Case Study with Supporting Media and Simulation Exercise

Title: Securing Water Plants with CIE Principles

Real World Inspiration

The real-world inspiration for this Case Study looks into water treatment plants. The diagram below gives a brief overview of the operations (composed of 5 stages) of a water plant in Pittsburgh. As depicted, there are many steps required to deliver clean water. In addition to these steps, there are many points of failure that water plants must be careful to avoid, especially cybersecurity threats. This is especially concerning as water is such a vital resource for human survival and well-being. Many water plants use devices connected to the internet and cloud that can increase our attack surface. This exercise is primarily concerned with the 4th and 5th stages of the water plant. At these stages the water is treated with chemicals to sanitize it, which can introduce threats where an adversary could potentially change these values to harmful levels.

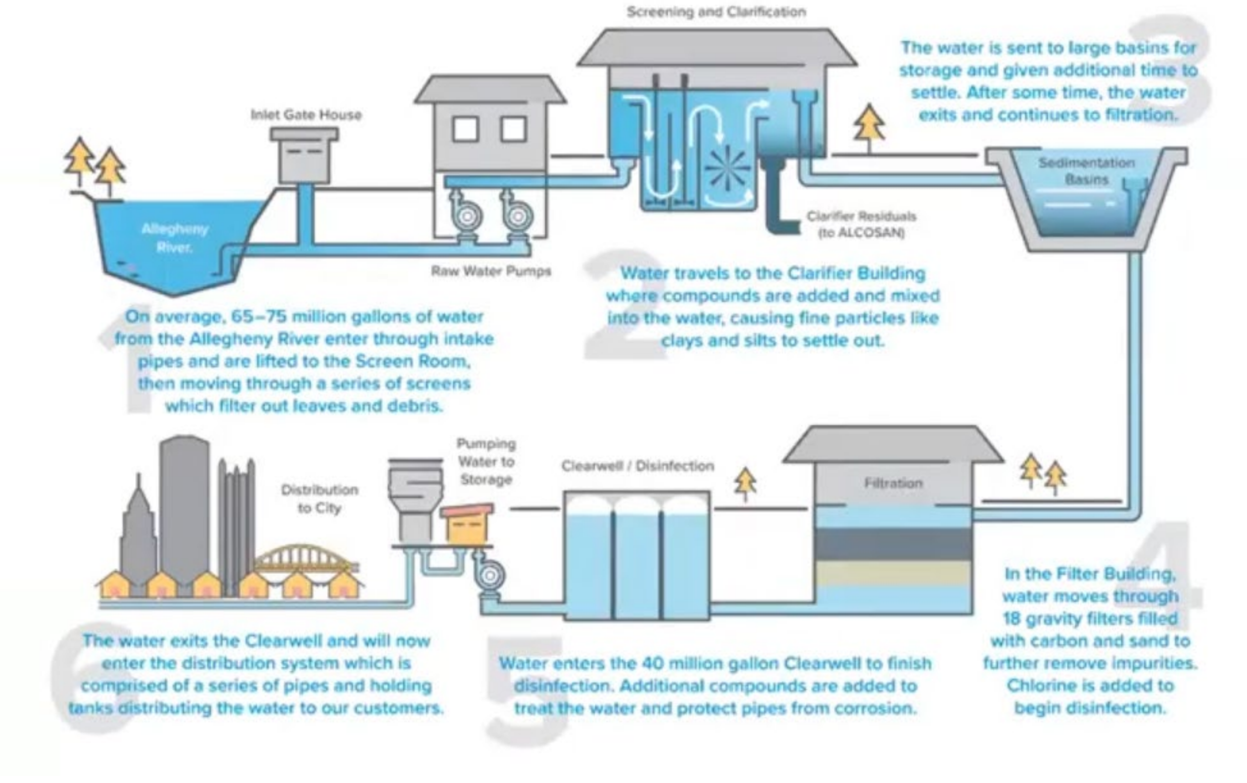

Screening and Clarification
Inlet Gate House
Allegheny River
Raw Water Pumps
Clarifier Residuals (to ALCOSAN)
Sedimentation Basins
3
The water is sent to large basins for storage and given additional time to settle. After some time, the water exits and continues to filtration.
1
On average, 65–75 million gallons of water from the Allegheny River enter through intake pipes and are lifted to the Screen Room, then moving through a series of screens which filter out leaves and debris.
2
Water travels to the Clarifier Building where compounds are added and mixed into the water, causing fine particles like clays and silts to settle out.
Distribution to City
Pumping Water to Storage
Clearwell / Disinfection
Filtration
4
In the Filter Building, water moves through 18 gravity filters filled with carbon and sand to further remove impurities. Chlorine is added to begin disinfection.
5
Water enters the 40 million gallon Clearwell to finish disinfection. Additional compounds are added to treat the water and protect pipes from corrosion.
6
The water exits the Clearwell and will now enter the distribution system which is comprised of a series of pipes and holding tanks distributing the water to our customers.

Figure 1: Simple Water Plant (Credit: Frank Sidari and PGH2O)

The specific attack addressed in this module is an attack that occurred in Oldsmar, Florida. An operator noticed their mouse moving on their screen and changed levels of sodium hydroxide from 100-ppm to 11,000-ppm. At these levels, the water severely damages any human tissue that it touches [1]. The operator quickly spotted this and reverted the changes. If this had not been spotted, the water could have reached the city in 24 to 36 hours. However, automated PH testing would have triggered an alarm and caught the change before anyone was harmed [1]. In this attack, the adversary gained access to the system through remote access software [3]. Computers used by water plant personnel were connected to all the water plants SCADA systems. They all had remote access software that shared the same password and were connected to the internet without a firewall. An employee with the login credentials had access to the plant controls via remote access [6]. The remote software had a unique username for each device that must be known, but it is best practice to have unique passwords as well. Initially, it was believed that the attack was from an external adversary. However, upon further examination it was deemed to be more likely an insider attack from a disgruntled employee who had access to water systems from outside the plant.

Motivated by the CIE principles, there are several steps that the water plant could have taken to stop this attack. The remote software was not used for 6 months before the attack [2]. In this case, one possible countermeasure would be removing the software. Remote access software is inherently dangerous with them enabling complete control of a device that they are connected to. Disabling this helps enforce **Design Simplification** as we are removing any unnecessary features to reduce the attack surface. Another countermeasure that could help is installing a firewall on the network to only allow access from authorized devices. The plant could have implemented better **engineered controls**. Through bounding the PH levels or requiring separation of privileges (where multiple employees must agree on change), we can engineer our system to be less vulnerable. To prevent insider attacks, it is recommended to apply separation of privilege or duty, auditing, access control, onboarding and offboarding policy. Implementing auditing helps detect anomalies as we can track employee actions and see if they have engaged in a suspicious activity. We must be careful about what to audit to ensure privacy and efficiency. If we track every mouse click there is too much data to go through. The onboarding policy helps with our **organizational culture** as it would help ensure that employees will follow cybersecurity principles and accordingly behave in a trustworthy manner. For the offboarding policy we recommend that employees' access to company systems to be closed or revoked when they depart. This could include taking actions such as removing all their accounts, so they cannot access company systems and blocking all company data that they have access to. There may be room for improvement regarding access controls in this case. The computers used by water plant personnel had complete access to all the SCADA systems on the plant. If each employee was responsible for only certain parts of the water plant, then each employee's workstation should only access stations they are responsible for.

Along with specific recommendations, we present general recommendations for water plants. If the water plant needs remote software for their operation, then one option they could consider is an isolated network (not connected to the internet). If remote access to the plant using internet access is necessary, then they should consider using a DMZ that would include a firewall to vet network traffic for defense in depth. A DMZ is subnetwork that includes services or devices that can be accessed by external users. As general practice we recommend assigning unique and strong passwords to every account and device. This helps enforce **planned resilience**, as even if an attacker has a password, they can only access that specific system. We also recommend an onboarding policy for every device to fully understand their vulnerabilities. This applies to cybersecurity controls, as we are only as secure as our least secure device. Lastly, we recommend keeping all hardware and software up to date to prevent known vulnerabilities from being exploited.

Media Feature for the General Audience

For a custom media clip designed by faculty and students at the University of Pittsburgh, please click on the video file found here: [**https://youtu.be/a5QJ71xhjrE]**

This video will provide students with a thorough overview of key engineering concepts and the importance of simulation practice. News reporting and real-life depictions emphasize how engineering problems and solutions are perceived by greater audiences. Having this investigative approach will improve the student's ability to relate the different principles in various areas of engineering. By the end of this segment, students will gain a deeper understanding of how CIE Principles are applied and visualized in practical scenarios, enhancing comprehension of complex cyber engineering systems. Narrative is essential to understanding why the core principles found in CIE Principles are considered and applied.

Future Policy Implications

In response to the cyberattack on Oldsmar, Florida's water treatment facility, recommendations for organizational policies should focus on improving cybersecurity measures to prevent similar incidents. The electric power grid industry offers relevant practices that the water treatment sector could adopt.

Firstly, it is important to discuss the stakeholders and players involved in water treatment to better understand future policy implications. The most important body is The Water Industry Skills Advisory Committee (WISAC), which plays a pivotal role in developing and maintaining the skills and competencies of the workforce, ensuring that water treatment professionals are well-trained and capable. Government agencies, such as the Environmental Protection Agency (EPA) and local and state water authorities, regulate water quality standards and oversee treatment plants and distribution networks. Water treatment plant operators manage daily operations to ensure compliance with these standards. Engineers and technicians design and maintain the necessary infrastructure, while chemists and microbiologists conduct quality testing and develop improved treatment methods. Public health officials monitor public health, conduct risk assessments, and respond to waterborne disease outbreaks. Researchers and scientists innovate new technologies and study environmental impacts. Environmental NGOs and advocacy groups push for stricter regulations, raise public awareness, and conduct independent testing. Consulting firms offer expertise in project design, implementation, and regulatory compliance. Equipment manufacturers and suppliers provide essential materials and technology. Municipalities and local governments manage water resources and infrastructure to meet community needs. Finally, the public use water, report quality issues, and can sometimes support conservation efforts and sustainable water management policies. Together, these actors ensure effective, sustainable, and safe water treatment processes that protect public health and the environment.

Next, just like the electric power grids, water treatment facilities should foster collaboration between OT and IT teams as it is essential to ensure both networks are robust and secure. OT teams focus on the reliable and safe operation of physical processes and machinery, while IT teams handle data management, cybersecurity, and information flow. Effective communication and cooperation between these teams can lead to comprehensive security strategies, streamlined operations, and the integration of advanced technologies for improved efficiency and safety in water treatment processes.

The biggest issue the industry faces in terms of cybersecurity is legacy systems. Many water treatment facilities operate with outdated operational technology (OT) that was not originally designed with cybersecurity in mind. These legacy systems often lack the necessary security features to defend against modern cyber threats and can be difficult to upgrade or replace due to their critical role in daily operations. This challenge is compounded by limited financial and human resources, which further complicates the ability to invest in new technologies, conduct regular security assessments, and hire skilled cybersecurity professionals. Addressing the integration and upgrade of these legacy systems is essential to enhance the overall cybersecurity posture of water treatment facilities. Water treatment managers are hesitant to upgrade these legacy systems due to the potential operational disruption. Upgrading systems can lead to temporary disruptions in operations, which can be risky and difficult to manage for water as that is necessary for people to survive. Chief security information officers, who handle an organization's information, cyber, and technology security, are often at odds with managers on updating these legacy systems.

Drawing on practices from the power grid sector, it's advisable to implement more rigorous monitoring of network activity, along with stricter controls on who can access critical systems. Multi-factor authentication, proper access control, and continuous monitoring of unusual activities could be crucial. One unusual activity could be in the form of an insider attack, which occurs when an individual within the organization, such as an employee, contractor, or any other person with authorized access, intentionally or unintentionally misuses their access to cause harm or steal sensitive information. These attacks can be particularly damaging because insiders typically have legitimate access to the systems and data they target, making it harder to detect their malicious activities. To prevent insider attacks from employees who have been removed from the system, as soon as an employee's departure is confirmed, all access to physical and digital systems should be immediately revoked. This includes deactivating keycards, usernames, accounts, passwords, and remote access permissions. Reducing insider threats also involves creating a culture of security awareness and regular training for employees. This includes educating staff about the importance of cybersecurity, recognizing signs of potential insider threats, and encouraging them to report suspicious activities. Additionally, conducting regular audits and reviews of access controls can help identify and mitigate potential vulnerabilities.

Moving on, developing robust incident response plans along with regular security audits and upgrades would ensure that security measures keep pace with evolving cyber threats.

Lastly, encouraging a closer collaboration between government agencies and private sector cybersecurity experts, like the partnerships seen in the electric grid sector, could enhance the sharing of best practices and improve overall security readiness.

Expand Your Understanding with a Laboratory Exercise

The Model for This Project is Created by Julio Romeo: Romeo, (2017) activated_sludge_plants_simulink_model,
JulioArielRomero/activated_sludge_plants_simulink_model: simulink model for Wastewater Treatment Plants (WWTPs) based on activated sludge (github.com)

USE CASE

- Users will simulate a false data injection attack (Person in the Middle attack)
- Performed by “injecting” a constant value into the input of a certain metric
  - Ex. recycling factor
- Runs of the simulation before and after the attack can be compared using output graphs
  - Determine if safety was compromised
- Importance in bounding/monitoring values and securing network
- **Cyber Secure Supply Chain Control -** This represents an attack where there is a vulnerability in our device, such as a back door. This is a result of poor supply chain management. We should try to find any vulnerabilities with the devices our suppliers provide us with and the suppliers themselves.

- **Engineered Controls** – The countermeasure of this attack represents this principle as we engineer in a failsafe to stop the system if it detects any anomalies.

(a) Simulation Set-Up

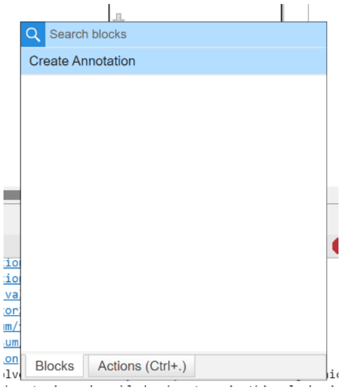
1. Unzip the lab source code folder named Team-2-Water_Sector-M-Week-7_Code.zip
2. After the download Open Matlab
(a) Click on browser folder and open activated_sludge_plants_simulink_model_master.
(b) You can find this file by going to the same directory that you just unzipped the file into.
(c) Right click on the file "activated_sludge_plant" and select add folders and add subfolder to path.
(d) Click on modelo_asm1_v2.slx to run the simulation.
3. Run the system. It should return a missing file error. Click on open file next to the error message and open import_data.m

Task 0: Visualize the Baseline

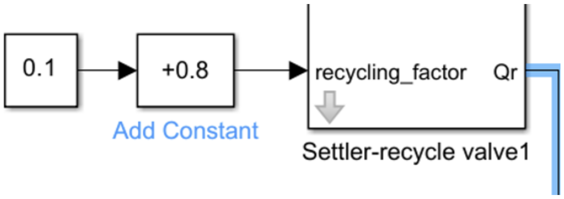
We need to get the baseline graphs to see how the system operates under normal conditions. Run the file again, and while running click on the right most block scope3, which should bring up 5 graphs. The x-axis represents time in seconds and the y-axis is in g COD.m^{-3} [7]. COD represents Chemical Oxygen Demand, a measure of the amount of oxygen required to oxidize a substance in water [4]. Thus, g COD.m^{-3} is the concentration of matter in water that can be oxidized in grams of COD per cubic meter of water. Look at the graph from the second to the bottom. This is the level of particulate inert organic matter. Notice how the level of this never goes above 50 g COD.m^{-3}. This will become relevant later in the lab.

Task 1: Injection Attack

Step 1: Our first attack is an injection attack where we add in a block that acts as a backdoor. To do this move your mouse next to the leftmost Settler-recycle valve on the screen. Then find the Contant value that is being inputted to the reactor. Double-click near this constant value to bring up a search bar as shown below:



Step 2: Once we get here, look up "adder" in the search block and select the first option. Set the value in the block to 0.8. Remove the connection from the 0.1 constant and attach the 0.8 constant block as shown below.



Step 3: Once you have completed all these steps, you may run the program.

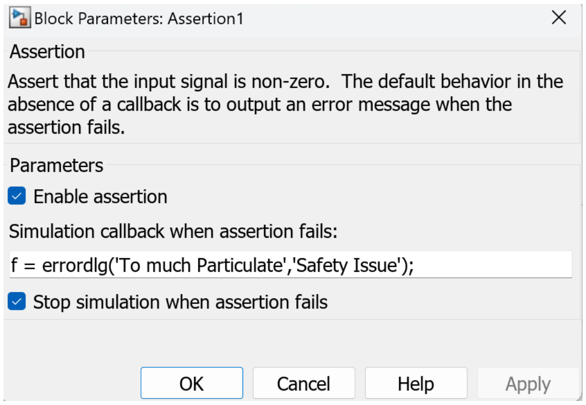
Step 4: Take a screenshot of the graphs like you did in task 0. Notice how the peak of the graph is higher. This is because we increase the Recycling factor. This is the fraction of water being recirculated in the model, which when increased also increases the buildup of particulate matter.

Task 2: Countermeasure

Step 5: Create a new block called "Compare to Constant" and another block called "Assertion". This represents testing of water levels at a water plant, comparing it to a value to ensure that it is bounded. This represents our engineering control, as we implement physical measures to keep water levels in proper bounds.

Step 6: For the first Simulink block ("Compare to Constant"), set the operator to be "<=" and set the value to be 50 with output type Boolean

Step 7: Set the values of assertion block to match the picture, then connect the operator block to the assertion block.


Block Parameters: Assertion1

Assertion

Assert that the input signal is non-zero. The default behavior in the absence of a callback is to output an error message when the assertion fails.

Parameters

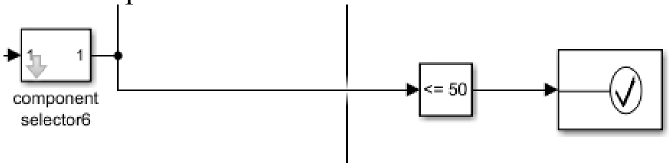
☑ Enable assertion

Simulation callback when assertion fails:

f = errordlg('To much Particulate','Safety Issue');

☑ Stop simulation when assertion fails

Step 8: On the output wire of the component selector 6 block, CTR + click the wire and connect it to the operation block as follows:



Step 9: Run the program.

(a) Expected Result

Changing different parameters in how a system operates can easily have impacts on the outputs of a system. We must monitor the system outputs of water plants to be able to detect anomalies to prevent any public health crisis. The system should have stopped when the particulate inert organic matter reached 50 g COD.m^{-3}, much like how a plant should stop operation, when their water levels are dangerous.

Lab Questions:

1. What does the assertion block do in conjunction with the comparator block?
2. Do some research on what chemicals are used to regulate water parameters in water plants. What chemicals may be dangerous if modified?
3. What steps can we take to secure a network to prevent a man-in-the-middle attack?
4. What CIE principles are at play when we are implementing our countermeasures other than engineered controls?

Further Reading and Useful Public Video Links

For further reading, the following references would be suitable to explore at your convenience.

[1] Greenberg, Andy. “A Hacker Tried to Poison a Florida City’s Water Supply.” *Wired*, 8 Feb. 2021, www.wired.com/story/oldsmar-florida-water-utility-hack/.

[2] CNN, Alex Marquardt, Eric Levenson and Amir Tal. “Florida Water Treatment Facility Hack Used a Dormant Remote Access Software, Sheriff Says.” *CNN*, 10 Feb. 2021, www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html.

[3] Clark, Mitchell. “Turns out That Florida Water Treatment Facility Left the Doors Wide Open for Hackers.” *The Verge*, 11 Feb. 2021,

www.theverge.com/2021/2/10/22277300/florida-water-treatment-chemical-tamper-teamviewer-shared-password.

[4] “Chemical Oxygen Demand (COD) - Water Quality Parameter | Hach.” *Sea.hach.com*, sea.hach.com/parameters/chemical-oxygen-demand.

[5] Romeo, (2017) activated_sludge_plants_simulink_model, JulioArielRomero/activated_sludge_plants_simulink_model: simulink model for Wastewater Treatment Plants (WWTPs) based on activated sludge (github.com)

[6] “Cybersecurity Advisory for Public Water Suppliers | Mass.gov.” *Www.mass.gov*, www.mass.gov/info-details/cybersecurity-advisory-for-public-water-suppliers.

[7] Alex, Jens, et al. “Benchmark Simulation Model No. 1 (BSM1).” *Benchmark Simulation Model No. 1*, 2018, iwa-mia.org/wp-content/uploads/2019/04/BSM_TG_Tech_Report_no_1_BSM1_General_Description.pdf .

Authors

This paragraph should provide a two-sentence biography of each student on the team giving credit for the contribution. Simply list names in alphabetical order based on your last name.

My name is Aditya Madupur and I am a rising junior at the University of Pittsburgh. I am studying neuroscince and am interested in exploring cybersecurity risks in various fields like healthcare.

My name is Ken Barrett, and I am a rising senior at the University of Pittsburgh. I am currently studying computer science and mathematics and I have interests in AI and Cybersecurity.

My name is Alex Bennett, I am a Digital Media major at the University of Pittsburgh with a minor in Creative Writing and certificate in Broadcasting. Additionally, I work in radio and film production.

My name is Cam Mickey and I am a rising senior at the University of Pittsburgh. I am currently studying Computer Science and Film and Media Studies.