SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions

Prageeth Gunathilaka, Daisuke Mashima, and Binbin Chen
Advanced Digital Sciences Center
1 Fusionopolis Way, #08-10 Connexis North Tower
Singapore 138632
{prageeth.g, daisuke.m, binbin.chen}@adsc.com.sg

ABSTRACT

Electrical substations are crucial for power grids. A number of international standards, such as IEC 60870 and 61850, have emerged to enable remote and automated control over substations. However, owing to insufficient security consideration in their design and implementation, the resulting systems could be vulnerable to cyber attacks. As a result, the modernization of a large number of substations dramatically increases the scale of potential damage successful attacks can cause on power grids. To counter such a risk, one promising direction is to design and deploy an additional layer of defense at the substations. However, it remains a challenge to evaluate various substation cybersecurity solutions in a realistic environment. In this paper, we present the design and implementation of *SoftGrid*, a software-based smart grid testbed for evaluating the effectiveness, performance, and interoperability of various security solutions implemented to protect the remote control interface of substations. We demonstrate the capability and usefulness of SoftGrid through a concrete case study. We plan to open-source SoftGrid to facilitate security research in related areas.

Keywords

Smart Grid; Cybersecurity; Electrical substations; IEC 60870; IEC 61850; Software-based testbed

1. INTRODUCTION

In power grid systems, electrical substations play crucial roles to deliver electricity from generators to consumers. Besides transforming the voltage level at various stages, they also control the power flow and grid topology. There can be thousands of electrical substations under a single utility company. For instance, there are over 11,000 transmission/distribution substations in Singapore as of March 2016 [1], 26 of them operating at 230KV or a higher voltage. In order to manage power grids in an effective and timely manner, modernization of electrical substations is highly demanded, and a number of standard technologies, such as IEC 60870 and IEC 61850 [23], have been established for providing remote control and automation functionality.

Risks exposed by substations' remote interfaces

Although the use of such technologies reduces the operational cost and improves the quality and stability of electricity services, it has at the same time opened a door for cyber attackers. For instance, cyber attacks could be mounted via network [25, 31] to inject malicious control commands to circuit breakers and transformers. Although the IEC 62351 standard [22] has been defined to secure standard power grid and energy system protocols, it is unfortunately not yet widely used in practice. Even if the communication protocols were completely secure, it is still possible that attacks could be mounted by misusing or abusing the systems in the control center. For instance, disgruntled insiders might send out malicious control commands by abusing their access privilege to the system. Moreover, attackers may utilize malware to hijack the system. Possibility of such attacks cannot be fully eliminated even with typical cybersecurity measures, such as user authentication, access control, anti-virus systems, etc., are in place.

Such risks have already been exhibited in several real-world incidents. In Tempe, AZ in 2007, accidental activation of a load-shedding program in an energy management system (EMS) opened 141 circuit breakers and caused large-scale blackout, affecting 98,700 customers corresponding to 399 MW [42]. Although this was not the result of cyber attacks, this incident demonstrated the level of damage a potential attack may make. More recently, in the Ukraine incident in December, 2015, the control center system was hacked by means of malware to send out a number of commands to open circuit breakers, and the attack made 30 substations offline for hours, which affected over 230,000 customers [45]. This incident not only demonstrated that securing remote control interface of electrical substations is a crucial problem that requires immediate solution, but it also shows the importance of having additional layers of defense that can remain effective even when traditional cybersecurity measures are bypassed.

Providing new layers of defense at substations

According to IEC TC57 technical report [23], remote control commands sent to electrical substations are mediated by the gateway of each substation, which is also responsible for protocol translation (e.g., between IEC 60870-5-104 and IEC 61850). A gateway with security features can intercept,

CPS-SPC'16, October 28 2016, Vienna, Austria.
© 2016 ACM. ISBN 978-1-4503-4568-2/16/10...$15.00
DOI: http://dx.doi.org/10.1145/2994487.2994494

inspect, and pre-process remote control commands, hence it is an ideal place for providing an additional layer of defense.

For example, application-layer firewalls that can provide deep packet inspection capability at substations have attracted increasing attention over the past few years. As another concrete example of substation cybersecurity solutions, our recent work proposed the design of an *active command mediation* system (also called A*CMD system in this paper) [30], which inspects all remote control commands and actively mediates their execution to mitigate potential impact of malicious commands. For example, an A*CMD system can delay the execution of a circuit-breaker-opening command by a few hundred milliseconds (the delay is decided in an autonomous and probabilistic manner), subject to the grid's operating requirements. This is to avoid the situation where a large number of such commands are issued by an attacker and all get executed. When such attacks happen, the introduced delay allows individual A*CMD systems to spare some time buffer to assess the situation and withdraw any pending commands that can make the situation worse. Since active mediation like this is carried out even when no abnormal behavior has been detected by firewalls or intrusion detection systems, an A*CMD system is complementary to other detection-based security mechanisms and is effective against attacks mounted from a legitimate control center system, such as insider attacks.

Evaluating substation cybersecurity solutions

In order to evaluate various security solutions developed for securing of remote control interface of modern substations (e.g., the A*CMD system), it is mandatory to have a testing environment where a variety of remote control attacks can be simulated and the effectiveness of a security solution, i.e., how much they can reduce the security risk of a power grid, can be evaluated. It is also important for grid operators to evaluate the interoperability and performance overhead of security solutions before their actual deployment. Based on our survey about existing cyber-physical system and smart grid testbeds, we found that existing testbed solutions are either hard to access (e.g., they are composed of dedicated hardware and require on-site access), have limited scale (especially if they are hardware-based), or require substantial amount of time and learning efforts to set up and operate. These have motivated us to design a software-based smart grid testing environment that can facilitate researchers, engineers, and grid operators to conduct high-fidelity assessments of security solutions for modernized electrical substations. Towards this, we make several contributions:

- We first enumerate key requirements and desired properties of a testbed for evaluating substation cybersecurity solutions.
- We developed *SoftGrid*, a turn-key, software-based testing environment that is designed for handy, end-to-end, and high-fidelity evaluation of substation cybersecurity solutions. We foresee an increasing need for conducting such evaluations, hence we plan to open-source our testbed implementation (excluding third-party products and libraries).
- We evaluate the performance and scalability of SoftGrid. Furthermore, through a case study where we use SoftGrid to assess an A*CMD system prototype, we demonstrate the usefulness and capability of the SoftGrid testbed.

The rest of this paper is organized as follows. In Section 2 we discuss related work. Section 3 enumerates design goals, and Section 4 presents the design and implementation of SoftGrid, along with its performance and scalability measurements. Section 5 presents a case study using SoftGrid to evaluate an A*CMD prototype, followed by discussion about application to other security solutions in Section 6. We conclude the paper with future directions in Section 7.

2. RELATED WORK

Standard protocols that are widely used in modernized substations, such as IEC 60870 and 61850 [23], are often vulnerable against replay attacks and man-in-the-middle attacks [25, 31]. Although IEC 62351 [16, 22, 33] has been established to provide standard guideline to secure the communication, owing to its relatively heavy requirements (e.g., reliance on public-key cryptography), it is not yet widely deployed in practice.

A variety of solutions that can contribute to securing automated/digitized electrical substations have been proposed [12, 27, 32, 39, 40, 41]. For example, [12] provides advanced firewalls that are specifically designed for SCADA systems. [29, 40] extend the Bro intrusion detection system to detect malicious power grid commands. Firewalls and intrusion detection systems can raise alarms and block attacks when they detect unusual packet format and content, but may fail to block malicious but legitimately-looking commands. Such commands can be issued by either insiders or external attackers who somehow get access to the system, e.g., by means of malware (as demonstrated in the incident in Ukraine in 2015 [45]). The active command mediation (A*CMD) system [30] is another new proposal for enhancing security at substation gateways. It is complementary to aforementioned efforts and aims at mitigating impact of cyber attacks even when other security measures are somehow bypassed. As will be further described in Section 5.1, an A*CMD system is, as part of a substation gateway, responsible for intercepting and actively mediating incoming remote control commands to mitigate the impact of attacks. One example of mediation scheme, as proposed in [30], is artificially delaying control commands to buy time for attack detection mechanisms. Instead of delaying commands, another substation security solution [28] proposes a command-reversing approach that issues reversing control commands when a certain control commands are flagged as attacks.

While the industry and research community have proposed several promising technical solutions for securing modern substations, whether such solutions can cross the chasm and make it to real deployment highly depends on whether their effectiveness, performance, and interoperability can be convincingly proved. For the sake of evaluation of smart grid technologies, including cybersecurity aspects, a number of smart grid testbeds have been implemented, such as [6], [36], and [44]. Several of them consist of real power-grid devices to accomplish high-fidelity assessment. However, hardware-based testbeds are not easily accessible or portable. Namely, on-site visit and certain kind of partnership with the testbed provider is often required. Moreover, hardware-based approaches usually do not scale well. They also offer limited flexibility for quick configuration and customization that are needed for testing different solutions under different kind of power grid settings. Last but not the least, they require huge introductory cost for deployment as well as intensive personnel training.

There are also a number of efforts that develop software-based solutions for evaluating smart grid and/or cyber-physical systems. The design and implementation of such testing solutions are still an active research area, and some notable efforts include [7, 8, 18, 19, 21, 26, 34, 35, 37, 38]. For instance, [35] put emphasis on intrusion detection systems within substations, supporting IEC 61850 GOOSE and SMV protocols. [37] and [38] aimed at more generic use cases, such as analysis involving renewable integration, demand response, microgrids, and so forth. However, neither of them is specifically designed for cybersecurity assessments. OpenMUC [7], which we leveraged in implementing our testbed, provides good support to evaluate a product's interoperability with international standards, but it does not provide an end-to-end evaluation that includes physical impact analysis. On the other hand, PowerWorld [8] only offers power grid simulation and entirely lacks the cyber side. In terms of architecture, a testbed presented in [18] is similar to ours. They emulate cyber-side using Emulab [43], a widely-used network emulator, which is connected to a power grid system simulated with SimuLink on a PC called "simulation core". On the paper their primary focus is to evaluate the impact of attacks, and the presented testbed doesn't have built-in support of the latest standard protocols used in our context, namely IEC 60870-5-104 and IEC 61850. The same authors published another advanced testbeds [19, 34]. These testbeds can evaluate attacks that are outside of our scope, such as control code rewriting targeting PLCs. Furthermore, integration of multiple types of cyber-physical systems, e.g., power systems and railway systems, is in their scope. However, they are not specifically designed for power grid systems and therefore lacks some of the key features we desired.

Davis et al. [17] proposed a framework to model dependencies between cyber and physical sides of smart grid systems. Similar to our testbed, their work is purely software-based and uses PowerWorld simulator [8] for physical impact evaluation. While their solution can also be used for assessing physical impact of cyber attacks on power grid systems, their framework models the cyber attacks in a more abstract level (e.g., they do not simulate the packets of specific SCADA protocols). In addition, their focus is not to evaluate real devices/prototypes, but to support architecture design and review of secure cyber-physical systems.

When we attempted to evaluate our proposed A*CMD solution [30] (see more description in Section 5.1), we were not able to find a suitable testbed that meets all key requirements we desired (see Section 3). This has motivated us to design and implement our own software-based testbed. Our work targets specifically at an evaluation environment for easy, scalable, and high-fidelity evaluation of substation cybersecurity solutions.

3. DESIGN GOALS

The conceptual view of our envisioned testbed is shown in Figure 1. As mentioned in Section 2, the direct motivation and goal for our testbed are to provide a high-fidelity testing environment for an active command mediation (A*CMD) solution proposed by us [30]. Through detailed requirement analysis, we found that the same testbed will actually be able to support the evaluation of other types of security solutions for remote control interface of modernized substations, such as firewalls [12], intrusion detection systems (IDS) [27, 40], etc., that are deployed between the control center and Intelligent Electronic Devices (IEDs), which are communication endpoints connected to physical devices in power grids. The modules in shaded boxes (i.e., the control center, IEDs, power system devices, and a power system simulator) form the main components of our testbed, and a substation security solution that is to be deployed between the control center and IEDs (e.g., substation gateways, firewalls, IDSes, and A*CMD systems etc.) can be directly plugged into the testbed for different types of evaluation, in terms of their effectiveness in mitigating attacks, performance, and interoperability. Moreover, the design should support the evaluation of multiple substations, which are equipped with the same or heterogeneous security solutions.

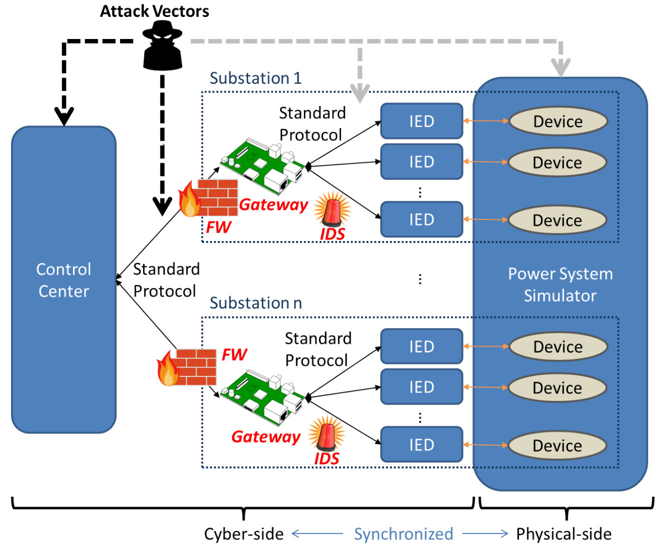


Figure 1: A conceptual view of a testbed. The testbed components are marked in shaded blue boxes. The testbed can evaluate different types of solutions, including gateways, IDSes, and firewalls, as illustrated in the figure.

In the following, we enumerate the key requirements and desired properties that we identified.

- **Real-world interoperability:** It is highly desirable if the testbed can be used to assess products or prototype solutions that are meant for actual deployment. Also, our goal is to evaluate a substation cybersecurity solution in a setting that resembles a real-world environment. To achieve so, it requires the testbed modules that interface with the substation cybersecurity solution under test to be able to communicate directly with those real-world solutions or devices. Since we focus on security solutions that are to be deployed at or around the substation gateways, the testbed needs to have a control center module and IED modules that can communicate with the solution under test using standard protocols. In this paper, we focus on IEC 60870-5-104 and IEC 61850 protocols since they are increasingly adopted in power grid systems.

- **Flexible and scalable power grid configuration:** A substation cybersecurity solution needs to be tested against a variety of power grid configurations. Hence, the testbed needs to be flexible enough to allow users to conveniently define different power grid settings. Besides flexibility, it is highly desirable for a testbed solution to support settings that resemble large-scale power grid systems. In fact, scalability is a major limitation of hardware-based approaches. For instance, the hardware-based testbed used in [36] includes only 16 buses. A solution may perform very differently in a system with a few dozen buses, as compared to a larger system with hundreds or even thousands of buses. In this sense, software-based approach is desirable.

- **Tight cyber-physical synchronization:** To be used for testing of substation cybersecurity solutions, it is important that both cyber infrastructure and physical power system in the testbed can work in a tightly synchronized manner. For instance, from the perspective of a substation gateway device under test, the cyber side and physical side should behave just like that in a real environment. More specifically, once some incoming remote control commands are received and executed, their impact on the physical systems, as the outcome of the control commands, should be reflected in real-time to the subsequent interrogation commands issued to the substation gateway.

- **Advanced evaluation supports:** The testbed should offer features for monitoring and logging power grid status for both online and offline analysis and evaluation. The key metrics to be monitored depend on the purpose of the experiments. For example, they may include the amount of power flow on each transmission line, status of circuit breakers, generation and/or load amount, voltage on each bus, power grid frequency, etc. In addition, threshold-based violation detection based on these measurements is also desired. Based on our survey, most of the existing software-based testbed implementations rely only on steady state simulation. However, some grid stability issues, such as short-term frequency deviation, may only be visible during transient state. Thus, to complement steady state simulation, the integration of transient stability analysis is highly desired for detailed impact assessment. Additionally, feasibility to manage and repeat/reproduce experiments is a general requirement for a testbed, which we also must implement.

- **Turn-key solution:** Besides meeting the requirements discussed above, we aim at a testbed that is easy to set up and operate. For users (e.g., grid operators and security solution vendors), some of which might not be IT experts, to quickly construct the testing environment, a turn-key solution that requires minimal configuration (e.g., just by defining power grid for simulation and plugging in a security solution to be tested) is highly demanded.

- **Easy modeling of relevant attack vectors:** The testbed should support the simulation of different types of cyber attacks that are within the scope, as shown in Figure 1. Since in this work our key concern is the remote control interface of substations, we primarily focus on the evaluation of attacks that either hijack the control center system to send out malicious control commands (as in the case of the recent Ukraine incident [45]), or launch replay attacks and man-in-the-middle attacks via network, as well as security solutions against them. They are highlighted with dark-colored arrows in Figure 1. We envision that in the future it is demanded to simulate other attack vectors, such as attacks launched locally against selected substations, attacks remotely or locally compromising firmware or configuration of IEDs, and attacks launched directly on physical components. We mark them with light-gray arrows in Figure 1. Extension of the testbed to cover them are left for our future work.

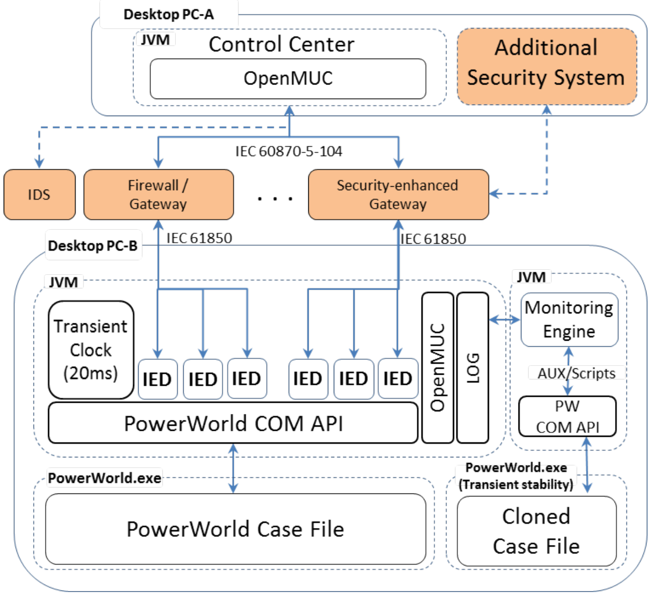


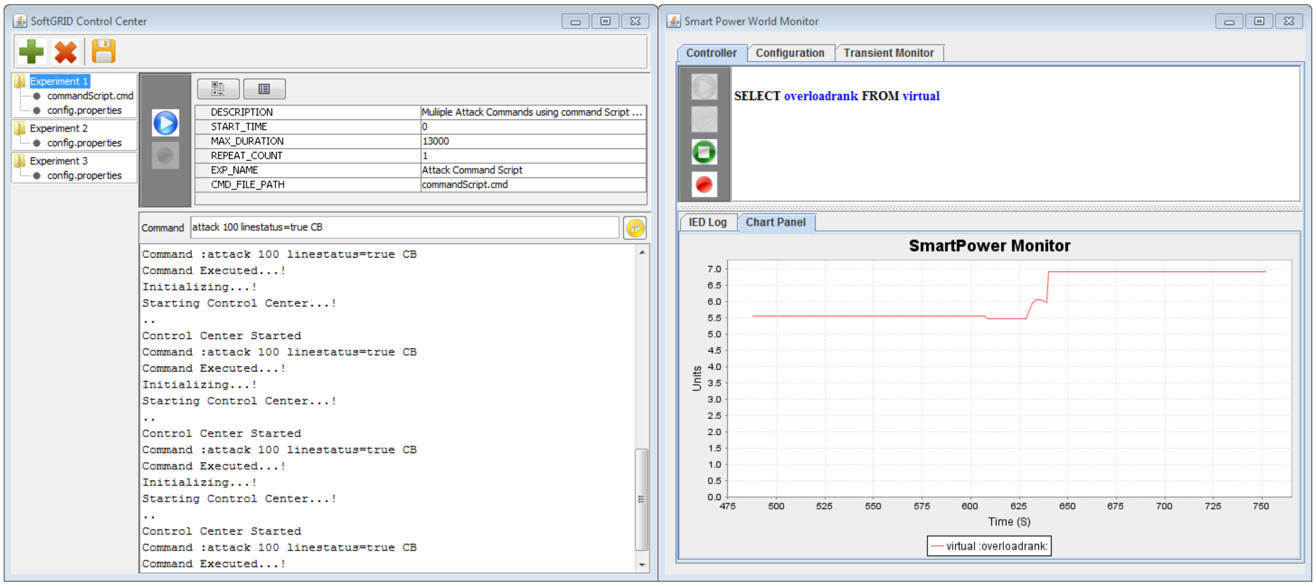
Figure 2: Implementation overview of SoftGrid testbed. Desktop PC-A and B can be the same PC. Components with shaded boxes represent security solutions under test that are plugged into the SoftGrid testbed. A cloned case file is used for transient stability analysis to reflect the up-to-date state.

4. SOFTGRID: A SOFTWARE-BASED SMART GRID TESTBED

In this section, we discuss our testbed design to meet the goals discussed in Section 3 and also evaluate the implementation of SoftGrid in terms of performance and scalability.

4.1 Design & Implementation

In this section, we present the design and implementation of our *SoftGrid* testbed for evaluating substation security solutions in terms of their effectiveness, performance and interoperability. Figure 2 shows the architecture of the SoftGrid testbed. Shaded components show examples of possible security solutions/devices that can be evaluated, such as intrusion detection systems (IDSes), firewalls, and security-enhanced gateways. In our design, they can be plugged into the SoftGrid testbed easily. Note that the substation security solutions under test often require the support from some



DESCRIPTION	Muliiple Attack Commands using command Script ...
START_TIME	0
MAX_DURATION	13000
REPEAT_COUNT	1
EXP_NAME	Attack Command Script
CMD_FILE_PATH	commandScript.cmd

Command attack 100 linestatus=true CB

```
Command :attack 100 linestatus=true CB
Command Executed...!
Initializing...!
Starting Control Center...!
..
Control Center Started
Command :attack 100 linestatus=true CB
Command Executed...!
Initializing...!
Starting Control Center...!
..
Control Center Started
Command :attack 100 linestatus=true CB
Command Executed...!
Initializing...!
Starting Control Center...!
..
Control Center Started
Command :attack 100 linestatus=true CB
Command Executed...!
```

```
SELECT overloadrank FROM virtual
```

Figure 3: Screenshots of SoftGrid. Control Center Window (left) shows the communication traffic with the substations, and Monitoring Window (right) shows the power grid status of interest and observed violations.

external system component, such as an attack detection system deployed at the control center. Our testbed includes a place-holder to be used for implementing a server-side security component, which may interact with a security solution under test via a secure communication channel protected by TLS. Below, we discuss our approaches to meet the design goals enumerated in Section 3.

4.1.1 Standard-compliant Control Center and IED

To meet the real-world interoperability goal, it is crucial that the components that interact with the security solution under test, namely the control center and IEDs, must support standardized protocols that are supported by the solution. Our initial implementation supports IEC 60870-5-104 at the control center side and IEC 61850 MMS at the IED side. This is a common configuration of many power grid systems in Europe and Asia. To implement such standard protocols, we employed an open-source library called OpenMUC [7]. Our implementation is extensible to support other protocols such as DNP3, Modbus, and so forth.

On top of OpenMUC, SoftGrid's control center module implements a command-line user interface for sending interrogation and control commands to substations, and a text-based console to display interrogation results (see Figure 3). Likewise, IEDs that are compliant with IEC 61850 MMS are implemented using OpenMUC. In the real systems, there are a variety of IEDs. For instance, some IEDs, such as protection relays, may have advanced protection and control functionality. In our current implementation, however, each IED is modeled as a simple communication endpoint that receives interrogation and control commands and sends back responses. This is because the current focus of SoftGrid testbed is to assess solutions for securing the remote control interface of substations. Hence, we have not modeled possible abnormal behavior that may happen within a substation network. For the sake of simplicity, we currently define a 1-to-1 mapping between an IED and a power system device. This can be easily extended to support the case where a single IED operates multiple physical devices. IEDs are implemented as threads running on a Java VM. Each IED runs on its own thread, and different IEDs listen to different communication ports. Associated power system devices (e.g., circuit breakers, transformers, etc.) and their parameters are defined in IED Capability Description (ICD) files written in standard Substation Configuration Language (SCL), which are made available to a security solution under test for easy setup. By loading these ICD files (or a Substation Configuration Description file, also called a SCD file, that defines an entire substation), a security solution (e.g., a gateway) can be easily configured to interact with the IEDs in SoftGrid. We should also note that default ICD files and SCD file are generated automatically according to model definitions of a simulated power grid (i.e., a PowerWorld case file explained later). Therefore, basic experiments can be started immediately after loading a designed PowerWorld case file, satisfying the turn-key property.

SoftGrid also supports the simulation of multiple substations. In such a setting, IEDs are grouped according to the configuration of each substation, and the corresponding sets of ICD files are loaded on the corresponding substation gateways to define which IEDs are under their control. The same mapping is also configured on the control center.

4.1.2 Cyber-physical Integration

To support flexible and scalable power grid configuration, we employed the PowerWorld simulator [8], a high-fidelity power system simulator widely used by academia as well as industry users. PowerWorld allows users to arbitrary define power grid topology and detailed configuration of each physical component. With that, SoftGrid can simulate different power grid settings by loading different PowerWorld case files. We use a 37-bus system [20] shown in Figure 4 in our case study later. We also tested larger power grid systems, e.g., the 2000-bus system from [11], and found that PowerWorld can simulate such systems on commodity PCs with very low processing latency.

To achieve our third design goal on tight cyber-physical synchronization, we keep a PowerWorld instance running throughout the experiment, and bridge our IED modules with PowerWorld using PowerWorld's COM APIs. To ensure up-to-date status of a simulated power grid is available to the testbed, *Transient Clock* module is responsible for periodically requesting PowerWorld for recalculation (e.g., every 20ms in our current implementation) to reflect changes made by control from IEDs or perhaps by direct manipulation on PowerWorld. During the simulation, when IEDs receive incoming control commands, the requested changes (e.g., opening/closing a specified circuit breaker) are sent to PowerWorld via the COM API. Then, the outcome (changes in power flow, voltage, etc.) from the simulator will be visible to IEDs. In our preliminary evaluation, the turn-around time of PowerWorld is short (in milliseconds), even when we simulate large power systems. In this way, from the perspective of the security solution under test, the simulated power grid behaves similar to a real system.

4.1.3 Monitoring and Evaluation Support

Various logs are generated on the control center and IEDs. The control center records history of control or interrogation commands it sends out as well as responses received from IEDs. Through the interrogation response, at anytime during the simulation, the control center can learn the status of power grid, such as bus voltage, amount of power flow on each transmission line, and so forth.

On the other hand, IEDs record received commands along with timestamp. In addition, each IED periodically (e.g., every 20ms) polls status information from a physical component on a power grid simulator and logs them on *Monitoring Engine*, which is used not only for a variety of evaluation regarding impact on grid stability but also for visualization on *Monitoring Window*. As can be seen on the figure, Monitoring Window implements an "SQL-like" front end (see the top pane of Monitoring Windows in Figure 3) so that a user can select log data to be displayed. By implementing the detailed grid status monitoring and logging on the IED side instead of the control center side, we can minimize the communication overhead caused by the monitoring tasks.

Moreover, data logged by Monitoring Engine (e.g., timestamp and payload of received commands) are also used to generate an input file, called an *AUX file*, for PowerWorld's transient stability analysis, which is passed to a separate instance of PowerWorld simulator via PowerWorld COM API for transient state simulation. In this way, while our testbed primarily uses steady state simulation on PowerWorld for online simulation, the logged data can be used to reconstruct command timings and sequences to perform transient stability analysis, which allows us to further investigate impact on the power grid during transient state. The transient stability analysis can be run either in batch or automatically in near real-time manner, Monitoring Engine can also log and count typical violations in voltage, frequency, etc. based on criteria suggested by, e.g., Western Electricity Coordinating Council (WECC) [14].

4.1.4 Attack Vector Modeling

Our control center module can be reused as an attack source that is abusing and/or impersonating the control center system to send malicious control commands. For instance, an attacker that takes full control of the control center system can be simulated in such a way. SoftGrid provides some example attack scenarios (e.g., sending "open" commands to all or randomly-selected circuit breakers) to facilitate attack experiments. In addition, the same interface supports simple attack scripts, each line of which specifies a control command and timestamp at which the command is sent out. Using this feature, users can not only simulate well-designed, time-sensitive attacks but also to easily repeat or reproduce experiments. Addition of more features is part of our future work.

Our testbed also can be extended in the future to support the other attacker models shown in Figure 1. For instance, physical attacker can be simulated by implementing an additional attacker module that directly calls PowerWorld COM API. Attacks mounted from inside of a substation can also be simulated, for example, by a module that spreads bogus IEC 61850 messages directly to IEDs. In either case, the impact of attacks can be evaluated on PowerWorld.

4.2 SoftGrid's Performance & Scalability

To evaluate the performance and scalability of SoftGrid testbed, we picked 4 case files created for PowerWorld, ranging from a grid with 37 buses to one with 2000 buses as listed in Table 1. Because of the turn-key property discussed earlier, we can easily switch case files and run experiments. The UIUC 150-bus system [13] and the Texas 2000-bus system [11] are synthetic, but they are designed based on public information of real, state-wide power grid systems. We deployed a control center module, a Java VM running all IEDs, and a PowerWorld simulator on a PC with 32GB memory and Intel i7-6700 CPU (3.40 GHz), called a testbed PC. We setup one substation gateway, which implements basic protocol translation between IEC 60870-5-104 and IEC 61850 MMS on another PC with 16GB memory and Intel i7-6620 CPU (3.50 GHz). For each PowerWorld case file, the number of IEDs, each of which corresponds to one power system device in the simulated power grid, is also shown in Table 1. For example, the GSO 37-bus case file contains 37 buses, 41 transmission lines with circuit breakers, 9 generators, 22 loads, 8 shunt reactors, and 15 transformers, and therefore in total there are 132 IEDs. Based on the definition of the case file, our testbed automatically generates 132 ICD files and 1 SCD file that a security solution under test (i.e., the protocol translation gateway here) may need to access and control these components.

We first measured the number of interrogation commands SoftGrid can process every second. As can be seen in Table 1, for all case files, the number of processed commands per second was over 500, which means that interrogation of all IEDs can be processed in less than a second for 37-bus, 118-bus, and 150-bus systems. We were not able to find specific information about the desired throughput for interrogation commands, so we studied a network traffic trace captured in a real substation system. The duration of the trace was 21 hours and it contained 351 distinct Information Object Addresses (IOA), each of which corresponds to individual data point on a device [2]. The trace contained 954 commands in total, including clock synchronization, interrogation, and control commands. Among them, the number of control commands was 204. Moreover, the maximum number of commands in any minute was 16, which translates to a peak load of about 0.26 commands per second (for 351 IOAs in the system). As a rough estimate, if we simply extrapo-

Table 1: SoftGrid performance with power grids of different scale

Case File	# of IEDs	Commands per Second	Response Time	Avarage CPU Usage	Max Memory Usage
GSO 37-bus [20]	132	> 500	297 ms	13 %	150 MB
IEEE 118-bus [3]	460	> 500	328 ms	15 %	3 GB
UIUC 150-bus [13]	547	> 500	329 ms	15 %	3 GB
Texas 2000-bus [11]	7,273	> 500	471 ms	16 %	4.5 GB

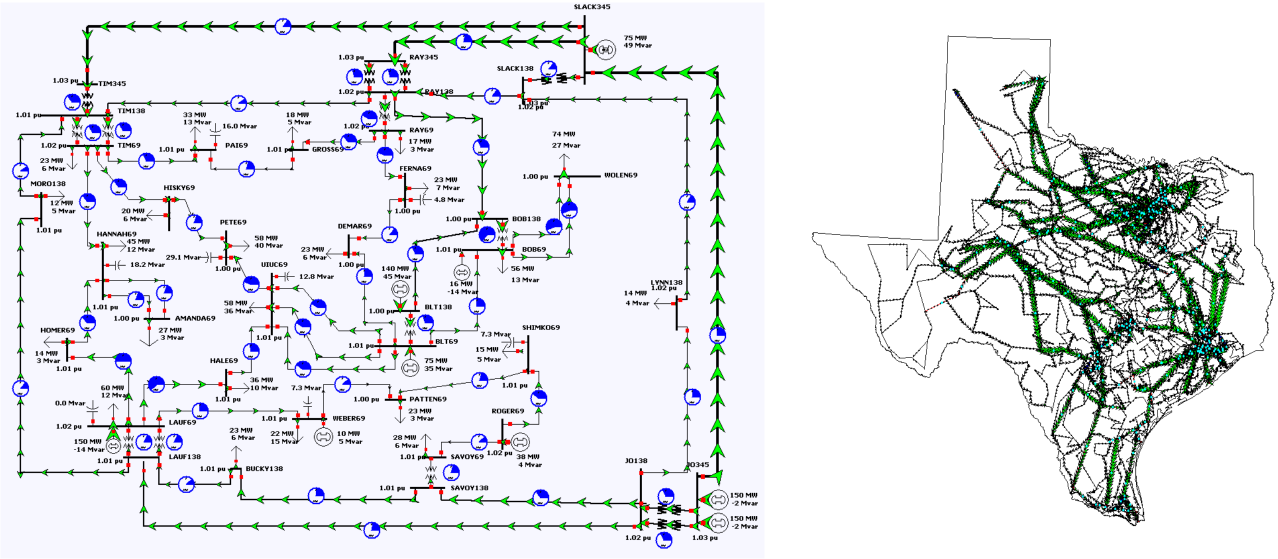


Figure 4: Examples of simulated power grids (37-bus system on the left and 2000-bus system on the right)

late the number of commands per seconds and assume one IED correspond to one IOA, a 2000-bus system with 7,243 IEDs would only have around 5 commands per seconds (i.e., 5/351 × 7243). Likewise, in the trace we captured at most 20 interrogation requests per hour (i.e., around 0.005 per second), which can be in the same way extrapolated to 0.1 command per second in the case of the 2000-bus system. Thus, communication scalability of SoftGrid testbed by far exceeds these numbers and allows us to run even stress testing on a security solution under test. If higher interrogation command throughput is needed, one can potentially split the IEDs into multiple sets (e.g., according to their regions) and run them on different PCs.

The average response time for interrogation measured at the control center (i.e., duration after sending an interrogation request till receiving the corresponding response) and average CPU usage and max memory usage on the testbed PC when handling these numbers of interrogation commands are also measured (Table 1). Regarding the average response time, a guideline issued by IEEE Power Engineering Society [24] says that delivery time requirements for monitoring and control information is 1 second in case a node is external to a substation (e.g., the control center). Our measurements are less than 500ms for all case files, and therefore meeting this requirement. Based on our observation about resource usage, CPU and memory usage of our testbed modules are small enough for commodity PCs, and all components, including a PowerWorld simulator, can fit into a single PC, which offers the ease of setup and portability.

5. PUTTING SOFTGRID INTO USE

The motivation to develop the SoftGrid testbed is to allow researchers and developers to evaluate the effectiveness and performance of substation cybersecurity solutions of interest. It also enables users, such as grid operators, to assess a new solution's interoperability with existing infrastructure before actual deployment. In this section, we will take an active command mediation (A*CMD) system prototype [30] as a concrete example to demonstrate how the SoftGrid testbed can help such evaluation.

5.1 An A*CMD System Case Study

We first provide a brief overview of the A*CMD system, which is specifically designed for securing remote control interface of substations [30]. At the high-level, an A*CMD system aims to offer an additional layer of security that can mitigate impact of cyber attacks on power grids even when other security measures are circumvented. The A*CMD system must be able to implement non-bypassable mediation of remote control commands and is responsible for inspecting and processing them with minimal coordination with external system components.

As in the reference model of modernized electrical substations [23], each substation has a system component called "Proxy/Gateway" (called gateway hereafter). A gateway is mainly responsible for protocol translation (e.g., from IEC 60870-5-104 to IEC 61850 and vice versa) because a protocol for substation remote control is, in most cases, either IEC 60870-5-104 or DNP3 while the standard for intra-substation communication is IEC 61850. Thus, the gateway needs to

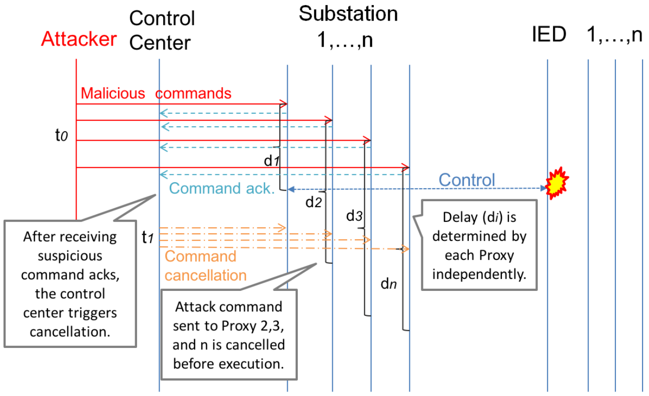

Attacker
Control Center
Substation 1,…,n
IED 1,…,n
Malicious commands
t0
d1
d2
d3
dn
Control
Command ack.
t1
Command cancellation
After receiving suspicious command acks, the control center triggers cancellation.
Attack command sent to Proxy 2,3, and n is cancelled before execution.
Delay (di) is determined by each Proxy independently.

Figure 5: Overview of mitigation by command-delaying. Each substation adds artificial delay ($d_1, \ldots, d_n$) for each control commands. If an attack is detected by Control Center and canceled during the time window (i.e., commands sent to Substation 2, 3, . . . , n), the corresponding malicious commands are never executed, and thereby impact on power grid can be reduced.

mediate all remote control commands, making it an ideal place for deployment of the A*CMD system.

An A*CMD system can host a variety of security mechanisms, such as rule-based/context-based command filtering, and command rescheduling or rewriting. Among them, we here discuss command-delaying as proposed in [30], which has been implemented in our prototype. Under the command-delaying approach, the A*CMD system in each substation independently adds artificial time delays before executing the control center's commands on targeted IEDs. The purpose of the artificial delay is to provide an attack detection system, which is often implemented at the control center, with time buffer to detect attacks and then to cancel any suspected control commands. If the detection and cancellation can happen before the delay expires, they are never executed on IEDs, and thereby the number of malicious commands executed can be reduced. The overview of the scheme and an example message flow are illustrated in Figure 5. The amount of delay that can be added is subject to the grid's operating requirements. According to the guideline provided by IEEE [24], in the typical remote control scenario delay of around 1-2 seconds does not negatively affect normal operations.

As shown in Figure 5, an attack detection and response system in the control center examines command acknowledgments sent from the A*CMD systems via a secure communication channel. Note that, while this specific implementation of A*CMD relies on such a centralized attack detection module, it is also possible to design fully autonomous A*CMD scheme, e.g., a command canceling scheme that uses the local sensor readings to make the decision. This, however, is outside of the scope of this paper.

5.2 Experiment Setup

Our setup is shown in Figure 7. In our experiment, the whole SoftGrid testbed software is installed on a single Windows 7 PC with Intel Core i7-6700 CPU (3.4GHz) and 32GB memory. We use PowerWorld version 19 and the 37-bus system case file [20]. SoftGrid generates one ICD file for each IED in the simulated grid (corresponding to generators, transformers, circuit breakers, shunt reactors, and loads). Each ICD file was around 3KB in size and contained the data variables as well as the control parameters according to the PowerWorld case file. When started, SoftGrid reads all the ICD files and initializes an IED thread for each power system component. Besides the IEDs and PowerWorld, we also installed the control center module on the same PC. As an additional security system at the control center, we implemented a mock Attack Detection & Response System. In our experiment, we consider a situation where all commands sent to substations are malicious, and the detection system simply issues command cancellation after a certain delay (50ms for the experiments in this paper to emulate a relatively simple attack detection algorithm). On the other hand, the artificial delay added by A*CMD at each substation is set to be 400ms, which is applied 70% of randomly selected remote control commands.

The solution to be tested here by using SoftGrid is a substation gateway that implements A*CMD's command-delaying logic. We will call it *A*CMD gateway*. The A*CMD gateway is a Raspberry Pi [9] running on Linux OS, and its protocol translation and A*CMD logic are implemented based on Java (J2SE Embedded) and OpenMUC. We chose Raspberry Pi as our prototyping platform since it has sim-

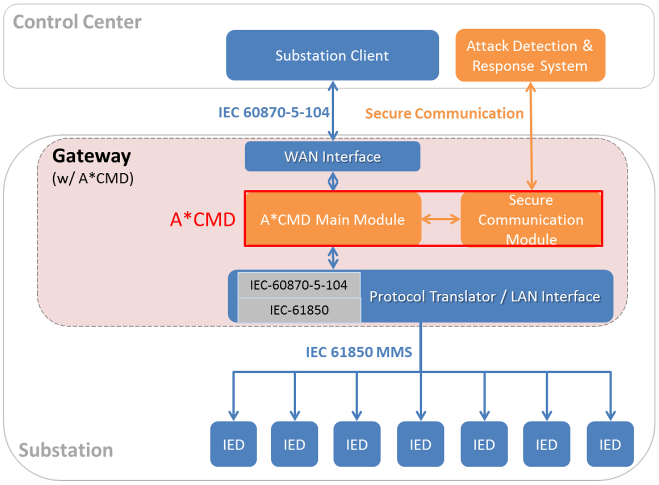


Figure 6: Module architecture of a substation with an active command mediation (A*CMD) system

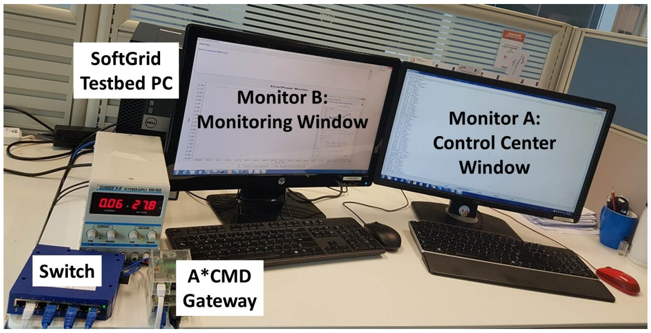

SoftGrid Testbed PC
Monitor B: Monitoring Window
Monitor A: Control Center Window
Switch
A*CMD Gateway

Figure 7: An example setup of a SoftGrid testbed

Table 2: A*CMD performance measurements

Setup	Commands per Second	CPU Usage (%)	Memory Usage (%)
Without A*CMD	33	23.97	13.60
With A*CMD	33	36.70	15.40

ilar hardware spec to some commercial protocol translators (e.g., [4, 15]). As illustrated in Figure 6, the A*CMD gateway includes protocol translation functionality, WAN interface module that supports IEC 60870-5-104 for communicating with the control center, LAN interface module for interaction with IEDs via IEC 61850 MMS, and A*CMD modules. It is connected to the PC via a SPIDER II industry-grade switch [10].

5.3 Testing Interoperability and Performance

This section reports our experience testing the A*CMD gateway's interoperability and performance. Our goal here is not to evaluate the performance of this particular prototype, but rather to demonstrate the usage of SoftGrid.

5.3.1 Interoperability Testing

One of the crucial evaluation criteria especially from the perspective of grid operators is to ensure a security solution works with their existing smart grid infrastructure. As discussed in Section 4, in our testbed, the control center speaks IEC 60870-5-104 while IEDs supports IEC 61850 MMS. Under this setting, the A*CMD gateway under test is expected to at least: (1) send and receive IEC 60870-5-104 messages for communication with the control center, (2) perform correct translation between IEC 60870-5-104 and IEC 61850, (3) routing messages correctly, and (4) send and receive IEC 61850 MMS messages for communication with IEDs.

Through the experiments where the control center sends interrogation commands and control commands, we confirmed that the translated commands are sent to the intended IEDs according to the protocol. The commands are also properly translated and the status of associated power system devices is changed as instructed. In the case of interrogation commands, we also observed that the response message conveying the right information is returned back to the control center. SoftGrid's power simulation and monitoring interface provides an intuitive and end-to-end way to verify the interoperability of the device under test. Furthermore, its tight cyber-physical synchronization allows complicated testing to be conducted.

To conduct such interoperability testing, the testbed (both the control center and IEDs) needs to support protocols to be tested. Hence, supporting other popular protocols, such as DNP3 and Modbus, for broader applicability of SoftGrid is part of our future work.

5.3.2 Performance Testing

To evaluate the performance of the A*CMD gateway, we used SoftGrid to do some stress testing of the prototype. We started by identifying the maximum throughput of commands that it can handle stably. We utilized multiple sending threads in our control center and configured all the threads to send periodic commands. We found the limit of the A*CMD gateway by gradually reducing the inter-transmission interval until the A*CMD gateway begins to have backlog.

As shown in the results in Table 2, the A*CMD gateway we tested can process 33 control commands per second, without showing any system instability issues or increasing trends in CPU and memory usage during an over-night experiment. Such a measurement can be done on SotfGrid by counting the number of responses based on logs generated on the control center. The reported throughput is high enough for typical power grid use cases (see our discussion in Section 4.2). The measurements with a gateway without A*CMD (i.e., the gateway just behaves as a protocol translator) was also shown in the same table. We observed similar throughput regardless of whether the A*CMD functionality is enabled or not. Hence, the bottleneck was posed by other modules, and we identified the protocol translation module consumed most of the resources and processing time.

This experiment shows that SoftGrid can help assess the performance of a security solution and identify potential bottlenecks on the tested device. As shown earlier in Section 4.2, SoftGrid can support more than 500 commands per second, making it possible to conduct such a stress test.

5.4 Evaluating Effectiveness of A*CMD

We used SoftGrid to simulate cyber attacks that abuse remote control interface of electrical substations, so as to evaluate the effectiveness attained by the A*CMD gateway. The goal of our experiments here is not to present comprehensive evaluation results for the A*CMD gateway, but to demonstrate the capability of the SoftGrid testbed.

For this purpose, we considered an attacker that obtained full control of the control center system and has capability to send any remote control commands, as in the case happened in Ukraine [45] To simulate the attack, we continuously sent "open" commands to all circuit breakers in our testbed, while monitoring the *OverloadRank* in the PowerWorld (also called "performance index"). OverloadRank is a numerical value that is calculated based on the ratio of actual power flow against capacity of transmission lines and collectively indicates the status of power flow in the entire grid [17]. This value typically goes up when some transmission lines become overloaded, and it goes down when some lines are opened. Hence, the change of the OverloadRank value indicates instability in the simulated power grid system. We performed experiments with and without the A*CMD feature for the sake of comparison.

The red, dashed line in Figure 8 shows the OverloadRank values during the attack without the support of A*CMD. As can be seen, there is a huge fluctuation of the OverloadRank metric. In comparison, when the A*CMD system is enabled (see the blue, solid line in Figure 8), there is no obvious change in the OverloadRank metric. This shows that A*CMD solution eliminates most of the undesirable events under the simulated attack scenario. Besides OverloadRank metric, our testbed allows detection of violations based on transient stability analysis on PowerWorld. In this specific experiment, we did not observe any violation in terms of frequency, bus voltage, or power flow limits when A*CMD was present. In comparison, when there is no A*CMD system, the frequency fluctuates widely between 59.39Hz and 60.71Hz, which violates the widely-used 0.5Hz threshold. We repeated the attack experiments for 10 times with different random seeds (the randomness was used by the A*CMD system to make their delay decisions) and reported the summary of observed violations in Table 3. As can be seen,

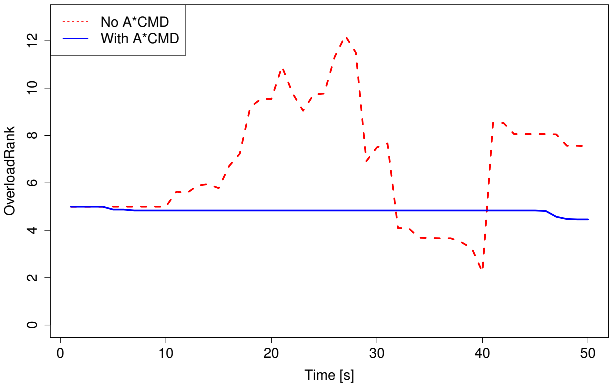


Figure 8: Change in OverloadRank during attack (Created based on data logged by SoftGrid)

Table 3: Effectiveness of the A*CMD solution in reducing violations

Type of Violation	Without A*CMD	With A*CMD
Occurrence of Frequency Violation [times]	10	1
Average # of Buses with Voltage Violation	36.7	1.3
Average # of Overloaded Lines	7.8	0.3

overall we observed significant reduction of violation when A*CMD is in place, which demonstrates its potential as an additional line of defense. Several SoftGrid features, including the tight cyber-physical synchronization and transient stability analysis, are crucial for carrying out such studies, which can provide valuable evidence for estimating a security solution's potential impact on power grid operations.

6. EVALUATING OTHER SECURITY SOLUTIONS AND ATTACKS

In this section, we briefly discuss application of a SoftGrid testbed for evaluating other types of substation cybersecurity solutions, while leaving detailed evaluation and experiments for future work.

6.1 Firewall

A variety of filtering rules might be implemented on a firewall deployed at the perimeter of substations. For instance, firewall might be used to restrict the external host (e.g., a control center) to communicate with. In such a case, we can establish a control center system with a different IP address to see if commands sent by it are blocked. More advanced firewall product may implement deep packet inspection features, which analyze a payload of each packet. To evaluate such configuration, for instance, the control center module can send a message with a function code that is supposed to be blocked. The evaluation would be performed not only before deploying a firewall in the production environment but also before the update of firewall rules.

6.2 Intrusion Detection System (IDS)

We consider a specific IDS solution [28] as a concrete example. The proposed solution deploys an IDS at each individual substation, which sniffs and parses incoming messages and, when they contain control commands, reports them back to a central IDS at the control center. The central IDS that simulates the impact of each control command to determine whether it is a malicious one. Upon detection of a malicious command, the control center will send a new command to reverse the malicious command that has been executed. Such a scheme can be evaluated in a way similar to our A*CMD gateway case study. By operating the control center module, we can send random or targeted attack commands to see whether they are treated as expected. SoftGrid can further conduct evaluation of the whole solution, e.g., what would be the impact of their command-reversing strategy compared to a command-canceling alternative.

SoftGrid can also be used for evaluating other types of IDSes that support IEC60870-5-104 protocol, such as [40]. However, to evaluate the mitigation of physical impacts, a mechanism to respond or resolve the detected attacks must additionally be implemented.

6.3 Rate-limiting

To counter large-scale attacks that abuse the substation remote control interface of substations, one plausible countermeasure that device vendors and grid operators may consider would be to implement rate-limiting (i.e., enforcement of the maximum number of commands that are executed in a certain time unit). Such a simple scheme could be implemented even on top of low-end protocol translators. SoftGrid can be used, in a way similar to the experiment discussed in Section 5.4, to select the appropriate threshold to attain desired level of resilience.

6.4 Sequential Attacks and Countermeasures

Recent research demonstrated that attack commands that are sequentially injected at well-crafted times can cause more significant impact compared to simultaneous attacks [46]. On SoftGrid, a user can script attack commands and timings at which they are sent to substations. Therefore, such a sequential attack can be simulated for evaluating physical impacts. The same paper further discusses a defense mechanism against sequential attacks, which (somehow) prevents critical nodes from removal. Such a defense strategy can be implemented on a gateway, which blocks a certain type of control commands sent to critical nodes, and mitigation gained by the gateway can be also evaluated on SoftGrid.

6.5 Combination of Multiple Solutions

Although we have been discussing individual security solutions so far, it is also possible to apply SoftGrid to evaluate the overall effectiveness of the combination of multiple substation security solutions. For instance, following the defense in depth concept, a grid operator may consider putting together firewalls, IDSes, and the A*CMD systems, which are complementary to each other, to protect its system. All of these solutions can be plugged into the SoftGrid testbed to evaluate how the combined system works.

7. CONCLUSION

Modern electrical substations expose significant cybersecurity risk through their remote control interfaces. While different security solutions have been proposed to mitigate such risk, it remains highly challenging to bring these solutions closer to real-world adoption. In this paper, we proposed SoftGrid, a software-based smart grid testbed that can enable easy and high-fidelity evaluation of substation cybersecurity solutions. By supporting standard smart grid protocols, it allows a real-world device/prototype system to be tested for their interoperability, performance, and effectiveness. SoftGrid supports flexible configuration of different power grid system setups, and can scale to simulate a 2000-bus power grid system on a commodity PC while providing tight cyber-physical synchronization. It also has built-in support for advanced metric logging for monitoring of grid status. We demonstrated the usefulness of SoftGrid through a case study that evaluates an active command mediation (A*CMD) system prototype [30].

Our future work includes multiple directions. First, we plan to add features for distributed setup, such as the use of distributed Java VMs to run IEDs over multiple PCs, and the integration of virtual network technologies such as Mininet [5] or Emulab [43] to emulate complicated network topology. Implementing additional functionality (e.g., standard-compliant system components other than simplified control center and IEDs) can be useful for the evaluation of other types of substation cybersecurity solutions and attack vectors. We also plan to support other smart grid and SCADA protocols, such as DNP3 and Modbus, for broader testbed applicability. Support of other, low-cost power flow simulators, such as ones available on Matlab, is also in our scope. Last but not least, we plan to open-source SoftGrid (excluding third-party products) not only to facilitate security research in related areas but also to receive feedback for further enhancement[1].

Acknowledgment

The work was in part funded under the Energy Innovation Research Programme (EIRP, Award No. NRF2014EWT-EIRP002-040), administrated by the Energy Market Authority (EMA) and in part by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A∗STAR). The EIRP is a competitive grant call initiative driven by the Energy Innovation Programme Office, and funded by the National Research Foundation (NRF).

8. REFERENCES

[1] Facts and figures. http://www.singaporepower.com.sg/irj/servlet/prt/portal/prtroot/docs/guid/106b5b67-d148-2f10-14a7-a6b7bbef1871?sppatab=About%20SP%20PowerAssets. [accessed on 7-Apr-2016].

[2] Iec 60870-5-104 master driver manual. https://www.kepware.com/products/kepserverex/drivers/iec-60870-5-104-master/documents/iec-60870-5-104-master-manual/. [accessed on 25-Jul-2016].

[3] Ieee 118-bus system. http://icseg.iti.illinois.edu/ieee-118-bus-system/. [accessed on 28-Jul-2016].

[4] Kw-61850. http://www.keweitech.com/product_more.asp?id=45. [accessed on 16-Jun-2016].

[5] Mininet. http://mininet.org. [accessed on 28-Jul-2016].

[6] National SCADA test bed: Fact sheet. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf. [accessed on 19-Jul-2016].

[7] OpenMUC. https://www.openmuc.org. [accessed on 7-Apr-2016].

[8] PowerWorld. http://www.powerworld.com/. [accessed on 7-Apr-2016].

[9] Raspberry Pi 1 Model B. https://www.raspberrypi.org/products/model-b/. [accessed on 22-Jun-2016].

[10] SPIDER-Switches. http://www.hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/Unmanaged-Switches/SPIDER-Switches/index.phtml. [accessed on 08-Jul-2016].

[11] Texas 2000-june 2016. http://icseg.iti.illinois.edu/synthetic-power-cases/texas2000-june2016/. [accessed on 28-Jul-2016].

[12] Tofino pre-defined protocols, controllers and applications. https://www.tofinosecurity.com/sites/default/files/AN-113-Tofino-Pre-Defined-Controllers-and-Protocols.pdf.pdf. [accessed on 19-Jul-2016].

[13] Uiuc 150-bus system. http://icseg.iti.illinois.edu/synthetic-power-cases/uiuc-150-bus-system/. [accessed on 28-Jul-2016].

[14] WECC-0100 proposed transient voltage criteria. https://www.wecc.biz/. [accessed on 7-Apr-2016].

[15] Bueno Electric. Iec-60850 gateways. http://www.buenoptic.net/iec-61850-gateways. [accessed on 16-Jun-2016].

[16] F. Cleveland. Iec 62351 security standards for the power system information infrastructure. *IEC TC57 WG15 Security Standards ver*, 14, 2012.

[17] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer. A cyber-physical modeling and assessment framework for power grid infrastructures. *Smart Grid, IEEE Transactions on*, 6(5):2464–2475, 2015.

[18] B. Genge and C. Siaterlis. Developing cyber-physical experimental capabilities for the security analysis of the future smart grid. In *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, pages 1–7. IEEE, 2011.

[19] B. Genge, C. Siaterlis, and M. Hohenadel. Amici: An assessment platform for multi-domain security experimentation on critical infrastructures. In *International Workshop on Critical Information Infrastructures Security*, pages 228–239. Springer, 2012.

[20] J. D. Glover, M. S. Sarma, and T. Overbye. *Power system analysis and design*. China Machine Press, 2004.

[21] J. Hong, S. S. Wu, A. Stefanov, A. Fshosha, C. C. Liu, P. Gladyshev, and M. Govindarasu. An intrusion and defense testbed in a cyber-power system

[1] Further details about SoftGrid are available at https://www.illinois.adsc.com.sg/softgrid/

environment. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–5, July 2011.

[22] IEC TC57. IEC 62351 Parts 1-8 - Information Security for Power System Control Operations. *International Electro technical Commission Std*, 2009.

[23] IEC TC57. IEC 61850-90-2 TR: Communication networks and systems for power utility automation – part 90-2: Using iec 61850 for the communication between substations and control centres. *International Electro technical Commission Std*, 2015.

[24] IEEE Power Engineering Society. IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.

[25] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andren, C. Seitl, F. Kupzog, and T. Strasser. Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations. In *Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on*, pages 1–8. IEEE, 2015.

[26] G. Koutsandria, R. Gentz, M. Jamei, A. Scaglione, S. Peisert, and C. McParland. A real-time testbed environment for cyber-physical security on the power grid. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, pages 67–78. ACM, 2015.

[27] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. K. Iyer. Adapting bro into scada: building a specification-based intrusion detection system for the dnp3 protocol. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, page 5. ACM, 2013.

[28] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer. Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. *Smart Grid, IEEE Transactions on (to appear)*.

[29] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer. Semantic security analysis of scada networks to detect malicious control commands in power grids. In *Proceedings of the first ACM workshop on Smart energy grid security*, pages 29–34. ACM, 2013.

[30] D. Mashima, P. Gunathilaka, and B. Chen. An active command mediation approach for securing remote control interface of substations. In *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*. IEEE, 2016.

[31] P. Maynard, K. McLaughlin, and B. Haberler. Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks. In *Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014*, pages 30–42. BCS, 2014.

[32] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan. An intrusion detection system for iec61850 automated substations. *Power Delivery, IEEE Transactions on*, 25(4):2376–2383, 2010.

[33] R. Schlegel, S. Obermeier, and J. Schneider. Assessing the security of iec 62351. In *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, pages 11–19. British Computer Society, 2015.

[34] C. Siaterlis, B. Genge, and M. Hohenadel. Epic: a testbed for scientifically rigorous cyber-physical security experimentation. *IEEE Transactions on Emerging Topics in Computing*, 1(2):319–330, 2013.

[35] C.-C. Sun, J. Hong, and C.-C. Liu. A co-simulation environment for integrated cyber and power systems. In *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 133–138. IEEE, 2015.

[36] R. Tan, H. H. Nguyen, E. Y. S. Foo, X. Dong, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi. Optimal false data injection attack against automatic generation control in power grids. In *7th International Conference on Cyber-Physical Systems*, 2016.

[37] S. Tan, W.-Z. Song, Q. Dong, and L. Tong. Score: Smart-grid common open research emulator. In *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pages 282–287. IEEE, 2012.

[38] S. Tan, W.-Z. Song, S. Yothment, J. Yang, and L. Tong. Scoreplus: An integrated scalable cyber-physical experiment environment for smart grid. In *Sensing, Communication, and Networking (SECON), 2015 12th Annual IEEE International Conference on*, pages 381–389. IEEE, 2015.

[39] C. Ten, J. Hong, and C. Liu. Anomaly detection for cybersecurity of the substations. *Smart Grid, IEEE Transactions on*, 2(4):865–873, 2011.

[40] R. Udd, M. Asplund, S. Nadjm-Tehrani, M. Kazemtabrizi, and M. Ekstedt. Exploiting bro for intrusion detection in a scada system. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, pages 44–51. ACM, 2016.

[41] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde. Protecting smart grid automation systems against cyberattacks. *Smart Grid, IEEE Transactions on*, 2(4):782–795, 2011.

[42] J. M. Weiss. Control systems cyber security—the need for appropriate regulations to assure the cyber security of the electric grid. In *US Congress Testimony, October*, 2007.

[43] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar. An integrated experimental environment for distributed systems and networks. *ACM SIGOPS Operating Systems Review*, 36(SI):255–270, 2002.

[44] T. A. Youssef, A. T. Elsayed, and O. A. Mohammed. Dds based interoperability framework for smart grid testbed infrastructure. In *Environment and Electrical Engineering (EEEIC), 2015 IEEE 15th International Conference on*, pages 219–224, June 2015.

[45] K. Zetter. Inside the cunning, unprecedented hack of ukraine's power grid. http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [accessed on 7-Apr-2016].

[46] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He. Resilience analysis of power grids under the sequential attack. *Information Forensics and Security, IEEE Transactions on*, 9(12):2340–2354, 2014.