



Attacks on smart grid: power supply interruption and malicious power generation

Sridhar Adepu¹ · Nandha Kumar Kandasamy¹ · Jianying Zhou¹ · Aditya Mathur^{1,2}

Published online: 4 July 2019
© Springer-Verlag GmbH Germany, part of Springer Nature 2019

Abstract

Electric power supply is an essential component for several sectors including manufacturing, healthcare, building management, water distribution, and transportation systems. Hence, any interruption in electric power is likely to have an undesirable impact on the overall operation of any residential or commercial ecosystem. The serious impacts of power supply interruption attacks have been realized in the recent cyber incidents such as the Ukraine power blackout. It is also evident from recent incidents that both network and process vulnerabilities are crucial for an adversary to cause an adverse impact on the operation. This paper reports an investigation into power supply interruption and malicious power generation attacks focusing on process and network vulnerabilities. The investigation was conducted in two steps: First, a vulnerability assessment was conducted on a fully operational electric power testbed. Next, the vulnerabilities discovered were exploited to perform different types of power supply interruption attacks and malicious power generation attacks. The attacks were executed using control code modification and SMA, a PV converter manufacturer, portal manipulation. The attacks reported here are useful for researchers and smart-grid operators to design and develop effective protection, detection, and response mechanisms.

Keywords Critical infrastructure · Cyber-physical systems · Smart-grid security · Industrial control system · Cyber-attacks · SCADA security · Power interruption attacks · Malicious power generation

1 Introduction

A cyber-physical system (CPS) [30] consists of a physical process controlled through a computation and communication infrastructure. CPSs have become ubiquitous in modern life, e.g., software controlling cars, airplanes, and even critical public infrastructure such as water treatment plants and railways. A CPS is often a complex engineering system that integrates embedded computing technology into the physical

phenomena. For example, in an energy storage system (ESS), a programmable logic controller (PLC)/embedded controller may start the charging process of the ESS during energy surplus. However, the charging process must be stopped when the ESS reaches a predetermined state-of-charge (SOC) limit. The SOC of the ESS is usually computed by the PLC using various sensors such as voltage, current, and temperature. The PLCs/controllers in a CPS can be viewed as a system that transforms the state of the process. At any instant, the PLCs receive data from sensors, compute the control actions, and apply these actions to specific devices. In an ESS, the actuators include bidirectional power electronic converters and circuit breakers, while the sensors include voltage, current, and temperature sensors.

Power systems and smart-grids are often geographically spread and require intelligent control to operate. Automation increases the vulnerability of the system to cyber-attacks [6,33]. Many government agencies such as Homeland security and ICS-CERT reported [23] attacks against power systems. Researchers are investigating the current and future challenges in smart-grid security [38] and focusing on the importance of cyber-security in smart-grid systems.

✉ Sridhar Adepu
adepu_sridhar@mymail.sutd.edu.sg

Nandha Kumar Kandasamy
kumar_kandasamy@sutd.edu.sg

Jianying Zhou
jianying_zhou@sutd.edu.sg

Aditya Mathur
aditya_mathur@sutd.edu.sg

¹ iTrust, Singapore University of Technology and Design, 8 Somapah Rd, Tampines, Singapore

² Department of Computer Science, Purdue University, 610 Purdue Mall, West Lafayette, USA

Grid modernization to realize smart-grid scenarios could only be effective [56] if the overall system's safety from cyber-security perspective is satisfied. Many research efforts utilizing real-time digital simulators [20] are being carried out across the world. However, in terms of implementation/translation of developed technologies, it is important to evaluate the defense mechanisms in a physical testbed [4,12].

The need for studying the inherent differences between the theoretical and actual industrial-grade systems motivated us to study the security of a physical smart-grid system developed based on modern industrial standards and contribute to the existing work. This work is an attempt to identify common vulnerabilities that may be overlooked due to a standard operating procedure in smart-grid domain. Note that a well-known vulnerability in network safety might be overlooked in a CPS environment as the upgrading process is usually less frequent. Hence, it is important to evaluate the impact of cyber-attacks and demonstrate these in a testbed.

Contributions: (a) Experimental investigation into the exploitation of vulnerabilities in the Electric Power and Intelligent Control (EPIC) testbed. (b) Design and launch of attacks using multiple procedures. (c) Analysis of the impact of attacks on EPIC.

Novelty: Attacks reported in the literature focus primarily on transmission systems, loss of a line that can create undesirable loading on remaining lines and generators, automatic generation controllers (AGC) [31,39], etc. Little attention has been paid to the distribution systems or the individual components that are more vulnerable than the highly secured transmission systems. For example, to the best of our knowledge, the possibility of attack scenarios on commonly used renewable energy inverters through a conventional home personal computer (PC) is not reported in the literature. This paper demonstrates that such overlooked common vulnerabilities could be effectively used to attack smart-grids, particularly the distribution systems having multiple energy sources.

Further, for an adversary to cause impact on the operation, it is essential to have both network and process vulnerabilities. Lack of anyone would result in an attack that does not benefit the attacker. For example, the popular Stuxnet [29] was successful because the acceleration resulted in degradation of the centrifuges; if the acceleration were not to cause machine degradation, the attack would have been a harmless intrusion. In this paper, we investigate both network and process vulnerabilities to design attacks. Note that a network vulnerability might be a reported CVE (common vulnerabilities and exposures) or a never reported zero day vulnerability. *Organization* The remainder of this work is organized as follows: Preliminaries and background details are discussed in Sect. 2. Attack design is described in Sect. 3. Section 4 presents the architecture of EPIC—an industrial-grade smart-grid testbed. Vulnerabilities in EPIC are detailed in Sect. 5.

Attacks on circuit breakers and power settings are presented in Sects. 6 and 7, respectively. Section 8 presents the malicious power generation attack.¹ Discussion on experiments and analysis of reported attacks is presented in Sect. 9. Related work and conclusions are discussed in Sects. 10 and 11, respectively.

2 Preliminaries and background

This section introduces the context in which the problem is studied, smart-grid environment, the possibility of modifying control logic in PLCs and how to launch attacks using PLC logic manipulation, modification of SMA portal settings, modification of communication channel, and vulnerability assessment in an Industrial Control System (ICS).

2.1 Problem context

Power supply is crucial for the effective operation of many sectors such as manufacturing, health care, building management, and water systems. Furthermore, a major portion of the transportation network is already electrified, e.g., in metro rail systems or in the process of electrification, e.g., electric vehicles [65]. Hence, an interruption in the power supply would have a hazardous impact on the overall operation of any residential, industrial, and commercial ecosystem [60]. The impacts of power supply interruption attacks have been realized in the recent cyber incidents such as the Ukraine power blackout [33] which affected over 200,000 civilians. The economic impact of power supply interruption on industrial sectors could be correlated from regular load shedding process in developing countries [3,9]. Though these interruptions are not due to cyber-attacks a similar, if not more, impact is expected.

Attacks on power supply availability could be even more fatal when they affect the health sector, as most of the medical devices as well as storage of medicines often need uninterrupted power supply [19]. Other sectors such as water distribution, transportation, and communications are also inter-dependent on the power supply availability [54]. Given the ability to interrupt the power supply, an attacker could either carry out attacks resulting in major blackout such as the Ukraine power blackout [33] or can even target individual organizations. For example, a power supply interruption attack on the data centers [24] serving a financial sector could cause chaos in finance and business sectors [54].

A simple power supply interruption attack to a single high-rise residential building could affect the occupants with lack

¹ Malicious power generation can subsequently lead to accelerated aging and hence possible power supply interruption. Hence, we have considered it as a stealthy way of achieving power supply interruption.

of water supply (operation of the overhead water pump needs electricity), communications, etc. This simple power supply interruption would result in approximately S\$790² loss for the utility company for a single building in addition to any regulatory fines. Given the above scenarios, it is important to investigate the power supply interruption attacks on ICS found in common systems such as industries, commercial buildings, and residential buildings.

Malicious power generation It is a special class of attack which can be defined as the attack that affects the normal operation of power generation by a given set of generators, in such a manner that the balance is affected in multiple aspects. For example, if two generators are designed to supply equal power, the attack can target to modify the balance say to 75:25. In doing so, the attacker can (1) increase the losses (as higher current is flowing in one generator), (2) increase the aging factor of the overloaded generator, (3) increase the wear and tear of the overloaded generator and hence the maintenance schedule, and (4) finally, create an unexpected trip (power supply interruption) during peak load conditions.

Note that aging of any electrical equipment is linked to its loading level and has a nonlinear relationship; the higher the loading, the faster would be the aging. For example, IEEE standard C57.91-1995 and later versions provide detailed information on loading and its relation to the aging process for transformers.

2.2 Smart-grids

Though there is no widely agreed upon definition of smart-grid, a generally accepted description is “an electricity supply network that uses digital communication technologies to detect and react to local changes in usage.” Hence, a smart-grid would have components enabled with information and communication technologies (ICT). The ICT and intelligence could be effectively used to increase the robustness, efficiency, etc. For example, in a conventional grid, during peak hours, the only way to manage the generation-demand balance is to generate as much energy as needed, possibly resulting in higher losses. In the case of smart-grids, ICT together with intelligence could be used to shift the non-critical load to off-peak periods and hence reduce the losses. A high-level architecture of a smart-grid is shown in Fig. 1; it can be observed that the smart-grid contains multiple interacting components. The interactions between individual sources/loads at the residential level to the bulk power operation level introduce vulnerabilities that were nonexistent, or not common, prior to the advent of smart-grids.

Communication structure in smart-grids Smart grid usually consists of distributed control systems ranging from home

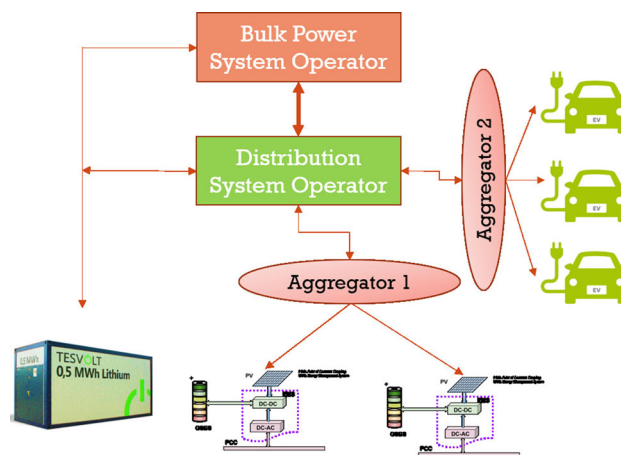


Fig. 1 Electric power distribution system architecture [15]. Aggregators for distributed generation and electric vehicles, bulk energy storage connected to distribution system operator, and its interaction with bulk power system operator can be observed

energy management systems (HEMS) to distribution energy management system [55]. The control system itself is a collection of PLCs, each controlling a specific portion of the physical process. State of the physical process is collected by sensors and sent to the controller (PLC). Based on the control logic in PLC, it takes the decision regarding actuator commands, which is forwarded to the actuators. Each PLC communicates with a set of sensors and actuators via a local network using a multilayer network that is also referred to as the *field bus* network [61].

Power systems There are various terminologies in the study of power systems; however, for this study, it is important to know what are apparent power, real power, and reactive power, and their relationship with voltage and frequency. The choice of apparent power (S_n) is important in the design of electrical equipment; apparent power can be considered equivalent to the physical limit or maximum capacity. The apparent power has two components, namely real power (P_n) and reactive power (Q_n), represented as $S_n = P_n + jQ_n$. This relationship among apparent, real, and reactive power is shown in Fig. 2 as the power triangle.

Mismatch in power generated and consumed may lead to instability. Mismatch in real power causes frequency stability-related issues, whereas reactive power mismatch causes voltage stability-related issues [59]. Decreasing the real power leads to frequency drop while increasing the real power leads to an increase in frequency. Reactive power consumption would result in a voltage drop, and reactive power injection would result in a rise in voltage.

2.3 Control logic modification

A PLC includes firmware and control logic, where changes to the firmware are protected with hashing algorithms and

² <https://www.ema.gov.sg/cmsmedia/News/Media%20Release/2016/SP%20Services%20Rolls%20Out%20Redesigned%20Bill.pdf>.

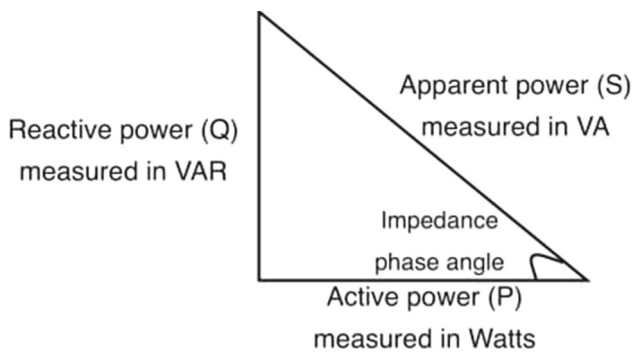


Fig. 2 Power triangle relating apparent power to active (real) power and reactive power (Pythagorean theorem)

digital signatures. However, control logic modifications in most cases are not protected by any measure [18]. Thus, an attacker could tamper with the PLC control logic either by gaining physical access to it or over the network.

Access to the PLC logic and the ability to modify the control logic offer an attacker direct physical access or access to a network. When an attacker has access to the development software, the attacker can upload the modified control logic into the PLC or download the original version from it [69]. The intent of an attacker might be to launch a denial of service attack or to compromise the sensor and actuator readings [18] in the PLC logic. Even though it might be considered straightforward to identify whether an attacker can get into the system, exploring the capabilities is essential for the design of defense strategies. Hence, using an operational smart-grid, this paper explores the capabilities of an attacker upon entry.

Denial of service attack By adding a piece of code in the ladder logic of a PLC program, the PLC could be thrown out of control or stopped. It eventually damages the process being controlled by the particular PLC. The malicious code sometimes brings the PLC state into an infinite loop; in this case, the PLC is inactive in controlling the concerned physical process.

Sensor, actuator manipulation By changing the PLC code in the ladder logic of a PLC program, one can change the data that are extracted from the remote input–output (RIO) unit and send the modified data to the control logic.

2.4 Modifying SMA settings

SMA portal [62] is a web-based application protected by username and password. SMA portal is an essential component for defining the operation of converters used for solar photovoltaic (PV) systems and ESS. Though there are no reported cases of a security breach in SMA's web portal, it is not impossible to do so. The attacker could either use the stored user name and password in a Supervisory Control and

Data Acquisition (SCADA) workstation or may crack the password to get into the web application. The web application has many settings that control the overall operation of the inverters in the system. For example, the maximum power setting determines the maximum power supplied by the inverter, which could be used to create an imbalance if used at an appropriate time. The network-related settings are further protected with an additional password named as “*GRID GUARD CODE*”. Hence, the attacker should have access to the unique password to control the inverters using Modbus/TCP-IP.

In the above scenario, it is assumed that the attacker has access to a SCADA workstation and is capable of modifying the settings in the SMA portal. The attacker might have direct physical access or access through the network. In this case, the intent of an attacker is to change the settings in such a way that bidirectional power flow will affect the power balance in the system.

2.5 Modifying communication channel

The communication infrastructure of a smart-grid is often connected to an external network. Such connections render a smart-grid susceptible to cyber-attacks. The presence of wireless communications among the smart-grid infrastructure makes it even more vulnerable to cyber-attacks. Such attacks could compromise the communication links between sensors and PLCs, as well as the links among the PLCs. Once one or more such links have been compromised, an attacker could use one of the several strategies to send fake state data to one or more PLCs possibly leading to component damage. *Compromise through direct physical access* An inside attacker with direct physical access has a range of additional options. In this case, the attacker could re-wire networking cables and manipulate the sensors. The attacks could be denial of service, MITM, and data injection.

2.6 Vulnerability assessment in ICS

Vulnerability assessment follows the steps:³

1. listing assets and resources in the system,
2. assigning importance to the resources,
3. identifying security vulnerabilities in each asset and resource, and
4. proposing mitigation for the most serious vulnerabilities.

To understand the vulnerabilities in an ICS, it is also important to understand the processes/steps through which an attacker could exploit these. An attacker who wishes to attack

³ <https://www.secureworks.com/blog/vulnerability-assessments-versus-penetration-tests>.

an ICS may go through the following steps before launching the attack: gain access to the ICS network, perform reconnaissance and understand the process, and gain control of the ICS.

Kaspersky [26] summarized the findings of their research on ICS vulnerabilities as follows: (1) The number of vulnerabilities in ICS components keeps growing, (2) vulnerabilities are exploitable, (3) ICS vulnerabilities are widely diversified, and (4) not all of the vulnerabilities found in 2015 are fixed. Over the years, the number of vulnerabilities being reported has increased. To be more specific, “19” vulnerabilities were reported in 2010, whereas the number of vulnerabilities reported in 2015 was “189.” Even though many vulnerabilities are removed by the product manufacturers, owing to operational reasons, the ICS management might postpone the upgrades. At least 5% of the vulnerabilities published by ICS-CERT were not fully fixed. Sometimes the vulnerable component might be removed from the market and vendor support may not be available for such components.

3 Attack design

Our focus is to investigate, in the context of a smart grid, capabilities of an attacker including access rights and the parameters an attacker could, and needs to, manipulate to achieve a specific goal. Though this work does not focus on complete threat modeling for smart grid systems, parameter manipulations discussed can be linked to various threat models. We describe the identification of parameters and the limits at which the physical process reaches vulnerable state. For example, a fully charged battery is vulnerable to damage under attack, but a battery with 50% state of charge, i.e., how full the battery is, still has time to reach the state where it is vulnerable to physical damage.

The focus in this work is on two kinds of vulnerabilities: (1) network vulnerabilities including all cyber vulnerabilities such as in PLCs and network and (2) process vulnerabilities including process interconnections and how an attacker can damage the physical process as, for example, in malicious power generation discussed in the later part of this section. The attacks designed and described in this work are based on the specific attacker goals such as power interruption and malicious power generation. The attacker can leverage on any of the existing or novel threat models to execute such attacks, i.e., the attack design is always applicable to the system and is independent to the network threat model employed.

Attacker’s capability We classify an attacker’s capability based on the type of access, namely: (1) access to control logic and the modification rights that are achieved through one of the vulnerabilities, (2) access to communication channels in the plant network and rights to modify them, (3) access to SMA settings in the SCADA PC and rights to modify them,

and (4) access to perform a DDoS attack. Based on the above attacker capabilities, two classes of attacks were designed: power interruption and malicious power generation.

Power interruption attacks Two classes of power supply interruption attacks are demonstrated based on the observation from an experimental smart-grid operating under normal circumstances. This operational model is investigated under the following scenarios: (1) the attacker manipulates circuit breakers in different stages (generation, transmission, smart-home, and micro-grid; for example, an attacker might *close* or *open* one or more circuit breakers, and (2) the attacker manipulates power settings in different stages as for example, by modifying the maximum power settings in different power generation sources.

(1) Attacker manipulates circuit breakers in different stages Here we consider a smart-grid as consisting of four stages including generation, transmission, micro-grid, and smart-home. Each stage is controlled by its own PLC/controller, and communication channels exist between the SCADA, Distributed Control Systems (DCS), and Energy Management System (EMS) to each PLC/controller and between the PLCs/controllers. It is possible for an attacker to (a) enter into the communication network and manipulate the control tags that are being issued by PLCs/controllers, (b) target any one of the PLC/controllers to perform a DDoS attack and make it inactive, (c) manipulate the PLC/controller logic to perform different kinds of attacks, and (d) enter the SCADA workstation and manipulate the settings in the SMA portal. Based on the above four modes, an attacker can manipulate different actuators, circuit breakers in this case, in different parts of the smart-grid to perform power supply interruption attacks.

(2) Attacker manipulates the power settings in different stages By changing the power settings from the originally intended settings, an attacker could achieve power supply interruption. Power settings can be manipulated as follows: (a) Through PLC code alterations such as, for example, by adding malicious code that sends a higher speed, hence higher power, to the Variable Speed Drive (VSD) to affect the power balance and hence trip the system. (b) Setting portals, for example the maximum power, say in SMA web portal, of the bidirectional inverter could be set higher than the maximum load demand in the micro-grid which will cause the system to trip due to power imbalance. (c) Communication channel for example, the speed commands sent to the VSD from a PLC could be modified such that the VSD runs at a higher speed than required which will affect the power balance and hence trip the system. Based on the above three approaches, an attacker can manipulate the power settings to achieve an intent.

Malicious power generation Here an attacker’s intention is to manipulate the power generated by different generators. This can be achieved by loading a particular generator heav-

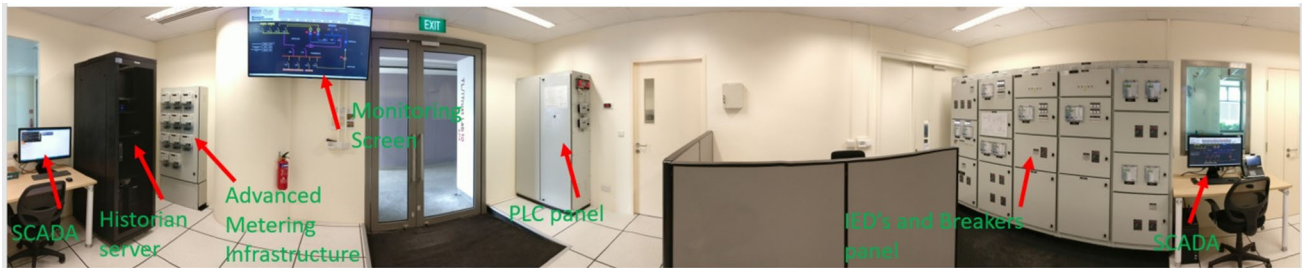


Fig. 3 EPIC control room, 360-degree view. The picture shows different physical components including the SCADA workstation, IED and breaker panel, PLC panel, Historian server, advanced metering infrastructure (AMI), and the monitoring screen

ily in order to cause damage either in terms of accelerated aging or by affecting the maintenance schedule. In this work, for malicious power generation, we consider the attacks on Real Power Generation (P) and not Reactive Power Generation (V). It can be observed that the attack design focuses on disturbing the process before looking at the network vulnerabilities in detail. We believe that it is an important step in developing the defense mechanism for smart grid components which are geographically distributed and might be practically impossible to protect all the components at all instances. The choice of defense implementation has to be derived based on the existence of process vulnerabilities in addition to any from network vulnerabilities.

4 Architecture of EPIC

This section presents the structure of EPIC. Pictorial views of EPIC⁴ are shown in Fig. 3 [1]. EPIC is an electric power testbed which reflects the real world power system in a small-scale smart-grid. It consists of four stages, namely generation, transmission, micro-grid, and smart-home and is capable of generating 72 kVA of power.

Generation (G): In this stage, local generators produce the power required for the remaining stages. The motors connected to the generators are driven by the university grid supply where EPIC is housed. **Transmission (T):** With the help of transformers, this stage supplies/distributes power to the smart home stage. **Micro-grid (M):** With the help of PV and batteries, this stage acts as an extra source of power generation and storage. **Smart Home (S):** This stage has two load banks rated 15 kVA and 30 kVA. The other two water test beds, namely SWAT and WADI [1], are also connected at this stage. EPIC is capable of simultaneously supplying power to both testbeds.

Communications layout The communication layout (Fig. 4) consists of High-availability Seamless Redundancy (HSR) and Media Redundancy Protocol (MRP) switches that are

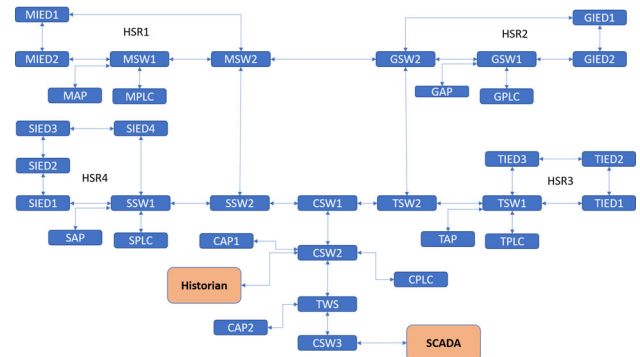


Fig. 4 EPIC communication layout: programmable logic controllers (PLCs), intelligent electronic devices (IEDs), access points (APs), switches (SWs). PLC in generation is represented as GPLC, similarly transmission (TPLC), smart-home (SPLC), micro-grid (MPLC). All other components in the communication layout also prefixed with G, T, S, and M, respectively, for generation, transmission, smart-home, and micro-grid

used in a ring network for redundancy. EPIC uses the IEC 61850 [37] standard as a communication protocol for the electrical substation and automation system. The communication layout (Fig. 4) consists of the SCADA workstation, Historian, PLCs, Intelligent Electric Devices (IEDs), Access points (APs), and Switches (SWs).

Component description (1) Two conventional generators, each 10 kVA, are run by 15-kW VSD-driven motors. (2) A-34 kW PV system, together with an 18-kW battery system. (3) A-105 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. (8) PCvue [53] is used for programming SCADA and CoDeSys [13] for programming the PLCs. **Electrical layout** The electrical layout of EPIC is shown in Fig. 5. Main power supply for driving the prime mover motors (representing diesel engines), referred to as M1 and M2, is obtained from the university's grid through the main circuit breaker (main CB). The generators referred to as G1 and G2, and the power supply from PV and battery system, are tied together in a bus, which opens the options for having grid-connected as well as an islanded mode of operations.

⁴ <https://itrust.sutd.edu.sg/research/testbeds/electric-power-intelligent-control-epic/>.

Fig. 5 Electrical layout in EPIC. *CB* circuit breaker, *VSD* variable speed drive, *M* motor, *IED* intelligent electric device. Electrical connections are shown in red lines, and mechanical coupling is shown as "MC" (color figure online)

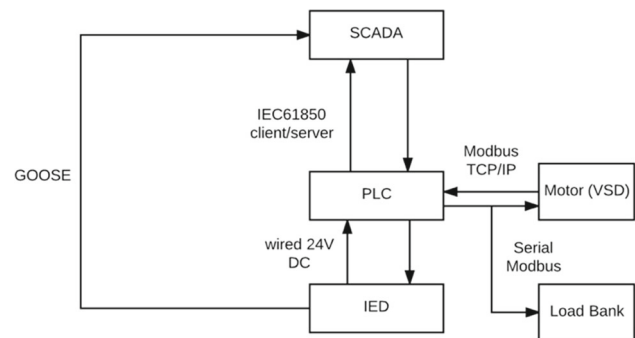
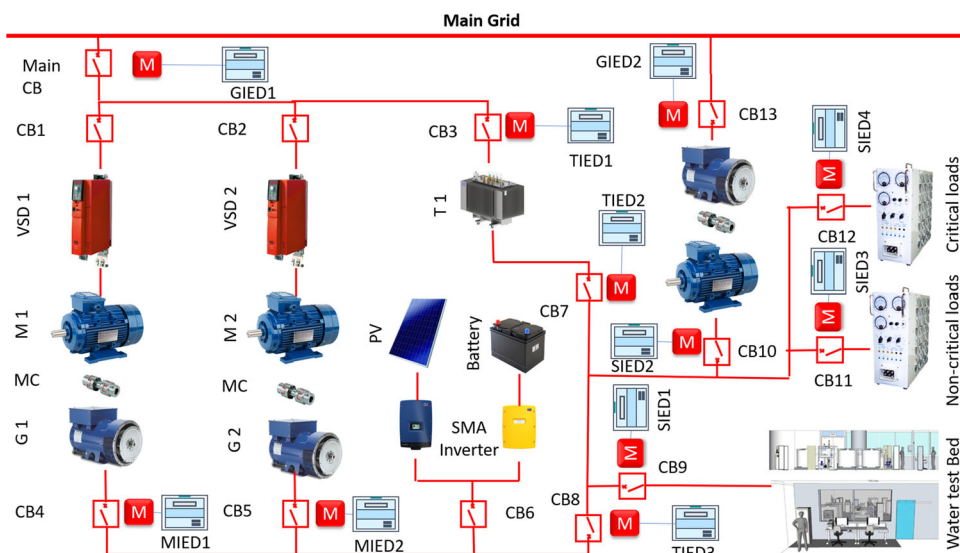


Fig. 6 Network flows in EPIC shows the different communication protocols employed between different components in the testbed

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 load demand and the grid connection is disabled. Having a prime mover-based generator, instead of grid emulator [12], opens up the possibility of studying the security issues related to AGC. AGC could be realized through variable speed drives VSD1 and VSD2.

Network flow Network flow in EPIC is shown in Fig. 6. It consists of data obtained from the IEDs which are then processed by PLCs. Based on the control logic in the PLCs, commands are issued to the end devices such as VSDs, load demand, and also to the SCADA system for monitoring and supervisory control. Client-server communication is used between SCADA, PLCs, and IEDs. EPIC uses different communication protocols including Modbus TCP/IP, Modbus serial, IEC 61850 standard, and GOOSE.⁵ EPIC uses the IEC 61850 communication protocol for the electrical substa-

tion and automation system. GOOSE and MMS⁶ are used in the ring network for data transfer between relays and the SCADA workstation. PLCs communicate to variable speed drives and load banks through the Modbus channel.

5 Vulnerability assessment in EPIC

Vulnerability assessment is carried out by following the steps described in Sect. 2.6

List of assets and resources in the system The assets in EPIC are listed in Table 1. Note that vulnerability assessment depends on the components used in the system. SCADA workstation is running on a windows machine in EPIC which has an EternalBlue exploit. It is possible for a remote attacker to access the system and manipulate or execute malicious commands.

In PLCs (Table 1:WAGO), the host is running on an outdated SSH server. This dropbear has multiple vulnerabilities and handles the client-server applications. It allows a remote attacker to upload arbitrary or malicious code and a local attacker to access the process memory. While PLC is communicating through Modbus, the attacker can use dropbear SSH (multiple vulnerabilities) to enter into PLC and manipulate the process.

IEDs are located in the control center and communicate with the rest of the system using IEC 61850 protocol. Different IEDs protect different parts of the system such as motors, generators, transformer, and loads. The firmware and control logic of the IEDs are updated through dedicated ports and limit the access to authorized personnel. There are no reported vulnerabilities in IEDs with respect to firmware and control logic. However, during the maintenance period,

⁵ Generic Object Oriented Substation Events.

⁶ Manufacturing Message Specification.

Table 1 Assets table

Asset/resource type	Version/model used	Location
SCADA system	SCADA system from PCvue solutions is used for the application. PCvue 11 is used in EPIC	SCADA system is running on a personal computer with Windows 7 OS
PLCs	PLC series “PFC200 CS 2ETH RS” from WAGO is used in EPIC to control various operations	Control and network panel, and works based on the firmware and control logic program. Communicates using Modbus TCP/IP communication in few cases
IEDs	SIPROTEC relays from Siemens are 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 maintain the overall process. The Firmware update is through a dedicated port
VSD	SEW Eurodrive along with the corresponding motor is used in EPIC	Located in motor/generator room and has dedicated firmware and control logic. The Firmware and configuration update can be carried from SCADA PC
PV and battery inverters	SMA Sunny Tripower is used for PV (on roof top); SMA Sunny Island is used for battery system (battery room). A dedicated SMA cluster controller is also used in EPIC.	Control option is only enabled with a “GRID GUARD CODE”; if it is enabled, MODBUS TCP/IP can be used for read/write operation. The 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

firmware or control logic can be modified by an attacker. Such modifications can have a serious impact on the physical safety of the process.

VSDs are used to control the speed of the motors (similar to a diesel engine in real cases) that are “mechanically coupled” to respective generators and hence are used to control the speed of the generators. The VSDs have a firmware and a control logic that could be updated/modified from the SCADA workstation. An insider, with access to the workstation, can upload malicious code/logic into the VSD, which eventually affects the physical process and the system. The VSDs also receive the speed settings via Modbus TCP/IP protocol. The Modbus protocol does not employ any security feature and hence is vulnerable to attacks on the communication channel.

The password sync [42] feature in Hirschmann switches allows an attacker to obtain sensitive information by sniffing the network. This enables an attacker to intercept the packets in the network and modify them. The vulnerabilities [47–

51] in Hirschmann wifi access points and switches allow an attacker to hijack and manipulate the packets.

PV and battery inverters Network control option can only be enabled with a “GRID GUARD CODE.” Once it is enabled, MODBUS TCP/IP can be used for read/write operation. Malicious commands could be sent to the inverters through Modbus vulnerabilities. A firmware update can be carried out from SCADA PC (SMA’s Web portal). The *EternalBlue* vulnerability can also be exploited to obtain access to SCADA workstation and subsequently to the SMA web portal. This access could be used to change the maximum operating power of the inverters that can affect system stability.

Vulnerabilities ICS-CERT [23] has identified many vulnerabilities in generic ICS/SCADA systems, and a subset relevant to the EPIC is listed in Table 2.

EternalBlue EternalBlue [52] is a vulnerability in server message block (SMB) protocol and is mentioned in CVE-2017-0144 [14] catalog. SMB server mishandles the packets from remote attackers eventually allowing access to the sys-

Table 2 Vulnerability information

S. no.	Vulnerability	Description
1	CVE-2017-0144	This vulnerability focuses on Microsoft Windows and was used in the wannaCry ransomware attack
2	CVE-2016-7406 CVE-2016-7407 CVE-2016-7408 CVE-2016-7409	The Dropbear SSH vulnerability allows a remote attacker to enter the system and execute malicious code
3	CVE-2012-6068	This vulnerability enables an unauthorized attacker to get administrative access to the control logic in the PLCs
4	CVE-2017-0267 CVE-2017-0268 CVE-2017-0269	There are several vulnerabilities in Microsoft's server message block that enables access to stored files

tem. Attacks similar to the “wannaCry” attack were studied in automotive sector [72] and identified as an emerging threat to critical infrastructures and ICS.

Dropbear SSH 2016.74.0 with multiple vulnerabilities Dropbear is a client–server application. When a remote host is running an outdated SSH server, there exist multiple vulnerabilities that could be exploited. The common vulnerabilities are listed next. (1) When handling the usernames, format flaw exists [43] and is triggered as a string format. This allows an attacker to execute arbitrary code. (2) Improved OpenSSH files allow a context-dependent attacker [44] to execute malicious code. (3) Flaws in dbclient allow remote attacker [45] to execute arbitrary code and, during compilation [46], allow a local attacker to access process memory.

CoDeSys⁷ Unauthenticated Command-line access CoDeSys allows remote attackers to execute commands via the command-line interface and transfer files. This vulnerability allows an unauthorized attacker to obtain administrative access to PLC logic and modify the control logic [41].

Default admin password on the web server: [21,23] Usually manufacturers use a set of default passwords during installation and configuration of their hardware and software. If the operating management fails to change the default passwords, the attacker can use those default passwords provided by the manufacturer and exploit the concerned system. Later it could be used to modify the functions of the overall control system.

⁷ CoDeSys is a development environment for programming controllers such as WAGO PLCs.

6 Attacks on circuit breakers

Based on the assessment carried out in EPIC, we identified the vulnerabilities described in Sect. 5. Information described above was used in the design and execution of power supply interruption attacks by manipulating the circuit breakers and their status.

6.1 Attack design

A total of 16 attacks that can be launched on EPIC were designed (Table 3). The attacks could be launched at different stages and using four different parameter manipulations.

Experiment A The attack for this experiment is designed based on the assumption that the attacker uses vulnerabilities such as EternalBlue, SMB, and CoDeSys to compromise the network and can modify and upload PLC code into different PLCs. During the attack, the adversary modifies the code such that when the respective CB is closed, the code automatically opens the CB and gives a false indication to the SCADA system and the operator. A prefix G is added to indicate that the attack is carried out on the PLC controlling the generator CBs and prefixes T, M, and S are used for transmission, micro-grid, and smart-home, respectively.

Experiment B The attack for this experiment is designed based on the assumption that the CB is open and the DDoS attack is launched on the corresponding PLC which disables closing of the CB. It could also be assumed that the attack is launched immediately after a trip operation such that the operator would not be able to close the CB. This could either be realized from the network or by using malicious code uploaded into the PLC forcing it to enter an infinite loop immediately after the trip operation. It is assumed that either the attacker has the same capabilities as in *Experiment A* or is already inside the network.

Experiment C The attack for this experiment is designed such that the packets sent from the SCADA workstation to the PLCs are modified such that a close operation is altered to an open operation and a false data indicating closed status is sent back to the SCADA system. It is assumed that the attacker is already inside the network.

Experiment D The attack in this experiment is designed based on the assumption that the attacker uses vulnerabilities such as EternalBlue, SMB, and CoDeSys to enter the network and can modify the power settings in the web portal. It is also assumed that the attacker either uses the stored password or has the capability to crack it. During the attack, the attacker waits until the trip operation and then executes a DDoS attack. Combining Experiments A through D with four stages G–S, we derived 16 different attacks. For example, when *Experiment A* is conducted on the generation stage, it is labeled as *Experiment GA*. In *Experiment GA*, the attack is launched on

Table 3 Attack matrix on circuit breaker

Stages/ways	PLC code (A)	DDoS (B)	MITM (C)	SCADA PC + DDoS (D)
Generation (G)	PLC code of the GPLC is modified to trip the breakers CB, CB1, and CB2. A false indication is sent to SCADA	GPLC is the target; a DDoS is executed on it	The attacker modifies the command from SCADA to GPLC and the indication from GPLC to SCADA	The attacker modifies the power setting in SMA portal to trip the whole system and does a DDoS on the GPLC
Transmission (T)	PLC code of TPLC is modified to trip the breakers CB7 or CB8. A false indication is sent to the SCADA.	TPLC is the target; a DDoS is executed on it	The attacker modifies the command from SCADA to TPLC and the indication from TPLC to SCADA	The attacker modifies the power setting in SMA portal to trip the whole system and does a DDoS on the TPLC
Micro-grid (M)	PLC code of MPLC is modified to trip the breakers CB4 and CB5. A false indication is sent to the SCADA	MPLC is the target; a DDoS is executed on it	The attacker modifies the command from SCADA to MPLC and the indication from MPLC to SCADA	The attacker modifies the power setting in SMA portal to trip the whole system and does a DDoS on the MPLC
Smart-home (S)	PLC code of SPLC is modified to trip the breakers CB9 to CB12. A false indication is sent to the SCADA	SPLC is the target; a DDoS is executed on it	The attacker modifies the command from SCADA to SPLC and the indication from SPLC to SCADA	The attacker modifies the power setting in SMA portal to trip the whole system and does a DDoS on the TPLC

the GPLC to either open CB, or CB1 and CB2, or all three circuit breakers. The attack matrix is shown in Table 3.

6.2 Attack execution

Vulnerabilities mentioned in Sect. 5 were exploited to enter the system and manipulate the respective control tags in different ways such as mutating data across communication channels, PLC logic manipulation, and DDoS.

Experiment A Dropbear SSH vulnerability and unauthenticated command-line access in CoDeSys allow the attacker to manipulate the PLC code. These two vulnerabilities were used to manipulate the PLC code.

Experiment B This experiment was conducted by sending 1 million UDP packets per second to the concerned PLC to render it non-responsive and/or inactive.

Experiment C In this experiment, the vulnerabilities in a communication channel were used to enter into the network and an MITM attack between the SCADA workstation and PLC was launched.

Experiment D This experiment exploited the vulnerabilities in Windows 7 OS to enter the SCADA workstation and perform DDoS and/or modifications on the web portal.

6.3 Results: experiment A (PLC code manipulation)

This subsection presents outcomes observed during the power supply interruption attack based on manipulation of the control code in PLCs. The attack can be correlated with experiments GA, TA, MA, and SA.

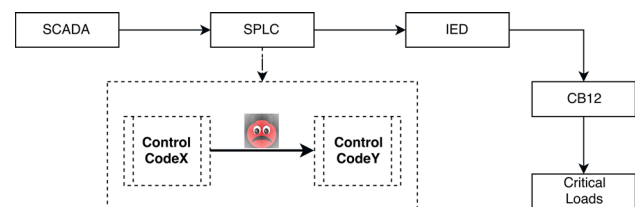


Fig. 7 Power supply interruption attack, showing the process in which the attacker modifies the control code using one of the existing vulnerabilities

Original system During normal operation, in order to supply power to the critical loads, circuit breakers CB1, CB4, CB8, and CB12 (Circuit Breakers (CB_x) shown in Fig. 5) should be closed. SPLC controls the opening and closing of CB12. Whenever power supply is required for the critical loads, a close command is issued from the SCADA to the SPLC. The SPLC has the control code (Control Code_X shown in Fig. 7) that issues a subsequent command to the SIED4 for closing CB12. SIED4 will eventually control the closing operation of the breaker and enables the power supply to the critical loads.

Attack design The attacker's intention is to interrupt power to the critical loads. An attacker can achieve this intent by opening the circuit breaker, e.g., CB12 and respective CBs in other cases, giving a false indication to the operator through SCADA and disabling further closing of the circuit breaker. *Attack vector:* In this experiment, EternalBlue exploit was used to enter the SCADA workstation and those in CoDeSys to upload malicious control code into the SPLC. The original and malicious control codes are shown as *Control Code_X* and

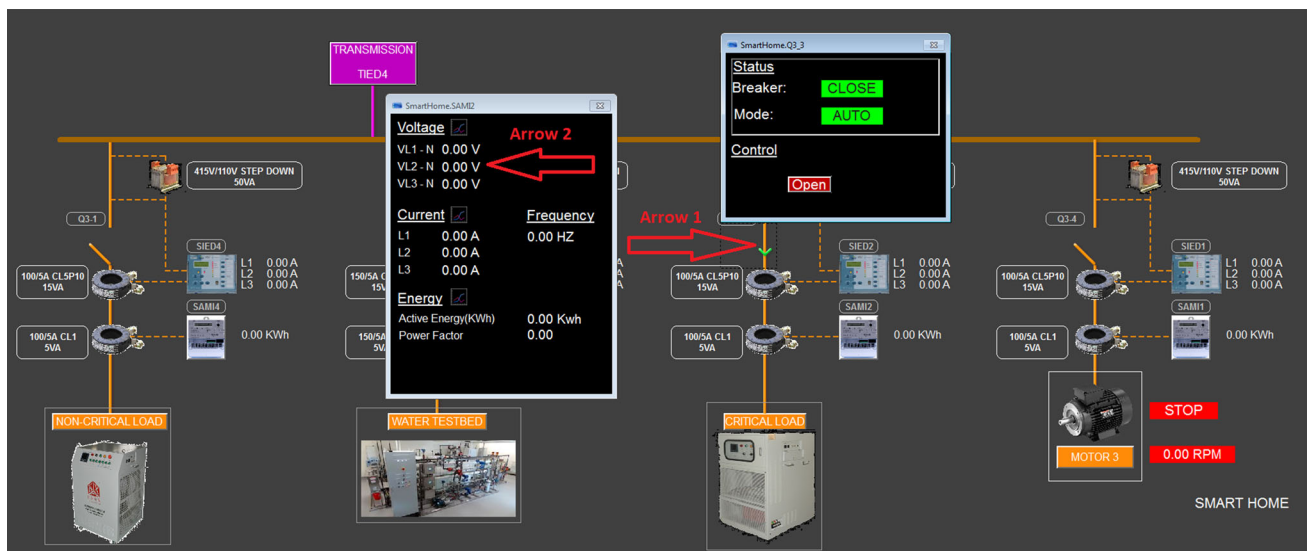


Fig. 8 SCADA screenshot showing the status after the attack was launched, arrow 1 shows the closed indication of CB, but arrow 2 shows the voltage (zero) measured by the meter below, indicating that no power supply was available, i.e., CB is open

Control Code Y, respectively, in Fig. 7. As a consequence, the circuit breaker opened immediately after a close command was executed, further close commands were disabled, and a false close status was displayed at the SCADA screen. Hence, the operator at the SCADA workstation was unable to control CB12. This resulted in a power supply interruption to the critical loads. This is observed from Fig. 8 where arrow 1 shows the “close” status of CB, but arrow 2 shows the voltage (zero) measured by the meter below, indicating that no power was available, i.e., the CB is open. This experiment was repeated for all the cells shown in the attack matrix in Table 3. The experiment was conducted using two scenarios, namely operation under the normal scenario, i.e., the power is supplied to the critical loads, and operation under malicious scenario, i.e., the power is not supplied to the critical loads.

6.4 Results: Experiments B and D (DDoS attack)

In this case, the attacker uses the vulnerabilities of the communication channels to enter the network and flood the PLCs with UDP packets. After the network was flooded with UDP packets, the circuit breaker was tripped; the operator was unable to control the tripped breaker.

The screenshots in Figs. 9 and 10 are from the SCADA workstation under normal scenario and when the attack was executed on SPLC, respectively. The results are identical for all PLCs, and hence, only the results corresponding to SPLC are presented.

7 Attacks on power settings

In this section, we describe how the knowledge of network vulnerabilities identified in Sect. 5 was used to manipulate the power settings of different energy sources to realize power supply interruption.

7.1 Attack design

The attacks are similar to those in the attack matrix in Table 3 and presented in Table 4. A brief description of the attacks is as follows.

Experiment A The difference from the previous attack matrix in Table 3 is that an attacker modifies the PLC code such that the speed settings sent to VSD are modified to a higher value, say, by 1%.

Experiment B A static setting is sent to the VSD, following which the PLC becomes inactive as a result of DDoS. Hence, the VSD/generator will not respond to changes in load demand.

Experiment C In this attack, the attacker modifies the commands issued by PLC before they arrive at the VSD.

Experiment D The attacker modifies the power settings in SMA portal to trip the entire system.

Table 4 shows that there are few cells where “*Not applicable as there are no generators*” is mentioned. This is due to the fact that there were no generators available for manipulation in such cases. For example, the transmission stage does not have any generator and is shown in Fig. 5. Hence, there are no components for modifying speed/power settings. Web portal-based power settings are only available for PV/battery inverters, and hence, “*web portal*”-based settings are not

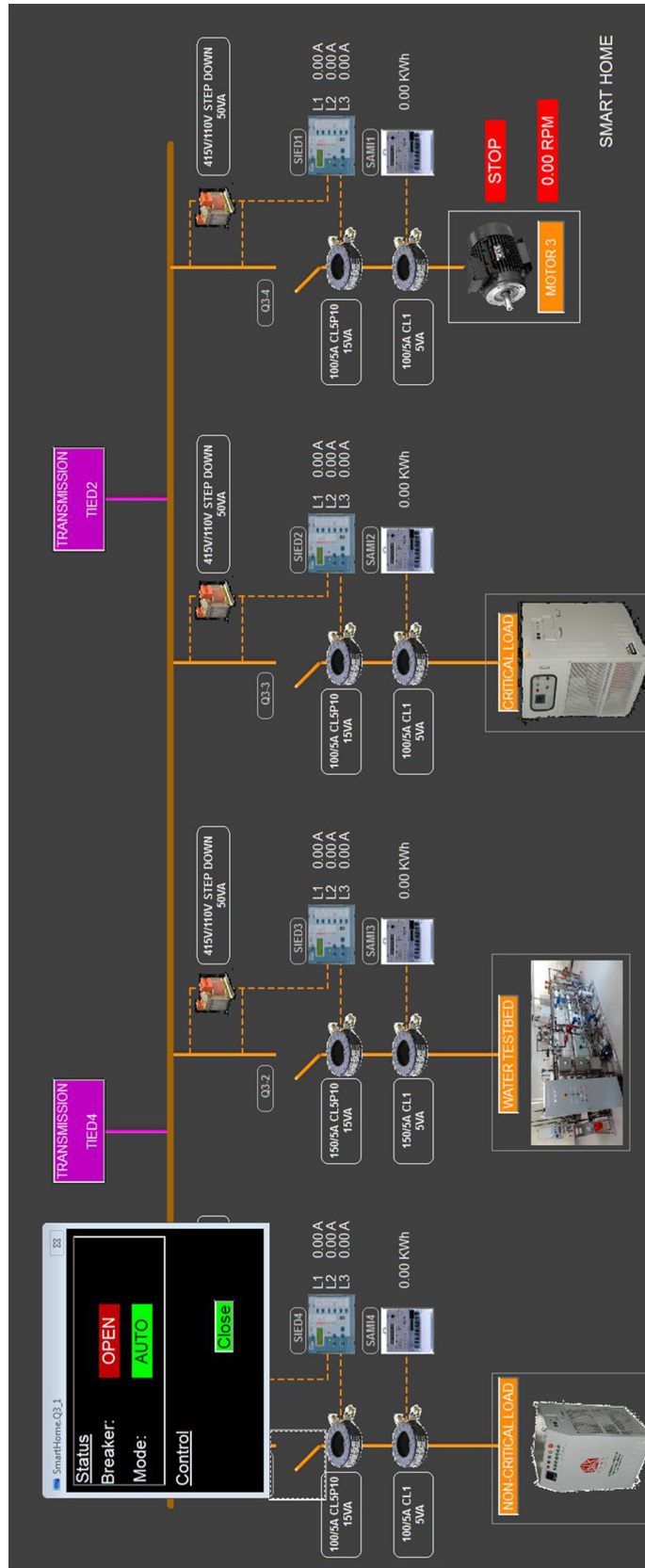


Fig. 9 Smart-home without DDoS attack: the circuit breaker is in normal operation, which can be observed from the control command being enabled and valid state, i.e., open status and AUTO mode displayed. Refer to Fig. 10

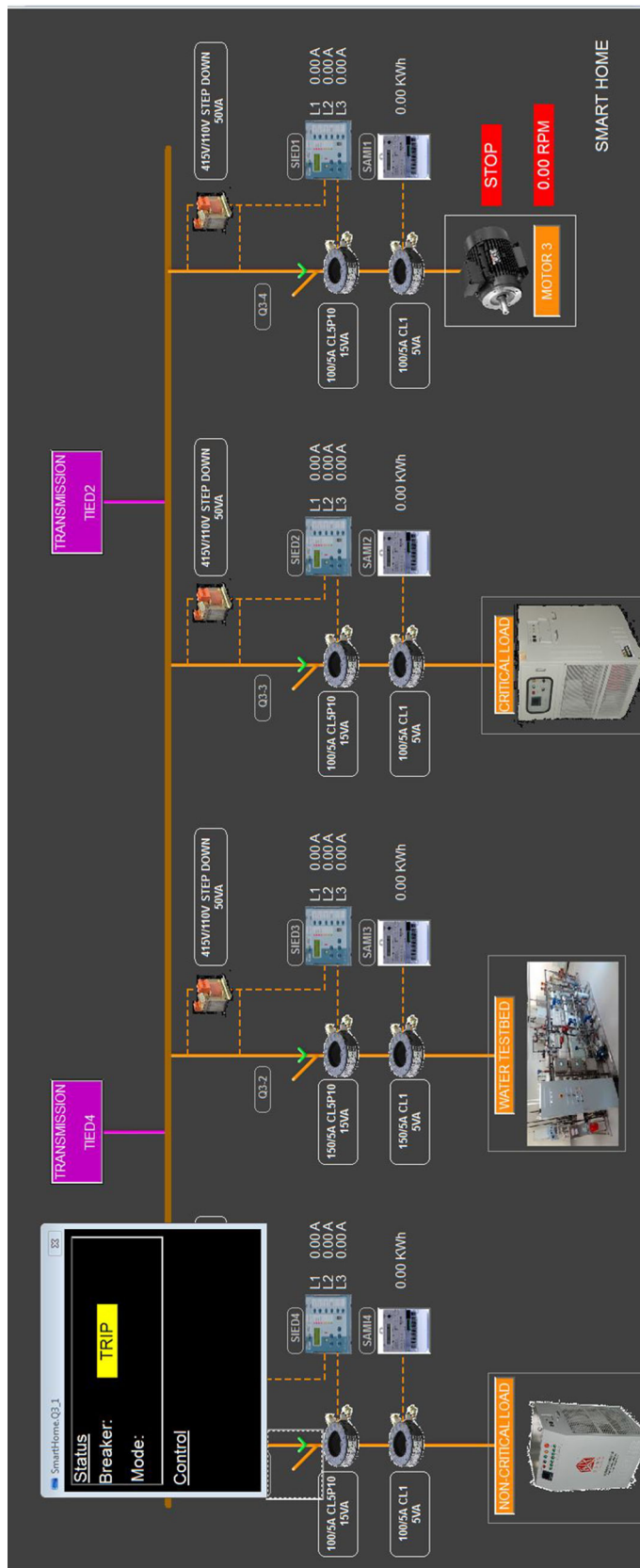


Fig. 10 Smart-home with DDoS attack: the circuit breaker was tripped and the system is in in-valid state, i.e., neither ON nor OFF and lack of control option; refer to Fig. 9.

Table 4 Design of attacks on power settings

Stages/ways	PLC code (A)	DDoS (B)	MITM (C)	SCADA PC + web portal (D)
Generation (G)	The PLC Code of the GPLC is modified such that the speed setting sent to VSD is modified to a higher value, say, by 1%	The PLC Code in the GPLC is modified such that the speed setting sent to VSD is modified to a higher value, say, by 1% more and carry out DDoS on the GPLC	The attacker modifies the command from GPLC (increases by 1%) and sends it to the VSD	Not applicable as there is no web portal for settings of a generator
Transmission (T)	Not applicable as there are no generators	Not applicable as there are no generators	Not applicable as there are no generators	Not applicable as there are no generators
Micro-grid (M)	Not applicable as there are no PLC controlling settings of PV + battery	Not applicable as there are no PLC controlling settings of PV + battery	NA	The attacker modifies the power setting in SMA portal to trip the entire system.
Smart-home (S)	Not applicable as there are no generators	Not applicable as there are no generators	Not applicable as there are no generators	Not applicable as there are no generators

applicable in other stages such as transmission and smart-home.

7.2 Attack execution for selected cases

Experiment GA In this experiment, the power setting at which the speed of VSD should accelerate to enable equal power sharing among the two generators G1 and G2 was modified.⁸ In this case, the control logic was modified such that G2 could not take over power when it is synchronized as the second generator.⁹ Vulnerabilities [14] of Windows 7 OS were exploited to enter the SCADA workstation. Dropbear SSH vulnerability and unauthenticated command-line access in CoDeSys allow an attacker to manipulate the PLC code. These two vulnerabilities were exploited to manipulate the PLC code.

Experiment MD The maximum power setting in the SMA web portal for the PV/battery inverters was changed to a value higher than the maximum load demand of critical loads. Vulnerabilities [14] of Windows 7 OS were exploited to enter the SCADA workstation which is the authorized location for modifying SMA portal settings.

7.3 Results from selected experiments

Experiment GA This subsection presents the impact of the power supply interruption attack based on the power settings of the generator's PLC code and can be correlated with attack experiment GA in Table 4.

⁸ The proportion of power sharing could be different, i.e., 60-40, but the logic remains unchanged.

⁹ Synchronization is carried out for incoming generators to ensure that the voltage, frequency, and phase angle of the incoming generator are same as those of the existing generators.

Original system As an example, during normal operation, to supply power to the critical loads, generators G1 and G2 will share the power equally. The SPLC has the control code that issues a subsequent command to the VSDs to run at a specific speed (1500RPM in this case), for enabling equal power sharing among the two generators. The normal operation is shown in Fig. 11, i.e., the apparent power is equally shared between the generators. The time-domain representation of power sharing before the attack was launched is shown in Fig. 12 and marked as normal.

After the attack was launched on generator G1, i.e., the speed of the prime mover of G2 reduced by 0.2RPM when generator G1 is supplying more power and hence disabling the power sharing process. This attack scenario is marked in Fig. 12 where it can be observed that whenever G2 is supplying more power than G1, G1 takes over until equal power is shared among the two. However, when G1 is supplying more power, G2 fails to take over even after synchronization. This resulted in G1 supplying more power under scenarios where G2 is synchronized as the second generator. The above condition will eventually result in tripping of G1 due to prolonged overload condition.¹⁰

Experiment MD This section presents the power supply interruption attack based on power settings in the SMA web portal and can be correlated with experiment MD in Table 4.

Original system Under normal operation, in order to supply power to the critical loads, CB1, CB4, CB8, and CB12 (CBx in Fig. 5) must be closed. Assuming that the power is supplied only to the critical loads, the maximum power from the inverter as set in the SMA portal should be less than

¹⁰ An inverse relationship exists between the percentage of overload and tripping time, i.e., the higher the overload, the shorter will be the tripping time.

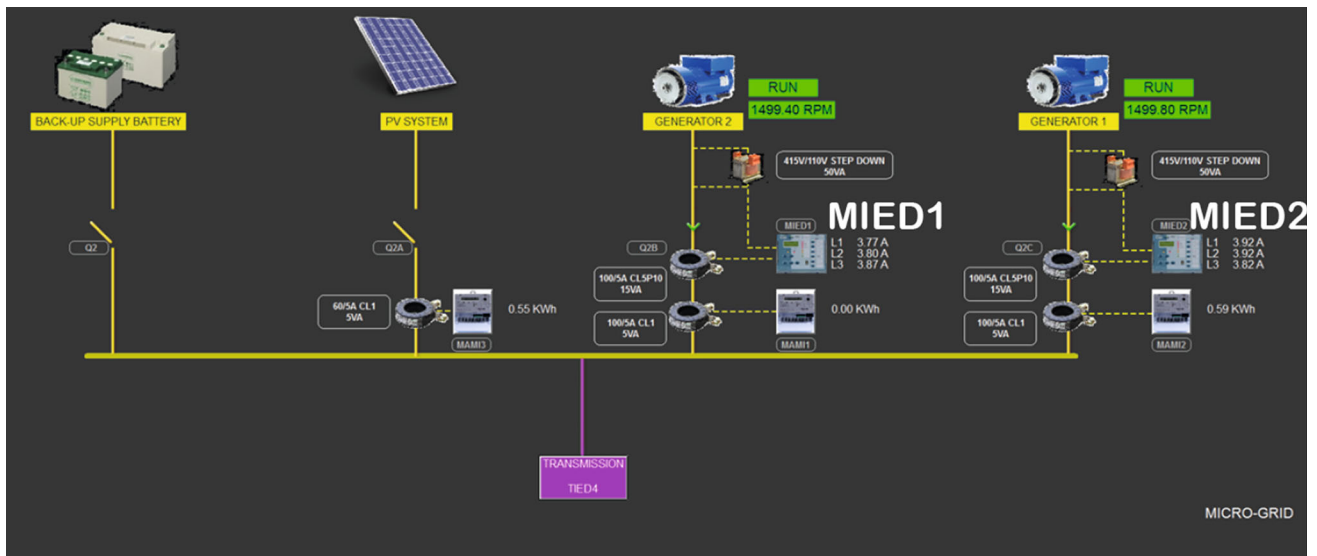


Fig. 11 Normal operation during which the load is share equally between generators 1 and 2 can be observed from L1–L3 being approximately same on MIED1 and MIED2

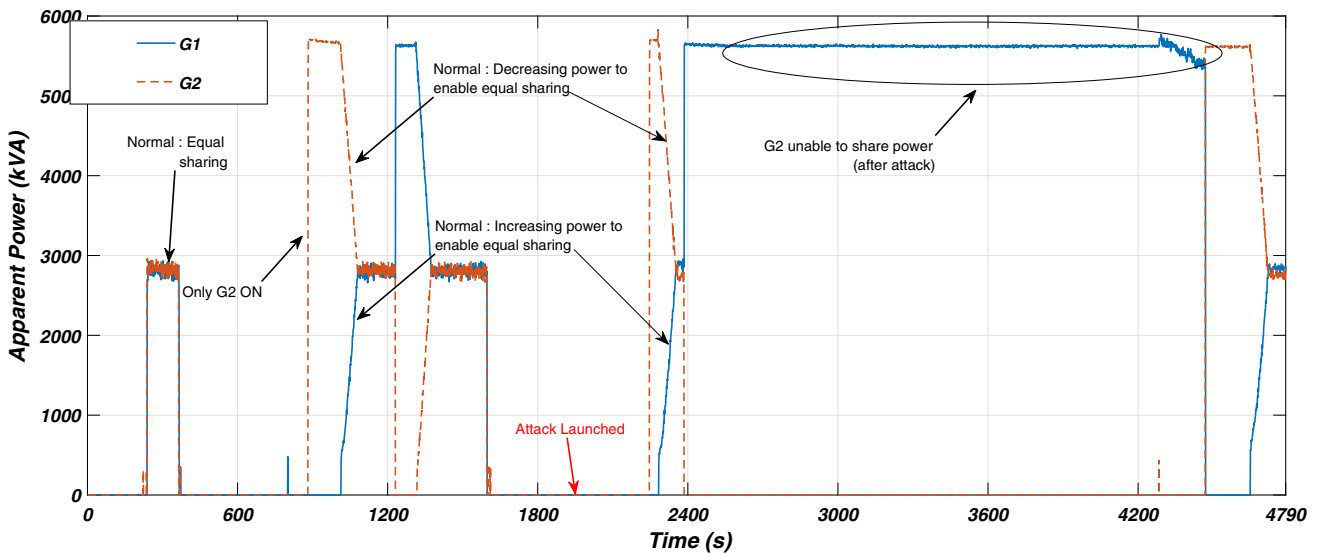


Fig. 12 Apparent power during load sharing between generators G1 and G2. When G2 is unable to share the power, the vulnerability of G1 to trip under overload, i.e., during peak load conditions, increases dramatically. The time-domain representation of power sharing before

the attack was launched is shown and marked as normal. Observe that before attack launch at around 1900 s, G1 and G2 shared power irrespective of the condition, whereas after the attack launch, G2 was unable to share the power, i.e., between 2400 and 4300 s

or equal to the power consumed by the critical loads. If the power generated from the PV + battery system is greater than the power consumed, it will result in tripping of the entire system due to power imbalance.

In this experiment, EternalBlue exploit was used to enter the SCADA workstation and used the default username/password to login into the SMA portal. The power setting was at 125% for critical loads. This is a deliberate setting as the power generated from PV + battery system would be intermittent and will not trip the system immediately, such as at night or

when the battery is not fully charged. But, under certain conditions, say during daytime and the battery is fully charged, it will result in frequent tripping as and when the power generation increases beyond the load demand due to increasing solar irradiance. Figure 13 shows the tripping event in the SMA portal “external grid disconnected due to excess freq. at phase L1 (505)”. Figure 14 shows the time-domain response of the process when there is a negative real power flow. The tripping event occurred because the battery was charged fully

Fig. 13 Zoomed SMA portal showing the exit grid events, i.e., termination of power supply from PV + battery systems

External grid disconnect due to excess freq. at phase L1 (505)	13.09.2017	11:09
Time adjusted / new time (10109)	13.09.2017	11:08
Time adjusted / old time (10108)	13.09.2017	11:07

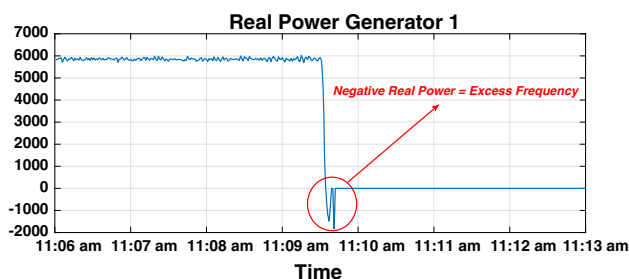


Fig. 14 Reverse power and tripping event from Historian, i.e., termination of power supply from generator indicated with zero power. Y-axis is the real power

and the power generated by PV was higher than the power consumption in critical loads.

8 Malicious power generation attack

The attacker's intention, in this case, is to manipulate the power generated from a particular generator to achieve a different set of goals. For example, the attack focuses on overloading one generator higher than the other, so that the maintenance schedule is offset as the overloaded generator needs more frequent maintenance due to additional wear and tear. This eventually leads to accumulated damage in the long run, as the overloaded generator was not serviced at the appropriate times due to malicious operation. The attack could be further classified into two types: attacks on the real power generation and attacks on reactive power generation. A detailed information of attacks on the real power is mentioned in Table 5 and attacks on reactive power is out of the scope of this paper.

8.1 Prime mover attack or attack on real power generation

Controlling the speed of the motor can change the frequency of the generator as per the following equation:

$$n = 120/p * f, \quad (1)$$

where n = shaft rotation speed (rev/min, rpm), f = frequency, and p = number of poles.

Generators are required to be maintained at a fixed frequency, 50 Hz or 60 Hz, in order to ensure the stability of the system as explained in Sect. 2.2. If the load remains constant

and the power input increases due to the accelerated speed of the rotor, the frequency will increase or the real power shared by the generator will increase. This will shift the load from the other generators to the generator under attack thus overloading it, i.e., with reference to normal operation and not the actual overload. Such attacks do not cause any immediate impact but increase the aging process of the attacked generator in the long run.

Attack design Two attacks were designed and launched on EPIC using this mode as the attack could be launched in two different ways.

Experiment A The adversary modifies the code such that the speed is always mutated by factor $+\delta$. This would result in excessive real power generated/shared by the generator under attack.

Experiment B The attack is designed such that the packets sent from PLC to the VSD are modified by factor $+\delta$. It is assumed that the attacker is already inside the network.

Normal operation In this experiment, both generators G1 and G2 shown in Fig. 5 are connected to the load and hence should share the required real and reactive power equally during normal operation. The normal operation is shown in Fig. 15, i.e., the apparent power is equally shared by both the generators, and the time series representation is shown in Fig. 16. Ramping of power (both up and down) by the generators G1 and G2 is shown in Fig. 17. The following observations are noted. (1) Initially generator G2 was supplying the entire power to the load when G1 was not available. (2) After 201 s when the generator G1 was available, power was shared equally among two generators. (3) When generator G2 was not available after 401 s, generator G1 was supplying the entire power to the load. (4) After 600 s, the power is equally shared among the two generators. The two cases in Figs. 16 and 17 are a representation of the normal scenario.

Attack execution The attack is launched on generator G1, i.e., the speed of the prime mover of G2 is reduced by 0.2 RPM when generator G1 is supplying more power and hence disabling the power sharing process.¹¹ The attack scenario is shown in Fig. 18 where it can be observed that whenever G2 is supplying more power than G1, G1 takes over the power until equal power is shared by the two. However, when G1 is supplying more power, G2 fails to take over even after syn-

¹¹ We did not increase the speed owing to safety concerns; the attack was executed in reverse logic.

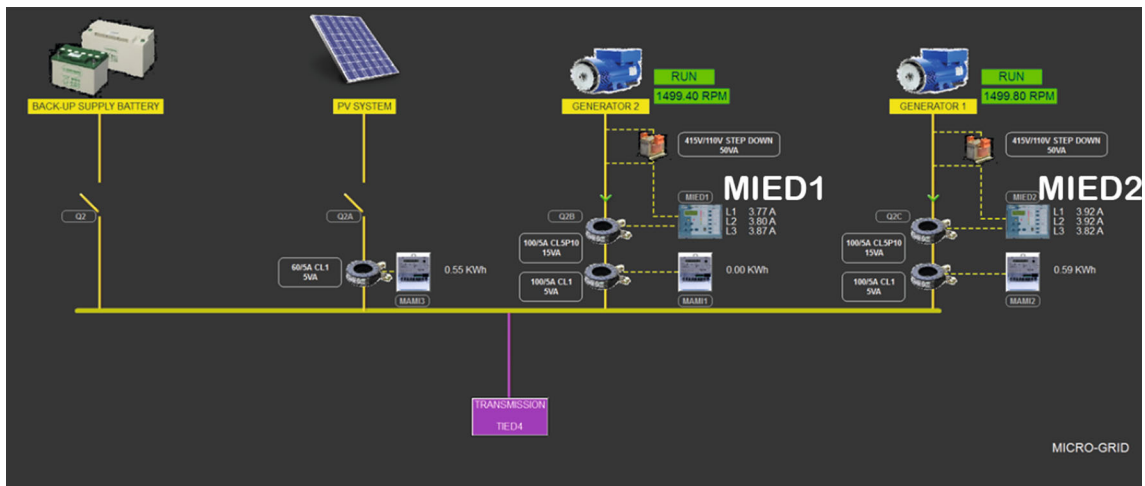


Fig. 15 Normal operation showing equal load sharing: The equal power supply is shown at MIED1 and MIED2 with respect to two generators which can be observed for approximately equal value on L1–L3 of both the IEDs

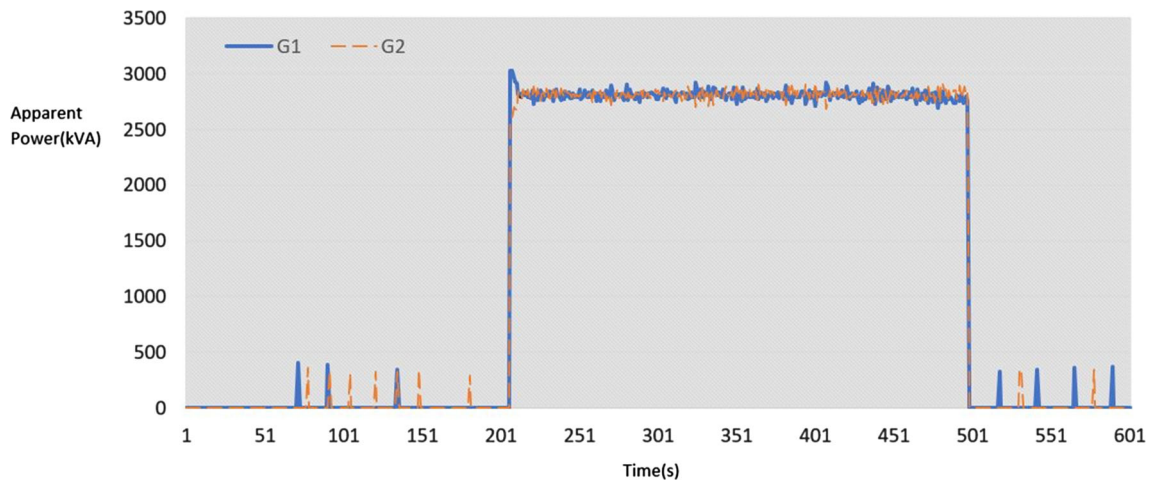


Fig. 16 Steady-state equal load sharing among G1 and G2, from around 200s to 500s

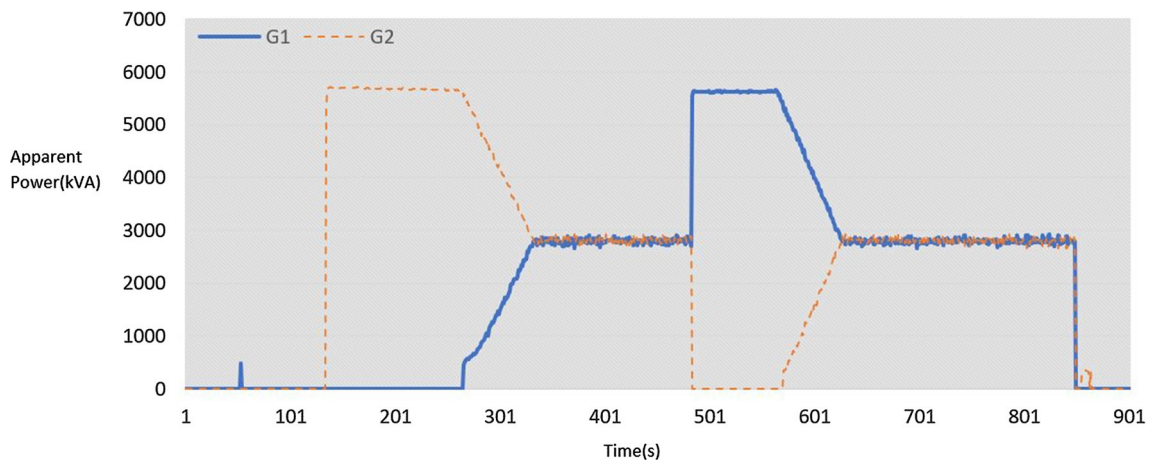


Fig. 17 Ramping power to enable equal sharing among G1 and G2; G1 ramps up the power around 280s and G2 around 580s

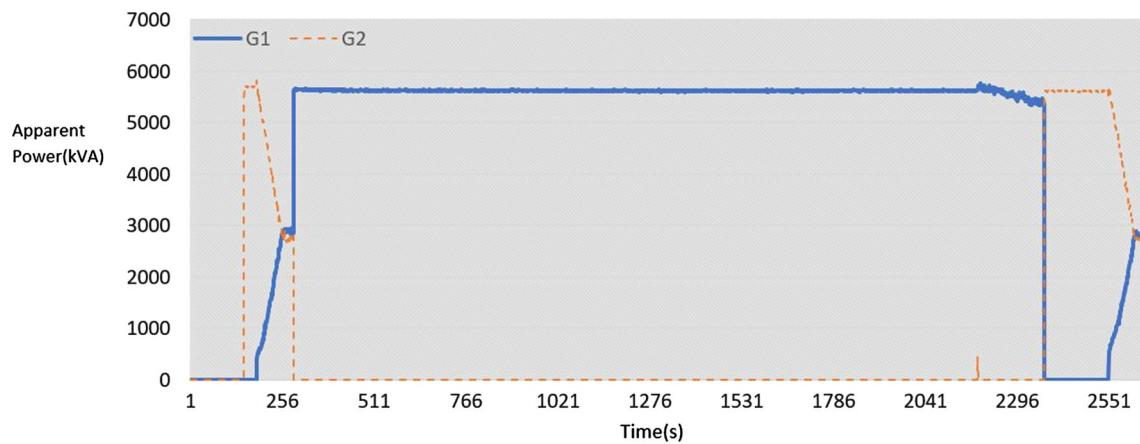


Fig. 18 Load sharing among generators G1 and G2 during the attack period. No attack scenario can be observed around 250 s, and the attack scenario can be observed around 2100 s

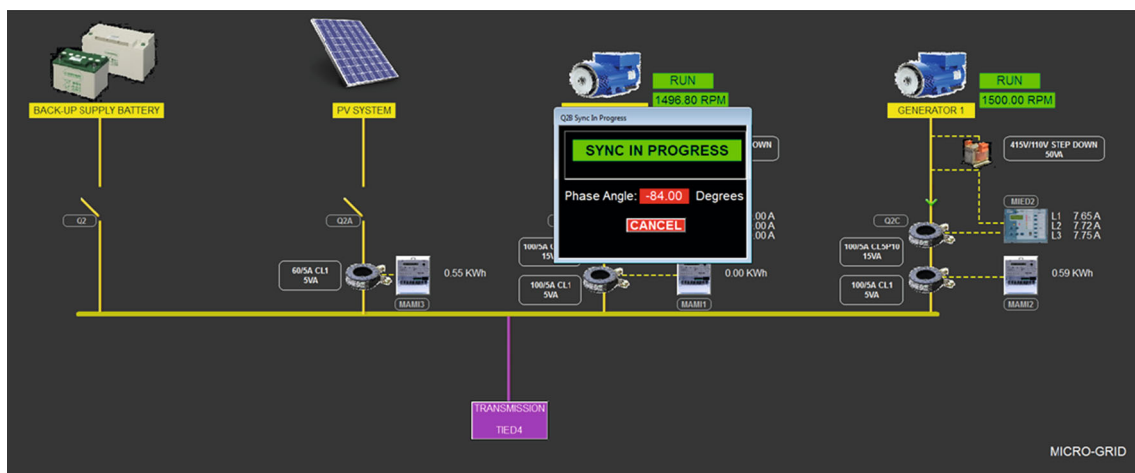


Fig. 19 Synchronization process during attack period: Here generator G1 supplying entire load, when we want the second generator G2 to supply power along with G1, it checks the sync process as shown in figure and shares the load with generator G1

chronization.¹² This will result in G1 supplying more power under the scenarios when G2 is synchronized as the second generator when G1 is already supplying power. It was also observed that the synchronization process took much longer than usual after the attack was launched. The corresponding SCADA screenshots are shown in Figs. 19 and 20. In fact, this delay itself could be considered as an attack as this disables the availability of G2 when there is a sudden/instantaneous power requirement. However, we are not focusing on the attack on the synchronization process in this paper.

Table 6 shows a summary of the attacks analyzed in this work.

¹² Synchronization is carried out for incoming generators to ensure that the voltage, frequency, and phase angle of the incoming generators are the same as the existing generators.

9 Discussion

In this section, we revisit the attacks and the attack matrices in Tables 3 and 4. Factors considered here include (i) the difficulty level of launching the attack on EPIC, (ii) impact of the attack with respect to the stage at which it is launched and the type of attack launched, (iii) time at which the attack could be launched, (iv) the time required to realize the attack, and (v) the capabilities of the attacker required to launch the attacks.

Difficulty in launching an attack: The difficulty in launching an attack depends on various factors such as the stage at which the attacker intends to launch the attack, the component targeted for the attack, etc. For example, the likelihood of a PLC controlling a generator that is secured or the likelihood that the measures implemented for minimizing the vulnerabilities, is usually high considering the fact that these subsystems are managed by professionals. However, such measures are

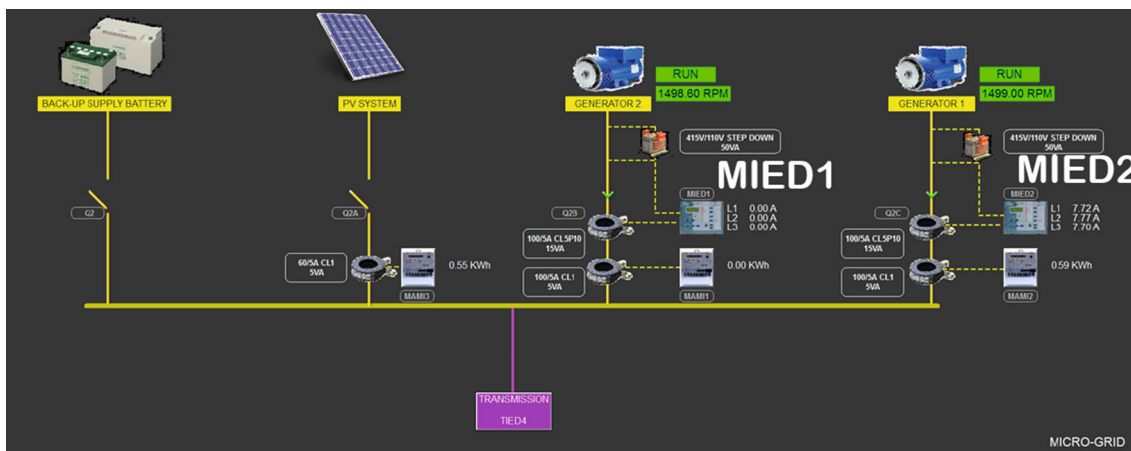


Fig. 20 Generator G1 is supplying the entire load: This situation occurs after an attack. However, though two generators are running as shown, only generator G1 is supplying the entire load which can be observed from L1–L3 values of MIED1 and MIED2

Table 5 Malicious power generation attacks

Type	PLC code (A)	MITM (B)
Attack on real power generation (P)	The PLC code of the GPLC is modified such that the speed setting sent to VSD is set to a higher value say 1% more	The attacker modifies the command from GPLC (say increases by 1%) and sends it to the VSD

less likely to be implemented when the PLC/controller is intended to control a smart-home or individual loads as these are often managed by non-professionals. Also, the physical access to the concerned PLCs is less protected in a consumer environment than in other parts of the grid. With respect to the targeted component, given that the attacker has access to the PLC, the information required for modifying the code to change breaker status, which is only one line in the control code, is less than the information required to modify the speed settings, requiring modifications on multiple lines of code. Hence, it is easier to launch an attack on a circuit breaker compared to an attack for changing the power settings of a generator.

Impact with respect to a stage in the power grid The impact of an attack launched on the generation stage is much higher than the impact of an attack launched on the smart-home. This is because the attack on the smart-home affects only the concerned loads, i.e., say critical loads (refer to Fig. 5 critical loads), whereas an attack on the generator affects the overall system, i.e., non-critical loads and other connected systems (other testbeds in the environment where the experiments are conducted). An attack on the micro-grid can also affect the stability of the system (*Experiment GD* from Table 3) and leads to overall system trip due to power imbalance. A similar impact was also observed on the transmission stage, i.e., it affects a larger portion of the grid.

Time to perform an attack Irrespective of the time at which the attack was launched, the attack on the generator and trans-

Table 6 Analyzed attacks

Attack	Corresponding figures
Power supply interruption attack on circuit breakers based on DDoS	Figures 9, 10
Power supply interruption attack on power settings based on PLC code manipulation	Figures 11, 12
Power supply interruption attack on power settings based on SMA portal manipulation	Figures 13, 14
Malicious power generation attack on VSD speed based on communication signal manipulation	Figures 15, 16, 17, 18, 19, 20

mission stages resulted in a complete blackout. The impact of an attack on individual loads depends on the operating pattern and the time at which electric power is needed. For example, refrigerator and freezer units have ON and OFF periods that cycle one after the other [25]. An attack targeted (*Experiment SA* in Table 3) at power supply interruption during an ON interval will increase the vulnerability of the products stored in the refrigerator or freezer, whereas a random attack will most likely have a lesser impact.

Time to realize an attack The impact of an attack could be realized immediately as in case of *Experiment GA* described in Table 3. Alternately, it could be sufficiently long as in case of *Experiment MD* described in Table 4, where the impact is directly linked to the inherent intermittent nature of the solar PV. Among the different types of attacks in Tables 3 and 4, the attacker should have the highest capability for successfully launching MITM attacks. This is due to high computation needs of the MITM attacks, considering the time-critical nature of the system. To launch other types of attacks, the attacker should have the ability to identify the usernames and passwords.

The feasibility of an attack, i.e., realizing the attacker's intent, depends on whether the targeted entity uses the standard cyber-security protocols or not. For example, in the case of EPIC, vendors were asked to design the system with state-of-the-art components. Vulnerabilities were evaluated after the testbed was deployed. It was observed that the system satisfied all *Operation Technology*-related standards. However, it could not fulfill the security requirements based on recently reported vulnerabilities, e.g., *EternalBlue*. Such conditions are applicable to all legacy systems as well. Hence, it is realistic that an adversary could use these vulnerabilities together with social engineering to launch such attacks.

Studies, such as the one reported here, could be useful for the operators of ICSs to re-evaluate cyber-security scores with respect to *Information Technology*-related standards. For example, in the case of attacks on power settings, the SMA portal itself follows the hierarchy of cyber-security measures such as suggestions to have customized passwords, unique code for changing control settings, etc. However, under weak password scenario, or through social engineering, the adversary could get access to this critical information and execute the attack.

Even though state-of-the-art ICT is used for power system operation and control, it is highly likely that there would be unexplored and unfixed vulnerabilities as pointed out by ICS-CERT. The ICS used for the power system operation and control should be frequently evaluated against the ever-evolving vulnerabilities in the ICT domain. This paper would be helpful for researchers in exploring the possible vulnerabilities and respective attack scenarios (as new as *EternalBlue* on SMA power setting, which was not believed to exist before). It is also useful to develop defense mechanisms for the existing vulnerabilities.

10 Related work

Previous work in this area can be divided into two groups as presented as follows:

Attack modeling and analysis Attacks have been modeled as noise in sensor data [28]. Attack models designed specifi-

cally for CPS [2] often include a variety of deception attacks such as surge, bias, and geometric [10]. Further, attack models reported in the literature are a modified version of attack models designed for network security [64] and rarely consider the physical aspects of a CPS. Recent surveys on ICS privacy, safety, and security indicate [27,40] the different areas of focus in ICS security.

Resilient control is an essential requirement for the control system that manages a Smart Grid. For example, resilient interconnection requirements for cyber-physical control systems are reported in [8] where the authors describe the policy enforcement system to incorporate optimal self-healing services by considering control structural capacities, the super-node theory, and the IEC-62351 standard. Furthermore, resilience can also be improved by using an architecture that is specifically designed for such requirements. One such resilient architecture for the Smart Grid is presented in [36]. Researchers have reported case studies on power substation networks [16] where the authors studied detailed characterization of an ICS to determine its behavior either from the perspective of traditional IT networks or from the basic principles of ICS operation. It can be observed from the above cited studies that understanding the physical process limitations is a key step toward deriving the trade-off between resilience and security. Hence, the attack design from physical vulnerability stand point, described in this work, is an essential approach for improving the resilience of a Smart Grid.

Two virtual testbeds, created for investigating cyber-attacks, are described in [57]. However, results presented in this paper clearly demonstrate the importance of investigating the attacks in an operational industrial-grade system. In [35], the authors describe the design of a system to respond to cyber-security breach incidents when different areas of the network are totally unprotected against cyber-attacks. Detection of anomalies, response to incidents, tests of accuracy, and maintenance, as well as recovery of states and control in crisis situations, have been studied [7].

Attacks on power systems Data integrity attacks on smart-grid systems are studied extensively in the literature. One such study [66] presented a detailed analysis on the impact of a data integrity attack on real-time pricing (RTP) in smart-grids. False data injection attacks on AGC were studied and validated with experimental results in [63,67]. The authors in [67] show that with eavesdropped sensor data, it is possible to derive system constants and launch an optimal attack on AGC. A similar study was presented in [70] focusing on false data injection attacks on the state estimation to create load redistribution (LR). The authors also presented a quantitative analysis of the damage to power systems because of LR attacks. The authors in [58] presented a control framework using digital signature and time stamping for authen-

titating the control commands issued to renewable energy source inverters that provide reactive power support.

A survey of the conceptual expansion of real-time monitoring systems, detecting the anomalies, analyzing the impact of attacks, and mitigation framework appears in [68]. Physical impact assessment, carried out for cyber-physical systems, particularly a boiler system using hardware-in-loop (HIL) simulations, is reported in [22]. Potential exploits in substation have been explored followed by studies on attacks such as malicious fault injection attacks and hardware Trojans that can be employed for compromising substation-level IEDs [11]. The impact of SCADA system's vulnerabilities on the overall power system reliability is an important factor to be considered [71]. Earlier studies focused on false data injection attacks on power systems [34]. The use of invariants for detecting attacks on CPS has been proposed in [5,17,32].

11 Conclusions

An experimental investigation into vulnerability assessment was undertaken on an operational 72-KVA electric power testbed. It is shown that an attacker could compromise various smart-grid controllers and gain full control of the grid and thus alter its operation. More specifically, this work reports on an investigation into power supply interruption attacks and malicious power generation attacks with a focus on network and process vulnerabilities.

Ongoing work focuses on the implementation of additional cyber-security measures to mitigate different risks, launching systematic attacks to evaluate the resilience of EPIC and conduct experiments to understand the cascading effects across critical infrastructure such as water systems and electric power systems.

Acknowledgements This work was supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-040), and administered by the National Cybersecurity R&D Directorate. The Electric Power and Intelligent Control (EPIC) testbed was made possible through funding from Ministry of Defence, Singapore, NRF, and the SUTD-MIT International Design Centre (IDC).

Compliance with ethical standards

Ethical approval We did not use animals and Human participants in the study reported in this work.

References

1. Adepu, S., Kandasamy, N.K., Mathur, A.: EPIC: an electric power testbed for research and training in cyber physical systems security. In: *Computer Security*, pp. 37–52. Springer, Cham (2018)
2. Adepu, S., Mathur, A.: Generalized attacker and attack models for cyber-physical systems. In: *Proceedings of the 40th International Computers, Software and Applications Conference*, pp. 283–292. IEEE (2016)
3. Adepu, S., Mathur, A.: Using process invariants to detect cyber attacks on a water treatment system. In: *Proceedings of the 31st International Conference on ICT Systems Security and Privacy Protection—IFIP SEC*, pp. 91–104. Springer, New York (2016)
4. Adepu, S., Mathur, A.: Assessing the effectiveness of attack detection at a hackfest on industrial control systems. *IEEE Trans. Sustain. Comput.* **1**(1), 1–14 (2018)
5. Adepu, S., Mathur, A.: Distributed attack detection in a water treatment plant: method and case study. *IEEE Trans. Dependable Secure Comput.* (2018)
6. Adepu, S., Prakash, J., Mathur, A.: Waterjam: an experimental case study of jamming attacks on a water treatment system. In: *IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 341–347. IEEE (2017)
7. Alcaraz, C., Lopez, J.: Wasam: a dynamic wide-area situational awareness model for critical domains in smart grids. *Future Gen. Comput. Syst.* **30**, 146–154 (2014)
8. Alcaraz, C., Lopez, J., Choo, K.-K.R.: Resilient interconnection in cyber-physical control systems. *Comput. Secur.* **71**, 2–14 (2017)
9. Amadi, H.N.: Impact of power outages on developing countries: evidence from rural households in Niger Delta, Nigeria. *J. Energy Technol. Policy* **5**(3), 27–38 (2015)
10. Cárdenas, A.A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S.: Attacks against process control systems: risk assessment, detection, and response. In: *Proceedings of the 6th ASIACCS*, pp. 355–366 (2011)
11. Chattopadhyay, A., Ukil, A., Jap, D., Bhasin, S.: Towards threat of implementation attacks on substation security: case study on fault detection and isolation. *IEEE Trans. Ind. Inform.* **14**(6), 2442–2451 (2018)
12. 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)
13. CODESYS: CODESYS- industrial IEC 61131-3 PLC programming. <https://www.codesys.com/> (2018). Accessed 1 July 2019
14. CVE-2017-0144: Windows SMB remote code execution vulnerability. <https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144> (2017). Accessed 1 July 2019
15. FitzPatrick, G.J., Wollman, D.A.: NIST interoperability framework and action plans. In: *Power and Energy Society General Meeting*, pp. 1–4. IEEE (2010)
16. Formby, D., Walid, A., Beyah, R.: A case study in power substation network dynamics. *Proc. ACM Meas. Anal. Comput. Syst.* **1**(1), 19 (2017)
17. Gamage, T., McMillin, B., Roth, T.: Enforcing information flow security properties in cyber-physical systems: a generalized framework based on compensation. In: *IEEE 34th Annual Computer Software and Applications Conference Workshops (COMP-SACW)*, pp. 158–163, July 2010
18. Govil, N., Agrawal, A., Tippenhauer, N.O.: On ladder logic bombs in industrial control systems. *CoRR* (2017)
19. Greenwald, P.W., Rutherford, A.F., Green, R.A., Giglio, J.: Emergency department visits for home medical device failure during the 2003 North America blackout. *Acad. Emerg. Med.* **11**(7), 786–789 (2004)
20. Hernandez, M., Ramos, G.A., Lwin, M., Siratarnsophon, P., Santoso, S.: Embedded real-time simulation platform for power distribution systems. *IEEE Access* **6**, 6243–6256 (2017)
21. Homeland Security: DHS common cybersecurity vulnerabilities in ICS. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

22. Huang, K., Zhou, C., Tian, Y.-C., Yang, S., Qin, Y.: Assessing the physical impact of cyber-attacks on industrial cyber-physical systems. *IEEE Trans. Ind. Electron.* **65**(10), 8153–8162 (2018)
23. ICS-CERT Advisories: <https://ics-cert.us-cert.gov/advisories>. Accessed 1 July 2019
24. Islam, M.A., Ren, S., Wierman, A.: Exploiting a thermal side channel for power attacks in multi-tenant data centers. In: *Proceedings of the 2017 ACM SIGSAC, CCS '17*, pp. 1079–1094 (2017)
25. Kandasamy, N.K., Tseng, K.J., Boon-Hee, S.: Virtual storage capacity using demand response management to overcome intermittency of solar PV generation. *IET Renew. Power Gen.* **11**(14), 1741–1748 (2017)
26. Kasper Sky: Industrial control systems vulnerabilities statistics. https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICs_Statistic_vulnerabilities.pdf. Accessed 1 July 2019
27. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. *Reliab. Eng. Syst. Saf.* **139**, 156–178 (2015)
28. Kwon, C., Liu, W., Hwang, I.: Security analysis for cyber-physical systems against stealthy deception attacks. In: *ACC*, pp. 3344–3349 (2013)
29. Langner, R.: Stuxnet: dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **9**(3), 49–51 (2011)
30. Lee, E.A.: Cyber physical systems: design challenges. In: *11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pp. 363–369. IEEE (2008)
31. Lin, H., Slagell, A., Kalbarczyk, Z., Sauer, P., Iyer, R.: Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. *IEEE Trans. Smart Grid* **9**(1), 163–178 (2018)
32. Lin, Q., Adepu, S., Verwer, S., Mathur, A.: Tabor: a graphical model-based approach for anomaly detection in industrial control systems. In: *Proceedings of the AsiaCCS*, pp. 525–536. ACM, Korea (2018)
33. Lipovsky, R.: New wave of cyber attacks against Ukrainian power industry. <http://www.welivesecurity.com/2016/01/11> (2016). Accessed 1 July 2019
34. Liu, Y., Ning, P., Reiter, M.: False data injection attacks against state estimation in electric power grids. In: *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp. 21–32 (2009)
35. Lopez, J., Alcaraz, C., Roman, R.: Smart control of operational threats in control substations. *Comput. Secur.* **38**, 14–27 (2013)
36. Lopez, J., Rubio, J.E., Alcaraz, C.: A resilient architecture for the smart grid. *IEEE Trans. Ind. Inform.* **14**(8), 3745–3753 (2018)
37. Mackiewicz, R.: Overview of IEC 61850 and benefits. In: *Power Systems Conference and Exposition, 2006. PSCE'06. 2006 IEEE PES*, pp. 623–630 (2006)
38. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. *IEEE Secur. Priv.* **7**, 75–77 (2009)
39. Meliopoulos, A.S., Cokkinides, G., Fan, R., Sun, L.: Data attack detection and command authentication via cyber-physical comodeling. *IEEE Des. Test* **34**(4), 34–43 (2017)
40. Mitchell, R., Chen, I.-R.: A survey of intrusion detection techniques for cyber-physical systems. *ACM Comput. Surv. (CSUR)* **46**(4), 55 (2014)
41. MITRE: CVE-2012-6068. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6068> (2012). Accessed 1 July 2019
42. MITRE: CVE-2016-2509. <https://cve.circl.lu/cve/CVE-2016-2509> (2016). Accessed 1 July 2019
43. MITRE: NVD-CVE-2016-7406. <https://nvd.nist.gov/vuln/detail/CVE-2016-7406> (2016). Accessed 1 July 2019
44. MITRE: NVD-CVE-2016-7407. <https://nvd.nist.gov/vuln/detail/CVE-2016-7407> (2016). Accessed 1 July 2019
45. MITRE: NVD-CVE-2016-7408. <https://nvd.nist.gov/vuln/detail/CVE-2016-7408> (2016). Accessed 1 July 2019
46. MITRE: NVD-CVE-2016-7409. <https://nvd.nist.gov/vuln/detail/CVE-2016-7409> (2016). Accessed 1 July 2019
47. MITRE: CVE-2018-5461. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5461> (2018). Accessed 1 July 2019
48. MITRE: CVE-2018-5465. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5465> (2018). Accessed 1 July 2019
49. MITRE: CVE-2018-5467. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5467> (2018). Accessed 1 July 2019
50. MITRE: CVE-2018-5469. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5469> (2018). Accessed 1 July 2019
51. MITRE: CVE-2018-5471. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5471> (2018). Accessed 1 July 2019
52. Nakashima, E., Timberg, C.: NSA officials worried about the day its potent hacking tool would get loose. *Washington Post*. 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 (2017). Accessed 1 July 2019
53. PCvue: Versatile HMI-SCADA software. <https://www.pcvuesolutions.com/index.php/products-a-technology/pcvue-hmiscada-48583> (2018). Accessed 1 July 2019
54. Poudineh, R., Jamsab, T.: Electricity supply interruptions: sectoral interdependencies and the cost of energy not served for the scottish economy. *Energy J.* **38**(1), 51–76 (2017)
55. Pourbabak, H., Chen, T., Zhang, B., Su, W.: Control and energy management system in microgrids. *arXiv preprint arXiv:1705.10196* (2017)
56. 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)
57. Reaves, B., Morris, T.: An open virtual testbed for industrial control system security research. *Int. J. Inf. Secur.* **11**(4), 215–229 (2012)
58. Rogers, K.M., et al.: An authenticated control framework for distributed voltage support on the smart grid. *IEEE Trans. Smart Grid* **1**, 40–47 (2010)
59. Saadat, H.: *Power Systems Analysis of McGraw-Hill Series in Electrical and Computer Engineering*. McGraw-Hill, New York (2002)
60. Schmidhalter, M., Reichl, J.: Assessing the socio-economic effects of power outages ad hoc. *Comput. Sci. Res. Dev.* **31**(3), 157–161 (2016)
61. Shrivastava, S., Adepu, S., Mathur, A.: Design and assessment of an orthogonal defense mechanism for a water treatment facility. *Robot. Autonom. Syst.* **101**, 114–125 (2018)
62. SMA: SMA-portal (2019). <https://www.sunnyportal.com/>. Accessed 1 July 2019
63. Sridhar, S., Govindarasu, M.: Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **5**(2), 580–591 (2014)
64. Stamp, M.: *Information Security: Principles and Practice*. Wiley, New York (2011)
65. Taljegard, M.: The impact of an electrification of road transportation on the electricity system in Scandinavia. Ph.D. thesis, Department of Space, Earth and Environment, Chalmers University of Technology (2017)
66. Tan, R., Badrinath Krishna, V., Yau, D.K., Kalbarczyk, Z.: Impact of integrity attacks on real-time pricing in smart grids. In: *Proceedings of the 2013 ACM CCS*, pp. 439–450. ACM (2013)
67. Tan, R., Nguyen, H.H., Foo, E.Y., Yau, D.K., Kalbarczyk, Z., Iyer, R.K., Gooi, H.B.: Modeling and mitigating impact of false data injection attacks on automatic generation control. *IEEE TIFS* **12**(7), 1609–1624 (2017)
68. Ten, C.-W., Yamashita, K., Yang, Z., Vasilakos, A., Ginter, A.: Impact assessment of hypothesized cyberattacks on interconnected

- bulk power systems. *IEEE Trans. Smart Grid* **9**(5), 4405–4425 (2018)
69. WAGO: Wago programmable logic controllers. <http://www.wago.us/products/components-for-automation/modular-io-system-ip-20-750753-series/plc/overview/> (2009). Accessed 1 July 2019
70. Yuan, Y., Li, Z., Ren, K.: Modeling load redistribution attacks in power systems. *IEEE Trans. Smart Grid* **2**(2), 382–390 (2011)
71. Zhang, Y., et al.: Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation. *IEEE Trans. Power Syst.* **31**(6), 4379–4394 (2016)
72. Zimba, A., Wang, Z., Chen, H.: Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express* **4**(1), 14–18 (2018)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Sridhar Adepu is a Ph.D. student in Information Systems Technology and Design Pillar at the Singapore University of Technology and Design. His research focuses on cyber-physical systems security.

Nandha Kumar Kandasamy is a Research scientist in iTrust, at the Singapore University of Technology and Design. His research interests are in electric vehicles and cyber-physical systems.

Jianying Zhou is a Professor of Pillar Information Systems Technology and Design at the Singapore University of Technology and Design. His research interests are in applied cryptography and cyber-physical system security.

Aditya Mathur is a Professor of Computer Science at Purdue University and Information Systems Technology and Design Pillar at the Singapore University of Technology and Design. He is the Center Director of iTrust, a center for research in cyber-security, that focuses on the design of secure critical infrastructure. His recent work focuses on the design of secure critical infrastructure including water and power systems.