Substation Physical Security

James Day, Physical Security Program Manager
Sacramento Municipal Utility District

APPA Engineering & Operations Technical Conference

Powering forward. Together.

SMUD®

Agenda

- SMUD Fun Facts
- Knowledge check
- What are we protecting from.
- What are we protecting against.
- What is needed for an effective attack.
- What is needed to defeat an attack.
- How do we know what to protect.
- Closing thoughts.

SMUD – Fast Facts

General Information

- SMUD employs approximately 2,000 individuals
- Service area of 900 square miles
- Population served is 1.4 million
- ~625,000 customers
- 477 miles of transmission
- Peak Load (MW):
  3,300 (SMUD), 5,000 (BANC)

Generation Specifics

- 1,000 MW of thermal generation
  (9 BES Units)
- 688 MW Hydro generation
  (7 BES Units)
- 100 MW of solar generation
- 230 MW of wind generation within the California ISO
- 50% Power from non-carbon emitting resources

NERC Registrations

TOP, TO, GO, GOP, TSP, TP, PA, RP, DP, PSE, LSE

- Also performs BA reliability compliance for the BANC

SMUD™

Knowledge Check

- Which answer best describes the characteristics of sound physical security principles:

A. Knowledge + Capability + Intent.

B. Threat + Vulnerability + Consequence = Risk.

C. Protection in depth.

D. All of the above.

E. None of the above.

(Answer on Slide 9)

What Are We Protecting From?

- Safety
  - Loss or degradation of protection systems or equipment that would create a hazard to employees and the public.
- Reliability
  - Loss of electric power system integrity and availability.
- Brand
  - Loss of reputation and confidence of customers and community.
- Revenue
  - Loss of revenue due to service disruption, labor and material costs.
- Compliance
  - Penalties, sanctions and publicity for non-compliance to regulatory requirements.

What Are we Protecting Against

What We Are Protection Against

- Unauthorized intruders
- Vandals
- Copper thieves
- Violent radicals and extremists
- Terrorists, foreign and domestic
- Disgruntled customers
- Disgruntled employees (insider threat)

What Is Needed To Effectively Attack

- Knowledge
  - The information you have or is available to you about your intended target.
- Capability
  - The ability of an adversary to attack with a particular attack method.
- Intent
  - The desire or design to conduct a type of attack or to attack a type of target.

What Is Needed To Defeat An Attack

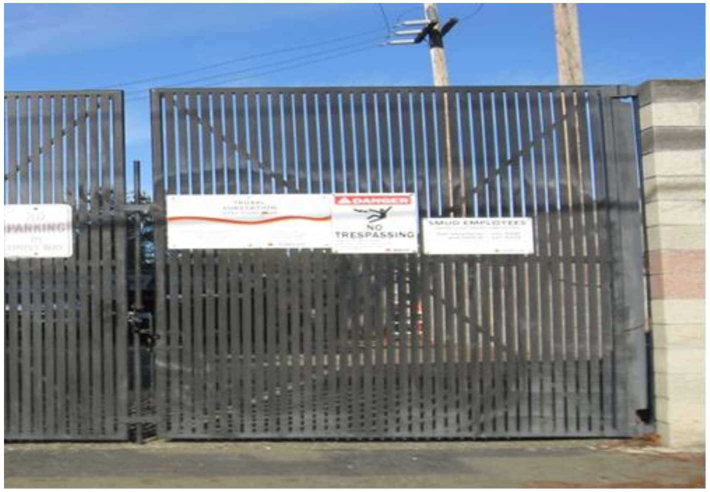
- Physical Security Concepts

  The following concepts provide a physical protection systems approach in designing and implementing physical security measures that will mitigate the impact on assets should a physical attack occur: (Answer to knowledge check is E, None of the Above)

  - Deter
  - Detect
  - Delay
  - Communicate
  - Assess
  - Respond
  - Intelligence
  - Audit

Deter

- Visible physical security measures installed to induce individuals to seek other less secure targets.
  - – Signage to warn intruders.
  - – Perimeter barriers.
  - – Security lighting.
  - – Clear zones
  - – Security presence, fixed or random.



Detect

- Physical security measures installed to detect unauthorized intrusion and provide local and/or remote intruder annunciation.
  - Intrusion detection.
  - Cameras (CCTV).

Delay

- physical security measures installed to delay an intruder's access to a physical asset and provide time for incident assessment and response.
  - Fences
  - Block walls
  - Gates
  - Bollards
  - Hardened locks

Communicate

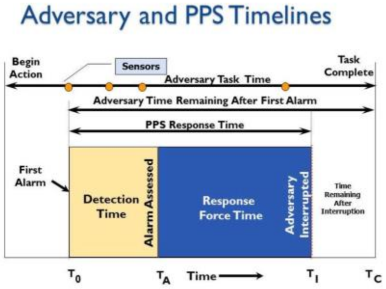
- Communication systems utilized to send and receive alarm/video signals and voice and data information. Also, includes the documented process to communicate detected intrusions.
  - Physical Access Control System ("PACS").
  - Fiber
  - Microwave
  - Modem
  - Wireless

Assess

- The process of evaluating the legitimacy of an alarm and the procedural steps required to respond.
  - Nuisance alarm.
  - Employee generated.
  - Valid intrusion.
    - What are you going to do about it?

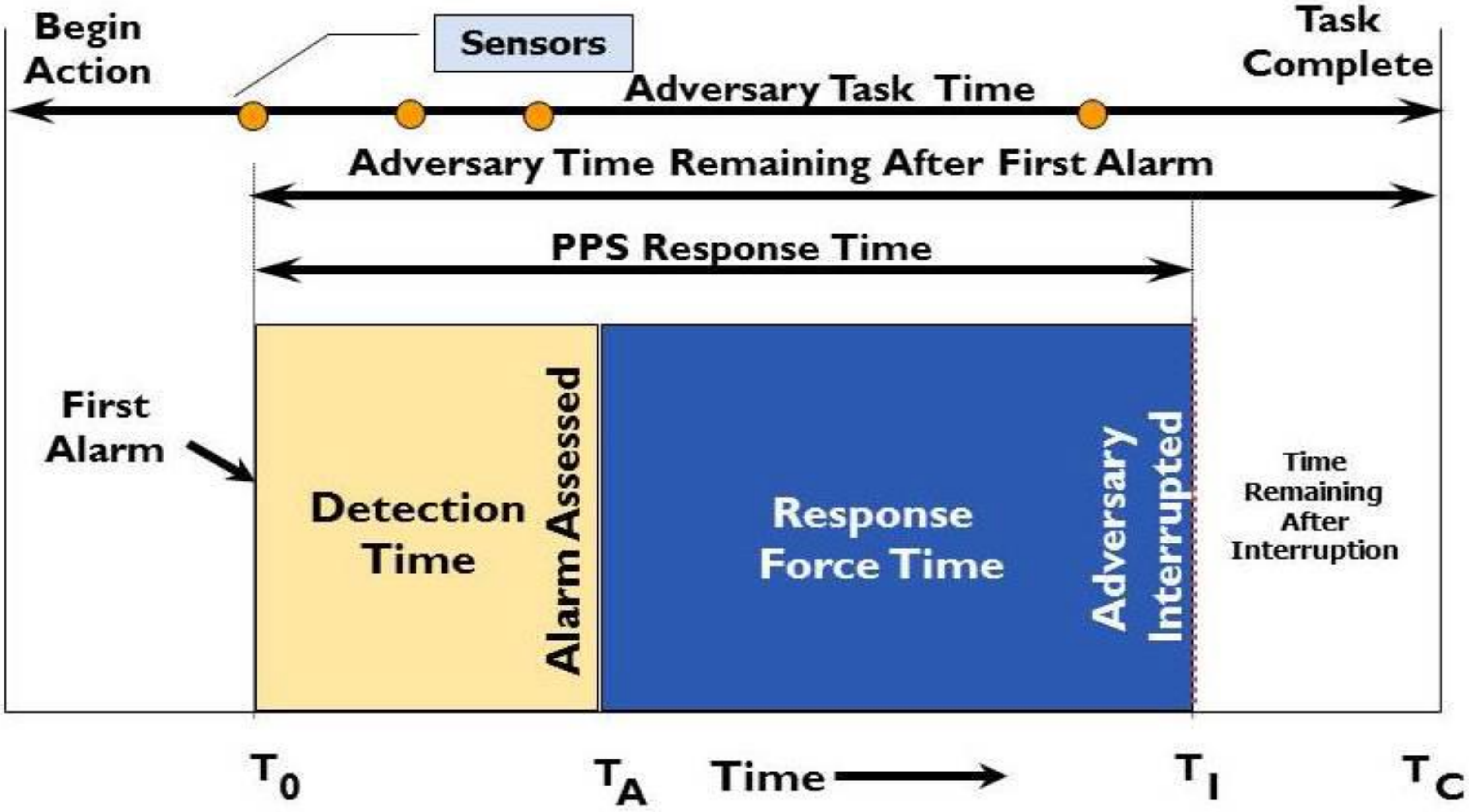
Respond

- The immediate measures taken to assess, interrupt, and/or apprehend an intruder.
  - Do you have armed drones available? If not, you're likely limited to your response plan.
  - Will your physical controls allow for attack intervention or merely forensics?
  - Who will respond?
    - Guard force
    - LLEA
    - Operations personnel


Adversary and PPS Timelines

  - How long can you delay vs. how long will your response take to get on site?
    - 15 minute delay + 30 minute response = problem

Adversary and PPS Timelines



Intelligence

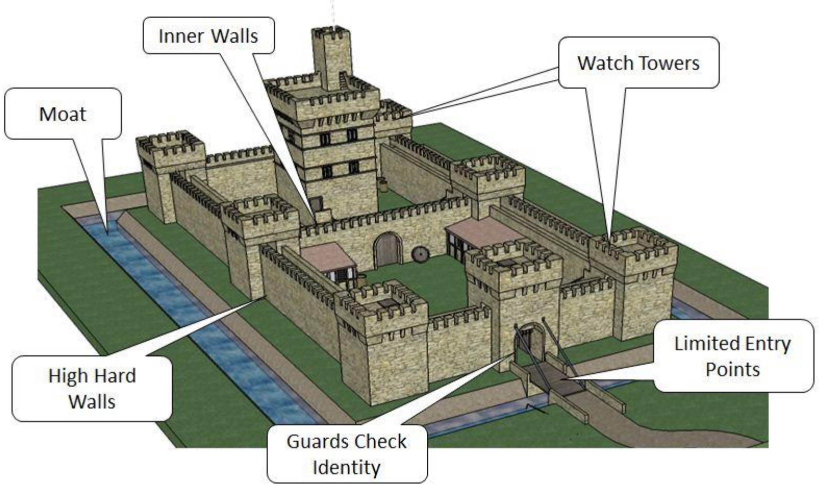
- Measures designed to collect, process, analyze, evaluate and interpret information on potential threats.
  - – Local law enforcement.
  - – State and Federal agencies.
  - – Local and national news
  - – Your community.

Audit

- The review and inspection of physical security measures to evaluate effectiveness.
  - Response plans.
  - Security assessments.
  - Event analysis.
  - Maintenance & Testing.

Protection in Depth

- Adversary must defeat or avoid numerous varied types of overlapping protective devices to achieve objective.



  - System redundancy
  - Complimentary sensors
  - Complimentary barriers
  - Guards and Local Law Enforcement

How Do We Know What To Protect, And What It Will Take To Protect It

- Vulnerability and Risk Assessments.
  - – Like opinions, everybody has one.
  - – Some examples:
    - Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability (CARVER)
    - DHS Enhanced Critical Infrastructure Protection Infrastructure Survey Tool (ECIP/IST)
    - Attack Tree Modeling
    - Threat, Hazard Identification and Risk Assessment (THIRA)
  - – Find what works for you.

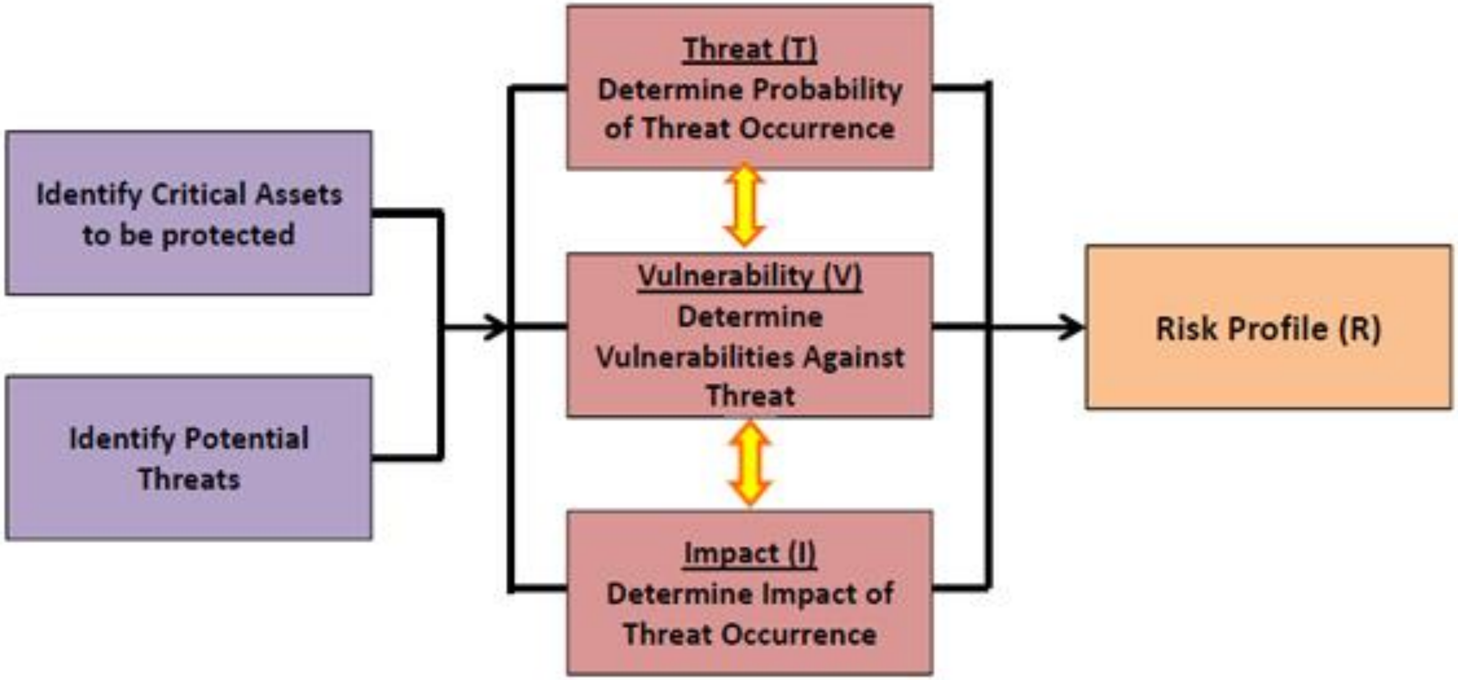
Vulnerability and Risk Assessment

- Can be very resource intensive.
- Not a one man job.
  - Physical security.
  - Cyber Security.
  - Yes, engineers and operators.
  - Facilities personnel
  - Local, State and Federal agencies.

VR Assessment Basics

- They mostly all boil down to a variation of:

Risk Assessment Methodology



Identify Critical Assets to be protected

Identify Potential Threats

Threat (T)
Determine Probability of Threat Occurrence

Vulnerability (V)
Determine Vulnerabilities Against Threat

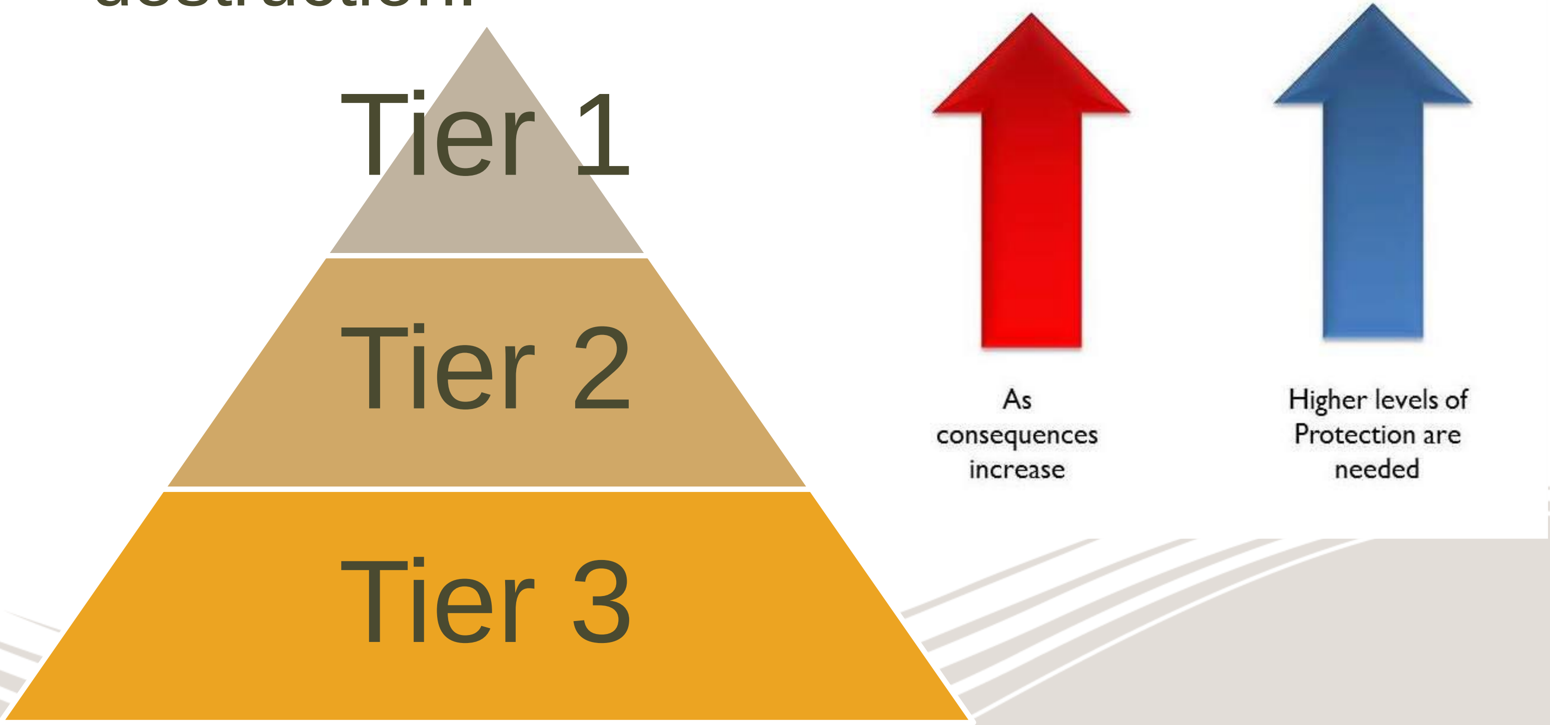
Impact (I)
Determine Impact of Threat Occurrence

Risk Profile (R)

Risk = Threat (T) x Vulnerability (V) x Impact (I)

Tiered Approach to Physical Security

- Apply security resources in a proportional manner based on the impact of loss or destruction.



Tier 1

Tier 2

Tier 3

As consequences increase

Higher levels of Protection are needed

Closing Thoughts

- It is better to have a plan and not need one than to need a plan and not have one.
  - Security Plans
  - Response Plans
  - Business Continuity
  - Security Design Standards
- Partner with Local Law Enforcement
  - Information Sharing
  - Tours
  - Access to Facilities
  - Training
- Good Physical Security Practices = Compliance

Questions?

Powering forward. Together.

SMUD®