Received: March 26, 2025. Revised: April 26, 2025.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Classified Unauthorized Attack Detection & Protection for Secured Experimental Water Distribution Incorporated Industrial Automation Tools

Venkateswarlu G[1,2]* **Santosh R Desai[3]**

[1]*Department of Electrical and Electronics Engineering, B.M.S. College of Engineering-Research Center, Visvesvaraya Technological University, Belagavi 590018, Karnataka, India*
[2]*Department of Electronics and Instrumentation Engineering, CVR College of Engineering, Hyderabad, 501510 Telangana India*
[3]*Department of Electronics and Instrumentation Engineering, B.M.S. College of Engineering, Visvesvaraya Technological University, Belagavi 590018, Karnataka, India*
* Corresponding author's Email: venkigummadilli@gmail.com

Abstract: The proposed work addresses various challenges for securing water distribution from physical and cyber physical attacks. This work is implemented in the experimental test bed of an automation environment for water distribution. The Programmable Logic Controller (PLC) enables the water supply actuators (Solenoid Valves & Pumps) to distribute water at prescheduled times automatically. However, these actuators are susceptible to attacks, as unauthorized power supply sources can cause the actuators to malfunction during unscheduled & scheduled timings. Most current research endeavours focus on identifying attacks during only the scheduling phase. In this paper, the developed algorithm identifies the attacks for different scenarios that occur mainly in the unscheduled phase (absence of controller actions to the actuators), detect the attack's density level and notify the attacks through the Graphic Operation Terminal (GOT). Furthermore, to secure water distribution from cyber physical attacks this paper successfully introduced multidimensional security measures such as IP security for PLC from cyber physical attack, security for unauthorized read/write operations from/to the water distribution controller, block security for programming files of the controller, a remote security from illegal access through engineering tool and other security. The proposed system demonstrated a high detection rate of 96.875% in the One-Proportion Z-Test. The test yielded an extremely small p-value (5.69×10^{-8}) and a standard error of proportion of 0.08839, providing strong statistical evidence to reject the null hypothesis. The analysis of false positive and false negative rates in attack detection revealed an overall accuracy of 97.37% and a precision of 96.88%, indicating the system's effectiveness and reliability in identifying cyber-physical attacks within the water distribution network.

Keywords: Automation, Attacks, Cyber physical attack, Graphic operation terminal **(**GOT**)**, Programmable logic controller **(**PLC**)**, Security, Water distribution.

1. Introduction

Critical infrastructures like oil/gas industries, nuclear plants, and Water Distribution Systems (WDS) are primarily administered using digital automation systems. These systems consist of diverse components, including PLC, Supervisory Control and Data Acquisition (SCADA)/GOT, networking devices, sensors, and actuators [1, 2]. Control operations for WDS can be managed from centralized digital systems like SCADA or GOT. It is foremost to propose solutions to enhance security in the WDS and uphold against cyber physical attacks on PLC, filed elements and security threats [3]. Several key innovations, such as correlation attack detection, significantly enhance the performance and applicability of industrial automation systems [4].

Advancements in technology and computing capabilities have enabled control equipment-PLC to incorporate network features with inadequate or poor security measures [5]. A method was proposed for detecting and mitigating attacks that target the input

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

memory of PLC [6]. Maroochy Water Services in Queensland, Australia, faced one of the pioneering occurrences of a cyber-physical attack within the water supply sector in 2000. In this event, a disgruntled contractor aimed explicitly at the SCADA system led to the discharge of a substantial volume of wastewater into waterways and parks [7].

In 2011, another recorded cyber-attack took place where the perpetrators successfully remotely turned off a water pump belonging to a utility in Central Illinois [8]. The water distribution and purification industry has been the target of several aggressive cyber- security attacks, some of which have been detected, revealed, & documented [9]. A classifier technique was introduced to identify cyber-physical attacks at water distribution system by leveraging the distinction between normal & abnormal conditions in sensor datasets, and from the perspective of potential attackers, the task involves utilizing TCP/IP packets, deciphering the parameters & values exchanged in the communication among control devices [10]. Researchers have increasingly focused on the cybersecurity challenges within water systems. However, compared to other fields, the exploration of cyber-attacks on water distribution systems remains relatively underexplored, with only a limited number of studies addressing this issue [11-13]. Discrepancies between SCADA readings and simulated model (EPANET model) values were categorized as representing normal or abnormal states of the system. This model-based approach was recognized as the top-performing solution in the Battle of the Attack Detection Algorithms competition [14].

Trapped air in pipelines can lead to various adverse effects, such as pressure surges, reduced flow, or complete blockage [15,16]. This phenomenon has been a research subject for many decades, with several comprehensive reviews available [17]. Air can be removed by using air valves or through hydraulic methods, which involve analysing the line's configuration and predicting the flow conditions necessary for the effective removal of entrapped air [18]. The minimum critical velocity is required to clear air pockets from large-diameter pipes; similar research for smaller diameters is currently lacking [19]. The basic theft identification idea states that the two sensors' flow rate readings may be identical If no leak is discovered [20]. The capabilities of PLCs enable the establishment of a fully automated water distribution system. According to Global Market Insights recent research report, the global market for PLC was valued at approximately 11.7 billion U.S. dollars in 2024, as depicted in Fig. 1. Projections indicate compound annual growth rate

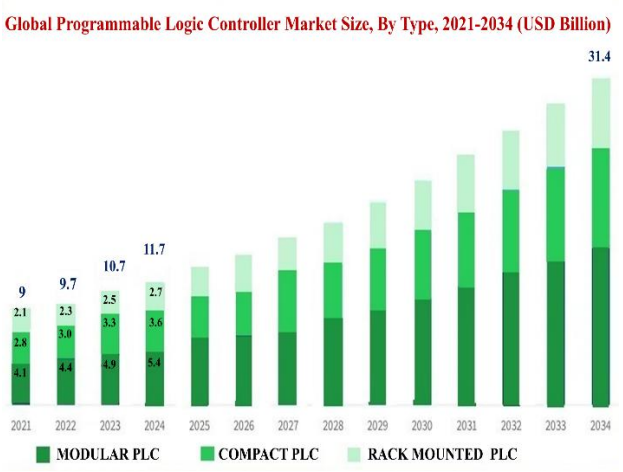

Figure. 1 Worldwide market of the PLC.

exceeding highest percent, with the market anticipated to surpass 31.4 billion U.S. dollars by 2034 [21].

An unsupervised SCADA data-driven method was applied to detect integrity attacks on a simulated WDS. It identified consistent and inconsistent states of SCADA systems [22]. An intelligent identification method was proved in the field, representing its capability to precisely identify and localize pipeline leakages [23]. Identified failures in cyber-physical water distribution system networks using machine learning models for C-Town water distribution under cyber-attacks, pipe leaks/bursts, and physical attacks [24]. The attack was discerned by monitoring alterations in sensor dynamic outcomes related to input and output memory attacks.

These attacks were detected while the PLC was actively engaged in control operations [25]. Manipulating the water level in the PLC and random noise injection can be detected by general-purpose method-Dynamic Watermarking, where the attacks were experimentally verified and validated with the numerous cyber-attack scenarios on a water tank level automation system controlled by PLC [31].

In this proposed work, an experimental testbed replicating a clean water supply system was constructed using technologies presently employed in industry to explore the concepts experimentally. Mitsubishi FX5U PLC and GS series GOT were effectively utilized for the test bed development of an automation system for water distribution. Four pivotal elements of smart WDS include PLC, Solenoid Valves, Sensors, and SCADA/GOT. There will be a massive scope for attacking the PLC and Solenoid Valve to perform unauthorized manipulations of the water distribution process. Attacks on water distribution can manifest in two distinct methods. Firstly, external power is supplied

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

to the solenoid valves through unauthorized individuals replicating controller outputs. The second avenue involves illegal access to the PLC, allowing for the manipulation of programming, control actions, and numeric values.

This paper alternatively formulates an algorithm to identify attacks involving external power provision to Solenoid Valves and pumps when the PLC control actions are disabled. Furthermore, it visually presents comprehensive details of the cyber-physical attacks on the WDS and introduces multiple security authentication techniques to protect the PLC from illegal access. As discussed in the literature, some algorithms could identify attacks during the scheduled water distribution process controlled by the PLC. The algorithm proposed in this paper is designed to detect classified attacks under various conditions mainly during the non-scheduled operational periods of water distribution supervised by the PLC. This proposed work also introduced a novel technique to detect attack density.

Implementing more security measures for PLC algorithms, remote access, IP address access, and additional access to PLC is mandatory to safeguard the water distribution system from cyber-attacks. These initiatives establish fundamental security for the cyber-physical water distribution system. The proposed work implements several fundamental security measures to protect the cyber-physical system responsible for water distribution against unauthorized access This paper is structured as follows: a brief background of water management, attack detection problems, alternatives, and challenges are presented in Section 1. Section 2 provides details of experimental endeavours & the design of the emulated testbed for the water distribution model, focusing on integrating household sensors and actuators with PLC & GOT. In Section 3, the classified attack detection techniques/methods are discussed. Section 4 introduces security functions for WDS. Section 5 presents the results obtained from the experiments that were conducted. Finally, Section 6 offers the paper's conclusion followed by references.

2. Experimental endeavour and testbed to emulate the real water distribution model

The experimental endeavours outlined in this proposed system are designed to address various challenges in the water distribution system. A review of existing research on the detection of physical and cyber-physical attacks in water distribution systems revealed a common limitation: most approaches detect attacks only during the scheduled phase of water distribution, when water is actively being supplied to end users.

However, in automated water distribution system, such methods are limited to identifying anomalies only during active water supply periods. In scenarios where water is being automatically scheduled to one station but not scheduled to another (both stations under the control of a central/main station), attackers can exploit this gap. Specifically, they can illegally supply voltage (e.g., 230V AC or 24V DC) directly to the solenoid valve—bypassing the PLC controller—causing the valve to open and enabling unauthorized water extraction.

Moreover, attackers can even activate the main/sub pipeline solenoid valve through illegally supply voltage during non-scheduled times, allowing water theft from multiple points without detection. The proposed work is specifically designed to detect and address such unauthorized manipulations, including those occurring outside scheduled supply phases, thereby enhancing the security and integrity of automated water distribution systems.

In addition to the discussions above, it was observed that many existing research efforts have focused on implementing encryption techniques to protect PLC memory and controller programming files from cyber-physical attacks in water distribution systems. Building upon these foundations, the proposed work enhances the security of the PLC to further strengthen the automation system against various threats. The following multi-layered security mechanisms have been incorporated into the proposed WDS system:

a. IP Filter Security: Access to the PLC is restricted through IP filtering, allowing only predefined IP addresses. This ensures that attackers cannot access the PLC without knowledge of the exact permitted IP address.

b. Block Password Protection: Even if an attacker discovers the correct IP address, a block password is required to access the programming interface. Without this password, the attacker cannot open or modify the PLC program.

c. Read/Write Operation Security: In the event that an attacker bypasses the block password, additional security measures prevent unauthorized read/write operations, safeguarding the PLC’s logic and data from manipulation.

d. Communication Port Security: To protect against unauthorized remote access through SLMP (Seamless Message Protocol) or FTP (File Transfer Protocol), remote access controls are implemented. These prevent external devices from communicating with the PLC via unsecured ports.

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

e. Extended Security for GOT and IoT Devices: Similar security mechanisms have been applied to GOT and IoT devices associated with the automation system, ensuring comprehensive protection across all connected components.

The identified Research Questions (RQ) seek answers by implementing the proposed automation techniques. RQ1: Is it possible to detect classified attacks & protect the WDS from unauthorized attacks during the absence of PLC control actions? RQ2: Is it possible to provide security to the WDS programming files? RQ3: Is it possible to develop IP address security and give access to only the designated devices to communicate with the WDS controller? RQ4: is it possible to identify the density of the attack? This work introduces various techniques to fulfil the requirements outlined in the research questions. An experimental test bed was established for water distribution, comprising eight houses divided into two substations (Fig. 2).

The WDS is consistently integrated with PLC, GOT, and web-enabled devices. To implement a fully automation system for the proposed water distribution model, point-type High-Level Sensor (HLS), Medium-Level Sensor (MLS), Low-Level Sensor (LLS), and ultrasonic water level sensors are incorporated into the overhead tank (shown in Fig. 2). Each house is equipped with a flow sensor and a solenoid valve (Fig. 2), labeled as follows:

Flow Sensors: FS-S1H1 (Flow Sensor for Substation 1, House 1), FS-S1H2 (Flow Sensor for Substation 1, House 2), and so on.

Solenoid Valves: SV-S1H1 (Solenoid Valve for Substation 1, House 1), SV-S1H2 (Solenoid Valve for Substation 1, House 2), and so forth.; in addition to that, solenoid valves are strategically positioned along the main pipeline, Substation-1 pipeline, and Substation-2 pipeline. All these sensors and solenoid valves are seamlessly integrated with the FX 5U PLC through appropriate signal conditioning circuits (5V-24V Switching circuit) and relay circuits, as illustrated in Fig.3. Ethernet communication between the PLC and GOT module is established in this work to maximize data transmission speed. The PLC communicates with a Hub switch router to enable remote web-based supervisory functions for establishing connectivity. The features of the FX5U PLC facilitate wireless connectivity between the controller of WDS and IoT devices. Monitoring and control operations can be executed from IoT devices (web Function) (refer to Fig. 3).

The PLC's web functions offer historical data regarding unauthorized access and incorrect authentications [29]. Users can remotely inspect the PLC's present values or error status without specialized engineering tools. The extensive abilities of the FX5U model PLC enable the connection of a significantly larger number of sensors and actuators. The classified attack detection can be visually exhibited on the GOT using graphical operations (shown in Fig. 4)., specifically the GS series model GOT -Mitsubishi. The water flow sensor output is a 5V peak pulse. However, the opto-isolator terminals

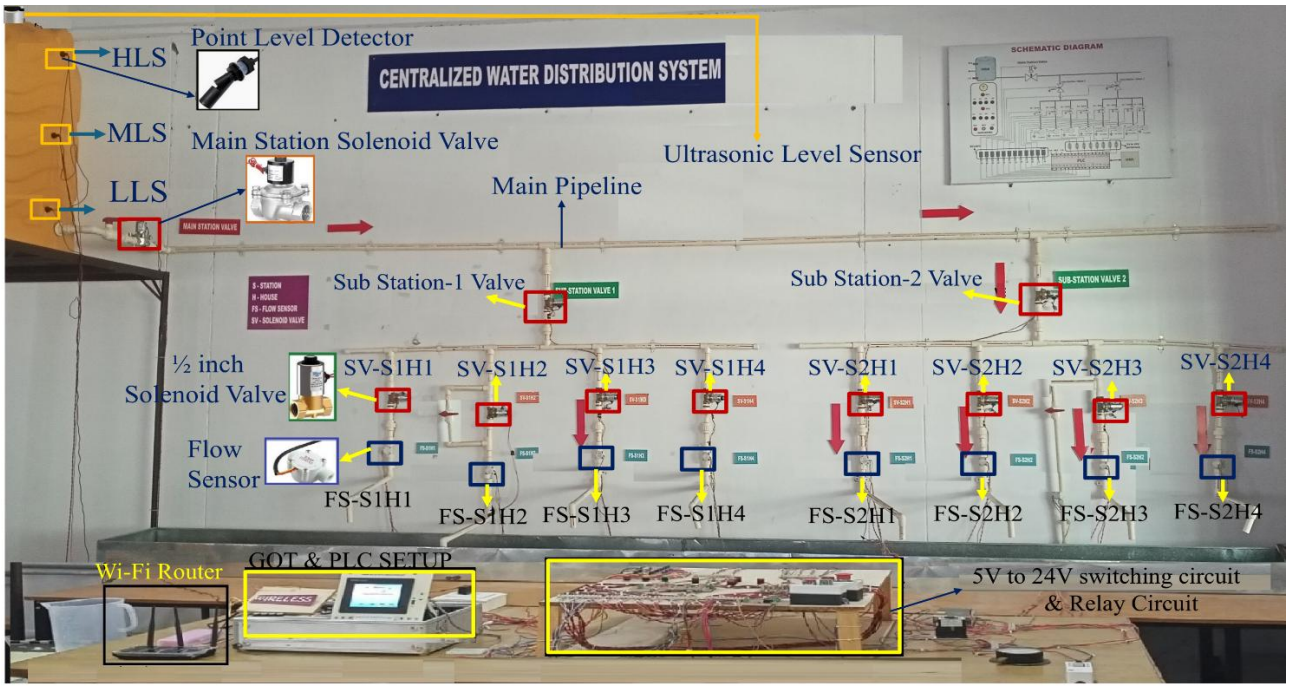

Figure. 2 Experimental model of the proposed water distribution system

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

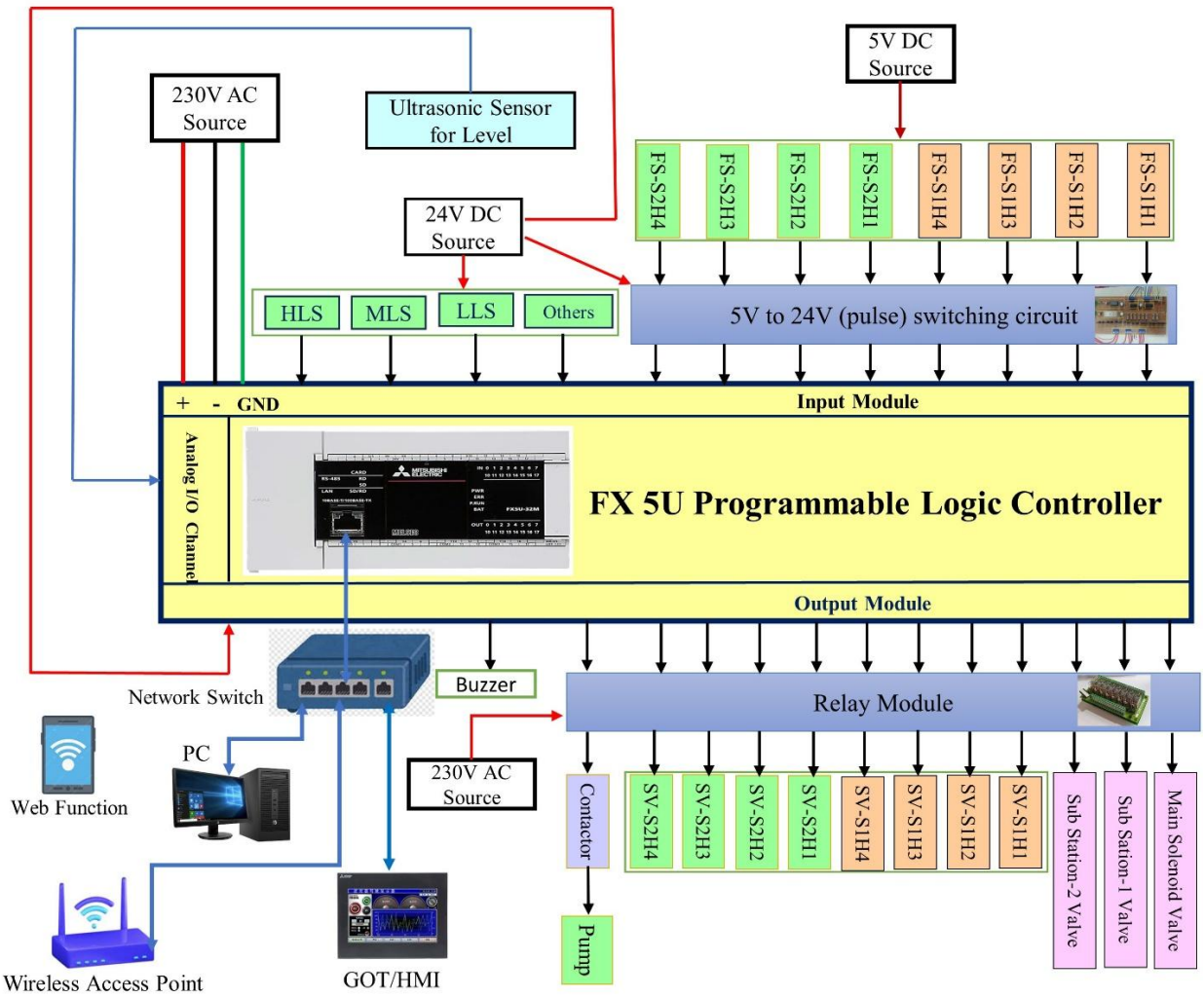

Figure. 3 Block representation of the proposed water distribution model

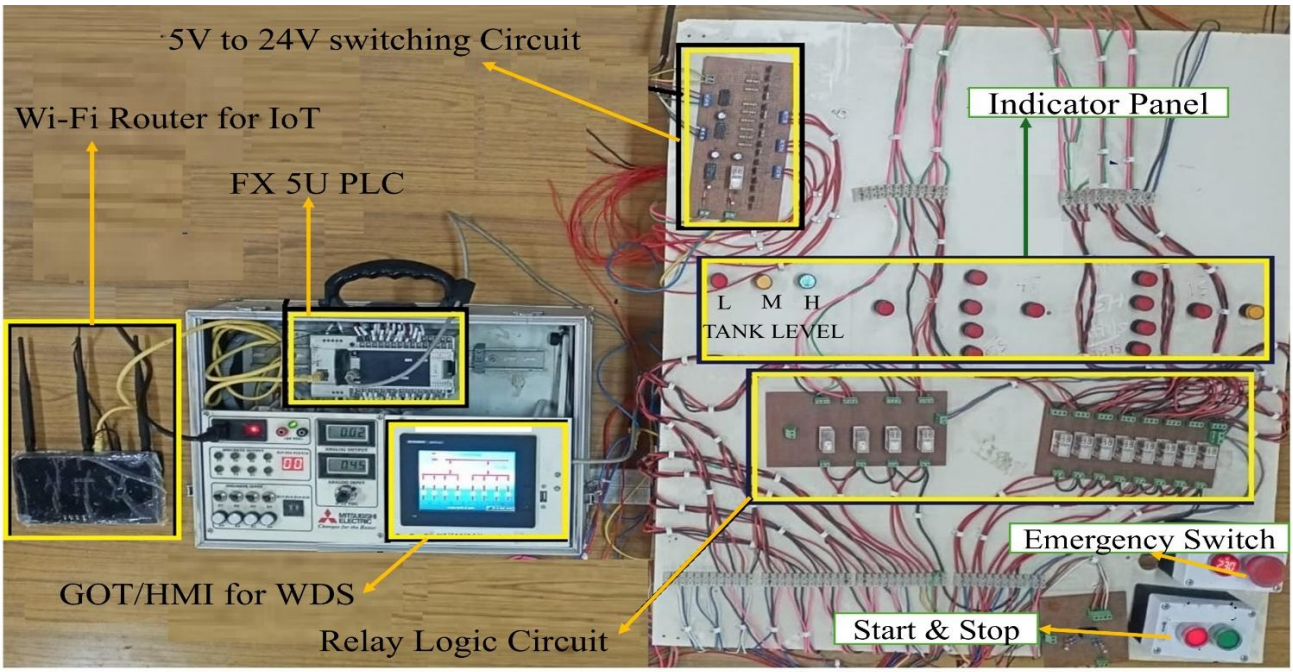

Figure. 4 Control panel-incorporated PLC, GOT, switching circuit & relay circuit

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

of the input module of the PLC operate at a specified voltage of 24V. A switching circuit (signal conditioning circuit) was integrated to achieve a smooth transition from 5V to 24V (Fig. 4).

All the solenoid valves operate at 230V AC. To integrate them with the PLC, a driver circuit-relay module (Fig. 4) is used, as the PLC outputs can directly handle voltages only up to 24V. An indicator panel was developed to know the status of sensors and actuators by the field operators.

The capabilities of the FX5U PLC empower the development of an automation system for water distribution with user-friendly programming [26]. The GX Works3 PLC programming software introduces numerous new features and technologies to ensure a seamless engineering environment solution, easy troubleshooting, advanced error diagnosis, and graphics-based system configuration [27]. GT Designer 3, a robust engineering software, is utilized to craft professional graphical screen designs for GOT. It offers enhanced features, including reduced screen creation time, automatic scaling with changes in GOT type, increased flexibility, the ability to create custom libraries with self-configured objects, comprehensive security settings, and advanced simulation capabilities [28].

In the communication scenario for I/O field elements- sensors and switches are interlinked with the input module of the PLC in the sourcing mode [30]. Three-point type water level horizontal floating sensors (HLS, MLS, and LLS) are linked from the overhead tank to the PLC (connected to X11, X12, and X13 terminals, respectively), as depicted in Fig. 5. An ultrasonic water level sensor is also connected to diagnose water availability in the overhead tank. The Master start and stop buttons are linked to X14 and X15 terminals. The water supply pump to the overhead tank is related to the PLC's Y0 terminal. The input and output terminals of the PLC incorporate an opto-isolator circuit, safeguarding the PLC CPU from malfunctions or power fluctuations [26].

The flow sensor resulted in 450 pulses per Liter. FX 5U PLC input terminals (X0-X7) operate at high speed of response as response time is 10micro sec. The eight Flow Sensors (FS-S1H1, FS-S1H2, FS-S1H3, FS-S1H4, FS-S2H1, FS-S2H2, FS- S2H3, and FS-S2H4) under two substation houses are integrated to X0, X1, X2, X3, X4, X5, X6, X7 terminals respectively (illustrated in Fig. 5). The long counter function is initiated in the PLC programming to quantify pulses, providing a measurement for the supplied water to the end users. The proposed WDS incorporates 11 Diaphragm type Solenoid Valves (USD type, Brass) into the pipeline system. It includes one solenoid valve for the Main pipeline, two for Substations, and eight for houses, as shown in Fig. 5. All solenoid valves operate at 230V AC voltage.

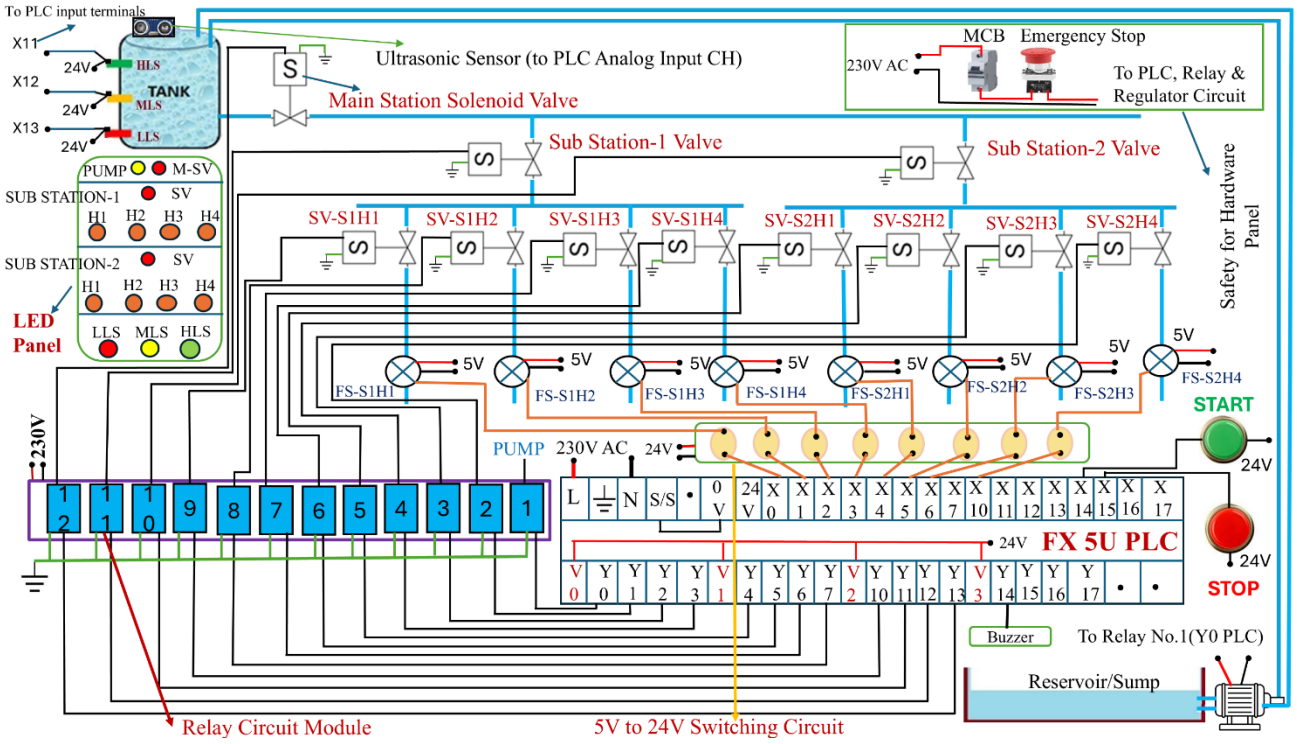

Figure. 5 Schematic representation of I/O filed elements communication with PLC

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

The eleven solenoid valves (Main station-SV, Substation-1 SV, Substation-2 SV, SV-S1H1, SV-S1H2, SV-S1H3, SV-S1H4, SV-S2H1, SV-S2H2, SV-S2H3 & SV-S2H4) are linked to the Y13, Y12, Y11, Y10, Y7, Y6, Y5, Y4, Y3, Y2, Y1 terminals of the controller, respectively (Fig.5). The output terminals of the controller are connected to the solenoid valves through the driver circuit (Relay module). The addresses of the input and output terminals and their respective connected devices are detailed in Table 1.

In the process of clean water distribution, the proposed research involved the development of an experimental test bed as discussed above for water distribution to end users that emulates real-world scenarios in villages or cities. The attack identification results for the proposed work are derived from experiments conducted on a physical testbed built with modern industrial control equipment. The outcomes of our study align with the classified attack detection through diverse case studies.

3. Method- Classified attack detection technique

This section outlines the technique for detection of water theft attacks concerning unauthorized access to actuators in the absence of PLC control actions. A method of Boolean Algebraic equations (Eqs. (1)-(19)) was developed to detect the classified attack and density of attack. Utilizing the built-in real-time clock in the PLC CPU module, along with special registers and instructions, we could preschedule water supply for end-users in the coming days, months, and years. This clock functionality allowed us to preschedule water supplies well into 2079 year. Water delivery to end-users occurs automatically according to predetermined schedules in this envisioned automation system.

The PLC remains inactive during non-scheduled times, abstaining from any control actions. The algorithm is implemented to identify attacks initiated at the actuators by external power supply sources during periods of not scheduling of water supply, and the detection of attacks is visually presented through a user alarm in the GOT. All actuators operate with a 230V AC signal. An attacker can steal water by externally sourcing a 230V AC signal, regardless of PLC control commands. In such instances, the proposed algorithm utilizes the (Eqs. (1)-(19)) for attack detection. The detection of attacks at various locations and under different scenarios is reflected in the status of PLC memory bits, specifically M10, M11, M12, M13, M14, M15, M16, M17, M18, and M40 to M50, as outlined in Table. 2.

In this proposed study, attacks are generated & detected in two distinct scenarios. Case-1: Attacks are initiated solely on the solenoid valve. Case -2: Attacks are initiated on both solenoid valve & pump.

3.1 Case-1: Attacks are initiated solely on solenoid valves

3.1.1. Attack identification at the main pipeline

The memory bit M10 (Eq. (1)) indicates the attack identified at the main pipeline. If the PLC control operation (M23) is disabled (i.e., water distribution is not scheduled), the PLC turns OFF the main solenoid valve (Y13) and the attack at main solenoid valve is created by supplying the external power supply by the attacker to bypass the PLC control signal. However, if any of the following conditions is TRUE (The impact of the attack is

Table 1. PLC I/O Terminal addresses mapping & respective connected filed devices

S. No	Input address mapping		Output address mapping	
	Name of the device	Connected terminal	Name of the device	Connected terminal
1	FS-S1H1	X0	Pump	Y0
2	FS-S1H2	X1	SV-S2H4	Y1
3	FS-S1H3	X2	SV-S2H3	Y2
4	FS-S1H4	X3	SV-S2H2	Y3
5	FS-S2H1	X4	SV-S2H1	Y4
6	FS-S2H2	X5	SV-S1H4	Y5
7	FS-S2H3	X6	SV-S1H3	Y6
8	FS-S2H4	X7	SV-S1H2	Y7
9	Pump Actuation Detector	X10	SV-S1H1	Y10
10	HLS	X11	Substation-2 SV	Y11
11	MLS	X12	Substation-1 SV	Y12
12	LLS	X13	Main station-SV	Y13
13	Master start	X14	Buzzer	Y14
14	Master stop	X15	Ultrasonic Sensor	Analog-Input CH1

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

Table 2. PLC Memory bits and their description

S. No	Memory Bit	Description	Memory Bit	Description
1	M10	Attack Identification at the main pipeline	M29	Water flow identification at S2H2
2	M11	Attack Identification at S1H1	M30	Water flow identification at S2H3
3	M12	Attack Identification at S1H2	M31	Water flow identification at S2H4
4	M13	Attack Identification at S1H3	M32	Falling Edge of tank level-Ultrasonic sensor
5	M14	Attack Identification at S1H4	M33	Positive Edge of HLS O/P
6	M15	Attack Identification at S2H1	M34	Positive Edge of MLS O/P
7	M16	Attack Identification at S2H2	M35	Positive Edge of LLS O/P
8	M17	Attack Identification at S2H3	M36	Rising Edge of tank level-Ultrasonic sensor
9	M18	Attack Identification at S2H4	M40	Attack Identification at S1H1, including pump
10	M20	Negative Edge of HLS O/P	M41	Attack Identification at S1H2, including pump
11	M21	Negative Edge of MLS O/P	M42	Attack Identification at S1H3, including pump
12	M22	Negative Edge of LLS O/P	M43	Attack Identification at S1H4, including pump
13	M23	PLC control operations enable/ disable	M44	Attack Identification at S2H1, including pump
14	M24	Water flow identification at S1H1	M45	Attack Identification at S2H2, including pump
15	M25	Water flow identification at S1H2	M46	Attack Identification at S2H3, including pump
16	M26	Water flow identification at S1H3	M47	Attack Identification at S2H4, including pump
17	M27	Water flow identification at S1H4	M49	Attack detection at the pump
18	M28	Water flow identification at S2H1	M50	Attack density level (High/Low)

observed through manipulations in the water level of the overhead tank):

- Negative edge of the tank Low-Level sensor (M22) or Medium-Level sensor (M21), or High-Level sensor (M20).
- Falling edge (M32) of the tank water level based on the ultrasonic sensor.

Then, the memory bit M10 (Eq. (1)) will be set to "1," indicating a potential physical attack detected in the main pipeline of the WDS.

$$\mathrm{M10} = \overline{Y13}\,(\mathrm{M20} + \mathrm{M21} + \mathrm{M22} + M32)\,\overline{M23} \quad (1)$$

The classifier technique was employed to detect attacks in sensor datasets under normal and abnormal conditions, specifically during the presence of PLC operations control of water distribution [10]. However, in the proposed work, Case-1 and Case-2 studies implemented an algorithm to identify classified attacks, specifically the unauthorized access of actuators in the absence of PLC control operations.

3.1.2. Attack identification at substation-1 end users

Memory bits M11, M12, M13, and M14 (Eqs. (2)- (5) respectively) signify the detection of attacks at substation-1 corresponding to the four houses (S1H1, S1H2, S1H3, S1H4). If the Substation-1 valve is OFF (Y12 = 0), but flow is detected at any of the houses under station-1 (M24 = 1 / M25 = 1 / M26 = 1 / M27 = 1) corresponding to S1H1, S1H2, S1H3, and S1H4, and the following conditions are met:

- PLC control operations are disabled (M23 = 0)
- A primary attack is identified at the main pipeline (M10 = 1)
- Individual end-user solenoid valves are OFF (Y10 = 0, Y7=0, Y6=0, & Y5 = 0) as controlled by the PLC.

Then, memory bits M11, M12, M13, and M14 (Eqs. (2) - (5) respectively) will be set to "1," indicating an attack at the respective houses in Substation-1. This mechanism detects attacks at S1H1, S1H2, S1H3, and S1H4 in the absence of PLC control action for individual houses. Additionally, it can identify attacks at individual houses even when PLC control actions are ON for the main valve and Substation-1 valve.

$$M11 = M24.\overline{Y10}.\overline{Y12}.\ M10 + M24\,.\overline{Y10}\,.M23 \quad (2)$$

$$M12 = M25.\overline{Y7}.\overline{Y12}.\ M10 + M25\,.\overline{Y7}\,.M23 \quad (3)$$

$$M13 = M26.\overline{Y6}.\overline{Y12}.\ M10 + M26\,.\overline{Y6}\,.M23 \quad (4)$$

$$M14 = M27.\overline{Y5}.\overline{Y12}.\ M10 + M27\,.\overline{Y5}\,.M23 \quad (5)$$

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

3.1.3. Attack identification at substation-2 end users

Memory bits M15, M16, M17, and M18 (Eqs. (6)- (9) respectively) signify the detection of attacks at station 2 corresponding to the four houses (S2H1, S2H2, S2H3, S2H4). If the Substation-2 valve is OFF (Y11 = 0), but flow is detected at any of the houses under station-1 (M28 = 1 / M29 = 1 / M30 = 1 / M31 = 1) corresponding to S2H1, S2H2, S2H3, and S2H4, and the following conditions are met:

- PLC control operations are disabled (M23 = 0)
- A primary attack is identified at the main pipeline (M10 = 1)
- Individual end-user solenoid valves are OFF (Y4 = 0, Y3=0, Y2=0, & Y1 = 0) as controlled by the PLC

Then, memory bits M15, M16, M17, and M18 (Eqs. (6)- (9) respectively) will be set to "1," indicating an attack at the respective houses in Substation-2. The proposed Boolean equations identify the attack at S2H1, S2H2, S2H3, & S2H4 with the absence of PLC control action for individual houses and also the presence of PLC control action for main valve and substation-2 valve

$$M15 = M28.\overline{Y4}.\overline{Y11}.\ M10 + M28\ .\overline{Y4}\ .M23 \quad (6)$$

$$M16 = M29.\overline{Y3}.\overline{Y11}.\ M10 + M29\ .\overline{Y3}\ .M23 \quad (7)$$

$$M17 = M30.\overline{Y2}.\overline{Y11}.\ M10 + M30\ .\overline{Y2}\ .M23 \quad (8)$$

$$M18 = M31.\overline{Y1}.\overline{Y11}.\ M10 + M31\ .\overline{Y1}\ .M23 \quad (9)$$

3.2 Case-2: Attacks are initiated on both solenoid valves and the pump

The unauthorized external power supply creates attacks at both the pump and the solenoid valves. The ensuing equations lead to identifying these attacks across different end-users, occurring when the attacks occur at the pump, main station, substations, and individual houses. In contrast to other domains, investigating attacks on water distribution systems is relatively unexplored, with only a limited number of studies dedicated to addressing this issue [11-13]. The proposed research sought to identify attacks across various dimensions, including those targeting pumps, main pipelines, and individual houses, and assess the density levels of such attacks. This study yields satisfactory outcomes across many dimensions of attacks.

3.2.1. Identification of density of attack and attack on pump

When the outflow from the overhead tank exceeds the inflow, it indicates a higher attack density, particularly in the absence of PLC-controlled pump operations. The provided equations ((Eqs. (10)- (11) respectively) represent the attack density level and the corresponding detection of attacks on the pump, respectively. If the PLC control operation is disabled (i.e., during the non-scheduling phase, where M23 = 0), the control signal to the pump is also disabled (Y0 = 0). However, if an attacker supplies external power to the pump, bypassing the PLC, the system detects unauthorized pump actuation through a high signal on X10 = 1. As a result, the pump begins to fill the overhead tank, leading to water theft. If the rate of water theft (outflow) from the overhead tank exceeds the rate of inflow, the water level begins to drop abnormally. This triggers the negative edge detection on multiple water level sensors—High (M20), Medium (M21), Low (M22)—as well as the ultrasonic sensor (M32). When all these indicators are simultaneously activated, the system identifies that the intensity of the attack is high (M50=1).

Attack detection on pump encompassing the Positive edge of tank water level sensor High (M33), Medium (M34), Low (M35) & ultrasonic sensor (M36), PLC control operations enable or disable (M23), Pump-PLC O/P terminal address (Y0), and attack density level (M50). If M49 is in a logic state of "1," it signifies the attack detection on the pump. If M50 is in a logic state of "1," it represents a higher density of attack detection. The novelty of this proposed work lies in its ability to identify the density level of attacks. The proposed algorithm determines the density level of attacks without supporting additional sensors.

$$M50 = X10.\overline{Y0}\,(M20\ +\ M21 + M22 + M32)\,\overline{M23} \quad (10)$$

$$M49 = \overline{Y0}\,(M33\ + M34\ +\ M35 +\ M36)\,\overline{M23} + M50 \quad (11)$$

3.2.2. Attack identification with substation-1 end users along with the pump

Memory bits M40, M41, M42, and M43 ((Eqs. (12)- (15) respectively) signify the detection of attacks at station 1, along with pump corresponding to the four houses (S1H1, S1H2, S1H3, & S1H4). These memory bits are triggered by the following

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

multiple conditions, Where the attacks are created by supplying unauthorized external voltage to the solenoid valves and pump.

- The Substation-1 valve is OFF (Y12 = 0) by the PLC-Control
- Flow is detected at any of the houses (M24 = 1 / M25 = 1 / M26 = 1 / M27 = 1)
- An attack is identified at the main pipeline (M10 = 1)
- An attack is identified at the pump (M49 = 1)
- Individual end-user solenoid valves are OFF (Y10 = 0, Y7 = 0, Y6 = 0, Y5 = 0) by the PLC control.

When these conditions are met, memory bits M40, M41, M42, and M43 will be set to "1," indicating an attack at the respective houses in Station 1.

$$M40 = M24.\overline{Y10}.\overline{Y12}.\ M10.\ M49 \quad (12)$$

$$M41 = M25.\overline{Y7}.\overline{Y12}.\ M10.\ M49 \quad (13)$$

$$M42 = M26.\overline{Y6}.\overline{Y12}.\ M10.\ M49 \quad (14)$$

$$M43 = M27.\overline{Y5}.\overline{Y12}.\ M10.\ M49 \quad (15)$$

3.2.3. Attack identification with Substation-2 end users along with the pump

Memory bits M44, M45, M46, and M47 signify the recognition of attacks at station 2, along with pump corresponding to the four houses (S2H1, S2H2, S2H3, & S2H4). These memory bits are a result of various factors, substation-2 valve ON/OFF (Y11), flow Identification (M28, M29, M30, & M31) at S2H1, S2H2, S2H3, & S2H4 respectively, attack detection at main pipeline (M10), & Pump (M49), and Individual end user's solenoid valve ON/OFF (Y4, Y3, Y2 & Y1). A logic "1" in M44, M45, M46, and M47 (Eqs. (16)- (19) respectively) signifies the detection of an attack at the respective houses in Station 2 and pump, following the similar logic operations described in Section 3.2.2.

$$M44 = M28.\overline{Y4}.\overline{Y11}.\ M10.\ M49 \quad (16)$$

$$M45 = M29.\overline{Y3}.\overline{Y11}.\ M10.\ M49 \quad (17)$$

$$M46 = M30.\overline{Y2}.\overline{Y11}.\ M10.\ M49 \quad (18)$$

$$M47 = M31.\overline{Y1}.\overline{Y11}.\ M10.\ M49 \quad (19)$$

4. Security functions for the automation of water distribution system

Security measures for PLC program files have been implemented at various levels within the water distribution system to safeguard against unauthorized access to WDS controller (PLC).

4.1 Security for program files of the controller

A groundbreaking attack vector was implemented to find the unauthorized manipulation of PLC memory [6]. In the proposed work, alternatively, a file authentication has been established to secure the

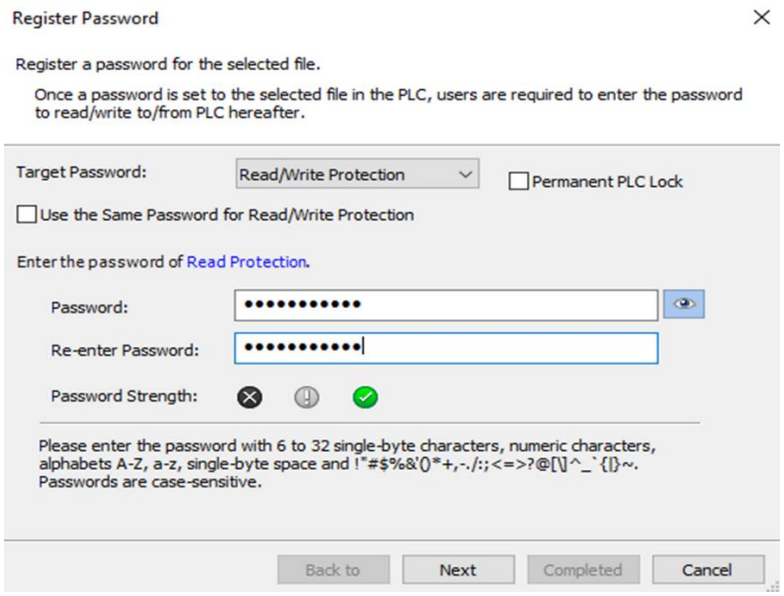

Figure. 6 Register file authentication for read/write protection of PLC for WDS

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

PLC programming, preventing unauthorized access for read/write & manipulation of programming (presented in Fig. 6). The proposed functionality restricts any program manipulations and grants permission solely to authorized individuals to read and write the algorithms.

It was found that much research works on attack detection aimed to identify the attack concerning normal and abnormal conditions of data drive models [14,22]. However, trapped air in pipelines and pressure surges also cause abnormal flow rates rather than attacks [15, 16, 19]. Hence the attack identification method with respect to abnormalities may produce inaccurate result. In such a case, introducing security functions to the controllers in various aspects strengthens the cyber-physical system for water distribution.

The proposed work introduced various security functions to protect the cyber-physical systems. In the case of unauthorized access being successful for the read operation of the water distribution PLC program, the block password authentication (indicated in Fig. 7) doesn't allow the attacker to open the PLC programming file of WDS.

4.2 Security from illegal access through remote communication

In 2011, there was another documented cyber-attack in which the culprits successfully turned on a water pump remotely, affecting a utility in Central Illinois [8]. In my proposed work, the remote security function protects against unauthorized access from external devices. Specific remote security has been configured for the proposed WDS to ensure security authentication, as depicted in Fig. 8. Remote authentication is verified when a connection is sought through an engineering tool, SLMP, and FTP port communication from external devices. An error will occur on the connected device if the authentication is not validated, as the CPU module restricts unauthorized access.

4.3 IP Security Function

Some cyber-attacks include interpreting parameters and values exchanged during communication among control devices through TCP/IP packets [10]. The IP filter function is crucial for preventing unauthorized access to the water distribution system from external devices. This functionality identifies the IP address of the access source and prohibits access from an unauthorized IP address. The parameters specify which IP addresses of external devices are permitted or denied, effectively restricting access, as illustrated in Fig. 9. In this proposed system, access has been granted to the personal computer's IP address (192.168.3.138) and our laboratory personal computer's IP address (192.168.3.141).

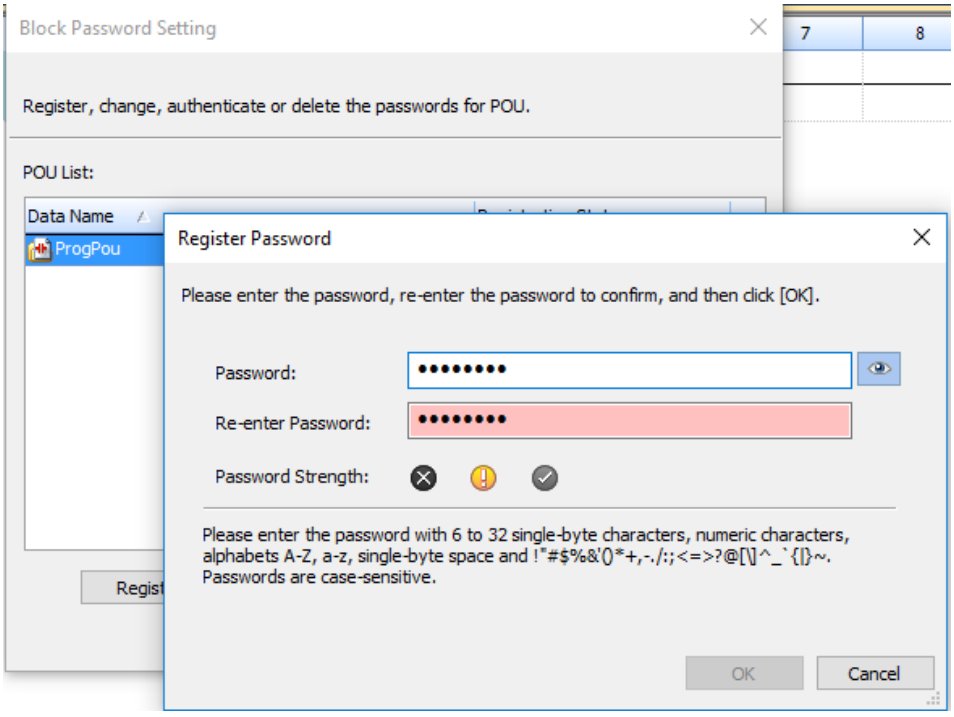

Figure. 7 Register block secure authentication for programming files of PLC for WDS.

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

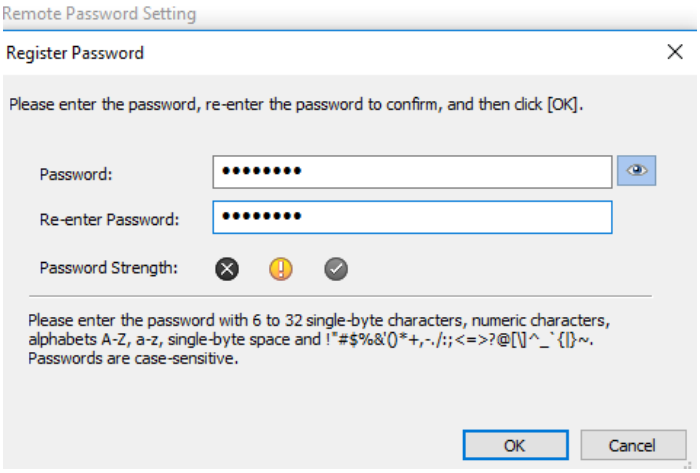

Figure. 8 Register remote authentication for connection protection of PLC from unauthorized access.

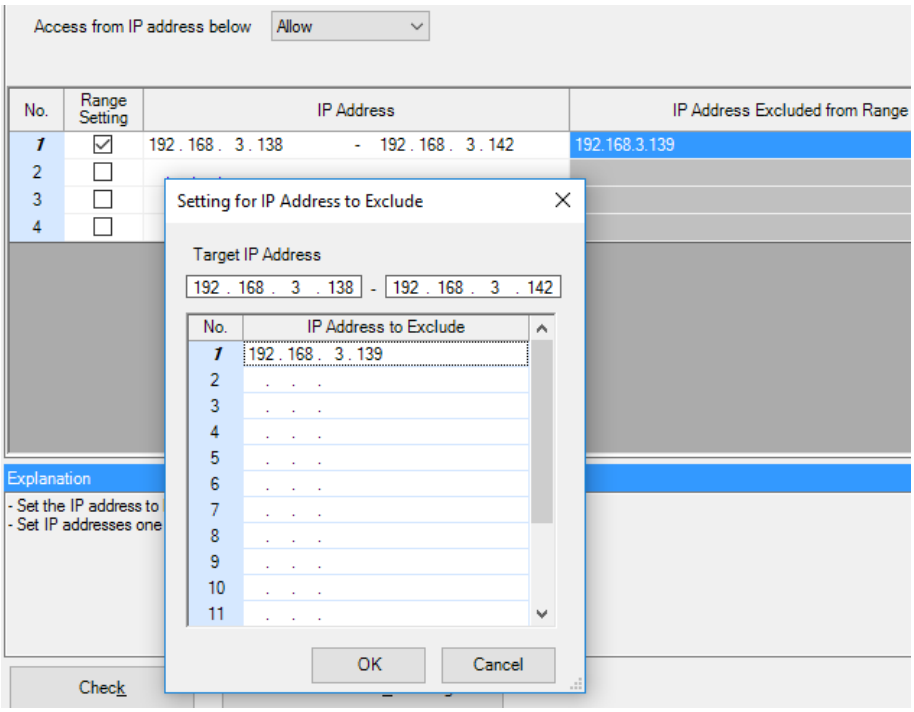

Figure. 9 Configuration settings for IP security filter functions

It is recommended to use this function in environments connected to the Wi-Fi router (IP: 192.168.3.142) for IoT applications and exclude the IP address (IP: 192.168.3.139) from the selected range of access IP addresses. In such a way, the PLC allows access to the filtered IP address of external devices.

4.4 Security Authentication for GOT Module

The GOT simple series model (GS2107-WTBD) has activated security level authentication for the water distribution supervisory graphical panel, as illustrated in Fig. 10. Authentication is necessary to monitor and control water distribution operations through GOT. Additionally, security levels were added to the graphical switches for control operations. The GOT interface provides operators with a user-friendly environment, making security crucial to prevent illegal actions by unauthorized individuals. The implementation of security-level authentication for devices in GOT serves to safeguard the WDS from illegitimate operations. In the proposed GOT system, security measures have been implemented for graphical switches used to control pumps and

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

Figure. 10 Security authentication for GOT module for WDS supervisory operation

solenoid valves, ensuring that only authorized operators can perform WDS supervisory operations using a security key.

4.5 Security Authentication for IoT Device

Supervisory operations for water distribution can be performed remotely through a web browser. This section introduced the web pages utilized with the Web server function. The web page is compatible with standard web browsers on personal computers, tablet terminals, or smartphones, allowing the reading and writing of data from/to a device of the PLC module with valid authentication. Operators and external individuals access the web page once it is enabled through security authentication, as illustrated in Fig. 11.

Upon selecting "System Web page" for the authority of window display, which allows remote control operations, the initial display window after login showcases information pertinent to the PLC-CPU module. The webpage-module Information includes the model's name, production number, firmware version, IP address, and MAC address. Additionally, this web page presents the status of Power, error, P. RUN, and battery, as depicted in Fig. 12.

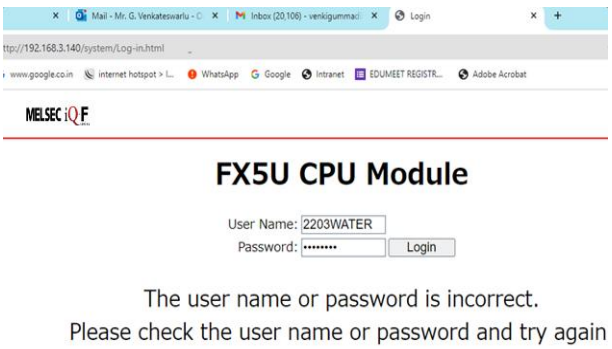

Figure 11. Valid security authentication is required in the web browser for WDS operations

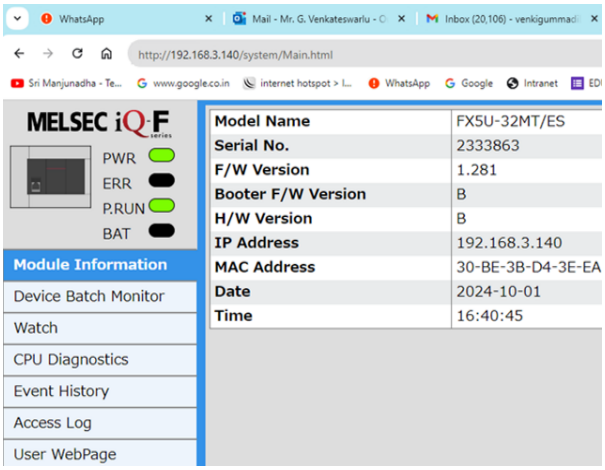

Figure. 12 PLC model information and CPU status in the web browser

5. Experimental results

The attacks recognized in this proposed water distribution system are promptly demonstrated on the GOT (displayed in Fig. 13, 14 and 15) with corresponding dates and times. As discussed in Section 3, this study deliberately induced attacks by applying illegal external voltage sources. The identified attacks are illustrated in Fig. 13, with the first attack on the main pipeline registered at 11:51 AM, the second on Station-1 House-3 (S1H3) at 12:37 PM, and the third on Station-1 House-1 (S1H1) at 12:41 PM on 09th Sep 2024. The operator verified these occurrences at 11:52 AM, 12.39 PM & 12.43 PM on the same day. As outlined in Section 3, deliberate attacks were initiated at the pump by applying unauthorized external voltage sources. The identified attacks on the pump are depicted in Fig. 14, with the initial attack on the pump recorded at 01:04 PM on 09th Sep 2024. The operator confirmed these incidents at 1:05 PM on the same day. A buzzer is triggered whenever a physical attack is detected at the WDS.

As discussed in case 2 of section 3, the attacks on both solenoid valves of individual houses under station-1 & 2 and the pump were created experimentally and displayed the instant alarms of attacks on the graphical screens GOT. The identified attacks are illustrated in Fig. 15, with the attack on Pump & S1H3 registered at 03:16 PM, the next attack on Pump & S2H3 registered., at 03:20 PM, and the third on Pump & S2H4 registered at 04:27 PM on 10th Sep 2024. The operator verified these occurrences at 03.16 PM, 03.22 PM & 04.28 PM, respectively, on the same day. The proposed work introduced a novel algorithm to ascertain whether the attack density is categorized as High or Low, as outlined in Eq. (10).

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

Received: March 26, 2025. Revised: April 26, 2025.

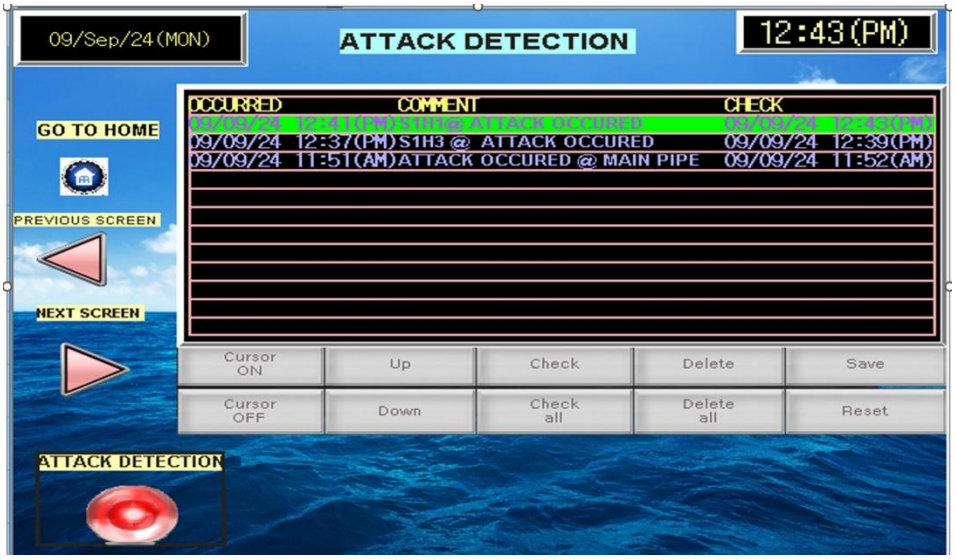

Figure. 13 GOT screen for alarm system of attack detection at main pipeline & houses under substations of WDS

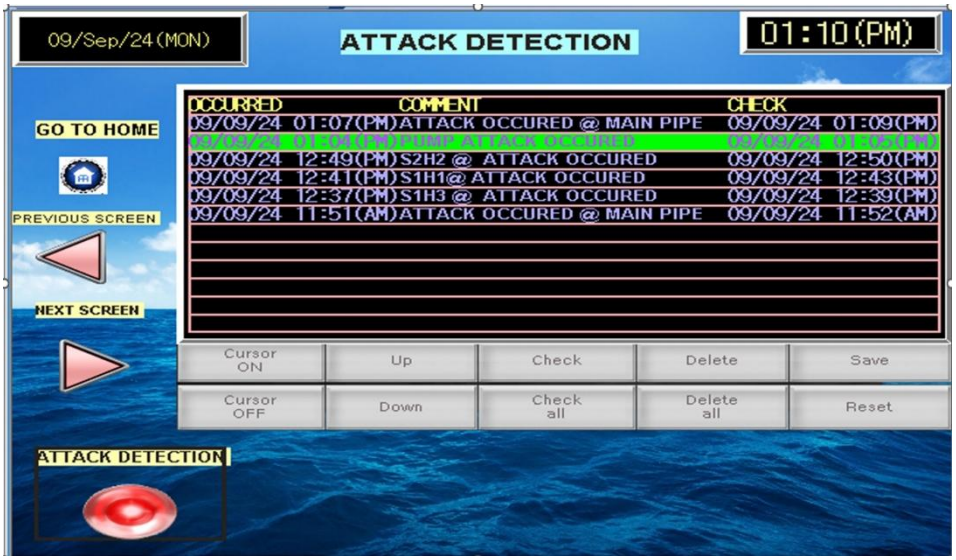

Figure. 14 GOT screen for alarm system of attack detection at the pump of water distribution

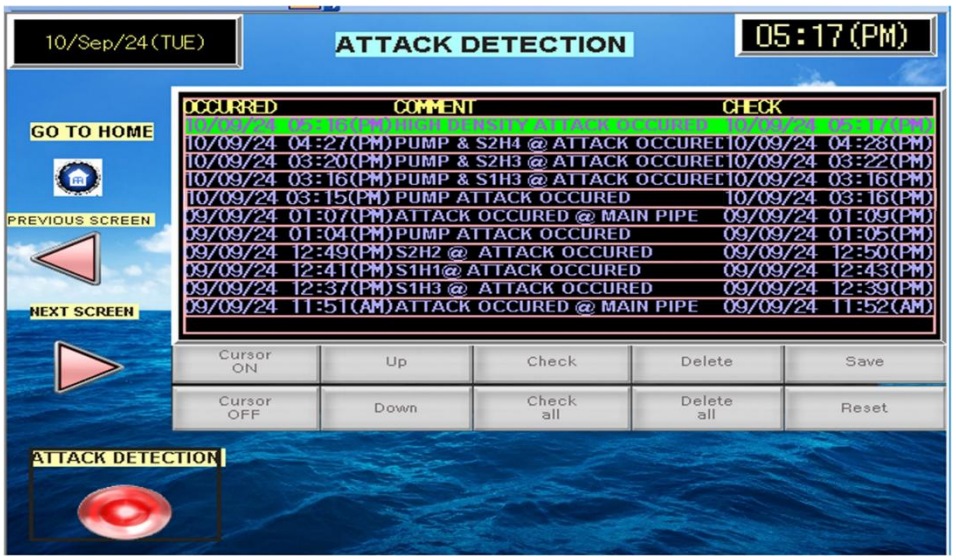

Figure. 15 GOT screen for alarm system of density of attack and attack at both pump & houses under sub stations of water distribution

 DOI: 10.22266/ijies2025.0630.45

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

An attack scenario was experimentally executed by extracting a higher liquid outflow from the overhead tank in the absence of PLC control actions. The occurrence of a high-density attack was identified and displayed on the Graphic Operator Terminal, as illustrated in Fig. 15, recorded at 5:16 PM on 10th Sep 2024. The operator verified these incidents at 5:17 PM.

5.1 Statistical validation of detection rates

The concepts of false positives, false negatives, true positives, and true negatives [32] strengthen the contextual discussion in the Results Analysis. This analysis highlights the proposed water distribution system's effectiveness in reducing detection errors and improving its accuracy in responding to unauthorized activities. As per the experimental test results for the proposed work, it was noticed that

True Positives (TP)- Correctly detected Attacks: **31**,

False Negatives (FN)- Attacks occurred but not detected: **1.**

From the results (TP & FN), it was clearly seen that one attack was not detected by the proposed system. In this case, the attacker tried to open the solenoid valve by sending power from an external source instead of using the PLC. However, due to an air lock in the pipeline, no water came out even though the valve was open. Because of this, the sensors could not sense any water flow, so the system did not detect the attack. Although no water was stolen, the attempt to steal was still made by the attacker.

False Positive (FP)- No attack but system **incorrectly flagged** as attack: 1

True Negative (TN)- No attack and system correctly did **not** flag it: 43

From the analysis of False Positives (FP) and True Negatives (TN), it was observed that one instance was incorrectly flagged as an attack. In this case, the solenoid valve malfunctioned and opened slightly without any input signal, causing a small amount of water to flow through the pipeline. Although this was not an actual attack, the system identified it as one. However, this false alert proved useful, as it helped us identify and troubleshoot the issue with the solenoid valve. The performance metric of the proposed work is calculated with the following Eqs. (20) - (26).

$$\text{TPR (True Positive Rate)} = \frac{\text{TP}}{\text{TP+FN}} \quad (20)$$

$$\text{TNR (True Negative Rate)} = \frac{TN}{TN+FP} \quad (21)$$

$$\text{FPR (False Positive Rate)} = \frac{FP}{FP+TN} \quad (22)$$

$$\text{FNR (False Negative Rate)} = \frac{FN}{FN+TP} \quad (23)$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (24)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (25)$$

$$\text{F1 Score} = 2.\frac{\text{Precision .TPR}}{\text{Precision+TPR}} \quad (26)$$

Table 4 provides the summary of accuracy, precision, true and false rate of the proposed system. It was noticed that the proposed system proved with high accuracy 97.37% and very low false positive and false negative rates (2.27% and 3.13% respectively). These findings validate the system's capability to minimize detection errors and enhance the overall security of the water distribution network against cyber-physical attacks.

Table 4. Summary table for performance analysis of attack detection

S. No	Metric	Value
1	TPR	96.88%
2	TNR	97.73%
3	FPR	2.27%
4	FNR	3.13%
5	Precision	96.88%
6	Accuracy	97.37%
7	F1 Score	96.88%

5.2 Statistical significance testing

In the proposed work, attack detection outcomes are binary (1 for detected, 0 for not detected), resulting in extreme proportions close to 0 or 1. Therefore, we have chosen to perform a One-Proportion Z-Test to statistically validate the detection performance. A total of 32 attack scenarios were tested, out of which 31 were successfully detected, and 1 attack went undetected.

This analysis aims to estimate whether the proposed attack detection system implemented in a water distribution network is operating at a statistically significant level above random chance. The hypothesis test [33] concludes whether the measured detection rate significantly exceeds a standard detection rate of 50% and Significance level (α): 0.05. Eqs. (27) - (30) represent the mathematical formulations of the statistical parameters: Observed

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

Proportion ($\hat{p}$), Standard Error (SE) of the Proportion, Z-Statistic (Test Statistic), and p-Value (One-Tailed), respectively, used in the attack detection analysis of the automatic water distribution system.

- Null Hypothesis **(H_0):** p = 0.5 (Proposed system detect the attacks at a rate of 50%)
- Alternative Hypothesis **(H_1):** p > 0.5 (Proposed system detect the attacks at a rate significantly higher than 50%)

$$\textbf{Observed Proportion } (\hat{p}) = \frac{x}{n} = 0.968 \quad (27)$$

x: number of successful detections (in your case, 31)
n: total number of attacks tested (in your case, 32)

$$\textbf{Standard Error (SE)} = \sqrt{\frac{(p_0)(1-p_0)}{n}} = 0.08839 \quad (28)$$

p_0: hypothesized population proportion under the null (here, 0.5)
n: sample size (32).

$$\textbf{Z-Statistic} \text{ (Test Statistic)} = \frac{(\hat{p}-p_0)}{SE} = 5.30 \quad (29)$$

$$\textbf{p-Value (One-Tailed)} = P(Z > z) = 1 - \Phi(Z) = 5.69 \times 10^{-8} \quad (30)$$

Φ(Z): cumulative distribution function (CDF) of the standard normal distribution.

The p-value is the area under the curve to the right of the Z-statistic.

From the statistical calculation, Since the p-value (5. 69 × 10 -8) is extremely small (< 0.05), We can strongly reject the null hypothesis. There is significant evidence that the attack detection rate (96.88%) is greater than 50%. The test yielded a Z-statistic of 5.30 with a p-value of 5. 69 × 10^{-8}, which is far below the conventional significance level of 0.05. as shown in Fig. 16. This indicates that the system performs well in identifying attacks in the tested scenarios.

The file Authentication function is employed as a preventive measure against unauthorized access, including the potential destruction of data and programs. Attempts to read/write the PLC program for water distribution control necessitate unlocking the password set for the CPU module programming file, as depicted in Fig. 17. It serves as a crucial safeguard to deter unauthorized access.

In the case of unauthorized person access, if the attacker successfully reads the programming file from the PLC to the personal computer, the opening of programming in the personal computer is restricted by the block password authentication, as shown in Fig. 18. In such a way, the proposed system provides security in all aspects.

Efforts were made using an unauthorized personal computer to establish communication with the PLC CPU through the MELSOFT tool. However, the remote password authentication function prevented the attempt, prompting the need to input the remote password, as illustrated in the screen (Fig. 19) that appears during communication.

Once the correct remote password is entered, the engineering tool proceeds with unlock processing and gains access to the CPU module.

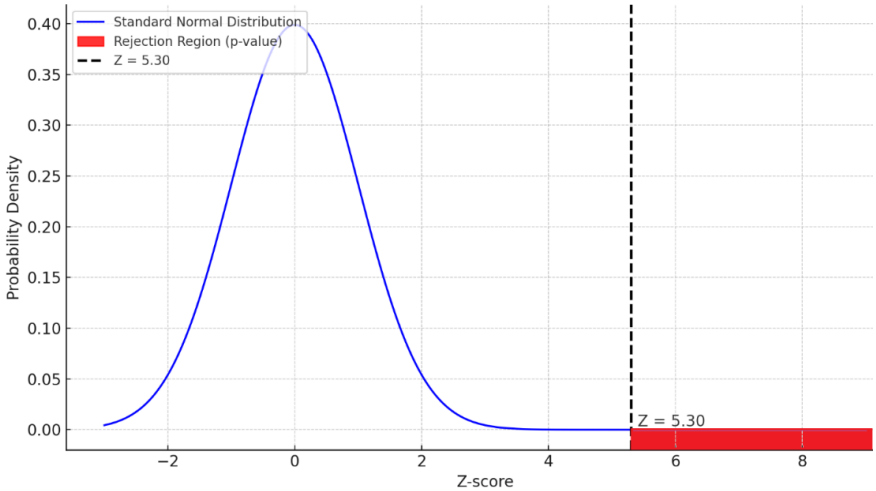

Figure. 16 One Proportion Z-Test: Right Tailed test for attack detection rate

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

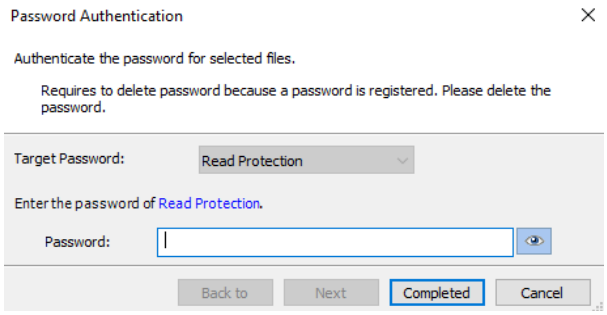

Figure. 17 Password authentication is required for read/write files from PLC

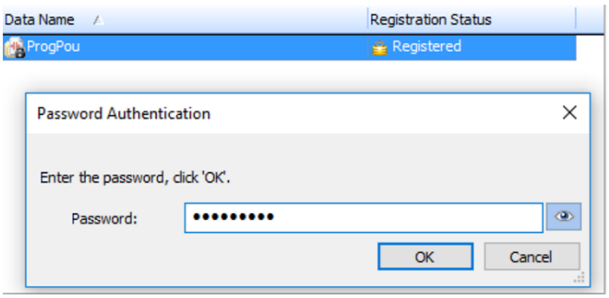

Figure. 18 Block password authentication is required to open the program in the PC software window

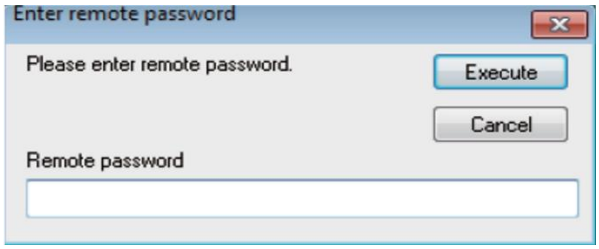

Figure. 19 Remote password authentication for PLC communication.

Another attempt was made to establish communication with the PLC for unauthorized read/write operations from a computer with the IP address 192.168.3.135. However, the enabled IP address filter function successfully prevented illegal access, prohibiting any attempt to access through a direct connection with MELSOFT, as depicted in Fig. 20. The configured security functions protect the WDS controller from multiple angles

The access login history to the web server, operations conducted-event history, and the IP address of the access source are viewable, as depicted in Figs. 21 and 22. It allows for monitoring the frequency of access, each operation performed, and any unauthorized access to the web server. Specifically, entries S.No.17 to 21 (presented in Fig. 21) detail unauthorized login operations on 1st Oct 2024 at the timings 16:43:14, 16:43:34, 16:43:50, 16:44:04 & 16:44:17 respectively. The successful access was registered on 1st Oct 2024, at 16:44:28. The event history retrieved from the CPU module, including the occurrence date, event type & code, status, and summary, is displayed in Fig. 22. This work may help to address the primary challenges of securing industrial processes from unauthorized access, particularly while employing industrial automation technologies for water distribution processes.

The proposed Boolean algebraic approach efficiently identified attacks on the water distribution system across various case studies by analyzing sensor data and the enable/disable signals for solenoid valves and the pump from the PLC. A comparative analysis with existing methodologies for attack identification and cybersecurity in water distribution is presented in Tables 5 and 6. The key

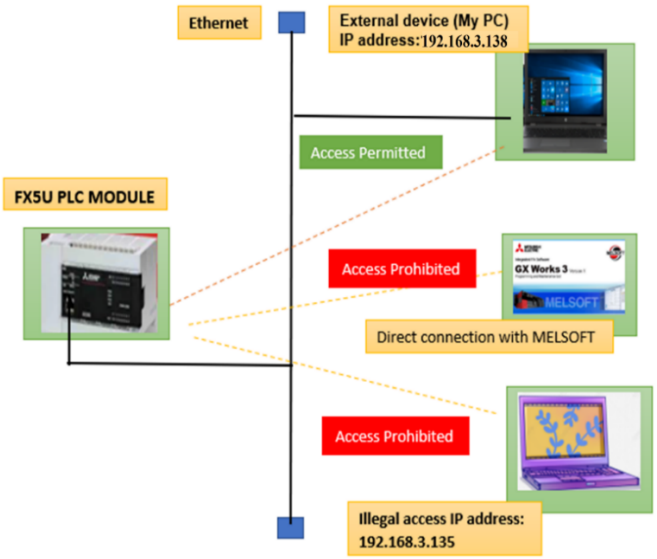

Figure. 20 IP security function & direct connection security for PLC from illegal

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

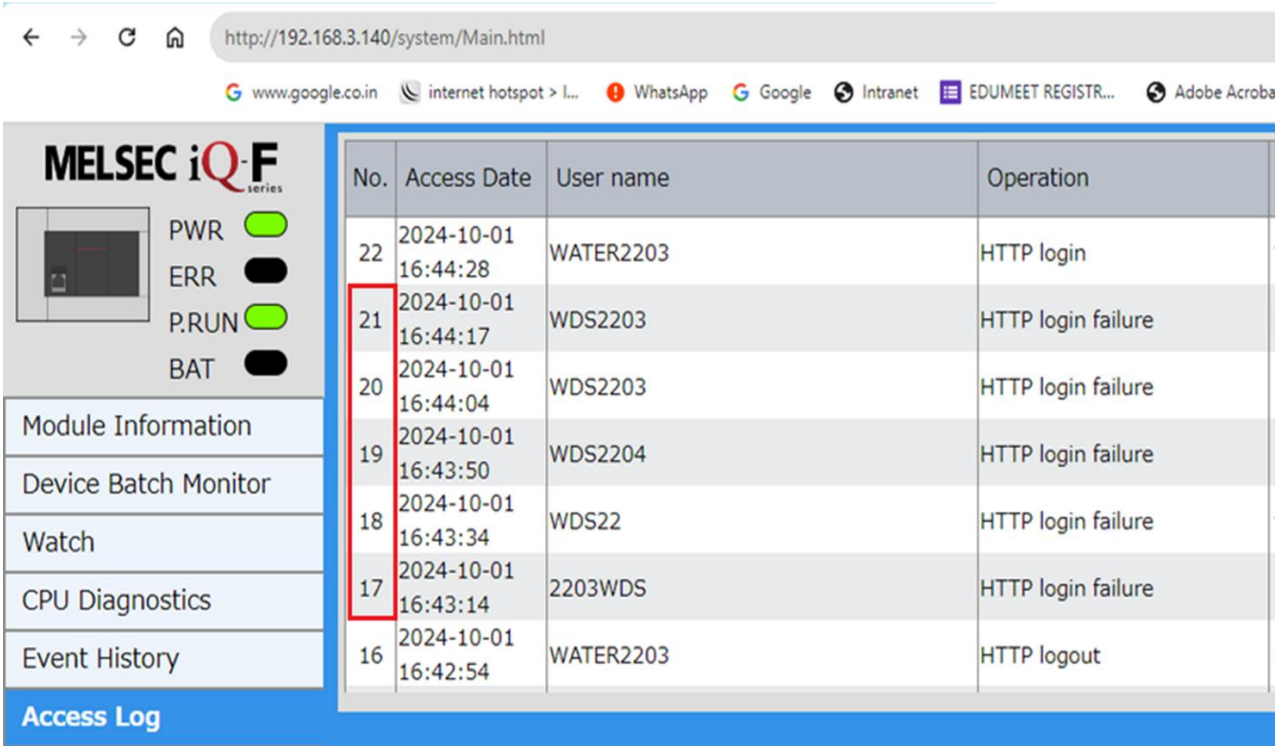

Figure. 21 Web Access Log information of PLC for WDS

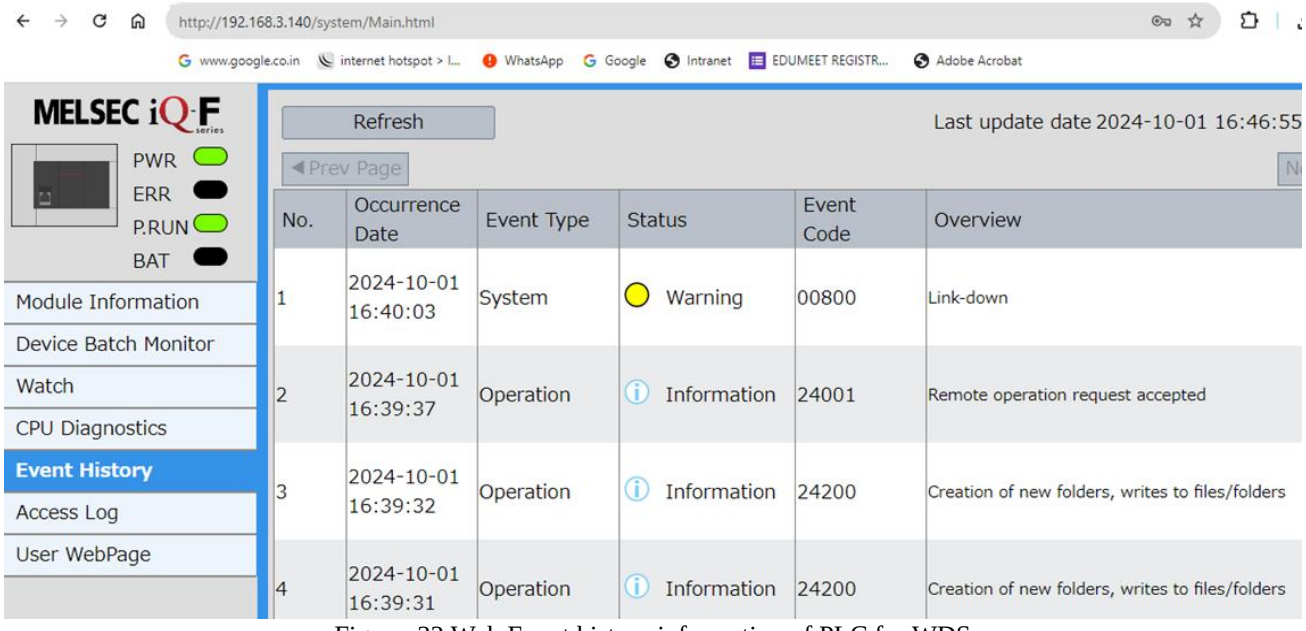

Figure. 22 Web Event history information of PLC for WDS

components considered for this analysis included the type of attack, proposed methodologies, security measures introduced, actions taken in response to attacks, novelty, and the mode of attack detection. The findings highlight that the proposed method uniquely implemented multidirectional security measures for the water distribution against cyber-physical attacks. These measures include IP security for the WDS controller-PLC, protection against unauthorized read/write operations, safeguarding programming files from unauthorized access, remote security against illegal access through engineering tools, secure communication via SLMP and FTP protocols, and authentication for graphical operations and web logins. In contrast, many existing methodologies primarily focus on defending systems from memory-based attacks, underscoring the novelty of the proposed approach.

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

Table 5. Comparison of the proposed work with current scenarios

The Work	Type of attack/failure created & detected	Attack level density detection	Mode of attack detection	Proposed Algorithm/ Technique
N. Kadosh et. al, 2020 [10]	Creating imbalanced datasets of simulated attacks	☒	Attack detection was performed with respect to classifying normal and abnormal conditions in **scheduling phase** of water distribution.	One-class classification technique by analyzing collected sensors data
A. Robles-Durazno. et.al, *2019*[6]	Creating the attacks to the input memory of the PLC & illegal computer connection	☑ Severity of the attack depends on probability of an attack to succeed	Utilizes a wide variety of protocols supported for external access by controller to perform the attacks to the input memory of the PLC	Algorithm for detection of attacks to the PLC input memory
Proposed work	Supply unauthorized external power supply to the actuators and unlawful access to the controller (PLC)	☑	Attack detection is performed majorly in the **absence (non- scheduled phase)** of a controller's (PLC) actuating signal for water distribution.	Boolean function algorithm with real sensor's & controller's data
HH. Addeen et. al, 2024 [31]	manipulating the water level, activating and deactivating pump	☒	Attack detection is performed in the presence **(scheduled phase)** of a controller's (PLC) actuating signal for water distribution.	Conditional variational Autoencoder algorithm

Table 6. Comparison of the proposed work with current scenarios

The Work	IP Security for controller access	Classified attacks detection	Security for program read/write operation	Security for programming files/data	Remote Security for controller
N. Kadosh et. al, 2020 [10]	☒	☑	☒	☑	☒
A. Robles-Durazno. et.al, *2019*[6]	☒	☑	☒	☑	☒
Proposed work	☑	☑	☑	☑	☑
HH. Addeen et. al, 2024 [31]	☒	☑	☒	☑	☒

The proposed work effectively detected the classified attacks by identifying unauthorized power supply to actuators, particularly in the absence of PLC control actions, while also considering scenarios where PLC control actions were present. In contrast, many researchers have focused (described in Table. 5) on attack identification through methods such as creating imbalanced datasets of simulated attacks, manipulating nodal pressure, altering tank water levels, disrupting pump water flow, and inducing pipe leaks or bursts. This study introduced unique features to enhance the automation of the water distribution system, such as detecting attack density, identifying classified attacks during unscheduled times of PLC-controlled water distribution, and implementing multidirectional security measures.

Scalability-In this work, the iQ-F series PLC is utilized for both automation and attack detection,

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

supporting up to 512 I/O devices. For broader applications, the iQ-R series PLC offers the capability to integrate up to 4096 I/O devices. Furthermore, a single network (CC-Link IE Control) platform can support the integration of up to 120 PLCs, collectively handling approximately 500,000 I/O devices with high-speed data communication at 1 Gbps. This interconnectivity enables regional data sharing related to attack incidents in various areas and supports resource reallocation from regions with surplus water to those experiencing scarcity. Finite State Machines (FSM), data-driven approaches, and AI-based models are suitable for large-scale water distribution applications due to their scalability and ability to handle complex system behaviour.

6. Conclusion

This paper examined the repercussions of attacks on the automation system for water distribution, explicitly targeting solenoid valves and pumps when the control actions from the controller to WDS are inattentive and securing the system from cyber-physical attacks on the PLC in different scenarios. The execution analysis demonstrates that the proposed solutions for attack detection is highly effective & reliable. With a True Positive Rate of 96.88% and a True Negative Rate of 97.73%, the system accurately recognizes both attack events & normal conditions. The low False Positive Rate of 2.27% and False Negative Rate of 3.13% further confirms its robustness in reducing incorrect classifications.

Moreover, the Precision (96.88%), Accuracy (97.37%), and F1 Score (96.88%) reflect a well-balanced detection performance, combining both sensitivity & specificity. These results collectively specify that the detection mechanism is efficient, with minimal errors, and can be positively applied for real-time monitoring and protection of water distribution system against physical & cyber-physical threats. All identified attacks were presented successfully on the GOT, providing details such as the time of the attack and its classification.

The configured security function for PLC programming underwent testing, prompting authentication for read/write operations. The effectiveness of the remote security function, IP address access & web access securities were assessed in a real testbed environment by attempting access with an unauthorized system, yielding satisfactory results in preventing illegal access. The test results provided strong statistical evidence to reject the null hypothesis. With a p-value $\mathbf{(5.69 \times 10^{-8})}$ well below 0.05 and a detection rate of 96.88%, the system significantly outperformed random chance in identifying attacks.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

G. Venkateswarlu, as the primary researcher and corresponding author, conceptualized the study, designed the hardware setup for water distribution automation, developed the programming for the proposed methods, and conducted the experiments. Dr. Santosh R. Desai formulated the research questions based on the literature survey, carried out the data analysis, drafted the manuscript, and contributed to the algorithm's logic implementation. Both authors reviewed and approved the final manuscript.

Acknowledgments

We would like to express our gratitude to the Mitsubishi Electric Factory Automation Division - ATC CVRCE Hyderabad for their generous support in providing automation hardware and software tools.

References

[1] D. Upadhyay, S. Ghosh, H. Ohno, M. Zaman, and S. Sampalli, "Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator", *International Journal of Critical Infrastructure Protection*, Vol. 47, p.100705, 2024.

[2] K. Stouffer, K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, *Guide to operational technology (OT) security*, Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2023.

[3] H. H. Addeen, Y. Xiao, and T. Li, "A CVAE-based anomaly detection algorithm for cyber physical attacks for water distribution systems", *IEEE Access*, Vol. 12, pp.48321 - 48334, 2024.

[4] Y. Zhou, Z. Zhang, K. Zhao, and Z Zhang, "A novel dynamic vulnerability assessment method for Industrial Control System based on vulnerability correlation attack graph", *Computers and Electrical Engineering*, Vol. 119, p.109482, 2024.

[5] H. Hui, and K McLaughlin, "Investigating current PLC security issues regarding siemens s7 communications and TIA portal", In: *Proc. of 5th International Symposium for ICS & SCADA*

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

Cyber Security Research, Hamburg, Germany, pp. 67-73, 2018.

[6] A. Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell, and I. Maneru-Marin, "PLC memory attack detection and response in a clean water supply system", *International Journal of Critical Infrastructure Protection*, Vol. 26, p.100300, 2019.

[7] J. Slay, and M. Miller, "Lessons learned from the maroochy water breach", In: *Proc. of International conference on critical infrastructure protection*, Boston, pp. 73-82, 2007.

[8] J. Finkle, "US probes cyber-attack on water system", 2011. Available from: https://www.reuters.com/article/us-cybersecurity-attack-idUSTRE7AH2C320111121/ (Accessed 2024).

[9] M. M. Aslam, A. Tufail, KH. Kim, R. A. Apong, and MT. Raza, "A comprehensive study on cyber-attacks in communication networks in water purification and distribution plants: challenges, vulnerabilities, and future prospects", *Sensors*, Vol. 23, No.18, p.7999, 2023.

[10] N. Kadosh, A. Frid, and M. Housh, "Detecting cyber-physical attacks in water distribution systems: One-class classifier approach", *Journal of Water Resources Planning and Management*, Vol. 146, No. 8, p.04020060, 2020.

[11] S. Amin, X. Litrico, SS. Sastry, and AM. Bayen, "Cyber security of water SCADA systems Part II: Attack detection using enhanced hydrodynamic models", *IEEE Transactions on Control Systems Technology*, Vol. 21, No.5, pp.1679-1693, 2012.

[12] A. Rasekh, A. Hassanzadeh, S. Mulchandani, S. Modi, and MK. Banks "Smart water networks and cyber security", *Journal of Water Resources Planning and Management*, Vol. 142. No. 7, p.01816004, 2016.

[13] R. Taormina, S. Galelli, NO. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems", *Journal of Water Resources Planning and Managemen*t, Vol. 143, No. 5, p. 04017009, 2017.

[14] R. Taormina, S. Galelli, NO. Tippenhauer, E. Salomons, A. Ostfeld, DG. Eliades, M. Aghashahi, R. Sundararajan, M. Pourahmadi, MK. Banks, and BM. Brentan, "Battle of the attack detection algorithms: Disclosing cyber-attacks on water distribution networks", *Journal of Water Resources Planning and Management*, Vol. 144, No. 8, p. 04018048, 2018.

[15] JP. Ferreira, D. Ferras, DI. Covas, and Z. Kapelan, "Improved SWMM modeling for rapid pipe filling incorporating air behavior in intermittent water supply systems", *Journal of Hydraulic Engineering*, Vol. 149, No.4, p. 04023004, 2023.

[16] J. E. Lescovich, "Locating and Sizing Air-Release Valves", *Journal-American Water Works Association*, Vol. 64, No.7, pp. 457-461, 1972.

[17] C. Lauchlan, M. Escarameia, R. May, R. Burrows, and C. Gahan, "Air in pipelines-A literature review", *HR wallingford*, 2005.

[18] E. Tasca, M. Besharat, HM. Ramos, E. Luvizotto Jr, and B. Karney, "Contribution of air management to the energy efficiency of water pipelines", *Sustainability*, Vol.15, No.5, p.3875, 2023.

[19] D. May, J. Allen, and D. Nelson, "Hydraulic investigation of air in small diameter pipes", *International Journal of Hydraulic Engineering*, Vol. 7, pp. 51-57, 2018.

[20] V. Karthikeyan, Y. Palin Visu, and E. Raja, "Integrated intelligent system for water quality monitoring and theft detection", *Water Practice & Technology*, Vol.18, No.12, pp. 3035-3047, 2023.

[21] Global Market Insights, Programmable Logic Controller (PLC) Market Size - By End Use, Type, Component, Global Forecast, 2025 -2034, Feb 2025, Available from: https://www.gminsights.com/industry-analysis/programmable-logic-controller-market [Accessed: 2-Mar-2025].

[22] A. Almalawi, X. Yu, Z. Tari, A. Fahad, and I. Khalil, "An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems", *Computers & Security*, Vol. 46, pp. 94-110, 2014

[23] Y. Shen, G. Ye, F. Zheng, Z. Ye, and Z. Yu, "Intelligent identification method for pipeline leakage based on GPR time-frequency features and deep learning", *AQUA—Water Infrastructure, Ecosystems and Society*, Vol. 73, No. 7, pp.1421-1436, 2024.

[24] U. Parajuli, and S. Shin, "Identifying failure types in cyber-physical water distribution networks using machine learning models", *AQUA—Water Infrastructure, Ecosystems and Society*, Vol. 73, No. 3, pp.504-519, 2024.

[25] A Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell, and I. Maneru-Marin, "Implementation and detection of novel attacks

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/

to the PLC memory of a clean water supply system", In: *Proc. of Technology Trends: 4th International Conference*, Babahoyo, Ecuador, pp. 91-103, 2019.

[26] Mitsubishi Electric-MELSEC iQ-F, "MELSEC iQ-F FX5U User's Manual (Hardware)", 2023, Available from: https://www.mitsubishifa.co.th/files/dl/jy997d55301u.pdf [Accessed 2024]

[27] Mitsubishi Electric- MELSEC iQ-F Programming, "MELSEC iQ-F FX5 User's Manual (Application)", 2023, Available from: https://www.allied-automation.com/wp-content/uploads/2015/05/MITSUBISHI_manual_plc_fx5_application.pdf [Accessed 2024].

[28] Mitsubishi Electric-Human Machine Interfaces [HMI's]-GOT, "MELSOFT GT Works3 engineering software" 2023, Available from: https://www.mitsubishielectric.com/fa/products/hmi/got/smerit/gt_works3/index.html [Accessed 10th November 2024].

[29] Mitsubishi Electric-MELSEC iQ-F Web Function, "Web Server Function Application Guide Using Web Page Startup and Introduction", 2023, Available from: https://dl.mitsubishielectric.co.jp/dl/fa/document/catalog/plcf/l08643/l08643-a.pdf [Accessed 2024]

[30] N. Kohpeisansukwattana, N. Siriwattananon, and E. Charoenwanit, "Developing a Mobile Game Application to Enhance Learning Experience in Programmable Logic Controller (PLC) Wiring beyond the Laboratory", *International Journal of Interactive Mobile Technologies*, Vol. 18, No. 4, 2024

[31] H. H. Addeen, Y. Xiao, and T. Li, "A CVAE-based anomaly detection algorithm for cyber physical attacks for water distribution systems", *IEEE Acces*s, Vol. 12, pp. 48321 - 48334, 2024.

[32] J. Han, M. Kamber, and J. Pei, "Data Mining: Concepts and Techniques", Vol. 3. Morgan Kaufmann (imprint of Elsevier), Waltham, USA. 2011.

[33] D. D. Wackerly, W. Mendenhall, and R. L. Scheaffer, *Mathematical Statistics with Applications*, Vol. 7, Duxbury Press, United States, USA, 2007.

This article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
License details: https://creativecommons.org/licenses/by-sa/4.0/