DISSERTATION

METHODOLOGY TO ENHANCE SECURITY OF WATER UTILITY SYSTEM THROUGH RTU HARDENING

Submitted by

Augustus William Davies

Department of Systems Engineering

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2022

Doctoral Committee:

Advisor: V.Chandrasekar

Joel Dubow
John Borky
Christopher Weinberger

Copyright by Augustus William Davies 2022

All Rights Reserved

ABSTRACT

METHODOLOGY TO ENHANCE SECURITY OF WATER UTILITY SYSTEMS THROUGH RTU HARDENING

Water utility security is becoming a focus of critical infrastructure security. The Environmental Protection Agency (EPA) and the White House recently launched a cyber security plan for the water sector [1]. “Cyberattacks represent an increasing threat to water systems and thereby the safety and security of our communities,” said EPA Administrator Michael S. Regan. “As cyber-threats become more sophisticated, we need a more coordinated and modernized approach to protecting the water systems that support access to clean and safe water in America. EPA is committed to working with our federal partners and using our authorities to support the water sector in detecting, responding to, and recovering from cyber incidents.” [1]. Yet it is not just cyberattacks. As demonstrated in this dissertation, water utilities are vulnerable to physical and human attacks.

The water utility subsystem, in direct contrast with sensors and actuators that monitor, meter, and treat water and wastewater, is the RTUs (Remote Telemetry Unit). This subsystem controls the engineering devices, meters, and control systems the water utility uses to supply water and treat wastewater. These devices are distributed within the area served by the Utility. The RTU aggregates data from the Utility operational subsystems assigned to it and transmits it to the Main Telemetry Unit (MTU) and from there to the Supervisory Control and Data Acquisition (SCADA) system. A typical Metropolitan water utility has around 100 RTU, 2 MTU, and 1 SCADA.

Preventing and reducing the impacts of exploits of RTU vulnerabilities are the focus of this study. To attain this goal, a design methodology was created that resulted in a hardened RTU that was constrained to be used within existing water utilities. The performance of the enhanced RTU was compared to the existing standard RTU under normal operating conditions and an attack. The results show the value of the enhanced RTU. The enhanced RTU responded faster, restored operations faster, and prevented physical and cyber-attacks.

ACKNOWLEDGEMENTS

First of all, I would like to thank my Lord and Savior, Jesus Christ, for everything he has done for me, always watching over me, and with him, all things are possible.

I want to thank my program advisors, Dr. Collins and Dr. Chandra, for their help for the past three years. Again, a special thanks to my committee members Dr. Weinberger and Dr. Borky, who taught me systems engineering and Advanced system model-based systems engineering and provided me with valuable knowledge as a Systems Engineer. I would also like to extend a heartfelt thanks to Ingrid Bridge for her immense administrative support throughout my studies at CSU.

A special thanks to my off-campus advisor, Dr. Dubow, for the countless hours and meetings for discussions, review of materials, and teaching me the practicality of systems engineering and cybersecurity integration in systems engineering. He has been an excellent academic advisor, counselor, and teacher during my studies at CSU. Thank you so much.

Heartfelt thanks to my parents, Anthony Davies and Beatrice Davies, all of the blessed memory, for making me who I am. To them, education is the key. A special thanks to Dr. Reginald Cann and Mrs. Theresa Cann for their support and guidance since coming to the United States.

Finally, a special thanks go to my wife Gloria for all of her support, encouragement, and patience. To my children: Augustus Jr., Benedict, Theophilus, and Beatrice, thanks so much for being with me through thick and thin.

PREFACE

The security of the water utility system is essential to the daily life of citizens. It is an integral part of the National Critical infrastructure. While this system functioned effectively for decades, it is now being attacked by outside actors who want to disrupt the water supply. These attacks are occurring with increasing frequency and intensity. This dissertation studies the system to derive ways to make it more resistant to attacks, sustain minor damage when attacked, and restore faster than possible.

The author has observed security issues with water utilities for over two decades. He spent 12 years in the Navy as an Electricians Mate First Class Petty Officer and Instrumentation specialist. He was responsible for power generation, degaussing and acoustic systems, 60 to 400 HZ converter system, Bow thruster systems, fins Stabilizer system, systems calibration and water supplies on ships ranging from mine-sweepers to aircraft carriers. In addition, he has taught and worked on water utility hardware and electronics in civilian life for four different water and wastewater utility companies and managed RTUs and SCADA. This dissertation was motivated by the growing awareness of major threats to the country's water supply and wastewater treatment. His goal was to explain the nature of these threats and develop a framework for addressing them.

After studying the system using literature review, simulations, surveys, and questionnaires from stakeholders, and personal experience as a system engineer and manager, it was concluded that the RTU is critically located near the field devices and not well protected against physical and cyber threats. Therefore, this dissertation focused on the components making up an RTU, its physical environment, and its interface to other components in the water

utility system. A constrain was to have selected components be commercially available and interoperable with existing water utility systems. The most vulnerable parts of the RTU were identified. Methods to make the RTU more resistant to attacks, more resilient to survive such attacks, and more effective communication and coordination responses within the SCADA system are evaluated to verify that this dissertation's goals were met.

Chapter 1 defines the remote telemetry unit of the SCADA, the subsystems of the RTU, and how data propagates from field devices to the RTU. The Remote Telemetry Unit (RTU) is a critical subsystem of the water utility system. The interface between the systems field components and the upstream control systems uses the RTU data to control the water supply system's operation and the communication hub at remote locations.

Chapter 2 presents a literature review of the RTU in water utility systems. It elaborates on research already conducted and published, researched RTU, MTU, SCADA, and vulnerable areas that need advanced research. The chapter explains the role of RTU in the water utility system in terms of data gathering from the field devices and how exploits of RTU by bad actors can inflict damage to water users and other infrastructure. Again, this chapter goes over the architecture and functions of RTU SCADA systems. Overview of a water utility system is discussed, the RTU's vulnerability, and what researchers have done to tighten security systems.

Chapter 3 presents the architecture and functions of RTU SCADA systems and explains the data gathering process using a survey questionnaire from field personnel working with RTU. Then, together with years of experience of the author and literature reviews, proposed changes to existing RTU designs to improve robustness, resilience, and response time. Furthermore, this chapter presents the history of the RTU water system and how improving RTU security will significantly improve water utility system security, reliability, and resilience. Hence, the reason

for the focus of the RTU in this research. Lastly, chapter 3 describes the choice and validation of the research topic and the need to enhance RTU designs in water utility systems using MBSE methodology.

Chapter 4 applies MBSE methodology to develop a conceptual design for an enhanced RTU. Chapter 4 further indicates that many existing RTUs can be upgraded at a reasonable cost. Finally, the design goal benefits were stated, including emergency alerts to the local law enforcement, control room operator, and stakeholders for quicker response time, restoration time, and forensic data.

Chapter 5 describes component selection for the enhanced RTU design, prioritizing commercially available components that will fit in and interoperate with existing RTUs and water utility systems. Furthermore, Chapter 5 explains the differences between the existing RTU and the enhanced RTU components.

Chapter 6 compares the response of the existing RTU to that of the Enhanced RTU when a water utility is under physical attack, cyber-attack, or a combination of attacks looking at the system from different behavioral viewpoints, and specifically looking at the design architecture of the enhanced RTU.

Chapter 7 continued by describing the changes occurring in a system under cyber and physical attack by using a PLC ladder logic program of the type used to control utility operation formed a simulation to validate the activities of the enhanced RTU under attack.

Finally, chapter 8 describes how the enhanced RTU can be implemented in water utilities and its benefits to water utility infrastructure security.

DEDICATION

Dedicated to my dad Anthony Davies, my mother, Beatrice Davies, and my brother Joachim Davies, all of blessed memory.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1. Background

A water utility system needs to fulfill customers' water demands while ensuring water quality. Its users include homes, offices, industries, and farms. These systems have performed so reliably for so many decades that most customers are unaware of what goes on at the water treatment and distribution plants. Hence, they do not worry too much about these systems' cyber and physical security. This lack of focus on security has left water utility systems vulnerable to high-impact terrorism. This vulnerability has recently been well documented. These potential attack scenarios can, if orchestrated successfully, produce infrastructure disruption, water shortages, and even casualties on a massive scale. Studies conducted by personnel at Hach HST, Colorado State University, and the U.S. Army Corps of Engineers, among others, have shown that attacks on drinking water supplies could be mounted for between $0.05 and $5.00 per death, using rudimentary techniques, and could amass casualties in the thousands.[6]. Direct customers and connected civil infrastructure systems are quickly affected if water infrastructure is disabled.

Water supply is a distributed system, usually treated at one location (water filtration plant) and pumped to elevated storage tanks or underground storage facilities. Some water utility systems cover different altitudes and require pressure adjustment for pumping to household and industrial users.

Water utility systems usually consist of several subsystems depicted (Fig 1). First, a source of raw water such as a river, lake, or underground well to provide water for treatment and effluent is needed. Then a storage tank, a booster station, pressure-reducing valve stations (PRV), pumping stations, and distribution pipes form a water treatment and distribution network.

Each subsystem requires at least one RTU to interface with the sensors or the real-world devices (Fig. 1) to gather process variables and setpoints and communicate with SCADA through communication links.

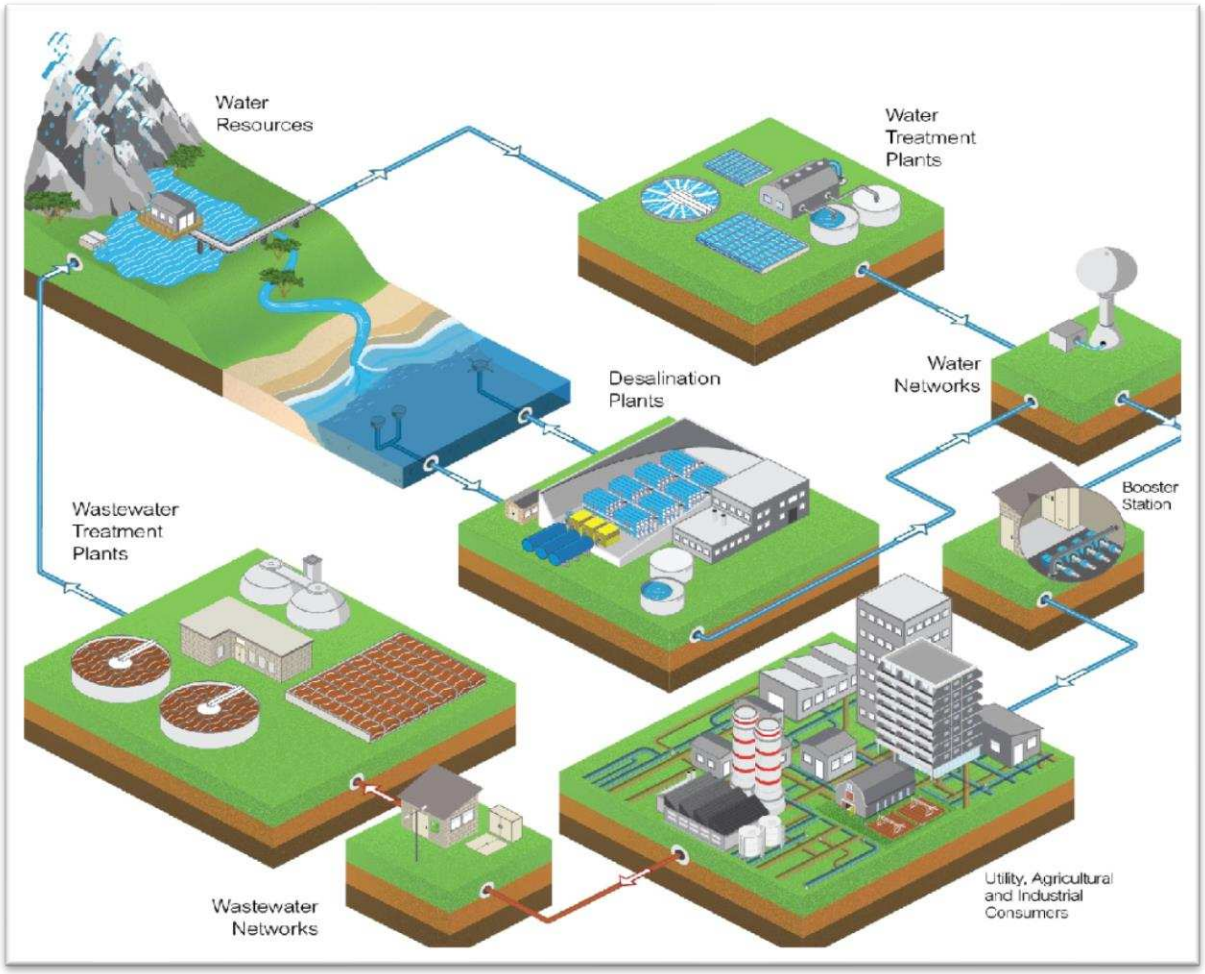


Fig. 1. Overview Water Resources & Water and Waste Water Network Diagram [32].

Data communication within a water utility starts from field sensors or actuators (fig. 1), and from there, the data is aggregated in an RTU PLC or DCS. These latter two components are located in the RTU enclosure. Next, data is aggregated and formed into a packet and transmitted to the Master Telemetry Unit (MTU) through a communication network such as an antenna, fiber optics, or microwave transmission media. Finally, the MTU level passes data to the SCADA and

from there to the Control Room Operator (CRO), who monitors alarms and arranges shutdown or throttling of processes as needed.

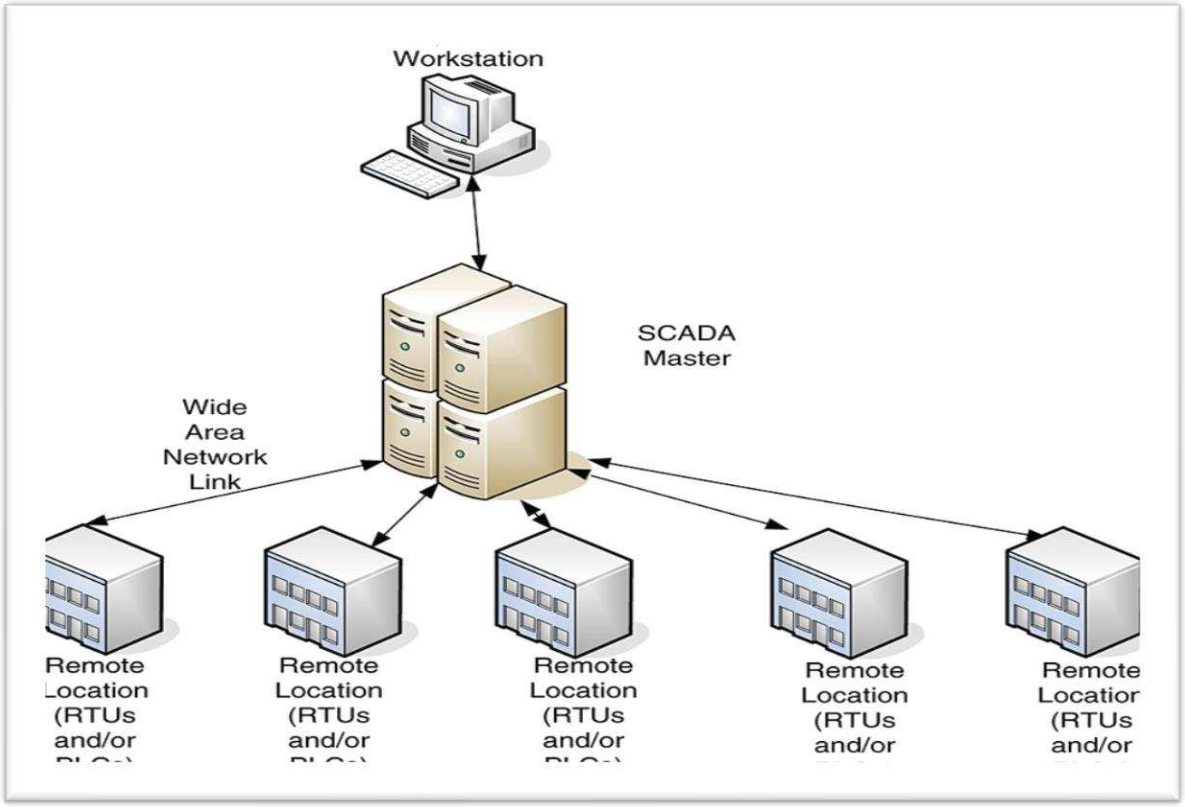


Fig. 2. Block diagram of a typical SCADA System showing RTU [33]

While there are many parts to the system, the SCADA system, and its connected components are the water treatment and handling subsystems of the Utility and are thus the primary targets for attacks to damage human and infrastructure systems. The RTU connects to the sensors and actuators and forms the eyes and ears of the system. If they are damaged, it disables the ability of the system to respond effectively to attacks or even function normally. Therefore, this dissertation will focus on the RTU since it is closest to the critical system data and is the primary target for attackers.

An RTU exploit can degrade the entire distribution system. For example, suppose an actor could access RTU components such as the RTU communication circuit or antenna radio frequency locally or remotely. In that case, the actor could control the RTU upstream data communications and send false or disruptive control signals to the associated field devices such as sensors and actuators to upset the water treatment, pumping, mixing, and purification processes.

In another example, most present-day RTUs contain Programmable Logic Controllers (PLCs) and support downloading control logic through serial communication ports. This makes the RTU vulnerable because altering or injecting commands from the program could alter controlling chemical dosage, changing other plant processes, and water utility system configurations. A hardened RTU system [25] will offer more robust alarms, management of disruptions, and data capture for post-event forensic analyses to mitigate many of these threats.

The RTUs are the eyes and ears of the water utility system. They capture sensor data from the field devices, other RTUs, field instruments, and PLCs. The RTU outputs go to MTUs (Master Terminal Unit, sometimes included inside the SCADA system), but sometimes the outputs are used to control related distributed systems.

Recent cyber-attacks on water utility systems indicate that bad actors outside the united states penetrated the networking systems [14]. Some gained access to the MTU but were unsuccessful in inflicting damage. Attempts to compromise the water supply may show up at various configuration nodes of the RTU or the MTU. The MTU is the data aggregator, data warehouse, data conditioner for all RTUs and serves as a gateway for cyberattacks attacking the RTU. The RTU can also be attacked via physical and IOT intrusions.

1.2. Water System Security Data Sources

According to the Department of Homeland Security (DHS) [26], there are about 160,000 public water systems and more than 16,000 municipal wastewater systems in the U.S. The need to protect them is urgent, and many agencies are being mobilized to address this need. Many publications have described water utility systems attacks [5]. Recent attacks on water utilities were aimed at the SCADA and the remote terminal units [12]. Prominent among the water-focused agencies facing this issue are the National Rural Water Association (NRWA), American Water Works Association (AWWA), Water Information Sharing and Analysis Center (Water-ISAC), Department of Homeland Security (DHS), and the Environmental Protection Agency (EPA). In addition, a variety of topics regarding water security are under active investigation in the Cybersecurity and Infrastructure Security Agency (CISA).

There are sixteen critical national infrastructure sectors as outlined in Presidential Policy Directive-21 (PPD-21), "Critical Infrastructure Security and Resilience," and elaborated in the 2013 NIPP [5]. Number 16 is the water and wastewater system responsible for providing drinking water and wastewater treatment under the EPA [27]. , The department of homeland security has enumerated the number and type of all these components for U.S. water utility systems as part of their National Infrastructure Protection Plan [26].

On an international level, The U.N. Sustainable Development Goals (SDG) program has stated an urgent need to conduct extensive research on emerging and future global water security issues, document these studies, and disseminate them [23].

1.3. Water Utility and Population

Generally, a water utility system consists of complex components such as pipes, pumps, reservoirs, valves, hydrants, meters, and backflow preventers critical in maintaining physical integrity [23]. Fortunately, more than 85 percent of the U.S. population receives potable water from these drinking water systems, and about 75 percent of the U.S. population has sanitary sewage treated by these wastewater systems. The remainder depends on domestic wells. Drinking water and wastewater systems are grouped into the water sector, one of 18 critical infrastructure sectors recognized by homeland security experts and officials as vital systems and networks that need protection [1, 10].

Surface sources account for 78% of all water withdrawals [18]. Overwhelmingly, most households in the United States rely heavily on water utility from local or municipality water utility systems [27]. Therefore, it is essential to keep the water demand to customers. Water treatment and distribution must be dynamic, with all the components working together while maintaining coordination between instruments, field devices, and human interactions from operators, technicians, and engineers.

Water supply must accommodate the varying elevations in the water utility area since these cause pressure drop or pressure increases, which may require a booster station to boost or increase the water pressure or PRV to reduce the pressure to avoid damages to pipelines and equipment. In addition, water utility systems receive water from water reservoirs above the supply areas, such as hills or water towers [23, 29]. Thus, maintaining secure constant static head pressure for the water to flow from tanks or reservoirs to customers requires a modern water utility.

1.4. Examples of Security Incidents and Causes

Recent attacks on water and wastewater systems have alerted the general public that the bad actors are learning the system, trying to stay ahead, devising ways to attack soft targets in the water utility system, seeking ransom money, and attempting to inflict damage destroy national assets. A more detailed description of recent attacks on water utility systems is found in chapters 6 and 7.

A Review of Cybersecurity Incidents in the Water Sector published in the Journal of Environmental Engineering 146 (2020) reviewed 15 cybersecurity incidents in the water and wastewater sector within the context of industrial network architectures and attack-defense models [28]. The incidents covered many vulnerabilities and situations and spanned over 18 years. The study presents a critical review of disclosed, documented, and malicious cybersecurity incidents in the water sector to inform safeguarding efforts against cybersecurity threats [28]. The information is valuable to system engineers and IT engineers in protecting physical and cyber security threats to the water utility systems.

Security breaches in water utility systems include those readily predicted from models and others external to the engineering or science water utility systems.

An example of the latter is when one of the authors saw a water booster pump turn on and off without activation from an operator or SCADA. An indication that the “pump has started” appeared on the SCADA display. This indication surprised the control room operators. This issue continued unmitigated for weeks until the author took charge of the situation. The author used his extensive troubleshooting experience to determine why a critical booster station that served a densely populated city malfunctioned that way.

The malfunction was contained within the water utility system and included the communication system used by the Utility and the leased phone company. It took joint coordination between the communication provider and the water utility to develop a solution. It took several weeks because it occurred intermittently (about one every week). After diagnosing the fault, the author had to explain the tone-generated signal phenomenon used to start and stop pumps at the booster station. The leased phone company was invited to the water utility booster station, where the author used test instruments to prove that the issue was coming through their lines.

Table 1. Root Cause and Corrective Solution to a Water Booster Station Unexplained Control.

Root Cause	**Corrective Solution**
4 - 20 mA Long Open cable run	Use of wireless communication, Wi-Fi, Microwave, with protected endpoints
No Cybersecurity measures	Use of systems that support cybersecurity integration, updates, Firewalls, etc. Keep security controls current.
Outdated Controls	Retire systems that cannot support cybersecurity measures.
Unprotected RTU	Replaced with Robust, Hardened RTU

A cyber exploit is exemplified by a power outage scenario lasting hours and days, especially in metropolitan areas. This electrical outage is an example of a cross-system exploit of cybersecurity threats to national infrastructures. While many critical infrastructure systems use backup power systems such as diesel generators and batteries until the regular power is restored, many distributed water supply systems do not. Furthermore, backup power systems are usually manually intensive and event-dependent. A more robust system would reduce the burden,

expense, and time of such disruptions for these events. For power issues, the effect is seen and observed quickly. However, the water utility system responds more slowly to water outages, but service resumption impacts are just as damaging to water consumers.

One of the first widely studied attacks in the water supply sector occurred in 2000 at Maroochy Water Services (Queensland, Australia). A disgruntled contractor attacked the SCADA of a sewage system, releasing almost 1 million liters of wastewater into waterways and parks [5]. Had the wastewater been released into the water supply in a metropolitan area would have caused significant damage, injuries, and death. On April 23, 2020, the Israeli National Cyber-Directorate (INCD) issued a security alert that the agency had received reports of intrusion attempts at its wastewater treatment plants, water pumping stations, and sewers SCADA systems network. However, the report did not go into detail [43]. Instead, the agency urged companies active in the energy and water sectors to change passwords for all internet-connected systems. In addition, the agency suggested that systems be taken offline until proper security measures could be implemented [43].

These incidents are monitored and made available to security stakeholders by security organizations and utilities, including the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which provides a control system security focus in collaboration with US-CERT [24, 41]. Together they conduct vulnerability and malware analyses, provide on-site support for incident response and forensic analysis, and provide situational awareness to organizations. They also offer recommended practices for control systems such as RTU and SCADA on the ICS-CERT website for integrating industrial Control Systems Cybersecurity with Defense-in-Depth Strategies [41]. modest Bowman Avenue Dam in Rye Brook

Between August 28 and September 18, 2013, hackers obtained unauthorized remote access to the SCADA system at the Bowman Avenue Dam, a small hydraulic infrastructure located at Modest Bowman Avenue Dam in Rye Brooks, New York, used to control water flow as a function of water levels and temperatures in the Blind Brook creek [28]. The hackers were able to penetrate the SCADA system but could not open the sluice gate to cause harm because the sluice gate was out of service due to maintenance. Instead, the attacker used a standalone computer of the SCADA system to access its control network, which uses IoT via a cellular modem. Gaining access to the RTU of a SCADA system can allow a hacker to manipulate setpoints and process variables to inflict damage to the water utility system [28].

According to ICS-CER, 25 water utilities reported cybersecurity incidents in 2015, making water and wastewater (WWS) the third most targeted sector [24]. Because there are 160,000 public water systems in the United States (USEPA, 2019), one may conclude that cybersecurity risk to individual WWS is low, and most systems are secure. However, many cybersecurity incidents either go undetected and consequently unreported [27] or are kept secret because doing so may jeopardize the utility victim's reputation, customers' trust, and loss of revenue. In addition, cybersecurity breaches of the SCADA system, often cyberattacks can be used to gain control of the RTU PLC controls and data logger and conditioners [3, 8, 41].

In another recent attack, hackers gained access to computers at a small Colorado water utility. The Fort Collins-Loveland Water District (FCLWD), and its wastewater counterpart, were attacked by malware that encrypts victims' computer files and demands online payment to unlock them [28]. Normal water utility operations resumed with no system damage, but the ransomware prompted the water district to switch out its information technology service provider and call the FBI. First reported by the Coloradoan [28], the case remains an active investigation.

The FCLWD and the South Fort Collins Sanitation District treat and distribute water to 45,000 customers in northern Colorado [28].

More recently, a hacker remotely accessed the Oldsmar Florida water treatment plant. The targeted system controls the chemicals added to the water to make it safe to drink. According to the local sheriff, the exploit increased sodium hydroxide - lye - from 100 parts per million to 11,100 parts per million. However, the hack was stopped by an operator who noticed the change after five and a half hours [20, 52]. The attack came through the internet via a contractor PC that accessed the plant's remote access system. Then, the attacker issued commands through the MTU, down to the RTU. From there, the commands went to the controller for adding Sodium Hydroxide to the water.

Remote terminal units are in continual contact with field devices that monitor and control the water specific processes within the water utility system. The enhanced robust RTU proposed by this dissertation will provide a faster and more granular control and field device monitoring so that future hacks are detected faster, managed more locally, and analyzed more quickly. These enhanced RTU capabilities would have helped prevent, mitigate, and provide more precise and useful data for restoring operations and attacker attribution. For larger utilities and more complex attack vectors, enhanced RTUs will be necessary. For others it will be improve security and provide proof of due diligence and due care.

This research's primary focus is to mitigate exploits and improve the remote telemetry unit's resilience against physical or cyber threats.

Combined cyber-physical attacks usually target the Supervisory Control and Data Acquisition (SCADA) system and RTU subsystems such as the Programmable Logic Controllers

(PLCs) that locally operate pumps, chemical processes, and valves [4, 19]. For example, a medium-size water utility system may have over 100 RTU sites distributed to maintain water pressure to users. Since, remote Terminal Units communicate with MTUs and SCADA using LAN, WAN, or Cloud links, disruptions or degradation anywhere in this chain can propagate and degrade the entire water utility system.

1.5. Water Utility Subsystems

To elaborate the water utility system discussion, Washington. D.C. (725 sq. miles) has over 100 RTUs and serves more than 1 million residents and 1.6 million residents in neighboring jurisdictions [55]. Therefore, even a slight improvement in RTU security is a significant reduction in potential loss due to attacks for the region. Figures 4, 5, and 6 show the water utility subsystems with RTUs for monitoring and data transmission [29].

Fig. 3. Map of Wash. D.C. dist. Service Area [55].

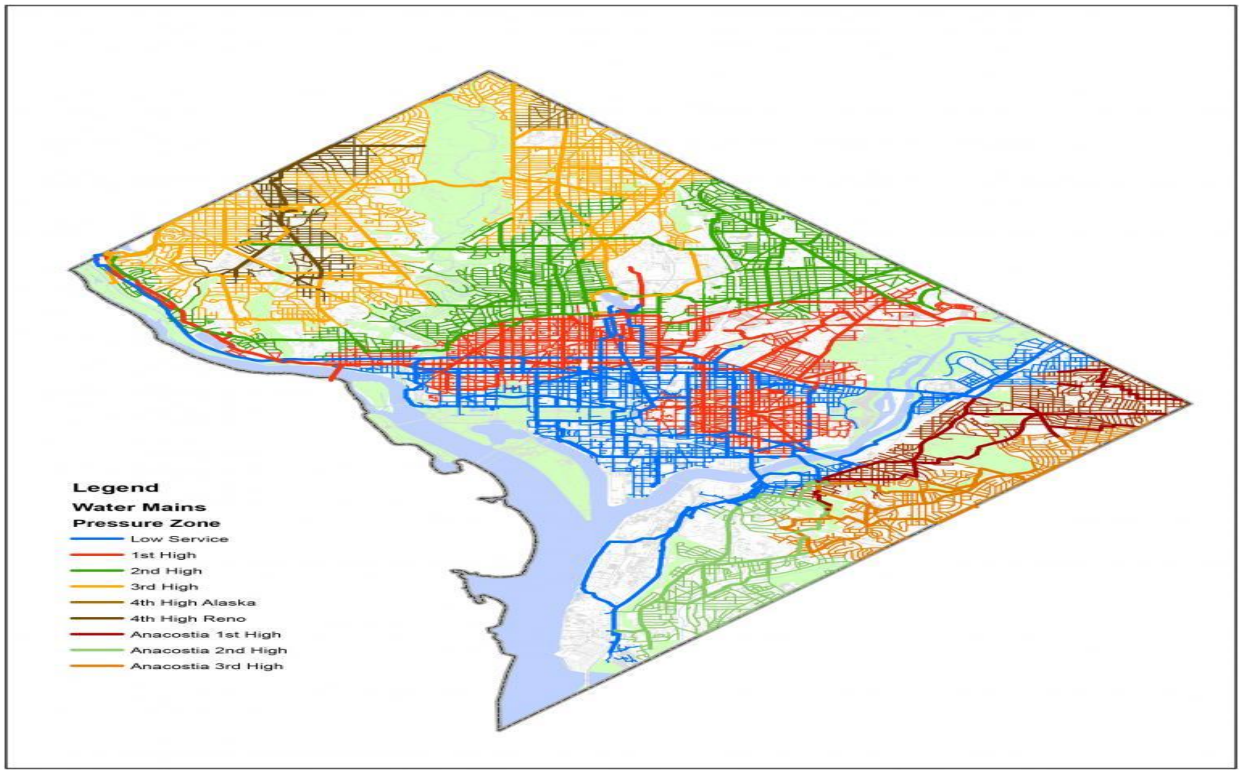


Fig. 4. Wash. DC dist. Pressure zones map [55].

Water is treated at one location (water filtration plant) and then pumped to an elevated or underground storage tank. It is then distributed to customers in different areas according to altitude. Every Pressure Reducing Valve (PRV), Boaster station, or storage tank has an RTU associated with it (fig. 6). The RTU is the gateway to water treatment, pumping, storage, actuators, and sensors. Unfortunately, there is a growing trend of physical and cyber security threats on public water utility systems.

Fig. 5 Water Pressure Management Diagram [29].

Fig. 6. Elevated Water Tank [32]

Water utility tanks such as elevated Tanks (fig. 6) and underground tanks have RTU located on-site to gather field data before sending it to SCADA via the MTU. Furthermore, Control Room Operator (CRO) or authorized management can initiate process changes from SCADA to RTU via the MTU.

Fig. 7. Water Booster Station [29].

The eyes and ears of a boaster station are the station RTU. The remote terminal unit (RTU) gathers system pressure, flow readings, pump status, space flooding, and valve status. A booster station is an essential subsystem of the water utility system where the water system's pressure is boosted to compensate for higher elevation.

Fig. 8. Water Pressure Reducing Station (PRV).

Securing the RTU and communications subsystems within the water utility system is critical. This dissertation uses a systematic design methodology, based upon Model Based System Engineering (MBSE) to design a security enhanced RTU. A number of security options are included in the design, although a specific RTU may not include all of them. They include RTU-external equipment such as a camera and voice recorder and an embedded data logger to track system performance and configuration data for attack mitigation, system restoration and forensic response.

1.6. Statement of Hypothesis and Approach

There is a need to harden the RTU and shift many security functions from upstream SCADA downstream to locate it closer to the data sources and operational equipment of the Water Utility System.

This dissertation focuses on developing a design methodology and prototype designs to enhance the remote telemetry unit (RTU) security and integrate it into existing water utility security.

CHAPTER 2: BACKGROUNG AND LITERATURE REVIEW

2.1. Chapter Introduction

Water filtration processes, wastewater treatment and water storage infrastructure have advanced significantly over the past few decades. As a result, water quality has improved considerably due to technical advances and enforcement of water regulations by the EPA and other governmental regulatory bodies. Long experience with water systems and extensive engineering made drinking water safe and available. Technology paved the way for enhancing the speed and precision of monitoring and controlling water utility systems. These include smart transmitters, PLCs, RTUs, communication devices to keep water pressures to the desired level for distribution, for hydrants, for industries, hospitals, and farms, to mention a few. In addition, manufacturers of pumps, motors, and other devices have improved their product quality, including modularity, cost, efficiency, and closed-loop processes to supply water 24/7 to intended users of water.

The initial topic choice arose from the author's years of experience with military and water utility systems. This experience guided the literature review in selecting and evaluating the relevance and significance of prior work cited in this chapter. In addition, it provided a starting point to identify where changes to existing RTU designs would improve robustness, resilience, and response time. The survey result from peers, academic coursework, advisory committee inputs at Colorado State University, and the recent increased attacks on water utility systems altered the types of changes needed. The validation of the choice of this research topic was obtained by gathering stakeholder data through a survey questionnaire of professionals who work with RTU, as reported in chapter 3.

There was a time when water utility cyber-physical attacks were barely on water utility to-do lists. The paradigm has shifted drastically to the extent that security concerns are at the forefront of every discussion regarding a water utility system. On January 27, 2022, the current Administration released a statement to expands Public-Private Cybersecurity Partnership to Water Sector. The action plan was developed in close partnership with the Environmental Protection Agency (EPA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Water Sector Coordinating Council (WSCC) [53]. The need to secure water utility is an urgent priority and the main stakeholders are onboard to look for solutions to mitigate the cyber and physical attacks on WUS. This dissertation will contribute to the action plan to protect WUS.

The vulnerability of our water supplies to disruption and contamination by potential terrorist or malicious acts has been well documented. Moreover, these potential attack scenarios can produce casualties on a massive scale if orchestrated successfully. For example, studies conducted by personnel at Hach HST, Colorado State University, and the U.S. Army Corps of Engineers, among others, have shown that attacks on drinking water supplies could be mounted for between $0.05 and $5.00 per death, using rudimentary techniques, and could amass casualties in the thousands over hours [6]. Enhancing the existing RTU to protect the field devices as proposed in the dissertation is an important step.

According to the Department of Homeland Security (DHS), the Water and Wastewater Systems Sector is vulnerable to various attacks, including contamination with deadly agents; physical attacks, such as releasing toxic gaseous chemicals; and cyber-attacks. The DHS also states that the result of any variety of attacks could be large numbers of illnesses or casualties and a denial of service that would impact public health and economic vitality [1]. The Environmental Protection Agency (EPA) again recognizes this same problem that local drinking

water and wastewater systems may be targets for terrorists and other would-be criminals wishing to disrupt and cause harm to your community water supplies or wastewater facilities. In addition, there is a physical cybersecurity concern with water utility systems.

Water utility security is a shared responsibility involving water suppliers, wastewater utilities, government, law enforcement, and citizens. We can all be involved in homeland security by playing an essential role in protecting our critical water resources [1]. Unfortunately, regardless of which improvements have been made to the critical water infrastructure physical and cyber security, they are inadequate to meet the growing threat.

2.2. Smart Water Network

Smart sensors, including transmitters, detect and convert a signal from one form to another and send the signal to a remote location. Two additional critical components of intelligent water networks are arguably the programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) system [12]. The communication hub, aggregator, mediator between the two subsystems, and the critical subsystem that protect the water tanks, booster station, pressure reducing valve is the RTU. Together, these networked devices grant modern water utility systems superior reliability, autonomy, and efficiency. However, they expose physical and cyber infrastructures to cyber-physical attacks (CPAs), as noted by a recent editorial [7]. The critical role of water utility systems makes them attractive targets for terrorism and cyber warfare [1, 8, 9, 12]. Thus, raising concerns regarding their vulnerability and potential damages to economies and local communities.

2.3. Cyber-Physical Systems (CPSs):

Water treatment and distribution involve electromechanical devices and human interactions amongst operators, technicians, and engineers. Some of the actions rely heavily on humans, including startup, process changes, troubleshooting, and after-hours on-call [12]. Cyber-physical systems (CPSs) are combining physical processes with computation and networking. In a CPS, embedded networking devices monitor and control the physical processes, usually in real-time, with regular feedback interactions between the system's cyber and physical spaces [4]. However, Physical security is a significant concern in all primary operations in the United States and globally, including water, electric grid, manufacturing, transportation, hospitality businesses, and farming. CPSs are steadily replacing legacy infrastructures in different domains (e.g., energy, transportation, and manufacturing) due to their enhanced performance and imparted by advanced design and superior abstraction [12].

Furthermore, breaking down the system into subsystems and components resulted in more reliance on RTUs, the Internet, and other communication devices for data collection and transportation. The breakthrough represented by CPS and other new technologies such as the Internet of Things (IoT) and the Internet of Service (IoS) [50].

2.4. Vulnerability of Water Utility Systems

The danger to the water utility system (WUS) from cybersecurity and physical threats is a headache to national security agencies. In the case of a water outage or attack on water utility, the consequences are slower to emerge and longer to mitigate. As for other critical infrastructures, the threat of cyber-attacks to WUS represents an increasingly significant concern [12]. EPA is aware of the vulnerability of WUS as published in numerous articles daily on this subject. In one article, EPA emphasized that "Drinking water utility systems are also increasingly

vulnerable to interruption in service from a terrorist attack, an industrial accident, extreme weather events, and aging water infrastructure." EPA seeks to improve the ability of water utilities to prevent, prepare for, respond to, and recover from water contamination incidents that threaten public health and the integrity of our drinking water systems.

The EPA Water Security Test Bed (WSTB) is located at the Department of Energy Idaho National Laboratory near Idaho Falls, Idaho. Unfortunately, at the moment, there is no systematically defined categorization, security controls or mitigation solution to WUS vulnerabilities as there is for Federal Computer Systems with NIST standards. Yet time is of the essence, as observed from the recent attacks of WUS. This dissertation develops a methodology that yields an enhanced RTU to provide reduce vulnerabilities, mitigate the most serious breaches and provide data to reduce time to restore operations. It is important to note that all major components and groups are needed to continue to provide secure and safe water supplies to the population [1, 10].

2.5. Attack Vectors on RTU and SCADA

Of all the national critical infrastructures in the United States, the water utility system has received fewer research funds and few rapid initiative funds such as Small Business Innovation Research (SBIR). As a result, it remains one of the most vulnerable infrastructures even though an adverse effect could be disastrous for users, communities, or cities. Inappropriately diminished perceptions of these threats are linked to the concept that water and wastewater systems, designed for ease of maintenance access, have little built-in capabilities for dealing with external adverse intervention visible to the public. [22].

Below are factors contributing to the recently increasing number and effectiveness of attacks on SCADA, RTU, and other Industrial Control Systems [41].

- Industrial Control Systems (ICS) such as RTU and SCADA play a critical role in manufacturing, including water treatment, oil and gas, and the electric grid.
- Bad actors target ICS to cause interruption of services, operations, financial losses, and threats to human lives combine with less attention to their security compared to administrative and management computer systems.
- ICS are high-value targets for threat actors that aim at disrupting business operations and processes for extortion or sabotage purposes.
- Technological advancement in computers and telecommunications has led to ICS (RTU, PLC, SCADA) connection to intranets and communication networks, hence, an increased attack surface [41].

One commonality is that most cyber security experts point out that RTU and SCADA systems are often vulnerable to the same vulnerabilities. For example, a publication by Pierluigi Paganin, 2021, emphasized that "Most of them lack security by design and are vulnerable to a broad range of attacks. Vulnerabilities in the systems control software, improper network segmentation, misconfigurations, are some of the most common attack vectors." Other factors that have fueled cyber-attacks against ICS/SCADA systems include [41]:

- The lack of device inventory and assessment;
- The use of legacy systems and devices running outdated hardware and software;
- The lack of network segmentation
- Limited access control and permission management
- Inadequate security policies for the ICS
- The lack of ICS specific configuration change management
- The lack of formal ICS awareness program and security training

- The lack of adequate password policy
- Unsecure remote access of ICS components

Claroty Research Team82 Summary [56].

A specific factor increasing attacks on RTUs and SCADA systems in a water utility is well described by the Claroty Research Team82 and summarized as follow [56]:

1. The critical manufacturing, energy, water and wastewater, and commercial facilities sectors, all designated as critical infrastructure sectors, were the most impacted by vulnerabilities disclosed during 1H 2021.
2. In 1H 2021, 80.85% of vulnerabilities disclosed were discovered by external sources (Fig. 9). The external sources include several research organizations, including third-party companies, independent researchers, and academics.

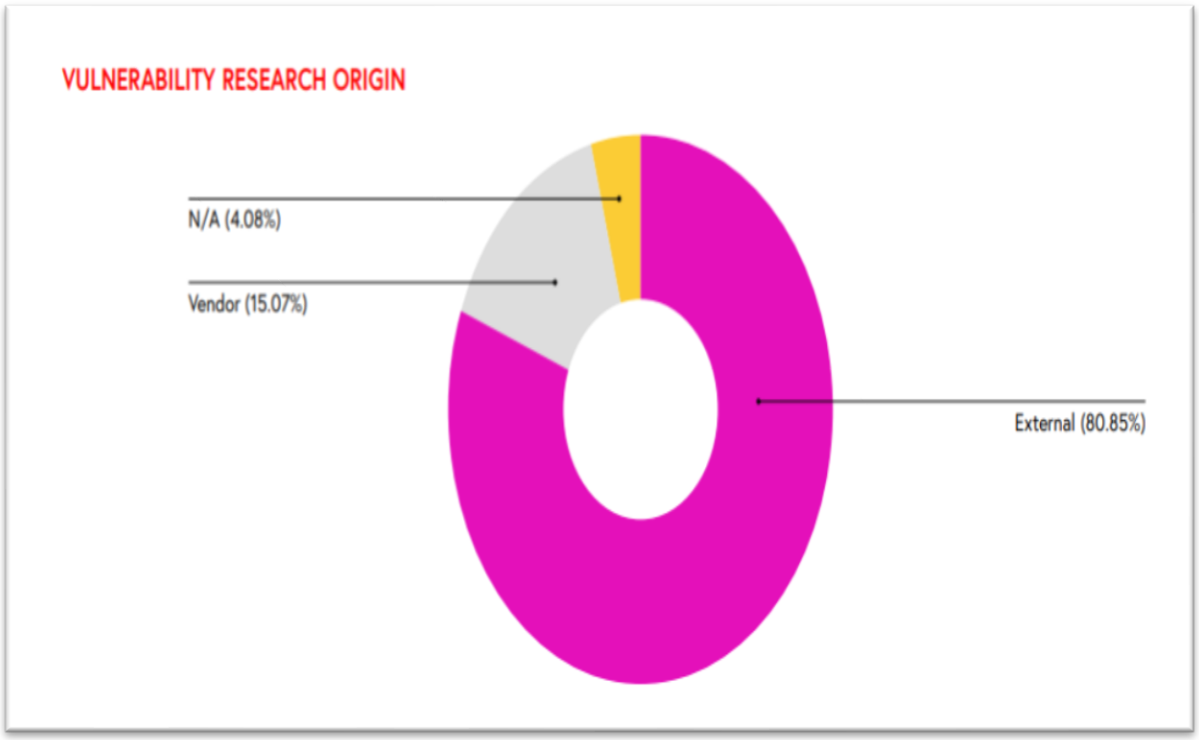


Fig. 9. Breakdown of vulnerabilities by origin of discovery [56]

3. Since 23.55% of vulnerabilities affect the Operations Management (Level 3) level of the Purdue Model, below, this explains why we saw many of the vulnerabilities affect software components. In addition, about 30% of vulnerabilities found affect the Basic Control (Level 1) and Supervisory Control (Level 2) levels of the Purdue Model. Naturally, when affecting these levels, an attacker can also reach lower levels and affect the process itself, which makes them an attractive target.
4. The Purdue model, dating back to the early 1990's, was one of the first to separate the architecture into an IT information zone and an OT operational Zone. It was later adopted into the International Society of Automation standard ISA-99
5. A monthly breakdown of vulnerabilities indicates that the critical manufacturing, energy, water and wastewater, and commercial facilities sectors were affected by multiple vulnerabilities disclosed during every month of 1H 2021.

   Of note, Claroty discovered and disclosed ten vulnerabilities affecting products at Level 2 of the Purdue Model of ICS security [56].
6. The process networks. This level includes SCADA servers, Human Machine Interfaces (HMIs), and other equipment overseeing industrial processes [56].
7. Local Attack Vectors: On the other hand, vulnerabilities exploitable through local attack vectors rose to 31.55% from 18.93% in the 2H 2020. For 72.14% of those vulnerabilities, the attacker relies on user interaction to perform actions required to exploit these vulnerabilities, such as social engineering through spam or phishing.
8. The majority of ICS and SCADA vulnerabilities disclosed during 1H 2021 affected Level 3: Operations Management (Historian, OPC Server, etc.) followed by the Level 1: Basic

Control (controllers, PLCs, RTUs) and Level 2: Supervisory Control (HMIs, SCADA and engineering workstations).

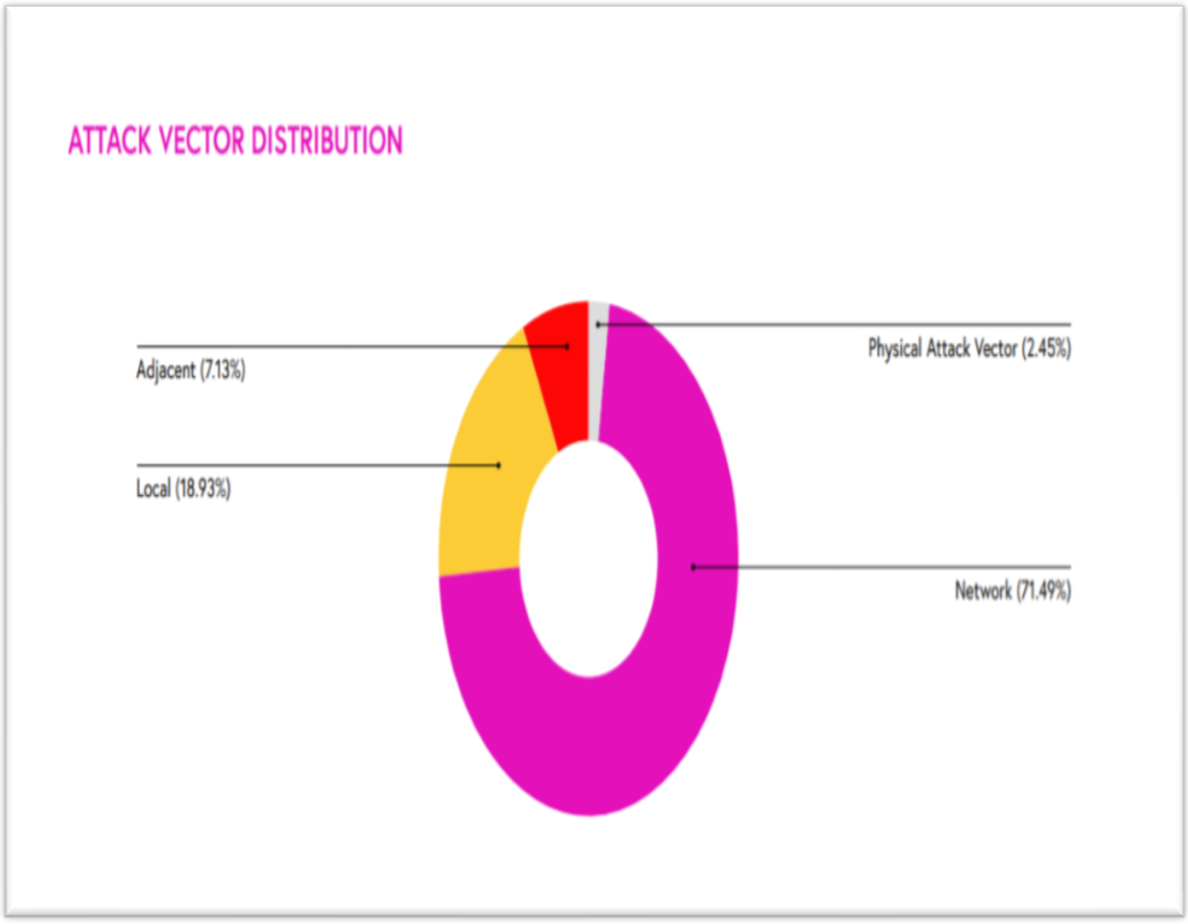


Fig. 10. Breakdown of new researchers reporting ICS vulnerabilities [56].

Fig 10 shows the attack vector distribution breakdown for Industrial Control Vulnerabilities (Claroty Team82, 2021). Based on recent cyberattacks on WUS and literature review, it is not surprising that 71.47% comes from networks. Followed is local Vector with 18.02%, Adjacent recorded 7.13%, and lastly, the physical attack vector for 2.45%.

These include the 41 discovered by the Claroty Research Team and all others discovered and publicly disclosed by other researchers, vendors, and organizations within the same period.

Claroty's sources of information include the National Vulnerability Database (NVD), ICS-CERT, CERT@VDE, Siemens, Schneider Electric, and MITRE [56].

2.6. Remote Terminal Unit (RTU) Architecture and Functions

Remote Terminal Units (RTUs) act as sub-stations in SCADA architecture [16]. Each sub-station has an RTU to gather data about the system's state, including field node parameter values. The functions of RTU include data gathering and transmission of collected data to the Master Terminal Unit (RTU). Remote terminal stations collect information/data from sensors or actuators connected with the physical environment and process information back to the master station depending on the master request [16].

RTUs are geographically distributed over different sites, collecting and processing real-time information to master stations using link LAN/WAN (radio signals, telephone line, cable connection, satellite and microwave media). Therefore, the role of RTU in water utility is critical. Unfortunately, most remote stations are not staffed, so operators, engineers, and technicians know what is going on at the remote locations through RTU.

Remote terminal units consist of a power supply, a Programmable Logic Controller (PLC) or microprocessor, Uninterruptible Power Supply (UPS), radio, antenna, and inputs/outputs. In addition, there may be a backup generator at the RTU site, depending on RTU size, function, or applications. Figure 11. shows a typical component layout in an existing RTU that can be incorporated into MBSE and cameo Enterprise Architecture 19.0.

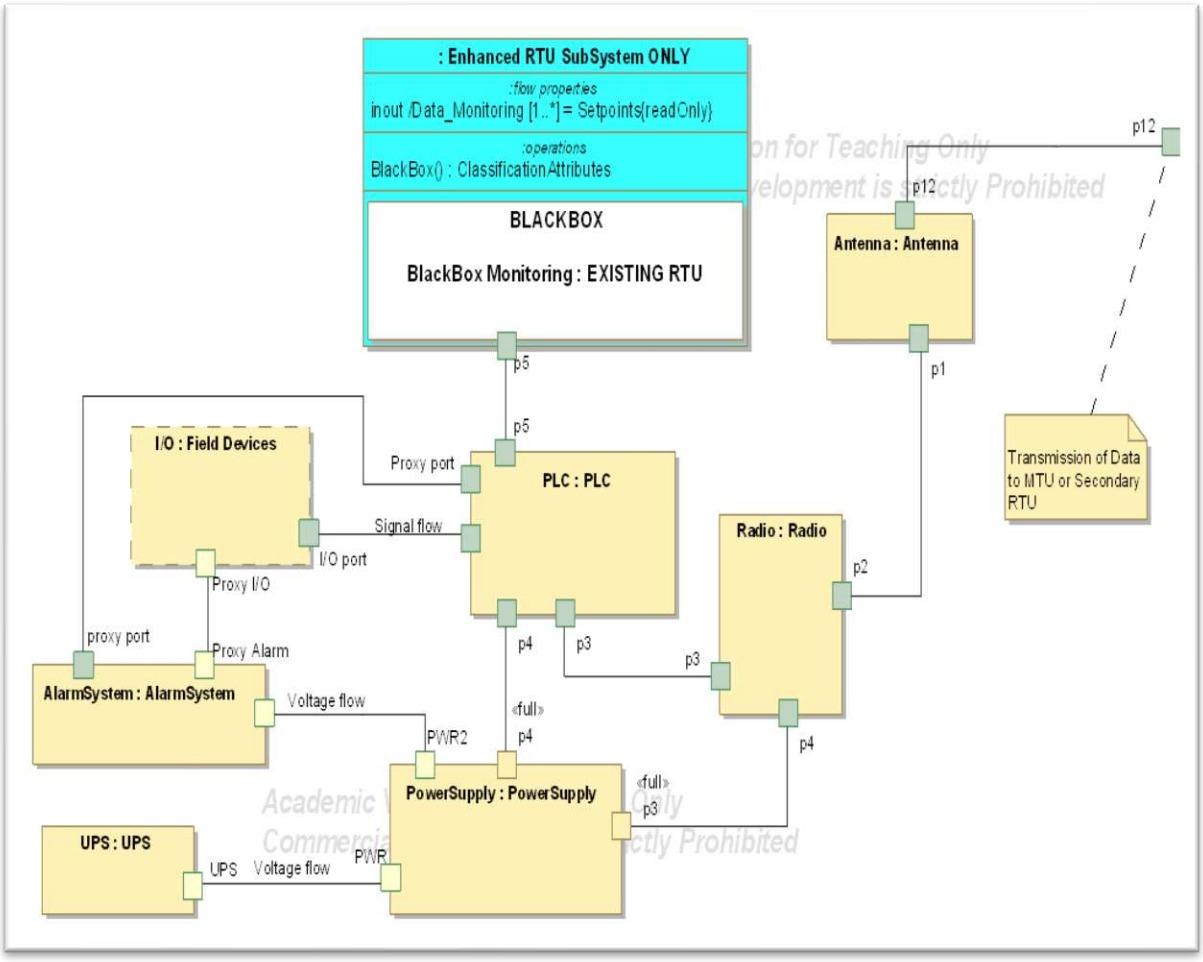


Figure 11. Block Diagram showing RTU subsystems

2.7. Supervisory Control and Data Acquisition (SCADA)

Supervisory control and data acquisition (SCADA) systems are the interface between the Water Utility business IT functions (Control Room, Utility Servers) and the OT water Utility operations (MTU-RTU-Field Devices). They are almost uniformly used to monitor and control industrial processes such as water and wastewater treatment and distribution [17]. SCADA in water and wastewater monitoring operations provides a common operating picture of what is occurring to stakeholders. This information is incorporated into decision support functions

guiding resource allocation and analyze data regularly rather than in segments [36]. In addition, digital monitoring field devices make the data they receive more accurate and up-to-date

Furthermore, SCADA provides the necessary functionality of real-time monitoring, logging/archiving of data, report generation, trend analysis, and automation for industrial processing and manufacturing. As a result, SCADA helps detect anomalies and inconsistencies in day-to-day operations and provides efficient and accurate automated monitoring, crucial to wastewater treatment facilities as overflows can result in EPA regulation violations and costly fines [36].

The SCADA interface to the physical water system is through the master telemetry unit (MTU) and the remote terminal units (RTU). Different communication networks are used to communicate between the MTUs and the RTUs. SCADA software performs global or system-wide optimization of subsystems and directs alerts, alarms, and malfunctions to the appropriate audiences [30].

Supervisory SCADA forms the communications backbone in manufacturing, such as water treatment and water utility systems. In addition, the Supervisory Control and Data Acquisition (SCADA) system play essential roles within real-time industrial control, operations, and communication such as electric stations, oil stations, and water purification plants. The RTU's interface with field devices and the MTU aggregates the data and transmits it to SCADA [33].

CHAPTER 3: RESEARCH METHODOLOGY

3.1. Introduction

Because of the need to focus water utility security enhancements closer to the source of the operating systems and data, it became clear that the component nearest them would need to be redesigned. In addition, the RTU component needed to be enhanced while remaining interoperable with the existing water utility information and physical systems. This chapter describes the methodology used to design and evaluate an RTU meeting the enhancement and interoperability requirements.

In terms of security gains, this methodology yielded designs that helped prevent exploits, minimize their impact, shorten the time restore operation, and provide data to help first responders and forensic law enforcement operators. In addition, these designs would satisfy the central security goal of raising the cost of water system attacks to threat actors.

3.2. Methodology

This consisted of modeling existing RTUs, using Model-Based Systems Engineering (MBSE) to combine functional requirements and constraints on the enhanced RTU, followed by selecting components appropriate to security enhanced RTUs starting from existing component technology (to assure interoperability). Then simulating field behavior of the RTU in normal operation and under attack, and finally using the predicted behaviors to derive metrics for comparing the performance of existing RTUs to the enhanced robust RTUs.

3.3. Research Strategy

The strategy was to use the methodology at all stages of the dissertation and continually validate the outcomes in the research goals.

This amounted to validating the choice of topic and the resulting goal of hardening the RTU initially. That was followed by using MBSE to develop a design environment of the RTU and use that as a framework to explore design choices. MBSE enabled the designer to determine and identify critical nodes and highlight design choices. Once these were identified, MBSE results were combined with existing Water utility operations to determine: 1) Enhanced RTU Requirements; and 2) Design parameters of the Enhanced RTU. Following that, 1) the enhanced RTU was analyzed using MBSE, and 2) specific implementations of the Enhanced RTU were developed. Finally, 3) These design performance in the field was simulated, 4) Validated by comparing results to observed present-day RTU operations, and 5) Comparing existing and enhanced RTU attack responses. A PLC ladder programming is both a simulation and operational procedure sequence. This choice was made because over ninety percent of water utilities use PLC ladder logic in their operations [35, 37]. It would have been most helpful if MBSE outputs could be ported to PLC programs to test design outputs in real-world operating sequences immediately.

3.4. Peer Group Survey Data to Validate Focus on RTU

Prior to the long-term task of focusing the dissertation research on the RTU, the choice was validated by surveying field personnel in various water utility companies who know the RTU functions, data collection, and transmission within the SCADA system and their present-day operational security environment. The survey also elicited their inputs concerning the

security requirements for exiting RTU for defending against physical and cybersecurity threats (Details are provided in Appendix B). The survey questions were grouped to allow unified, consistent results, organized as shown below:

1. Participants Background details
2. Policies and Procedures
3. RTU Vulnerability Section
4. RTU Configuration vulnerabilities
5. RTU Communication Vulnerabilities
6. Management Controls of RTU
7. Operational Controls of RTU
8. Suggested Enhancement Methods.

3.5. Survey Sample Selection

A qualitative sample method [44] was used to gather the data for this topic validation task. Appendix B shows the participant attribute criteria: data collection, years of experience of sampled personnel working with RTU, observations of communication interruptions, management principles on RTU security, and other security issues. Field personnel made up of experts who work with RTU daily were selected. The participants know the RTU system integration with MTU and SCADA for water and wastewater systems and have several years of working experience with remote telemetry units. Unfortunately, some invited participants could not provide specific data due to security reasons, fear of losing their jobs, and schedule pressure.

3.6. Summary Topic Analysis Conclusions

Based on the survey results, the literature review, recent water utility security events, and my own experience, the following conclusions regarding topic and scope were drawn:

1. Water utility systems are increasingly vulnerable to physical and cyber-attacks and need to be hardened to assure a reliable water utility for users.
2. The Remote Telemetry Unit (RTU) is a critical and independent water utility central control system subsystem.
3. The RTU is the interface between the field components of the water utility system and the upstream control systems that monitor, control, and operate the water supply business. It is thus the closest to the source of critical utility data and operations.
4. Improving RTU security is essential for responding effectively to the latest generation of threats to Water Utility safety, availability, and continuity of operations. Some of the functional improvements that an enhanced RTU will provide include: decreasing the time to detect exploits, providing more information in less time to system stakeholders, decreasing the post-exploit restoration time, enhancing ongoing situational security awareness, and offering enhanced forensic information for post-exploit operations.
5. Enhancing existing RTUs even without the complete enhancement package described here will increase utility security.

3.7. Research Constraints

In order to have a near to intermediate-term security improvement for existing water utilities, the enhanced design will have to satisfy some constraints. These constraints are enumerated below: The Enhanced RTU shall be based on an open architecture described by open architecture definitions, networking requirements, and software assessment criteria.

- The enhanced RTU design shall follow MBSE design principles.

- The enhanced RTU architecture subsystem shall be operationally compatible with present-day water utility systems, including maximum allowable size, weight, network topology, bandwidth, frequency, and data transmission speed.
- The enhanced RTU operation shall conform to applicable standards, including NEC, NFPA 70E, OSHA, ANSI, and IEEE.
- The enhanced RTU shall be compatible with the existing water utility, network, and enterprise information systems.
- The enhanced RTU shall implement security requirements specified in the water utility system requirements and system security plan.

3.8. Research Assumptions

The enhanced RTU architecture has been prepared based on assumptions that will enable the enhancements to be incorporated into existing RTU devices. If these assumptions are not met, a new RTU subsystem will need to be designed. This is a more costly and time-consuming option, but probably not prohibitively. We discuss both possibilities in the chapters below. The assumptions underlying enhancing and existing RTUs include:

- The enhanced RTU system will be the primary data and operational resource for water utility sensors, control systems, and actuators.
- The hardware for the existing RTU system will have enough physical space and spare I/O in the PLC to support the project.
- The processor memory in the existing RTU and SCADA system will be large enough to support the integration of the enhanced RTU components.

- The location of the existing RTU is feasible and practical to support the proposed Enhanced RTU functionality.
- The Enhanced RTU will be required to be sufficiently modular to accommodate new functions, technologies, and new cutting-edge processes to remain operationally effective and supportable.

3.9. Research Limitations

This research focuses on the Remote Telemetry Unit (RTU), whose outputs go to the MTU and from there to the SCADA system in water utility systems. It is currently one of the weakest security nodes and needs the highest priority for hardening.

Therefore, the scope of this research is limited to enhancing the RTU, focusing on using feasible and affordable enhancements. Connections upstream to the MTU and SCADA and downstream to physical field components are mentioned when necessary to explain or demonstrate enhanced RTU features or functionality. While RTUs are used in manufacturing and infrastructure with dispersed subsystems and industrial automated controls, this research focuses on RTUs utilized in water treatment facilities, wastewater treatment facilities, and water utility systems.

3.10. Systems Architecture of the Enhanced RTU in Water Utility Systems

This section provides a high-level description of a Water Utility System (WUS). This solution encompasses the requirements described in the enhanced RTU system Requirements. The CAMEO Enterprise Architecture Modeling Software (a mainline MBSE software tool) was used to guide the architecture and incorporate the requirements of the enhanced RTU. This tool

guided the enhanced RTU system architecture, system and subsystem dependencies, activity and Use Cases, and how the subsystems can successfully function together. The CAMEO MBSE tool provided:

- Capture design considerations
- Capture architecture level technical design decisions
- Serve as the primary material for architecture and design reviews
- Identify the architecturally significant Use Cases that were input to the SWUS model
- Identify the technical risks confronting the SWUS project that could compromise project success

3.11. Logical/Functional viewpoint of the enhanced RTU

This design view defines the system elements, services, functions, information exchanges, and other behaviors depicted in the Operational Viewpoint (OV) using Blocks. The Logical Viewpoint (LV) is independent of particular technologies or products and represents a functional definition of the system or enterprise [1]. A reference architecture block diagram decomposes the RTU into a block diagram incorporating constituent components.

A Functional View (sometimes called a Logical View, or even a Logical Architecture by others) shows the functionality required to fulfill the User's Needs. For the enhanced RTU, the reference architecture shows all the subsystems and how they connect to aid data transmission within the RTU and data transmission from the RTU to MTU or field devices.

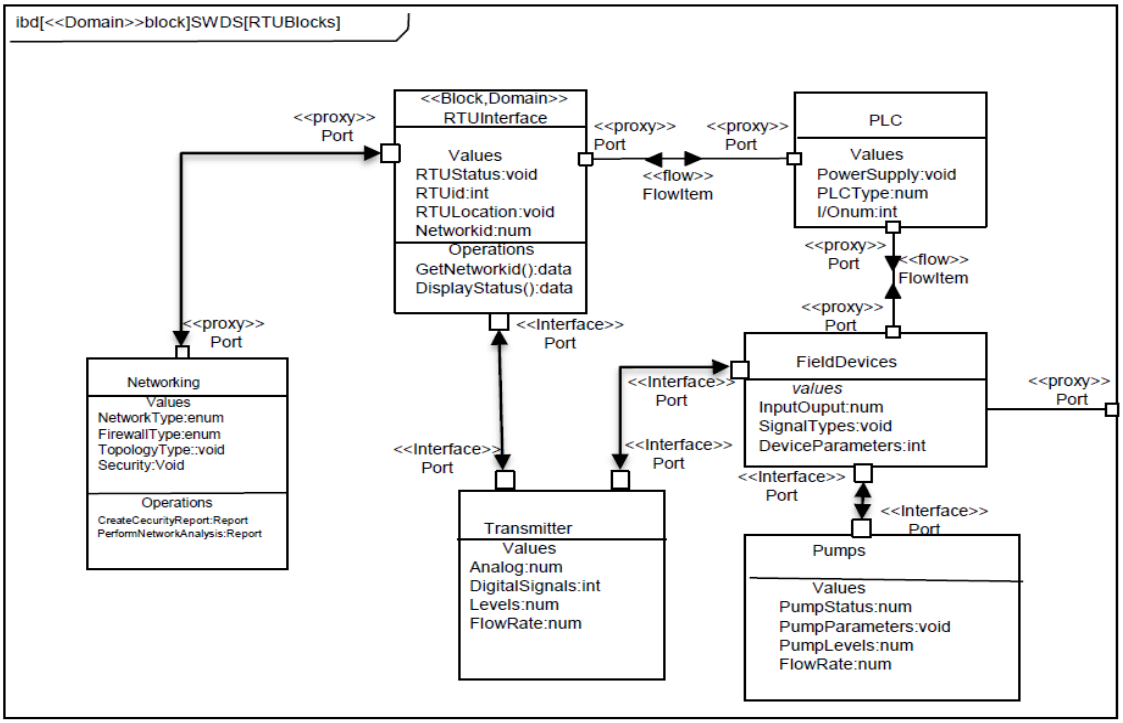


Fig. 12. Internal Block Diagram of RTU

Figure 12 shows the internal block diagram (IBD) of the RTU and its decomposition into the various subsystems, showing the connectivity of the major components and identification of entry and exit points (Borky & Bradley, 2019). Securing the endpoints is critical to the robustness of the enhanced RTU.

The figures below elucidate the features of the enhanced RTU. Figure 13 is a block definition diagram (BDD) of the enhanced RTU within the SCADA system, showing the communication path to the MTU and then to SCADA, as shown in figure 14. In addition, the SCADA system's overall requirements are simplified by eliminating the networking subsystem. This enhancement eliminates utility corporate entities and outsiders from the SCADA system and prevents cyber attackers from gaining access to water utility systems.

Fig. 13 shows the modified data flow between the enhanced RTU and the MTU. Data flow is contained within the SCADA-MTU-RTU chain and isolated from the Utility Corporate environment. Furthermore, the improved RTU shall prevent bad actors from manipulating or changing critical setpoints to control field devices, including pumps, motors, chemical mixers, and system pressure.

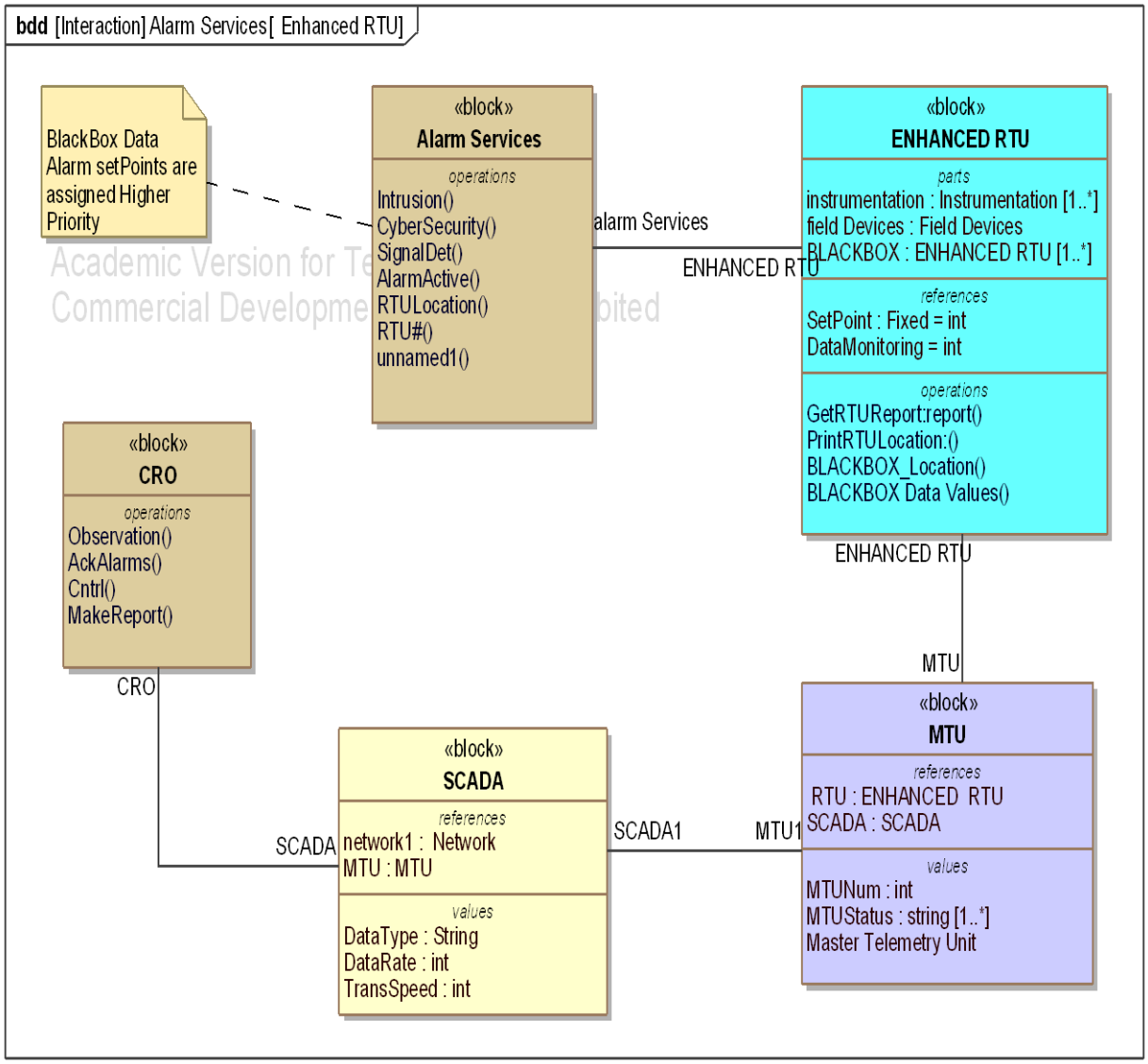


Fig. 13. Block Definition Diagram of Enhanced RTU Alarm Services.

3.12. Service Taxonomy of the enhanced RTU

Services Taxonomy for the Secured Water Utility System (SWUS) describes the domains and their interfaces and Ports. In addition, it describes the types of services for each subsystem and component within the SWUS and displays Behavior Diagrams. Table 9 below describes this taxonomy for the Enhanced RTU.

Table 2. Enhanced RTU Service Taxonomy from an operational viewpoint

System Service	Use Cases	Domains	Domain Services
RTU: Main communication hub for remote sites: Distribution Tanks, PRV, Boaster Station, W/W pumping stations.	Gathering Data from remote station. Cyber Attack on RTU. Physical Attack on RTU.	Communicate with Other RTU, MTU and SCADA. SCADA connectivity with network/cloud.	Uses Wireless, leased lines, Fiber optics, Micro wave to communicate to SCADA vis RTU and MTU. Third Party Vendors. Contractors
Field Device: Pumps, motors, Sensors etc.	Pumping controls, HOA, HMI	Sensors, Alarm systems, Security, Instrumentation	Maintain Constant pressure, controls in automatic mode. Monitor setpoints Direct effect on water utility s
Data Transmission: Remote Station Data, Alarm Status etc.	Performing Data transfer, transmission mode. Transmission rate	Transmission and network protocol management, packet switching	Network Security, Instrumentation, RTU and SCADA communications.
Intrusion: One of the Weakest links in water utility systems. Vulnerability point of entry/exit, Insider and disgruntled employees.	Sensing issues, Security measures Security Enforcement	Physical Intrusion, Cyber Intrusion, RTU, MTU and SCADA. Access Management	Point of Attack due to lack of surveillance, intrusion detection. No setpoint monitoring. Regular and periodic system testing

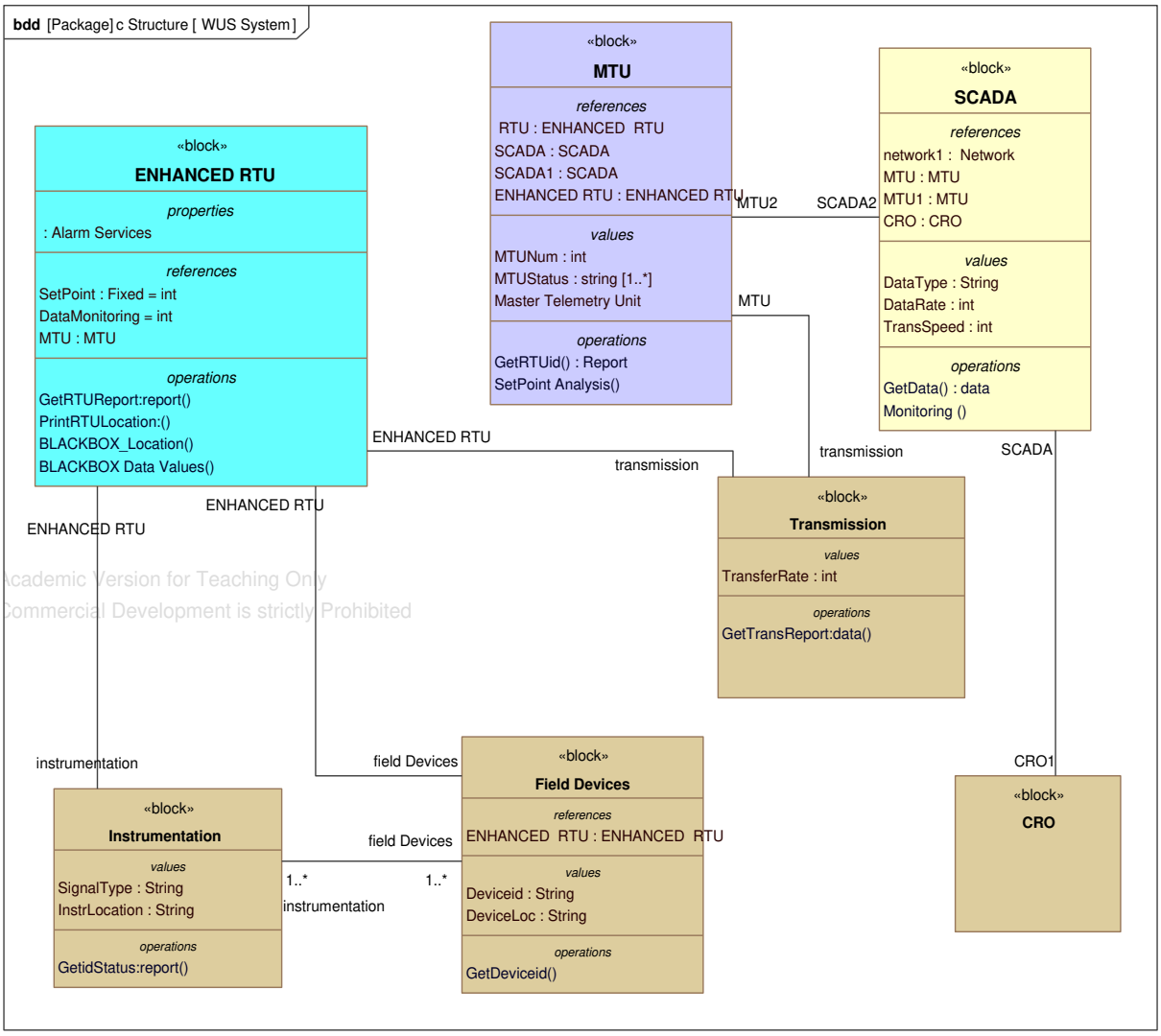


Fig. 14. BDD Diagram of WUS with Enhanced RTU in SCADA Subsystem.

Fig14 is a block definition diagram of WUS with enhanced RTU, developed in Cameo system Architecture, based upon requirements developed using MBSE [2] methodology, and incorporating literature and survey results. Figure 15 is a simplified functional requirement for the enhanced RTU. It provides stakeholders a compact overview of the subsystems and their uses. In addition, it is a CAMEO output that provides high-level design requirements to check and help maintain consistency throughout the design.

Table 3. Enhanced RTU Subsystems Requirements for Enhanced RTU

#	Name	△ Text
1	R 16.1.5 SCADAReqts	Centralized monitoring, Remote cntrl of field devices: HMI, Historian, Diagnostic software, Reports
2	R 16.1 SCADA	Centralized Monitoring, Remote Control of Field Devices, HMI, Historian, Diagnosstics, Thrends
3	R 16.1.3 CRO	CRO shallbe located at the Central Control Station to monitor, make informed decisions, route emmergencies to appropriate personnel
4	R 16.1.9.1.1 UPS	Each RTU will have UPS to provide power to the system in case of power loss.
5	R 16.1.8 MTU	Main SCADA Hub, Comms, HMI, algorithms, Data manipulations, Transmission, Historian, secured Location.
6	E 16.1.9.1.4 Transmission	Mode of transmission: Microwave, Fiber Optics, FCC assigned HZ, Leased Phone lines, Antenna, Transceivers
7	R 16.1.9.1.2 FieldDevices	Primary I/O to PLC,to RTU, to MTU and SCADA Pumps, motors, instruments from the field.
8	E 16.1.9.1 ENHANCED RTU with	Remote Comms Center, PLC, field devices, comms to MTU Black Box
9	R 16.1.4 On-Call Staff	The system shall have on-call personnel 24/7, as a subject matter expert shall be able to respond quickly, perform immediate and controlling actions
10	R 16.1.10.1 Network / Protocol	Type of Protocol used for Transmission, Network Architecture Networking Connections Removed from SCADA
11	R 9 Instrumentation	Use of various Instruments: P&ID connections, Level, flow, gases, chemical levels and Dosages.

Academic Version for Teaching Only
Commercial Development is strictly Prohibited

3.13. Chapter Conclusions

This chapter describes the choice and validation of the research topic. It supports the conclusion to focus on the RTU as a component distinct from the SCADA. The need to enhance RTU designs in the context of water utility systems required the capabilities of MBSE in order to elucidate the specific design criteria needed to realize the enhanced RTU. The initial topic choice arose from the authors' years of experience with military and civilian water utility systems

combined with a literature review. The validation of the choice of this research topic was obtained by gathering stakeholder data through a survey questionnaire of professionals who have hands-on experience with water system utility RTUs.

CHAPTER 4. USE OF MBSE TO DEVELOP A CONCEPTUAL DESIGN

4.1. Chapter Introduction

This chapter describes how Model-Based Systems Engineering (MBSE) principles and tools were employed to develop a security-enhanced RTU starting from an existing RTU. The enhanced RTU receives control commands from the SCADA through the MTU before transmitting them to field devices. The desired functionality of the enhanced RTU is to have it test these data to ensure:

- Process variables are within the allowable range.
- Time-stamped data received and transmitted for validation and referencing.
- To Detect out-of-range control data and variations.
- To Prevent data manipulation by requiring data source validation and certification.
- Finally, send alarms to stakeholders through the MTU/SCADA data chain to detect a suspicious signal.

An implementation decision for the enhanced RTU is to decide how to implement these functionalities. For example, depending on organizational budget and culture, it may be better to deploy changes incrementally.

The design preliminaries described the problem, followed by a literature review of relevant topics and publications. This chapter focuses on the next step in the methodology, the use of MBSE to analyze requirements, conceptual analysis, and design of the enhanced RTU. The MBSE functions employed CAMEO Enterprise software to obtain a high-level system

architecture and design and decompose the SCADA-MTU-RTU-Field Devices into subsystems, and the targeted RTU was then extracted for further analysis.

Figures 16 and 17 below show an advantageous conclusion made clear using this methodology: the reduction in the number of communication nodes, attack points, and integrated system data flows. The latter allows for improved data aggregation and processing and is centralized, easier to monitor and defend cyber defense nodes.

Figure 16 below shows the data flow entering and leaving the existing RTU. The major subsystems and connectivity are shown together with a soft entry point for the cyber-attack signal to penetrate to SCADA to inject malicious signals, extract critical data, or hold the SCADA for ransom. The networking subsystem of the SCADA is one of the soft targets that has contributed to the increasing number of cyberattacks and ransomware attacks on water utilities in the United States. Cyber attackers (mainly located outside the shores of the United States) on water utilities demand blackmail ransom money and threaten damage to the critical water infrastructure.

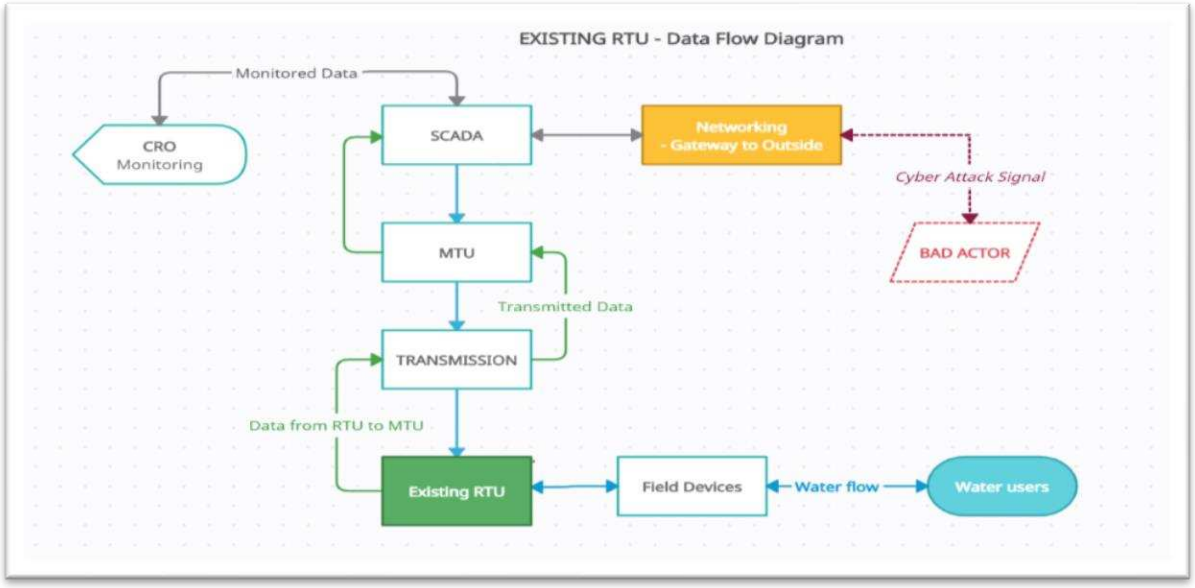


Fig. 15. Data Flow Diagram of SCADA with Existing RTU

The data flow analysis shows that the SCADA links to the Control Room Operator (CRO) and system stakeholders on its output and the RTU on its input sides. When the RTU is captured or breached, a bad actor located far away can inflict damage by manipulating process setpoints to cause sanitary sewage overflows of wastewater and water main breaks to disrupt other critical infrastructure usages. Furthermore, bad actors controlling RTUs can control pumping stations, water utility booster stations, pressure-reducing valves to hospitals military facilities, and demand a hefty ransom before restoring services.

This removes one of the most significant soft targets for cyber-or physical attacks. The enhanced RTU (fig 17) is the closest subsystem to the field devices and needs to protect the final system parameters and setpoint variables for stakeholders. Its simplified data flow and connectivity reduce its attack surface. Combining data at fewer nodes allows for more efficient data conditioning and deconfliction.

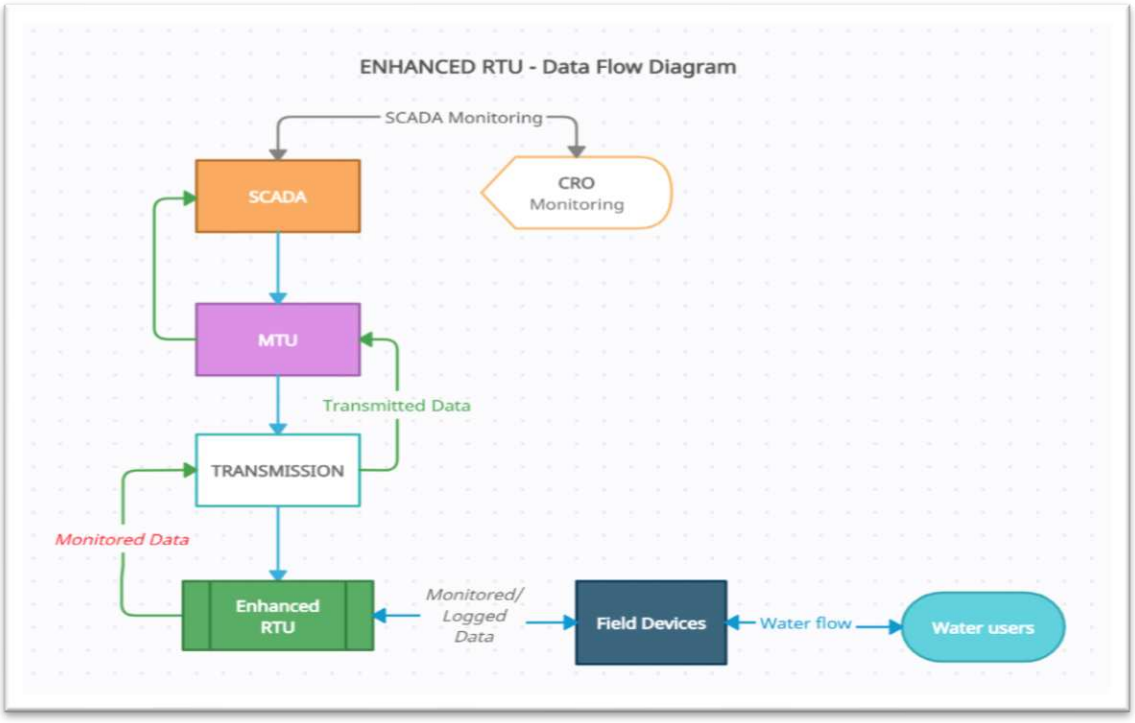


Fig. 16. Enhanced RTU data flow diagram with more secured monitoring and controls

Figure 16 is a non-branching, one-line diagram of a water utility system SCADA with enhanced RTU. The RTU is the closest to the water utility system and wastewater system, field devices, hence, the reason for enhancing the RTU subsystem of the SCADA.

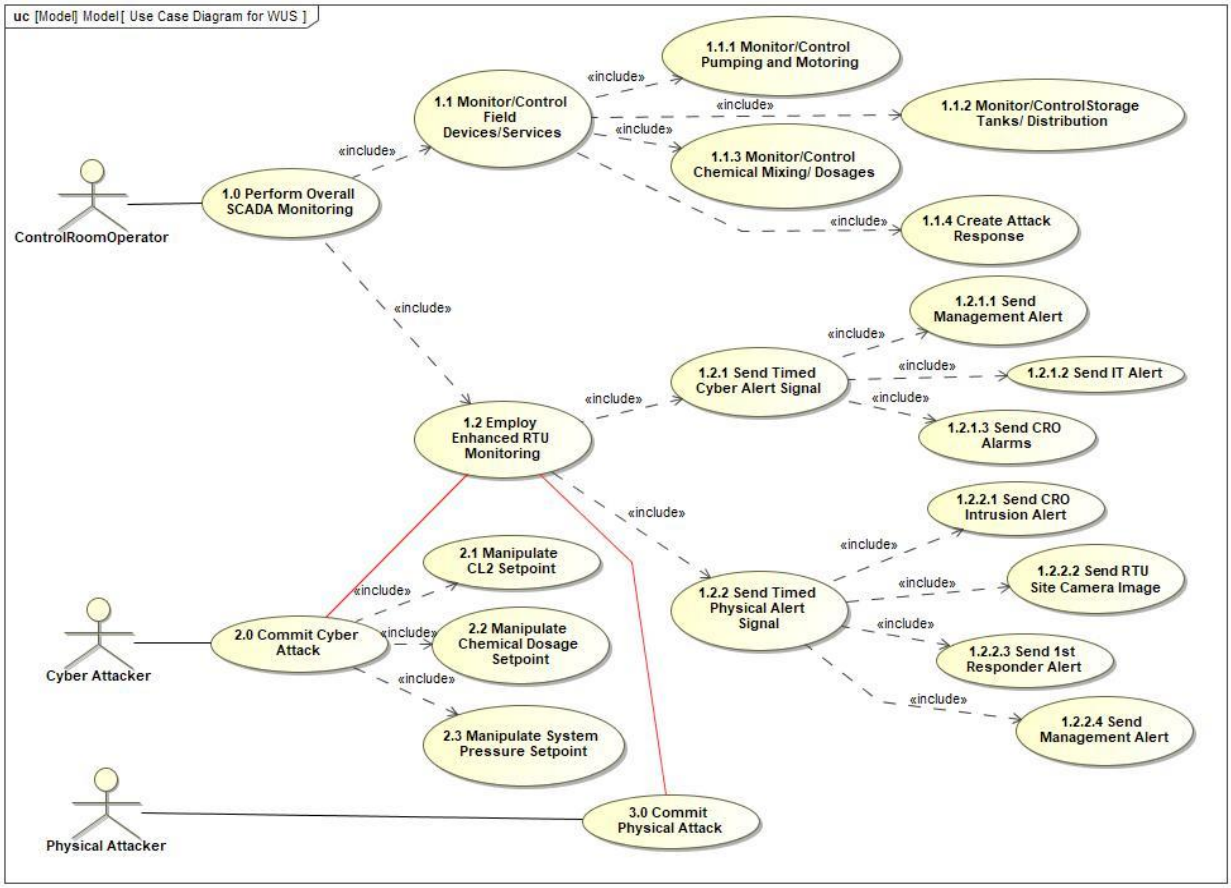


Fig. 17. Use Case of WUS Simplified SCADA with Enhanced RTU

Use Cases describe system transactions with an external system (Actor) to show communications among system transactions. For example, Fig 17 describes a bad actor (cyber attacker) far away trying to penetrate through SCADA to manipulate chemical set points for a water utility system and hoping that the control room operator (CRO) would not detect the exploits. The use of the enhanced RTU will detect out-of-range setpoint manipulation and trigger alarms to CRO, management, stakeholder, and first responders. In another example, a bad actor

(physical attacker) physically attacks the RTU to change setpoints to cause harm. Furthermore, the enhanced RTU detects an intruder presence, sends alarm signals to CRO, Stakeholders, and First Responders, and activates the station video/audio camera.

4.2. Adding Components to enhance RTU Security

This section describes components to add to existing RTUs to mitigate the aforementioned threats. The addition of these subsystems will enhance RTU physical and cyber RTUs security:

1. An intrusion alarm.
2. An audio and image/video capture device.
3. An embedded operational, configuration, and event data recording module (black box)
4. Enhanced and ruggedized communication components for the RTU to transmit and receive system data.

Adding the subsystems to the existing RTU will modify the data flow within the RTU and the associated linked subsystems. Therefore, these additions must be evaluated based on value, cost, and compatibility. The Enhanced RTU with additional components is shown in fig 18.

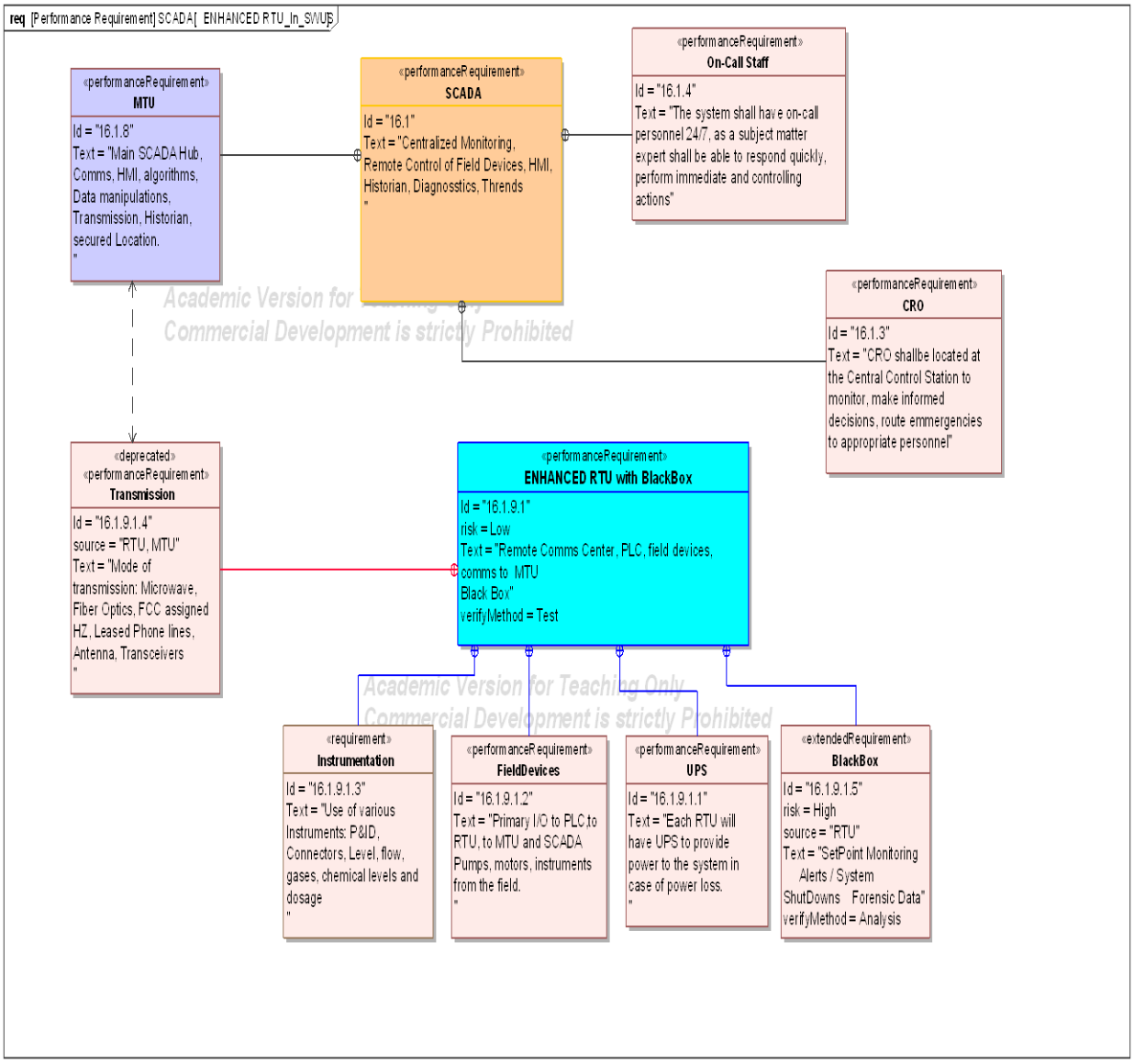


Fig. 18. Requirement: WUS SCADA with Enhanced RTU decomposition:

The MBSE decomposition of a subsystem into components is shown in fig 18. The enhanced RTU subsystem breaks down into components: instrumentation, field devices, uninterruptible power supply (UPS), black box, and transmission.

The enhanced RTU will add the following security functionality:

1. The cameras will send images to the embedded recorder and simultaneously through the MTU to the CRO to monitor the RTU environment 24/7.

2. The embedded recorder will detect changes and anomalies in input control data that indicate attacks or natural upsets and activate an emergency response protocol.
3. An intrusion alarm appears on the SCADA user interface with audio to alert the operator.
4. Ensure a call to the local emergency response and law enforcement if required.
5. Provide a real-time physical and digital view of the RTU site.
6. The operational and environmental data recording module (black box) records and stores a user-defined set of operating parameters for the sensors and actuators and enough memory to record time-series data for diagnostic, forensic, and risk analyses.

4.3. How Existing RTUs in the Field can be Enhanced

It is impractical to replace most RTUs and install new robust RTUs because of the cost and labor involved. However, even upgrading existing RTUs with partial enhancements will provide short-term benefits and significant improvement to water utilities.

The location and the space within the RTU cabinet will be determining factors for in-place upgrading. From the author's experience and the survey questionnaire answers, most RTU cabinets have sufficient space to accommodate most proposed security enhancements.
In addition to physical space, upgrading an existing RTU requires the following:

1. Sufficient physical space in the RTU enclosure for a black box or status module
2. Enough unused I/O in the PLC / Digital Control System
3. Sufficient PLC processor memory
4. A suitable location to support the new system communication and monitoring upgrades.

An RTU system upgraded in the manner described here will withstand significant natural and artificial interferences.

4.4. Software and Configuration Upgrade methodology for the Enhanced RTU

Changing the RTU configuration and software on-site is accomplished through suitable changes in the PLC programs. The upgrades proposed here will provide lower latency, more granularity, and more directly complete sensor, actuator, and control state data for local alarms and upstream control systems and operators. These will enable faster and better after-action investigations and enable upstream decision support to guide non-specialist utility field operation crews. In addition, the remote telemetry unit upgraded in the manner described here will withstand significant natural and artificial interferences. Finally, the RTU data logs will provide maintenance flags based on sensor inputs and system maintenance models.

4.5. MBSE Based Architecture for the Enhanced RTU

Model-Based Systems Engineering (MBSE) principles emphasized the practical aspects of translating user needs into operationally effective, affordable, and supportable systems [2]. Enhancing the existing RTU to withstand physical and Cyber-attacks, respond more quickly to attacks, and have local mitigation options against attacks will help ensure the safety of the water users. According to Isenberg (2002), in terms of external vulnerabilities, the primary terrorism risk exposure resides in water utility systems, which is in stark contrast to the concept of large reservoirs and Water Treatment Plants (WTPs). The RTUs are used extensively in water utility and therefore need protection.

A successful application of Model-Based Systems Engineering (MBSE) and MBSAP begins with the activities required to understand the problem space, the requirements and constraints of the program, and the role of modeling in achieving a satisfactory system solution [2]. For that matter, a systematic approach using MBSE to enhance existing RTUs will follow along with the requirement, analysis, design, implementation, verification, and validation to

design a robust RTU for water utility systems. Chapters one and two describe the need to secure water utility systems (water treatment and distribution and wastewater treatment).

4.6. Model of the Enhanced RTU

The enhanced RTU is designed using the Model-Based Systems Engineering (MBSE). It allows better development, analysis of systems, better consideration of activities and functions, better decomposition of subsystems, and final product testing to ensure stakeholder satisfaction. However, integrating the system into the existing water utilities, RTUs use PLC programming languages like the ladder logic. For example, the existing RTU for most water utility companies uses Ladder Logic as the primary programming language [28, 37].

Ladder Logic is the most commonly used PLC programming language. It is graphically programmed with simple contacts that simulate the opening and closing of relays, counters, timers, shift registers, and math operations. However, it is not the only language used in PLCs. Others are Functional Block Diagram, Structured Text, Instructional List, and Sequential Function Chart.

In the United States, the most common language used to program PLCs is Ladder Diagram (LD), also known as Relay Ladder Logic (RLL) [37]. Furthermore, Ladder logic is widely used to program PLCs, which require sequential control of a process or manufacturing operation. In addition, ladder logic is helpful for simple but critical control systems or reworking old hardwired relay circuits [28].

Furthermore, Ladder logic, the primary programmable logic controller (PLC) programming language, is simple and represented graphically as relay contacts and coils. Ladder logic does a lot more today than it used to. PLCs are commonly used for analog control, tracking part data (barcodes, test results, calibration), controlling motion, and many other tasks.

Nevertheless, ladder logic is still the dominant language [37]. Appendix C is the ladder diagram of the Secured Robust RTU.

4.7. Component Selection for Enhanced RTU

4.7.1. Video Surveillance solutions

An example of a secured video surveillance Honeywell MaxPro NVR & Video Surveillance solutions [45] can help increase security across various applications in small to medium installations. The MaxPro NVR uses Honeywell's high-definition cameras as part of a high-definition, powerful IP recording system and viewing [45]. Again, It is an open platform that supports integrations with many third-party devices and includes 360-degree camera support and a standard for a real-time streaming protocol (RTSP). Mobile apps, web clients, and desktop clients allow easy system management from whatever device works best. As long as adjacent cameras cover the area, one can use the video surround feature to track subjects as they move between areas with a simple double-click on the panel where they are visible.

Fig 19. Honeywell MaxPro NVR Video Surveillance [45]

4.7.2. Pro USB Flash Drive Audio Recorder Voice Activated [41]

The Pro USB Flash drive with voice activation, 25-day standby life, and 24-hour continuous recording provides a recorded date and time-stamped files on Windows or Mac computers for evidence gathering during physical attacks on RTU or MTU. It also provides adjustable record quality settings, allowing PCM, XHQ, or HQ for better sound quality with a clear voice recording with the built-in embedded amplified mic. It is simple in construction and used with no lights to indicate its recording. Again, the Pro USB Flash drive pick-up a voice range of 40 feet in optimal conditions. Finally, it provides a 2-hour recharge rate, 8GB memory, can store up to 24 hours in PCM, 144 hours in XHQ, and 288 hours in HQ mode [41].

Fig 20. Pro USB Flash Drive Audio Recorder Voice Activated [41].

4.7.3. Switch Snap Action SPDT 4A 250V

The snap action limit switch is a snap action SPDT 4A 250V. It is robust, sealed against gasses and moisture, used in explosion-proof areas. Again, it operates within 20°C to 60°C and is suitable for RTU locations. Moreover, it is affordable and can easily be mounted inside the RTU cabinet [46].

Fig 21. Switch Snap Action SPDT 4A 250V [46]

4.7.4. 900 MHZ YAGI Antenna

Fig 22. RFMAX RY-900-2-7-SNR-19 Yagi Antenna [43]

The RFMAX RY-900-12-7-SNF-19 is a heavy-duty, Gold Anodized, 900 MHz Yagi Antenna operating within the 880-960 MHz ISM frequency range [43]. This TY900 antenna model is the RFMAX "premium" offering, with a total IP67 rating to withstand severe outdoor weather conditions. The SNR-19 Yagi Antenna is suitable for 900 MHz spread spectrum applications, SCADA system radios operating in the unlicensed 896-940 MHz frequency range, and all applications working in 900 ISM Band. It features 360-degree welds around each of the

seven elements, no gamma match to ice up, corrode or detune, and has gold anodizing added for overall corrosion resistance.

Key features [43]:

1. Suitable for RTU stations in Water utility
2. Frequency: 880-960 MHz
3. No. of Elements: 7
4. Dimension (LxH): 24 x 6.6 inches
5. Peak Gain: 12.2 dBi
6. Max Input Power: 200 watts
7. Wind Survival Rating: 136 MPH
8. Cast Aluminum Mounting Kit Included
9. 19 Inch Cable & N-Female Connector
10. Provides performance and durability

4.8. Chapter Conclusions

The study indicates that many existing RTUs can be upgraded at a reasonable cost. Others will need replacement. Ultimately an enhanced RTU will include sufficient functionality to rebalance the entire Field Device-RTU-MTU-SCADA-Control room signal chain. However, that is a longer-term program. The enhanced RTU's benefits include more detailed emergency messages to the local law enforcement, and emergency response units provide quicker response time, restoration time, and forensic data. Finally, critical security alerts will be transmitted to

surrounding utilities to enable systemic responses and activate countermeasures and security alerts.

MBSE is the current industry practice for managing complexity and optimizing delivered capability in information-intensive systems and enterprises [2]. It allows for better designing, analyzing, and troubleshooting complex systems, and it would have been great if, after the system development cycle processes, it could be uploaded into the RTU directly.

CHAPTER 5: DISCUSSION OF ENHANCED RTU COMPARED TO EXISTING RTU

5.1. Introduction

The enhanced RTU design considers the existing RTUs and supports the integration. As a result, the enhancement will reduce the water utility services' cost, time, and interruption. The enhanced RTU system will have all or most of the existing RTU components and the proposed components, namely the Video recorder, Intrusion alarms, and the Black box. In addition, the enhanced RTU will provide physical security at the RTU sites and against any physical attacker trying to manipulate process setpoints.

5.2. Enhanced RTU Subsystem

The enhanced RTU will have hardened communications to prevent attacks from bad actors and protect field devices that control the process. A first-level mitigation strategy is to upgrade the RTU to make it robust for hackers and threat actors. Another level in preventing and mitigating cyber-attacks requires alerting individual first responders, identifying potential vulnerabilities entry and exit points, enumerating possible countermeasures for the threats, and system restoration options. The remote telemetry units are downstream from SCADA, so exploits can often propagate to field devices and the central WUS. Since the SCADA and RTU connection is central to systemic damage, it must be considered in any upgrading of the RTU.

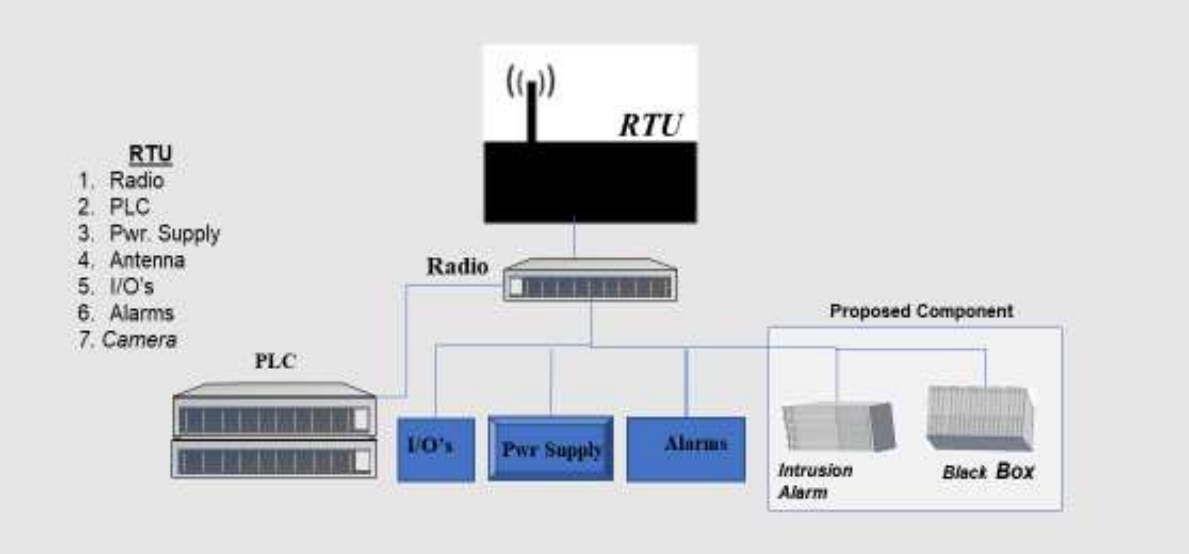


Fig. 23. Proposed RTU components showing Intrusion Alarm and Blackbox

The enhanced RTU system will have all or most of the existing RTU components and the proposed components, namely the Video/intrusion alarms and the Black box. The Intrusion alarm will signal for an actor's physical presence while the video recorder will capture the perpetrator's activities and voice. A control room operator will receive an alert and a real-time video of the RTU site event.

5.3. Differences between the Enhanced RTU and Existing RTU

The use of system engineering to improve Water Utility Systems by enhancing existing RTU is an essential step in protecting critical water infrastructure. The survey of the existing RTU, literature review, questionnaire results from peers all point to the need to enhance existing RTUs. This assertion aligns with the author's years of experience with field devices-RTU-MTU-SCADA chain systems. Table 5 shows the significant differences between the enhanced RTUs and the existing RTUs.

Recent attacks on water utility systems have led to erroneous ransom payments to cyber attackers while keeping it quiet to maintain stakeholders' reputations and leaving the issues

unresolved. It is evident from table 5 that it will take a joint effort to resolve this issue, and therefore every little contribution is significant to saving lives.

Table 4. Differences between Enhance RTU and Existing RTU

Feature/Component	Enhanced RTU	Existing RTU
Design	- The use of MBSE principles and CAMEO Enterprise software helps identify and eliminates soft targets in the system. -Provides a Systematic approach: Requirements, Analysis, Design, Implementation, V/V, and implementation.	Unable to identify soft targets due to no structural engineering principles.
Data Monitoring	Data entry and exiting RTU is monitored within the setpoints of the process and **cannot be altered** by **external means.**	When executed, data from MTU to RTU can be altered when a bad actor gains access.
Intrusion Alarm	Physical access to RTU will trigger an alarm to CRO, Management, and First Responders.	Access to RTU generate no alarm.
Forensics	Captured Audio/Video for forensics and investigation	No Video/Audio is captured
Blackbox	Data is recorded and stored in the Blackbox for forensics.	No Blackbox in existing RTU
Real-time Monitoring	Enhanced RTU provides Real-time monitoring of physical and cyber-attacks.	No real-time monitoring from physical or cyber attacks
Response Time	Faster response time to alert and capture data	Dependence on CRO for alerts.
Cyberattack Detection	RTU will detect attacks by comparing data requests and setpoint values to alert stakeholders.	RTU processes requests when received from MTU.

5.4. Process of Incorporating Robustness in RTU Design

The enhanced RTU modifies the system configuration and incorporates the new system models. The good news is that changing the physical RTU configuration and software on-site can often be done through software in the PLC programs. Utility system operations crews are

often the initial responders to breaches or exploits. Most remote stations do not have water utility workers at night. Therefore, operators, engineers, and technicians know what is happening at remote locations through central system data derived from RTU data.

Remote terminal units deliver current status information of physical devices connected within SCADA. The upgrade proposed here will provide lower latency, more granularity, and state data control for local alarms, upstream control systems, and operators. In addition, the upgrade will enable faster and better after-action investigations and decision support to guide non-specialist utility field operation.

Although the water leaving a treatment plant typically meets EPA's water quality requirements, water could degrade via normal system aging and interrupts or deliberate tampering during its transit through the various distribution system components (e.g., storage tanks and pipes) and become unsuitable for human consumption [4]. An upgraded, enhanced RTU will utilize water quality data from sensors measuring water quality to mitigate these extrinsic events. These data will be used in embedded functionality and recorded in the black box monitoring component. In addition, the enhanced RTU will communicate to stakeholders and CRO based on role and need to enhance system maintenance and restoration operations.

Data flow into RTU comes in two main ways. First, data flow between the master terminal units and the RTU, as discrete or binary. Sources include binary data from an on-off switch or data from analog signals that may have been converted to binary using a transmitter or analog to digital converter (ADC). Second, data flows from field devices such as pumps, motors, and flow meters to PLC or Digital Control Systems (DCS) within the RTU system.

Some of these signals are analog, while others are digital. The PLC can accept both signals depending on the PLC type. A mediator such as ADC or DAC, or signal conditional,

makes either form of signal suitable for transmission. Figure 25 is a data flow diagram of an RTU showing the major subsystems and their connectivity for most existing RTUs. This diagram is a baseline for most RTUs and will be the starting point for the upgraded RTU.

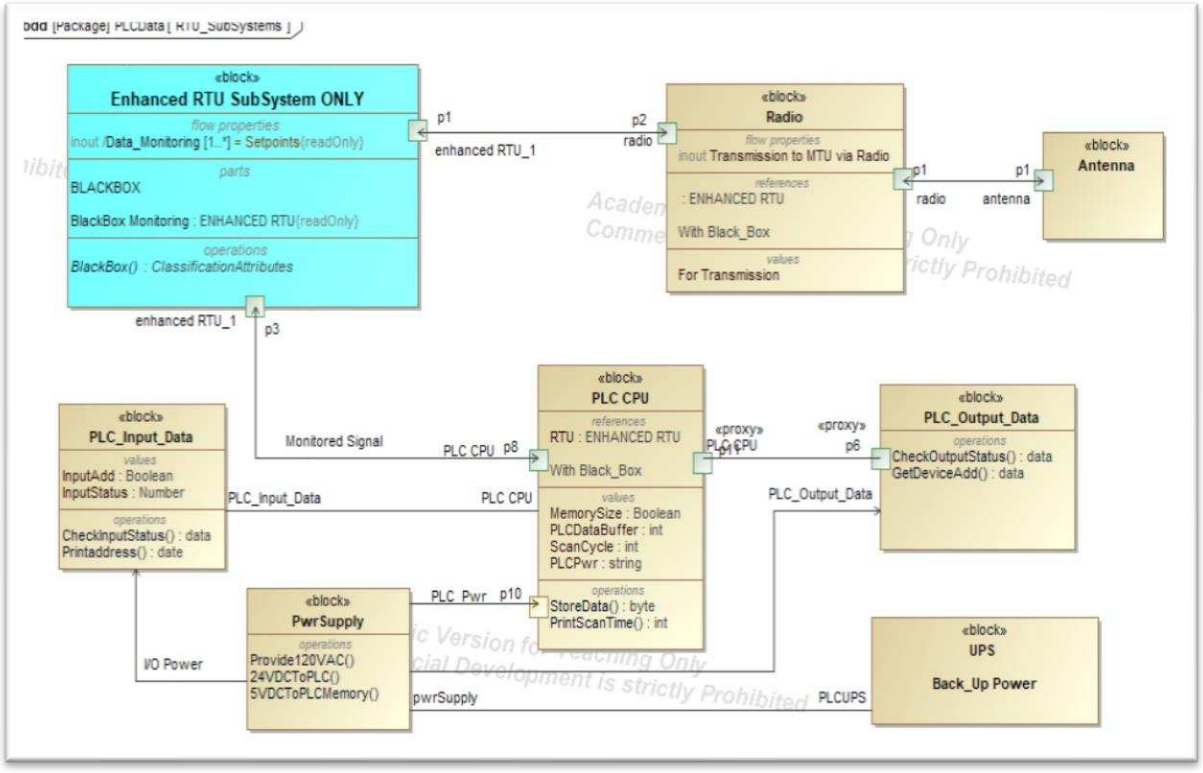


Fig. 24. SCADA Subsystems with Enhanced RTU

Data flow into RTU comes in two main ways. First, data flow between the master terminal units and the RTU, as discrete or binary. Sources include binary data from an on-off switch or data from analog signals that may have been converted to binary using a transmitter or analog to digital converter (ADC). Second, data flows from field devices such as pumps, motors, and flow meters to PLC or Digital Control Systems (DCS) within the RTU system. Some of these signals are analog, while others are digital. The PLC can accept both signals depending on the PLC type. A mediator such as ADC or DAC, or signal conditional, makes either form of

signal suitable for transmission. Figure 24 is a data flow diagram of an RTU showing the major subsystems and their connectivity for most existing RTUs. This diagram is a baseline for most RTUs and will be the starting point for the upgraded RTU.

Chapter 5. Summary

This chapter explains the significant differences between the existing RTU and the enhanced RTU components, data flow, and signal propagation to stakeholders, including water utility management, control room operator, and first responders. In addition, the chapter explains why the enhanced RTU will benefit water utilities by providing lower latency, more granularity, and more directly complete sensor, control state data for local alarms, upstream control systems, and operators.

CHAPTER 6: SECURITY RESPONSE OF ENHANCED RTU UNDER THREAT AND EXPLOITS

6.1. Introduction

This chapter compares the response of the existing RTU to that of the Enhanced RTU when the utility is under physical attack, cyber-attack, or a combination of attacks. The comparison is facilitated by looking at the system from different behavioral viewpoints. Specifically, by having the design architecture of the enhanced RTU developed using MBSE to show the data flow, the time response of data transmission, and the connectivity of the RTU within the SCADA (SCADA-MTU-RTU-field devices) system in the face of threats and exploits.

6.2. Chapter Objectives

This chapter aims to elucidate differences amongst the existing and enhanced RTUs in exploit attack circumstances to identify and estimate the benefits of enhancements. It will also provide a way to evaluate differences in responses to exploits not discussed or even attempted at this time. This objective will be attained with a three-step process:

First, existing RTUs will be described and predictions using the new enhanced RTU components and how the Enhanced RTU would have performed under such attacks;

Second, the comparison draws on the responses of industry-standard PLC models for all the components;

Third, the comparison is made of the amount of reduced attack vulnerability, faster restoration of operations, more effective first responder, and forensic responses arising from providing now presently unavailable information.

6.3. Examples of Attacks on RTU

When bad actors capture or take control of an RTU, components settings can be altered to create life and property-threatening events. An attack causing mass casualties has yet to occur, but that is not a cause for relaxation. The World Trade Center was attacked in 1993, and "only" six people were killed. The 2001 attack killed five hundred times that amount. Three examples of water utility attacks and their consequences are described below:

6.3.1. Example 1: Loss of 120V A/C to RTU at a Water Treatment Facility- Cost and impact of Using Existing RTU Vs. Enhanced RTU

In this example, a power outage event created a risk of substantial financial cost and alarm and potentially a civil emergency arising panicked stakeholders and water users. This event occurred at a state-of-the-art water treatment facility on the East Coast. A control room operator generated a report to the on-call personnel stating that the CRO could not see or control critical processes from SCADA (hence the RTU). The CRO could not see alarms or functionality reports flowing from the field components to the RTU, MTU, from there to the SCADA, and from the SCADA back to the Control Room. The field components in this example were water utility tanks, booster stations, and pressure-reducing valves. Therefore, the CRO had no way of monitoring the processes, setpoint changes, or initiating an automated contingency plan. Ad hoc actions would likely have exacerbated the situation. In a military facility, this sort of situation would have activated a "security alert," but in even an advanced water utility, it was treated as a typical operational event.

This water utility has provided safe, reliable, quality, sustainable, and affordable water services to over 1 million people in its urban community for over 100 years. A significant exploit

with substantial damages would damage its credibility and reputation, potentially causing fatalities, financial losses, equipment damage, and community emotional losses. In this example, the malfunction caused utility operators and engineers to work overtime to maintain utility services manually since automated functions usually provided by even an existing RTU were unavailable. This incident lasted for days until the systems were restored to operational conditions (Table 5). Figure 26 depicts the sequence of events that occurred in this cyber attack

This incident spread customer fear, utility staff overtime costs, EPA violation fines, and personnel costs for keeping the system going, diagnosing the problem, and ultimately restoring operations. The exploit also resulted in substantial exposure to additional or follow-up exploits arising from diverting attention from regular tasks such as monitoring water treatment chemicals for process setpoints, PH, water flow, and system pressure.

In this situation, had an event and configuration logger been included in the RTU, as proposed for the enhanced RTU, the mitigation responses would have limited exploit damage because they would have been able to inspect event logs and damage location. Furthermore, stakeholders, utility executives, first responders, and law enforcement would have received a common operating picture so that stakeholders would have been able to deploy resources more rapidly and more efficiently.

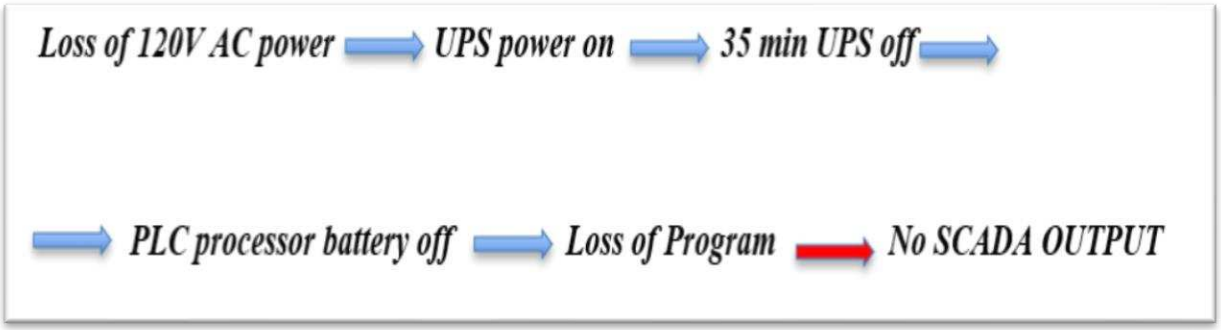


Fig. 25. Loss of 120V A/C to RTU at a Water Treatment Facility

6.3.2. Differences between the responses

The Existing Water Utility RTU responded to the power Loss as follow:

- Loss of 120V A/C power, UPS power off after approximately 35 min.
- Loss of PLC power.
- Finally, Loss of PLC Ladder Logic program.
- No communication from RTU to MTU
- No input to SCADA
- CRO sees blank SCADA screen.

The Enhanced RTU will be part of the utility emergency response as follows:

- Enhance RTU will log the traffic to the devices connected to it.
- Enhanced RTU will trigger audio and video recording around the RTU.
- Enhanced RTU will send an Alarm to MTU upon losing 120V A/C power to the RTU (Security Alert).
- The RTU will detect out-of-range signals or signal rate of change and respond to maintain system stability, performance, and survival.
- MTU would scan other RTUs for security alerts and report the location, event type, and number of RTUs experiencing upsets.
- Data aggregated at the RTU location will transmit to MTU upon receipt of a valid data extraction certificate and from there to the SCADA.
- The SCADA would scan other utility information systems and nearby utilities and send a common operating alarm picture to the control room.
- The CRO utility emergency response team will contact medical, infrastructure, and law enforcement stakeholders to determine the extent of the exploit.

- A stakeholder group would decide which type of forensic, first responder, and restore operations plans are best in this situation.

None of this functionality exists now. Implementing it will vastly enhance the effectiveness of incident response and reduce the time to manage and mitigate utility damage.

The embedding of a data logger event and configuration recorder and data checker, while commercially available, is not yet integrated within utility operations. Will provide local intelligence nearer to the data source and do so at costs compatible with other system components. Once deployed, it will record data and configuration values, detect suspicious or unallowed changes in value, and perform simple statistical tests of data from sensors, actuators, control systems, associated configuration, and operating parameters.

6.3.3. Estimated Costs of Damage between the two RTU's:

The ENHANCED RTU will reduce or prevent the following losses that will be incurred for water utilities using only existing RTU's:

- On-call overtime/Emergency pay for days
- Loss of UPS and associated costs
- Loss of PLC Program, and costs of reinstalling PLC program by the Programmer.
- The costs to maintain order and deal minimize regulatory and litigation costs by demonstrating best available technology due diligence.
- Danger to water treatment processes, including chemical mixers and dosages.
- Costs of EPA and other state and local environmental agency violations fees.
- Maintaining quality of water to customers, health issues, and court settlements and fees.

6.4. The Case of a Security Breach at a Water Treatment Facility in Harrisburg, PA.

A second example of how an enhanced RTU will mitigate a security breach is seen in the case of a water treatment facility in Harrisburg, PA, in 2006.

A hacker planted a computer virus on the laptop computer of an employee. The hacker operating outside the US then used the infected laptop as an entry point to install malicious software on the plant's computer system. Furthermore, the report stated that the attack could have affected the plant's normal operations. For example, it could have altered the concentration levels of disinfectants in the portable water [28]. Damages caused by the attack are still being assessed, including SCADA equipment replacement and software upgrades, monitoring services, a new physical server, and professional services.

6.4.1. Harrisburg PA: Differences in exploit damage estimates between the two RTUs.

The Harrisburg cyber attacker accessed the existing RTU and others available to the employee's personal computer by planting a computer virus on an employee's laptop computer. The attacker, at this point, could have used that access to harm any subsystems within the WUS. For example, the attacker could have sent a dangerous request to MTU - RTU chain to increase or decrease setpoints to the field devices, including chemical mixers, dosages, system pressure, chlorine level, and storage tanks. The existing RTU will accept requests from MTU and will execute the request.

On the other hand, the enhanced RTU would have detected a request from MTU that was outside the allowable limit of the process setpoint. At that instant, the Enhanced RTU would trigger on the event that any preset limits were exceeded, or other preset events trigger mitigation actions send prioritized alerts along with aggregating RTU inputs and outputs.

In parallel to this, prepare a support information package. Upon a certified data pull request, these data will be delivered to the MTU.

The enhanced RTU has its own security rules built into the PLC and the event recorder, such as those described below;

- Enhanced RTU will not respond to commands that set operating parameters outside the minimum and max set points.
- Enhanced RTU would prepare and transmit data packets for transmission to the MTU and perform preset mitigations such as throttling processes and triggering video and audio situation recording.
- First responders get situational awareness from all the RTUs upon receiving a certified extraction ticket from the RTU.
- The RTU packets are aggregated into a report by the MTU and sent to the Control Room through the SCADA.

Upon receipt of situation reports from RTUs, MTU, and SCADA, the first responders begin medical, forensic, public communication, and restoration of operations. Utility operators manage the water utility control system.

6.4.2. Cost of Damage estimates for the two RTUs

The cost of damage was estimated to be ongoing and very substantial, including deaths, hospitalization, destruction of critical national infrastructure, environmental effect, EPA violations and fines, contamination of water, water users, and WUS employees' private data [6, 20, 37]. The investigation continues, and the authorities are still trying to attribute the full attack and end the consequences.

Because of its near real-time response for alert and mitigation, the Enhanced RTU would have provided faster and more detailed incident parameter values to Management and other incident response stakeholders. It is faster and more complete by definition since no such data and reports are available now. This provides extra time, location, and incident description information that is the lifeblood of any incident response and would save substantial damage and attack attribution time. Any time saved can be translated into dollars and utility mission performance metrics.

6.5. A Hacker Remotely Accessed the Oldsmar Florida Water Treatment Plant – Cost and Impact estimates Using Existing RTU Vs. Enhanced RTU

A hacker remotely accessed the Oldsmar Florida water treatment plant through the MTU, RTU, and chemical treatment subsystem [20, 37, 52]. The target was the subsystem that controls the chemicals added to the water to make it safe to drink. According to the local sheriff, the exploit changed the level of sodium hydroxide (lye) from 100 parts per million to 11,100 parts per million [37]. This hack took five and a half hours for an employee to notice the change on the SCADA screen.

A later report released by Security Today [52] found that the website hosting the watering hole attack code was a Florida water utility contractor site. Once the harmful code was inserted into the legitimate site, the attacker collected information. The report also indicated that the hack started on December 20, 2020 and stayed on the SCADA until February 16, 2021. Finally, the report indicated that the actor also likely used the desktop sharing software Team Viewer to gain unauthorized access to the system [52].

The WUS IT subsequently instructed this plant operator to shut down SCADA to restrict remote access. The attack sequence traveled through the internet using a contractor channel and entered the plant's remote access system. Then, the compromised commands passed through the MTU down to the RTU. Finally, data from the RTU was transmitted to the controller/actuator for adding Sodium Hydroxide to the water [20, 37].

6.5.1. Differences between the Responses

For this cyber-attack, the Existing RTU response added little to secure the health of water system customers:

- It Depended on how long and what actions the operator took.
- Systems relying on human intervention to catch perpetrators have a limited probability of stopping most attacks.
- Existing RTUs would have communicated to field devices to execute the cyber attacker's requests.
- Existing RTUs will not detect and mitigate harmful commands or detect misconfiguration indicators of attack.

Under the same cyber-attack, the Enhanced RTU would have performed the following:

- The Enhanced RTU will not respond to commands outside the minimum *and max* set points process.
- Enhanced RTU would send emergency alarms data sets through the MTU.
- The Enhanced RTU has preset setpoints and changes ranges for field components. Out-of-range values or change ranges will energize a Critical Relay to aggregate data for transmission up the control chain.

- The Enhanced RTU does not depend on individual operators catching the manipulation of process setpoints to issue persistent alerts. Individual operators are best at detecting attack patterns and choosing the most effective responses amongst a group of alternatives.
- The enhanced RTU is an automated system that mitigates major impacts faster than manual detection of existing RTUs and aggregates situational awareness data. This will far exceed existing emergency response capabilities.

6.5.2. Estimated Oldsmar Cost of Damage for the two RTUs

The Enhanced RTU would have detected and reported chemical set point manipulation. Then, depending upon pre-programmed actions, it could have, paused or shut down the valve and reported them to those in the emergency response chain in near real-time. As a result, the system would not have relied on a skilled operator who was at the right place at the right time. All critical process setpoints showing min and max instantaneous values or average values over preset times will be monitored and logged. RTU responses will also be pre-programmed and include triggering alarms, sending alarms to the MTU and SCADA to see other suspicious events in other parts of the water utility, throttling down the process, or activating valve isolations.

The Enhanced RTU would have improved the Oldsmar Florida Water Treatment Plant system response by shortening the response time and preventing excessive dosing. This figure is an activity diagram. The black box shown in the enhanced RTU monitors data from the MTU by comparing the data requested to data setpoints of the process variable. The process setpoints are fixed and cannot be altered by any external means. Unfortunately, the bad actor has penetrated through SCADA and sends irrational setpoint altering requests from MTU to RTU.

The function of the enhanced RTU is depicted in the activity diagram (fig 27), involving specific actions and object exchanges. The enhanced RTU has an embedded data logger that logs the inputs of all the critical set points to be controlled. For this simulation, four process variables are selected, although, in practice, the number of process parameters can be a multiple of this number:

1. The chlorine level in the water (CL2)
2. PH of the water
3. Chemical Dosage
4. System Pressure

Regular monitoring (logging and testing) of setpoints and other configuration data by the data logger will establish a baseline for system operation at peacetime. When a cyber attacker gains access to the RTU, critical process setpoints are available for manipulation. Out-of-range setpoint or configuration values will trigger internal mitigation when possible and the transmission of alarms up the signal chain. This solution would have prevented deaths and extensive water supply damage by the Florida attacker in two ways. One is by limiting or throttling chemical dosages from within the RTU, and the other is by initiating a chain of events that would result in a common operating picture being sent to utility executives, first responders, and law enforcement personnel.

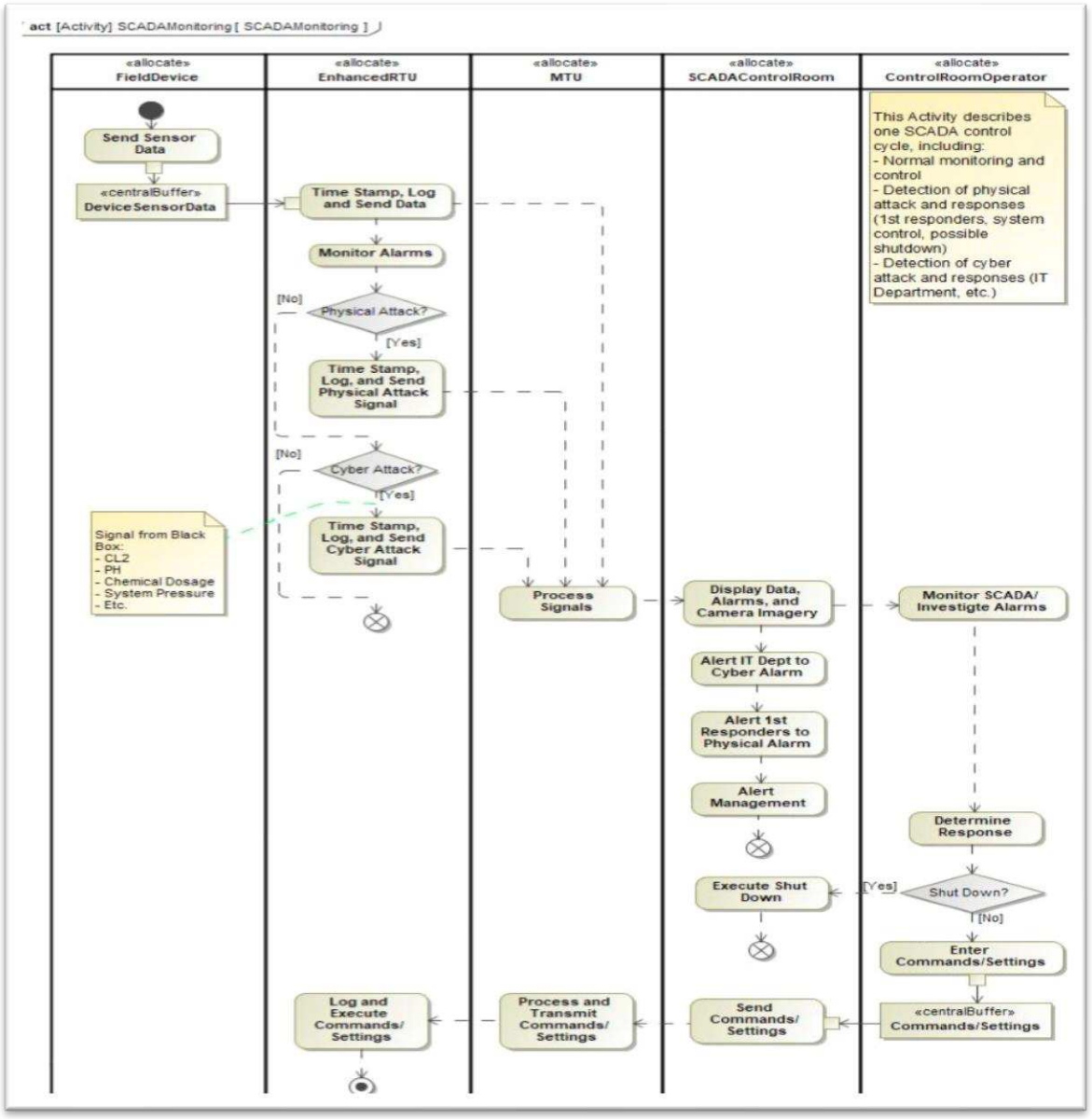


Fig. 26. Activity Diagram of Data Flow for Physical and Cyber Attacks on RTU and Mitigation

An Activity diagram (fig. 26) is an example of a behavior diagram used to represent any flow inherent in a system, such as processes, operations, or flow, to represent an action [2]. This activity diagram starts at the enhanced RTU containing the additional black box data logger. Any physical attack to the enhanced RTU will trigger a series of signals to the MTU and consequently

to SCADA. The following alarms will be activated: RTU site video/audio, alarm to CRO, first responders, and management.

The next activity is a cyber-attack on the water utility system. Presently, a cyber attacker manages to penetrate water utility SCADA and request a change in process setpoint using a GUI or PC. The request goes to MTU, and the request will be honored. The request will then go to the RTU, and the existing RTU will honor the request. Like in the case of Oldsmar, the requested change of sodium hydroxide dosage from 100 ppm to 11,100 ppm will be honored by existing RTUs. However, in the case of the enhanced RTU, the black box data logger will detect an out-of-range limit, which will trigger alarms to CRO, stakeholders including management, IT department, and first responders.

Physical attacks on the RTU and connected control systems can cause unexpected shutdowns, drinking water contamination, and wastewater release to cause human death and other environmental health issues. From an enhanced RTU viewpoint, these types of exploits would be treated in the same manner as cyber exploits, and the system's robustness would be similarly improved. The specific physical enhancements include audio and video logging of the local environment and, hopefully, the perpetrator. These data would be sent to First Responders and Management upon receipt of a valid certificate by the RTU. The unauthorized opening of the RTU door will trigger audio and video recording and the transmission of alarms to the embedded logger and data aggregator for storage and later transmission to the MTU.

6.6. Use Case of a Combined Physical and Cyber Attack

The Use Case of coordinated cyber-attack and physical attacks is shown in Fig 28, summarized below.

A bad actor launches a cyber-attack on a WUS with a malicious intention to change a critical process setpoint (for example, CL2, Chemical dosage, system pressure, or pH) to inflict damage to water users. The requested setpoint is transmitted from the SCADA-MTU-RTU chain. The RTU receives the request and compares it to the black box setpoint limits. Then, the RTU will sense an abnormality and alert CRO, stakeholders, and the IT department. The RTU will not process the abnormal request from the cyber attacker.

Furthermore, when a bad actor tries to access the RTU to change setpoints physically, the RTU will send alarms to CRO, stakeholders, first responders. At the same time, a series of alarms will be activated, including RTU site camera, CRO viewing of the site, alarms to IT and first Responders. Data gathered by RTU black box will be used for forensics and investigations. If the attack is successful, the bad actor gains access to the RTU. As described above, the enhanced RTU will prevent the manipulation of setpoints.

The Use Case for the combined cyber and physical attack on an enhanced RTU is shown in the Use Case with Combined Physical and Cyber Attacks and Mitigation strategy (fig 28). The figure depicts actions, including variations, that a system performs that yields an observable result of a value to an actor, a set of scenarios involving a common user goal [2]. A combined attack on the RTU-MTU-SCADA chain highlights the enhanced RTU functionality to detect, alert, and monitor data flow in water utility systems. Fig 28 shows that the RTU is the last component subsystem that interfaces with the field devices. Therefore, either a physical attack on RTU or a cyber-attack from SCADA-MTU or directly on the RTU (antenna example) will be detected, and inbuilt mitigation of cancellation software executed to minimize attack damage. In addition, data will be aggregated and formatted for communication back through the MTU/SCADA to stakeholders, as explained in chapter 7.

An example of this type of cyber-attack occurred in a Water Treatment Facility in Harrisburg, PA, in 2006, where the FBI suspected, for example, that the bad actor could have altered the concentration levels of disinfectants in the potable water [28]. Under the same Use Case scenario in fig 27, the enhanced RTU will prevent data manipulation send alerts to stakeholders and first responders.

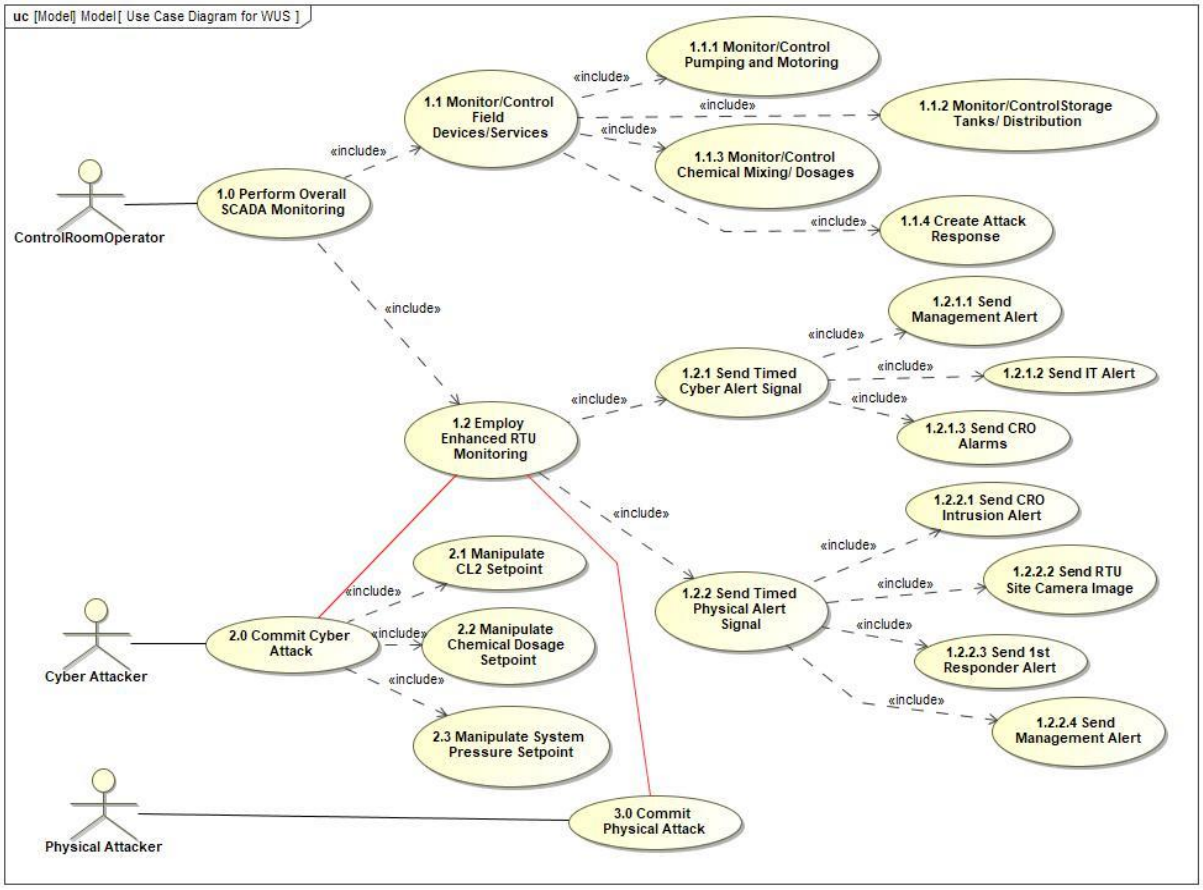


Fig. 27. Use Case with Combined Physical and Cyber Attacks and Mitigation strategy.

An existing RTU used in a water utility system is shown below. The networking, including the cloud, WAN, and LAN, forms SCADA networks [7, 10, 12, 16] created entry points for bad actors who have exploited several nodes or attack vector openings on the network sides. In addition, recent attacks on water utilities show that the water utility systems are vulnerable to cyber and physical attacks [1, 3, 6, 19].

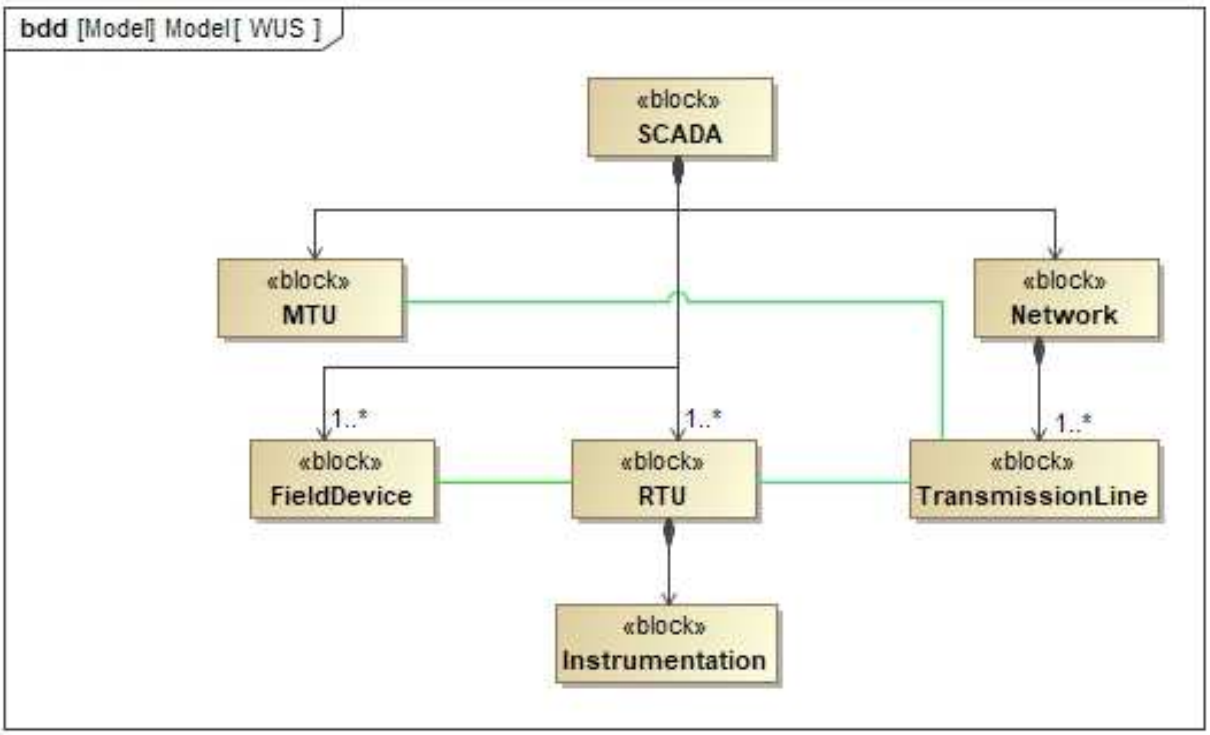


Fig. 28. Block Definition Diagram of Water Utility System with Existing RTU

Contrary to the existing RTU system in fig 28, the Enhanced RTU system is more robust, provides critical data monitoring, transmits critical alarms to stakeholders, provides data forensics, prevents process setpoints manipulations, provides time-stamped data anomalies for utility management, and finally provides video/audio information. An enhanced RTU within the SCADA system is shown in Figure 29. The block domain diagram shows the separation of the networking domain from the SCADA system and the addition of a black box data logger to the SCADA system. This design removes the entry point that bad actors enter the water utility system.

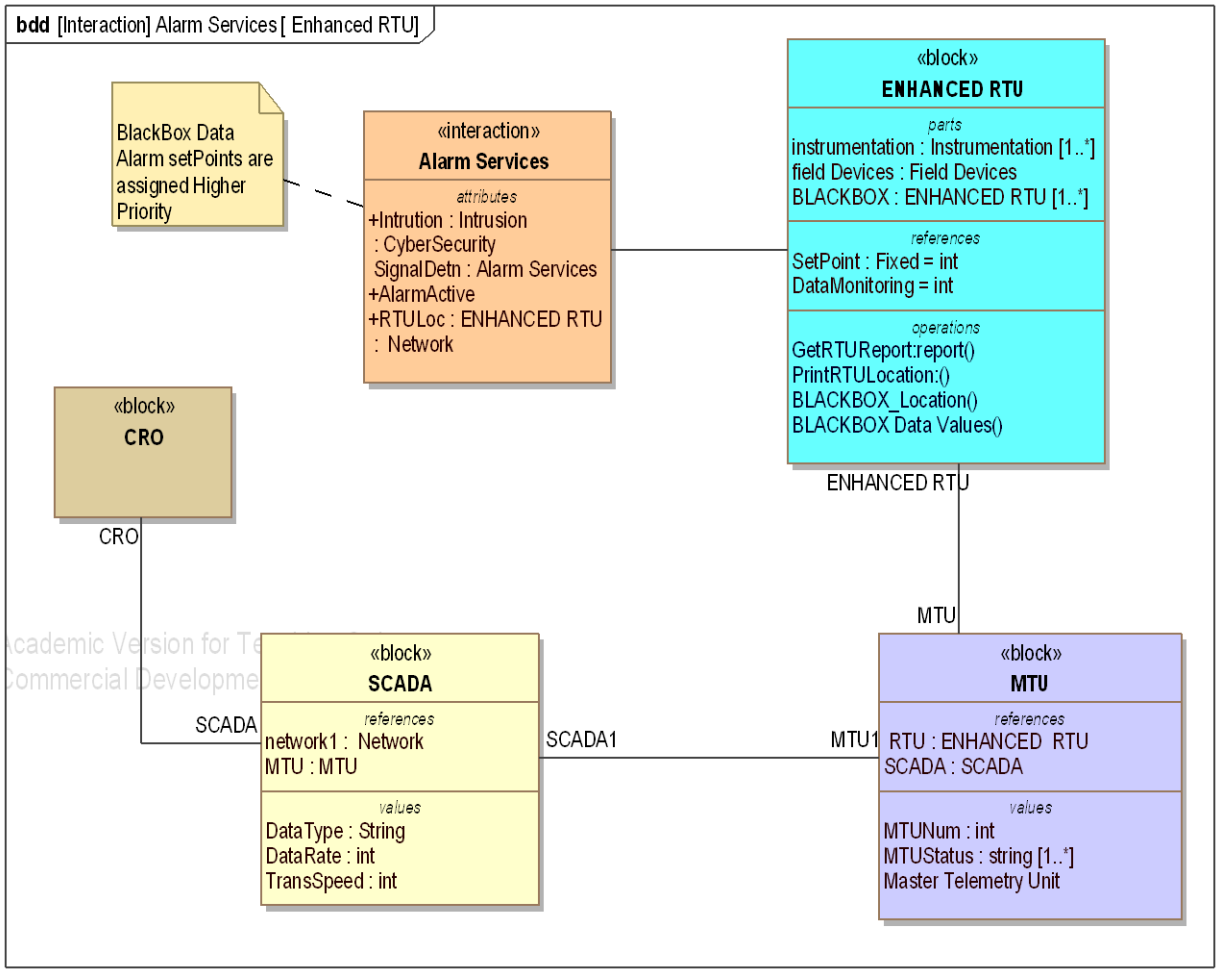


Fig. 29. Block Definition Diagram showing RTU with Black Box

6.7. The use of PLC to simulate attacks on Water Utilities:

The earlier sections of this chapter described various examples of physical and cyber-attacks on existing and enhanced RTUs. The next step is to validate this design enhancement of the proposed RTU to see if the design requirements were met. A PLC simulation of the RTU was used to accomplish this because it is the interface to the systems attackers will use to damage or degrade the water delivered to customers.

The PLC model defines which components activate or deactivate and which command to water utility operational components are carried out. This is seen by tracing the paths of cyber or physical attacks. The attacks most typically setpoints and connectivity of components attached to the RTU. Once these exploits change system parameters, the attack proceeds until an operator, customer, or other employee notices abnormal system behavior. As reported in the examples above, this attack detection can take hours, days, or even months. Much damage can occur in the interim.

In a physical attack, the actor directly accesses the RTU and either damage or destroys equipment or alters PLC instructions or settings.

At present, there are no intrinsic safeguards against these behavior modifications or component damage. Therefore, the enhanced RTU is set up to monitor component inputs and outputs and rapidly detect them.

A PLC simulation will apply to almost all utility systems. It is worth noting that other system modeling tools can create sophisticated models, but these models are not tuned to present water utility hardware. For example, MBSE is valuable in the design phase but is not yet demonstrated or certified for utility operation.

Figure 30 shows the PLC ladder logic instruction for an enhanced RTU. The RTU PLC program describes how various sensors and transducers are activated or deactivated. The figure below represents the start of a program of operation. In Chapter seven, the program will run for different attack scenarios and, at rest, how a combined physical and cyber-attack would affect the PLC program.

A physical attack on RTU triggers audio/visual signals to SCADA as follows: The first two rungs in fig. 30 show the water utility system's regular start/stop operation at peace times.

Rungs 002, through rungs 008, shows a physical attack on the RTU by a bad actor opening the RTU door. Rung 009 is the response to the remote-control room operator to initiate valve isolations. Lastly, the Black Box uses Rung 009 through 013.

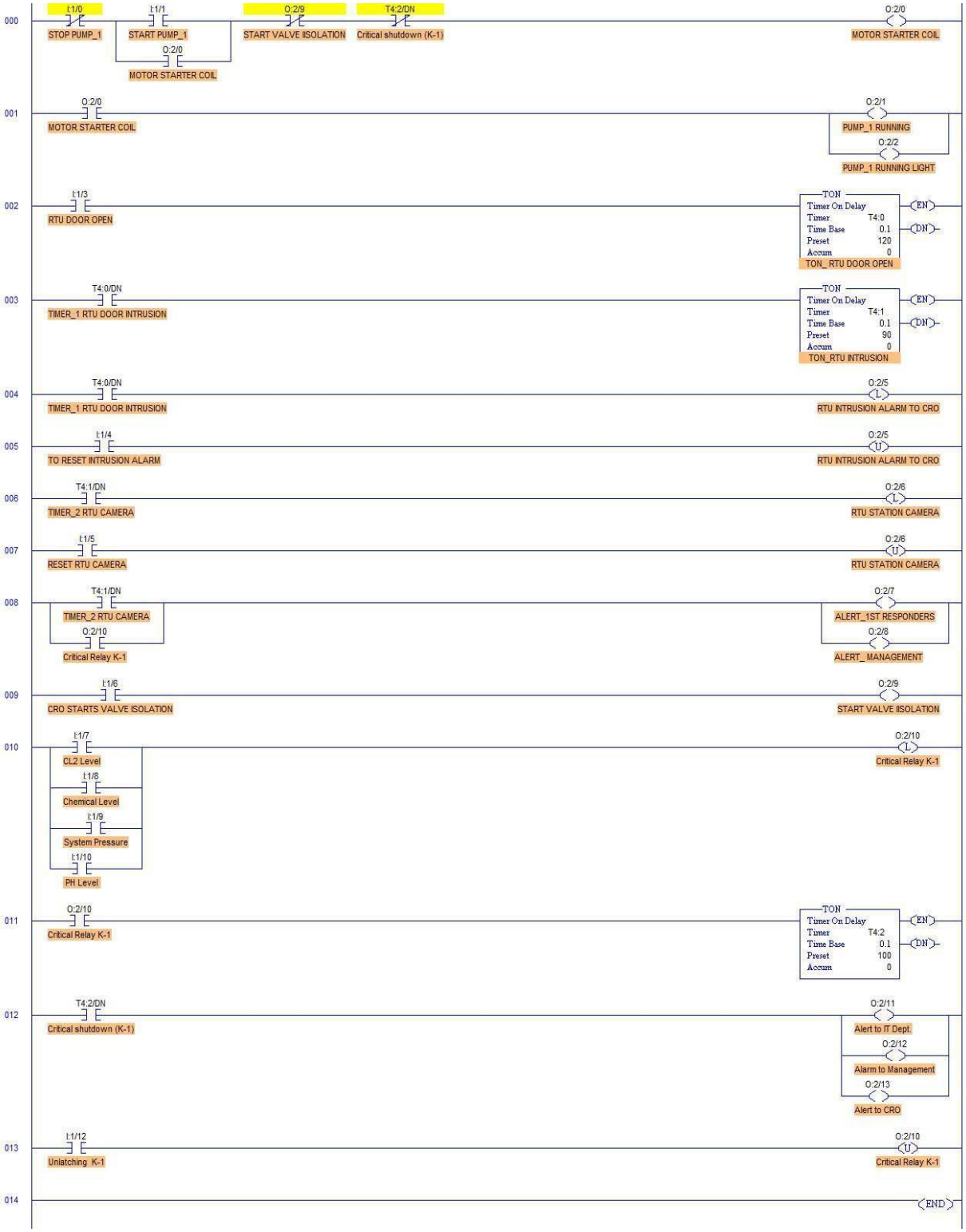


Fig. 30. PLC Ladder Logic for the enhanced RTU

6.8. Chapter Conclusions

The existing RTU and the enhanced RTU were reviewed, and their performance was examined under physical attack, cyber-attack, or a combination of attacks. The enhanced RTU's design architecture developed based on MBSE principles provides intrinsic advantages compared to present-day RTUs, explained in chapter 7. The enhanced RTU architecture shows data flow within the RTU, time response of data transmission, and the connectivity of the many RTUs within the SCADA system against threats and exploits. The comparison is of the response of the enhanced RTU to existing RTUs made by modeling both using identical industry-standard PLC models exhibit intrinsically for faster restoration of operations, first responder, and forensic responses. In addition, the RTU subsystem connects to field devices and control systems that comprise water treatment, water utility, and wastewater handling. Finally, the enhanced RTU improves the existing RTU, sending alarms to CRO and stakeholders and improving data transmission and water users.

CHAPTER 7: DETAILED USE CASE: COMBINED CYBER AND PHYSICAL ATTACK: INTERNAL AND EXTERNAL VIEWPOINTS FROM RTU

7.1. Introduction

This chapter extends the combined cyber and physical attack example summarized in the previous chapter by presenting two viewpoints. One is a field-device-centric PLC simulation since the utility operators will experience the event and respond to it. The second is a descriptive review similar to an after-action report to stakeholders and utility executives. These two viewpoints are centered around how the existing RTU and the Enhanced RTU will affect the course of the attack, the system's response, the restoration of services, and the impact of the attacks. It, therefore, will examine and verify the advantages of the enhanced RTU.

A PLC Ladder Logic program replicates the system response since it is the functional language for digitally switching and controlling the water utility control systems, valves, sensors, and actuators. Thus, it mimics the enhanced RTU behavior components as explained in the Use Case and the Activity diagrams in chapter 6. Appendix C shows the PLC Ladder Logic for the Enhanced RTU, and the behavior of the inputs and outputs as the attack unfolds. PLC Ladder Logic software was chosen since it is a vendor-independent image of the state of the devices used to perform pumping, purification, water treatment, flow controls monitoring, inputs/outputs energization, and controls. It is also the industry standard for controlling water utility RTU operations.

7.2. High-level Description of Attacks and Mitigation by Enhanced RTU:

This section extends that of chapter 5 and Chapter 6, which described the design of the enhanced RTU using MBSE principles and the use of Cameo Enterprise Architecture 19.0

software to simulate the sequence of actions, activities, responses, data flow channels, bad actor intentions, stakeholders' actions, and the Black box data logger monitoring of setpoints. Therefore, it was instrumental in choosing the devices and layout of the enhanced RTU.

These outputs depict data provide the data flow and context for the RTU components to localize an upset, forensic purpose and identify potential remediation options to help utility incident response teams and Law Enforcement. The enhanced RTU will continue recording physical, video, and audio data until they are halted and reset after restored water utility services.

7.3. PLC Simulation of Cyber-attack or Physical attack on Enhanced RTU

This section describes how the system changes in response to the simulated attack on the RTU-MTU-SCADA chain currently used at water utilities when a bad actor remotely tries to change set points a physical attack or cyber-attack on a water utility system.

This PLC behavioral ground-level simulated event shows how the device connections and setpoints are changed for both types of RTU and how the different RTU will respond in response to the attack or upset. In addition, the enhanced RTU provides state data, location, situational data, and mitigation options to minimize the impact of cyber and physical attacks. For this discussion, a physical attack will be aimed at the RTU PLC instructions to alter system behavior, while the cyber-attack will be aimed at the SCADA to change the system behavior using high-level system software API’s or GUI controls.

In a Physical-attack, an attacker decides to attack a typical structure containing an RTU that includes connections to controls and field devices, as described in chapter 6. As the bad actor gains physical access to SCADA to alter system set points such as the purification chemical concentration, the enhanced RTU near the field devices provides detection and intervention to

prevent destructive set point manipulations. Once inside, the attacker can change or disable any sensor or actuator connected to the existing RTU. The enhanced RTU, with its RTU, Latched intrusion alarm, will provide alarms and notifications as soon as this occurs and prevent setpoint changes. It is noteworthy that a typical water utility has over 100 RTUs to pump, treat and transport and distribute water and wastewater to customers. Attacks on these RTU can damage property, water availability, and human health.

Figures 31 through 40 are the PLC simulation that shows which switches are connected or disconnected, which power lines are active, and which alarms or internal control or logging routines are active. Moreover, device connections respond to either incoming PLC instructions or preset system operating instructions that the RTU and utility have configured for operation in major and under attack conditions.

The behavior of the RTU PLC simulation during this attack as explained below:

1. The RTU black box gathers forensic data, intentions, or plans of the bad actor.
2. The RTU sends alarms to stakeholders, including the information technology department, control room operator, and utility management.
3. The enhanced RTU shuts down the sodium hydroxide pump from the connected pump actuator. This rapidly ensures human safety and prevents the pumping of toxic chemicals contaminated water to users, including; houses, hospitals, military bases, farms, storage tanks, and factories.
4. The enhanced RTU alarms include priority interrupts that override the normal scan cycle to send critical data and notices to stakeholders quickly.
5. Finally, management ensures verification of isolation valves and shutdowns of SCADA subsystems, customer communications, and law enforcement.

Figure 31 – 40 shows step-by-step events and actions during the attacks. The enhanced RTU generated responses. Since PLC is an operational language, it is a good representation of the static system behavior, with differences arising from individual device dynamic parameters such as latency, switching times, execution sequence timing, and imitating the interconnection of relays to perform specific logical tasks.

Figure 30 is the start of the simulation where the water utility systems, including motor controls, pumps, and chemical mixers, are ready to start a system. At this point, all output contacts are de-energized, valves are either closed or opened.

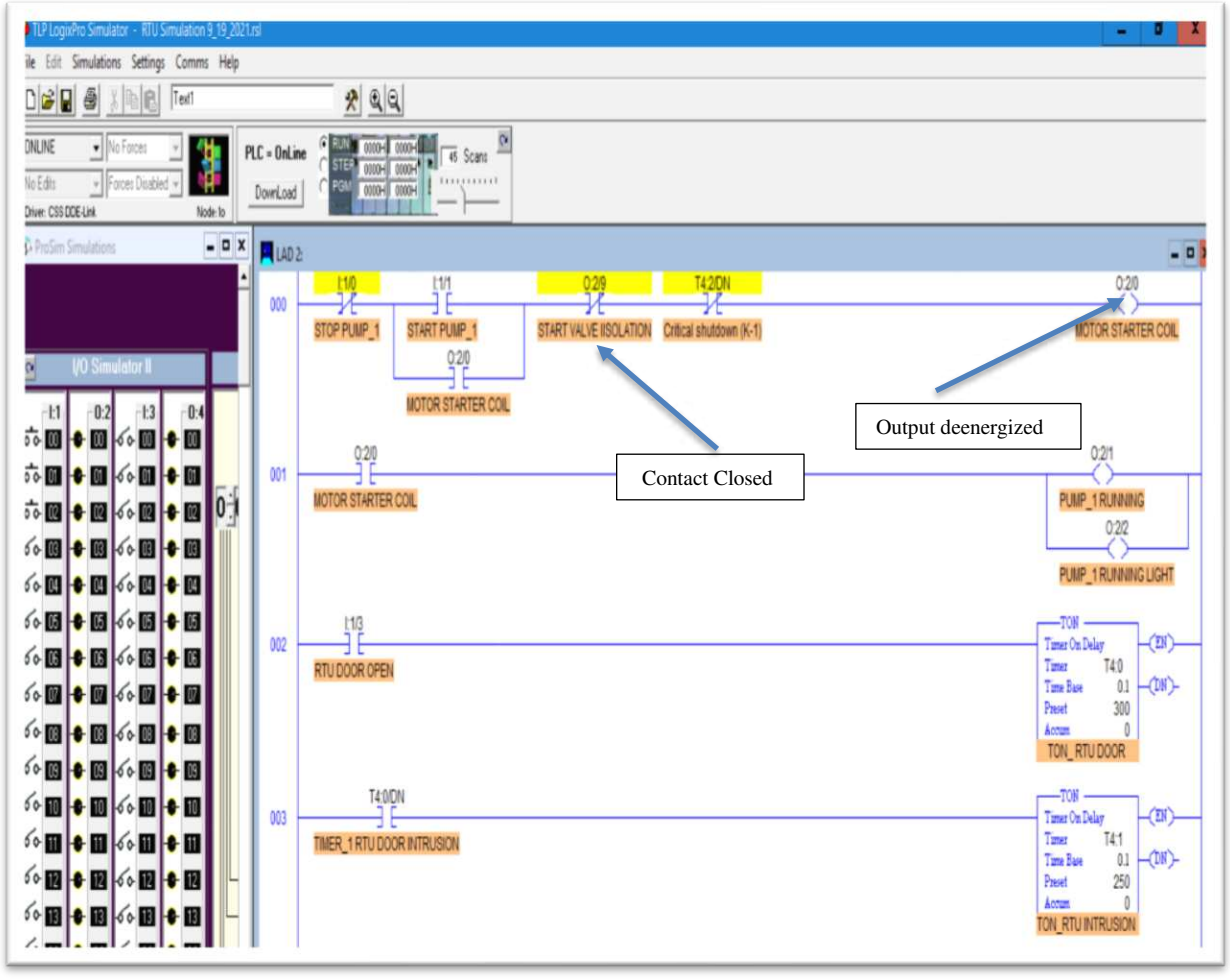


Fig. 31. RTU Simulation showing System OFF with no I/O energized

Fig 31 shows a typical peacetime operation of electromechanical devices, including pumps, mixers, motors used in water treatment and distribution, lift stations, and wastewater treatment facilities. It indicates when the start “pushbutton” (either a physical button or an instruction to make a connection) is held in a close position to complete the circuit to enable the pump and motor coils to energize and for the holding circuit to complete.

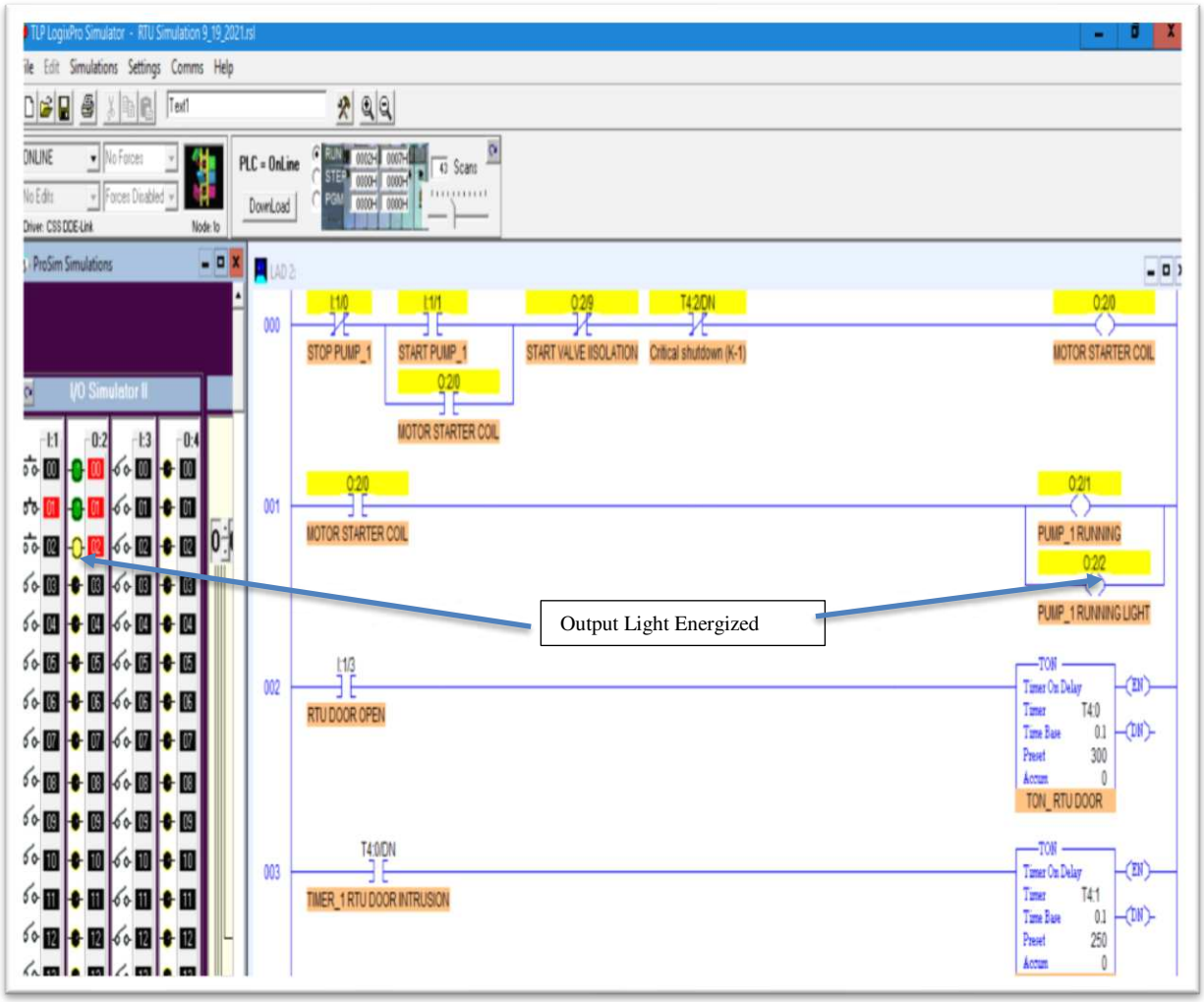


Fig. 32. PLC Simulation showing a System running in normal operation

Figure 32 also shows when the start pushbutton is held in a closed position, and the holding-contact or seal-in contact is closed to allow the pump to run normally. At this point,

indicator lights show that the pump is running, and the motor started coil energized. Again, this is just before the start push button is released.

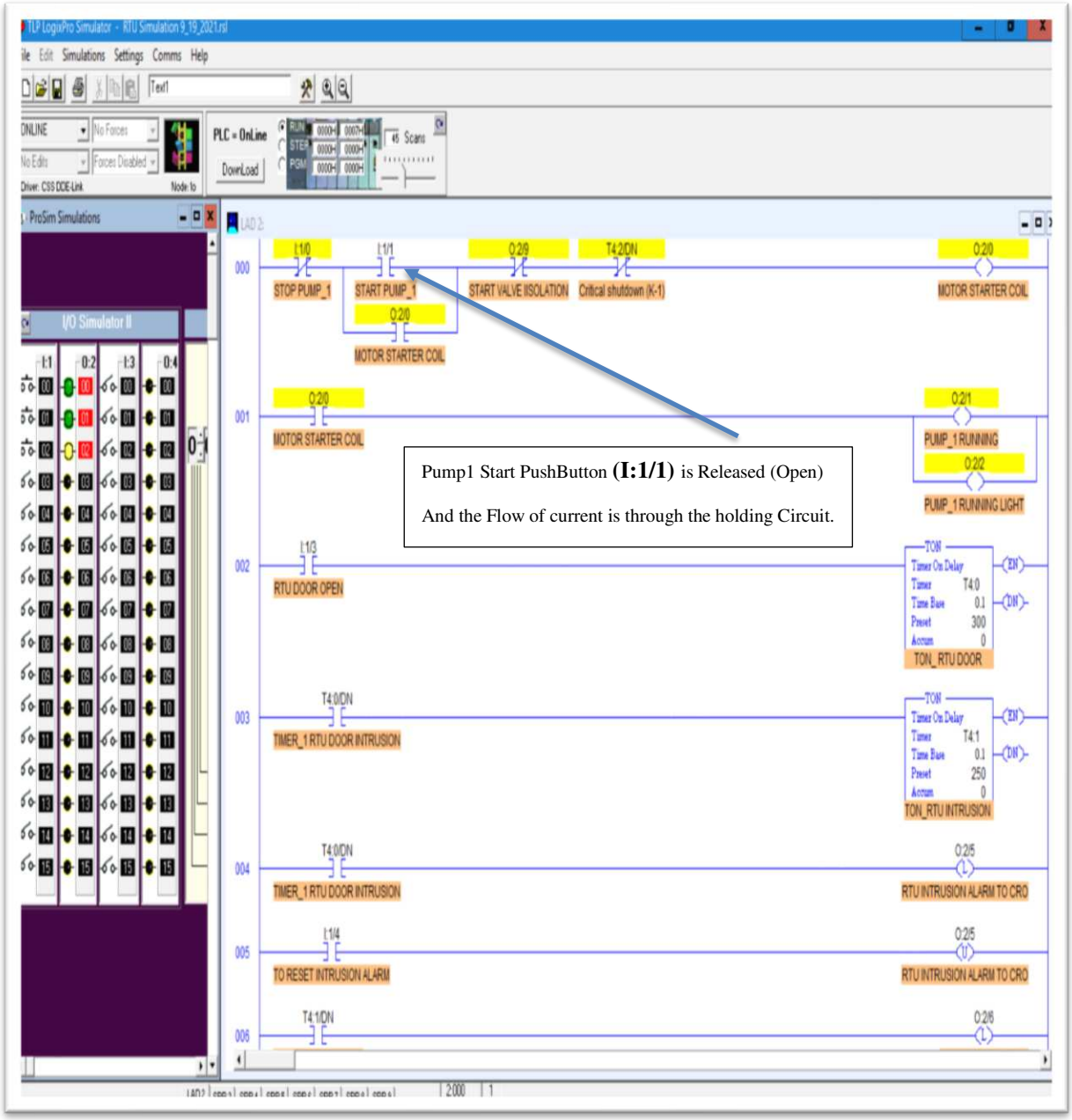


Fig. 33. RTU Simulation showing system running during normal operation.

Fig 33 shows the normal operation of electromechanical devices such as a pump after the initial energization of the start circuit, and the holding contact provides the path for electron flow

through the start/stop circuit. At this point, the system is running normally, and there are no physical or cyber-attacks on the water utility system.

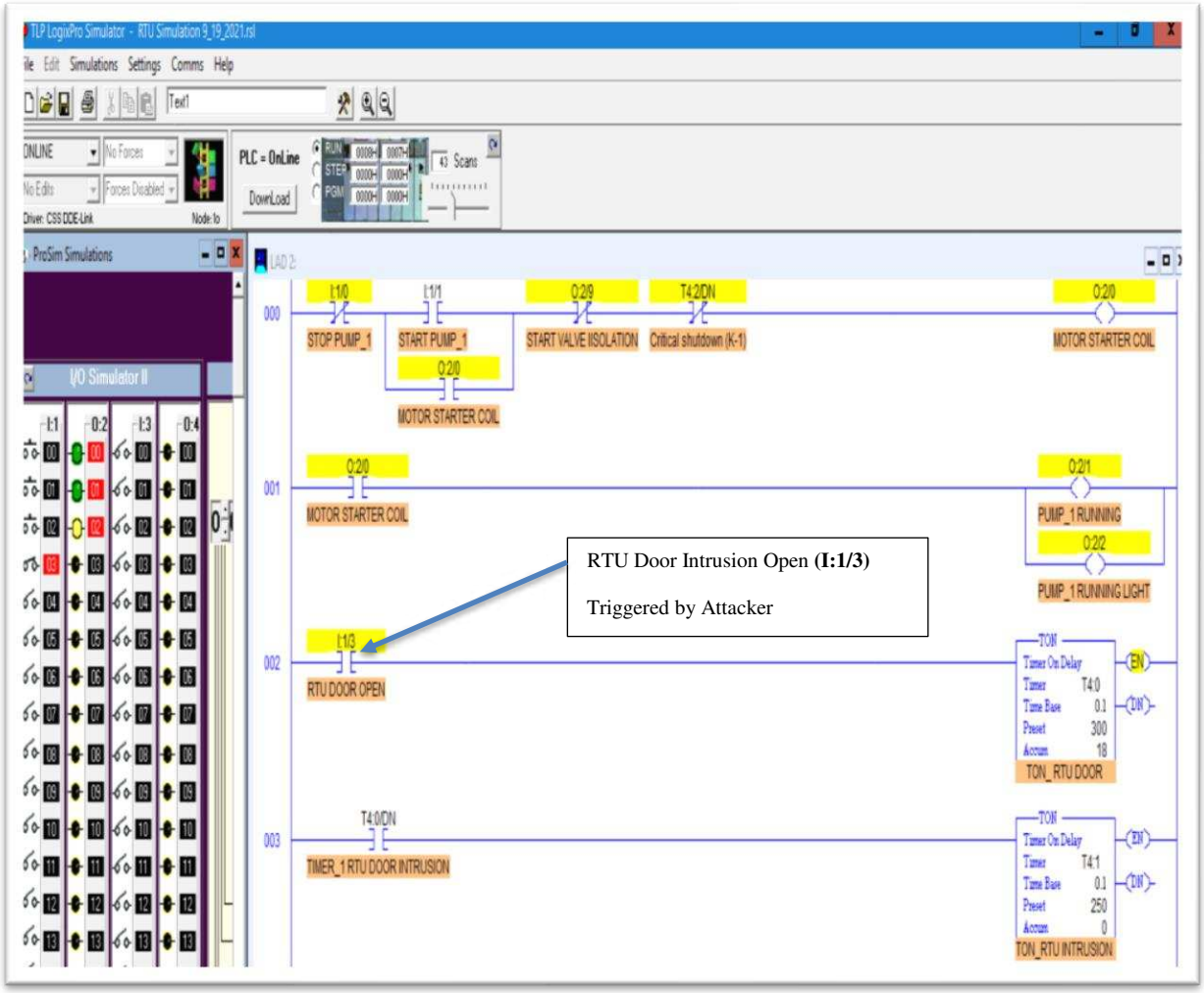


Fig. 34. RTU Simulation showing system running normal operation but with physical intrusion into subsystem RTU

A physical intrusion into the RTU space is initiated:

A Physical attack on the RTU enclosure will trigger an alarm sequence and ultimately an alarm signal to stakeholders, management, and CRO. The specifics are defined locally, and the enhanced RTU provides options for response not presently available. The Utility management will specify an operational sequence to deactivate the alarm with a unique code that activates the

RTU audio and camera. This serves a dual purpose to capture stakeholders for accountability, controlled access log, and authentication. Furthermore, the video/audio and forensic data will be sent to the data logger and stored in its database. Finally, the RTU site camera will activate and send alarms to the control room operator, stakeholders, and first responders when an individual field operative is present and operator under duress.

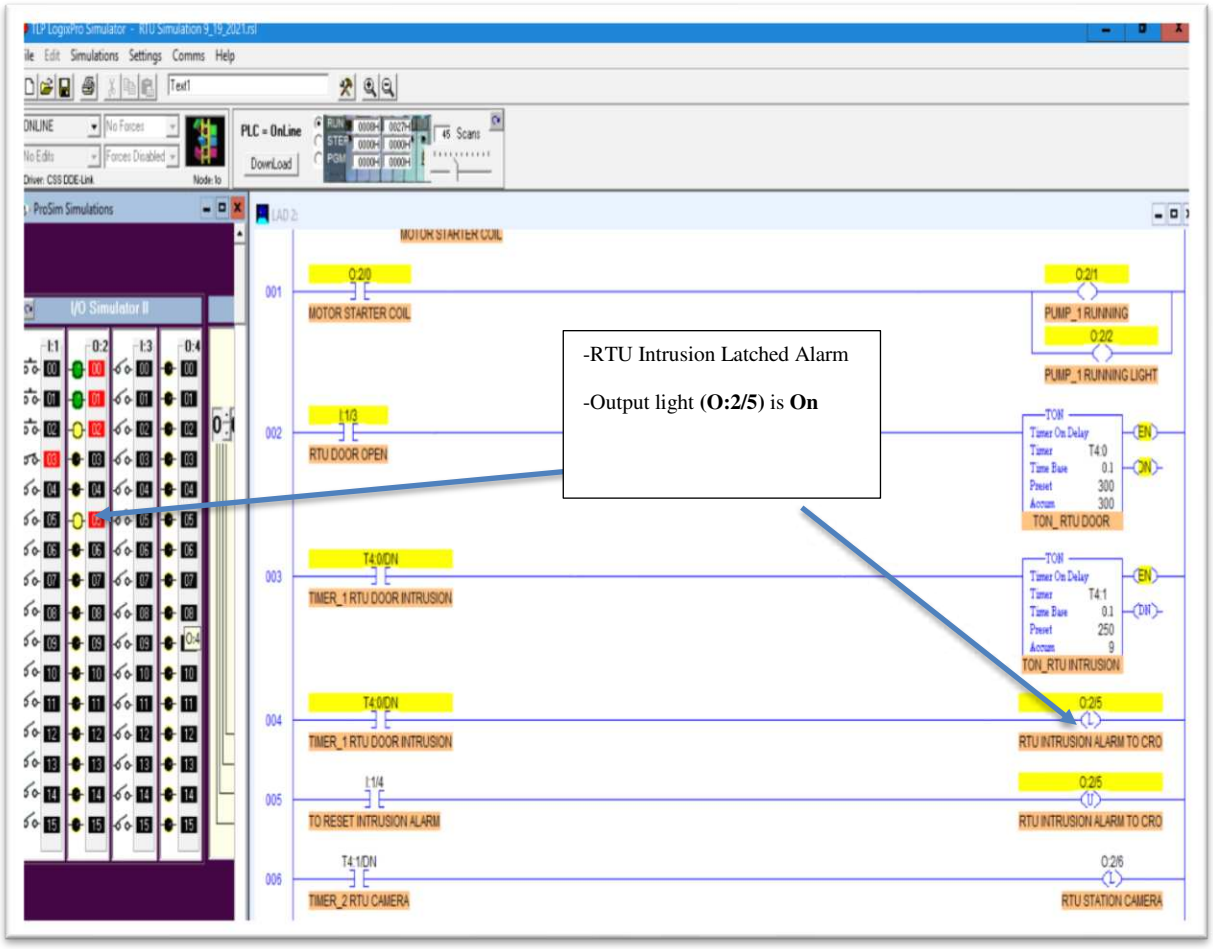


Fig 35. RTU under physical attack - door opened, alarms sequence activated, here alarms go to SCADA and CRO.

At this point, the RTU Latched Intrusion alarm (Latched) is sent to the data logger and, upon receipt of a valid certificate, forwarded to the MTU, the SCADA (for incorporation in a

report detailing issues at other RTUs and other computer systems) and the control room operator (CRO). Output RTU Intrusion light is Latched on.

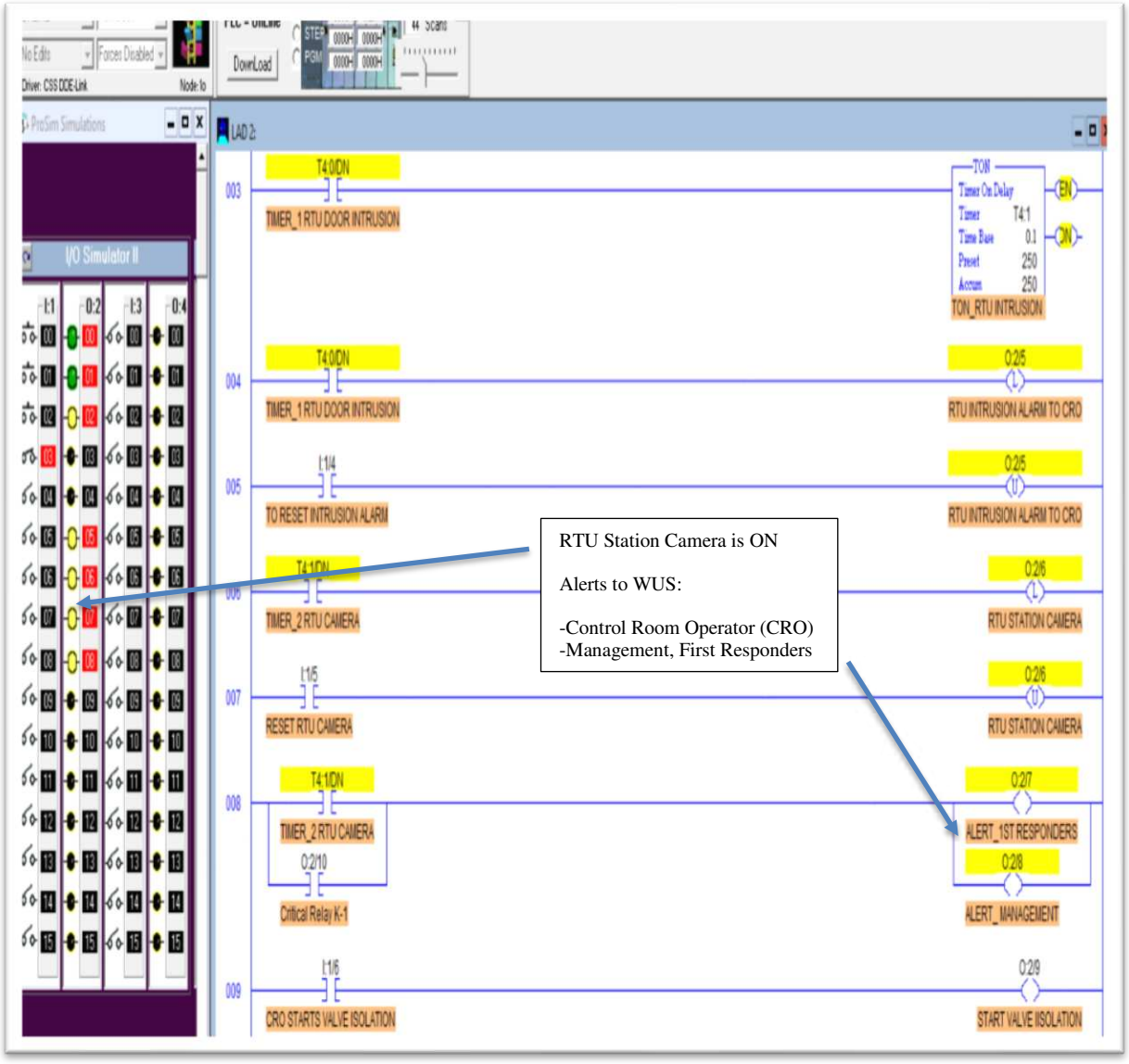
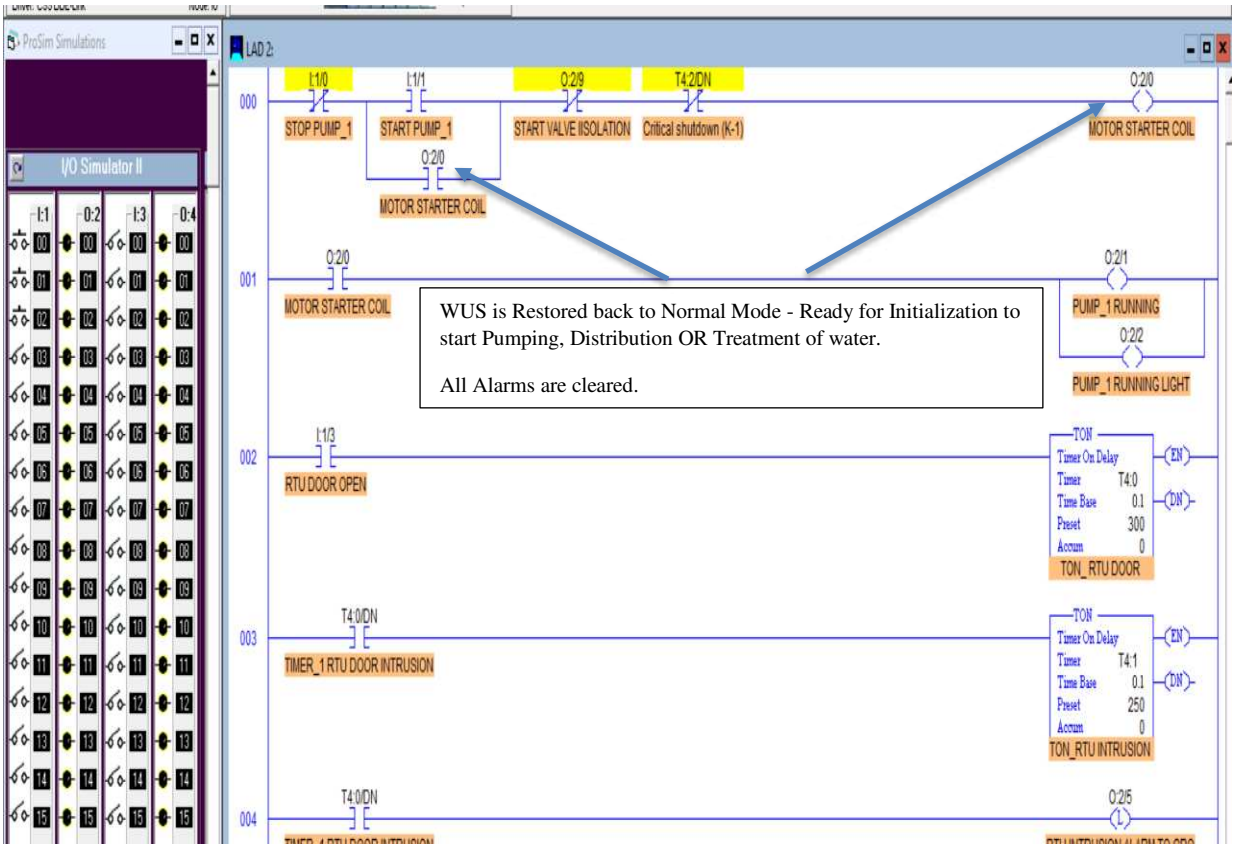


Fig. 36. RTU under physical attack, Alarms and video activated

After the logging and data transmission occurs, the bad actor is being viewed and recorded by the control room operator and management. This is shown in figure 35, with the arrows pointing to the RTU Station Camera on the right-hand side and the camera energized

light on the left side of the I/O simulator. Then, built-in autonomous response programs are triggered to minimize damage and aggregate data and alarms for transmission to first responders to assist in apprehending the perpetrator. Another unique feature of the enhanced RTU is that the system does not depend on CRO operators for responding to an intruder or hacker.

Figure 36 shows that the pumps and other controls are throttled or switched off in a pre-determined response to the alarm. The PLC diagram will show that the attack is contained, and the time sequence of attack and containment will all be stored as a time series in the data logger. When all automated reports are transmitted and evaluated, it will be up to management to issue a restore operations command sequence so the RTU and its connected water utility components facility site may be re-started even before event attribution and attacker apprehension are completed.



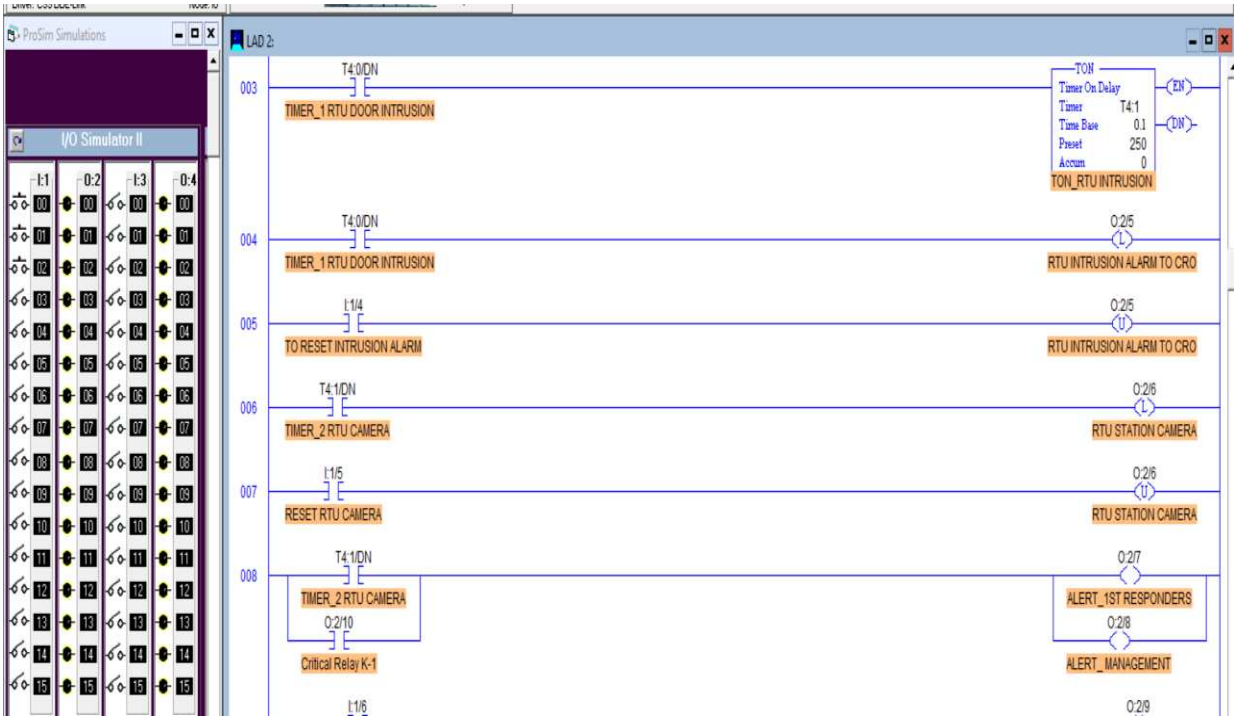


Fig. 37. RTU under physical attack investigated, system restored to offline mode.

Figure 36 shows that the water utility system and the RTU have been restored to normal operations after system alarms, local and central mitigations, and reporting to the Utility Emergency Response team, followed by alarm reset, sampling, and testing of water and component configurations. Forensic and first responders will continue investigations, apprehension, and lessons learned processes.

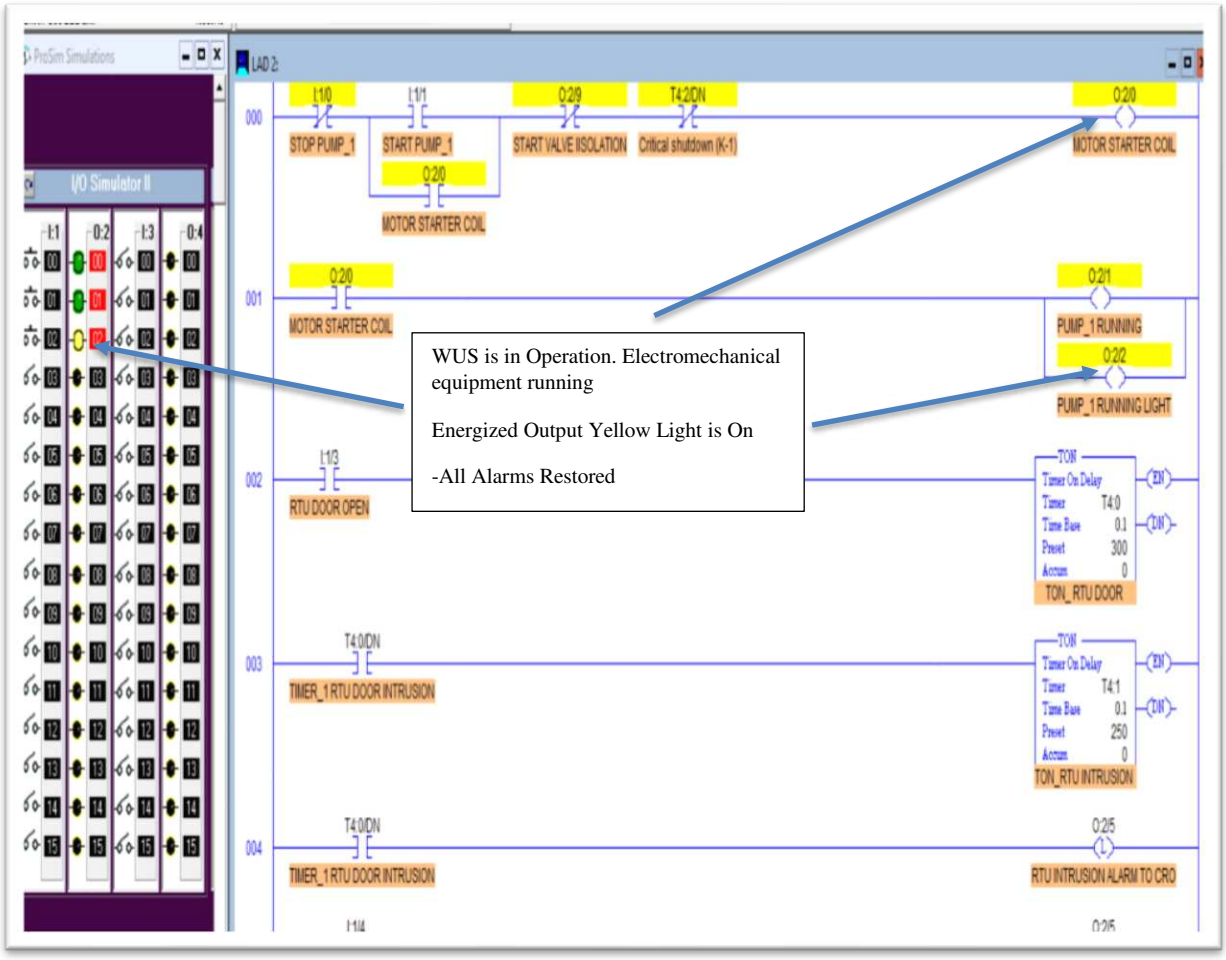


Fig. 38. RTU operations are restored post attack and placed to normal operation.

Figure 37 shows that the water utility system and the RTU have been restored to normal operations of services.

Cyber-attack on Utility through SCADA and RTU;

It is important to note that the enhanced RTU system will 1) detect and mitigate simultaneous cyber and physical attacks. The responses are independent of attempting to degrade, destroy or alter system performance. 2) The report sent from the enhanced RTU to CRO, and stakeholders will inform there were two attacks: their targeted and present status. The

Existing RTU will not do that. The existing RTU data will not tell first responders that there have been two attacks. In cyber security, time is damaging. For example, in the Oldsmar water plant attack, it was reported that it took five and a half hours for an employee to notice the change.

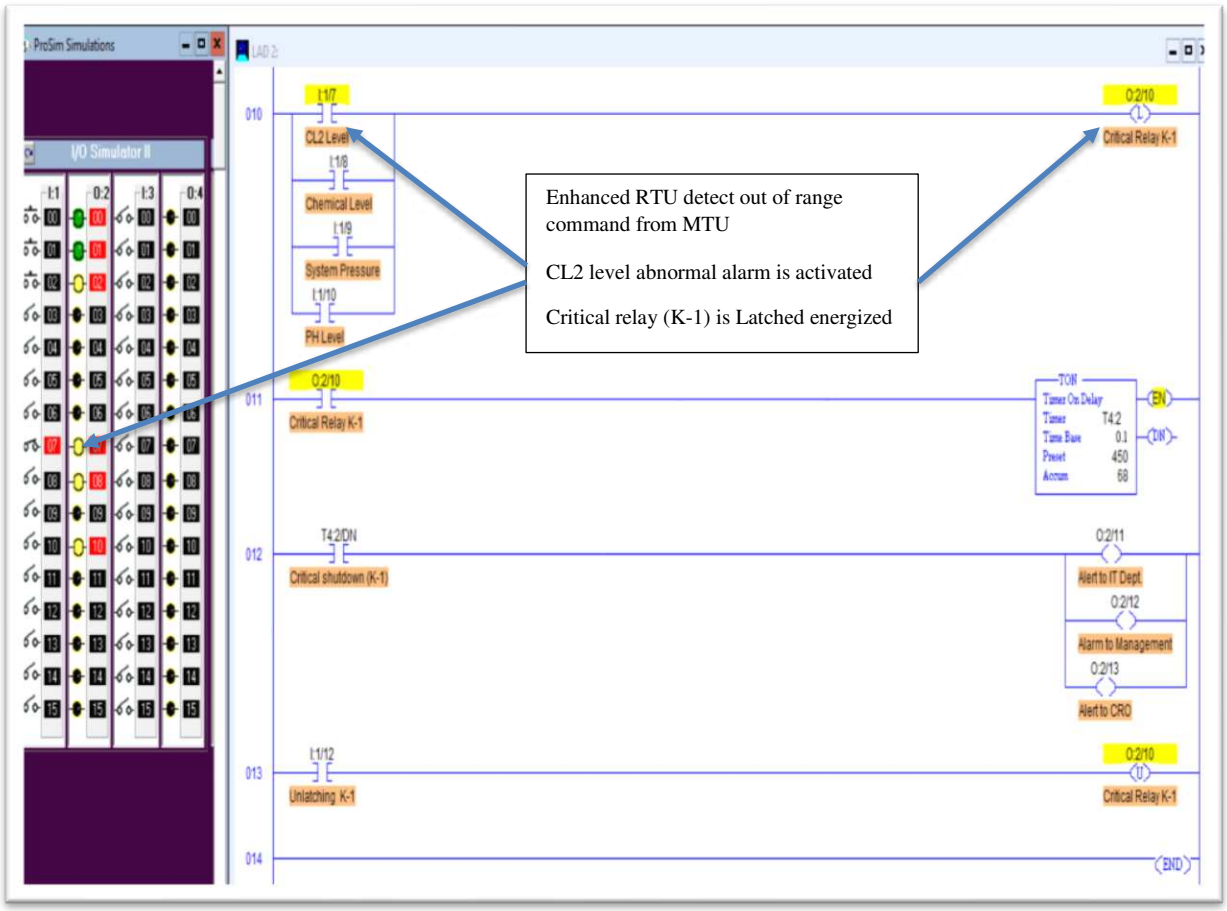


Fig. 39. RTU in operation but under cyber-attack - CL2 level out of range manipulation

Fig 38 shows water utility processes under cyber-attack. A bad actor outside the United States gets access to the SCADA and uses the GUI or API to change setpoints, such as chlorine dosage to abnormal concentration, to inflict damage and kill water users. The enhanced RTU black box will detect the abnormal chlorine setpoint and the rate of change of concentration. The Utility will program the RTU to either throttle concentration increases or prevent change and lock the concentration, thus preventing the perpetrator's action.

In addition, the embedded black box recorder aggregates data for the incident report, triggers audio or video if appropriate, and sends an alarm to the MTU –SCADA and CRO so the utility emergency response team can initiate appropriate actions. Following the situation report sent to the CRO by this RTU and others under attack or experiencing performance degradation, the management will send a restore operations command to restart processes and possibly have a site team examine systems or devices for damage.

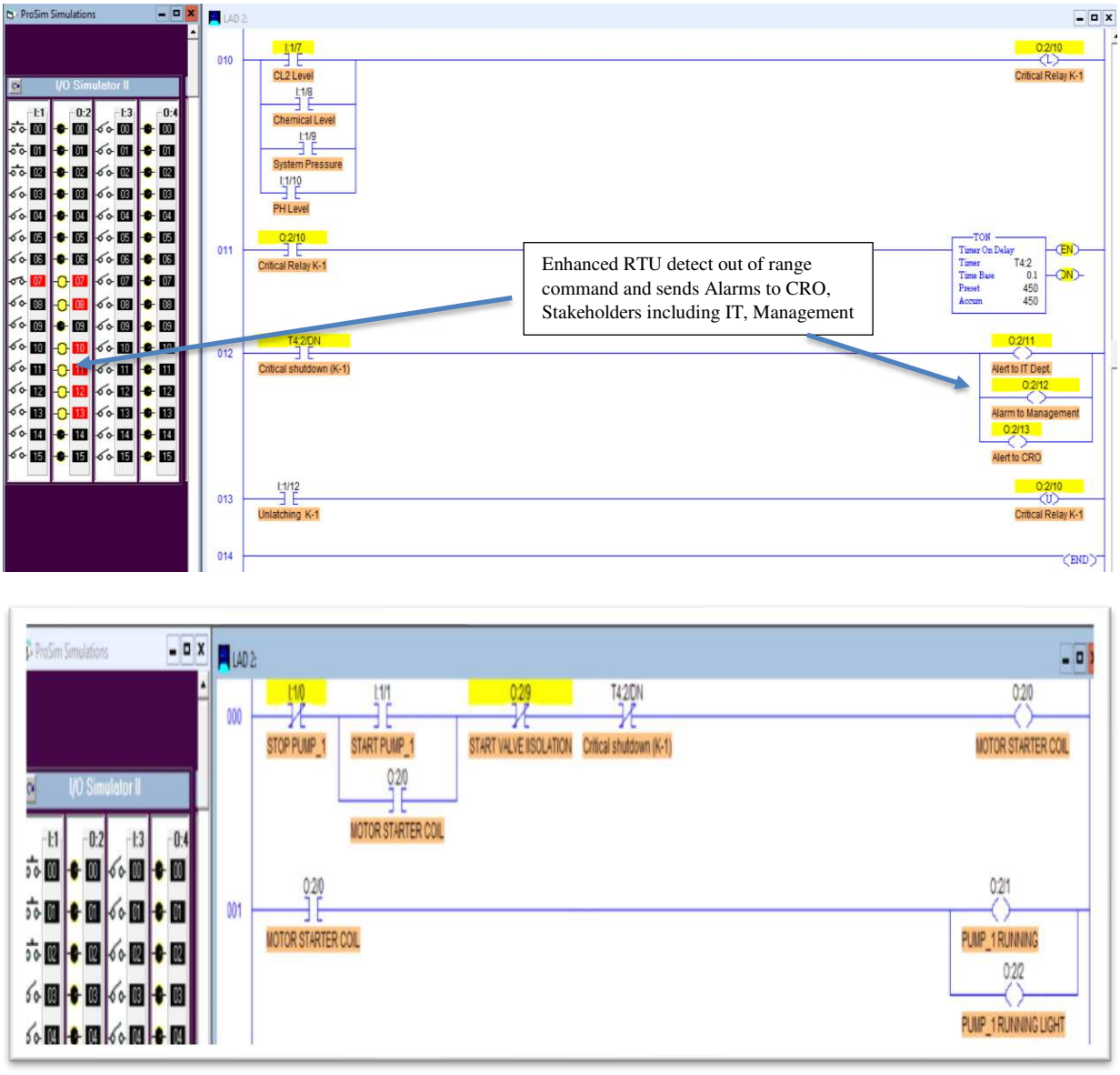


Fig. 40. Water Utility under cyber-attack - Alarms activated, and system is shutdown

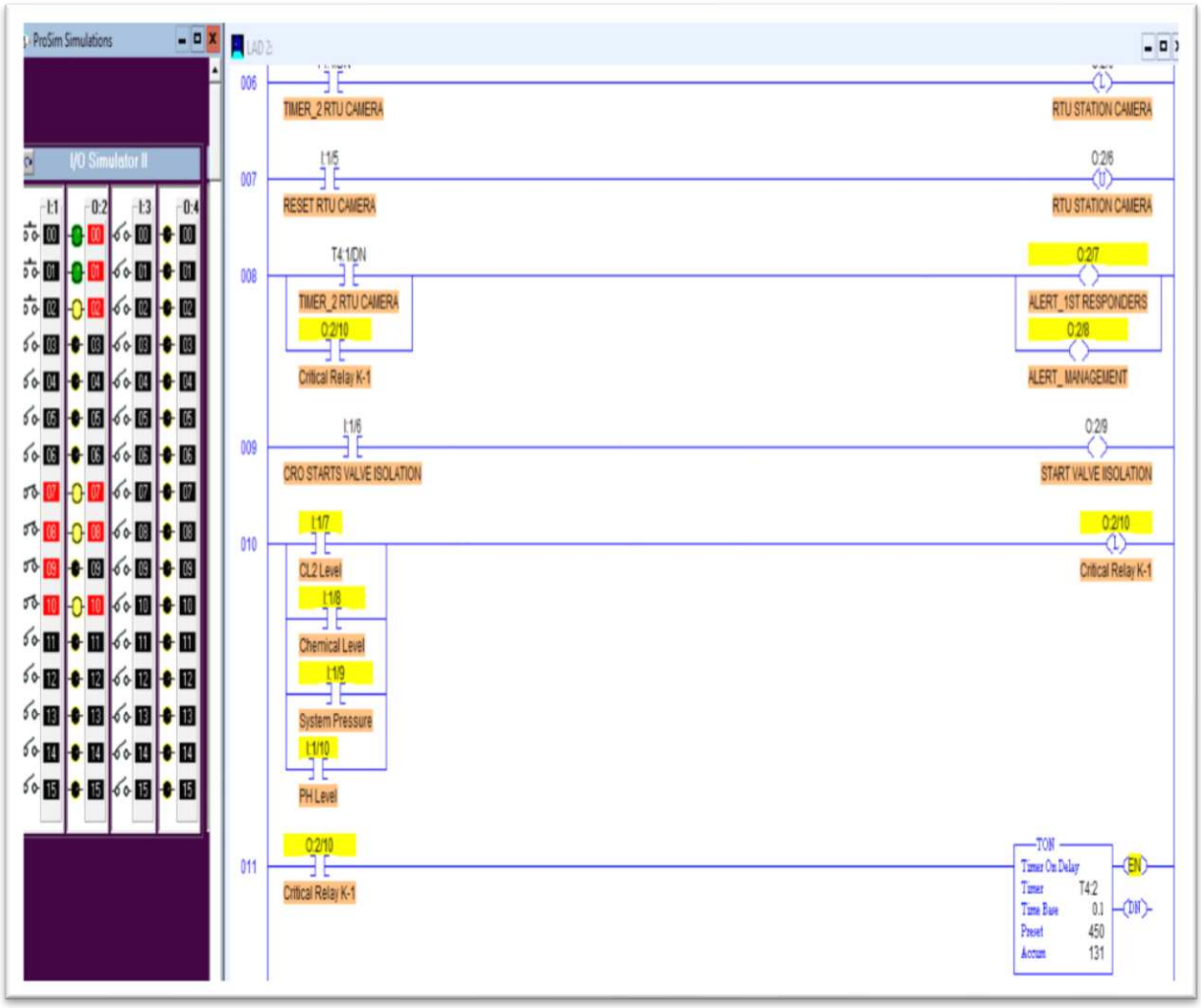


Fig. 41. RTU monitoring connections for 4 critical process variables as inputs

Fig 40 shows a subset (chosen for simplifying the description) of the process variables that the enhanced RTU black box will monitor. For example, this simulation uses chlorine, chemical, system pressure, and pH monitoring. The number of observables and controllable a particular component needs depends upon the specific component. In addition, the RTU can exchange data through all channels needed. This feature allows management to communicate effectively with neighboring water utilities and other critical infrastructure to determine if multi-

pronged attacks are occurring and to activate cross-connection valves shutdown, especially for water utilities that purchase water from another utility and distribute it to customers.

7.4. Description of Existing RTU Subsystem Responses and Messages to Utility Managers, Stakeholders and First Responders.

Thus, in the case of cyber-attack on EXISTING RTU, the following sequence will occur;

1. The actor obtains access to the RTU enclosure.
2. The actor then increases the Sodium Hydroxide concentration to fatal levels.
3. A control room operator may or may not notice the increase or may or may not be aware of what it means. In any event, the SCADA sensor loop scans all the RTUs in series, so the scan cycle time is the shortest response time of the system.
4. The first observable response to the attack could be hospitalized and dying. Hopefully, the attacker has not planned a 2-stage exploit.
5. Law enforcement, the DHS, the EPA, the Water Utilities, and the media will investigate whom to blame.

7.5. Chapter Conclusion

This chapter describes the changes occurring in a system under cyber and physical attack. It identifies the value of the enhanced RTU using instructions to components and subsystems that are typical of those observed in present-day operations. A PLC ladder logic program of the type used to control utility operation formed a simulation (minus physical response non-idealities) was used to validate the activities of the enhanced RTU to show physical and cyber-attacks on the water utility system. It is seen that the components used to enhance the RTU operating in their verified and validated performance envelopes will minimize or in some cases prevent

damage to water utility operations including: public health through contamination, disruption of water and wastewater services, environmental impact, environmental fines, and avoidance of paying erroneous ransom fees.

Details of how the enhanced RTU will respond and mitigate attacks were described. The enhanced RTU contains physical intrusion alarms, audio, and video monitors, ruggedized antennas, and an embedded data logger to monitor component input and output signals. This will restrict setpoints beyond the allowable process range and provide early warnings and alarm signals to SCADA, utility management, stakeholders, and first responders.

CHAPTER 8: CONCLUSIONS AND RECOMMENDATIONS

8.1. Conclusions

Remote Telemetry Units (RTUs) in water utility systems are critical because they are the interface to the utilities operating hardware, meters sensors and control. Existing RTUs are vulnerable to attack from many sources. Several research and upgrades within the SCADA subsystems are used in water utilities, yet the number of attacks have increased. The enhanced RTU proposed in this dissertation is a step to mitigate the existing RTU vulnerabilities and improve detection of exploits that threaten water critical system mission success.

Furthermore, a more secure and resilient RTU architecture will increase the security of water utility and wastewater systems, decrease the time to restore operations after an upset, reduce the time to identify and track those responsible. Furthermore, the enhanced RTU will substantially enhance situational awareness of cyber and physical attacks for those involved in water systems security. Finally, the new design will provide the information needed to develop a system-wide common operating picture to better control its security and non-security aspects.

8.2. Primary Contributions of this Dissertation

There are several contributions to this work. First, the Enhanced RTU would mitigate physical and cyber threats to water utility systems. Secondly, the enhanced RTU would save lives, prevent EPA fines and violations, limit critical infrastructure destruction, and give faster notice to water utility management and stakeholders to minimize or eliminate breaches of water users and stakeholders' data. Thirdly, the embedded data and configuration recorder would retain time-stamped and time-series data to be used for further investigation.

Water and wastewater utility systems are critical national infrastructures dedicated to supplying water for life sustenance and treating wastewater from homes, offices, and industries before effluent into the water bodies. The entire distribution system has several subsystems that make it possible for such essential processes. Even though the water utilities cover large areas, the operation makes it possible by using electromechanical devices such as pumps, motors, transmitters, mixers, generators, RTUs, MTU, and finally coming under the umbrella of SCADA.

This paper contributes to securing one of the critical subsystems of the water utility system, the RTU, using a systematic design methodology described in Chapters 4,5 and 6.

The author's experience combined with an extensive literature review showed that the RTU was the most vulnerable component in the Utility. Next, this hypothesis was verified by field personnel who work with RTUs through a questionnaire. It confirmed that RTU security is of serious concern to people in the field. Next, effective Model-Based System engineering (MBSE) principles were utilized to specify the architecture, observables, controllable, and data flows needed to design a new enhanced RTU.

The final step was the transition from the MBSE design into Ladder Logic since it is the preferred programming software used in the United States. Finally, a Ladder Logic program was executed to verify setpoints, process variables, relay energization, execution time, and response to changes.

8.3. Recommendations

The advancement in networking and data transmission from one remote location to another has been made easy and accessible to employees, management, vendors, and contractors. Unfortunately, as a result, many network nodes have been created and are exploited by bad

actors to attack water utility companies. While the digitization of water utilities has improved efficiency in many ways, it has also made them vulnerable to disruption. The enhanced RTU will contribute to reducing this vulnerability. Accompanying the deployment of enhanced RTUs are a set of recommendations enumerated below. The prioritization will depend on the particular utility, risk profile, risk appetite, and budget constraints.

The recommendations include:

1. Upgrade existing RTUs with alarm, camera audio, and upgraded antenna
2. Add a data logger, associated data filtering, and data report templates.
3. Enhance sensors outputs so that RTU can record the state of attached subsystems data.
4. Reduce attack surface by reducing the number of network connections to RTUs and other WUS components.
5. Develop a risk management framework for water utilities
6. Update control room software to integrate enhanced RTU-MTU-SCADA chain
7. Institute and enforce cyber-physical security standards.
8. Water utility systems research should address the incorporation of the enhanced RTU in security and software for MTU and SCADA. Some examples of this are described in Chapter six of the dissertation.
9. MBSE should be upgraded to incorporate PLC for simulating utility behavior for water, electricity, and other infrastructure
10. Research to develop embedded control hardware for RTU real-time data logging and local controls in RTU.
11. Government and other institutions to fund research in optimizing MTU and SCADA systems with enhanced RTU to improve cyber-attack mitigation strategies.

REFERENCES

[1] EPA, White House launch cybersecurity plan for water sector. Retrieved from https://www.waterworld.com/drinking-water/press-release/14232852/epa-white-house-launch-cybersecurity-plan-for-water-sector. Water World, February 2022.

[2] Borky J. M & Bradley I. H. (2019). Effective Model-Based Systems engineering. Springer International Publishing.

[3] Davies A. W., Dubow J. B., Borky J. M., Collins G. Analyzing and Mitigating Water Utility System Vulnerabilities. AWWA Journal, January 2022.

[4] Lee, E. A. (2008). "Cyber physical systems: Design challenges." 2008 11th IEEE Int. Symp. on Object-Oriented Real-Time Distributed Computing (ISORC), IEEE, New York, 363–369.

[5] Slay, J., and Miller, M. (2008). Lessons learned from the Maroochy water breach. Springer, Boston.

[6] Dan Kroll, Karl King, Terry Engelhardt, Mark Gibson, and Katy Craig, Hach Homeland Security Technologies. Terrorism Vulnerabilities to the Water Supply and the Role of the Consumer Water Security White Paper. Retrieved from https://www.waterworld.com/water-utility-management/article/16219980/terrorism-vulnerabilities-to-the-water-supply-and-the-role-of-the-consumer-a-water-security-white-paper/. Water World, March 9, 2010.

[7] Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., and Banks, M. K. (2016). "Smart water networks and cybersecurity." J. Water Resour. Plann. Manage., 01816004.

[8] Dakin, R., Newman, R., and Groves, D. (2009). "The case for cybersecurity in the water sector." J. Am. Water Works Assoc., 101(12), 30.

[9] Horta, R. (2007). "The city of Boca Raton: A case study in water utility cybersecurity." J. Am. Water Works Assn., 99(3), 48.

[10] Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyberwar, and other cyber threats, Center for Strategic and International Studies, Washington, DC.

[11] Cominola, A., Giuliani, M., Piga, D., Castelletti, A., and Rizzoli, A. E. (2015). "Benefits and challenges of using smart meters for advancing residential water demand modeling and management: A review." Environ. Modell. Software.

[12] Taormina, S., Tippenhauer, N., Galleli, S., Ostfeld, A., Salomons, E. (2016). Assessing the effect of cyber-physical attacks on water utility systems. Conference Paper, May 2016.

[13] Anderson, R. (2008). Security engineering. John Wiley & Sons.

[14] Amin, S., Litrico, X., Sastry, S., and Bayern, A. M. (2013a). “Cyber Security of Water SCADA Systems - Part I: Analysis and experimentation of Stealthy Deception Attacks." IEEE T. Contr. Syst. T., 21(5), 1963-1970.

[15] Kosut, O., Jia, L., Thomas, R. J., and Tong, L. (2010). “Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures." Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, IEEE. 220-225.

[16] Shahzad, S., A. Aborujilah, S. Musa and M. Irfan, 2014b. The SCADA Review: System Components, Architecture, Protocols and Future Security Trends. J. Comput. Sci., (8): 1418-1425, 2014. DOI: 10.3844/ajassp.2014.1418.1425

[17] Stouffer, J. and K. Kent, 2006. Guide to Supervisory Control and Data Acquisition (SCADA) and industrial control systems security. Recommendations of the National Institute of Standards and Technology.

[18] Maupin, M., et al. (2014) Estimated Use of Water in the United States in 2010. U.S.G.S.

[19] SWAN, 2018. What is smart water Network? Retrieved from https://www.swan-forum.com/about/

[20] Kardon Steve (2021) Florida Water Treatment Plant Hit with Cyber Attack. Retrieved from https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/

[21] Birkett, D. M. (2017). Water Critical Infrastructure Security and Its Dependencies. Journal of Terrorism and Research, JTR, Volume 8, Issue 2–May 2017. Retrieved from https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.1289/galley/991/download/

[22] Gillette, J., Fisher, R., Peerenboom, J., & Whitfield, R. (2002). Analyzing Water/Wastewater Infrastructure Interdependencies 6th International Conference on Probabilistic Safety Assessment and Management (PSAM6). San Juan, Puerto Rico, USA, 23-28 June 2002.

[23] Zyl, J. V. (2014) Introduction to Operation and Maintenance of Water utility systems Edition 1. ISBN 978-1-4312-0556-1

[24] ICS-CERT. NCCIC/ICS-CERT year in review: FY 2015. U.S. Department of Homeland Security, Washington, DC., 2016b.

[25] Hieb Jeffrey (2008). Security Hardened Remote Terminal Units for SCADA Network.

[26] Critical Infrastructure Sectors. (2017). Department of Homeland Security (DHS). Retrieved from https://www.dhs.gov/critical-infrastructure-sectors

[27] Water Watchers. Helping to protect your local water system. Retrieved from https://www.epa.gov/sites/production/files/2015 10/documents/waterwatchers_revised2.pdf

[28] Amin Hassanzadeha, Amin Rasekhb, Stefano Galellic, Mohsen Aghashahid, Riccardo Taorminae, Avi Ostfeldf, M. Katherine Banksg. A Review of Cybersecurity Incidents in the Water Sector. Retrieved from Journal of Environmental Engineering 146 (2020)

[29] Water Pressure Management Diagram. Retrieved from http://nwhydrotech.com/packaged-stations

[30] Joar Jacobsson, (2021). SCADA Reference Architecture. Retrieved from https://foreseeti.com/scada-reference-architecture/

[31] B.R. Mehta and Y.J. Reddy, (2015). Industrial Process Automation Systems Design and Implementation https://www.sciencedirect.com/book/9780128009390/industrial-process-automation-systems#book-info

[32] Overview of water treatment and Distribution SCADA and RTU Systems (2021). Retrieved from schneider-electric.com/scada&telemetry.

[33] Zahran M., Yousry A. and Abulmagd A. (2011). Block diagram of standard SCADA System. Retrieved from https://www.researchgate.net/figure/Diagram-shows-three-main-components_fig1_263375097

[34] Honeywell MaxPro NVR Video Surveillance. Retrieved from https://www.nepps.com/product-category/cctvcameras/?gclid=EAIaIQobChMIiqGckbWj8wIVjbjICh2HQgckEAAYASAAEgKqo_D_BwE

[35] Isenberg D (2002) Securing U.S. Water Supplies. CDI Terrorism Project. http://www.cdi.org/terrorism/water-pr.cfm

[36] Water Infrastructure Resilience. Retrieved from https://www.epa.gov/emergency-response-research/water-infrastructure-resilience

[37] Jonathan Creig, (2021). Florida water treatment plant was involved in second security incident before poisoning attempt: report. Retrieved from. https://www.zdnet.com/article/florida-water-treatment-plant-was-involved-in-second-security-incident-before-poisoning-attempt-report/

[38] Peng Yu, (2021). Open Industrial Control System Design Model Puzzle. Shanghai Industrial Automation Instrumentation Research Institute, PLC open China Organization.

[39] Christian Brecher, Johannes A. Nittinger, Andreas Karlberger (2013). Model-based control of a handling system with SysML. Retrieved from https://core.ac.uk/download/pdf/82354387.pdf

[40] Michael Stephen, 2019. Ladder Logic in Programmable Logic Controllers (PLCs). Retrieved from https://control.com/technical-articles/ladder-logic-in-programmable-logic-controllers-plcs/

[41] Pierluigi Paganin, 2021. ICS/SCADA threats and threat actor. Retrieved from https://resources.infosecinstitute.com/topic/ics-scada-threats-and-threat-actors/

[42] Alliance Water Resources. Improved Water & Wastewater Systems Monitoring and Automation with SCADA. Retrieved from https://alliancewater.com/how-does-scada-help-water-and-wastewater-management/

[43] Israel National Cyber Directorate (INCD): Targeted attacks on Israeli water supply and wastewater treatment facilities. Retrieved from https://ics-cert.kaspersky.com/reports/2020/09/24/threat-landscape-for-industrial-automation-systems-h1-2020/

[44] Pro USB Flash Drive Audio Recorder Voice Activated. Retrieved from https://spycentre.com/collections/audio-surveillance/products/pro-usb-flash-drive-audio-recorder

[45] Block diagram of a typical SCADA System showing RTU. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.698

[46] RFMAX RY-900-2-7-SNR-19 Yagi Antenna for RTU Stations. Retrieved from https://www.rfmax.com/products/ry-900-12-7-snf-19-900-mhz-yagi-antenna-heavy-duty-7-element-yagi-for-880-960-mhz-ism-with-12-dbi-gaiin-kathrein-scala-equivalent

[47] Understanding an Important Qualitative Research Method. Retrieved from https://www.thoughtco.com/participant-observation-research-3026557

[48] Honeywell MaxPro NVR Video Surveillance. Retrieved from https://www.security.honeywell.com/All-Categories/video-systems/maxpro-nvr-and-vms

[49] Honeywell Snap Action Switch SPDT 4A 250V. Retrieved from www.honeywell.com

[50] L. Atzori et al., The Internet of Things: A survey, Computer. Networking (2010), Retrieved from https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf

[51] Victoria Young (June 2021). Harrisburg recovering from cyber-attack, plans full investigation. Retrieved from https://independenttribune.com/news/local/harrisburg-

recovering-from-cyber-attack-plans-full-investigation/article_c3902e0a-b26a-11eb-af94-3b0b4ba99b48.html

[52] Jeremy Rasmussen (April 2021). Lessons Learned from Oldsmar Water Plant Hack. Retrieved from https://securitytoday.com/articles/2021/04/05/lessons-learned-from-oldsmar-water-plant-hack.aspx

[53] Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector. January 27, 2022. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector

[54] Mission Secure. The Purdue Enterprise Reference Architecture. February 10, 2021. Retrieved from https://www.missionsecure.com/blog/purdue-model-relevance-in-industrial-internet-of-things-iiot-cloud

[55] DC Water at a Glance. Retrieved from https://www.dcwater.com/dc-water-glance. May 17, 2021.

[56] Claroty Team82. CLAROTY BIANNUAL ICS RISK & VULNERABILITY REPORT: 1H 2021. Retrieved from https://claroty.com/wpcontent/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf

APPENDIX A

PUBLISHED PAPER IN AWWA - ANALYZING AND MITIGATING WATER DISTRIBUTION SYSTEM VULNERABILITIES

Analyzing and Mitigating Water Distribution System Vulnerabilities

Augustus W. Davies

Doctoral Student, Department of Systems Engineering, Colorado State University, Colorado, USA

Dr. George COLLINS
Dept of Electrical Comp ENGR
Colorado State University
Colorado, USA
gcollins@rams.colostate.edu

Dr. Joel DUBOW
Dept of Systems Engineering
Colorado State University
Colorado, USA
jdubow@msn.com

Dr. John BORKY
Dept of Systems Engineering
Colorado State University
Colorado, USA
Mike.borky@engr.colostate.edu

Key Takeaways:

- Water distribution systems are vulnerable to physical and cyber-attacks, especially engineering subsystems used in water distribution.
- Security is critical for Remote Telemetry Units (RTUs) because they can be a targeted for malicious service disruptions.
- Changes to existing RTU designs that improve its robustness, resilience, and response times should minimize potential exploitation.

Keywords—Remote Telemetry Unit (RTU), Main Terminal Unit (MTU), PLC, Physical Cyber Security, SCADA, Control Room Operator (CRO).

WATER UTILITY SECURITY INCIDENTS

Water and wastewater utility face numerous cyber and physical threats, and distribution and collection systems offer unique opportunities for acts of mischief and terrorism. Some of these threats are enhanced because water systems are geographically distributed, physically accessible, often isolated, and relatively unprotected.

For example, on April 23, 2020, the Israeli National Cyber-Directorate (INCD) issued a security alert that the agency received reports of intrusion attempts at its wastewater treatment plants, water pumping stations, and sewers SCADA systems network, but did not go into specific details about the entry point(s). The agency urged personnel at companies active in the energy and water sectors to change passwords for all internet-connected systems. The agency suggested all passwords be changed, and systems were taken offline until proper security measures were in place [27].

In another attack, hackers gained access to computers at a small Colorado water utility. The Fort Collins-Loveland Water District (FCLWD), and its wastewater counterpart, were attacked by malware that encrypts victims' computer files and demands online payment to unlock them [22]. Normal water distribution operations resumed with no system damage, but the ransomware prompted the water district to switch out its information technology service provider and call in the FBI, and the case remains under active investigation [23].

More recently, a hacker remotely accessed the Oldsmar Florida water treatment plant. The targeted system controls the chemicals added to the water to make it safe to drink. According to the local sheriff, the exploit increased sodium hydroxide - lye - from 100 parts per million to 11,100 parts per million. However, the hack was thwarted within minutes by a plant operator, and officials restricted remote access. The attack came through the internet via the plant's remote access system. Then, through the MTU, down to the RTU. From there, to the controller for adding Sodium Hydroxide to the water.

In a more recent attack on the water distribution system, a US water company WSSC Water experienced a ransomware attack that affected non-essential business systems in May. This incidence was reported by WSSC water.com, the Security Affairs by Pierluigi Paganini, and CBS Baltimore on June 27, 2021. The FBI, Maryland Attorney General, and state and local homeland security officials were also notified. According to CBS Baltimore, all individuals are encouraged to remain vigilant and closely examine their financial statements and report anything suspicious to their bank or card issuer. Individuals can also access identitytheft.gov to report any suspicious activity and to learn how to freeze their credit. The company operates filtration and wastewater treatment plants; fortunately, the attack did not impact the water quality, but the investigation is still ongoing.

In one full-scale example of disruption of water distribution , a large-sized utility had one of its water booster pumps turn on and off without activation from an operator or SCADA. An indication that the "pump has started" appeared on the SCADA display, but this surprised the control room operators. The malfunction was not only within the water distribution system, but also included the communication system used by the Utility. The issue continued for weeks until it was referred to the author, and it took joint coordination between the communication provider

and the water utility to develop a solution. Table 1 summarizes the root cause and corrective solutions followed in this instance.

TABLE 1. Potential Issues and Solutions to Unexplained Behavior after an Incident at a Full-Scale Booster Pump Station

Root Cause	**Solution**
4 - 20 mA Long Open cable run	Use wireless communication (Wi-Fi, Microwave) with protected endpoints
No Cybersecurity Measures	Use systems that support cybersecurity integration, updates, Firewalls, etc.; keep security controls current
Outdated Controls	Retire systems that cannot support cybersecurity measures
Unprotected RTU	Replaced with Protected RTU

Cyber-attacks are becoming common, and they pose real threats to utility security and operational integrity. In 2015, the US Department of Homeland Security (DHS) responded to 25 cybersecurity incidents in the water sector. Security focused organizations like the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provide a control system security focus in collaboration with US-CERT [28]. Together they conduct vulnerability and

malware analysis, provide on-site support for incident response and forensic analysis, and provide situational awareness to organizations like AWWA.

REMOTE TELEMETRY UNITS

Cyber-physical attacks usually target the Supervisory Control and Data Acquisition (SCADA) system and RTU subsystems such as the Programmable Logic Controllers (PLCs) that locally operate pumps and valves [13]. A medium-size water distribution system may have over 100 RTU sites distributed to maintain water pressure to users. The SCADA inputs are RTUs responsible for collecting data, filtering the data, aggregating all the data, and transmitting them to the MTU server. RTUs are the eyes and ears of the system, capturing sensor data from the field devices, other RTUs, field instruments, and PLCs.

The MTU aggregates the data for the SCADA, and the output goes to the water distribution system central processing system. Water supply systems usually consist of several subsystems as depicted in Figure 1. RTUs communicate with each other, MTUs, and SCADA using communication links such as LAN/WAN or Cloud; this includes radio signals, telephone lines, cable connections, satellites, and microwave media. Disruptions or degradation anywhere in this chain can propagate and degrade the entire water distribution system.

RTUs are often located in isolated areas and frequently lack physical security or onsite cameras. The ICS-CERT offers recommended practices for control systems such as RTU and SCADA on the ICS-CERT website for integrating industrial Control Systems Cybersecurity with Defense-in-Depth Strategies [28].

In light of recent water distribution systems attack [3] [7] [11] [24], the water industry should understand that RTUs could be exploited by someone with malicious intent if they access

components such as the RTU communication circuit or antenna radio frequency. Cybersecurity breaches to the SCADA could allow an actor to gain control of the RTU and threaten finished water quality or distribution system operations. Once they control the RTU communications and the associated field devices such as sensors and actuators, they can upset the data to manipulate the response of upstream controls. For quick restoration of water and wastewater systems programmed PLCs after unexplained shutdowns, power outages, duplicate program for the PLC located in the RTU is kept in the RTU by some Utilities. As a result, an actor can gain access to the storage device to inflict damage. Attempts to compromise a utility's water supply could be detected at various configuration nodes in the system and from there to the Master Control Station.

When exploited, RTUs allow access to field devices that monitor and control processes within the water treatment facilities as well as the water distribution system. A more robust RTU will provide faster and more granular input/output control and field device monitoring so that future hacks of this type are detected, analyzed, and fixed more quickly using event details and forensic data. RTU components can be made more robust by including external equipment such as cameras and voice recorders; these can provide critical real-time and forensic information to SCADA and control operation room operators to initiate action, share vital information with other water utility companies, and alert law enforcement and first responders.

An RTU system that offers more robust alarms, managed disruption solutions, and data capture for post-event forensic analyses could mitigate some water system threats. To that end, a "black box recorder" of the type used in aircraft and other systems for failure and service degradation detection is suggested for the RTU and is described in the following sections.

RTU SECURITY AND RELIABILITY REQUIREMENTS.

For this study, water distribution systems were analyzed with a focus on their RTU via a model-based system engineering (MBSE) approach [1]. This approach enables parametric analyses of upstream systems and downstream components whose modifications improve resilience and security.

As shown in Figure 1, RTUs have subsystems that include PLCs, power supplies, radios, antennas, modems, and input/output. An RTU subsystem with modularity, redundant components, and multiple paths techniques will increase the RTU subsystem's reliability and robustness when available. Nevertheless, extrinsic physical disruption by actors will remain a significant risk. An actor gaining physical access to an RTU can cause loss of control signal, data loss, and contamination of drinkable water intended for human consumption.

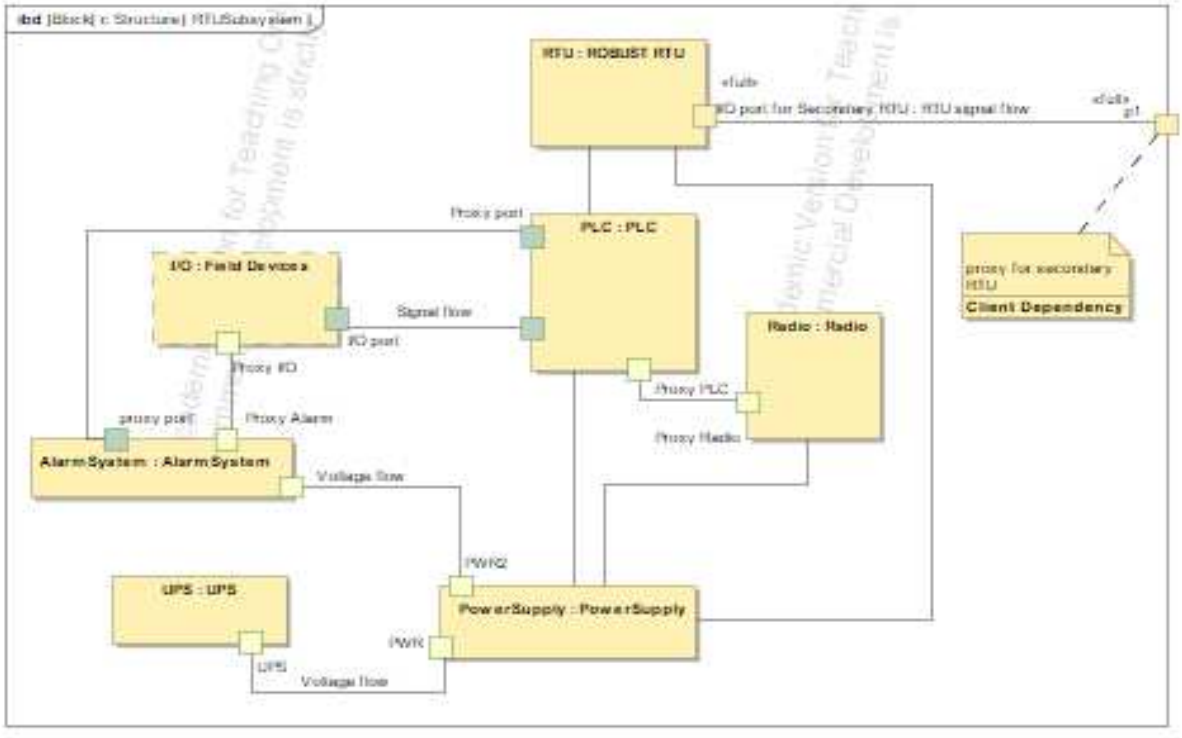


Fig. 1. Current RTU Components

Since RTUs are distributed in the field, they transmit their data via telemetry that must be "hardened" or properly secured. Other RTU security goals include:

1. Reduce vulnerability to vandalism and theft, especially when installed at street level in urban environments
2. Enable frequent wireless data transmission of larger packet sizes without placing significant demands on the battery powering the wireless modem of an RTU or PLC
3. Maintain event flow by protecting data from the field devices through the main terminal units to SCADA
4. If they rely on third-party wireless networks for data transmission, equip RTUs and PLCs with attack mitigation strategies to allow continuous data monitoring, authentication, and authorization
5. Isolate MTUs in a dedicated office building with constant supervision and monitoring by the IT department
6. The MTU server capacities require bandwidth for enhanced alert, alarm and response messaging
7. The RTU component package includes external equipment such as cameras and voice recorders

Using an operational viewpoint of an RTU provides a logical perspective of its architecture by defining the processes, information, and entities needed to fulfill the security requirements. The operational viewpoint's primary focus is the system requirements, decomposition of requirements, system testing, and subsystem testing [1][2]. The remote locations of RTUs constrain its design options. On-call personnel responding to water

distribution system emergencies are usually one-person crews, often at night. RTUs are downstream from SCADA, so exploits can often propagate to field devices and the central water distribution system. The connection between SCADA and the RTUs is central to systemic damage, so it must be considered in any upgrade [18].

SCADA SYSTEMS AND RTUs

RTU complexity drives communication system characteristics such as:

- openness
- interoperability
- networking
- packet switching
- data transmission
- cyber-attack sophistication
- threat actors

Older SCADA systems used a monolithic architecture that was based on standalone or mainframe systems with little to no networking capabilities. Some utilities still use monolithic architecture, but because they are highly vulnerable to physical and cyber-attacks, they should be upgraded to enhance their security.

The next generation of SCADA used a distributed architecture that included communication processors, human machine interface, RTUs, and databases. The distributed architecture system has several access points to field devices such as chemical dosage detection, flow measurement, and control feedback signals to pumps and motors.

The current generation of SCADA uses a network system architecture. Significant improvement has been realized by using wide area network (WAN) protocols such as the TCP/IP, UDP, and cloud computing for communication between the MTU and RTU, which separates the RTU portion of communications with field devices from the MTU. Networked SCADA architecture allows open architecture communication protocols and standards, enabling SCADA functionality using LAN and WAN topology [26]. The RTU is considered a localized, physically isolated subsystem of the SCADA.

Larger utilities often have a specific IT department to take care of the MTU and SCADA system. The integrated network system's resulting complexity also increases its attack surface and vulnerability. As a result, most public utility computing resources are spent on the network defense for regular updates, data backups, and recovery, which leaves the field devices and RTUs relatively more vulnerable to threat actors.

ADDRESSING RTU VULNERABILITIES

For RTUs in water distribution systems, the five most significant physical vulnerabilities and their fixes to make them more robust are as follows:

1. **Vandalism:** Installing a secured camera on site will capture intruders within the RTU location and alert the control room operator
2. **Voice control spoofing:** An embedded voice activation recorder can capture intruder voices, accents, etc.; this can serve as a deterrent or help during prosecution
3. **System alert to threat response unit:** A robust RTU can call first responders to request they investigate the site

4. **RTU and downstream exploits:** As described subsequently, install a "black box" in the RTU that can gather real-time forensic data to assist incident response and analysis
5. **System-wide coordination:** A more robust RTU can send messages to surrounding utilities to alert, inform, and provide critical data to maintain mission performance

BUILDING SECURITY IN RTUS

It is possible to make RTUs better to detect and respond to cyber and physical threats, and specifically, adding these two subsystems can make RTUs more secure:

1. An intrusion alarm with image/video capture
2. An operational and environmental data recording module (black box)

Adding these subsystems will also modify the data flow within the RTU and the subsystems it links to as shown in Figure 2.

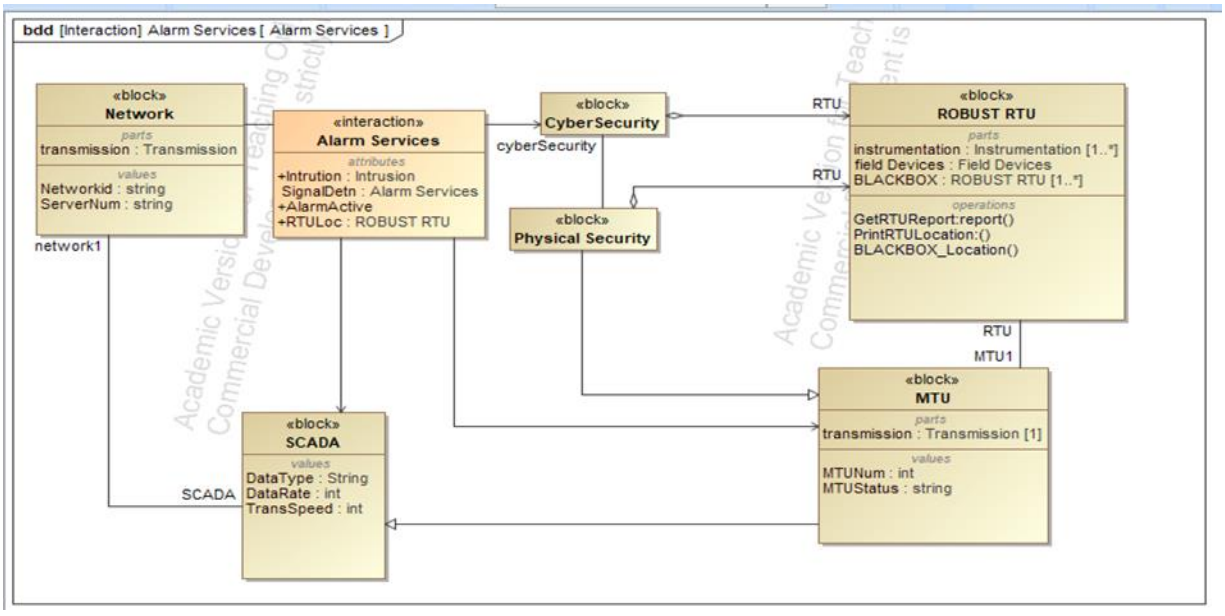


Fig. 2. Robust RTU with Blackbox within SCADA

The subsystem with the intrusion alarm will include video/camera with a system data recorder, storage, and processing. The cameras will send images to the control station to monitor the RTU environment 24/7. The alarm functions will detect changes and anomalies that indicate attacks or natural upsets and activate an emergency response protocol. The intrusion alarm will appear on the SCADA user interface with audio to alert the operator, and it can call the local emergency response and law enforcement. As part of the emergency response protocol, a real-time view of the RTU site is captured, and the emergency response team will carry out incident response protocols such as activating valves for isolation, shutdowns of pumps and motors.

The other subsystem, the operational and environmental data recording module (black box), records and stores a user-defined set of operating parameters for diagnostic, forensic, and risk analyses. This recorder will have inputs for the sensors and actuators (with some redundancy from the alarm function) and enough memory to record time-series records of these data as long as needed. This approach also improves logging and monitoring of sensors and actuators.

The space in the RTU system will be a determining factor in how it can be upgraded. Most RTU housings have additional space to accommodate the proposed security updates. For some newer RTUs, extra space will need to be made during design. The physical location of an RTU will need to be reexamined in the light of enhanced security functionality and placed strategically to maximize subsystem utility.

Changing the physical RTU configuration and software on-site can often be accomplished through software in the PLC programs. The upgrades proposed here will provide lower latency, more granularity, and more directly complete sensor, actuator, and control state data for local alarms and upstream control systems and operators. These will enable faster and better after-action investigations and include decision support to guide non-specialist utility field

operation crews. Water quality data from sensors can be recorded in the black box monitoring component and, using embedded functionality, it can trigger mitigation of water quality events.

Upgrading an existing RTU requires the following:

1. Sufficient physical space in the RTU enclosure for a black box or status module
2. Enough unused I/O in the PLC / Digital Control System
3. Sufficient PLC processor memory
4. A location sufficient to support the new system communication and monitoring upgrades

An RTU system upgraded in the manner described here will withstand significant natural and man-made interferences. It will record electronic and video operations for forensic review, and the RTU will have an automated maintenance process based on sensor inputs and system maintenance models.

A use case would be of an actor intruding on an RTU to disrupt operations. At that time, the associated camera and voice-activated recorder would capture their activities and voice. A control room operator will receive an alert and a real-time video of the RTU site event. More rapidly than at present, emergency messages to the local law enforcement and emergency response units are mobilized. Finally, critical security alerts will be transmitted to surrounding utilities to enable systemic responses and activate countermeasures and security alerts.

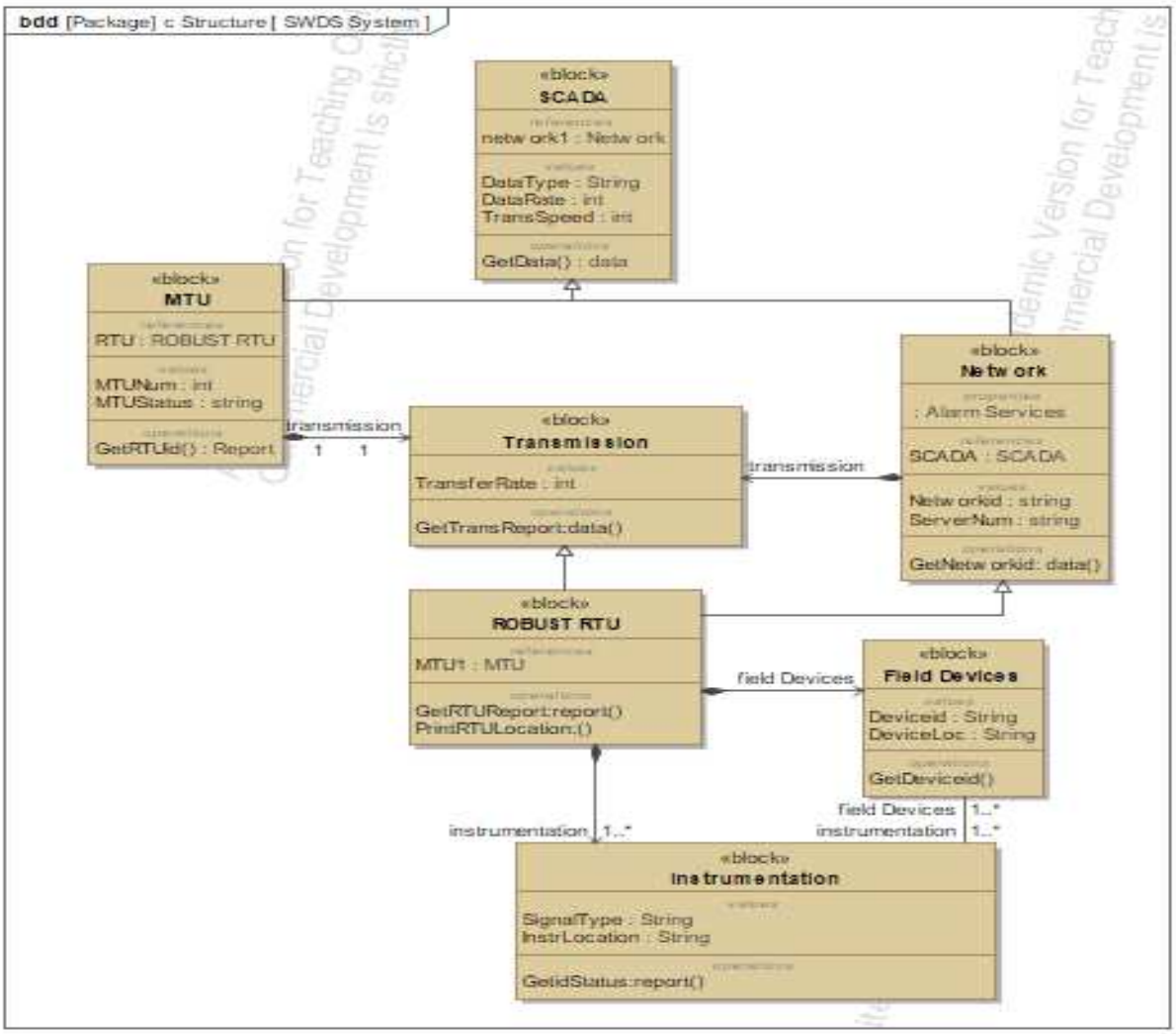


Fig. 3. SCADA Subsystems with More Robust RTU

CONCLUSIONS

RTUs in water distribution systems are vulnerable to physical and cyber- attacks. Utilities can enhance the security and resilience of their water distribution systems by making their RTU more robust to reduce vulnerabilities and improve detection of exploits that threaten system mission success.

The more secure and resilient RTU architecture described here should increase the security of water distribution Systems, decrease the time to restore operations after an upset, and reduce the time to identify and track those responsible. It would also substantially enhance situational awareness of system attacks. In addition, the new design supports a system-wide common operating approach for better utility control.

REFERENCES

1. Borky J. M & Bradley I. H. Effective Model-Based Systems engineering
2. Kossiakoff, A., Sweet, W. N., & Seymour, S. (2011). Systems engineering principles and practice: principles and practice. Retrieved from https://ebookcentral.proquest.com
3. Humphreys Brian E. (July 8, 2019). Critical Infrastructure: Emerging Trends and Policy Considerations for Congress.
4. Emerson Industry Week FAQ. How to Protect your PLC Control Systems from Security Threats.
5. Dakin, R., Newman, R., and Groves, D. (2009). "The case for cybersecurity in the water sector. " J. Am. Water Works Assoc. 101(12), 30.
6. E. Kovacs (2017). "New SCADA Flaws Ransomware, Other Attacks. Retrieved from https://www.security week.com
7. EPA. Water Infrastructure Resilience and Incidence Response. Retrieved from https://www.epa.gov/homeland-securityresearch/water-infrastructure-resilience-and-incident-response
8. Horta, R. (2007). "The city of Boca Raton: A case study in water utility cybersecurity. " J. Am. Water Works Assn., 99(3), 48.
9. Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyberwar, and other cyber threats, Center for Strategic and International Studies, Washington, DC.
10. Taormina, S., Tippenhauer, N., Galleli, S., Ostfeld, A., Salomons, E. (2016). Assessing the effect of cyber-physical attacks on water distribution systems. Conference Paper, May 2016.
11. Anderson, R. (2008). Security engineering. John Wiley & Sons.
12. Amin, S., Litrico, X., Sastry, S., and Bayen, A. M. (2013a). "Cyber Security of Water SCADA Systems -Part I: Analysis and experimentation of Stealthy Deception Attacks." IEEE T. Contr. Syst. T., 21(5), 1963-1970.
13. Kosut, O., Jia, L., Thomas, R. J., and Tong, L. (2010). "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures." Smart Grid

Communications (SmartGridComm), 2010 First IEEE International Conference on, IEEE. 220-225.

14. INCOSE. System Engineering Handbook, 2017.

15. Blanchard, B., & Fabrycky W. (2006). Systems Engineering and Analysis. Risk management. Pages 710 – 712.

16. National Communications System (NCS) (2004) 'Supervisory control and data acquisition (SCADA) 'systems,' Technical Information Bulletin, October, Vol. 4.

17. Shaw, W.T. (2013) 'SCADA system vulnerabilities to cyberattack,' Article, Electric Energy [online] https://electricenergyonline.com/?page=show_article&article=181

18. Water Boaster Station. Chartfield Engineer PC Retrieved from http://chatfieldengineers.com/water-distribution-systems/

19. United Nations Educational, Scientific and Cultural Organization (UNESCO) Water Security and the Sustainable Development Goals, UN-Water, 2013.

20. Ransomware attack hits North Carolina water utility following hurricane. Retrieved from https://www.csoonline.com/article/3314557/ransomware-attack-hits-north-carolina-water-utility-following-hurricane.html

21. Blake Sobczak. E&E News reporter. Hackers Force Water Utilities to Sink or Swim. Published on Thursday, March 28, 2019. Retrieved from https://www.eenews.net/stories/1060131769

22. The Coloraoan new. Published 1;20 P.M. MT, March 14, 2019, retrieved from https://www.coloradoan.com/story/money/2019/03/14/cyberattacker-demands-ransom-colorado-utility/3148951002/

23. Lee, E. A. (2008). "Cyber-physical systems: Design challenges."" 2008 11th IEEE Int. Symp. on Object-Oriented Real-Time Distributed Computing (ISORC), IEEE, New York, 363–369.

24. A Brief History of the SCADA System. Retrieved from https://www.processsolutions.com/a-brief-history-of-the-scada-system/

25. Zhang, P. Remote Terminal Unit (RTU). Advanced Industrial Control Technology. Retrieved from https://www.sciencedirect.com/topics/engineering/remote-terminal-unit

26. Israel National Cyber Directorate (INCD): Targeted attacks on Israeli water supply and wastewater treatment facilities. Retrieved from https://ics-cert.kaspersky.com/reports/2020/09/24/threat-landscape-for-industrial-automation-systems-h1-2020/

27. Industrial Control Systems Cybersecurity ICS-CERT. https://us-cert.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2011.pdf

APPENDIX B

SURVEY QUESTIONS ON RTU SYSTEMS SECURITY RISK AND VULNERABILITY ASSESSMENTS

by

Augustus Davies
Graduate Student, System Engineering Department
Colorado State University

Introduction Page

Water treatment plants (WTP) and water utility systems (WDS) use electromechanical and control devices as well as staff (Operators, Technicians, Engineers) to produce and distribute high-quality drinking water. One of the critical process control devices used is the Remote Terminal Units (RTU). The RTUs are used at pumping stations, booster stations, pressure reducing stations, water tanks, and wastewater facilities within a municipal service area. Remote Terminal Units play an essential role in the water utility system because they are the eyes and ears of the process. The RTU provides inputs to the Main Transmission Unit (MTU), also called the hub, which in turn provides data to SCADA.

The purpose of this survey is to assess the vulnerability of RTU, within WDPs and WDS. This survey will further examine the security requirements for exiting RTU against physical and cybersecurity threats. Your input and participation will be kept anonymous at your choice. It will help my doctoral research at Colorado State University Systems Engineering Department. Finally, the results of the survey will be utilized in conference papers, publications, and discussions to help improve RTU designs.

The survey consists of 14 questions, and you would have to answer all questions marked (*).

SURVEY QUESTIONS ON RTU SYSTEMS SECURITY RISK AND VULNERABILITY ASSESSMENTS

Participants Background Details

*1. Which of the following best describes your organization?

- o Water utility
- o Wastewater Utility
- o Both water/wastewater utility
- o Gas
- o Power
- o Other (please specify)

*2. Which of the following best describes your current job role?

- o Management
- o Engineer
- o Technician
- o Contractor
- o Other (please specify)

*3. Which of the following best describes the department you are attached to?

- o Engineering
- o IT
- o Facility Maintenance
- o Repair Shop
- o Other (specify)

*4. How many years have you been in the public Utility business?

- o Less than a year
- o 1-5 years

- 6-10 years
- 10-15 years
- More than 15 years

***5. POLICY AND PROCEDURES**

	Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral
In my organization, adequate security policies are Implemented for RTU system					
Adequate security training is implemented for the RTU system					
Adequate training is provided on RTU security architecture and design					
Adequate policies for RTU systems hardware/software are implemented					
My organization conducts adequate periodic audits on security policy.					
My organization has implemented adequate physical security measures at all RTU sites.					
My organization has implemented security measures to alert the control room operator					
In my organization, adequate police presence and patrols are provided for each RTU location.					
My organization has adequate disaster recovery documentation.					
My organization has provided adequate policies on videos and cameras at all RTU stations.					

***6 RTU VULNERABILITY SECTION**

	Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral
My organization enforces periodic RTU testing for the security changes					
My organization has physical security for all RTU sites					
My organization implements a physical parameter control for all RTU locations					
My organization has backup plans for all RTUs.					
My organization implements a physical parameter control for all RTUs.					
My organization implements locked RTU cabinet at all RTU stations					
My organization ensures all RTU intrusion alarm is sent to 911					
Most RTU are located at obscured or isolated areas.					

***7 RTU: CONFIGURATION VULNERABILITY**

	Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral
Periodic updates and configuration are implemented at all RTU locations.					
My organization implements encryption to secure password at all RTU and MTU stations					
My organization ensures an access control list (ACL) at all RTU stations.					

My organization uses security parameters at all RTU stations.					
My organization has implemented a firewall to protect all RTU locations					

***8. RTU: COMMUNICATION VULNERABILITIES**

	Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral
Communication between RTUs is constantly being monitored.					
Communication between RTU and SCADA are encrypted					
My organization authenticates users of the RTU system.					
My organization ensures integrity checks are performed on all RTU locations.					
In the case of RTU Intrusion, Alarm is sent to 911					
In the case of RTU Intrusion, Alarm is sent to the Control Room Operator.					

***9. MANAGEMENT CONTROLS OF RTU**

	Strongly Disagree	Disagree	Agree	Strongly Agree	Neutral
My organization implements a security assessment system.					
My organization has identified a person in charge (PIC) to conduct a security assessment					

My organization ensures routine security assessments at all RTU locations.					
My organization has specific plans instituted to control and maintain security.					
My organization has implemented RTU security training for all employees.					

***10. OPERATIONAL CONTROL OF RTU**

Which of the following policies are documented, implemented, and updated at your organization? (select if applicable)

- ○ Policies for Access Control
- ○ Policies for employee termination or transfer.
- ○ Policies for Third-party Security
- ○ Policies for physical protection for all RTUs.
- ○ Policies for Contingency Planning
- ○ Policies for RTU maintenance
- ○ Policies for Incident Response
- ○ Policies for RTU Security Training

11. If you could implement changes in the RTU system, what changes/upgrades would you recommend?

12. In your opinion, how secured are the RTU at the remote stations?

13. Do you have any suggestions on how to improve the security of the RTU system at your organization?

14. Are employees at your RTU sites physically secured?

Thank you very much for your participation.

APPENDIX C

FUNCTIONAL ANALYSIS OF RTU AND SCADA

Functional Elements	Functional Requirements (FR)
Signal flow	4-20 mA signals from Transmitters & field instruments to RTU & PLC Discrete and Analog signals from pump controls to PLC & MTU
Water utility System	Supply Water to Customers Maintain Water Pressure for Household, Fire Hydrants Network of Tanks and Reservoir
RTU	Main Hub at remote stations receiving and transmitting signals from Radio, PLC, UPS,
CRO	Located at Main Facility monitoring signal and manned 24/7
SCADA	Central point for Communications Software to bind all signals from stations Historian for data for Trend analysis
UPS	Provides backup power to RTU, Server, PLC
Radio	Located in the RTU, MTU sites Transmits and receives signals
Antenna	Forms part of communication Transmit signals from RTU to MTU/SCADA Vulnerable to attacks, interference
Sensor Exploitation	Field sensors including level, ultrasonic, flow, etc. to feed PLC Converts one signal to another and sends a final signal to RTU, MTU, etc. Critical to alarms, intrusion, pump, etc.

Instrumentation	Field equipment talks to PLC/RTU through the field instruments Forms eyes and ears on PLC/RTU, SCADA Vulnerable to attacks and interference
Alarming System	Means of intrusion detection for RTU Uses signal from instruments and Actors
Power Supply	Provide Power to the RTU, Radio & Instrumentation and Controls
Remote Stations	Remote station with RTU Including PRV, Boaster Station, Pumping Station, Reservoir
PLC	Located in RTU. Received data from sensors and field devices Vulnerable from physical/cyber attack

APPENDIX D

PLC LADDER LOGIC AND MBSE SYSTEMS FOR THE ROBUST RTU

Appendix C shows research on the use of MBSE or Ladder Logic for the PLC in the RTU to control field devices in the water utility system. First, the Remote Telemetry Unit controls electromechanical devices, including pumps, motors, mixers, levels, flows, transmitters, and actuators. Then, the data gathered from the remote location are transmitted to the MTU and SCADA. Below are examples of the use of PLC ladder Logic or MBSE in RTUs.

- An alternate approach would be to use a more generic system modeling tool to capture overall architecture and connect it to the more specialized tools for specific purposes. This would allow users to apply the best practices of modern Model-Based Systems Engineering (MBSE), such as OMG SysML (Systems Modeling Language), to the RCS domain.

  Reference:
  Dirk Zwemer, 2017. Applying MBSE to Railway Control System Part 1. Retrieved from https://intercax.com/2017/08/16/railway-control-system-modeling-part-1

- The key issue in front of these experts will be how to perfectly solve the structured, modular, how to implement the structured system engineering (MBSE) to build IT OT endogenic fusion, how to implement a model-based system engineering (MBSE).

  Reference:
  Peng Yu (2021). Open Industrial Control System Design Model Puzzle. Shanghai Industrial Automation Instrumentation Research Institute, PLC open China Organization.

- A Model-Based Systems Engineering (MBSE) approach consists in using a formal digital language to specify, design, analyze and verify a system. It enables the implementation of workbenches providing modeling services such as edition, visualization, transformation, comparison, storage, etc.

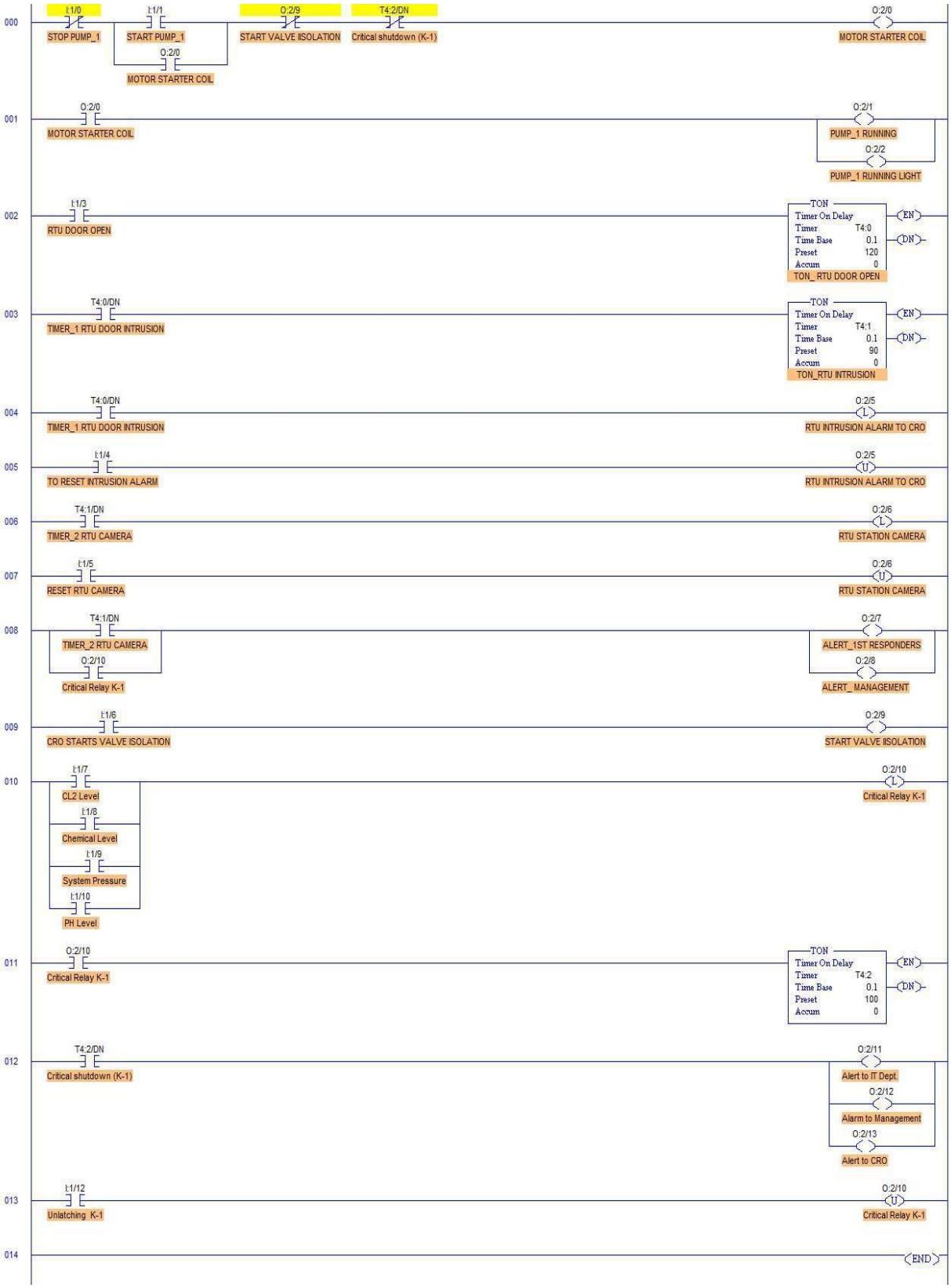
  Reference:
  Capella. Using a formal digital language. Retrieved from https://www.eclipse.org/capella/what_is_mbse.html

- An object-oriented extension of the IEC 61131-3 standard has also recently been adopted, but regarding the possible level of abstraction there is still a gap between MBSE and PLC programming. Again, splits up model and code and does not encourage the use of the model during the operational phase of the PLC.

  Reference:
  Christian Brecher, Johannes A. Nittinger, Andreas Karlberger. Model-based control of a handling system with SysML. Retrieved from https://core.ac.uk/download/pdf/82354387.pdf

- Of the various languages one can use to program a PLC, ladder logic is the only one directly modeled after electromechanical relay systems.

  Reference:
  Michael Stephen, 2019. .Ladder Logic in Programmable Logic Controllers (PLCs). Retrieved from https://control.com/technical-articles/ladder-logic-in-programmable-logic-controllers-plcs/


000
I:1/0
STOP PUMP_1
I:1/1
START PUMP_1
O:2/0
MOTOR STARTER COIL
O:2/9
START VALVE ISOLATION
T4:2/DN
Critical shutdown (K-1)
O:2/0
MOTOR STARTER COIL
001
O:2/0
MOTOR STARTER COIL
O:2/1
PUMP_1 RUNNING
O:2/2
PUMP_1 RUNNING LIGHT
002
I:1/3
RTU DOOR OPEN
TON
Timer On Delay
Timer T4:0
Time Base 0.1
Preset 120
Accum 0
EN
DN
TON_ RTU DOOR OPEN
003
T4:0/DN
TIMER_1 RTU DOOR INTRUSION
TON
Timer On Delay
Timer T4:1
Time Base 0.1
Preset 90
Accum 0
EN
DN
TON_RTU INTRUSION
004
T4:0/DN
TIMER_1 RTU DOOR INTRUSION
O:2/5
L
RTU INTRUSION ALARM TO CRO
005
I:1/4
TO RESET INTRUSION ALARM
O:2/5
U
RTU INTRUSION ALARM TO CRO
006
T4:1/DN
TIMER_2 RTU CAMERA
O:2/6
L
RTU STATION CAMERA
007
I:1/5
RESET RTU CAMERA
O:2/6
U
RTU STATION CAMERA
008
T4:1/DN
TIMER_2 RTU CAMERA
O:2/10
Critical Relay K-1
O:2/7
ALERT_1ST RESPONDERS
O:2/8
ALERT_ MANAGEMENT
009
I:1/6
CRO STARTS VALVE ISOLATION
O:2/9
START VALVE ISOLATION
010
I:1/7
CL2 Level
I:1/8
Chemical Level
I:1/9
System Pressure
I:1/10
PH Level
O:2/10
L
Critical Relay K-1
011
O:2/10
Critical Relay K-1
TON
Timer On Delay
Timer T4:2
Time Base 0.1
Preset 100
Accum 0
EN
DN
012
T4:2/DN
Critical shutdown (K-1)
O:2/11
Alert to IT Dept.
O:2/12
Alarm to Management
O:2/13
Alert to CRO
013
I:1/12
Unlatching K-1
O:2/10
U
Critical Relay K-1
014
END

APPENDIX E

SWITCH SNAP ACTION SPDT 4A 250V

Digi-Key Part Number	480-5901-ND
Manufacturer	Honeywell Sensing and Productivity Solutions
Manufacturer Product Number	GXE51A1B
Supplier	Honeywell Sensing and Productivity Solutions
Description	SWITCH SNAP ACTION SPDT 4A 250V

Product Attributes

TYPE	DESCRIPTION
Category	Switches Snap Action, Limit Switches
Mfr	Honeywell Sensing and Productivity Solutions
Series	GXE
Package	Bulk
Part Status	Not For New Designs
Circuit	SPDT
Switch Function	On-Mom
Current Rating (Amps)	4A (AC), 150mA (DC)
Voltage Rating - AC	250 V
Voltage Rating - DC	25 V
Actuator Type	Side Rotary, Roller
Mounting Type	Chassis Mount
Termination Style	Cable Leads
Ingress Protection	IP66 - Dust Tight, Water Resistant
Features	Explosion Proof

TYPE	DESCRIPTION	
Operating Force	25gfm	
Release Force	-	
Pretravel	26°	
Differential Travel	8°	
Overtravel	-	
Operating Temperature	-20°C ~ 60°C	
Operating Position	26°	
Electrical Life	-	
Mechanical Life	2,000,000 Cycles	
Base Product Number	GXE51	

APPENDIX F

900 MHZ YAGI ANTENNA. HEAVY DUTY 7 ELEMENT YAGI FOR 880-960 MHZ ISM WITH 12 DBI GAIN. KATHREIN SCALA EQUIVALENT

The RFMAX RY-900-12-7-SNF-19 is a heavy duty, Gold Anodized, 900 MHz Kathrein - Scala equivalent Yagi Antenna operating within the 880-960 MHz ISM frequency range. This TY900 antenna model is the RFMAX "premium" offering, with a full IP67 rating to withstand severe outdoor weather conditions. This is suitable for 900 MHz spread spectrum applications, SCADA system radios that operate in the unlicensed 896-940 MHz frequency range and for all applications working in 900 ISM Band. This unit features 360-degree welds around each of the seven elements, no gamma match to ice up, corrode or detune, and has gold anodizing added for overall corrosion resistance. This design provides performance and durability equivalent to PCTel, Laird, Kathrein, Larsen, Scala, Wilson, L-Com, etc.

Key features:

11. Frequency: 880-960 MHz
12. No. of Elements: 7
13. Dimension (LxH): 24 x 6.6 inches
14. Peak Gain: 12.2 dBi
15. Max Input Power: 200 watts
16. Wind Survival Rating: 136 MPH
17. Cast Aluminum Mounting Kit Included
18. 19 Inch Cable & N-Female Connector
19. 5 Year Factory Warranty!

https://www.rfmax.com/products/ry-900-12-7-snf-19-900-mhz-yagi-antenna-heavy-duty-7-element-yagi-for-880-960-mhz-ism-with-12-dbi-gaiin-kathrein-scala-equivalent

APPENDIX G

OTHER MATERIALS FOR THE ENHANCED RTU

Older SCADA systems used a monolithic architecture based on standalone or mainframe systems with no networking capabilities. Some utilities still use monolithic architecture, but because they are vulnerable to physical and cyber-attacks, they should be upgraded to enhance their security. The next generation of SCADA used a distributed architecture that included communication processors, human-machine interface, RTUs, and databases. In addition, the distributed architecture system has several access points to field devices such as chemical dosage detection, flow measurement, and control feedback signals to pumps and motors.

The current generation of SCADA uses a network system architecture. Significant improvement has been made by using wide area networks (WAN) protocols such as the TCP/IP, UDP, and cloud computing for communication between the MTU and RTU, which separates the RTU portion of communications with field devices from the MTU. These enhanced communication capabilities are accompanied by increased security risks. In addition, networked SCADA architecture allows open architecture communication protocols and standards, enabling SCADA functionality using LAN and WAN topology (Lee, 2008).

Timing for RTU Subsystem Response

The communication network of a SCADA system connects RTUs with MTUs. Sometimes between RTUs. Communication links take many forms, including leased lines, public-switched telephone networks (PSTNs), Internet Protocol (IP) based landlines, dedicated frequency, radio, microwave, and satellite.

The alarms or signals generated from the energization of the critical relay (K-1) will be assigned the highest alarm category. This category of alarm management provides notification of factual information to critical stakeholders and operators promptly. The goal is to assist the operator in preventing or minimizing system downtime and catastrophic situations such as water contamination to users by overriding noncritical actions such as polling. Therefore, telemetry systems must be hardened and respond to rapid state changes and alarms.

Considerations of the Architecture of the Enhanced RTU

Table 2 showing vulnerable subsystems and components of SCADA

System	**Security Feature**	**Measures**	**Model element**
MTU	Cyber/Procedural Security Measures	Fire wall, Virus protection,	Adapter Component Domain
MCC	Cyber/Procedural Security Measures	Cameras, intrusion detection, firewall	Subsystem CDM System Service
RTU	Cyber/Physical	Camera, Intrusion detection, Call to First Responders, Black box for data forensics, Setpoint monitoring	PLC, Radio Subdomain Black box Site security
Antenna	Cyber/Physical	Camera, intrusion alarms	Modem Component
Interface/Ports	Cyber/Physical	Intrusion alarms, synchronization faults	Network Interface Card (NIC)

Structural Perspective shows a breakdown of the SWUS into domain composition diagrams. Fig 21 shows a Block Definition Diagram (BDD) of the SWUS depicts a top-level partitioning of the architecture into Domains, showing functional and process values, operations, and parts. Again, this section shows the Internal Block Diagram (IBD) of the SWUS domains with ports and User Roles.

Requirement for the Enhanced RTU

This section describes the functional and activity analyses of the RTU for upgrading. A functional analysis divides the SCADA system into subsystems and describes their functions (Table 4) to enumerate its components and functions. Data flows from the field instruments to the RTU and the MTU. In addition, functional analyses include all of the functions that SCADA and RTU systems must perform to meet security and robustness requirements (Table 4). Contrary, non-functional requirements, also known as system quality attributes, describe the behavior of the enhanced RTU of the SCADA system and the constraints of its functionality. Examples of non-functional requirements include usability, reliability, performance, supportability, scalability, and interoperability.

Existing RTU System

Fig. 23 shows the existing RTU components layout which is missing the critical component for intrusion detection, video/voice recorder. To qualify for upgrade, and to make it enhanced, the following questions:

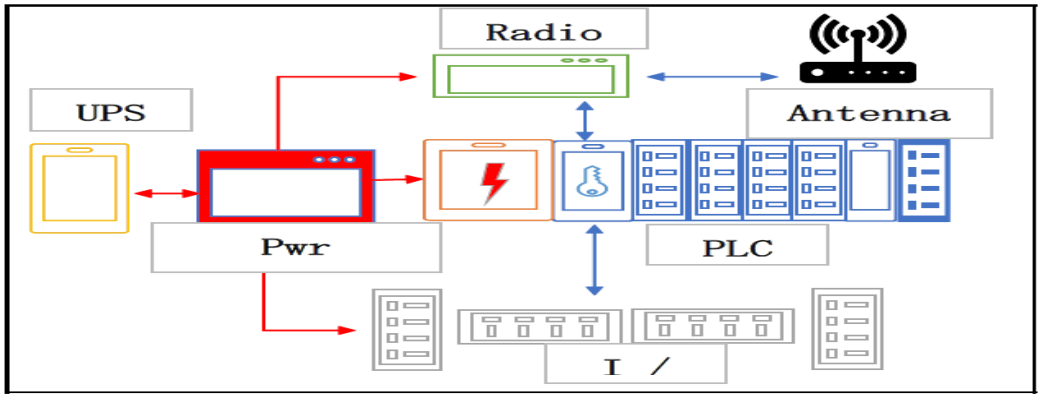


Fig. 41. Data flow in existing RTU

i. Sufficient available physical space in the RTU enclosure for a black box or status module

ii. Enough unused I/O in the PLC / DCS system;

iii. Sufficient PLC processor memory is enough to support the upgrade.

iv. A location sufficient to support the new system communication and monitoring upgrade.

Table 3. Non-cyber vulnerabilities and solutions to make RTUs more Robust

Vandalism	Installing a secured camera on site will capture intruders within the RTU location and alert the control room operator
Voice control spoofing	An embedded voice activation recorder can capture intruder voices, accents, etc., this can serve as a deterrent or help during prosecution
RTU and downstream exploits	As described subsequently, install a "black box" in the RTU that can gather real-time forensic data to assist incident response and analysis
Internal treat including disgruntled employee	Restricted access to Enhanced RTU. RTU site camera and access control to record and send anomalies to CRO and management.
Hz Interference – electronics, freq. manipulation near RTU	Enhanced RTU monitors/restrict changes to endpoints of process variables including chemical dosage, system pressure, CL2 level etc.
Natural disturbances e.g. Earth quake	Enhanced RTU will detect abnormal process changes to the selected parameters, shut down and send alert to CRO and management. RTU site camera will capture event.

Vulnerabilities leading to cyberattacks on water utility systems, as indicated in chapter 2, including physical, vandalism, and natural disturbances, need more attention. The enhanced RTU subsystems are described below.

The author discusses the changing attack surface of RTU subsystems in water utility systems, and how exploits propagate to upstream SCADA systems and downstream to sensors, monitors, and actuators to degrade performance, safety, and water availability. The proposed changes to existing RTU designs will improve its robustness, cost of damage, detection time, mitigation, and time to respond, which will minimize the impact of exploiting vulnerabilities.

Physical Viewpoint (PV)

The PV completes the architecture modeling, which is the basis for implementing an enhanced RTU prototype's capabilities. The PV is the transition from design to implementation, which involves selecting specific hardware and software products, software programming language(s), a detailed standards profile, messaging and networking solutions, and other aspects of a point design [2].

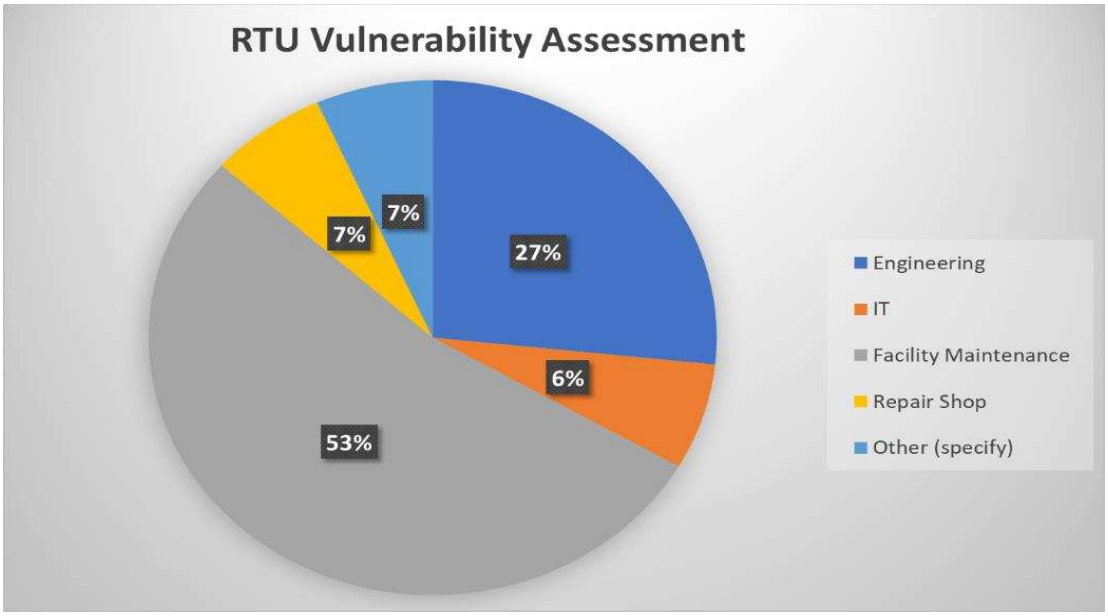


Figure 29. RTU Vulnerability Assessment

Responses from the organizational perspective of securing RTU and enforcing policies to ensure RTU sites are protected revealed an urgent need to secure the RTU. The following safety measures were validated during the questionnaire:

1. Lack of physical and perimeter controls at the RTU sites.
2. Lack of RTU intrusion alarm to first responders for security backup for utility personnel and the critical RTU that feeds SCADA system.
3. RTU cabinet doors are not adequately locked nor protected against bad actors.

4. Intrusion alarm to the control room operator (CRO) needs enforcement.
5. Organizational security backup plans for RTU, on-call personnel are not existing.

Furthermore, responses obtained from the questionnaire emphasized what the author observed in the various utilities that he worked. Hence, the objective of this thesis, to propose enhancing existing RTUs and adding security features to make RTUs robust and hardened against physical and cyber threats in the water utility system.

The bar graph below shows the responses from the questionnaire on RTU communications. Again, it shows the vulnerability of the communication of data from RTU to the MTU of the SCADA system.

Furthermore, the MBSE principle [2] and the use of Cameo Enterprise Architecture 19.0 software helped enhance and analyze the proposed Enhanced RTU by integrating a new black box subsystem within the RTU of the SCADA architecture. In addition, the principles ensured interrelationship between the subsystems and the components, a clear pictorial diagram of each subsystem and connectivity, and dependencies within the RTU.

Making the RTU Secured and Robust against physical and cyber threats using Ladder Logic programming language make existing RTUs operator friendly, will provide continuity of knowledge base for the majority of Engineers, Technicians, and Operators who work with RTU. Results from the questionnaire, literature review, and author's experience indicate that the Ladder logic software is preferred. Below are some of the advantages of ladder logic. Existing RTUs have ladder logic which makes the enhancement favorable.

1. Cost of savings
2. Provides validation of coil energizing and contact open/close.
3. It provides validation of I/O, Timers, coils, and field devices
4. Periodic report generation.
5. Allows reprogramming and improvements.

APPENDIX H

UPCOMING PRESENTATION 1:

WATER ENVIRONMENTAL FEDERATION'S TECHNICAL EXHIBISHION AND CONFERENCE (WEFTEC) 2022

TOPIC: RTU HARDENING TO ENHANCE WATER UTILITY SECURITY

ABSTRACT

Authors/Presenters:

1. Augustus W. Davies
   WSSC Water, Laurel, Maryland
   Doctoral Student, Department of Systems Engineering,
   Colorado State University, Fort Collins, Colorado, USA

2. Dr. Venkatachalam, Chandra
   University Distinguished Professor
   Colorado State University
   Department of Electrical and Computer Engineering, Fort Collins, Colorado. USA

3. Dr. J. B. Dubow
   Faculty Affiliate of Colorado State University
   Department of Systems Engineering, Fort Collins, Colorado. USA
   He is presently a Principal in Anantara Systems, Vienna, Virginia, USA

4. Dr. John M. Borky
   Faculty Affiliate of Colorado State University
   Department of Systems Engineering, Fort Collins, Colorado. USA

5. Dr. Chris Weinberger
   Colorado State University
   Assistant Professor in the Mechanical Engineering
   Department of Mechanical Engineering, Fort Collins, Colorado. USA

TOPIC: Resilience and Security (Including Emergency Operations and Safety)

FOCUS AREA: Research and Technology

Learning objectives:

1. RTU hardening will enhance water utility security
2. Automated setpoint checking will prevent many damaging attacks

Keywords:

SCADA, RTU, MTU, CRO, Cybersecurity, Setpoint Monitoring, Resilience, Alarms, physical security.

1. Objective:

Water Utility security is increasingly a focus of critical infrastructure security. The EPA and the White House recently launched a cyber security plan for the water sector [3]. This paper describes how hardening the RTU will improve water sector cybersecurity. RTU is the water utility component in direct contact with the sensors and subsystems that distribute, treat, and monitor water and wastewater infrastructure. This hardening will also reduce the vulnerability of the water utility to cyber-attacks.

2. Status

At present, we have a methodology to design, implement and simulate new RTU subsystems and suitably modify its MTU-SCADA-Control Room control chain. The enhancement focused on compatibility and interoperability with existing water utility technology, thereby minimizing or eliminating the need to invest in new components. The simulations use

PLC, the industry standard for simulation and operation or water utilities [2]. It is a continuation of work published earlier.

3. Methodology

The methodology consisted of using MBSE (Model-Based System Engineering) [1] to guide in enhanced RTU design; selecting components appropriate to hardening present RTUs; simulating the existing and enhanced RTU using PLC; simulating both RTUs under attack, and then comparing their performance.

Simulating the RTU as a system including SCADA in MBSE determined the critical nodes and highlighted design choices. The MBSE analysis used CAMEO Enterprise software for obtaining a high-level system architecture and design. It enabled the SCADA-MTU-RTU-Field Devices system to be decomposed into subsystems. The RTU subsystem was extracted to allow a more detailed analysis of RTU design parameters.

Once these were identified, existing Water utility operations and MBSE results were combined to determine: 1) Requirements; and 2) Design parameters of the Enhanced RTU. Following that, 1) the enhanced RTU was analyzed, and 2) specific implementations of the Enhanced RTU were developed. Finally, 3) These designs simulated, 4) Validated using present-day RTU operation programs, and 5) Test simulations of existing and enhanced RTU robustness in regular operation and under some attack scenarios. PLC Ladder Logic program and modeling were employed because over ninety percent of water utilities use PLC ladder logic in their operations.

The enhanced RTU receives control data from the SCADA through the MTU before applying it to field devices. It tests these data to ensure it is within the range of the process variables, provides time-stamps for referencing, detects out-of-range controls, and finally sends alarms to stakeholders through the MTU/SCADA data chain when a suspicious signal is detected.

Findings

The security enhancements follow from two considerations. First, the enhanced RTU will increase situational awareness and mitigation at the primary data source locations for water systems. Second, an embedded component will retain time-stamped records of the RTU Input/output signals. These data will be tested for abnormal, or out-of-bounds values and questionable values reported; Third, enhancing RTU alarming and antenna functionality will improve component robustness and reliability.

4. Significance

The enhanced RTU improves exploit detection, makes incident response quicker, and reduces the time to restore operations.

The enhanced RTU will substantially improve situational awareness of cyber and physical attacks for those involved in water systems security. It will provide the information needed to develop a system-wide common operating picture better to control its security and non-security aspects better.

The final step was the transition from the MBSE design into Ladder Logic since it is the preferred programming software used in the United States. Enhanced RTU simulation and testing used Ladder Logic programming.

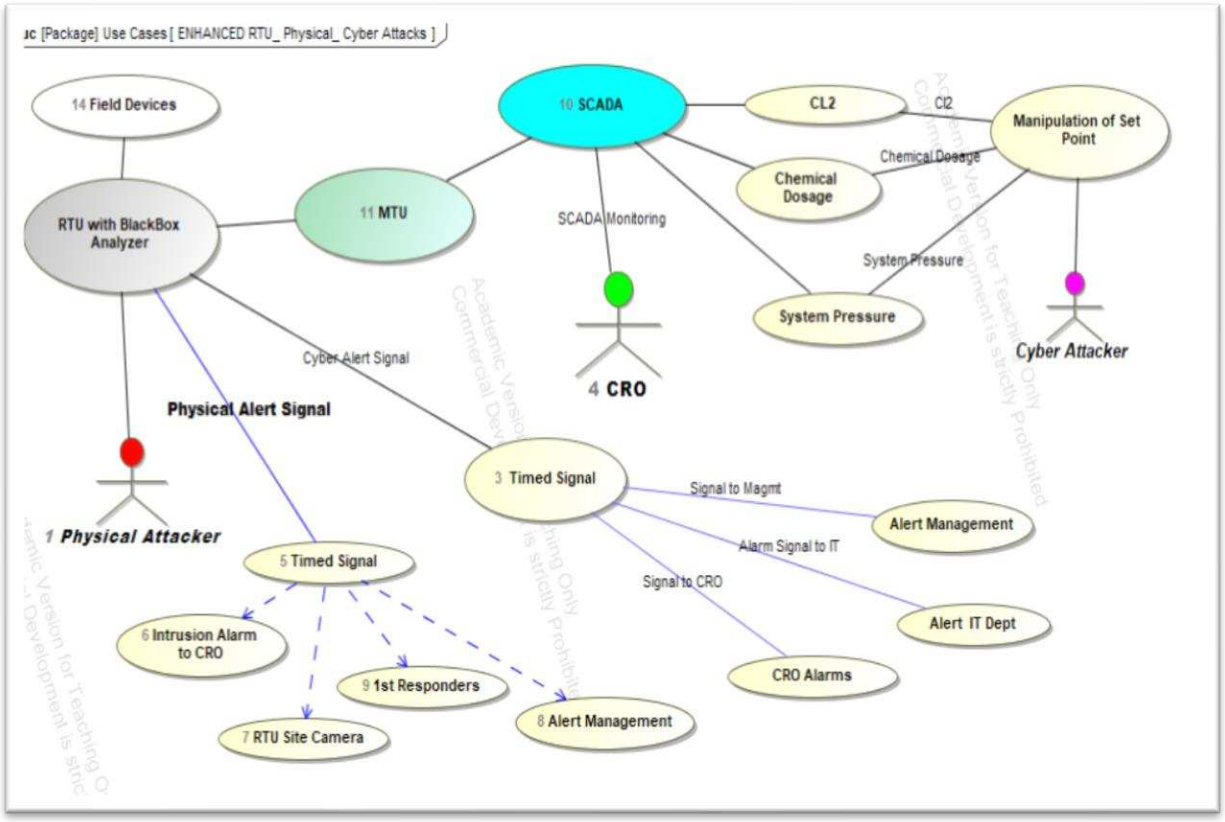


Fig 1. Use Case of Enhanced RTU in WUS SCADA System [2]

Figure 1 is a simplified one-line diagram of secured water utility system (SWUS) SCADA with enhanced RTU. The RTU is the closest to the water utility system and wastewater system, field devices, hence, the reason for enhancing the RTU subsystem of the SCADA. When a bad actor accesses the RTU, they can alter process setpoints to increase or decrease chemical levels and other critical system parameters. Again, PH levels and system pressure can affect the final delivered portable water to consumers and fire hydrants.

Moreover, a bad actor can cause sanitary sewage overflows of wastewater and water main breaks to disrupt roads and other critical infrastructure usages. Furthermore, bad actors in control of RTUs can control pumping stations, water utility booster stations, pressure-reducing valves to hospitals military facilities, and demand a ransom before restoring services.

References

[1] Borky J. M & Bradley I. H. (2019). Effective Model-Based Systems engineering. Springer International Publishing.

[2] Davies A. W., Dubow J. B., Borky J. M., Collins G. Analyzing and Mitigating Water Utility System Vulnerabilities. AWWA Journal, January 2022.

[3] EPA, White House launch cybersecurity plan for water sector. Retrieved from https://www.waterworld.com/drinking-water/press-release/14232852/epa-white-house-launch-cybersecurity-plan-for-water-sector. WaterWorld, February 2022.

[4] Taormina, S., Tippenhauer, N., Galleli, S., Ostfeld, A., Salomons, E. Assessing the effect of cyber-physical attacks on water distribution systems. Conference Paper, May 2016.

[5] Ferrier, P. The Cyberattacker demands ransom from Northern Colorado utility. Retrieved from https://www.coloradoan.com/story/money/2019/03/14/cyberattacker-demands-ransom-colorado-utility/3148951002/. Coloradoan News. March 24, 2019,

[6] Dan Kroll, Karl King, Terry Engelhardt, Mark Gibson, and Katy Craig, Hach Homeland Security Technologies. Terrorism Vulnerabilities to the Water Supply and the Role of the Consumer Water Security White Paper. Retrieved from https://www.waterworld.com/water-utility-management/article/16219980/terrorism-vulnerabilities-to-the-water-supply-and-the-role-of-the-consumer-a-water-security-white-paper/. WaterWorld, March 9, 2010.

APPENDIX I

UPCOMING PRESENTATION 2:

GLOBAL SECURITY EXCHANGE (GSX) SEPTEMBER, 2022 PRESENTTION

TOPIC: RTU HARDENEING TO ENHANCE WATER UTILITY SECUTIRY

Authors/Presenters:

1. Augustus W. Davies
   WSSC Water, Laurel, Maryland
   Doctoral Student, Department of Systems Engineering,
   Colorado State University, Fort Collins, Colorado, USA

2. Dr. Venkatachalam, Chandra
   University Distinguished Professor
   Colorado State University
   Department of Electrical and Computer Engineering, Fort Collins, Colorado. USA

3. Dr. J. B. Dubow
   Faculty Affiliate of Colorado State University
   Department of Systems Engineering, Fort Collins, Colorado. USA
   He is presently a Principal in Anantara Systems, Vienna, Virginia, USA

4. Dr. John M. Borky
   Faculty Affiliate of Colorado State University
   Department of Systems Engineering, Fort Collins, Colorado. USA

5. Dr. Chris Weinberger
   Colorado State University
   Assistant Professor in the Mechanical Engineering
   Department of Mechanical Engineering, Fort Collins, Colorado. USA

ABSTRACT

Water Utility security impacts other critical infrastructure components and is thus a focus for improving security. The RTU is closest to daily utility operations, including sensors, meters, and control subsystems that distribute, treat and monitor water and wastewater.

RTU hardening reduces water utility vulnerability to physical and cyber-attacks, provides faster and more precise alerts and forensic data, and a shorter time to restore operations. This presentation describes a methodology and a design that enhances RTU and water utility security.

Enhancements include set point checking, intra-component communication certification, data logging, audio-visual monitoring, and antenna hardening.

Finally, the presentation compares the incident response of a present-day RTU with that of an Enhanced RTU.