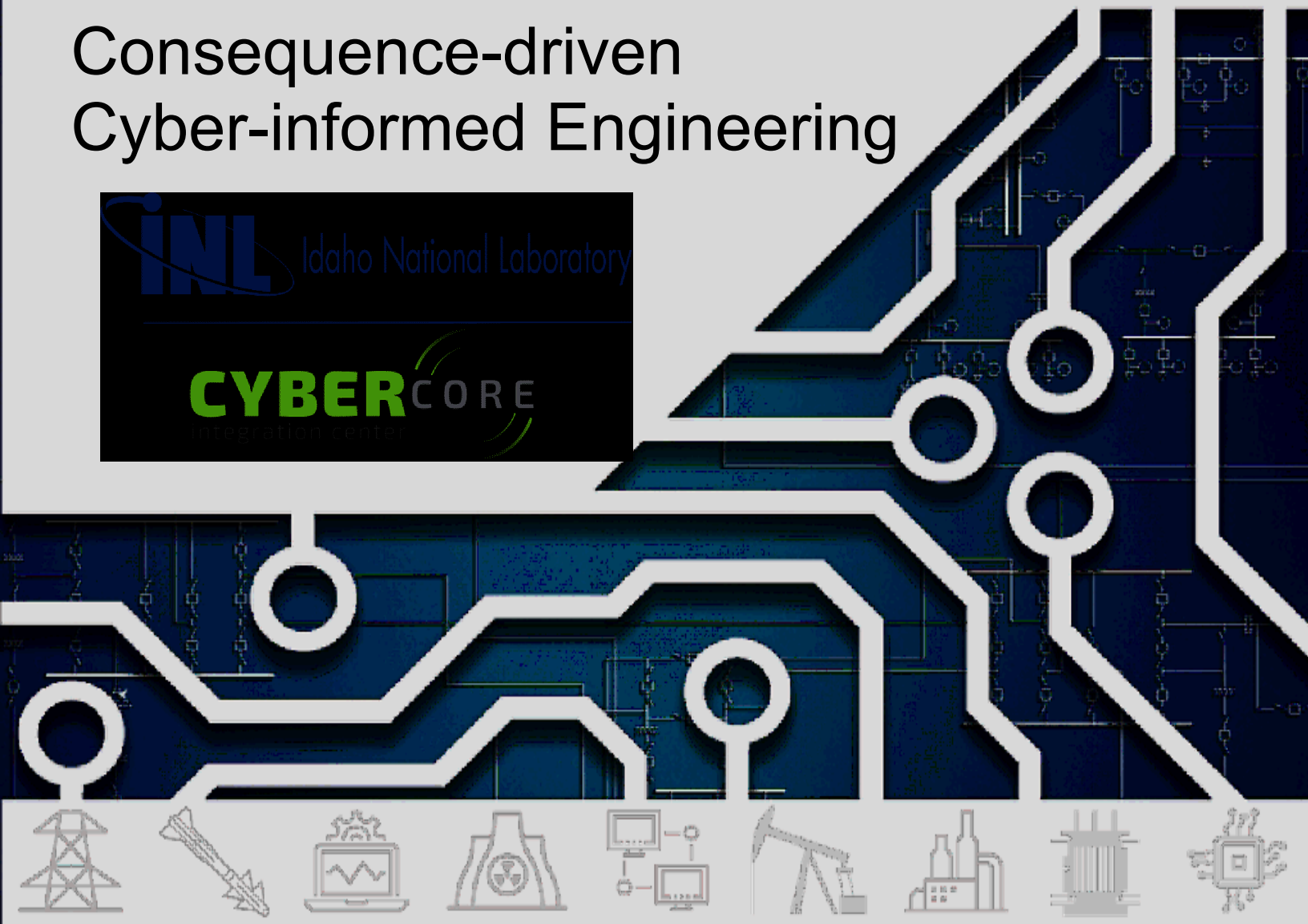
CCE Case Study: Baltavia Substation Power Outage

Consequence-driven Cyber-informed Engineering



Cybercore Integration Center
Idaho National Laboratory

May 12, 2020

INL-EXT-20-58092

Baltavia Substation Power Outage

CCE Case Study

A Cybercore Product

Idaho National Laboratory
Cybercore Integration Center
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of National & Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

Baltavia Substation Power Outage

Introduction

In this case study, we will examine a fictional event broadly inspired by the real power outages in Ukraine that took place in December 2015 and December 2016—both the result of cyber-enabled sabotage. The adversaries in these well-documented attacks gained access to a few power companies' corporate networks, pivoted to industrial control system (ICS) networks, and created widespread physical effects in the form of power outages.

2015 Ukraine Attack, an Introduction

Figure 1 is an infographic that helps summarize the 2015 Ukraine power system cyber-attack.

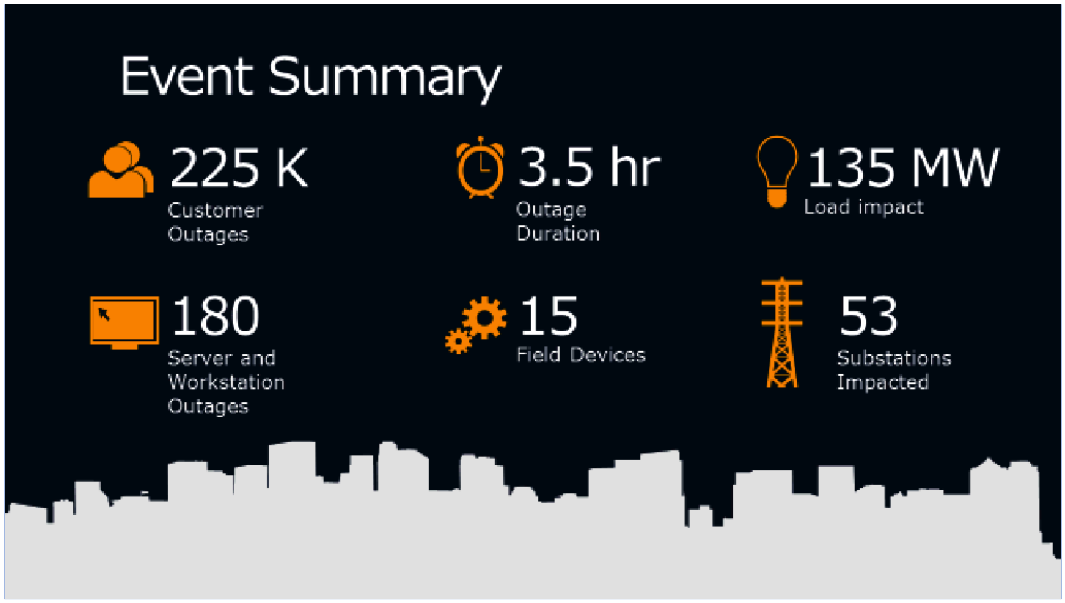


Figure 1. Graphical representation of the 2015 attack on Ukraine's electrical grid.

The December 2015 power outages in Ukraine were the result of a coordinated cyber-attack on three power distribution companies involving roughly 53 substations within their associated service areas. The attack focused on supervisory control and data acquisition (SCADA) and distribution management system (DMS) platforms and leveraged the unverified trust of established remote access capabilities.

The attackers caused outages by using the engineered functionality of the controls platforms to manipulate circuit breakers within the substations. Attackers also prevented an immediate restoration of normal power delivery by targeting core supporting functions of centralized control: field communications (altered firmware uploaded to station Serial-to-Ethernet gateway devices) and operator visibility ("wiping" hard drives of operator workstations and servers). Malicious modifications to uninterruptable power supply (UPS) configurations were also discovered. Attack preparation involved first gaining access to the companies' business networks (via spear phishing), harvesting credentials and escalating privileges, and using the stolen, trusted ICS accounts for remote VPN access to the power system networks.

Although many customers were affected by the outage, the utilities' field personnel were able to perform manual system operations; consequently, they restored power to customers in a relatively short amount of time—less than 4 hours.

2016 Ukraine Attack, an Introduction

Now we will look at the 2016 Ukraine power system cyber-attack. Fewer details related to this event have been made public. Figure 2 is an infographic that summarizes what we do know about the Ukraine power system cyber-attack.

Figure 2. Graphical representation of the 2016 attack on Ukraine's electrical grid.

The December 2016 events in Ukraine were quite different from those in the previous year. For example, the 2016 attack impacted a single transmission-level substation and 200 MW of customer load.

A switch to manual operations again aided the quick recovery of power delivery functions at the affected substation. While the total customer demand loss was greater than it was in the 2015 incident, the 2016 event was of shorter duration (just 1.25 hours) and fewer individual customers experienced a power outage.

Investigation by private cybersecurity firms following this outage uncovered malware capable of mapping networks and executing commands within an ICS environment. While the 2015 attack relied on direct interaction with a SCADA/DMS platform via a remote operator, the malware discovered following the 2016 attack was designed to automatically enumerate on-network ICS devices using specific ICS communications protocols. The malware also contained capabilities to issue commands to those devices.

Note the increased risk presented to asset owners/operators—instead of having to maintain covert

access, the adversary is only required to get the malware to the right network "by hook or by crook" and provide a trigger for execution. In addition, this approach also potentially shortens the amount of time needed for an adversary to position itself for an attack. The approach is also modular (configurable and transferable) to other organizations leveraging similar communications protocols.

The Fictional Attack, an Introduction

With the 2015 and 2016 attacks in mind, we will now explore how to apply the CCE methodology to identify worst-case functional impacts and determine High Consequence Events (HCEs) in a fictional case study.

DISCLAIMER #1

This case study is a work of fiction. It is the product of the authors' imaginations, written to reinforce the understanding of the CCE methodology. Names, locations, events, corporations, regions, countries, and incidents are fictitious. Any resemblance to actual countries or events is purely coincidental.

DISCLAIMER #2

Any references to specific equipment, vendors, or technologies in this study does not imply increased susceptibility to cyber-attack over other brands or devices. The equipment in this study is "typical" equipment often found in the industry. As a work of fiction, some features were modified to support the narrative.

It is January 2017, and Baltavia's transmission[1] utilities seek to better prepare themselves in the face of threats posed by adversaries. Despite the operational risks presented by a rapidly aging coal-fired generation fleet, Baltavia is working to establish itself as a net power provider (see Figure 3 below) to European markets.

[1] See Appendix A for a glossary of key electric sector terminology.

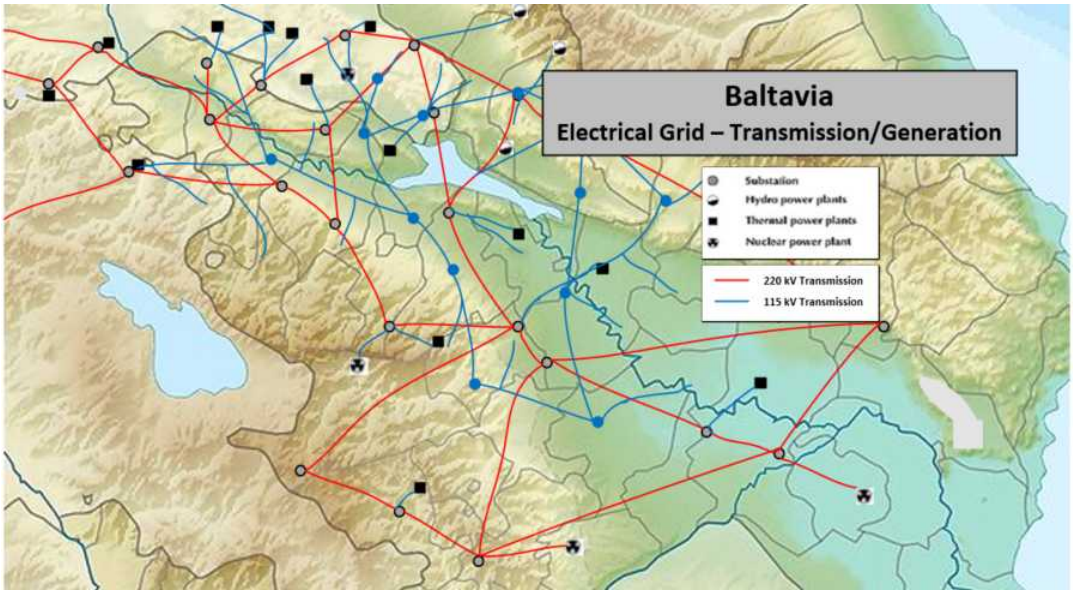


Figure 3: Asset systems in the Baltavian electrical power grid.

Capital projects are approved for transmission substation upgrades with a focus on reliability and modernization. A portion of the preparation involves upgrading transmission substations with new direct current (dc) power management systems that will automate battery health monitoring and emergency ac/dc power[2] transfer. Additionally, this will improve remote control and monitoring capabilities.

Foreign adversaries are concerned with Baltavia's ambitions to be viewed as a reliable net power provider. They wish to deny any opportunity for the country to discuss potential sales of electricity to European markets. Utilities and the Baltavian government fear that a cyber-enabled outage would be a roadblock to their business goal of selling electricity to western Europe, if not ruin the prospect altogether.

Baltavia's ability to deliver energy to Western markets relies on infrastructure connectivity (transmission and distribution) and power generation capabilities. Figure 4 provides a snapshot of Baltavian power system assets, their geographic dispersion internally, and their proximity or interface with neighboring countries.

[2] "alternating current." See Appendix A for a glossary of key electric sector terminology.

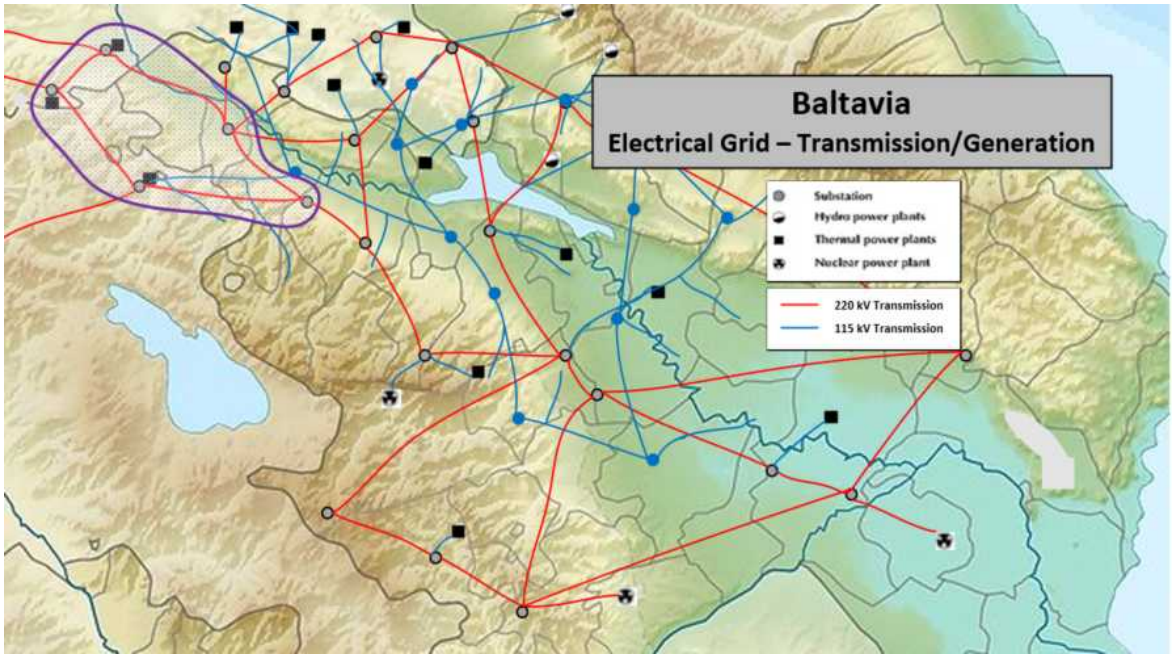


Figure 4: Asset systems in the western Baltavian electrical transmission grid.

Electrical power generation and local demand are met via the generation and distribution systems, respectively. The critical function of power delivery to the Eurozone market relies on the Baltavian transmission system.

The five substations that comprise the western portion of the transmission system are arranged roughly in a ring structure to provide redundant pathways for power delivery (see Figure 5). The ring structure ensures that if a single substation is taken completely out of service by a disruption, the remaining substations on the loop will still be able to provide connectivity.

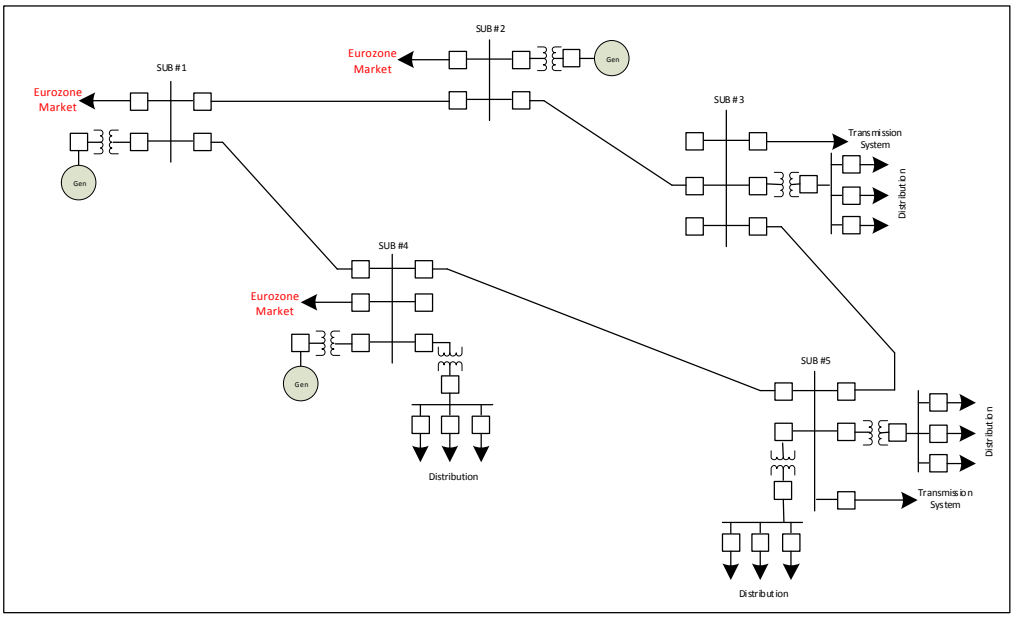


Figure 5. Bus one-line diagram of asset systems in the western Baltavian electrical transmission grid.

While power delivery to the Eurozone market is still possible with an outage at a single key delivery point, both throughput and system resilience capabilities would be negatively impacted if the outage lasted more than 6 hours. More importantly, such an event (especially a malicious cyber-enabled event) would erode European Union (EU) confidence in Baltavia's ability to reliably supply power. This would damage the EU's perception of energy security in Baltavia. Compromise of a critical control or operational component in the transmission system would also lead the utility to question their own ability to restore and maintain system integrity.

Each critical substation shares similar general topology. Dual transmission feeds provide the connectivity to the greater loop, and a third line provides connectivity to the target European market systems. Transmission voltage at each is established at 220kV. The bus structure of each substation is shown in Figure 6. As mentioned earlier, each of the substations also provides some generation capacity to offset internal (Baltavian) and external power demands.

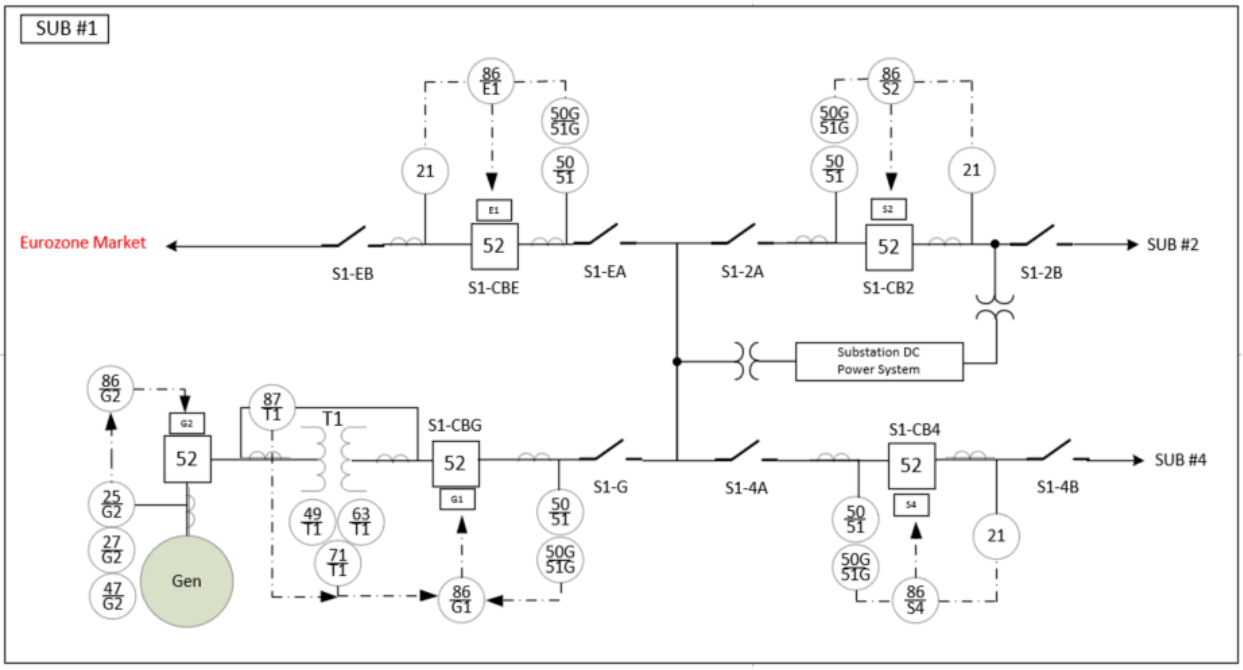


Figure 6: Substation #1 bus/breaker schematic, illustrating the bus structure of each substation.

The three critical transmission substations with connectivity to the EU Market have been equipped with a new auxiliary dc power system (see Figure 7). The dc system is comprised of a battery management system (controller, ac/dc rectifier electronics, on-board maintenance bypass, and transfer capabilities), dc power distribution infrastructure (breakers, panels, wiring, etc.), a battery bank, and a resistive load bank. The dc system is a redundant system with multiple taps used to provide power to all substation control and protective devices, communications infrastructure, breakers, and switch actuators. If the dc power system is incapacitated (battery failure, controller failure, loss of ac power supply and charging, etc.), the ability to automatically and remotely control and monitor the substation is lost. The battery management system provides control and monitoring of the dc system, a configuration interface, communications capabilities, and battery bank charging functions. Battery health/charge is critical—from a degraded charge state, it can take up to 24 hours to restore batteries to a usable voltage level.

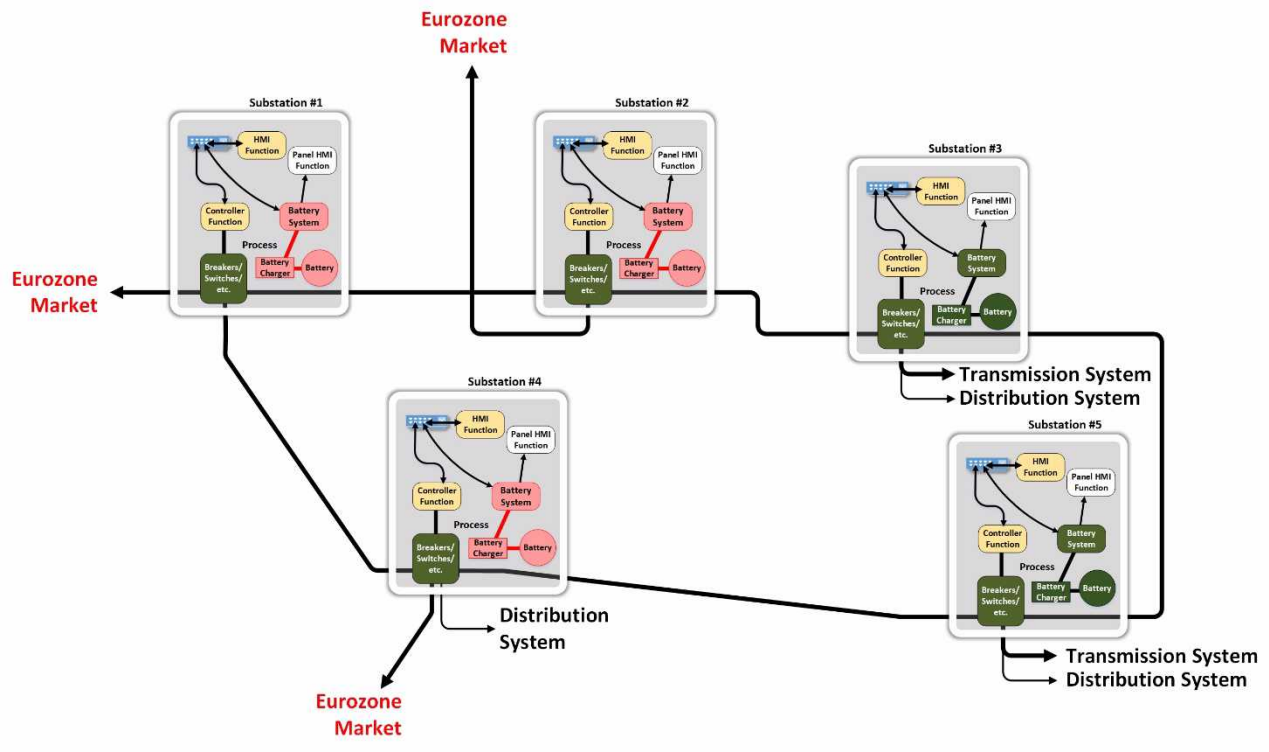


Figure 7. Critical substations with the new auxiliary dc power system and/or SCADA upgrades.

Centralized transmission system operations, as well as generation dispatch, are performed remotely from a control center at the utility headquarters. Transmission operations (control/monitoring of the transmission system infrastructure) are implemented via a commercial-off-the-shelf (COTS) SCADA platform, while generation dispatch uses an automatic generation control (AGC) module within the utility Energy Management System (EMS). Each of the five transmission substations in the western ring have been recently commissioned with full SCADA capabilities via new front-end servers located at the HQ control center. The other transmission substations have active telemetry and metering; however, because necessary upgrades have not been made, they do not have supervisory control capability from the control center.

Communications and control engineering staff have access to the SCADA system network for station device configuration and troubleshooting activities. Although individual substation control and protection devices function independently from the SCADA system, without SCADA operability, automated remote management of stations and the greater transmission system is reduced to manual operations via radio. Because of staffing “cost optimization” measures, there are only enough linemen available to handle manual local response duties at a limited number of substations at any given time. Travel and staging time for a site visit averages 3 hours or more.

Operating procedures are such that if a station’s SCADA system values are suspected of being erroneous, field personnel will be deployed for validation of the subject substation device/system telemetry points. Loss of communications similarly requires dispatch of field crews to verify system integrity. Because of the travel time involved to and from substations and the limited availability of field personnel, the absolute minimum estimate for issue resolution time is 3 hours per site.

Due to present elevated political and economic pressures, an extended outage (6+ hours) at a critical substation would be intolerable. Although a somewhat shorter outage (2 hours or less) could put Eurozone power delivery hopes at risk, such an event may be recoverable through transactions by government officials and utility management.

CCE Steps – Substation Case Study

Phase 1: Consequence Prioritization

Objective:

Functional disruption of Baltavia's full power delivery capabilities to Eurozone markets for 6 hours or more.

Scope:

This transmission system loop was designed for high reliability, but it can only operate at full capacity using all three critical substation "Eurozone market" delivery points. While it is conceivable that three separate transmission substations could be taken down as a result of a simultaneous attack on the utility, an outage at even a single critical substation would negatively impact the power system delivery capability and raise doubts around Baltavian transmission operation reliability.

Boundary Condition:

Functional disruption at a single critical transmission substation, resulting in a reduction of Baltavian full power delivery capabilities to Eurozone markets for 6+ hours.

Events:

1. Transmission-level interconnect breakers are opened at a critical power delivery substation.
2. Transmission-level interconnect breakers at a critical power delivery substation are opened, and the SCADA system at the control center is made inoperable.
3. Loss of local and remote communications capability at a critical power delivery substation.
4. The dc power system capabilities in a critical power delivery substation are degraded, and transmission-level interconnect breakers are opened.

cyber-Events:

1. Open all transmission-level interconnect breakers at a critical delivery substation.
    a. Adversary gains access to the substation network and triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects.
2. Open all transmission-level interconnect breakers at a critical delivery substation, and then disable the HQ control center SCADA capabilities.
    a. Adversary gains access to the substation network and triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects. Adversary then delivers and executes a 'KillDisk'-type program on the primary and backup front-end field communications servers at the control center, rendering SCADA functions inoperable.
3. Disrupt local and remote communications (including SCADA) at a critical substation, prompting the dispatcher to deploy field crews to investigate.
    a. Adversary gains access to the substation network and disrupts communications and SCADA functionality by installing malicious firmware on the substation communications gateway device. Dispatcher follows protocol to "roll" a field crew and manually isolate

communications at the critical substation pending onsite inspection and resolution.

4. Degrade substation station dc power system capabilities in a critical power delivery substation and open all transmission-level interconnect breakers.
    a. Adversary gains access to the substation network and manipulates the configuration of the battery management system. Modifications reduce battery bank recharging capability and dc power availability. The dc system capacity is degraded to a level insufficient for sustained support of substation SCADA, protection, and operations infrastructure. Attack ensures that no indications are presented to system operators while the charging system is at reduced capacity. Adversary triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects.

Scoring:

Here is a list of potential criteria:

- ***Area Impacted (Not Applicable)***: severity determined by the number of substations that are impacted by the event. In this example, the substation serving the critical facility is more important than the others, and any event resulting in a loss of power at this substation will be assigned the highest score.
- ***Attack Breadth***: severity determined by the extent to which a targeted technology or system is deployed. The greater the span of impacted systems, the more difficult it will be to restore following an adverse event. Of note, attack breadth moves beyond the number of devices impacted, since this value also considers the additional resources needed for restoration, such as additional personnel or financial expenditures
- ***Cost (Not Applicable)***: severity determined by direct financial loss to the utility as a result of the failure scenario including restoration costs which is the cost to return the system to proper operation, not including any legal or other reparations as a result of the failure
- ***Duration***: severity determined by length of power outage resulting from event
- ***System Integrity Confidence***: severity determined by the degree to which restoration and recovery efforts can restore system integrity with confidence following the event (i.e., a system not operating as expected or intended, or, alternatively, malicious operation conducted by unauthorized users). One factor to consider is whether the initial attack propagates in multiple systems, and therefore complicates restoration efforts. All of these may negatively impact an organization's confidence in their system following an adverse event.
- ***Safety (Not Applicable)***: severity determined by the potential impact on safety, including injuries requiring first aid or loss of life. For example, the power system outage results in health hazards or mortalities directly tied to the lack of available electric power.

Scoring cyber-Events

	Severity Scoring			
	None (0)	**Low (1)**	**Medium (3)**	**High (5)**
Attack Breadth $\beta = 1$		Elements of the system are vulnerable to an exploit that is active and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.
Duration $\delta = 3$		Return of all service in less than 2 hours.	Return to service in between 2 to 6 hours.	Return to service in greater than or equal to 6 hours.
System Integrity Confidence $\varepsilon = 2$		Asset owner has ability to restore and is confident in restoration integrity.	Asset owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset owner has ability to restore but is not confident of restoration integrity.

Scoring cyber-Event 1

Adversary gains access to the substation network and triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects.

	Severity Scoring			
	None (0)	**Low (1)**	**Medium (3)**	**High (5)**
Attack Breadth β = 1		Elements of the system are vulnerable to an exploit that is active and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.
Duration δ = 3		Return of all service in less than 2 hours.	Return to service in between 2 to 6 hours.	Return to service in greater than or equal to 6 hours.
System Integrity Confidence ε = 2		Asset Owner has ability to restore and is confident in restoration integrity.	Asset Owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset Owner has ability to restore but is not confident of restoration integrity.

Score for cyber-Event 1:

$\beta 1 + \delta 1 + \varepsilon 1 =$

$1 + 3 + 2 = \mathbf{6}$

Scoring cyber-Event 2

Adversary gains access to the substation network and triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects. Adversary then delivers and executes a 'KillDisk'-type program on the primary and backup front-end field communications servers at the control center, rendering SCADA functions inoperable.

	Severity Scoring			
	None (0)	**Low (1)**	**Medium (3)**	**High (5)**
Attack Breadth β = 1		Elements of the system are vulnerable to an exploit that is active and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.
Duration δ = 3		Return of all service in less than 2 hours.	Return to service in between 2 to 6 hours.	Return to service in greater than or equal to 6 hours.
System Integrity Confidence ε = 2		Asset Owner has ability to restore and is confident in restoration integrity.	Asset Owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset Owner has ability to restore but is not confident of restoration integrity.

Score for cyber-Event 2:

$\beta 3 + \delta 3 + \varepsilon 5 =$

$3 + 9 + 10 =$ **22**

Scoring cyber-Event 3

Adversary gains access to the substation network and disrupts communications and SCADA functionality by installing malicious firmware on the substation communications gateway device. Dispatcher follows protocol to "roll" a field crew and manually isolate communications at the critical substation pending on-site inspection and resolution.

	Severity Scoring			
	None (0)	**Low (1)**	**Medium (3)**	**High (5)**
Attack Breadth β = 1		Elements of the system are vulnerable to an exploit that is active and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.
Duration δ = 3		Return of all service in less than 2 hours.	Return to service in between 2 to 6 hours.	Return to service in greater than or equal to 6 hours.
System Integrity Confidence ε = 2		Asset Owner has ability to restore and is confident in restoration integrity.	Asset Owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset Owner has ability to restore but is not confident of restoration integrity.

Score for cyber-Event 3:

$\beta 1 + \delta 3 + \varepsilon 1 =$

$1 + 9 + 2 =$ **12**

Scoring cyber-Event 4

Adversary gains access to the substation network and manipulates configuration of the battery management system. Modifications reduce battery bank re-charging capability as well as dc power availability. The dc system capacity is degraded to a level insufficient for sustained support of substation SCADA, protection, and operations infrastructure. Attack ensures that no indications are presented to system operators while the charging system is at reduced capacity. Adversary triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects.

	Severity Scoring			
	None (0)	**Low (1)**	**Medium (3)**	**High (5)**
Attack Breadth β = 1		Elements of the system are vulnerable to an exploit that is active and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel, etc.) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.
Duration δ = 3		Return of all service in less than 2 hours.	Return to service in between 2 to 6 hours.	Return to service in greater than or equal to 6 hours.
System Integrity Confidence ε = 2		Asset Owner has ability to restore and is confident in restoration integrity.	Asset Owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset Owner has ability to restore but is not confident of restoration integrity.

Score for cyber-Event 4:

$\beta 3 + \delta 5 + \varepsilon 5 =$

$3 + 15 + 10 =$ **28**

HCE Identification

Using these criteria, **cyber-Event 4 scores the highest and will serve as the HCE**.

Phase 2: System-of-Systems Analysis

Creating a Preliminary Block Diagram

The starting point for Phase 2, System-of-Systems Analysis (SoS Analysis), is the creation of a relatively simple, high-level block diagram for each HCE to help with visualizing the cyber manipulation required to accomplish the outcome. This exercise helps narrow the scope of analysis, organizes the physical and functional connections between the target components and the affected systems, and minimizes the volume of information collected to describe each HCE. The block diagram provides a starting point for identifying what information and system accesses the adversary needs to accomplish the HCE and will be used to define and organize the data collection efforts. See Figure 8 for an example HCE block diagram.

High Consequence Event:

Adversary gains access to the substation network and manipulates the configuration of the battery management system. Modifications reduce battery bank recharging capability, as well as dc power availability. The dc system capacity is degraded to a level insufficient for sustained support of substation SCADA, protection, and operations infrastructure. Attacker ensures that no indications are presented to system operators while the charging system is at reduced capacity. Adversary triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects.

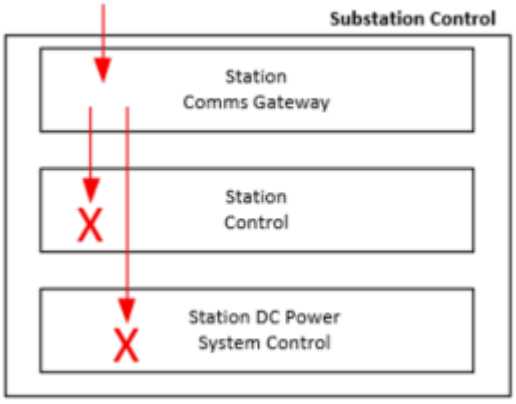


Figure 8. Block diagram of the HCE.

"Perfect knowledge" Benefits

Most of the activity in Phase 2 will involve identifying, collecting, and organizing documentation relevant to an HCE to build a comprehensive knowledge base of key details for the SoS Analysis. The goal is to obtain "perfect knowledge" of the system(s) relevant to the HCE. To help organize the collection and analysis activities, a functional description can be developed based on the HCE block diagram. This is often best done by starting with the target components that must be affected to cause the HCE and working backwards. Consider the following:

- What systems and equipment are involved in the HCE?
- What documentation is needed to describe interconnected systems and dependencies?
- What relationships with other entities are involved?

The functional description can be represented as a hierarchical data structure or taxonomy. Using this functional taxonomy as the basis for investigation, the CCE Team will begin collecting and organizing key details. Relevant information to support this work includes details of interconnected systems and dependencies, controllers, technical manuals, diagrams, protocols, access lists, associated manufacturers, trusted relationships, contractors, suppliers, emergency procedures, and personnel.

The SoS Analysis proceeds in parallel during information collection by building an understanding of the critical systems and processes. The process is iterative, and as the CCE Team identifies specific information gaps from the SoS Analysis, time is taken to adjust the detailed information collection to close these gaps. While not all-inclusive, the resulting information will build upon the initial HCE block diagram and will ideally result in perfect knowledge.

This will benefit the organization by both identifying critical information and determining where it resides. For example, is the critical information on internal servers or a public-facing server? To help ensure continued data collection efforts remain focused on the HCE, it may help to build out the original diagram throughout Phase 2. This helps produce diagrams with greater detail as more data is collected and aggregated. The point of Phase 2 is to be aware of all the information that an adversary would need to execute a successful attack. A typical taxonomy for this use case is shown in Table 1.

Table 1: Substation HCE taxonomy example.

HCE Taxonomy: Substation Case Study
What: By Company Business Function/Equipment/Entity
Function Group Role Info Object
Engineering
Physical System Design
Hardware (Electrical/Mechanical/Process/Civil Engr)
Physical System (Main) Layout Drawings
Single-line diagram(s)
Sub#1 one-line diagram
Sub#1 Switchgear Layout
Sub#1 Battery system one-line diagram
Physical System (Ancillary) Layout Drawings
Station Battery and Battery Monitoring and Control System
Physical System Equipment User Manuals
Station Battery and Battery Monitoring and Control System
Control System Design (Digital & Analog)
Personnel
Power System Design Engineer
Contact Information
Substation Engineer
Contact Information
ICS/SCADA Design Engineer
Contact Information
Relay/Protection Engineer
Contact Information
Software / Firmware
Software (Main) Specs
ABB MultiProg PRO RTU560 Software
ABB RTUtil560 Configuration Application
BMT Battery Management System application (DGK Enterprise)
Automation/Control – Control Center System
System-wide Network Communications Diagram
SCADA comms diagram(s)
SCADA Vendor/Make/Components
SCADA ICS
SCADA I/O Tagname Configuration and List
HMI I/O associated with Sub#1 Device Status and Control
Platform Components – App Server: I/O Server
Make/Model of Computer
Dell Precision 3630 Tower - MSWin
Platform Components – App Server: HMI
Make/Model of Computer
Dell Precision 3630 Tower - MSWin
Program/Config Files
SCADA HMI Sub#1 HMI Layout
Platform Components – App Server: Engineering WorkStation
Make/Model of Computer
Dell Precision 3630 Tower - MSWin
Platform Components - File Server: Utility Engineering File Server
Make/Model of Computer
Dell Precision 3630 Tower - MSWin

Program/Config Applications
BMCS Configuration Software
ABB MultiProg PRO RTU560 Software
ABB RTUtil560 Configuration Application
Utility Documentation
Remote Access Policy and Procedure
Remote Access Security Configuration and Approval
Control System Component Logic Flow Diagrams
Sub#1 SCADA Circuit Breaker Logic Flow Diagram
Platform Components - Substation Engineer Laptop
Make/Model of Computer
Dell Precision 7540 Laptop
Automation/Control - Remote System
Control System Layout Drawings
Sub#1 SCADA system block diagram
Control System Wiring Diagrams (Components)
Sub#1 Bus, Device & Relaying wiring diagrams
Circuit Breaker S1CB-E, S1CB-2 and S1CB-4
Sub#1 CB-E/-1/-2 wiring diagrams
Disconnect Switches: S1-EB, S1-EA, S1-2A, S1-2B, S1-4A, S1-4B, and S1-G
Sub#1 wiring diagrams – each switch component unit
Control System Wiring Diagrams (I/O)
Sub#1 RTU560 wiring diagram
Sub#1 Bus, Device & Relaying schematic diagrams
Sub#1 RTU Rack Module Configuration
Sub#1 RTU I/O wiring diagram
Control System Wiring Diagrams (Comms)
Sub#1 ICS Communications Diagram
Control System Wiring Diagrams (Pwr)
Sub#1 RTU560 Power Wiring Diagram
Control Platform Components (RTU)
Make/Model of RTU
ABB RTU560
Program/Config Applications
ABB MultiProg PRO RTU560 Configuration Application
Program/Config Files
ABB RTU560 and I/O Module System Components
ABB MultiProg PRO RTU560 Configuration Application Sub#1 Config File(s)
ABB MultiProg PRO RTU560 Configuration Application Configuration Software Screenshot
Component User Manuals (including auto / manual capabilities)
ABB RTU560
ABB MultiProg PRO RTU560 Configuration Application
Component Subsystem Specs
ABB RTU560 tech specs
Sub#1 Relay/RTU Platform Config Applications specs
Control Platform Components (BMCS)
Make/Model of BMCS
BMT Battery Monitoring and Control System Product Specs
Program/Config Applications
BMT Battery Monitoring and Control System BMCS Configuration File
Program/Config Files
BMT Battery Monitoring and Control System BMCS Panel Screenshot
Component User Manuals (including auto/manual capabilities)
BMT Battery Monitoring and Control System BMCS Operation and Service Manual
Battery System Equipment Sizing Calcs
Operation and Failure Mode Study

Communications
Design/Operations
Network Architect/Engr
Architecture Directory Services/Authentication Design
Certificate-based authentication
Logical network diagrams - Internal ICS Zones
Logical network diagrams - Internal OT infrastructure
Comms Components - Fiber Optic Network
System Fiber Optic Layout
Area Fiber Optic Infrastructure
Remote Comms Components
Gateway Configuration Backup and Documentation
Sub#1 ICS Communications Diagram
Switch User Manual
Ethernet switch (24-Port Ethernet Switch)
Operations
Personnel
Contact Information
Contact Information
Operations Documentation
System Operations Procedures
ICS HMI Operating Procedures (including HCE Critical Components)
ICS HMI Operating Procedures (including Bkrs/Switches)
ICS Abnormal Operating Procedures (including HMI/Panel Alarms)
ICS Abnormal Operating Procedures (including HMI/Panel Alarms)
Other Systems Monitor and Control Operating Procedure
Battery Monitor and Control System Operating Procedure
System User Manual Documentation
System SCADA User Manual Documentation
Control/Automation Component User Manuals
ABB RTU560 tech manuals
BMT ADV1 Battery Monitoring and Control System
Maintenance
Personnel
Contact Information
Contact Information

System Description

In order to analyze the system to develop Attack Scenarios in Phase 3, the CCE Team must collect as much relevant information as possible. The information helps summarize the key details to support a deeper level of knowledge of the system operations, personnel support activities, system configuration, and other aspects of the operation. To accomplish this, a System Description is developed that details the key information that an adversary may need to obtain access and accomplish the HCE through cyber means. This description should summarize the functional block diagram and provide traceability to all the information collected in Phase 2 by describing where the information resides and who has access to it. This will be the output of Phase 2 and the input to Phase 3. A System Description for this use case is shown and detailed below.

System Description: Transmission System

Power delivery to the European market is delivered via the western Baltavian transmission grid. The five substations[3] that comprise the western portion of the transmission system are arranged roughly in a ring structure to provide redundant pathways for power delivery (see Figure 9). The ring structure ensures that if a single substation is taken completely out of service by a disruption, the remainder of the substations on the loop will still be able to provide connectivity. Power delivery to the European markets is provided via substations #1, #2, and #4 specifically. All three substations need to be online for maximum stability and power delivery capacity.

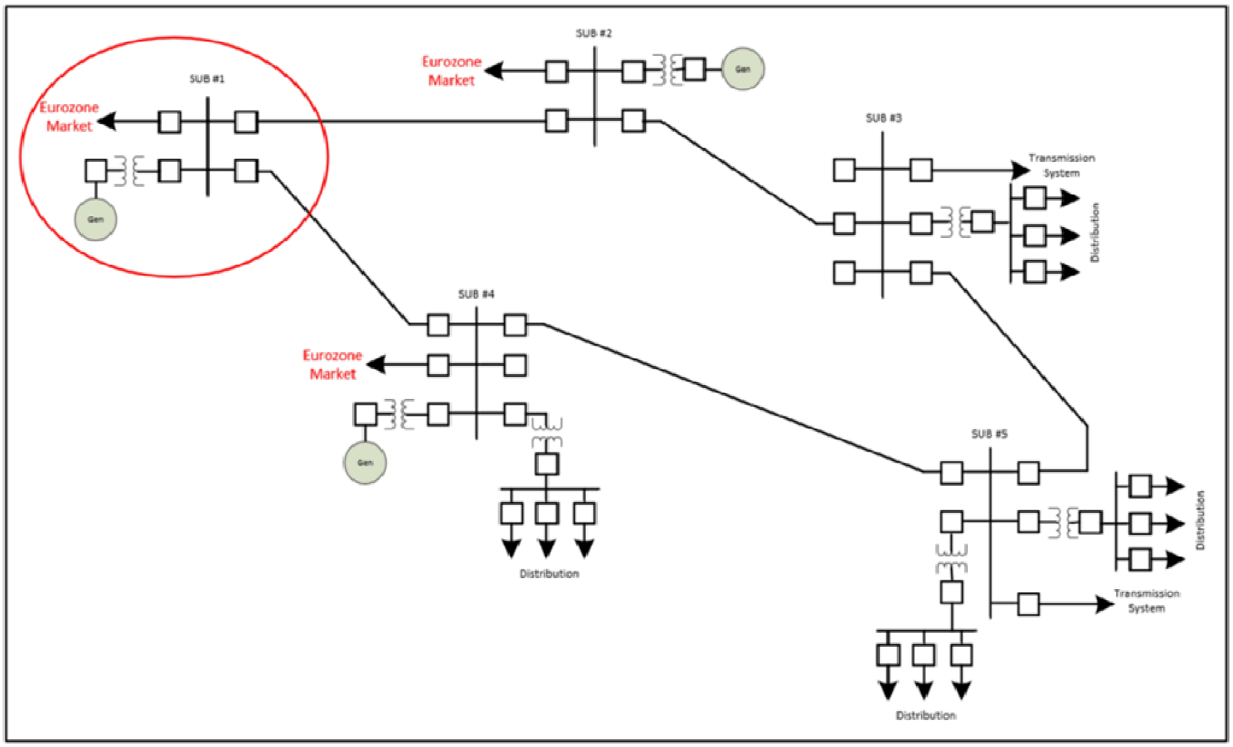


Figure 9: Transmission system western ring bus/one-line.

[3] See Appendix A for a glossary of key electric sector terminology.

System Description: Critical Substations

Each critical substation shares similar general topology. Dual transmission feeds provide the connectivity to the greater loop, and a third line provides connectivity to the target European market systems. Transmission voltage at each is established at 220kV. The bus structure of each substation is shown in Figure 10. As mentioned earlier, each of the substations also provides some generation capacity to offset internal (Baltavian) and external power demands.

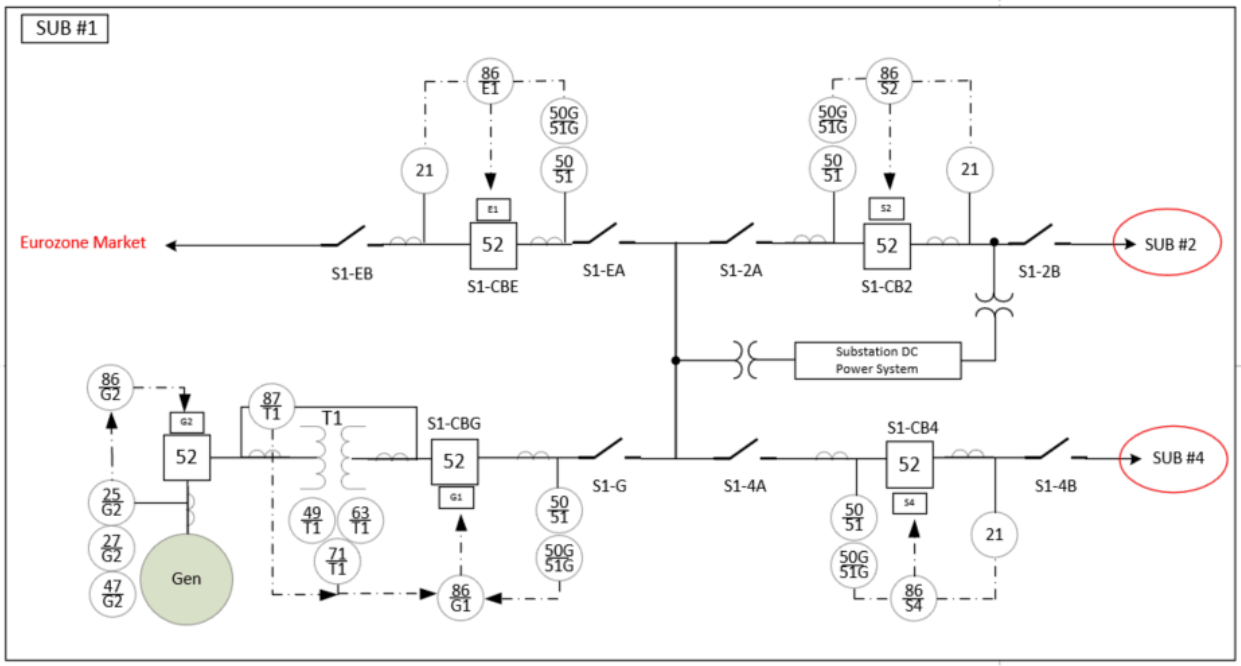


Figure 10: Substation #1 bus/protection schematic.

System Description: System Operations

Centralized transmission system operations, as well as generation dispatch, are performed remotely from a control center at the utility headquarters. Transmission operations (control/monitoring of the transmission system infrastructure) are implemented via a COTS SCADA platform, while generation dispatch uses an AGC module within the utility EMS. Each of the five transmission substations in the western ring have been recently commissioned with full SCADA capabilities via new front-end servers located at the HQ control center. The other transmission substations have active telemetry and metering; however, they do not have supervisory control capability from the control center since the necessary upgrades have not been made.

Communications and control engineering staff have access to the SCADA system network for station device configuration and troubleshooting activities. Although individual substation control and protection devices function independently from the SCADA system, without SCADA operability, automated remote management of stations and the greater transmission system is reduced to manual operations via radio. Because of staffing “cost optimization” measures, there are only enough linemen available to handle manual local response duties at a limited number of substations at any given time.

Travel and staging time for a site visit averages 3 hours or more.

System Description: System Communications

SCADA and individual substation operational environments reside on separate dedicated subnets within the corporate private network address space, see Figure 11. SCADA functionality is communicated to each substation controller (ABB RTU560) over ethernet on the SCADA subnet. The ABB RTU560 provides communications to local devices on the substation control subnet via separate onboard ethernet interface.

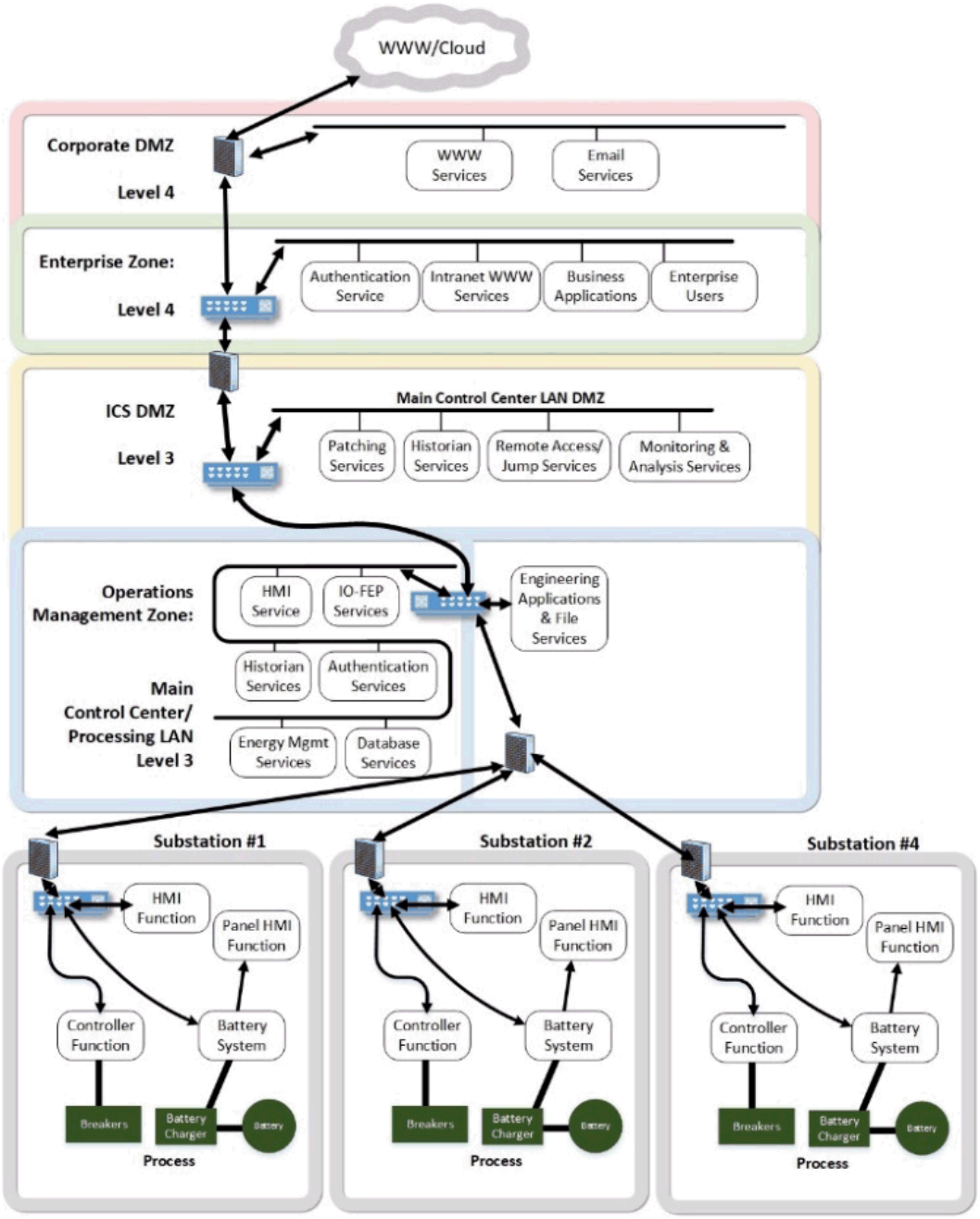


Figure 11. Utility power system SCADA communications.

System Description: Substation Control

Local monitoring and control capabilities are provided via a dedicated station controller platform. At the western grid critical substations, this critical device is an ABB RTU560. The station controller provides capabilities for SCADA communications, field device (e.g., breaker and switch actuator) operations, power system protection task/sequence logic processing, physical and logical I/O tagging, dc power system communications, station events analysis, alarming, and protocol concentration. See Figure 12 below for substation major functional grouping and group relationship to station control.

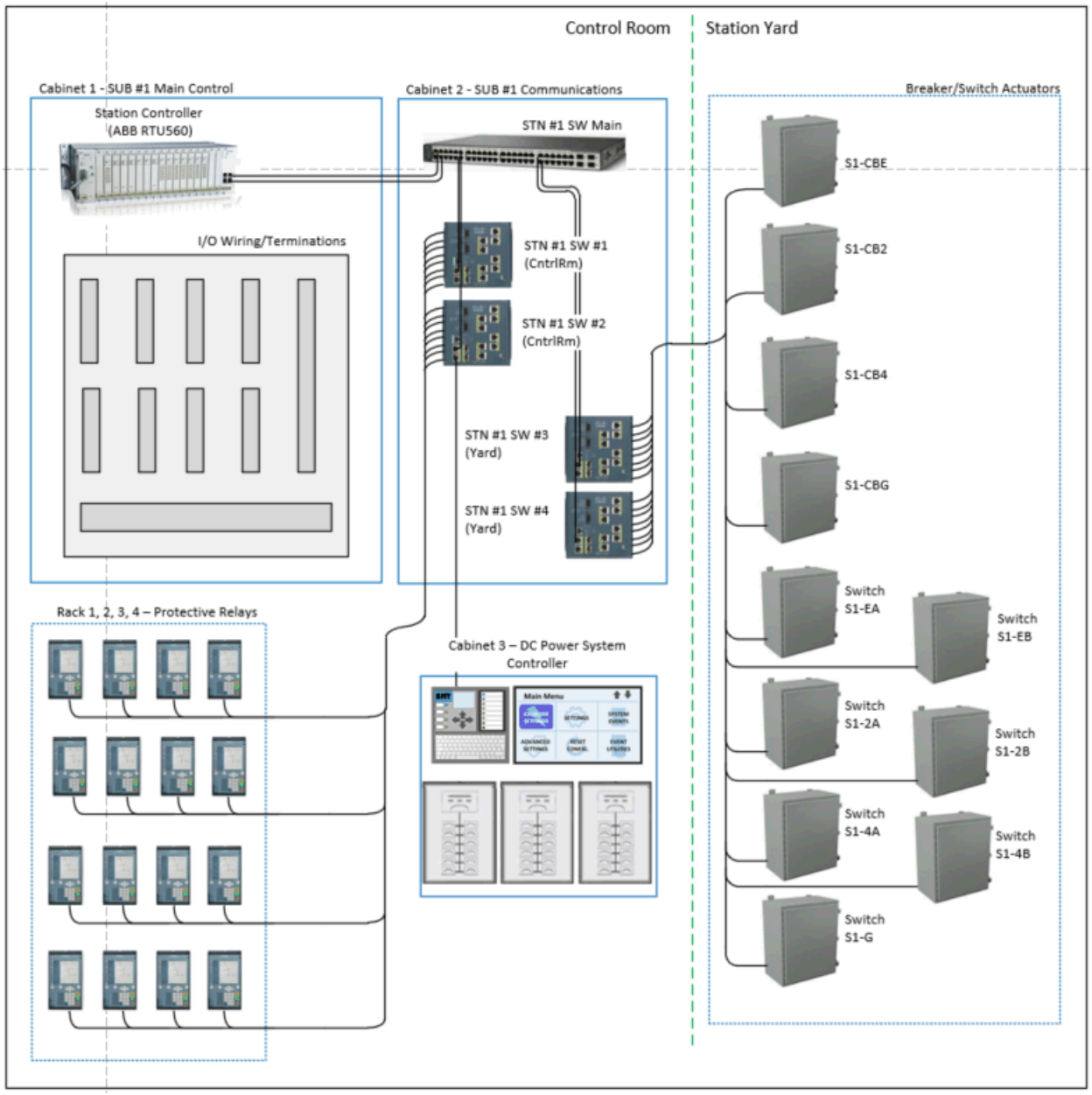


Figure 12. Station control via ABB RTU560 direct to breaker actuators.

System Description: Substation dc Power System

The three critical transmission substations with connectivity to the EU market have been equipped with a new auxiliary dc power system. The dc system is comprised of a battery management system (controller, ac/dc rectifier electronics, on-board maintenance bypass and transfer capabilities), dc power distribution infrastructure (breakers, panels, wiring, etc.), a battery bank, and a resistive load bank. The dc system is a redundant system with multiple taps used to provide power to all substation control and protective devices, communications infrastructure, breaker and switch actuators.

If the dc power system is incapacitated (battery failure, controller failure, loss of ac power supply and charging, etc.), the ability to automatically and/or remotely control and monitor the substation is lost. The battery management system provides control and monitoring of the dc system, a configuration interface, communications capabilities, and battery bank charging functions. Battery health/charge is critical—from a degraded charge state it can take up to 24 hours to restore batteries to a usable voltage level.

Phase 3: Consequence-based Targeting

The summary of the HCE-relevant information collected in Phase 2 is drafted into a System Description, which forms the basis of Phase 3, Consequence-based Targeting. The goal of Phase 3 is to develop *plausible* **Attack Scenarios**. The CCE Team uses an adversary perspective to identify different ways to achieve the HCE, analyzing the data from Phase 2 and collecting additional details as required. The **System Targeting Description** is used to summarize and reference all the key details that are required for the Attack Scenarios. It should be noted that the findings in Phase 3 are not all inclusive; they represent a set of possible approaches (**Technical Approaches**) to disrupting critical systems or functions. At the same time, these identified attack scenarios may be limited or informed by the Boundary Conditions defined in Phase 1. The **Target Details** describe each location where manipulation or compromise occurs in an Attack Scenario to make the HCE possible and includes all the technical details an adversary would need.

Phase 3 is a targeting effort at its core, during which organizations systematically identify the necessary steps for adversary success—all from the adversary's perspective. A key component to this approach is identifying the critical information needs and targets, as well as access and actions required for the adversary to achieve the desired effect. These **Critical Needs** are tied to accomplishing the HCE, such as the technical requirements for the implant (**Development**), or the access required to deliver an implant (**Deployment**). Critical Needs can and will be identified outside of an entity's network boundary or direct control (vendors, suppliers, subcontractors, regulatory or financial filings), as well as publicly available, open-source information found in various places. An entity's ability to identify what these Critical Needs are, where they reside, and who has access to them is a crucial step in understanding and ultimately mitigating risk.

For the CCE Team, the definition of critical information should extend well beyond documentation. An adversary will need to understand precisely how a process or piece of equipment operates in order to achieve a desired effect. To gain this type of knowledge, the adversary may need to acquire equipment, software, configuration files, or even access somewhere in the supply chain.

System Targeting Description

High Consequence Event: Adversary gains access to the substation network and manipulates configuration of the battery management system. Modifications reduce battery bank recharging capability, as well as dc power availability. The dc system capacity is degraded to a level insufficient for sustained support of substation SCADA, protection, and operations infrastructure. Attack ensures that no indications are presented to system operators while the charging system is at reduced capacity. Adversary triggers station isolation and de-energization by opening breakers on the three transmission-level interconnects.

System Description Parsing

Baltavia transmission system grid location and substation identification (subsystem and station IDs):

Transmission System: Power delivery to the European market is delivered via the western Baltavian transmission grid. The five substations that comprise the western portion of the transmission system are arranged roughly in a ring structure to provide redundant pathways for power delivery (see Figure 13). The ring structure ensures that if a single substation is taken completely out of service by a disruption,

the remainder of the substations on the loop will still be able to provide connectivity. Power delivery to the European markets is provided via substations #1, #2, and #4. All three substations need to be online for maximum stability and power delivery capacity.

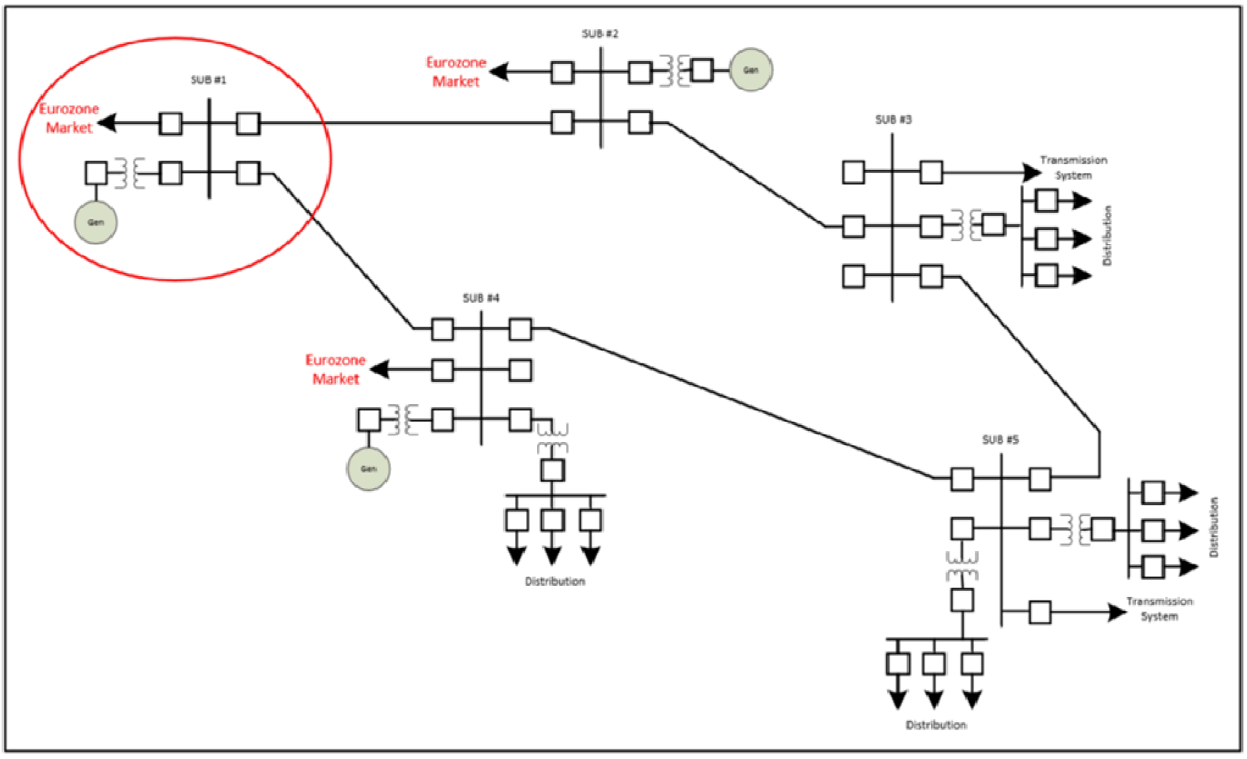


Figure 13. Five substations that comprise the western portion in a ring structure.

Critical substation bus/power delivery infrastructure (station isolation, breaker identification):

Critical Substations: Each critical substation shares similar general topology. Dual transmission feeds provide the connectivity to the greater loop, and a third line provides connectivity to the target European market systems. Transmission voltage at each is established at 220kV. The bus structure of each substation is shown in Figure 14. As mentioned earlier, each of the substations also provides some generation capacity to offset internal (Baltavian) and external power demands.

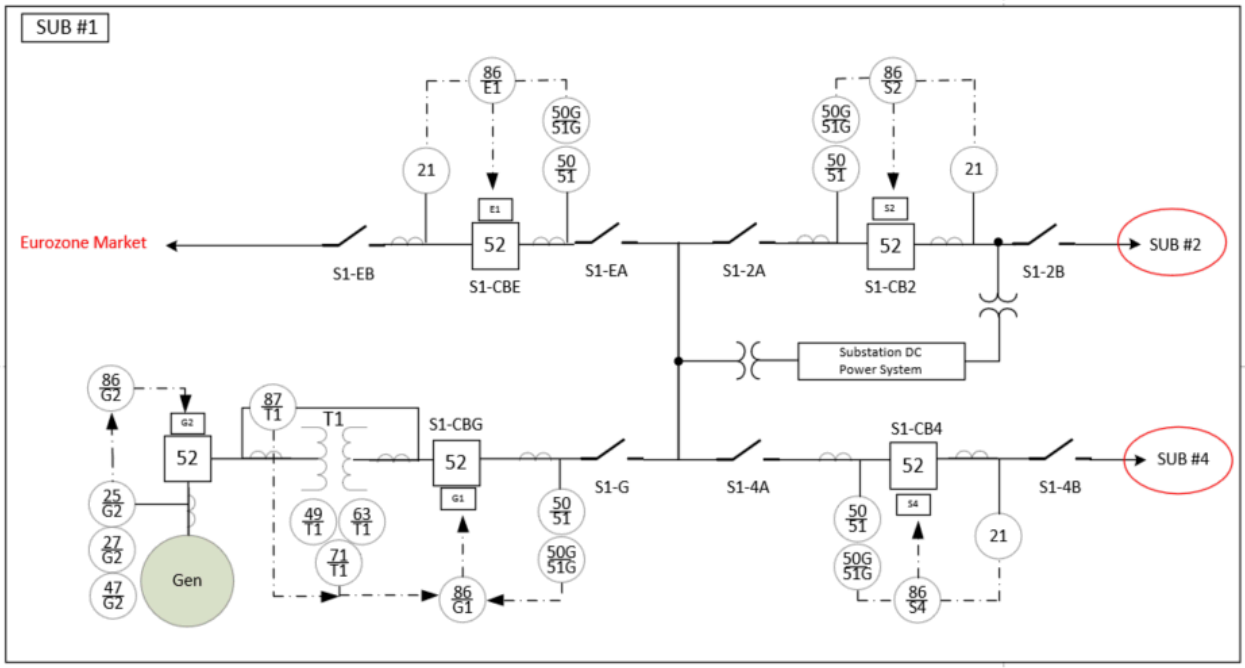


Figure 14. Substation 1's bus structure.

Critical substation control (controller capabilities, communications, circuit breaker operation):

Substation Control: Local monitoring and control capabilities are provided via a dedicated station controller platform. At the western grid critical substations, this critical device is an ABB RTU560. The station controller provides capabilities for: SCADA communications, field device (e.g., breaker and switch actuator) operations, power system protection task/sequence logic processing, physical and logical I/O tagging, dc power system communications, station events analysis, alarming, and protocol concentration. See Figure 15 on the next page for substation major functional grouping and group relationship to station control.

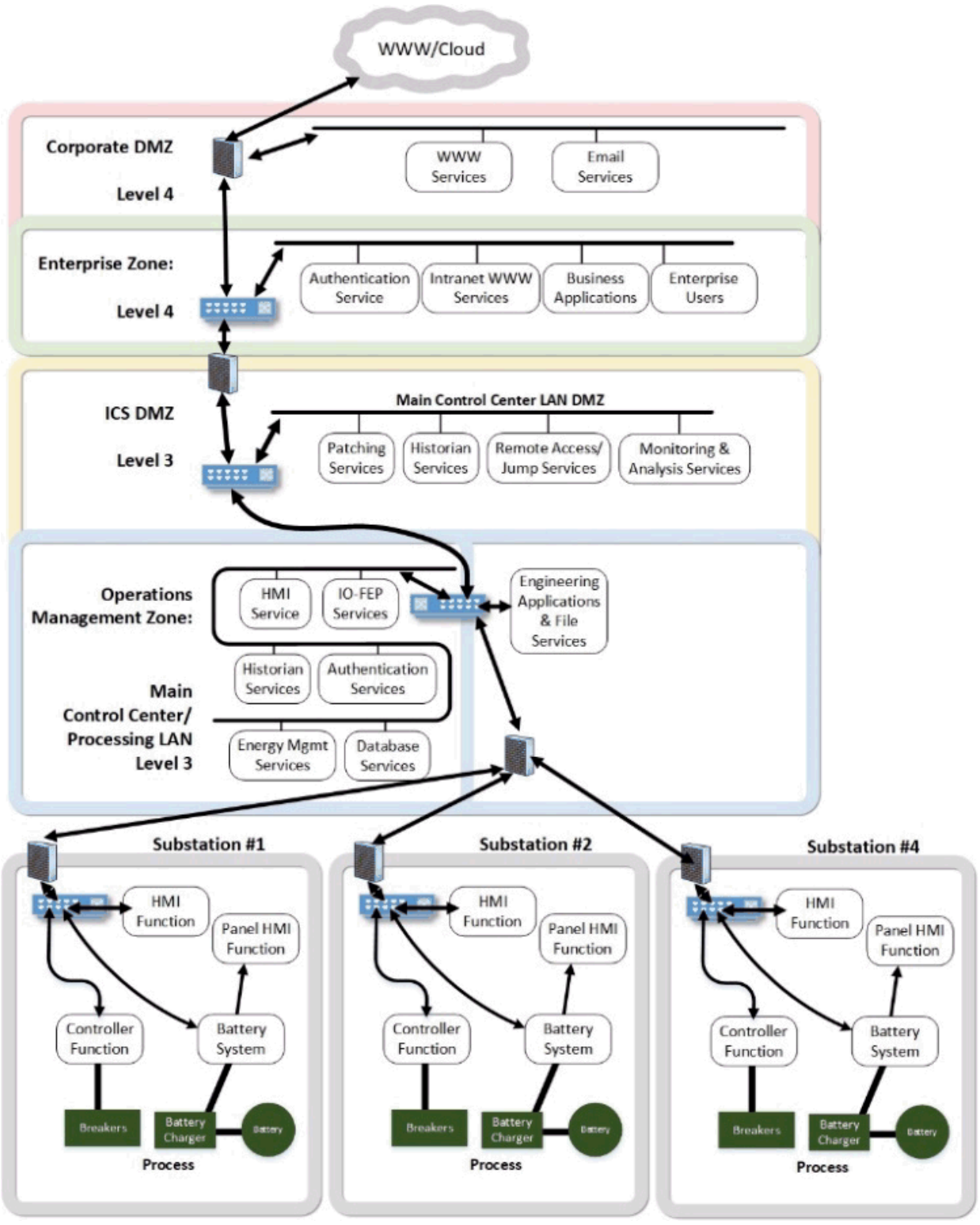


Figure 15. Substation major functional grouping.

Critical substation equipment power (dc power system - ID, capabilities, comms, restoration limitations):

Substation dc Power System: The three critical transmission substations with connectivity to the EU Market have been equipped with a new auxiliary dc power system. The dc system is comprised of a battery management system (controller, ac/dc rectifier electronics, on-board maintenance bypass and transfer capabilities), dc power distribution infrastructure (breakers, panels, wiring, etc.), a battery bank, and a resistive load bank. The dc system is a redundant system with multiple taps used to provide power to all substation control and protective devices, communications infrastructure, breaker and switch actuators. If the dc power system is incapacitated (battery failure, controller failure, loss of ac power supply and charging, etc.), the ability to automatically and/or remotely control and monitor the substation is lost. The battery management system provides control and monitoring of the dc system, a configuration interface, communications capabilities, and battery bank charging functions. Battery health/charge is critical—from a degraded charge state it can take up to 24 hours to restore batteries to a usable voltage level.

Critical substation communications (network connectivity, key components, data flow):

System Communications: SCADA and individual substation operational environments reside on separate dedicated subnets within the corporate private network address space. SCADA functionality is communicated to each substation controller (ABB RTU560) over ethernet on the SCADA subnet. The ABB RTU560 provides communications to local devices on the substation control subnet via separate onboard ethernet interface.

Critical systems operations (control hierarchy, control capabilities, incident response limitations):

System Operations: Centralized transmission system operations, as well as generation dispatch, are performed remotely from a control center at the utility headquarters. Transmission operations (control/monitoring of the transmission system infrastructure) are implemented via a COTS SCADA platform, while generation dispatch uses an AGC module within the utility EMS. Each of the five transmission substations in the western ring have been recently commissioned with full SCADA capabilities via new front-end servers located at the HQ control center. The other transmission substations have active telemetry and metering; however, because necessary upgrades have not been made, they do not have supervisory control capability from the control center. Communications and control engineering staff have access to the SCADA system network for station device configuration and troubleshooting activities. Although individual substation control and protection devices function independently from the SCADA system, without SCADA operability, automated remote management of stations and the greater transmission system is reduced to manual operations via radio. Because of staffing “cost optimization” measures, there are only enough linemen available to handle manual local response duties at a limited number of substations at any given time. Travel and staging time for a site visit averages 3 hours or more.

System Analysis for Targeting

Additional analysis of key systems, components, people, processes, digital connectivity, data flows, etc. that “fill in the gaps” and enables an adversary to assemble a relationally contiguous system targeting description for attack.

Key additional targeting information and steps (reconnaissance—open source and target environment)

Remote Connectivity: Targeted Substation and dc Power System Controllers

With creation of a free online account at each controller vendor website (substation - ABB, dc power system - BMT), "anonymous" review of technical documentation reveals a software application platform feature common to automation products—caching previously configured network communication paths. The communication paths are created by the support personnel as part of remote online controller engagement. The feature is utilized out of convenience by system technical support staff because it eliminates the need to remember and reconfigure complex network location/IP specifics associated with each of potentially dozens/hundreds of supported controllers in a large asset environment.

Technical Support Personnel

Engineering/Operations On-Call Support schedule on the SCADA/Ops data/file server identifies a utility substation engineer by name. Online research provides member profile on LinkedIn. Open-source research produces the employee's home address. Social engineering confirms employee's ISP and further reconnaissance provides the employee's home router Wi-Fi network ID. Continued investigation of available documentation on the SCADA/Ops data/file server produces a "remote access procedure" for engineering/operations on-call personnel.

Engineering Laptop

The details of an engineering laptop used for backshift support is described in the "remote access procedure" found on the SCADA/Ops data/file server. This includes the specifics of the hardware and the remote access software, as well as the engineering applications (BMT ADV1 Configurator, ABB RTUtil 560 Configurator, and ABB MultiprogWT Configuration Software).

Technical Approach

Target 1 (T1): Utility Substation Engineer's Laptop

Access:

Compromised home Wi-Fi router and substation engineer's laptop connected to home Wi-Fi network during on-call support.

Timing/Triggering:

Immediately upon substation engineer's laptop connection to home Wi-Fi network.

Action/Payload:

Two separate malware payloads (P1 and P2) are installed on the laptop, reference Figure 16. When the laptop is subsequently connected to the Utility SCADA Network, malware payload P1 will target and compromise the Substation #1 Battery Management Control System, and the malware payload P2 will be dropped on the SCADA Engineering Workstation and executed to target and manipulate the critical power delivery substation (Substation #1) infrastructure control.

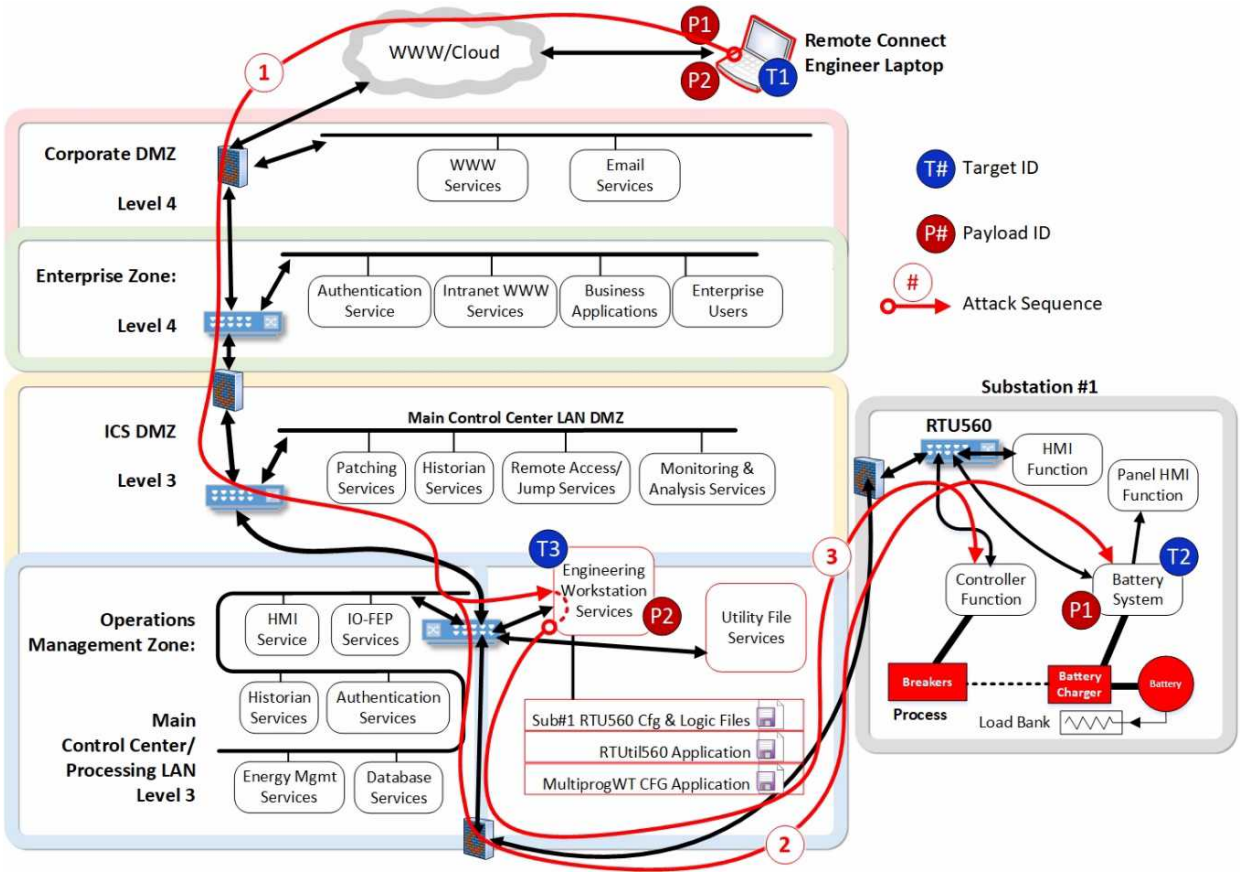


Figure 16. HCE attack communications path via SCADA to Sub#1 Battery System and RTU560 Station.

Target 2 (T2): Substation #1 Battery Management Control System

Access:

The substation engineer's laptop certificate-based authentication and VPN server configuration for remote access through the company firewall to the utility SCADA network.

Timing/Triggering (Malware P1 BMT Battery Management System Drop):

Immediately upon the substation engineer's laptop VPN connection to SCADA network.

Action/Payload:

Leveraging the substation engineer's escalated privileges, the malware deployment control on the laptop downloads the malware payload P1 to the Substation #1 BMT dc power system controller for malicious modifications to the BMT battery management software, see Figures 17 and 18. The modification will target the battery charging control function to degrade its operation resulting in the battery electrical potential being discharged through the station load bank. The software modifications also ensure that both ethernet-dependent and local HMI alarming are suppressed. System operators remain unaware that the charging system is at reduced capacity and after 12 hours, available stored battery power is insufficient to support critical substation loads: SCADA infrastructure, protective relays, and breaker actuators.

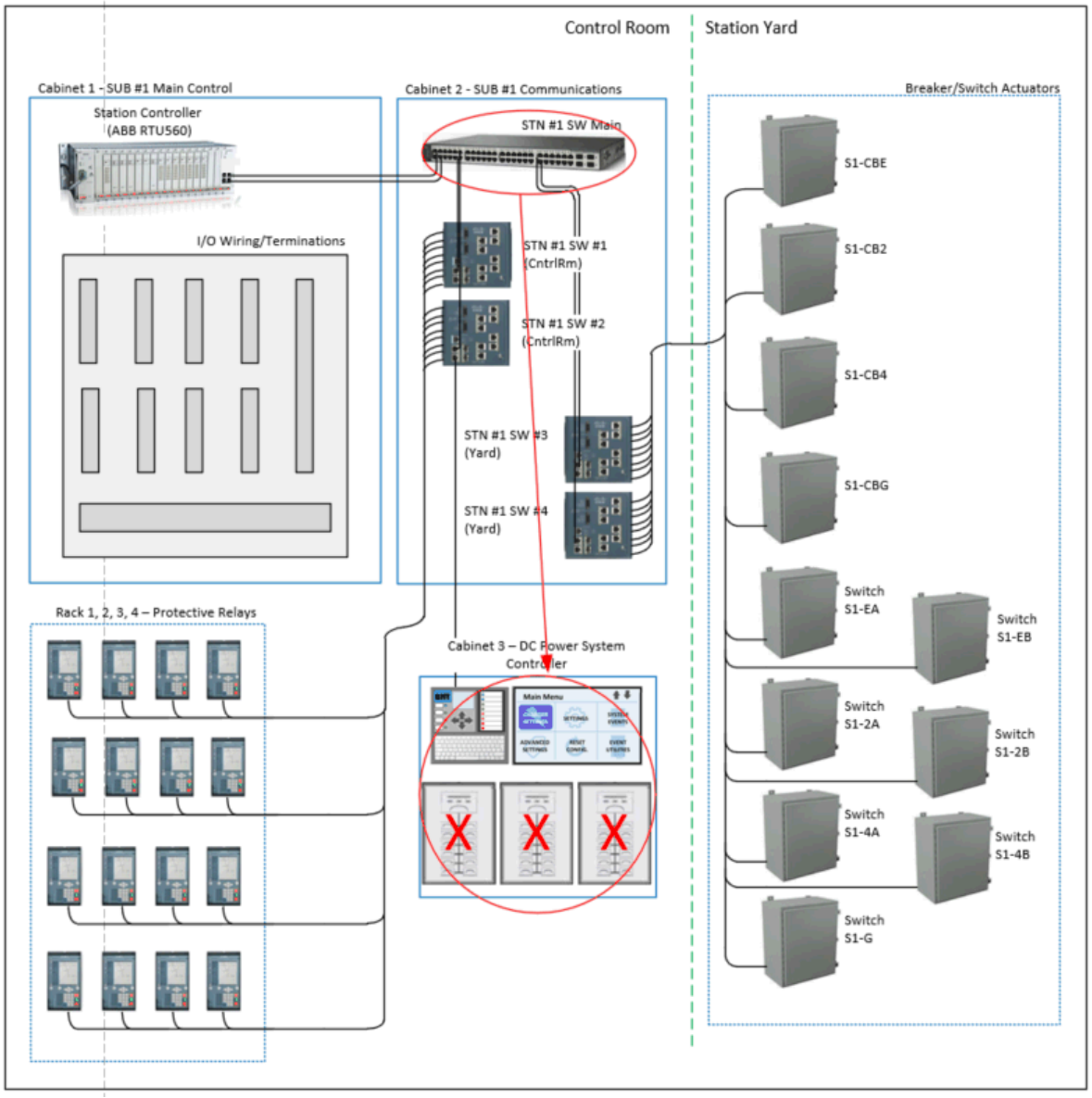


Figure 17. HCE attack on dc power system controller.

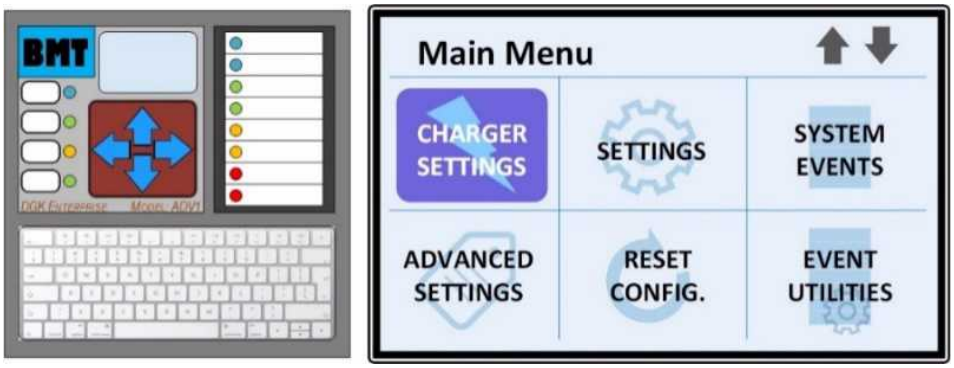


Figure 18. (L) Battery Management System Controller and (R) Battery Management System Application.

Target 3 (T3): SCADA Engineering Workstation

Access:
The substation engineer's laptop certificate-based authentication and VPN server configuration for remote access through the company firewall to the Utility SCADA network.
Timing/Triggering (Malware P2 SCADA Engineering Workstation Drop):
Immediately upon the substation engineer's laptop VPN connection to SCADA network.
Action/Payload:
Leveraging the substation engineer's escalated privileges, the malware deployment control on the laptop downloads the malware payload P2 to the SCADA Engineering Workstation. This malware will target the Substation #1 power system infrastructure.
Timing/Triggering (Malware P2 Execution):
Malware P2 payload will execute and take actions on the Substation #1 power system control after a 12-hour time delay as measured from drop time on the SCADA Engineering Workstation located within the Engineering Applications and File Services functional area.
Action/Payload:
With the dc power system impacted and using the ABB MultiProg PRO RTU560 configuration software and Substation #1 project file on the local SCADA engineering workstation host, the malware establishes communication natively to the Substation #1 RTU560 (see Figures 19).

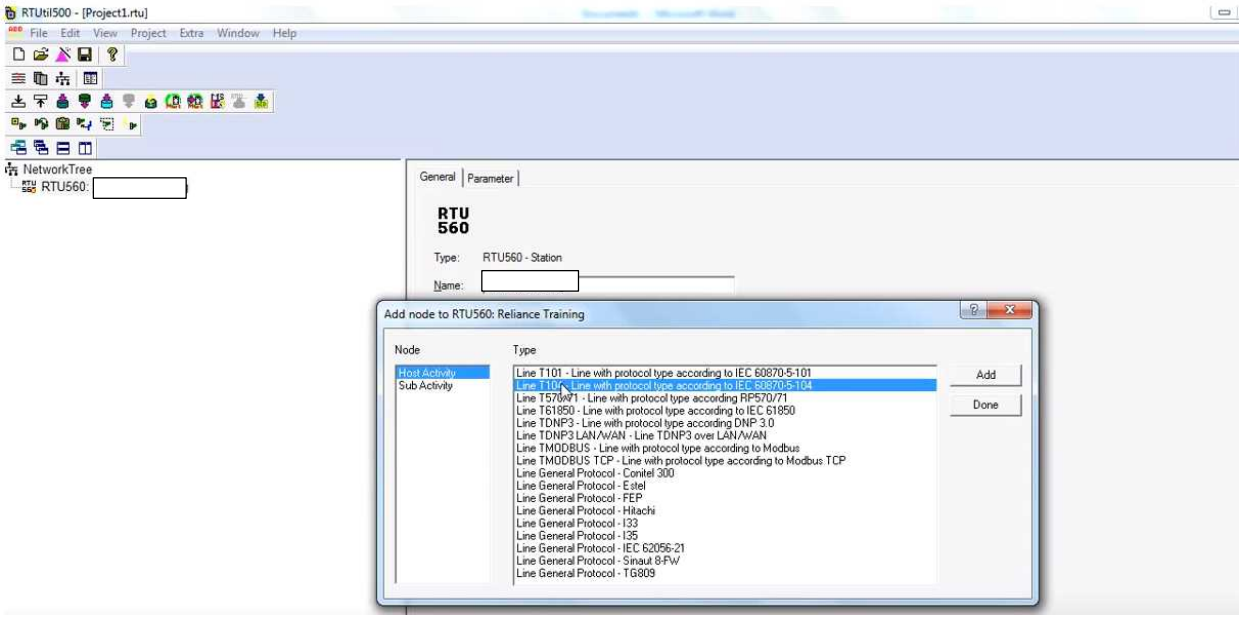


Figure 19. ABB RTUtil 560 Application from Engineering Workstation to configure RTU560 System.

From here, leveraging engineered functionality provided by the ABB MultiProg PRO RTU560 Application (see Figure 20) and based on the breaker "trip" logic (see Figure 21), the attacker initiates station breaker operations on substation transmission circuit breakers S1-CBE, S1-CB2, S1-CB4, and S1-CBG (Figure 22 and 23).

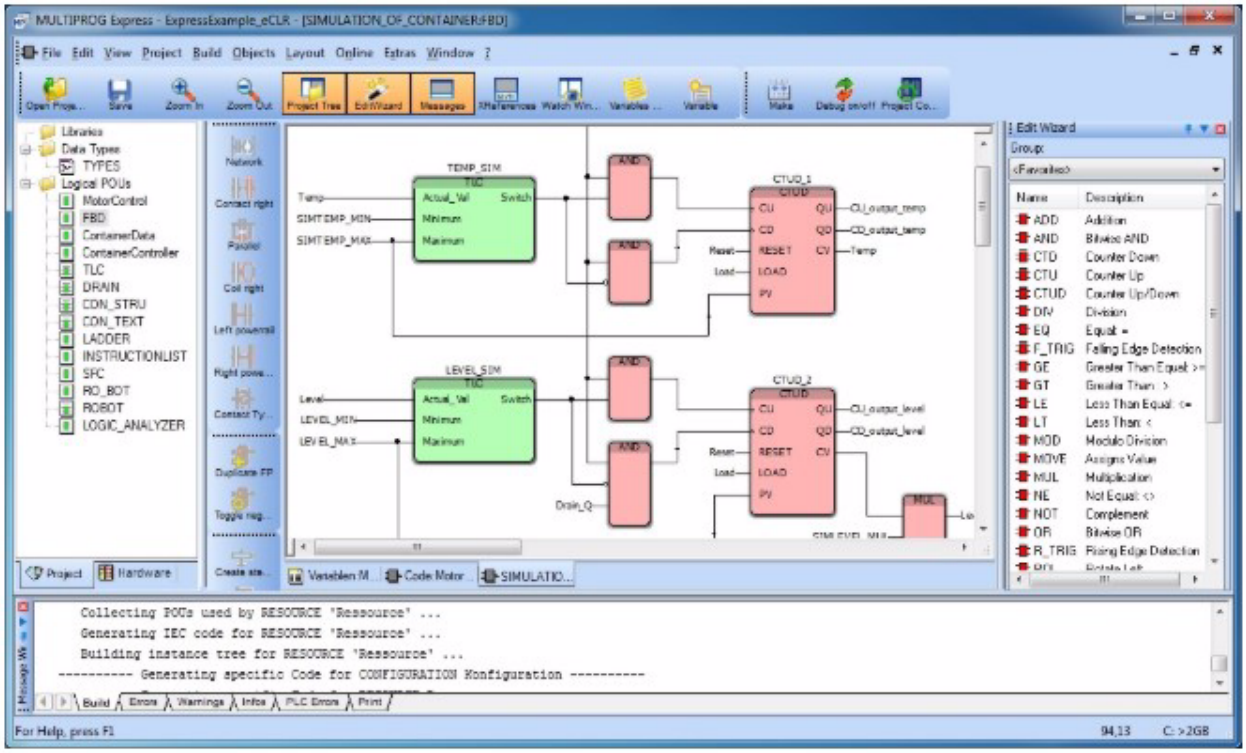


Figure 20. ABB MultiprogWT Configuration Software to ABB RTU560.

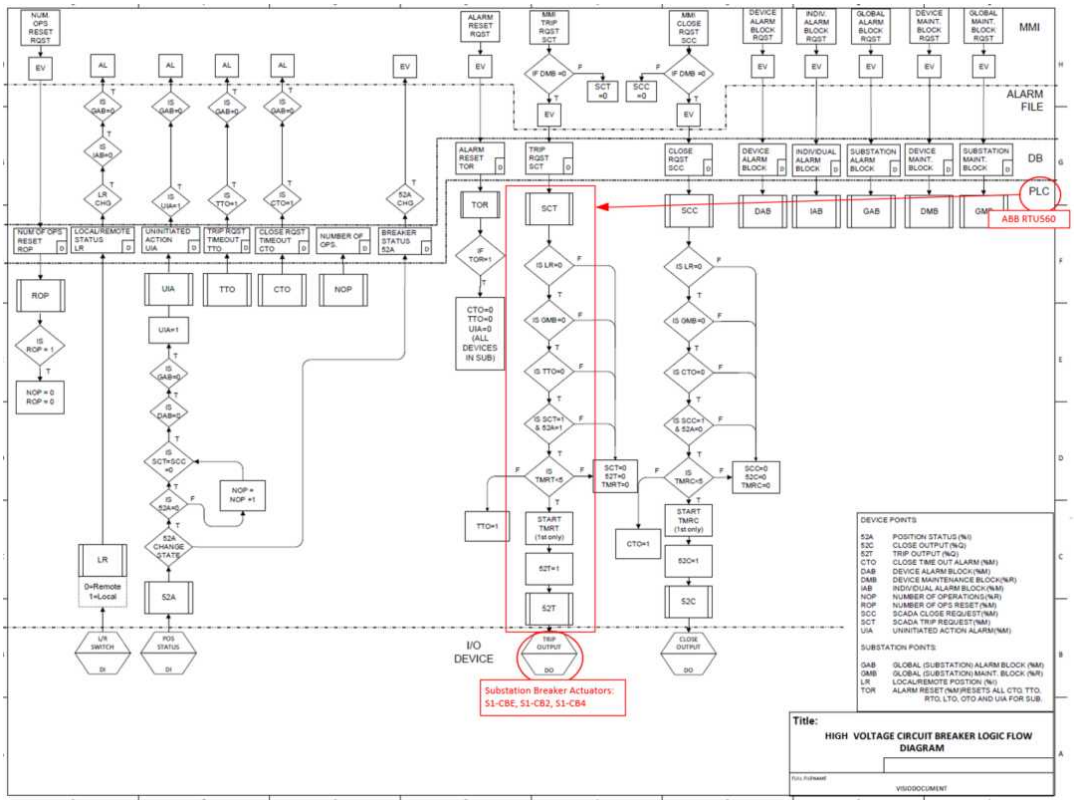


Figure 21. Power system control trip logic used during the HCE attack.

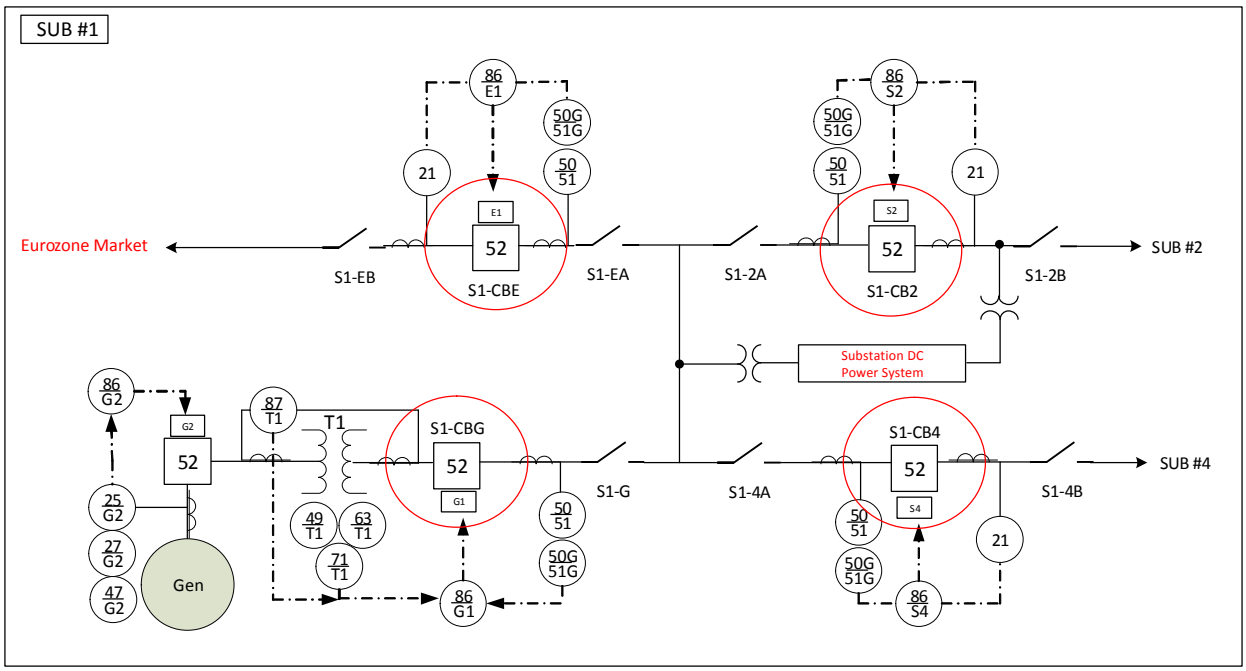


Figure 22. Schematic for HCE attack.

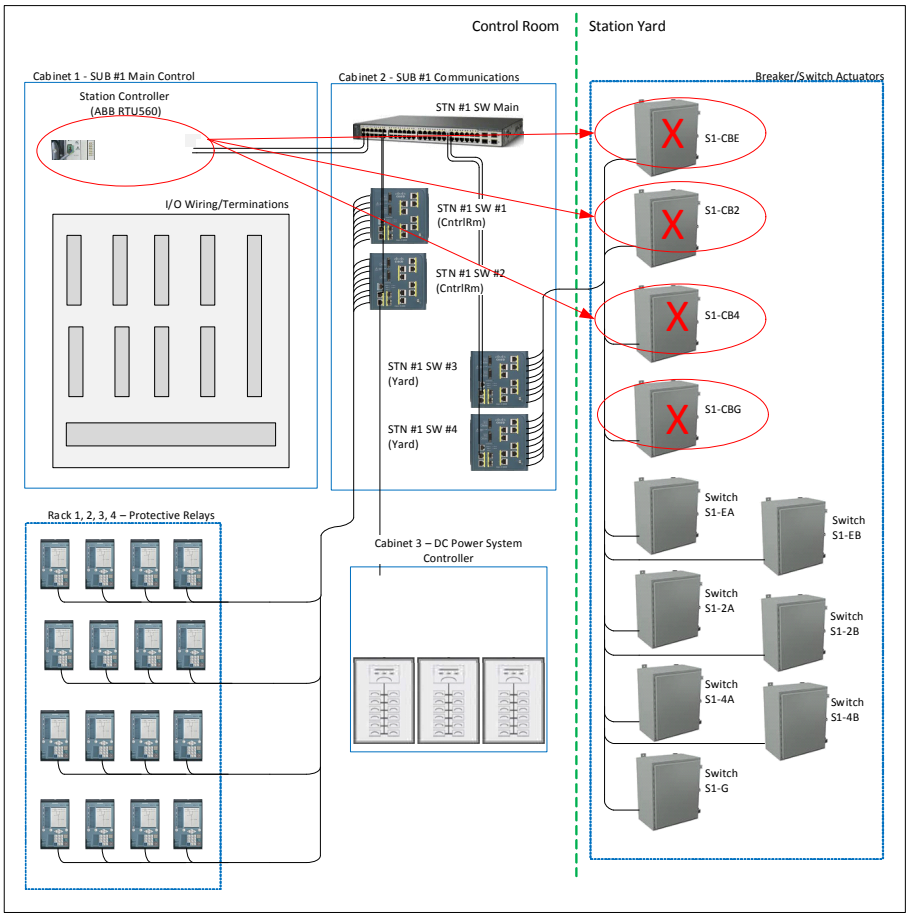


Figure 23. Station functional groups and control used during HCE attack.

The loss of bus connectivity from the transmission system isolates the substation and removes the substation ac supply to the station BMT battery management system. The ac and dc power sources at the substation are lost. Adequate battery-stored dc power is unavailable from the battery system. Attempts from the utility control room SCADA operator to exercise breaker actuation causes excessive demand and damage on individual battery cells.

Target Details

The critical components involved in the HCE provide power system control, monitoring, and protection operability for Substation #1. A utility SCADA engineer laptop or workstation provides a familiar operating environment from which to stage the attack, but malicious modifications need only take place in the Substation #1 dc power BMT battery management system and at the Engineering Workstation that contains the ABB MultiProg PRO RTU560 application.

The preliminary HCE diagram can then be updated, as shown in Figure 24, to represent the complete sequence of events and components involved in the HCE attack. The engineer's laptop was the first target, T1, where the attacker payloads, P1 and P2, were installed. When the engineer connected remotely, the P1 payload was transmitted, installed, and initiated in the T2 BMT Battery Charger Management System and the P2 payload was transmitted and installed in the T3 Engineering Workstation, which will initiate a 12-hour timer. When the timer expires, the breaker and switch operations will be transmitted directly to the substation #1 RTU560 via the ABB MultiProg PRO RTU560 Configuration Application.

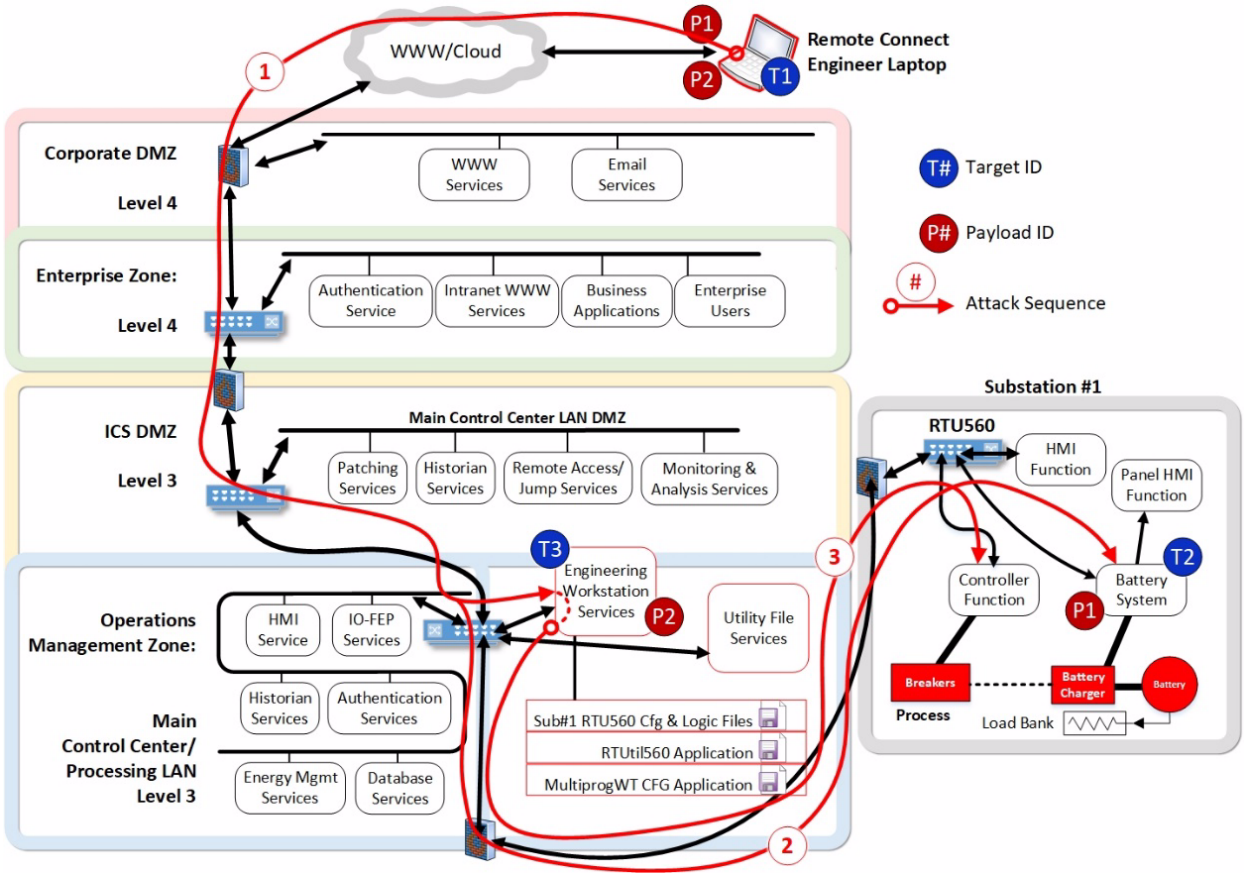


Figure 24. Updated HCE attack scenario.

Adversary efforts to expand understanding of the critical systems and devices would likely involve development of a critical component list (see Table 2), which is a subset of Phase 2 taxonomy line items, and with details available via open-source vendor literature (where not provided already on the compromised workstation or file server).

Table 2: Critical Components

Utility SCADA Engineer Laptop	Name	Dell Laptop
	Function	SCADA Engineer Portable App/Data Host
	Vendor	Dell
	Model	Precision 7540
	OS/Misc	x64, Windows 10 Enterprise
	Protocols	TCP/IP/Ethernet, SSH, SNMP, HTTPS, HTTP, Telnet, DNP3, SEL Fast Message
Utility SCADA Engineering Workstation	Function	SCADA Engineer App/Data Host
	Vendor	Dell
	Model	Precision 3630 Tower
	OS/Misc	x64, Windows 10 Enterprise
	Protocols	TCP/IP/Ethernet, SSH, SNMP, HTTPS, HTTP, Telnet, DNP3, SEL Fast Message
Utility SCADA File Server	Function	SCADA Utility File Server
	Vendor	Dell
	Model	Precision 3630 Tower
	OS/Misc	x64, Windows 10 Enterprise
	Protocols	TCP/IP/Ethernet, SSH, SNMP, HTTPS, HTTP, Telnet, DNP3, SEL Fast Message
Substation Controller	Name	ABB RTU560
	Function	Substation Control
	Vendor	ABB
	Model	RTU560
	Protocols	Ethernet, IEC 61850 MMS, IEC 60870-101/104, Modbus TCP, IEEE C37.118, LG 8979, CP2179, Telnet, DNP3, EtherCAT
ADV1 Battery Management Controller	Name	BMT Battery Management Controller
	Function	Substation DC Battery Management System
	Vendor	DGK Enterprise
	Model	ADV1
	Protocols	Ethernet, Modbus, DNP3
ABB RTUtil 560 Configuration Software	Name	RTUtil 560
	Function	RTU560 system configuration
	Vendor	ABB
	Model	RTUtil 560
ABB MultiprogWT Configuration Software	Name	MultiprogWT RTU Logic Configurator
	Function	Logic configuration for RTU560 Controller
	Vendor	ABB
	Model	MultiProg-wt
BMT Battery Management system application	Name	ADV1 Configurator
	Function	Battery Management System configuration
	Vendor	DGK Enterprises
	Model	ADV1

Critical Needs - Development

Component	Critical Needs for Development	Location/Availability
Substation Engineer Dell Precision 7540 Laptop	Operating system	On board, available at initial compromise
	VPN	Utility/Networking Data/app server
	Certificate-based authentication	Utility/Networking Data/app server
	Security/Monitoring Software and Configuration	Utility/Security Data/app server
SCADA Engineering Workstation Dell Precision 3630 PC Tower	Operating system	Open source
	VPN	Utility/Networking Data/app server
	Certificate-based authentication	Utility/Security Data/app server
	ABB RTUtil 560 Configurator	On board - SCADA Engineering Workstation
	ABB MultiprogWT Configuration Software	On board - SCADA Engineering Workstation
Utility SCADA/Ops File Server Dell Precision 3630 PC Tower	Operating system	Open source
	Diagram- Sub#1 Bus/Breaker Schematic	On board - Utility/SCADA Ops File Server
	Diagram- Sub#1 Breaker Control Diagram	On board - Utility/SCADA Ops File Server
	Diagram- Sub #1 Breaker Control Logic Diagram	On board - Utility/SCADA Ops File Server
	Diagram- Sub #1 Communications Schematic	On board - Utility/SCADA Ops File Server
	Diagram- SCADA Systems Network Topology Diagram	On board - Utility/SCADA Ops File Server
	Document- SCADA User Manual	On board - Utility/SCADA Ops File Server
	Document- Operating Procedure: Station Isolation	On board - Utility/SCADA Ops File Server
	Document- Operations Schedule/On-Call Duty List	On board - Utility/SCADA Ops File Server
	Document- Remote Access Authorized Users List	On board - Utility/SCADA Ops File Server
	Document- Remote Access Policy and Procedures	On board - Utility/SCADA Ops File Server
BMT ADV1 Battery Management Controller	Product specs / manuals	Open source
	Battery system one-line diagram	Utility SCADA/Ops File Server
	Battery charger failure (alarm) operations procedures	Utility SCADA/Ops File Server
	Utility maintenance procedures	Utility SCADA/Ops File Server
	Files- ADV1 Sub#1 Configuration File	Utility/Sub#1Cfg/Battery
BMT ADV1 Battery Management System Configurator	Software and associated documentation	(Purchase)
	Utility software update procedures	Utility SCADA/Ops File Server
ABB RTU560	Product specs / manuals	Open source

In order to develop the attack that delivers the HCE, an adversary would need to understand the detailed functionality of each critical component, as well as the operational context for use of the technologies. Documentation providing these function and context details would be part of the adversary's critical needs. Table 3 on the next page provides an example list of Critical Needs, including likely artifact location.

Critical Needs - Deployment

Controller	Diagram- Sub#1 Bus/Breaker Schematic	Utility/SCADA Ops File Server
	Diagram- Sub#1 Breaker Control Diagram	Utility/SCADA Ops File Server
	Diagram- Sub #1 Breaker Control Logic Diagram	Utility/SCADA Ops File Server
	Sub#1 Comms Gateway specs / configurations	Utility SCADA/Ops File Server
	RTU560 wiring diagram	Utility SCADA/Ops File Server
	Files- RTU560 Sub#1 Configuration File	Utility/Sub#1Cfg/RTU
ABB RTUtil 560 Configurator	Software and associated documentation	(Purchase)
	Utility software update procedures	Utility SCADA/Ops File Server
ABB MultiprogWT Configuration Software	Software and associated documentation	(Purchase)
	Utility software update procedures	Utility SCADA/Ops File Server

Phase 4: Mitigations and Protections

Phase 4 "Mitigations and Protections" covers exactly that—mitigation and protection strategies. Using the CCE framework for Phase 4 in Figure 25, we will attempt to come up with recommendations around protections and mitigations for the power system operator in anticipation of the HCE scenario.

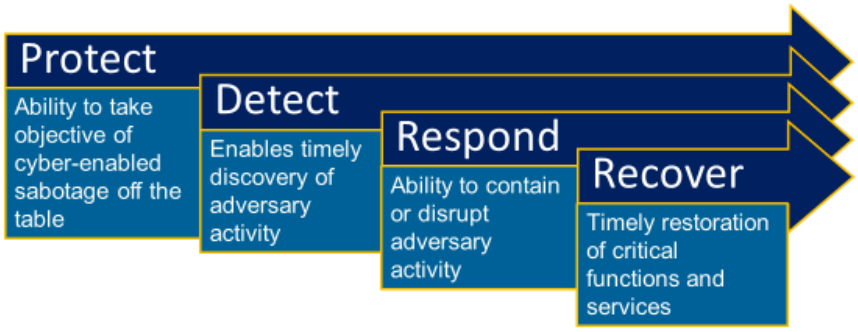


Figure 25. Mitigation & Protection framework.

PROTECT

Engineering: Battery Management System Network Isolation and Hardwired I/O

- Remove capabilities for remote network access to the Battery Management System device. Maintain SCADA and local monitoring/alarming capabilities via physical aux contacts and/or dedicated "out-of-band" networking that is isolated from the general station network.

Operations: Station dc Power System Health/Availability Verification

- Separate, non-networked device-level dc battery system monitoring that provides alarming for under/over voltage, as well as other critical dc system parameters. Validation occurs visually via local HMI and/or transducer display. Operator verifies that dc power system parameters are within (+/- X%) of desired ranges (and local control setpoint) on a fixed time basis by procedure (such as, "check setpoint hourly as part of rounds"). This would also require the operator to have a response procedure (detailed in section below).

If these measures are not implemented, please consider the following. With digital access (remote via

utility networks or locally via laptop), because the substation power system and battery management systems are programmable/configurable (for the purpose of improved operational efficacy and efficiency - automated fault/anomaly response), complete mitigation of the attacks in this HCE is not likely, short of replacing automated controllers with purely electromechanical devices. However, the substation dc power system ac tap location, Battery Management System network connectivity, and the general substation attack surface presented in this scenario can be greatly reduced through several design, device, and network security improvements. A few of these are identified below.

Substation dc Power System ac Tap

- Although the existing dual supply approach provides excellent operational resiliency, in order to also eliminate complete dependence on the substation transmission feed to the substation, at least one of the ac taps should be located on the transmission system—but "upstream" of the switches controllable from the subject substation controller. This engineered, physical change maintains dual ac sourcing for the critical dc Power System, but it also eliminates impact capabilities from a single digital component and system (Substation HMI -vs- SCADA Server).

Substation Network Architecture

- Network segmentation, access control, and monitoring: small-scale industrial firewall (industrial protocol-aware) for establishing dedicated substation subnet, access control, and traffic DPI analytics for IDS/IPS. Effectiveness requires out-of-band management for support. Segmentation should include separating the cyber-enabled devices by voltage class and function.
- Implement an ICS-aware perimeter device at the field substations, if possible, or at the control center to ensure only the function codes used by the utility are allowed with a protocol.
- Configure the Substation perimeter communications devices (e.g., communications gateway) to only accept control commands from the SCADA control center I/O server.
- Eliminate remote access to substation, except for specific devices/accounts in the SCADA zone.
- No direct internet access.
- If appropriate for the operation size, consider implementing Area of Responsibility control logic to limit the scope of what a single operator workstation can impact.

RTU

- Disallow remote device configuration of RTUs.
  - Single dedicated serial port for SCADA I/O
  - No direct communications with SCADA servers. Configure SCADA data export/push/write via serial comms to Substation ABB RTU560 for secure delivery outside of substation network environment. SCADA writes should be limited to operating parameters only, with hard-coded range limiters.
- If remote device configuration is required from substation network environment:
  - Single network comm interfaces plus single dedicated serial port for SCADA I/O
  - No direct communications with SCADA servers, same limitations as above.
  - Substation Communications Gateway provides dedicated authentication/access control.

- If remote device configuration is required from SCADA zone, same as above with implementation of additional substation zone access control and monitoring requirements, such as dedicated MFA at substation firewall, out-of-band communications, permissive from the utility control center, session limitations, secondary device-authentication at Substation Communications Gateway, etc.
- Disable remote firmware upload capability administratively on the field devices. Ensure it is not being performed out of band through a directly attached device in the field.
- Local device configuration (vendor-specific to our example scenario)—if possible, disable the webserver diagnostics service to prevent remote modifications.
- Local device configuration (vendor-specific to our example scenario)—disable "parameter loading" capability.

Substation Engineer Data/App Server, Workstation, and/or Laptop

- Access control includes multifactor authentication to SCADA zone authentication server.
- Endpoint protection that includes malware, script control, and application whitelisting.
- All data-at-rest file storage uses encryption (production-critical, business-critical, etc.).

Additional security improvements (greater environment)—these can certainly make an attack more difficult to execute and will impose additional costs on an adversary.

All Network Environments

- Firewall-enforced zone segmentation, access control, and network traffic DPI analytics for IDS/IPS at zone boundaries.
- Controlled use of administrative privileges in all zones.

DETECT

Device Event Monitoring and Analysis

- Deploy and/or configure device-level dc battery system supply monitoring that provides alarming for under/over voltage, as well as other critical dc system conditions. Alarming should be hardwired to station notification controller and communicated out-of-band (dedicated SCADA network) to control center. Distributed monitoring at the individual device improves overall reliability and reduces risk of adversarial "masking" a more centralized approach.
- Enable automated logging on communications gateways.
- Enable automated logging on protective relays.
- Enable automated logging on RTUs.

Network Monitoring and Analysis

- Provide capture and Deep Packet Inspection (DPI) of all ingress/egress network traffic at SCADA zone interface router
- Provide capture and DPI of all ingress/egress network traffic at each substation local gateway
- Dedicated network IDS/IPS at SCADA and substation zone interfaces
- Employ anomaly detection, network whitelisting monitoring, or behavioral analytic detection
- Implement communications baselines

Improved Endpoint Malware Detection

- Deploy malware signature detection at host and network level

Account monitoring and control

- Endpoints
- Implement directory level detection of abnormal logins to detect credential theft and pivot

For your consideration:

- Detection activities can be resource intensive. There are constant changes and alerts that need attention and proper staffing to be effective.
- What detection capabilities does your organization have currently?
- Does your organization belong to any communities to help share information about possible or actual attacks?

RESPOND

Operations: Station dc Power System Health/Availability Verification (reference Protect from above).

- Operator takes immediate actions per: Station dc Power System Failure response procedure. Steps include immediate SCADA control center notification, network isolation of battery management system, configuration validation/correction at local battery management system interface, dc power system voltage verification (manual spot measurements using hand-held meter), and continuous local monitoring of dc power system health restoration. Operator also initiates cybersecurity response and troubleshooting protocol.

Incident Response and Management - General

- Fully developed Incident Response (IR) and Management Plan for Operations and Business Environments
- Annual hands-on practice of IR and Management Plan
- Operations personnel on staff to support manual operations for widely distributed, multi-station event
- Out-of-band communications infrastructure, operable and available 24/7 to support Ops staff
- Establish chain of command in advance of emergencies
- Open communication channels between OT and IT (and corporate)

For your consideration:

- Does your organization have a clear communication and action plan for an attack?
- Do you have checklists to follow (to avoid missing steps)?
- Has someone been given authority to make emergency decisions (i.e., shut down functions or systems)?
- Who will speak for the company if the press gets involved?
- How will information sharing be managed?

RECOVER

Operations: Station dc Power System Functional Restoration (reference Respond from above).

- Depending on conditions discovered during response activities, possibly disconnect existing dc system supply at distribution and provide temporary/mobile dc supply (battery units, diesel/gas generator with dc rectifiers, etc.) in its place until the permanent system can be restored and validated.

Incident Recovery - General

- Fully developed Recovery Plan for Operations and Business Environments
- Annual hands-on practice of Recovery Plan
- Operations personnel on staff to support manual operations for widely distributed, multi-station event.
- Out-of-band communications infrastructure, operable and available 24/7 to support Ops staff
- Maintain local manual control capabilities for substation components
- Ensure configuration data backups
- Tested recovery (dry run)
- Encrypted storage for sensitive files

For your consideration:

- A clear roadmap and a realistic timeline for recovery are key for getting back to full operation.
- Does your organization have a plan?
- Recovery plans often involve using backups and restoring a system to its pre-attack condition—is this enough?
- This stage can become an opportunity to strengthen areas that were previously neglected—are there systems that need to be updated (software, hardware, training materials, etc.)?

Appendix A: Key Terms

Electricity
A secondary power source harvested from the mechanical work that is exerted from a turbine to a coupled, rotary magnet that spins around copper coils within a generator. The purpose of the primary fuel's energy is to create mechanical power that can be transformed into electrical power.

Electrical power
The instantaneous flow of electrical charges, or currents, which serve as the means to perform work. Currents are driven by an electromotive force, or voltage, which represents the driving potential for performing work. Electrical power flow is instantaneous and finite. Commercially viable storage options do not currently exist. The flow of electricity is governed by electromagnetic properties of the materials that make up the electric grid. Circuits are constructed to establish a path for power to flow, and flow can be controlled in a system using protective elements such as fuses, breakers, relays, and capacitors.

The structure of ***electricity delivery*** can be categorized into three functions: generation, transmission, and distribution, all of which are linked through key assets known as substations as represented in Figure 20.

Figure 26: Electricity delivery process.

The Grid
Layout of the electrical transmission system; a network of transmission lines and the associated substations and other equipment required to move power. In the United States, the combined transmission and distribution network is often referred to as the "power grid" or simply "the grid." In the United States, there is no single grid, rather three distinct interconnections (the Eastern Interconnection, Western Interconnection, and the Texas Interconnection). Power demand fluctuates throughout the day and across regions with varying population densities because utility-scale electricity storage does not exist. To keep the electrical systems always balanced, generation operators must dispatch enough power required to supply demand. Power dispatch is coordinated by the plant operator and a transmission system operator making communications critical at generation facilities.

Transmission
Power transmission lines facilitate the bulk transfer of electricity from a generating station to a local distribution network. These transmission lines are designed to transport energy over long distances with minimal power losses which is made possible by stepping up or increasing voltages at specific points along the electric system. The components of transmission lines consist of structural frames, conductor lines, cables, transformers, circuit breakers, switches, and substations. Transmission lines that interconnect with each other to connect various regions and demand centers become transmission networks and are distinct from local distribution lines. Typical transmission lines operate at 765, 500, 345, 230, and 138 kV; higher voltage classes require larger support structures and span lengths.

Power Distribution
The power distribution system is the final stage in the delivery of electric power, carrying electricity out of the transmission system to individual customers. Distribution systems can link directly into high-voltage transmission networks or be fed by sub-transmission networks. Distribution substations reduce high voltages to medium-range voltages and route low voltages over distribution power lines to commercial and residential customers.

Substations
Equipment that switches, steps down, or regulates voltage of electricity. Also serves as a control and transfer point on a transmission system. Substations not only provide crucial links for generation, but they also serve as key nodes for linking transmission and distribution networks to end-use customers. While a substation can provide several distinct system functions, most utilize transformers to adjust voltage along the electric system. A substation may be designed initially for the purpose of bulk power transmission but may also incorporate an additional transformer to distribute power locally at a lower voltage. Power lines are classified by their operational voltage levels, and transmission lines are designed to handle the higher voltage ranges (typically > 100kV). Transformer equipment at substations facilitate energy transfer over networks that operate at varying voltage levels. A substation generally contains transformers, protective equipment (relays and circuit breakers), switches for controlling high-voltage connections, electronic instrumentation to monitor system performance and record data, and fire-fighting equipment in the event of an emergency. Some important functions that are carried out at substations are voltage control, monitoring the flow of electricity, monitoring reactive power flow, reactive power compensation, and improving power factors.

Transformer
Electrical device that changes the voltage in ac circuits. Transformers are critical equipment in delivering electricity to customers, but many are in isolated areas and are vulnerable to weather events, acts of terrorism, and sabotage. The loss of transformers at substations represents a significant concern for energy security in the electricity supply chain due to shortages in inventory and manufacturing materials, increased global demand in grid developing countries, and limited domestic manufacturing capabilities. Substations are highly specific to the systems they serve, which also limits the interchangeability of transformers. Replacing a transformer is associated with a long delivery lead time because they are generally difficult to transport due to their size and weight, and larger, more sophisticated models are manufactured abroad. Failure of even a single unit could result in temporary service interruption. Although power transformers come in a wide variety of sizes and configurations, they consist of two main components: the core; made of high-permeability, grain-oriented, silicon electrical steel, layered in pieces; and windings; made of copper conductors wound around the core, providing electrical input and output.

Electrical Energy
The generation or use of electric power over a period, usually expressed in megawatt hours (MWh), kilowatt hours (KWh), or gigawatt hours (GWh), as opposed to electric capacity, which is measured in kilowatts (KW).

(see also: DOE/OE-0017)

Protective relays
Detect abnormal or unsafe conditions by comparing real-time operating parameters with pre-programmed thresholds. When those threshold values are met or exceeded, the relay will initiate an action—such as opening a circuit breaker—to isolate the components under fault condition (abnormal current) and prevent potential equipment damage. Relays were originally electromechanical, but today they are typically microprocessor based due to the increased functionality such devices provide.

Auxiliary dc control power system
Consists of batteries, battery management system (rectifier/charger/monitoring/config), and the dc power distribution to dependent loads: SCADA infrastructure (server, workstation, HMI, network devices); protective relays, and substation RTUs that monitor and operate circuit breakers and switches, and actuators. Under normal operation, power availability is managed to recover the battery voltage after a discharge and to maintain the float voltage while supporting any self-discharge losses in the battery system. The aux dc system is sized and operated to meet the demand of continuous, intermittent, medium-rate and momentary high-rate loads (trip coils and dc motors). Upon failure of the battery charger or loss of its ac supply, the battery bank must support the station continuous loads along with the intermittent and momentary loads that may occur before the battery charger is repaired or the ac supply is restored.

Supervisory Control and Data Acquisition (SCADA) systems
Highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and wastewater collection systems, oil and gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations, such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

Common major control components include the following:

- **Control Server.** A control server hosts the DCS or supervisory control software that is designed to communicate with lower-level control devices. The control server accesses subordinate control modules over an ICS network.
- **SCADA Server**. The SCADA server is the device that acts as the 'master' in a SCADA system. Remote terminal units and PLC devices (as described below) located at remote field sites usually act as 'slaves.'
- **Remote Terminal Unit (RTU).** The RTU, also called a remote telemetry unit, is a special purpose data acquisition and control device designed to support SCADA "remote" deployments. RTUs are field devices that often support a variety of communications mediums. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is then referred to as an RTU.
- **Programmable Logic Controller (PLC).** The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, drum switches, and

mechanical timer/counters). PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCSs. Other controllers used at the field level are process controllers and RTUs; they provide the same control as PLCs but are designed for specific control applications. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.

- **Intelligent Electronic Devices (IED).** An IED is a "smart" sensor/actuator containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. An IED could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA and DCS systems allows for automatic control at the local level.
- **Engineering Workstation.** A desktop or laptop PC-scale cyber asset where engineers and technicians utilize the appropriate software and design tools to perform system and device troubleshooting, configuration, tuning, and maintenance tasks.
- **Human-Machine Interface (HMI).** The HMI is software and hardware that allows human operators to monitor the state of a process under control, modify/configure some control setpoints within engineered limits, and may provide manually overriding of automatic control functions in the event of an emergency. The HMI typically displays process parameter and status information, process alarming, and historical process data points for operators, administrators, managers, business partners, and other authorized users. The location, platform, and interface may vary a great deal. For example, an HMI could be a dedicated platform in the control center or a laptop on a protected LAN in the process environment.
- **Data Historian.** The data historian is a centralized database for logging all process information within an ICS. Information stored in this database can be accessed to support various analyses, from statistical process control to enterprise level planning. The trending application generally resides on the Historian server.
- **Input/output or Front-end Processor (IO or FEP) Server**. The IO/FEP server is a control component responsible for collecting, buffering and providing access to process information from control sub-components such as PLCs, RTUs and IEDs. An IO server can reside on the control server or on a separate computer platform. IO/FEP servers are also used for interfacing third-party control components, such as an HMI and an EWS.

(see also: NIST 800-82)