Journal of Physics:
Conference Series

PURPOSE-LED
PUBLISHING™

PAPER • OPEN ACCESS

Risk Analysis of Water Grid Systems Using Threat Modeling

To cite this article: Fiza Abdul Rahim *et al* 2022 *J. Phys.: Conf. Ser.* **2261** 012015

View the article online for updates and enhancements.

ECS The Electrochemical Society
Advancing solid state & electrochemical science & technology
ECS UNITED
247th ECS Meeting
Montréal, Canada
May 18-22, 2025
Palais des Congrès de Montréal
Showcase your science!
Abstracts due December 6th

Risk Analysis of Water Grid Systems Using Threat Modeling

Fiza Abdul Rahim[1], Norziana Jamil[2], Zaihisma Che Cob[2], Lariyah Mohd Sidek[3] and Nur Izz Insyirah Sharizan@Sharizal[2]

[1] Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia
[2] College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia
[3] Institute of Energy Infrastructure, Universiti Tenaga Nasional, Malaysia

norziana@uniten.edu.my

Abstract. Critical infrastructure systems consist of physical and cyber assets that are essential to the operation of the economy and the government. As one of the most important critical infrastructures worldwide, the water sector has become vulnerable to new risks in the form of cyber threats that can severely impact public health, and are difficult to detect. A water grid system (WGS) plays an important role in guarding the business processes of the water sector against possible threats and risks. Threat modeling can be used to analyze threats to the WGS. It is applied to identify points of access to the assets and devices of the system, classify threats to them, assess the risks posed by them, and suggest mitigation measures. Each threat is classified based on its type according to the STRIDE methodology, and the results of the threat classification can be used to assess the level of risk by using the DREAD methodology. This yields a risk rating for each threat that can be used to devise mitigation measures to minimize the risk posed by it. Through the threat modeling stage, it is known that the high-risk threats on WGSs are tampering with a risk score of 14, denial of service threats with a risk score of 13, and repudiation threats with a risk score of 12. The results of the ranking are used to formulate recommendations in the form of mitigation controls against these threats.

1. Introduction

Cyberattacks on critical infrastructure are becoming a cause of increasing concern worldwide [1]. As part of such infrastructure, the water sector has become increasingly vulnerable due to the use of automated monitoring and control systems, such as the Supervisory Control and Data Acquisition System (SCADA). It is thus an easy target for attackers as most network devices of the infrastructure are often accessible to the public and lack sophisticated security features.

The integration of operational technology (OT) networks, Information Technology (IT) networks, and the standard design of industrial control systems (ICS) is ushering in the digital age of the industrial sector, including the water industry. The important OTs generated from its assets includes those for water storage, power generation, recreation, navigation, irrigation, electric damage mitigation due to floods, sediment control, and mine tailings impoundment. These assets provide a variety of economic, environmental, and social benefits, but this can be offset by the risk of the damage caused in the event of their failure.

Various kinds of cyberattacks have been reported in recent years that have targeted the water sector, including a water treatment facility in Florida [2], water facilities in Israeli [3], and a dam in New York [4]. Many countries have developed guidelines and cybersecurity programs in an effort to protect the water sector. However, a practical approach should be considered, as suggested by [5], because the integration of newly developed smart components into IT networks and legacy equipment in OT networks is a vulnerable combination that needs to be addressed whenever a component is added, updated, or removed [6].

Dam breaches or failures may have a significant impact on human infrastructure, and can result in many casualties. As the number of elements of the dam system increases, so does the total amount of communication that takes place. This leads to an increase in the number of potential weak points that attackers can exploit [6]. Hence, it is important to ensure appropriate management to reduce the risk posed [7].

The continuous monitoring of a water grid system (WGS) provides a steady stream of data to identify and rectify security-related shortcomings in the system. This can be used to identify the threats posed by and behaviors of attackers to anticipate when and how they may occur, and to prepare adequate countermeasures. This is achieved via an iterative process known as threat modeling; a systematic approach to design policies against various security threats and possible mitigation strategies. This should be the basis of assessing risk and designing security systems for computer and information systems [8]. Hence, prior to determining where the vulnerabilities exist and ensuring that the system is safe, an efficient threat model needs to be established for any given information system.

With regard to the WGS, a threat is any action or event that might result in a malfunction of the system and its services, such as component failure, that can jeopardize the confidentiality, integrity, and availability of the system. While defining security requirements, threats are analyzed based on their criticality and probability of occurrence, and solutions to them are provided based on either mitigating the threat or accepting its risk, as definitions of functionalities and requirements are constantly evolving.

The appropriate identification and rating of threats based on the above requirements define the functionality and services provided by the system and, thus, the appropriate selection of countermeasures that can minimize the potential of attackers to abuse the system. In this respect, threat modeling considers the system from an adversary's point of view to allow developers to predict possible attack targets and develop responses to queries about what the system is intended to protect against. Threat ratings allow security professionals to know where to start when the system requires corrections to identified vulnerabilities.

This study focuses on identifying threats using the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) threat model to identify potential threats, which are then rated using the DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability) risk rating model. The remainder of this paper is structured as follows: Section 2 provides an overview of cybersecurity and cyberattacks related to the water sector, and Section 3 describes the methodology used. Section 4 describes the proposed threat model and resulting attack probabilities, and Section 5 details the implications on security risks to the water sector, and offers the conclusions of this study.

2. Literature Review

This section reviews work on cybersecurity in the water sector in general and provides an overview of the threat assessment model for WGSs.

2.1. Cybersecurity in the water sector

Safeguarding the water sector against cybersecurity threats is considered a national priority [1] because it is part of a country's critical infrastructure. The growing use of automated surveillance and control systems, such as SCADA, for water utilities, has increased cyber-vulnerabilities in the water system [9]. The operations of this infrastructure can be an easy target for an attacker as most network devices are often public facing and easily accessible in the absence of security features.

Most industrial sectors, including the water sector, are embracing the digital age through the integration of OT networks, IT networks, and the standard architecture of ICS. Such integration, however, poses considerable security risks [1] because most ICS devices and protocols are not intended to enable security features. In addition, as OT networks prioritize to availability and IT networks prioritize to confidentiality, combining the two can be difficult. The recovery option is difficult to implement immediately along with critical and real-time business operations in OT because system operations are likely to be interrupted.

The interdependence of ICT equipment and other components makes it clear that the challenges posed by cybersecurity include IT-related dangers and physical threats [10]. Therefore, various mitigation efforts have been implemented to protect the water sector against threats to cybersecurity. For example, NIST highlighted in its guideline that it is critical to consider the influence of cyberthreats on the physical system, dependent systems, and the physical environment when establishing secure ICS [11]. Other ICS security activities should involve continually upgrading the security standards, protocols, and devices [1].

2.2. Modeling cyberattacks

Numerous warnings of cyberattacks on critical infrastructure, and the water sector in particular, have been issued, including those related to ransomware attacks, ICS tampering, valve and flow operations, and chemical treatment formulations [12]. A water utility was attacked in February 2021, and the cybercriminals were able to remotely control the system to modify the volume of water flow and the number of chemicals used to treat it [2]. Similar attacks were reported on Israeli water management facilities in 2020 [3].

In collaboration with Guidewire, the results of a hypothetical cyberattack on an American hydroelectric dam, simulated by global professional services firm AON, showed that such a cyber-incident could cause economic losses of up to $56 billion for local businesses and communities [13]. Another attack on the computer system of a New York dam occurred in 2013, where a hacker allegedly affiliated with the Iranian government accessed confidential files containing usernames and passwords [4].

To protect dams against cyberattacks, the relevant authorities need to identify the specific threats, and may request assistance from cybersecurity experts to establish a suitable defense mechanism [14]. To improve the security of control systems for dams, the US Department of Homeland Security has outlined a cybersecurity program that includes the identification, assessment, risk management, and response and recovery of cyber-assets [15].

An approach has been proposed to address cyber-threats at different levels by incorporating risk assessment and threat modeling to develop security requirements [5]. To detect weaknesses in the security architecture of the dam, the authors of [6] performed a risk analysis of two configurations, namely, water contamination and the overflow of the water tank. In this study, we focus on threat modeling for WGS architecture.

3. Methodology

The proposed modeling methodology is shown in Figure 1, and follows proposals in [16–18]. It features (a) the identification of assets of the IoT device, (b) identification of access points to the device, (c) classification of threats, (d) rating of the identified threats, and (e) proposal of countermeasures to mitigate each threat.

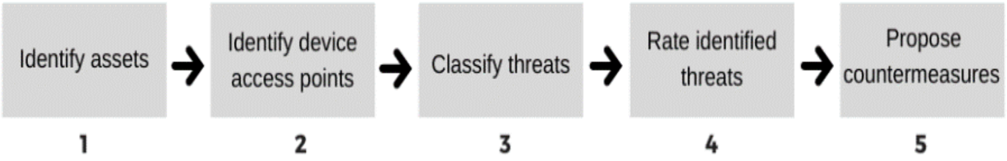

Figure 1. Threat modeling methodology [16–18]

3.1. Identification of assets

The most crucial step in threat modeling is asset identification because they are the main targets of attacks. Attackers refer to persons or processes that threaten the asset from the system or the environment in which it is used. An asset is any valuable component of a system that is owned by the organization that interests attackers. Assets in the environment may evolve dynamically and require security controls to suit the conditions that are not usually expected in the design phase [19]. The assets of WGSs include various interconnected systems, numerous hardware and software components, networks, cabling, power source, power outlets, and different kinds of users interacting with the system.

3.2. Identification of access points of device

Access points are the assorted interfaces threat posing attackers, whereby the attackers may utilize to obtain unauthorized asset privileges. Examples of access points in systems include hardware ports, login screens and user interfaces, open sockets, and configuration files. When an access point has been identified, trust boundaries for it within the system can be defined, and are used to indicate places where the level of trust fluctuates [20]. Trust levels stipulate the quantity of trust necessary to access a given part of the system. For example, a network may constitute a trust boundary such that anyone may access the web via the network, but not anyone outside the corporation can have access to the corporate network.

3.3. Classification of threats

Threats may result from the activities of legitimate users of a system (insiders), who are authenticated and authorized to use the services provided by the system, or from the activities of unauthorized users (outsiders). Threats often originate from weaknesses in design, implementation, or configuration, and are a cause for concern to any or all who use information management systems. The knowledge gathered from the detection of access points can help identify potential threats due to them. Threat classification is performed by using the STRIDE methodology, as shown in Figure 2.

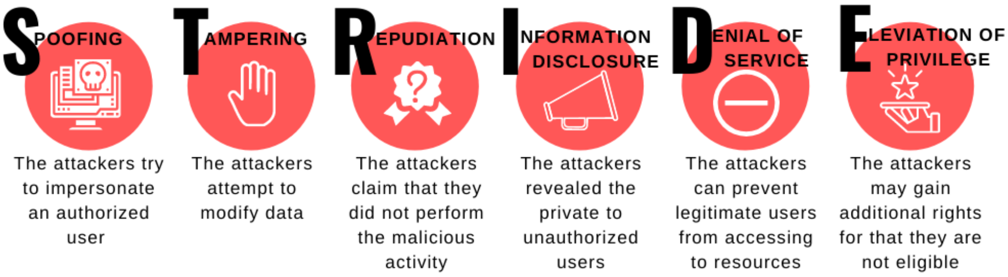
SPOOFING
The attackers try to impersonate an authorized user
TAMPERING
The attackers attempt to modify data
REPUDIATION
The attackers claim that they did not perform the malicious activity
INFORMATION DISCLOSURE
The attackers revealed the private to unauthorized users
DENIAL OF SERVICE
The attackers can prevent legitimate users from accessing to resources
ELEVIATION OF PRIVILEGE
The attackers may gain additional rights for that they are not eligible

Figure 2. STRIDE methodology.

3.4. Rating of identified threats

Following the identification of threats using the STRIDE model, the DREAD risk assessment model is used to assess, analyze, and find the probability of risks by rating each threat. By using the DREAD model, a risk rating is assigned to a given threat by asking the questions shown in Figure 3.

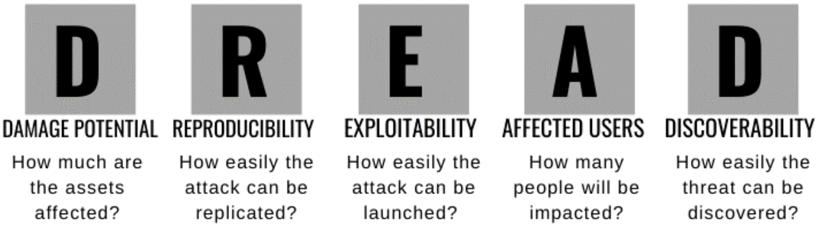
D
DAMAGE POTENTIAL
How much are the assets affected?
R
REPRODUCIBILITY
How easily the attack can be replicated?
E
EXPLOITABILITY
How easily the attack can be launched?
A
AFFECTED USERS
How many people will be impacted?
D
DISCOVERABILITY
How easily the threat can be discovered?

Figure 3. DREAD risk assessment.

Once the threat has been assessed through the assignment of a rating to each item (high, medium, and low) with corresponding values of 3, 2, 1, and 0, the overall risk rating is then obtained by adding the ratings of all items, calculating the average of all five DREAD categories, and comparing the averages. Values from 12 to 15 are considered high, those from 8 to 11 are medium, and values from 5 to 7 are low.

3.5. Proposing countermeasures to mitigate threats

The risk ratings are used by development teams to make informed decisions on prioritizing fixes to software, identifying security controls for an application, and tackling potential threats in a timely manner according to their severity and impact. This leads to a secure environment that uses resources more effectively to avoid potential hazards.

4. Risk Analysis of WGSs Using Threat Modeling

4.1. WGS system architecture

WGSs are composed of water supply pumps, reservoir tanks, pipes, and valves. These systems have a range of elements, including water pressure sensors, water quality sensors, water level sensors, programmable logic controllers, and SCADA. These elements enable the automated operation of the system. The total amount of communication increases with the number of elements, and this leads to more weaknesses that attackers can exploit.

The main task of the WGS is to deliver the requisite volumes of clean water. If an element of the cyber-physical system or the WGS is accessible to attackers, this may compromise the overall process. Attacks can vary from data misuse, false alarms, and halted water delivery to tank overflows and even water contamination, depending on the attacker’s intention.

The analysis in this paper is based on a reference architecture of the WGS shown in Figure 4. The trust zone of components is first identified within Layer 0, and then in Layers 1, 2, and 3 respectively. Trust zones at the control center in the environment of Layer 4 include SCADA and a monitoring system. Layer 5 contains two zones: one that covers the OT and a second dealing with the application server.

Layer 0 refers to the water field or devices of the plant used to generate analog data and send them to other layers while receiving commands from other devices from other layers to ensure the safety and stability of the entire plant. For example, the pump provides sufficient pressure to overcome the operating pressure of the system to move the fluid at the required flow rate. Physical access to this layer should be controlled and monitored using appropriate security measures to prevent intruders from accessing the water plant. Multiple security measures can slow down anyone who tries to harm the water facility, where this may provide more time to detect a problem and respond to it.

Layer 1 consists of devices that receive and process information from those of Layer 0, and act as a control component of the overall system. If the restriction on physical access is not appropriately applied, the integrity of Layer 1 devices may be compromised as the information processed in Layer 1 is sent back to devices in Layer 0. As most controllers are equipped with remote connectivity, it is important for the operators and supervisors to understand how cyber-threats associated with the IT network can affect their OT network.

In Layer 2, a human–machine interface (HMI) serves as a graphical user interface that allows interaction between the human operator and the controller hardware. It can display status information and historical data gathered by devices in the ICS environment. It is also used to conduct system status checks, and to respond to alarms or any other issues that arise during the water treatment process.

Layer 3 separates human-to-human from machine-to-machine communications, where only authorized communications are permitted between the upper and lower layers. The gateway transports to the switch and then to another layer. This part is labeled a machine-to-machine (M2M) layer that features interactions among various devices and machines connected to the Internet and to one another.

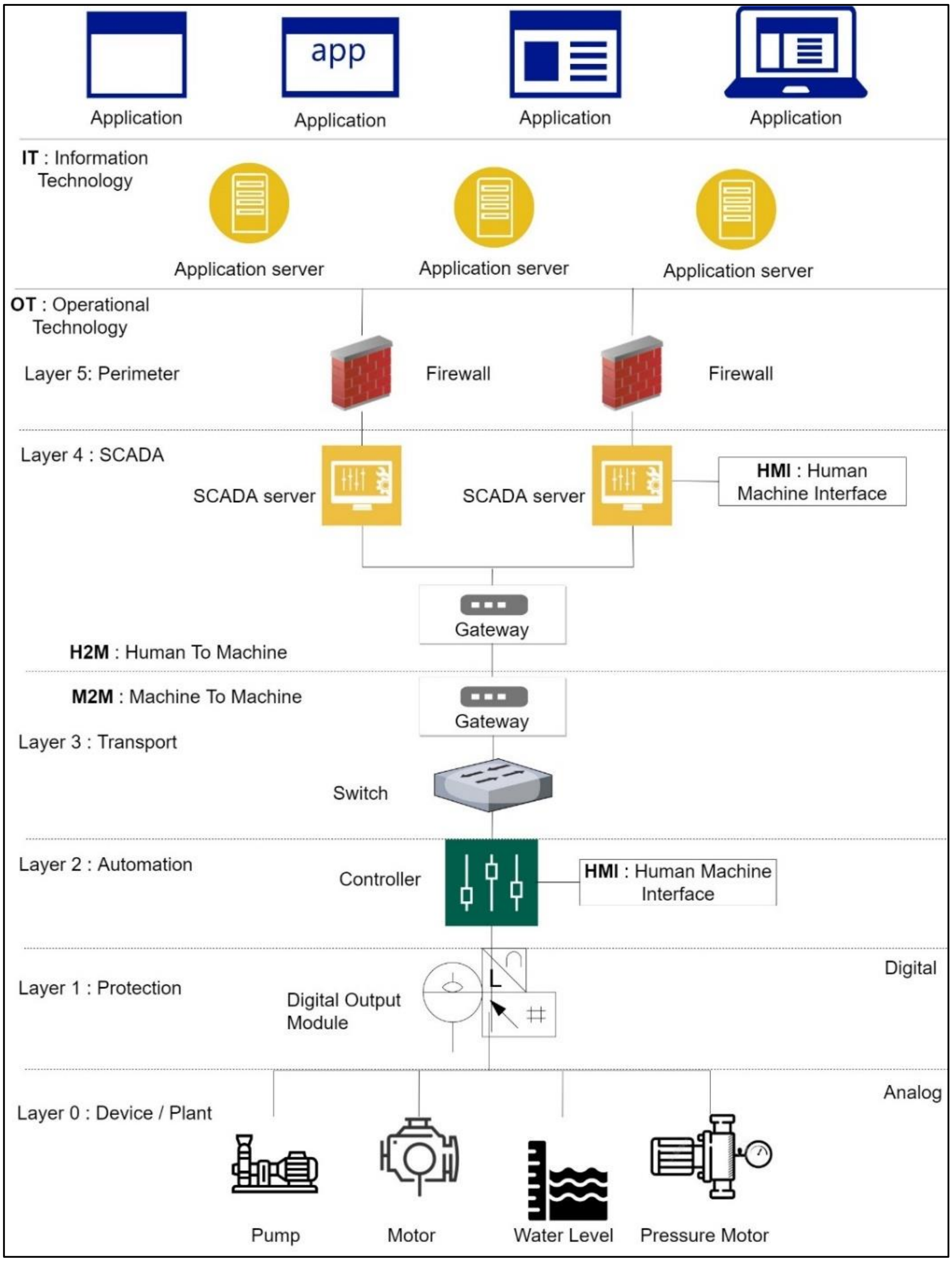

Figure 4. A reference architecture of the water grid system.

Layer 4 is known as SCADA, and is the foundation of the water system infrastructure. The components of SCADA consist of heterogeneous devices, such as intelligent electronic devices, programmable logic controllers, remote terminal units, control servers, and routing and security devices. These components focus on data collected from lower layers for analysis, visualization, and monitoring. SCADA devices communicate with one another under various communication protocols, physical media, and security-related properties. The failure of or attacks on such networks can make the data unavailable or allow attackers to inject false data into the system, leading to incorrect system estimations and control decisions that can cause critical damage.

Layer 5 provides a physical and logical separation between water ICS and the enterprise network. It comprises a virtual private network solution that establishes a secure tunnel that allows for unidirectional data flow, such as from the OT to the IT zone.

4.2. WGS threat modeling

In general, threat modeling aims to identify threats and vulnerabilities within IT-related system architectures. Furthermore, it helps implement security and privacy from design into practice. In this study, the Microsoft Threat Modeling Tool is used because it is one of the most commonly used methods in research on threat modeling. It works based on data flow diagrams that describe data stores, processes, and communication lines, and provides information on threats based on the STRIDE model. In the model itself, different trust zones are identified according to layers.

Figure 5 shows the threat model based on the architecture in Figure 4. The threat model system comprises a data flow diagram of the architecture. Modeling the architecture and threats obtained from the risk assessment yielded 154 threats. They were classified according to STRIDE as shown in Table 1.

Table 1. Threat Assignment to Category

Threat	Amount
Spoofing	30
Tampering	15
Repudiation	22
Information Disclosure	2
Denial of Service	46
Elevation of Privilege	39

The threats identified by the model were used to identify the security-related countermeasures and outline the procedures required to avoid them. The threats showed how various attacks might be carried out through the exploitation of particular system vulnerabilities. For the assessment, we relied only on the threats shown in Table 2.

Once the threats had been identified using the STRIDE model, the DREAD risk assessment model was used to classify the risks posed by them, by qualifying, analyzing, and prioritizing them. Using the DREAD model, the threats were ranked in terms of their potential for damage, the reproducibility of the attack, the ease of exploitation by malicious individuals, the affected users, and the way that loopholes in the system may be exploited. A summary of the risk assessment is presented in Table 3.

4.3. Proposing Countermeasures

Once the risk value of each threat is known, mitigation controls can be drawn up to reduce the risk of each. This threat rating can also be used to compile a list of mitigations against threats according to the highest risk-related priorities. Based on the threat rating data in Table 3, mitigation methods can be developed according to the classification of threats. The list of threat assessments can be organized in accordance with the levels of risk so that threats that pose a high risk can be prioritized. Table 4 presents an example of the countermeasures proposed to mitigate the threats described in Tables 2 and 3.

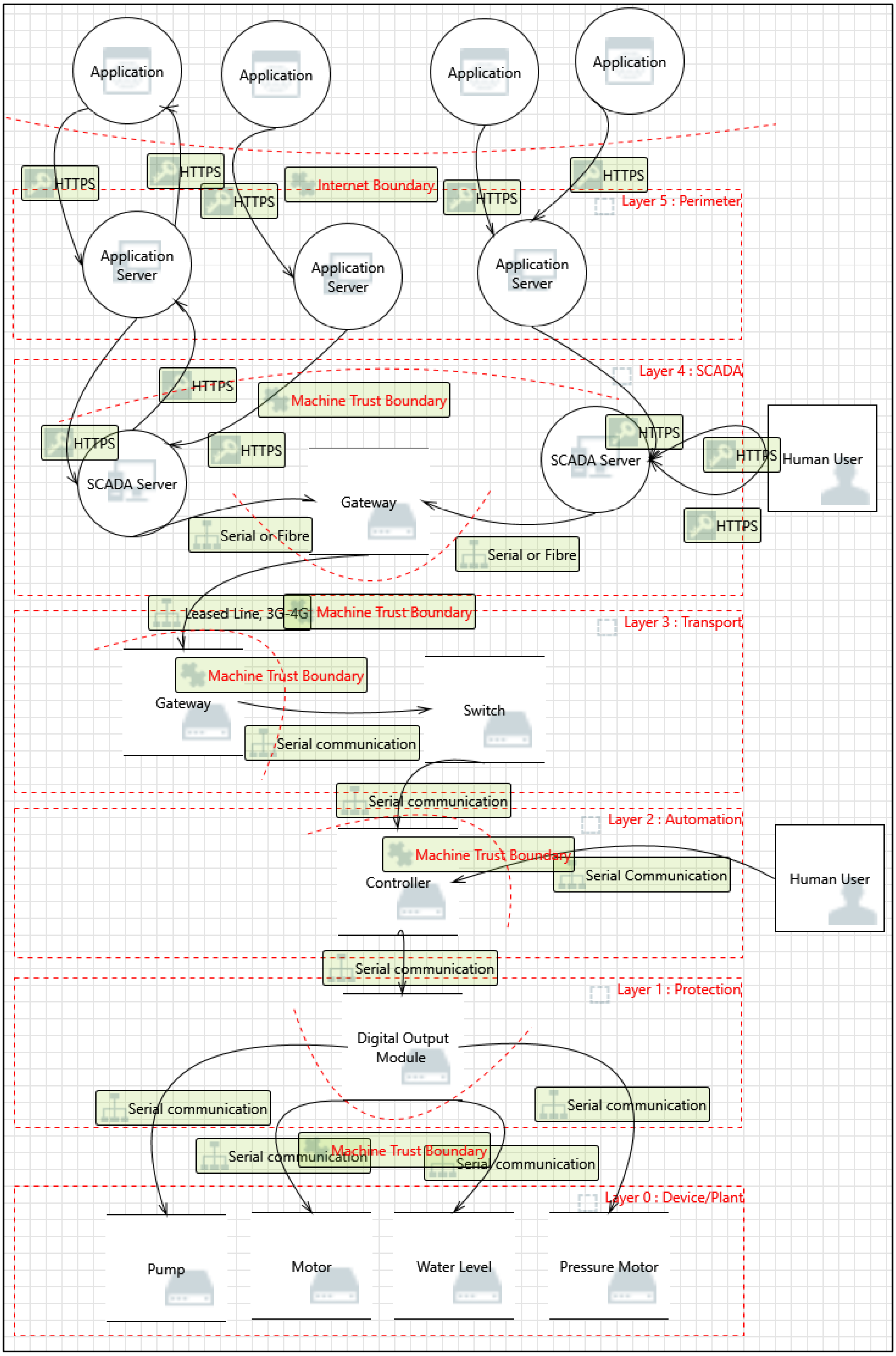

Figure 5. Data flow diagram of water grid system.

Table 2. List of threats

ID	Threats	Category	Description
248	Data Store Inaccessible	Denial of Service	An external agent prevents access to a data store on the other side of the trust boundary.
289	Data Store Denies Gateway Potentially Writing Data	Repudiation	The gateway claims that it did not write data received from an entity on the other side of the trust boundary.
329	Elevation by Changing the Execution Flow in Application Server	Elevation of Privilege	An attacker may pass data into the application server in order to change the flow of program execution within it to the attacker's choosing.
330	Cross-site Request Forgery	Elevation of Privilege	The attack can be carried out in many ways, such as by luring the victim to a site under the control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable website that the victim will visit.
339	Potential Data Repudiation by Application Server	Repudiation	Application server claims that it did not receive data from a source outside the trust boundary.
358	Application Server Process Memory Tampered	Tampering	If the application server is given access to memory, such as shared memory or pointers, or is given the ability to control what the application executes (for example, passing back a function pointer.), then it can tamper with the application.
366	Spoofing the SCADA Server Process	Spoofing	SCADA server may be spoofed by an attacker, and this may lead to unauthorized access to the application server.
367	Cross-site Scripting	Tampering	The web server “Application Server” could be subject to a cross-site scripting attack because it does not sanitize untrusted inputs.
371	Elevation Using Impersonation	Elevation of Privilege	Application server may be able to impersonate the context of the SCADA server to gain additional privilege.
383	Spoofing the Human User External Entity	Spoofing	Human users may be spoofed by an attacker and this may lead to unauthorized access to the SCADA server.
386	Potential Process Crash or Stop for SCADA Server	Denial of Service	SCADA server crashes, halts, stops or runs slowly, in all cases violating an availability metric.
389	SCADA Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of Privilege	Human users may be able to remotely execute code for the SCADA server.
392	Spoofing of Destination Data Store Controller	Spoofing	The controller may be spoofed by an attacker, and this may lead to data being written to the attacker's target instead of the controller.
393	The Controller Data Store Could Be Corrupted	Tampering	Data flowing across serial communication may be tampered with by an attacker. This may lead to corruption of the controller.
398	Data Flow Serial Communication Is Potentially Interrupted	Denial of Service	An external agent interrupts data flowing across a trust boundary in either direction.
407	Weak Credential Transit	Information Disclosure	Credentials on the wire may be sniffed by an attacker. Information may be used to attack other parts of the system, or simply be a disclosure of information leading to compliance violations.

Table 3. Threat Rating using DREAD Model

ID	Threats	Category	D	R	E	A	D	Total	Rating
248	Data Store Inaccessible	Denial of Service	3	1	1	3	1	9	Medium
289	Data Store Denies Gateway Potentially Writing Data	Repudiation	3	2	2	2	2	11	Medium
329	Elevation by Changing the Execution Flow in Application Server	Elevation of Privilege	1	2	2	1	2	8	Medium
330	Cross-site Request Forgery	Elevation of Privilege	3	1	1	3	1	9	Medium
339	Potential Data Repudiation by Application Server	Repudiation	3	2	2	3	2	12	High
358	Application Server Process Memory Tampered	Tampering	2	3	3	3	3	14	High
366	Spoofing the SCADA Server Process	Spoofing	3	2	1	3	2	11	Medium
367	Cross-site Scripting	Tampering	3	2	2	3	2	12	High
371	Elevation Using Impersonation	Elevation of Privilege	1	2	2	1	2	8	Medium
383	Spoofing the Human User External Entity	Spoofing	2	3	3	1	3	12	High
386	Potential Process Crash or Stop for SCADA Server	Denial of Service	3	2	2	3	3	13	High
389	SCADA Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation of Privilege	1	2	2	2	2	9	Medium
392	Spoofing of Destination Data Store Controller	Spoofing	3	2	1	3	2	11	Medium
393	The Controller Data Store Could Be Corrupted	Tampering	3	2	2	3	2	12	High
398	Data Flow Serial Communication Is Potentially Interrupted	Denial of Service	3	2	2	3	3	13	High
407	Weak Credential Transit	Information Disclosure	3	3	2	2	1	11	Medium

Table 4. Example of threat countermeasures

Threat Category	Threats	Countermeasures
Spoofing	Spoofing the SCADA Server Process Spoofing of Destination Data Store Controller Spoofing the Human User External Entity	Authentication

Tampering	Application Server Process Memory Tampered	Application hardening
	Cross-site Scripting	
	Controller Data Store Could Be Corrupted	
Repudiation	Data Store Denies Gateway Potentially Writing Data	Logging
	Potential Data Repudiation by Application Server	
Information Disclosure	Weak Credential Transit	Segregation, encryption
Denial of Service	Data Store Inaccessible	Redundancy
	Potential Process Crash or Stop for SCADA Server	
	Data Flow Serial Communication is Potentially Interrupted	
Elevation of Privilege	Elevation by Changing the Execution Flow in Application Server	Device or application hardening
	Cross-site Request Forgery	
	Elevation Using Impersonation	
	SCADA Server May be Subject to Elevation of Privilege Using Remote Code Execution	

5. Conclusion

Threat modeling on WGSs aims to predict cyberattacks that may occur on the system and provides measures to mitigate such threats. The STRIDE methodology is used to identify and classify threats on the system, and the risk of each threat is then assessed using the DREAD risk rating model. The results of this ranking provide information on three categories of threats that pose a high risk to the monitoring and controlling systems of dams: tampering, denial of service, and repudiation. The main focus of preventive measures as an effort to minimize risks on the WGS is to exercise mitigation controls in these three categories. Further research in threat modeling in a similar environment may combine risk calculations using other risk assessment tools for comparison.

Acknowledgments

This research is supported by the Ministry of Higher Education Malaysia and Universiti Tenaga Nasional (UNITEN), under the Transdisciplinary Research Grant Scheme (TRGS) of Grant No. ‘TRGS/1/2020/UNITEN/01/1/2.’

6. References

[1] Hassanzadeh A, Rasekh A, Galelli S, Aghashahi M, Taormina R, Ostfeld A, et al. A Review of Cybersecurity Incidents in the Water Sector. J Environ Eng. 2020;146:03120003.

[2] Kardon S. Florida Water Treatment Plant Hit With Cyber Attack - Industrial Defender [Internet]. Ind. Def. 2021 [cited 2021 Aug 5]. Available from: https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/

[3] Kerstein B. Israel Thwarts Major Coordinated Cyber-Attack on Its Water Infrastructure Systems | Jewish & Israel News Algemeiner.com [Internet]. The algemeiner. 2020 [cited 2021 Aug 5]. Available from: https://www.algemeiner.com/2020/04/26/israel-thwarts-major-coordinated-cyber-attack-on-its-water-infrastructure-command-and-control-systems/

[4] Gosk S, Winter T, Connor T. Iranian Hackers Claim Cyber Attack on New York Dam. Time [Internet]. 2015; Available from: http://time.com/4160114/iranian-hackers-new-york-dam-cyber-attack/

[5] Marksteiner S, Vallant H, Nahrgang K. Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. J Inf Secur Appl [Internet]. Elsevier Ltd; 2019;49:102389. Available from: https://doi.org/10.1016/j.jisa.2019.102389

[6] Krivokuca S, Stojanovic B, Hofer-Schmitz K, Neskovic N, Neskovic A. Smart water distribution system communication architecture risk analysis using formal methods. 2020 28th Telecommun Forum, TELFOR 2020 - Proc. 2020;

[7] Ismail N. Issues and Problems towards the Sustainable Dam Management System in Malaysia. Int J Innov Manag Technol. 2014;5.

[8] Gupta R, Tanwar S, Tyagi S, Kumar N. Machine Learning Models for Secure Data Analytics: A taxonomy and threat model. Comput Commun [Internet]. Elsevier B.V.; 2020;153:406–40. Available from: https://doi.org/10.1016/j.comcom.2020.02.008

[9] Srinivas Panguluri , William Phillips JC. Protecting water and wastewater infrastructure from cyber attacks. Front Earth Sci. 2011;5:406–13.

[10] Clark RM, Hakim S, Panguluri S. Protecting water and wastewater utilities from cyber-physical threats. Water Environ J. 2018;32:384–91.

[11] Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A. Guide to Industrial Control Systems (ICS) Security [Internet]. NIST Spec. Publ. 800-82 rev 2. 2015. Available from: http://industryconsulting.org/pdfFiles/NIST Draft-SP800-82.pdf

[12] Germano JH. Cybersecurity Risk & Responsibility in the Water Sector. 2019;6–19. Available from: https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013

[13] Honea M, Yamamoto Y, Laux J, Guiliano C, Hart M. Silent Cyber Scenario: Opening the Flood Gates. 2018.

[14] Schoolmeesters R. Site security is a critical aspect of dam safety that shouldn' t be overlooked or disregarded. Lesson Learn. 2018.

[15] U.S. Department of Homeland Security. Dams Sector Cybersecurity Program Guidance. 2016.

[16] Alhassan JK, Abba E, Olaniyi OM, Waziri VO. Threat Modeling of Electronic Health Systems and Mitigating Countermeasures. Int Conf Inf Commun Technol Its Appl (ICTA 2016). 2016.

[17] Meier JD, Mackman A, Dunner M, Vasireddy S, Escamilla R, Murukan A. Improving web application security: Threats and countermeasures [Internet]. Microsoft. 2003. Available from: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

[18] Omotosho A, Ayemlo Haruna B, Mikail Olaniyi O. Threat modeling of Internet of Things health devices. J Appl Secur Res [Internet]. Routledge; 2019;14:106–21. Available from: 10.1080/19361610.2019.1545278

[19] De Faveri C, Moreira A. Designing Adaptive Deception Strategies. Proc - 2016 IEEE Int Conf Softw Qual Reliab Secur QRS-C 2016. 2016;77–84.

[20] Kaur N, Kaur P. Mitigation of SQL Injection Attacks using Threat Modeling. ACM SIGSOFT Softw Eng Notes. 2014;39:1–6.