A survey of industrial control system testbeds

Yangyang Geng¹, Yi Wang², Wenwen Liu¹, Qiang Wei¹*, Ke Liu¹, Haolan Wu¹

¹ State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, 450001, China. ² Department of Research and Development Center, Beijing sifang automation co.,ltd, Beijing, 100085, China.young9471@163.com

Abstract. Industrial Control System (ICS) testbed is the basis of ICS safety research. In order to build an ICS testbed, it is necessary to have a deep understanding of the current research status. This paper introduced the structure and composition of the typical ICS system. Then it simply analyzed the technical characteristics, system framework and advantages and disadvantages of four types of typical ICS testbeds. Finally, it summarized application scenarios of ICS testbed and pointed out some problems in testbed construction and the development direction of ICS testbed with the fusion of cyber and physical.

1. Introduction

ICS is a computer-based system for monitoring physical processes. It is widely used in many key national infrastructure industries such as energy, transportation, water, security, food, and large-scale manufacturing[1]. With a large number of ICS control devices connected to the Internet, the security risks that were originally only generated in the physical world can now achieve the same goal through network attacks, which leads to severe challenges for ICS information security.

With the outbreaks of ICS viruses such as Stuxnet, Duqu, Flame, Blackenergy, Industroyer, Triton, ensuring the information security of ICS becomes a hot research question that must be solved. ICS safety testing helps to ensure safe operation at industrial sites, but the high availability requirements of ICS make it difficult to conduct research directly in real-world production environments. Therefore, the researchers try to build an ICS testbed to simulate real ICS and deploy it in a safely executed experimental environment.

Based on the characteristics of the fusion of cyber and physical, it is necessary to simulate the information interaction of the network layer and simulate the business process of the physical layer when constructing the ICS testbed. Since the construction of the ICS testbed is a high-cost, long-term, and high-volume project, it is difficult for researchers to build an experimental environment for full-scale pure physical reproduction. Usually, different types of testbeds are built according to research requirements and realistic capabilities. ICS Network components and field devices are configured by technologies such as physical replication, software simulation and emulation, and virtualization. The design and implementation of the testbed need to consider a variety of factors, in general, to meet the following four requirements[2]: (1) fidelity: the experimental testbed needs to reproduce the real system of the research object as accurately as possible. (2) Repeatability: The experimental testbed should ensure that the same repeated experiments yield the same or statistically consistent results. (3) Measurement accuracy: The experimental testbed should be able to accurately monitor the experimental process and will not interfere with the experimental results when performing observation and test actions. (4) Safe Execution: The experimental testbed should ensure that the activities in the
testbed are isolated and that the experiment does not have a devastating effect on the physical system and personal safety.

2. Typical ICS structure and composition

The system frameworks, hardware and software devices, and network protocols of ICS vary widely in different industries. The Purdue Model provides a good reference for the construction of the ICS testbed. As shown in Figure 1, Purdue model divided the ICS into the following four areas:

1. Safety zone: This zone includes systems and devices for managing ICS security functions to avoid dangerous failures in the system when hardware failures or system outages occur.
2. Control Zone: This zone includes systems and equipment for monitoring, controlling and maintaining the automated operation of the logistics process. These systems and devices are deployed in the same geographical location and they are the core of the entire control system.
3. Demilitarized Zone: This zone provides a “buffer” that can share data between manufacturing and enterprise zones, enabling information sharing between information systems and physical systems.
4. Enterprise Zone: This zone mainly includes traditional non-ICS specific devices and systems, which use the data input from the manufacturing area to perform supervision and planning functions throughout the ICS.

3. ICS testbed classification

According to the different implementation and configuration methods of the testbed, the ICS testbeds are divided into four categories: physical simulation testbed, software simulation testbed, semi-physical simulation testbed and virtualized testbed. The remainder of this section will detail the key technologies, implementation methods, advantages and disadvantages of each type of testbed.

3.1. Physical simulation testbed

The physical simulation testbed uses real hardware and software to configure the network layer and the physical layer. In order to assess the vulnerability of ICS and improve the safety of industrial infrastructure, the US Department of Energy (DOE) has issued the National SCADA TestBed (NSTB) program[3] and built 17 network security testbeds. Idaho National Laboratory built a 61-mile 138kV transmission testbed, which is the world's first grid-tested environment with full-scale replication of real hardware and software equipment, including seven substations and more than 3,000 monitoring sites.

In general scientific research, it is difficult for researchers to build large-scale national ranges with pure physical reproduction because of the limited cost. Therefore, researchers use a small amount of necessary core physical components to build a minimum ICS test environment. For example, in order to study the impact of cyber attacks on ICS, researchers in Singapore University of Technology and Design used real-world physical devices simulated three ICS testbeds including water treatment systems, water distribution systems, and power systems. Figure 2 shows a six-stage water treatment testbed SWaT[4], which is widely used in ICS safety research[5-9]. The Lancaster University in the UK built a large testbed[10-11] based on the Purdue reference model. The testbed consists of six
manufacturing areas, an ICS demilitarized zone and an enterprise zone. The Network device and control device of the testbed is multi-vendor and multi-type physical device. In addition, there are some smaller testbeds, the Netherlands Organisation for Applied Scientific Research has developed a safety testbed to develop a safer control system architecture[12]. Idaho State University built PowerCyber[13-14] for power grid communication testbeds. Mississippi State University built an ICS testbed for vulnerability discovery[15].

3.2. Software simulation testbed
Unlike the physical simulation testbed, the software simulation and emulation testbed use a single software or multiple software to jointly simulate the related components of hardware and software in the ICS control center, communication architecture, field devices, and physical processes. For example, DETER, Emulab, CORE, ns2, OPNET, OMNet++, SSFnet, RINSE and other network simulation tools are used to simulate the control center communication network. STEP7, RSEmulate, Modbus Rsim, Soft-PLC and other softwares are used to simulate the programmable logic controller (PLC) and other field devices communication process. Matlab, Modelica, Ptolemy, PowerWorld and other simulation tools are used to model the physical process.

3.2.1. Simulate ICS components with a single simulator
Almalawi et al. used a single simulator to simulate ICS components. As shown in Figure 3, Almalawi developed the framework of the SCADAVT testbed[16]. The CORE simulator is used to simulate I/O modules and field devices, Modbus communication servers and other network components. IOModuleGate is used to implement the IOModules protocol. And the performance impact of integrity attacks and denial of service attacks on the water distribution system is analyzed by the measurement data from the simulator and corresponding supervised process parameters.

3.2.2. Co-simulating ICS components with multiple software
Some researchers use a variety of different softwares to co-simulate the network, control equipment, and physical processes of the testbed. To create a scalable, repeatable research environment for Cyber-Physical Systems (CPS), Antonioli et al. developed a simulation toolbox MiniCPS[20] that simulates CPS communication and physical interaction, showing the attack scenarios and defense methods with MiniCPS for real systems. As shown in Figure 4, MiniCPS uses the python library to simulate the network traffic of components such as PLC and network traffic in CPS, which is connected to the upper layer control network of the Mininet simulation and the physical layer API in the lower layer and completes the interaction with the network layer and the physical layer signals through the industrial protocol.
As shown in Figure 5, Genge et al. designed a testbed that includes a network layer, a physical layer, and an intermediate three-layer framework of cyber-physical link layers[21]. At the network layer, Emulab is used to accurately configure the physical topology in a simulated virtual topology. In addition, the network layer includes code that runs inside the PLC. The network physical link layer implements the memory function of the PLC, which is used to complete the read and write interaction of input and output with the network layer and the physical layer. At the physical layer, the physical process is modeled using the Simulink simulator to execute the business processes of the controlled physical system.

In order to test the power system requirements and evaluate the vulnerability and attack methods in the smart grid environment, the researchers used the PowerWorld simulator to simulate the physical process of the grid[22-25]. RINSE, OPNET, PSAT and other simulation softwares were used to simulate control network.

Software simulation is a low-cost, reusable construction method of testbed that is easy to reconfigure and maintain, providing a rich set of scenarios for security testing and evaluation. However, the software and hardware vulnerabilities in the system exist only in the specific code base. The software simulation and emulation method is difficult to verify the hardware and software vulnerabilities and malicious viruses in the real system due to the lack of interaction with the real software and hardware. Given the limited capabilities of network security analysis and verification, it is difficult to achieve high fidelity requirements for testbed.

3.3. Semi-physical simulation testbed

From the different ICS component implementation methods, the semi-physical simulation testbed can be divided into the following three categories: (1) Using physical devices simulates a control network and using software simulates physical processes. (2) Using software simulates the control network and using physical devices simulates the physical process. (3) Using physical devices and software to jointly simulate the control network and using software simulates the physical process.

3.3.1. Physical simulation of control network and software simulation of physical processes

As shown in figure 6, Candell et al. constructed the Tennessee Eastman(TE) factory model testbed[26], which simulated the demilitarized zone, operating zone and control zone in the ICS. Except for the TE process was modeled with Ricker Simulink in the control zone, other applications such as HMI, PLC, service sites, and switches were simulated using real physical devices.

SIATERLIS et al. established the European testbed EPIC[27][28], which combines a true Information and Communication Technology(ICT) test platform with the Emulab software simulator.
to provide a high fidelity network layer and experimental ability for multiple heterogeneous critical infrastructures.

3.3.2. Physical simulation of physical processes and software simulation of control network
Queiroz et al. developed the SCADASim test framework that used real hardware to simulate physical processes and software to simulate the control networks[29]. SCADASim supports the integration of industry standard protocol modules with real-world devices, which can be used to develop a series of SCADA system simulations to assess the impact of network attacks on communications and physical processes. SCADASim provides pre-defined modules for building SCADA simulations, which rebuilds typical SCADA components with the discrete event simulation engine OMNET++ and provides inter-model communication between the models. In addition, MATLAB/Simulink is used to simulate hardware components. But only sensors and actuators use real physical hardware in SCADASim.

In another testbed that also built by Queiroz[30], in order to study the impact of the DDoS attack on the SCADA system of the water plant, OMNET++ is used to simulate control network and Lego Mindstorms NXT is used to simulate PLC and other hardware devices. What’s more, the libModbus library is used to implement Modbus communication and real sensors and actuators are used to simulate water plants.

3.3.3. Physical and software co-simulation of control network and software simulation of physical processes
Hahn et al. used the method of co-simulation to simulate components at the same level. As shown in Figure 7, Hahn built a smart grid security testbed PowerCyber at Iowa State University to study the impact of cyber attacks on the smart grid[31]. PowerCyber’s network layer includes a control center and several substations. The control center supports general SCADA functions. The substation consists of RTUs and Intelligent Electronic Devices(IEDs). The DNP3 protocol is used for communication between the control center and the substation RTU. In the substation, the status and commands between the IED and the RTU are communicated by using the IEC 61850 protocol. The physical layer deploys two simulators, DlgSILENT and RTDS, to simulate a 9-bus power system model.

Ghaleb did a similar job and developed a general testbed SCADA-SST[32]. SCADA-SST has both real SCADA and virtual SCADA devices. SCADA-SST includes three types of nodes: virtual node, external node and interface node. The virtual nodes are SCADA related devices (such as PLC, RTU, HMI, etc.) that are simulated with OMNet++. The external node is a physical SCADA device located.
outside of the OMNet++ virtual network. The interface node allows communication between the virtual node and the external node. All components can be placed in any desired network topology, and users can easily build a network topology with easy coding.

The semi-physical simulation testbed uses some real hardware and software, which has high fidelity and can provide more reliable experimental data. But the low flexibility and high cost of such testbeds limit the scale of the testbed, which is often difficult to support large-scale information security experiments.

3.4. Virtualized testbed
In order to build a low-cost, high-fidelity, reusable, and easy-to-maintain testbed, virtualization technology is used to build ICS testbed in recent years. Early virtualized testbeds used python scripts to virtualize test platform components such as HMI and PLC and implemented them in separate virtual machines[33]. Although multiple metrics were used to improve system fidelity, the system was not sufficient to simulate different industrial processes.

Mainstream controllers such as Siemens, Schneider, and Omron are closed-source commercial devices. Suppliers have limited information on hardware and firmware, making it difficult to virtualize these mainstream controllers. So one of the biggest obstacles to virtualize high-fidelity ICS testbeds is the lack of open source virtualized PLCs.

Fortunately, Alves et al. developed an open source controller OpenPLC to provide a method for virtualizing controllers[34]. OpenPLC is the first fully functional standardized open source PLC, which supports all five programming languages based on IEC61131-3 and Modbus/TCP, DNP3 and other commonly used SCADA protocols.

Formby et al. developed the GRFICS framework based on the work of Alves[35]. GRFICS virtualized the entire ICS network and physical processes. As shown in Figure 8, HMI and PLC were implemented using open source AdvancedHMI and OpenPLC software respectively. The 3D game engine was used to visualize the physical process. The GRFICS testbed can be used to practice common methods of ICS attacks and exploits, in the meanwhile, observing the impact of network attacks on physical processes.

Alves et al. used the same method to develop a new modular architecture for the SCADA test platform and virtualized the various components of the SCADA system[36-37].

The virtualized testbed enables researchers to conduct low-cost, replicable security studies in a real ICS configuration environment with an IT architecture. However, virtualized complex physical processes involve a large amount of computation. So, the hardware requirements of the computer are high. Currently, virtualization technology can only virtualize and configure open source controllers and related software in virtual machines, and it is difficult to test and verify vulnerabilities related to mainstream controllers in the Industrial site.
4. Testbed application scenario
The ICS testbed is widely used in ICS network security research. Figure 9 lists the application scenarios of testbeds, which mainly includes the following aspects:

   (1) Attack technology research: Evaluate the impact of different types of malicious network attacks on physical systems.

   (2) Defense technology research: Research on defense methods and mitigation measures against various attack technologies.

   (3) Vulnerability assessment: Research the vulnerability discovery and exploit technology of related software and hardware in the testbed.

   (4) Education: Enhance students' ICS related theoretical knowledge and provide ICS network attack and defense practice verification.

   (5) Security Control System Development: Design a more secure control system framework to improve the ability to deal with security threats.

   (6) Functional test: Test the reliability network delay and other physical performance indicators of the control system.

   (7) SCADA training: Train SCADA field operators to improve operator safety awareness.

   (8) Security verification: Evaluate the network security compliance of the control system.

   (9) Forensic analysis: Study the forensic analysis technology of SCADA system. Analyze the data in the firmware, PLC program logic, network traffic, HMI, historical database and other services.

   (10) Safety standards development: Research and develop safety standards that are consistent with the industry.

   (11) Cyber Security Competition: Provide an experimental environment for the CTF Cyber Security Capture Race.

5. Main Problems and Development Direction
The development of ICS testbed is a high-cost, labor-intensive and time-intensive project. Researchers expect to build scalable testbed with higher assurance at lower cost. We analyzed the existing ICS testbed and concluded four shortcomings:

   (1) Lack of hardware-software interaction: Most of the current testbeds use software simulation control layer hardware, which lack of real hardware and software interaction and has low fidelity. So, it is difficult to meet the real software and hardware requirements in ICS attack and defense technology research.

   (2) Virtualization technology is not suitable for closed source proprietary devices: The control system contains a large number of proprietary hardware and software, which are difficult to implement by virtualization technology.

   (3) The integrity of physical process simulation is inadequate: It is difficult to simulate all system states by using software simulation and virtualization technology. Physical process modeling of industrial processes is mostly abstract and simplified, which is difficult to simulate network attacks of physical process under the condition of cyber-physical.

   (4) Insufficient diversity and heterogeneity of equipment: Most testbeds are only equipped with hardware from a single supplier, which is difficult to meet the vulnerability assessment of specific protocols and equipment.

With the deep integration of informationization and industrialization, ICS is gradually changing to cyber-physical system(CPS). In order to study, analyze and verify the security vulnerabilities and attack and defense technologies of ICS devices, protocols, networks and other levels under the condition of cyber-physical, the future trend is to build more perfect network hierarchy, more heterogeneous field hardware devices and more simulation testbed based on the previous text. In view of the shortcomings of the ICS testbed mentioned above, this paper puts forward four development directions of building ICS testbed:

   (1) Building a typical ICS network framework including external network, company network, demilitarized zone monitoring network and field network, which can simulate the multi-level, high
fidelity and strong interaction network, which is necessary in the research of ICS attack and defense technology.

2) Using virtualization technology to virtual operating system and installing real software to simulate the relevant nodes in external network, company network and monitoring network. And building a large-scale, scalable and highly practical testing network to facilitate the recovery of snapshots back to a critical state for repeatable experiments.

3) Simulating the field network by using multi-vendor real field equipment. Proprietary equipment vendors do not provide open-source firmware and it is very difficult to virtualize the field equipment. So the key to improve the fidelity and complexity of the testbed is using real field equipment to build the testbed.

4) Using industry-specific simulation software and real sensors and actuators to simulate the physical process. Including of simulating the business process, physical characteristics, constraints, fault response and so on, which can simulate the stealthy attacks related to physical process for ICS.

6. Conclusion
ICS testbed plays an important role in promoting vulnerability assessment, attack and defense technology. In this paper, we analyzed the implementation methods of ICS related components in typical testbeds. The advantages and disadvantages of four types of testbeds were compared. Based on the shortcomings of existing testbeds, the future research direction of testbeds was discussed. In the future work, our ICS testbed will be built according to the above ideas, including virtual multi-layer network, physical simulation of field control devices and hybrid physical process modeling with physical simulation and software simulation.

Acknowledgments
This work was financially supported by the National Natural Science Foundation of China(61833015) and National Key R&D Program of China(2016YFB0800203).

References
[1] Stouffer K, Falco J, et al. Guide to industrial control system (ICS) security, SP800-82[R].Gaithersburg: National Institute of Standards and Technology (NIST), 2011.
[2] Siaterlis C, Garcia A P, et al. On the Use of Emulab Testbeds for Scientifically Rigorous Experiments[J]. IEEE Communications Surveys & Tutorials, 2013, 15(2): 929-942.
[3] Barnes K, Johnson B. National SCADA Test Bed Substation Automation Evaluation Report[J]. Automation, 2009, 30(1): 45-55.
[4] Mathur A P, Tippenhauer N O. SWaT: a water treatment testbed for research and training on ICS security [C]// Proc of International Workshop on CySWater. Piscataway, NJ: IEEE Press, 2016: 31-36.
[5] Ghaeini H R, Tippenhauer N O. HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems [C]// Proc of Acm Workshop on Cyber-physical Systems Security & Privacy. New York: ACM Press, 2016: 103-111.
[6] Rocchetto M, Tippenhauer N O. On Attacker Models and Profiles for Cyber-Physical Systems [C]// Proc of the 21th European Symposium on Research in Computer Security. Berlin: Springer Press, 2016: 427-449.
[7] Adep S, Mathur A. An Investigation into the Response of a Water Treatment System to Cyber Attacks [C]// Proc of the 17th IEEE International Symposium on High Assurance Systems Engineering. Piscataway, NJ: IEEE Press, 2016: 141-148.
[8] Urbina D, Cardenas A, et al. Limiting The Impact of Stealthy Attacks on Industrial Control Systems [C]// Proc of Acm Sig sac Conference on Computer & Communications Security. New York: ACM Press, 2016: 1092-1105.
Systems. Berlin: Springer Press, 2018: 110-126.

[10] Green B, Hutchison D, et al. Testbed diversity as a fundamental principle for effective ICS security research[J]. Inter-national Journal of Critical Infrastructure Protection, 2011, 4(2): 88-103.

[11] Green B, Le A, et al. Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research [C]// Proc of the 10th USENIX Workshop on Cyber Security Experimentation and Test, Berkeley: USENIX Association, 2017: 123-138.

[12] Christiansson H, Luiijf E A M. Creating a European SCADA Security Testbed [C]// Proc of International Conference on Critical Infrastructure Protection, Berlin: Springer Press, 2008: 237-247.

[13] Hahn A, Kregel B, et al. Development of the PowerCyber SCADA security testbed [C]// Proc of the 6th Annual Workshop on Cyber Security and Information Intelligence Research. New York: ACM Press, 2010: 11-18.

[14] Hahn A, Govindarasu M. An evaluation of cybersecurity assessment tools on a SCADA environment [C]// Proc of Power & Energy Society General Meeting. Washington: IEEE, 2011: 1-6.

[15] Morris T, Srivastava A, et al. A control system testbed to validate critical infrastructure protection concepts[J]. Inter-national Journal of Critical Infrastructure Protection, 2011, 4(2): 88-103.

[16] Almalawi A, Tari Z, et al. SCADAVT-A framework for SCADA security testbed based on virtualization technology[C]// Proc of IEEE Conference on Local Computer Networks. Piscataway, NJ: IEEE Press, 2013: 639-646.

[17] Tesfahun A, Bhaskari D L. A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures[J]. Automatic Control & Computer Sciences, 2016, 50(1): 54-62.

[18] Hussain A, Amin S. NCS security experimentation using DETER [C]// Proc of the 1st international conference on High Confidence Networked Systems. New York: ACM Press, 2012: 73-81.

[19] Farooqui A A, Zaidi S S H, et al. Cyber Security Backdrop: A SCADA testbed [C]// Proc of Computing, Communications & It Applications Conference. Piscataway, NJ: IEEE Press, 2014: 98-103.

[20] Antonioli D, Tippenhauer N O. MiniCPS: A toolkit for security research on CPS Networks [C]// Proc of the 1st ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, New York: ACM Press, 2015: 91-100.

[21] Siaterlis C, Fovino I N, et al. A cyber-physical experimentation environment for the security analysis of networked industrial control systems[J]. Computers & Electrical Engineering, 2012, 38(5): 1146-1161.

[22] Morris T, Vaughn R, et al. SCADA Cyber Security Testbed Development [C]// Proc of the 38th North American Power Symposium, Piscataway, NJ: IEEE Press, 2012: 2338-2345.

[23] Mallouhi M, Alnashif Y, et al. A testbed for analyzing security of SCADA control systems (TASSCS) [C]// Proc of IEEE ISGT. Piscataway, NJ: IEEE Press, 2011: 1-7.

[24] Singh P, Garg S, et al. A testbed for SCADA cyber security and intrusion detection [C]// Proc of International Conference on SSCIC. Piscataway, NJ: IEEE Press, 2015: 111-116.

[25] Jurisic B, Holjevac N, et al. Framework for designing a smart grid testbed [C]// Proc of the 36th International Convention on Information & Communication Technology Electronics & Microelectronics. NJ: IEEE Press, 2013: 1247-1252.

[26] Candell Jr. R, Zimmerman T A, et al. An Industrial Control System Cybersecurity Performance Testbed[J/O]. NIST Int-eragency/Internal Report, 2015, (2015-12-10)[2018-11-10]. https://doi.org/10.6028/NIST.IR.8089.

[27] Siaterlis C, Genge B, et al. EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation[J]. IEEE Trans on Emerging Topics in Computing, 2013, 1(2):319-330.

[28] Siaterlis C, Genge B. Cyber-physical testbeds[J]. Communications of the Acm, 2014, 57(6): 64-73.

[29] Queiroz C, Mahmood A, et al. SCADASim—A Framework for Building SCADA Simulations[J].
IEEE Trans on Smart Grid, 2011, 2(4): 589-597.
[30] Queiroz C, Mahmood A, et al. Building a SCADA Security Testbed [C]// Proc of the 3rd International Conference on Network and System Security. Piscataway, NJ: IEEE Press, 2009: 357-364.
[31] Hahn A, Ashok A, et al. Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid[J]. IEEE Trans on Smart Grid, 2015, 4(2): 1-6.
[32] Ghaleb A, Zhioua S, et al. SCADA-SST: a SCADA security testbed [C]// Proc of Industrial Control Systems Security. Piscataway, NJ: IEEE Press, 2017: 1-7.
[33] Reaves B, Morris T. An open virtual testbed for industrial control system security research[J]. International Journal of Information Security, 2012, 11(4): 215-229.
[34] Alves T R, Buratto M, et al. OpenPLC: An open source alternative to automation [C]// Proc of the 4th IEEE Global Humanitarian Technology Conference. Piscataway, NJ: IEEE Press, 2014: 585-589.
[35] Formby D, Rad M. Lowering the Barriers to Industrial Control System Security with GRFICS [C]// Proc of USENIX Workshop on Advances in Security Education. Berkeley: USENIX Association, 2018: 23-32.
[36] Alves T, Das R, et al. Virtualization of Industrial Control System Testbeds for Cybersecurity [C]// Proc of Annual Industrial Control System Security Workshop, 2016: 10-14.
[37] Alves T, Das R, et al. Virtualization of SCADA testbeds for cybersecurity research: A modular approach[J]. Compute-rs and Security, 2018, 77: 531-546.