

PHYSICAL SECURITY YESTERDAY, TODAY & TOMORROW

ADVANCED TECHNIQUES FOR SUBSTATION BALLISTIC THREAT ANALYSIS

Alan Sowell
VP, Project Management
POWER Engineers

Purpose & Learning Objectives

The purpose of this program is to help attendees gain a better understanding of substation physical security systems and standards.

At the end of this presentation, you will be able to:

- Describe the CIP-014 Physical Security Standard and why it was developed
- Implement current physical security analysis processes and tools
- Describe the future of physical security (threats, requirements & analysis)



THE PAST



FLORIDA PUBLIC POWER



Metcalf Attack

- April 16, 2013
- Critical Communication Lines Cut
- >120 Shots Fired
- 17 Transformers Severely Damaged
- **\$15M** in Damages



The Problem

CIP-014-2 - Identify and protect grid assets, that if rendered inoperable or damaged from a physical attack could result in instability, or cascading/catastrophic failure. Protect the critical assets in a substation that may cause a catastrophic failure on the system.



THE PRESENT



FLORIDA PUBLIC POWER



Recent Attacks



Duke

- Rammed Gate
- Shot Transformers
- **45,000** Without Power



Tacoma

- 4 Substations Vandalized
- Transformers Damaged
- **14,000** Without Power

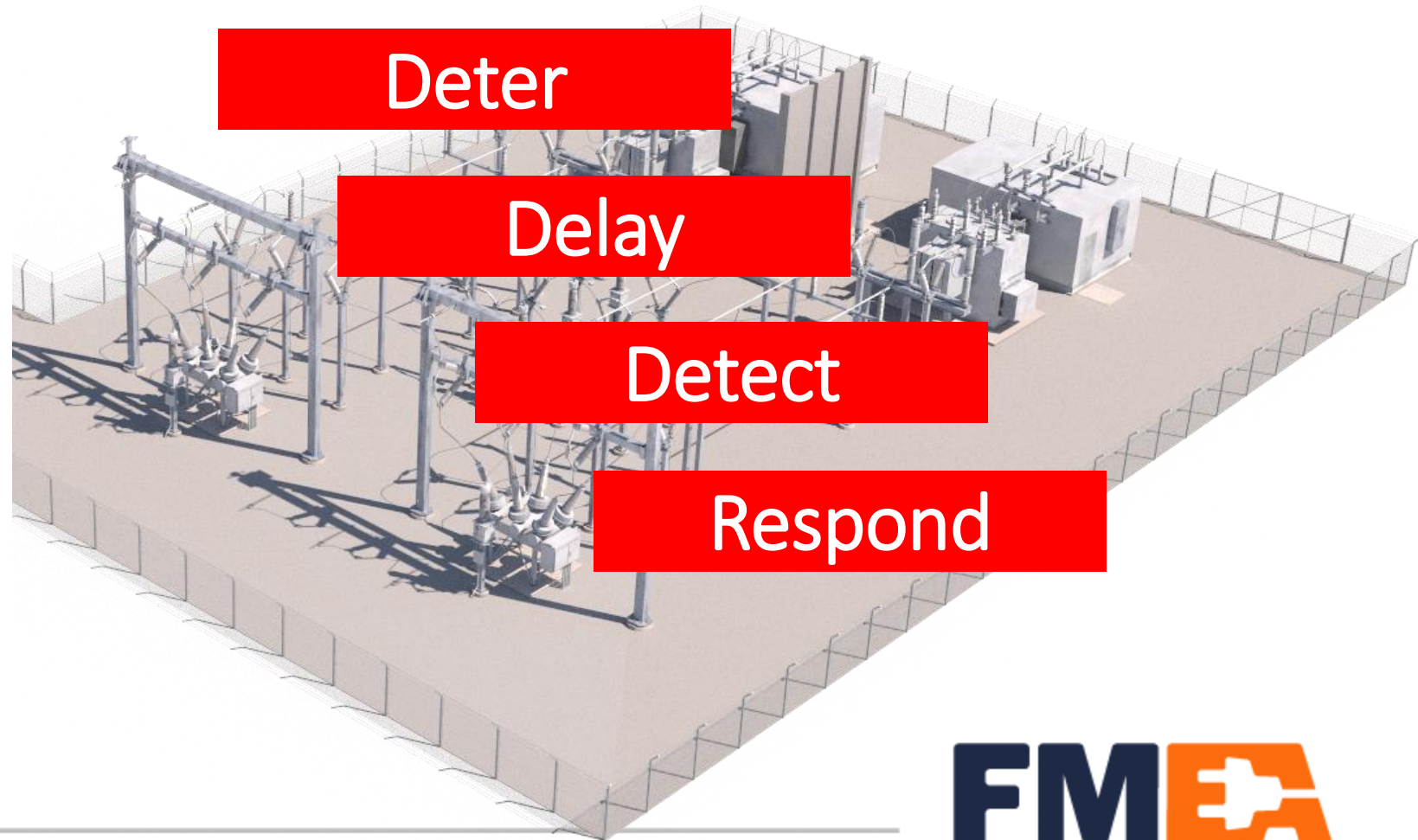


BGE

- Conspiracy to Attack Multiple Substations
- **1M** Without Power if Successful

Physical Security Systems

- Ballistic Rated Walls
- Gates
- Ground Radar
- Access Control
- CCTV
- Fence Detection
- Layered Approach



Security Cameras and Radar



Upgraded Gate & Expanded Metal Fence



Ballistic Walls



Transformer Ballistic Wall



Transformer Wraps



SE GP T NP PT 14
Unrestricted © Siemens Energy, 2021

SE GP T NP PT
Unrestricted © Siemens Energy,

Example of Reduced Risk Progress Based on Mitigations Over Time

System Control Center Threat Vectors	2016 Assessment		2018 Assessment		2021 Assessment	
	Probability of Success		Probability of Success		Probability of Success	
	Weighting	Ranking	Ranking	Success Prob.	Ranking	Success Prob.
Vehicle Borne Improvised Explosive Device (VBIED)	4.0	Very High	3.0	High	3.0	High
Portable Improvised Explosive Device (IED)	4.0	Very High	3.0	High	1.0	Low
Forced Entry Attack	2.0	Medium	1.0	Low	1.0	Low
Coordinated Assault	1.0	Low	3.0	High	3.0	High
Sabotage	1.0	Low	1.0	Low	1.0	Low
Small Arms Ballistic Attack	1.0	Low	1.0	Low	1.0	Low
Direct Fire Weapon Ballistic Attack	1.0	Low	1.0	Low	1.0	Low
Asset Theft	1.0	Low	1.0	Low	1.0	Low

THE FUTURE



FLORIDA PUBLIC POWER



Ground Radar, Stereo Cameras and AI



FLORIDA PUBLIC POWER

FMEA
FLORIDA MUNICIPAL ELECTRIC ASSOCIATION

Ground Radar with AI

Target detected inside Area of Interest, classified as Human by AI

AI

MORE VIDEOS

0:09 / 0:51

Time	Priority Level	State Level	Slide Name	Message	Source	Owner
17:57:14 11/03/2019	1	1	New	External Event	WAGS-ALARM	
17:57:51 11/03/2019	1	1	New	External Event	WAGS-ALARM	
17:58:36 11/03/2019	1	1	New	External Event	WAGS-ALARM	

DESKTOP-408155A

YouTube

Ground Radar with AI

The image is a screenshot of a video player. On the left, there is a dark sidebar menu with the following items: OPTIONS, PROFILES, PRESETS, RADARS, CAMERAS (with a sub-item 'Hikvis1'), ALARM ZONES, and COVERAGE ZONES (with a sub-item 'Coverage_ihuv2f'). Below the menu is an 'EDIT COVERAGE ZONE' panel with a text input for 'Name' containing 'Coverage_ihuv2f', and radio buttons for 'Area type' with 'Include' selected. A 'MORE VIDEOS' button is also visible. The main video area is split into two parts. The left part shows an aerial satellite view of a road with a green radar beam and a purple detection zone. A red speech bubble points from the text 'Easily Mask out roads & unwanted areas' to a road in the image. The right part shows a video feed of two people walking in a field, with green bounding boxes around them. A red speech bubble points from the text 'Detect only in Area of Interest' to the people in the video. In the top right corner of the video player, there are 'Watch later' and 'Share' buttons. A small tooltip at the bottom of the radar view says 'Click cancel to undo changes. Drag handles or markers to edit features.'

Watch later Share

Easily Mask out roads & unwanted areas
Detect only in Area of Interest

Click cancel to undo changes.
Drag handles or markers to edit features.

EDIT COVERAGE ZONE ✕
Name Coverage_ihuv2f
Area type
● Include
● Exclude
MORE VIDEOS
Hikvis1
Coverage_ihuv2f

Ground Radar with AI

The screenshot displays a ground radar interface. On the left is a dark sidebar with a menu containing: OPTIONS, PROFILES, PRESETS, RADARS, CAMERAS (with a sub-item 'Hikvis1'), ALARM ZONES, and COVERAGE ZONES (with a sub-item 'Coverage_ihuv2f'). The main area is split into two panels. The left panel is an aerial view with a purple radar beam and a green target icon. A red callout box points to this area with the text: "Vehicles on the road detected by radar but masked out by AI". The right panel is a live video feed from a camera labeled 'Hikvis 1', showing a person walking on a path with green bounding boxes around them. A 'Target Info' box at the bottom center of the video feed displays: "person", "5.94km/h", "49.38m", "conf.0.99", and "detected by sr5001.98". In the top right corner of the video player, there are "Watch later" and "Share" buttons. A "MORE VIDEOS" button is located in the bottom left corner of the interface.

FLIR Drone Jamming Device





FLORIDA PUBLIC POWER

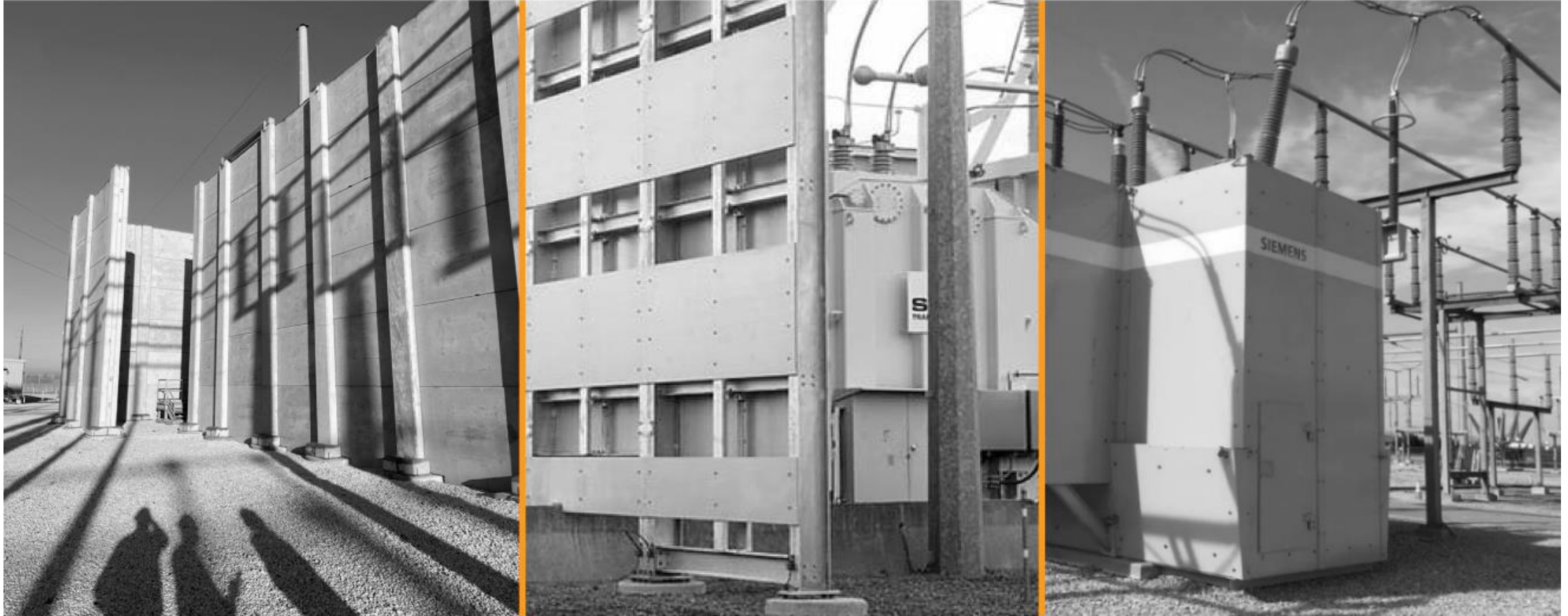
FMEA
FLORIDA MUNICIPAL ELECTRIC ASSOCIATION



FLORIDA PUBLIC POWER

FMEA
FLORIDA MUNICIPAL ELECTRIC ASSOCIATION

A BRUTE FORCE APPROACH TO CIP 14.2 PROTECTION



BALLISTIC WALL

TRANSFORMER BALLISTIC WALL

TRANSFORMER WRAP

The Challenge



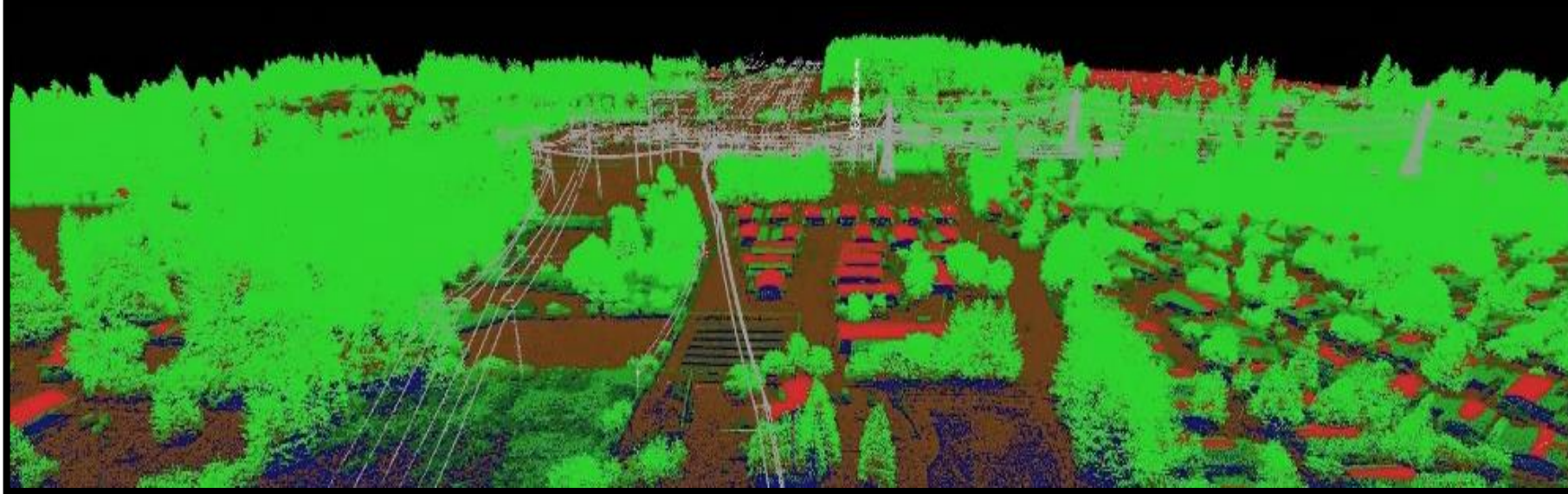
Question

“How can we reduce construction costs for security walls and maintain Physical Security?”

Answer

“...build only what’s needed.”

Data Collection





E-ISAC

- Quality analysis and rapid sharing of security information on how to mitigate complex threats to the grid.
- Occasionally over hundreds of reports of physical attacks per month



What does this mean?

- Recent uptick in physical attacks to NON CIP-014 substations
- Subsequent loss in revenue for Utilities/PUCs
- Loss of critical customers (i.e., hospitals, Big Tech)
- Increased likelihood of attacks
- Likely expansion of CIP-014
- Increased priority to protect critical assets
- Increased need for security experts and analysis tools
- Passing along the costs to rate payers?
- Improve communication and awareness of potential threats



QUESTIONS



For Questions on any of the concepts or technologies in this presentation, Contact:



Chris Ott
Sr. Project Engineer
Physical Security
503-892-6869



Alan Sowell
VP, Project Management
770-605-1700

