THREAT AND VULNERABILITY ASSESSMENT

Distribution Substation

Prepared by:

Darren T. Nielsen, CPP, PSP, PCI

07/25/2019

NAVIGANT

TABLE OF CONTENTS

DISCLAIMER

This report ("report") was prepared for BVES on terms specifically limiting the liability of Navigant Consulting, Inc. (Navigant), and is not to be distributed without Navigant's prior written consent. Navigant's conclusions are the results of the exercise of its reasonable professional judgment. By the reader's acceptance of this report, you hereby agree and acknowledge that (a) your use of the report will be limited solely for internal purpose, (b) you will not distribute a copy of this report to any third party without Navigant's express prior written consent, and (c) you are bound by the disclaimers and/or limitations on liability otherwise set forth in the report. Navigant does not make any representations or warranties of any kind with respect to (i) the accuracy or completeness of the information contained in the report, (ii) the presence or absence of any errors or omissions contained in the report, (iii) any work performed by Navigant in connection with or using the report, or (iv) any conclusions reached by Navigant as a result of the report. Any use of or reliance on the report, or decisions to be made based on it, are the reader's responsibility. Navigant accepts no duty of care or liability of any kind whatsoever to you, and all parties waive and release Navigant from all claims, liabilities and damages, if any, suffered as a result of decisions made, or not made, or actions taken, or not taken, based on this report.

CONFIDENTIAL DOCUMENT

This report contains confidential and proprietary information. Any person acquiring this report agrees and understands that the information contained in this report is confidential and, except as required by law, will take all reasonable measures available to it by instruction, agreement or otherwise to maintain the confidentiality of the information. Such person agrees not to release, disclose, publish, copy, or communicate this confidential information or make it available to any third party, including, but not limited to, consultants, financial advisors, or rating agencies, other than employees, agents and contractors of such person and its affiliates and subsidiaries who reasonably need to know it in connection with the exercise or the performance of such person's business.

EXECUTIVE SUMMARY

On Tuesday, July 23, 2019, in response to the California Public Utilities Commission Order D-19-01-08, on Physical Security, Darren T. Nielsen, CPP, PSP, PCI, of Navigant Consulting, Inc., conducted interviews and a vulnerability assessment in reference to the Substation.

The purpose of the threat and vulnerability assessment is to identify electric distribution assets that may merit special protection, and measures to address potential security risks and reduce the potential of long-term outage to an identified distribution facility that meets the following criteria: *Distribution Facility that serves installations necessary for the provision of regional drinking water supplies and wastewater services (may include certain aqueducts, well fields, groundwater pumps, and treatment plants).* BVES has no other substations that meet the other six CPUC criteria listed in the order.

These interviews provided additional insights for the assessor to process the information obtained from the Subject Matter Experts (SMEs) and helped to focus the site tour on ways a physical attack on the substation from outside the fence-line could occur, identify the vulnerabilities and critical assets of the Substation, and identify potential hostile surveillance points in the surrounding area.

The assessment included the 3 critical distribution assets of the facility and a 34kV feed line to uncover security weaknesses, and potential threats which could impact the BVES distribution capabilities should a physical attack take place. The following personnel listed below were consulted as the SMEs and interviewed as part of the assessment.

The Bear Valley Electric Service team consisted of:

Paul Marconi -Director

Jeff Barber -Field Operation Supervisor

The assessment is the source for the development of the Physical Security Mitigation Plan which identifies mitigation, protection, prevention and resiliency efforts to mitigate the risk of long-term outage to the Substation.

SITE OVERVIEW

Site Description

The Substation is a 20 ft x 25 ft distribution substation located in close proximity of a Wastewater treatment plant. The site is an unmanned substation located in a residential area. The primary function is a subsidiary station of an electricity generation, transmission and distribution system where voltage is transformed from high to low voltage. The site is the primary feed for the wastewater treatment facility and serves approximately 800 utility meters during peak demand.

The Substation is located at:

Grid Coordinates Latitude: Longitude:

Aerial View from Google Maps depicting the confined area of approximately 20 ft wide x 25 ft deep where the critical assets are located. The top of the picture is due North.

Deleted photo

CIP Confidential

Critical Assets

The following assets were identified by the SMEs and the assessor as critical to the operation of Substation:

Transformers: There are 3 transformers located adjacent to each other from West to East.

Replacement Cost: $20,000 per transformer **Replacement Time:** 6 Hours/24 Man hours

Voltage Regulators: There are 3 Voltage regualtors located adjacent to each other from West to East.

Replacement Cost: $15,000 per regulator **Replacement Time:** 6 Hours/ 24 Man hours

Circuit Breaker: This is a single electrical device used to control, protect and isolate electrical equipment. Circuit Breakers are used to interrupt any short circuits or overload circuit that may occur on the network. This type of equipment is directly linked to the reliability of the electric system.

Replacement Cost: $40,000 **Replacement Time:** 4 hours/ 16 Man hours

Transmission Lines: 34kV feed line to Substation

Replacement Cost: $75,000 **Replacement Time:** 16 hours/64 man hours

Off-line Impacts

Operationally – The water facility would be affected. However, there are current plans to install an 8 megawatt solar facility that will also feed direct power to the site.

Commerce – Power outage to the community recreation and vacation tourism would have a negative impact on business owners affecting the company's reputation.

Environmental – There would be an environmental impact if the facility was offline for a long period of time. The environmental impact may include water scarcity, inability to clean wastewater and minimize water pollution.

Customers Served - The Substation serves approximately 800 service meters at peak demand and the Regional Wastewater Agency.

Resiliency Measures - Bear Valley Electric Service has a very strong business continuity plan that ensures adequate square parts are in their inventory and are able to appropriately respond to an outage and perform operational recovery of the site quickly. The substation has approximately 10 spare units of each critical asset on hand and stored in a secured facility approximate 5 miles away. Additionally, BVES has a trailer mounted transformer station that can handle the load on a temporary basis until operations can be fully restored.

There is a redundant path that can be field switched from the Shay Substation to have load picked up and rerouted to serve the customer base in this service area.

Unique Characteristics

A number of unique characteristics exist at or near the Substation that have the potential to introduce additional risks, threats and vulnerabilities to the site. The following unique characteristics were considered while evaluating threats and vulnerabilities to the Substation.

To the north of the substation is the treatment plant powered by the Substation. There are several buildings that could conceal an active assailant shooting position.

Additionally, a small hill beyond the facility to the north could be a shooting platform with line of sight to the critical assets.

Note: The unmanned gate that is open during business hours increases the vulnerability and aids an attacker in gaining access.

The area to the south is residential in nature, but indicators of recreational vehicle traffic is present and provides unimpeded access to the substation, potentially allowing damage to occur with little likelihood of intervention or apprehension.

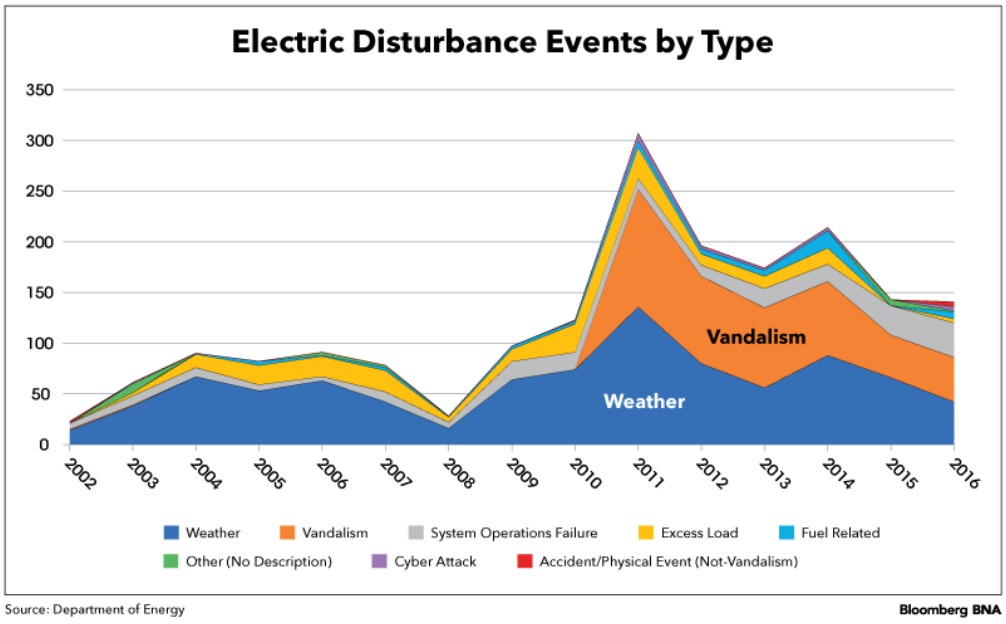
CIP Confidential

The view below is the west side personnel access gate controlled by a standard commercial grade padlock and chain. Note: the 2-inch chain link fence with inserted slates designed to obscure vision from distance offers no close-in concealment of the critical assets within the fence line.

The east side of the perimeter fence is bowed. The 45 degree outrigger topped with the 3-strand barb wired is bent and loose. This weakness increases the ability for an attacker to climb the fence.
There is overgrown vegetation that could be used as a starter for a fire or concealment for a threat actor, armed with tools or supplies for arson or other criminal activities.

Prior History of Attack

Utilities are mandated by the Department of Energy's, Office of Electricity Delivery and Energy Reliability (OE) to report the causes of major interruptions or outages through the Electric Emergency Incident and Disturbance Report (OE-417). Electrical Disturbance Events by Type provides OE-417 statistics of incidents caused by actual or suspected physical attacks, sabotage, and vandalism:



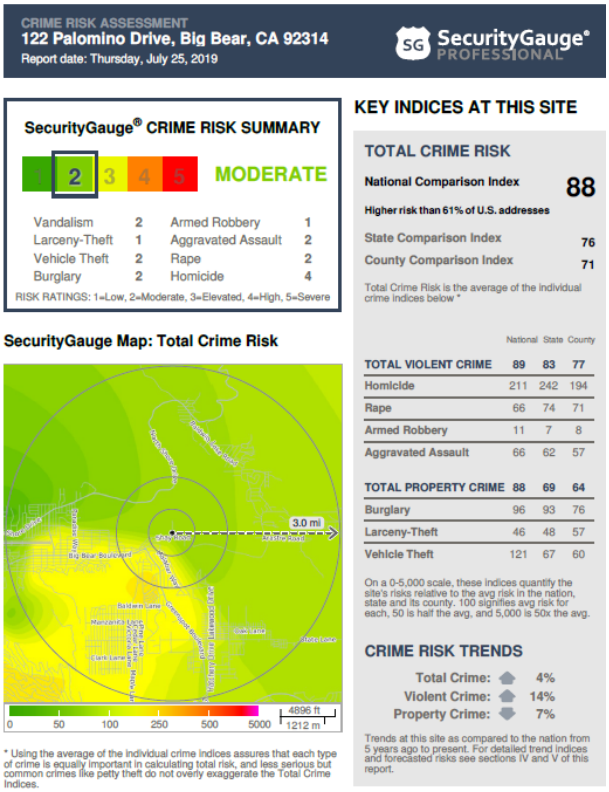
The table above depicts a history of electrical disturbances affecting the bulk electrical system. Many of the attack incidents did not result in an arrest or identification of a suspect, which leaves the motives unknown. Some incidents may be a result of low level criminal theft or vandalism. However, others may suggest a more calculated and targeted attack.

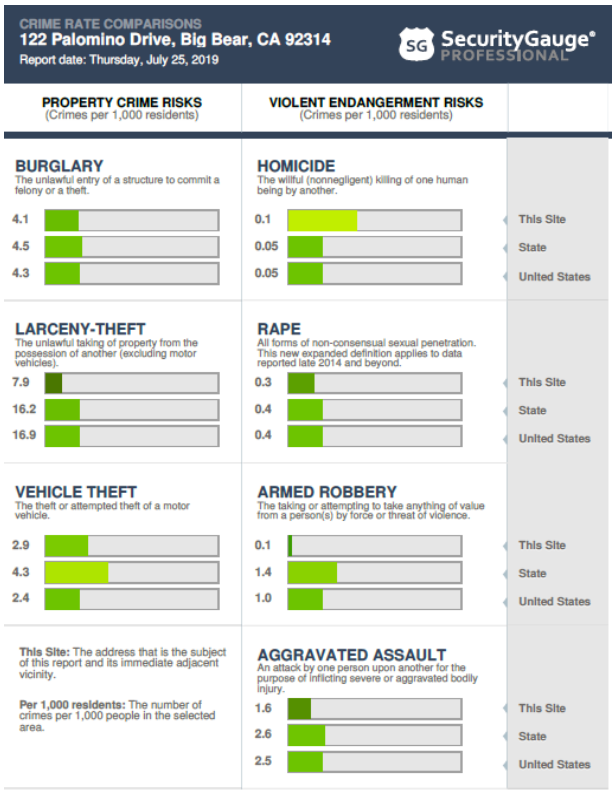
While the overall numbers remain relatively small, the trend in the number of incidents targeting electrical sites and control rooms have been increasing based on information from the E-ISAC. Nearly 40% of attacks since 2002 have targeted substations/switchyards or control centers within the WECC region.

Attacks on Electrical Sites 2002 – July 2019				
Area	Total	Rifle/Gunshot	IED/Explosives	Insider Threat
North American Grid	95	62	14	19
WECC region	36	24	5	7

Crime Statistics

The assessor collected the most current (2019) statistics from Security Gauge for site specific details inserted below that indicate the risk is moderate for vandalism. Theft is considered to be low and trending down.





The FBI uniformed crime report for 2017 indicates a downward trend from the 2016 numbers.

The table below is a summary of relevant criminal activity for the City of Big Bear Lake, CA.

City	Burglary	Arson	Property Crime
Big Bear Lake	49	3	178

Based upon a thorough review of all available information, there has not been a documented or reported physical attack, security breach or an OE-417 report submitted for the Substation.

Adversarial Groups

To assist with establishing the Attack Likelihood an assessment of adversarial groups and their potential tactics was completed. Two adversarial groups were considered during the threat analysis: Criminal and Domestic Extremism. The assessment of these groups provided a general threat level each presents to the electric system based on intent, capability, presence in the region, history of incidents, plots, or sensitive but unclassified intelligence reporting involving the electric system.

Criminals: For the purposes of this threat assessment, criminals will be considered those individuals or groups who intend to engage in illegal activity, but not motivated by an ideology (environmental, political, religious, etc.). There are individuals within the WECC region that have perpetrated criminal activity against the bulk electric system numerous times in the past and it is anticipated they will continue to do so in the future. Criminal groups may have greater intent and capability for lower level crimes focusing on burglary, theft, fraud, counterfeiting, vandalism, and trespassing, as opposed to sabotage, which may require insider knowledge. However, crimes such as theft, burglary, and vandalism still have the potential to disrupt operations of the electric system, whether intentional or otherwise.

Domestic Extremism: For the purposes of this threat assessment, domestic extremism groups will be considered those committing potentially disruptive, harmful, or destructive criminal acts, while motivated by an ideological cause. Individuals or groups do not need to be defined as ‘terrorists’ by law enforcement to be considered a domestic extremism. Domestic extremism groups have a limited presence in the region when compared to other areas of the United States; however, the groups can increase their numbers for specific events. These groups have conducted vandalism, facility break-ins, and arson within the region, but none recent and not against electrical infrastructure. There is some intelligence to suggest domestic extremism groups within the U.S. have had the intent and capability to attack the power grid; however, there is no intelligence to suggest a campaign specifically against the company is currently being planned.

The following list pertains to persons, groups, and organizations that can be characterized as potential threats across the nation to the Bulk Electric and distribution system:

- Domestic Terrorist Organizations
- Outlaw Motorcycle Gangs
- Lone Wolf Terrorist
- Extremist Protest Groups
- Environmental Groups
- Militia Groups
- Organized Criminal Groups
- Miscellaneous Independent Criminals
- Disgruntled Employees
- Disgruntled Customers / Contractors

- Joint Regional Intelligence Centers
- Electricity Information Sharing and Analysis Center (E-ISAC) The E-ISAC website reports there are currently no threats to the Bulk Electric System. Bill Lawrence, the CSO and Vice President provided updated TLP- White materials.
- Homeland Security Information Network (HSIN) Daily Open Source Infrastructure Report - http://www.dhs.gov/dhs-daily-open-source-infrastructure-report
  The Protective Security Advisor (PSA) for the Southern California Region has a working relationship with Southern California Edison and other adjacent utilities with a reputation for directly sending out notifications for threats to critical infrastructure within the region.
- WECC Physical Security Work Group (PSWG)
- ASIS Utilities Security Council (USC)

During the TVA process, the assessor conferred with all of the agencies listed above to gather threat intelligence within the state and region against Bulk Electric System and distribution facilities. Based on the intelligence received, there are no active threats directed at Substation or other similar facilities in the state.

As part of the ongoing coordination to address security related concerns of the site the director of BVES, Paul Marconi meets on a monthly basis with local Law Enforcement and Fire Mitigation partners receiving information on local and regional threats:

Michael Antonucci- San Bernardino County, Office of Emergency Management, Manager
Phone (909) 356-3930 Email: Michael.Antonucci@oes.sbcounty.gov

Lt. Michael Salinas, California Highway Patrol, Arrowhead District Commander
Phone (909) 867-2791 Email: msalinas@chp.ca.gov

Jeff Willis- Big Bear Fire Department, Fire Chief
Phone (909) 866-7566 Email: jeff.willis@bigbearfire.org

Mitch Dattilo- San Bernardino County Sheriff's Office- Captain
Phone (909) 866-0100 Email: mdattilo@sbcsd.org

Design Basis Threat

The threat assessment consisted of reviews and analysis of reports from the intelligence community as well as communication with industry partners to identify potential adversary groups and their tactics. The assessment identified the following potential attack types that will be considered throughout the assessment:

Arson: The willful or malicious burning of property (such as a building) especially with criminal or fraudulent intent. Though the act typically involves buildings, the term arson can also refer to the intentional burning of other things, such as infrastructure, vehicles, vegetation or stored records. Assumptions:

1) Adversary desires to cause sufficient irreparable damage to the electrical site and throws an incendiary device at critical assets (e.g. Molotov cocktail).
2) The adversary has sufficient general knowledge of which components could cause damage or disruption while minimizing risks of self-injury during the act.

Scenario: Adversary desires to set fire to the vegetation areas outside the fence line to disrupt the site's functionality or the adversary throws an incendiary device from the fence line or enters the perimeter and pours accelerant on critical assets in an attempt to degrade or destroy them.

Ballistic Attack – Small Arms: The targeting of specific assets contained within the site or switchyard perimeter by an adversary who has physically breached the facility perimeter with the use of small arms (e.g. a rifle with an undetermined caliber). Assumptions:

1) Adversary desires to position themselves in the shooting position without detection and depart the area without apprehension after the event.
2) Adversary desires to engage a target at or below 300 meters from numerous hostile surveillance points.

Scenario: Adversary enters the heavy vegetation on the 360 Degree perimeter under the cloak of night and fires upon the transformer radiator causing mineral oil leakage that could lead to overheating and possible fire.

Explosive Device – Man Portable (IED): an event involving the deployment of a small explosive charge (e.g. contained within a backpack or pipe bomb) by an adversary to damage or disable all or a portion of an evaluated asset within a site. Assumptions:

1) Entry inside the secured perimeter fence is not required (e.g. a backpack thrown over the fence).
2) Targeted assets must be within 21 meters of the perimeter fence.

Scenario: Adversary throws a homemade pipe bomb over the small fenced in area from either direction, in the close proximity to any of the 3 transformers causing irreparable damage and the need for a replacement transformer.

Sabotage: an act in which an adversary acts to disrupt, or damage assets located within the perimeter of the facility. This includes incidents targeting the facility assets themselves and intentional acts at the facility intended to impact the transmission and distribution systems. Assumptions:

1) Adversary desires to enter the area undetected and depart the area without being apprehended.
2) The adversary has sufficient general/insider knowledge of which components could cause damage or disruption while minimizing risks of self-injury during the act.

Scenario: Adversary desires to enter Substation to turn off or disable switches and/or steal grounding copper wire, in the process is removing operational fail-safes to the site's equipment.

Vehicle-Ramming Attack: an assault in which an adversary deliberately rams a vehicle into a building, fence, or other property to cause significant damage to the site. Assumptions:

1) Adversary utilizes a passenger vehicle or steals nearby heavy equipment (bulldozer, forklift, etc.)
2) Vehicle is used to breach the fence line of the perimeter with the intention of crashing the vehicle into critical assets with the intention of causing damage to critical assets onsite

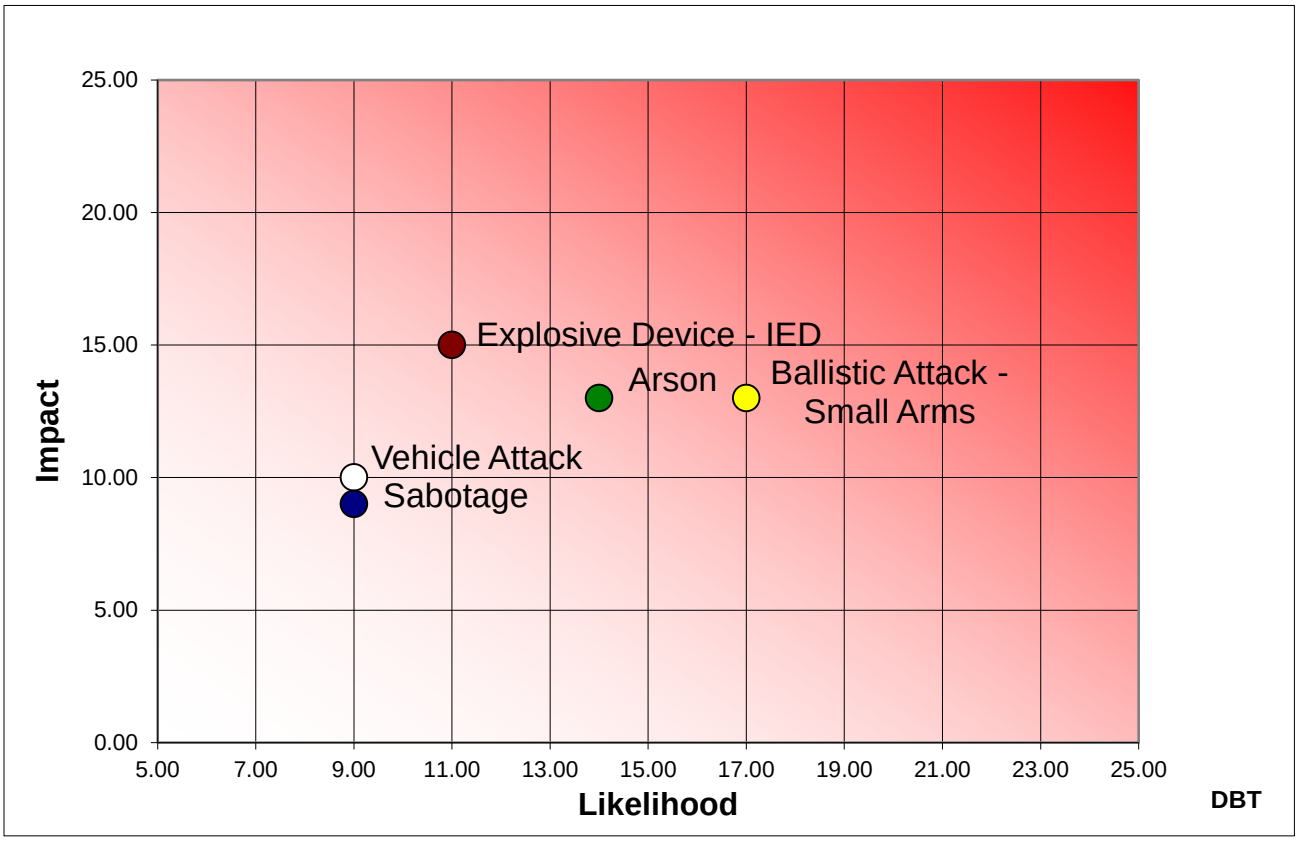
Scenario: Adversary breaches vehicle gate for a high-speed vehicle approach to breach the fence line of Substation, crashing into critical assets.

Drones/UAS: As the use of civilian owned drones have seen a significant increase in the last few years, it was determined that the use of drones or unmanned aerial vehicles may develop into an active threat but is currently still emerging and being refined. As additional information is received domestically and abroad, this threat may evolve as to its probability of use directed at the utility

industry or assets. If this occurs, the use of drones or unmanned aerial vehicles may be evaluated and assessed at the discretion of BVES leadership personnel, however, at the time of this assessment there was not sufficient information leading to the belief that drones were a credible threat.

Threat Spectrum

A Threat Spectrum based on the impact of the above listed attack types and their likelihood of happening. Following is a visual depiction of the threat spectrum ranking the threats according to impact and likelihood:



Site Security Assessment

Perimeter Fence- The entire facility is enclosed by approximately 90 feet of perimeter fencing. The fencing is made up of standard non-energized 7 ft 9-guage, 2-inch diamond-mesh chain-link topped with 3-strand barb wire with a 45-degree angle outrigger. There are no perimeter intrusion detection capabilities onsite. The fences are worn and have several areas that are broken down. The bottom of the fence is not recessed into the ground and can be lifted and breached. There are currently areas where the ground has been eroded due to weather and animal life, creating a security vulnerability. The fencing holds signage on all 4 sides in English warning of high voltage danger. The east and south perimeter has overgrown brush and ragweed bushes that could be used as cover and concealment.

South Side of substation

East side of substation

Gates- There is one personnel gate secured with a padlock and chain on the west side and additional two panel vehicle swing gate on the North side of the site secured with a standard commercial grade padlock and chain.

Terrain & Vegetation- The surrounding terrain is relatively flat and wide open with overgrown grass and other vegetation adjacent to the East fence line that provides multiple hostile surveillance points

from the east, west, and south. The wastewater treatment facility has several buildings and a black top parking lot.

Signage- Well designed safety and security signage can serve to provide legal property boundary definition, safety and security instructions, notification procedures, warnings for restricted areas and can be a deterrent to potential attackers. The only signage present on each side of the perimeter fence is a danger sign.

Access Control- The substation is located behind the controlled access gate into the water treatment facility that stays open during normal business hours. No other barriers exist to mitigate vehicle ramming or control access to the personnel gate.

Locks & Key Control- The current access control is a commercial grade padlock and chain with an uncontrolled system key.

Photo removed due to Signage identified site in question

CCTV- None

Lighting- Minimal streetlight to illuminate the substation

Intrusion Detection- None

Procedural- BVES has fully implemented Emergency Response and Business Continuity Plans. In addition, BVES has formalized security procedures for response to incidents.

Personnel- Unmanned facility with limited key accountability.

Principles of Physical Security

The principles of physical security are much the same as a thousand years ago with moats and drawbridges acting as deterrents and delay, however the technology has thankfully improved. Sound physical security requires a strategic approach that collectively deters, detects, delays, assesses, communicates and responds to any unauthorized access attempt to the site.

Deter:

- Deny adversaries access to the information and other resources they require to conduct attack planning
- Dissuade adversaries from conducting an attack through site hardening with an emphasis on the perception of an increased likelihood of failure or capture
- Project a sufficiently hostile view of the environment to an adversary so as to create a "target shift' whereby the potential attacker seeks a more attractive opportunity for success.

Detect:

- To identify threat or attack behaviors at every stage of an attack – planning, reconnaissance, deployment
- Increase the likelihood of malicious actors' detection through a combination of naturally occurring or man-made activity monitoring capabilities
- Initiate an appropriate response to a threat or attack as early in the attack timeline as possible
- Monitor for the introduction of people or things that should not normally be present
- Maintain integrity of access controls such as rigorous key management programs
- Loss of information or assets which have been moved off site

Delay:

- Maximizing the time between the detection of an attack (at any of the stages in the attack timeline) and an attacker reaching an asset(s) location to facilitate the potential interdiction or apprehension
- Limit availability/access to information in order to prevent an adversary developing an optimized attack plan – thereby increasing the attack timeline and further increasing the chances of detection

Assess:

- To identify if threat is credible, is individual supposed to be on or near the site.
- Follow procedure controls and inquire from Control or System Operations on an individual's reasoning for being on site.
- Determine appropriate response levels and initiate in a timely manner.

Communicate:

- To be able to contact and potentially direct response resources to an issue quickly and efficiently.
- Contacting employees, managers, contracted security officers, designates, or law enforcement.

Respond:

- An effective response counters the identified activity of an unauthorized person within a site.
- Depending on the severity, response may either be an employee, contracted security officer or law enforcement.

Prevention:

- Understanding the risk and deploying effective countermeasures to decrease the vulnerability.

Recover:

- An effective recovery plan minimizes downtime with on hand inventory, and periodic testing to ensure procedures are current, and employees are able to perform the task required to restore normal operations.

Vulnerabilities to DBT's

The Threat Assessment team reviewed each vulnerability based on current measures in place and identified potential security gaps which an adversary could exploit for nefarious purposes. The findings were broken down and identified using each potential attack type.

Arson:

Threat: Arson		**Site: Substation**
Objective	**Status**	**Countermeasures installed to mitigate vulnerability exposed by the threat.**
Deter	Current	Perimeter Fence, Signage
	Gap	No trespassing signage beyond the fence perimeter
Detect	Current	None
	Gap	No ability to detect adversaries at perimeter or beyond
Assess	Current	None
	Gap	No fire detection, intrusion detection, motion lighting, camera systems or video analytics
Delay	Current	Perimeter Fence (minimal) 10-30 seconds
	Gap	Perimeter fence provides minimal delay (7-10 seconds)

Communicate	Current	Alert LE, initiate response through procedural controls (Land Line, Cellular, Radio)
	Gap	No dedicated safety and security monitoring, No talk-down PA capability at the site
Respond	Current	Badged Law Enforcement Officer response time approximately 5- 10 minutes Onsite Personnel response time is 10-15 minutes
	Gap	The site does not have 24/7 onsite security technology, security officers or roving patrols

Ballistic Attack:

Threat: Ballistic Attack		**Site: Substation**
Objective	**Status**	**Countermeasures installed to mitigate vulnerability exposed by the threat.**
Deter	Current	None
	Gap	Critical assets are in the open and can be identified from beyond the perimeter
Detect	Current	None
	Gap	No ability to detect adversaries at perimeter or beyond.
Assess	Current	None
	Gap	No camera systems or video analytics
Delay	Current	No delay measures or ballistic protections currently deployed
	Gap	Multiple shooting lanes and hostile surveillance points for an adversary to attack the site
Communicate	Current	Alert LE upon notice, initiate response through procedural controls (Land Line, Cellular)

	Gap	No dedicated safety and security monitoring, No talk-down PA capability at the site
Respond	Current	Badged Law Enforcement Officer response time approximately 5-10 minutes BVES Personnel response time is 5-10 minutes during normal business hours
	Gap	The site does not have roving patrols.

Explosive Device:

Threat: Explosive Device		**Site: Substation**
Objective	**Status**	**Countermeasures installed to mitigate vulnerability exposed by the threat.**
Deter	Current	Perimeter Fence, Signage
	Gap	Perimeter fence is short and does not mitigate an adversary throwing a device into the substation at identified critical assets
Detect	Current	None
	Gap	No ability to detect adversaries at perimeter or beyond
Assess	Current	None
	Gap	No ability to assess adversaries at perimeter or beyond
Delay	Current	Perimeter Fence (minimal), Access Control (Mechanical)
	Gap	Perimeter fence provides minimal delay (7-10 seconds)
Communicate	Current	Alert LE upon notice, initiate response through procedural controls (Land Line, Cellular)

	Gap	No dedicated safety and security monitoring, No talk-down PA capability at the site
Respond	Current	Badged Law Enforcement Officer response time approximately 5-10 minutes BVES Personnel response time is 5-10 minutes
	Gap	The site does not have roving patrols

Sabotage:

Threat: Sabotage		**Site: Substation**
Objective	**Status**	**Countermeasures installed to mitigate vulnerability exposed by the threat.**
Deter	Current	Perimeter Fence, Signage
	Gap	Replace Danger Signs as they are faded/illegible, no security signage beyond the fence perimeter
Detect	Current	Random surveillance scans of Water treatment by plant employees and BVES employees accessing the site periodically
	Gap	No ability to detect adversaries at perimeter or beyond
Assess	Current	Human Observation
	Gap	No ability to assess without CCTV
Delay	Current	Perimeter Fence (minimal), Access Control (Mechanical)
	Gap	Perimeter fence provides minimal delay (7-10 seconds), physical key control
Communicate	Current	Upon notification initiate response through procedural controls (Land Line, Cellular)

	Gap	No dedicated safety and security monitoring, No talk-down PA capability at the site
Respond	Current	Badged Law Enforcement Officer response time approximately 10-20 minutes BVES Personnel response time is 5-10 minutes
	Gap	The site does not have 24/7 onsite security officers or roving patrols

Vehicle Attack:

Threat: Vehicle Attack		**Site: Substation**
Objective	**Status**	**Countermeasures installed to mitigate vulnerability exposed by the threat.**
Deter	Current	None- Chain link fence is exposed on all 4 sides when access control gate is open
	Gap	No anti-ram gates, standard chain link fence perimeter
Detect	Current	None
	Gap	No ability to detect unauthorized vehicle that entered site using an unmonitored gate
Assess	Current	Random Human Observation
	Gap	The site is unmonitored
Delay	Current	Perimeter Fence (minimal), Access Control (Mechanical) Terrain in the winter months
	Gap	Perimeter fence provides minimal defense, no barriers in place along fence-lines, no anti-ram or crash rated gates and fencing controlling access to the wastewater facility
Communicate	Current	Alert LE, initiate response through procedural controls (Land Line, Cellular)
	Gap	No dedicated safety and security monitoring, No talk-down PA capability at the site

Respond	Current	Badged Law Enforcement Officer response time approximately 5-10 minutes BVES Personnel response time is 5-10 minutes
	Gap	The site does not have 24/7 onsite security officers or roving patrols

Perimeter Standoff

As threats become more dynamic in an environment where response capabilities can be limited and effects more severe, standoff from Critical assets can be crucial to affecting change during the target selection phase, increase the probability of generating a target shift, and aid in earlier detection. Standoff distance is best defined as the distance that can be obtained between a Critical asset and a particular threat. Detailed in the following sections are observations for each external threat vector based on the current site layout.

Arson & IED: All of the critical assets of the substation are close to the estimated 21-meter maximum IED range, and vulnerable to attack from someone outside the fence line. The critical assets being inside the small confined substation has maximum risk from an IED or incendiary attack from the entire fence line.

Ballistic Attack (Small Arms): The greatest vulnerability to the 3 critical assets within this particular threat vector is derived from the substation's location. It was estimated that an adversary would potentially fire at a target within a 300-yard range. The photos reveal that there are many areas in which an adversary could conceal themselves within the 300-yard radius and have a clear line of site to multiple critical assets.

Lighting: Current lighting systems provide minimal illumination to the critical assets as well as the access gates. A lighting system is in effect near the northwest fence line perimeter of Substation. Illumination of critical assets at night increases the likelihood of an adversary who plans on shooting at the facility, of being able to clearly find their intended target under the concealment of night. The site was not assessed during nighttime conditions.

CARVER is an offensive target assessment tool originally developed for use by the U.S. Military and the Intelligence Community in evaluating the vulnerabilities of enemy assets and determining how best to exploit those vulnerabilities to attack a target. The CARVER Vulnerability Assessment process is currently being used in the Department of Homeland Security's Automated Critical Asset Management System (ACAMS). ACAMS provides a set of tools and resources that help law enforcement, public safety and emergency response personnel assess Critical Infrastructure/Key Resource (CI/KR) Asset vulnerabilities.

The CARVER methodology addresses both physical security of a facility and the operational capabilities of terrorists or other adversaries by quantifying the likelihood of an attack based on target weaknesses. It acts as a target selection tool that uses a numerical ranking methodology to identify targets most attractive to attack by an adversary. To assess the likelihood of attack for a potential target, CARVER analyzes the following targeting criteria:

- **C**riticality **-** Single points of failure, degree of importance to the system
- **A**ccessibility **-** Ease of access to critical points of a facility or asset, and their exposure to adversarial acts
- **R**ecoverability **-** The time and effort to recover system operation after an adverse event
- **V**ulnerability **-** Level of exposure to attack based on adversary capability
- **E**ffect **-** Scope and magnitude of adverse consequences that would result from malicious actions and response to them
- **R**ecognizability **-** Ability of an adversary to recognize assets, security systems, vulnerabilities, etc.

This assessment was completed through the eyes of an adversary and encompasses the following basic principles: Examination of all security programs from the terrorist or adversary's viewpoint, (i.e., how would I, if I were the adversary, attack this asset and what would I target?); A determination is made as to what countermeasures would be required to prevent the terrorist or adversary from achieving success and thus launching and completing the operation; and the assumption that conspicuous security procedures and equipment will not stop a determined terrorist or other adversary.

The relative risk for each threat and target combination is determined using algorithms to analyze potential consequences, relative importance of targets to the aggressor, and security vulnerability levels. Countermeasures are then developed to minimize the risk and; subsequently, the

methodology is re-applied to determine if risk reduction is achieved. This iterative process is continued until the most cost-effective method of reducing the risk to an acceptable level is identified.

CARVER Scale

The values 1-5 are used to calculate Risk and Probability of Attack (Pa) in the CARVER Matrix. The higher the number the higher the Risk and Probability of Attack.

Value	C	A	R	V	E	R
5	Damage or loss of this asset will significantly impact/stop the assets output or operations	Easily accessible, unlimited access with no security measures to prevent or detect	Extremely difficult to replace, long down time	A dedicated adversary with little capability and expertise can easily damage or destroy asset	Very high: damage will have significant sociological, economic, or reputational impacts, including loss of life and injuries	Easily recognizable and requires little or no training to identify
4	Damage or loss of this asset will greatly reduce the assets output or operations	Accessible, limited access with some basic security measures in place to prevent (fence, doors, locks, etc.)	Difficult to replace with long down time	A dedicated adversary with some capability and expertise most likely will damage or destroy asset	High: damage will have sociological, economic, or reputational impacts, including some loss of life and injuries	Easily recognizable and requires a small amount of training to identify
3	Damage or loss of this asset will reduce the assets output or operations	Somewhat accessible, but threat of observation exists. Some security measures are in place (such as CCTV or onsite personnel)	Replaceable with a relative short down time	A dedicated adversary with capability and expertise can easily damage or destroy asset	Moderate: damage may have sociological, economic, or reputational impacts, with no loss of life and may have injuries	Difficult to recognize and may be confused with other equipment and requires some training to identify
2	Damage or loss of this asset may reduce the assets output or operations	Difficult to gain access, physical security barriers, observation, and alarms are in place. Access granted to authorized personnel only.	Easily replaceable in a short time	A dedicated adversary most likely does not have the capability to damage or destroy asset	Low: damage may have sociological, economic, or reputational impacts, with no loss of life or injuries	Difficult to recognize, easily confused with other equipment and requires extensive training to identify
1	Damage or loss of this asset will not impact output or operations	Not accessible, defined means of intervention in place.	Immediate replacement, spare parts are readily available or asset redundancy	A dedicated adversary does not have the capability and expertise to damage or destroy asset	None: damage or loss of this asset will have no unfavorable impact	Unrecognizable except by experts

CARVER Rating - Arson							
Substation							
Asset	C	A	R	V	E	R	Total
34kV Feed line	5	4	1	5	2	5	22
Transformers	5	4	1	5	2	4	21
Circuit Breakers	5	4	1	5	2	4	21
Voltage Regulator	5	4	1	5	2	4	21

CARVER Rating - Ballistic Attack							
Substation							
Asset	C	A	R	V	E	R	Total
34kV Feed line	5	4	1	5	2	5	22
Transformers	5	4	1	5	2	4	21
Circuit Breakers	5	4	1	5	2	4	21
Voltage Regulator	5	4	1	5	2	4	21

CARVER Rating - Explosive Device IED							
Substation							
Asset	C	A	R	V	E	R	Total
34kV Feed line	5	4	1	5	2	5	22
Transformers	5	4	1	5	2	4	21
Circuit Breakers	5	4	1	5	2	4	21
Voltage Regulator	5	4	1	5	2	4	21

CARVER Rating - Sabotage							
Substation							
Asset	C	A	R	V	E	R	Total
34kV Feed Line	5	4	1	5	2	5	22
Transformers	5	4	1	5	2	4	21
Circuit Breakers	5	4	1	5	2	4	21
Voltage Regulator	5	4	1	5	2	4	21

CARVER Rating - Vehicle Attack							
Substation							
Asset	C	A	R	V	E	R	Total
34kV Feed line	5	4	1	5	2	5	22
Transformers	5	4	1	5	2	4	21
Circuit Breakers	5	4	1	5	2	4	21
Voltage Regulator	5	4	1	5	2	4	21

CLOSING STATEMENT

The motivation for the physical hardening of a site is based on generating a desired “target shift” away from Substation assets. The perceived physical security condition of a site is most often drawn from the first security component encountered by a potential adversary. BVES will need to use CPTED in conjunction with electronic based security initiatives and other physical security elements wherever possible to minimize program cost, reduce the target attractiveness of a given asset, and increase the sustainability of the security features at the Substation. CPTED is based on four fundamentals:

- Natural Surveillance: The adversary does not want to be seen. Increasing the probability of detection through the reduction of surveillance areas, increasing "normal" user traffic, and minimizing the number of places an adversary can hide.

- Territorial Reinforcement: The use of walls, signage, gates, landscaping and fences to express ownership and control of a given area. Potential offenders perceive this control and are aware of transition points between public and private realms.

- Natural Access Control: The effective use of signage, barriers and landscaping to naturally flow pedestrian traffic around the site as well as to designate authorized entrances.

- Maintenance: The proper cleanliness and maintenance of the site. This includes clean, undamaged, and serviceable signage as well as the site and nearby grounds free of trash and debris.

The utilization of CPTED principles in conjunction with traditional security measures such as surveillance cameras, electronic access control devices, intrusion detection equipment, roving security patrols and law enforcement engagement will produce a holistic and sustainable security program. This security program is traditionally less expensive to maintain, operate, and provides a significant prevention component.

The next steps BVES will need to take in the coming months are to address some of the immediate concerns with the ease of site accessibility, no substantive concealment or delay to the critical assets, and no detection and assessment capabilities. However, a more detailed Physical Security Plan with recommendations that will mitigate the threats to the site's critical assets is provided congruently for considerations.

Upon successful implementation of new security measures that are designed to mitigate the five identified threats, a supplemental assessment may be conducted by BVES to appropriately determine the post mitigation ratings. If and when new threat intelligence is obtained and there is a credible threat in the state or region directed at Bulk Electric System facilities or BVES distribution assets, the assessor and management team will reconvene to determine if current security measures are sufficient to mitigate the new threat and if not, then deploy new and additional security measures.

Revision History

Revision	Contact	Description of Changes	Revision Date
Original	Darren T Nielsen Paul Marconi	Original	7/25/2019

Assessor's Certification Verification

My Certifications

Certification	Certification #	Certification Date	Renewal Due Date
CPP	14589	05/24/2010	12/31/2019
PCI	16088	12/21/2012	01/31/2022
PSP	15782	06/16/2012	01/31/2022

Assessor's Biography

Professional Summary

Darren joined Navigant's Global Energy practice in January 2019 as an Associate Director. He was most recently a Manager of Physical & Cyber Security Audits & Investigations at the Western Electricity Coordinating Council (WECC). He is extremely effective in a variety of related areas that include planning, execution of special operations, administrative audits, and the development and implementation of a broad range of topics involving internal and external compliance.

Professional Experience

Western Electricity Coordinating Council | Manager, Physical & Cyber Security Audits & Investigations

- Directly responsible for oversight of comprehensive on-site and off-site audits of registered entities in compliance with NERC reliability standards and WECC regional reliability standards, with a special emphasis on the Critical Infrastructure Protection (CIP) Physical & Cyber Security standards.
- Oversaw development and conducted training workshops on a national level for Critical Infrastructure Protection Standards.
- Managed the compliance audit & Investigations processes of the WECC CMEP related to the CIP standards; cyber and physical
- Supervised the Cyber Security Audit Teams during the performance of CMEP processes to include risk assessment, mitigation plan acceptance, completion and validation
- Created and supervised preparation of audit reports with a focus on clear findings documentation and logic trails.
- Supported the Vice President, Entity Oversight in the implementation of the WECC CMEP and specifically the implementation and development of processes associated with audits and mitigation plans.

- Assisted enforcement staff as needed in preparing evidence for use in hearings, settlements, and appeals.
- Developed and presented at WECC Compliance Meetings, Regional Working Group Meetings, NERC and FERC Meetings.
- Developed individual development programs to increase expertise and competency; build bench strength for the department and company.

As a Senior Compliance Auditor at WECC:

- Conducted comprehensive on-site and off-site audits of registered entities in compliance with NERC reliability standards and WECC regional reliability standards, with a special emphasis on the Critical Infrastructure Protection (CIP) Physical & Cyber Security standards.
- Developed and conducted training workshops on a national level for Critical Infrastructure Protection Standards.
- CIP - Directly responsible for the implementation, design, and compliance of policy and procedure to meet the NERC Critical Infrastructure Protection guidelines at all facilities system-wide.
- Direct oversight for proactive audits, regulatory overview and corrective action.
- Managed and had direct oversight for security incidents/investigations regarding internal/external matters.
- Managed risk and threat assessments for all company facilities annually.
- Managed the overall process for policies and procedures development and disposition.
- Assisted the Director in providing direction and oversight to Corporate Security functions.
- Interacted and partnered with Senior Management on issues related to policy, procedures, information governance, and Human Resource matters.

Arizona Public Service | Corporate Security Program Advisor

- CIP - Direct responsibility for the implementation, design and compliance of policy and procedure to meet the NERC Critical Infrastructure Protection guidelines at all facilities system-wide.
- Chair of the Western Electricity Coordinating Council (WECC) Physical Security Workgroup.
- Gained an authoritative understanding of the CIP Standards used to document and ensure APS achieved compliance in accordance with NERC requirements. Zero infraction audit achieved
- Conducted proactive audits, risk and threat assessments for all company facilities annually.
- Assisted the Director in providing direction and oversight to Corporate Security functions.
- Developed a working and professional relationship with the law enforcement personnel at the Arizona Counter Terrorism Information Center (ACTIC).
- Interacted and partnered with senior leadership on issues related to policy, procedures and human resource matters.
- Investigated security incidents assigned by the Security Director regarding internal/external criminal matters and revenue recovery issues.

Phoenix Police Department | Police Sergeant

- Supervisor responsibilities for responders, encompassing vast array of different scenarios.
- Coordinated work with various community leaders and organizations to formulate policies and procedures to assist with quality of life issues.
- Prepared daily training and managed day-to-day operations of the command officers unit including all administrative, investigative, and human resource issues.
- Developed and conducted training in the areas of occupational safety, hazardous materials, traffic safety, substance abuse and other safety-related issues.

As a police officer with the Phoenix Police Department, held responsibility for:

- First response to various types of criminal and non-criminal events.
- Creating and maintaining, strong, positive, professional relationships with customers, colleagues, and community partners.
- High level organizational skills with respect to managing investigations, briefing superiors, ensuring compliance in all legal and internal regulations, caring for personal property and health and welfare of citizens.
- Working with community leaders, political figures, and community professionals to provide drug identification education and training.

Work History

- Associate Director, Navigant
- Manager, Physical & Cyber Security Audits & Investigations, Western Electricity Coordinating Council
- Manager, Corporate Security Compliance & Investigations, Southern Cal Edison
- Corporate Security Program Advisor, Arizona Public Service |
- Police Sergeant, Phoenix Police Department

Certifications, Recognitions, Memberships, and Awards

- Executive Board member (President) of Silent Witness of Arizona, a non-profit 501 c(3)
- ASIS International Board of Directors 2018-2020 Term
- ASIS International Council Vice President (2016-2019 term)- Appointed to Board of Directors 2018
- ASIS International Utilities Security Council (Chair) 2012-2015
- ASIS International Physical Security Council (Member)
- ASIS, Certified Protection Professional (CPP), Board Certified in Security Management
- ASIS, Physical Security Professional (PSP), Board Certified in Physical Security
- ASIS, Professional Certified Investigator (PCI), Board Certified Investigator
- ISC^2, Certified Information Systems Security Professional (CISSP)

- NDPC, Certified Homeland Protection Professional (CHPP)
- BRCCI, Certified Business Resilience Auditor (CBRA)
- BRCCI, Certified Business Resilience Manager (CBRM)
- BRCCI, Master Attainment Business Resilience (MABR)
- ISACA, Certified Information Systems Auditor (CISA)
- ISACA, Certified Information Security Manager (CISM)
- United States Marine Corps 1990-1997 (2) Meritorious Promotions
- Medal of Lifesaving 2001 Phoenix Police Department
- Professional of the Year 2004 Arizona Safety Education Association
- Outstanding Young Arizonan 2004 Arizona Junior Chamber
- Distinguished Service Award 2005 Phoenix Police Department
- Council Chairman of the Year 2015 ASIS International

Education

- MBA (emphasis in Leadership) With Distinction, Northern Arizona University Phoenix Campus
- BA, Police Science (Summa Cum Laude), Ottawa University Phoenix, AZ
- ASIS International Security Executive Management Program, Wharton School, University of Pennsylvania