

Article

MITRE ATT&CK Based Evaluation on In-Network Deception Technology for Modernized Electrical Substation Systems

Daisuke Mashima 

Advanced Digital Sciences Center, Singapore 138602, Singapore; daisuke.m@adsc-create.edu.sg

Abstract: In recent years, cyber attacks against critical infrastructure have been increasing and are becoming stealthy and persistent. Attackers or malware may be hiding in the system after penetration to collect system information. They would further make lateral and vertical movement to seek target devices under the radar of existing cybersecurity measures. In order to counter such emerging attack vectors, in-network deception technology is attracting attention. In-network deception technology utilizes an apparently real but dummy (often virtual) devices deployed throughout the infrastructure to capture the attackers' reconnaissance activities. In this paper, we pick one concrete design and implementation of in-network deception technology for IEC 61850 standard compliant smart substation systems in smart grid, named DecIED, and discuss its effectiveness in countering high-profile attacks that were recently witnessed in the real world. The evaluation is conducted based on the MITRE ATT&CK Matrix for industrial control systems, which tabulates phases and tactics of cyberattack against industrial control systems.

Keywords: smart grid; IEC 61850; cybersecurity; deception technology; MITRE ATT&CK Matrix



Citation: Mashima, D. MITRE ATT&CK Based Evaluation on In-Network Deception Technology for Modernized Electrical Substation Systems. *Sustainability* **2022**, *14*, 1256. <https://doi.org/10.3390/su14031256>

Academic Editor: Zubair Baig

Received: 28 December 2021

Accepted: 21 January 2022

Published: 23 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Smart power grid systems, such as the other types of modernized critical infrastructures, are currently attractive target of cyber attacks. Due to the fact that a power grid is arguably the most fundamental infrastructure that supports other critical infrastructures, attackers, including cyber terrorists and state-backed hackers, are motivated to attack the availability and stability of the power grid operation. While the cybersecurity for the critical infrastructure has been attracting efforts from both industry and academia, we have unfortunately witnessed a number of real world incidents in the past decade. Some of the incident almost resulted in a significant disaster (e.g., destruction of nuclear plants), and others actually caused large-scale power outage.

Due to the significance of incidents, a number of cybersecurity solutions have been proposed by academia as well as the industry to protect our critical infrastructure. For instance, in the power grid domain, IEC 62351 standards [1] have been proposed by International Electrotechnical Commission (IEC) to define security specification for communication protocols such as IEC 61850, IEC 60870-5-104, and so forth. Moreover, cybersecurity technologies are proposed for securing modernized power grid systems, starting from intrusion detection systems to remote attestation [2]. However, as illustrated by Tan [2], each technology has advantages and disadvantages, and no single solution is perfect. Thus, it is desired to combine multiple, heterogeneous cybersecurity solutions that are complementary to each other, realizing defense in depth. In order to add additional layers of defense, deception technologies, which utilize “decoy” devices and/or network of them for deceiving attackers, are attracting attention.

Deception technologies can be categorized into two types: honeypot and in-network deception. The former is usually implemented as a realistic system infrastructure or devices that are intentionally exposed to the external network (e.g., the Internet) for luring attackers in the wild to collect threat intelligence. Honeypots are recently proposed and utilized in the

industrial control systems domain, such as [3–8]. While honeypot in enterprise IT domains has a history already, solution for industrial control systems, or more broadly cyber-physical systems, are still in an early stage. More specifically, although success criteria for honeypot systems include “realism” in terms of both cyber and physical characteristics and behavior of the system, it is not trivial and, thus, is not pursued well except for a few examples, including [9,10]. Honeypots, particularly ones for industrial control systems, are typically implemented as the system completely isolated from the real system infrastructure, mainly due to necessity to avoid any negative impact on the real, production system. On the other hand, in-network deception technologies are blended in the real system infrastructure to monitor activities of persistent attackers in the infrastructure while misleading and/or confusing them with fake system topology and status information to mitigate or slow down the attacks. Technology of this sort for smart grid systems is still rare even in the academia, except for DecIED [11] and DefRec [12]. The latter requires deep integration of software-defined networking and, thus, requires major upgrades in the existing smart grid network architecture. On the other hand, the former can be integrated relatively easily by connecting a security appliance to the substation network and make application-level configuration changes on existing devices. Since these technologies are still new, to our knowledge, the effectiveness of them against real-world cybersecurity threats against real-world smart grid systems has not extensively studied yet.

Therefore, in this paper, focusing on one specific in-network deception technology for smart grid systems we have developed, namely DecIED, we discuss the deployment strategies of the in-network deception technology towards its practical integration into a production environment. Then, using a MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) matrix for industrial control systems (ICS) [13], which formulates cyber attack procedures and tactics at each attack phase, we discuss where and how technologies such as DecIED can contribute to mitigating attacks against ICS. We further discuss effectiveness against high-profile cyber incidents in power grid domains, such as Stuxnet [14] and Ukraine incidents [15]. To our knowledge, we are the first to evaluate in-network deception technologies for smart grid systems in terms of MITRE ATT&CK framework; thus, the discussion made in this paper guides the deployment of the in-network deception solutions into real-world smart grid systems to implement defense in depth.

The rest of this manuscript is organized as follows. Section 2 elaborates modernized power grid systems based on IEC 61850 international standards. We then provide a summary of design and implementation of the deception technology for IEC 61850 compliant smart grid systems, called DecIED [11], in Section 3. Discussions on real-world deployment of deception technologies for smart grid systems as well as its effectiveness against high-profile, real-world incidents are made in Section 4. Finally, we conclude the paper in Section 5.

2. IEC 61850 Based Smart Grid Systems

IEC 61850 is the international standard for substation automation and monitoring and is widely adapted by many power grid operators. In this section, because DecIED [11] relies on the characteristics and specification of IEC 61850 standards, we provide an overview of devices that are deployed in the IEC 61850 based smart power grid system. We then discuss communication protocols defined in IEC 61850, namely MMS (Manufacturing Messaging Specification), GOOSE (Generic Object Oriented Substation Event), and SV (Sampled Values).

2.1. ICS (Industrial Control Systems) Devices in Smart Grid

In the smart grid infrastructure, arguably substation is one of the most important components that is responsible for reliably delivering electricity from generator to consumers through control of power grid topology as well as transformation of voltage at stages. Smart grids consist of a large number of such substations. Substations are responsible

for monitoring and control at different layers of power grid systems, such as generation, transmission, and distribution, and a power grid involves a large number of substations. For instance, even in a small country such as Singapore, there are over 10,000 substations, based on recent statistics.

In each substation, to realize timely and efficient management and monitoring, intelligent devices such as PLCs (programmable logic controllers) and IEDs (intelligent electronic devices) are deployed. They exchange measurements and status information with each other by using the computer network in order to implement a various protection functions that are necessary for preventing physical damages and grid instability [16–18].

An IED is located at the boundary of the cyber side and physical side of the smart grid system. While they exchange IEC 61850 messages over computer network, they also interact with physical power grid components in the substation, such as circuit breakers, transformers, and so forth. Communication among IEDs typically has stringent latency requirements [19–21]. Communication models of IEC 61850-compliant IEDs will be elaborated in Section 2.2.

PLCs are also often found in substation systems, and they implement logic for automated control based on power grid measurements and status [22]. PLCs receive power grid measurements reported by IEDs, checks them against its logic and thresholds, and, when necessary, it sends out control commands to the IEDs. Such communication is typically performed by using the IEC 61850 MMS (Manufacturing Messaging Specification) protocol, which will be elaborated in Section 2.2. In this manner, they can implement automated control that involves multiple IEDs. In this paper, we mainly focus on the design and implementation of deception IED devices, while a similar design is applicable for implementing deception PLC devices by internally using open-source implementation such as OpenPLC61850 [23].

2.2. IEC 61850 Communication Models

International Electrotechnical Commission (IEC), which is an standard body working on standardization of power grid technologies, has defined the standardized communication to be used among devices in the substation network for substation automation, namely IEC 61850 [24,25]. As shown in Figure 1, modernized substation systems that are designed with IEC 61850 standards, consists of multiple levels of network. SCADA/HMI (supervisory control and data acquisition/human-machine interface) and substation gateway are responsible for protocol translation between wide-area network and local-area network, general-purpose and engineering workstations, servers (e.g., VPN interfaces), routers, firewalls, and PLCs. Moreover, they are connected to “station bus” (or also called station-level network) while merging units (MUs), which are meters and sensors that collect power grid measurements, such as power flow, voltage, and frequency, and physical power grid devices that are connected to “process bus” (also called process-level network). IEDs are usually connected to both buses to interact with both the cyber and physical side of the smart grid system. Station-bus communication is performed via IEC 61850 MMS (Manufacturing Messaging Specification) protocol while the communication in the process bus utilizes IEC 61850 GOOSE (Generic Object Oriented Substation Event) and SV (Sampled Values) protocols. Communication observed in typical substation systems includes the following.

SCADA/HMI sends remote control commands and interrogation commands (i.e., request for measurements) to IEDs and PLCs using IEC 61850 MMS. While the former is observed only when a human operator takes an action, the latter is usually automated and periodic. PLCs also utilizes MMS protocol for querying measurements and status from IEDs, and if the input from IEDs matches a pre-programmed criteria, it sends out control commands for automated control. The MMS protocol is a unicast communication over TCP/IP, where IED works as the server and SCADA/HMI, PLCs, etc., work as clients. MMS also supports a periodic reporting service, in which IEDs periodically pushes reports to the requester by using the established TCP/IP session.

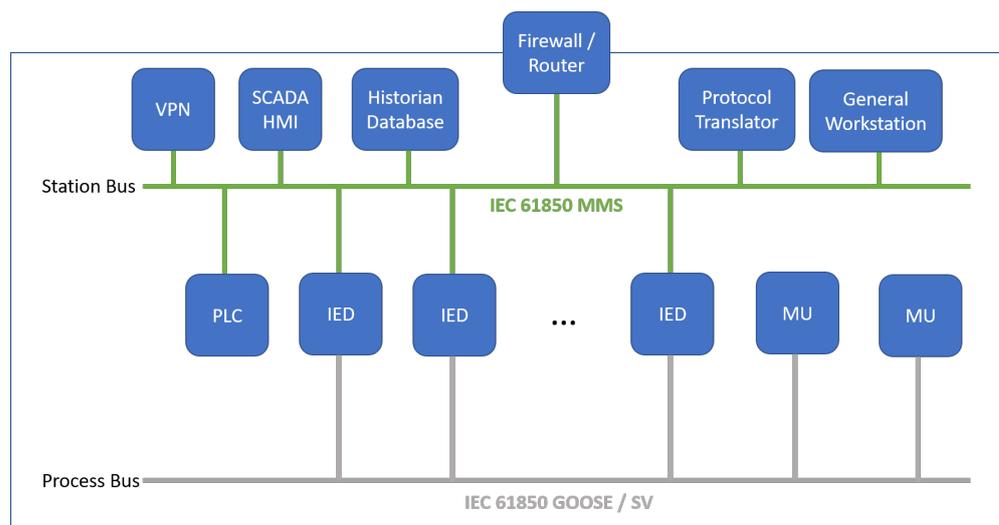


Figure 1. Typical Structure of modernized substation in smart grid.

Process-bus communication is more time critical and requires lower latency (e.g., less than 2 ms for the most critical communication [21]). Thus, IEC 61850 GOOSE and SV protocols used there employ link-layer multicast communication with a publisher–subscriber model [26]. Each IED (and MUs) can play roles as either or both of publisher and subscriber. While the format of payload is very similar, the purposes of GOOSE and SV are different. The GOOSE protocol is utilized for announcing status updates (e.g., open/close status of circuit breaker that the IED is responsible for) with other IEDs. SV protocol, on the other hand, carries digitized analog measurements [27] from the power grid, including voltage, current, etc. Both protocols are the key enablers for protection functions such as over/under-current protection, over/under-voltage protection, and differential protection. We can find another major difference between GOOSE and SV in terms of communication model. SV is always sent with a very high frequency and with fixed interval. For instance, in a 50 Hz power grid system, the specification requires that 4000 SV messages are sent for each data point. On the other hand, GOOSE is sent with a longer interval (hundreds of milliseconds to seconds) if there is no status update event. However, messaging frequency should be increased (up to a few milliseconds interval) to ensure timely delivery of the status change.

2.3. Cybersecurity Incidents against Modernized Power Grid systems

In this section, we briefly discuss the overview of notable cybersecurity incidents in the smart grid domain.

2.3.1. Stuxnet Worm

The first notable incident in power grid sectors is Stuxnet worm that targeted Iranian nuclear power plants in 2010 [14]. Traditionally, the control system, including a SCADA (supervisory control and data acquisition) system or OT (operation technology) system, which is a system for monitoring and controlling physical plants, in industrial control systems is considered secure owing to so-called “air-gap,” which refers to its isolation from the other systems or network. However, Stuxnet worm succeeded in bypassing this air gap by taking advantage of its capability to infect via a USB drive. The USB drive carrying this malware was connected to a workstation in the SCADA infrastructure. Stuxnet targeted an engineering workstation that were used to manage PLCs in the system, which then maliciously re-configured PLCs to manipulate the rotation speed of the centrifuge units of the nuclear power plant. In addition, this sophisticated malware sent apparently normal data to the SCADA HMI (human machine interface) system to hide the situation.

2.3.2. Ukraine Power Plant Attack in 2015

In 2015, power plants in Ukraine was attacked by hackers [15]. This was a very well prepared attack, and it is said that the attack started 6 months before the incident. The attacker first utilized a traditional cyber attack strategy. Phishing emails were sent to the targeted employees of power grid companies, and their computers were infected with a malware called BlackEnergy. The BlackEnergy malware conducted information gathering in the enterprise IT system to find meaningful information, such as the presence and configuration of VPN (virtual private network) interfaces to enable remote access to OT infrastructure as well as login credentials. Then, the attacker utilized such information to penetrate the OT infrastructure, bypassing the air gap in a manner different from Stuxnet. After having footprint in the OT systems, the attacker compromised SCADA control system, which was then remotely manipulated to inject malicious control commands to open a large number of circuit breakers. The attacker also deployed measures to delay the recovery actions. The incident, as a result, caused a massive power outage that lasted for hours.

2.3.3. CrashOverride/Industroyer

Ukrainian power plants were attacked again in 2015. In this incident, a malware called Industroyer or CrashOverride was utilized [28]. One notable capability of the malware is that it alone can send messages compliant to standards used in the modernized power grid systems, such as IEC 61850 and IEC 60870, under the control by an remote attacker via command and control channel. This implies that, once this malware infects any of the devices in the power grid control system, an attacker could inject malicious control commands without compromising the SCADA HMI workstation, as was the case in 2015 incident discussed earlier.

2.3.4. Stealthy, False Data Injection Attacks

While it is not yet witnessed in real-world systems, stealthy attacks to confuse or mislead control systems by means of false, malicious data injection are attracting emerging attention [29–31]. While malicious data injected into the target system may vary depending on target system components (e.g., state estimators and protection relays) as well as the purpose of attackers, the attack vector to be utilized before mounting such attacks would be either remote hacking of any of the devices in the control infrastructure or planting malwares in them. Once these are successfully performed, the compromised devices, either autonomously or under remote control by attackers via command and control channels, start sending fake data to disturb the system.

3. DecIED: Deception Technology for IEC 61850 Based Smart Grid

In-network deception is one type of cybersecurity solution that introduces a number of decoy (virtual) devices that are apparently indistinguishable from real devices in the real system. The aim of the in-network deception technology is to counter attackers or malware that have successfully penetrated into the infrastructure somehow. Specifically, by presenting the fake cyber-physical system view to the attacker, we can make the attackers' reconnaissance activities difficult and less accurate. It is even possible to help us detect active probing by attackers or lateral movements by them. Due to the fact that the in-network deception solution for smart grid systems is almost non-existent, as a proof-of-concept solution to provide in-network deception for IEC 61850 compliant substation systems, *DecIED* has been developed, which pretends to be a real, IEC 61850 compliant IED (also called a *base IED* hereafter for description) [11]. Below, we summarize requirements for deception devices for smart grid systems, and then discuss the system design for realizing these goals.

1. Imitation of device characteristics visible to attackers;
2. Imitation of communication model, patterns, and timings;
3. Sufficient scalability and easy integration into existing infrastructure.

The first property is needing to look indistinguishable from attackers' (including malware) perspective, who may be attempting to find target devices by means of network scanning. The information that an attacker can obtain by active or passive network scanning would include hardware (MAC) addresses, which include the identity of device vendors, open network ports and network services running on the device, and device or OS fingerprints, which are calculated by inspecting protocol stack implementation of OS running on each device. For instance, by using a popular tool such as Nmap [32], these can be made available to the attackers. DecIED addressed this challenge by studying real IED devices deployed in a smart grid security testbed [22] to study such device characteristics. The device fingerprints collected from the real devices are also configured on the deception devices by using an open-source software called Honeyd [4].

Secondly, in the industrial control systems, behaviours of devices, including communication patterns that are visible to attackers, are largely deterministic. For instance, SCADA HMI workstation would be periodically querying measurements and device status from all devices by using IEC 61850 MMS protocol. PLCs are also collecting information of power grid systems in the same manner for the sake of automated control. IEC 61850 GOOSE and SV protocols are utilized for communication among IEDs. Deception devices also implement the same communication patterns. The important thing here is that the deception device should be equally interrogated by SCADA HMI and PLCs and also exchanging power grid measurements and statuses similar to real devices. To achieve this, it is mandatory for deception devices to share (or replicate) the cyber-physical system view of the power grid system to imitate the real device. DecIED addressed this challenge by taking advantage of the IEC 61850 GOOSE and SV messages exchanged on the process bus. Due to the fact that these messages are sent over the link-layer multicast, the messages are received by all devices on the same network, including deception devices at the same time. Moreover, DecIED can be configured with the same internal logic as the real IED (i.e., how the measurements are processed and how the IED reacts to them) to imitate device behaviors.

Last but not the least, because one of the key success criteria for in-network deception is to deploy as many deception devices as possible, scalability is important. For instance, one of the strategies of deception technology is the k -anonymous smoke screen [33], which deploys $k - 1$ deception devices for each real device to lower the probability for an attacker to successfully pinpoint the real device; obviously, larger k implies better security. At the same time, it is also important that the solution can be easily deployed and integrated into the existing infrastructure. Due to the fact that update and upgrade of devices or infrastructure is a universal challenge in the industrial control systems, this property is crucial. In this direction, all DecIED deception devices are run on a single security appliance box (e.g., industrial PC) as light-weight processes, each of which binds a virtual network interface equipped with different network addresses.

The architecture overview of DecIED is illustrated in Figure 2. As demonstrated in [11], the developed DecIED can realize an imitation of device characteristics and observable behaviours such as communication patterns. Moreover, in terms of scalability, we confirmed that more than 200 DecIED instances can stably run on a commodity industrial PC. Discussion on how the deployment of DecIED is possible without negatively affecting the existing, real system infrastructure is also included in the same paper. For a detailed discussion on design, implementation, and evaluation, we refer the interested readers to [11]. The following section discusses how DecIED deployment can help counter or mitigate cybersecurity incidents that were witnessed in recent years.

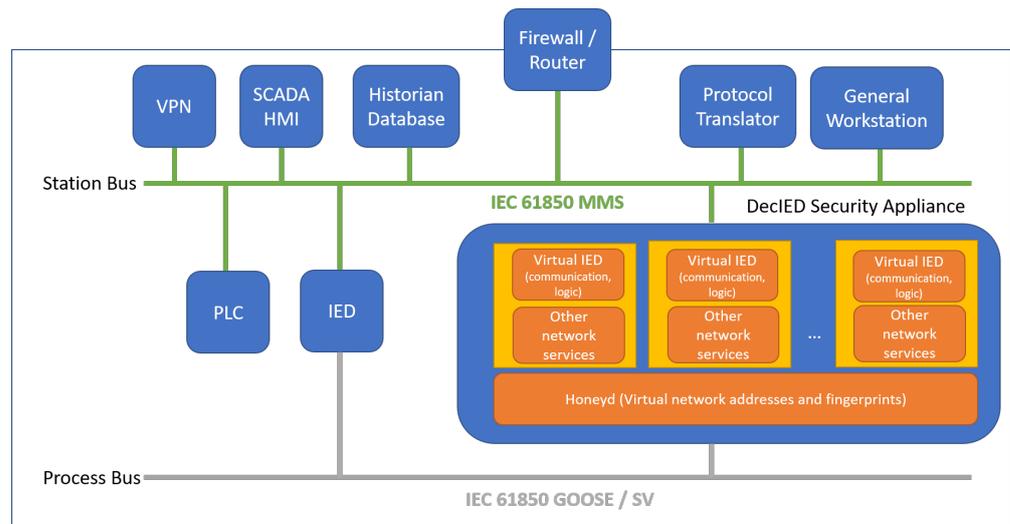


Figure 2. Deployment and module architecture of DecIED [11].

4. Deception Technology for Countering Real-World Threats

DecIED discussed in the previous section enables practical, scalable deployment of deception defense for IEC 61850-compliant smart grid systems. Specifically, the large number of deception/decoy devices that look and behave real IEDs can be implemented without negatively affecting the normal and legitimate operation of real IEDs and other SCADA devices. In this section, we discuss how the DecIED solution can help counter the notable cybersecurity incidents discussed in Section 2.3. We first discuss the positioning of deception technologies on the spectrum of attack tactics, with particular focus on DecIED technology and then discuss combination with other cybersecurity solutions to enhance the effectiveness in a realistic deployment. We then discuss how deception technologies can counter high-profile cyber incidents that targeted smart power grid systems in the recent years.

4.1. Assessment on MITRE ICS ATT&CK Matrix

MITRE systematized a comprehensive knowledge base based on real world cyber incidents and formulated cyber attackers' behaviour over multiple stages/phases. For each stage, a set of tactics taken by attackers was listed. While the original ATT&CK Matrix was for general IT systems, they later published a version for industrial control systems (ICS) [34], which is shown in Figure 3.

We overlaid mitigation provided by DecIED on top of the MITRE ATT&CK Matrix in Figure 3. Blue-colored cells indicate attack tactics mitigated by DecIED. As can be seen in the figure, DecIED can provide mitigation in "Discovery", "Lateral Movement", "Collection", "Command and Control" and "Impair Process Control" stages of the attacks against ICS. For instance, the presence of indistinguishable decoy devices makes it difficult for attackers to pinpoint target devices as well as to learn cyber-physical system topology and plant status by means of active and passive data collection. Lateral movements are also mitigated and even detected by DecIED as soon as an attacker touches any DecIED instances. If an attacker or malware sends any data over the network to well-known ports or application ports that are often utilized by industrial control systems devices, attempting to access or propagate itself, it can be captured by DecIED instances with high probability. Uploading malicious firmware to IEDs can also hit DecIED instances, which is, thus, alarmed likewise. If unauthorized commands are injected, it triggers an alarm as soon as they are received by DecIED instances.

| Initial Access | Execution | Persistence | Privilege Escalation | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|-------------------------------------|---------------------------|------------------------|---------------------------------------|---------------------------|-------------------------------------|---------------------------------|------------------------------------|-------------------------------------|-------------------------------|------------------------------|----------------------------------|
| Drive-by Compromise | Change Operating Mode | Modify Program | Exploitation for Privilege Escalation | Change Operating Mode | Network Connection Enumeration | Default Credentials | Automated Collection | Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Exploit Public-Facing Application | Command-Line Interface | Module Firmware | Hooking | Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | Data from Information Repositories | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Exploitation of Remote Services | Execution through API | Project File Infection | | Indicator Removal on Host | Remote System Discovery | Lateral Tool Transfer | Detect Operating Mode | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| External Remote Services | Graphical User Interface | System Firmware | | Masquerading | Remote System Information Discovery | Program Download | I/O Image | | Block Reporting Message | Spoof Reporting Message | Loss of Availability |
| Internet Accessible Device | Hooking | Valid Accounts | | Rootkit | Wireless Sniffing | Remote Services | Man in the Middle | | Block Serial COM | Unauthorized Command Message | Loss of Control |
| Remote Services | Modify Controller Tasking | | | Spoof Reporting Message | | Valid Accounts | Monitor Process State | | Data Destruction | | Loss of Productivity and Revenue |
| Replication Through Removable Media | Native API | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Protection |
| Rogue Master | Scripting | | | | | | Program Upload | | Device Restart/Shutdown | | Loss of Safety |
| Spearphishing Attachment | User Execution | | | | | | Screen Capture | | Manipulate I/O Image | | Loss of View |
| Supply Chain Compromise | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of Control |
| Transient Cyber Asset | | | | | | | | | Rootkit | | Manipulation of View |
| Wireless Compromise | | | | | | | | | Service Stop | | Theft of Operational Information |
| | | | | | | | | System Firmware | | | |

Figure 3. DecIED on ATT&CK ICS Matrix. Blue color indicates tactics mitigated by DecIED.

4.2. Potential Combination with Other Cybersecurity Measures

As discussed in the previous subsection, in general, deception technologies are mainly intended for misleading or confusing attackers to lower the effectiveness of attack and/or to slow down the progress of attack. However, if it is combined with other cybersecurity measures, the effectiveness and capability of deception technology can be enhanced.

Let us first consider the use with intrusion detection systems (IDS). Intrusion detection systems monitor either or both network and system states to detect indication of cyber attacks. IDSes are categorized into two groups: network-based and host-based. In the context of industrial control systems, because of the resource limitation on devices as well as importance of low-latency processing and availability, network-based IDSes are more popular. Network-based IDSes monitors the protocol used, the number of packets per unit time, the size of messages, and sometimes more advanced features derived from packet payloads [2].

When we consider an attack sending malicious control commands to IEDs, if an attacker has a sense that deception technologies (e.g., nine DecIEDs for each real IED to enable 10-anonymity [11]) are deployed to make it difficult for the attacker to identify the target (real) IED, one possible attack strategy would be to send false control commands to all 10 devices at the same time. An intrusion detection system that monitors the number of packets can easily detect such a traffic pattern and can trigger prevention measures, which can prevent another set of attack commands sent to another real IED. However, one limitation here is that the first malicious command cannot be prevented. In order to overcome such a limitation, we can consider further integrating network traffic aggregation and mediation technologies. For instance, vBump [35] utilizes existing VLAN (virtual local area networks) technology in industrial switches for transparently enforcing mediation by a central server, called vBump server, to implement network traffic policing. Using this technology along with DecIED, we can implement a rule to block traffic of a certain source once a packet from it is destined at any of the deception IED instances. More specifically, with the vBump technology, all attack commands sent to multiple destination IEDs at the same time are intercepted by VLAN-enabled industrial switches and then sent to the

central vBump server. The vBump server then can check whether the destination device is a DecIED instance or not. If this is the case, the vBump server can drop all other packets sent by the same source.

4.3. Security Discussion with Real Incidents

4.3.1. Stuxnet Attack

Stuxnet is one type of worm, which attempts to self-reproduce and propagate in the network while seeking for targets. After penetrating into OT infrastructure, the malware made lateral movements to find targets. While Stuxnet aimed at finding Windows PCs that are running a certain software, such lateral movements are often performed by exhaustively and sequentially accessing active IP addresses found in the network. Therefore, if enough DecIED instances are deployed in the OT network, it is likely that the malware hits any of them before identifying the actual target.

ATT&CK Matrix based on assessment on [13] is shown in Figure 4. From the figure, we can see that DecIED can provide mitigation against its attack tactics on Discovery, Lateral Movement, Collection, Command and Control, and Impair Process Control phases. The only exception is “I/O Image” in the Collection phase, which is specifically about the internals of PLCs and, thus, outside of the scope of DecIED.

| Initial Access | Execution | Persistence | Privilege Escalation | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|-------------------------------------|--------------------------|------------------------|---------------------------------------|---------------------------|-------------------------------------|---------------------------------|------------------------------------|-------------------------------------|-------------------------------|------------------------------|----------------------------------|
| Drive-by Compromise | Change Operating Mode | Modify Program | Exploitation for Privilege Escalation | Change Operating Mode | Network Connection Enumeration | Default Credentials | Automated Collection | Commonly Used | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Exploit Public-Facing Application | Command Line Interface | Module Firmware | Hooking | Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | Data from Information Repositories | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Exploitation of Remote Services | Execution through | Project File Infection | | Indicator Removal on Host | Remote System Discovery | Lateral Tool Transfer | Detect Operating Mode | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| External Remote Services | Graphical User Interface | System Firmware | | Masquerade | Remote System Information Discovery | Program Download | I/O Image | | Block Reporting Message | Spoof Reporting Message | Loss of Availability |
| Internet Accessible Device | Hooking | Valid Accounts | | Rootkit | Wireless Sniffing | Remote Services | Man in the Middle | | Block Serial COM | Unauthorized Control Message | Loss of Control |
| Remote Services | Modify Control Tasks | | | Spoof Reporting Message | | Valid Accounts | Monitor Process | | Data Destruction | | Loss of Productivity and Revenue |
| Replication Through Removable Media | Native | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Protection |
| Rogue Master | Scripting | | | | | | Program Upload | | Device Restart/Shutdown | | Loss of Safety |
| Spearphishing Attachment | User Execution | | | | | | Screen Capture | | Manipulate I/O Image | | Loss of View |
| Supply Chain Compromise | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of Control |
| Transient Cyber Asset | | | | | | | | | Rootkit | | Manipulation of View |
| Wireless Compromise | | | | | | | | | Service Stop | | Theft of Operational Information |
| | | | | | | | | | System Firmware | | |

Figure 4. Mitigation against Stuxnet on ATT&CK ICS Matrix. Blue color indicates tactics mitigated by DecIED. Red symbols indicate attack tactics utilized by Stuxnet.

4.3.2. Ukraine Power Plant Attack in 2015

In this incident, the massive outage was caused by (human) attackers that remotely manipulated a SCADA system to inject a large number of fake commands to open circuit breakers. In this setting, if the SCADA system is configured only with real IEDs in the substation, DecIED solution does not help. Thus, it has to be combined with additional measures so that even an attacker who has control on the SCADA system cannot tell which IEDs are the real ones. In this scenario, DecIED can help trigger other security measures, such as intrusion detection systems, when it receives suspicious commands from the SCADA.

As discussed in [11], such a configuration of SCADA is made possible by only registering both real IEDs and DecIED instances on the SCADA system. In this manner, both real and deception IEDs are interrogated by SCADA in an indistinguishable manner. Since DecIED instances share the status with the real IEDs and, thus, send the same data, it does not affect the integrity of the power system view. The only assumption required here is that a legitimate human operator needs to know which one is the real IED so that it can send a control command to a right target when necessary. If a persistent attacker observes which IEDs the control commands are sent to, it would be possible break the deception. However, we should note that manual control is a very rare event and the majority of SCADA communication is for the periodic exchange of measurements.

4.3.3. Ukraine Power Plant Attack in 2016

The DecIED is considered effective for this sort of attack in multiple directions. First, if a malware, which can infect smart grid control devices such as IEDs, attempts lateral movements or reconnaissance to explore targets, there is a high probability that such attempts steps on DecIED instances, which brings the event into the operator’s attention. Secondly, even if malware is completely passive, when it starts sending malicious control commands to IEDs, it will hit DecIED with high probability. For instance, if we deploy 10 DecIED instances for each real IED, assuming malicious control commands are sent sequentially, the chance that the first attempted command hits the real device is 10%.

Assessment on ATT&CK ICS Matrix is found in Figure 5. As seen in the figure, DecIED can provide mitigation against all attack tactics in Discovery, Lateral Movement, Collection, Command and Control, and Impair Process Control phases.

| Initial Access | Execution | Persistence | Privilege Escalation | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|-------------------------------------|---------------------------|------------------------|---------------------------------------|---------------------------|-------------------------------------|---------------------------------|------------------------------------|-------------------------------------|-------------------------------|------------------------------|----------------------------------|
| Drive-by Compromise | Change Operating Mode | Modify Program | Exploitation for Privilege Escalation | Change Operating Mode | Network Connections Enumeration | Default Credentials | Automated Collection | Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Exploit Public-Facing Application | Command Line Interface | Module Firmware | Hooking | Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | Data from Information Repositories | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Exploitation of Remote Services | Execution through API | Project File Infection | | Indicator Removal on Host | Remote System Discovery | Lateral Tool Transfer | Detect Operating Mode | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| External Remote Services | Graphical User Interface | System Firmware | | Masquerade | Remote System Information Discovery | Program Download | I/O Image | | Block Reporting Message | Spoof Reporting Message | Loss of Availability |
| Internet Accessible Device | Hooking | Valid Accounts | | Rootkit | Wireless Sniffing | Remote Services | Man in the Middle | | Block Serial COM | Unauthorized Control Message | Loss of Control |
| Remote Services | Modify Controller Tasking | | | Spoof Reporting Message | | Valid Accounts | Monitor Processes | | Data Destruction | | Loss of Productivity and Revenue |
| Replication Through Removable Media | Native API | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Protection |
| Rogue Master | Scripting | | | | | | Program Upload | | Device Restart/Shutdown | | Loss of Safety |
| Spearphishing Attachment | User Execution | | | | | | Screen Capture | | Manipulate I/O Image | | Loss of Control |
| Supply Chain Compromise | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of Control |
| Transient Cyber Asset | | | | | | | | | Rootkit | | Manipulation of View |
| Wireless Compromise | | | | | | | | | Service Stop | | Theft of Operational Information |
| | | | | | | | | | System Firmware | | |

Figure 5. Mitigation against CrashOverride on ATT&CK ICS Matrix. Blue color indicates tactics mitigated by DecIED. Red symbols indicate attack tactics utilized by Stuxnet.

4.3.4. Stealthy, False Data Injection Attacks

In general, in-network deception technologies do not directly prevent stealthy false data injection attacks from impacting the control system in the smart grid, since they

are not designed to detect or block any malicious data. However, similarly to the cases discussed in Sections 4.3.2 and 4.3.3, DecIED can detect attackers' or malware's activities in the preparation stage.

5. Conclusions

Deception technologies are promising solutions that can provide an additional layer of security for protecting modernized industrial control systems, including smart power grid systems. On the other hand, such a technology in the industrial control system domain is still in its early stage. Therefore, it is not yet systematically studied where and how in-network deception technologies contribute in order to counter cyber attacks against industrial control systems. In this paper, we elaborated the positioning of in-network deception technologies in terms of the MITRE ATT&CK matrix. We further discussed one concrete implementation of in-network deception technologies for IEC 61850 based smart grid systems, DecIED, as well as deployment strategies based on state-of-the-art technology from academia to qualitatively evaluate the mitigation provided by it. Evaluation based on real-world cyberattack scenarios against smart grid is also provided. Based on our observation, in-network deception technologies, specifically DecIED [11], are considered promising for countering high-profile security incidents that we have witnessed in the past decade. We hope the discussion made in this paper, along with the study on other types of cybersecurity solutions for smart grid [2], will encourage and guide deployment planning of in-network deception solutions to effectively realize defense in depth.

Our future work includes the evaluation of in-network deception technologies against sophisticated/intelligent human attackers, which could utilize a number of heuristics and domain knowledge to identify decoy devices from real ones. Such an evaluation is possible by using it in a blue-team/red-team hacking competition events involving cybersecurity experts (similar to [36]) or to deploy it as part of a honeypot, which is made accessible to real attackers or malware on the Internet.

Funding: This work is supported by the National Research Foundation, Prime Minister's Office, Singapore, under the Energy Programme and administrated by the Energy Market Authority (EP Award No. NRF2017EWT-EP003-047).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Nomenclatures

| | |
|--------------|---|
| GOOSE | Generic Object Oriented Substation Event |
| HMI | Human-machine interface |
| ICS | Industrial control systems |
| IEC | International Electrotechnical Commission |
| IED | Intelligent electronic device |
| MITRE ATT&CK | MITRE Adversarial Tactics, Techniques, and Common Knowledge |
| MMS | Manufacturing Messaging Specification |
| MU | Merging unit |
| OT | Operation technology |
| PLC | Programmable logic controller |
| SCADA | Supervisory control and data acquisition |
| SV | Sampled Values |
| VLAN | Virtual local area network |
| VPN | Virtual private network |

References

1. IEC 62351:2022 SER Series. Available online: <https://webstore.iec.ch/publication/6912> (accessed on 22 December 2021).
2. Tan, H.C.; Cheh, C.; Chen, B.; Mashima, D. Tabulating cybersecurity solutions for substations: Towards pragmatic design and planning. In Proceedings of the 2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), Chengdu, China, 21–24 May 2019; pp. 1018–1023.
3. Pothamsetty, V.; Franz, M. SCADA HoneyNet Project: Building Honey Pots for Industrial Networks. 2005. Available online: <http://scadahoneynet.sourceforge.net/> (accessed on 22 December 2021).
4. Provos, N. Honeyd—a virtual honeypot daemon. In Proceedings of the 10th DFN-CERT Workshop, Hamburg, Germany, 25–26 February 2003; Volume 2, p. 4.
5. Digital Bond. 2016. Available online: <http://www.digitalbond.com/tools/scada-honeynet> (accessed on 30 April 2017).
6. CONPOT ICS/SCADA Honeypot. 2020. Available online: <http://conpot.org> (accessed on 22 December 2021).
7. Buza, D.I.; Juhász, F.; Miru, G.; Félegyházi, M.; Holczer, T. CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot. In *International Workshop on Smart Grid Security*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 181–192.
8. Kołtyś, K.; Gajewski, R. Shape: A honeypot for electric power substation. *J. Telecommun. Inf. Technol.* **2015**, *4*, 37–43.
9. Mashima, D.; Chen, B.; Gunathilaka, P.; Tjiong, E.L. Towards a grid-wide, high-fidelity electrical substation honeypot. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 89–95.
10. Mashima, D.; Kok, D.; Lin, W.; Hazwan, M.; Cheng, A. On Design and Enhancement of Smart Grid Honeypot System for Practical Collection of Threat Intelligence. In Proceedings of the 13th USENIX Workshop on Cyber Security Experimentation and Test, online, 10 August 2020.
11. Yang, D.; Mashima, D.; Lin, W.; Zhou, J. DeclIED: Scalable k-anonymous deception for IEC61850-compliant smart grid systems. In Proceedings of the 6th ACM on Cyber-Physical System Security Workshop, Taipei, Taiwan, 6 October 2020; pp. 54–65.
12. Lin, H.; Zhuang, J.; Hu, Y.C.; Zhou, H. DefRec: Establishing Physical Function Virtualization to Disrupt Reconnaissance of PowerGrids' Cyber-Physical Infrastructures. In Proceedings of the 2020 Network and Distributed System Security Symposium (NDSS), San Diego, USA, 23–26 February 2020.
13. MITRE. Caterogy: Software. Available online: <https://collaborate.mitre.org/attackics/index.php/Category:Software> (accessed on 22 December 2021).
14. What Is Stuxnet? 2020. Available online: <https://www.mcafee.com/enterprise/en-sg/security-awareness/ransomware/what-is-stuxnet.html> (accessed on 22 December 2021).
15. Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. 2016. Available online: <http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> (accessed on 7 June 2017).
16. 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 Electrotechnical Commission Std: Geneva, Switzerland, 2015.
17. Mashima, D.; Gunathilaka, P.; Chen, B. Artificial Command Delaying for Secure Substation Remote Control: Design and Implementation. *IEEE Trans. Smart Grid* **2017**, *10*, 471–482. doi: 10.1109/TSG.2017.2744802. [CrossRef]
18. Roomi, M.M.; Biswas, P.P.; Mashima, D.; Fan, Y.; Chang, E.C. False Data Injection Cyber Range of Modernized Substation System. In Proceedings of the 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Tempe, AZ, USA, 11–13 November 2020; pp. 1–7.
19. Rashid, M.T.A.; Yussof, S.; Yusoff, Y. Trust system architecture for securing GOOSE communication in IEC 61850 substation network. *Int. J. Secur. Appl.* **2016**, *10*, 289–302. [CrossRef]
20. Esiner, E.; Mashima, D.; Chen, B.; Kalbarczyk, Z.; Nicol, D. F-Pro: A fast and flexible provenance-aware message authentication scheme for smart grid. In Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October 2019; pp. 1–7.
21. IEEE Power and Energy Society. *IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation*; IEEE Power and Energy Society: Piscataway, NJ, USA, 2005.
22. Electric Power and Intelligent Control (EPIC) Testbed. 2018. Available online: https://itrust.sutd.edu.sg/wp-content/uploads/sites/3/2019/02/EPIC_technical_details-231018-v1.2.pdf (accessed on 12 February 2019).
23. Roomi, M.M.; Ong, W.S.; Mashima, D.; Hussain, S.S. OpenPLC61850: An IEC 61850 MMS compatible open source PLC for smart grid research. *SoftwareX* **2022**, *17*, 100917. [CrossRef]
24. IEC 61850—Communication Networks and Systems in Substations. Available online: <https://www.gegridssolutions.com/multilin/journals/issues/spring09/iec61850.pdf> (accessed on 22 December 2021).
25. Wester, C.; Adamiak, M.; Vico, J. *Practical Applications of IEC 61850 Protocol in Industrial Facilities*; IAS: Orlando, FL, USA, 2011; pp. 1–2.
26. Mudalige, K.K.; Kariyawasam, S. Implementation of an IEC 61850 Sampled Values Based Line Protection IED with a New Transients-Based Hybrid Protection Algorithm. Available online: <https://mspace.lib.umanitoba.ca/handle/1993/31306> (accessed on 22 December 2021).

27. Konka, J.W.; Arthur, C.M.; Garcia, F.J.; Atkinson, R.C. Traffic generation of IEC 61850 sampled values. In Proceedings of the 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS), Brussels, Belgium, 17 October 2011; pp. 43–48.
28. CrashOverride Malware. Available online: <https://www.us-cert.gov/ncas/alerts/TA17-163A> (accessed on 18 August 2017).
29. Sui, T.; Mo, Y.; Marelli, D.; Sun, X.; Fu, M. The vulnerability of cyber-physical system under stealthy attacks. *IEEE Trans. Autom. Control* **2020**, *66*, 637–650. [[CrossRef](#)]
30. Mo, Y.; Sinopoli, B. On the performance degradation of cyber-physical systems under stealthy integrity attacks. *IEEE Trans. Autom. Control* **2015**, *61*, 2618–2624. [[CrossRef](#)]
31. Sui, T.; Sun, X.M. The vulnerability of distributed state estimator under stealthy attacks. *Automatica* **2021**, *133*, 109869. [[CrossRef](#)]
32. Nmap: The Network Mapper. 2020. Available online: <https://nmap.org/> (accessed on 22 December 2021).
33. Al-Shaer, E.; Wei, J.; Hamlen, K.W.; Wang, C. CONCEAL: A Strategy Composition for Resilient Cyber Deception: Framework, Metrics, and Deployment. In *Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*; Springer International Publishing: Cham, Switzerland, 2019; pp. 101–124. [[CrossRef](#)]
34. MITRE. ATT&CK for Industrial Control Systems. Available online: https://collaborate.mitre.org/attackics/index.php/Main_Page (accessed on 22 December 2021).
35. Tippenhauer, N.O.; Chen, B.; Mashima, D.; Nicol, D.M. vBump: Securing Ethernet-based Industrial Control System Networks with VLAN-based Traffic Aggregation. In Proceedings of the 2th Workshop on CPS&IoT Security and Privacy, Virtual Event, 15 November 2021; pp. 3–14.
36. Adepu, S.; Liyakkathali, B.S.S.B. Performance Analysis of Distributed Attack Detection (DAD) Addendum to the Critical Infrastructure Security Showdown (CISS) 2019 Report. Available online: https://itrust.sutd.edu.sg/wp-content/uploads/sites/3/2020/06/CISS2019-Report-Addendum_final.pdf (accessed on 22 December 2021).