Attacking the Smart Grid using Public Information

Charalambos Konstantinou[*], **Marios Sazos**[†], **Michail Maniatakos**[‡]
[*]Electrical and Computer Engineering, New York University Polytechnic School of Engineering
[†]Center for Cyber Security, New York University Abu Dhabi
[‡]Electrical and Computer Engineering, New York University Abu Dhabi
E-mail: {ckonstantinou, marios.sazos, michail.maniatakos}@nyu.edu

Abstract—**Over the past years, sophisticated adversaries have infiltrated the control networks of energy companies around the globe. As attempts to compromise industrial control and information technology systems have soared, electric utilities increase their investments in cyber security as an important step to enhance resiliency of the power system. Although utility companies started adopting a defense in depth strategy, compliant with security reliability standards, the first step towards building effective mitigation strategies is to understand the attack vectors emerging from publicly available information. To this end, we utilize data from accessible resources to create a map of the topological and electrical structure of smart grid regions. Furthermore, we identify electronic devices able to control the critical electrical units in the system. The location and characteristics of these components are used in a simulation environment to study the interaction of controls and dynamics in the system. Lastly, we examine the paths of attacking control equipment and discuss the impact of such scenarios.**

I. Introduction

Electric power grid is the centerpiece of any country's economy since it provides the foundation stone of all other critical infrastructure sectors. As such, it makes an attractive target for adversaries. A successful attack on the control elements of the grid can cause a cascade of power outages with disastrous consequences in national security, public health and economy [1]. The recent discovery that BlackEnergy malware was used to cause the blackout in the Ivano-Frankivsk region of Ukraine [2], clearly indicates that power systems are vulnerable to digital threats. Since compromised control systems can cause very extensive damage (not only to electric grids but also to other critical infrastructures), the U.S. Department of Energy and the electricity industry have jointly invested $7.9 billion from 2009 till 2015 in projects aiming to modernize systems for the smart grid implementation, strengthen cyber security and improve interoperability [3].

Although power utilities are taking steps to establish better protection against attacks on the grid infrastructure, many of the products currently being deployed in power systems are not being designed with security in mind. Commercial-Off-The-Shelf (COTS) designs typically use common technologies and software that have both known and unknown security vulnerabilities. Also, weaknesses in network segmentation can allow attackers to penetrate the system through a network-based attack vector. For example, adversaries can exploit poorly configured firewalls to insert a malicious payload into the grid control units. Furthermore, nowadays adversaries mainly use readily available intrusion tools and exploit scripts that capitalize on widely known vulnerabilities. For instance, the attackers involved in operation Night Dragon (2010), which targeted oil, gas and energy companies, used common hacking tools in order to find project details and financial information about oil-gas exploration and bids [4].

In addition to the COTS software and hacker tools available on the Internet, thorough documentation such as electric industry publications, regional maps and Federal Energy Regulatory Commission (FERC) filings can provide sufficient data to adversaries. The dissemination of such information is driven from several reasons: *a)* public-interest groups or regulations are demanding data to monitor the environmental performance and impact of electric utilities, *b)* justify electricity rates based on how operating procedures are provided, *c)* government intervention to ensure transparency amongst competing companies, *d)* ensure the operation and development of a safe and efficient electricity sector, etc. [5]–[8]. This information can enable hackers to identify and infiltrate critical points in transmission and distribution systems as well as in the communication infrastructure. For example, if public resources disclose information describing that administrative and organizational LANs are connected to Energy Management Systems (EMS)[1], then attackers could gain access to the smart grid control centers.

In this work, using public information gleaned from the web, we demonstrate how an attacker can create a map of grid regions and document their characteristics. The knowledge regarding the smart grid structure, control units and the implemented communication protocols are the baseline for identifying related vulnerabilities. Specifically, we examine code flaws in the design implementation of a protection relay. This commercial relay controller is deployed in the network of a particular distribution utility, polling data directly from the Supervisory Control And Data Acquisition (SCADA) master or a Remote Terminal Unit (RTU).

The disclosure of critical substations location and the features of their control equipment are used in a simulation study. The purpose is to model the collected information and specify the most critical set of elements to be attacked. In addition, we present how several control systems can be accessed and managed through different paths. As a result, an adversary can report spurious data to the control center or even modify settings to disable protection mechanisms and therefore trigger

[1] An EMS is a system of computer-aided tools used by operators of power utilities to monitor and coordinate the flow and distribution of electricity.

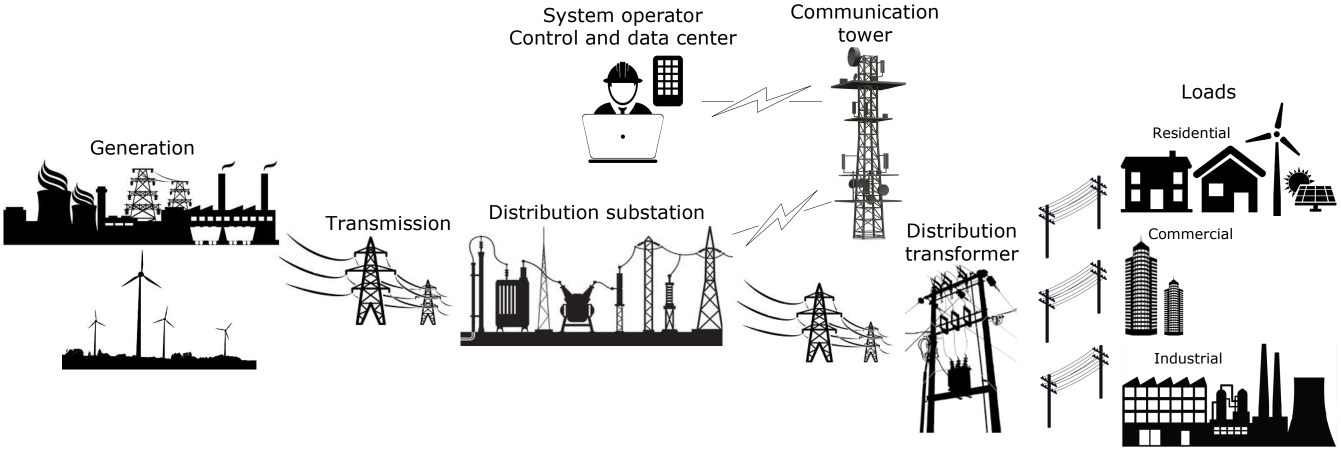


Fig. 1: Power grid architecture.

an outage. The implications of such attack paths are modeled and discussed.

The rest of the paper is organized as follows. Background on grid architecture is given in Section II. Section III describes publicly available data on the web regarding power systems. The section also explains how to access and alter control equipments operation. The modeling of the collected data, the results regarding control units exploitation and the impact discussion of the presented attacks are shown in Section IV. The paper concludes with final remarks in Section V.

II. Background

The structure of smart grid indicates a complex cyber physical system, designed to support the needs of a growing population. For example, in 2013, the U.S. had approximately 125 million household consumers of electricity and the grid could carry over 1,063 gigawatts of power [6]. As seen in Figure 1, the smart grid structure consists of generating stations where electrical power is produced, high-voltage transmission lines that carry power from power plants to distribution substations, and step-down transformers and distribution lines whereby the voltage can be lowered allowing the electricity to be delivered to consumers. Electric utilities typically distinguish between consumers based on the type of activity they perform: residential, commercial and industrial. In addition, over the past years renewable-based electricity (particularly solar PV and wind power) has been growing rapidly worldwide and integrating into existing grids. The grid infrastructure is also equipped with cyber systems that improve smart grid reliability, security, and efficiency. These systems include communication networks, control automation systems and Intelligent Electronic Devices (IEDs). Utilities participate in energy markets and coordinate with independent system operators which monitor the operation of smart grid.

Controlling and monitoring grid elements is achieved using Industrial Control Systems (ICS). ICS use information and communication technologies to control and automate stable operation of system processes [9]. The collection of telemetry data and the management of remote operations in the smart grid is performed through SCADA ICS. The overall structure of a SCADA system is often split into four distinct levels [10]: L1 – SCADA control and monitor software, L2 – remote communication networks (Ethernet, radio, serial, dial-up), L3 – Remote Terminal Units (RTUs) and IED controllers, and L4 – field instruments.

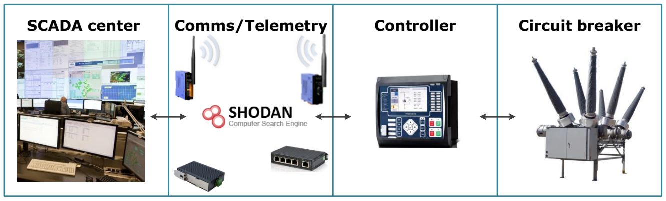


Fig. 2: The four levels of SCADA.

Many of the SCADA systems in today's grid are not designed with security features, allowing potential pathways for a cyber attack. This paper provides insights on how to maliciously control L4 field equipment such as Circuit Breakers (CBs) and their corresponding L3 controllers based on publicly available information. We consider an adversary who has access to exploits that allow execution of arbitrary malicious code. Shodan is a computer search machine designed to crawl the Internet in order to identify and index connected devices. The four levels of SCADA system in our case study are shown in Fig. 2.

III. Methodology

In this section, we describe public information provided by utilities, manufacturers and product distributors that can be associated with security risks. We also present how to control and access field equipment.

A. Public Information in the Electricity Sector

As more and more information is published on the web, security presents new challenges for critical infrastructures. The public resources regarding the operation and control of smart grid can be utilized by adversaries to launch a powerful attack. As a result, despite the defense-in-depth strategies to isolate and protect assets in the grid, sensitive public data might be the Achilles' heel towards exploiting system vulnerabilities.

The first step in attacking a smart grid deployed system is to identify which electric utility is in control of the target area [11]. The next step involves finding facts and details regarding the generation, transmission and distribution domains of the electric system. For example, utilities often provide data of generation units capacity and location, high-voltage transmission lines characteristics as well as the number and capacity of distribution substations [12], [13]. In addition, newsletter and success stories can reveal the technologies (e.g. communication protocols, models of controllers, SCADA structure, etc.) employed in the system [14]–[16].

The aforementioned information can be used to identify critical components in the system, especially if combined with detailed utility reports. For instance, a particular utility serving more than 3.3 million electricity customers in the U.S. allows public access to its corporate, regulatory, marketing and other files [17]. These files among others, disclose data and plans regarding the design of substations in order to address load serving needs [18]. In another case, the only electricity authority of a country provides important insights about the grid network through their annual reports [19]. Furthermore, there are utilities that publish their meetings videos online which contain essential information of the power system design characteristics [20]. Finally, a national electricity company, obliged under regulation laws, publishes annual planning statements for its water and electricity transmission system showing the forecast flows, fault levels, expected capacity and loading on each region of the transmission system for the following seven years [7], [13], [21].

The acquired data related to the power system may reveal vital points of the designed network which if being attacked can ultimately lead to cascading events. In general, power systems security and stability constraints (e.g. any loss-of-load) should not be violated in case of a single contingency condition ($N-1$) [22]. In the case of p failures ($N-p$ contingency), the power system should still have to restore stability allowing only a limited loss-of-load. To accomplish that, the grid is sectionalized through relays and CBs. From an attacker's perspective, the goal is to cause the maximum impact to the grid; thus, it is required to find those components p (e.g. generators, transformers etc.) that will cause $N-p$ contingency and lead to the collapse of the power system[2].

B. Control Units Operation

A contingency analysis study combined with the obtained public information should divulge those key components that when detached from the smart grid will lead to a power outage. To achieve that, an adversary needs to access the RTUs and IEDs that control such electrical elements. In order to attack these controllers it is necessary to find security weaknesses in their design and implementation.

Firmware, as the code and data written onto the non-volatile memory of a device, connects hardware and software modules and makes a system functional. Therefore, it is an ideal candidate for an adversary in order to obtain direct access to the internal components of a control unit. If the firmware of a control unit is altered maliciously, then the device would operate abnormally.

The firmware image of control equipment is often provided on the vendors or distributors web pages (public information). A web crawler module for example, could systematically search the web and gather firmware images of critical equipment [23]. In addition, the firmware could be acquired through physical access to the device, e.g. download the image from the communication port or even reverse engineer the firmware residing in the storage medium of the system [24]. Such devices can often be purchased through online auction websites at a fraction of the original price.

C. Access Path to ICS Devices

Over the last years, the number of sophisticated ICS-targeted malware has increased [25]. Furthermore, the modernization of the grid transformed legacy systems and networks that considered to be secured or air-gaped. Consequently, these systems can nowadays be reached and attacked.

In order to inject a malicious firmware file into an ICS device, adversaries may follow several approaches depending on the security level of each penetration path. For instance, the firmware image could be delivered to the smart grid unit by a malicious insider. In addition, injected firmware can be uploaded to ICS equipment through social engineering techniques e.g. Stuxnet worm was spread via infected USB drives. Adversaries can also hijack a vendor web page in order to create a rogue copy of the firmware. While the web page contents appear similar to the original one, the firmware link redirects to a malicious server. Due to the growth of search engines such as Shodan [26], a firmware image could be injected to the control equipment through a compromised network communication path. Finally, if all the above fail, the firmware can still be injected through the JTAG[3] access port or chip-off forensic methodologies [24].

In this work, the threat model allows an adversary to access the control equipment of CBs through the Shodan network engine. Shodan allows to search for Internet-connected devices based on their location (city, country, latitude/longitude), hostname, port, involved operating system, net (search based on an IP or /x CIDR[4]) and even find results within a timeframe. For instance, one could find Cisco devices on a particular subnet. Shodan is being used by researchers and hackers to identify and locate poorly configured or even unprotected devices – and increasingly, ICS and particularly SCADA systems fall into this category as potential targets for exploitation [27], [28]. In combination with fast Internet scanners like ZMap [29], the discovery of vulnerable ICS machines can be used as the network path to control critical assets of the grid.

Many of the ICS devices involved in the control of power infrastructure often have little or no security. These systems are often deployed to the field with their simple factory default credentials included in the manual of the device (which can be

[2] In such scenario, system frequency, voltage and power flows will deviate outside stability limits.

[3] JTAG: Joint Test Action Group - IEEE Std 1149.1 Standard Test Access Port and Boundary-Scan Architecture.

[4] CIDR: Classless Inter-Domain Routing.

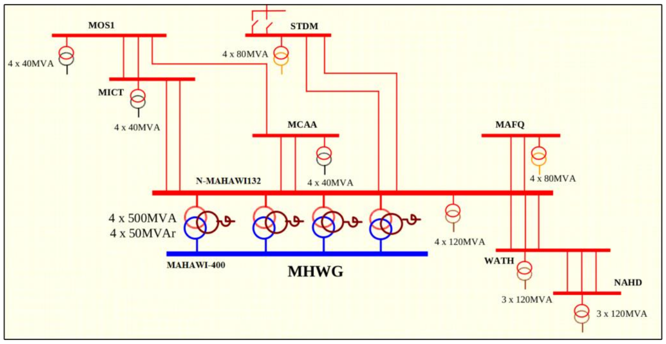


Fig. 3: Electrical power system topology of Mahawi Zone at the Eastern Region of Abu Dhabi, UAE [13].

found online). In 2010, ICS Cyber Emergency Response Team (ICS-CERT) issued an alert specifically addressing Shodan's ability to expose ICS vulnerabilities specifically referring to the risk of cyber attacks as systems "continue to use default user names and passwords and/or common vendor accounts for remote access to these systems" [30].

IV. Experiments

In this section, we present the modeling of a power grid region and the modification process able to disrupt the CBs controllers operation.

A. Power System Modeling

The modeling of a power system region is based on the amount of available data in a particular area. We focus on the Emirate of Abu Dhabi in UAE since the available resources for this region allow us to model accurately every part of the grid. Specifically, we study the high voltage power transmission network at the Eastern Region of Abu Dhabi (Mahawi zone) operated and maintained by TRANSCO [13], [21]. The effect of publicly available resources on power systems is examined through simulation studies. Power flow system analysis is performed using the PowerWorld software package that utilizes the Newton-Raphson algorithm [31].

According to TRANSCO, the existing 220/33 kV Watbha and Mahawi substations are expected to be replaced in 2016 by new substations. The information about the stations in the region of study is shown in Table I. The N-MAHAWI132 substation will be connected through four 500 MVA transformers[5] at MAHAWI-400 grid station. The connections between the stations at the Mahawi area and the transmission line characteristics are given in Table II. Fig. 3 presents the power system topology of the region.

The contingency analysis of the study region indicates that the most critical parts are the MAHAWI-400 grid station and the STDM substation. According to the power system topology and load flow diagrams of TRANSCO [13], the Mahawi zone in 2020 is planned to operate in isolation from the other Eastern regions. However, the CBs at the STDM station are expected to switch generation in case of emergencies (e.g. faults, maintenance, attacks etc.) in order to guarantee power supply to the Mahawi zone from the rest Eastern area.

TABLE I: Grid stations and substations at the Mawahi Zone.

Grid station/Substation Name	Code	Voltage (kV)
Mahawi	MAHAWI-400	400/132 kV
Watbha	WATH	132/33 kV
Mahawi	N-MAHAWI132	132/33 kV
Mussafah	MOS1	132/11 kV
Mussafah M12	MICT - M12	132/11 kV
Mohd Bin Zayed	MCAA	132/11 kV
Al Nahda	NAHD	132/33 kV
Mafraq	MAFRAQ	132/22 kV
Capital District	STDM	132/22 kV

TABLE II: Transmission line data*.

From	To	#Circuits	Length (km)
N-MAHAWI132	WATH	3	11
N-MAHAWI132	MCAA	2	9.5
N-MAHAWI132	STDM	2	8.8
N-MAHAWI132	MICT - M12	2	10.7
N-MAHAWI132	MAFRAQ	2	5
WATH	NAHD	3	5
MOS1	MICT - M12	2	4
MOS1	MCAA	1	3.6

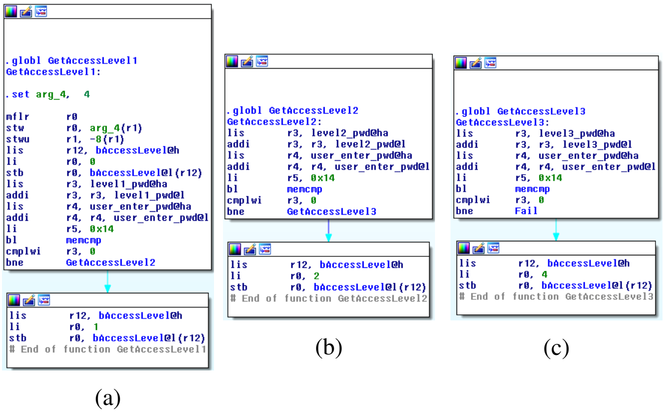
*The 132 kV underground transmission lines have size 1200 sq.mm and constructed with solid cable, cross-linked polyethylene (XLPE). The positive-sequence impedance and admittance as well as the zero-sequence impedance of the lines are as follows: $Z_1 = 0.023 + j0180$ Ω/km, $Y_1 = j77.00\ \mu S/km$, and $Z_0 = 0.240 + j0.120\ \Omega/km$. Thermal rating of the lines is equal to 1000 A [230 MVA].

B. Exploiting Control Equipment Vulnerabilities

In this part, we discuss the analysis and findings related with the firmware of a CB relay controller, Cooper Form 6 (CF6) [32]. CF6 is a microprocessor-based controller used in feeder loop sectionalizing schemes. It can send the appropriate signals for interrupting and reclosing an AC circuit to the connected CB. CF6 is part of the distribution substation equipment of many utility companies such as Clinton Utilities Board (CUB) [15], [33]. CUB is an electrical distributor that serves approximately 30k customers in Clinton, Tennessee and the surrounding area.

The firmware of the CF6 is acquired from the compressed software package ProView of CF6 available at the vendor's website [34]. The image is a 32-bit Executable and Linking Format (ELF) file based on PowerPC architecture. At first we disassemble the binary image using IDA [35], and then reconstruct the firmware: rebuild functions, determine the base address, collect information from strings and rebuild symbols. As a result, we locate functioning critical structures and extract data related with routines behavior. Following, we provide three test cases describing the discovered findings and firmware modifications.

[5] Z_{ps} = 24% (positive sequence impedance of primary-secondary winding of the transformer).



(a)

```
.globl GetAccessLevel1
GetAccessLevel1:

.set arg_4,  4

mflr      r0
stw       r0, arg_4(r1)
stwu      r1, -8(r1)
lis       r12, bAccessLevel@h
li        r0, 0
stb       r0, bAccessLevel@l(r12)
lis       r3, level1_pwd@ha
addi      r3, r3, level1_pwd@l
lis       r4, user_enter_pwd@ha
addi      r4, r4, user_enter_pwd@l
li        r5, 0x14
bl        memcmp
cmplwi    r3, 0
bne       GetAccessLevel2
```

```
lis       r12, bAccessLevel@h
li        r0, 1
stb       r0, bAccessLevel@l(r12)
# End of function GetAccessLevel1
```

(b)

```
.globl GetAccessLevel2
GetAccessLevel2:
lis       r3, level2_pwd@ha
addi      r3, r3, level2_pwd@l
lis       r4, user_enter_pwd@ha
addi      r4, r4, user_enter_pwd@l
li        r5, 0x14
bl        memcmp
cmplwi    r3, 0
bne       GetAccessLevel3
```

```
lis       r12, bAccessLevel@h
li        r0, 2
stb       r0, bAccessLevel@l(r12)
# End of function GetAccessLevel2
```

(c)

```
.globl GetAccessLevel3
GetAccessLevel3:
lis       r3, level3_pwd@ha
addi      r3, r3, level3_pwd@l
lis       r4, user_enter_pwd@ha
addi      r4, r4, user_enter_pwd@l
li        r5, 0x14
bl        memcmp
cmplwi    r3, 0
bne       Fail
```

```
lis       r12, bAccessLevel@h
li        r0, 4
stb       r0, bAccessLevel@l(r12)
# End of function GetAccessLevel3
```

Fig. 4: GetAccessLevel firmware function of CF6 in IDA disassembler: (a) Level 1 (View), (b) Level 2 (Operate) and (c) Level 3 (Modify).

Cooper Form 6 recloser controller:

1) CF6 supports serial communication through the rear panel ports (two RS-232 and one of RS-485/Serial Fiber Optic/Ethernet). The user can configure which back port shall have the communication protocol (Modbus/DNP3/2179/IEC 870-5-101). The firmware includes the implementation of the 9-bit uLan communication protocol which is used to transfer data over the RS-485 link. The presented modification changes the amount of bits allowed to be exchanged in each communication session. By altering the argument modification of a `cmpwi` instruction to a larger number, we effectively overflow the communication link rendering the RS-485 port useless.
2) CF6 requires a password in order to access the user level necessary to initiate any scheme setting to the CF6 control. CF6 has three access levels. Each level defines user privileges: view, operate, and modify. The `SHA-1` hash value of the default access credentials are stored in the .rodata section of the ELF file of firmware. In addition, we leverage the function that checks the access level during initialization shown in Fig. 4, in order to bypass the authentication and thus grant access to non-legitimate users.
3) The CF6 supports DNP3 communication protocol. DNP3 data is sent to a remote terminal server via a TCP socket connection using the terminal server's IP address. When the relay initializes the DNP3 configuration to communicate over TCP/IP, the user needs to specify the outstation IP address and the subnet mask. In addition, the user can name the network of the connection. The modification sets the IP address and subnet mask to values which correspond to the attackers remote server. As a result, the adversary can control the relay controller remotely through DNP3 protocol.

C. Impact Discussion

The function of an IED relay in the operation of a power system is to limit or prevent damage due to overloads and faults, therefore minimizing their effect on the rest of the system. In this section, we discuss the impact of firmware

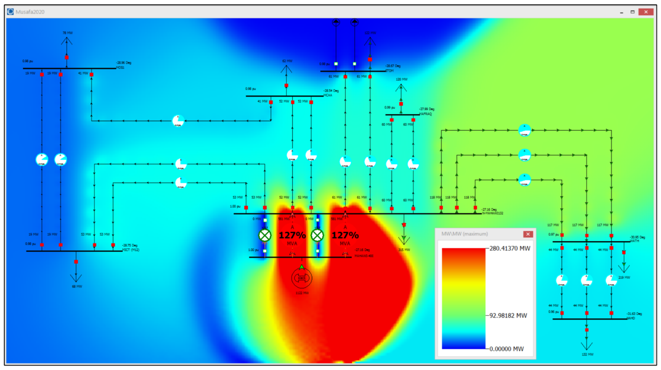


Fig. 5: Active power contour of Mahawi zone when two MAHAWI-400 CBs are tripped.

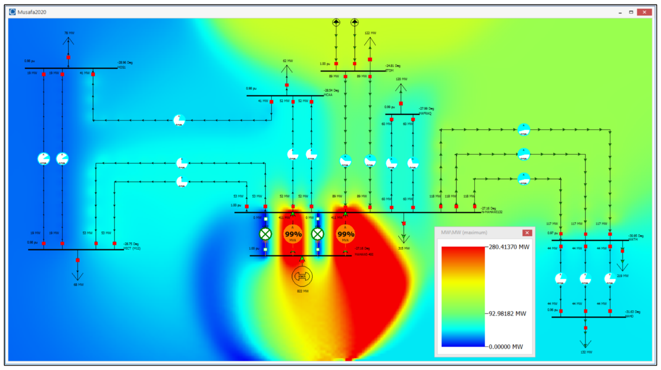
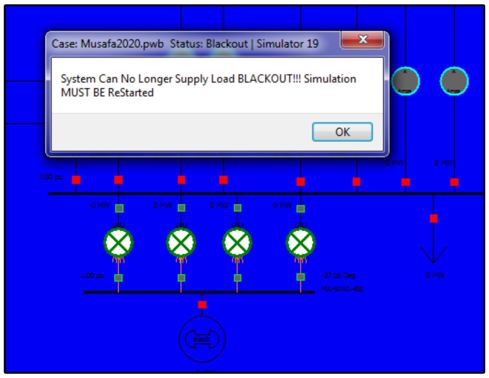


Fig. 6: Active power contour of Mahawi zone when two MAHAWI-400 CBs are tripped and the zone is connected to the rest of Eastern region grid.

attacks on CF6 relay if applied to the station CBs of the Mahawi zone power model.

According to our threat model, the relay as a CB controller can be controlled by a malicious user through the communication channels to the device. ICS radar of Shodan engine for instance, exposes at the time of the submission 588 and 13,949 Internet-facing systems that use DNP3 and Modbus protocol respectively [36]. The adversary at first can access such devices from the network using the default passwords in order to upload the modified malicious firmware image. This can be also achieved through the other techniques mentioned in Section III-C. Doing that, the attacker can manage the status signal in order to close or trip the CB.

The power analysis of the Mahawi zone identified MAHAWI-400 grid station and STDM substation to be the most important components of that particular region. As a result, Fig. 5 displays the active power flow on Mahawi system one-line diagram and contours the results for ease of interpretation in the scenario which two of the CBs at the MAHAWI-400 grid station are attacked. When the zone is connected through the STDM substation to the rest of the Eastern region grid, the thermal effects on the transmission lines are decreased as shown in Fig. 6. In the case which the Mahawi zone is isolated from the Eastern region grid and all the CBs at the MAHAWI-400 grid station are attacked, the system is collapsed and leads to a blackout (Fig. 7).



Case: Musafa2020.pwb Status: Blackout | Simulator 19

System Can No Longer Supply Load BLACKOUT!!! Simulation MUST BE ReStarted

Fig. 7: Network collapse at Mahawi zone when four MAHAWI-400 CBs are tripped.

V. Conclusions

In this paper we demonstrated how public information can be utilized in order to identify critical regions of the smart grid. We also presented that the operation of control equipment can be accessed and modified based on the difficulty level of various penetration paths. The acquire data are utilized in a simulation study to demonstrate an attack scenario on the power system operation.

Acknowledgment

This work was supported by the Center for Cyber Security, NYU Abu Dhabi, and the NYU Abu Dhabi Global PhD Fellowship program.

References

[1] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Nov 2015, pp. 283–288.

[2] M. Assante, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," [Online]: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid, 2016.

[3] M. Amin, "The Case for Smart Grid: Funding a new infrastructure in an age of uncertainty," [Online]: http://www.ferc.gov, 2015.

[4] McAfee, "Global Energy Cyberattacks: Night Dragon," [Online]: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

[5] J. Momoh and L. Mili, *Economic Market Design and Planning for Electric Power Systems*, IEEE Press Series on Power Engineering. Wiley, 2009.

[6] U.S. Energy Information Administration, U.S. Department of Energy, "International Energy Statistics," [Online]: http://www.eia.gov/.

[7] Regulation & Supervision Bureau, "System planning," [Online]: http://rsb.gov.ae/en/sector/system-planning.

[8] Roland Berger Strategy Consultants, "Study regarding grid infrastructure development: European strategy for raising public acceptance," [Online]: https://ec.europa.eu/energy/sites/ener/files/documents/20140618_grid_toolkit_report.pdf.

[9] S. McLaughlin, C. Konstantinou, et al., "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. PP, no. 99, pp. 1–19, 2016.

[10] Schneider Electric, "SCADA Systems, White paper," [Online]: http://www.schneider-electric.com.

[11] Wikipedia, "List of United States electric companies," [Online]: https://en.wikipedia.org/wiki/List_of_United_States_electric_companies.

[12] "Dalton Utilities Facts," [Online]: http://www.dutil.com/residential/elec_facilities.php.

[13] TRANSCO, "2012 Seven Year Electricity Planning Statement," [Online]: http://www.transco.ae/media/pdf/Final-2012%207YPS-Attachments.pdf.

[14] "Dalton Utilities awards $7.4 million SCADA contract to Invensys Process Systems," [Online]: http://www.waterworld.com/articles/2001/10/dalton-utilities-awards-74-million-scada-contract-to-invensys-process-systems.html.

[15] ProSoft Technology, "The power of industrial wireless in Cumberland," [Online]: http://www.prosoft-technology.com/NEWS-EVENTS/Success-Stories/Industry/Power/The-power-of-industrial-wireless-in-Cumberland%E2%80%A6.

[16] "Hometown Connections International, LLC," [Online]: http://www.hometownconnections.com/news/the-right-software-applications-integrate-core-utility-functions/.

[17] Xcel Energy, "Directory files," [Online]: https://www.xcelenergy.com/staticfiles/.

[18] Xcel Energy, "Hiawatha Project," [Online]: https://www.xcelenergy.com/staticfiles/xe/Corporate/Corporate%20PDFs/HiawathaAppendixD1-D2.pdf.

[19] Electricity Authority of Cyprus, "Annual Reports," [Online]: https://www.eac.com.cy/EN/EAC/FinancialInformation/Pages/AnnualReports.aspx.

[20] Clinton Utilities Board, "YouTube channel," [Online]: https://www.youtube.com/channel/UCpy8qIkcIXBlYXuFA5h7iRw.

[21] TRANSCO, "2013 Seven Year Electricity Planning Statement," [Online]: http://www.transco.ae/media/pdf/20137YPS-Main%20Report.pdf.

[22] NERC Standard TPL-001-4, "Reliability Standards for the Bulk Electric Systems of North America," 2014.

[23] A. Costin, J. Zaddach, et al., "A Large Scale Analysis of the Security of Embedded Firmwares," in *Proceedings of the 23rd USENIX Security Symposium (USENIX Security)*, 2014.

[24] M. Breeuwsma, M. De Jongh, et al., "Forensic data recovery from flash memory," *Small Scale Digital Device Forensics Journal*, vol. 1, no. 1, pp. 1–17, 2007.

[25] U.S. Department of Homeland Security, "Industrial Control Systems Cyber Emergency Response Team, Year in Review," [Online]: https://ics-cert.us-cert.gov/, 2014.

[26] "SHODAN search engine for Internet-connected devices," [Online]: https://www.shodan.io/.

[27] "SHODAN - Industrial Control Systems," [Online]: https://www.shodan.io/explore/category/industrial-control-systems.

[28] Eireann P Leverett, "Quantitatively assessing and visualising industrial system attack surfaces," *University of Cambridge, Darwin College*, 2011.

[29] "ZMap - Network Scanner," [Online]: https://zmap.io/.

[30] U.S. Department of Homeland Security, "ICS-ALERT-10-301-01," [Online]: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01, 2010.

[31] "PowerWorld Simulator," [Online]: http://www.powerworld.com/.

[32] "Form 6 Recloser Control," [Online]: http://www.cooperindustries.com/content/public/en/power_systems/products/controls_and_relays/recloser_controls/form_6.html.

[33] "Clinton Utilities Board," [Online]: http://www.clintonutilities.com/.

[34] "Cooper Form 6 Recloser Control v401 Firmware," [Online]: http://www.cooperindustries.com/content/public/en/power_systems/products/controls_and_relays/recloser_controls/proview-software-for-form-6-control1.html.

[35] "IDA disassembler and debugger," [Online]: https://www.hex-rays.com/products/ida/.

[36] "Shodan ICS Radar," [Online]: https://ics-radar.shodan.io/.