Implementation Considerations for Electronic and Physical Security Improvements for CIP-014

November 8, 2016

Agenda

- Introductions
- What Brought Us Here
- Utility Industry Observations
- Approach and Management of CIP-014
  - Threat and Vulnerability Assessments
  - Developing Mitigation Options
- Collaborative Approach to Physical Security
  - Mitigation Implementation
- Questions

Background

- PG&E's Metcalf – April 16, 2013
- Mainstream Press
  - *Wall Street Journal*
  - *USA Today*
- Media Drives Industry
- March 7, 2014 – FERC Directs NERC (ERO)

The attack was **"the most significant incident of domestic terrorism involving the grid that has ever occurred"** in the U.S., said Jon Wellinghoff, who was chairman of the Federal Energy Regulatory Commission at the time.

- *Wall Street Journal*, Feb. 4, 2014

"Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer," said the memo, which was reviewed by the *Journal*.

- *Wall Street Journal*, March 13, 2014

Additional Notable Events

- October/November 2015 Kershaw County, SC
- October 2015 Edmonton, Canada
- November 2015 Erie, Pa
- April 2014 Newfoundland, Canada
- August 2013 Lake Placid, FL
- September 2012 Tahlequah, OK
- **March 2015 Bakersfield, CA**
  - **First Night – 2 people spotted at 4 a.m., contract security call local PD**
    - **Damaged Transformer by cutting wires**
  - **Second Night – cut in through same hole**
    - **Breached control shelter, powered down equipment, cutting cords**

Why Does This Matter

- 2 Events Increase Security Spending
  - Ink on Paper – Regulation
  - Blood on Pavement – An Event
- Utilization of Insurgency Tactics
- Demonstrated
  - Preoperational Surveillance
  - Preoperational Planning
  - Detailed Target Selection
- Infrastructure – Water/Power
  - Soft Targets
  - Societal Reliance
- Leading Indicator of Dynamic Threat Shift?

Approach and Management of CIP-014

Industry Observations

- Utilities Being Active
  - CIP-014 Sites
  - “Company Critical” Sites
- NERC CIP-014 & Security Programs
- Prescriptive vs. Nonprescriptive
- Uncertainty of Minimums
- “Security” Firms Emerging
- Writing “The Story”

Conducting the Threat Assessment

- Terminology
  - Threat – who the bad guy is
  - Risk – what the bad guy could do
  - Vulnerability – how the bad guy can do it

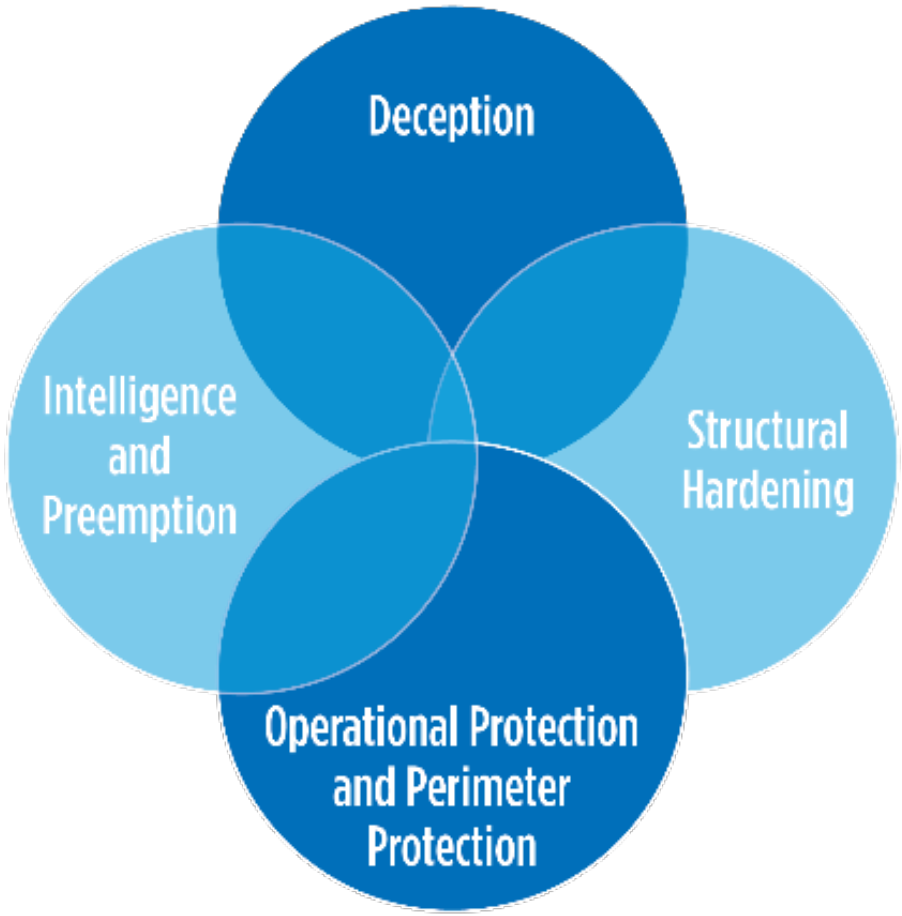
Conducting the Threat Assessment

- Based on Source Data
  - Federal Government (U.S. and Canada)
  - Provincial Government
  - Local Law Enforcement
  - Utility-specific Incident Reports
  - Utility-wide Incidents

Conducting the Threat Assessment

- Threat Assessment **IS**
  - Information to Guide Vulnerability Assessment
  - Information to Guide Adversary Assumptions
  - A Snapshot of Time
  - Perishable
- Threat Assessment **IS NOT**
  - Static
  - A Detailed List
  - Does Not Address Probability of Event

Conducting the Vulnerability Assessment



Conducting the Vulnerability Assessment

- Thinking Like the Adversary
  - Understanding the Attack Model
    - Event Selection
    - **Target Selection**
    - Preoperational Surveillance
    - Attack Mobilization
    - Attack Dry Runs
    - Attack Sequence

- Nuclear Security vs. Substation Security

Vulnerability Assessment

- Define the Adversary
  - Complex – Asset Shooting
  - Basic – Copper Theft
- Measure Site in Relation to Adversary Risks
  - Copper Theft
  - Trespass
  - Asset Shooting
  - Improvised Explosive Device
  - etc.

Risk Assumptions Sample 1

- **Asset Theft**: the unauthorized removal of facility assets.
  - Assumptions:
    - Adversary desires to remove the assets while minimizing potential detection or evidence that would lead to apprehension.
    - Assets subject to theft are to be both man portable spools and large truck transported spools of high value commodities, such as copper.
    - Motivation for asset theft events is not driven by a desire to harm a facility, but rather to acquire the asset components being removed.
      (Harm to the facility and operation can occur based on the type(s) of assets stolen and the downtime associated with asset replacement.)

Vulnerability Assessment

- Thinking Like the Adversary
  - Attack Considerations
    - Target Attractiveness
    - Ease of Attack – Success/Vulnerability
    - Likelihood of Attack
  - Adversary Attack Routes
  - Terrain
  - Population Densities
  - Identifying Pros and Cons

Vulnerability Analysis

Target Attractivness	Range
Very High	5
High	4
Medium	3
Low	2
Very Low	1

Likelihood of Event	Range
Very High	81-100
High	61-80
Medium	41-60
Low	21-40
Very Low	0-20

Vulnerability	Range
Very High	0.8
High	0.6
Medium	0.4
Low	0.2

Vulnerability Analysis

		Likelihoodof Event	Facility Attractiveness	Scenario Likelihood	Likelihood of Success	Risk
Sample Site 1	Forced Entry (Electric)	90	3	270	0.6	162
	Theft (Electric)	100	2	200	0.4	80
	Small Arms	10	5	50	0.8	40
	Sabotage	8	3	24	0.2	4.8
	VBIED	1	5	5	0.8	4
	Coordinated	1	5	5	08	4
	Standoff	1	5	5	0.6	3
	Explosive	3	1	3	0.2	0.6
Sample Site 2	Forced Entry (Electric)	90	1	90	0.4	36
	Theft (Electric)	100	1	100	0.2	20
	Small Arms	10	1	10	0.2	2
	Sabotage	8	3	24	0.8	4.8
	VBIED	1	5	5	0.8	4
	Coordinated	1	4	4	0.8	3.2
	Standoff	1	1	1	0.8	0.8
	Explosive	3	2	6	0.4	2.4

An Effective Security Plan

- **Deter – Target Shifting**
  - Lighting, signs and physical changes
- Detect – Identify Adversary
  - Intrusion detection and cameras
- Delay – Slow Access
  - Anti-rams devices, enhanced/secondary fences, asset barriers
- Respond – Documented Protocols for Owner and Law Enforcement

Defining Mitigation Strategy

- Devaluing the Target
  - Target Shift
  - Method Shift
- Deterrence Model
- Detection Model
- Peanut Butter Approach
- Develop Assumptions of Risks
  - Assessment without Assumptions

Defining Mitigation

- Based on:
  - Site Constraints – Rural vs. Urban
  - Industry Trends
  - Project Experience
  - Operational Tempo
  - Congruent with Security Strategy
  - Environmental Considerations
  - Proven Technologies

Mitigation Selection – Utility Considerations

- Security Officers
  - Cost
  - Observe and Report vs. Intervention
  - Liability Issues
  - Adversary Action
- SOC Personnel
  - Defining Response
  - System & Team Capabilities
  - Response CANNOT Start Until Detection

Mitigation Selection – Utility Considerations

- Cameras
  - Pros/Cons
    - Thermal
    - IR Illuminated
    - Visual Trespass
    - Over Abundance
    - Maintenance and Testing

Mitigation Selection – Utility Considerations

- Intrusion Detection
- Long Range Detection
  - Pros/Cons
    - Nuisance Alarms
    - Native Animals
    - Terrain
    - Maintenance and Testing

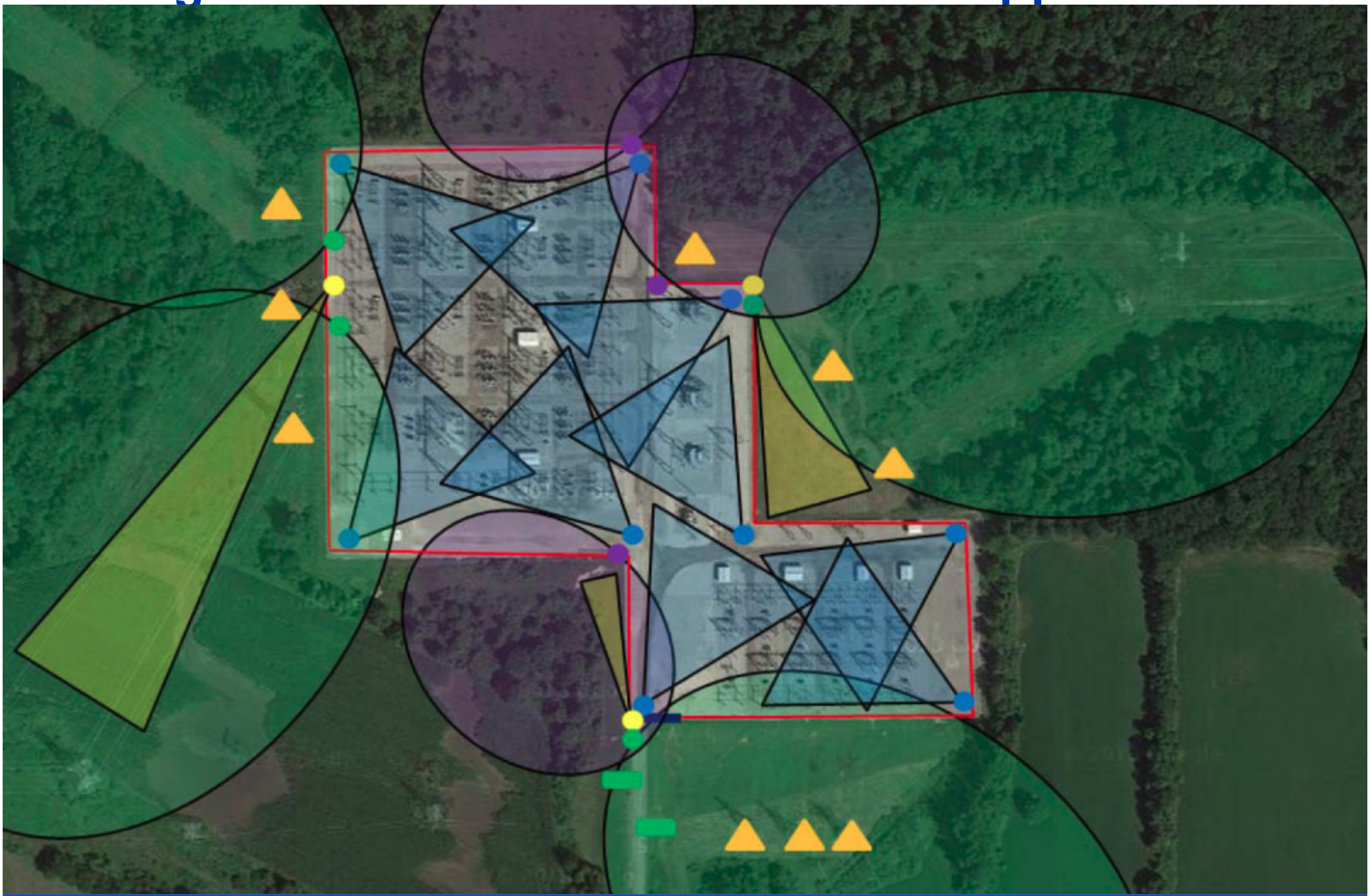
Mitigation Selection – Utility Considerations

- Fencing/Barrier Options
  - Pros/Cons
    - Walling Effect
    - Vegetation
    - Visibility

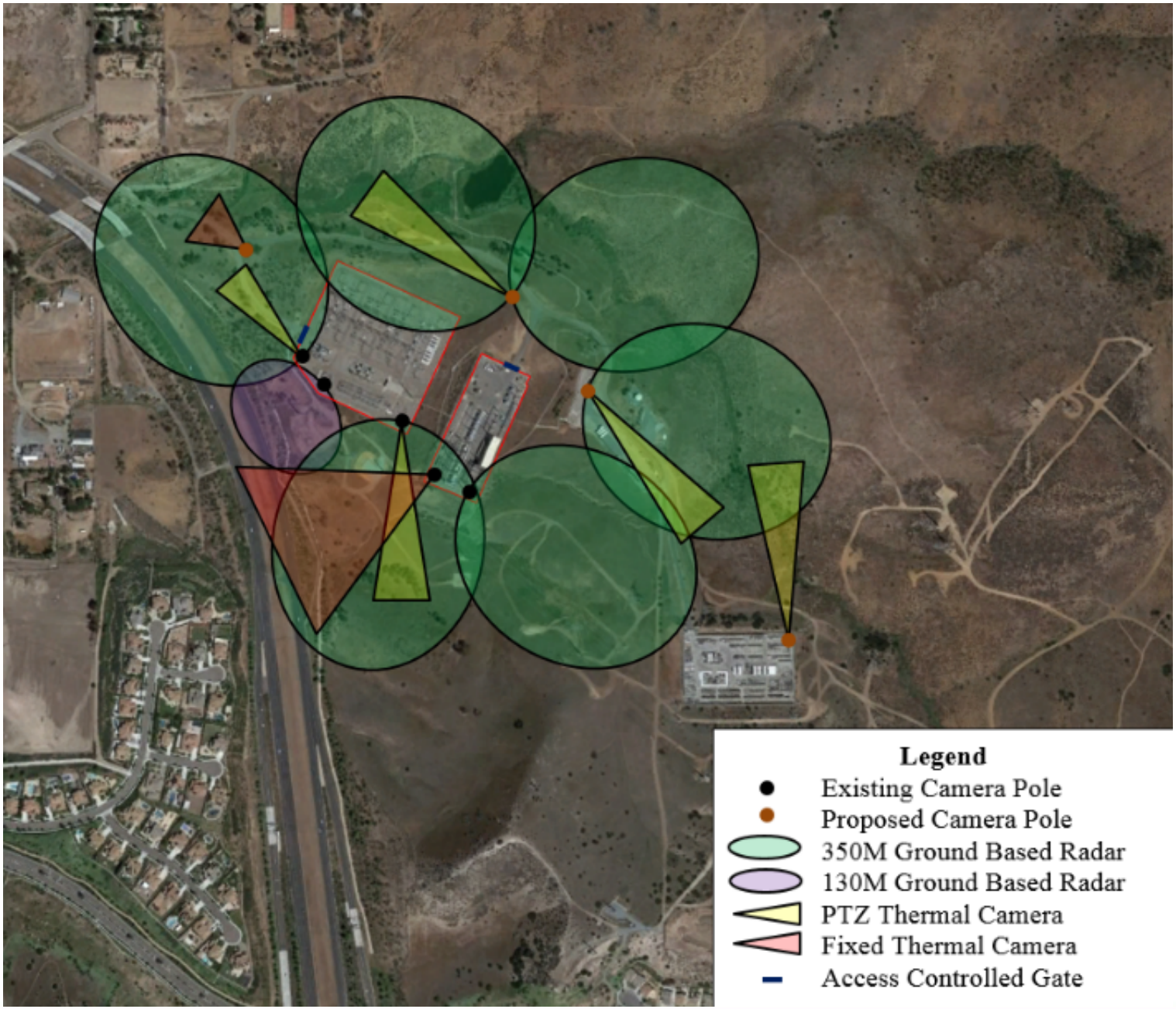
Mitigation Selection – Utility Considerations

- T-Walls/Ballistic Barriers
  - Pros/Cons
    - Ballistic?
    - Cost/Benefit
    - Visibility

Mitigation Selection – Consolidated Approach



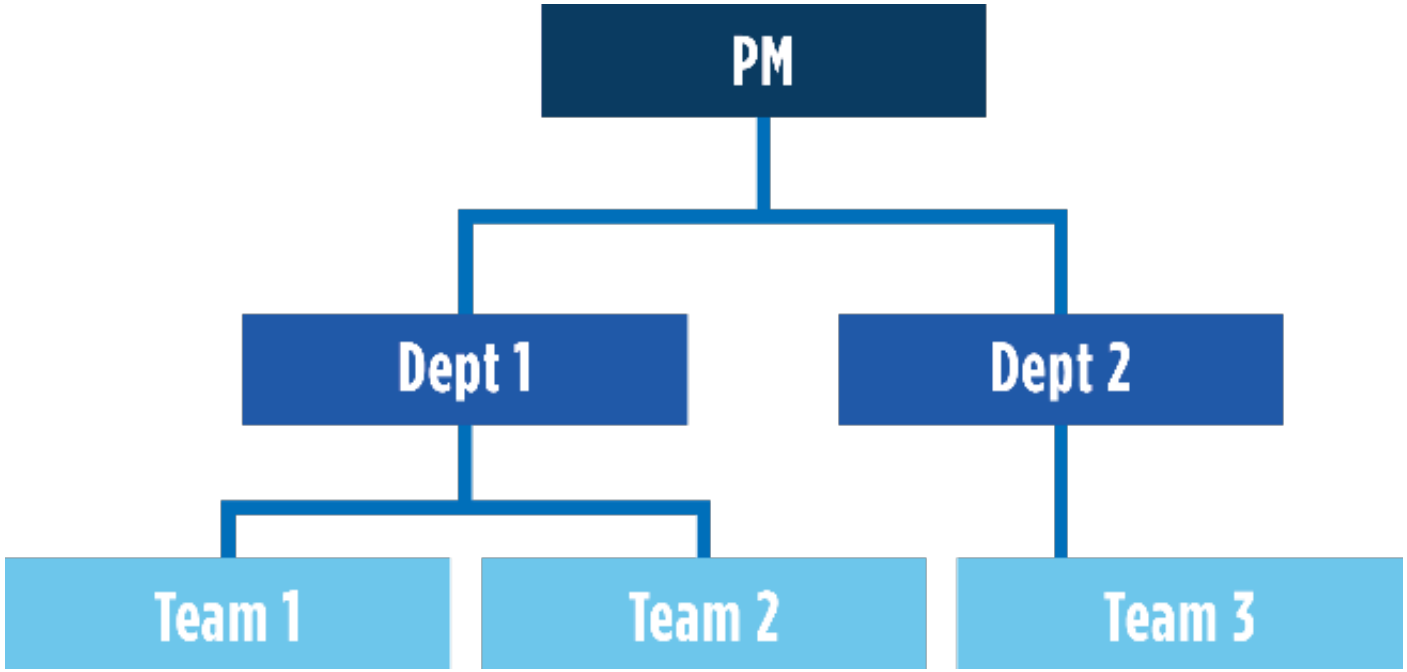
Mitigation Selection – Consolidated Approach



Implementation Considerations

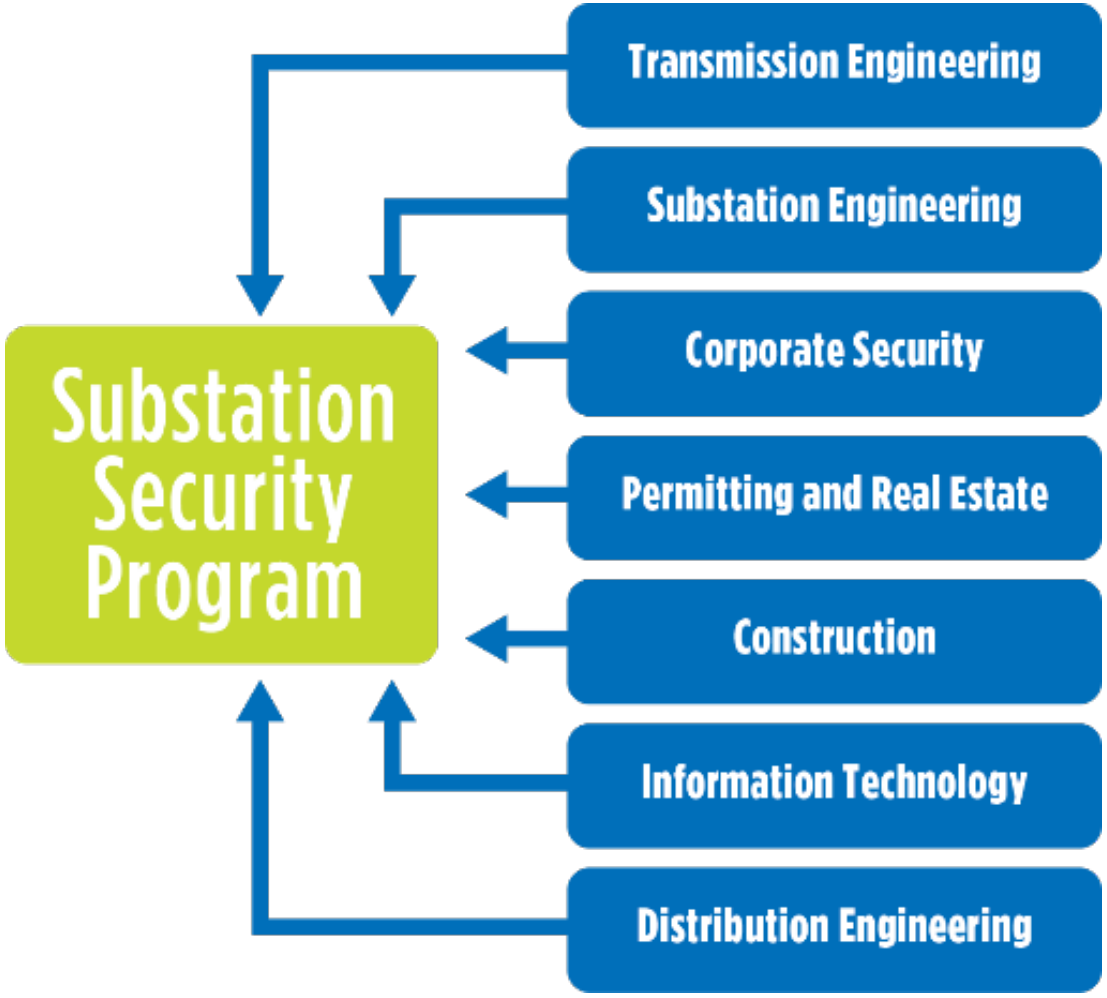
Successful Corporate Structure

- Identify Departments & Accountability
  - Assign Ownership to Single Group
  - Assign Task Manager from Each Department
  - Compliance & Support from Top Down



Collaborative Approach

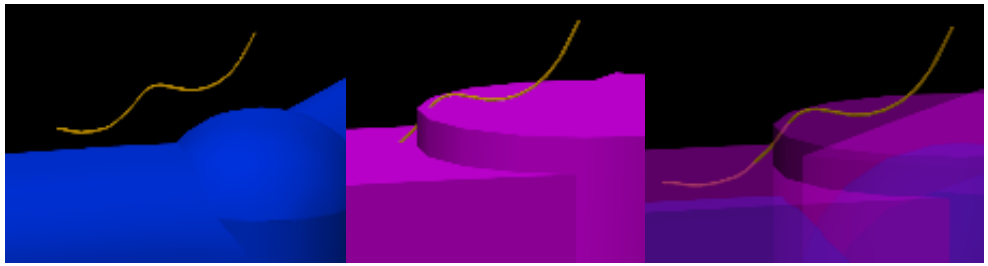
- Security Planning & Technologies
- Engineering Considerations
- Permitting, Real Estate and the Public
- And Everybody Else

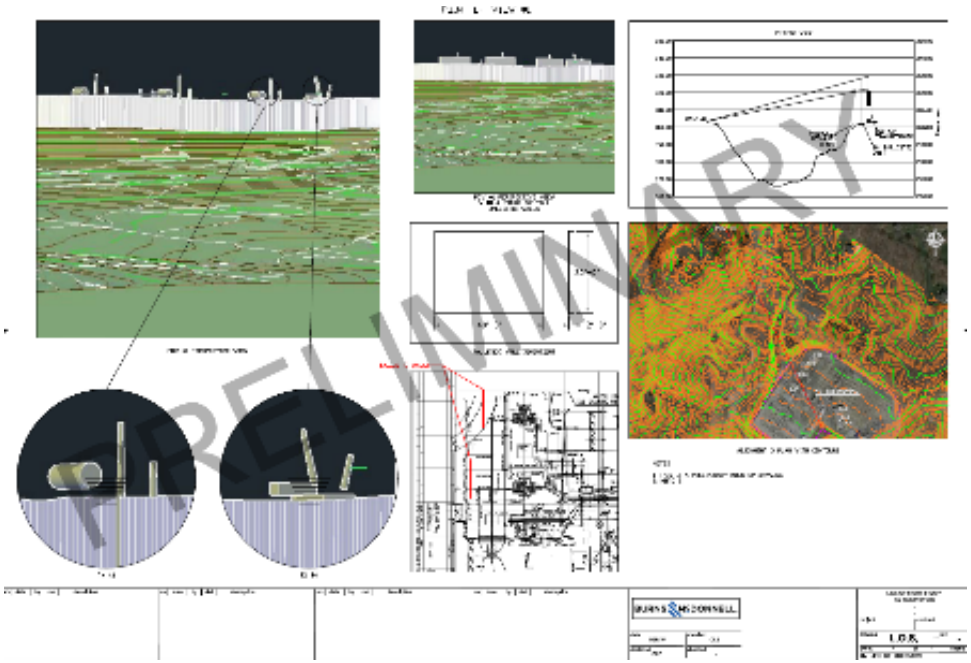


Engineering Considerations

Surveys and Line of Sight

- OH (LiDAR), UG, & Topo
  - LiDAR for LOS & **Clearances**
  - Obstruction Mitigation
  - Permitting Requirements
  - Manufacturing Accuracy
- LOS
  - Determine Exposure
  - Perimeter vs. Asset





Engineering Considerations

Asset Barriers

- Primarily Enclosures & Transformers
- Ballistic Protection
  - Based on LOS
  - UL 752
- **De-rating Concern**
- **Clearances**
- **Maintenance**

Ratings of Bullet Resistant materials as identified by:
UL 752

Rating	Ammunition	Weight (grains)	Weight (grams)	min fps	max fps	Number of shots
Level 1	9mm Full Metal Copper Jacket with Lead Core	124	8.0	1175	1293	3
Level 2	.357 Magnum Jacketed Lead Soft Point	158	10.2	1250	1375	3
Level 3	.44 Magnum Lead Semi-Wadcutter Gas Checked	240	15.6	1350	1485	3
Level 4	.30 Caliber Rifle Lead Core Soft Point (.30-06 Caliber)	180	11.7	2540	2794	1
Level 5	7.62mm Rifle Lead Core Full Metal Copper Jacket Military Ball (.308 Caliber)	150	9.7	2750	3025	1
Level 6	9mm Full Metal Copper Jacket with Lead Core	124	8.0	1400	1540	5
Level 7	5.56mm Rifle Full Metal Copper Jacket with Lead Core (.223 Caliber)	55	3.56	3080	3383	5
Level 8	7.62mm Rifle Lead Core Full Metal Copper Jacket Military Ball (.308 Caliber)	150	9.7	2750	3025	5
Level 9	.30-06 caliber rifle, steel core, lead point filler, FMJ (APM2)	166	10.8	2715	2987	1
Level 10	.50 caliber rifle, lead core FMCJ Military Ball (M2)	709.5	45.9	2810	3091	1
Shotgun	12-Gauge Rifled Lead Slug 12-Gauge 00 Buckshot (12 pellets)	1 0z. 1.5oz	28.3 42	1585 1200	1744 1320	3 3

Southern States
The quality name in high voltage switching

Ballistic Paneling

Ballistic Protection: physically securing substations.

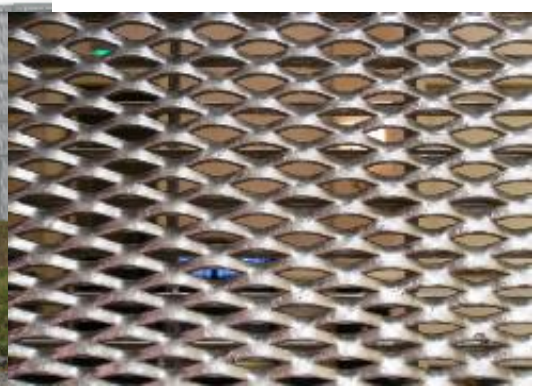
Engineering Considerations

Hardened Fence

- Perimeter Barriers
- K-Rated Gates
- Ballistic Protection
- Access Control
- Geotech Reports
- **Electrical Clearances**
  - Clearance Reports
- **UG Obstructions**
- **Site Drainage**

Standard	Rating	Vehicle Weight, lbs (kg)	Vehicle Speed, mph (km/h)	Rating	Allowable Truck Bed Penetration, ft (m)
DoS K-Ratings	K-Rating			L-Rating	
	K4	15,000 (6,800)	30 (48)	L1	20 to 50 (6.1 to 15)
	K8	15,000 (6,800)	40 (64)	L2	3 to 20 (0.9 to 6.1)
	K12	15,000 (6,800)	50 (80)	L3	< 3 (<0.9)
ASTM F2656-07 Standard	M-Designation			P-Rating	
	M30	15,000 (6,800)	30 (48)	P4	> 98 (> 30)
	M40	15,000 (6,800)	40 (64)	P3	23.1 to 98.4 (7.0 to 30)
	M50	15,000 (6,800)	50 (80)	P2	3.31 to 23 (1.0 to 7.0)
				P1	< 3.3 (< 1.0)

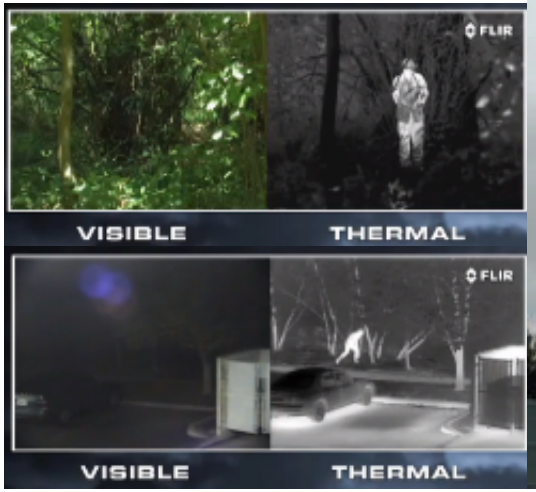
TABLE 1

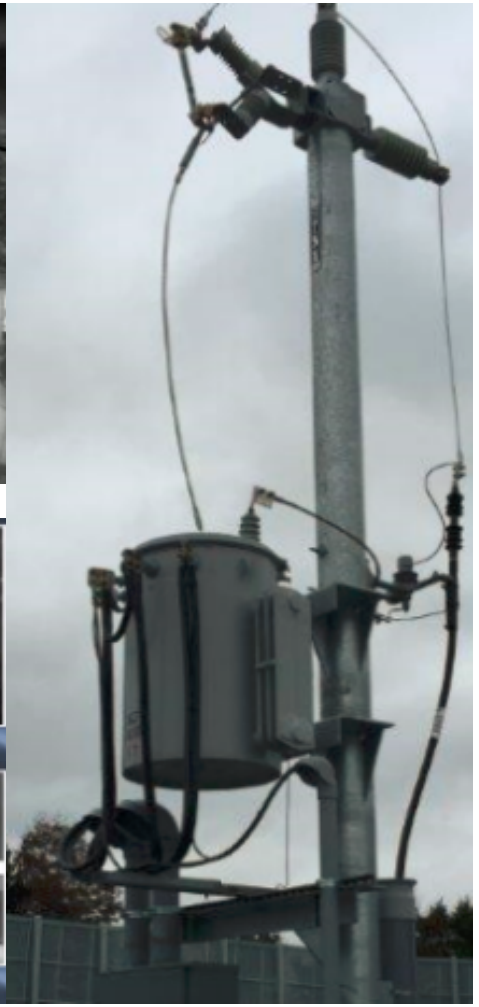


Engineering Considerations

Technology & Station Service

- Coordination w/ Security
  - Internal & External
- **Power Analysis**
  - Independent
  - Uprate
- **Bandwidth** (IT)
  - Leased Lines
- Telco Relocation

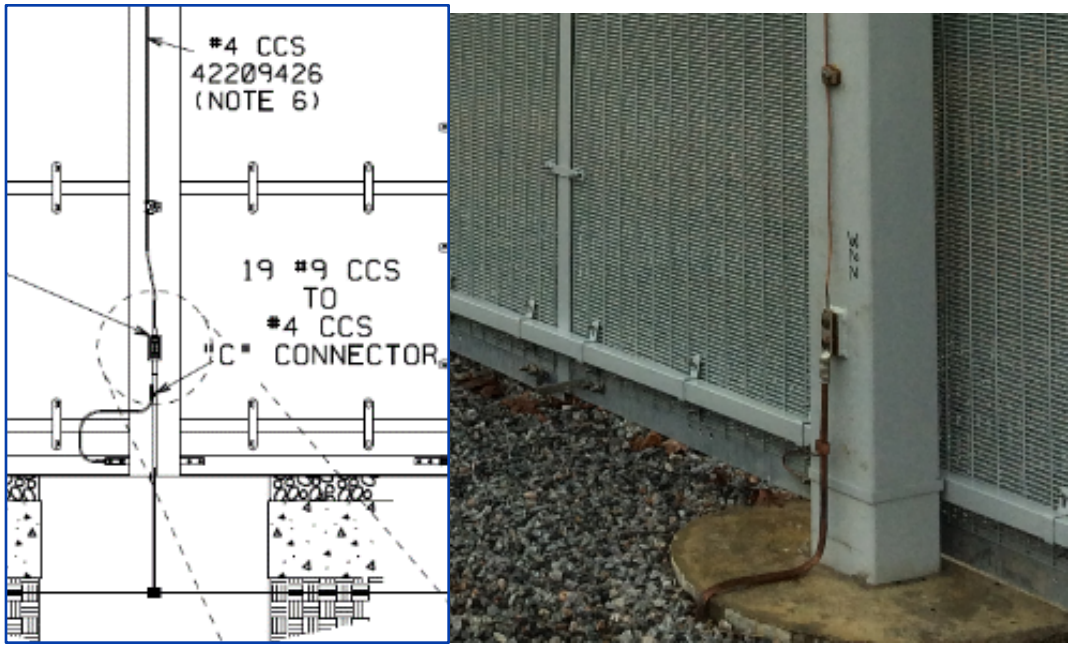




Engineering Considerations

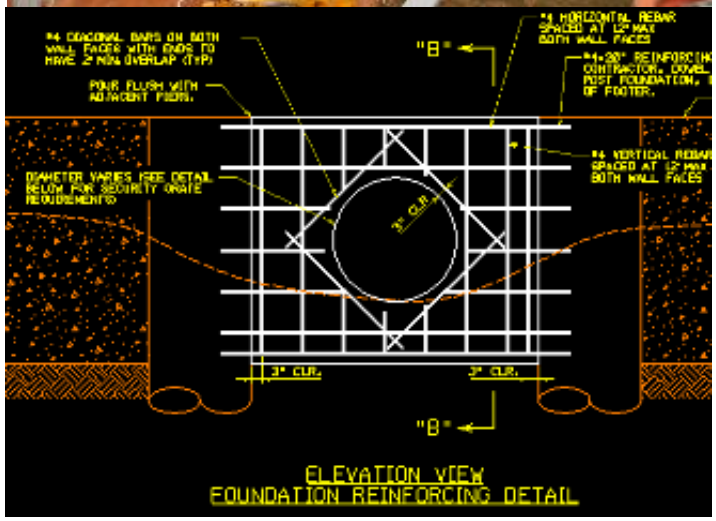
Grounding

- **Powder Coating**
- Panels & Posts
- Gates & Moving Parts
- Develop Standards
  - Manufacturer Solutions



Construction, Operations & Maintenance

- Construction
  - Survey Staking
  - E&S Controls
  - Temporary Fencing
- Operations & Maintenance
  - Ingress & Egress
    - Card Scanners
    - Internal Gate Opening
    - **Motorized (Roll-ups)**
    - Culverts

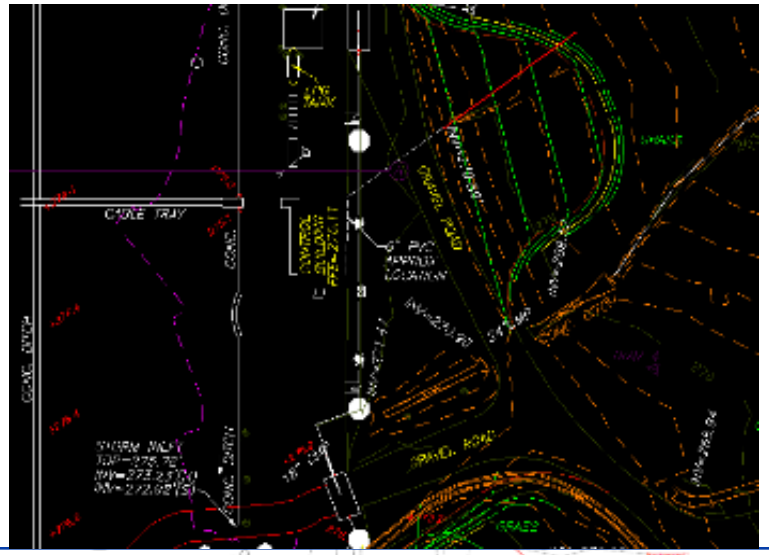


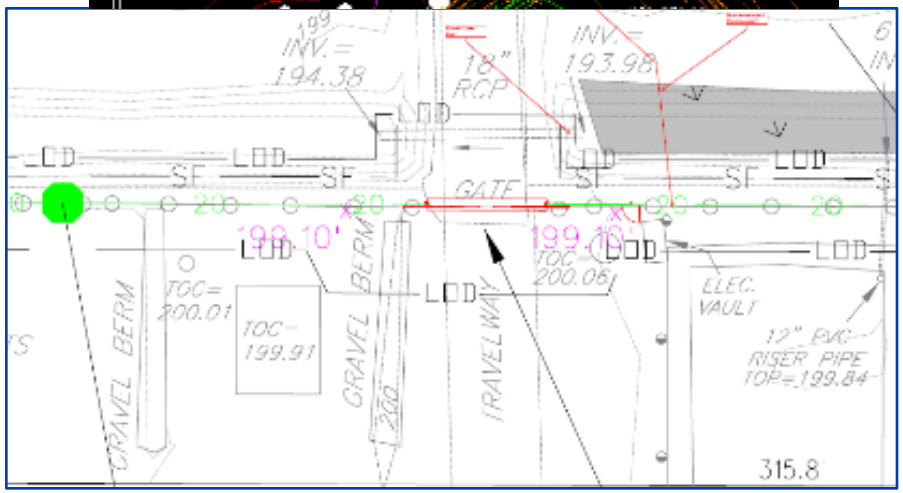
Permitting, Real Estate and the Public

- Assess the Needed Permits Immediately
  - Local
  - State/Provincial
  - Federal
- Rights and Restrictions of Current Site
  - Security Design Changes
  - Frequent Communication with Construction
- Future Needs at Site
  - Maintain Relationships

Permitting, Real Estate and the Public

- Common Requirements
  - Site Plan Amendments
  - Land Disturbance
  - Building Permits
  - Conditional Use Permits
- Construction Limitations
  - Linear Feet – Disturbed Earth
  - Dusk-to-Dawn Lighting
- Constant Communication





Timing is Everything

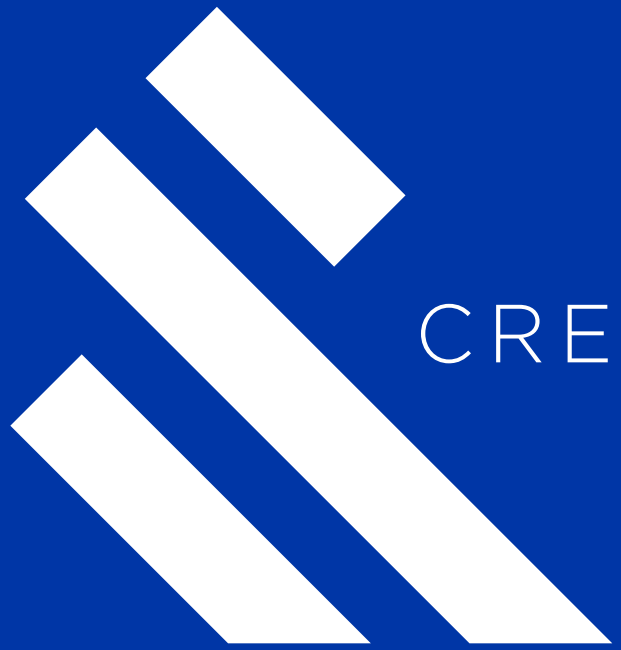
- Meetings Must be Scheduled
  - Local law enforcement
  - Neighbors
  - Public officials
- Develop a Plan
  - Level and means of communication
  - Consistent messaging
- *What do you know that we should know?????*

Anticipate Reaction

- Privacy Concerns
  - Cameras, motion sensors and lighting
  - Sound “gun shot” detectors
- Physical Changes
  - Fence heights or coloration
  - Drainage changes
  - Landscape removal

Questions

Robert J. Hope, CPP
Manager – Security Consulting
Burns & McDonnell Engineering
816-349-6754
rjhope@burnsmcd.com



CREATE AMAZING.