EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security

Sridhar Adepu(✉), Nandha Kumar Kandasamy, and Aditya Mathur

iTrust, Center for Research in Cyber Security, Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372, Singapore
adepu_sridhar@mymail.sutd.edu.sg,
{kumar_kandasamy,aditya_mathur}@sutd.edu.sg

Abstract. Testbeds that realistically mimic the operation of critical infrastructure are of significant value to researchers. One such testbed, named Electrical Power and Intelligent Control (EPIC), is described in this paper together with examples of its use for research in the design of secure smart-grids. EPIC includes generation, transmission, smart home, and micro-grid. EPIC enables researchers to conduct research in an active and realistic environment. It can also be used to understand the cascading effects of failures in one Industrial Control System (ICS) on another, and to assess the effectiveness of novel attack detection algorithms. Four feasible attack scenarios on EPIC are described. Two of these scenarios, demonstrated on EPIC, namely a power supply interruption attack and a physical damage attack, and possible mitigation, are also described.

Keywords: Critical infrastructure · Cyber Physical Systems · Smart-grid testbed · Smart-grid security · Cyber attacks

1 Introduction

A Cyber Physical System (CPS) [26] consists of a physical process controlled by a computation and communications infrastructure. Typically, a CPS contains Programmable Logic Controllers (PLCs) for computing control actions. The control actions are based on the current state of the system obtained through a network of sensors. A Supervisory Control and Data Acquisition (SCADA) workstation enables the control and monitoring of the physical process. This integration of PLCs, SCADA workstation, and other computing and communications elements is often referred to as an Industrial Control System (ICS).

Attacks against ICS have been reported on a regular basis [14]. Given our dependence on water, power, and other critical infrastructure, it is important that such infrastructure be secured against external and internal malicious actors. Researchers are investigating current and future challenges in smart grid security [16,31], and focusing on the importance of cyber security in smart grid

S. K. Katsikas et al. (Eds.): CyberICPS 2018/SECPRE 2018, LNCS 11387, pp. 37–52, 2019.
https://doi.org/10.1007/978-3-030-12786-2_3

systems. Grid modernization to realise smart grid scenarios could only be effective [36] when the overall system's safety from the perspective of cyber security, be certifiable. Researchers are utilizing real time digital simulators [22] to conduct similar studies. However, in such cases, an additional step (eventually evaluating it in a real system) would be required for implementation/translation of developed technologies. From, the survey in [11], it was observed that having the defense mechanisms evaluated in a physical testbed facilitates smoother translation of developed technologies. This motivates us to study the security in a physical smart-grid environment and contribute to the existing work.

Contributions: (a) Description of an operational Electric Power and Intelligent Control (EPIC)[1] testbed. (b) Use of EPIC in the design of novel cyber attacks on a smart-grid and assessment of the effectiveness of methods for defense against such attacks.

Organization: The remainder of this work is organized as follows: Sect. 2 presents the architecture of EPIC including physical process and communication network. Attack models and feasible attack scenarios are presented in Sect. 3 including experimental validation and the impact of selected attacks. A brief discussion on cascading effects is in Sect. 4. Similar testbeds and related work is in Sect. 5. We conclude in Sect. 6.

2 Architecture of EPIC

EPIC (Fig. 1) is an electric power testbed that mimics a real world power system in small scale smart-grid. Comprising of four stages, namely Generation, Transmission, Micro-grid, and Smart Home, EPIC is capable of generating up to 72 kVA power. It is designed to enable cyber security researchers to conduct experiments and assess the effectiveness of novel cyber defense mechanisms.

Fig. 1. EPIC control room: 360° view.

2.1 Views of EPIC

The following four views of EPIC are described next: physical process view, network architecture view, communication layout, and electrical layout.

[1] https://itrust.sutd.edu.sg/testbeds/electric-power-intelligent-control-epic/.

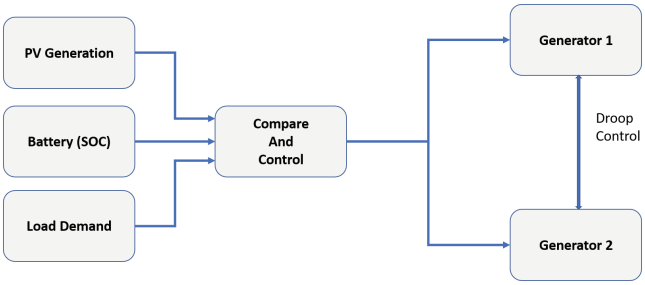

Fig. 2. EPIC physical process connectivity

Physical Process: EPIC physical process connectivity is shown in Fig. 2. It has two motor-driven generators (Generator1 and Generator2), Photovoltaic (PV) panels, Battery system–with state-of-charge (SOC) based control– and Load demand. Power required for the load demand is generated from two types of sources: motor-driven generators, and PV panels. The motor-driven generators replicate typical diesel engine-driven generators in which the mechanical power/energy is derived from the diesel engine and converted into electrical power/energy by the generator. However, having a diesel engine inside EPIC is not feasible due to laboratory constraints. Hence, a variable speed motor is used to drive the generators.

Solar power is used to meet part of the demand from critical and non-critical loads. This allows us to simulate different types of load scenarios such as peak demand, normal demand, etc. The load demand can be decoupled into real and reactive power. In any electrical bus, the real and reactive power generated needs to be balanced with the load demand for maintaining stability. In the case of EPIC, the real and reactive power balance is maintained by controlling the power from the generators and the charging process of the battery system based on the load demand (as shown by the compare and control block in Fig. 2). Droop control is used for controlling the operation of generators connected in parallel. It ensures that load shared by each generator replicates its characteristics, i.e., the speed or voltage changes with respect to the load demand, in the overall system.

EPIC Architecture: EPIC (Fig. 3) has four stages, namely Micro-grid, Smart Home, Transmission, and Generation. These atages are connected to a master PLC using a communication bus. The master PLC connects to SCADA workstation using a gateway. Each of the four stages in EPIC has its own switches, PLCs, a power supply unit, and protection and communication systems in a fiber optic ring network. The individual ring networks are shown in Fig. 4. For example, in ring HSR1, MIED1, MIED2, MSW1 and MSW2 are connected using fiber optic cables in a ring format.

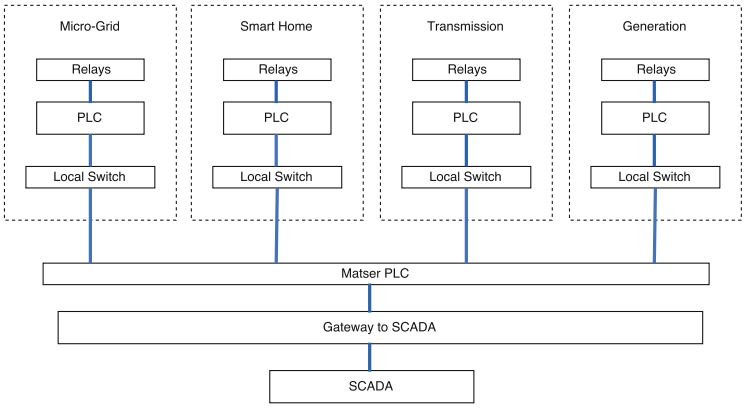

Fig. 3. EPIC architecture

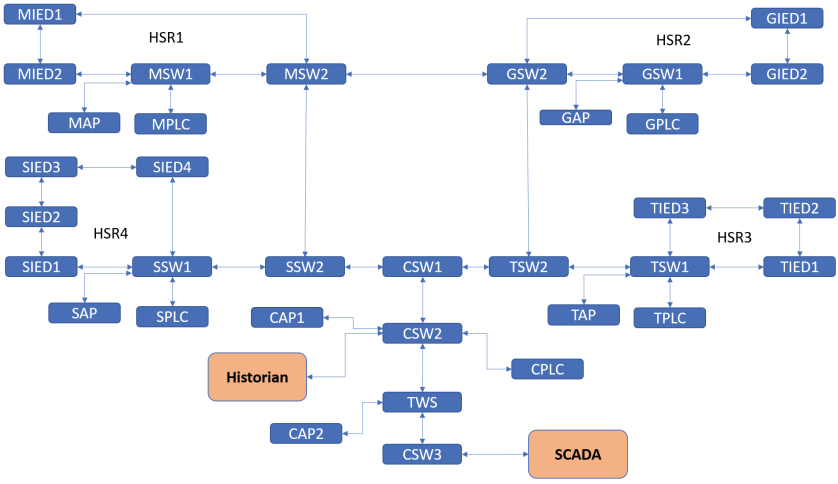

Fig. 4. The EPIC communication layout; Programmable Logic Controllers (PLCs), Intelligent Electronic Devices (IEDs), Access points (APs), Switches (SWs). PLC in generation is represented as GPLC, similarly Transmission (TPLC), smart home (SPLC), Micro-grid (MPLC). All other components in the communication layout also prefixed with G, T, S and M, respectively, for generation, transmission, smart home and micro grid.

The master PLC is responsible for the control of the overall operation. The SCADA workstation is used to monitor the entire system and provides supervisory control. PLCs manufactured by WAGO [1] corporation are used for controlling the opening/closing of breakers and also for implementing the synchronization logic for the generators. Breaker interlocks are implemented between transmission, smart home, and micro-grid to prevent a clash in the system voltages and frequency. Breaker interlocks are physical contacts that implement a

certain group of logical protection functions. For instance, an auxiliary contact from the breaker used for one generator could be used for preventing the closing of the breaker in the second generator when synchronization is not complete.

Communications Layout: The communication layout of the EPIC is shown in Fig. 4. High-availability Seamless Redundancy (HSR) and Media Redundancy Protocol (MRP) switches are used in the ring network. HSR is primarily designed for use in redundantly coupled ring topologies. It uses two network ports and incorporates a DAN H (Double Attached Node for HSR) that connects the two interfaces to form a ring. HSR achieves redundancy by sending duplicate frames from both the ports of an HSR connection. In the event of a failure of one frame, data will be transmitted via the other network path which is still intact. In case of similar failure in MRP, the network employs the Ring-Open status mode of communication. For instance, in case of failure of a link connecting two clients, both ring ports of the manager will be forwarding the packets; the clients adjacent to the failure have a blocked and a forwarding ring port; the other clients have both ring ports forwarding. Hence redundancy would be achieved.

EPIC uses the IEC 61850 [28,29] standard as a communication protocol for the electrical substation and automation system. This protocol runs over TCP/IP and is capable of obtaining a response from different parts of the system within four milliseconds. IEC 61850 includes standard features such as standardization of data names, fast transfer of events and data storage, etc.

Generic Object Oriented Substation Event (GOOSE) [15] and Manufacturing Message Specification (MMS) [40] are used in the ring network for data transfer between Intelligent Electronic Devices (IEDs) and the SCADA workstation. The fieldbus communication among physical processes to PLCs, master PLC, and SCADA is realized through selectable wired and wireless channels. Here, the operator has to choose the option of using either wired mode or wireless mode of communication. This feature enable researchers to investigate the cyber security of power grid systems in both wired and a wireless channels. For example, jamming related attacks could be studied for the wireless mode of operation.

In the communication layout (as shown in Fig. 4), apart from the SCADA and Historian, we have PLCs, IEDs, Access points (APs), Switches (SWs). PLC in generation is represented as GPLC, similarly Transmission PLC as TPLC, smart home PLC as SPLC, Micro-grid PLC as MPLC. All other components (some of the components details are shown in Table 1) in the communication layout also prefixed with G, T, S and M respectively for the generation, transmission, smart home and micro grid.

Electrical Layout: The electrical layout of EPIC is shown in Fig. 5. Main power supply for driving the prime-mover motors, referred to as M1 and M2, are obtained from the university's grid through the main circuit breaker (main CB). Having a prime-mover based generator, instead of grid-emulator [11], opens up the possibility of studying the security issues related to Automatic Governor Controllers (AGCs). AGC could be realized through variable speed drives VSD1 and VSD2. The generators referred to as G1 and G2, and the power supply

Table 1. Components in the communication layout

Component	Model	Location
SCADA system	SCADA System from PCvue solutions is used for the application. PCvue 11 is used in EPIC	SCADA System computer running on Windows 7
PLCs	PLC series 'PFC200 CS 2ETH RS' from WAGO is used in EPIC to controll various operations	Control and network panel and works based on the firmware and control logic program. Communicates with Modbus TCP/IP communication in few cases
IEDs	SIPROTEC relays from Siemens is used for protection and control in EPIC	Located in the control center and communicates with rest of the system using IEC-61850 standards. Firmware and the control logic maintains the overall process
VSD motors with dedicated firmware and control logic	SEW Eurodrive-8227136	Located at the generator room near the generators
PV and battery inverters	SMA Sunny Tripower for PV (on roof top), SMA Sunny Island for battery system (battery room). A dedicated SMA cluster controller is also used in EPIC	Control option is only enable with a 'GRID GUARD CODE', if it is enabled MODBUS TCP/IP can be used for read/write operation. Firmware update can be carried out from SCADA PC (SMA's Web portal)
Network switches	HIRSCHMANN	Network Control panel
Access points	HIRSCHMANN OpenBAT-R is used in EPIC for Wifi access points	Network Control panel

from PV and battery system is tied together in a bus, which enables options for having grid-connected as well as an islanded mode of operations. The grid-connected mode is the mode where the sources and load demand are operated in the presence of the main grid, whereas in the islanded mode only the local generators supply power to meet the demand and grid connection is disabled.

The security issues related to a transmission system could be studied using the Transformer (T1) based Tie-line. Tie-line is usually a power supply line connected in parallel to the existing distribution system and can supply additional power in the event of excess load demand or insufficient power generation.

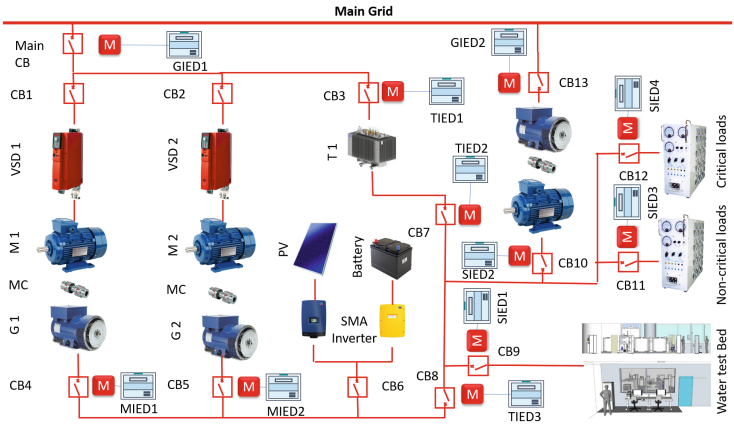

Fig. 5. Electrical layout in EPIC.

Since the transformer has the on-line tap changing functions, the security issues associated with such operations, often given less importance than deserved in the literature, could be studied. On-line tap changing function is employed in distribution transformers to avoid voltage deviations beyond the allowed limits. In many distribution systems, the allowed voltage fluctuations are to be maintained within ±5%. Whenever the voltage fluctuates beyond the allowed limits due to load fluctuations, the tap settings are changed to maintain the voltage within the limits. Hence, if an adversary gets control of the PLC in-charge of the tap-changing functions, serious voltage related issues may arise.

Components Description: (1) Two conventional generators (10 KVA each) are run by 15 kW VSD driven motors. (2) A 34 kW PV system, together with an 18 kW battery system. (3) A 15 kVA 3-phase voltage regulator. (4) Two load banks capable of emulating 45 kVA load bank. (5) 10 kW motor-generator. (6) Molded Case Circuit Breakers. (7) A SCADA system and a historian, PCvue [35] is used for programming SCADA. (8) PLC series *'PFC200 CS 2ETH RS'* from WAGO [1] is used in EPIC to control the process, and Codesys[2] [12] for programming the PLCs.

3 Experiments with EPIC

The following attack scenarios were designed using the attacker profiles in [37]: power supply interruption attacks (nation-state profile), nuisance tripping attacks (cyber-criminal), physical damage attacks (insider profile), and attacks related to economic advantage (nation-state). The four attack scenarios, and two selected scenarios implemented in EPIC, are described next.

[2] CoDeSys is an integrated development environment for programming controllers such as WAGO PLCs.

3.1 Feasible Attack Scenarios

Based on the vulnerability analysis of the power grid, different attacks can be designed and launched to capture the grid behavior in terms of affected components, properties, performance [5] and the cascading failures of the system. It is feasible to launch a variety of attacks on EPIC and study their impact. Four such attack types, discussed in the literature, are described below.

1. *Power supply interruption:* These are false data injection attacks on SCADA and PLC system that can lead to power supply interruption or tripping the overall system. An attack on the load demand control, either on the load banks or on other connected test-beds, can result in underutilization of the system components. False data injection attacks on local EMS may increase the active power from the renewable energy source and battery system.
2. *Nuisance tripping:* Malware attack on the firmware of PLCs can result in nuisance tripping by triggering the protection functions in IEDs. Such an attack could result in extended power supply interruption (intermittent). Nuisance tripping attacks can also be launched on secondary control from utilities or local EMS by disabling active power curtailment of renewable energy sources [25].
3. *Physical damage:* Though attacks that can cause physical damage [44] are not directly launched on EPIC, the process can be emulated using the motor-generator load combination and load banks for power system components such as battery systems. The attack could be false data injection such as erroneous voltage and temperature measurement in battery systems or attack on the firmware of power conversion system.
4. *Economic advantage:* These are false data injection attacks which can create an economic gain [21] to the attacker such as recording reduced or increased amount of power injected from the renewable energy sources. False data injection attacks on the control systems of various components, to cause accelerated aging or over utilization, can also be launched on the local EMS, PLCs, and the SCADA workstation.

From the four possible attack scenarios mentioned above, two attacks were selected and are explained in detail in the remainder of this section.

3.2 Power Supply Interruption Attack

During the normal operation of EPIC, circuit breakers CB1, CB4, CB8, and CB12 must be closed to supply power to the critical loads (Fig. 5). The SPLC (smart home PLC) controls the opening and closing of CB12. Whenever power supply is required for the critical load, a close command is issued from the SCADA to the SPLC. Subsequently, the SPLC (Control CodeX as in Fig. 6) issues a command to the IEDs to close CB12. The affected IED will eventually control the closing operation of the breaker thus enabling power to the critical loads.

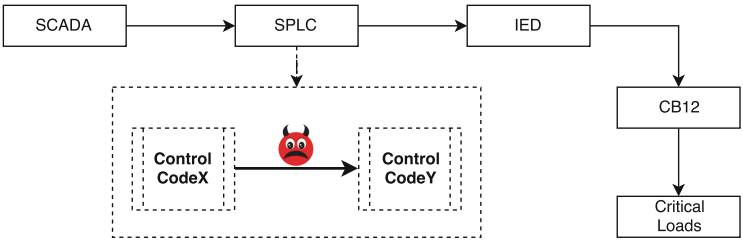

Fig. 6. Power supply interruption attack

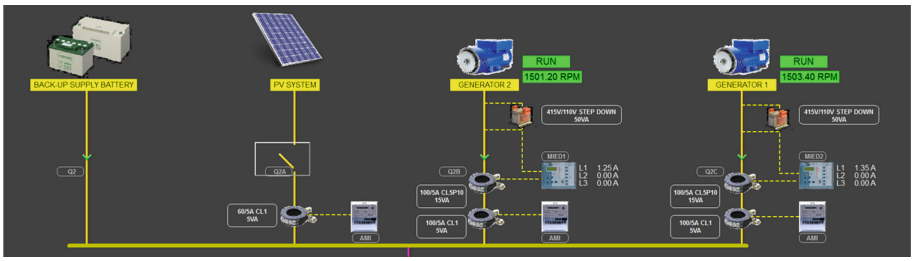

Fig. 7. Protection with machine learning predictors in IED layer for attack targeting complete destruction of SBS.

Attack Design: We assume that the attacker's intention is to interrupt power to the critical loads. The attacker can achieve this intent by opening the circuit breaker CB12, giving a false indication, i.e. "the breaker is closed," to the operator through the SCDA workstation, and disabling further closing of the circuit breaker.

Attack Vector: The attacker uses the vulnerabilities [13,33] to enter the SCADA workstation. Vulnerabilities in CoDeSys (see footnote 2) are used to modify the control code inside a PLC.

EternalBlue [10,24]*:* This exploit focuses on Microsoft Windows and was used in the WannaCry ransomware attack in 2017. EternalBlue [33] is vulnerability CVE-2017-0144 [13] in the server message block (SMB) protocol.

CoDeSys Unauthenticated Command-Line Access [32]*:* The CODESYS allows remote attackers to execute commands via the command-line interface and transfer files. This vulnerability allows an attacker to obtain administrative access to the PLC logic thus enabling the modification of the control logic.

Experiments and Results: Two experiments were conducted. In each case, EPIC was run in normal mode and then the attack was launched. In the first experiment power was supplied to the critical loads as desired. In the second experiment, the EternalBlue exploit was used to enter the SCADA workstation and

used the vulnerabilities in CoDeSys to upload the malicious control code to the SPLC. The original control code is shown as *Control CodeX* in Fig. 6 and the malicious control code as *Control CodeY*. As a result, the circuit breaker opened immediately, the command to close the breaker was disabled, and the SCADA workstation reported the circuit breaker as closed. Hence, the operator observing the screen at the SCADA workstation was unable to control the circuit breaker (CB12). As intended, this attack resulted in power supply interruption to the critical loads.

Mitigation: To overcome the EternalBlue vulnerability, the windows-based machine needs to be updated to the latest version of the operating system. However, CoDeSys vulnerability does not have any possible mitigation measures at the time of writing this paper.

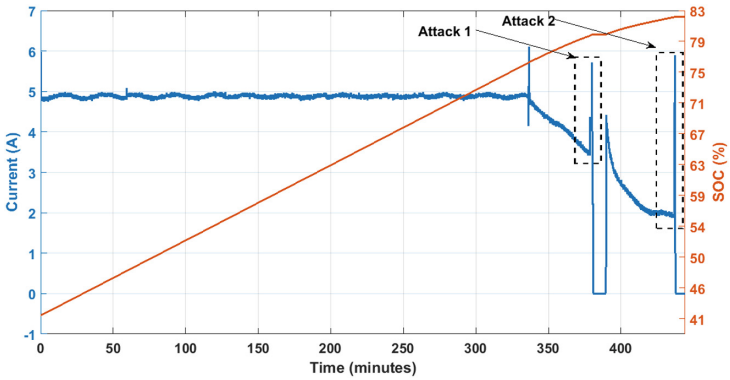

Fig. 8. Impact of Attack 1 and Attack 2 on the charging current of the battery system.

3.3 Physical Damage Attack

Figure 7 shows the portion of EPIC used for in this study, namely the "BACKUP-SUPPLY BATTERY" used only for supplying control power during a complete black-out. The "BACKUP-SUPPLY BATTERY" is charged using Generator 1 and Generator 2. The measurements from MIED1 and MIED2 represent the charging current of the battery. During normal operation, the battery is charged with a constant current (approximately 5A) until 75% SOC and a continuously decreasing current beyond 75% SOC.

Attack Design: The intention of the attacker is to increase the charging current in the region beyond 75% SOC and lead to increased temperature and eventually physical damage to the battery.

Attack Execution: It is assumed that the attacker is capable of modifying the measurements carried out by the Battery Management System (BMS) of the inverters, and can cause overcharging resulting in physical damage to the batteries. The attack scenario of overcharging the battery is implemented by adding load in the downstream to avoid any possible physical damage to the battery system. Doing so will result in increased charging current as seen by MIED1 and MIED2.

Experiment and Results: I Fig. 8, shows the impact of Attack 1 and Attack 2 on the battery charging current. Inherently, the IDMT scheme in IEDs is not designed to protect the increase in current during the CV region as technically no over current is seen by the system. However, continuously supplying higher current in the CV region will result in increased temperature and hence physical damage to the battery system.

Mitigation: A new model is proposed by combining the Inverse Definite Minimum Time (IDMT) concept in over-current protection with machine-learning based predictors and the actual charging current of the battery system. The tripping time, i.e. enabling protection against physical damage is given as follows.

$$T_{trip} = \frac{k * m}{\int_{n-k}^{n} (\frac{|I_n^m| - |I_n^p|}{I_n^p})^2}, \tag{1}$$

where $\forall\ I_n^m > 0\ \&\ |I_n^m| - |I_n^p| > 0$, k is the time taken for charging/discharging at rated current, I_n^m is the current measured at n^{th} time stamp, I_n^p is the output from machine learning algorithm which is not described in this paper (the algorithm similar to the one described in [23] can be used for prediction), and m is the on-field trip setting multiplier.

The equation for the tripping time is derived from the standard IDMT protection [34] by including I_n^p along with I_n^m rather than using I_n^m alone. Hence, the scheme, instead of relying only on the measured value, uses the deviation from usual value predicted by the machine learning predictors. The square term in the equation is used for getting an extremely inverse characteristics, i.e., speed of tripping increases at a much faster pace compared to the error, as described in standard IDMT and summation of past k values to identify the cumulative variation rather than instantaneous transients. Such transients are usually eliminated by including the time component [34]. In practice, m is selected by the operator based on heuristics, a usual procedure for IDMT protection. In the experiment, m is chosen as 1, and the authors did not change m as no nuisance tripping was observed. As the IEDs do not have in-built modules for implementing the protection scheme, the above protection scheme is implemented using PLCs (MPLC) for the system in Fig. 7 and the results are in Fig. 8.

Figure 8 shows the charging current of the battery system. It can be observed that the transient at the 325th minute is not identified as an attack as the cumulative error was within the limit. The system restored quickly back to the normal state from the transient state. The attack scenarios near 360th minute (Attack 1)

and 440th minute (Attack 2) were successfully identified and the system protected. It can be observed from Fig. 8 that the battery system is protected by tripping the entire system based on the measurement from IEDs through circuit breaker 'Q2' in the distribution control/switchboard. Tripping is indicated with zero current in Fig. 8.

The transients post attack scenario (after Attack 1 around 400th minute) is not mis-identified as an attack. The speed at which the system should trip could be controlled by changing the value of m which is an on-field variable similar to trip selector setting in the IDMT protection scheme. Choice of m is crucial as higher value for m results in under protection (higher possibility of damage) and lower value for m results in over protection (nuisance tripping). A heuristic approach would be suitable for selecting m. It was observed that the overall time taken for the protection scheme to identify the attack and protect the system was in the order of seconds.

4 Cascading Effects

Many CPSs depend on one another and are connected via some physical or cyber infrastructure. For example, a public transit system uses electricity and hence is connected to the power grid via several intermediate elements each of which could also be considered a CPS. Such interconnections through one or more infrastructure CPS lead to the following challenge. *What methods and tools are needed to understand the cascading effects of cyber attacks in one CPS on other connected CPS?* It is important to consider this challenge in the context of interconnected CPSs. For example, the impact of cyber attacks on a smart meter in a smart grid could propagate to other subsystems in the grid before progressing outside of the grid to other connected systems.

EPIC supplies power to two testbeds, namely a Secure Water Treatment (SWaT) and a Water Distribution (WADI) SWaT [30] is a scaled down water treatment plant that is capable of producing five gallons/minute of filtered water. SWaT has a six-stage filtration process that mimics a large modern water treatment plant. WADI [8] is an operational testbed supplying 10 US gallons/min of filtered water. It represents a scaled-down version of a large water distribution network in a city. This connection between three plants allows one to study the interdependencies between CPS and how cyber attacks on one can affect the other. Such work is helpful in advancing the design of secure interconnected public infrastructures. CPSs often depend on each other implying that a disturbance due to cyber attack in one is likely to have a significant impact on the operation of another. Significant attention is currently being devoted to ensuring that such systems are resilient to cyber attacks. The notion of cyber security was nearly non-existent when many of these systems were designed and built. Hence, while such systems may be functionally sound, they are prone to successful cyber attacks as has been demonstrated in the past [43]. Thus, subsystems for intrusion prevention and detection, network attack detection, and the like are being installed in the existing CPSs to prevent and detect cyber attacks.

5 Related Work

Research related to work in this paper is divided into two parts: work related testbeds and that related to attack scenarios.

Similar Testbeds: There exist a number of electric power testbeds. Some of these allow simulation of large systems and do not actually produce electric power. Simulation based testbeds allow large scale attack analysis. Operational testbeds offer more realistic environments and scenarios than those based exclusively on simulation. [9] presents efforts to model the smart power grid in real time by developing a *"smart grid testbed"*. A smart grid testbed for electric power distribution system is presented in [42]. This system is designed to emulate distribution grid by focusing on analyzing power system components, renewable energy integration, power quality issues, and consumer load behavior in the smart distribution grid. Pulau Ubin pilot Micro-grid Test-Bed [17] is located in Singapore at the jetty area of Pulau Ubin– an island north-east of Singapore. This test-bed aims to assess the reliability of electricity supply within a micro-grid infrastructure using intermittent renewable energy sources such as solar photovoltaic (PV) technology. This micro-grid mainly focuses on clean energy, reliable electricity supply, cost competitive electricity and scalability issues at present. A software based smart grid testbed for evaluating substation cyber security was reported in [20]. Due to the importance of smart-grid security, researchers have focused on the development of smart grid testbeds. [11] provides a four step taxonomy based on smart grid domains, research goals, test platforms, and communication infrastructure. The Cyber-Physical Experimentation Environment for RADICS (CEER) at The University of Illinois at Urbana-Champaign employs a production quality software to flexibly (and remotely) define experiments, configure testbed resources, and run an experiment. EPIC can serve as a useful hybrid of the above systems (the hybrid of physical process and cyber-layer forming an ICS), by implementing both cyber and physical processes for security research. The physical process can be defined and configured using the PLCs and SCADA system, as well as any specific Energy Management System. Based on the physical process, the desired attack scenarios and defense mechanisms can be implemented and tested using an array of network components available in EPIC.

Attacks and Attack Scenarios: Grid modernization to realize smart grid scenarios could only be effective [36] if the overall system's safety from cyber security perspective is satisfied. Though, many research efforts utilizing real time digital simulators [22] are underway, having the defense mechanisms evaluated in a physical testbed offers advantages in terms of implementation/translation of developed technologies as indicated in [11]. A resilient architecture for the smart grid is presented in [27]. Researchers have reported case studies on power substation networks [18]. Privacy preserving methods in the advanced metering infrastructure based on the influence of dataset characteristics is presented in [41]. Integrity attacks on real time pricing in smart grids [19] were investigated against their impact and countermeasures. Security of economic dispatch

in power system operations has been investigated [38]. In [39], authors present an overview of the network services provided by devices found in EPIC and discuss how this information can be used to implement practical threat scenarios.

In the future, we are planning to use EPIC testbed similar to our water testbed and conduct experiments [2–4,6,7] which we already conducted on SWaT.

6 Conclusion and Future Work

This paper presents a smart grid testbed named EPIC for research in the design of secure smart-grids. Also presente are possible attack scenarios, consequences of such attacks, and potential mitigations. The combination of testbeds and dependency among the testbeds enables the design of realistic scenarios. The connection of EPIC to two other testbeds for water treatment and water distribution enables the study of impact of multiple simultaneous attacks on two or more CPSs. Design of additional attacks, and mitigations, are planned for the future.

References

1. Wago Programmable Logic Controllers (2009). http://www.wago.us
2. Adepu, S., Mathur, A.: An investigation into the response of a water treatment system to cyber attacks. In: Proceedings of the 17th IEEE High Assurance Systems Engineering Symposium, Orlando, January 2016
3. Adepu, S., Mathur, A.: Distributed attack detection in a water treatment plant: method and case study. In: IEEE Transactions on Dependable and Secure Computing (2018, to appear)
4. Adepu, S., Mathur, A.: Distributed detection of single-stage multipoint cyber attacks in a water treatment plant. In: Proceedings of the 11th ACM Asia Conference on Computer and Communications Security, pp. 449–460. ACM, New York, May 2016
5. Adepu, S., Mathur, A.: Generalized attacker and attack models for cyber-physical systems. In: Proceedings of the 40th Annual International Computers, Software and Applications Conference, Atlanta, USA, pp. 283–292. IEEE, June 2016
6. Adepu, S., Shrivastava, S., Mathur, A.: Argus: an orthogonal defense framework to protect public infrastructure against cyber-physical attacks. IEEE Internet Comput. **20**(5), 38–45 (2016)
7. Adepu, S., Mathur, A.: Assessing the effectiveness of attack detection at a hackfest on industrial control systems. arXiv preprint arXiv:1809.04786 (2018)
8. Ahmed, C.M., Palleti, V.R., Mathur, A.: WADI: a water distribution testbed for research in the design of secure cyber physical systems. In: The 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, April 2017
9. Biswas, S.S., Kim, J.H., Srivastava, A.K.: Development of a smart grid test bed and applications in PMU and PDC testing. In: 2012 North American Power Symposium (NAPS), pp. 1–6 (2012)

10. Caulfield, T., Ioannidis, C., Pym, D.: The U.S. vulnerabilities equities process: an economic perspective. In: Rass, S., An, B., Kiekintveld, C., Fang, F., Schauer, S. (eds.) GameSec 2017. LNCS, vol. 10575, pp. 131–150. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-68711-7_8
11. Cintuglu, M.H., Mohammed, O.A., Akkaya, K., Uluagac, A.S.: A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutor. **19**(1), 446–464 (2017)
12. CODESYS: Codesys-industrial IEC 61131–3 PLC programming (2018). https://www.codesys.com/
13. CVE-2017-0144: Windows SMB remote code execution vulnerability (2017). https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
14. ICS-CERT Advisories (2018). https://ics-cert.us-cert.gov/advisories
15. Du, L., Liu, Q.Y.: The design of communication system on the real-time relay protection based on goose. In: 2012 Asia-Pacific Power and Energy Engineering Conference, pp. 1–5 (2012)
16. Dumitrache, I., Dogaru, D.I.: Smart grid overview: infrastructure, cyber-physical security and challenges. In: 2015 20th International Conference on Control Systems and Computer Science, pp. 693–699 (2015)
17. EMA: Pulau ubin micro-grid test bed (2013). https://www.ema.gov.sg/Pulau_Ubin_Micro-grid_Test_Bed.aspx
18. Formby, D., Walid, A., Beyah, R.: A case study in power substation network dynamics. Proc. ACM Meas. Anal. Comput. Syst. **1**, 19 (2017)
19. Giraldo, J., Cárdenas, A., Quijano, N.: Integrity attacks on real-time pricing in smart grids: impact and countermeasures. IEEE Trans. Smart Grid **8**, 2249–2257 (2017)
20. Gunathilaka, P., Mashima, D., Chen, B.: SoftGrid: a software-based smart grid testbed for evaluating substation cybersecurity solutions. In: Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy. CPS-SPC 2016 (2016)
21. He, Y., Mendis, G.J., Wei, J.: Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans. Smart Grid **8**(5), 2505–2516 (2017)
22. Hernandez, M., Ramos, G., Lwin, M., Siratarnsophon, P., Santoso, S.: Embedded real-time simulation platform for power distribution systems. IEEE Access **6**, 6243–6256 (2017)
23. Kandasamy, N.K., Badrinarayanan, R., Kanamarlapudi, V.R.K., Tseng, K.J., Soong, B.H.: Performance analysis of machine-learning approaches for modeling the charging/discharging profiles of stationary battery systems with non-uniform cell aging. Batteries **3**(2), 18 (2017)
24. Kharraz, A.: Techniques and solutions for addressing ransomware attacks (2017)
25. Langner, R.: Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur. Priv. **9**(3), 49–51 (2011)
26. Lee, E.A.: Cyber-physical systems: design challenges. Technical Report UCB/EECS-2008-8, EECS Department, University of California, Berkeley, January 2008. http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html
27. Lopez, J., Rubio, J.E., Alcaraz, C.: A resilient architecture for the smart grid. IEEE Trans. Industr. Inf. **14**, 3745–3753 (2018)
28. Mackiewicz, R.: Overview of IEC 61850 and benefits. In: Power Systems Conference and Exposition, 2006. PSCE 2006. 2006 IEEE PES, pp. 623–630. IEEE (2006)

29. Mascarella, D., Chlela, M., Joos, G., Venne, P.: Real-time testing of power control implemented with IEC 61850 GOOSE messaging in wind farms featuring energy storage. In: 2015 IEEE Energy Conversion Congress and Exposition (ECCE), pp. 6710–6715 (2015)
30. Mathur, A.P., Tippenhauer, N.O.: SWaT: a water treatment testbed for research and training on ICS security. In: International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater), USA, pp. 31–36. IEEE, April 2016
31. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Secur. Priv. **7**, 75–77 (2009)
32. MITRE: CVE-2012-6068 (2012). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6068
33. Nakashima, E., Timberg, C.: NSA officials worried about the day its potent hacking tool would get loose. Then it did. Washington Post (2017). https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loosethen-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html
34. Paithankar, Y.G., Bhide, S.: Fundamentals of Power System Protection. PHI Learning Pvt. Ltd., New Delhi (2011)
35. PcVue: PcVue: versatile HMI-SCADA software (2018). https://www.pcvuesolutions.com/index.php/products-a-technology/pcvue-hmiscada-48583
36. Qi, J., Hahn, A., Lu, X., Wang, J., Liu, C.C.: Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys. Syst.: Theory Appl. **1**(1), 28–39 (2016)
37. Rocchetto, M., Tippenhauer, N.O.: On attacker models and profiles for cyber-physical systems. In: Askoxylakis, I., Ioannidis, S., Katsikas, S., Meadows, C. (eds.) ESORICS 2016. LNCS, vol. 9879, pp. 427–449. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45741-3_22
38. Shelar, D., Sun, P., Amin, S., Zonouz, S.: Compromising security of economic dispatch in power system operations. In: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2017)
39. Siddiqi, A., Tippenhauer, N.O., Mashima, D., Chen, B.: On practical threat scenario testing in an electric power ICS testbed. In: Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, pp. 15–21 (2018)
40. Sørensen, J.T., Jaatun, M.G.: An analysis of the manufacturing messaging specification protocol. In: Sandnes, F.E., Zhang, Y., Rong, C., Yang, L.T., Ma, J. (eds.) UIC 2008. LNCS, vol. 5061, pp. 602–615. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-69293-5_47
41. Tudor, V., Almgren, M., Papatriantafilou, M.: The influence of dataset characteristics on privacy preserving methods in the advanced metering infrastructure. Comput. Secur. **76**, 178–196 (2018)
42. Tunaboylu, N.S., Shehu, G., Argin, M., Yalcinoz, T.: Development of smart grid test-bed for electric power distribution system. In: 2016 IEEE Conference on Technologies for Sustainability (SusTech), pp. 184–187 (2016)
43. Weinberger, S.: Computer security: is this the start of cyberwarfare? Nature **174**, 142–145 (2011)
44. Zeller, M.: Myth or reality? Does the aurora vulnerability pose a risk to my generator? In: 2011 64th Annual Conference for Protective Relay Engineers, pp. 130–136 (2011)