On Practical Threat Scenario Testing in an Electric Power ICS Testbed

Ahnaf Siddiqi
Singapore University of Technology and Design, Singapore
ahnaf_siddiqi@alumni.sutd.edu.sg

Nils Ole Tippenhauer
Singapore University of Technology and Design, Singapore
nils_tippenhauer@sutd.edu.sg

Daisuke Mashima
Advanced Digital Sciences Center, Singapore
Daisuke.m@adsc-create.edu.sg

Binbin Chen
Advanced Digital Sciences Center, Singapore
Binbin.chen@adsc-create.edu.sg

ABSTRACT

Industrial control system networks in real world usually require a complex composition of many different devices, protocols, and services. Unfortunately, such practical setups are rarely documented publicly in sufficient technical detail to allow third parties to use the system as reference for their research. As a result, security researchers often have to work with abstract and simplified system assumptions, which might not translate well to practice.

In this work, we provide a comprehensive overview of the network services provided by industrial devices found in the EPIC (Electric Power and Intelligent Control) system at SUTD. We provide a detailed network topology of the different network segments, enumerate hosts, models, protocols, and services provided. We argue that such a detailed system description can serve as an enabler for more practical security research. In particular, we discuss how the reported information can be used for emulating a diverse set of important threat scenarios in the smart grid domain. In addition, the provided details allow other researchers to build more detailed models or simulations.

ACM Reference Format:
Ahnaf Siddiqi, Nils Ole Tippenhauer, Daisuke Mashima, and Binbin Chen. 2018. On Practical Threat Scenario Testing in an Electric Power ICS Testbed. In *CPSS'18: The 4th ACM Cyber-Physical System Security Workshop, June 4, 2018, Incheon, Republic of Korea.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3198458.3198461

1 INTRODUCTION

Industrial Control Systems (ICS) are a part of a country's national critical infrastructure which provide the control, monitoring, and distribution of resource. Examples include water distribution, water treatment, electric power grid, oil pipelines, and transportation systems. In recent years, industrial control devices have been increasingly connected to local and remote networks to allow remote supervision and control. To enable that supervision and control, commonly a combination of proprietary industrial protocols and Internet protocols are used. These systems are attractive cyber attack targets and thus researchers are actively identifying new attacks and formulating new methods to defend [12]. Actual production ICS are expensive and critical, and thus not ideal testing grounds for academic security experiments. As a result, researchers are forced to rely on abstract models [23], small-scale prototypes of parts of the system, or a simulation of the cyber and physical process [14].

The above methods of running their experiments are generally simplified and only attempt to focus on their topic of interest. They often do not include the typical set of devices and protocols that run on the studied system, beyond the selected device or protocol that they focus on. As such, a full and detailed network architecture description of the experimental setup, as well as a complete enumeration of the devices, protocols, network services, functionality mappings, and etc. are often absent, which would otherwise allow the researchers to present and evaluate their work in a more comprehensive and practical setup.

In this paper, we provide required details for the EPIC electric power ICS system at SUTD. Our main goal is to provide a detailed summary of the testbed system setup from the "cyber" perspective. The information provided is expected to be useful for the community to reason about attacker and systems models, attack vectors, and countermeasures. We leave the actual physical process description as out of scope, while noting that components in the cyber, e.g., intelligent electronic devices (IEDs) are tightly coupled with and responsible for operating on physical components. We summarize our contributions in this paper as follows:

- We present the network topologies used and underlying design decisions made in the testbed, and discuss their potential impacts on security.
- We enumerate and summarize the protocols and services that are running on all networked devices in the system, with information about the specific models and manufacturers of all the major devices.
- We discuss a list of end-to-end threat scenarios that can be emulated on the testbed and how they may benefit from the detailed information provided in this work.

The structure of the paper is as follows: In Section 2, we provide the overview of each of the subsystems in the testbed. In Section 3, we provide the network layout of each of the subsystems in details and discuss the protocols used and services provided. We then discuss the emulation of the threat scenarios in the testbed in Section 4. We briefly summarize related work in Section 5, and conclude the paper in Section 6.

2 BACKGROUND

The Electric Power and Intelligent Control (EPIC) testbed was constructed at SUTD with the purpose to allow security researchers

CPSS'18, June 4, 2018, Incheon, Republic of Korea

ACM ISBN 978-1-4503-5755-5/18/06…$15.00
https://doi.org/10.1145/3198458.3198461

to conduct experiments to assess the effectiveness of attack or defense mechanisms. While the overall physical and cyber system was specified by us, the actual selection of devices, network design, and overall implementation was performed by a third party from the industry, selected through a tendering process. As such, the overall system is expected to resemble similar systems in industry. The procurement value for the system was approximately 750k USD (including setup). We have a permanent lab engineer position to operate the lab, support research, and perform maintenance.

EPIC consists of four distinct physical process segments: i) Generation, ii) MicroGrid, iii) Transmission/Distribution[1], and iv) Smart Home. We briefly summarize them as follows. A detailed description of the physical process is out of scope of this work[2].

Generation. This segment uses local generators to produce the power required for the system along with power drawn directly from the grid. The local generators are in fact driven using live main connection as well.

MicroGrid. This segment is connected to rooftop photovoltaics (PV) cells, inverters, and batteries. They work as an extra power source that supplements the generation segment.

Transmission/distribution. This segment representative of a distribution grid, supplying power to SmartHome. An transformer is used to step up/down the voltage to the smartHome.

Smart Home. This segment consists of two load banks, 15kVA and 30kVA respectively, with programmable variable resistors, inductive and capacitive loads. In addition, the motors of the generation segment can be used as loads in the Smart Home segment to represent loads such as electric cars charging, washing machines etc. If used as such, the motors are controlled by Variable Speed Drives (VSDs) which are managed by the Smart Home controller.

3 NETWORK, PROTOCOLS, AND SERVICES

This section first briefly introduces the overall network topology in EPIC. Then, the devices, protocols, and services are discussed.

3.1 Communication Network Topology

The overall network topology of EPIC system is a hybrid of both Ethernet star and ring structure, as shown in Figure 1. Each physical segment is locally controlled by a programmable logic controller (PLC), and a variable number of Intelligent Electrical Devices (IEDs) which control relays and other power system devices. The number of IEDs in each network section depends on how many relays and other devices are to be controlled to operate the power. The PLC and IEDs are connected to a local switch, which itself is connected to the ring network mentioned above (see Figure 2). The main supervisory and monitoring elements reside on the network in a star topology. The historian, the ring switch (CSW1), the main wireless access point (CAP2), and the control PLC (CPLC) are all connected to a switch (CSW2). This is connected to the SCADA (supervisory control and data acquisition) panel through a router. The router divides the link layer into two broadcast domains. This prevents Link-layer broadcast and multicast traffic in the plant networks from reaching the SCADA. The router is used to replicate similar setups in large scale power systems, in which the substations are not directly in the same link layer broadcast domain as the SCADA. The access point CAP2 provides a mechanism to connect to the control segment (but not to the SCADA). This allows for communication with devices in the operating section of the plant. Communication to SCADA using wireless is blocked in default setting for security reasons. The ring segment consists of the ring switch, CSW1, and the four control segments, each of which also has a ring topology. The ring topology provides a highly available communication infrastructure between devices. The solar cluster controller (SCC) is also in the same link layer. It controls the inverters connected to the photovoltaic system, which is connected to the batteries in the system via a switch. Table 4 in the appendix provides an overview of all the devices that are present in the system along with the model/version of the devices and their manufacturers. The short names used in the table will be used hereafter to refer to the devices.

3.2 Protocols and Services

As illustrated in Figure 3, the system has two main protocols in place which allow the communication of data from the physical processes to the SCADA: Manufacturing Message Specification (MMS), a request/response protocol, and Generic Object Oriented Substation Event (GOOSE), a multicast publisher-subscriber protocol. They are part of IEC 61850 protocol suite [17].

The PLC communicates with the IEDs using MMS to obtain information from the sensors and actuators to assess and instruct operational work in each of the segment. The data obtained from the IEDs are stored in the PLC. The SCADA also retrieves information from both the PLC and IED using the same protocol. The IEDs multicast information using GOOSE so that other IEDs in the physical segments can receive them. Each IED listens to the multicast messages as they are programmed to execute certain functions depending on the data. Each of the segment has a redundancy in place. The HSR/PRP protocol is used for persist communication under a single network component failure so that the PLC/SCADA can continue to access the IEDs. A brief overview of the protocols are presented below.

Manufacturing Message Specification (MMS) is a standard (ISO 9506) dealing with messaging systems for transferring real time process data and supervisory control information between networked devices or computer applications. The standard is developed and maintained by the ISO Technical Committee 184 (TC184). The protocol uses Connection Oriented Transport Protocol (COTP), which sits on top of TCP/IP. It is a server/client protocol.

Generic Object Oriented Substation Events (GOOSE) is a subdivided part of Generic Substation Events (GSE) which is a control model defined as per IEC 61850, which provides a fast and reliable mechanism of transferring event data over entire substation networks. GOOSE is a multicast protocol, which operates on the link layer. This provides facility to transfer the same event message to multiple physical devices.

High-availability Seamless Redundancy (HSR) is a network protocol that provides seamless fail-over against failure of any network component. This redundancy is invisible to the application. HSR nodes have two ports and act as a switch (bridge), which allows them to be arranged into a ring or meshed structure, without dedicated switches. This is in contrast to the companion standard Parallel Redundancy Protocol (IEC 62439-3 Clause 4), with which HSR shares the operating principle.

[1] Device names in this segment refer to it as transmission, we use the term distribution here as voltages are low (400V).

[2] Additional information is available at https://itrust.sutd.edu.sg/research/testbeds/electric-power-intelligent-control-epic/.

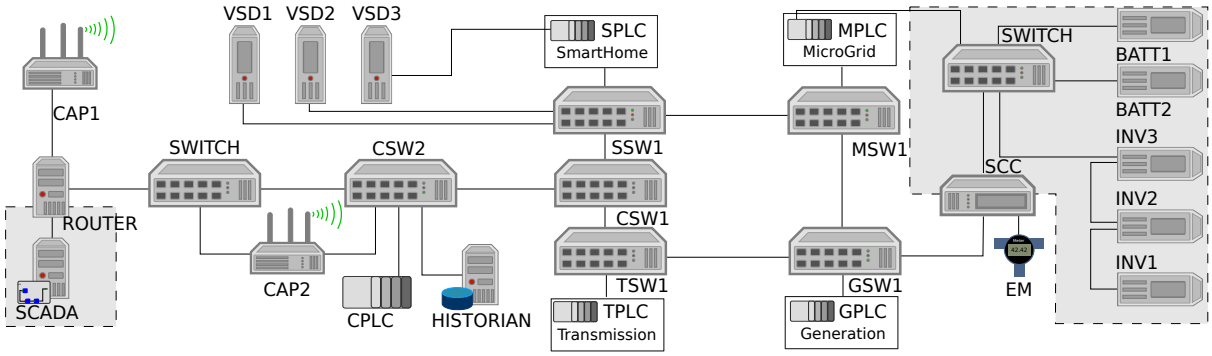

Figure 1: Overview of EPIC Network. A ring topology connects the individual process stages with their main PLCs. The overall network is segmented into three Link layer broadcast domains (two smaller ones are highlighted in grey with dashed border).

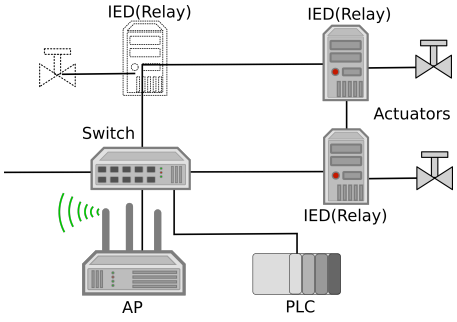

Figure 2: General structure of a process segment. IEDs are communicating with actuators and sensors through analog communication, and are also connected to the overall Ethernet Link layer broadcast domain.

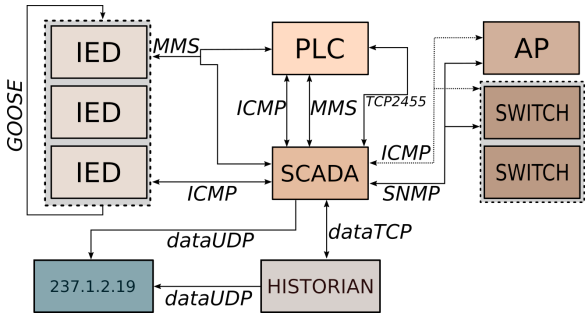

Figure 3: Main Protocols

There are several other protocols that run on the system for host discovery, broadcast, and other services. Table 1 lists the protocols that are available at each of the devices. A few of the protocols referred in the table are unidentified. We briefly present the main information about these protocols in the following.

TCP-2455 is a protocol over TCP/IP running on port 2455. It is a proprietary protocol that provides the "wago-io-system" service by *Wago*. The devices in participation are SPLC and WS. When the source is WS, two sizes of payloads are provided: 24 and 26 bytes. This seems to be an affirmation message. Otherwise, when the SPLC is the source, payload sizes are either 89 or 397 bytes.

dataTCP is an unidentified protocol in the system traffic over TCP/IP. This is observed between HIST and WS. The port assigned to HIST is 55255 and to WS is 53807. The data transferred between them varies depending on the source. If the source is HIST, the payload size is fixed at 71 bytes which indicates that it could be an affirmative packet. Otherwise, if the source is WS, the payload data varies between 2300 to 3100 bytes.

dataUDP is an unidentified protocol in the system traffic over UDP. Several devices are communicating over this unidentified protocol and as such, multiple source ports are being used across the devices. The protocol is partially multicasted, e.g. by the Historian and the SCADA workstation to destination IP 237.1.2.19. Based on manuals, in some instances the dataUDP could be *SMA Speedwire*, required to communicate with devices in the Solar generation segment (not verified by us so far). For packets which are not broadcast or multicast, some information is listed below:

Table 1: Protocols actively used by devices in EPIC

Name	GOOSE	HSR/PRP	MMS	CLASSIC-STUN	SNMP	SSDP	ICMP	IAAP	SMB	IGMP	dataUDP	dataTCP	TCP-2455
[GTM]IED[12]	●	-	●	-	●	-	●	-	-	-	-	-	-
SIED[1234]	●	-	●	-	●	-	●	-	-	-	-	-	-
[GTMC]PLC	-	-	●	-	-	-	●	-	-	-	-	-	-
SPLC	-	-	●	-	-	-	●	-	-	-	-	-	●
[GTMS]AP; CAP1	-	-	-	-	●	-	●	-	-	●	-	-	-
CAP2	-	-	-	-	●	-	●	●	-	●	-	-	-
[GTMSC]SW[1]	-	-	-	-	●	-	●	-	-	-	-	-	-
CSW2	-	●	-	-	●	-	●	-	-	-	-	-	-
VSD[123]	-	-	-	●	-	-	-	-	-	-	-	-	-
BATT1	-	-	-	-	-	-	-	-	-	●	●	-	-
BATT2	-	-	-	-	-	-	-	-	-	●	●	-	-
SCC	-	-	-	-	-	-	-	-	-	●	●	-	-
EM	-	-	-	-	-	-	-	-	-	●	●	-	-
INV1	-	-	-	-	-	-	-	-	-	●	-	-	-
INV[23]	-	-	-	-	-	-	-	-	-	●	●	-	-
HIST	-	-	●	●	-	●	●	-	●	●	●	●	-
WS	-	-	-	-	●	●	-	-	●	●	●	●	-
FW	-	-	-	-	-	-	-	-	-	-	-	-	-

- Packets between batteries (BATT1 and BATT2) and SCC. The source and destination port both are 9522, which is used by SMA Speedwire. The payload varies. Most of the time the payload is either 458, 498, or 506 bytes. However, there are some packets with payloads of 58 and 142 bytes.
- Packets between SCC and inverters (INV1, INV2, and INV3). The source and destination are both 9522. The payload size is not consistent. However, packets of sizes 498 and 218 bytes are more common.

Other than the protocols listed in Table 1, several services are also available. Table 2 lists the services we have found on each device. The ports associated with each of these services are open and if authentication is required, the default one is used. We note that industrial devices expose a range of services that might be relevant to security, which are commonly not discussed in related work on testbeds.

Table 2: Services hosted by devices in EPIC

Name	HTTP	HTTPS	SSH	Telnet	Telnet over TLS	DNS	MSRPC	netbios-ssn	Microsoft-DS	MS-WBT-server	HTTP-proxy	pyro	.NET remoting services	(port-300)	(port-[1947,1981,4410])
[GTM]IED[12]	●	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SIED[1234]	●	-	-	-	-	-	-	-	-	-	-	-	-	-	-
[GTMSC]PLC	●	●	●	-	-	-	-	-	-	-	-	-	-	-	-
[GTMS]AP; CAP[12]	●	●	●	●	●	-	-	-	-	-	●	-	-	-	-
GTMSC]SW[12]	●	●	●	●	-	-	-	-	-	-	-	-	-	-	-
VSD[123]	●	-	-	●	-	-	-	-	-	-	-	-	-	●	-
BATT[12]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SCC	●	-	-	-	-	-	-	-	-	-	-	-	-	-	-
EM	●	-	-	-	-	-	-	-	-	-	-	-	-	-	-
INV[123]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
HIST	-	-	-	-	-	-	●	●	●	●	-	-	-	-	-
WS	●	●	-	-	-	-	●	●	●	-	-	●	●	-	●
FW	●	●	●	-	-	●	-	-	-	-	-	-	-	-	-

Table 5 in the appendix specifies the mapping of communication flows for the devices in the system. The mapping is segregated according to the protocol headed under "Type". The header "Bi-directional" signifies the communication flow is going in both directions. The traffic could be response packets to previous requests or separate packets.

ICMP and IGMP. The SCADA WS uses periodic ICMP (Internet Control Message Protocol) traffic, specifically *ping*, to verify availability of networking components such as the switches, IEDs, and many other devices (roughly every 30 seconds). IGMP (Internet Group Management Protocol) is used to manage the multicast setup for the other protocols used in the system.

3.3 General security comments

The router before SCADA server is a Hirschmann EAGLE30 firewall, but there is no firewall rules configured in the default setting. As a result, if an attacker is able to associate to the access point (e.g., by guessing credentials), it can communicate with almost all devices in the network. In addition, the whole network is essentially consisting of two link layer broadcast domains (separated by the router). We assume this implementation choice was made to enable exchange of IEC 61850 GOOSE traffic (which is directly sent over link layer to achieve low network delay) between relevant devices (e.g. historian and IEDs directly). As a result, link layer attacks such as ARP (Address Resolution Protocol) spoofing are possible for most devices by anyone connected to the main network. In terms of reliability, CSW1 is a single point of failure for all communication between the process segments and the historian and SCADA.

4 EPIC FOR PRACTICAL ICS SECURITY RESEARCH

In the earlier sections, we have gone through technical details of the testbed. In this section, we discuss how those details can help researchers perform practical cyber security experiments. We first discuss real-world threat scenarios, focusing on those derived from NESCOR (National Electric Sector Cybersecurity Organization Resource) cyber security failure scenarios [20], and then how we can emulate such scenarios on EPIC for designing and evaluating cyber security solutions.

4.1 Threat Scenarios

NESCOR failure scenarios [20] cover malicious or non-malicious cyber security events in various system segments in power grid systems, such as wide area monitoring, protection, and control (WAMPAC), distributed energy resources (DER), smart metering infrastructure (AMI), distributed grid management (DGM), among others. A failure scenario is associated with a system segment and assigned an index number. For example, DER.3 refers to the third failure scenario for DER system in [20]. Attack vectors or building blocks that can be evaluated on the testbed include:

- Malware, malicious firmware, and configuration on field devices (e.g., discussed in DER.3, DER.5, WAMPAC.8)
- Physical attack against field devices (e.g., AMI. 27, AMI.32, DGM.3)
- Communication link attack (e.g., AMI.14, DGM.1, WAMPAC.2, WAMPAC.11, WAMPAC.12)
- Malicious insiders (e.g., AMI.1, DER.16, DGM.11)
- Stolen/Compromised field service tools (e.g., AMI.21)

After gaining their footholds in the network, the next steps for attackers include:

- Reconnaissance / probing for collecting sensitive information (e.g., important feeders or transformers) to prepare for large-scale attacks.
- False data injection for confusing the SCADA and control center systems (e.g., state estimation or power flow simulation) or for hiding traits of other attacks.
- Malicious command injection to cause physical impact on the power grid systems.
- Denial of service for preventing smart grid communication to prevent or slow down responses to attacks etc.

We next select several scenarios of different categories and discuss how they can be emulated on EPIC based on the knowledge derived from the system details we provided earlier.

4.2 Emulation of Threat Scenarios on EPIC

AMI.1 is a typical insider attack scenario, where an authorized individual abuses the system to send out malicious control commands (namely remote disconnect commands). This type of attack can be emulated on SCADA (WS), by scripting an attacker's behavior or by manually operating the HMI. In a similar manner, attacks such as the power plant attacks in Ukraine [8, 29] can be emulated, where

Table 3: Mapping selected NESCOR threat scenarios to EPIC. DER.16 is about malicious command injection, AMI.1 is about insider attack, DGM.1 is about a DoS (denial of service) attack, WAMPAC.2 is about a communication link attack, DGM.3 is about physical attack, and DER.3 is about malware on field devices (E: Entry point, X: Target)

Name	DER.16	AMI.1	DGM.1	WAMPAC.2	DGM.3	DER.3
WS		E	X	X	-	X
HIST	-	-	X	X	-	-
FW	-	-	-	E	-	-
CPLC	-	-	-	X	E	E
CAP	-	-	E	E	-	-
CSW	-	-	-	E	-	-
GIED	-	-	-	X	X	X
GPLC	-	-	-	X	E	E
GAP	-	-	E	E	-	-
GSW	-	-	-	E	-	-
TIED	-	-	-	X	X	X
TPLC	-	-	-	X	E	E
TAP	-	-	E	E	-	-
TSW	-	-	-	E	-	-
MIED	-	-	-	X	X	X
MPLC	-	-	-	X	E	E
MAP	-	-	E	E	-	-
MSW	-	-	-	E	-	-
SCC	E	-	-	-	-	E
BATT	X	-	-	-	-	X
INV	X	-	-	-	-	X
SIED	-	-	-	X	X	X
SPLC	-	-	-	X	E	E
SAP	-	-	-	E	-	-
SSW	-	-	-	E	-	-
EM	-	X	-	-	-	-
VSD	-	-	-	-	-	-

an HMI is remotely controlled by an attacker to send out a large number of circuit breaker open commands. On the SCADA WS in EPIC, we can also evaluate impact of attacks caused by malware, such as CrashOverride [1, 2] that has capability to serve as an IEC 61850 server to send out malicious control commands. Furthermore, we can emulate situation caused by system malfunction. For example, in Tempe, Arizona [27] in 2007, a load shedding program was accidentally activated and resulted in power outage.

Besides control commands to meters or circuit breakers, we can emulate attacks targeting distributed energy resources, e.g., as described in DER.16 scenario. On EPIC, batteries and inverters are regarded as distributed energy resources, and they are controlled by SCC. Here, for example, commands that manipulate charging status of batteries could bring the grid into unstable state. The security measures to mitigate these threats include access control system on WS or HMI or implementation of command authentication mechanism in the field [18, 19].

Due to the lack of security (in particular authentication, integrity protection, and encryption) of IEC 61850 MMS used in EPIC, it is possible to perform spoofing attacks and to inject malicious messages in the SCADA monitoring and control communication, like WAMPAC.2 scenario. Such messages could mislead the SCADA system to initiate wrong control commands. Manipulated sensor readings also would lower the situation awareness of SCADA, and compromise the integrity of the information stored in the Historian. An attacker would also be able to take advantage of the wireless network through the access points in physical segments of EPIC. Alternatively, an attacker could be directly connected to the switches and the router (FW) as a Man-in-the-Middle, enabling the attacker to intercept and modify any messages exchanged via those systems. Possible countermeasures against this threat would be to enhance security of messaging, e.g., by implementing IEC 62351 [10].

DGM.1 is a scenario where wireless communication is jammed to prevent monitoring and control. Such an attack can be emulated on EPIC by, for example, generating a large amount of dummy traffic to exhaust the bandwidth or actually jamming wireless access points.

In EPIC, PLCs play an important role for controlling power system components. A threat that an attacker attempts physical access to compromise substation equipment is discussed in DGM.3. As mentioned earlier, the EPIC testbed includes Wago Kontakttechnik's 750-82-2 PLCs which are known to have vulnerability to allow an attackers to modify or delete arbitrary files [26]. Such a vulnerability allows us to assume not only insider attacks but also external attackers with physical device access. PLCs are typically connected to IEDs, which in return operates on physical components to make influence on the power grid. The impact of cases that abuse field service devices used for configuration and maintenance of field devices (e.g., AMI.21), can also be evaluated in the similar manner.

Malware on field devices (e.g., DER.3) can also be mounted on PLCs, which control circuit breakers etc. and also SCC, which controls inverters and batteries. As discussed in earlier sections, EPIC involves some devices with known vulnerability [26, 28]. With this knowledge, researchers will be able to even design and implement malware on those devices to see the potential impact. Besides NESCOR failure scenarios, research of other emerging attack vectors, such as ransomware targeting industrial control devices [11], can be performed in the similar way.

5 RELATED WORK

ICS Testbeds. In [15], authors discuss an electric power testbed which uses an RTDS [16] for physical process simulation. Two relays connect the simulated physical process to two substations, which are connected to a SCADA system. Similar systems were presented (without details on network communications) in [4, 25].

Other testbeds concentrate on the physical process (simulation), mostly without actual cyber components (networks, industrial devices, industrial protocols), e.g. [6].

In [7], a complex system of several testbeds is discussed, constructed to measure the performance impact of security measures on ICS operations. The authors do not provide details on all protocols required to operate the systems, and which devices are exactly involved in exchanges.

In [13], the authors discuss the design and implementation of a similar testbed (with small actual physical water process). In particular, overall network architecture is discussed, and devices and software used are presented in details. In contrast to the testbed discussed in this work, the implementation was performed by researchers in [13]. In our work, we provide more details on the devices, protocols, and particular interactions. In addition, we discuss the application of NESCOR threat scenarios.

Security Research Using Testbeds. The following works focus on insights gained from testbeds, instead of the testbeds themselves.

For example, detection of attacks are discussed and experimentally tested in [3] and [24]. In all the cases mentioned here, a comprehensive analysis of a system is only made possible because of the availability of the system. If such as system is not available, simulations are generally used or a prototype is created which lacks a complete interaction between different parts of the system. We hope the information provided in this work supports building simulation and emulation models of similar systems (e.g. based on combined network emulation and software and process simulation [5]), and to design and implement similar systems in the future.

Security Research Using Simulations. SoftGrid [14] is an open-source, software-based smart grid tested that is designed for evaluating cyber-security solutions (e.g., security enhanced substation gateways, industrial firewall, and intrusion detection systems) in a realistic, standard-compliant environment. While it has advantages in terms of scalability and configurability, its fidelity is not comparable to hardware-based testbed like EPIC. For example, attacks exploiting device specific vulnerabilities, such as [26, 28], are difficult to emulate. Other software-based approach, including [9, 21, 22], also suffer from the similar limitations.

6 CONCLUSIONS

In this work, we provided a detailed discussion of devices and protocols involved in operations of the EPIC testbed at SUTD. In particular, we argue that the actual complexity of protocols and services required to operate real-world ICS are often overlooked in related work. We provided enumerations of devices and their versions, protocols and the active participants, and discuss their use in the system. In addition, we listed the default services listening on the devices in EPIC, of which not all are required for operation. To the best of our knowledge, such information is not provided in related work. We expect that such details are useful for other researchers (without access to similar testbeds) to understand industrial setups better. As example application of this information, we discussed the application of the NESCOR failure scenarios to provide scenarios for experimental security research in EPIC. We share example PCAP traffic captures of traffic in EPIC at https://research.scy-phy.net/epic/.

7 ACKNOWLEDGEMENTS

This research is partially supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore under grant NRF2014-NCR-NCR001-40, and NRF's Campus for Research Excellence and Technological Enterprise (CREATE) programme.

REFERENCES

[1] 2017. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf. (2017). (Date last accessed on Aug. 18, 2017).

[2] 2017. CrashOverride Malware. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-163A. (2017). (Date last accessed on Aug. 18, 2017).

[3] Sridhar Adepu and Aditya Mathur. 2016. Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment Plant. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*. ACM, 449–460. https://doi.org/10.1145/2897845.2897855

[4] U. Adhikari, T.H. Morris, and Shengyi Pan. 2014. A cyber-physical power system test bed for intrusion detection systems. In *Proceedings of IEEE PES General Meeting*. 1–5.

[5] Daniele Antonioli and Nils Ole Tippenhauer. 2015. MiniCPS: A Toolkit for Security Research on CPS Networks. In *Proceedings of ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC)*. ACM, New York, NY, USA, 91–100. https://doi.org/10.1145/2808705.2808715

[6] Aditya Ashok, Pengyuan Wang, Matthew Brown, and Manimaran Govindarasu. 2015. Experimental evaluation of cyber attacks on Automatic Generation Control using a CPS Security Testbed. In *Proceedings of IEEE Power Energy Society General Meeting*. 1–5.

[7] Richard Candell, Timothy Zimmerman, and Keith Stouffer. 2015. An industrial control system cybersecurity performance testbed. *National Institute of Standards and Technology. NISTIR* 8089 (2015).

[8] Defense Use Case. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. (2016).

[9] Justyna Joanna Chromik, Boudewijn RHM Haverkort, Anne Katharina Ingrid Remke, Carina Pilch, Pascal Brackmann, Christof Duhme, Franziska Everinghoff, Artur Giberlein, Thomas Teodorowicz, and Julian Wieland. 2017. Context-aware local Intrusion Detection in SCADA systems: a testbed and two showcases. In *8th IEEE International Conference on Smart Grid Communications, SmartGridComm 2017*.

[10] Frances Cleveland. 2005. IEC TC57 Security standards for the power system's information infrastructure-beyond simple encryption. In *Proceedings of Transmission and Distribution Conference and Exhibition*, Vol. 2006. 1079–1087.

[11] David Formby, Srikar Durbha, and Raheem Beyah. 2017. Out of control: Ransomware for industrial control systems. (2017). www.cap.gatech.edu/plcransomware.pdf

[12] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu. 2017. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Design Test* 34, 4 (Aug 2017), 7–17. https://doi.org/10.1109/MDAT.2017.2709310

[13] Benjamin Green, Anhtuan Lee, Rob Antrobus, Utz Roedig, David Hutchison, and Awais Rashid. 2017. Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research. In *Proceedings of USENIX Workshop on Cyber Security Experimentation and Test (CSET)*. USENIX Association.

[14] Prageeth Gunathilaka, Daisuke Mashima, and Binbin Chen. 2016. SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions. In *Proceedings of ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC)*. ACM, 113–124.

[15] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu. 2013. Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. *IEEE Transactions on Smart Grid* 4, 2 (2013), 847–855.

[16] R Kuffel, J Giesbrecht, T Maguire, RP Wierckx, and P McLaren. 1995. RTDS-a fully digital power system simulator operating in real time. In *Proceedings of Conference on Communications, Power, and Computing (WESCANEX)*, Vol. 2. IEEE, 300–305.

[17] RE Mackiewicz. 2006. Overview of IEC 61850 and Benefits. In *Proceedings of Power Systems Conference and Exposition (PSCE)*. IEEE, 623–630.

[18] Daisuke Mashima, Prageeth Gunathilaka, and Binbin Chen. 2018. Artificial Command Delaying for Secure Substation Remote Control: Design and Implementation. (2018). To appear in IEEE Transactions on Smart Grid.

[19] Sakis Meliopoulos, George Cokkinides, Rui Fan, Liangyi Sun, and Bai Cui. 2016. Command authentication via faster than real time simulation. In *Proceedings of Power and Energy Society General Meeting (PESGM)*. IEEE, 1–5.

[20] National Electric Sector Cybersecurity Organization Resource (NESCOR). 2013. Electric Sector Failure Scenarios and Impact Analyses. (2013).

[21] Chih-Che Sun, Junho Hong, and Chen-Ching Liu. 2015. A co-simulation environment for integrated cyber and power systems. In *Proceedings of Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 133–138.

[22] Song Tan, Wen-Zhan Song, Steve Yothment, Junjie Yang, and Lang Tong. 2015. ScorePlus: An integrated scalable cyber-physical experiment environment for Smart Grid. In *Proceedings of Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 381–389.

[23] William G. Temple, Binbin Chen, and Nils Ole Tippenhauer. 2013. Delay Makes a Difference: Smart Grid Resilience Under Remote Meter Disconnect Attack. In *Proceedings of the IEEE Conference on Smart Grid Communications (SmartGridComm)*. https://doi.org/10.1109/SmartGridComm.2013.6688001

[24] David Urbina, Jairo Giraldo, Alvaro A. Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. 2016. Limiting The Impact of Stealthy Attacks on Industrial Control Systems. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. https://doi.org/10.1145/2976749.2978388

[25] V. Urias, B. Van Leeuwen, and B. Richardson. 2012. Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. In *Proceedings of Military Communications Conference (MILCOM)*. 1–8.

[26] T. Weber. 2017. Critical CODESYS vulnerabilities in WAGO PFC 200 Series. (2017). https://www.sec-consult.com/en/blog/advisories/wago-pfc-200-series-critical-codesys-vulnerabilities/index.html

[27] Joseph M Weiss. 2007. Control Systems Cyber Security—The Need for Appropriate Regulations to Assure the Cyber Security of the Electric Grid. (2007). US Congress Testimony, October.

[28] Willem Westerhof. 2017. SMA Vulnerabilities. (2017). https://horusscenario.com/practical-proof/

[29] Kim Zetter. 2016. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. [Online]. Available: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. (2016). (Date last accessed on Jun. 7, 2017).

Table 4: Devices in EPIC. S=Siemens AG Energy Mgmt, W=Wago Kontakttechnik, H=Hirschmann Automation, SEW=SEW Eurodrive, SMA=SMA Regelsysteme, HP=Hewlett Packard

	IP	Name	Model	Manuf.
IED	172.16.1.11	GIED1	7SR1205-2JA87-1CAO/EE	S
	172.16.1.12	GIED2	7SR2203-2AA87-0EA0/DD	S
	172.16.2.11	TIED1	7SR2422-2AA87-0BA0/DD	S
	172.16.2.12	TIED2	7SR2203-2AA87-0EA0/DD	S
	172.16.2.13	TIED3	7SR2203-2AA87-0EA0/DD	S
	172.16.3.11	MIED1	7SR2203-2AA87-0EA0/DD	S
	172.16.3.12	MIED2	7SR2203-2AA87-0EA0/DD	S
	172.16.4.11	SIED1	7SR1205-2JA87-1CA0/EE	S
	172.16.4.12	SIED2	7SR1205-2JA87-1CA0/EE	S
	172.16.4.13	SIED3	7SR1205-2JA87-1CA0/EE	S
	172.16.4.14	SIED4	7SR1205-2JA87-1CA0/EE	S
PLC	172.16.1.41	GPLC	750-8202/(025-001)	W
	172.16.2.41	TPLC	750-8202/(025-001)	W
	172.16.3.41	MPLC	750-8202/(025-001)	W
	172.16.4.41	SPLC	750-8202/(025-001)	W
	172.16.5.41	CPLC	750-8202/(025-001)	W
AP	172.16.1.31	GAP	OpenBAT-R	H
	172.16.2.31	TAP	OpenBAT-R	H
	172.16.3.31	MAP	OpenBAT-R	H
	172.16.4.31	SAP	OpenBAT-R	H
	172.16.5.31	CAP1	OpenBAT-R	H
	172.16.5.32	CAP2	OpenBAT-R	H
Switch	172.16.1.1	GSW1	RSP35	H
	172.16.1.2	GSW2	RSP35	H
	172.16.2.1	TSW1	RSP35	H
	172.16.2.2	TSW2	RSP35	H
	172.16.3.1	MSW1	RSP35	H
	172.16.3.2	MSW2	RSP35	H
	172.16.4.1	SSW1	RSP35	H
	172.16.4.2	SSW2	RSP35	H
	172.16.5.1	CSW1	RSPL30	H
	172.16.5.2	CSW2	RSP35	H
VSD	172.16.5.11	VSD1	MOVIDRIVE MDX60B/61B	SEW
	172.16.5.12	VSD2	MOVIDRIVE MDX60B/61B	SEW
	172.16.5.13	VSD3	MOVIDRIVE MDX60B/61B	SEW
Solar	172.16.5.14	BATT1	SUNNY ISLAND 8.0H	SMA
	172.16.5.15	SCC	CLCON-10 (A1)	SMA
	172.16.5.16	EM	EMETER-10	SMA
	172.16.5.17	BATT2	SUNNY ISLAND 8.0H	SMA
	172.16.5.21	INV1	Sunny Tripower 10000TL	SMA
	172.16.5.22	INV2	Sunny Tripower 10000TL	SMA
	172.16.5.23	INV3	Sunny Tripower 10000TL	SMA
SCADA	172.16.5.100	HIST	-	HP
	172.18.5.60	WS	-	HP
	172.16.6.1 172.18.5.1	FW	FWEagle 30	H

A APPENDIX

We provide a list of all networked devices in EPIC in Table 4. Data flows in EPIC identified by us are summarized in Table 5.

Table 5: Data Flow in EPIC. T=Type. The arrow indicates flow direction: bi-directional (↔), uni-directional (→).

T	Source	Flow	Destination
ICMP	WS	↔	G[SW1, SW2, IED1, IED2, AP, PLC]
	WS	↔	T[SW1, SW2, IED1, IED2, AP, PLC]
	WS	↔	M[SW1, SW2, IED1, IED2, AP, PLC]
	WS	↔	S[SW1, SW2, IED1, IED2, IED3, IED4, AP, PLC]
	WS	↔	CSW[12]; CAP[12]; CPLC
IGMP	WS	→	224.0.0.22
	GCMS[AP]	→	224.0.1.76
	CAP[12]	→	224.0.1.76
	BATT[12]	→	239.12.255.[254, 255]; 239.12.1.33
	SCC	→	224.0.0.1; 239.12.255.[253,254]; 239.12.0.205
	EM	→	224.0.0.251
	INV[123]	→	239.12.0.181; 239.12.255.[254,255]
	HIST	→	239.255.255.250; 237.1.2.19; 224.0.0.[251, 252]; 234.5.6.7
MMS	GPLC	→	GIED[12]
	TPLC	→	GIED2; TIED[23]
	MPLC	→	MIED[12]
	SPLC	→	[MG]IED[12]; SIED[1234]
	WS	↔	[GTMSC]PLC; [GM]IED[12]; TIED[123]; SIED[1234]
dataUDP	HIST	→	237.1.2.19
	WS	→	237.1.2.19; 172.18.255.255; 255.255.255.255
	BATT1	→	SCC
	BATT2	→	172.16.5.17, SCC
	BATT[12]	→	239.12.255.253
	SCC	→	239.12.255.[253,255]
	SCC	↔	INV[123]
	EM	→	239.12.255.254
	INV[23]	→	239.12.255.253
SSDP	HIST	→	239.255.255.250
	WS	→	239.255.255.250
SNMP	WS	↔	[GTMSC]SW[12]
	WS	↔	GIED[12]; TIED[23]; MIED2; SIED[12]
	WS	↔	[GTMS]AP1; CAP[12]
MDNS	HIST	→	224.0.0.251
	WS	→	224.0.0.251
SMB	HIST	→	172.16.255.255
	WS	→	172.16.255.255
Other	WS	↔	SPLC (protocol: TCP-2455)
	HIST	↔	WS (protocol: dataTCP)
	CAP2	→	224.0.1.76 (protocol: IAPP)
	WS	↔	VSD3 (protocol: CLASSIC-STUN)