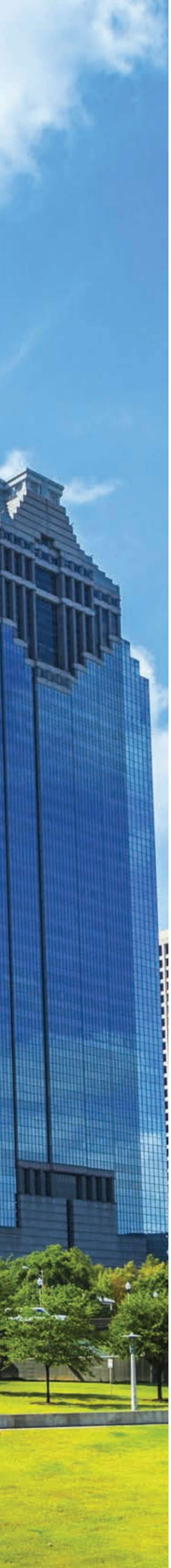
ENSC MAGAZINE

Houston, Texas

Volume 2 | Edition 2 | Fall 2019



Time flies!

Preparations have begun for our upcoming ENSC in Houston, Texas, co-hosted by CenterPoint Energy. It just seemed like it was a short while ago that we had the ENSC in San Francisco, but father time does not slow down for anyone, and the 21st ENSC is just around the corner. Please make sure that you spread the word to your colleagues about supporting the conference. We opened up early discount registration starting in October for those wanting to book in 2019. Our ENSC Council has been working hard to raise the bar for each and every ENSC conference and tailor the conference to fit the needs of the industry. In 2020, we are planning on enhanced round table sessions to spread the knowledge of underground networks. In addition, our engineering course is being tweaked to expand on designing a new spot network using real time data and models for load flow. In the maintenance and troubleshooting departments, expect a more hands on approach with the equipment than in years past. Our drive to educate in the area of power distribution continues and we look forward to your participation!

In our effort to increase awareness in many areas of network underground, the accompanying ENSC magazine is a handy reference for key articles and support material. This will be our 4th addition of the digital and print versions. Please take a look at Portland General's new Marquam substation build and subsequent network protector feeder changeover article authored by Ricardo Garcia. This is a really good story on what it looks like when things go as planned and the effort that goes into making sure a project of this scale goes off as expected.

We are always looking for great content for both the ENSC and the ENSC magazine, so please send us your thoughts.

We look forward to seeing everyone at the ENSC in Houston in 2020!

Respectfully,

Mark Faulkner
Product Line Manager
Eaton

ENSC Advisory Council Members:

Maria Ly
Pacific Gas and Electric

Shane Powell
Alabama Power Company

Ryan Bradeen
Avista Corp.

Rick Kernan
Xcel Energy

Robert Spelman
Pepco Holdings Inc.

ENSC Magazine

Tony Oruga, P.E.
Eaton
1520 Emerald Rd.
Greenwood, SC 29649

AntonioROruga@eaton.com
(864) 330-2461

TABLE OF CONTENTS

ENSC – The Network Solutions Magazine

SAVE THE DATE

Hosted by: CenterPoint Energy

April 6th-9th 2020

Sponsored by: EATON Powering Business Worldwide

21st Annual Electrical Network Systems Conference

HOUSTON, TX

System Communications on Secondary Networks

Bob Page, Lead Product Engineer, Eaton

Monitoring the secondary network has become more commonplace in the network underground, as out-of-sight and out-of-mind is no longer the industry norm. As part of the industry's initiatives for providing safer environments for employees and pedestrians alike and providing remote observation through communications, intelligent decisions can now be made in the areas of predictive maintenance and failure mitigation. How this is accomplished varies vastly depending on a plethora of factors. The three most common factors that drive the solution are the utility's specific requirements, infrastructure and planned funding.

Once these three main factors are established the ideal communications system for the utility will start to take shape. This article was created to provide users with a synopsis of considerations when evaluating what type of system is right for you. When looking to gain visibility, control, and analytics from a secondary network monitoring system there are several points of interest:

**Note - Examples are based on Eaton offerings*.

Network Protector

- Interval Data logging (Voltages, Currents, VA, kVA, PF, number of operations etc.) to identify loading characteristics, predict maintenance schedules that could be determined from the load of the network and/or number of operations of the protector.
- Email notifications can be sent directly from the Eaton VaultGard that will notify users of any data point monitored by the network protector relay when it exceeds a user defined alarm value (location intrusion, protector status, overloading, etc.)
- Remote operation that eliminates the risk involved sending crew members down in a vault to manually open/close a protector/primary switch.
- Leveraging communications for personal safety (remote racking, ARMS, RAD) when maintenance work is being performed

Network Transformer

- Due to the high costs associated with network transformer change outs and the aftermath from a failed transformer, utilities are interested in monitoring factors that decrease the life expectancy of the transformer and show early warning signs of pending trouble. The primary aging factors of transformers are temperature and time. Therefore, monitoring the temperature in the transformer tank along with the ambient temperature is necessary for predicting the life expectancy or providing predictive data. These analytics can be performed to monitor transformer health such as gas analysis, pressure, oil level and environmental conditions.

Primary Side Switch/Interrupter

- More utilities are leveraging the use of a primary fault interrupter for point isolation, to avoid the nuisances with dropping the substation feeder and having all protectors associated with the feeder respond versus have just isolation at the required network protector/transformer combination.
  - Protective relays are added for primary fault protection. Eaton's VisoVac come standard with the Digitrip protective relay which can be used with VaultGard to remotely control, activate ARMS and monitor all measured and calculated data on the medium voltage side.

Vault, Location or Environmental

- Vault ambient temperature plays an important role in the life expectancy the equipment inside the vault and should be monitored.
- Intrusion alarm at vault or location entrances are common among many utilities to alert on an unauthorized person entering the vault.
- Vault float switches should be installed in every underground vault that is susceptible to flooding. This switch can alert dispatch through SCADA or crew members via VaultGard email as well as autonomously starting a pump motor to remove the water.
- Equipment protection such as fire protection is a consideration, especially for building vault spaces. Using a system such as Eaton's high thermal event system can provide autonomous protective control if sensors pick up heat on the collector or inside the protector.

Cybersecurity

The method of how the world communicates is dynamic and ever-changing. As a result, for every new advancement in technology there are often new cybersecurity threats developed to challenge the security of that new advancement. Utility communications are susceptible to those same cybersecurity threats. Every utility has their own policies and practices in place to protect, detect and respond to cybersecurity threats.

Identifying specific policy, guidance or prescriptive standards to address cybersecurity is beyond the purpose of this article but should be reviewed with local utility directors responsible for compliance with established industry mandates. Cybersecurity comes in many styles with different motives.

Common Utility Threats:

- Disgruntled Insiders
- Competing Financial interests
- Nuisance hackers
- Terrorist organizations/foreign governments

Example Cyber-attack techniques:

- Mapping – The process of gathering information about a network with the intent of using this data to exploit a weakness or do damage.
- Ping sweeper – An automated program to determine the IP addresses of machines on the network by simply observing which addresses respond to a ping message.
- Port scanner – The technique of sequentially contacting IP port numbers on a device and seeing how it responds.
- War dialers – A computer program used to identify the phone numbers that can successfully make a connection with a computer modem.
- War drivers – The act of locating and possibly exploiting connections to wireless LANs while driving.
- Denial of Service (DoS) – A deluge of counterfeit network traffic directed at a host computer. The goal of this attack is to consume system resources and thereby make legitimate access to the network or system difficult if not impossible. Some common forms are buffer overflow attack, TCP SYN field attack, smurf attack, and viruses.
- Physical infrastructure attack – Damaging some portion of the communications infrastructure.
- Application layer threat – Attacking known weaknesses in computer programs or by replacing applications with "Trojan horse" versions.
- Gaining access – The desire and ability to take control over some portion of the network or the cyber assets on the network. Some common techniques are password attacks, packet sniffing, spoofing, and man-in-the-middle attacks.

Every utility should create a security policy to educate all persons in the organization (including contractors/consultants) on what they can and cannot do. All points into the network and connections to all IEDs should be controlled and contain the minimum features:

- Backup and Recovery of data
- Controlled User access
- Activity Logging and Alarming
- Firewalls/connections to the enterprise
- Virtual Private Networks (VPN)

Eaton VaultGard™ Security Features:

- Authorization, Authentication and Accounting for Access control – The VaultGard supports Remote Authentication Dial-In User Service (RADIUS) protocol for remote authorization, authentication and accounting. Local access may be made with a locally stored password when the RADIUS server is unavailable. The locally stored passwords are remotely updateable and can be changed on predetermined intervals. The device can log accesses and changes when local credentials are used and set a status flag indicating local access.

The VaultGard also can be configured as a client in a Lightweight Directory Access Protocol (LDAP) network.

From a cyber security standpoint, the use of RADIUS is the recommended protocol for authorization and authentication due to its ability to perform multilevel authentication with the use of multiple servers. There are a several differences between RADIUS and LDAP network design and operation used for Centralized Authentication that is beyond the scope of this article, but should be reviewed prior to implementation.

- Secure Provisioning and Management – When configuring, provisioning or managing a device remotely using a network interface; the transport is encrypted. VaultGard has a Disposal function, to remove all configurations and reset the device for reuse or disposal. The function will erase or destroy the data storage media to a level that will prevent unauthorized access or recovery.

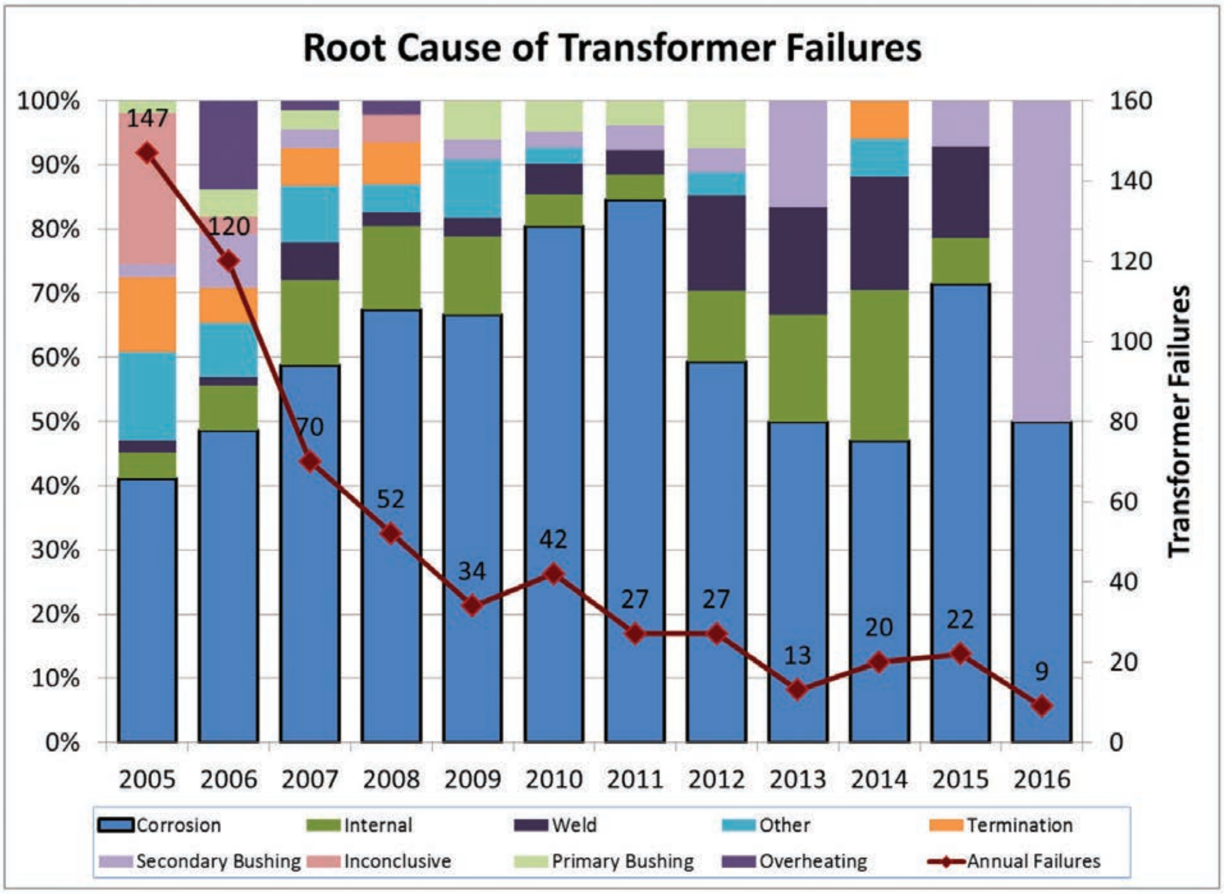
- Communication Security – Communications security is maintained throughout the communication path using physical/electronic protection mechanisms between the relay and VaultGard. Communications security is at the VaultGard level. The application uses strong encryption, data integrity verification and authentication to communicate with backend systems. The device supports IPsec VPN (with IKE) to the enclave firewall.

- Device and System Level Security
  The VaultGard provides the following features:
  - Supply a recommended operating baseline of open ports and services. All unused ports or service shall be disabled.
  - Support security login banners: The banner displays as a modal dialog on which the user must click an agree button before continuing to the VaultGard screen.
  - Log anomalies, user access, status changes of processes/applications, configuration changes, upgrade events, command and control operations.
  - Verify firmware, software and configuration before booting.
  - Support a secure remote update process that is centrally managed. Support automated patching of associated firmware and software.
  - VaultGard does NOT execute any arbitrary code uploaded by the user. All actions initiated by the user, including configuration file upload, are controlled by strictly typed and enforced data parameters.

There are only two vectors by which malware could possibly be installed; root access and firmware upload. VaultGard addresses each risk by the following:

1. Root access is only granted by enabling SSH and by uploading a public key file, which requires RADIUS authorization.
2. The second potential point of entry is firmware upload. Starting with firmware version 1.2.0 series, the VaultGard firmware distributions are signed.

Network Transformer and Location Communications



Con Edison – ENSC Magazine Volume 1, Edition 1 2018

- Security Standards supported by VaultGard
  FIPS PUB 140-2
  FIPS PUB 197
  NIST Special Publication 800-53
  NIST Special Publication 800-56A
  NIST Special Publication 800-57
  NIST Special Publication 800-97
  NIST Special Publication 800-121
  NIST Special Publication 800-124
  NIST Special Publication 800-153

Network transformers are typically the most expensive, heaviest and largest piece of equipment located in the secondary network system. They can experience heavy loading and most are installed in locations with harsh environmental conditions. Systemic transformer issues can create a large financial burden for the utility and cause increased liability. Therefore, monitoring of the network transformer is crucial for predictive maintenance and network system reliability. Typical monitoring of the network transformer can include the following:

- Oil level – main tank, switch tank and termination chamber
- Oil temperature – main tank, switch tank, termination chamber or tank surface temperature
- Pressure – main tank, switch tank and termination chamber
- Sudden pressure – main tank
- DGA – dissolved gas analyzer

Rugged subsurface rated gauges are ideal for transformer sensing especially in the underground vault space. These gauge outputs are collected through a gateway module that will transmit this data back through the user's communication medium. Ideal configurations use a separate collector from the network protector relay to make unique IP address configurability available. The amount of cable runs and penetrations should be considered when developing a network transformer communication scheme. In most cases, location or environmental monitoring and control can be accomplished using the same gateway depending on the number of configurable inputs. Monitoring and control can include the following:

- Ambient temperature
- Water level
- Gas monitoring
- Intrusion alarms
- Control for fans, pumps, lights

Control functionality can include SCADA activated, localized intelligent-activation or analog control of devices.

Portland General's Network Substation Improvement Project

Ricardo J. Garcia, Sr Network Planning Engineer
Frederick Harris, Distribution Planning Manager
Kenneth Atagabe, Sr Operations Network Engineer
Ezra Richards, PMO Manager
Daniel McArdle-Jaimes, Sr Communications Consultant

Headquartered in Portland, Oregon, Portland General Electric (hereinafter referred to as PGE) provides electric service to over 850,000 customers in 51 cities in Oregon. PGE servers the downtown Portland area with a unique low-voltage network system. Today, this unique system consists of a total of 5 network groups with each having 4 primary network feeders and a total 239 network transformers combine, serving over 2,100 commercial and residential customers, including 24/7 businesses such as: hotels, restaurants, convenience stores, and federal/state facilities.

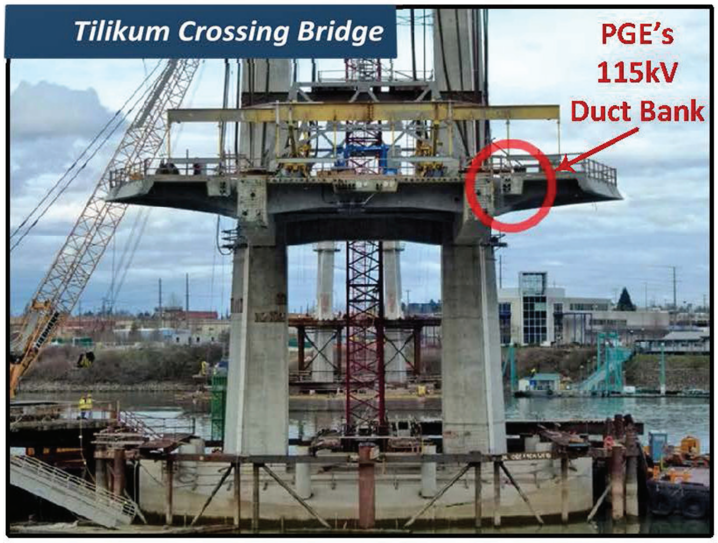
In December 1997, PGE's T&D Planning team completed a risk evaluation of the continuing operation of PGE's 11kV submarine cables that reside in the bed of the Willamette River, while considering the projected radial load growth in the South Waterfront area. The risk evaluation and area capacity analysis concluded that for PGE to increase reliability for the downtown Core and meet South Waterfront's load growth, PGE must build a new network substation near downtown Portland with the ability to serve both the downtown network as well as surrounding radial areas. Only this solution will effectively address the operational risk of the submarine cables and provide future transformation capacity. Thus, in 2003, PGE embarked on a 16-year strategic project plan that included the following key components: upgrading network transformers, splitting an eight-feeder network group to two four-feeder network groups, converting eight-feeder from 11kV to 13kV, reconstructing two distribution substations, constructing a new (Marquam) substation, and constructing new underground transmission and distribution pathways in an extremely dense area.

Marquam Substation Project

The resulting Marquam Substation Project provided paralleled 13kV distribution sources to Portland's downtown network system and new radial sources for future development of the South Waterfront area. Additionally, Marquam substation was designed to be served from two existing 115kV transmission lines and one new 115kV underground transmission line sourced from the east-side of the Willamette River.

With the new 115kV underground transmission source, PGE worked with local government agencies to place a 115kV duct bank inside the decking of the Tilikum Crossing Bridge which at that time was in the process of being engineered.

To improve network system operations, Marquam Substation's 13kV design consisted of four 13kV buses in a ring-bus configuration served by three 50 MVA substation transformers. New feeder getaway pathways from Marquam



Substation consisted of four 48-inch diameter casings that were bored through the Interstate-405 underpass; each of these casings consisted of 14 six-inch conduits. The resulting tunnels were 235 feet long with an upward angle of 10.5 degrees; each tunnel reached its target by three-quarters of an inch or less. With the Interstate-405 bore completed, one of the final excavation tasks was to complete full conduit pathways to the nearest interconnection locations to the existing 11kV network primary feeders in the downtown Portland area.

Group Network System Cutover

To transition the two old Stephens' 11kV group network systems to the new Marquam substation 13kV network system, PGE planned two 60-minutes customer outages for a "drop-and-pick" group network system cutover. PGE's Engineering team evaluated the possibility of a "close-transition" cutover but concluded that the difference of transmission and distribution source voltages, bus voltage phase angles, and available fault current could pose operational risk and minimize safe execution.

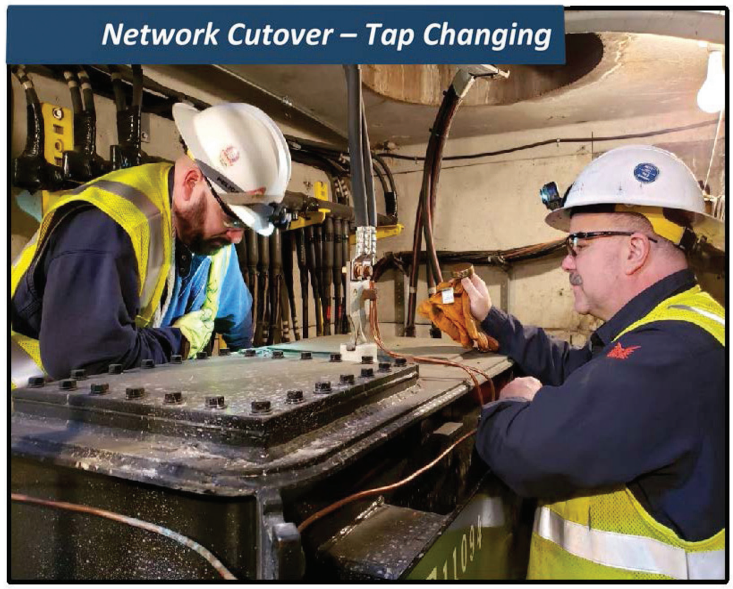
During the operational planning of the cutover, PGE's engineering team evaluated the greatest risks associated with the execution of a drop-and-pick cutover. The risk analysis concluded that the three most immediate operational risks were: (1) the variances on closing time among the first network protectors from the time of energizing Marquam's 13kV primary feeders, (2) phase sequence being rolled at the interconnection point of Marquam and Stephens network feeders, and (3) cable limiters in the 216-volt secondary mains that had no indication as to whether they were blown. To address these risks, PGE's Operations Team developed plans: (1) to manually close all the 216V grid network protectors before re-energizing the network system from Marquam Substation, (2) to extensively test the phasing at Marquam Substation, Stephen Substation, and at the join point of both primary cables, and (3) to manually measure the currents at specific secondary grid manhole locations.

PGE's Communications Team worked with local/state agencies to identify the two outage dates and expected durations of the outages, and then, planned an extensive communication and outreach strategy to fully inform PGE's downtown customers. To support this initiative, the Communications Team developed: mailers/fact sheets, email notifications, posters for storefronts and transit stops, a website, and social media postings. The Communications Team also worked with the City and County to inform the visually impaired community and worked with the Joint Homeless Outreach Team to raise awareness of the outages. Additionally, PGE hosted several workshop meetings with local and state agencies to: gather feedback, address public concerns, and review emergency preparation procedures for each outage date. To ensure safety of high-rise buildings, PGE's Key Customer Team engaged in multiple conversations with building facility managers to review electrical equipment safety, elevator safety, outage duration, back-up generation, and emergency contact information during the outage.

At PGE, customer and employee safety are the highest priority on any job; thus, as the outage dates approached, PGE activated an Emergency Operation Center (EOC) with the Portland Police Department to safeguard and protect all members of the public and PGE employees. Additionally, to ensure smooth operations, PGE's Operation Team trained extensively through several "dry-run" scenarios to ensure understanding of job tasks and appropriate response to any situation.

The famous quote "everybody has a plan until they get punched" resonated with the Operations Team 2.5 weeks before the first downtown outage. As PGE completed the

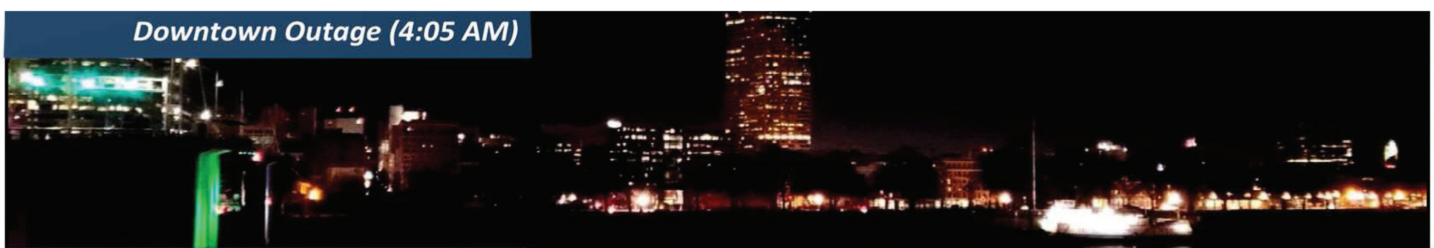

Network Feeder Conduits

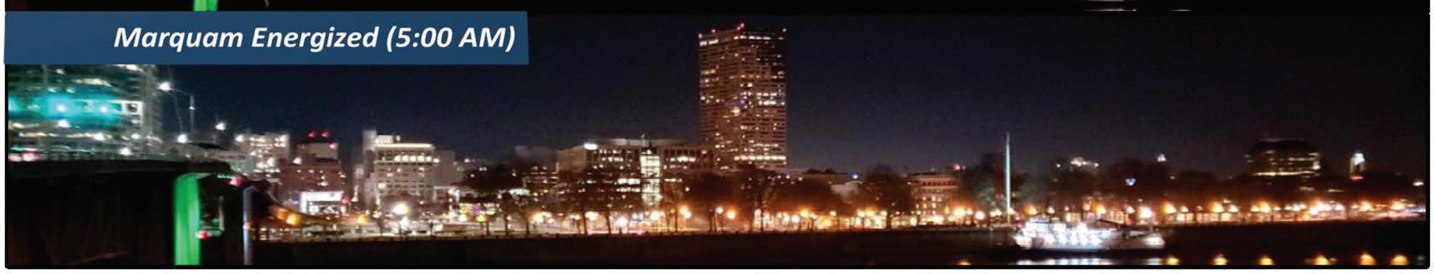

Network Cutover – Tap Changing

construction of the Marquam 13kV feeder getaways, after a planned outage, one of PGE's existing submarine cables failed its insulation test multiple times. Without a clear definition of the root cause, the decision was made to re-energize the specific submarine cable without any network load and monitored relaying operations for faults. Fortunately, the breaker held closed and load was transferred back. A week after this event, a section of primary lead cable located in downtown faulted due to unknown reasons, damaging several sections of lead cable and burning five (5) network protector relays. Since it did not affect the first group network cutover, PGE's Operations Team decided to postpone repairs until the first outage was completed, so electrical work can be completed on time.

On the days of the Group Network System Cutovers (Sunday, March-10 and Sunday, March-24), PGE had the support of over 180 PGE employees and contractors. This supporting cast facilitated: network switching operations, substation operations, internal/ external communications, and public safety. At approximately 10 PM, PGE's network crews initiated tap-changing procedures for over 40 network transformers on two network feeders. Around 1 AM, while de-energized, these two network feeders were connected to the new Marquam Substation. At 4 AM, PGE's dispatchers simultaneously and manually opened the reminder two network feeder breakers, executing a full downtown outage. Immediately afterward, network line crews initiated a manual close of all 216V grid network protectors. At approximately 5 AM, through an "All-Close" SCADA command, PGE's dispatchers successfully re-energized the downtown network from the new Marquam Substation.

The network substation improvement project is a testament of the selfless dedication of PGE's Operations, Planning, and Execution teams to perform at the highest level and to provide Portland with a safer, smarter, and cleaner electric grid.


Downtown Outage (4:05 AM)


Marquam Energized (5:00 AM)

Network Relay Trip Settings with Low-Loss Network Transformers

David R Smith, PE, Network Systems Consultant

INTRODUCTION

In low-voltage networks supplied from dedicated primary feeders (feeders serving only network transformers), all network protectors on a primary feeder must open automatically when the feeder breaker at the substation is opened in absence of a fault. **Figure 1** shows a simplified three feeder network where the primary feeders supply network transformers for the 208Y/120-volt grid network, and transformers for a two-unit 480Y/277 volt spot network.

Figure 1 shows the situation at the instant where the breaker for Feeder 2 is opened, but with all network protectors on the feeder still closed. Shown with each network protector on Feeder 2 with the arrow labeled "P" is the direction of the real power flow in the protector. In some protectors on Feeder 2 the real power flow is into the network, and in some protectors the real power flow is in the reverse direction or out of the network. The reason for this is that at the network-side terminals of each protectors on Feeder 2, the voltage magnitude and angle of the secondary network is different. In the protectors connected to the network with a more leading angle, the power flow is in the reverse direction, and at protectors connected to the network with a lesser angle, the power flow is in the forward direction. A misconception is that when the feeder breaker is first open and all protectors are still closed, the real power flow in all protectors is in the reverse direction. But because of circulating currents via the network transformers and primary feeder, there are both forward and reverse power flows in the protectors

Assuming all protectors on feeder 2 have a sensitive reverse current trip setting of 0.2% of protector CT rating, or less, the network relay sensitive trip characteristic will be satisfied in one or more protectors with a reverse power flow, due to the circulating currents. After the first protector opens following opening of the feeder breaker, the system topology changes, but in the remaining closed protector some will have a reverse power flow, and some will have a forward power flow, due to circulating currents. As the protectors sequence open, ultimately the condition will exist where all but one network protector is closed. In the last closed protector, the reverse power flow is due to the no load losses of all network transformers on the primary feeder, and from I2R losses in the network transformers and primary feeder cables from transformer exciting current, and cable charging current. In most systems, if all protectors have a sensitive reverse current trip setting of 0.2% or less, all protectors should open when the feeder breaker is opened in absence of a fault. This is true even with low-loss network transformers on the feeder where the excitation current of a transformer is less than the sensitive reverse current trip setting used for the network relay.

Figure 2 shows the MPCV relay sensitive gull-wing trip characteristic. This trip characteristic gives significant margin for reliable detection of capacitive backfeed currents, and for reliable detection of high-current backfeeds to multi-phase faults on the primary feeder when the network transformer leakage impedance has a high X to R ratio. The gull-wing trip characteristic is the optimum for application in network protectors in grid and spot networks fed from dedicated primary feeders,

In **Figure 2**, "RT" is the sensitive reverse current trip setting, which is the magnitude of the current leading the network voltage by 180 degrees (θI equal to 180 degrees in **Figure 2**) required to satisfy the relay sensitive trip criterion. "RT" typically is set between 0.10% to 0.20% of the network

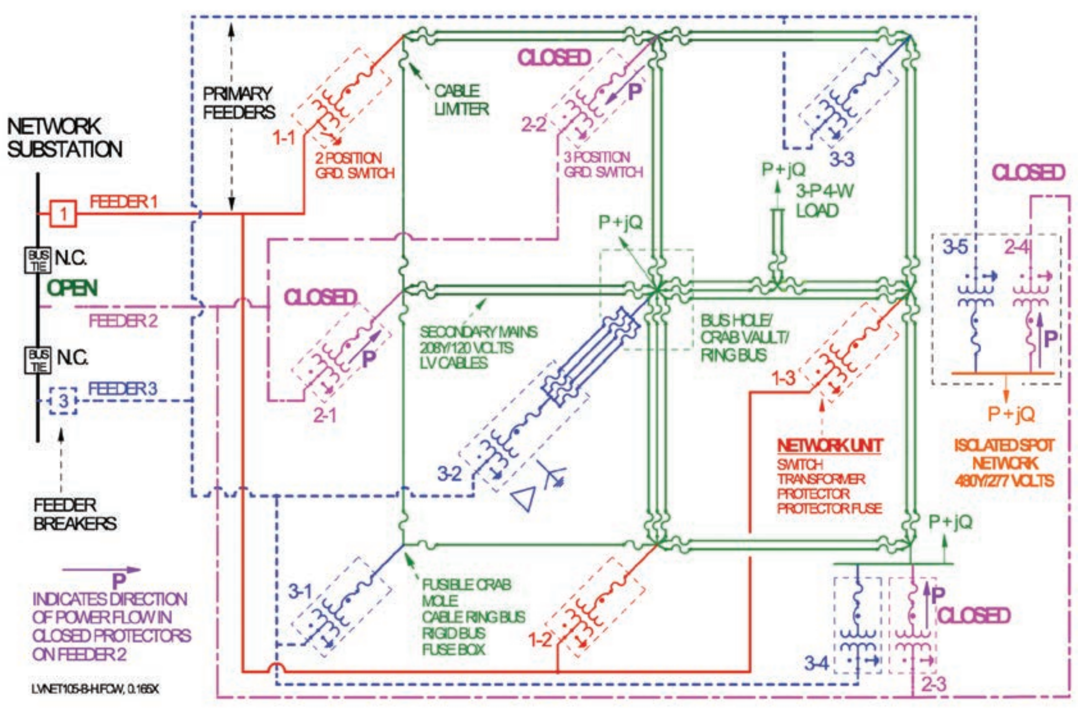


Figure 1 **Simplified three-feeder system supplying grid network and a spot network**

protector current transformer (CT) rating. For example, for a protector on a 500 kVA 216-volt transformer, having CT's rated 1600 to 5 amperes, 0.2% corresponds to 3.2 amperes. For current angle θI other than 180 degrees, the magnitude of the current required to satisfy the sensitive trip characteristic, ITRIP, is different than RT.

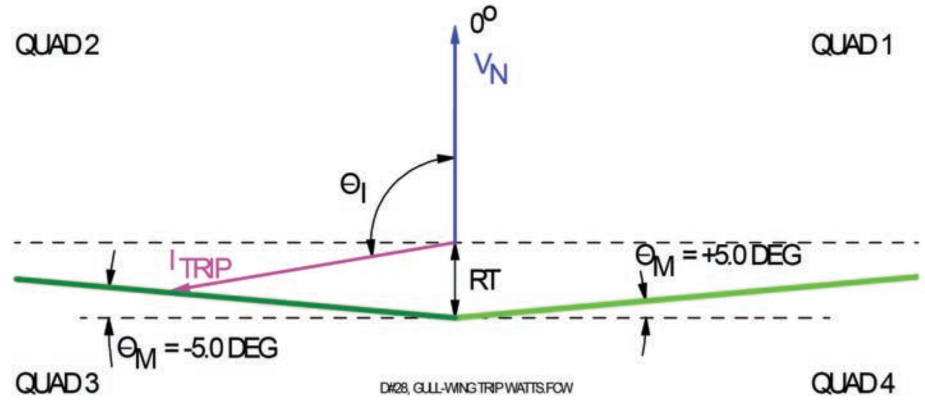


Figure 2 Network relay with gull-wing sensitive trip characteristic

Protector tripping on current of its own network transformer

In some systems, and in particular in spot networks, a vacuum switch, vacuum breaker, or fused switch is applied at or near the HV terminals of the network transformer as shown in **Figure 3**. When the breaker or switch is opened in absence of a fault, there are no circulating currents in the protector on the secondary side, as occur when there are multiple network transformers on the primary feeder as in **Figure 1**.

For the system in **Figure 3**, when the fused switch is opened for any network transformer, it is desired that the network protector on the secondary side opens automatically. However, if the network transformers have low losses and low exciting current, the relay sensitive trip characteristic may not be satisfied for a typical trip setting of 0.2% of protector CT rating. In the system of **Figure 3**, where the protectors failed to open when the HV switch was opened, the network relay sensitive trip setting was 0.20% of CT rating, or 3.2 amperes at 480 volts. **Figure 4** shows the relay sensitive trip curve, the transformer exciting current, IE, the primary cable charging current reflected to the secondary side, IE, and the current in the network protector, INWP. The exciting current of the 1000 kVA network transformer, IE, was 0.18% of transformer rated current (1202.8 amperes at 480-volts) or 2.165 amperes. With the no-load losses of the transformer being 1357 watts, the angle by which the exciting current, IE, leads the network line-to-ground voltage is 180 degrees minus 41.08 degrees, or 138.92 degrees as shown in **Figure 4**. The total current in the protector, INWP in **Figure 4** is the transformer exciting current, IE, plus the charging current, IC, of the 40 feet of 4/0 PILC cable between the transformer and the switch. This charging current reflected to the secondary side, IC, is 0.43 amperes as shown by the blue phasor in **Figure 4**. The total current in the

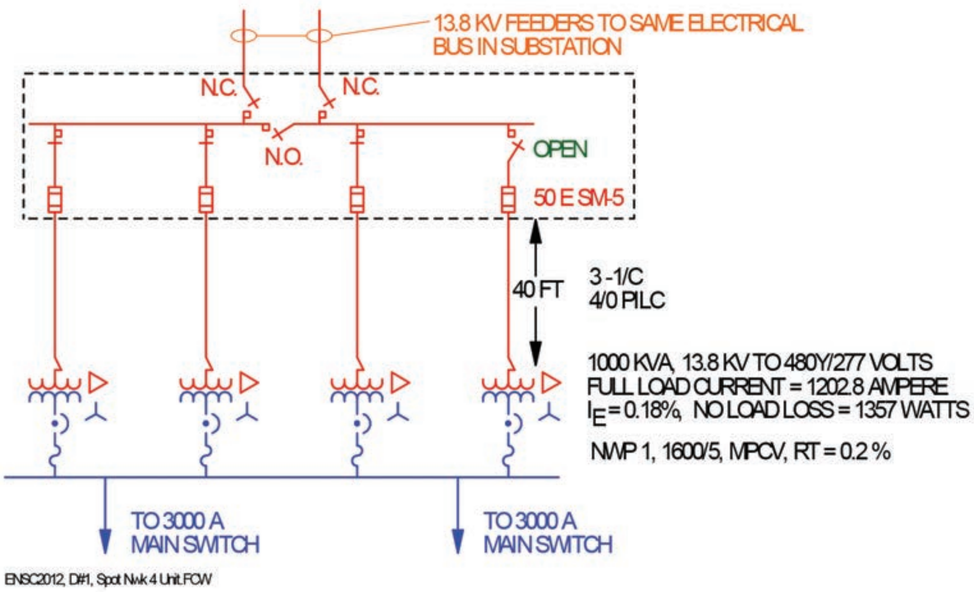


Figure 3 System where network protector must trip from transformer exciting current and primary cable charging current.

network protector, INWP, is 1.919 amperes leading the network voltage by 148.25 degrees as shown by the black phasor in **Figure 4**. With the total current in the protector being 1.919 amperes, and the sensitive reverse current trip setting being 3.2 amperes, with the trip characteristic and settings of **Figure 4**, it is clear that when the primary HV switch in the system of **Figure 3** is opened, the network protector will not trip.

With reference to **Figure 4**, for the current in the network protector, INWP, 1.919 amperes at 148.25 degrees, to intercept the sensitive trip curve, the sensitive reverse current trip setting, "RT" must be reduced from 3.2 amperes to a lower value. **Figure 5** shows that if RT is set to 1.720 amperes, which is 0.1075 percent of CT rating, the sensitive trip characteristic will just be satisfied.

To assure that the protector will open when the switch on the HV side is opened, a relay sensitive trip setting of about 80% of the calculated setting should be made, which is 0.086% of CT rating. Then the HV switch should be opened to confirm that the protector will open automatically.

When fuses are applied at the HV side of network transformers as shown in **Figure 6**, there are two other issues that must be investigated to assure that the system responds properly for faults on the HV feeder, at either FAULT LOCATION 1, or at FAULT LOCATION 2.

For a fault at LOCATION 1, the desired sequence is that the feeder breaker at the substation open, and the network protectors associated with the faulted feeder open. When fuses are applied at the HV side of the network transformer, they must not blow under high-current backfeeds to faults between the feeder breaker and the fuses. At the maximum backfeed current, the fuses must be slow enough to allow the network relay to make its trip contact and open the protector. This is also true for the network protector fuse under high current backfeeds. Should the protector fail to open for a high-current backfeed for a fault at LOCATION 1, the protector fuses and not the HV fuses should clear. At the maximum backfeed current, the fuse on the HV side should be no faster than the protector fuse, taking into account transformer turns ratio and the type of fuse on the HV side for faults between the feeder breaker and fuses.

For a fault at LOCATION 2 in **Figure 6**, between the HV fuse and the network transformer, it is desired that the fuse in the faulted phase or faulted phases blow, and that the feeder breaker at the substation remains closed. The fuse time-current characteristics should be coordinate with the phase and ground time overcurrent relays for the feeder breaker at the substation. Assuming that this coordination is achieved, a fault at LOCATION 2 in **Figure 6** will blow the fuse(s) in just the faulted phase(s), and the station breaker remains closed. For such conditions, the network relay sensitive trip characteristic must be satisfied so that the network protector on the secondary side opens. This can be easily evaluated by simulating the fault and blown fuse condition which gives currents and voltages at the protector associated with the faulted feeder. From these currents and voltages, with the MPCV relay the positive-sequence current and positive-sequence voltage seen by the relay are easily found, along with the angle between the positive-sequence current and positive-sequence voltage. Then it is simple to determine if the relay sensitive trip characteristic is satisfied for the fault and blown fuse condition.

For a fault at LOCATION 2 in **Figure 6**, if the feeder breaker at the substation has both instantaneous current relays and time overcurrent relays, it is possible that the fuse(s) in the faulted phase(s) will blow, and the instantaneous current relay (device 50) for the station breaker will pickup, tripping the station breakers. The response depends upon fuse size and time-current characteristics, the available fault current, and the pickup of the instantaneous current relays for the station breaker.

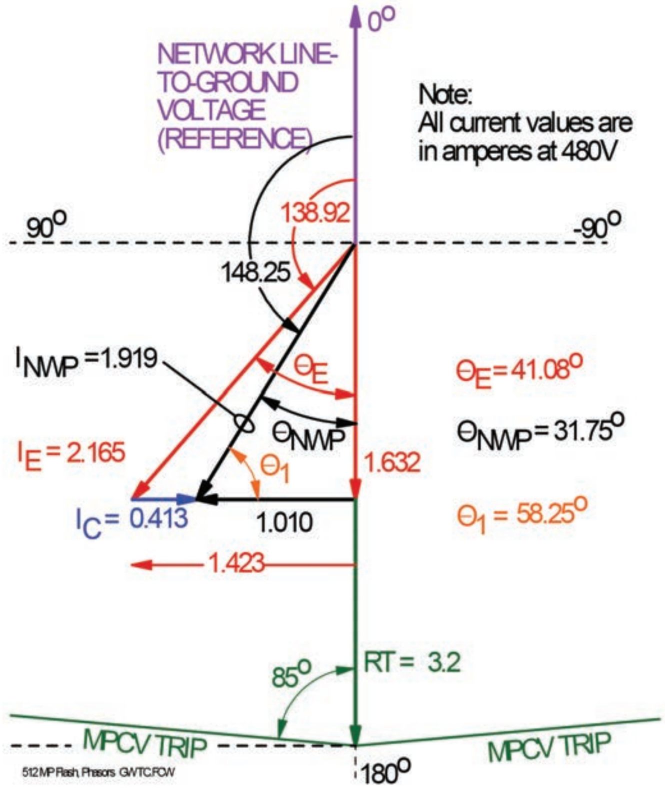


Figure 4 Current phasors for system and parameters in Figure 3, superimposed on relay sensitive trip characteristic.

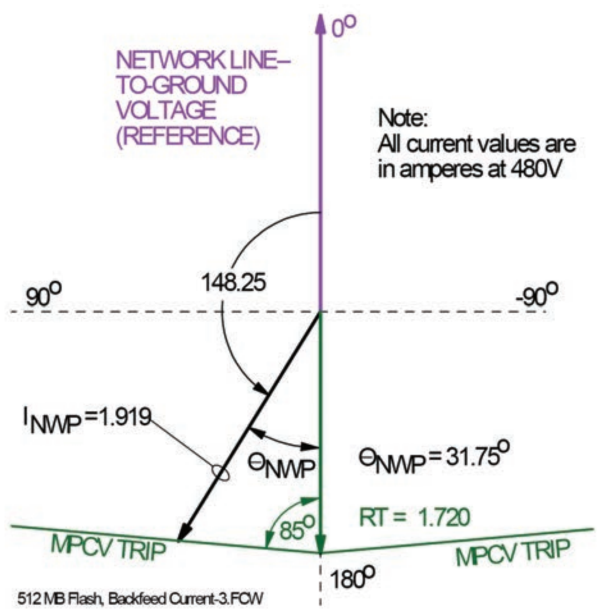


Figure 5 Reverse current trip setting, RT, for which network protector current intercepts trip curve.

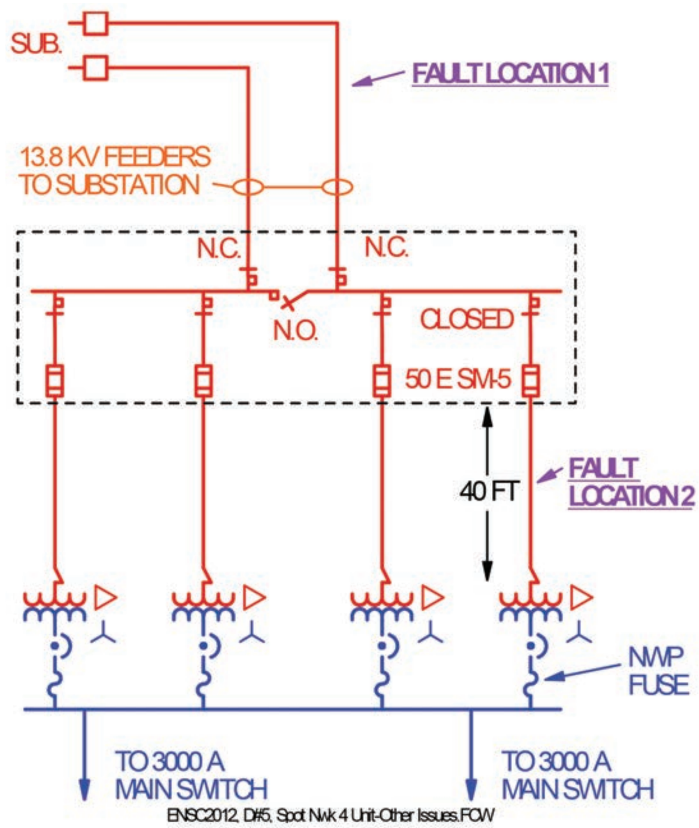


Figure 6 HV feeder fault locations with fuses on HV side of network transformers.

Protector tripping on current from two network transformers

Figure 7 shows a 13 kV network feeder with a three-way switch, with the switch for one leg open. There are just two 2000 kVA 480-volt network transformers on the feeder beyond the switch leg that is closed. When the utility with this system opened the feeder breaker at the substation, only one of the two protectors on the feeder opened automatically. The feeder remained live on backfeed.

For the 2000 kVA network transformer in spot network 2, the exciting current was 0.21% of network transformer rated current, with a no-load loss of 2063 watts. For the 2000 kVA network transformer for spot network 2, the exciting current was 0.22 % of transformer rated current, with a no-load loss of 2066 watts.

When the feeder breaker in **Figure 7** was opened, the exciting current and no-load losses for the two network transformers were supplied from the secondary side of the transformers. In addition, since the voltage on the secondary side of the two network transformers in the spot networks was different, there was a circulating current when both protectors were closed. This produced a reverse power flow in the closed protector at spot network 2, of sufficient magnitude that the relay sensitive trip characteristic was satisfied, and the protector tripped, giving the condition shown in **Figure 8**. But the protector in the spot network at spot network 1 did not open automatically.

The network relay in the closed protector had a reverse current trip setting of 8.8 mA, which is 0.176 % of the protector CT rating. This corresponds to a current of 5.28 amperes in the protector. **Figure 9** shows the sensitive trip characteristic of the relay used on the CM-52 protectors, where the reference phasor, the network line-to-ground voltage, VN, is drawn horizontal rather than vertical as in **Figure 2**.

The current phasors in **Figure 9** are drawn to scale, where the sensitive reverse current trip setting, "RT" is 5.28 amperes at 180 degrees. Adding the excitation current of the two network transformers, the vector resultant is 10.43 amperes as shown with the red phasor, leading the network line-to-ground voltage, VN, by 118.7 degrees. Adding the primary cable charging current reflected to the 480 volt side, or 30.223 amperes at an angle of -90 degrees, to the resultant exciting current gives the current in the network protector, INWP, shown with the orange phasor in **Figure 9**. For the selected trip characteristic for the relay in this application, it is seen from **Figure 9** that the protector current does not lie in the trip region.

Note from **Figure 9** that for the network relay used in this application, the angle of the sensitive trip curve is adjustable. For the top half of the trip curve, the angle of the trip curve relative to the network voltage is 85 degrees, just as with the MPCV gull wing sensitive trip characteristic. But for the bottom half of the curve, the angle of the trip curve is perpendicular to the network line-to-ground voltage reference, VN. From the trip curve and current phasors

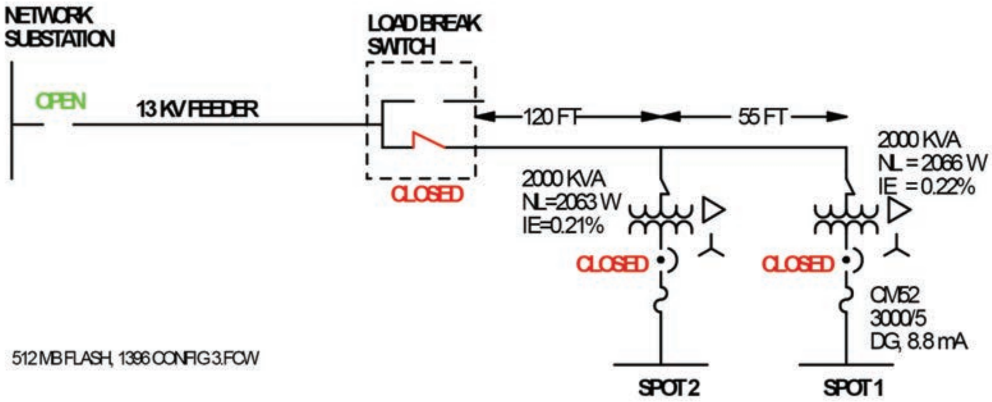


Figure 7 Feeder with two 2000 kVA 480-volt network transformers with feeder breaker open.

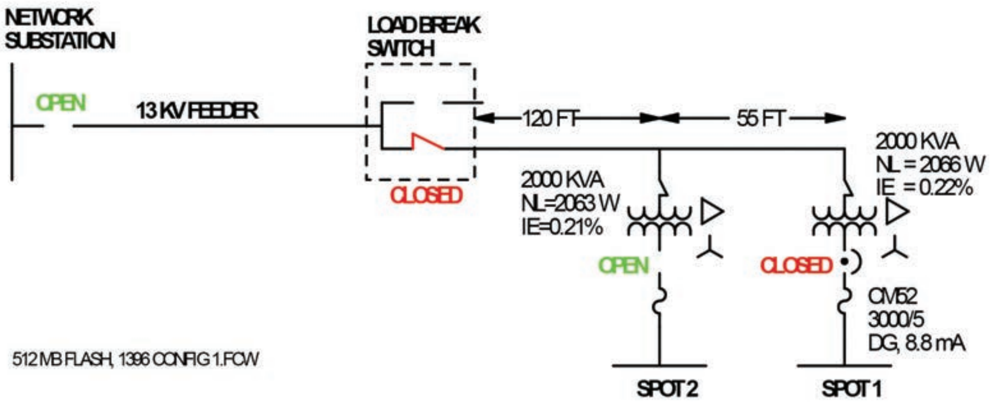


Figure 8 Feeder breaker and protector on one 2000 kVA network transformer open.

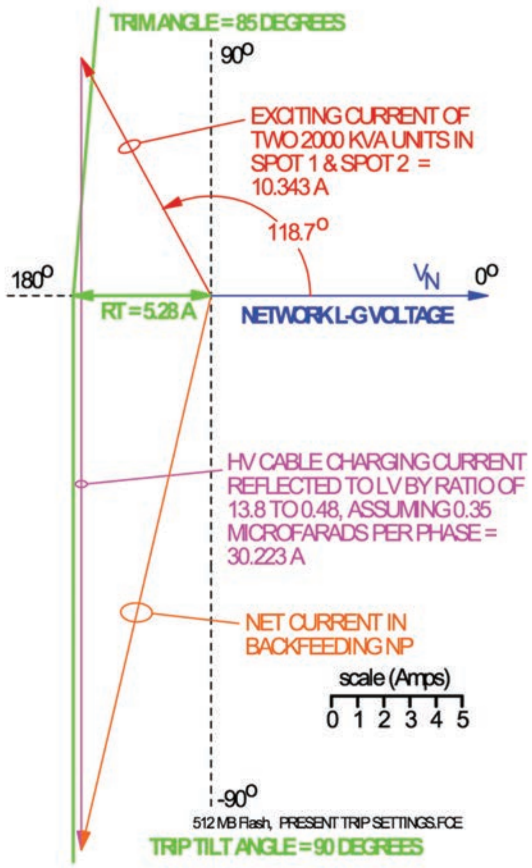


Figure 9 Current phasers superimposed on relay sensitive trip curve.

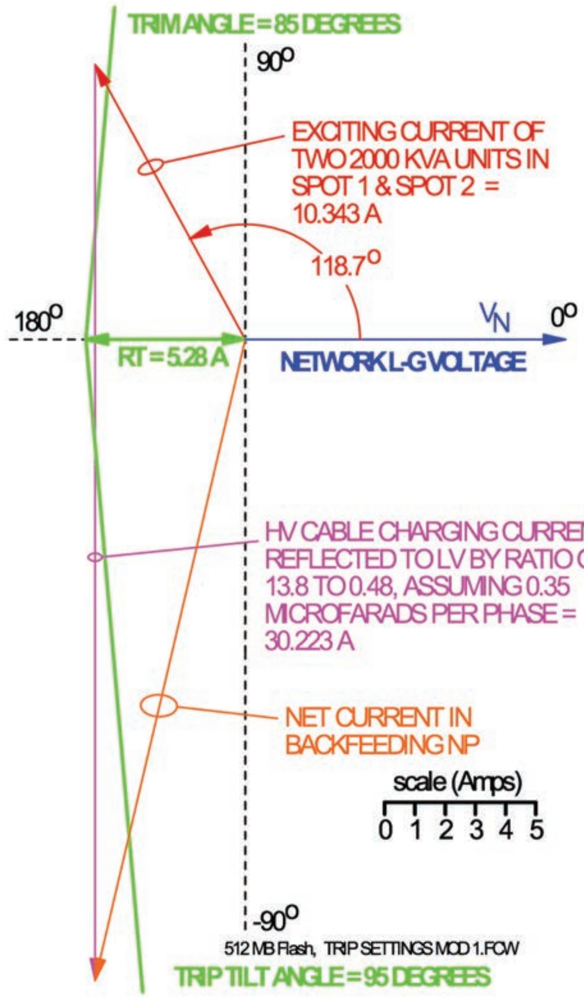


Figure 10 Current phasors with RT of 5.28 Amperes, but with gull-wing trip characteristic.

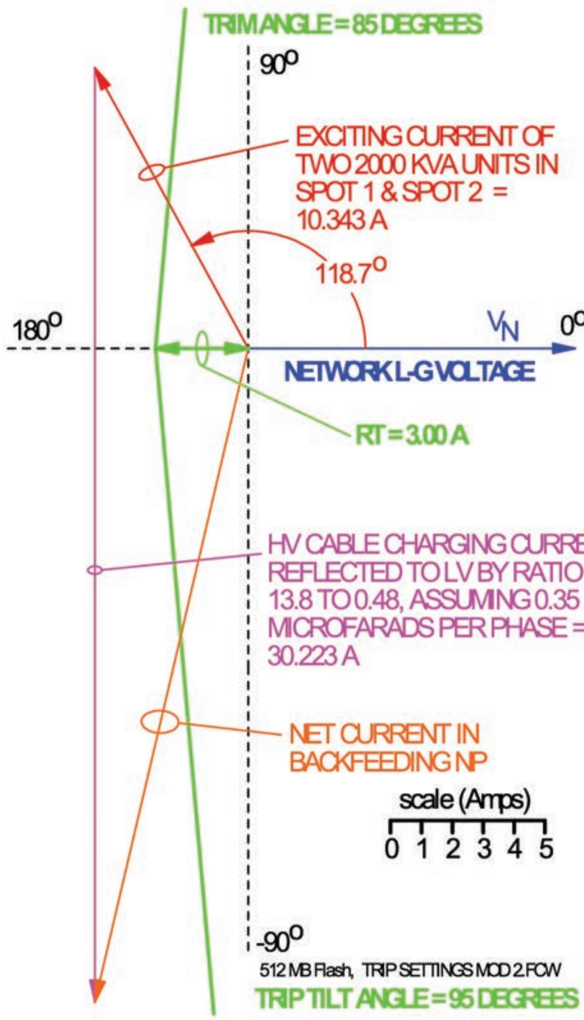


Figure 11 Current phasors with RT set 0.10% and the gull-wing trip characteristic.

in **Figure 9**, it is seen that the relay sensitive trip curve is not satisfied.

If the relay in this application is configured so that the trip curve emulates the gull-wing characteristic of the MPCV, as shown in **Figure 10**, the current in the network protector in Spot 1 will lie in the trip region, as shown by the orange phasor where RT is still set at 5.28 amperes at 480-volts.

To provide greater margin and allow for tolerances in the relay and in system data, setting the reverse current trip setting to 0.10 % of protector CT rating, or 3.0 amperes as shown in **Figure 11**, results in the protector current, the orange phasor, lying well within the trip region. Note from **Figure 11** that the trip characteristic is the same as that of the MCV relay (gull-wing) characteristic with an RT setting of 0.10 percent of protector CT rating.

Some operators, who have a standard reverse current trip setting of 0.20% of protector CT rating, may be hesitant to lower it to 0.10%. In most spot network systems where the primary feeders come from the same electrical bus in the substation, lowering RT from 0.20% to 0.10 % of CT rating will have no effect on protector operation under normal loading, and will not result in protectors cycling or pumping under normal loading.

Summary

When the network protector with a typical sensitive reverse current trip setting of 0.20% of CT rating is used in protectors on low loss network transformer, if the system can be configured such that the backfeed in a protector is due to just the exciting current of one transformer plus cable charging current, the protector may not open in absence of a fault. Furthermore, as shown by the second example in this article, when the protector is supplying the excitation current of two transformers and primary cable charging, the protector with a trip setting of 0.20 % may not open. Some system operators are applying vacuum breakers at or near to the HV terminals of network transformers for 480-volt spot networks. The main purpose of these breakers is to clear faults in the 480-volt portion of the system or in the network transformer. Tripping of these breakers may be initiated with operation of heat sensors, ground fault relay schemes, or other fault detection devices. Regardless, it usually is desired that when the vacuum breaker is opened in absence of a fault, the network protector on the secondary side opens automatically.

Trip settings of 0.10% of CT rating or less may be needed to assure the protector will open when it is backfeeding just one network transformer and primary cable. With the MPCV microprocessor relay, its sensitive trip characteristic (gull wing) is such that it can have an RT setting that will trip the protector when applied with low-loss network transformers.

Avista Network Vault Trespassing Event

Ryan Bradeen, Operations Manager, Avista Corp.

Headquartered in Spokane, WA, Avista Utilities provides electric service to 379,000 customers and natural gas to 343,000 customers in three states. Touting a unique underground delivery system in downtown Spokane's core, one of only a few such networks in the country, this hidden system was constructed in 1889 by Washington Water Power, known now as Avista.

Avista's underground downtown network consists of 150 transformer vaults, 182 network protectors and 1,000 manholes, ranging in size from 1 ½ boxcars down to spaces barely large enough for two Avista cablemen. The vaults and manholes are connected by a grid of conduit encased in protective concrete through which electric cable is stretched. Incredibly, much of the cable system and all of the infrastructure that was installed in the early 1900's is still in use today.

Most of the electricity used to supply the downtown network is renewable hydropower from the nearby Spokane River. The Upper Falls and Monroe Street dams supply two downtown substations. The power is then split into quadrants with four feeder lines to each area, making outages a rare problem in this dense cable network.

At Avista, three cablemen crews respond to trouble, install services, install transformers and network protectors and take great pride in keeping the lights on in Downtown Spokane.

The service area of the Downtown Network is relatively small, about one mile by one mile. Network crews can often times recognize situations that are taking place and in early 2019 one of the Avista crews saw something out of the ordinary.

Zach Muller, a Network Foreman, noticed police activity and first responders near the Qwest spot vault in downtown Spokane. To his surprise, there was an unauthorized person in the vault. The man had removed the 250 lb. grate, jumped down on top of the transformer and was casually exploring the energized 277/480 spot vault. Network crews immediately collaborated with the fire department and police department.

THE SPOKESMAN-REVIEW

Monday, March 04, 2019 Spokane, Washington Est. May 19, 1883

Washington Idaho WA Government

NEWS > SPOKANE

Avista cut power to much of downtown Spokane for 10 minutes due to trespasser

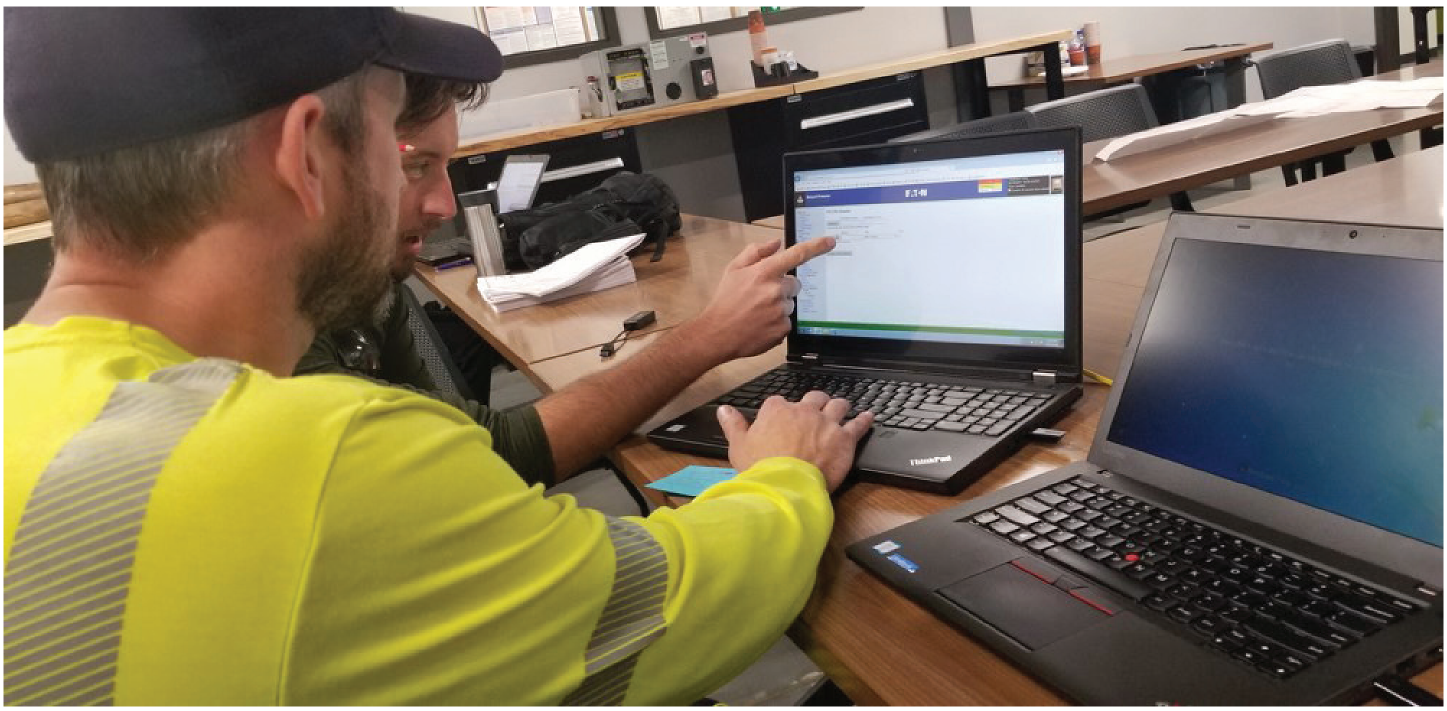
UPDATED: Mon., Oct. 29, 2018, 4:55 p.m.

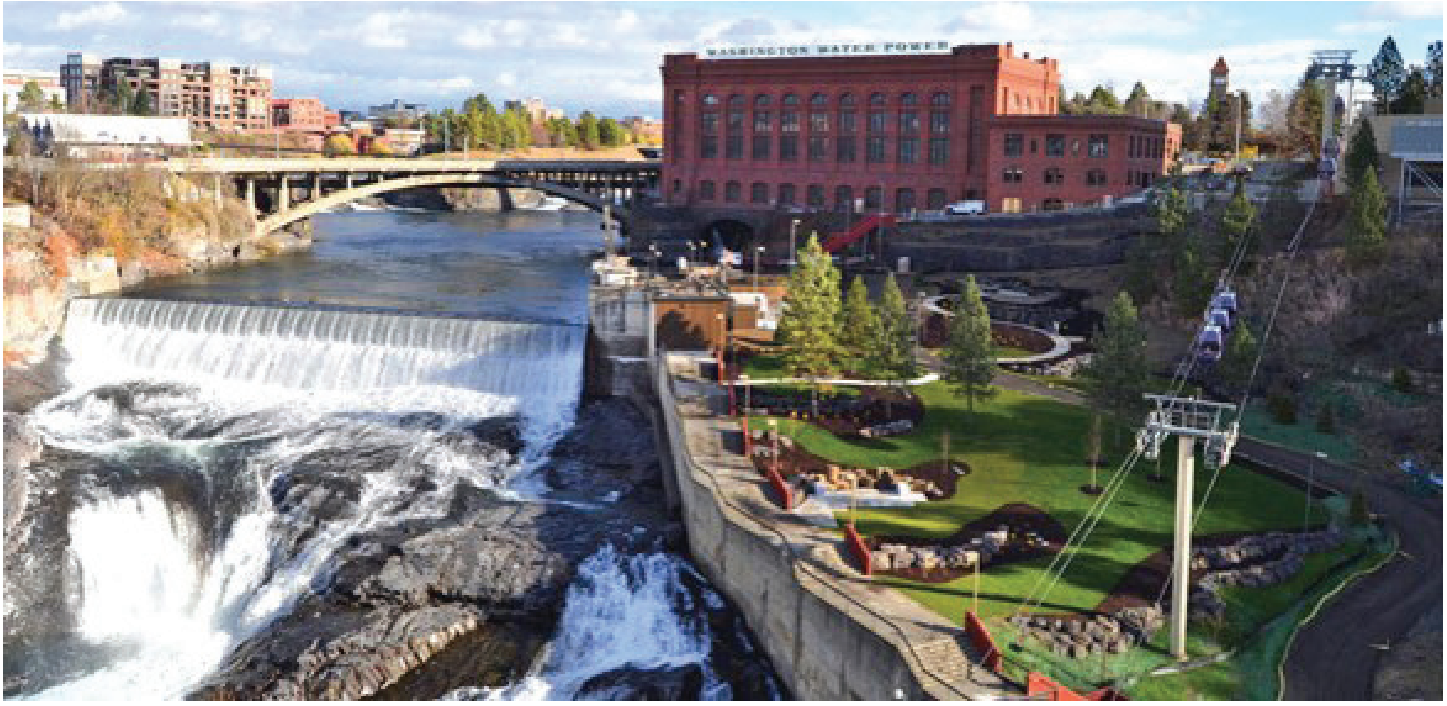
Looking west above downtown Spokane, the railroad tracks of the BNSF railroad can be seen angling from the lower right, past the old Northern Pacific Depot and continuing west toward Seattle. At far left, Interstate 90, completed in the late 1960s, represents Americans' move away from rail travel. Around 1970, the NP merged with Great Northern and other lines to become Burlington Northern, which is now BNSF. Photo is from June 4, 2018. Jesse Tinsley/THE SPOKESMAN-REVIEW (Jesse Tinsley / The Spokesman-Review)

Avista crews opened vault hatches so that the first responders could begin negotiating with the man to coax him out of the vault.

After about an hour of negotiating, the man in the vault became confused, aggressive and was endangering himself, equipment and the customer owned property. At this moment, the Spokane Police Chief, Spokane Fire Chief and Avista were faced with making a decision to proactively take down the Network. Avista, the police chief and the fire chief devised plan and there was lots of brainstorming taking place. Ideas of using a Taser gun were proposed but what if the police officer missed and hit cable? Tear gas was also discussed but what if that pushed him into more of a rage than he was already in. Ultimately, the plan that made most sense was to kill the network, making it safe for the officers to enter. The goal was to subdue the man, rescue him out of the vault and re-energize the network as safely and efficiently as possible.

Over the last 42 years, there have been limited network outages, the longest lasting only 7 hours due to a vault fire. There are no records of de-energizing the system proactively. As it is well known in the network community the lights always stay on and often times processes, resources and budgets are ignored because of the redundancy of network systems. While de-energizing the system in theory seemed simple, it presented several unknown challenges and some excellent opportunities to improve.





How can we improve?

- **Internal Communication**- It took nearly 8 minutes to de-energize the system and had this been a true emergency 8 minutes to de-energize is too long. This challenge created a good opportunity to improve communication and breakdown silos within the organization. In order to improve, education of network systems was of high priority. Yearly network training is currently in place for all switching at Avista.
- **External communication**- Downtown customers are accustomed to always having the lights on. When the lights go out, chaos and confusion begins. After the incident, a custom message geared toward downtown customers was established. The goal was to identify customers, building managers and City of Spokane representatives to give indication of an outage prior to it taking place.
- **Secured grates**- After the incident Avista surveyed grates. The inspection proved that not all grates were secured. Currently, all grates have been secured to eliminate this type of incident in vault locations.
- **Vault ownership identification**- Over the years Avista owned facilities have become unidentifiable. In the trespassing incident, first responders were not able to understand ownership of the facility and what type of facility it was. Avista teamed up with local company to help implement signage for Avista vaults. Avista and Designer Decal paired up and designed a practical and durable vault tag to be applied at surface level. The tag indicates Avista ownership and also includes specifics for the crews such as vault number, feeders in vault and how many bays in the vault.
- **Network protector communication**- Prior to the incident, Avista has tried to implement communications to network protectors for nearly 18 years. Budget constraints, resources and the redundancies of the network slowed and nearly hauled the project. The trespassing incident jump started the communications project and Avista network engineering capitalized on the opportunity. In the fall of 2019, the Avista network team, with the help of Eaton, will commission its first network protectors utilizing the sophisticated network tool of VaultGard. In the future, Avista will utilize the tool to isolate vaults, trouble shoot and collect real-time data to better utilize the network system. The safety of the public and crews is paramount and Avista believes VaultGard will help engineer out hazards.

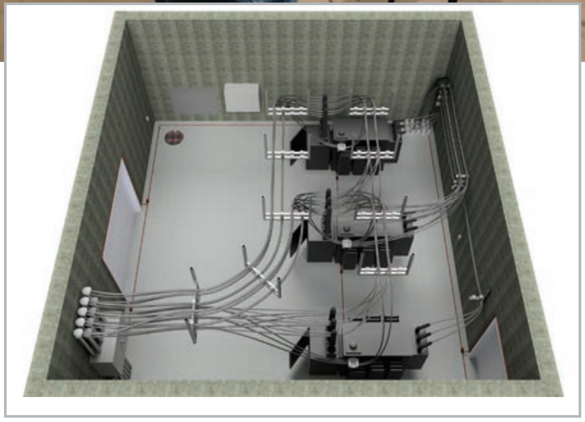
Overall, the trespassing incident created and highlighted areas of improvement for Avista. Avista is striving to improve at a rapid pace in order to maintain a safe, reliable and a rewarding service for the downtown core of Spokane with keeping the safety of crews and the public at the forefront.

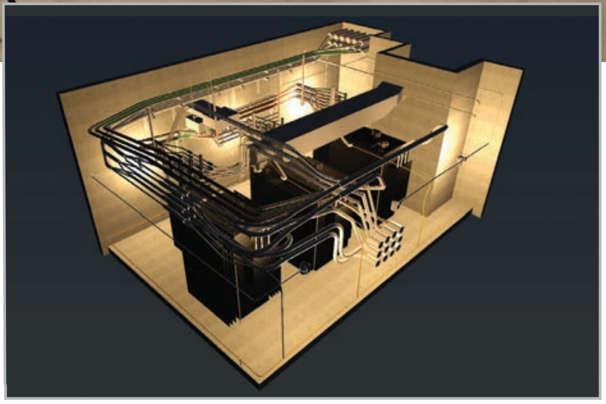
3D Modeling & Scanning at Lincoln Electric System

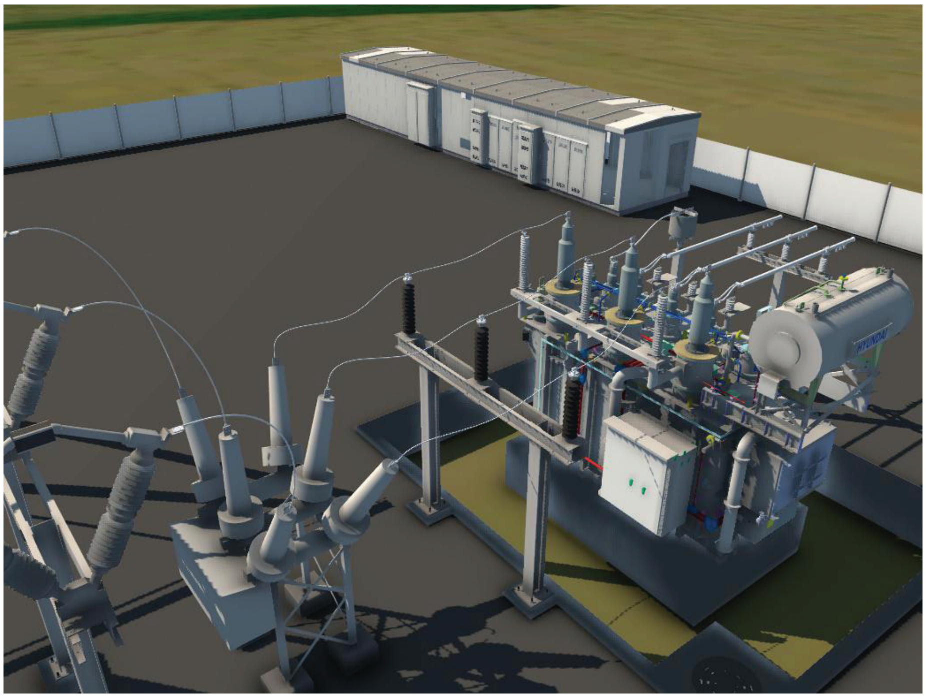
Ryan Kohn, Supervisor GIS/CAD, Lincoln Electric System

Located in Lincoln, Nebraska, Lincoln Electric System (LES) service territory spans approximately 200 square miles and provides electricity to about 280,000 people. LES is proud of its generating capacity portfolio that is comprised of one-third coal, one-third natural gas and one-third renewable energy. Overall, LES operates 38 network vaults that serve power to its ever-growing downtown area.

LES utilizes technology and innovative hardware to improve processes to better meet the needs of our customers. During an assessment period, LES identified a few key areas for improvement: implementation of Lidar scanning to improve accuracy of asset records and evolve from a 2-D to a 3-D design/record environment.







Lidar Scanning

Scanning for LES became a reality when we identified the need to capture the true state of our network vault system. During a thorough review we found deviations and missing crucial dimensions from our prints and records. Prior to scan data, LES had basic "As-built" records of its network system, but as we all know an "As-Built" is only as good as the information that came back to those responsible for updating them. Because of this, we needed to find a better way of capturing our utility assets spatial location, connectivity and relationship to each other, and lidar scanning seemed to be the answer. Our first scan project was a three-transformer network vault that we felt would serve as a good Proof of Concept (POC)to solidify the buy-in necessary for us to purchase a lidar scanner for ourselves. During this POC we found that scanning was relatively quick and simple. Once scanned, we registered the scan in Autodesk Recap, a software that we already had bundled into Autodesk's AEC suite. After registering and viewing the scan, we instantly realized we now had a record that would completely change our existing workflow. We now would able to eliminate the need for our network technicians to travel to the vault to collect design information. The days of multiple site visits to collect design information would be gone! The engineer now can measure, flythrough, pan and view the vault in its entirety to make the best business decision – all at the comfort of their desk! This is all possible because the Lidar scans are accurate to +/- 6mm, measurable and have high-resolution images.

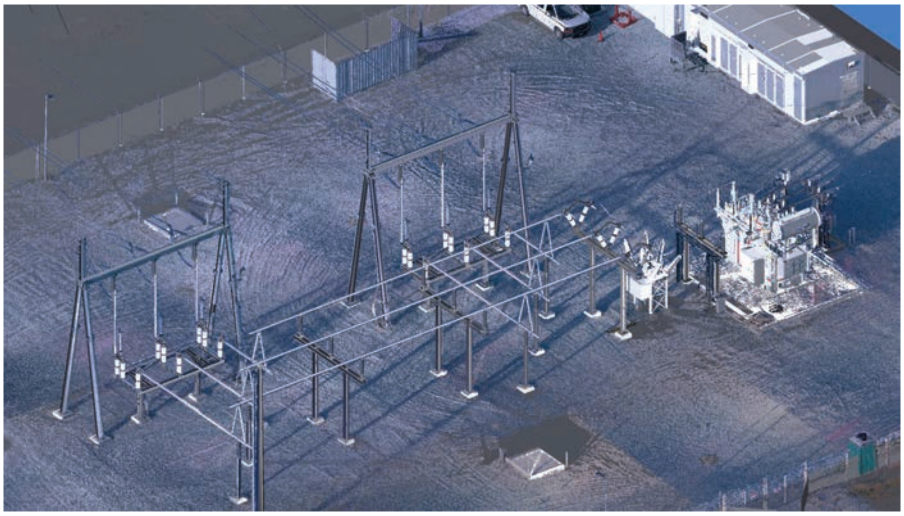
Due to the success of this POC, we now have our own Lidar scanner and have recently completed the scanning of all LES network vaults. Staff now have a comfort level that we haven't had in years with the accuracy our network system records.

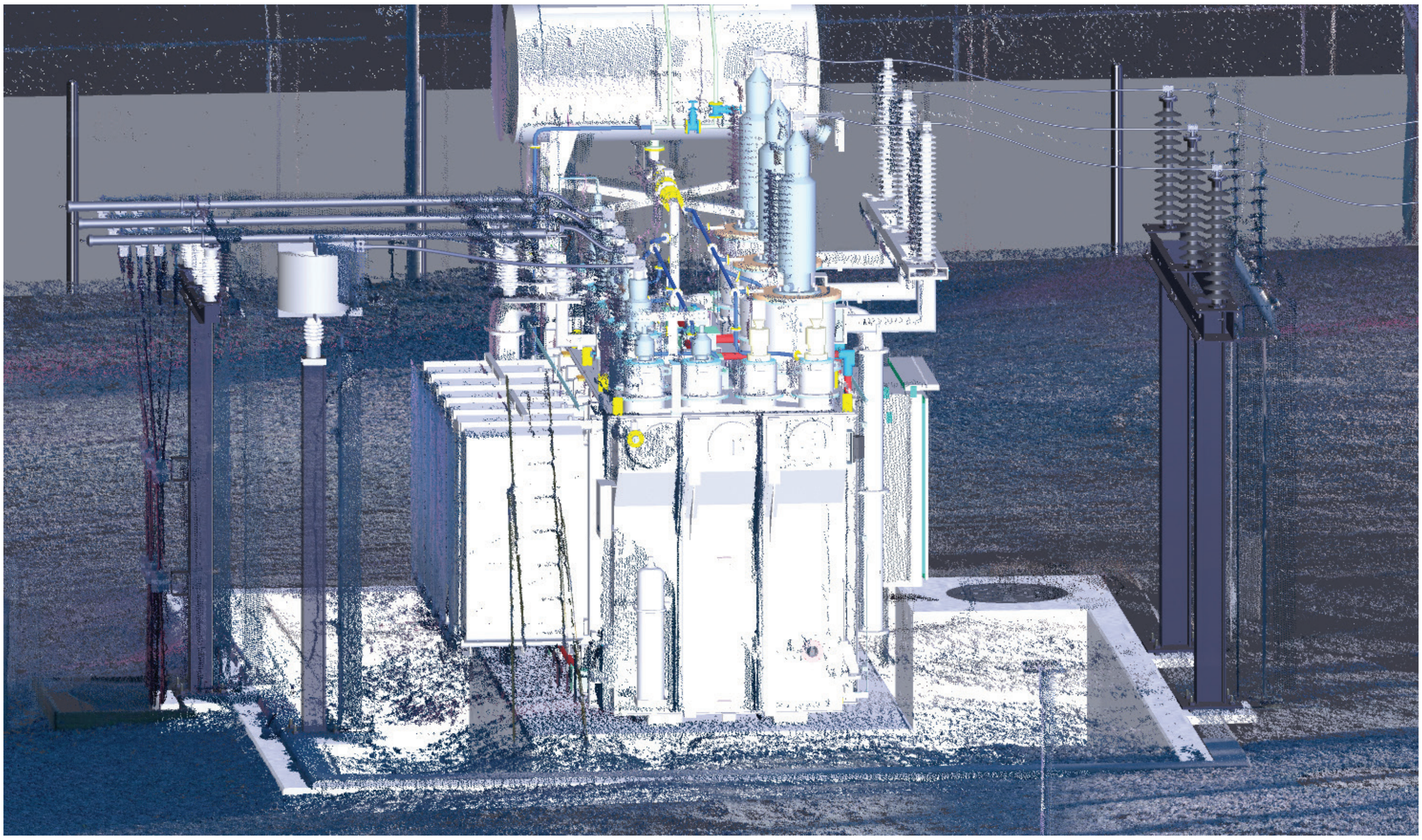
2-D to 3-D to Reality

Due to the success of scanning our network vaults, we felt the natural step was to start 3-D modeling our substations. Up to this point, LES created parts in 3-D but LES felt the best way to maximize any substation scan data was to use it to validate the true "As-built" conditions, and to do that, a 3-D model must first be created. To ensure that we had the proper buy-in and that this would work for us, we created the Substation the way we have always done it in 2-D, and then at the same time built it as a 3-D model. This first substation took some time to build. This was mainly due to creating all the parts from scratch and determine how to properly constrain them to each other. LES has identified existing parts and have heard from others in the industry to "not make your parts too detailed," but LES has taken a different stance. LES builds most of the parts it uses using micrometers and calipers. Why you may ask? LES believes that computer processing power will only get better and today will be the slowest it will ever be. We feel that if you build it to the highest standard now, you will never need to rebuild the part later. To date, LES has created four substations using the modeling method and never plans to look back.

Integration of Models and Scans

Now that we have both high accuracy point clouds and 3-D models, we have the data we need to validate the design against what was built in the field. At first this was more perceived as a cool feature, but now we have started to realize the power of what it can really do. We now can ensure proper clearances from our desks and can take measurements to prove clearance without taking a substation offline. We have also reduced, or in some cases eliminated, the need to travel to the site for verifications. LES is fortunate to have a great crew that constructs our substations accurately; however, if there were any issues in





the construction process, it will now be caught by overlaying the scan on the model. In the above transformer picture, you can see there is a discrepancy between our design (3-D model) and what was built (Lidar scan). This now will be reviewed by engineering to ensure compliance, something that may not have been caught without modeling and scanning.

What's Next

LES feels the next big integration will be virtual reality (VR). Because of this, we have recently started updating our computers RAM, adding high-end video cards and boosting memory so that we can use our mobile desktops to run the software required to leverage VR. We envision the ability to use our Lidar scan data and models in a VR application. This ability would allow engineer and technician to be in the same room discussing the same network vault at the same time, all in the comfort and safety of the office. We feel this will eliminate any misconceptions of how the vault is configured and strengthen the understanding of any constraints or problems the new design may present.

I think the utility sector has always done a great job of asking the question "Why?". In many ways, that has worked well and created a solid foundation for supporting "the way we have always done it"; however, with ever-changing technology, the question we may need to ask now is "Why not?".

CYME power engineering software

Eaton's CYME software offers detailed distribution system modeling and advanced analytical capabilities, which are perfect for:

- Network-wide system planning and analysis using historical data and forecast
- Distributed energy resources hosting capacity analysis and impact studies
- What-if contingency scenarios assessment
- Grid efficiency optimization
- Protection scheme validation
- Power quality and system reliability improvement

Secondary grid network analysis

Tackle the complexity of low-voltage secondary networks with CYME software, which offers:

- Detailed modeling of secondary network components, including network protectors with complete relay settings
- Robust power flow and short circuit algorithms for unbalanced meshed systems
- Efficient single- or multi-contingency scenarios (n-p) analysis
- Load estimation through the processing of telemetry data with the Distribution State Estimator module
- Integration to time-series databases and data lakes with the Dynamic Data Pull module

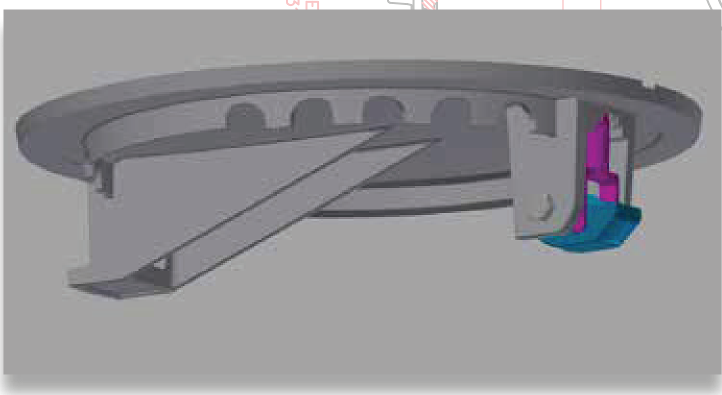
Contact Eaton for a demonstration of our CYME software and solutions:
cymeinfo@eaton.com.

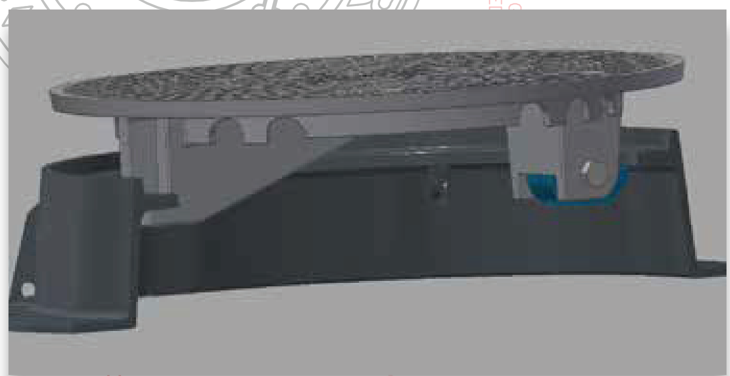
EATON
Powering Business Worldwide

NEENAH FOUNDRY

Mitigating the Damage Caused by Underground Explosive Events

Neenah Foundry's Controlled Pressure Release Manhole Covers eliminate the inherent dangers of flying covers and add a level security to the underground infrastructure.



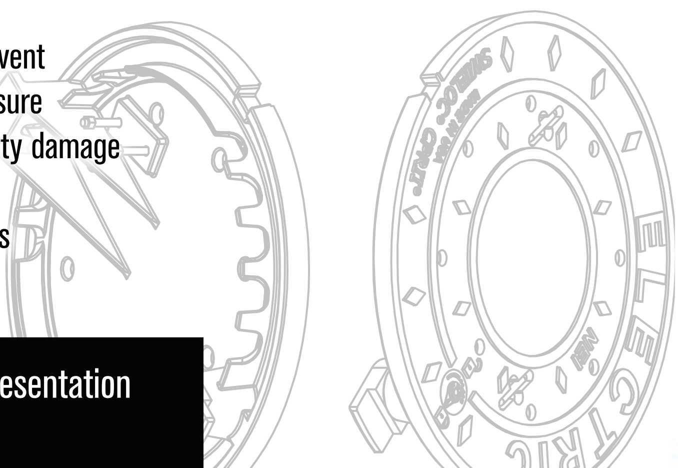


During an explosive event the upward travel of the CPR cover is limited to a maximum of 4" by an engineered lug and latch. With the help of specially designed exhaust ports the pressure is released 360° downward around the perimeter of the manhole opening.

With the help of several Utilities these covers have been tested extensively at EPRI in Lenox MA for over a decade.

Why the CPR cover by Neenah?

- Cover does not leave the frame during an event
- Controlled rise of cover and release of pressure
- Reduces the possibility of injury and property damage
- Successfully tested at EPRI
- Helps prevent theft and unauthorized access
- Works with many existing frames



For more information or to arrange a presentation
visit us at **www.Swiveloc.com**
or call us **920-252-3563**

NEENAH FOUNDRY

GridAdvisor Insight optical sensors

Shining a light on underground networks with real-time metrology and intelligence

Eaton's GridAdvisor optical sensor is available in a variety of easy-to-install packages with a standardized interface, including the optical standoff insulator voltage sensor and the optical deadbreak elbow adapter sensor.

The status of your underground network shouldn't be a deep, dark secret

Eaton's GridAdvisor™ all-optical medium-voltage and current sensor system provides a highly accurate view of underground networks, resolving the difficult and time-consuming process of diagnosing, troubleshooting and fixing issues.

Retrieving real-time site metrology and intelligence on today's electrical distribution system, substations and underground distribution locations, the GridAdvisor optical sensor platform facilitates unparalleled precision across multiple voltage classes and has the ability to identify potential failures before they occur.

Because the sensor relies on light to sense voltage and current, the solution eliminates problems often caused by other technologies, including high voltage at the test point, false test failures when crews hi-pot the cable, and unwanted leakage current during testing.

To learn more, visit
Eaton.com/opticalsensor

EATON
Powering Business Worldwide

Follow us on social media to get the latest product and support information.

Covering your needs for reduced exposure with network systems

Eaton's phasing and test rod for VisoBlock secondary disconnect has your crew covered when it comes to improving the safety of maintenance and testing on a network system. An accessory for the VisoBlock secondary disconnect, the phasing and test rod provides a safer method for isolating users when working on a network system.

Crews can more safely power a test set and check for proper phasing on the network protector without risking contact with energized parts. The phasing and test rod is a fully insulated rod that pulls isolated source and load side voltages to two touch ports on the front of the rods. For reduced exposure, these functions can also be performed with the network protector door closed.

The network protector test kit can be powered from the network bus without the need for connecting clips to an energized bus. When using the leads provided with the phasing test rod kit, all exposure to energized parts is eliminated. The carrying case offers safe storage of the phasing test rods and associated leads.

To learn more, visit
Eaton.com/nwp

We make what matters work.

EATON
Powering Business Worldwide

Follow us on social media to get the latest product and support information.


Xcel Energy®


N237BS