Cybersecurity Test-Bed for IEC 61850 based Smart Substations

Y. Yang[1], H. T. Jiang[1], K. McLaughlin[2], L. Gao[1], Y.B. Yuan[1], W. Huang[1], S. Sezer[2]
(1. Jiangsu Electric Power Company Research Institute, Nanjing, China, yyang09@qub.ac.uk;
2. Centre for Secure Information Technologies (CSIT), Queen's University Belfast, Belfast, UK)

***Abstract*—With the development and deployment of IEC 61850 based smart substations, cybersecurity vulnerabilities of supervisory control and data acquisition (SCADA) systems are increasingly emerging. In response to the emergence of cybersecurity vulnerabilities in smart substations, a test-bed is indispensable to enable cybersecurity experimentation. In this paper, a comprehensive and realistic cyber-physical test-bed has been built to investigate potential cybersecurity vulnerabilities and the impact of cyber-attacks on IEC 61850 based smart substations. This test-bed is close to a real production type environment, and has the ability to carry out end-to-end testing of cyber-attacks and physical consequences. A fuzz testing approach is proposed for detecting IEC 61850 based intelligent electronic devices (IEDs) and validated in the proposed test-bed.**

***Index Terms*—Smart Substation, IEC 61850, Cybersecurity, Test-bed, Fuzz testing**

I. Introduction

IEC 61850 [1] based smart substations have played a significant role in power system operation, becoming increasingly complex and interconnected as state-of-the-art information and communication technologies (ICT) are adopted. The increased complexity and interconnection of supervisory control and data acquisition (SCADA) systems have exposed them to a wide range of cybersecurity threats. These threats are not only external, such as terrorists, hackers, competitors, or industrial espionage, but also from internal entities, such as ex-employees, disgruntled employees, vendor personnel for maintenance and troubleshooting, and site engineers. In practice, a threat actor may gain unauthorized cyber access to SCADA systems, exploit vulnerabilities and thereafter launch elaborate attacks which may lead to catastrophic physical damage.

Although the IEC 62351 standard [2] has provided a framework for the cybersecurity design of the IEC 61850 protocol, problems remain and major manufacturers do not generally implement adequate security in their intelligent electronic devices (IEDs) [3]. In recent years, during the construction of smart substations, utilities and manufacturers have paid more attention to the interoperation of devices and implementation of functions, than to cybersecurity consideration and testing. Nevertheless, research on the cost-effective cybersecurity for IEC 61850 based smart substations is still at an early stage. Much more in-depth investigation and analysis of specific vulnerabilities and cyber-attacks is required. To this end, this paper proposes a comprehensive and realistic SCADA-specific cyber-physical test-bed to investigate potential vulnerabilities using simulated cyber-attacks. This test-bed environment meets this challenge by enabling real attack scenarios to be analyzed, and effective cybersecurity countermeasure technologies to be proposed and evaluated for the smart substation cyber domain.

II. Background

A. IEC 61850

IEC 61850 is an international standard for the design of electrical substation automation, which is developed by international electrotechnical commission (IEC) technical committee 57 (TC57). The abstract data models defined in IEC 61850 can be mapped to many protocols. Current mappings in this standard are mainly to manufacturing message specification (MMS), generic object oriented substation event (GOOSE), and sampled measure values (SMV) [4], [5]. The MMS protocol is applied in the substation level based on the Client/Server mode, which runs over TCP/IP networks. The GOOSE and the SMV protocols are both based on publish/subscription mechanism in substation local area networks (LANs) using high speed switched Ethernet. The IEC 61850 protocol stack is shown in Fig. 1. In terms of the transport layer in Fig. 1, international standards organization (ISO) transport (ISO/IEC 8073) means connection oriented transport protocol (COTP), and RFC 1006 stands for ISO transport services on top of the TCP (TPKT) (The TCP port for TPKT traffic is 102).

B. Fuzz Testing

In conventional IT security, fuzz testing [6] is regarded as one of the most useful techniques in finding vulnerabilities of software and protocol implementations [7]. In protocol fuzzing, a fuzzer sends virtually unlimited test cases using invalid or falsely manipulated data, within the framework defined by a given protocol specification, to a protocol

This work was supported in part by Natural Science Foundation of Jiangsu Province under Grant Number BK20140114, and the European FP7 project SPARKS.

978-1-4673-8040-9/15/$31.00 ©2015 IEEE

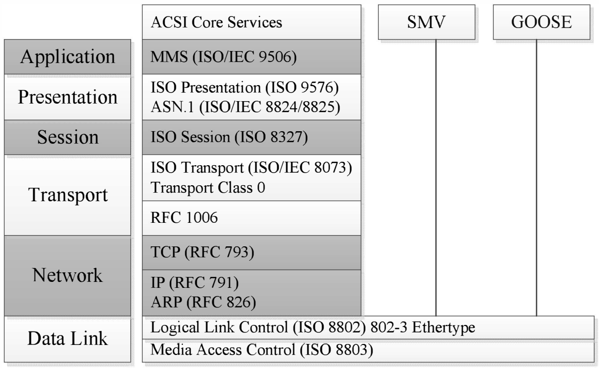


Figure 1. IEC 61850 protocol stack

implementation. Using effective test cases as input information enables security vulnerabilities to be found in the application, which were not anticipated by the protocol designers or software developers. Therefore, fuzz testing is an effective approach to improve the security and reliability of protocol implementations [8].

III. Investigation on Cybersecurity in IEC 61850 based Smart Substations

A. *Cyber-Physical Test-Bed*

In order to investigate potential cybersecurity vulnerabilities in IEC 61850 based smart substations, a cyber-physical test-bed has been built, as shown in Fig. 2. The test-bed consists of the simulation level, process level, bay level and substation level. In the simulation level, a real time digital simulator (RTDS) is utilized to model multiple power system scenarios and simulate transient characteristics and behaviors of modelled power systems. A universal relay test set and commissioning tool, as a programmable voltage and current source, is an optional simulator to realize steady and transient simulation. In the process level, merging units (MUs) are connected in the SV/IEEE1588 network, and intelligent terminals (ITs) are connected in the GOOSE/IEEE1588 network. The process level networks are Ethernet switch-based fiber-optic networks. The bay level IEDs include relays, measure-control devices, fault recorder, network analyzer, and time synchronization IED. The bay level IEDs are connected in the process level networks and the substation level network. The substation level consists of the monitoring system, engineering workstation, SCADA database, remote terminal unit (RTU), and a laptop to launch cyber-attacks. The substation level network, a switch-based cable network, supports MMS, GOOSE and simple network time protocol (SNTP). The control center communicates with the smart substation using IEC 60870-5-104.

B. *Investigation of Cyber-Attacks in the Smart Substation*

In the test-bed, a number of cyber-attacks are simulated and investigated as follows,

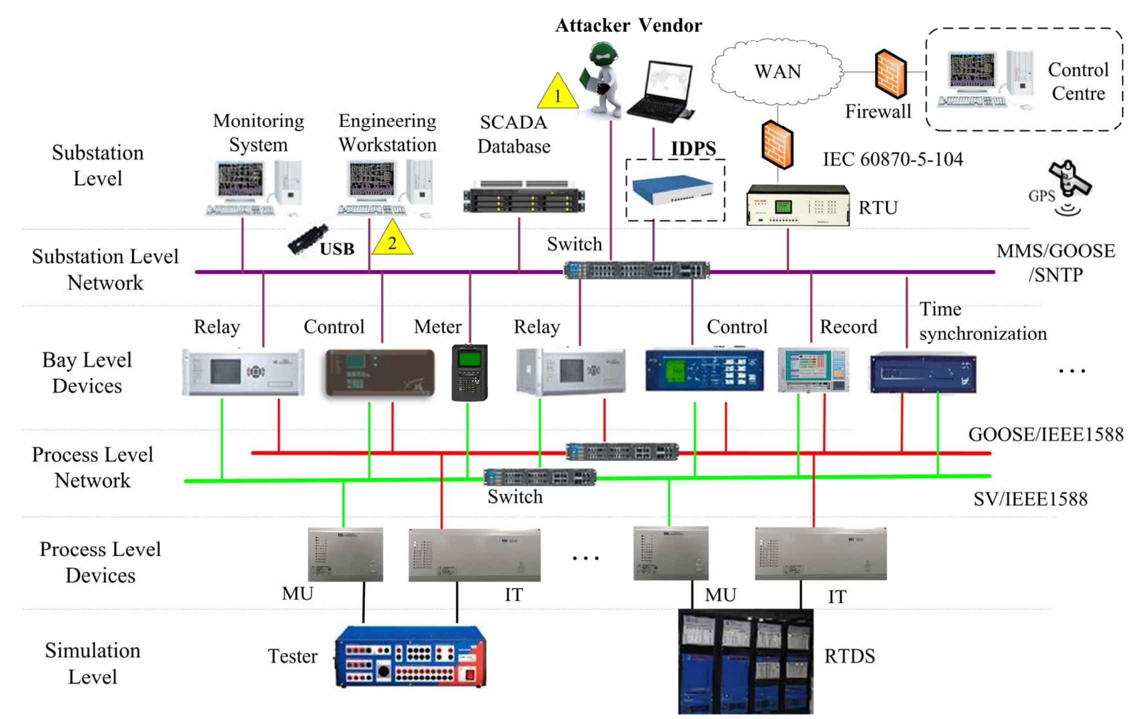


Figure 2. Cyber-physical test-bed of IEC 61850 based smart substation

1) Reconnaissance attack: A reconnaissance attack allows an attacker to identify potential targets before attacking. In this test-bed, the reconnaissance attack is launched by the laptop, as shown by the yellow triangle with the number 1 in Fig. 2, to obtain the online IED information such as IP addresses. An attacker could utilize this information to launch more effective attacks.

2) Malformed packet attack: In this test-bed, malicious IEC 61850 client software generates malformed packets based on the IEC 61850 protocol and sends them to IEDs. The malformed packet may crash the IEC 61850 protocol stack and cause IED communication failure or status exception, which could threaten secure and reliable operation of the smart substation.

3) DoS attack: This DoS attack is launched to occupy all the enable report control blocks of IEDs, which are instantiated at configuration time in the Logical Node (LN) in this test-bed. The targeted IED cannot respond to normal connection requests.

4) Address resolution protocol (ARP) spoofing attack: In the test-bed environment, an ARP spoofing attack [9] is launched by the laptop to broadcast ARP packets with the IP address of the monitoring system in the substation level network. After the attack, the IEDs communicate with the malicious laptop, rather than the monitoring system.

5) Man-in-the-middle (MITM) attack: The MITM attack allows an attacker to redirect communication traffic between the monitoring system and the IED to the malicious laptop in the substation level network [9]. On one hand the attacker sends malicious remote control commands and modified protective setting values by impersonating the monitoring system, on the other hand the attacker, the impersonated IEDs, sends false, abnormal, or even malformed messages to the original monitoring system. In this test-bed environment, the MITM attacks can make the monitoring system and the IEDs abnormal, and even make the grid failure possible.

6) Configuration tampering: SCL files are the foundations of the secure, steady, reliable operations of IEC 61850 based smart substations. In this test-bed, the threat actor has tampered with the configured IED description (CID) file in the protection relay, and the relay operates incorrectly when simulated grid faults appear.

7) Operation system/database attack: The operation system/database is exploited using known vulnerabilities in this test-bed. For example, *VxWorks*, the embedded real-time operating system in some IEDs, is attacked using the wind river debug vulnerability (WDV).

The possible effects of the cyber-attacks on smart substations, as outlined above, are shown in Table I.

TABLE I. THE IMPACT OF CYBER-ATTACKS ON SMART SUBSTATIONS

Cyber-attack Impact	*2)*	*3)*	*4)*	*5)*	*6)*	*7)*
Failure to tripping protection				✘	✘	
Unwanted operation of protection				✘	✘	
Blocking protection				✘	✘	
Disruption of communication for protection	✘	✘	✘	✘	✘	✘
Network disruption within substation	✘	✘				✘
Abnormal or disruption of monitoring system	✘	✘	✘	✘	✘	✘
Denial of service from control centre	✘	✘	✘	✘	✘	✘
Misjudgement of dispatchers				✘		
Erroneous post analysis				✘		✘

C. Substation Attack Scenarios

According to the above-mentioned investigation in the test-bed, potential substation attack scenarios are identified as follows,

- *Stuxnet*-like malware can propagate via infected removable USB drives and LAN communications, as shown by the yellow triangle with the number 2 in Fig. 2, and can be designed to sabotage SCADA systems with direct physical consequences.
- A maintenance engineer's laptop is directly connected to the switch network in the smart substation, as shown by the yellow triangle with the number 1 in Fig. 2.
- Due to the maintenance engineer's unintended misuse, the laptop may gain access to unauthorized IEDs from other manufacturers, which may cause communication disruption, or even operation failure. Traditional malware such as viruses and worms, or advanced *Stuxnet*-like malware may penetrate the IT control environment of the smart substation via a laptop. Furthermore, the same laptop has the potential to infect a number of smart substations by the same maintenance engineer.
- During maintenance, the engineer may access the Internet by wireless to download electronic materials or perform remote maintenance. This may be utilized by a threat actor as a conduit to penetrate the substation automation system.

The smart substation is also vulnerable to further exploitation: it lacks real-time detection approaches for cybersecurity; the IEDs lack the ability to identify whether control commands are from a legal user; and the IEDs in the smart substation typically lack cybersecurity penetration testing before being put into operation. To attempt to address these practical cyber-security problems, the next section proposes a fuzz testing approach to detect IEC 61850 protocol vulnerabilities for IEDs in the test-bed.

IV. FUZZ TESTING FOR IEC 61850

In a smart substation, an attacker may send invalid or unidentified packets to "fuzz" IEDs using a malicious IEC 61850 client illegally connected to the substation level network. Such injected packets, including abnormal remote commands and set points, may bring a normal process into unintended states and/or cause an IEC 61850 server to freeze or other unexpected behaviors [11]. Malformed packets transmitted to IEDs may lead to denial of service by crashing an IEC 61850 protocol stack [12]. One of the mitigation measures for the malformed packet attack is to test the robustness of IEDs using the fuzzing technology, identify potential protocol vulnerabilities, and then feed back to manufacturers to address the found issues by upgrading programs before real operation of smart substations.

IEC 61850, based on an object-oriented modelling approach, adopts state machines to define and delineate complex protocol service and functional behaviors of IEDs. In terms of security and reliability testing for the IEC 61850 communication stack, the IEC 61850 protocol is more difficult to be tested than those without such complex state machines. In addition, the IEC 61850 based IEDs to be tested in smart substations have complicated logical models, including numerous logical nodes, data, and data attributes. Current testing approaches for protocol security and reliability are based on capturing, mutating, and then replaying messages between the tester and the IED. However, due to the complexity of IEC 61850, conventional testing methods may be inefficient when replaying too many redundant packets. On top of that, the test process has to stop when an IED under test no longer responds due to malformed packets sent by the tester.

A. *Fuzz Testing Implementation in the Test-Bed*

An automatic fuzz testing approach is proposed, and has been implemented in the test-bed environment to test the security and reliability of the IEC 61850 protocol stack implementation, as well as the robustness of IEDs. The core idea of the IED robustness testing is to send test cases with malformed messages to the IED, and then check the communication status of the IED. The robustness of the IED depends on its response to the malformed messages. In terms of test cases with the same malformed message, the more the number of unhandled exceptions and unexpected behaviors are, the worse the robustness of the IED is. The proposed fuzzing is a black box testing method, which only needs to know the IEC 61850 protocol, rather than the specific implementation of communication module inside the IED [13].

In order to implement the above fuzz testing method, a test platform has been built, which includes a fuzzing simulator, IEDs, a remote-controlled power strip, and a switch, as shown in Fig. 3. In Fig. 3, the fuzzing simulator runs the proposed fuzz testing method as an IEC 61850 client. The IEDs are IEC 61850 based servers, which include 10 real protection relays, as well as 8 measurement and control devices for 220kV and above smart substations. The Ethernet switch connects the fuzzing simulator and the IEDs. The power strip in Fig. 3 can be remotely controlled by the simulator in order to turn on or off the IEDs. The proposed fuzz testing steps are as follows:

1) As an IEC 61850 client, the fuzzing simulator accesses the IED as an IEC 61850 server. In this case, the normal communication is built between the IEC 61850 client and the server in the test-bed, and normal communication packets are captured by *Wireshark* .

2) In the fuzzing simulator, the collected messages are pre-processed by removing useless and redundant data, in order to generate a set of initial sample messages. A number of test cases with malformed messages are constructed from the sample messages, using mutation-based fuzzing methods.

3) During the fuzzing process, the malformed messages are automatically sent to the IEDs one by one, and the malformed messages which cause the IED communication failure or status exception are recorded into a log file.

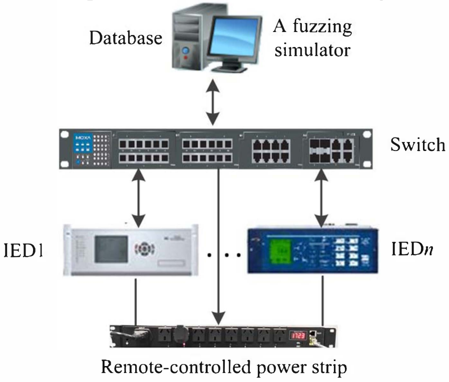


Figure 3. A test platform for fuzz testing of IEC 61850

4) The fuzzing simulator can automatically detect the status of the IED tested. If the IED is crashed due to the fuzz testing, the fuzzing simulator will send a control command to the remote-controlled power strip to restart the crashed IED, so that the fuzz testing can continue to test the next malformed packet after the IED restarting.

5) After the fuzz testing, the robustness reports of the tested IEDs are attained according to the ability of IEDs to addressing malformed packets.

B. *Experimental Results*

In the proposed fuzzing test-bed, 18 IEC 61850 based IEDs from several mainstream manufacturers were tested using the proposed fuzzing approach.

The fuzz testing revealed that most of the IEDs had cyber vulnerabilities, with various levels of risk. The levels of risks (i.e., high, medium, low) are defined according to the recovery time after the communication disruption. The common consequences discovered due to “successful” fuzzing are the following:

① The human machine interface (HMI) of the IED tested has no response;

② The dispatcher in the control center cannot remotely control the IEDs in smart substations.

③ The IED cannot normally connect to the monitoring system;

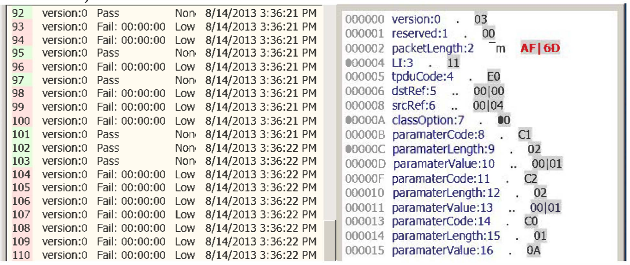
④ The IED cannot communicate with the RTU;

⑤ The IED communication programming is overflowed;

For example, the fuzzing simulator sent an IEC 61850/MMS packet with a malformed payload to a real line protection relay, as show in Fig. 4. The HMI of the relay device under test had no response.

To be exact, the value of the field *packetLength* in the TPKT layer is abnormal (*AF 6D*), as shown by the red field in Fig. 4. Based on analyzing the captured packets via *Wireshark*, any normal connection request is not successful after the fuzz testing, and the abnormal status can only be recovered by restarting the device, as shown in Fig. 5.

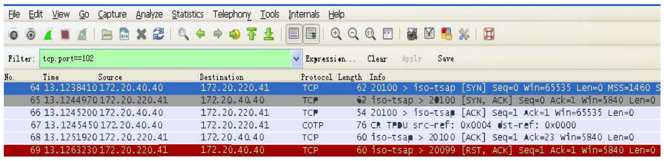
Similarly, other vulnerabilities of this relay device are identified, as show in Table II.



```
92   version:0  Pass            Non  8/14/2013 3:36:21 PM
93   version:0  Fail: 00:00:00  Low  8/14/2013 3:36:21 PM
94   version:0  Fail: 00:00:00  Low  8/14/2013 3:36:21 PM
95   version:0  Pass            Non  8/14/2013 3:36:21 PM
96   version:0  Fail: 00:00:00  Low  8/14/2013 3:36:21 PM
97   version:0  Pass            Non  8/14/2013 3:36:21 PM
98   version:0  Fail: 00:00:00  Low  8/14/2013 3:36:21 PM
99   version:0  Fail: 00:00:00  Low  8/14/2013 3:36:21 PM
100  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:21 PM
101  version:0  Pass            Non  8/14/2013 3:36:21 PM
102  version:0  Pass            Non  8/14/2013 3:36:22 PM
103  version:0  Pass            Non  8/14/2013 3:36:22 PM
104  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:22 PM
105  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:22 PM
106  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:22 PM
107  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:22 PM
108  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:22 PM
109  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:22 PM
110  version:0  Fail: 00:00:00  Low  8/14/2013 3:36:22 PM
```

```
000000 version:0           .   03
000001 reserved:1          .   00
000002 packetLength:2      ¯m  AF|6D
000004 LI:3                .   11
000005 tpduCode:4          .   E0
000006 dstRef:5            ..  00|00
000008 srcRef:6            ..  00|04
00000A classOption:7       .   00
00000B paramaterCode:8     .   C1
00000C paramaterLength:9   .   02
00000D paramaterValue:10   ..  00|01
00000F paramaterCode:11    .   C2
000010 paramaterLength:12  .   02
000011 paramaterValue:13   ..  00|01
000013 paramaterCode:14    .   C0
000014 paramaterLength:15  .   01
000015 paramaterValue:16   .   0A
```

Figure 4. The payload of a malformed packet in the fuzzing simulator



Filter: tcp.port==102

```
No.  Time       Source         Destination    Protocol Length Info
64 13.1238410 172.20.40.40   172.20.220.41  TCP      62 20100 > iso-tsap [SYN] Seq=0 Win=65535 Len=0 MSS=1460 S
65 13.1244970 172.20.220.41  172.20.40.40   TCP      62 iso-tsap > 20100 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
66 13.1245200 172.20.40.40   172.20.220.41  TCP      54 20100 > iso-tsap [ACK] Seq=1 Ack=1 Win=65535 Len=0
67 13.1245450 172.20.40.40   172.20.220.41  COTP     76 CR TPDU src-ref: 0x0004 dst-ref: 0x0000
68 13.1251920 172.20.220.41  172.20.40.40   TCP      60 iso-tsap > 20100 [ACK] Seq=1 Ack=23 Win=5840 Len=0
69 13.1263230 172.20.220.41  172.20.40.40   TCP      60 iso-tsap > 20099 [RST, ACK] Seq=1 Ack=1 Win=5840 Len=0
```

Figure 5. The captered TCP packets in the *Wireshark*

TABLE II. VULNERABILITIES OF THE RELAY UNDER TEST

Protocol layer	Field name	Abnormal value	Consequence	Risk level
TPKT	Package Length	AF 6D; 9D 7F; 86 EE; CB D7	①, ②, ③, ④	High
COTP	source reference	C3 37	①, ②, ③, ④	High
Session	identifier	OC	①, ②, ③, ④	High
MMS	Length	00; EB	①	Medium

During the fuzzing process, other cyber vulnerabilities in the cyber space of the smart substation were identified besides the vulnerabilities of IEDs, for example, vulnerabilities of operation systems and database, butter overflows of configurable software, and overflows of the IEC 61850 protocol stack. At present, more than 20 types of cyber vulnerabilities are collected into a vulnerability database for smart substations.

According to aforementioned discussion and results, the proposed fuzzing approach is simple and effective to detect the vulnerabilities of IEC 61850 and evaluate the robustness of IEDs in the test-bed.

V. CONCLUSION

Compared with physical security for conventional substations, research and development for cybersecurity of IEC 61850 based smart substations is still at an early stage. This paper proposes a cyber-physical test-bed for smart substations to investigate potential vulnerabilities using simulated cyber-attacks. The initial investigation results show that most of IEDs under test in the test-bed exhibit cyber vulnerabilities with various levels of risk. It is important to note that these cyber vulnerabilities may affect the secure and stable operation of SCADA in the smart substation. Based on the test-bed, which is closely matched to the operation of live substations, the presented fuzzing approach has been implemented and validated. Initial experiments have shown it to be effective for identifying cyber vulnerabilities in IEC 61850 IEDs, and useful to improve the robustness of IEDs in smart substations. The cybersecurity test-bed allows end-to-end testing of cyber-attacks and physical consequences, as well as experimental validation of proposed cybersecurity countermeasures for smart substations. In response to the challenge represented by these inherent device vulnerabilities, the authors' future work focuses on a comprehensive intrusion detection and prevention system (IDPS) for IEC 61850 substations, as shown in Fig. 2. This IDPS will be proposed, implemented, and tested using the cyber-physical test-bed presented in this work.

REFERENCES

[1] *Communication Networks and Systems in Substations*, IEC Std. 61850.

[2] *Power Systems Management and Associated Information Exchange – Data and Communications Security.* IEC Std. 62351.

[3] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *Proc. 2012 IEEE Globecom Workshops,* pp. 1508-1513.

[4] *Communication networks and systems for power utility automation— Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3,* IEC Std. 61850, 2011.

[5] *Communication networks and systems for power utility automation— Part 9-2: Specific communication service mapping (SCSM) — Sampled values over ISO/IEC 8802-3,* IEC Std. 61850, 2011.

[6] G. J. Myers, *The Art of Software Testing*, John Wiley and Sons, 1979.

[7] H. C. Kim, Y. H. Choi, and D. H. Lee, "Efficient file fuzz testing using automated analysis of binary file format," *Journal of Systems Architecture*, vol. 57, pp. 259-268, 2011.

[8] A.F. Sui, W. Tang, J. J. Hu, M. Z. L. C. Technology, S. L. C. W. Z. Nanlu, C. y. District, et al., "An Effective Fuzz Input Generation Method for Protocol Testing," in *Proc. 2011 IEEE 13th International Conf. on Communication Technology*, pp. 728-731.

[9] P. Maynard, K. McLaughlin, B. Haberler, "Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks," in *Proc. 2014 the 2nd Int'l Symposium for ICS & SCADA Cyber Security Research*, pp.30-42.

[10] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, et al., "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks," *IEEE Trans. on Power Delivery*, vol. 29, pp. 1092-1102 2014.

[11] B. Reaves and T. Morris, "Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 5, pp. 154-174, 2012.

[12] T. Morris, S. Pan, J. Lewis, J. Moorhead, N. Younan, et al., "Cybersecurity testing of substation phasor measurement units and phasor data concentrators," in *Proc. 2011 the 7th Annual ACM Cyber Security and Information Intelligence Research Workshop*, no. 24.

[13] H. T. Jiang, Y. Yang, W. Huang, and Y. J. Guo. "Robustness Testing Method for Intelligent Electronic Devices," *2014 Asia-Pacific Electronics and Electrical Engineering Conf.,* Shanghai, China, December 27-28, 2014. *(Accepted)*