Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies

David E. Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith
Schweitzer Engineering Laboratories, Inc.

Presented at the
Power and Energy Automation Conference
Spokane, Washington
March 21–23, 2017

Previous revised edition released October 2016

Originally presented at the
43rd Annual Western Protective Relay Conference, October 2016

Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies

David E. Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith
Schweitzer Engineering Laboratories, Inc.

***Abstract*—On December 23, 2015, a "temporary malfunction of the power supply" in three provinces in Ukraine resulted in power outages that lasted up to six hours and affected 225,000 customers. Following the event, an investigation identified evidence that several regional Ukraine power control systems had been compromised by cyber attacks. This was the first publicly documented successful cyber attack on an electric utility's control system. Both asset owners and government officials around the world now are asking, "What happened and could a similar cyber attack happen in our control systems?"**

This paper provides an analysis of the Ukraine cyber attack, including how the malicious actors gained access to the control system, what methods the malicious actors used to explore and map the control system, a detailed description of the December 23, 2015 attacks, and methods used by the malicious actors to erase their activities and make remediation more difficult.

We then present a detailed description of securing utility power system control systems based on best practices, including control system network design, whitelisting techniques, monitoring and logging, and personnel education.

The paper concludes with a discussion of mitigation methods and recommendations that would have protected the Ukraine control system and alerted personnel in advance of the cyber attack.

I. Introduction

Starting at 3:30 p.m. on December 23, 2015, the Kyiv, Prykarpattia, and Chernivtsi electric control center HMIs began opening and closing circuit breakers without input from operators. The resulting unauthorized operations resulted in the loss of power to approximately 225,000 customers across Ukraine [1] [2]. Operators at the three operations centers were unable to regain remote control of more than 50 substations affected by the incident. After six hours and the loss of over 130 MW of load, operators restored power by sending technicians to the substations and manually controlling the power system [3] [4] [5].

Complicating the situation and reducing operator communications, the malicious actors also launched a telephony-based denial of service attack, using automated systems to overload the phone systems of the utilities.

Post-power outage analysis found that firmware was corrupted on serial-to-Ethernet converters at substations, uninterruptible power supplies (UPS) for both the server room and the telephony system were remotely turned off, and the hard drives of numerous computers were corrupted.

This event was the first successful cyber-induced power outage that disrupted an electric power grid. To mitigate future attempts at disruption of electrical power by cyber means, it is critical that other electric power organizations learn from the Ukraine incident.

We begin in Section II with a detailed walk-through of the attack. Section III describes a best-known design for a secure control system, and Section IV examines a best-known design in context of the Ukraine incident.

Throughout this paper, we will use several terms translated from Ukrainian. The first is обленерго, "oblenergo," which is a regional power distribution entity. It can be combined with a region, such as Київобленерго "Kyivoblenergo," which is the distribution entity for Kyiv and its surrounding area. An область, or "oblast," is a county or region of Ukraine. The Ivano-Frankivsk Oblast, which was affected in the incident, is also sometimes referred to by its traditional name of Prykarpattia. Prykarpattia and Chernivtsi are in western Ukraine, while Kyiv (the capital) is in central Ukraine, see Fig. 1.

Fig. 1. Regions Affected by the Ukraine Cyber-Induced Power Outage.

II. The Ukraine Cyber Attack

The information presented regarding the Ukraine networks and the attack is from our research and public accounts by the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [5] [6], Electricity Information Sharing and Analysis Center (E-ISAC) [7], and the government of Ukraine [3].

A. Cyber Attack Overview

The Ukraine cyber attack was directed at six oblenergos, but only three were directly affected by power losses: Kyiv, Prykarpattia, and Chernivtsi [1] [2] [5]. The other three oblenergos were successfully intruded upon but did not experience operational impacts [5]. The successful attacks

were focused at the distribution level. Based on the information available, we concluded that the following stages occurred during the attack campaign.

1. An initial email spear phishing attack lures recipients into opening an attached Microsoft® document with a macro that installs Black Energy 3 (BE3) onto corporate workstations.
2. BE3 and other tools perform reconnaissance and enumeration of the network and provide an initial backdoor for the hackers into the corporate network.
3. As a result of network reconnaissance, the malicious actors discover and access the oblenergos' Microsoft Active Directory® servers that contain corporate user accounts and credentials.
4. With the harvested credentials, the malicious actors use an encrypted tunnel from an external network to get inside the oblenergo network, establishing a presence on the oblenergo control system networks.
5. Malicious actors discover and access the control center supervisory control and data acquisition (SCADA) human-machine interface (HMI) servers and substations. While a router separates corporate and SCADA networks, the firewall rules are improperly configured.
6. On December 23, 2015, at 3:30 p.m., the malicious actors begin their power outage attacks by entering operations and SCADA networks through backdoors on the compromised SCADA workstations. The malicious actors take control away from HMI operators and then open breakers.
7. The malicious actors perform several other actions with the intent of complicating the responses of control operators and increasing the effort required to return the system to normal operating conditions. These actions include:
   a. Launching a coordinated Telephony Denial of Service (TDoS) attack that floods call centers to prevent legitimate calls from getting through.
   b. Disabling the UPSs for the control centers.
   c. Corrupting the firmware on a remote terminal unit (RTU) HMI module and serial-to-Ethernet port servers.
8. Malicious actors execute KillDisk malware in an attempt to wipe out the control center HMIs and pivot-point workstations.

B. Detailed Analysis of Attack

Malicious actors gathered data from the Ukraine networks over many months. A thorough review of the activities leading up to the attack and during the attack is useful to understand the complexity of event. The numbers in Fig. 2 correspond to the various stages of the attack as outlined in this section.

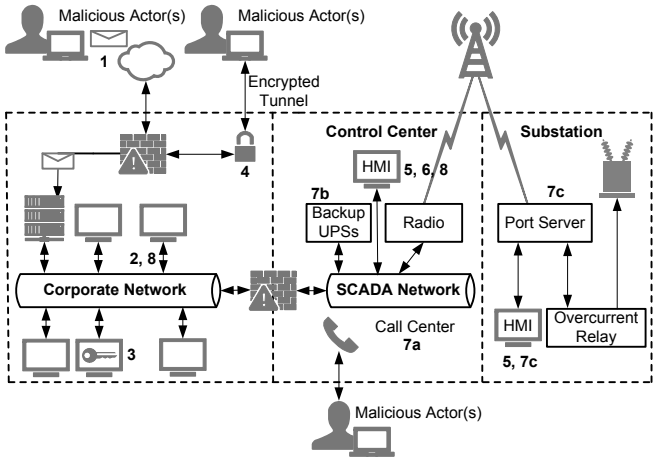

Fig. 2. Extrapolated Model of the Network and Attack.

1) Stage 1: Spear Phishing

In March of 2015, malicious actors used spear phishing to compromise hosts that would allow them access to target networks [4]. The malicious actors targeted individuals in the oblenergos with spear phishing files that appeared to be official correspondence from the Ukrainian Energy Ministry [8]. These emails contained a Microsoft Excel® spreadsheet or a Microsoft Word document [9]. Opening the document and enabling the macros led to the installation of BE3 on that computer. Numerous users were compromised in this way.

2) Stage 2: Malware Used to Explore and Move in Network

Reconnaissance and enumeration of the compromised network occurred over many months, with BE3 and other tools facilitating lateral movement through the computer networks [7]. According to ICS-CERT, BE3 compromised one or more computers at each of the six oblenergos via spear phishing; however, ICS-CERT could not confirm "whether the malware played a role in the actual cyber attacks" [5].

In April of 2015, the malicious actors installed additional backdoor malware on the compromised machines. This malware provided the malicious actors easier access to the compromised computers. Ukrainian Deputy Energy Minister Oleksander Svetelyk stated that there was "evidence that [the malicious actors] started collecting information [about the oblenergo networks] no less than six months before the attack" [10].

3) Stage 3: Credentials Obtained

At the Prykarpattiaoblenergo, the Active Directory server was one of the compromised computers, possibly leading to a brute force attack on the passwords stored there. At the Kyivoblenergo, the malicious actors intercepted passwords using an unknown method. Although BE3 does have a password-stealing plug-in, there was no indication of finding that particular plug-in within the compromised networks [5].

4) Stage 4: Virtual Private Network Tunnel Created

With the compromised credentials, the malicious actors used an encrypted tunnel, which ICS-CERT terms a virtual private network (VPN), to establish a presence on the oblenergo networks. The malicious actors used standard remote access tools to gain access to the control system

network HMIs: Remote Desktop Protocol (RDP), Remote Administrator (Radmin), and Secure Shell (SSH). Malicious actors formed this encrypted tunnel with only user name/password credentials; the oblenergo networks did not require a two-factor authentication [5].

5) Stage 5: Compromise and Reconnaissance of HMI Computers

Access to one of the computers at the oblenergos provided credentials for remote access to the HMI application, which in turn allowed the malicious actors to interact remotely with the control system. Prior to the attack, malicious actors performed reconnaissance on and compromised at least 17 local dispatch center HMIs, which connect to over 50 substations [5].

6) Stage 6: Manipulate Circuit Breakers

The attack on the first oblenergo manipulated an initial circuit breaker at 3:30 p.m. Eastern European Time (EET). The attack on the next oblenergo began one minute later at 3:31 p.m., followed by the attack on the third oblenergo at approximately 4:00 p.m. The operators were able to watch, but not stop, the malicious operators from using their computers and manipulating the HMI. Ukraine operators captured and shared a video of this with ICS-CERT [4].

At 4:10 p.m., the utility operators responded to the outages at one oblenergo by disabling an HMI administrator account. The malicious actors continued shutting down the system using a second HMI administrator account. Later, the utility operators shut down the entire SCADA system and finally the VPN. The total time for the cyber attack was approximately 60 minutes [7]. Eventually, the operators pulled all SCADA systems offline and went to manual mode, which was the only way they could restore power [11]. One oblenergo was able to disable remote access, but only in time to save one substation.

The attack disconnected circuit breakers within minutes of each other, suggesting that multiple malicious actors manually orchestrated the attack. There is no evidence of automatic attacks; the movements of the mouse cursors across HMI screens were like those of a person performing the action [4]. The attack, across at least 17 local dispatch centers, took place in a very short time frame, and at least some aspects of the attack would have required a team of malicious actors.

ICS-CERT concluded that "The cyber attack was reportedly synchronized and coordinated, probably following extensive reconnaissance of the victim networks" [5].

7) Stage 7: Additional Attack Actions

a) Telephony Denial of Service

The malicious actors launched a TDoS attack to disrupt operations and restoration in the Prykarpattiaoblenergo and the Kyivoblenergo. The call centers were overwhelmed with bogus automated calls from foreign phone numbers. The Kyivoblenergo documented them as a technical failure occurring in the call center [7]. Later, the Kyivoblenergo publicly stated that the TDoS attack affected its ability to respond quickly because it did not have situational awareness without the HMI running and was unable to receive calls about where outages had occurred [4].

b) UPS Remote Access and Shutdown

Shortly before 3:30 p.m., the malicious actors used the UPS remote management interfaces to schedule a shutdown of the UPSs for the computer servers in the Kyivoblenergo for later in the afternoon [4] [5]. At Prykarpattiaoblenergo, the UPS for the private branch exchange (PBX) was also shut down in the same manner [4]. This was likely done to interfere with incident response and restoration efforts [5].

c) Malicious Firmware Update

The malicious actors rendered an unknown number of substation serial-to-Ethernet devices inoperable by corrupting their firmware [7]. The manufacturer was unable to fix the devices that had the compromised firmware [6].

8) Stage 8: Execute KillDisk on Target Computers

All three oblenergos claimed that the actors wiped some systems using the KillDisk malware at the conclusion of the cyber attack. KillDisk erases selected files on target systems and corrupts the master boot record, which renders the systems inoperable [5].

ICS-CERT also verified that in at least one instance, a daughter board in an RTU, running Windows Embedded Compact (CE) to drive a local HMI, was overwritten by the KillDisk malware. The RTU manufacturer was unable to restore or fix the RTU [7].

III. Creating a Robust Control System Architecture

To create a robust control system architecture with a solid defense, an organization should consider three concepts.

- Identify risk and develop a plan for managing that risk.
- Implement effective controls to manage the risk.
- Create a defense-in-depth model that allows effective and efficient security controls.

A. Risk Assessment and Management

Risk assessment and management allows organizations to identify, measure, and control organizational risk. These two facets ensure security controls are implemented in balance with the organization's operations. The oblenergos did not sufficiently perform these functions before the cyber incident.

Risk assessment is a function to identify vulnerabilities and threats, understand their impact, and determine which controls will best mitigate those threats. Risk assessment has the following objectives:

- Identify assets and their value
- Identify vulnerabilities and threats
- Calculate threat probability and business impact
- Balance threat impact with security control cost

An asset can be tangible or intangible. Tangible assets include equipment, software, facilities, systems, and personnel that an organization depends on in order to function and do business. Intangible assets include data, reputation, and intellectual property valuable to the organization.

The oblenergos have many tangible assets to consider and keep track of, from the perimeter firewall gateways all the way down to the control system HMI and RTUs. Intangible

assets for the oblenergos include the network topology and employee credentials. Asset value includes:

- Value of replacement
- Cost to maintain
- Damage in cost if lost
- Penalties or fines if lost

Vulnerability is an absence or weakness of a security control or countermeasure inside the system. Lack of or outdated malware protection on network devices and lack of proper email filters to prevent phishing attacks are examples of vulnerabilities. Vulnerability assessments are part of the overall risk management function and should be conducted on a periodic basis.

A threat is realized when an exploit exists for a vulnerability. An example of a threat occurrence is when the malicious actors deployed malware for infiltration and proliferation on the networks of the oblenergos.

To identify threats, it is often helpful to consider threat agents. Threat agents are typically grouped into the following six categories:

- **Human**: Includes malicious actors, nonmalicious insiders and outsiders, terminated personnel, and terrorists.
- **Technical**: Includes equipment failures, software failures, malware, and incompatible technologies.
- **Physical**: Includes facility entrance issues, badge issues, and video monitoring issues.
- **Environmental**: Includes outside telephone company issues, road traffic issues, nearby construction, and hazardous material spills.
- **Natural**: Includes floods, tornadoes, fires, earthquakes, hurricanes, and lightning strikes.
- **Operational**: Includes process and procedures issues that impact the organization's ability to secure its assets.

Vulnerabilities and threats are combined to determine a likelihood of an event occurrence. An event with high likelihood and high impact would be given the highest priority for mitigation. Quantifying dollar amounts for discrete events and then identifying how often per year such events will occur prioritizes them for implementing security controls for mitigation.

B. Security Controls

In modern power systems, there are a wide range of security controls available to aid the control system defender. NIST provides a structure and grouping for these security controls in [12], which it calls "Security Control Identifiers and Family Names." We have found this to be extremely useful when considering security controls for all control systems, not just electric power. We include a subset of those controls with their NIST group type [13].

1) Isolate Control Systems

Security Control Family: Access Control

BE3 infiltrated the Ukraine enterprise systems through social engineering and other similar methods. If the control system is connected to enterprise or other networks, it is possible that malware like BE3 may affect the control system. Techniques such as creating segmented networks using firewalls and protecting data using communication cryptography are critical to eliminating, or at least limiting, the impact of malware. To minimize network exposure:

- NEVER connect control systems to the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network by monitoring the firewall access control lists carefully and only allowing traffic that is needed for the safe operation of the system.
- If remote access is required, employ secure methods such as VPNs, recognizing that a VPN is only as secure as the connected devices and proxies and two-factor authentication.

A control system should include demarcation points that allow for the system to be isolated at different levels. We discuss a technique for defining and creating these demarcation points in Section C.

2) Baseline, Log, and Continuously Monitor Control Systems

Security Control Family: System and Information Integrity as well as Incident Response

Continuous network monitoring is critical to catch intruders or infections, and an organization should monitor all network segments. Different network segments will show different monitoring results. Sometimes, by combining the data from network segments, we can see problems that are not obvious in a single network segment. It is also necessary to use automated monitoring and log reviews as the amount of data to be processed and considered becomes too large to manually parse [14].

Many different netflow analyzers, intrusion detection systems (IDS), intrusion prevention systems (IPS), and network access control (NAC) applications are available today. While these indicators are somewhat lagging, they provide the system operators with network state awareness, network traffic baselines, the state of network ports, and analysis capabilities. The static nature of traffic in a properly isolated control system network makes monitoring and security awareness of the control system state easier to maintain and analyze than in corporate networks.

Control systems are fixed-function systems. When control systems are in operation, there should be no reason for adding unknown applications or running unknown processes. Whitelist systems block all unknown and undesired applications from executing, including malware.

Baselining is a critical part of monitoring; how do we know what is wrong, unless we have a baseline to tell us what is right? Baselines should include as many data points from as many different devices (network devices, sensors, and all controllers) as possible, and should stretch over enough time to determine regular/normal patterns. Automated baselining and polling for settings and firmware changes in many devices can be accomplished using a programmable logic controller (PLC).

Alarms are the most direct and immediate way that a control system has to interact with the human operators. Alarms should be preprogrammed to trigger whenever the normal operation of the control system deviates beyond preprogrammed and acceptable bounds. Alarms can be set for a range of triggers, including breaker action, password changes, and other critical events.

Logs are a valuable tool for alerting and coordinating incident response as well as determining what happened after something goes wrong. After we deal with the immediate problem, it is critical to figure out how the problem occurred and prevent it from happening again. The same applies for a cyber attack. Properly configured logs will help us to discover how far into the network the attacker got, what they modified, and how they gained access in the first place.

3) Patch, Update, and Maintain

Security Control Family: Maintenance and Configuration Management

New threats emerge every day. Creating processes that ensure control systems are up to date is critical to maintaining a secure system. Processes include monitoring news, blogs, mailing lists, and other sources. Additionally, NERC requires that patches be evaluated at least once every 35 days [15]; we suggest setting a monthly schedule to perform patches and updates. When updating firmware or software, updates should be performed using digitally signed firmware from the manufacturer.

4) Have Contingency Plans

Security Control Family: Contingency Planning and Incident Response

In the event of a cyber incident or equipment failure, restoring control system functionality quickly is paramount. Have a recovery plan in place that includes device images, control system designs/schematics, and restoration procedures [16]. Practice these plans to ensure an appropriate response.

5) After Action Reports and Lessons Learned

Security Control Family: Risk Assessment and Awareness and Training

If an event occurs on your control system, take the opportunity to analyze why the situation occurred and learn from it. Use available data such as syslogs, event reports, sequence-of-event reports, and other recordings to do a thorough analysis of the event.

6) Ensure Physical Security

Security Control Family: Physical and Environmental Protection

Much of cyber security focuses on electronic penetration from an internal network or the Internet. However, we must also secure physical aspects of the control system. Often, the front port of a device is left with default passwords, and if an intruder can cut through the fence surrounding the control system facility, they can easily electronically access the devices through this unprotected port.

7) Ensure Complex Passwords

Security Control Family: Identification and Authentication and Access Control

Default passwords are set at the factory and allow users to quickly configure systems out-of-the-box. However, to protect their system from attack, users should change the default password to something unique and cryptographically strong as part of the commissioning process.

It is also necessary to ensure that the user-created passwords are sufficiently complex and random. Easy-to-guess or simple passwords can provide easy access into the control system. Frequent password rotation, the process through which passwords are changed periodically, is also a necessary security requirement.

C. Defense-in-Depth Strategy

Not all parts of the control system require the same level or type of security. The NIST 800-53 comprehensive set of security controls provides guidance to determine and develop a defense-in-depth approach with ICS-CERT. This defense-in-depth method has been proposed by the United States Department of Homeland Security [17], Oman, Schweitzer, and Frincke [18], and many other researchers.

We have modified and expanded the defense-in-depth model control system in related work [19] and show a précis of this method in Fig. 3.

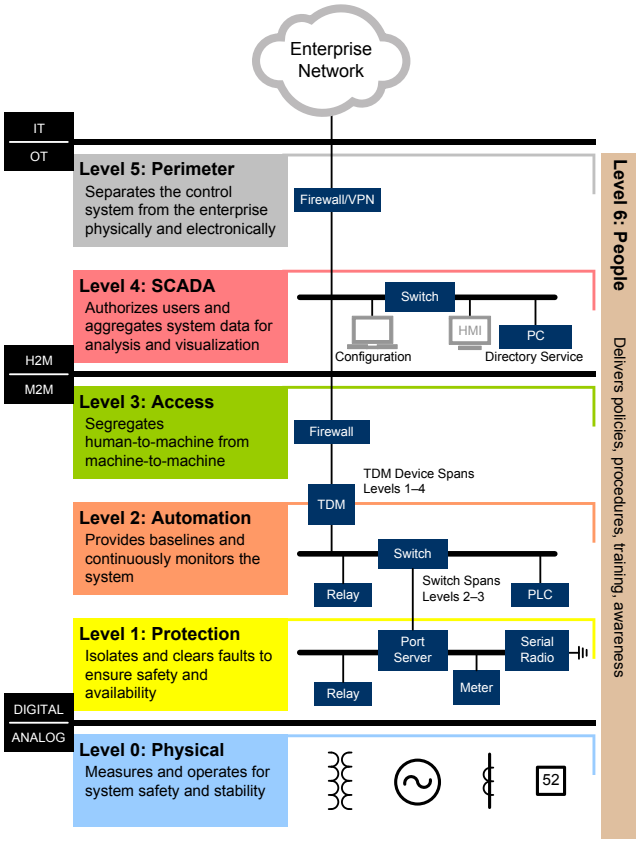

Fig. 3. Defense-In-Depth Model

Many U.S. utilities are adopting a layer-based security model, where each level builds more security into the network to protect critical resources and applications. Security controls

at the appropriate levels allow the user to efficiently monitor, detect, and deter attempts to circumvent the security. Demarcation points define human-to-machine (H2M) interaction with the system (laptop or workstation), application of products in the system (HMI, RTU, relay), and communications protocols (SCADA or protection protocols). Under this security model, users design protection settings in such a way that devices can continue to properly operate if they must be isolated from the network as a mitigation step once an attack has been detected.

1) Level 0: Physical

Level 0 security involves physical controls. To ensure system availability, substation physical security focuses on keeping intruders away through deterrence: obstacles, borders, visible signs, visible cameras, etc. Detective and defensive measures in the form of alerts and alarms provide intrusion detection. Examples include door alarms, occupancy sensors, light sensors, and flashing indicators. Physical locks with badge authentication are becoming a standard in critical U.S. substations. Level 0 security controls are also layered together, providing more information on intruder access and movement.

2) Level 1: Protection

Devices at Level 1 are real-time embedded systems, configured for specific safety, control, and actuation of Level 0 equipment such as valves, sensors, or breakers. Level 1 devices have settings and firmware revision configuration baselines. Firmware updates are digitally signed for verification before being installed.

Communications are point-to-point, point-to-multipoint, noninterleaved, or serial in nature. This nonrouted communications helps ensure data integrity and deter data injection, spoofing, or remote eavesdropping. Relay protection equipment information, including settings, should be stored in secure and redundant databases with access limited to power engineers. Isolating Level 1 machine-to-machine (M2M) network and communications channels from human interaction ensures the necessary real-time processing and communications for rapid control of the system.

While access control technology and protocols such as LDAP and RADIUS may make sense in enterprise systems, excluding them from this level in control systems reduces the attack surface and complexity of Level 1 devices. Limiting direct user interaction with equipment at this level and restricting access through dedicated access points reduces system maintenance and monitoring requirements. The extra complexity of LDAP and RADIUS results in a greater likelihood of misconfiguration by the end user and improper implementation by the manufacturer. Proper Authentication, Authorization, Accountability (AAA) and logging can still be achieved without the added complexity. As seen by the Ukraine incident, people are typically the most targeted and compromised asset in an organization. It is not prudent to directly tie 24/7 end-user access to Level 1 devices. Level 1 devices restrict login attempts, capture failed login attempts, and generate alerts.

Internal diagnostics and continual memory scans not only ensure proper operation of Level 1 equipment but also act as whitelist malware protection. Whitelist malware protection is superior to blacklist signature-based antimalware for embedded devices because the devices perform a specific function and nothing more.

3) Level 2: Automation

Communications from higher levels into Level 1 go through Level 2 devices. Level 2 devices filter and process those communications and prevent certain activities, such as denial-of-service attacks, unsigned firmware updates, injected SCADA controls, and unauthorized remote engineering access, from reaching Level 1 devices. Level 2 provides a protocol break between incoming communications and Level 1 equipment.

Continuous monitoring and baselining are a focus of Level 2. Automation equipment (such as a PLC) baselines and monitors changes in control system settings and firmware revision configurations. Level 2 devices collect and aggregate system alarms for the control system via Syslog for analysis.

Level 2 devices create and manage strong passwords that Level 1 devices need in order to perform certain functions such as changing settings or collecting data. Level 2 devices also maintain a quick isolation point should an attack compromise Level 1 equipment.

4) Level 3: Access

Devices at this level separate, restrict, and filter the human-to-machine levels from the machine-to-machine levels. A specific function at this level is to proxy only authenticated access from the approved SCADA devices for those users with access privileges to machines in the lower levels. A stateful firewall at this access level creates a demilitarized zone (DMZ) of Level 4 for the control system.

Level 3 also maintains a quick isolation mechanism for Level 2 if it is compromised. Because Level 2 contains control system logic for higher performance and efficiency in the control system, it is important to be able to quickly isolate it from the control system in the event of an attack.

5) Level 4: SCADA

Level 4 is the level where users will interface directly with the control system when necessary. Level 4 devices handle tasks like user authorization. Control system data analysis and visualization take place at this level. Users should isolate any necessary localized control system HMI to Level 4, along with other required software on general operating system computers. Disallowing general operating system devices from levels below Level 4 reduces complexity and overall attack surface in the system.

Locating Active Directory services for the control system at this level separates and isolates user accounts from the corporate systems. Transient devices, workstations, or laptops necessary for maintenance and engineering access to the control system use the Level 4 network. User access in the Level 4 network forces these devices to have the latest patches and updated malware protection.

Software such as Splunk, depicting security posture and system state, is necessary at this level. Other Electronic Access Control or Monitoring Systems (EACMS) continuously monitor and analyze traffic for intrusions into the control system.

6) Level 5: Perimeter

Level 5 is the access point for the control system or substation. It incorporates wide-area communications equipment along with firewalls into the corporate or business networks. Between control systems (such as substations), Time Division Multiplexing (TDM) communications equipment provides deterministic machine-to-machine communications necessary for effective real-time control on the system. TDM segregates and encrypts traffic, protecting it against spoofing and data injection.

All business-related data necessary for reporting on the control system is on unidirectional protocols and channels via the Level 5 firewalls. VPN access into corporate systems is not allowed to bridge Level 5.

An Operational Technology Software-Defined Network (OTSDN™) enables traffic engineering, whitelisting, and a deny-by-default architecture for the control system network. Besides providing inherent intrusion detection and prevention, OTSDN optimizes fault recovery performance, necessary for control systems.

7) Level 6: People

A culture of security is as vital for a critical infrastructure organization as safety. The policies, procedures, training, security awareness, risk analyses, and other human-based techniques that ensure the security of the system are in this level. Level 6 spans all the other levels due to the impact of things like policies and procedures at all levels of the control system.

IV. Security Evaluation of the Ukraine Incident

One of the main difficulties with analysis of the Ukraine outage is that there are not enough detailed reports (syslog, event reports, IDS reports) that can point to what actually happened in the system from a cyber perspective. Establishing controls to provide overall system baselining, logging, and monitoring for post-event analysis and root-cause determination would provide this insight. Having these tools in place would have allowed investigators to analyze as-built systems versus in-service systems. Investigators could have reviewed system logs to determine when systems began to misoperate. Real-time indicators would have provided operators with performance indicators.

In Ukraine, limiting control to a select few servers and workstation computers would have limited the attack surface and sped up response times. A whitelist antimalware on those dedicated control system Windows workstations or laptops, along with baseline comparison tools, would have prevented BE3 from propagating on Ukraine utility systems and devices. IDS, IPS, and NAC applications should detect some of the BE3 means of propagation as well as the BE3 network calls. Properly configured and maintained firewalls and VPNs would have isolated all but a select few devices in select networks from being pivot points for BE3. Logging settings changes and firmware updates, baselining those modifications, and then continuous monitoring of those baselines would be very effective security measures against BE3 even if the utility did not have the means to set, change, or manage passwords or their credentials in the relays or IEDs.

Table I summarizes the threats that were seen in the Ukraine incident and lists controls that could prevent these types of threats from being successful in the future.

TABLE I
SECURITY CONTROLS TO PREVENT THREATS LIKE THE UKRAINE INCIDENT

Stage	Threat	Security Controls
Overall	Lack of asset and system knowledge	Monitoring (intrusion detection systems, netflow analysis, baselines, logging)
1. Initial Access to Enterprise Network	Spear phishing	- Training - Email security controls (remove attachments, automatically scan attachments)
2. Pivot in Enterprise Network	Malware (BE3)	- Antivirus - IDS - Host based firewalls
3. Elevate Privileges	Compromised credentials: - Software keylogger - Brute force	- Ensuring user least privilege - Password rotation - Antivirus - Strong credentials - IDS - Syslogs
4. Maintenance Access	Tunnel access	- Good firewall rules - Multifactor authentication - VPN controls - Monitoring
5. Gain Access to Control System	Remote access to HMI/SCADA	- Network segmentation - Ensure user least privilege
6. Attack	Remote access to breaker/control system	- Strong authentication - Encrypted remote access - Quick isolation - Dedicated or nonpublic communication channels - Incident planning
7. Attack Complication		
a)	Telephony DoS	- Backup communications - Call blocking - Asset knowledge
b)	UPS remote access	- Network segmentation - No interactive remote access - Strong authentication
c)	Malicious firmware update	- Firmware validation (hashing, signatures) - Hardware backups (hot and cold systems) - Recovery procedures
8. Destroy Hard Drives	Malware (KillDisk)	- Automatic data backups - Antivirus

V. Conclusion

Industrial control systems provide many benefits for the automation and remote control of power systems, including situational awareness and automated network configuration. The Ukraine cyber-induced power outage demonstrated that a

determined malicious actor can exploit a control system that is not based on defense-in-depth design principles. The Ukraine power outage was not a result of a single vulnerability. Rather, a handful of small network design and control shortcomings allowed the malicious actors to eventually turn off the power.

In this paper we describe a layered security approach that is appropriate for each type of control system device. Good cyber security includes people, hardware, software, policies, and procedures, regardless of whether we are considering an enterprise network or a control system. The Ukraine cyber incident was an unfortunate event that disrupted thousands of households. A positive outcome of the event is that it has made electrical power companies evaluate their security postures and consider implementing ideas discussed in this paper.

VI. References

[1] Molbuk News Agency, "Chernivtsioblenergo also suffered cyber attacks from Russia," viewed August 21, 2016. Available: http://molbuk.ua/chernovtsy_news/104328-chernivcioblenergo-takozh-zaznalo-kiberataky-z-rosiyi.html.

[2] Prykarpattiaoblenergo Corporate Web Page, "Energy liquidate the consequences of a major accident in the Carpathian region," viewed August 26, 2016. Available: http://www.oe.if.ua/showarticle.php?id=3413.

[3] Ukrainian Ministry of Energy and Coal, "The Work Group to Study the Causes of the Temporary Malfunction of Power Supply Companies, Which Took Place December 23, 2015," January 2016. Available: http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245082298.

[4] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," WIRED, March 2016. Available: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[5] ICS-CERT, "Alert (IR-ALERT-H-16-056-01AP): Cyber-Attack Against Ukrainian Critical Infrastructure," Department of Homeland Security, March 2016. Available: http://www.eenews.net/assets/2016/07/19/document_ew_02.pdf.

[6] ICS-CERT, "Advisory (ICSA-16-152-01): Moxa UC-7408-LX-Plus Firmware Overwrite Vulnerability," Department of Homeland Security, May 2016. Available: https://ics-cert.us-cert.gov/advisories/ICSA-16-152-01.

[7] E-ISAC, SANS, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[8] P. Polityuk, "Exclusive: Hackers May Have Wider Access to Ukrainian Industrial Facilities," Reuters, January 2016. Available: http://www.reuters.com/article/us-ukraine-cybersecurity-exclusive-idUSKCN0V51H1.

[9] V. Kremez, "APT Malware Analysis: BlackEnergy Додаток1 Excel VBA Dropper," viewed August 23, 2016. Available: http://www.vkremez.com/cyber-security/apt-malware-analysis-blackenergy1-excel-vba-dropper.

[10] P. Polityuk, "Ukraine Sees Russian Hand in Cyber Attacks on Power Grid," Reuters, February 2016. Available: http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.

[11] iSIGHT Partners, "Cyber Attacks on the Ukrainian Grid: What You Should Know." Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

[12] National Institute of Standards and Technology. Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Rev. 4, April 2013. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[13] J. Smith, J. Pereyda, D. Gammel, "Cybersecurity Best Practices for Creating Resilient Control Systems," proceedings of the International Symposium on Resilient Control Systems, Philadelphia, PA, 2016.

[14] P. Oman, E. O. Schweitzer, III, and J. Roberts, "Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions," proceedings of the 3rd Annual Western Power Delivery Automation Conference, Spokane, WA, April 2001.

[15] NERC, "Critical Infrastructure Protection, V5," 2015. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[16] E. O. Schweitzer III, D. Whitehead, A. Risley, and R. Smith, "How Would We Know?" proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[17] K. Barnes and B. Johnson, "Introduction to SCADA Protection and Vulnerabilities," Idaho National Engineering and Environmental Laboratory, January 2004. Available: http://www.inl.gov/technical publications/Documents/3310860.pdf.

[18] P. Oman, E. O. Schweitzer, III, and D. Frincke, "Concerns About Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems," proceedings of the 27th Annual Western Protective Relay Conference, Spokane, WA, October 2000.

[19] J. Smith, N. Kipp, D. Gammel, "Defense in Depth Security for Industrial Control Systems," Proceedings of the Electricity Engineers' Association Conference & Exhibition, Wellington, NZ, 2016.

VII. Biographies

Dave Whitehead joined Schweitzer Engineering Laboratories, Inc. (SEL) in 1994. He is currently the vice president of Research and Development and also oversees SEL's Government Services Division. He is a member of the SEL Board of Directors. Mr. Whitehead received his BSEE from Washington State University and his MSEE from Rensselaer Polytechnic Institute. Mr. Whitehead is a senior member of the IEEE and chairs the Power and Energy Society Substations C6 group that addresses serial cryptographic protocols. Mr. Whitehead currently holds 51 patents worldwide with several others pending and is a registered Professional Engineer in Washington, New York, Michigan, and North Carolina.

Kevin Owens is a graduate of the University of Illinois at Chicago with a BS in Electrical Engineering and has been actively working in the electrical power and control industries since 1994. His career experience includes paralleling switchgear design, network security design, product/software development, and cybersecurity for industrial control systems (ICS). Mr. Owens is presently a senior research engineer at Schweitzer Engineering Laboratories, Inc. (SEL). He has been with SEL since February 2014 and carries with him over 30 years of ICS design and cybersecurity experience.

Dennis Gammel is a graduate of the University of Idaho with a BS in Applied Mathematics and has been actively working in the computing and communications industries since 1996. His career experience includes network security design, CS network architecture, embedded product development, ASIC simulation, and firmware design with RTOS application development. Mr. Gammel is presently a research and development director at Schweitzer Engineering Laboratories, Inc. (SEL), responsible for security technology designed for and implemented in SEL product lines. He has been with SEL since March 2005 and carries with him over 20 years of secure firmware and network engineering experience.

Jess Smith is a Research Engineer with Schweitzer Engineering Laboratories with a PhD in Computer Science and a MS in Computer Engineering. She has experience working for both the government and industry in the cyber security realm. In industry, Dr. Smith has focused on both methods for securely integrating control systems with the modern internet as well as leading efforts to better educate electric power control organizations on the security of their control systems. Dr. Smith's research areas include control system security and supply chain security.