MSICST: Multiple-Scenario Industrial Control System Testbed for Security Research

Wei Xu[1, 2], Yaodong Tao[2, 3], Chunfang Yang[4, *] and Huiqin Chen[5]

Abstract: A security testbed is an important aspect of Industrial Control System (ICS) security research. However, existing testbeds still have many problems in that they cannot fully simulate enterprise networks and ICS attacks. This paper presents a Multiple-Scenario Industrial Control System Testbed (MSICST), a hardware-in-the-loop ICS testbed for security research. The testbed contains four typical process scenarios: thermal power plant, rail transit, smart grid, and intelligent manufacturing. We use a combination of actual physical equipment and software simulations to build the process scenario sand table and use real hardware and software to build the control systems, demilitarized zone, and enterprise zone networks. According to the ICS cyber kill chain, the attacker is modeled, and two typical attack scenarios are constructed in the testbed. Through research into this security solution, whitelist-based host protection and a new Intrusion Detection System (IDS) are proposed and tested.

Keywords: Industrial control system, security testbed, simulation, attack, network.

1 Introduction

Industrial Control Systems (ICSs) are employed in numerous critical infrastructure assets including power generation, transmission and distribution, transportation, oil and gas, and chemical production. Information and Communication Technologies (ICT) have been widely adopted in modern ICSs. Many ICSs and devices are connected to the Internet [Andreeva, Gordeychik, Gritsai et al. (2016)] and show an increasing trend year over year [Xu, Tao and Guan (2018)]. Because ICSs are different from traditional IT systems [Stouffer, Falco and Scarfone (2011)], traditional security solutions cannot completely solve ICS security problems [Weiss (2008)]. In addition, ICSs control the actual physical process. Thus, cyberattacks will cause serious consequences. For example, Stuxnet was injected into the Natanz nuclear facilities in Iran in 2010, destroyed more than 1,000 centrifuges [Albright, Brannan and Walrond (2010); Kushner (2013)]. Hackers compromised information systems of three power distribution companies in Ukraine in

[1] University of Science and Technology of China, Hefei, Anhui, 230026, China.

[2] National Joint Engineering Lab for ICS Security of 360ESG, Beijing, 100000, China.

[3] Shenyang Institute of Computing Technology of CAS, Shenyang, Liaoning, 110168, China.

[4] Zhengzhou Science and Technology Institute, Zhengzhou, Henan, 450001, China.

[5] University of Michigan Transportation Research Institute, USA.

[*] Corresponding Author: Chunfang Yang. Email: chunfangyang@126.com.

CMC. doi:10.32604/cmc.2019.05678

December 2015, and about 230,000 people were left without electricity for 1 h to 6 h [Liang, Weller, Zhao et al. (2017)]. The WannaCry ransomware that broke out in 2017 also infected control networks of some enterprises, causing serious losses [Lee (2018); Nick, Jenny and Stu (2017)]. The cybersecurity of ICSs has received increased attention from industry and research communities.

The primary objective of an ICS security testbed is to discover ICS vulnerabilities and to study and evaluate cybersecurity implementation. This has become a hot topic in ICS security research [McLaughlin, Konstantinou, Wang et al. (2016)]. Researchers have built several ICS testbeds, which were used for ICS attack simulations, ICS vulnerability detection, education and training, research, and verification of security solutions [Holm, Karresand, Vidstrom et al. (2015)]. However, few of these testbeds simulated a complete enterprise network or realistically simulated the complete ICS attack process.

This paper introduces the Multiple-Scenario Industrial Control System testbed (MSICST) for security research. In Section 2, we introduce related works on ICS security testbeds. The architecture and construction process of the MSICST testbed, detailing the four process scenarios and other parts of the testbed, are introduced in Section 3. Security experiments conducted on the MSICST testbed, including vulnerability discovery, attack scenario simulations, and security solution research, are introduced in Section 4. Finally, a brief summary and future work plan are given.

2 Related works

Smart-grid SCADA (Supervisory Control and Data Acquisition) testbeds have always been a research hot spot [NIST (2014)]. Different research institutions have developed many smart grid testbeds, among which the National SCADA Test Bed (NSTB) in the United States is the most representative. NSTB is a large-scale electric power grid testbed built by the Idaho National Labs with funding from the US Department of Energy. NSTB uses actual physical grid components and commercially available hardware and software to build a grid control system that includes 61 miles of 128-kV transmission lines and 13.8-kV distribution lines, 7 substations, and more than 3,000 monitoring and control points. NSTB includes a variety of wireless and wired communication standards and protocols including TCP/IP, ATM, 802.11, GSM, ICCP, Modbus, DNP3, and more. It can be used to control system cybersecurity assessments, standard developments, outreach and training, etc. [DoE (2018); Morris, Srivastava, Reaves et al. (2011)]

The National Institute of Standards and Technology developed a cybersecurity testbed for industrial control systems. The testbed constructs three process scenarios: a chemical process manufacturing scenario based on the Tennessee Eastman model [Downs and Vogel (1993)], a robotic collaborative assembly scenario, and a wide-area-network SCADA scenario. Common ICS attacks such as Denial of Service (DoS), replay attack, and Man-In-The-Middle (MITM) attack are simulated on the testbed, and the performance of the control system after being attacked and deploying cybersecurity products is measured [Candell, Zimmerman and Stouffer (2015); Candell, Stouffer and Anand (2014)].

Researchers at the Joint Research Centre of the European Commission built an experimental platform based on the control system of a typical turbo-gas power plant. The experimental platform has been used to study the effects of some ICT attacks against control systems, including SCADA system phishing, Domain Name System (DNS) poisoning, DoS worms, and Modbus/DNP3 worms. Countermeasures such as secure ICS protocols and an Intrusion Detection System (IDS) for control systems were proposed and tested [Fovino, Masera, Guidi et al. (2010)].

Researchers at Mississippi State University built a testbed that includes real hardware and software as well as real-world physical processes for pedagogy and cybersecurity research. The testbed consists of seven actual physical processes and their control systems, including a water storage tank, raised water tower, factory conveyor belt, gas pipeline, industrial blower, steel rolling operation, and a smart grid transmission control system. The researchers used the testbed for Human Machine Interface (HMI) vulnerability discovery, developed a serial Modbus and DNP3 data logger, and developed and tested a statistical IDS [Morris, Srivastava, Reaves et al. (2011)].

The Lancaster ICS testbed, based on a Hardware-In-the-Loop (HIL) concept, constructs a complete enterprise network that consists of six manufacturing zones, an ICS demilitarized zone, and an enterprise zone. The researchers conducted cybersecurity studies and experiments on this testbed [Green, Lee, Antrobus et al. (2017); Green, Paske, Hutchison et al. (2014)].

The Singapore University of Technology and Design developed the Security Water Treatment testbed, which has a real water treatment capacity of 5 gallons per hour. Three attacker models with different permissions were constructed in the testbed. Attack experiments such as system reconnaissance and compromise through wireless networks were carried out, and the impacts of these attacks on the physical processes were studied [Mathur and Tippenhauer (2016)].

Many testbeds model control systems and their associated networks using various simulation technologies rather than actual physical equipment. These are called software-only testbeds [Holm, Karresand, Vidstrom et al. (2015)]. Graphical Realism Framework for Industrial Control Simulations is a free open-source and software-only ICS network testbed developed through simulation technology. It includes a virtual HMI in the control room, a virtual Programmable Logic Controller (PLC) controlling the plant, and a simulation of the physical process itself using the popular Unify 3D game engine [Formby, Rad and Beyah (2018)].

3 Construction of MSICST testbed

Fig. 1 shows the logical network architecture of the testbed based on the Purdue Enterprise Reference Architecture, which includes an enterprise zone, Demilitarized Zone (DMZ), and control zone [Williams (1994); Bodungen, Singer, Shbeeb et al. (2016)]. Four industrial process scenarios are constructed in the control zone, including a thermal power plant scenario, rail transit scenario, smart grid scenario, and smart manufacturing scenario. In each process scenario, the actual physical process is simulated by a sand table, the control system is constructed with commercially available hardware and software, and in some scenarios, a combination of software simulations and actual physical equipment is used to build a more real and comprehensive process behavior. We also built an attacker model and an observer and monitoring network in the testbed. The attacker model can be used for attack experiments. The observer and management network is used to manage the entire testbed and to record and analyze network traffic and to log data.

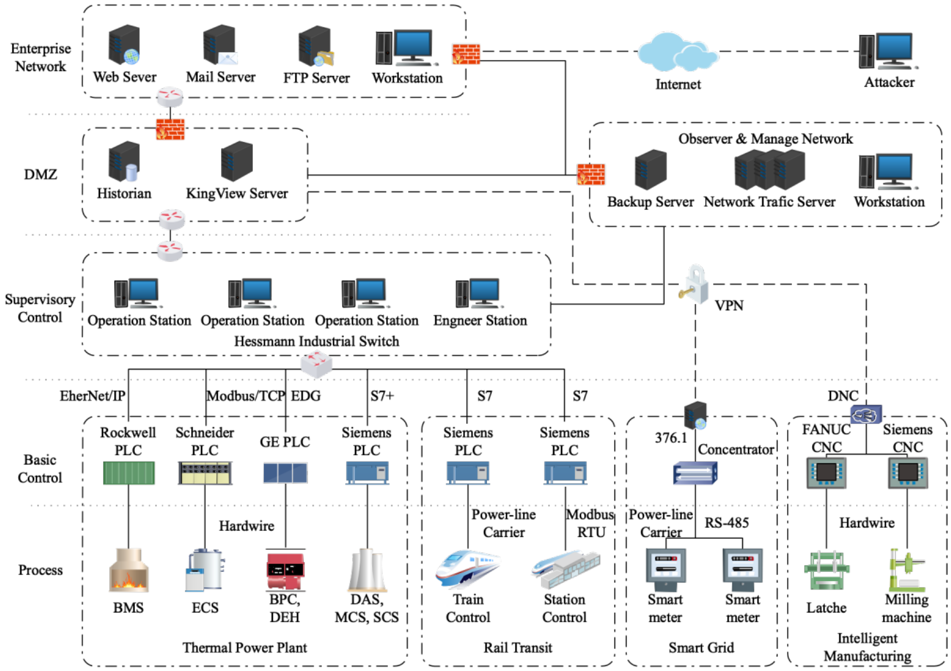

Figure 1: High-level network logical architecture diagram of MSICST testbed

3.1 Four process scenarios of control zone

3.1.1 Thermal power plant scenario

The basic principle of a thermal power plant is to generate electricity from fossil fuels. Fossil fuel burns water in a boiler to generate steam, and the steam drives the steam turbine to rotate, the steam turbine drives the generator, and the generator generates electric energy by cutting the magnetic field lines.

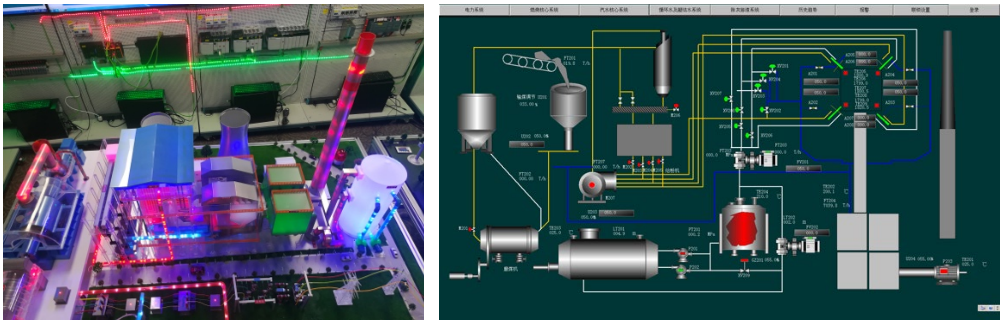

Figure 2: Photo of sand table (left) and one HMI page screenshot (right, HMI of combustion system) of thermal power plant scenario

We simulate the process of a thermal power plant through a sand table, which combines software simulations and actual physical equipment. As shown on the left of Fig. 2, we made a sand table to simulate the physical process of a thermal power plant, including three systems: combustion system, steam-water system, and electrical system. There is also a simulation software running synchronously with the sand table. The software implements the user interface through Flash, processes the simulation of the thermal power plant through C#, and connects to the physical PLCs of the control system through external Input and Output (IO) interface hardware. The combustion system includes coal handling, coal grinding, combustion, air supply, air introduction, dust removal, desulphurization, and smoke exhaustion. The steam-water system includes a superheater, steam drum, high-pressure steam, steam turbine, cooling tower, deaeration, pressurization, and heating. The power system includes generators, transformers, high-voltage switches, and standby generators.

Coal conveyor motors and conveyor belts, coal grinding motors, boiler fans, turbines and generator motors, and boiler internal temperature sensors are used the actual physical equipment. The air heater simulates the combustion process, and the boiler fan blows strips to simulate flame. Water, steam, smoke, and electric current are simulated by Light Emitting Diode (LED) lamp belts and smoke generators.

The control system is basically consistent with the monitoring and management system of a real power plant, including a Data Acquisition System (DAS), Modulation Control System (MCS), Burner Management System (BMS), Sequential Control System (SCS), Electrical Control System (ECS), Turbine Bypass Control System (BPC), and Digital Electronic Hydraulic control system (DEH).

Table 1: Controller information in thermal power plant scenario

Vendor	Brand and Model	Monitoring and Control Points	Controlled System
Siemens	Simatic S7-1200	64	DAS, MCS and SCS
Rockwell	Controllogix 1756	32	BMS
GE	Versamax	32	BPC and DEH
Schneider	Quantum	24	ECS
Total		152	

As shown in Tab. 1, DAS, MCS, and SCS adopt a set of control systems (Siemens-S7-1200), BMS adopts an independent set of control systems (Rockwell-Controllogix 1756), ECS uses an independent set of control systems (Schneider Quantum), and BPC and DEH adopt a set of control systems (GE VersaMax). There are 152 monitoring and control points in this scenario.

Referring to the HMI of a real thermal power plant, we use KingView to implement the HMI of the thermal power plant scenario, which consists of five monitoring pages to monitor and control the operation of the plant from different angles. The right side of Fig. 2 shows a page of the HMI of the thermal power plant scenario.

Similar to WinCC, KingView is an integrated system that consists of standard industrial computer software and hardware platforms. It has the advantages of strong adaptability, good openness, easy expansion, economy, and a short development cycle.

3.1.2 Rail transit scenario

We made a rail transit simulation sand table, which was simplified and based on a subway line in a Chinese city. The sand table includes three stations, circular rail transit lines, and two trains. There are two operating stations and one maintenance station in the three stations. The operating stations have shielded doors, elevators, air conditioners, gates, firefighting capability, and other facilities. The two trains are equipped with variable frequency motors that can run and stop on the track under the control system, and can communicate with the control system through the power carrier. Signal equipment such as traffic lights is placed on the track. The sand table is basically the same as a real rail transit system, but the scale is reduced. The gates, shield doors, elevators, and so on can also be driven by the motors, and they are also equipped with manual control switches. The left side of Fig. 3 is a photo of the rail transit sand table.

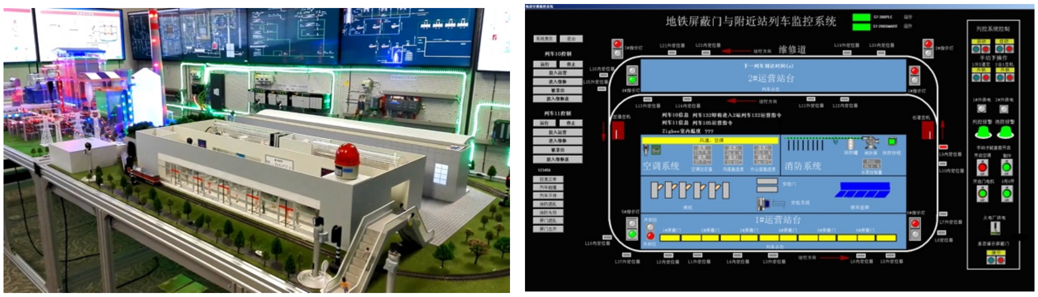

Figure 3: Photo of sand table (left) and HMI screen (right) of rail transit scenario

The difference is that the train uses 24 V of low voltage instead of high voltage, 18 Hall sensors on the track, and magnets installed on the train to locate the train instead of Global Positioning System (GPS). In addition, the air conditioner only uses the water flow to simulate the switch effect without real effect.

Table 2: Controller information in rail transit scenario

Vendor	Brand and Model	Monitoring and Control Points	Controlled Systems
Siemens	Simatic S7-300	62	Station Systems
Siemens	Simatic S7-200SMART	28	Track and Train System
Total		90	

In order to achieve automatic control of the trains and station operation, we use two PLCs for control. As shown in Tab. 2, a Siemens S7-300 is used to control the relevant systems of the station, including the power supply system, elevator motor control, entrance and exit gate control, ventilation and air conditioning control, signal light control, arrival information display, and shielded door control. The PLC communicates with the field equipment through a Modbus RTU. A Siemens S7-200SMART is used to control the track positioning module, track signal, turnout motor, train speed, train positioning, train anti-collision, and communication between the trains and stations. The PLC and trains communicate through a power line carrier. There are 90 monitoring and control points in this scenario.

As shown on the right of Fig. 3, the HMI of an entire platform is implemented in KingView, which communicates with two PLCs using the S7 communication protocol. It can monitor the running status of the trains and stations in real time, and can manually and automatically control the stations and trains.

3.1.3 Smart grid scenario

The power grid is the infrastructure of power transmission, and it is an economical and fast way to transfer energy. Owing to the large number of sites, wide geographical distribution, and diverse communication methods, the control system of the smart grid is a typical SCADA system. The power grid is also a research hot spot for ICS security testbeds. The protocols, devices, and physical processes used by the power grid have great specialties, and the grid enterprises are relatively concentrated. In order to truly simulate the characteristics of the Chinese power grid, we developed a grid testbed scenario in cooperation with the research institute affiliated with the State Grid Corporation of China.

Table 3: Device information for smart grid scenario

Vendor	Brand and Model	Type
Wisdom	FKCA23-DF6203	Smart Meter
Sanxing	DTZY188-G	Smart Meter
Hexing	DJGZ23-HX3200	Concentrator

The power physical process is divided into power generation, power transmission, power substation, power distribution, power utilization, and power dispatch. The testbed scenario we implemented mainly concentrates on the power consumption part. A SCADA system constructed with smart meters, concentrators, and a main station device can display the power consumption of an area in a centralized manner through the Web, and can remotely read the meter and remotely switch off the power.

We selected several devices that are widely used in China. We used two models of smart meter: Wisdom FKCA23-DF6203 and Sanxing DTZY188-G. The concentrator was a Hexing DJGZ23-HX3200. Tab. 3 presents detailed device information. The main station device stores data and has a web server function, and the user can access the terminating device through the browser for remote operation.

3.1.4 Intelligent manufacturing scenario

Computer numerical control (CNC) is the basis of intelligent manufacturing. It consists of many components that can independently complete digital control. It generally contains a controller, memory, and HMI. The operating status can be viewed through the HMI screen, and the parameters can be adjusted via the HMI button. However, a traditional CNC system does not connect to an external network, and it needs to obtain the running record data through a USB flash disk, SD card, etc. The operators cannot adjust parameters remotely via the network. In order to improve the intelligence level of the manufacturing industry and realize the collaborative manufacturing of multiple machines, the Distributed Numerical Control (DNC) system was developed. The DNC system consists of a DNC server and several controlled CNCs. The DNC server can acquire the status of each CNC in real time through the network, and can remotely adjust the parameters of each CNC in real time to realize the collaborative manufacturing of multiple CNCs.

Table 4: Device information in intelligent manufacturing scenario

Vendor	Brand and Model	Controlled System	Type
Siemens	808d	Milling Machine	CNC Controllers
FANUC	0i-TF	Lathe	CNC Controllers
Integ-Foever	Integ-DNC		DNC Server

We established an intelligent manufacturing test platform in cooperation with the research institutes of China Aerospace Science and Technology Corporation (CASC). The intelligent manufacturing testbed was built using real equipment, including two machine tools, two CNC controllers, and a DNC server. As shown in Tab. 4, the CNC controllers are a Siemens 808d CNC controller and a FANUC 0i-TF CNC controller, which are widely used in the market. The FANUC CNC controller has a built-in communication module and uses the Focus communication protocol developed jointly by GE and FANUC corporation. The Siemens CNC controller does not have a built-in communication module. We added a Moxa expansion card to communicate with an external network through the Modbus protocol. The Siemens CNC controls a milling machine, and the FANUC CNC controls a lathe to simulate two typical process scenarios of the CNC. According to a suggestion from our partner, we adopted the Integ-DNC networking system of Integ-Foever as the DNC server. The testbed was deployed in our partner's lab, and we can access this testbed scenario via VPN for security research.

3.2 Demilitarized zone

Although most industrial control systems adopt some measures to achieve isolation from external networks, they usually achieve weak separation through a DMZ, which also provides an attack path for cyberattacks [Fovino, Masera, Guidi et al. (2010)]. We also used this method in the testbed to establish a DMZ in which data historians and the KingView server were deployed. The KingView server can collect and display the status of each process scenario in a unified way. The KingView server and data historian are deployed on the Windows Server 2008 operating system. The enterprise zone network can access the DMZ, and the DMZ can access the control zone network. However, the enterprise zone network cannot directly access the control zone network, and a weak separation is achieved in this way. This separation is implemented by specific rules of the iptalbes firewall.

3.3 Enterprise zone

In the enterprise zone, we simulate the deployment of office networks in normal enterprises, including Web servers, mail servers, and office workstations. Owing to cost considerations, we did not deploy information systems such as Enterprise Resource Planning or the Management Information System, which are commonly deployed by enterprises.

As shown in Tab. 5, the office workstation adopts a Commercial Off-The-shelf (COT) software and hardware configuration, uses the common Windows 7 operating system, runs common office software such as the Microsoft Office series software, and is connected to the Internet.

Table 5: Some workstations and servers in testbed

Position	Software	Operating System
DMZ	KingView	Windows Server 2008
Enterprise Zone	Microsoft Office	Windows 7

3.4 Other parts of MSICST testbed

3.4.1 Attacker model

A cyberattack against an ICS is very different from the traditional IT network attack. According to the ICS cyber kill chain model [Assante and Lee (2015)], the attack process is divided into two stages. The first stage is the same as the IT cyber kill chain [Martin (2013)], and the second stage attacks the ICS in order to destroy the physical process. The existing ICS testbed mainly studies some attacks in the second stage and cannot simulate the complete ICS cyber kill chain. We want to simulate the complete ICS network kill chain process in the testbed, starting from attacking the enterprise zone network, and going step by step to achieve the purpose of destroying the physical process. We build an attacker model in which the attacker connects to the Internet, does not physically touch the enterprise network, and cannot access the enterprise network. If the attacker wants to attack the ICS system, he first must enter the enterprise zone network through penetration attacks. There is no additional authority after entering the enterprise zone network. It is necessary to further penetrate the DMZ to enter the control zone network step by step and ultimately achieve the purpose of destroying the physical process. This attack process not only conforms to the ICS cyber kill chain model but is also a common process of multiple ICS cybersecurity events, so it is more realistic.

3.4.2 Observe and manage network

We deploy a monitoring network in the testbed that mirrors the network traffic through the Switched Port Analyzer (SPAN) port of the switches and the routers, and stores the traffic data centrally. By monitoring and analyzing the traffic, we can get a deeper understanding of the characteristics and details of the attack, and develop IDS specially for ICS systems on this basis. In addition, the system logs of the operator stations, engineer stations, firewalls, and network devices can be uploaded to the monitoring server though syslog protocol, which provides a basis for subsequent association analyses.

In the management network, a system backup server and software warehouse server are deployed. The virtual desktop server is realized by VMware Horizon View, and the virtual machine is connected remotely by a thin client, which can be quickly recovered after an attack and provide reconfigurable architectures. In addition, the combination of virtualization and a thin client improves the flexibility and replicability of the testbed.

4 Experiment on MSICST testbed

4.1 Vulnerability discovery

First, we verified the known vulnerabilities of the software and hardware in the testbed. We took advantage of the S7 and Modbus protocol's lack of encryption and identity authentication vulnerabilities to send commands directly to the PLC, which creates equipment downtime. Using the Ettercap tool to perform an MITM attack on the HMI and PLC, we can make the HMI display false PLC data. This method can also be used to perform Modbus command injection attacks. It also verifies the PLC device DoS attack through the ultra-long Ping package.

In addition, we conducted system vulnerability discovery for a specific type of PLC device. The firmware of the PLC was downloaded by a tool provided by the manufacturer, and a reverse analysis of the firmware was carried out. We scanned the network ports and services of the device through Nmap and Simple Network Management Protocol (SNMP), and fuzzed the protocol and service of the device through Peach Fuzzer. We found that there are some vulnerabilities in the protocols, authentication, and services of the device. We informed the device manufacturer about the relevant information. These results are not discussed in this paper, as the ethical disclosure process is ongoing.

4.2 Attack scenarios

We built two attack scenarios through disclosed vulnerabilities and cyberattacks that occurred against ICSs.

4.2.1 Attack scenario 1

As shown in Fig. 4 and Tab. 6, the attacker sends a spear phishing email to the target, which contains an attachment in Microsoft PowerPoint file format. The attacker used Microsoft Office 2007 vulnerabilities (CVE-2014-4114) to include malicious software in this attached file. The employees infect the malicious software when opening the attachment file on office workstations of the enterprise zone, and the attacker gains the authority of the enterprise zone. Then, the attacker uses the CVE-2008-4250 vulnerability to attack the KingView server in the DMZ zone. This vulnerability allows for the remote execution of arbitrary code through a remote procedure call to gain the authority of the server, thus penetrating the DMZ network. Then, through this server, the same vulnerability penetrates the operation station of the control zone. Finally, the remote stop CPU (Central Processing Unit) command is sent to the Siemens PLC of the power plant through the operator station, which causes the DAS, MCS, and SCS systems to stop running, and the entire power plant stops working. Because the power is interrupted, the rail transit system stops running. In this attack scenario, all attacks after the user opens the email can be automatically completed by the malicious software. The entire process takes no more than 1 min.

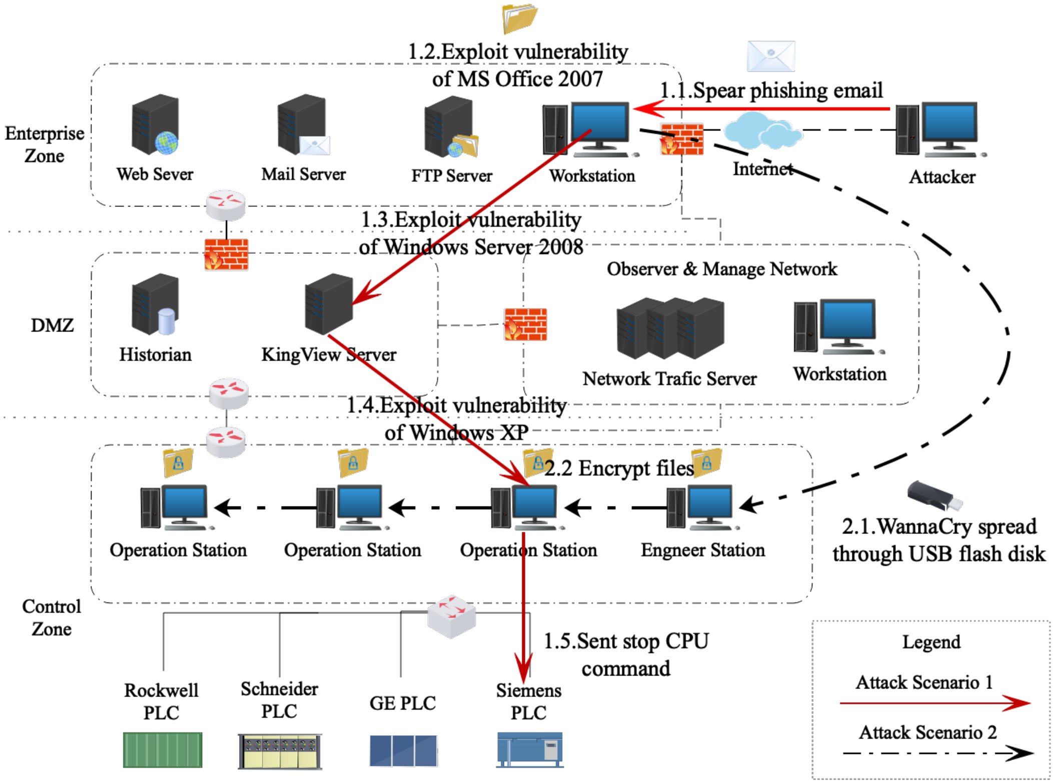

Figure 4: Attack process diagram of two attack scenarios

Table 6: Vulnerabilities used in attack scenarios

Attack Scenario	Attack Process	Vulnerability
1	Spear phishing email	CVE-2014-4114
	Intranet Penetration	CVE-2008-4250
	ICS attack	Exploit-db: 19831 [Beresford (2012)]
2	Malware delivery	BadUSB [Nohl and Lell (2014)]
	Malware spread	CVE-2017-11780

4.2.2 Attack scenario 2

As shown in Fig. 4 and Tab. 5, the enterprise zone network is infected with WannaCry ransomware. The internal staff copies files from office workstations to the engineering station through a USB flash disk for upgrades and maintenance. The WannaCry ransomware spreads to the control zone through the USB flash disk and exploits vulnerabilities (CVE-2017-11780) to spread through port 445 in the control zone network. Thus, all engineering stations and operation stations stop running, and the files are encrypted.

The attack process of scenario 1 is basically the same as the first phase of the Ukrainian blackout accident [Liang, Weller, Zhao et al. (2017)]. After obtaining control of the HMI, BlackEnergy attacked the circuit breaker of the power grid, and the attack scenario simply sent a stop CPU command to the PLC. Then, the attack process was basically complete. Scenario 2 is the actual infection process of WannaCry in many industrial enterprises [Lee (2018); Nick, Jenny and Stu (2017)]. In addition, Stuxnet enters the control network in a similar way [Kushner (2013)].

4.3 Security solutions

Security solutions are an important research topic for the ICS testbed. Some researchers have tried to improve the architecture and increase the security of the ICS protocol via methods such as the secure Modbus protocol [Nai Fovino, Carcano and Masera (2009)], Secure DNP3, and DNPSec [Majdalawieh, Parisi-Presicce and Wijesekera (2007)]. These solutions can improve the security of newly deployed ICSs, but according to the characteristics of the ICSs, these systems may be in service for a long time [Stouffer, Falco and Scarfone (2011)]. To increase the security of an ICS in use, security solutions may be added to the original system. This paper mainly considers this issue.

If an HMI is implemented based on COT software and hardware, software updates cannot be performed in time. If traditional antivirus software is used in an ICS system, it will be difficult to update the virus database in time. We try to use whitelist-based host protection software, which records the programs that the workstation has already run and the signatures of the files of these programs to form a whitelist. When a subsequent program needs to run, the protection software checks whether the signature is already on the whitelist. If it is on the whitelist, it is allowed to run, and if it is not on the whitelist, it is not allowed to run. This protection program occupies fewer resources and does not conflict with the control software. Even without upgrading, it can prevent some unknown attacks. After testing, this method can effectively protect against the attack methods in our attack scenarios.

There are fewer firewall products available for ICS networks that can identify the industrial control protocol, and the control network has higher requirements for network delays. Deploying a firewall may increase the delay and affect the control process, but deploying the IDS system and detecting the network through mirror traffic and discovering attacks is a better solution. Nai et al. [Fovino, Masera, Guidi et al. (2010)] proposed a behavior-based IDS system, and Formby et al. [Formby, Rad and Beyah (2018)] also implemented IDS through Snort. Wan et al. [Wan, Yao, Jing et al. (2018)] proposed an event-based anomaly detection method to identify misbehaviors using nonpublic industrial communication protocols. Through the construction process of attack scenarios, we find that the ICS attack process requires a combination of common IT vulnerabilities with ICS-specific vulnerabilities. In order to better prevent such attacks, we propose a new IDS solution that combines traditional IT system IDS and behavior-based ICS-specific IDS. Traditional IT network IDS can effectively identify malicious behaviors such as ARP spoofing, DNS spoofing, traditional worms, viruses, and Trojans. Behavior-based IDS can detect attacks on control systems in time. At present, the function of our behavior-based IDS is relatively simple. It can only detect unauthorized parameter modifications, the remote turning-on or turning-off of devices, and firmware downloads and uploads. In addition, it can only alarm and cannot effectively block attacks, but it can find existing ICS attacks very effectively.

5 Conclusion

This paper presented the MSICST testbed, a multiple-scenario hardware-in-the-loop ICS testbed for security research, which contains a complete enterprise network such as an enterprise zone network, DMZ, and control zone network. The control zone network contains four typical process scenarios: thermal power plant, rail transit, smart grid, and intelligent manufacturing. In order to conduct security research, the testbed also includes an attacker model, observer, and management network. Using the testbed, we conducted vulnerability discovery on the control device and found some vulnerabilities. We constructed two attack scenarios to simulate real ICS cyberattack events. We studied the security solutions and a whitelist-based host protection technology. From this, a new IDS solution was proposed. The IDS solution combines traditional IT system IDS and behavior-based ICS-specific IDS.

In the future, we will expand to more process scenarios, and we will deploy more devices and protocols such as robotic control systems and other processes of the power grid. Additionally, we will introduce the steganography technology [Zhang, Qin, Zhang et al. (2018)] to conceal attacks, and add steganalysis [Yang, Luo, Lu et al. (2018); Ma, Luo, Li et al. (2018)] and machine learning [Xiang, Zhao, Li et al. (2018)] technology in order to evaluate the security.

References

Albright, D.; Brannan, P.; Walrond, C. (2010): *Did Stuxnet Take Out 1,000 Centrifuges Atthe Natanz Enrichment Plant*? Institute for Science and International Security.

Andreeva, O.; Gordeychik, S.; Gritsai, G.; Kochetova, O.; Potseluevskaya, E. et al. (2016): *Industrial Control Systems and Their Online Availability*. Kaspersky Lab.

Assante, M. J.; Lee, R. M. (2015): *The Industrial Control System Cyber Kill Chain*. SANS Institute.

Beresford, D. (2012): Siemens simatic s7-300/400-cpu start/stop module (metasploit). https://www.exploit-db.com/exploits/19831.

Bodungen, C. E.; Singer, B. L.; Shbeeb, A.; Hilt, S.; Wilhoit, K. (2016): *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions*. McGraw-Hill Education.

Candell, R.; Stouffer, K.; Anand, D. (2014): A cybersecurity testbed for industrial control systems. *Proceedings of the 2014 Process Control and Safety Symposium*.

Candell, R.; Zimmerman, T.; Stouffer, K. (2015): *An Industrial Control System Cybersecurity Performance Testbed*. National Institute of Standards and Technology.

DoE (2018): National scada test bed. https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

Downs, J. J.; Vogel, E. F. (1993): A plant-wide industrial process control problem.

Computers & Chemical Engineering, vol. 17, no. 3, pp. 245-255.

Formby, D.; Rad, M.; Beyah, R. (2018): Lowering the barriers to industrial control system security with GRFICS. *USENIX Workshop on Advances in Security Education. USENIX Association.*

Fovino, I. N.; Masera, M.; Guidi, L.; Carpi, G. (2010): An experimental platform for assessing scada vulnerabilities and countermeasures in power plants. *3rd Conference on Human System Interactions*, pp. 679-686.

Green, B.; Lee, A.; Antrobus, R.; Roedig, U.; Hutchison, D. et al. (2017): Pains, gains and plcs: ten lessons from building an industrial control systems testbed for security research. *10th USENIX Workshop on Cyber Security Experimentation and Test. USENIX Association.*

Green, B.; Paske, B.; Hutchison, D.; Prince, D. (2014): Design and construction of an industrial control system testbed. *PG Net-the 15th Annual Post Graduate Symposium on the Convergence of Telecommunications*.

Holm, H.; Karresand, M.; Vidstrom, A.; Westring, E. (2015): A survey of industrial control system testbeds. *Secure IT Systems*, vol. 9417, pp. 11-26.

Kushner, D. (2013): The real story of stuxnet. *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53.

Lee, M. (2018): Boeing is the latest wannacry ransomware victim. https://www.forbes.com/sites/leemathews/2018/03/30/boeing-is-the-latest-wannacry-ransomware-victim/.

Liang, G.; Weller, S. R.; Zhao, J.; Luo, F.; Dong, Z. Y. (2017): The 2015 ukraine blackout: implications for false data injection attacks. *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318.

Ma, Y.; Luo, X.; Li, X.; Bao, Z.; Zhang, Y. (2018): Selection of rich model steganalysis features based on decision rough set α-positive region reduction. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2.

Majdalawieh, M.; Parisi-Presicce, F.; Wijesekera, D. (2007): Dnp Sec: distributed network protocol version 3 (DNP3) security framework. *Advances in Computer, Information, and Systems Sciences, and Engineering*, pp. 227-234.

Martin, L. (2013): Cyber kill chain. https://www.lockheedmartin.com/enus/capabilities/cyber/cyber-kill-chain.html.

Mathur, A. P.; Tippenhauer, N. O. (2016): Swat: a water treatment testbed for research and training on ICS security. *International Workshop on Cyber-Physical Systems for Smart Water Networks*, pp. 31-36.

McLaughlin, S.; Konstantinou, C.; Wang, X.; Davi, L.; Sadeghi, A. R. et al. (2016): The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039-1057.

Morris, T.; Srivastava, A.; Reaves, B.; Gao, W.; Pavurapu, K. et al. (2011): A control system testbed to validate critical infrastructure protection concepts. *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 88-103.

Nai, F.; Carcano, A.; Masera, M. (2009): Secure modbus protocol, implementation, tests and analysis. *Proceeding of the Third Annual IFIP Working Group*, vol. 11, pp. 22-25.

Nick, K.; Jenny, G.; Stu, W. (2017): Wannacry attack hits renault, 200,000-plus victims. https://www.marketwatch.com/story/wannacry-attack-hits-renault-200000-plusvictims-2017-05-15.

NIST (2014): *Measurement Challenges and Opportunities for Developing Smart Grid Testbeds Workshop*. National Institute of Standards and Technology.

Nohl, K.; Lell, J. (2014): Badusb-on accessories that turn evil. *Black Hat USA*.

Stouffer, K.; Falco, J.; Scarfone, K. (2011): *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82.

Wan, M.; Yao, J.; Jing, Y.; Jin, X. (2018): Event-based anomaly detection for non-public industrial communication protocols in SDN-based control systems. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 447-463.

Weiss, J. (2008): *Assuring Industrial Control System (ICS) Cyber Security*. Center for Strategic and International Studies.

Williams, T. J. (1994): The purdue enterprise reference architecture. *Computers in Industry*, vol. 24, no. 2-3, pp. 141-158.

Xiang, L.; Zhao, G.; Li, Q.; Hao, W.; Li, F. (2018): TUMK-ELM: a fast unsupervised heterogeneous data learning approach. *IEEE Access*, vol. 6, pp. 35305-35315.

Xu, W.; Tao, Y.; Guan, X. (2018): The landscape of industrial control systems (ICS) devices on the internet. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, pp. 1-8.

Yang, C.; Luo, X.; Lu, J.; Liu, F. (2018): Extracting hidden messages of MLSB steganography based on optimal stego subset. *Science China Information Sciences*, vol. 61, no. 11, pp. 1-3.

Zhang, Y.; Qin, C.; Zhang, W.; Liu, F.; Luo, X. (2018): On the fault-tolerant performance for a class of robust image steganography. *Signal Processing*, vol. 146, pp. 99-111.