# Development of a Testbed for Process Control System Cybersecurity Research

Dongqing Chen, Yong Peng
China Information Technology Security Evaluation Center
Beijing 100085, China
e-mail: warina@126.com, pengy@263.net

Huazhong Wang
Department of Automation
East China University of Science and Technology
Shanghai 200237, China
e-mail: hzwang@ecust.edu.cn

***Abstract*—Testbed plays an important role in the cybersecurity research of process control system. It helps us design and test solutions to various attacks against control system. A hybrid structure process control testbed, combining programmable logic controllers and other real process control systems with simulated Tennessee-Eastman process, was proposed in this paper. Principles and details of the testbed are described in the paper. Cybersecurity scenario on the testbed through Modbus worm attack was implemented to show the adverse impact on process control system and the industrial process being controlled.**

***Keywords-testbed; process control; cybersecurity; TE process***

## I. INTRODUCTION

Industrial control systems, especially the distributed control systems(DCS) used in process industry, play very important roles in many critical infrastructures, e.g. power generation, water and wastewater treatment, oil mining and refining and so on. With the widely use of modern information technology in process control system, the traditional isolated control system was made into a network system. Although many benefits are achieved with such technical innovation, the side effects is also obvious, it exposes the process control system to various cyber attacks, which threats the security of critical infrastructures. Stuxnet attack on the Iranian nuclear power facilities makes the cybersecurity issue to an alarm stage[1]. It happened even when the facilities and its control system were highly secured, located underground physically and electromagnetically isolated from insecure networks.

Securing the industrial control systems is a complex and even very difficult task because of little attention been paid on it in the past. In light of the growing prevalence of cyber attacks on the computer networks and systems in various infrastructure worldwide, study on the cybersecurity of industrial control systems, especially those used in the critical infrastructures, is of great importance.

Because of the differences between industrial control system and IT system used in business applications, it is difficult to use the IT cybersecurity techniques available directly to tackle the problems within industrial control system. For example, industrial control system may works continuously as long as several years, any modification or updates to the on-line control system may cause unexpected damages to the process and equipments. Countermeasures to mitigate the control system risk should be tested carefully before they were put into use. Therefore, it is important to develop testbed, instead of the real industrial process, for the study of process control system cybersecurity research.

The cybersecurity testbed is used to identify existing industrial control system vulnerabilities, develop vulnerability taxonomies to identify common cybersecurity deficiencies in need of solutions development, and to serve as a platform for validating research cybersecurity solutions which serve industry and government[2]. Testbed offers a low cost means to model industrial control systems and the effects of cyber security attacks on such systems.

Study on testbed within the process control system cybersecurity research community is a hot topic recently. The Idaho National Labs (INL) National SCADA Testbed, supported by Department of Energy, USA, is a large scale testbed dedicated to control system cybersecurity assessment, standards improvement, outreach, and training[3]. The British Columbia Institute of Technology (BCIT) houses a process control system testbed known as the Industrial Instrumentation Process Laboratory. The BCIT lab includes a fully operational distillation column, evaporator, a batch pulp digester, a chemical blending reaction process, and power boiler. The BCIT lab includes a variety of SCADA equipment including Emerson DeltaV and Provox distributed control systems, F&P MC5000 controllers, Foxboro I/A digital control systems, Rockwell PLC-5s, Schnieder 984 and Quantum programmable logic controllers, Honeywell TDC 3000 distributed control systems, Bailey Net90 distributed control system, GE/Fanuc Series 90/70, Series 90/30 programmable logic controllers with Genius I/O, and other field devices, such as valves and measurement instrumentations[4].

Although there are many cybersecurity researches on the industrial control system in the past decade, only a few of them are focused on the control equipments themselves, and even few conclusions are made public. In this paper, we present the design and development of a process control testbed for control system security studies. Since we are eager to investigate the cybersecurity of the widely used control systems, several different programmable logic controllers and distributed control system is adopted in the testbed. Because of the focus of this research being on the real cyber layer, and the advantages associated with simulated process, the simulated Tennessee-Eastman process is adopted in this study.

The rest of the paper is organized as follows. Section II analyzes and summaries the issues with control system test beds for cybersecurity research. Section III presents the details of the development of the control system testbed. Cybersecurity study on the testbed is shown in Section IV. Finally, conclusions are made in Section V.

## II. CONTROL SYSTEM TESTBED FOR CYBERSECURITY

Process control system, which can be regarded as a cyber-physical system(CPS), is consists of cyber layer including control system hardware and software, control and communication network, and physical layer, i.e. the industrial process itself. Therefore, the control system testbed is also consists of cyber layer and physical layer. The cyber layer and physical layer of the testbed can be either real or simulated component, it is reasonable to classify the testbed based on such features. In this sense, three categories of cyber layer and two categories of physical layer implementtations can be identified by now. For cyber layer implementtations the following approaches were found: only real components[5]; hybrid one, i.e. real components combined with simulated ones[6]; and only simulated components[7]. On the other hand, for physical layer implementations, two categories can be found: only real components[8]; and only simulated components[9]. Different approaches possess advantages and disadvantages. For example, testbed in which the cyber layer consisting exclusively of real components provides few experiment management capabilities and is dedicated to specified process, but it is intuitive in display the results when the control system is under attack and can be connected to the control system easily. Furthermore, the cybersecurity problems associated with intelligent field devices, such as measurement instruments, valves can also be tackled. The field bus used in the plant layer can be accessed by invader and through which attack of the control system is possible. As for the hybrid cyber layer proposals, which combine multiple simulation models together with real components, increase the functionalities and flexibility of testbed. But it mainly targeted towards a specific domain such as power transmission and distribution. For the approaches that use simulators for both cyber and physical layers without any real components, its functions is limited due to the diversity and complexity of protocols, systems and architectures. Besides, for the process control system cybersecurity research, investigate the vulnerabilities inhered in the real control components and control system architectures is an urgent and the most important aspect, which is infeasible with such approaches. It is meaningful to develop a testbed with real cyber layer.

As for the simulations of the physical layer, different tools are used because the process features related with the industrial domains closely. For example, Power World, being an interactive package that simulates high voltage power generation and distribution, is widely used in power system. Matlab, a general purpose simulation package, can be used in different domains. There are more simulation packages such as OMNeT++, OPNET and RINSE for the cyber layer simulation. To help the integration of different simulators to construct integrated testbed, some common distributed framework for simulation was proposed. For example, high level architecture (HLA), involved in IEEE 1516 standard, is widely used in a verity of testbeds development.

## III. DEVELOPMENT OF TESTBEDS FOR PROCESS CONTROL SYSTEM CYBERSECURITY RESEARCH

### A. *Description of Tennessee-Eastman Process*

Tennessee-Eastman(TE) chemical process is a testbed widely used in plant-wide control strategy design, multi-variable control, optimization, predictive control, estimation /adaptive control, nonlinear control, process diagnostics and education. The complexity associated with it also makes it suitable for cyber-physical security related studies[10]. The TE chemical plant is a process with 41 measured parameters and 12 manipulated variables. The manipulated variables are the control actions based on the measured parameters to maintain certain operational goals such as constant reactor temperature. The architecture of the TE process includes five main units: a two-phase reactor, a product condenser, a recycle compressor, a vapor/liquid separator and a product stripper. More details on the TE process can be found in the original paper by Downs and Vogel[11].

### B. *Structure of Testbed based on TE Process*

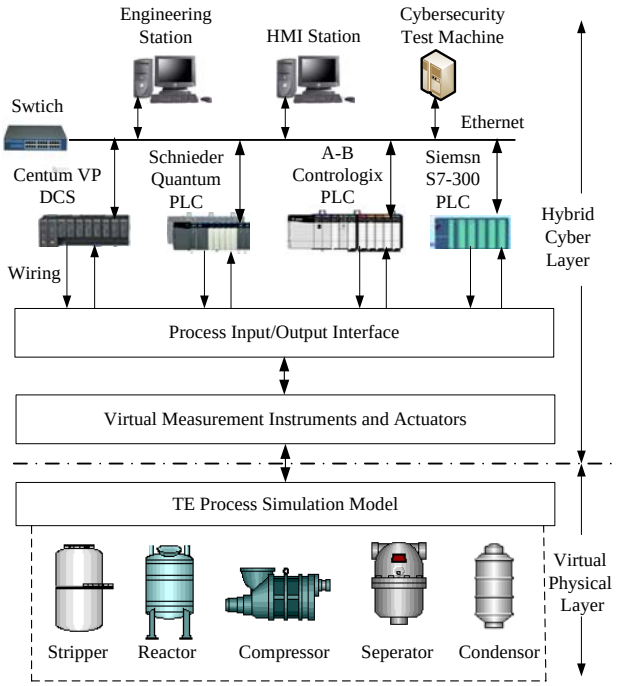


Figure 1. Structure of the proposed hybrid testbed.

In this paper, a hybrid control system testbed based on the TE process is proposed. The structure is shown in Fig.1. The testbed consists of a virtual physical layer, i.e. the simulated TE process, and a hybrid cyber layer including physical control system and virtual measurement instruments and actuators. When simulated models are used, it is difficult

and meaningless to use physical measurement instruments and actuators. It is the reason why the hybrid cyber layer is adopted in our research.

In the proposed testbed, several different industrial control systems, such as SCADA and distributed control system, are adopted in the cyber layer of the testbed in order to study the vulnerabilities existing in these widely used systems. The SCADA equipments include Siemens S7-300 programmable logic controller, Schneider Quantum programmable logic controller, Allen-Bradely Contrologix programmable logic controller, and human machine interface software including GE iFix, Invensys In touch and Wellincontrol Kingview. Yokogawa Centum VP distributed control system, which is used in the process industry worldwide, is also included in the testbed.

### C. Principles of the Testbed

The testbed can be divided into several parts from the bottom to top, i.e. from the physical layer to the cyber layer. Obviously, the TE process simulation model is in the bottom. The interface between the TE process simulation model and the physical control system is in the middle part. On the top are the physical control systems from different vendors. Data flows between the three parts during the operation. Matlab is used to simulate the TE process. The PCI analog input and output cards from Advantech Corporation are used as the interface hardware. The analog output channel of the PCI I/O card is connected to the analog input channel of the programmable logic controllers. The analog input channel of the PCI I/O card is connected to the analog output channel of the programmable logic controllers. During every simulation step, the measured parameters of TE model is send to the programmable logic controller through the analog output channel of PCI I/O card, while the manipulated variable, which is the output of the PID control algorithm running in the programmable logic controller, is obtained from the analog input channel of the PCI I/O card. By this way, the closed-loop control of the TE process by commercial industrial control system is achieved. The simulated process and real control system are integrated into one testbed.

In our testbed, the Matlab simulation program running in the computer where the PCI I/O cards are pluged. Industrial control computer from Advantech Corporation is used because it possesses more PCI slots than the commercial computer. The interface program for the PCI I/O cards in the Matlab simulation environment is developed. It is important to configure the right signal types, i.e. voltage or current and their ranges before connecting the PCI I/O card with the I/O channels of programmable logic controller. To ease the simulation, only part of the manipulated variables and measured parameter was used in the research, and only S7-300 programmable logic controller is used as the control equipment. A full scale simulation of the TE process and more than one controller being used as the control equipments will be the future work.

### D. Human machine interface of the TE process

Human machine interface (HMI) software is widely used by operators in the control center of a control system, especially SCADA system. The HMI software displays the data acquired from programmable logic controllers, remote terminal units and other controllers in the field. It also allows the operator to manipulate parameters, response to alarms, configure the operation environment of the system that is under the operator's supervisory control authority. Typically, the HMI software mimics the look and feel of a tangible control panel, with elements like switches, dials, sliders, readouts, and the process flowchart. The HMI of the testbed is developed with Invensys In touch.

The HMI is the primary access to enter the control system. It runs on the general personal computer with frangible Windows operating system. Vulnerabilities existing in the HMI, communication protocols, operation system, and program software for controller such as Siemens Step 7 are likely to be utilized by the invader. For example, when the communication between the HMI and the controllers is manipulated by the worm, command injection attacks can inject false control and configuration commands into control system. The data displayed on the HMI may be different from the real parameters in the controller when the control system is under attack. The parameters in the HMI are in normal even if the process is abnormal. Therefore the operators are cheated and can make no efforts to prevent the control system from being devastated. By integrating the HMI into the testbed, vulnerabilities existing in the HMI can also be analyzed and evaluated.

## IV. CASE STUDY

Insiders, crackers, internal and external malware, Organized groups (including terrorism and hacktivism) are all among the threats to process control system. Despite many different kinds of attacks can be carried out against process control system, they can be classified in a limited number of categories[8]:

1) *Remote authentication dial in user service denial of dervice (DoS).*
2) *Domain credential stolen/external connection DoS.*
3) *Intranet virus infection.*
4) *Data network worm infection.*
5) *Process network malware infection.*
6) *Phishing attacks and local DNS poisoning.*

One or combination of the attacks above to the control system may destroy the availability, integrity and confidentiality of the system.

In this part we carry out a case study on the cybersecurity research through the process network Modbus worm attack. Modbus worm attack can seize control of the slaves in the process network by exploiting the lack of authentication and integrity mechanisms in the Modbus protocol. To damage the process in relatively short time, the important parameters, such as the minimum/maximum value of parameters/control variables are likely to be the target of the attack. Such kind of attacks may cause the accumulation of products by completely opening valves that feed products into process units, and by completely closing valves that free products from the process units [12].

In the attack scenario, Schneider Quantum programmable logic controller is used to control the simulated TE process. The controller also communicates with the HMI with Modbus/TCP protocol. Assuming the Modbus worm has an access to enter the process network of the targeted testbed. We can use the worm developed to target the registers of the Quantum programmable logic controller. The Modbus worm implemented in this research is a variant of the Modbus DoS worm. After discovering the Quantum programmable logic controller as the infected machine, the worm sends a set of correlated Modbus messages to the machine in order to enforce A/C feed ratio a step change by ten percent while maintaining B composition constant after 8 hours from the start of the TE process simulation.

The operation parameters, reactor pressure and level of the TE process for 48 hours are shown in Fig.2. Although the control system overcomes the action enforced by the attacker and brings the parameters to normal, the effect of the attack on the process is obvious. The process may go to unstable if large step change is made by the attacker. Other scenario can also be enforced on the testbed to show the seriousness of cyber attack.

The attack scenario in this paper requires the attacker having access to the control network and having some prior knowledge of target control system. Nevertheless, it is critical for control engineers, operators and security people to be aware of the cyber threats by this case study.

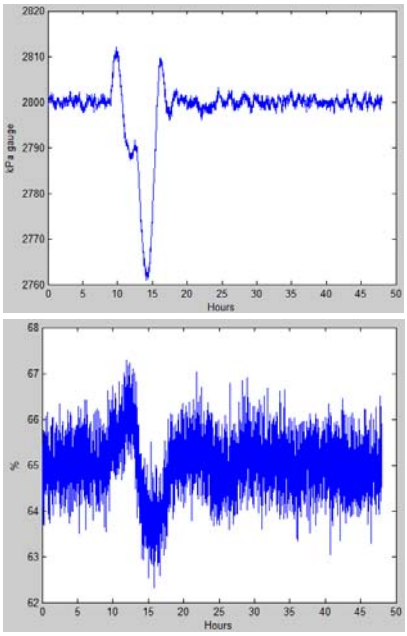


Figure 2. Effects of the attack on reactor pressure and level.

## V. CONCLUSIONS

More and more security incidents happened all over the world indicate the need for developing process control system testbed for conducting security experiments. In this paper, a hybrid testbed integrating both simulated TE process and real industrial control system are presented. The physical part of the testbed can be connected to other control systems easily if cybersecurity of such control system is to be investtigated, which means the testbed is configurable.

We also show the effect of cyber attack on the testbed through the process network Modbus worm attack. By modifying the parameter, the process may be disturbed or even destroyed. This research is based on the real and widely used industrial control system, not the simulated one, which makes our research diverges from other approaches. Currently we are undertaking more attack scenarios on the testbed, and risk assessment, development, and deployment of countermeasures and validation on the testbed are our future work.

## REFERENCES

[1] Y. Peng, C.Q. Chang, F.Xie, Z.H.Dai et al., “Industrial control system cybersecurity research,” Journal of Tsinghua University(Sci & Tech), vol. 52, pp. 1396-1408, 2012.

[2] T. Morris, A. Srivastava, B. Reaves et al., “A control system testbed to validate critical infrastructure protection concepts,” International journal of critical infrastructure protection, vol. 4, pp. 88–104, 2011.

[3] Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program, Idaho National Laboratory, IdahoFalls, Idaho83415, November, 2008. http://www.inl.gov/scada/publications/d/inl_nstb_common_vulnerabilities.pdf.

[4] Industrial Instrumentation Process Lab. http://www.bcit.ca/applied-research /tc/facilities/industrial.shtml

[5] I. N. Fovino, M. Masera, L. Guidi and G. Carpi, “An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants,”. 3rd Conference on human system interactions (HSI), 2010; pp. 679–86.

[6] W. Chunlei, F. Lan and D. Yiqi, “A simulation environment for SCADA security analysis and assessment,” Proceedings of the 2010 international conference on measuring technology and mechatronics automation; 2010, pp. 342–349.

[7] C. Davis, J. Tate, H. Okhravi et al., “SCADA cyber security testbed development,” Power Symposium, 2006. NAPS 2006, 38th North American, 2006, pp. 483–488.

[8] I. N. Fovinoa, L. Guidib. M. Maseraa and A. Stefaninia, “Cyber security assessment of a power plant,” Electric Power Systems Research, vol.81, pp. 518–526, 2011.

[9] D. Nicol, C. Davis and T. Overbye, “A testbed for power system security evaluation,” International Journal of Information and Computer Security, vol.3, pp. 114-131, 2009.

[10] B. Genge, C. Siaterlis, I. N. Fovino and M. Masera, “A cyber-physical experimentation environment for the security analysis of networked industrial control systems,” Computers and Electrical Engineering, vol.38, pp.1146-1161, 2012.

[11] J. Downs and E. Vogel, “A plant-wide industrial process control problem,” Comput Chem Eng, 1993, vol.17, pp. 245–255.

[12] A. Cárdenas, S. Amin, Z. Lin et al., “Attacks against process control systems: risk assessment, detection, and response,” Proc. the 6th ACM symposium on information, computer and communications security, 2011, pp. 355–366.