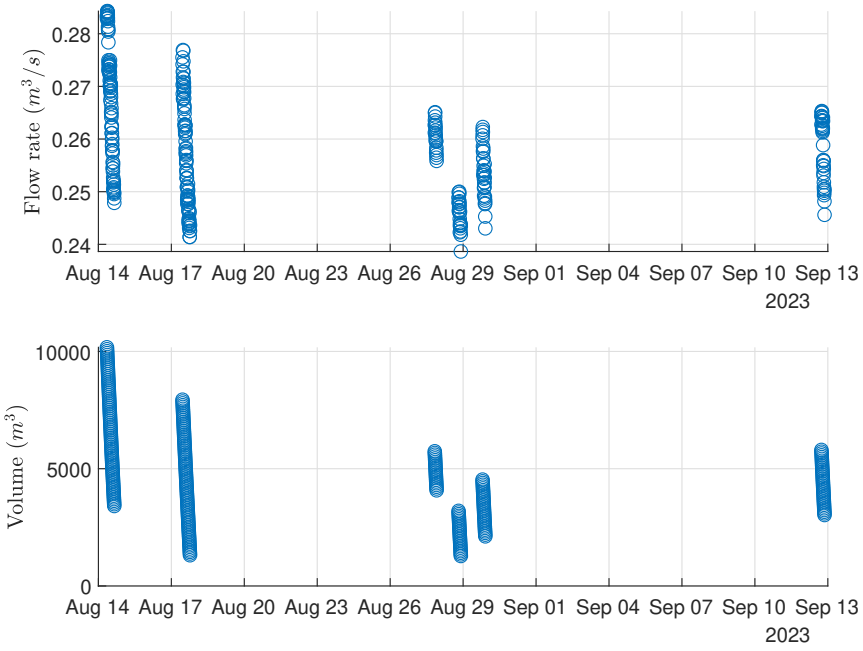


Figure A-1: Training data pump 6

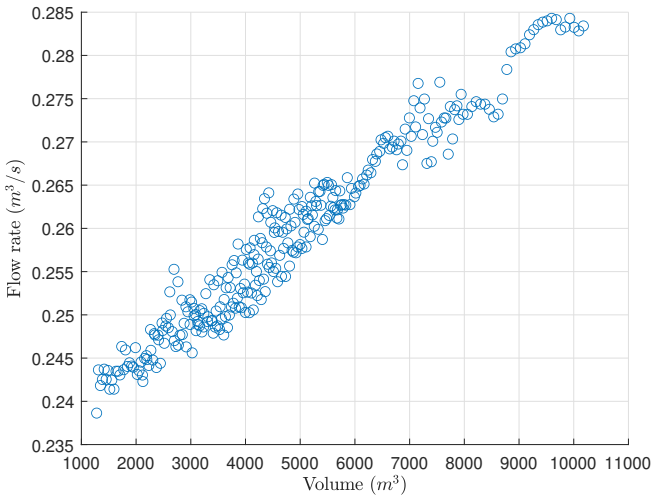


Figure A-2: Correlation volume and flow training data pump 6

Figure A-3: Training data pumps in parallel

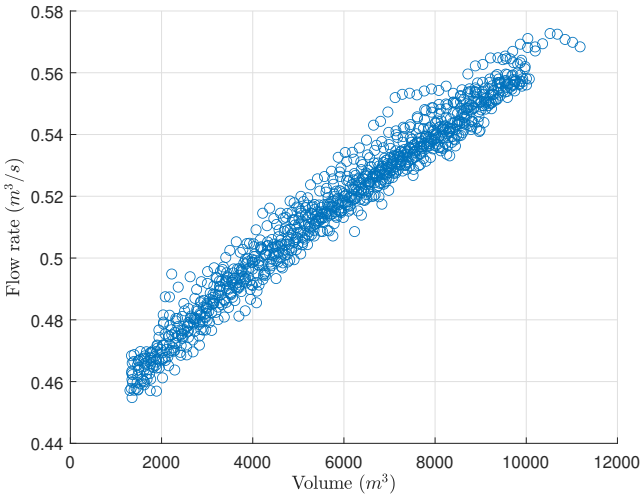


Figure A-4: Correlation volume and flow training data pumps in parallel

A-2-2 Draining mode | Changing rpm

In Figure A-5, the flow rate and the valve angles for pump 5 and Motor-Controlled Valve $(MCV)_{36}$ when the draining process is terminated is illustrated. In Figure A-6, the flow rate and the valve angle measurements for pump 6 and MCV_{37} when the draining process is terminated is depicted.

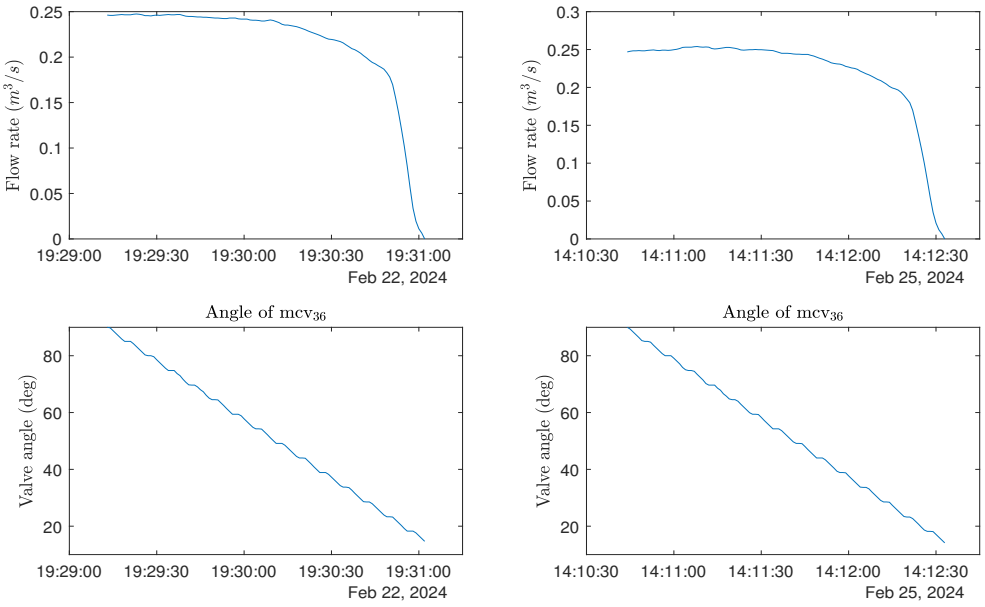


Figure A-5: Training data identification loss coefficients butterfly valve and decreasing h_{pump} where the upper graphs show the flow rate and the lower graphs show the valve angels of MCV_{36}

In Figure A-7 and Figure A-8, the flow rate and the valve angles of MCV_{36} and MCV_{37} are shown respectively for the increase of the rotational speed of pump 5 and 6 to initiate the draining process.

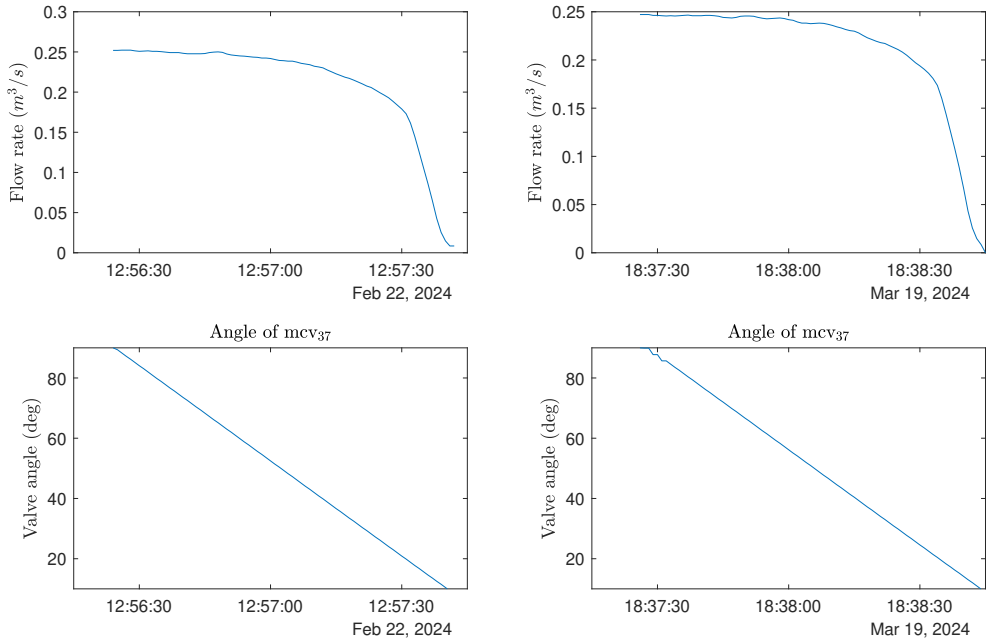


Figure A-6: Training data identification loss coefficients butterfly valve and decreasing h_{pump} where the upper graphs show the flow rate and the lower graphs show the valve angels of MCV_{37}

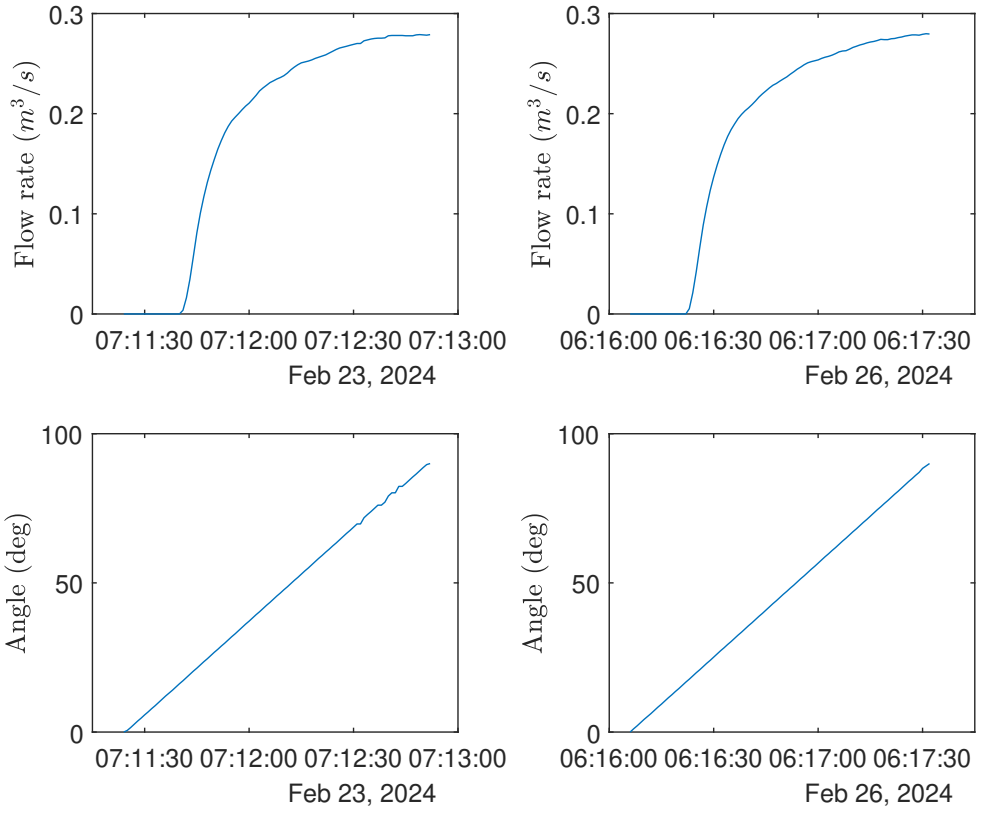


Figure A-8: Training data identification loss coefficients butterfly valve and increasing h_{pump} of pump 6, where the upper graphs show the flow rate and the lower graphs the valve angles of MCV_{37}

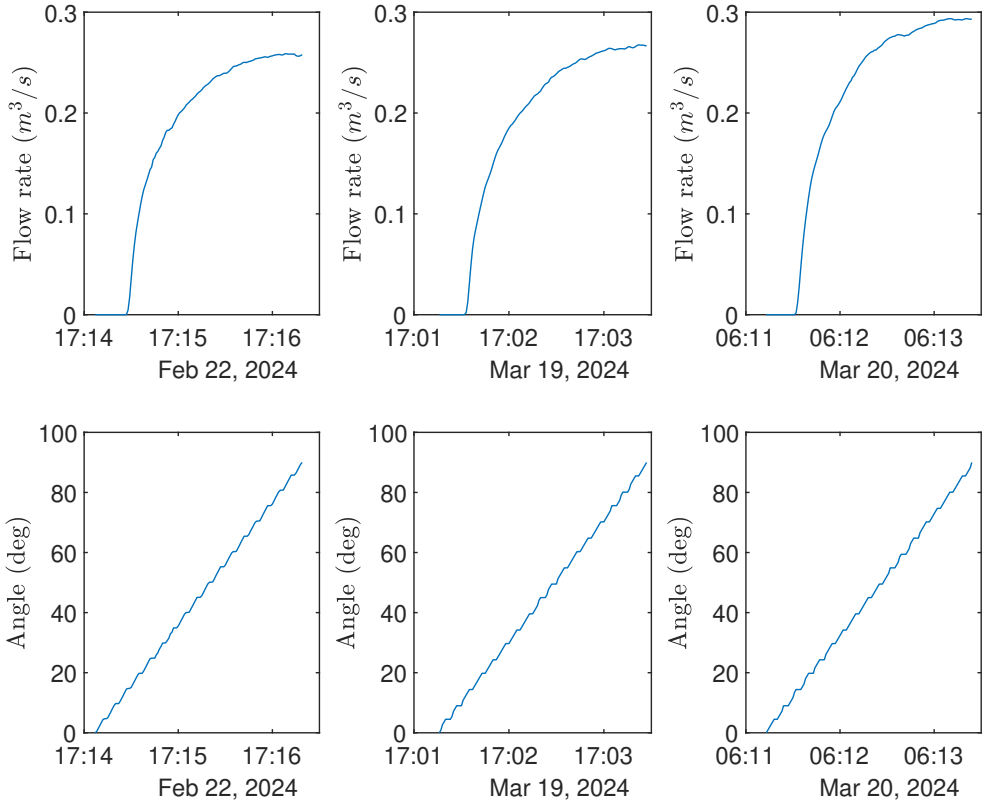


Figure A-7: Training data identification loss coefficients butterfly valve and increasing h_{pump} of pump 5, where the upper graphs show the flow rate and the lower graphs show the valve angles of MCV_{36}

A-2-3 Replenishing mode

In Figure A-9, Figure A-10, Figure A-11 and Figure A-12 the flow rate, valve angles, volume and pressure measurements of one day of training data are depicted respectively.

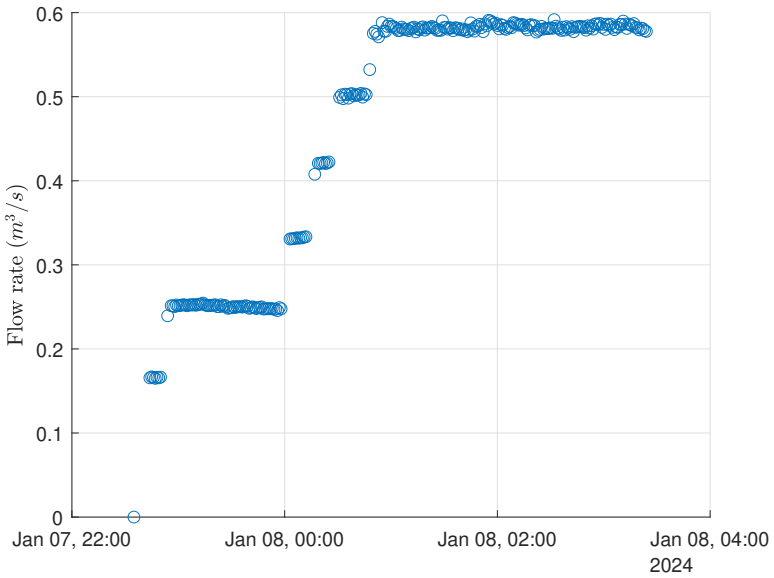


Figure A-9: Training data of the flow rate replenishing

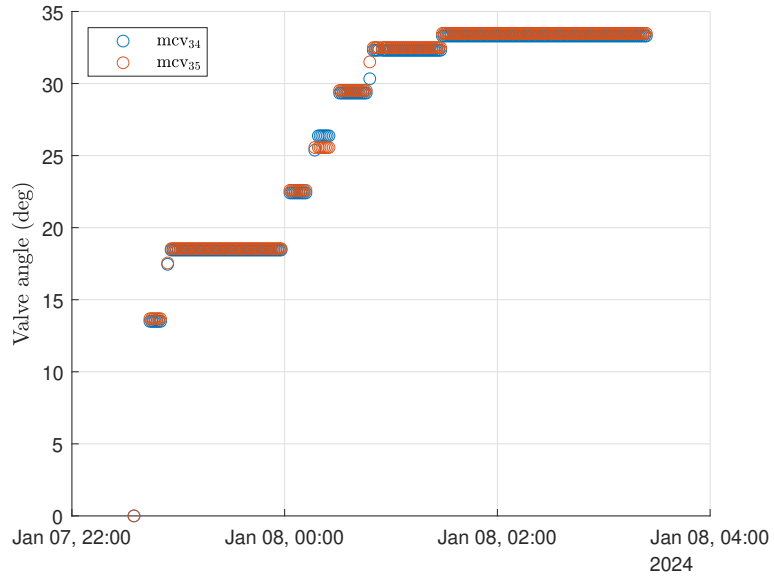


Figure A-10: Training data of the valve angles of MCV_{34} in blue and MCV_{35} in red

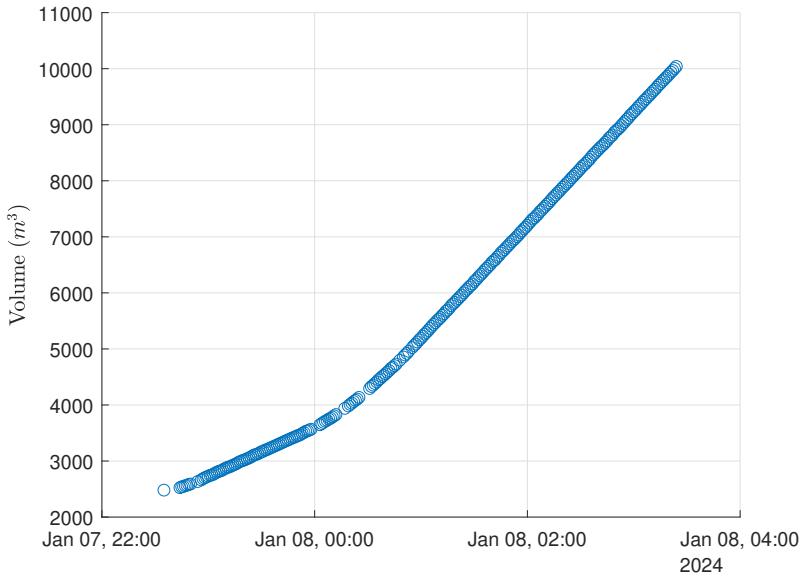


Figure A-11: Training data of the volume while replenishing the reservoir

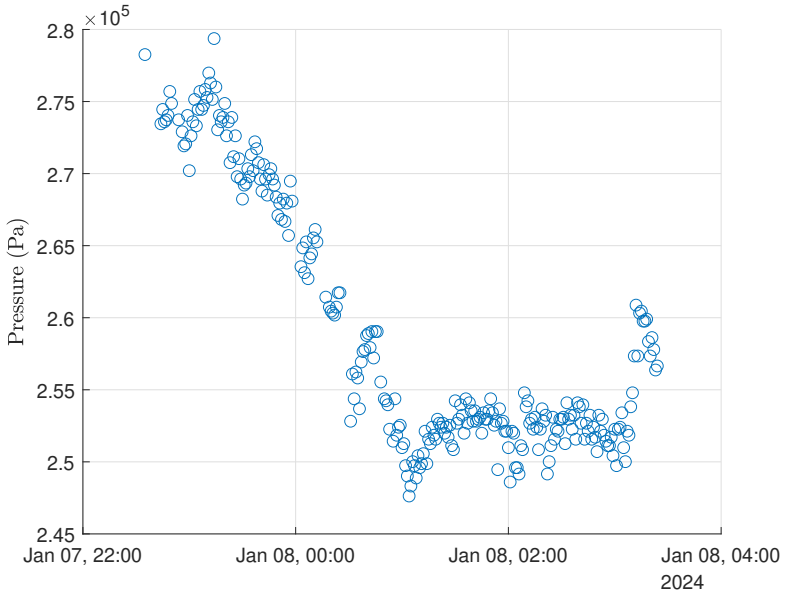


Figure A-12: Training data of the pressure while replenishing the reservoir

A-3 Final model parameters

Draining													
Crpm	a_1,	a_2,	b_1,	b_2									
Pump 5	-97.5,	87.5,	34.9,	25									
Pump 6	-107,	97.2,	35.5,	24.5									
Parallel	-18.4,	28.36,	32.1,	22.9									
Increasing rpm	K_0,	K_{10},	K_{20},	K_{30},	K_{40},	K_{50},	K_{60},	K_{70},	K_{80},	τ,	t_d		
Pump 5	1000,	300,	80,	24.04,	10,	2.5,	0.4,	$4{\cdot}10^{-6}$,	0,	3,	10		
Pump 6	1000,	300,	80,	37.98,	10.8,	6.13,	5,	1.6,	1.5,	3	10		
Decreasing rpm	K_0,	K_{10},	K_{20},	K_{30},	K_{40},	K_{50},	K_{60},	K_{70},	K_{80},	τ,	θ_{off}		
Pump 5	1000,	301,	26,	23,	10,	2.53,	0.38,	0,	0,	2.88,	35		
Pump 6	1000,	299,	40,	23,	14,	6.13,	4.96,	1.61,	1.54,	2.57,	35		
Replenishing													
Sys parameters	z_1,	$L_{0.4}$,	$L_{0.6}$,	$L_{0.8}$,	$K_{m.4}$,	$K_{m.6}$,	$K_{m.8}$,	ϵ					
	-1,	4.2,	6.3,	14.8,	1.9,	1.3,	4.8,	0.013					
Loss coefficients	K_0,	K_{10},	K_{20},	K_{30},	K_{40}								
MCV_{34}	$1.1{\cdot}10^4$,	1526,	246,	61.7,	37.2,								
MCV_{35}	$1.1{\cdot}10^4$,	1522,	232,	3.5,	32.2								

Table A-2: Final model parameters

A-4 Pseudo codes attack

Algorithm 1 Full reservoir attack

Inputs:
N, u_5, u_6, flow_replay_two, flow_replay_one, valve_replay
Initialize:
i, k, l, flag_{p5}, flag_{p6}, flow, valve_36, valve_37
for i = 2:N **do**
  if $u_5(i) = 1 \,\&\, u_5(i-1) = 0 \,\&\, flag_{p6} = 1$ **then** ▷ P5 is started as second pump
    l = 1, $\text{flag}_{p5} = 1$
    flow(i) = flow_replay_two(l)
    [valve_36(i), valve_37(i)] = [valve_replay(l), 90]
    l = l + 1
  else if $u_6(i) = 1 \,\&\, u_6(i-1) = 0 \,\&\, flag_{p5} = 1$ **then** ▷ P6 is started as second pump
    l = 1, $\text{flag}_{p6} = 1$
    flow(i) = flow_replay_two(l)
    [valve_36(i), valve_37(i)] = [90, valve_replay(l)]
    l = l + 1
  else if $flag_{p5} = 1 \,\&\, flag_{p6} = 1$ **then** ▷ Both pumps are on
    flow(i) = flow_replay_two(l)
    [valve_36(i), valve_37(i)] = [90, 90]
    if $l \neq length(flow\_replay\_two)$ **then** ▷ Updating the index of the replay
      l = l+1
    end if
  else if $(u_5(i) = 1 \,\&\, flag_{p6} = 0) \,|\, (u_6(i) = 1 \,\&\, flag_{p5} = 0)$ **then** ▷ One pump on
    if $u_5(i) = 1 \,\&\, flag_{p5} = 0$ **then** ▷ pump 5 is started
      k = 2, $\text{flag}_{p5} = 1$
      flow(i) = flow_replay_one(k)
      [valve_36(i), valve_37(i)] = [valve_replay(k), 0]
      k = k + 1
    else if $\text{flag}_{p5} = 1$ **then** ▷ pump 5 is on
      flow(i) = flow_replay_one(k)
      [valve_36(i), valve_37(i)] = [valve_replay(k), 0]
    else if $u_6(i) = 1 \,\&\, flag_{p6} = 0$ **then** ▷ pump 6 is started
      k = 2, $\text{flag}_{p6} = 1$
      flow(i) = flow_replay_one(k)
      [valve_36(i), valve_37(i)] = [0, valve_replay(k)]
      k = k + 1
    else if $\text{flag}_{p6} = 1$ **then** ▷ Pump 6 is on
      flow(i) = flow_replay_one(k)
      [valve_36(i), valve_37(i)] = [0, valve_replay(k)]
    end if
  end if
end for
return flow, valve_36, valve_37

Algorithm 2 Empty reservoir attack

```
Inputs:
    flow_replay, pressure_replay
Initialize:
    i, m, N, flag, u_rep, flow, pressure
N = length attack
for i = 2:N do
    if u_rep(i) > 0 & flag = 0 then                ▷ Replenishing process is initialised
        k = 1,
        flag = 1
    else if u_rep(i) = 0 & flag = 1 then           ▷ Replenishing process is terminated
        flag = 0
    end if
    if flag = 1 then
        if k = length(flow_replay) then            ▷ The end of the replay data set is reached
            flow(i) = flow_replay(k)
            pressure(i) = pressure_replay(k)
            m = m + 1
        else
            flow(i) = flow_replay(k)
            pressure(i) = pressure_replay(k)
            k = k + 1
            m = k
        end if
    else                ▷ After the replenishing, keep collecting the pressure measurements
        if m > 1 then
            pressure(i) = pressure_replay(m)
            m = m + 1
        else
            pressure(i) = pressure_replay(1)
        end if
    end if
end for
return u_rep, flow, pressure
```

A-5 Cyber attack detection results

In Figure A-13 and Figure 5-1 the physical impact of the full reservoir is illustrated. From these graphs, it can be noted that the simulation of the actual volume exceeds the maximum volume of the reservoir, leading to overflow.

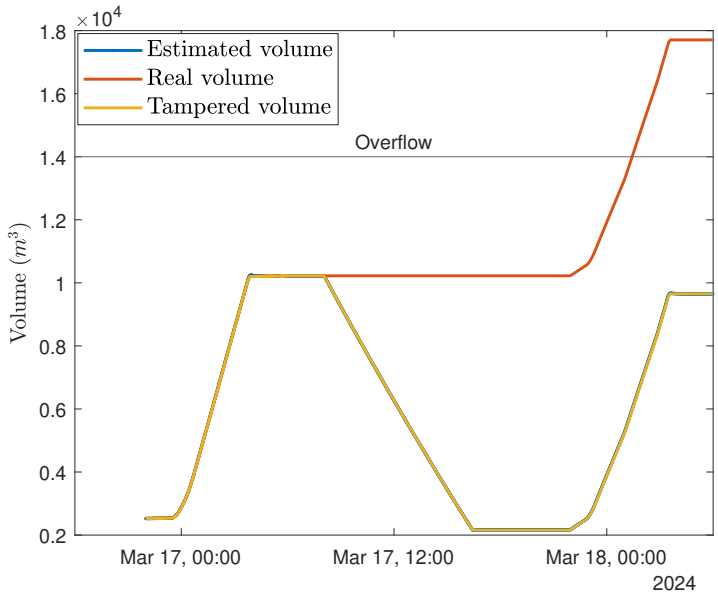


Figure A-13: Physical impact of the full reservoir attack in the case where one pump is operational. The estimated volume is indicated in blue, the actual volume in red, and the the tempered volume measurement in yellow.

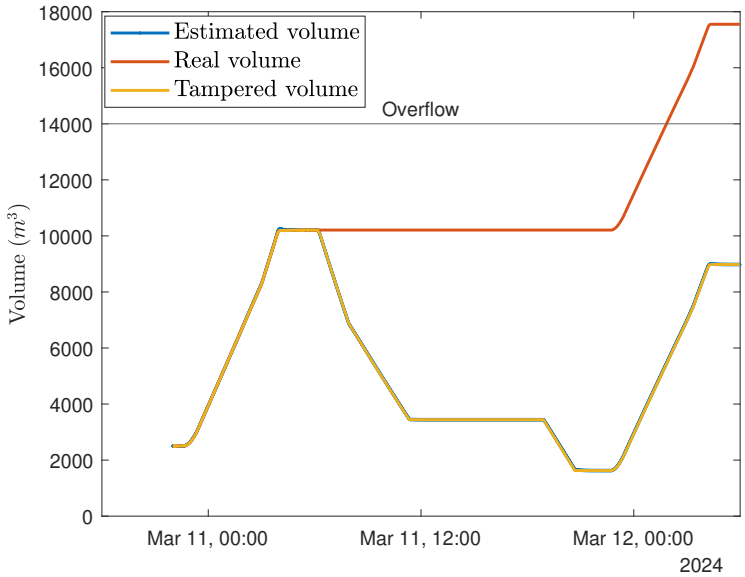
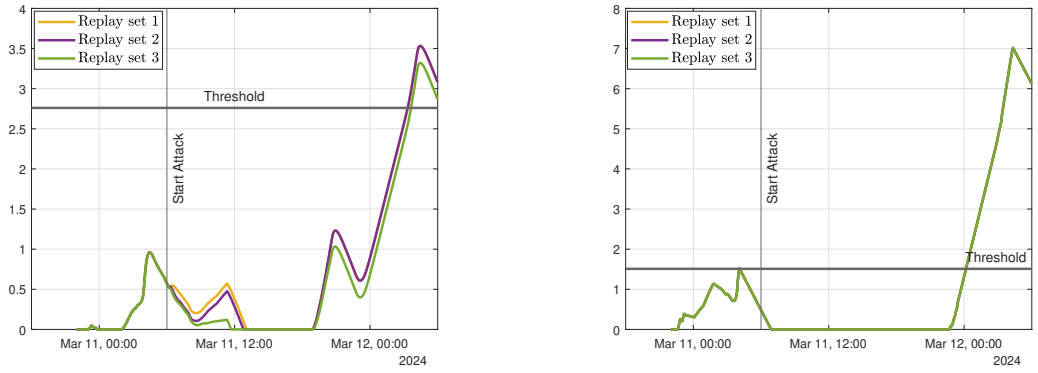


Figure A-14: Physical impact of the full reservoir attack in the case where varying number of pumps are operational. The estimated volume is indicated in blue, the actual volume in red, and the the tempered volume measurement in yellow.

In Figure A-15, the results of the Non-Parametric Cumulative Sum (NP-CUSUM) for the volume and the replenishing flow rate in the case a varying number of pumps is on are shown. These graphs show that both exceed the predefined threshold, leading to the detection of the

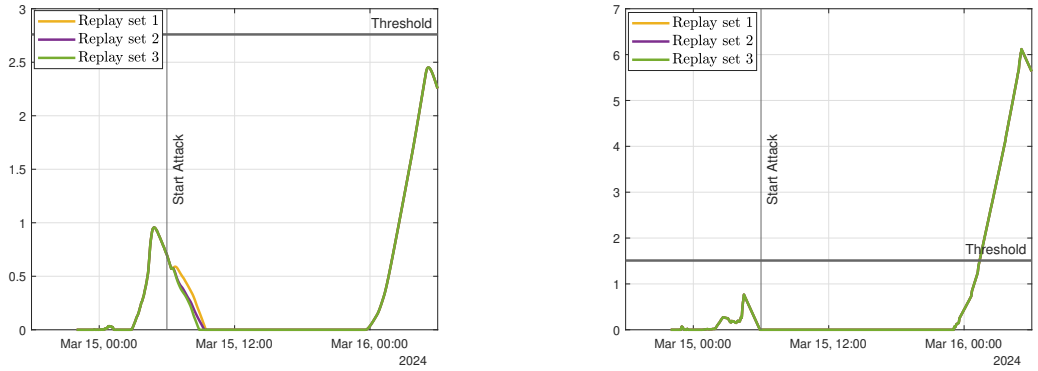
attack for all three replay sets during the replenishing mode.



(a) NP-CUSUM volume **(b)** NP-CUSUM replenishing flow rate

Figure A-15: NP-CUSUM of the volume and replenishing flow rate in the case a varying number of pumps is on. The threshold indicated in blue, the NP-CUSUM of the replay sets 1, 2 and three are in yellow, purple and green, respectively.

In Figure A-16, the results of the NP-CUSUM for the volume and the replenishing flow rate in the case two pumps are on are shown. These graphs show that both exceed the predefined threshold, leading to the detection of the attack for all three replay sets during the replenishing mode. It is noted that the attack is not detected during the disruption of the input signal but afterwards.



(a) NP-CUSUM volume **(b)** NP-CUSUM replenishing flow rate

Figure A-16: NP-CUSUM of the volume and replenishing flow rate. The threshold indicated in blue, the NP-CUSUM of the replay sets 1, 2 and three are in yellow, purple and green, respectively.

In Figure A-17 and Figure A-18, the physical effect of the empty reservoir attack simulated by two different input datasets is illustrated. In both figures, it can be seen that the reservoir volume reaches its low level within an hour of draining. This shows that the objective of the attack is reached during high demands of the consumer net. Furthermore, it becomes evident that the estimated volume deviates from the tempered volume. This can be explained by the fact that the replayed flow rate, which is used to compute the tempered volume, differs from the estimated flow rate based on the input signals to the valves.

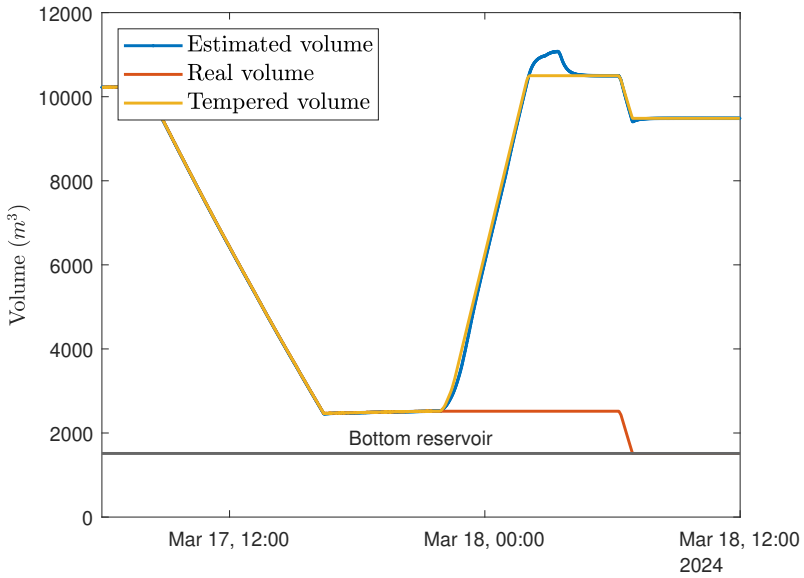


Figure A-17: Physical impact of the empty reservoir attack simulated by the input dataset of March 11th. The estimated volume is indicated in blue, the actual volume is in red, and the tempered volume measurement is in yellow.

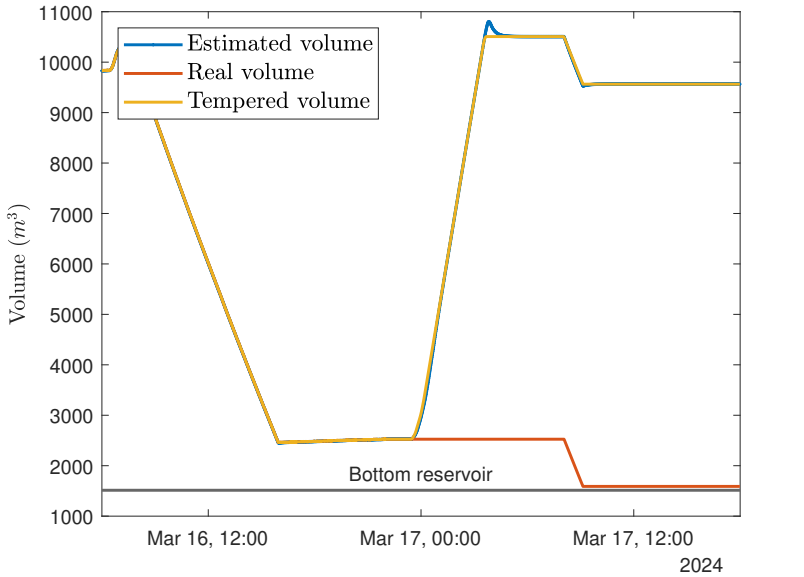
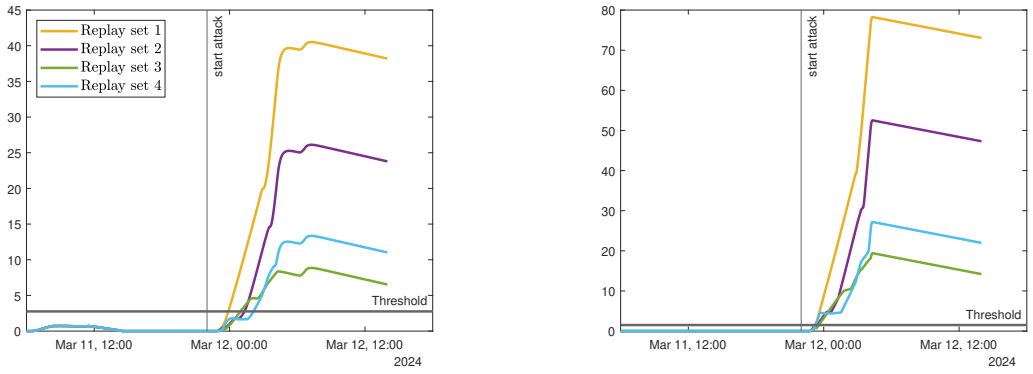


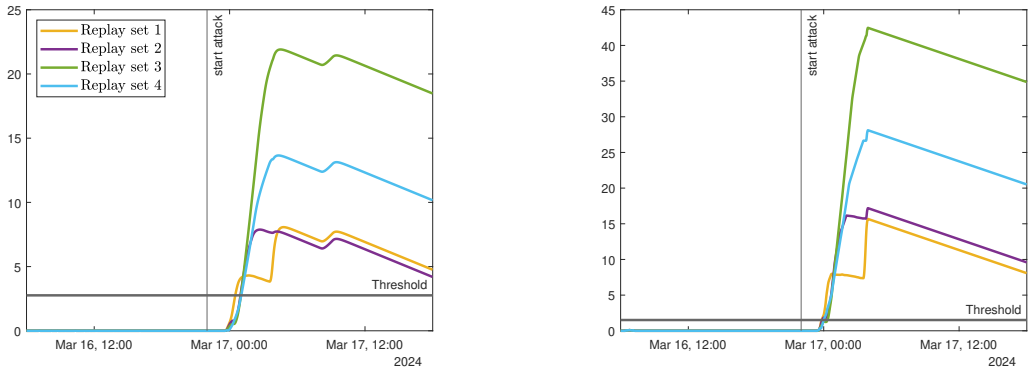
Figure A-18: Physical impact of the empty reservoir attack simulated by the input set of March 17th. The estimated volume is indicated in blue, the actual volume is in red, and the tempered volume measurement is in yellow.

In Figure A-19 and Figure A-20, the results for the NP-CUSUM of the volume and replenishing flow rate during the empty attack are shown. In both figures, it is apparent that the designed detector can detect the launched attacks within a time window of approximately two hours.



(a) Volume **(b)** Replenishing flow rate

Figure A-19: NP-CUSUM of the volume and the replenishing flow rate during the empty attack simulated by the input dataset of March 11th. The NP-CUSUM of the replay sets 1, 2, 3 and 4 are in yellow, purple, green and light blue, respectively.



(a) Volume **(b)** Replenishing flow rate

Figure A-20: NP-CUSUM of the volume and the replenishing flow rate during the attack simulated by the input dataset of March 16th. The NP-CUSUM of the replay sets 1, 2, 3 and 4 are in yellow, purple, green and light blue, respectively.

Bibliography

[1] Tschroub Abdelghani. Industrial control systems (ics) security in power transmission network. In *2019 Algerian Large Electrical Network Conference (CAGRE)*, pages 1–4, Algiers, Algeria, February 2019. IEEE.

[2] Hayatullahi Bolaji Adeyemo, Rami Bahsoon, and Peter Tiňo. Surrogate-based Digital Twin for Predictive Fault Modelling and Testing of Cyber Physical Systems. In *2022 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)*, pages 166–169, December 2022.

[3] Chuadhry Mujeeb Ahmed, Carlos Murguia, and Justin Ruths. Model-based Attack Detection Scheme for Smart Water Distribution Networks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 101–113, Abu Dhabi United Arab Emirates, April 2017. ACM.

[4] Chuadhry Mujeeb Ahmed, Venkata Reddy Palleti, and Aditya P. Mathur. WADI: a water distribution testbed for research in the design of secure cyber physical systems. In *Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks*, pages 25–28, Pittsburgh Pennsylvania, April 2017. ACM.

[5] Chuadhry Mujeeb Ahmed, Venkata Reddy Palleti, and Vishrut Kumar Mishra. A practical physical watermarking approach to detect replay attacks in a CPS. *Journal of Process Control*, 116:136–146, August 2022.

[6] Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M. Bayen. Cyber Security of Water SCADA Systems—Part I: Analysis and Experimentation of Stealthy Deception Attacks. *IEEE Transactions on Control Systems Technology*, 21(5):1963–1970, September 2013. Conference Name: IEEE Transactions on Control Systems Technology.

[7] Saurabh Amins, Xavier Litrico, S. Shankar Sastry, and Alexandre M. Bayen. Cyber Security of Water SCADA Systems—Part II: Attack Detection Using Enhanced Hydrodynamic Models. *IEEE Transactions on Control Systems Technology*, 21(5):1679–1693, September 2013. Conference Name: IEEE Transactions on Control Systems Technology.

[8] Angevaare, Ted. *General Knowledge of OT-Cybersecurity*. TAPS, August 2019.

[9] Qi Ao. An Intrusion Detection Method for Industrial Control System against Stealthy Attack. In *2020 7th International Conference on Dependable Systems and Their Applications (DSA)*, pages 157–161, November 2020.

[10] Aström, K.J. and Wittenmark, B. *Computer-Controlled Systems*. Prentice-Hall, 3rd edition, 1997.

[11] Mazen Azzam, Liliana Pasquale, Gregory Provan, and Bashar Nuseibeh. Grounds for Suspicion: Physics-Based Early Warnings for Stealthy Attacks on Industrial Control Systems. *IEEE Transactions on Dependable and Secure Computing*, 19(6):3955–3970, November 2022. Conference Name: IEEE Transactions on Dependable and Secure Computing.

[12] Mogens Blanke and Jochen Schröder, editors. *Diagnosis and fault-tolerant control*. Springer, Berlin ; New York, 2nd ed edition, 2006. OCLC: ocm71336524.

[13] Alvaro A. Cardenas, Saurabh Amin, and Shankar Sastry. Secure Control: Towards Survivable Cyber-Physical Systems. In *2008 The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500, June 2008. ISSN: 2332-5666.

[14] Edward J. M. Colbert and Alexander Kott, editors. *Cyber-security of SCADA and Other Industrial Control Systems*, volume 66 of *Advances in Information Security*. Springer International Publishing, Cham, 2016.

[15] CSIS. Significant Cyber Events List. Technical report, Center for Strategic & International Studies, September 2023.

[16] Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. Attacks against process control systems: risk assessment, detection, and response. pages 355–366, March 2011.

[17] Seyed Mehran Dibaji, Mohammad Pirani, David Bezalel Flamholz, Anuradha M. Annaswamy, Karl Henrik Johansson, and Aranya Chakrabortty. A systems and control perspective of CPS security. *Annual Reviews in Control*, 47:394–411, January 2019.

[18] K.T Erickson. Programmable logic controllers. 15(1):14–17, 1996.

[19] L. Faramondi, F. Flammini, S. Guarino, and R. Setola. Evaluating Machine Learning Approaches for Cyber and Physical Anomalies in SCADA Systems. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 412–417, July 2023.

[20] Riccardo M.G. Ferrari. Model Based Fault Diagnosis: Detection Observer, July 2020.

[21] Alexander J Gallo. Plug-and-play fault-tolerant and cyber-secure control: application to future distribution networks.

[22] Brendan Galloway and Gerhard P. Hancke. Introduction to Industrial Control Networks. *IEEE Communications Surveys & Tutorials*, 15(2):860–880, 2013. Conference Name: IEEE Communications Surveys & Tutorials.

[23] Virgil D. Gligor. A Note on Denial-of-Service in Operating Systems. *IEEE Transactions on Software Engineering*, SE-10(3):320–324, May 1984. Conference Name: IEEE Transactions on Software Engineering.

[24] BSI group. Industrial control system security: Top 10 threats and countermeasures 2022, March 2022.

[25] Chingiz Hajiyev and Fikret Caliskan. The Innovation Approach to Fault Detection. In Robert Murphey and Panos M. Pardalos, editors, *Fault Diagnosis and Reconfiguration in Flight Control Systems*, volume 2, pages 187–223. Springer US, Boston, MA, 2003. Series Title: Cooperative Systems.

[26] Amin Hassanzadeh, Shimon Modi, and Shaan Mulchandani. Towards effective security control assignment in the Industrial Internet of Things. In *Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, WF-IOT '15, pages 795–800, USA, December 2015. IEEE Computer Society.

[27] Amin Hassanzadeh, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and Katherine Banks. A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering*, 146(5):03120003, May 2020. arXiv:2001.11144 [cs].

[28] Mashor Housh and Ziv Ohar. Model-based approach for cyber-physical attack detection in water distribution systems. *Water Research*, 139:132–143, August 2018.

[29] Yan Hu, Hong Li, Tom H. Luan, An Yang, Limin Sun, Zhiliang Wang, and Rui Wang. Detecting stealthy attacks on industrial control systems using a permutation entropy-based method. *Future Generation Computer Systems*, 108:1230–1240, July 2020.

[30] Yan Hu, Hong Li, Hong Yang, Yuyan Sun, Limin Sun, and Zhiliang Wang. Detecting stealthy attacks against industrial control systems based on residual skewness analysis. *EURASIP Journal on Wireless Communications and Networking*, 2019(1):74, March 2019.

[31] Yan Hu, An Yang, Hong Li, Yuyan Sun, and Limin Sun. A survey of intrusion detection on industrial control systems. *International Journal of Distributed Sensor Networks*, 14(8):1550147718794615, August 2018. Publisher: SAGE Publications.

[32] IBM. Distribution of cyber attacks across worldwide industries in 2022. Survey, Statistica, February 2023.

[33] IBM. IBM X-Force Threat Intelligence Index 2024. Technical report, 2024.

[34] Central States Industrial. How to Read a Pump Curve: Complete Guide, May 2022.

[35] International Electrotechnical Commission. IEC standard 61158, April 2019.

[36] International Society of Automation. ISA95, 1990.

[37] Rolf Isermann. *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer, Berlin ; New York, 2006. OCLC: ocm61703226.

[38] Mengsen Jia and Ping Zhang. Detection of Cyber Attacks on a Water Distribution Testbed. In *2022 IEEE Conference on Control Technology and Applications (CCTA)*, pages 1354–1359, August 2022. ISSN: 2768-0770.

[39] Dong-Seong Kim and Hoa Tran-Dang. *Industrial Sensors and Controls in Communication Networks: From Wired Technologies to Cloud Computing and the Internet of Things*. Computer Communications and Networks. Springer International Publishing, Cham, 2019.

[40] P. J. Lefebvre and W. P. Barker. Centrifugal Pump Performance During Transient Operation. *Journal of Fluids Engineering*, 117(1):123–128, March 1995.

[41] Dan Li, Dacheng Chen, Baihong Jin, Lei Shi, Jonathan Goh, and See-Kiong Ng. MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks. In Igor V. Tetko, Věra Kůrková, Pavel Karpov, and Fabian Theis, editors, *Artificial Neural Networks and Machine Learning – ICANN 2019: Text and Time Series*, Lecture Notes in Computer Science, pages 703–716, Cham, 2019. Springer International Publishing.

[42] Matt Bishop. *Computer Security Art and Science*. Addison-Wesle Porfessional, 2nd edition edition, November 2018.

[43] Peter Maynard, Kieran McLaughlin, and Berthold Haberler. Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks. BCS Learning & Development, September 2014.

[44] Gauthama Raman M.r. and Aditya P. Mathur. AICrit: A unified framework for real-time anomaly detection in water treatment plants. *Journal of Information Security and Applications*, 64:103046, February 2022.

[45] Carlos Murguia and Justin Ruths. On Reachable Sets of Hidden CPS Sensor Attacks. In *2018 Annual American Control Conference (ACC)*, pages 178–184, June 2018. ISSN: 2378-5861.

[46] Nils Müller, Charalampos Ziras, and Kai Heussen. Assessment of Cyber-Physical Intrusion Detection and Classification for Industrial Control Systems. In *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 432–438, October 2022.

[47] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Technical Report NIST CSWP 04162018, National Institute of Standards and Technology, Gaithersburg, MD, April 2018.

[48] Venkata Reddy Palleti, Vishrut Kumar Mishra, Chuadhry Mujeeb Ahmed, and Aditya Mathur. Can Replay Attacks Designed to Steal Water from Water Distribution Systems Remain Undetected? *ACM Transactions on Cyber-Physical Systems*, 5(1):1–19, January 2021.

[49] European Parliament. The NIS2 Directive, February 2023.

[50] Fabio Pasqualetti, Antonio Bicchi, and Francesco Bullo. Consensus Computation in Unreliable Networks: A System Theoretic Approach. *IEEE Transactions on Automatic Control*, 57(1):90–104, January 2012. Conference Name: IEEE Transactions on Automatic Control.

[51] Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thomas Lagkas, and Antonios G. Sarigiannidis. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Communications Surveys & Tutorials*, 22(3):1942–1976, 2020.

[52] Claudia Rodríguez Martínez, Marcos Quiñones-Grueiro, Cristina Verde, and Orestes Llanes-Santiago. A Novel Approach for Detection and Location of Cyber-Attacks in Water Distribution Networks. In Yanio Hernández Heredia, Vladimir Milián Núñez, and José Ruiz Shulcloper, editors, *Progress in Artificial Intelligence and Pattern Recognition*, Lecture Notes in Computer Science, pages 79–90, Cham, 2021. Springer International Publishing.

[53] University of Sheffield S Beck and R Collins. Moody Diagram, 2012.

[54] Henrik Sandberg and Andre M.H. Teixeira. From control system security indices to attack identifiability. In *2016 Science of Security for Cyber-Physical Systems Workshop (SOSCYPS)*, pages 1–6, April 2016.

[55] Branka Stojanović, Helmut Neuschmied, Martin Winter, and Ulrike Kleb. Enhanced Anomaly Detection for Cyber-Attack Detection in Smart Water Distribution Systems. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, pages 1–7, New York, NY, USA, August 2022. Association for Computing Machinery.

[56] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. Guide to Industrial Control Systems (ICS) Security. Technical Report NIST SP 800-82r2, National Institute of Standards and Technology, June 2015.

[57] Riccardo Taormina and Stefano Galelli. Deep-Learning Approach to the Detection and Localization of Cyber-Physical Attacks on Water Distribution Systems. *Journal of Water Resources Planning and Management*, 144(10):04018065, October 2018. Publisher: American Society of Civil Engineers.

[58] Riccardo Taormina, Stefano Galelli, Nils Ole Tippenhauer, Elad Salomons, Avi Ostfeld, Demetrios G. Eliades, Mohsen Aghashahi, Raanju Sundararajan, Mohsen Pourahmadi, M. Katherine Banks, B. M. Brentan, Enrique Campbell, G. Lima, D. Manzi, D. Ayala-Cabrera, M. Herrera, I. Montalvo, J. Izquierdo, E. Luvizotto, Sarin E. Chandy, Amin Rasekh, Zachary A. Barker, Bruce Campbell, M. Ehsan Shafiee, Marcio Giacomoni, Nikolaos Gatsis, Ahmad Taha, Ahmed A. Abokifa, Kelsey Haddad, Cynthia S. Lo, Pratim Biswas, M. Fayzul K. Pasha, Bijay Kc, Saravanakumar Lakshmanan Somasundaram, Mashor Housh, and Ziv Ohar. Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks. *Journal of Water Resources Planning and Management*, 144(8):04018048, August 2018.

[59] Andre Teixeira, Iman Shames, Henrik Sandberg, and Karl H. Johansson. Revealing stealthy attacks in control systems. In *2012 50th Annual Allerton Conference on Com-*

munication, Control, and Computing (Allerton), pages 1806–1813, Monticello, IL, USA, October 2012. IEEE.

[60] André Teixeira, Daniel Pérez, Henrik Sandberg, and Karl Henrik Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st international conference on High Confidence Networked Systems*, pages 55–64, Beijing China, April 2012. ACM.

[61] André Teixeira, Iman Shames, Henrik Sandberg, and Karl Henrik Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135–148, January 2015.

[62] Yaoyue Tian, Jiaqiang Wang, Zhaohui Qi, Chang Yue, Peng Wang, and Sungmin Yoon. Calibration method for sensor drifting bias in data center cooling system using Bayesian Inference coupling with Autoencoder. *Journal of Building Engineering*, 67:105961, May 2023.

[63] Lydia Tsiami and Christos Makropoulos. Cyber—Physical Attack Detection in Water Distribution Systems with Temporal Graph Convolutional Neural Networks. *Water*, 13(9):1247, January 2021. Number: 9 Publisher: Multidisciplinary Digital Publishing Institute.

[64] UNITED NATIONS EDUCATIONAL SCIENTIFIC AND CULTURAL ORGANIZATION. *UNITED NATIONS WORLD WATER DEVELOPMENT REPORT 2023: partnerships and cooperation for water*. UNITED NATIONS, S.l., 2023. OCLC: 1378100094.

[65] David I. Urbina, Jairo A. Giraldo, Alvaro A. Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. Limiting the Impact of Stealthy Attacks on Industrial Control Systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1092–1105, Vienna Austria, October 2016. ACM.

[66] Peter Van Overschee and Bart De Moor. *Subspace Identification for Linear Systems*. Springer US, Boston, MA, 1996.

[67] Michel Verhaegen and Vincent Verdult. *Filtering and system identification: a least squares approach*. Cambridge University Press, Cambridge, first paperback edition edition, 2011.

[68] Stelios Vrachimis, Srimanta Santra, Agathoklis Agathokleous, Pavlos Pavlou, Marios Kyriakou, Michalis Psaras, Demetrios G. Eliades, and Marios M. Polycarpou. WaterSafe: A Water Network Benchmark for Fault Diagnosis Research. *IFAC-PapersOnLine*, 55(6):655–660, January 2022.

[69] Shuheng Wei, Junjun Xu, Zaijun Wu, Qinran Hu, and Xinghuo Yu. A False Data Injection Attack Detection Strategy for Unbalanced Distribution Networks State Estimation. *IEEE Transactions on Smart Grid*, pages 1–1, 2023. Conference Name: IEEE Transactions on Smart Grid.

[70] Frank M. White and Rhim Yoon Chul. *Fluid mechanics*. McGraw-Hill series in mechanical engineering. McGraw-Hill education, New York, NY, eighth edition in si units edition, 2016.

[71] Sungmin Yoon and Yuebin Yu. Hidden factors and handling strategy for accuracy of virtual in-situ sensor calibration in building energy systems: Sensitivity effect and reviving calibration. *Energy and Buildings*, 170:217–228, July 2018.

[72] Xiaosong Zhao, Lei Zhang, Yixin Cao, Kai Jin, and Yupeng Hou. Anomaly Detection Approach in Industrial Control Systems Based on Measurement Data. *Information*, 13(10):450, October 2022. Number: 10 Publisher: Multidisciplinary Digital Publishing Institute.

[73] Karl J. Åström and Richard M. Murray. *Feedback systems: an introduction for scientists and engineers*. Princeton University Press, Princeton, 2008. OCLC: ocn183179623.

Glossary

List of Acronyms

CPA	Cyber-Physical Attack
CPU	Central Processing Unit
CPS	Cyber-Physical System
CUSUM	Cumulative Sum
DAE	Differential-Algebraic Equation
DCS	Distributed Control System
DMZ	Demilitarised Zone
DoS	Denial of Service
EU	European Union
FAR	False Alarm Rate
FCV	Flow Controlled Valve
FDI	False Data Injection
FOTD	First Order Time Delay
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IE	Industrial Ethernet
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
I/O	Input/Output
IP	Interior Point
IT	Information Technology
LAN	Local Area Network
LTI	Linear Time-Invariant

MSE Mean Squared Error
MITM Man In The Middle
MCV Motor-Controlled Valve
NIS Network and Information Security
NIST National Institute of Standards and Technology
NP-CUSUM Non-Parametric Cumulative Sum
OT Operational Technology
PERA Purdue Enterprise Reference Architecture
PID Proportional, Integral and Derivative
PLC Programmable Logic Controller
PROFIBUS Process Field Bus
QN Quasi Newton
RTU Remote Terminal Unit
SCADA Supervisory Control and Data Acquisition
SCR Single Classification Rate
SFEE Steady Flow Energy Equation
SQP Sequential Quadratic Programming
TNR True Negative Rate
TPR True Positive Rate
TTD Time To Detection
UIO Unknown Input Observer
VAF Variance Accounted For
WAN Wide Area Network
WDN Water Distribution Network

List of Symbols

ϵ Absolute wall roughness (m)
μ Absolute viscosity ($Pa \cdot s$)
ρ Fluid density (kg/m^3)
θ Valve angle (deg)
A_{res} Cross-section reservoir (m^2)
d Diameter (m)
f Darcy friction factor (N)
g Gravitational constant (m/s^2)
$h_{friction}$ Friction head loss (m)

h_{pump}	Pump head (m)
K_{valve}	Loss coefficient butterfly valve
L	Pipe length (m)
p	Pressure (Pa)
Re_d	Reynolds number
V	Velocity (m/s)
z	Level (m)
Q	Flow rate (m^3/s)