Exploiting Control Device Vulnerabilities: Attacking Cyber-Physical Water System

Parul Sindhwad, Faruk Kazi
Electrical Engineering Department, VJTI
Mumbai 400019, India
pvsindhwad_p21@el.vjti.ac.in,fskazi@ee.vjti.ac.in

***Abstract*—Industrial Control Systems (ICS) are transitioning from isolated, custom-built systems to those combining general-purpose computer hosts, wireless networks, and artificial intelligence. An increasing number of vulnerabilities in ICS devices are a major concern since it provides potential adversaries with a simple approach to exploit and attack unpatched ICS systems. This paper investigates attack paths that target unpatched system vulnerabilities and their impact on the ICS, as demonstrated using the Waste Water Treatment Plant (WWTP) testbed. Denial of Service (DoS), Buffer overflow, privilege escalation, and illegal command injection attacks are executed, and their impacts are investigated using CIA and STRIDE threat modeling. The main outcomes of the study are, 1) An update on public advisory CVE-2021-33834 by Moxa. 2) Demonstration of attack on a device with publicly accessible Proof of Concept (POC) of another device using Modbus buffer overflow vulnerability. Finally, various recommendations are provided that can be used for security penetration testing to identify security flaws, as well as directions for product developers to implement security by design.**

I. Introduction

A. Background

Industrial control systems (ICS) have expanded to include information technology (IT), and preconfigured components as part of the Internet of Things (IoT). Migration have progressed from solitary devices to sophisticated, complicated, open systems that are connected to the Internet [1] [2] [3]. The internet-connected ICS is a part of industries like oil, gas, water, and power plants. Compared to older, more standalone systems, present ICS are more complex and are digitally connected to external networks through the Internet [4]. Increasing ICS vulnerability is one of the repercussions of digital transformation [5]. The operation of this system has a direct impact on human life and the environment. Hence, any cyber attack, intentional or unintentional modification to these systems, can have devastating, potentially fatal consequences [6] [7]. It affects the system's availability, integrity, and confidentiality. According to the IBM security x-force study, [8] the number of published ICS vulnerabilities are on the rise. In 2020, there were 49 percent more vulnerabilities than in 2019. Figure 1 shows number of published ICS vulnerabilities from year 2011 to the year 2021 [9] [10].

Adversaries use both Zero-day and N-Day vulnerabilities to exploit ICS systems. A Zero-day exploit uses previously unknown flaws in software or hardware component. When a vulnerability is detected, vendors often offer a patch or mitigation. However, not all systems are promptly updated. It could take weeks to upgrade all of its systems, with ICS taking even longer. As a result, it allows attackers enough time to develop and deploy an exploit. Such vulnerabilities are known as N-Day vulnerabilities. They take advantage of previously disclosed vulnerabilities. Exposing Zero-day vulnerabilities requires significantly more time and effort. Using N-Day vulnerability, and publically available information, a low-skilled attacker may also create a stealthy ICS attack. N-day vulnerability is a risk to any network, specifically for ICS, due to the direct impact on human life and environment.

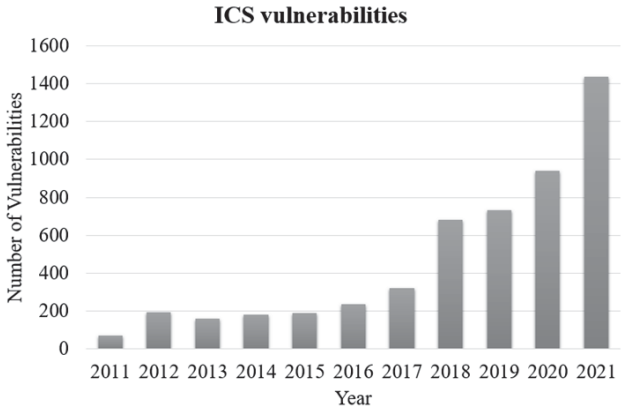

Fig. 1. Year-wise number of ICS vulnerabilities [9] [10]

For ICS, availability takes precedence; hence, installing a patch can cause system downtime, which may not be viable compared to IT. Frequently, systems are left in the field for more than a decade after their service support time period has expired. Hence, vulnerability discovery in older ICS components is still relevant due to the long life cycle of ICS components. Patching security flaws i n e xtensive a nd sophisticated systems is a tremendously tricky process requiring several stakeholders to make interdependent technological decisions [11]. Another critical aspect is the third party or open-source libraries used in codes. Fixes applied to these libraries may not always propagate to ICS components. Consider the example of the recent [12] Log4j vulnerability. It was present within a library used by many applications. Major OT vendors have published advisories about the impact of Log4j on their assets. This vulnerability can allow adversaries to execute remote code using specially crafted packets. Open-source or third

party library usage in the application development should be done with care, and proper updates of those libraries need to be done. ICS has seen several attacks that exploited device level flaws [13] [14] [15]. 2010, Stuxnet used five Zero-day and one N-Day vulnerability to exploit Natanz nuclear enrichment facility. While Zero-day vulnerabilities are uncommon, they can be used by determined attackers against what they believe to be vital targets [16]. In December 2016, a Ukrainian power outage was due to Industroyer malware, which exploited known vulnerability CVE-2015-5374 to cause DoS conditions to the Siemens SIPROTEC relays [17]. The attacker took advantage of known vulnerabilities in the case of WannaCry and NotPetya to access their systems and compromise multiple devices. In the "Kemuri" Water Company incident, an unpatched SQL injection vulnerability was exploited by adversaries [18]. The Early detection and patching of those vulnerabilities can help to strengthen the security of ICS.

B. Impact of cyber attack on the water system

Malicious activity can affect water system operations in various ways, with possibly substantial effects on public well being and the atmosphere. Some examples of such attacks are:

1) Changing chemical dosing in water treatment plants.
2) Unauthorized instructions variations in local processors which permit malicious users to take control of complete water systems potentially resulting in an unwanted unprocessed overflow of water sewage into channels.
3) Changing or deactivating the alarm threshold, which could delay exposure to malicious activity or water pollution.
4) Compromise system website.
5) Install warm like ransomware, which can deactivate complete or part of the system or process.

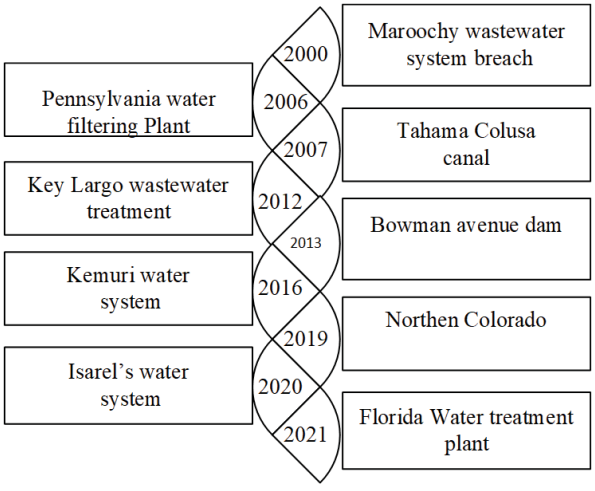

Fig. 2. History of cyber attack on the Water system

Several events have occurred in the past, compromising the functionality of water systems. Fig. 3 presents the timelines of major events. In the Maroochy breach case [19] ex-employee with physical access sent fake commands to the pumping station. Hackers in 2006 Pennsylvania [20] compromised the computer and used it to spread emails rather than targeting the control system. Another case where an ex-employee installed malware, with unkown impact occured in 2007, Tehama Colusa canal incident [21]. In 2012 Florida wastewater treatment plant [22] stolen credentials were utilized to modify, and delete information in districts' computer systems. Hackers targeted the computer system controlling the Bowman Avenue dam in 2013 [23]. Remote access was taken by the attacker of the PLC responsible to change the chemical level in 2016, Kemuri water case [24]. Ransomware attack locked out of essential technical and engineering information in the case of Northern Coloradoan, 2019 [25]. Israel's government requested its water utility companies to change their password, and operate the system offline for some time after discovering intrusion activities [26]. In February 2021, Florida's water treatment plant exploitation was an example of such a sneaky attack [27]. The perpetrator made an attempt to raise the concentration of sodium hydroxide to a point where it would have been hazardous to the residents. The intrusions were through an open Windows 7 obsolete operating system with a shared password for all computer systems at a plant, and the absence of a firewall. Additionally, the systems were connected directly to the internet. By examining the specifics of the vulnerability exploited by an attacker, it is abundantly evident that standard security methods like in IT are not followed in OT. In March, July, and August 2021, attackers launched ransomware attacks against various water treatment plants in the United States of America, specifically in Nevada, Maine, and California. In each of the three incidents, attackers gained access to the SCADA system at the water treatment plant, enabling administrators to monitor the facilities remotely. These types of attacks can potentially disrupt the water system's ability to supply clean, safe water, resulting in economic and legal consequences. The varied nature of the water industry, with its disparate sizes, unorganized regulatory structure, and the absence of cyber security governance standards, all contribute to substantial cyber security problems.

C. Literature review

General ICS systems consist of Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Supervisory Computers, Human Machine Interface (HMI), alarm systems, sensors, actuators, and communication links connecting them. ICS have a different standard protocol for their data communication. ICS primary design goals are safety and real-time monitoring of process parameters. The merging of IT and OT exposes the end devices to a new type of attack vectors [28] [29]. Normally, the attacker penetrates through the network and stops or modifies level 1 devices in the Purdue model [30] like PLC, RTUs parameters, and the network services. A study published in [31] demonstrates how an attacker might get sufficient knowledge of the ICS software by exploiting WinDbg vulnerabilities to manipulate an S7 PLC maliciously. Threat models and corresponding security controls are proposed for different IoT networks by

identifying device level vulnerabilities. Its practicality is illustrated through several scenario based tailored case studies in [32]. Various research and testbed facilities are available, that explore system weaknesses and their influence on the system. The SCADASim testbed used in [29] mimics ICS functions, and attack vectors DoS, Man in The Middle (MiTM), eavesdropping, and spoofing were investigated throughout the study. Testbed for Analysing Security of SCADA Control System (TASSCS), consisting of simulated level 1 devices (RTU, PLC) interacting through Modbus and DNP3 protocol, power system simulator, and OPNET. The objective was to defend SCADA systems against a variety of cyber attacks through the use of evaluation methods such as detection rate, false warnings, and monitoring [33]. The testbed for water system security are the Secure Water Treatment (SWaT) testbed [34] and water distribution testbed (WADI) [35], both deployed at iTrust center for research of the Singapore University of Technology and Design. SWaT testbed, the study is focused on attack detection algorithms, their effectiveness, and the cascade repercussions of ICS failure. The WADI testbed was utilized for security analysis, determining the mechanism for detecting threats, and the impact of an attack on the water distribution network. The work done in [35] is based on a concept that quantifies the effect of attacks on ICS by examining the behaviour of water distribution networks. It consists of an attack model for detecting potentially vulnerable system components and a MATLAB toolbox for studying the attack's time and duration specification. In the [36], the author developed unique MitM attack protection approaches to reduce data loss by leveraging algorithms performed in a virtual environment to simulate real-time events. SCADAVT is a Modbus/TCP based virtual SCADA model testing platform. An EPANET server is used to establish a testbed physical process to represent water distribution networks. The testbed is subjected to DoS and command manipulation attacks [37]. In [38], the author has proposed a risk analysis process for newly published vulnerabilities from an information systems perspective and presents a novel method to automatically predict the CVSS (Common Vulnerability Scoring System) vector of newly disclosed vulnerabilities.

D. Research gap

The literature studied focused on MiTM, DoS resource exhaustion, spoofing and eavesdropping attacks, and algorithm to detect and prevent them for ICS. The study performed in [32] proposes a threat vector and mitigation through a theoretical case study for the home, healthcare, and commerce domains by considering device level vulnerabilities. The impact of the N-Day vulnerability on ICS systems has not been thoroughly studied. Also, there is a lack of research evaluating the influence of public domain information on ICS exploitation and the possible attack on one device utilizing the POC of another device. A recent cyber attack at a Florida water treatment facility in February 2021, in which the amount of chemical dosing was remotely altered to a dangerous level, could potentially harm the health of the people. Hence, it is essential to evaluate security threats associated with the water system.

E. Contribution

The authors performed various cyber attacks using open-source tools and N-Day vulnerabilities on WWTP by exploiting the software, communication protocol, and hardware of the system. This paper demonstrates using WWTP how an adversary might attack ICS systems which can impact the availability, integrity, and confidentiality of the system using publically available information. Open-Source Intelligence (OSINT) framework is a methodology that unifies data, procedures, methodologies, tools, and strategies in order to assist the security team in properly identifying information regarding an adversary or their actions. Open-source information is a double edged sword. It is as easy for threat actors and adversary groups to gain access as it is for cyber security professionals and the intelligence community to use it for protecting the system. The major contributions of work are:

- The paper enlists types of ICS attacks in brief and their impact on the water system.
- WWTP security exploitation using publicly known system vulnerabilities. Based on our findings, the CVE-2021-33824 advisory was updated by Moxa.
- Examines the potential for device exploitation using a publicly available POC of a different device. This is demonstrated by exploiting the Moxa MB3480 gateway using public advisory CVE-2017-16740 published for Micrologix 1400 PLC.
- Threat mapping of attacks utilizing CIA and STRIDE threat models to assess their impact.
- Common Weakness Enumeration (CWE) is a universal online dictionary of categories for weaknesses and vulnerabilities in hardware and software maintained and updated by the MITRE Corporation. Through Modbus protocol vulnerability analysis, it was concluded that detailed ICS protocol fuzz testing at the vendor end could help to mitigate vulnerabilities like CWE-754 (Improper Check for Unusual or Exceptional), CWE-20 (Improper Input Validation).

F. Organization of Paper

The paper is structured as follows. Section 1 provides background, a literature review, and the impact of cyber attacks on water systems. Section 2 enlists typical ICS attacks in brief. In Section 3, the WWTP testbed used for the study is described. In Section 4 real-time practical exploitation of WWTP using different attack vectors and its implication in terms of CIA triad, and STRIDE threat modelling is presented. Section 5 provides observation and mitigation techniques. Moreover, the study highlights Tactics, Techniques, and Procedures (TTPs) used by adversaries to attack ICS systems.

II. ICS ATTACK

A. Typical ICS attacks

ICS are complex systems comprised of various system components, hence, have significant potential for exploitation

of asset specific vulnerabilities or misconfigurations. Physical based attacks aim to disrupt and harm physical processes, whereas network based attacks primarily target communication protocols and policies. Software based attacks exploits flaws in programs. Network based attacks provide entry opportunities, which can be followed by software vulnerability exploitation. Figure 2 shows types of ICS attacks and methods utilized.

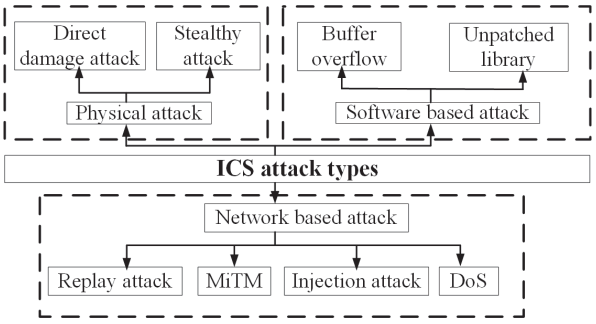

Fig. 3. Types of attacks on ICS

1) Physical Based attack: This attack alters the system's physical process. An attacker can launch such an attack after gaining access to the system via network based methods. Stealthy attacks and direct damage attacks are examples of a physical based attacks. In a security incident, the goal is to prevent an out of range data element (i.e., value change) from reaching a destination endpoint, which can result in undesirable physical action.

- Stealthy attacks aim to create small distresses in the system resulting in long term damages. This class of attacks is usually challenging to discover. A classic example of such an attack is Stuxnet on the Iranian nuclear enrichment plant resulted in centrifuges spinning faster than their regular operation routine, to the point of damaging them. For a long time, the victims were unaware that the physical damage to centrifuges was caused due to a computer virus and not due to physical wear and tear.
- Direct damage attacks disrupt the whole process by introducing a high degree of process discrepancies that make the system unsafe. Therefore, such attacks are of severe concern for causing damage to human life and the environment.

2) Software-based attacks: They are present due to a lack of security features of low quality code in the product or program, which causes it to behave insecurely. A sophisticated and large application has a greater chance of being insecure. Especially for applications using third party libraries, a sanity check is required before using them in the system. Two main categories of software based attacks due to buffer overflow and shared library vulnerabilities.

- Buffer overflow is an irregularity where a software program while writing data, overruns the buffer's capacity and then corrupts or overwrites the factual data or program. Buffer overflow arises from a lack of input validation which facilitates cross site scripting, path traversal vulnerability, and command injection. A method must be in place to ensure that the input is validated and does not permit a malicious user to access unauthorized privilege escalation.
- Third party library flaws They are used by many applications. vulnerability in the shared library propagates to the application using it. As discussed with the example of Log4j it's tough in the case of ICS assets to identify and fix such bugs.

3) Network-based Attack: There are many malicious activities that an unauthorized user can perform having access to the ICS network. They are

- Reconnaissance attack this category of attacks can be performed using different active and passive methods to identify a potential target within the system. The attacker conducts reconnaissance activities for several months before any ICS attack. Hence, monitoring network activity is vital to catch and break such reconnaissance activity.
- MiTM attack can help the attacker read, modify, command injection, packet drop any communication happening between two system components. It can modify the operating threshold of some devices, which can result in disturbing normal system behaviour to cause damage to the end user or the system itself.
- An injection attack can perform actions aiming to inject the system with malicious data, such as passing incorrect sensor reading to a SCADA targeting system or performing command injection targeting actuators. When attacks are on ICS components, it is difficult to determine whether legitimate or malicious users carried out the command due to IP spoofing in such an attack.
- Replay attack sends a legal message that has been captured by performing sniffing the communication between two system components can lead to breakdowns of the system.
- DoS attacks are the most dangerous attack in the case of ICS, resulting in system resource unavailability. The most common method used to perform DoS is TCP, UDP, or ICMP packet flooding. In most cases, the end device is unavailable during the attack; it resumes operation post attacks, but as the ICS, continuous availability is essential for defense against such attacks. Many studies are done in the literature to analyze system performance under system level and device level DoS attacks. It can be also due to ping of death where instead of exhausting the system resources by flooding a single packet can change the device state to fault/off state.

III. Target system

The purpose of WWTP is to treat industrial and human sewage in a way that allows their disposal without causing any health hazard to the environment, humans, and animals. The main methods are the precipitation of impurities, parting of solids from the liquid, and PH regulation. The effectiveness of

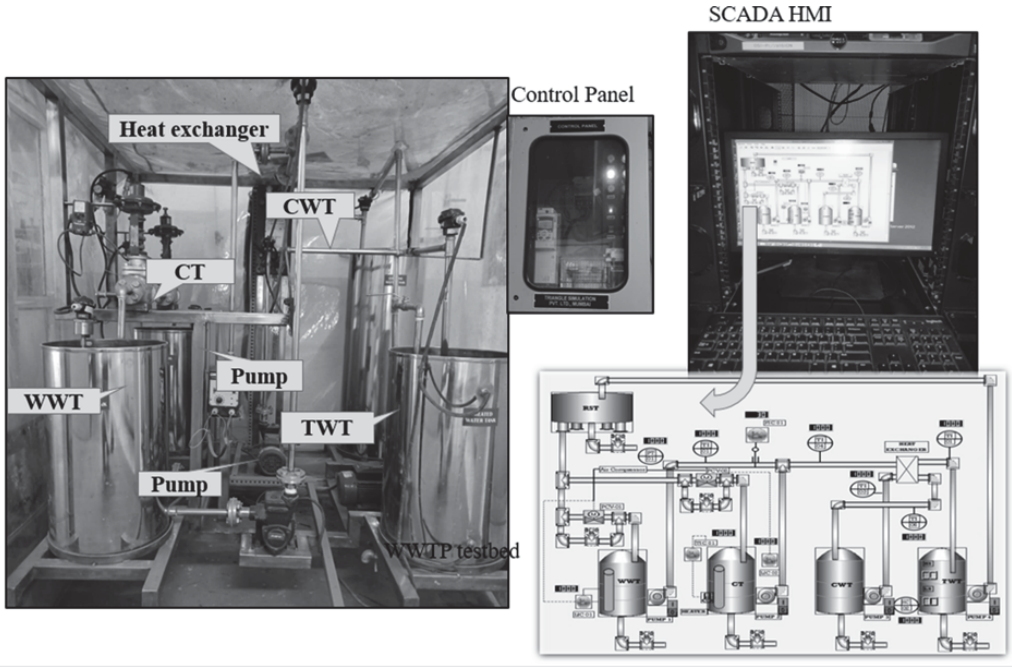

Fig. 4. WWTP testbed

the system highly depends on the reagents dosed precisely either in continuous or batch processes. The process is managed with the help of a flow based chemical dosing SCADA system which controls its amount to maintain a threshold. Figure 4 shows WWTP used for the study Testbed comprises five tank names Waste Water Tank (WWT), Chemical Tank (CT), Cooling Water Tank (CWT), Reservoir Tank (RT), and Treated Water Tank (TWT). Dosing of chemicals is done with the help of a dosing pump. A three phased centrifugal pump is used is operated using Variable Frequency Drive (VFD). VFD also operates a WWT outlet pump and cooling water, handled using a cooling water pump. A dosing pump is used to add chemicals in process steam from CT. TWT has low level and high level switches, depending on its status, the treated water pump operates. After the addition of chemicals, the temperature of the process fluid increases, which is then, cooled using the circulation of chilled water, then passed to TWT. The liquid from TWT is sent back to the RT. All the operations of motors and, pumps are through PLC and a gateway that is controlled and monitored using iVisionMax SCADA. WWTP testbed replicates industrial grade automation system with components at, Level 0 industry grade motor, relay, and pump; Level 1 Micrologix 1400 PLC and Moxa MB3480 Gateway; and Level 2 consists of iVisonMax SCADA.

IV. WWTP Testbed exploitation

The system can be compromised through vulnerability using various ways, to alter chemical set point, which would affect the quality of water; another can be DoS attack, which will make the PLC or Gateway unavailable for any communication. Authors have exploited vulnerability using OSINT, open-source tools (Wireshark, SMOD, nmap, Modbus poll, Modbus fuzzer, Metasploit) with in-house developed scripts and publicly available information. Figure 5 depicts the components of the WWTP at levels 0, 1, and 2, as well as a probable attack scenario. The attack vector 1 denotes a physical layer attack that an attacker can carry out with direct access to level 0 components. The second attack vector targets the communication link between the level 1, and level 0 components, allowing an attacker to compromise sensor readings or actuator commands. Attacks 3 and 4 are device level attacks, which allow an attacker to modify the configuration of the devices. Attack 5 compromises the communication link between SCADA and level devices, resulting in the loss of control via SCADA.

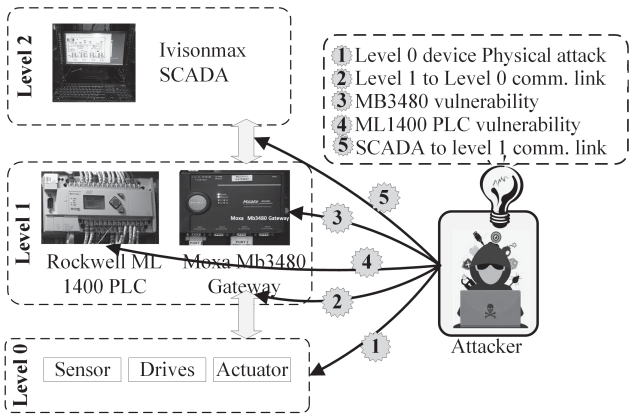

Fig. 5. WWTP testbed network component

For exploiting the WWTP system, the first step after getting

network access is to discover assets, their model, and firmware version. Adversaries can perform this reconnaissance activity using different methods like eavesdropping communication or network command. Micrologix 1400 and Moxa, both have a web server. When the user login webpage is opened, it shows complete device details on the homepage without authorized login as shown in Fig. 6. Information can also be extracted using the snmpwalk command. Device information is discovered as 1) PLC, ML1400 B, Rockwell Automation, Firmware 21.02 and 2) Moxa MB3480 Gateway, Firmware 2.6. The following section describes the execution method (EM) to perform the exploitation using public advisory (PA) and its corresponding common weakness enumeration (CWE).

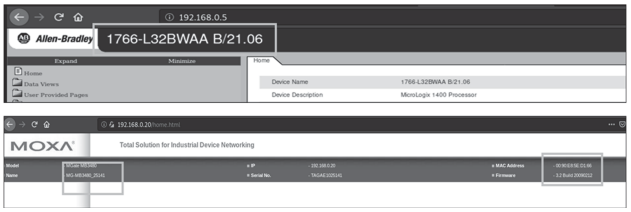

Fig. 6. Webserver page of Micrologix 1400 and Moxa MB3480

A. Attack scenario: Exploiting SNMP command

Micrologix 1400 PLC firmware flashing is performed through the specific simple network management protocol (SNMP) commands using control flash software. It uses SNMP commands to set object identifier (OID) firmware file name, IP address of the device from that the firmware file to be accessed, and a start firmware flashing command to begin the process.

-snmpset –c private -v 1 192.168.0.5 1.3.6.1.4.1.95.2.2.1.1.2.0 s “firmware.bin”

-snmpset -c private -v 1 192.168.0.5 1.3.6.1.4.1.95.2.2.1.1.1.0 a ”192.168.0.171”

-snmpset -c private -v 1 192.168.0.5 1.3.6.1.4.1.95.2.3.1.1.1.1.0 i 2

1) PLC power cycle:

- EM: A single SNMP packet can trigger the power cycle of the PLC. Its a third packet from the sequence of SNMP command send during firmware update process. Few OIDs were modified using the SNMP command, which remains unchanged even after doing firmware changes. These variables do not cause any direct harm to a running process, but these OID details are available on the webserver, so an unauthorized user can put a misguiding message on the webserver. Figure 7 shows device location OID modified using SNMP command [39].
- PA: CVE-2017-12090
- CWE ID: CWE-284, uncontrolled resource consumption

2) PLC firmware modification :

- EM:The only check is done to validate firmware in ML1400 PLC uses only checksum. Hence, it is possible to modify the firmware file as long as the net sum of any changes made is zero. This modified firmware can be uploaded using SNMP command explained in PLC power cycle section [40].
- PA: CVE-2016-5646
- CWE ID: CWE-284, Improper access control

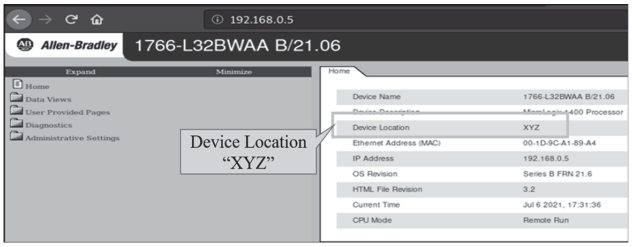

Fig. 7. Micrologix 1400 webserver OID modified “Device Location

B. Attack Scenario: Password discovery

1) Accessing password-protected ML 1400 PLC ladder logic:

- EM:By requesting specific bytes from the data file from the Micrologix 1400 PLC, it returns the master password. The software used to program ML 1400 PLC, RSLogix 500, has a weak password policy. If the encryption option is not selected it stores the password in clear text which can be discovered easily. If such a weakly password-protected PLC ladder logic file is intercepted by an unauthorized user can reveal project-related details [41].
- PA:CVE-2017-14472
- CWE ID:CWE-284, Improper access control

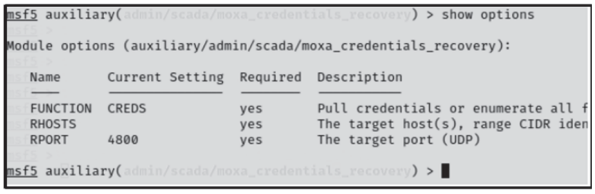

Fig. 8. Moxa MB3480 credential recovery exploit

2) Moxa MB3480 root password exposure:

- EM: Moxa MB3480 Gateway uses a protocol that is susceptible to unauthenticated credential retrieval. The device listens on 4800/UDP and will respond to direct traffic. The susceptible protocol is utilized by many lines and Moxa applications in order to manage and configure devices. In Moxa Gateway MB3480. admin credentials can be retrieved without authentication using metaspoilt as shown in Figure 8. In WWTP VFD is controlled using a gateway, successful result of this unauthorized access provides full control on the gateway functionality, the configuration of the device was changed which modified the command to VFD. Changing the device’s IP address, resulting in the device’s unavailability for any communication by SCADA. Script used:

auxiliary/admin/scada/moxa credentials recovery

- PA:CVE-2016-9637
- CWE ID:CWE-521 weak password requirement, CWE-255, credential management errors

C. Attack scenario: PLC fault state

- EM: PLC uses different data types to store values. When float value was set to 0cfffffffff PLC enters into fault state as shown in Figure 9. This value needs to be cleared via manual intervention, till cleared the PLC remains into fault state and unavailable for WWTP operation. [41].
- PA:CVE-2017-14470
- CWE ID: CWE-285, Improper authorization

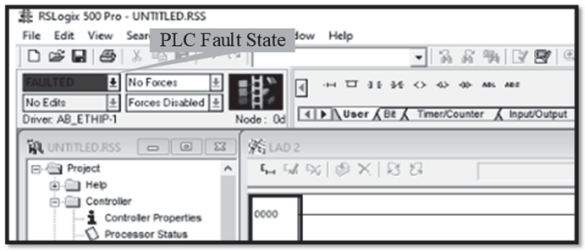

Fig. 9. Micrologix 1400 PLC in a fault state

D. Attack Scenario: Ladder logic deletion

- EM:If a packet containing multiple of 24 null bytes sent is sent to PLC over port 44818/TCP, it will cause the PLC to power cycle, enter a fault state, and clear the existing ladder logic. The device will additionally follow the same crash procedure if there is a before the crash section. No authentication over a network is required to execute this vulnerability. [42].
- PA: CVE-2017-12088
- CWE ID: CWE-285, Improper authorization

E. Attack scenario: DoS

1) DoS - ML 1400 PLC resource exhaustion :

- EM: This vulnerability exists in the session connection functionality of ML1400 PLC. By default, PLC supports ten simultaneous connections only, if this maximum number is reached, it will terminate the oldest connection to accepting the new connections. When numerous 'Register Session' packets were sent, legitimate connections were broken and it also prevent any new genuine connections to the PLC [43].
- PA: CVE-2017-12093
- CWE ID:CWE-410, insufficient resource pool

2) Moxa MB3480 Gateway web server DoS) :

- EM: As part of analyzing the different vulnerabilities of Moxa devices, CVE-2021-33824 was studied. The CVE description contained DoS service for Moxa MB3180 vulnerability. POC for the same was available [48]. On executing the same POC on Moxa MB3480 we found the same DoS result. The finding was submitted to Moxa, and accordingly, Moxa updated the public advisory to include Moxa MB3480 in the affected product list. [44].
- PA: CVE-2021-33823
- CWE-400, Uncontrolled resource consumption

Transaction ID	Protocol ID	Length	Unit ID	Functional Code	Data

Fig. 10. Modbus TCP/IP packet structure

F. Attack scenario: Buffer overflow

- EM: Micrologix 1400 PLC is configured to communicate over Modbus TCP protocol. Modbus packet structure consists of the Transaction ID to associate appeal near one-another, the Protocol ID helps to display the protocol is being used mostly it is 00, the Length to understand the extent of the request followed by, the unit id to identify communication is intended to whom, function to indicate the type of operation, and lastly the data as shown in Figure 10. When a Modbus packet with a length greater than 255 is sent, it results in a buffer overflow. This vulnerability was disclosed in CVE-2017-16740. Packets sent with length field 255, having only six bytes followed by incomplete packet 2 with length filed as six [45].
  packet1[] = "0000000000ff001500000000";
  packet2[] = "00000000000601";
  These two packets sent to Micrologix 1400 PLC resulted in a buffer overflow. When the same packets were sent to Moxa MB3480 gateway, the same result was observed. Vulnerability is mitigated for both devices with a firmware upgrade. Figure 11 shows Wireshark capture of two packets sent to Moxa MB3480 gateway. Source IP is "192.168.0.171", and Gateway IP is "192.168.0.20". Packet no 115 and 118 are the two buffer overflow packet sent to the Moxa gateway from the attacker kali machine. As seen from packet 131 Moxa gateway becomes unresponsive.
- PA: CVE-2017-16740
- CWE-119, Improper restriction, CWE-120, buffer copy without checking input

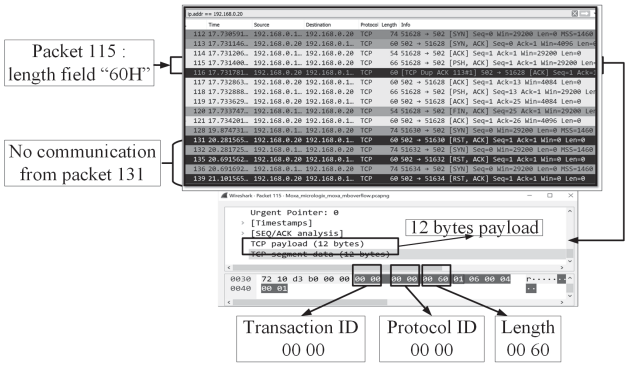

Fig. 11. Moxa MB3480 buffer overflow Wireshark capture

G. Attack scenario: Modification of network configuration

- EM: PLC controls various operations like managing the dosing pump, we could make changes to enable disable different protocols like SNMP, and Modbus. Method helped to modify network parameters, IP addresses. After performing this attack, PLC was unavailable for any communication through SCADA, while it continues to control the level 0 devices. Any command through SCADA for changing dosing level or start-stop command was unsuccessful [41].
- PA: CVE-2017-14462
- CWE-285, Improper authorization

Apart from exploiting WWTP using published vulnerabilities, insecure Modbus TCP Communication was exploited. The Modbus TCP protocol communicates in clear text, allowing an unauthorized user to comprehend the specifics of process directives and status information.

```
if (ip.proto == TCP && tcp.dst == 502) {
        if (search(DATA.data, "\xff\x00")) {
                msg("Found Modbus packet.....");
                replace("\xff\x00", "\x00\x00");
        }
}
```

Fig. 12. Ettercap filter to replace “ff” with “00”

- DoS: By sending a large amount of Modbus packets to the controller, it was possible to stop the communication with SCADA.
- Malicious command injection: By using a python script, malicious commands were sent to the controller, through which it stopped the function of a dosing pump. Due to lack of authorization, an attacker with network access can exploit this and disturb the system.
- Fuzzing, using open-source tool SMOD, writeAllRegister, writeSingleCoils were executed. It exposed all the process data details, which can be harmful if accessed by an unauthorized user.
- MiTM: By using the open-source Ettercap tool, the command given to PLC by SCADA was modified. Fig.12 shows the Ettercap filter file used to perform MiTM attack.

Threat modeling is an invaluable tool to achieve the ultimate purpose of a threat intelligence program for accurate documentation and reporting of threats. A good threat intelligence report helps the security defense and operations teams protect assets from threats and weaknesses. Fig. 13 presents a summary of the attack vector and its impact on WWTP in terms of the CIA (Confidentiality, Integrity, and Availability) triad. The goal of STRIDE threat modeling is to present the security measures which need to be taken based on the current information systems and threat landscape, as well as the most likely attacks, their methodology, motive, and target system which can be used to make more secure products and applications.

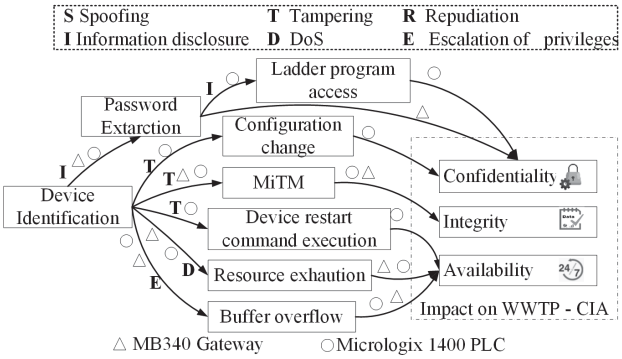

Fig. 13. Attack vector on WWTP and CIA, STRIDE threat modeling mapping

V. Observation and Mitigation Technique

Through this exploitation study, vulnerabilities related to software, as well as hardware, were used to create a cyber-physical attack on WWTP testbed. The impact of exploited vulnerability was analyzed. Any attacker with a low skill level using open-source tools can exploit it. Through the webserver, initially, the device model and firmware were identified, and later exploit was created to find the password of Micrologix 1400 PLC and Moxa MB3480 gateway. Through the password identified f or M icrologix 1 400 P LC, t he PLC ladder logic file w as e xposed t o fi nd th e cr itical va lue of chemical dosing. Through MiTM, we modified t he value. Eventually, the battle will require constant vigilance for new vulnerability discoveries and the applying fresh patches to address them. For ICS, patches are avoided due to the critical nature of maintaining the system’s availability. Modbus is the oldest OT protocol, there still exist many Modbus related vulnerabilities; a few recent vulnerabilities are mentioned in Table 1 [46]. On analysis, it was found that the vulnerabilities were due to a specific M odbus p acket, w hich compromises the standard rule of Modbus Packet format of length, allowed range of values sent out of bound mishandled by the device. Hence, device level protocol related fuzz testing performed methodically at the vendor sito can help to overcome such vulnerabilities. Fig. 14 highlights some proactive techniques proposed to enhance the security of ICS SCADA systems based on standard practices.

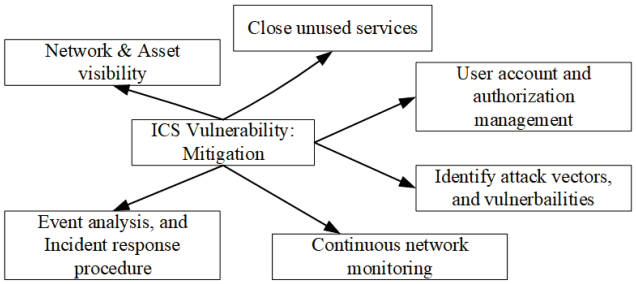

Fig. 14. ICS protection techniques

It can help manage weaknesses and avoid exploits when patches cannot be instantly deployed [47]. Vulnerabilities represent a significant risk to ICS. To mitigate the threat, end users must implement a number of preventive steps. A more proactive approach can be adopted by developers by applying security by design.

VI. Conclusion and Future Scope

The field of ICS security is intricate, and the result of implementing insufficient controls may have substantial consequences. Our findings give effective aspects for future research aimed at exposing underlying problems in present models and ultimately improving them. We demonstrate through extensive experiment findings that simple physical adversarial examples are easily realizable to develop assaults akin to the Florida water treatment facility attack (2021). Our observation also presents a practical example of a device specific buffer overflow vulnerability that can be leveraged to exploit devices from another vendor. Modbus protocol vulnerability highlights the need for deep study and fuzzing methods for ICS communication protocols, which can help to discover the protocol based vulnerability. The threat landscape present due to publicly available POC persists, which needs to be addressed. It is worth noting that Moxa has confirmed the vulnerabilities we reported and updated the corresponding advisory. As ICS systems remain unchanged for decades, finding vulnerabilities in older devices' firmware remains relevant. Future work is aimed at applying these vulnerability exploitation techniques and creating a framework for penetration testing of ICS assets.

VII. Acknowledgement

The authors wish to express their gratitude to CoE CNDS (Centre of Excellence-Complex and Non-linear dynamic systems) laboratory, VJTI, Mumbai, for providing support through cutting-edge research facility.

References

[1] G. Yadav and K. Paul, "Architecture and security of scada systems: A review," *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100433, 2021.

[2] M. R. Asghar, Q. Hu, and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies, and challenges," *Computer Networks*, vol. 165, p. 106946, 2019.

[3] K. K. Singh, A. Nayyar, S. Tanwar, and M. Abouhawwash, "Emergence of cyber physical system and iot in smart automation and robotics."

[4] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Computers Security*, vol. 25, no. 7, pp. 498–506, 2006.

[5] Y. Maleh, "It/ot convergence and cyber security," *Computer Fraud Security*, vol. 2021, no. 12, pp. 13–16, 2021.

[6] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on scada systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[7] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2013.

[8] C. Singleton, "X-force threat intelligence index 2021," pp. 43–5, 2021.

[9] U. ICS-CERT, "Year in review 2016," 2016.

[10] Claroty, Team 82, "Claroty Biannual ICS risk vulnerability report: 2H 2021." [Online]. Available: https://claroty.com/wp-content/uploads/2022/03/Claroty-Biannual-Report-2H-2021.pdf

[11] N. Dissanayake, A. Jayatilaka, M. Zahedi, and M. A. Babar, "Software security patch management-a systematic literature review of challenges, approaches, tools and practices," *Information and Software Technology*, vol. 144, p. 106771, 2022.

[12] R. Hiesgen, M. Nawrocki, T. C. Schmidt, and M. Wählisch, "The race to the vulnerable: Measuring the log4j shell incident," 2022.

[13] N. Ayres and L. A. Maglaras, "Cyberterrorism targeting the general public through social media," *Security and Communication Networks*, vol. 9, no. 15, pp. 2864–2875, 2016.

[14] K. E. Hemsley, E. Fisher *et al.*, "History of industrial control system cyber incidents," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2018.

[15] A. Hassanzadeh, A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld, and K. Banks, "A review of cybersecurity incidents in the water sector," *arXiv preprint arXiv:2001.11144*, 2020.

[16] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[17] J. Slowik, "Crashoverride: Reassessing the 2016 ukraine electric power event as a protection-focused attack," 2019.

[18] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Computer Communications*, vol. 155, pp. 1–8, 2020.

[19] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *International conference on critical infrastructure protection*. Springer, 2007, pp. 73–82.

[20] J. Lowe, J. Lasky, D. Gilbert, and K. Sheil, "Protecting industrial process control, automation and scada systems from cyber threats," OnePetro, 2007.

[21] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems," p. 100464, 2021.

[22] A. Hassanzadeh, A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld, and K. Banks, "A review of cybersecurity incidents in the water sector," 2020.

[23] BBC News, "Iranian hackers 'targeted' New York dam," 2015. [Online]. Available: https://www.bbc.com/news/technology-35151492

[24] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for iot-based smart grid networks," pp. 36–49, 2019.

[25] P. Ferrier, "Cyberattacker demands ransom from northern colorado utility," 2019.

[26] S. Mansfield-Devine, "Nation-state attacks: the escalating menace," pp. 12–17, 2020.

[27] J. Cervini, A. Rubin, and L. Watkins, "Don't drink the cyber: Extrapolating the possibilities of oldsmar's water treatment cyberattack," pp. 19–25, 2022.

[28] V. Urias, B. Van Leeuwen, and B. Richardson, "Supervisory command and data acquisition (scada) system cyber security analysis using a live, virtual, and constructive (lvc) testbed," in *Milcom 2012-2012 ieee military communications conference*. IEEE, 2012, pp. 1–8.

[29] G. Bernieri, F. Del Moro, L. Faramondi, and F. Pascucci, "A testbed for integrated fault diagnosis and cyber security investigation," in *2016 International Conference on Control, Decision and Information Technologies (CoDIT)*. IEEE, 2016, pp. 454–459.

[30] T. J. Williams, "The purdue enterprise reference architecture," *Computers in industry*, vol. 24, no. 2-3, pp. 141–158, 1994.

[31] H. Hui, K. McLaughlin, and S. Sezer, "Vulnerability analysis of s7 plcs: Manipulating the security mechanism," *International Journal of Critical Infrastructure Protection*, vol. 35, p. 100470, 2021.

[32] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams, "Threat model for securing internet of things (iot) network at device-level," *Internet of Things*, vol. 11, p. 100240, 2020.

[33] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "Scada system testbed for cybersecurity research using machine learning approach," *Future Internet*, vol. 10, no. 8, p. 76, 2018.

[34] A. P. Mathur and N. O. Tippenhauer, "Swat: A water treatment testbed for research and training on ics security," in *2016 international workshop on cyber-physical systems for smart water networks (CySWater)*. IEEE, 2016, pp. 31–36.

[35] C. M. Ahmed, V. R. Palleti, and A. P. Mathur, "Wadi: a water distribution testbed for research in the design of secure cyber physical systems," in *Proceedings of the 3rd international workshop on cyber-physical systems for smart water networks*, 2017, pp. 25–28.

[36] G. Narula, P. Nagrath, D. Hans, and A. Nayyar, "Novel defending and prevention technique for man-in-the-middle attacks in cyber-physical

TABLE I. RECENT MODBUS VULNERABILITIES

CVE-ID	Device Name	CVE-ID
CVE-2019-6819	Modicon M340	CWE-754
CVE-2018-7845	Modicon M340	CWE-754
CVE-2018-7844	Modicon Quantum, Modicon Premium	CWE-754
CVE-2020-7538	Schneider Electric Modbus Protocol	CWE-294
CVE-2020-7477	Simulator EcoStruxure Control Expert	CWE-754
CVE-2021-21964	SeaConnect 370W	CWE-287
CVE-2022-28613	Hitachi Energy RTU500 series	CWE-20

networks," *Cyber-Physical Systems: Foundations and Techniques*, pp. 147–177, 2022.

[37] A. Almalawi, Z. Tari, I. Khalil, and A. Fahad, "Scadavt-a framework for scada security testbed based on virtualization technology," in *38th Annual IEEE Conference on Local Computer Networks*. IEEE, 2013, pp. 639–646.

[38] C. Elbaz, L. Rilling, and C. Morin, "Fighting n-day vulnerabilities with automated cvss vector prediction at disclosure," Ph.D. dissertation, 2020.

[39] Cisco talos, "Allen Bradley Micrologix 1400 Series B SNMP-Set Processing Incorrect Behavior Order Denial of Service Vulnerability," 2018. [Online]. Available: https://talosintelligence.com/vulnerability_reports/TALOS-2017-0442

[40] Cisco Talos, "AB Rockwell Automation MicroLogix 1400 Code Execution Vulnerability," 2018. [Online]. Available: https://talosintelligence.com/vulnerability_reports/TALOS-2016-0184

[41] Cisco talos, "Cisco Talos Vulnerability Report," 2018. [Online]. Available: https://talosintelligence.com/vulnerabilityreports/TALOS-2017-0443

[42] Cisco Talos, "Allen Bradley Micrologix 1400 Series B Ethernet Card Malformed Packet Denial of Service Vulnerability," 2018. [Online]. Available: https://talosintelligence.com/vulnerability_reports/TALOS-2017-0440

[43] Cisco talos, "Allen Bradley Micrologix 1400 Series B PLC Session Communication Insufficient Resource Pool Denial of Service Vulnerability," 2018. [Online]. Available: https://talosintelligence.com/vulnerability_reports/TALOS-2017-0445

[44] Jian Xion, "Moxa CVE-POC Github," 2021. [Online]. Available: https://github.com/Jian-Xian/CVE-POC/blob/master/CVE-2021-33823.md

[45] Thiago Aleves, "Hacking PLCs and Causing Havoc on Critical Infrastructures, DEF CON 26," 2018. [Online]. Available: https://doi.org/10.5446/39750

[46] NVD, 2022. [Online]. Available: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=modbus&search_type=all&isCpeNameSearch=false

[47] A. A. Jillepalli, F. T. Sheldon, D. C. de Leon, M. Haney, and R. K. Abercrombie, "Security management of cyber physical control systems using nist sp 800-82r2," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017, pp. 1864–1870.