Chapter 6

AN INDUSTRIAL CONTROL SYSTEM TESTBED BASED ON EMULATION, PHYSICAL DEVICES AND SIMULATION

Haihui Gao, Yong Peng, Zhonghua Dai, Ting Wang, Xuefeng Han, and Hanjing Li

Abstract This paper demonstrates the utility of an industrial control system testbed that incorporates a universal, realistic, measurable, controllable and reusable experimental platform for cyber security research and testing. The testbed has a layered architecture that leverages physical devices and emulation and simulation technologies. The testbed enables researchers to create experiments of varying levels of fidelity for vulnerability discovery, product evaluation and system certification. The utility of the testbed is demonstrated via a case study involving an industrial boiler control system.

Keywords: Industrial control systems, cyber security, testbed, simulation

1. Introduction

Industrial control systems (ICSs) monitor and control processes in critical infrastructure assets [12]. Due to their increased connectivity with corporate networks and the Internet, industrial control systems are no longer immune to cyber attacks. Indeed, in 2010, the Stuxnet worm demonstrated to the world the seriousness of industrial control system vulnerabilities and the potential threats [9].

In order to protect industrial control systems, it is important to conduct cyber security research and testing to identify and mitigate existing vulnerabilities [1, 7]. However, testing and evaluation of actual industrial control systems are difficult to perform due to the uptime requirements and the risk of damage to operational systems. Therefore, it is necessary to build suitable experimental platforms to develop and test cyber security solutions for industrial control systems [9].

J. Butts and S. Shenoi (Eds.): Critical Infrastructure Protection VIII, IFIP AICT 441, pp. 79–91, 2014.

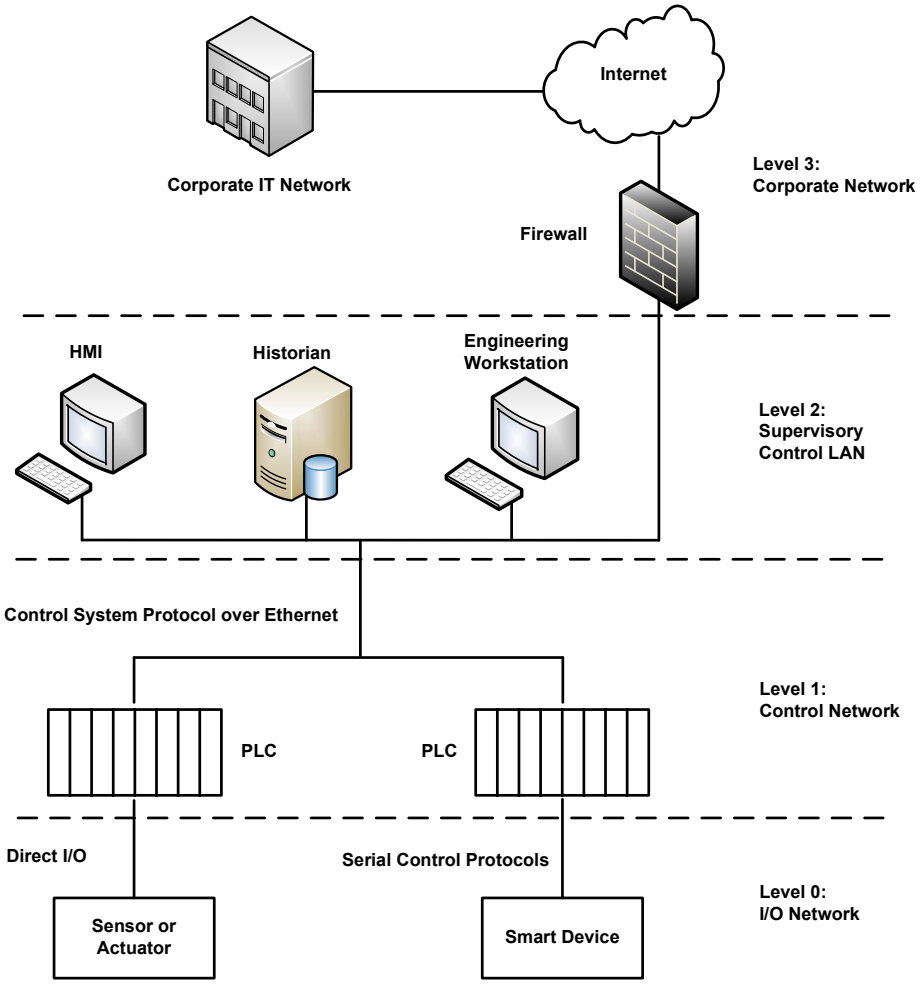

Figure 1. Industrial control system reference model.

The emulation, physical devices and simulation for industrial control systems (EPS-ICS) testbed presented in this paper seeks to address this problem. The testbed provides configurable fidelity using physical devices for core system components, while emulating or simulating the other components. The proposed solution is an inexpensive, albeit useful, approximation of an industrial control system environment. Indeed, the EPS-ICS testbed strikes the right balance between research requirements and construction costs.

2. Architecture

Figure 1 shows an example industrial control system reference model that conforms to the ANSI/ISA-99 standard [5]. The architecture is segmented into

four levels: (i) corporate network; (ii) supervisory control local area network (LAN); (iii) control network; and (iv) input/output (I/O) network.

In the ANSI/ISA-99 standard, the corporate network level (Level 3) is responsible for management and related activities (e.g., production scheduling, operations management and financial transactions) [11]. This level is consistent with traditional information technology, including the general deployment of services and systems such as FTP, websites, mail servers, enterprise resource planning (ERP) systems and office automation systems. The supervisory control LAN level (Level 2) includes the functions involved in monitoring and controlling physical processes and the general deployment of systems such as human-machine interfaces (HMIs), engineering workstations and historians. The control network level (Level 1) includes the functions involved in sensing and manipulating physical processes. Typical devices at this level are programmable logic controllers (PLCs), distributed control systems, safety instrumented systems and remote terminal units (RTUs). The I/O network level (Level 0) includes the actual physical processes and sensors and actuators that are directly connected to process equipment.

3. Testbed Construction

Industrial control system testbeds may be categorized as:

- Physical testbeds that are constructed using replication methodologies.
- Software (virtual) testbeds that are constructed using modeling methodologies.
- Hybrid testbeds that are constructed using replication and modeling methodologies.

A replicated testbed is a copy of a real system with the same physical devices and information systems. An example is the National SCADA Testbed (NSTB) of the U.S. Department of Energy [8]. Although a replicated architecture provides the highest fidelity, building an identical replica of a real-world system is usually cost prohibitive.

A software testbed uses modeling methodologies instead of actual physical devices; it typically includes a physical process simulator, network simulator and attack simulator. Such a testbed is a low cost solution for research focused on attacks on industrial control systems and the development of security strategies. However, due to the absence of real components and devices, the architecture provides low fidelity.

A hybrid testbed incorporates replicated devices and systems as well as software models. The architecture provides a high degree of fidelity and is also cost effective. The EPS-ICS testbed described in this paper is based on a hybrid architecture.

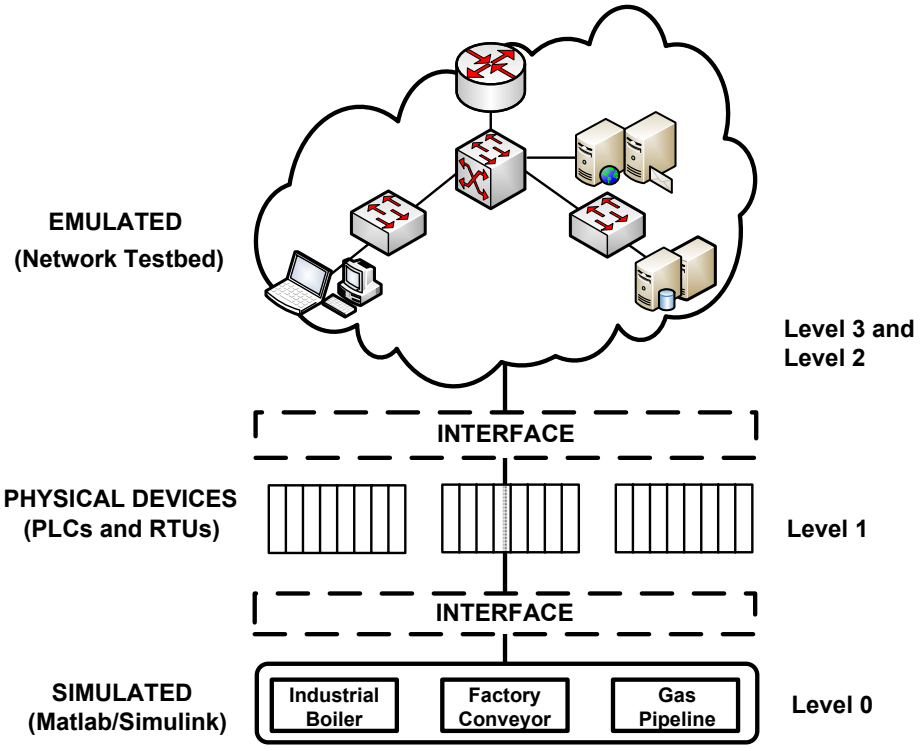

Figure 2. EPS-ICS testbed architecture.

4. EPS-ICS Testbed Architecture

Figure 2 shows the EPS-ICS testbed architecture. The architecture has four types of components: (i) emulated components; (ii) physical components; (iii) simulated components; and (iv) interface components. The industrial control system of interest is modeled as a single testbed comprising emulated, physical and simulated devices. Levels 2 and 3 of the ANSI/ISA-99 industrial control system reference model are implemented using emulation technologies similar to Emulab [2]. Level 1 of the reference model is implemented by replicating physical devices while Level 0 is implemented using simulated mathematical models of controlled processes developed with Matlab/Simulink.

Figure 3 shows the EPS-ICS network architecture. It is a dynamically controlled construct, consisting of a measurable and reusable experimental environment with switches, servers and other physical resources. The hardware includes wired and wireless nodes. Note that the testbed effectively models a corporate network (Level 3) and supervisory control LAN (Level 2).

The Level 1 control network is the core of the industrial control system reference model. The EPS-ICS testbed incorporates physical devices in Level 1 to achieve high fidelity for research and testing requirements.

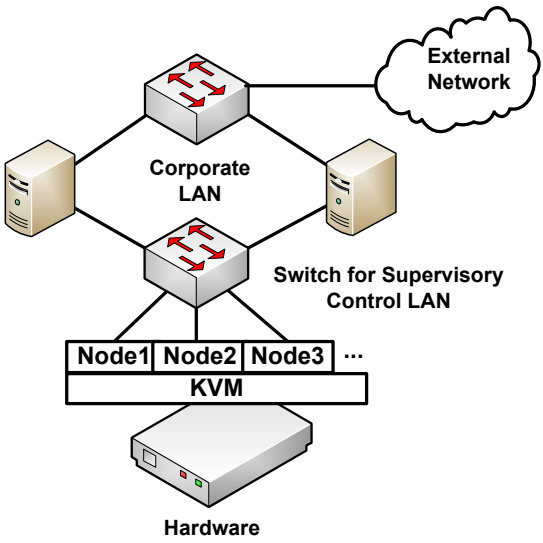

Figure 3. EPS-ICS network architecture.

The testbed uses Matlab/Simulink to construct Level 0 models in order to reduce costs and reuse I/O layer components. This flexibility enables the testbed to model a variety of controlled processes (e.g., steam boiler, storage tank and heat exchanger).

The EPS-ICS testbed effectively replicates the interactions between industrial control system components. Industrial control system components, such as the corporate network and supervisory control LAN, may be implemented as emulations or as physical components using the testbed interface. Thus, the EPS-ICS testbed can provide varying levels of fidelity to meet diverse research and testing objectives.

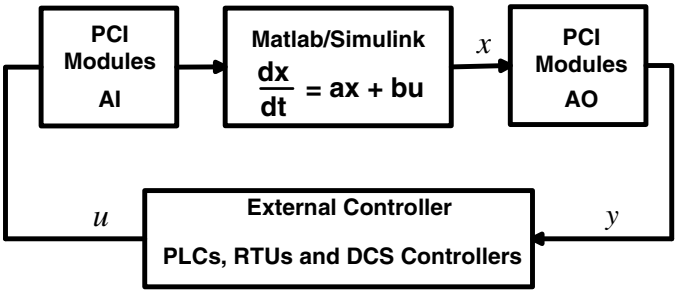

Figure 4. Interfaces between physical and simulated devices.

Interfaces between emulated and physical devices implement communications using IP routing (e.g., routers, layer-three switches and wired/wireless networks). Figure 4 shows interface communications between physical and

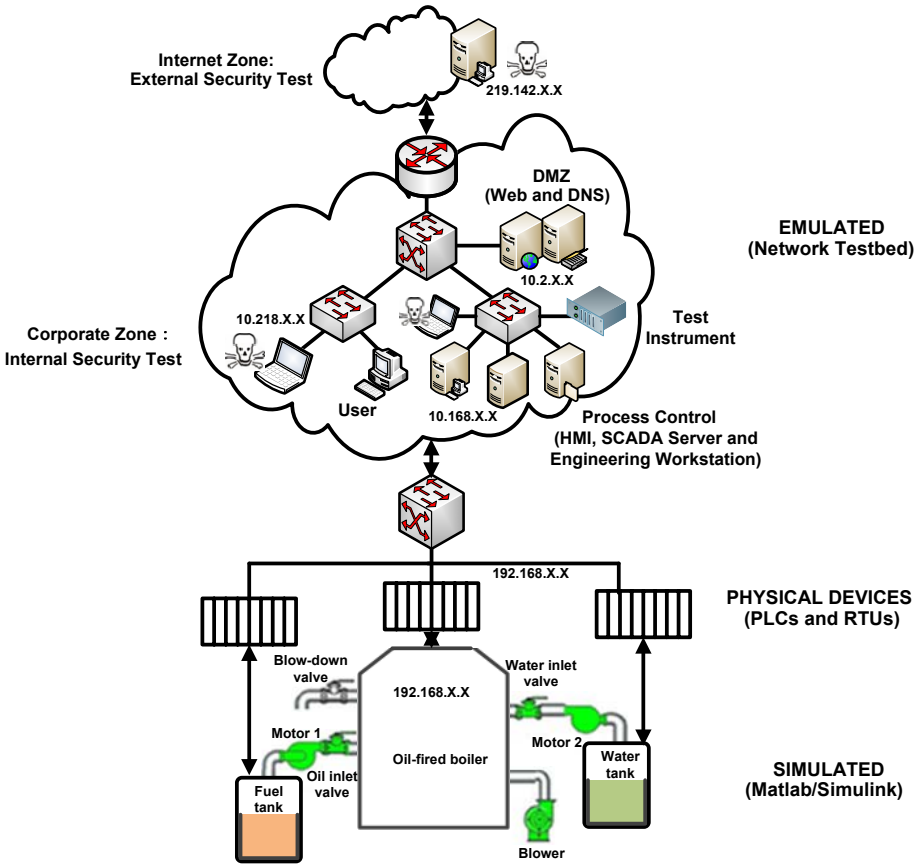

Figure 5. Industrial boiler control system based on the EPS-ICS testbed.

simulated devices; special hardware between the devices enables data exchange. Peripheral component interconnect (PCI) modules support full communications between Matlab/Simulink models and external controllers.

5. Experimental Setup and Results

This section shows how an industrial boiler control system is constructed using the EPS-ICS testbed.

5.1 Corporate and Control Networks

Figure 5 shows the experimental industrial boiler control system. The computers in the corporate zone are used to simulate daily office activities and internal security testing. The Internet zone is used for external security testing. Web servers and external DNS servers are deployed in the demilitarized zone

(DMZ) for external communications (e.g., Internet connectivity). HMI servers, SCADA servers and other production systems are deployed in the process control zone; they interact with field devices (e.g., PLCs). The process control functionality is represented by physical and simulated devices corresponding to the boiler system.

5.2 Industrial Boiler Control System Model

A Matlab/Simulink simulation model was developed by performing a comprehensive engineering analysis of an industrial oil-fired boiler. The control of the oil-fired boiler simulation model is achieved by integrating PLCs and RTUs in the industrial control network. The following sections describe the mathematical models of the furnace, boiler drum, riser, downcomer and superheater [3, 4, 10].

Furnace Model. The mass balance, energy balance and furnace radiation heat transfer equations are:

$$\dot{m}_f + \dot{m}_a - \dot{m}_g = V_f \frac{d}{dt}(\rho_g) \tag{1}$$

$$\dot{m}_f Q_f + \dot{m}_a h_a - \dot{m}_g h_g - Q_{rht} = V_f \frac{d}{dt}(\rho_g h_g) \tag{2}$$

$$Q_{rht} = \alpha_{hd} \sigma \psi F_l T_g^4 \xi \tag{3}$$

where $\dot{m}_f$ is the fuel flow into the furnace, Q_f is the fuel heat, $\dot{m}_a$ is the air flow into the furnace, h_a is the air enthalpy, $\dot{m}_g$ is the gas flow out of the furnace, h_g is the gas enthalpy, Q_{rht} is the radiation heat transfer, V_f is the furnace volume, ρ_g is the gas density, σ is the Boltzmann black body radiation constant, α_{hd} is the furnace emissivity, ψ is the furnace water degree, ξ is the fouling factor, T_g is the gas temperature and F_l is the furnace area.

Boiler Drum Model. The upper section of the boiler drum contains steam and the bottom section contains water. The liquid zone mass conservation, vapor zone mass conservation, drum energy balance and drum liquid level equations are:

$$\dot{m}_w + (1-x)\dot{m}_{rc} - \dot{m}_{dcin} - \dot{m}_{pw} - \dot{m}_{ec} = \frac{d}{dt}(\rho_w V_d^w) \tag{4}$$

$$\dot{m}_{rc} x - \dot{m}_s + \dot{m}_{ec} = \frac{d}{dt}(\rho_s V_d^s) \tag{5}$$

$$\dot{m}_w h_w + (1-x)\dot{m}_{rc} h_w + x\dot{m}_{rc} h_s - \dot{m}_{dcin} h_w - \dot{m}_s h_s - \dot{m}_{pw} h_w$$
$$= \frac{d}{dt}(\rho_s V_d^s h_s + \rho_w V_d^s h_w + M_{dm} C_{dm} T_d) - J V_d \frac{d}{dt}(P_d) + \dot{m}_{ec} h_s \quad (6)$$

$$V_d^w = \frac{1}{3}\pi L_v^2 (3r - L_v) + \frac{1}{2}(L-2r) r^2 (\theta - \sin\theta) \quad (7)$$

$$\theta = 2\cos^{-1}\left(\frac{r-L}{r}\right) \quad (8)$$

where $\dot{m}_w$ is the feed water flow from the economizer, x is the steam dryness, $\dot{m}_{rc}$ is the steam-water flow in the riser, $\dot{m}_{dcin}$ is the downcomer inlet flow, $\dot{m}_{pw}$ is the blow-down flow, $\dot{m}_{ec}$ is the dynamic evaporation flow, ρ_w is the saturated water density, V_d^w is the drum liquid zone volume, $\dot{m}_s$ is the steam discharge capacity, ρ_s is the steam density, V_d^s is the drum vapor zone volume, h_w is the feed water enthalpy from the economizer, h_s is the steam enthalpy, M_{dm} is the drum metal quality, C_{dm} is the drum metal specific heat capacity, T_d is the drum temperature, J is the unit conversion factor, V_d is the drum volume, P_d is the drum pressure, L is the drum length, r is the drum radius and $L_v = f^{-1}(V_d^w)$ is the drum liquid level.

Riser Model. The riser contains both liquid and vapor. The liquid zone mass conservation, vapor zone mass conservation, energy balance, metal energy balance, average ratio of vapor per cross-sectional area in the vapor zone, liquid zone accounted for in the riser length ratio, and steam volume in the riser equations are:

$$\dot{\mathrm{m}}_{dcout} - (1-x)\dot{m}_{rc} - \dot{m}_{evp} - \dot{m}_{ecl} = \frac{d}{dt}(\rho_w V_{rc}^w) \quad (9)$$

$$\dot{m}_{ecl} + \dot{m}_{evp} - x\dot{m}_{rc} = \frac{d}{dt}(\rho_s V_{rc}^s) \quad (10)$$

$$\dot{m}_{dcout} h_{dcout} - (1-x)\dot{m}_{rc} h_w - x\dot{m}_{rc} h_s + Q_{rc} =$$
$$\frac{d}{dt}(\rho_s V_{rc}^s h_s + \rho_w V_{rc}^w h_w) - J V_{rc} \frac{d}{dt}(P_d) \quad (11)$$

$$Q_{rht} - Q_{rc} = M_{mrc} C_{mrc} \frac{d}{dt}(T_{mrc}) \quad (12)$$

$$\varphi_{rc} = \frac{k}{1 + \frac{\rho_s}{\rho_w}(\frac{1}{x_s} - 1)} \tag{13}$$

$$\gamma_{rc} = \frac{\dot{m}_{dcout}(h_w - h_{dcout})}{Q_{rc}} \tag{14}$$

$$V_{rc}^s = V_{rc}(1 - \gamma_{rc})\varphi_{rc} \tag{15}$$

where $\dot{m}_{dcout}$ is the downcomer outlet water flow, $\dot{m}_{evp}$ is the evaporation generated by heat absorption, $\dot{m}_{ecl}$ is the dynamic evaporation flow, V_{rc}^w is the water volume in the riser, Q_{rc} is the medium heat in the riser, h_{dcout} is the medium enthalpy at the downcomer outlet, V_{rc}^s is the steam volume in the riser, V_{rc} is the riser volume, M_{mrc} is the riser metal mass, C_{mrc} is the riser metal specific heat capacity, T_{mrc} is the riser metal temperature, φ_{rc} is the liquid zone steam section ratio in the ascending pipe and x_s is the average steam dryness in the vapor zone.

Downcomer Model. The downcomer preheats the water supply and returns cool water to the bottom of the drum. The energy balance equation is:

$$\dot{\mathrm{m}}_{dcin} h_{dcin} - \dot{m}_{dcout} h_{dcout} = \frac{d}{dt}(\rho_w V_{dc} h_{dcout} + M_{mdc} C_{mdc} T_{mdc}) \tag{16}$$

where $\dot{m}_{dcin}$ is the inlet water flow, $\dot{m}_{dcout}$ is the outlet water flow, h_{dcin} is the inlet water enthalpy, h_{dcout} is the outlet water enthalpy, V_{dc} is the volume, M_{mdc} is the metal quality, C_{mdc} is the metal specific heat capacity and T_{mdc} is the metal temperature at the downcomer.

Superheater Model. The superheater increases the thermal energy. The mass balance and energy balance equations are:

$$\dot{\mathrm{m}}_{sin} - \dot{m}_{sout} = V_{sh} \cdot \frac{d\bar{\rho}_s}{dt} \tag{17}$$

$$\mathrm{Q_g} - \mathrm{M_{msh}} \cdot C_{msh} \cdot \frac{dT_{msh}}{dt} + \dot{m}_{\mathrm{sin}} \cdot h_{\mathrm{sin}} - \dot{m}_{sout} \cdot h_{sout} = V_{sh} \cdot \frac{d(\bar{\rho}_s \cdot \bar{h}_s)}{dt} \tag{18}$$

where $\dot{m}_{sin}$ is the inlet steam flow, $\dot{m}_{sout}$ is the outlet steam flow, V_{sh} is the superheater volume, $\bar{\rho}_s$ is the inlet and outlet average steam density, Q_g is the heat release of the gas, M_{msh} is the superheater metal mass, C_{msh} is the superheater metal specific heat capacity, T_{msh} is the superheater metal

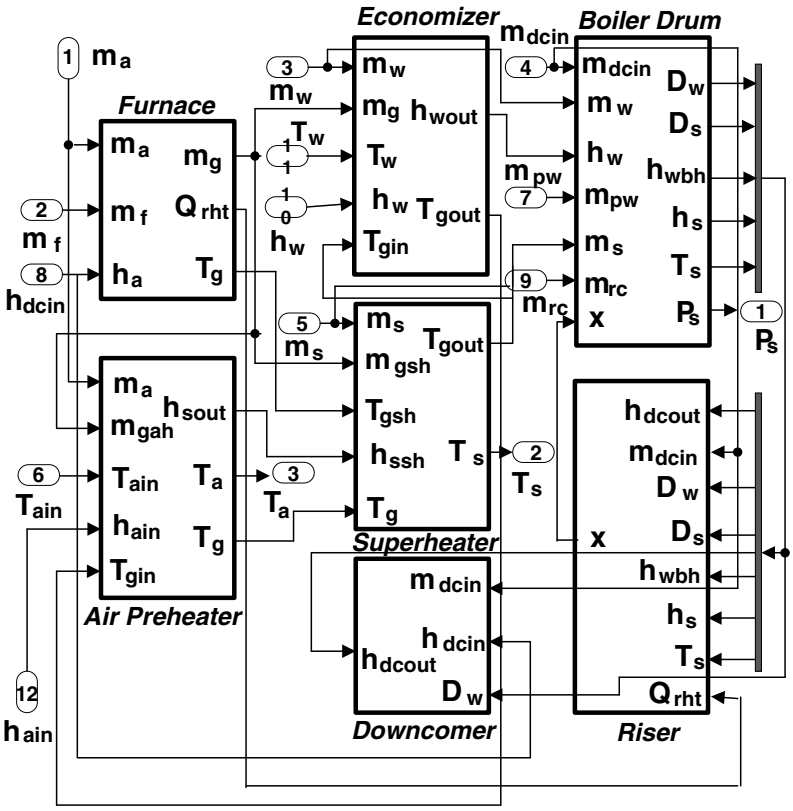

Figure 6. Simulation model of the oil-fired boiler.

temperature, h_{sin} is the inlet steam enthalpy, h_{sout} is the outlet steam enthalpy and $\bar{h}_s$ is the inlet and outlet average steam enthalpy.

Figure 6 shows the oil-fired boiler simulation model implemented using Matlab/Simulink. The boiler simulation model interacts with external controllers. The resulting EPS-ICS testbed can be used for cyber security research and testing.

5.3 Device Evaluation and Certification

Devices that are to be evaluated and certified interact with the EPS-ICS testbed via a network interface or TAP device using Layer 2 access. Table 1 shows some common testing devices that can interact with the EPS-ICS testbed [13].

Researchers can select three EPS-ICS access points for testing: (i) Internet zone; (ii) corporate zone; and (iii) process control zone. Figure 7 shows an example attack path that includes man-in-the-middle, denial-of-service and replay attacks. Table 2 lists the potential outcomes of and assessment [6].

Table 1. Common testing devices [13].

Tool	Availability	Certification	Critical Techniques
Achilles	Commercial	Achilles Certification	Fuzzing, Storm, Monitor
Mu-8000	Commercial	MUSIC Certification	Fuzzing, Monitor
Defensics	Commercial	None	Fuzzing
BreakPoint	Commercial	None	Fuzzing, Storm
beSTORM	Commercial	None	Fuzzing
Sully	Free	None	Fuzzing

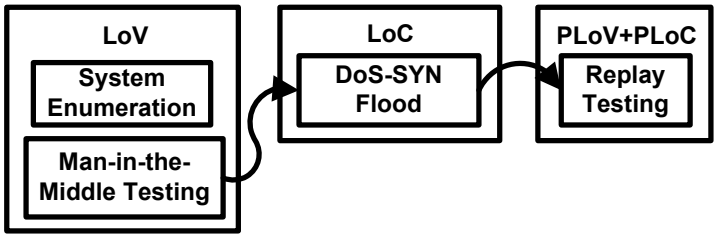

Figure 7. Test procedures and results.

Table 2. Description of vulnerabilities [6].

Terms	Device Under Test (DUT)
Loss of View (LoV)	DUT network stack no longer sends or processes legitimate network traffic
Loss of Control (LoC)	DUT process control functionality is disrupted
Permanent Loss of View (PLoV)	Loss of view persists; manual intervention is required to return DUT to normal state
Permanent Loss of Control (PLoC)	Loss of control persists; manual intervention is required to return DUT to normal state

The first step in the assessment is system discovery, which identifies information assets, operating system types, service ports and running applications. The second step involves a man-in-the-middle attack that tampers with the data transmitted between host computers and end devices. The third step involves a denial-of-service (SYN flood) attack that consumes end device resources. The fourth step involves a replay attack that bypasses password protection, uploads and modifies an end device program and disrupts system execution. Figure 8 shows the results of the assessment.

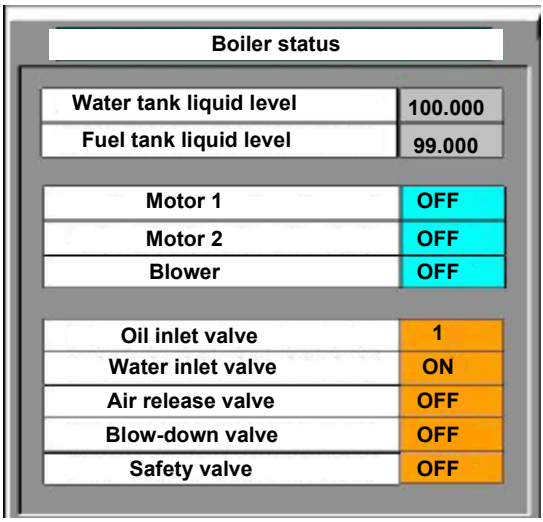

Figure 8. Assessment results.

6. Conclusions

The EPS-ICS testbed presented in this paper is designed specifically for industrial control system security research and testing. It seamlessly integrates emulation, physical device and simulation technologies to strike the right balance between fidelity and construction costs. The industrial boiler control system case study demonstrates the application and utility of the EPS-ICS testbed for industrial control system evaluation and certification. Future research will focus on the continued refinement of the EPS-ICS testbed, which will involve developing new monitoring and analysis techniques, expanding the applicability of the testbed and constructing a complementary cyber-physical testbed.

References

[1] M. Brandle and M. Naedele, Security for process control systems: An overview, *IEEE Security and Privacy*, vol. 6(6), pp. 24–29, 2008.

[2] Flux Research Group, Emulab, Total Network Testbed, School of Computing, University of Utah, Salt Lake City, Utah (`www.emulab.net`), 2014.

[3] M. Flynn and M. 0'Malley, A drum boiler model for long term power system dynamic simulation, *IEEE Transactions on Power Systems*, vol. 14(1), pp. 209–217, 1999.

[4] H. Gan, J. Zhang and H. Zeng, Development of main boiler simulation system for LNG ship, *International Journal of Advancements in Computing Technology*, vol. 4(17), pp. 466–475, 2012.

[5] International Society of Automation, Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts and Models, ANSI/ISA-62443-1-1 (99.01.01)-2007, Research Triangle Park, North Carolina, 2007.

[6] N. Kube, K. Yoo and D. Hoffman, Automated testing of industrial control devices: The Delphi database, *Proceedings of the Sixth International Workshop on Automation of Software Testing*, pp. 71–76, 2011.

[7] A. Neves Bessani, P. Sousa, M. Correia, N. Ferreira Neves and P. Verissimo, The CRUTIAL way of critical infrastructure protection, *IEEE Security and Privacy*, vol. 6(6), pp. 44–51, 2008.

[8] Office of Electricity Delivery and Energy Reliability, National SCADA Test Bed, Department of Energy, Washington, DC (`energy.gov/oe/technology-development/ energy-delivery-systems-cybersecurity/national-scada-test-bed`), 2014.

[9] C. Queiroz, A. Mahmood, J. Hu, Z. Tari and X. Yu, Building a SCADA security testbed, *Proceedings of the Third International Conference on Network and System Security*, pp. 357–364, 2009.

[10] H. Rusinowski, M. Szega and A. Milejski, Mathematical model of the CFB boiler co-fired with coal and biomass, *Proceedings of the Thirteenth International Carpathian Control Conference*, pp. 604–607, 2012.

[11] M. Schwartz, J. Mulder, J. Trent and W. Atkins, Control System Devices: Architectures and Supply Channels Overview, Sandia Report SAND2010-5183, Sandia National Laboratories, Albuquerque, New Mexico, 2010.

[12] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2013.

[13] W. Zhao, Y. Peng, Y. Gao, X. Han, H. Gao and W. Wang, Security testing methods and techniques of industrial control devices, *Proceedings of the Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 433–436, 2013.