Evaluation of SCADA Test Beds and Design of a New Software-Based Test Bed

İsmail Erkek
Information Security Engineering
Graduate School of Natural and Applied Sciences
Gazi University
Ankara, Türkiye
ismailerkek2014@gmail.com

Erdal Irmak
Electrical and Electronics Engineering
Faculty of Technology
Gazi University
Ankara, Türkiye
erdal@gazi.edu.tr

***Abstract*—Critical infrastructure sectors such as energy, public services, finance, transportation, water management, and production are crucial for national security. They rely on Supervisory Control and Data Acquisition (SCADA) systems for monitoring and control. A failure or cyber-attack on these systems can have severe consequences, including service disruptions, data breaches, and threats to human life, societal order, economy, and security. Hence, ensuring robust security measures for these systems is essential. This study conducts research on test bed centers designed to enhance the security of SCADA systems considered as critical infrastructure. Comparisons and analyses are made among physical simulation, virtualization, and software-based emulation environments in these test bed centers. It is evaluated that test bed centers based on physical simulation are both costly and limited to local environments. In the proposed study, a test bed is designed with a software-based approach, specifically focusing on the S7comm industrial communication infrastructure predominantly used by Siemens devices, which has been less utilized in the literature. The aim is to enhance the security of the S7comm communication protocol through experiments conducted on the test bed. The evaluation conducted at the end of the study suggests that working with various cybersecurity disciplines on the designed test bed would significantly contribute to the security of critical infrastructure.**

Keywords—SCADA, cybersecurity, critical infrastructure

I. Introduction

Systems that can lead to the disruption of a country's societal well-being, harm its national economy, or pose risks to national security in the event of functional malfunction or security breaches, information disclosures, or service interruptions, can be defined as critical infrastructure. In this regard, countries such as the US and EU have identified energy, water, transportation, healthcare, banking, nuclear/chemical facilities, and communication infrastructure as critical sectors and classified their respective infrastructures as critical infrastructure. Definitions of critical infrastructure have been established in the EU Commission's 2004 publication titled "Protection of Critical Infrastructure in the Context of Counter-Terrorism" [1], as well as in US legislation, describing them as "assets, systems, or related components that, if disrupted or destroyed, would have a significant impact on a member state by insufficiently maintaining vital social functions, health, safety, security, and the continuity of economic and societal well-being. In Türkiye, the critical infrastructure sectors aimed at ensuring national cybersecurity, protecting critical infrastructure, and enhancing resilience have been identified in the National Cybersecurity Strategy and Action Plan for 2020-2023 [2]. Significant activities are carried out to protect the critical infrastructure sectors defined as electronic communications, energy, finance, transportation, water management, and critical public services.

The monitoring, surveillance, and control of systems and infrastructure components used in critical infrastructure sectors are provided through SCADA. With the increasing prevalence and usage rates of information and communication technologies in recent years, integration efforts are conducted in SCADA systems when necessary, leading to a digital transformation. Security vulnerabilities, threats, and potential risks emerging in information and communication technologies can directly impact the sectors controlled by SCADA systems and potentially cause damage to the systems operating in these sectors.

Countries establish test bed centers, both independently and through collaborations with universities and government-supported institutions, to protect their critical infrastructure and conduct security research. These centers serve as controlled environments for security researchers to simulate and analyze potential cyber-attacks on critical infrastructures, allowing them to gain valuable insights and develop effective security measures. By conducting experiments and studies within these test beds, researchers contribute to the existing literature on cybersecurity and provide valuable input for the formulation of countries' strategies and policies. However, the physical location of many test beds within responsible institutions and organizations can limit access for independent security researchers, hindering their ability to contribute to the field. Efforts are being made to establish more open and collaborative test bed centers that facilitate the participation of diverse stakeholders and promote innovation in cybersecurity practices. These test bed centers, with their comprehensive evaluations and research outcomes, have the potential to significantly impact countries' cybersecurity strategies and policies, fostering a more resilient and secure critical infrastructure landscape.

Numerous test bed projects have been observed in the literature, designed and developed in physical, software-based, or virtualized environments to enhance cybersecurity in critical infrastructures across sectors. These projects incur significant costs for the institutions involved. Detailed information about some projects can be found in Table 1. The comprehensive insights provided by these test bed projects contribute to the advancement of cybersecurity practices and inform future developments in safeguarding critical infrastructures.

TABLE I. COMPARATIVE ANALYSIS OF SOME SCADA TEST BEDS

Ref.	Location	Protocol/System	Type	Scope
[3]	Augsburg University, Germany	RaspberryPi, OpenPLC, FreeRTOS	Physical simulation	Physical processing, control center
[4]	Federal Institute of Education, Sci. and Tech. of Sao Paulo, Brazil	Schneider PLC, Water Tank Emulation, Modbus TCP	Physical simulation	Physical processing, control center, field equipment
[5]	National Critical Infrastructure Test Bed Center, Sakarya Univ. Türkiye	DNP3, S7, EtherCAT, Modbus	Physical simulation	Physical processing, control center, field equipment
[6]	Mississippi State University, USA	Modbus, DNP3, GE, SCADAPack LP	Physical simulation	Physical processing, control center, field equipment
[7]	Gazi University, Türkiye	Profinet, S7, Siemens S7-300	Physical simulation	Physical processing, communication infrastructure
[8]	RMIT University, Australia	Modbus,CORE Emulator, EPANET	Virtualization	Physical processing, control center, field equipment
[9]	Singapore University, Singapore	Allen-Bradley, EtherNet/IP	Physical simulation	Physical processing, field equipment, communication infrastructure, IoT
[10]	Idaho University, USA	Matlab, Modbus, Modbus PLC Simulator	Software-based simulation, emulation	Physical processing, field equipment, communication infrastructure
[11]	New Orleans University, USA	Modbus, EtherNet/IP, Profinet, Schneider PLC	Physical simulation	Physical processing, control center, field equipment, comm. infrastructure
[12]	Sam Houston State University	Modbus, DNP3, OPC UA, Palo Alto, Cisco, Indusoft, ModRSSim	Physical simulation	Physical processing, control center, field equipment, comm. infrastructure

Sauer et al. developed an open-source SCADA test bed costing 500 Euros as part of their research and development activities. The test bed, designed for threat modeling, was used to create attack scenarios. The study concluded that open-source software and hardware can be utilized to develop a test bed for SCADA security [3].

Teixeira et al. developed a test bed center consisting of a control system for a water storage tank, which is a stage in the water distribution process. Various attack scenarios were applied to the test environment. The captured network traffic during the attacks was used to create a dataset for training and testing different machine learning algorithms [4].

Özçelik et al. developed a secure test bed infrastructure for waste and potable water management. The test bed, established under the National Critical Infrastructure Test Bed Center, serves for education, security research, and analysis/tests of attack and defense. It supports multiple ICS protocols such as DNP3, S7, EtherCAT, and Modbus. Each station in the processes is autonomously controlled by local RTUs/PLCs and protected by separate networks and firewalls. The developed SCADA applications allow for the selection of scenarios and alternative implementations, offering features like monitoring, recording, and cyber-attack detection [5].

Morris et al. developed a test bed center that combines various critical infrastructure sectors. It includes functional and physical control modules, utilizes commercial software and hardware infrastructure, and supports multiple industrial communication protocols. The test bed has been used in various research studies, focusing on security vulnerabilities and exploits [6].

Irmak et al. developed a basic test bed using Siemens S7-300 PLC to control physical processes. They demonstrated that industrial communication protocols could be manipulated by applying different types of attack scenarios on the test bed. They also discussed security measures that can be implemented against such attacks [7].

Almalawi et al. propose a test bed based on virtualization technology. They used EPANET software for water distribution systems and a proxy server. The CORE emulation software was employed for the virtualization environment. Two different attack scenarios were conducted in this virtual environment, and the results were analyzed [8].

Mathur and Tippenhauer developed a test bed called SWaT to understand the impact of cyber and physical attacks on a water treatment system. The test bed allows for evaluating the effectiveness of intrusion detection algorithms and analyzing the effectiveness of defense mechanisms under attack conditions. It also enables studying the consecutive effects of failures in one ICS on another dependent ICS. The SWaT test bed was made accessible over the internet for authorized researchers to conduct security research [9].

Koganti et al. implemented a virtual test bed environment using Matlab Simulink to control a distribution breaker system of an electrical grid. They conducted two cyber-attack simulations using the test bed environment and analyzed the results [10].

Ahmed et al. developed a fully functional test bed that models the physical processes of a gas pipeline, an energy transmission and distribution system, and a wastewater treatment plant. The test bed supports research activities related to SCADA systems, such as cybersecurity research, forensic investigations, and PLC programming, protocol analysis, and demonstration of cyber-attacks. The authors emphasized that the test bed provides a robust experimental environment with features like monitoring, recording, and showcasing different aspects of SCADA systems [11].

Kirshnan and Wei established a SCADA test bed environment, both hardware and software-based, for penetration testing, vulnerability analysis, and digital forensics. The test bed operates within a limited budget and supports laboratory-based activities. The authors also mentioned their plans to manage the test bed via a mobile application and conduct security testing [12].

Based on the literature reviews summarized above, it is evident that the cybersecurity of SCADA systems is highly important, and there is a widespread effort to develop test bed environments aimed at enhancing the security of these systems. Many of these test bed environments have been developed in physical settings and have been further advanced by the researchers involved. However, it is evaluated that preparing these environments using virtualization technology and an infrastructure that supports a wider range of industrial communication protocols would not only promote more researchers to work in this field but also provide a more flexible approach to easily incorporate new modules.

Therefore, it can be concluded that the development of test bed environments for SCADA security using open-source software and hardware, physical simulation setups, control systems, water tank emulations, and virtualization technology has gained significant attention. These test beds serve as crucial tools for research, analysis, and experimentation, enabling researchers to create attack scenarios, evaluate security measures, assess the effectiveness of defense mechanisms, and explore various aspects of SCADA systems. The continuous efforts in developing and improving these test bed environments contribute to advancing the field of SCADA security and strengthening the protection of critical infrastructure.

In this study, test bed centers developed to enhance the security of SCADA systems, as outlined in the literature, are examined, and the sectors to which these test beds are specifically developed are analyzed. Based on the analysis, it is observed that test bed centers designed through physical equipment tend to be localized for security research. To reach wider audiences and allow for future studies with different protocols and software, a test bed proposal capable of further development is suggested.

II. SCADA Systems and Components

A SCADA system monitors, tracks, and controls industrial processes as well as public infrastructure such as power, oil and gas, manufacturing, and transportation networks. In order to improve the performance of critical industrial system operations and provide better protection for the equipment used, a SCADA system collects and analyzes field data from industrial field devices in real-time for control and management [13].

A typical SCADA system consists of three main components: the Master Terminal Unit (MTU), which is defined as the central control station, the Remote Terminal Units (RTUs) defined as remote substation units, and the communication infrastructure that provides communication between these systems. The control center of SCADA is responsible for managing and supervising the overall system, storing process and system information, and in some cases, acting as a gateway between the resources in the enterprise network (operation network) and the industrial network, which supports commercial operations. Any interruption or disruption in the processes, due to the critical functions provided by the control center, can lead to serious consequences for the economy, public safety, and national security. Therefore, any external access or interface with other networks should be made secure and protected [14].

A SCADA system can be seen in different layers based on the connectivity of the various components with each other as well as with other networks such as the Internet. In Figure 2 that illustrates the infrastructure and layers of a typical SCADA system [15], layer 0 contains the individual field devices connected via a bus network. Layer 1 has controllers that receive input signals from the field devices and other controllers upon which they perform operations to steer the field devices by sending output signals to them. Layer 2 consists of the supervisory network, typically a local network connected to the lower layers for specific operations such as showing the current monitoring state at the HMI. Layer 3 is the operation DMZ, where historians, domain controllers, and application servers are located. Layers 4 and 5 correspond to the enterprise IT networks, in which the enterprise desktops and business servers operate. Most forensic analyses of SCADA systems involve layers 0-2, as they contain the components that control the underlying industrial processes. However, the analysis can extend to layers 3-5 if needed.

A. Master Terminal Unit (MTU)

MTU, or Master Terminal Unit, is a system that functions as a server receiving data from the RTU. The data received from the RTU is processed by the MTU and displayed in numerical and graphical form based on the collected data. The MTU operates in integration with the HMI (Human-Machine Interface) to facilitate data analysis. This provides a graphical interface that SCADA operators can easily understand. Through the MTU, communication and control of all equipment within the SCADA network can be monitored. Additionally, as mentioned before, the traffic related to SCADA communication can be viewed through a graphical interface provided by the HMI software. Moreover, commands can be sent to field equipment when necessary, and commands received from field equipment can be processed, while communication connections are monitored.

B. Remote Terminal Unit (RTU)

The Remote Terminal Unit (RTU) functions as the eyes, ears, and hands of the SCADA system. It collects data from field devices, processes the data, and acts as the eyes and ears of the Master Terminal Unit (MTU), transmitting signals to assist the main unit in evaluating the power system. When control commands are received from the MTU, they are sent to the devices through the RTU [16]. RTU devices are geographically distributed and send real-time data to the MTU via LAN or WAN connections. PLC (Programmable Logic Controller) devices are among the devices used within the scope of RTU.

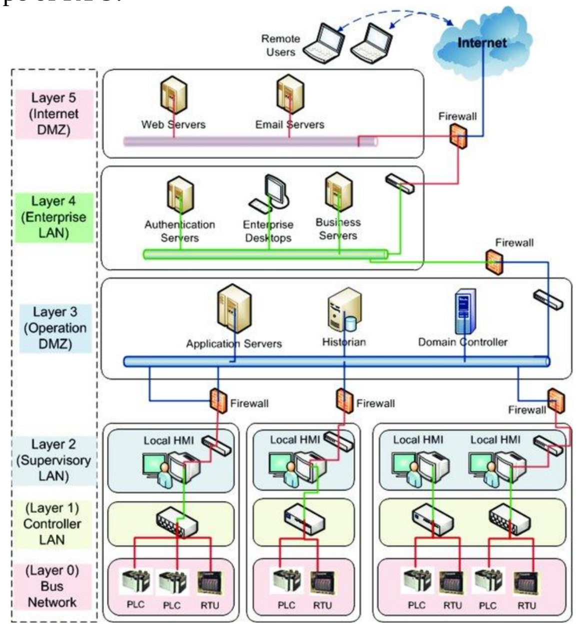


Fig. 1. Infrastructure and layers of a typical SCADA system [15]

C. *Communication Infrastructures*

Different types of communication protocols can be used in SCADA systems to facilitate communication between MTU, RTU, and field devices. With the advancements in information and communication technologies, the use of TCP/IP-based industrial communication protocols has become widespread, leading to increased adoption in SCADA networks. In the study conducted by Erkek and Irmak [17], the most commonly used industrial communication protocols in the industrial sector were queried using the Shodan search engine, and usage statistics were determined. Figure 2 presents the graphical representation of these usage statistics.

III. Importance of Test Beds for SCADA Systems

SCADA systems are real-time operating systems, and accessibility is a crucial requirement for these systems. However, they were originally designed to be relatively isolated from other networks and external access before the widely use of information technology in the SCADA domain and cloud-based SCADA applications, as well as the development of real-time business information systems [18]. Therefore, the industrial communication protocols used in the SCADA systems developed and deployed during this period were designed with a lesser focus on security. As a result, cybersecurity was not a significant concern for these systems in their early stages; rather, reliability, real-time performance, and accessibility were prioritized. However, with the technological trends and the emergence of real-time information sharing and analysis, the pathway for intercommunication between operational and enterprise networks with SCADA systems began to form. This interconnection allowed for more efficient remote control, management, and monitoring of industrial processes within the controlled system. While this integration brings advantages, it also introduces certain disadvantages. The security vulnerabilities that threaten information and communication technology systems have now become factors that directly threaten industrial systems.

Nowadays, SCADA systems and industrial control systems (ICSs) serve various critical infrastructure sectors such as electricity generation and distribution, water network control, natural gas distribution, traffic control, and more [19]. In ICSs, security tests can also be conducted, similar to traditional networks.

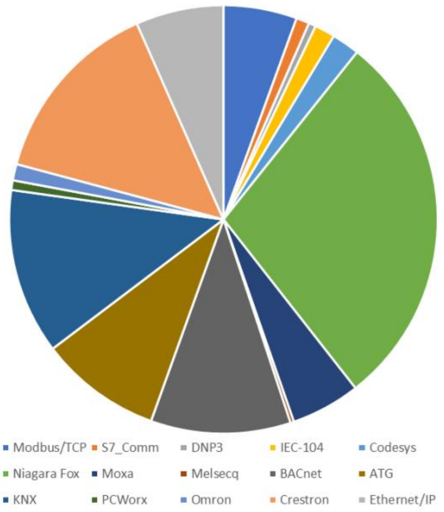


Fig. 2. Usage statistics of industrial communication protocols [17]

However, the continuous operation requirements of industrial facilities make it difficult, and in some cases impossible, to conduct research on real systems without interrupting their operation. The need for researchers to conduct their studies or test their products on a real ICS is increasing day by day. Therefore, test environments consisting of one-to-one models of the systems have been developed for analyzing these systems, which are continuously operational, non-stop, and do not allow any changes that could jeopardize the system. These test environments, called test beds, have been established in more than 30 countries to meet specific needs.

The purposes of test beds vary depending on the sector and objectives they serve. In a study conducted in 2015, it was found that 35% of test environments were established for vulnerability analysis, followed by 20% for training and 20% for testing defense mechanisms [20]. The distribution graph of these purposes is shown in Figure 3. In the same study, industrial communication protocols used in test beds were examined. It was observed that the most commonly used protocol was Modbus with 23%, followed by DNP3 with 21% and OPC with 9% [20]. The distribution graphs of the protocols used in test beds are shown in Figure 4.

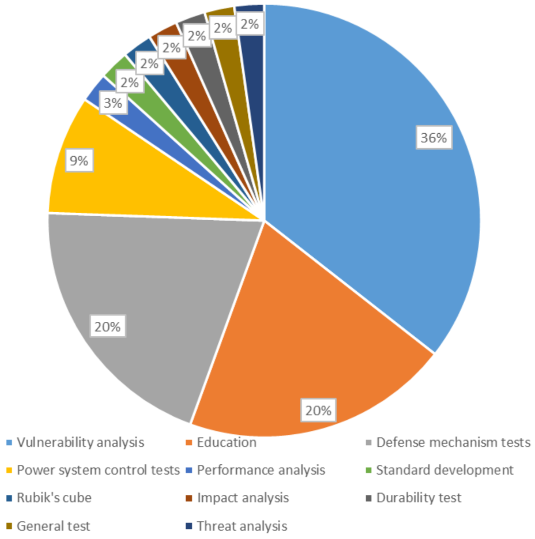


Fig. 3. Distribution of test bed studies according to their purposes [20]

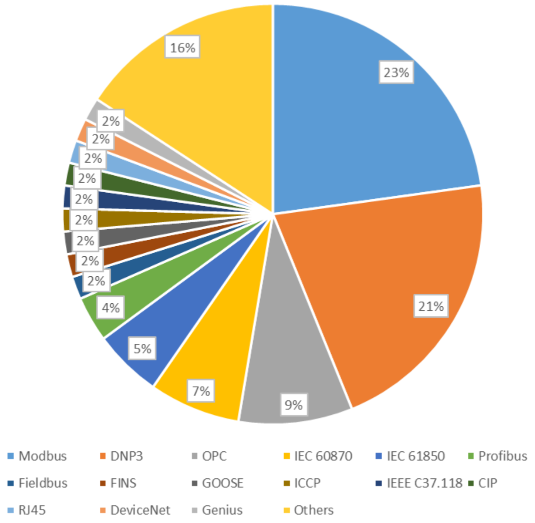


Fig. 4. Distribution of protocols used in test beds [20]

As summarized above, test bed studies have predominantly focused on physical systems, and it has been evaluated that the use of these systems in test beds limits the research activities of security researchers who focus on other aspects of ICS security. Additionally, although it has been observed that various industrial communication protocols are used in test bed environments, it has been found that some commonly used industrial communication protocols are not utilized in the industry. Therefore, it is recommended to establish a virtual test bed environment to contribute to the literature, cater to researchers working in this field, and provide opportunities for future developments. This would create an environment that allows for enhancing SCADA security, conducting vulnerability analysis, penetration testing, digital forensics examinations, artificial intelligence studies, and developing defense mechanisms.

IV. Design of a New Test Bed for SCADA Security

This study proposes the establishment of a test bed environment using virtualization technology as an alternative to the predominantly literature-based test beds that rely on physical equipment. By creating a virtualized test bed environment, it becomes possible to simulate SCADA systems applicable to various sectors and conduct essential security studies on these systems. Moreover, the utilization of virtualization technology allows for the creation of the test bed environment at significantly lower costs compared to physical systems. Furthermore, it provides the opportunity for ongoing improvement and development of projects using the employed software in future works.

As part of the study, the experimental setup developed to enhance the security of SCADA system components has been designed in a virtual environment, as mentioned before. The virtualization environment has been implemented using VmWare virtualization software, which enables the execution of the required operating systems for the test bed. Various types of simulation and emulator software will run on these operating systems. The proposed test bed will utilize software specified under the following headings.

A. *VMWare Virtualization Environment*

VMware is a virtual machine platform that allows the execution of an unmodified operating system as a user-level application [21]. The operating system running within VMware can be restarted, crashed, modified, and reinstalled without affecting the functionality of other applications running on the computer. Developed from operating system research at Stanford University, VMware serves as a virtual machine monitor, which acts as an additional software layer that virtualizes all hardware resources between the physical hardware and the operating system. Essentially, it creates a virtual execution environment known as a "virtual machine" (VM), enabling the simultaneous use of multiple VMs that are isolated from the real hardware and other activities of the underlying system. In this study, the Windows 7 operating system will be utilized as a virtual machine, with other components such as PLC programming, HMI, and communication modules operating on this virtualized system.

B. *Totally Integrated Automation (TIA) Portal*

TIA Portal serves as an engineering framework that enables the implementation of automation solutions across diverse industries worldwide. It offers engineers significant time, cost, and labor savings by encompassing the entire lifecycle of automation systems, from design and commissioning to operation and maintenance. Within TIA Portal, Siemens has developed SIMATIC STEP 7, a software specifically designed for configuring, programming, testing, and diagnosing all modular and PC-based SIMATIC controllers. It incorporates a range of user-friendly features [22]. In this study, the utilization of TIA Portal V13 and PLCSim V13, both developed by Siemens for PLC simulations, was undertaken.

C. *NetToPLCsim and EasyBuilder*

NetToPLCsim allows access to the network where the PLCSim application is running by utilizing the computer's network interface through TCP/IP (Iso-On-TCP) communication. It offers a convenient method for testing client applications (such as SCADA, HMI) in conjunction with S7-Plcsim, eliminating the need for an actual PLC [23].

EasyBuilder, developed by Weintek, is an HMI software that provides visualization capabilities to operators and can be utilized in various industries. In this study, the relevant HMI software was employed to observe changes in the configurations within TIA Portal by entering commands via the HMI [24].

D. *Design of Test Bed*

Within the scope of this study, a circuit is designed on the TIA Portal software installed on the Windows 7 operating system running on the VMware virtualization environment. The circuit includes two buttons, one in red and one in green. It is designed in such a way that pressing the green button turns on the lamp in the circuit, while pressing the red button turns off the lamp. The ladder logic diagram of the circuit in TIA Portal is shown in Figure 5.

For the PLC where the designed circuit program will be executed, the previously mentioned PLCSim simulator has been used. The screenshot of PLCSim is shown in Figure 6.

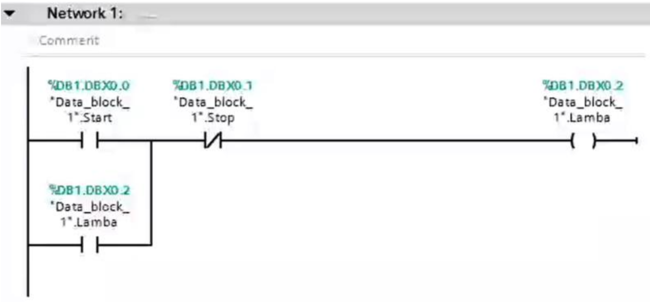


Fig. 5. The ladder diagram of the circuit used in the test bed in TIA portal

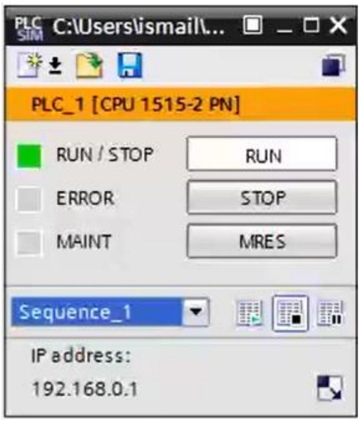
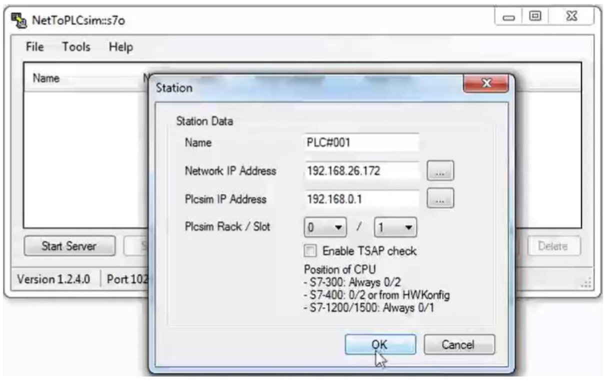


Fig. 6. Screenshot of the PLCSim simulator

PLCSim Simulator operates as a PLC in this experimental setup, and the circuit logic developed in TIA Portal runs on this simulator. However, industrial communication is required between TIA Portal and PLCSim. For this purpose, the previously mentioned NetToPLCsim communication emulator will be used. With this emulator, S7comm industrial communication will take place in the test bed environment. The NetToPLCsim emulator is shown in Figure 7. In order to provide an interface to the operator for this designed circuit in the test bed, an HMI design is created using the previously mentioned application called EasyBuilder. The operations performed on this designed HMI are capable of actively sending commands to the circuit in TIA Portal.



Station Data

Name: PLC#001

Network IP Address: 192.168.26.172

Plcsim IP Address: 192.168.0.1

Plcsim Rack / Slot: 0 / 1

□ Enable TSAP check

Position of CPU
- S7-300: Always 0/2
- S7-400: 0/2 or from HWKonfig
- S7-1200/1500: Always 0/1

Fig. 7. NetToPLCsim emulator

The HMI interface designed in this study is shown in Figure 8. It is considered highly beneficial for industrial communication protocols' security research to have this connection framework built on an industrial communication infrastructure. In the designed test bed, data transfer is performed using the S7comm industrial communication protocol, and Figure 9 displays the captured S7comm packets through Wireshark.

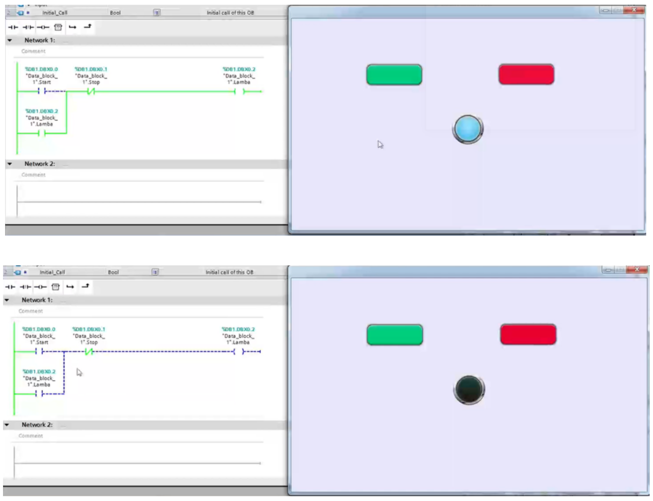
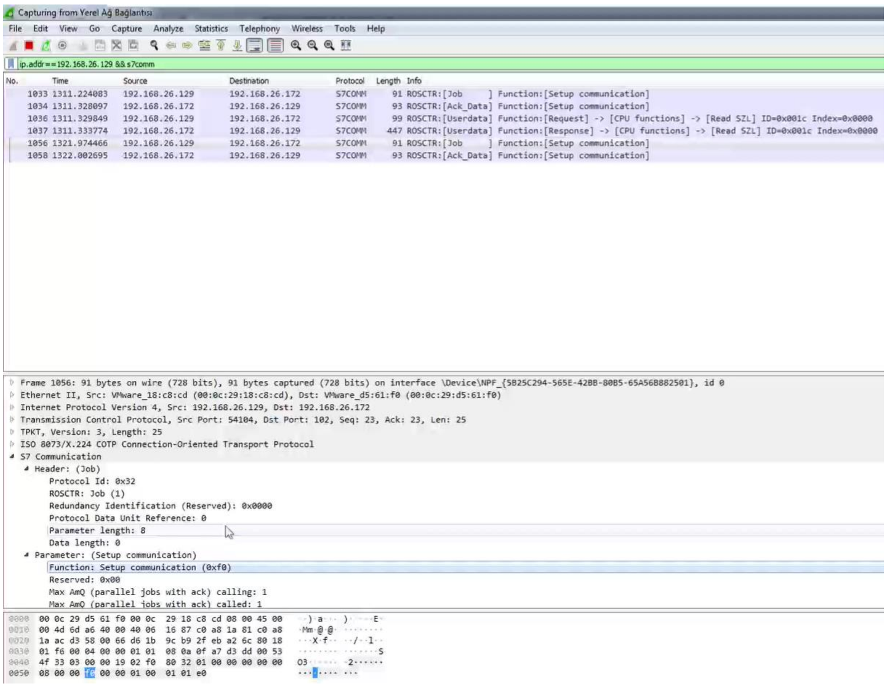


Fig. 8. TIA Portal and HMI views during the On and Off States of the lamp


Capturing from Yerel Ağ Bağlantısı
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==192.168.26.129 && s7comm

No.  Time         Source          Destination     Protocol Length Info
1033 1311.224083  192.168.26.129  192.168.26.172  S7COMM      91 ROSCTR:[Job     ] Function:[Setup communication]
1034 1311.328097  192.168.26.172  192.168.26.129  S7COMM      93 ROSCTR:[Ack_Data] Function:[Setup communication]
1036 1311.329849  192.168.26.129  192.168.26.172  S7COMM      99 ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL] ID=0x001c Index=0x0000
1037 1311.333774  192.168.26.172  192.168.26.129  S7COMM     447 ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x001c Index=0x0000
1056 1321.974466  192.168.26.129  192.168.26.172  S7COMM      91 ROSCTR:[Job     ] Function:[Setup communication]
1058 1322.002695  192.168.26.172  192.168.26.129  S7COMM      93 ROSCTR:[Ack_Data] Function:[Setup communication]

Frame 1056: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{5B25C294-565E-42BB-80B5-65A56B882501}, id 0
Ethernet II, Src: VMware_18:c8:cd (00:0c:29:18:c8:cd), Dst: VMware_d5:61:f0 (00:0c:29:d5:61:f0)
Internet Protocol Version 4, Src: 192.168.26.129, Dst: 192.168.26.172
Transmission Control Protocol, Src Port: 54104, Dst Port: 102, Seq: 23, Ack: 23, Len: 25
TPKT, Version: 3, Length: 25
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
S7 Communication
  Header: (Job)
    Protocol Id: 0x32
    ROSCTR: Job (1)
    Redundancy Identification (Reserved): 0x0000
    Protocol Data Unit Reference: 0
    Parameter length: 8
    Data length: 0
  Parameter: (Setup communication)
    Function: Setup communication (0xf0)
    Reserved: 0x00
    Max AmQ (parallel jobs with ack) calling: 1
    Max AmQ (parallel jobs with ack) called: 1

0000  00 0c 29 d5 61 f0 00 0c  29 18 c8 cd 08 00 45 00   ··)·a···)·····E·
0010  00 4d 6d a6 40 00 40 06  16 87 c0 a8 1a 81 c0 a8   ·Mm·@·@·········
0020  1a ac d3 58 00 66 d6 1b  9c b9 2f eb a2 6c 80 18   ···X·f····/··l··
0030  01 f6 00 04 00 00 01 01  08 0a 0f a7 d3 dd 00 53   ···············S
0040  4f 33 03 00 00 19 02 f0  80 32 01 00 00 00 00 00   O3·······2······
0050  08 00 00 f0 00 00 01 00  01 01 e0                  ···········
```

Fig. 9. S7comm packets captured in the test bed

V. Implementation of the Attack Scenario

Data manipulation is a potential attack vector that can be executed against SCADA systems and, if successful, can have severe consequences. The vulnerability arises from the lack of emphasis on security during the development of industrial communication protocols, where the focus is often on fast transmission rather than secure transmission of data. Consequently, data transmitted through these protocols can be easily manipulated. This allows malicious users to intervene in unauthorized traffic and manipulate data according to their own objectives. In this study, data manipulation was performed within the designed test bed setup. The S7comm communication protocol, which is extensively used in the test bed infrastructure, was thoroughly examined, and the function codes employed in this protocol were analyzed. By utilizing the snap7 library in Python, the flowing data through this protocol was scrutinized, and manipulation operations were carried out. The data manipulation process is depicted in Figure 10.

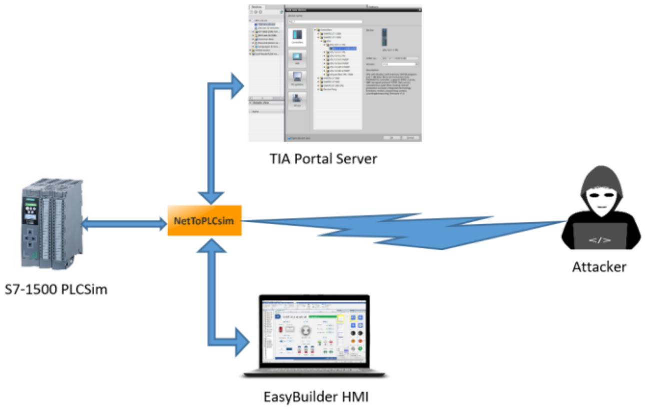


Fig. 10. The data manipulation process

During the data manipulation process carried out in the developed test bed environment, as mentioned earlier, manipulative operations were performed on the S7comm industrial communication protocol using the snap7 library. These operations utilized the S7comm function codes, allowing unauthorized reading and modification of data within the PLC memory blocks. As a result of these operations, unauthorized remote control of the lamp in the test bed environment was achieved, enabling unauthorized on/off operations.

VI. Conclusion and Evaluation

In this study, efforts to enhance the cybersecurity and resilience of critical infrastructure systems that have the potential to impact societal welfare, national economy, national security, and even human life have been examined. It has been evaluated that the practical studies on the security of industrial control systems are necessary to acquire and enhance these capabilities, and practical experience is best gained through practical applications. However, considering that the relevant systems operate in real-time and can pose significant financial losses and even endanger human life in the event of a functional failure, conducting security research on operational systems is deemed to carry significant risks. Therefore, the focus of this work has been on establishing test bed environments for security research on SCADA systems and conducting necessary security investigations within these environments.

In the scope of the study, it has been evaluated that a significant portion of test bed studies in the literature are designed on physical simulation environments, requiring substantial financial investments. Additionally, the location-specific nature of physical simulation environments makes it difficult for different security researchers to contribute to relevant studies. This situation hinders the progress of vulnerability analysis, penetration testing, digital forensics, and artificial intelligence studies related to SCADA security. Therefore, it has been assessed that test bed environments designed using open-source software would appeal to a larger number of researchers and increase the volume of research conducted in this field.

The literature review has revealed the use of various industrial communication protocols in test bed communication infrastructures. Widely used protocols in the industry such as Modbus, DNP3, and OPC are employed in the communication infrastructure of test beds. In this study, however, the S7comm protocol, predominantly used in the industrial communication infrastructure of Siemens devices, was utilized. The packet structure of the S7comm protocol was examined and analyzed in the test bed. Due to the flexibility of the simulation environment, different types of industrial communication protocols can be executed and tested in the test bed for analysis.

In the developed test bed, an attack scenario was implemented to contribute to vulnerability scanning and security research on industrial communication protocols. Within the scenario, a Python code was written using the snap7 library to unauthorizedly read and modify SCADA data remotely in the test bed environment. It was observed that unauthorized open/close operations could be performed on the lamp in the test bed using this code.

In conclusion, critical infrastructure systems that, when they lose functionality, get damaged, experience data breaches, or become subject to manipulation operations, can disrupt societal order, human life, economic losses, and national or global security. Therefore, it is crucial to establish and design these systems with a security-conscious approach. The establishment and development of test beds are seen as an important element for ensuring the security of these systems and for national security. In this regard, this study has presented a test bed environment that can be integrated into different sectors, has a wide impact area with low cost, and can appeal to a broad audience. Through this test bed, various studies aiming to enhance cybersecurity, such as vulnerability analysis, penetration testing, digital forensics, and machine learning, can be conducted. Thus, it is believed that this work will contribute to the security of SCADA systems, which are critical infrastructure components.

References

[1] ‘Commission of the European Communities: Critical Infrastructure Protection in the Fight against Terrorism’. Accessed: May 23, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702

[2] Republic of Turkey Ministry of Transport and Infrastructure, ‘National Cyber Security Strategy and 2013-2014 Action Plan’, Accessed: May 23, 2023. [Online]. Available: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf

[3] F. Sauer, M. Niedermaier, S. Kießling, and D. Merli, ‘LICSTER – A Low-cost ICS Security Testbed for Education and Research’, presented at the 6th International Symposium for ICS & SCADA Cyber Security Research 2019, BCS Learning & Development, Sep. 2019. doi: 10.14236/ewic/icscsr19.1.

[4] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, ‘SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach’, *Future Internet*, vol. 10, no. 8, Art. no. 8, Aug. 2018, doi: 10.3390/fi10080076.

[5] İ. Özçelİk, M. İskefiyeli, M. Balta, K. O. Akpinar, and F. S. Toker, ‘CENTER Water: A Secure Testbed Infrastructure Proposal for Waste and Potable Water Management’, in *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2021, pp. 1–7. doi: 10.1109/ISDFS52919.2021.9486364.

[6] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddi, ‘A control system testbed to validate critical infrastructure protection concepts’, *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 88–103, Aug. 2011, doi: 10.1016/j.ijcip.2011.06.005.

[7] E. Irmak, İ. Erkek, and M. M. Özçelik, ‘Experimental Analysis of the Internal Attacks on Scada Systems’, *Gazi University Journal of Science*, vol. 30, no. 4, Art. no. 4, Dec. 2017.

[8] A. Almalawi, Z. Tari, I. Khalil, and A. Fahad, ‘SCADAVT-A framework for SCADA security testbed based on virtualization technology’, in *38th Annual IEEE Conference on Local Computer Networks*, Oct. 2013, pp. 639–646. doi: 10.1109/LCN.2013.6761301.

[9] A. P. Mathur and N. O. Tippenhauer, ‘SWaT: a water treatment testbed for research and training on ICS security’, in *2016 International*

Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), Apr. 2016, pp. 31–36. doi: 10.1109/CySWater.2016.7469060.

[10] V. S. Koganti, M. Ashrafuzzaman, A. A. Jillepalli, and F. T. Sheldon, ‘A virtual testbed for security management of industrial control systems’, in *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*, Oct. 2017, pp. 85–90. doi: 10.1109/MALWARE.2017.8323960.

[11] I. Ahmed, V. Roussev, W. Johnson, S. Senthivel, and S. Sudhakaran, ‘A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy’, in *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, in ICSS ’16. New York, NY, USA: Association for Computing Machinery, December 2016, pp. 1–9. doi: 10.1145/3018981.3018984.

[12] S. Krishnan and M. Wei, ‘SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics’, in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2019, pp. 1–6. doi: 10.1109/ISDFS.2019.8757543.

[13] A. Stefanov, C.-C. Liu, M. Govindarasu, and S.-S. Wu, ‘SCADA modeling for performance and vulnerability assessment of integrated cyber–physical systems’, *International Transactions on Electrical Energy Systems*, vol. 25, no. 3, pp. 498–519, 2015, doi: 10.1002/etep.1862.

[14] S. Nazir, S. Patel, and D. Patel, ‘Assessing and augmenting SCADA cyber security: A survey of techniques’, *Computers & Security*, vol. 70, pp. 436–454, Sep. 2017, doi: 10.1016/j.cose.2017.06.010.

[15] I. Ahmed, S. Obermeier, M. Naedele, and G. G. Richard III, ‘SCADA Systems: Challenges for Forensic Investigators’, *Computer*, vol. 45, no. 12, pp. 44–51, Dec. 2012, doi: 10.1109/MC.2012.325.

[16] J. E. U. Cabus, İ. Bütün, and R. Lagerström, ‘Security Considerations for Remote Terminal Units’, in *2022 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC)*, May 2022, pp. 47–52. doi: 10.1109/ZINC55034.2022.9840542.

[17] I. Erkek and E. Irmak, ‘Cyber Security of Internet Connected ICS/SCADA Devices and Services’, in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, Dec. 2021, pp. 75–80. doi: 10.1109/ISCTURKEY53027.2021.9654285.

[18] U. P. D. Ani, H. (Mary) He, and A. Tiwari, ‘Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective’, *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 32–74, Jan. 2017, doi: 10.1080/23742917.2016.1252211.

[19] R. White, ‘Risk Analysis for Critical Infrastructure Protection’, in *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, D. Gritzalis, M. Theocharidou, and G. Stergiopoulos, Eds., in Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2019, pp. 35–54. doi: 10.1007/978-3-030-00024-0_3.

[20] H. Holm, M. Karresand, A. Vidström, and E. Westring, ‘A Survey of Industrial Control System Testbeds’, in *Secure IT Systems*, S. Buchegger and M. Dam, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2015, pp. 11–26. doi: 10.1007/978-3-319-26502-5_2.

[21] ‘Introducing VMware Cross-Cloud Services’, *VMware*. https://www.vmware.com/content/vmware/vmware-published-sites/us (accessed May 23, 2023).

[22] ‘TIA Portal’, *siemens.com Global Website*. https://www.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal.html (accessed May 23, 2023).

[23] ‘NetToPLCsim - Network extension for Plcsim’. https://nettoplcsim.sourceforge.net/ (accessed May 23, 2023).

[24] ‘EasyBuilder Pro’, *Weintek Türkiye*. http://weintek.com.tr/easybuilderpro/ (accessed May 23, 2023).