Process-Aware Cyberattacks for Thermal Desalination Plants

Prashant Rajput*, Pankaj Rajput†, Marios Sazos‡, Michail Maniatakos‡

*Computer Science and Engineering, Tandon School of Engineering, New York University
†Mechanical and Aerospace Engineering, Tandon School of Engineering, New York University
‡Center for Cyber Security, New York University Abu Dhabi
(prashanthrajput,prajput,marios.sazos,michail.maniatakos)@nyu.edu

ABSTRACT

In 2017, desalination industry was contracted to produce 99.8 million m^3/d of fresh water globally. In regions with a natural shortage of fresh water, desalination contributes up to 70% of drinking water. While state-of-the-art research has focused on securing the power grid, water treatment plants, and other critical infrastructure, not much attention has been given towards desalination plants. In this work, we perform interdisciplinary cyber threat analysis on a desalination plant model, presenting cyberattacks and analyzing their effect on the plant performance and equipment both from economics and mechanical engineering perspective. Our analysis shows that cyber actors can perform extensive financial damage by affecting the performance of the plant. We also perform control volume analysis and finite element analysis studies to investigate the possibility of Stuxnet-like attacks with the potential to cause mechanical damage and equipment failure.

CCS CONCEPTS

• **Security and privacy**; • **Hardware** → *Sensors and actuators*;

KEYWORDS

Cyber security; Desalination; Process aware attacks; Industrial control systems; Finite element analysis

ACM Reference Format:
Prashant Rajput*, Pankaj Rajput†, Marios Sazos‡, Michail Maniatakos‡. 2019. Process-Aware Cyberattacks for Thermal Desalination Plants. In *ACM Asia Conference on Computer and Communications Security (AsiaCCS '19), July 9–12, 2019, Auckland, New Zealand*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3321705.3329805

1 INTRODUCTION

Over 97% of the water on earth is seawater and is unsuitable for consumption due to its salinity. Another 2% is fresh water stored in the form of icecaps and glaciers, leaving 0.5% of fresh water on earth available for human consumption. Pollution has led to further decrease in the amount of usable water and many regions around the world do not have abundant fresh water supply for consumption [20]. Currently, approximately 1.2 billion people live in areas of water scarcity, and this figure is estimated to grow to 1.8 billion by 2025 [21].

Due to the limited supply of fresh water, researchers and the water industry have turned towards desalination: purification of saline water. Desalination is the process of separation of nearly salt-free fresh water from sea water and has been a field of ongoing research. Due to its extremely dry climate, the gulf region has been a "hot spot" for desalination advancement for alleviating water shortage. Increase in the demand of water has shifted focus to desalination as an alternative to fresh water for alleviating water shortage. In Saudi Arabia, desalination technology supplies approximately 60% of water demand in the country and produces more than 70% of the country's drinking water [9].

Despite the advances in desalination, the process is still expensive, complex, requires a steady state operation for optimum utilization of input resources, and also leads to some localized adverse impact on the ecosystem [14]. For instance, Multi-Stage Flash (MSF) desalination is a form of thermal desalination process which consumes about 5 to 6 KWh per m^3 and costs between \$0.62 - \$1.97 per m^3 of fresh water produced, based on the capacity of the desalination plant [14]. Steady state optimum utilization of input resources involves a close coordination between various activities performed by different parts of the plant. Moreover, the start-up procedure for a desalination plant is complicated and involves a strict sequence of steps and procedures to guarantee the safety of the plant [31]. Currently, desalination plants have both semi-automatic and fully-automatic start-up. Semi-automatic startup includes human operators performing crucial checks to guarantee the safety of the plant. Due to complexity, newer plants are moving towards fully automated operation. This guarantees no human error and also a steady-state operation during plant loading, but also expands the cyber threat surface [29].

At the same time, the gulf region has also been a prominent target of high-profile attacks on critical infrastructure. Saudi Aramco, the national petroleum and natural gas company of Saudi Arabia, was severely impacted by the Shamoon malware in 2012, wiping clean more than 75% of the company's enterprise computers [36]. The malware has allegedly resurfaced in 2016. The Flame malware, a computer worm which used Windows update to spread with sophisticated mechanisms for stealing information. This was the first Windows malware that used Bluetooth for discovering neighboring devices and to locate the infected machine. Moreover, it was written in Lua, which allowed the Command and Control (C&C) server to update the malware on the fly. The infamous Stuxnet, as well

AsiaCCS '19, July 9–12, 2019, Auckland, New Zealand

ACM ISBN 978-1-4503-6752-3/19/07…$15.00
https://doi.org/10.1145/3321705.3329805

as its close cousin Duqu which had similar design but with the main intent of stealing information. It spread using Microsoft Word document with a zero-day kernel exploit [6]. These are some of the prime examples of cyber warfare targeting the gulf region and its critical infrastructure.

Research on attacking and securing critical infrastructure has asymmetrically focused on a) the power grid, b) chemical processes, and c) water treatment, due to their paramount importance in critical infrastructure domain [16]. Despite the enormous growth of desalination industry in the recent years, it is still part of the definition of water-related critical infrastructure [8]. Therefore, in order to address the lack of published work on cybersecurity analysis of desalination plants, in this work we present:

(1) The first attempt, to the best of our knowledge, to perform cybersecurity analysis of desalination plants. We analyze and discuss cause and effect relationship of attacks that can be initiated by compromising the sensors, controllers, and actuators of the system modeled using Simulink.
(2) A novel methodology, using Finite Element Analysis (FEA), to quantify the potential of cyberattacks to induce mechanical damage and physically destroy components of a desalination plant, similar to Stuxnet.

The goal of this work is to bring attention to cybersecurity research on desalination plants and provide a set of attacks to be used as benchmarks in order to develop defenses for the desalination process. We particularly focus on *process-aware* cyberattacks that target the *process logic*, causing performance degradation of the process or mechanical failure [22]. In contrast, traditional IT attacks exploit bugs in either the software or the hardware leading to taking control of the computing devices (e.g., privilege escalation) or causing denial-of-service.

2 RELATED WORK

Several serious cyber attacks to the Industrial Control System (ICS) infrastructure have been reported over the last years [16]. These attacks can be broadly divided into a) traditional information technology attacks targeting the enterprise computers of ICS companies (such as Shamoon [36]), and b) operation technology attacks targeting specifically the ICS process, which is also the focus of this work.

In the latter category, the most famous case is Stuxnet, affecting Windows-based PCs that program specific Siemens Programmable Logic Controllers (PLCs). Compromised PLCs were reprogrammed to modify the operation, leading to mechanical damage. The worm initially entered the ICS network via a USB stick and went undetected by automated-detection system by using a digital certificate from a reliable company. The worm then spread inside the internal ICS network looking for specific PCs and once it found them, it first gathered data by spying on the operation and then used this data to deceive the outside controllers. Meanwhile, the compromised PLCs were reprogrammed to modify the operation which lead to mechanical damage. Although, Iran did not release specific details, it is estimated that Stuxnet destroyed 984 uranium enriching centrifuges and decreased the efficiency of Iran's nuclear program by 30% [7]. Another such (experimental) attack was the Aurora vulnerability, that was reported by U.S. Department of Energy's

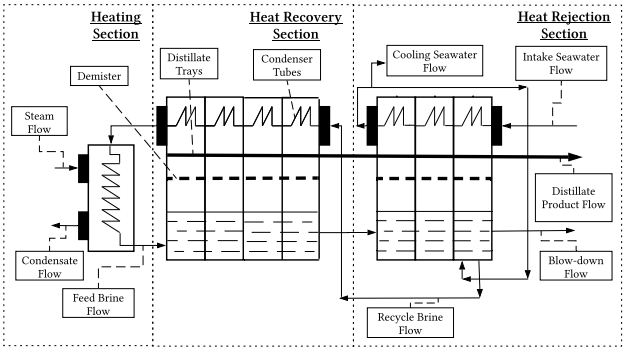


Figure 1: A typical Multi-Stage Flash desalination process.

Idaho laboratory. In this demonstration, the circuit breakers were intentionally opened and closed out of phase to rest of the power grid which caused damage to the connected generators. Out of phase open and close results in high electrical current and torque that is converted into mechanical stress possibly leading to failure. Moreover, this attack can also damage connected power system equipment such as motors and transformers [35]. While Aurora was just a test, Ukraine's power grid suffered a different fate when it was targeted on December 24, 2015. Three Ukrainian regional electricity distribution companies were attacked by coordinated cyber attacks which were executed within 30 minutes of each other. The attacks used spear email phishing to obtain access into the business network, stealing VPN credentials. Once inside the ICS network, adversaries issued commands to create service outage and then performed denial-of-service attack on call centers [26]. A follow-up attack on Ukraine also occurred in 2017.

Damn Vulnerable Chemical Process (DVCP) is an open-source framework that specifically targets research on offensive strategies in chemical processes. It includes simulations for Tennessee Eastman Process and Vinyl Acetate Process which allows researchers to study the consequences of cyber attacks on ICS [25]. Similar work has been done for investigating attack surface and corresponding defense mechanism for smart grids [24], as well as the oil and gas industry [32].

The closest academic work in the field of water treatment is the Secure Water Treatment (SWaT) testbed [27]. SWaT can be used to assess the effectiveness of attack detection and to understand the affects of failure, once the water treatment plant is compromised [13]. SWaT, however, focuses on reverse osmosis-based water treatment, which is fundamentally different compared to traditional thermal-based desalination. Cyber-security analysis of water treatment processes also appears in [4, 5]. These studies propose the use of multiple delay-differential observers for fault detection and isolation of a potential attack in water SCADA system. Observers use an analytic approximation of the canal hydrodynamics, and the model is capable of capturing the effect of both upstream and downstream flows. They are configured to be insensitive to one fault and sensitive to others, assuming no prior knowledge about the inputs.

Critical Infrastructure	Components	Attacks	Impact	References
Water Treatment Plant (SWaT)	1. Ultrafiltration system 2. Ultraviolet chlorine destruction unit 3. Reverse osmosis system	1. Multi CIP command attacks - Stop CPU, crash CPU, crash or reboot ethernet controller 2. Network attacks - ARP poisoning, Man-in-the-Middle attack 3. Evil-Twin attack - Impersonate a legitimate access point	1. Reduction in water production 2. Water overflow in the tank due to false sensor reading	[27] [28]
Smart Grid	1. Generating stations 2. Distribution substations 3. Transformers 4. Intelligent electronic devices	1. Device attack - Compromise a grid device (Relay controller, Circuit breaker) 2. Data attack - Bad data injection, alteration, deletion in network traffic 3. Network availability attack - Denial of Service (DoS) by flooding false information	1. System collapse (blackout) 2. Abrupt increase in load to cause circuit overflow	[24] [19]
Chemical Plant (Damn Vulnerable Chemical Process)	1. Vaporizer 2. Feed-effluent heat exchanger 3. Gas compressor 4. Gas removal system 5. Azeotropic distillation column	1. Production Damage - Reducing reactant inflow at control loops 2. Replay attack - Replay recorded packets 3. False data injection attack - Insert modified packets into the network 4. DoS attack - Flood network with packets	1. Production loss 2. Increase in reactor pressure	[25] [23]
Desalination Plant (MSF)	1. Heat exchanger 2. Condenser tubes 3. Steam ejector 4. Condensate ejector	1. Performance attack - Sensor, actuator, and controller attacks 2. Mechanical failure attack - Actuator attacks	1. Financial damage as a result of performance impact 2. Mechanical damage as a result of water hammer	This work

Table 1: Summary of different components of a critical infrastructure, attacks proposed in literature and their impact.

To the best of our knowledge, no research work has specifically targeted Multi-Stage Flash (MSF) desalination plants and analyzed the impact of cyberattacks on performance and mechanical components. Table 1 summarizes the basic differences between these critical infrastructures with regards to their components, attacks proposed, and their impacts.

3 MSF DESALINATION PROCESS: A PRIMER

Desalination is the process of converting high salinity sea water into potable water. Desalination technologies can be mainly divided into thermal (boiling sea water, collecting steam and leaving behind salt), crystallization (utilizing electric current to drive ions across a selectively permeable membrane separating water and salt), and membrane methods (using pressure to drive sea water through selectively permeable membrane leaving behind salt). Our focus is on Multi-Stage Flash desalination technique, falling under the thermal category, as this has been the most employed technique in the past and older desalination plants still use MSF as their technique for desalination. Some recent plants have started using membrane methods, but we target existing, legacy infrastructure built in an era when cybersecurity was not a priority. Still, most of the attacks described here also apply to other types of desalination plants such as Multi Effect Distillation, Thermal Vapor Compression and Mechanical Vapor Compression.

MSF desalination plants mainly consist of three sections, as shown in Fig. 1: (a) Heat Rejection Section, (b) Heat Recovery Section, and (c) Heating Section. Temperature of the seawater increases as it flows through the heat rejection section. It absorbs latent heat of condensation from the vapors of feed brine flowing inside the flashing chambers. Some of this heated seawater is then mixed with the feed brine while a part of it is rejected as cooling seawater. This process allows for a safe mixing of this new intake with the feed brine in the last stage. To control the maximum salinity inside flashing chambers, some part of this brine mixture is rejected as blow-down brine. High salinity reduces the amount of heat that can be absorbed by the brine which further reduces efficiency of the plant.

Mixture of this new brine, dubbed "recycle brine" is then sent to heat recovery section. As recycle brine flows through the condenser, it absorbs latent heat of condensation. These vapors are released by the feed brine flowing inside the flashing chambers and condense on the tube of the condenser. These flashed off vapors (distillate) pass through the demister and are then collected in a distillate tray. The flashing process takes place due to the decrease in the stage saturation temperature which reduces the corresponding stage pressure. After this, recycle brine enters heating section where it is heated using steam and then passes into flashing chambers as feed brine. Due to the use of recycle brine as feed brine, the amount of steam required to heat it to the top brine temperature is reduced. This recycle brine already absorbs heat released by the vapors while flowing through the heat recovery section [2].

4 THREAT MODEL AND ASSUMPTIONS

In this study, we use a Matlab Simulink model for simulating the operation of a MSF desalination plant ported from [10]. We investigate attack outcomes assuming 3 types of attacks:

(1) **Sensor Attacks:** In this scenario, adversary manipulates readings of the sensors, some of which are input to the controllers. This is a typical example of False Data Injection. The model has 4 flow rate, 3 level, 3 temperature, and 1 pressure sensors.
(2) **Actuator Attacks:** Adversary manipulates the signals to the valves of the plant. It should be noted that in our model all the actuators are valves. The model has 2 gas valves and 9 liquid valves.

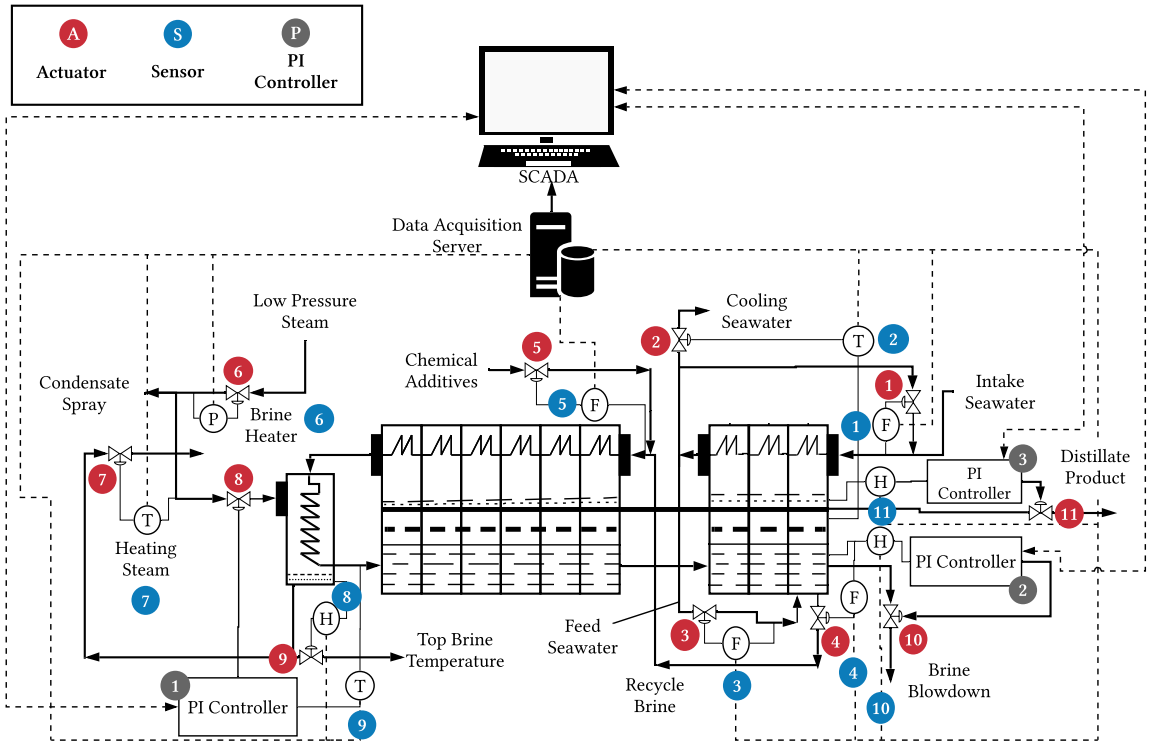


Figure 2: A typical MSF desalination process. Actuators (valves) are shown in red, and controllers (PI) are marked in gray. Sensors, marked in blue, include: F (Flow rate); H (Level); T (Temperature); P (Pressure).

Sr. No.	Actuators		Sensors		Controllers	
	Type of Valve	Flow	Type of Sensor	Sense	Type	Control
1	Fluid	Intake seawater rate	Flow	Intake seawater flow	PI	Input steam to brine heater
2	Fluid	Reject flow rate	Temperature	Cooling seawater temperature	PI	Blowdown flow rate
3	Fluid	Feed flow rate	Flow	Feed brine flow	PI	Distillate flow rate
4	Fluid	Recycle brine flow rate	Flow	Recycle brine flow		
5	Fluid	Chemical flow rate	Flow	Chemical additives flow		
6	Gas	Low pressure steam	Pressure	Intake steam pressure		
7	Fluid	Condensate spray	Temperature	Steam temperature		
8	Gas	Steam flow rate	Level	Condensate level in brine heater		
9	Fluid	Condensate inside brine heater	Temperature	Initial brine temperature		
10	Fluid	Blowdown flow rate	Level	Brine level in final stage		
11	Fluid	Condensate flow rate	Level	Distillate level in final stage		

Table 2: Actuators, Sensors and Controllers used in our simulation.

(3) **Controller Attacks:** Here, the adversary can modify the control parameters of the process. The model includes PI controllers which are control loop feedback mechanism used to get optimum response based on the values of P (Proportional) and I (Integral) parameters. The adversary can modify the P, I, and setpoint (desired output) of the controllers.

We assume that the adversary has compromised the ICS network inside MSF desalination plant and has access to the Supervisory Control and Data Acquisition (SCADA) system. Some of the techniques that can be used by the adversary to gain access into the network are mentioned below [30]:

(1) Using an infected device infiltrated inside the trusted perimeter as a source of entry point. For instance, an employee can be given an infected USB memory stick by using social engineering skills.
(2) By exploiting poorly configured firewall, weak passwords that are used to access VPN or spear email phishing for targeting victims into providing their passwords.
(3) In case of a compromised supply chain, preinstalling malicious codes and backdoors into devices that are supplied to the plant can provide direct access to the adversary. Using

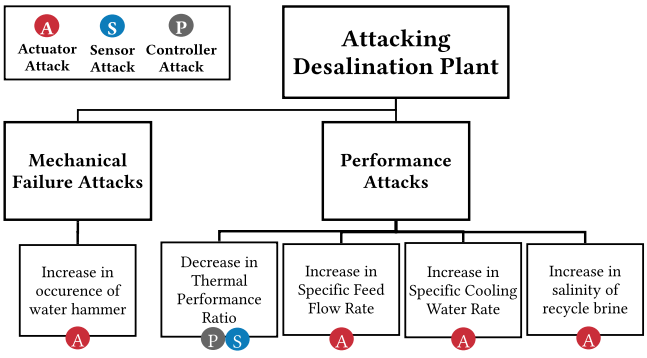


Figure 3: Attack tree for thermal desalination plants.

these compromised devices, malicious code can be spread across other devices on the network.

After internal network infiltration, the adversary has access to the PLCs that receive remote commands from SCADA system. This access can be used to manipulate P and I term values of the PI controller. A PI controller is a control loop feedback mechanism which is used to get optimum response based on the values of P and I parameters. Moreover, the adversary can also read values of the sensors that are connected to Data Acquisition Server (DAQ) and SCADA system. These values can be recorded during normal operation and then replayed for deceiving the monitoring module of SCADA system, similar to how Stuxnet was reporting appropriate values to the Human Machine Interface (HMI) of the operators.

Therefore, according to our simulation model, the adversary has access to 11 sensors, 3 controllers, and 11 actuators, as shown in Fig. 2 and Table 2 labels all the components in the simulation.

It should be emphasized that exploring new attack entry points, payload delivery, etc. are outside of the scope of this work. A wealth of attack vectors have been reported, such as social engineering, USB infiltration, spear email phishing, etc. It is also assumed that the adversary can read values of the sensors that are connected to the SCADA system. The contribution of this work lies on performing *process-aware* cyber threat analysis.

5 PROCESS-AWARE CYBERATTACKS

Process-aware cyberattacks [22] intelligently modify sensor or actuator signals, or the dynamic process being controlled and the implementation mechanism of the control algorithm. The attacks can be broadly categorized in two categories (Fig. 3): 1) Performance Attacks, which aim to stealthily incur financial damage to the plant operation, and 2) Mechanical Failure Attacks, which aim to physically destroy equipment.

This section introduces process-aware cyberattacks which are simulated in Section 6. The adversary needs to deceive the monitoring module of SCADA system by recording legitimate values of sensor signals during normal operation and replay these during the attack. But, just replaying the recorded values while decreasing the performance by a value grater than its steady state variation can cause suspicion and eventual detection of the attack. So, the adversary needs to find a balance between the decrease in performance as a result of an attack and the normal operation of the plant. For instance, in the case of Stuxnet, PLC logic was modified such that it caused the centrifuge to rotate at a higher speed for a fixed time and then it was again brought down to a normal value while sending recorded values to the monitoring system. This decreased the performance of the plant in the long term and also had eventual mechanical impact on the affected centrifuges.

5.1 Performance Attacks

The main objective of the adversary is to incur financial loss to the desalination plant while remaining within operational limits. For a desalination plant, distillate product is the critical output. Therefore, reducing the amount of distillate will cause financial loss to the company. There are four important performance criteria that are used for describing a desalination plant:

5.1.1 Thermal Performance Ratio. Thermal Performance Ratio (TPR) is defined as the ratio of the amount of distillate produced to the amount of steam supplied. A high TPR value means that more amount of distillate is produced per unit amount of steam supplied to brine heater. So, for decreasing the performance of the plant, the attacker has to decrease TPR such that the amount of distillate decreases per unit amount of steam supplied to the brine heater.

For decreasing TPR, the adversary can decrease the amount of steam supplied to brine heater or manipulate the setpoints of the controllers, in order to reduce the amount of steam flowing into the brine heater. Another approach would be to only change the P or I value of PI controller. Moreover, the adversary can also decrease the final stage brine level by increasing blowdown flow rate which reduces the overall feed brine flowing inside the flashing chambers. The attacker can also inject false sensor data and deceive PI controller into decreasing the amount of steam flow allowed into brine heater.

5.1.2 Specific Feed Flow Rate. The Specific Feed Flow (SFF) rate is defined as the ratio of feed sea water to the amount of distillate produced. The value of this performance parameter should be low, indicating that the amount of feed seawater input to the system is less than the amount of distillate produced.

The attacker can try to increase this parameter such that the plant does not operate at an optimum state. Increase in SFF implies that there is an increase in the amount of feed sea water required to produce unit amount of distillate.

5.1.3 Specific Cooling Water Rate. The Specific Cooling Water (SCW) rate is defined as the ratio of the amount of cooling seawater used per unit amount of distillate produced. This efficiency parameter should be low because the amount of distillate produced should be more than the amount of sea water required.

An actuator attack can increase the SCW parameter while also decreasing the corresponding distillate output.

5.1.4 Salinity Ratio. Salinity Ratio (SR) is defined as the ratio of top brine salinity to the salinity of intake seawater. This parameter should also be minimized, as an increase in the salinity ratio corresponds to an increase in the top brine salinity which reduces performance of the plant. Moreover, high salinity can increase the occurrence of localized corrosion, decrease in the flow rate of the brine and eventual blockage in the pipes.

Component	Property	Value	Unit
PI Controller 1	Setpoint	93	-
	Proportional gain	50	-
	Integral time	0.001	-
PI Controller 2	Setpoint	0.556818	-
	Proportional gain	-50	-
	Integral time	0.001	-
Actuator 2	Reject flow rate	95.35	ton/min
Actuator 3	Sea water feed rate	143.816	ton/min
Actuator 4	Recycle brine flow rate	217.25	ton/min
Actuator 10	Blow down flow rate	29.2841	ton/min

Table 3: Initial configuration of the components of the MSF desalination plant.

5.2 Mechanical Failure Attacks

The ultimate goal of the adversary in this scenario is to cause mechanical damage to the desalination plant. This can be performed in numerous ways depending on the specific plant. In this paper, however, we focus on an attack that can be performed on all thermal desalination plants, since it assumes the presence of water pipes and valves.

5.2.1 Water Hammer. Water hammer is a shock wave that is transmitted through a hydrodynamic flow when its motion is suddenly brought to a halt. Generally this huge spike in pressure is dissipated quickly, but if the pipe system is incapable of handling such a sudden spike in pressure, it might lead to some significant mechanical damage. Pressure profile of a wave moving in a fluid can be represented as:

$$\frac{\mathrm{d}P}{\mathrm{d}t} = \rho a \frac{\mathrm{d}v}{\mathrm{d}t} \tag{1}$$

where P represents pressure in the fluid, ρ represents the density of the fluid, a refers to the speed of sound through the fluid, which describes how quickly a pressure wave can propagate through the pipe, v is the velocity of the flowing liquid, t is the time over which the change in momentum occurs [15].

An abrupt change to the momentum of the fluid creates a pressure wave that travels through the pipe and subjects the pipe system to significant forces which increases the chance of mechanical damage. In our experiments, we have calculated internal stresses and displacement for studying the effect of the forces induced from the water hammer attack.

6 EXPERIMENTAL RESULTS

6.1 Experimental Setup

For studying performance attacks, we use a MATLAB Simulink model of an MSF desalination plant ported from [10]. This full-order model has been tested and validated against real plant data obtained from the Khubar II MSF plant in Saudi Arabia [3]. The model is a 22 stage MSF desalination plant, which consists of 3 Heat Rejection Sections and 19 Heat Recovery Sections. This process model is defined by nine variables: brine pool height, brine flow rate, salt mass fraction, brine temperature, distillate flow rate, distillate temperature, coolant temperature, vaporization rate, and stage pressure. Mass and energy balance for both brine and distillate is calculated for all the 22 stages and the brine heater. The brine and distillate flow rate is calculated using its correlation with brine level and distillate level respectively. Initial values for the components used in our experiments are mentioned in Table 3.

Mass and energy equations for all stages except for the last stage are written below [3].

Mass balance of brine pool:

$$\rho_{B,j} A_B \frac{dL_j}{dt} = B_{j-1} - B_j - V_j \tag{2}$$

where $\rho_{B,j}$ is the density of brine in stage j, A_B is the cross section area of brine chamber, L_j is the brine level in stage j, B_j is the brine flow rate in stage j and V_j is the vapor rate in stage j.

Energy balance of brine pool:

$$\rho_{B,j} A_B L_j Cp_{B,j} \frac{dT_{B,j}}{dt} = B_{j-1} Cp_{B,j}(T_{B,j-1} - T_{B,j}) - V_j(\lambda_{c,j} - Cp_{B,j}(T_{B,j} - T_0)) \tag{3}$$

where $\rho_{B,j}$ is the density of brine in stage j, A_B is the cross section area of brine chamber, L_j is the brine level in stage j, $Cp_{B,j}$ is the specific heat capacity of brine, $T_{B,j}$ is the brine temperature in stage j, B_j is the brine flow rate in stage j, $\lambda_{c,j}$ is the latent heat of vaporization and T_0 is the reference temperature ($0°C$).

Mass balance in distillate tray:

$$D_j = D_{j-1} + V_j \tag{4}$$

here D_j is the distillate flow rate in stage j and V_j is the vapor rate in stage j.

Energy balance of condenser tubes:

$$M_{C,j} Cp_{C,j} \frac{dT_{C,j}}{dt} = B_0 Cp_{C,j}(T_{C,j+1} - T_{C,j}) + U_j A_{HC} \Delta T_j \tag{5}$$

$$U_j A_{HC} \Delta T_j = V_j \lambda_j \tag{6}$$

here $M_{C,j}$ is the liquid holdup in condenser tube in stage j, $Cp_{B,j}$ is the specific heat capacity of brine, $T_{C,j}$ is the temperature of condenser in stage j, B_j is the brine flow rate in stage j, $T_{C,j}$ is temperature of condenser in stage j, U_j is the heat transfer coefficient of condenser tube, A_{HC} is the heat transfer area of condenser tube, w is the orfice width and V_j is the vapor rate in stage j.

Brine Flow:

$$B_j = w L_j K_j \sqrt{\rho_{B,j}(P_{j-1} - P_j + \rho_{B,j} g(L_j - Ch_j))} \tag{7}$$

where B_j is the brine flow rate in stage j, w is the orfice width, L_j is the brine level in stage j, K_j is the orfice discharge coefficient in stage j, $\rho_{B,j}$ is the density of brine in stage j, P_j is vapor pressure in stage j, g is the gravitational constant, C is orfice contraction coefficient and h_j is orfice height.

Distillate flow:

$$D_j = C_{D,j} \sqrt{\rho_{D,j} g L_{D,j}} \tag{8}$$

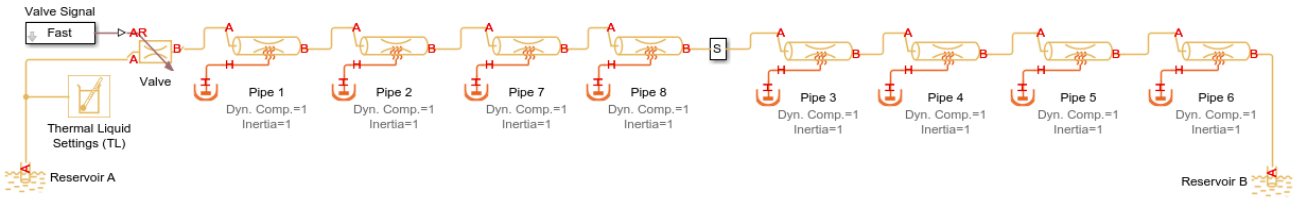


Figure 4: Model used for control volume analysis.

here D_j is the distillate flow rate in stage j, C is orfice contraction coefficient, $\rho_{D,j}$ is density of distillate, g is the gravitational constant and $L_{D,j}$ is the distillate level in stage j.

All the aforementioned equations are solved for each stage in MATLAB Simulink model. Estimated financial loss has been calculated by using the values presented in [14], considering a plant capacity of 50,000 ton of distillate per day and a continuous undetected attack operation of 5 years [1].

For evaluating the detrimental effects of water hammer in a pipeline and estimate its mechanical response, we created a novel computational framework using MATLAB and ANSYS. The analysis consists of two steps.

(1) Control volume analysis: Analysis of dynamic response of the fluid flow upon sudden valve closures using MATLAB.
(2) Finite element analysis: Analysis of the pipe segment in response to the pressure wave computed in the previous step (1) using ANSYS Mechanical.

The control volume analysis is performed using MATLAB. As shown in Fig. 4, this model consists of the valve being attacked, a pipe which is divided into 8 pipe segments, a sensor in the middle of the pipe for recording flow rate and pressure values, reservoir A and B used for establishing an initial flow in the pipe. The valve is modeled using Variable Local Restriction block, which simulates the pressure drop arising from a time-varying reduction in flow area as in the case of valves. A sensing setup is employed for measuring pressure and mass flow rate through the pipe during hammering. Each pipe segment can experience pressure losses and unsteady transient heating due to viscous friction and conductive heat transfer through the pipe wall. Moreover, the dynamic compressibility and fluid inertia effects are also included. Viscous friction is computed using the Darcy-Weibach law [33], while the heat exchange coefficient follows from the Nusselt number correlations [34]. The control volume analysis deals with the conservation of mass, momentum and energy [12]. The mass conservation equation for a single pipe segment (Fig. 4) can be written as,

$$\dot{m}_A + \dot{m}_B = v\rho\left(\frac{1}{\beta}\frac{dp}{dt} + \alpha\frac{dT}{dt}\right) \tag{9}$$

where $\dot{m}_A$ and $\dot{m}_B$ represents the mass flow rates through the ports A and B of a pipe segment, v is the volume of the fluid in the pipe segment, ρ is the isothermal liquid density, β is the bulk modulus of the pipe, α represents the isobaric thermal expansion coefficient, p is the liquid pressure in the pipe and T represents the temperature in the pipe.

The momentum balance for the pipe segment is broken into two parts, i.e., momentum conservation for the half pipe adjacent to port A (Eq. 10) and the remaining half adjacent to port B (Eq. 11).

$$A(p_A - p) + F_{v,A} = \frac{L}{2}\dot{m}_A \tag{10}$$

$$A(p_B - p) + F_{v,B} = \frac{L}{2}\dot{m}_B \tag{11}$$

where A represents the pipe cross-sectional area, p, p_A, p_B are the liquid pressures in the pipe, at port A and port B respectively. $F_{v,A}$ and $F_{v,B}$ are the viscous dissipation forces between the pipe volume center and ports A and B. This can be computed using Eq. 12 depending on the flow regime in the pipe segment.

$$F_V = \begin{cases} -\lambda\nu\left(\frac{L+L_{eq}}{2}\right)\frac{\dot{m}}{2D^2} & \text{(laminar flow)} \\ -f\nu\left(\frac{L+L_{eq}}{2}\right)\frac{\dot{m}|\dot{m}|}{2\rho DA} & \text{(turbulent flow)} \end{cases} \tag{12}$$

Here λ represents the pipe shape factor, ν is the kinematic viscosity of the liquid. L_{eq} is the equivalent length and D is the hydraulic diameter. f is the *Darcy friction factor* of the pipe and can be computed using the Haaland approximation (Eq. 13) for flows in turbulent regime [18].

$$f = \frac{1}{\left[-1.8log_{10}\left(\frac{6.9}{Re} + \frac{1}{3.7}\frac{r}{D}\right)^{1.11}\right]^2} \tag{13}$$

Lastly, the energy balance is modeled using Eq. 14

$$v\frac{d(\rho u)}{dt} = \dot{E}_A + \dot{E}_B + Q_H \tag{14}$$

$\dot{E}_A$ and $\dot{E}_B$ is the total energy flow rates through ports A and B. Q_H is the total heat flow rate through the pipe wall and consists of heat transfer via conduction (Q_{cond}) and convection (Q_{conv}), given by Eq. 15 and 16 respectively.

$$Q_{cond} = \frac{k_f A_H}{D}(T_H - T_f) \tag{15}$$

$$Q_{conv} = |\dot{m}_{avg}|C_{p,avg}(T_H - T_{in})\left(1 - e^{\frac{hA_H}{|\dot{m}_{avg}|Cp,avg}}\right) \tag{16}$$

Here $\dot{m}_{avg}$ is the average mass flow rate from A to B and is given by $(\dot{m}_A - \dot{m}_B)/2$. k_f is the thermal conductivity of the fluid. A_H is the total surface area of the pipe walls. T_H, T_f and T_{in} represent the temperature of the pipe, fluid and inlet respectively. Lastly, $C_{p,avg}$ is the specific heat evaluated at the average temperature.

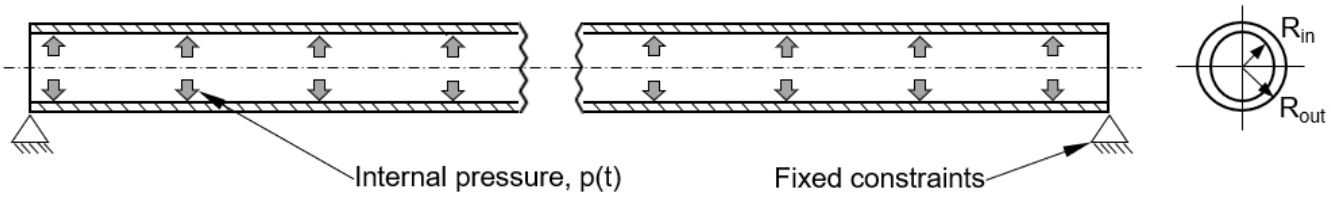


Figure 5: Schematic of the pipeline with boundary conditions used for finite element analysis.

The heat transfer coefficient h in Eq. 17 depends on the *Nusselt* number (Nu) and can be computed using,

$$h = Nu\frac{k_{avg}}{D} \tag{17}$$

In the case of turbulent flows, Nu is evaluated using the Gnielinski correlation [17] given by

$$Nu_t = \frac{\frac{f_{avg}}{8}(Re_{avg} - 1000)Pr_{avg}}{1 + 12.7\sqrt{\frac{f_{avg}}{8}}\left(Pr_{avg}^{2/3} - 1\right)} \tag{18}$$

where f_{avg}, Re_{avg} and Pr_{avg} are the Darcy friction factor, Reynolds number and Prandtl number evaluated at average temperature.

The above mentioned conservation equations are implemented for the pipe setup, and a steady state is established. The valve is then suddenly closed and the resulting transient pressure fluctuations $p(t)$ occurring inside the pipe are recorded. These results are then used in the next step to evaluate the structural response of the pipe element using ANSYS.

We choose Finite Element Analysis (FEA) for performing our mechanical simulations because the governing equation of structural mechanics cannot be solved directly for complex problems. The Finite Element Method (FEM) is used to compute the numerical solution of such structural analysis problems. In FEM, the structural problem is modeled with the help of discrete elements called 'finite elements' interconnected at discrete points called nodes. This allows the user to simulate extreme loading conditions which might be costly to test experimentally or difficult to recreate in a laboratory setting. Moreover, FEA has the advantage of visualizing the results which cannot be done theoretically or experimentally, for e.g. internal stress distribution. Hence, by visualizing the results we can better understand the safety of the structure and possible failure locations in the system.

This analysis is carried out to evaluate the stress concentration zones and to determine the distribution of deformation throughout the length of the pipe segment. The maximum displacement is a measure of the strength of the water hammer. The higher the displacement, higher is the chance of mechanical failures along the pipeline and its fixtures.

Fig. 5 shows the schematic of the geometry used for constructing the 3D Finite element model along with the boundary conditions used. The inner radius (R_{in}) and wall thickness of the pipe are set at 0.0134 m and 0.0025 m respectively. It is assumed that the pipe is supported at every 2.5 m. The FE model contains 540, 883 nodes, each having three translational and three rotational degrees of freedom. Structural steel was selected as the material of the pipeline and it's mechanical properties are presented in Table 4. The material is assumed to be isotropic and linear elastic. As mentioned earlier, the pipe is loaded with the time varying pressure profile $p(t)$ obtained using the control volume analysis. This pressure is uniformly distributed throughout the inner surface of the pipe.

Property	Value	Unit
Density	7850	kg/m^3
Young's modulus	$2e^{11}$	Pa
Poisson's Ratio	0.3	-
Bulk modulus	$1.6667e^{11}$	Pa
Shear modulus	$7.6923e^{10}$	Pa
Tensile yield strength	250	MPa

Table 4: Structural steel material properties used for FEA.

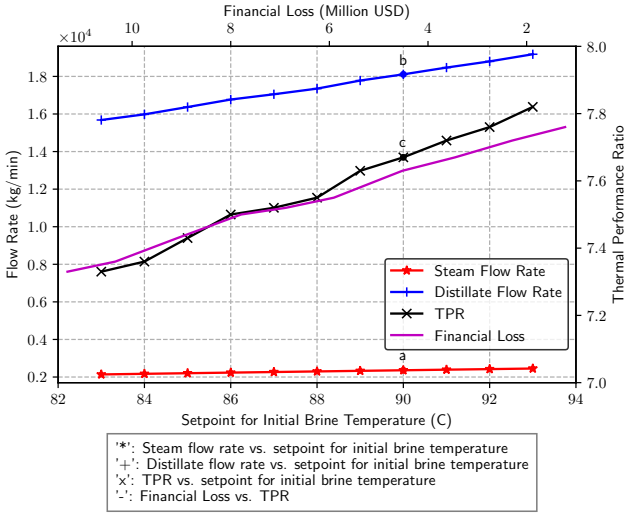


Figure 6: Change in distillate flow during attack to TPR by manipulating initial brine temperature. Financial loss w.r.t. TPR over a period of 5 years is shown in magenta.

6.2 Impact of Performance Attacks

6.2.1 Thermal Performance Ratio. Fig. 6 shows the relationship between TPR and the financial loss imposed by cyber attacks. It can be seen that as TPR decreases, financial loss increases. So, for causing a financial impact, intuitively, the adversary needs to

lower the TPR value corresponding to a lower amount of steam flowing into the brine heater. This in turn reduces the amount of distillate produced causing the aforementioned financial impact. For decreasing TPR, the setpoint of 'PI controller 1' can be adjusted, which in turn changes the input steam flow. It can be observed in Fig. 6 that a relatively small decrease in the amount of steam supplied to brine heater leads to large decrease in the amount of distillate produced and a corresponding decrease in TPR.

In our attack simulation, we change the setpoint from 93°C to 90°C (point 'a' in Fig. 6) which results in an average decrease of 1.07 ton/min (point 'b' in Fig. 6) in distillate production and a corresponding decrease in TPR (point 'c' in Fig. 6). If we assume an undetected attack and the plant operation of 5 years, the total estimated financial loss caused by this attack turns out to be more than $3 million considering a plant capacity of 50,000 ton of distillate per day.

Since the adversary needs to remain undetected for incurring maximum economic damage, decreasing the setpoint by a large amount is not advisable as this might lead to attack detection due to the use of additional quality control sensors that are not connected to the SCADA system. Another approach for decreasing the performance of a desalination plant while remaining within operational limits would be to change the P or I value of the appropriate PI Controller. For instance, by changing the I value of 'PI controller 1' from 0.001 to 1, reduces the distillate flow rate by 0.04 ton/min. This would effectively lead to an estimated financial loss of around $130K if the attack is undetected for 5 years. The adversary can also adjust the setpoint associated with 'PI Controller 2'. It was observed in our attack simulation that an increase in setpoint by 27% decreased the distillate flow rate by 0.08 ton/min while the blowdown flow rate remains constant. This loss of distillate product will incur an estimated financial loss of more than $250K assuming that the attack remains unnoticed for 5 years.

The attacker can also leverage false data injection for decreasing the performance of a desalination plant. For instance, in our attack simulation, injecting 'Sensor 9' which measures initial brine temperature with a value of 94°C instead of 93°C, decreases the steam flow to 1,000 kg/min which is the minimum allowed. This further reduces the distillate flow rate to just 4.57 ton/min. But such a drastic decrease, while effective, might be detected by the plant operators. So, the adversary in this case has to spoof the sensor signal only for a fixed repeating interval so that the overall average distillate flow rate is not decreased by a noticeable amount. In an effort to remain within operational limits, we injected false data to 'Sensor 9' of 'PI controller 1' at a repeating fixed time interval. This created a repeating interval where we decreased the distillate output and observed an average decrease of 0.7 ton/min in distillate output. Assuming a 5-years operation, this would lead to an estimated financial loss of more than $220K.

6.2.2 Specific Feed Flow Rate. Fig. 7 displays the relationship between the SFF rate and financial loss. It can be seen that as the SFF rate increases, there is also a corresponding increase in the financial loss incurred. This is because an increase in the amount of SFF signifies the use of more input feed brine flow for creating the same amount of distillate.

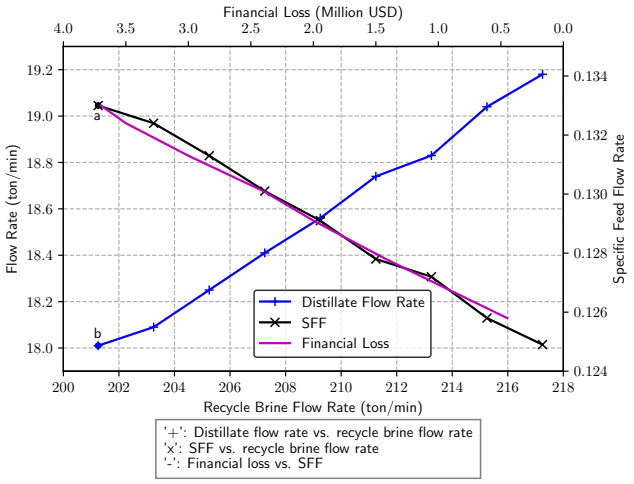


Figure 7: Change in distillate flow during attack simulation for SFF by manipulating recycle brine flow rate. Financial loss w.r.t SFF over a period of 5 years is shown in magenta.

In order to increase the SFF rate, the adversary can use an actuator attack to manipulate the actuators controlled by the SCADA system. For our attack demonstration, we increase the flow of feed sea water through 'Actuator 3' and decrease the flow of recycle brine through 'Actuator 4'. This effectively increases the amount of feed brine required and decreases the recycle brine, which in turn results in a reduction of the amount of distillate produced. As shown in Fig. 7, in our attack simulation, the SFF parameter is maximum at around 201 ton/min flow of recycle brine (point 'a' in Fig. 7) and the distillate produced decreases by 1.06 ton/min (point 'b' in Fig. 7). So, if the plant runs for 5 years without suspicion, the desalination plant in this case would incur an estimated financial loss of more than $3 million.

Fig. 8 displays the relationship between the SCW rate and the corresponding financial loss. It can be observed that as the SCW rate increases, financial loss increases as well. This is because an increase in SCW rate signifies an increase in the amount of required input cooling seawater for the same amount of distillate produced.

An actuator attack can be used to increase SCW. Ideally this value should be as low as possible, but the adversary can manipulate 'Actuator 2' for increasing the reject flow rate, which in turn increases the amount of cooling seawater required by the desalination plant. This increase in SCW parameter due to attack initiation can be observed in Fig. 8, where point 'a' represents the value of SCW parameter during normal operation and point 'b' represents the SCW value just after attack initiation.

6.2.3 Specific Cooling Water Rate:

6.2.4 Salinity Ratio. Actuator attacks can also be used to increase salinity ratio of a desalination plant. Fig. 9 shows the change in salinity of recycle brine with respect to operation cycles (One operation cycle is completed when the recycle brine circulates through all the 22 stages of a desalination plant).

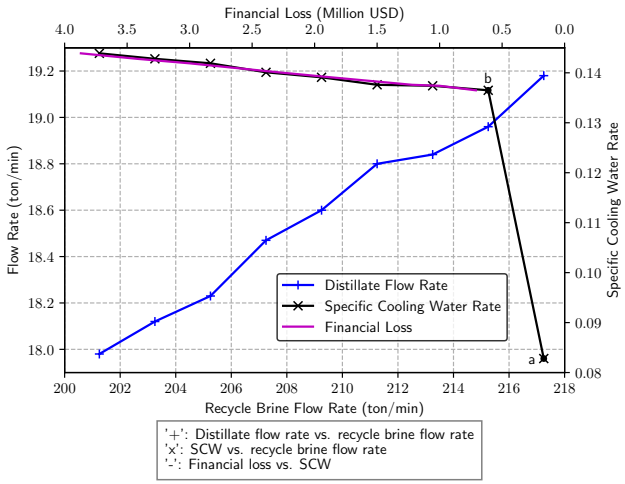


Figure 8: Change in distillate flow during attack simulation for SCW by manipulating recycle brine flow rate. Financial loss w.r.t SCW over a period of 5 years is shown in magenta.

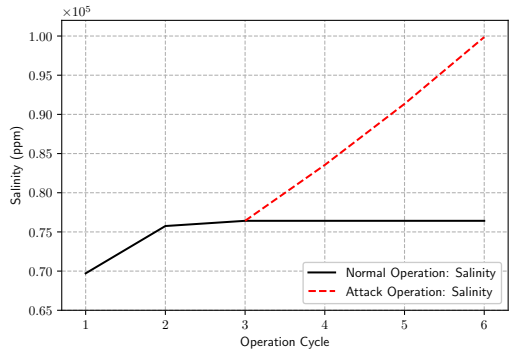


Figure 9: Change in salinity of seawater when Actuator 8 is attacked.

For instance, during normal operation, the desalination plant will remain in the salinity limit ranging from 63,765 ppm to 76,417 ppm which is shown by 2 operation cycles. The blowdown rate is adjusted such that maximum salinity of the plant remains in a safe range. We simulated an actuator attack repeating after fixed intervals by closing the blowdown valve which temporarily increased salinity from 76,417 ppm (point 'a' in Fig. 9) to as high as 99,863 ppm. Specifically, we temporarily blocked 'Actuator 10', which is used to control blowdown flow rate, such that more amount of recycle brine accumulated in final stage of flashing chamber, thus increasing the salinity. After reaching this maximum, 'Actuator 10' is switched back to normal operation.

To make this attack relatively unnoticed, the attack needs to be triggered only at specific intervals and fake data needs to be supplied to the SCADA monitoring system. Upon completion of the attack during each iteration, the blowdown valve was switched back to normal operation. Depending on the cyber attack motives, the adversary may choose to increase salinity with a much lower rate or also to a higher salinity value.

6.3 Impact of Mechanical Failure Attacks

6.3.1 Water Hammer. Water hammer can be initiated by incorrect operation of the actuators of the desalination plant. Fig. 10a shows the change in pressure in the pipe as a result of water hammer. It can be seen from the plot that there is a maximum increase in the pressure of about 5 Mpa.

By using the aforementioned pressure values, a FEA is performed in ANSYS. Fig. 10b shows the von Mises stress or equivalent stress induced in the pipe during the water hammer. This stress value is used to determine if the given material will fail due to yielding. It is evident that there are considerable internal stresses on the pipe as a result of pressure surge from the water hammer. The maximum von Mises stress observed in the FEA are of the order of $\approx 340MPa$, which is considerably higher than $215MPa$, the yield strength of the pipe material. The corresponding displacement in the pipe is plotted in Fig. 10c. It can be observed that the pipe experiences significantly violent displacements during water hammer. This type of excessive stress and displacement in the pipe can also lead to breakdowns at restraints and fixtures.

For modeling the stresses experienced by the pipe, we assume that the pipe is clamped at its two ends. The maximum displacement experienced by the pipe is in its middle portion and reaches a value of 19.938 mm. Moreover, fixtures supporting the pipe structure also experience von Mises stress of the order of $\approx 309MPa$. Overtime repeated occurrence of water hammer will cause mechanical damage due to fatigue that can be exploited to bring down the plant. In our attack demonstration leveraging recycle brine flow to perform water hammer, the adversary exploited access to actuators 1, 2, 4, and 10. It should again be emphasized that component destruction requires extensive pre-attack testing using the exact components in a lab setting.

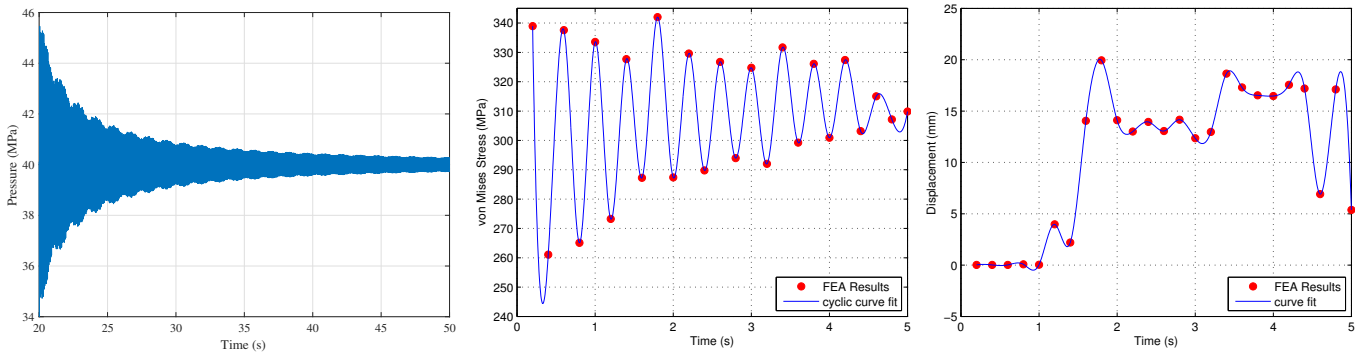
7 DISCUSSION

Table 5 summarizes the attacks presented in Section 6, while, Table 6 presents various attack vectors to achieve the corresponding effects.

7.1 Maximizing Impact

It is evident that the adversary has numerous entry points for performing various attacks, but not all the entry points will be equally effective for maximizing impact. For instance, according to our experiments, decreasing TPR by using only 'Actuator 8' incurs more financial loss when compared to decreasing the setpoint for 'PI Controller 2'. This is because 'Actuator 8' controls the flow of steam in the desalination plant which is more critical for the desalination output when compared to 'PI Controller 2'. As observed in Table 6, all demonstrated process-aware attacks maximize their effect when the actuators are attacked.

For initiating water hammer, it is most effective to target a combination of various actuators. This is because the input to the desalination plant finally accrues in the last flashing chamber. So, temporarily blocking blowdown flows such as reject cooling sea water, blowdown brine flow and increasing the input seawater rate, results in the increase of brine flowing through the desalination plant. This increase can be used for maximizing the increase in pressure surge.



(a) Pressure surge in the pipe (b) Von Mises Stress in the pipe (c) Displacement in the pipe

Figure 10: Finite element analysis results demonstrating the effects of water hammer on the plant pipes.

Attacks		Type	Methodology	Impact	Section
Performance Attacks	Thermal Performance Ratio (TPR)	Controller attack	1. Modify parameters of 'PI controller 1' 2. Increase setpoint of 'PI Controller 2'	Financial loss	6.2.1
		Sensor attack	Inject false data in'Sensor 9'		
	Specific Feed Flow Rate (SFF)	Actuator attack	Increase feed sea water flow at actuator 3 and decrease recycle brine flow at actuator 4	Financial loss	6.2.2
	Specific Cooling Water Rate (SCW)	Actuator attack	Increase reject flow rate at actuator 2	Financial loss	6.2.3
	Salinity Ratio	Actuator attack	Close blowdown valve (actuator 8)	Increase in salinity	6.2.4
Mechanical Failure Attack	Water Hammer	Actuator attack	Increase flow through actuators 1, 2, 4 and block flow at actuator 10	Mechanical Damage	6.3.1

Table 5: Summary of process-aware attacks for MSF desalination plants.

Impact	Attack Vectors		
	All	**Maximum Impact**	**Within Operational Limits**
Decrease in Thermal Performance Ratio	{A3} {A4} {A8} {P1} {P2} {S9} {S11} {A10}	{A8}	{P2}
Increase in Specific Feed Flow Rate	{A3,A4} {A8,A3} {S9,A3} {P1,A3} {S11,A3} {P2,A3}	{A3,A4}	{P2,A3}
Increase in Specific Cooling Water Rate	{A10,A2} {A8,A2} {S9,A2} {P1,A2} {S11,A2} {P2,A2}	{A8,A2}	{P2,A2}
Increase in Salinity Ratio	{A10} {P2} {P2,S11}	{A10}	{P2}
Water Hammer	{A1} {A2} {A3} {A4} {A10} {A11}	{A1,A2,A4,A10}	{A10}

Table 6: Summary of attack vectors per high-level impact.

7.2 Remaining within Operational Limits

For maximizing financial impact to the desalination plant, the adversary needs to remain within plant operation limits for avoiding suspicion. One of the reasons for fully automating of desalination plants in recent years is to increase the operation time of the plants in their steady state. Frequently, unforeseen circumstances such as variation in the seawater temperature from the expected value, or sudden decrease in the amount of steam in brine heater, affect the output distillate flow rate. This is considered normal and the control system of the plant will adjust to the new parameters.

Therefore, for the adversary to remain undetected during an attack, the distillate product flow rate should always be kept close to the operation limits. For instance, the optimum product flow rate in the simulation is 19.3 ton/min, while the range of distillate flow varies between 15 to 28 ton/min as shown in [11]. So, to remain undetected, an attack should maintain all measured variables within the noise limits, and avoid long stretches of undesirable plant states.

Another major part of is the footprint of the adversary in the control process. Depending on the specific configuration, sensor values and actuator commands may be replicated and logged. On the other hand, modifications of the P and I parameters of the controllers would require inspection of the internal logic of the control parameters. Modifying these parameters still allows the controller to reach its setpoint, but not in an optimal way.

One of the major assumptions in process-aware attacks is the adversary's prior knowledge about the control process and its implementation mechanisms. For instance, in our work, the adversary has prior knowledge about the sensors, actuators, and controllers in the MSF desalination plant. While this type of attack can effectively compromise a plant, it is hard to generalize to other plants, since it is process-specific. Traditional IT attacks, on the other hand, do not vary much between targets as the communication protocols, ports, computing components and their vulnerabilities might still remain consistent.

8 CONCLUSION

Industrial control systems security has been explored extensively in the literature, mainly focusing on the power grid, water treatment plants, and chemical processes. In this interdisciplinary work, we have explored potential cyber attacks both in economic terms (inducing financial loss) and mechanical aspects (destroying equipment). Performance attacks have been investigates on a Matlab desalination plant model, while mechanical attacks on an ANSYS model we developed. Results show that the adversary has a variety of options for inducing attacks that maximize impact while remaining within operational limits. Furthermore, the mechanical engineering study also demonstrates that there is the danger of equipment damage from the cyberspace. This work aims to motivate the need for cybersecurity research for desalination plants and serve as a platform for development of mitigations against process-aware attacks.

ACKNOWLEDGMENTS

This research was carried out in the Center for Cyber Security at New York University Abu Dhabi and was supported by the NYU Abu Dhabi Global PhD Fellowship program. We would like to thank the anonymous reviewers and Chengyu Song (UC Riverside) for their valuable feedback.

REFERENCES

[1] Hala Faisal Al-Fulaij. 2011. *Dynamic modeling of multi stage flash (MSF) desalination plant.* Ph.D. Dissertation. University College London.
[2] Imad Alatiqi, Hisham Ettouney, and Hisham El-Dessouky. 1999. Process control in water desalination industry: an overview. *European Conference on Desalination and the Environment* 126, 1 (1999), 15 – 32.
[3] Emad Ali, Khalid Alhumaizi, and Abdelhamid Ajbar. 1999. Model reduction and robust control of multi-stage flash (MSF) desalination plants. *Desalination* 121, 1 (1999), 65–85.
[4] Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M. Bayen. 2013. Cyber Security of Water SCADA Systems - Part I: Analysis and Experimentation of Stealthy Deception Attacks. *IEEE Trans. Contr. Sys. Techn.* 21, 5 (2013), 1963–1970. https://doi.org/10.1109/TCST.2012.2211873
[5] Saurabh Amin, Xavier Litrico, S. Shankar Sastry, and Alexandre M. Bayen. 2013. Cyber Security of Water SCADA Systems - Part II: Attack Detection Using Enhanced Hydrodynamic Models. *IEEE Trans. Contr. Sys. Techn.* 21, 5 (2013), 1679–1693. https://doi.org/10.1109/TCST.2012.2211874
[6] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Mark Felegyhazi. 2012. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet* 4, 4 (2012), 971–1003.
[7] T. M. Chen and S. Abu-Nimeh. 2011. Lessons from Stuxnet. *Computer* 44, 4 (2011), 91–93. https://doi.org/10.1109/MC.2011.115
[8] DHS. 2019. Water and Wastewater Systems Sector. Retrieved May 8, 2019 from https://www.dhs.gov/water-and-wastewater-systems-sector
[9] E. DeNicola and O. S. Aburizaiza and A. Siddique and H. Khwaja and D. O. Carpenter. 2015. Climate Change and Water Scarcity: The Case of Saudi Arabia. *Annals of Global Health* 81, 3 (2015), 342–353. https://doi.org/{https://doi.org/10.1016/j.aogh.2015.08.005}
[10] Emad Ali. 2002. Understanding the operation of industrial MSF plants Part I: Stability and steady-state analysis. *Desalination* 143, 1 (2002), 53–72. https://doi.org/{https://doi.org/10.1016/S0011-9164(02)00221-7}
[11] Emad Ali. 2002. Understanding the operation of industrial MSF plants Part II: Optimization and dynamic analysis. *Desalination* 143, 1 (2002), 73–91. https://doi.org/{https://doi.org/10.1016/S0011-9164(02)00222-9}
[12] Robert W Fox, Alan T McDonald, and Philip J Pritchard. 2004. Introduction to fluid dynamics. *John Wiley & Sons* (2004).
[13] Hamid Reza Ghaeini and Nils Ole Tippenhauer. 2016. Hamids: Hierarchical monitoring intrusion detection system for industrial control systems. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. 103–111.
[14] Younes Ghalavand, Mohammad Sadegh Hatamipour, and Amir Rahimi. 2015. A review on energy consumption of desalination processes. *Desalination and Water Treatment* 54, 6 (2015), 1526–1541. https://doi.org/10.1080/19443994.2014.892837
[15] Mohamed S Ghidaoui, Ming Zhao, Duncan A McInnis, and David H Axworthy. 2005. A review of water hammer theory and practice. *Applied Mechanics Reviews* 58, 1 (2005), 49–76.
[16] Jairo Giraldo, Esha Sarkar, Alvaro A Cardenas, Michail Maniatakos, and Murat Kantarcioglu. 2017. Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design & Test* 34, 4 (2017), 7–17.
[17] Volker Gnielinski. 1975. Neue Gleichungen für den Wärme-und den Stoffübergang in turbulent durchströmten Rohren und Kanälen. *Forschung im Ingenieurwesen A* 41, 1 (1975), 8–16.
[18] Skjalg E Haaland. 1983. Simple and explicit formulas for the friction factor in turbulent pipe flow. *Journal of Fluids Engineering* 105, 1 (1983), 89–90.
[19] Yi Huang, Mohammad Esmalifalak, Huy Nguyen, Rong Zheng, Zhu Han, Husheng Li, and Lingyang Song. 2013. Bad data injection in smart grid: attack and defense mechanisms. *IEEE Communications Magazine* 51, 1 (2013), 27–33.
[20] International Desalination Association. 2017-2018. *IDA Desalination Yearbook 2017-2018.* http://idadesal.org/publications/ida-desalination-yearbook/
[21] Akili D Khawaji, Ibrahim K Kutubkhanah, and Jong-Mihn Wie. 2008. Advances in seawater desalination technologies. *Desalination* 221, 1-3 (2008), 47–69.
[22] Farshad Khorrami, Prashanth Krishnamurthy, and Ramesh Karri. 2016. Cybersecurity for control systems: A process-aware perspective. *IEEE Design & Test* 33, 5 (2016), 75–83.
[23] Istvan Kiss, Bela Genge, and Piroska Haller. 2015. A clustering-based approach to detect cyber attacks in process control systems. In *2015 IEEE 13th international conference on industrial informatics (INDIN)*. IEEE, 142–148.
[24] Charalambos Konstantinou, Marios Sazos, and Michail Maniatakos. 2016. Attacking the smart grid using public information. In *17th Latin-American Test Symposium*. 105–110. https://doi.org/10.1109/LATW.2016.7483348
[25] Marina Krotofil and Alexander Isakov. [n. d.]. Damn Vulnerable Chemical Process-Vinyl Acetat Monomer. https://github.com/satejnik/DVCP-VAM [Accessed: 8 May 2019].
[26] Gaoqi Liang, Steven R Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. 2017. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems* 32, 4 (2017), 3317–3318.
[27] Aditya P. Mathur and Nils Ole Tippenhauer. 2016. SWaT: a water treatment testbed for research and training on ICS security. In *International Workshop on Cyber-physical Systems for Smart Water Networks*. 31–36. https://doi.org/10.1109/CySWater.2016.7469060
[28] Aditya P Mathur and Nils Ole Tippenhauer. 2016. SWaT: a water treatment testbed for research and training on ICS security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. IEEE, 31–36.
[29] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, and R. Karri. 2016. The Cybersecurity Landscape in Industrial Control Systems. *Proc. IEEE* 104, 5 (2016), 1039–1057. https://doi.org/10.1109/JPROC.2015.2512235
[30] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. 2012. Cyber-Physical Security of a Smart Grid Infrastructure. *Proc. IEEE* 100, 1 (2012), 195–209. https://doi.org/10.1109/JPROC.2011.2161428
[31] A. Al Radif. 2010. Operation of desalination plant. Retrieved May 8, 2019 from http://www.desware.net
[32] Pedram Radmand, Alex Talevski, Stig Petersen, and Simon Carlsen. 2010. Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries. In *24th IEEE International Conference on Advanced Information Networking and Applications*. 949–957. https://doi.org/10.1109/AINA.2010.175
[33] Hunter Rouse. 1937. Modern conceptions of the mechanics of fluid turbulence. *Trans ASCE* 102 (1937), 463–505.
[34] Stephen Whitaker. 1972. Forced convection heat transfer correlations for flow in pipes, past flat plates, single cylinders, single spheres, and for flow in packed beds and tube bundles. *AIChE Journal* 18, 2 (1972), 361–371.
[35] M Zeller. 2011. Common questions and answers addressing the aurora vulnerability. *Schweitzer Engineering Laboratories Report* (2011).
[36] S. Zhioua. 2013. The Middle East under Malware Attack Dissecting Cyber Weapons. In *IEEE International Conference on Distributed Computing Systems Workshops*. 11–16. https://doi.org/10.1109/ICDCSW.2013.30