Cyber-intrusion Auto-response and Policy Management System (CAPMS)

Final Scientific/Technical Report

Project Number: DE-OE0000675
Period of Performance: Oct 1, 2013 – Sep 30, 2015

November 11, 2015

PREPARED FOR:

U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
1000 Independence Ave., S.W.
Washington, D.C. 20585

PREPARED BY:

TABLE OF CONTENTS

Table of Figures

Table of Tables

Project Number:	DE-OE0000675
DOE PM:	James Briones
ViaSat PM:	Steve Lusk
Period of Performance:	Oct 1, 2013 – Sep 30, 2015
Status:	Complete

1 Introduction

The Cyber-intrusion Auto-response and Policy Management System (CAPMS) project was funded by a grant from the US Department of Energy (DOE) Cybersecurity for Energy Delivery Systems (CEDS) program with contributions from two partner electric utilities: Southern California Edison (SCE) and Duke Energy. The goal of the project was to demonstrate protecting smart grid assets from a cyber attack in a way that "does not impede critical energy delivery functions." This report summarizes project goals and activities for the CAPMS project and explores what did and did not work as expected. It concludes with an assessment of possible benefits and value of the system for the future.

This report was written in accordance with the "Scientific/Technical Report" requirements defined in DOE F 4600.2 section B.

1.1 Project Overview

The CAPMS project performed research and development followed by live demonstrations of a new system designed to detect and respond to sophisticated cyber intrusions against electric utility systems. This effort expanded the software capabilities of ViaSat's Trusted Network Platform (TNP) product along with constructing realistic simulations of energy delivery systems as well as attack scenarios at both partner utility locations.

The program was divided in two phases. The first phase addressed Research & Analysis, Design, Development, Integration & Test of the Cyber-intrusion Auto-response and Policy Management System capabilities at ViaSat test facilities. The second phase supported demonstrations of these new capabilities in an active power utility test grid at each partner's test facility.

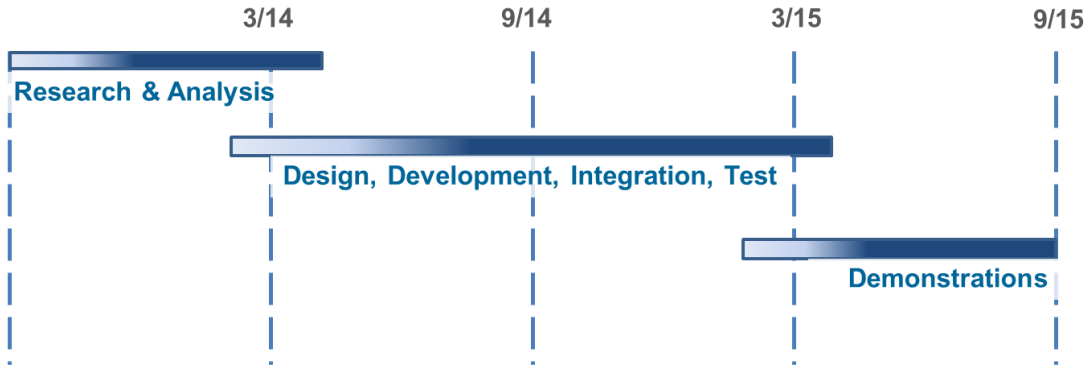

Figure 1: CAPMS Notional Schedule

For both SCE and Duke Energy we:

- Designed and built realistic utility control systems for a wide range of control networks: synchrophasor (transmission), substation protection relays (distribution), and microgrid (distributed energy resources.)
- Evaluated vulnerabilities of these systems to combined cyber and physical attacks.

- Built systems that could carry out some of these attacks in a lab environment.
- Built the CAPMS system and attendant security policies that are capable of detecting and responding to such intrusions.
- Explored response interactions between the security system, the operator, and the energy control systems.

Along the way we researched and prototyped:

- A variety of risk assessment approaches for industrial control systems.
- A variety of notations, algorithms and techniques for modeling cyber attacks.
- Software technology to enable us to build software able to correlate events from many sources mainly using message bus integration and event-driven services.
- Methods for providing real-time situational awareness to the operator.
- Opportunities to respond to intrusions autonomously.

1.2 Executive Summary

In each utility partner test lab we built and experimented with realistic attack scenarios that ranged from transmission, distribution, and distributed energy resources. From this experience we were able to better understand the vulnerabilities of a variety of energy delivery control systems and how to sense and respond to even subtle intruder actions.

The CAPMS program threat scenarios involved:

- Risk assessment followed by building the actual cyber attack hardware and software.
- Developing a security policy management system to configure and install executable policy objects into a new software program "policyd."
- Learning how to track the progress of a cyber intrusion and interact with both the operators and the control systems in a meaningful way.

The two CAPMS partner utilities took different approaches for their test labs and the security scenarios they wanted to explore. Southern California Edison decided to extend their existing TNP system (called the "Common Cyber Services" or CCS) around synchrophasors and which includes their portion of the Western Interconnection Synchrophasor Project (WISP.) SCE's approach touches on mainly the bulk energy transmission system and is representative of a SCADA system which is managed from a central operations center.

Duke Energy, on the other hand, explored using distributed computing for protecting systems at the substation (distribution) and microgrid (distributed energy resource) level. They wrote and released the "Distributed Intelligence Platform" specification ultimately to the Industrial Internet Consortium. We did two demonstrations with Duke Energy

- A DNP3 attack against a simulated microgrid which was staged live at the 10th Annual ICS Security Summit on February 23, 2015. See "Live ICS Attack Demo" slides on the SANS web site.
- An attack against a simulated microgrid using GreenBus from Green Energy Corp.

We discovered each case that the OT systems provided little useful information when a cyber attack was underway. Often it was misleading information indicating that a device lost connectivity, and in most cases they didn't report anything abnormal.

Legacy protocols are notoriously insecure and, as we discovered, are easily hijacked using readily available open source code. Intentional misconfiguration of equipment by persons with legitimate credentials poses a huge risk as well whether performed by negligent or untrained operators or by disgruntled employees. Energy control systems are built to be functional first. They typically do not check

every case where events or configurations are out of spec or even nonsensical. They definitely do not cover unusual events, configurations and operations that span multiple vendor toolsets.

The integration layer of "policyd" made it practical to correlate events across many different networks and platforms. These encompassed traditional IT cyber security, physical security such as perimeter alarms, and information about the state of the energy delivery system itself. The policy layer of "policyd" allowed us to quickly implement event correlation and response logic in rapid development cycles as we refined our sample cyber attacks. We also introduced a layered security system that implemented a second state-model of the protected grid assets in addition to what was already there. This let us detect misconfigurations, malware using correct credentials but unexpected settings and command sequences, spoofed sensor data from man-in-the-middle attacks, and so on.

We discovered that such a system can serve as a backup to normal maintenance and safety procedures as well as catching the most destructive sorts of insider attacks before they can cause harm. Many of the security policies were quite simple to implement but powerful because they could capture data from many systems and explain the attack to an operator in his or her own words.

We also discovered the need and usefulness of allowing the security system to create a dialog between the policies and the operator. While we did experiment with allowing the security system to take autonomous action (say, to trip the point of common coupling (PCC) relay on a microgrid) there were many more cases where this was not deemed safe or practical. In those cases we needed to raise an alert and make a recommendation, and we also added a function such that the security system could suggest an action and wait for operator approval before continuing.

We also found that sometimes the security policy could benefit from advice from the operator. Examples of this include enabling expensive security checks that might produce false positives (in which case the operator would forewarned) or when the security system suspected that a particular attack was happening and wanted confirmation. This dramatically reduced the effort to design security policies while increasing their usefulness.

1.3 Member Organizations

- Duke Energy, Emerging Technology Office,
  Contact: Lawrence, David C. (David.Lawrence@duke-energy.com)
- Southern California Edison, Advance Technology Office,
  Contact: Prakash Suvarna (prakash.suvarna@sce.com)

Table 1 - CAPMS Team Members

Organization	Name	Role
ViaSat	Steve Lusk	Program Manager
	Tim Collins	SW Architect
	Bakul Khanna	Sr. SW Engineer
	Jonathan Lawrence	Sys Engineer
	Nick Saunders	SW Lead
	Kalvin Chau	SW Engineer
	Salik Siddiqui	SW Engineer
Duke Energy	David Lawrence	Program Manager
	Rodney James	IT Manager
	Dwayne Bradley	Technology Manager
	John Camilleri (Green Energy)	Duke Contractor
Southern California Edison	Prakash Suvana	Program Manager
	En-Yi Lin	IT Systems
	Phil Carey	IT Manager

Organization	Name	Role
	Son Vo	Systems Engineer
	Brian Smith (Enernex)	SCE Contractor
	Ben Rankin (Enernex)	SCE Contractor
	Steve Van Ausdall (Xtensible)	SCE Contractor

2 Technology Overview

CAPMS was architected with ViaSat's Trusted Network Platform (TNP) as a basis for design. This next section provides background information on TNP, followed by a description of how we extended the TNP architecture with a new component for CAPMS called "policyd".

2.1 Trusted Network Platform (TNP)

The CAPMS project was a technology demonstration effort investigating the ability of a cybersecurity system to identify and respond automatically to attacks in a predefined way. The project is an addition to ViaSat's TNP implementation of the Common Cybersecurity System (CCS) standard, now being actively deployed and tested in Southern California Edison (SCE) substations. SCE worked with ViaSat to develop the TNP product for its base security infrastructure that SCE will be using to protect their next generation smart grid networks.

The TNP product provides a foundational set of security features, which aided the CAPMS initiative:

- Distributed agents – These are useful because they enable for distribution of sensor collection as well as distribution of responses. Distribution of agents provides a superset of features offered by a centralized solution with additional benefits which include standardized secure control/status communications, reduced latency of certain detections, reduced delay in instituting a response, distribution of processing-intensive logic, availability benefits, etc.
    - Secure point-to-point messaging is provided by the TNP system with the opportunity for extension in support of CAPMS goals.
    - Secure package distribution is necessary for the distribution of CAPMS policies.
- Asset management – Association with a policy and a given device requires knowledge of the device and of its properties. The TNP solution provides an asset management system which can be extended for use with the CAPMS problem set.

In addition to this, there are additional security features provided by TNP which provide an added benefit to the CAPMS goals:

- Sensor capabilities
    - Host integrity events, which provide status of whether device files have been modified.
    - Connection-related events, which provide notifications of when a device has established a secure connection to another device.
    - PKI-related events, which provide information about the certificate status of the device.
- Existing TNP Security Controls
    - Security association connections can be controlled by the TNP system.
    - PKI controls allow for modification of the certificate standing for a device.
    - Quality of Trust is a security metric, which can be influenced by events as well as influence the way a device is handled/regarded by its peers.

ViaSat designed the CAPMS system to be flexible, incorporating a broad set of data points to help provide a comprehensive view of the cyber-physical security status to a utility.

2.2 TNP with CAPMS

The CAPMS project divided the problem of detecting, interpreting and responding to cyber intrusions into two separate but dependent parts. The first part was to provide an effective framework for integrating

events from many sources: cyber security events such as network and host intrusion detection and deep packet inspection, physical security events such as proximity sensors and tamper alarms, and last but not least, events from the energy control systems themselves. We realized early on that we would need to correlate events from a great many systems including one of a kind energy control systems that we would never control ourselves. We would also need to watch for activity that went beyond whatever counted as "normal" activity as understood by the suppliers of these systems.

The second part of CAPMS was to build a system for modeling the behavior of an attacker and the utility's response to an intrusion in an abstract and network-agnostic manner. We started with an industry effort (National Electric Sector Cybersecurity Resource or NESCOR) to create generally applicable threat scenarios using "attack trees." While more of a risk assessment technique than a way to build executable policy specifications, the NESCOR idea of having broadly applicable threat descriptions suggested that someday there might be a community of security domain experts sharing machine-readable attack descriptions that we might use. As we dug deeper into the idea of modeling a cyber attack it became clear that for much of the time we could only track probabilities that one or another sort of attach might be in progress. This lead to the use of Bayes' Rule statistics in order to better handle variable confidence levels and shades of grey and the integration of Netica into our demonstration.

The resulting system can deploy and monitor executable security policies from a central management console (see Figure 2). These policies in turn correlate, interpret and respond to patterns of activity tailored to the actual systems they protect. CAPMS security policies benefit from deep knowledge of the specific combination of hardware and software used to build energy delivery systems. They can cope with network events ranging from attacks against insecure legacy protocols such as DNP3 to sophisticated malware designed and deployed by determined insiders.

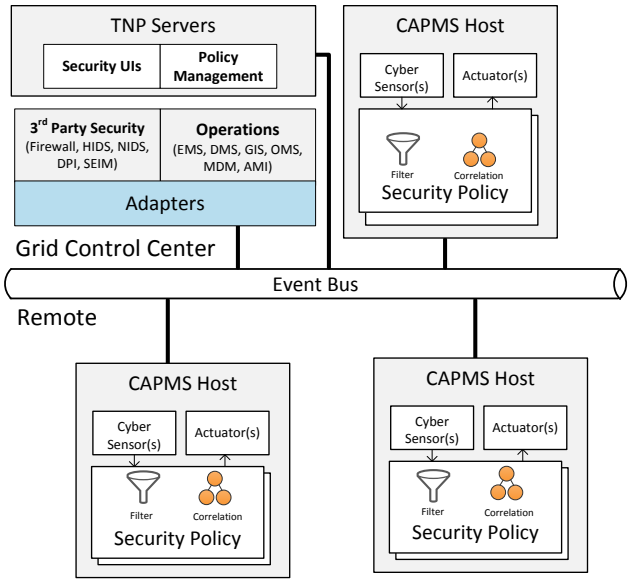

Figure 2: CAPMS Architecture

As shown in Figure 2, CAPMS security policies execute inside intelligent agents installed both in the operations center and at the network edge. These agents are a new component created during the CAPMS project called "policyd". TNP provides a centrally managed database of secure nodes and can install and operate security policies where needed. TNP provides technology to secure individual computers and their networks by a combination of IPsec, TLS, firewalls, PKI, host intrusion detection, network intrusion and anomaly detection and so on. It also provides a central element, alarm, and map (GIS) interface. The CAPMS program took advantage of TNP as a building out point. We can install and monitor security policies into policyd agents throughout the network and use TNP to visualize the security posture of the network.

3 Activity Summary

3.1 2013 Q4

The start of the DOE CAPMS program focused on the program start-up activities including addressing program award questions as well as staffing.

A Partner Kick-off meeting was held on Oct 31, 2013 via conference call introducing the team and summarizing the objectives for the program. Each of the team members have several years of experience working in the power utility sector and/or network security. Many of the members were recently assigned to the program and in some cases not all positions had been filled. Action items focused on supporting updates to the DOE Budget Justifications and supporting the DOE CAPMS Kick-off meeting.

The DOE CAPMS Kick-off meeting was held Dec 12, 2013 and was well attended by DOE representatives, Power Utility partners and ViaSat personnel. A hard copy of the PowerPoint presentation was provided at the meeting and an updated electronic version was provided to DOE PMO afterwards. Feedback after the meeting was positive: citing a strong team, appropriate test sights, clear objectives, and enthusiasm for the work.

ViaSat also met with both power utility partners individually to begin the program effort. The ViaSat CAPMS team visited SCE on Dec 4, 2103 to tour the SCE facility and to address the remaining contractual questions/issues. ViaSat held several meetings with Duke personnel to resolve budget justifications and to begin the analysis phase for the cyber-intrusion scenario. A visit to Charlotte NC occurred on Jan 15, 2013 to meet additional Duke personnel supporting the program, and to tour Duke Energy's McAlpine Creek substation.

3.2 2014 Q1

The second quarter of the DOE CAPMS project continued with the Research & Analysis phase by further investigations into QoT algorithm updates, expanding definitions of Cyber sensors and actuators, auto-response algorithms, and software architecture changes to the baseline CCS. This effort resulted in the following documents and trade studies:

- CAPMS System Specification (includes system requirements)
- CAPMS SW Architecture Design Note
- CAPMS Cyber Sensor and Actuator Design Note
- CAPMS Autonomous Intrusion Response Trade Study
- Quality of Trust (QoT) Enhancement Trade Study

We also spent time with Duke in understanding their utility network design, Comm Node Architecture, and reviewing potential threat scenarios. The threat scenarios were the most demanding in discussing scenarios that make the most sense for the network we are protecting. The result of this effort was a series of threat scenarios intended to be the basis of the CAPMS demonstrations.

This quarter included trips to Charlotte, NC for meetings with Duke as well as trips to Carlsbad for CCS-CAPMS architecture and program management reviews.

Efforts with SCE were limited due to delays in establishing a contract mutually agreeable for this project. ViaSat continued to work closely with SCE on our existing CCS programs. However for CAPMS the efforts had not yet started as a contractual agreement was not yet in place.

3.3 2014 Q2

The primary focus this quarter was the start of design and development, leveraging the research & analysis performed in the previous quarters. A significant effort was made in the definition of use cases

and causal algorithms used in processing new and existing cyber security events. Implementation of this processing began in a new service called "Policyd." The Policyd service is a standalone process that works with the existing system to process cyber security events from a variety of cyber sensors. The development effort was iterative allowing for prototypes of simple attack-trees, which we subsequently refined and improved. This effort resulted in the following design notes and studies:

- CAPMS Policy Service Design Note
- CAPMS Causal Algorithms and Use Cases Study
- Cyber Sensor and Actuator Study

Both Duke and ViaSat purchased equipment for staging the CAPMS system for test and demonstration. ViaSat equipment was installed and configured at our Marlboro MA facility and Duke's hardware was installed for preliminary testing at their Charlotte, NC test labs facility prior to going to their Mount Holly demonstration facility. SCE started hardware procurement this quarter to build out their Westminster, CA facility for the CAPMS demonstration.

3.4 2014 Q3

The primary focus for this quarter was the analysis and implementation of causal algorithms with ViaSat's Trusted Network Platform (TNP), and the development of threat scenarios with our utility partners. Implementation of the causal algorithms using Bayesian network processing yielded some interesting results for detecting attacks which caused multiple events. This effort was mostly "plumbing" as the details of the attacks continued to evolve. Having Bayesian processing as a tool in the attack trees helped determine the extent of an attack and the complexity of the threat scenarios. This development effort was iterative, and allowed us to develop simple attack trees into more complex implementations as the partner utility companies provided more detail to their threat scenarios.

Duke moved their test equipment to the Little Rock facility while the Mount Holly demonstration facility construction was underway. TNP software installation and integration with candidate distributed intelligent controllers had begun. We were in the early stages in identifying applications and input events to support the Duke threat scenarios.

SCE purchased TNP hardware this quarter to build out their Westminster CA facility for the CAPMS demonstration.

3.5 2014 Q4

3.5.1 Overview

The primary focus this quarter was the implementation of a new Policyd service that manages and controls the conditions for determining when a network is under attack, four new threats scenarios from SCE focusing on the Phasor network, and the implementation of DNP3 stateful packet sensing capability.

The new Policyd Service integrated into ViaSat's Trust Network Platform (TNP) uses a User defined policy that dictates when to report security events and when to respond with an automated response. All responses are User defined and can be modified as needed to tailor the security posture decided upon by the Network administrator. The Policyd Service provides a visual representation of the Utility Network as well as configuration options to control the level of sensitivity for specific events.

For SCE, four new threat scenarios were defined and were reviewed/vetted with the team. Each threat scenario addresses different areas of the SCE Phasor network and demonstrates how the attack can be detected and how it can be mitigated via an automated response.

We also made advancements in the Deep Packet Inspection (DPI) for SCADA protocol sensing. The DNP3 packet sniffing is new and provides the ability for TNP w/CAPMS to detect, report and respond to

DNP3 attacks. DNP3 attack scenarios were modeled after the work performed by Adam Crain and Chris Sistrunk. http://www.digitalbond.com/blog/2013/10/16/why-crain-sistrunk-vulns-are-a-big-deal/

3.5.2 SANS ICS Security Summit

A related effort this quarter has been the preparation for the first CAPMS demonstration at the *SANS ICS Security Summit* on Feb 24, 2015 in Orlando Florida. This demonstration was a snapshot of the work thus far on CAPMS and provided an initial look as to how TNP w/CAPMS would detect DNP3 attacks followed by possible responses to help mitigate the attack. This demonstration, recommended by Duke, provided visibility into one of the attack scenarios and provided industry experts the chance to comment and respond to the direction of the attack scenarios and responses.

3.5.3 SCE

SCE equipment arrived and was installed at their Westminster, CA demonstration facility. TNP software installation and integration with the SCE phasor test network began this quarter.

3.5.4 Duke

The Duke Mount Holly facility was almost complete this quarter providing fully networked labs and vendor test equipment for the final CAPMS demonstration in an active power utility test grid. For the ICS security summit Duke constructed a portable substation test network consisting of a MicroSCADA server, a Substation gateway and four substation relays. ViaSat integrated the TNP Server and Client w/CAPMS into this network along with a DNP3 attack script simulating a network intruder.

3.6 2015 Q1

3.6.1 SANS ICS Security Summit

The primary focus this quarter was a live demonstration of a DNP3 Attack Scenario at the 2015 SANS ICS Security Summit in Orlando Fl. This demonstration gave us an opportunity to pull together the various pieces of development we had been working on this past year, and provided a way for us to experiment with scripting attacks using open source DNP3 software as well as testing out our DNP3 deep packet inspection (DPI) implementation.

The demonstration consisted of a simulated substation built by Duke Energy, ViaSat's Trusted Network Platform (TNP) with CAPMS (Cyber-intrusion Auto-response and Policy Management System) monitoring the network, and an intruder planting a rogue Raspberry Pi on the substation network demonstrating how easy it is to intercept and take over a utility substation. The basis of the attack was modeled from a paper written by Adam Crain and Chris Sistrunk in 2013 which provides a detailed explanation of vulnerabilities in the DNP3 protocol and how an attacker could take advantage of a utility's substation network.

The demonstration provided an overview of how TNP w/ CAPMS could protect a vulnerable network and in this case detect when the network was under attack. Using Deep Packet Inspection (DPI) capabilities, CAPMS monitored the DNP3 SCADA network, and reported unusual activity to CAPMS. Based on Policy, CAPMS was able to respond by sending commands to the ABB Micro SCADA control system notifying the operator of the attack. Although not a full remediation action, it demonstrated our ability to mitigate an attack by providing the Network Utility operator with deeper Cyber Security information in addition to the normal operational data they have today.

3.6.2 SGIP

Other activities this quarter have been participating in the Smart Grid Interoperability Panel (SGIP) Open Field Message Bus (OpenFMB) working group. This effort was spear headed by Duke Energy's Emerging Technology Office (ETO) in an effort to formalize and document their technology roadmap for

enabling the operation and management of the electric power system in a non-invasive and affordable manner by employing open standard, interoperable, and distributed information systems.

The OpenFMB working group is currently working on several use cases that include cyber-attacks on solar farms and solar inverters. Our participation in these sessions provided us (ViaSat and Duke Energy) with several additional scenarios to be demonstrated in September.

Duke's Mount Holly facility was almost complete providing fully networked labs and vendor test equipment that we used for the CAPMS DOE demonstration in an active power utility test grid. ViaSat's TNP plus CAPMS along with the simulated substation rack from the SANS ICS security summit demo was the first set of equipment at this new location.

3.7 2015 Q2

The primary focus this quarter was the final definition of threat scenarios for both Duke Energy and SCE, and further preparation of the test facilities for the DOE demonstrations at both Duke Energy and SCE test facilities. In total there were three major Threat Scenarios each of which had variants:

1. Substation Attack via DNP3 control network
2. Microgrid Islanding Attack based on SGIP OpenFMB scenarios, and
3. Cyber attack on Synchrophasor network

3.7.1 DNP3 Substation Threat Scenario

Based on the Crain and Sistrunk paper defining vulnerabilities in Industrial Control Systems that implement DNP3, the demonstration presents how an adversary can easily take control of 4 relays using a Raspberry Pi and Open Source Software, e.g., OpenDNP3. This demo was first presented at the SANS ICS Security conference on Feb 23, 2015 in Orlando.

3.7.2 Microgrid Attack

The OpenFMB working group is currently working on several use cases that include cyber-attacks on solar farms and solar inverters. Our participation in these sessions has provided us (ViaSat and Duke Energy) with several additional scenarios that we demonstrated in September. At this time we were able to recruit Green Energy Corporation to provide their microgrid simulation software. Even though we were about a month too early to use their OpenFMB version of their software (which is based on the Object Management Group DDS protocol) we were able to use their "GreenBus" field bus system based on AMQP.

The use case was implemented on a network of National Instruments cRIO-9033 environmentally hardened control servers. These controllers hosted distributed software from Green Energy and ViaSat that realistically simulated:

- Distributed solar and CHP generation
- Energy storage (batteries)
- Controllable loads
- Energy management, optimization, scheduling and control
- Operation of the point of common coupling (PCC) relay over a DNP3 gateway

ViaSat provided security and management of all devices through our Trusted Network Platform (TNP) as well as detection/reporting of security events that could cause the microgrid to island from the grid. Forensic information to support operator diagnostics and policy management updates demonstrated how to prevent further attacks on the network.

3.7.3 **Synchrophasor Network Attack**

The SCE analysis of potential threats to a synchrophasor-based system identified four basic areas that could potentially be targeted by an attacker in order to interfere with proper system operation:

- Timing attacks
- C37.118 protocol attacks
- Network attacks
- Device attacks

SCE selected a testing scenario associated with a device level attack. Out of the four categories of attacks, this was deemed the most likely to potentially occur as a result of physical security challenges associated with these devices. These challenges stem from the likelihood that a field deployed cyber asset, such as a PMU, will be installed in a remote, unmanned facility where advanced physical security measures, such as those found at a utility control center may not be practical or effective. These physical security challenges make it likely that an adversary may choose this route over an attack launched remotely due to the fewer number of cyber defenses that would need to be circumvented or compromised.

Although there are numerous attacks that could be launched by an adversary when locally present within a remote facility such as a substation, the unauthorized change to a devices' configuration is perhaps one of the most difficult to detect before a system mis-operation occurs. A secondary benefit of focusing on this type of attack is that it may also be effective in detecting approved utility activity, which may not have been properly coordinated.

The potential impact of this type of attack would alter data that is consumed by operation applications. This altered data could potentially make it appear that a grid event is occurring when in fact one is not or inversely, to mask or camouflage a grid event from being detected in a timely manner. In either case, the result of such altered data could lead to a scenario where a Grid Operator, or operational application through automation, takes inappropriate action in response to what was perceived to be correct power system data.

The overall purpose of this testing is to validate the potential value that CAPMS type functionality could provide to a utility in supporting its grid operations efforts including interfaces with both the traditional Security Operations Center (SOC) Operator as well as the Grid Operator roles.

3.8 2015 Q3

This was an excellent quarter. Both demonstrations were performed as scheduled and provided much dialog amongst the attendees regarding advances in detecting complex attacks and responding in near real-time to protect the grid. At both demonstrations Carol Hawk, Manager of the Cybersecurity for Energy Delivery Systems (CEDS) Program for the DOE, stressed the importance of this work, and especially on the value of having the vendors and utility industry professionals working so closely together. "This is the model the DOE had envisioned for the grant" said Hawk who was pleased to see how well it came together.

Each day went as planned providing a full day of presentations, lab tours, and the final CAPMS demonstrations. In total, there were three major threat scenarios each of which had multiple variants:

1. Cyber attack on Synchrophasor network
2. Substation attack via DNP3 control network
3. Microgrid islanding attack based on SGIP OpenFMB scenarios

The Southern California Edison (SCE) demonstration was held on Sept 24, 2015 at the SCE Advanced Technology Lab in Westminster CA, with attendees from the DOE, SCE, Lawrence Livermore National Labs, and ViaSat. The Duke Energy Demonstration was held on Sept 29, 2015 at their Microgrid Training Facility in Mount Holly NC, with attendees from DOE, Duke Energy, Southern Co., and ViaSat.

4 Synchrophasor Attack Scenario - Southern California Edison

4.1 Threat Analysis

4.1.1 Objectives

As Information and Communications Technology (ICT) has become a key enabler utilized by utilities for more efficient and effective grid operations, it has also led to more complex and interconnected monitoring and control systems. Utilities now rely on network connectivity standards, within the system and external to the system, to adapt to changing business and operational environments. Advances in network connectivity standards, however, also provide new potential paths for undesirable activity, intentional or unintentional, which may affect the resilience of critical operational systems. The main objective of the threat analysis effort within the SCE CAPMS project was to gain a better understanding of the network sensor points and their correlations needed to detect a potential cyber event, malicious or otherwise, within a Wide Area Monitoring Protection and Control (WAMPAC) system that utilizes synchrophasor-based network connectivity standards such as IEEE C37.118. To accomplish this, SCE analyzed threats to these network-based systems with a focus on how they could potentially influence a utility's operational decision-making. The main components of this approach were examining network-attached synchrophasor device characteristics that an attacker could exploit and the informational impacts from the identified attacks.

4.1.2 Informational Impacts

Systems such as WAMPAC, which utilities utilize for real-time grid operations, are only as effective as the information provided to them. One method employed in the SCE threat analysis was to categorize attacks by the potential impact that they might have on the information within the system. When control system information is affected, the overall impacts to the utility can be severe as these systems are integral to the utility's ability to make critical operational decisions or take appropriate actions with their command and control capabilities. If an attacker's activities go unnoticed and affect the availability or integrity operational data or command and control capabilities, they could potentially affect the safety and reliability of the power grid itself. Improving the ability of a utility to detect and react to unauthorized cyber activity can directly affect its ability to operate the power grid in a resilient manner. The project utilized five basic information impact categories in this analysis as follows:

- **Distort** - A distortion or manipulation of information
- **Disruption** - A disruption in the flow of information
- **Destruction** - A destruction of information
- **Disclosure** - A disclosure of information which may provide an attacker with access to information they would normally not have access to and possibly leading to other compromises
- **Discovery** - A discovery of information not previously known that can be used to launch an attack on a particular target

Of the five categories, three (distort, disrupt, and destroy) were of particular interest as they have the most ability to likely impact the utility operational decision-making.

4.1.2.1 WAMPAC Architecture

Figure 3 illustrates a high-level view of a WAMPAC system architecture. The three key system components worth noting are:

- **Phasor Measurement Unit (PMU)** – measures electrical inputs, calculates and time stamps phasor(s)
- **Phasor Data Concentrator (PDC)** – time aligns data from multiple PMUs and also does basic data quality checks

- **Phasor Gateway** – utilized to securely exchange synchrophasor data between entities

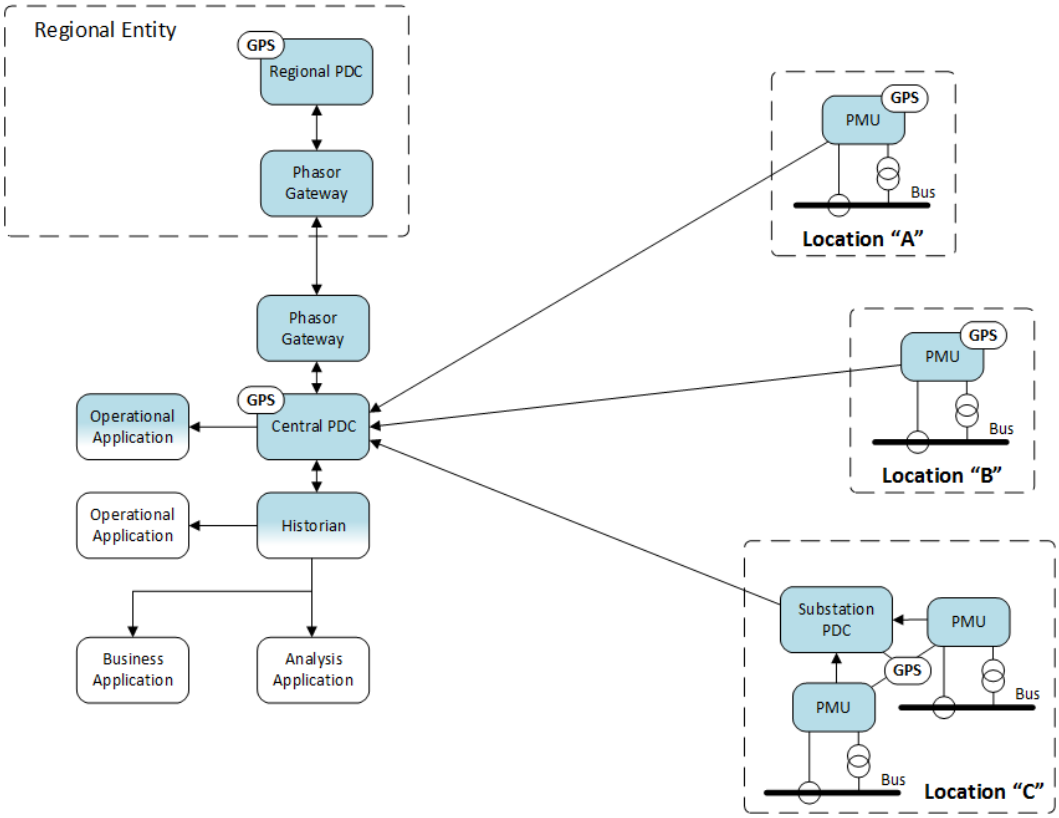

Figure 3: Example WAMPAC System Architecture

As part of the threat analysis, SCE cataloged attacks against these components aimed at disrupting their primary system functionality. Critical to the overall performance of the WAMPAC system is the reliance on a high precision time source at the various locations where these components are located.

Protocols and Standards

The project team also examined key protocols and standards utilized within WAMPAC systems for possible attack vectors as part of the threat analysis including:

- C37.118.2-2011, IEEE Standard for Synchrophasor Data Transfer for Power Systems
- IP based communications (both UDP and TCP)
- IRIG and NTP timing references

4.1.3 Process

The process utilized by SCE for the WAMPAC threat analysis consisted of three major steps as shown in Figure 4.

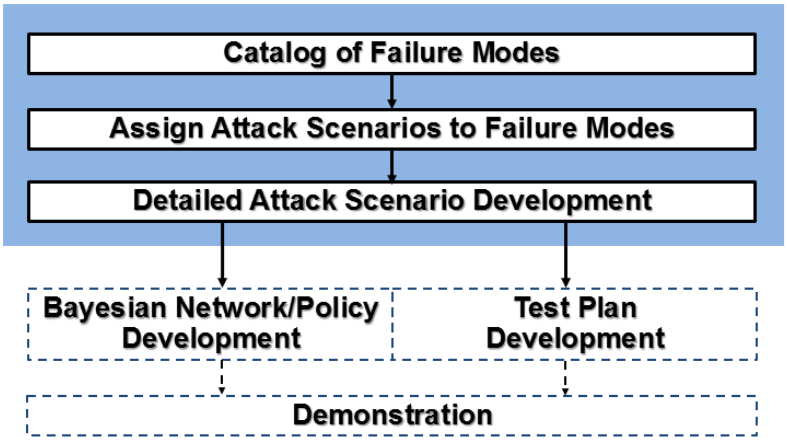

Figure 4: CAPMS Threat Analysis Process

Catalog Failure Modes

The first step of the SCE CAPMS threat analysis was to brainstorm possible failure modes within the WAMPAC system from the perspective of the system components performing their assigned functions and then correlate these failure modes against possible attack targets and attack types. This first step also identified the potential informational impact for each failure mode. This step of the analysis yielded 32 significant and distinct failure modes (resources available upon request from SCE). The goal of this step was to identify a representative set of failure modes, not an exhaustive list of all possible failure modes.

Assign Attack Scenarios to Failure Modes

From the master list of failure modes, the team developed a second matrix that identified at least one plausible attack scenario for each failure mode. In some cases, the team mapped multiple attack scenarios to a single failure mode, mainly due to multiple attack targets within the system. Part of this step was the categorization of these attacks based on the system component or function that they targeted. The SCE analysis of potential threats to a synchrophasor-based system identified four basic areas that an attacker could potentially target in order to interfere with proper system operation:

- **Timing attacks** - Attacks targeting the distribution of timing signals utilized by the individual components of the system
- **Application layer attacks** - Attacks targeting the application layer protocol (IEEE C37.118)
- **Network attacks** - Attacks targeting the network infrastructure utilized within the system with the intent of disputing information flows
- **Host attacks** - Attacks targeting hosts of the individual components of the control system (e.g. hardware/OS)

This step of the analysis yielded 53 plausible attack scenarios. The goal of this step was to identify a good representative set of attack scenarios, not an exhaustive list of all possible attacks on a WAMPAC system.

Legend

May not be relevent to SCE specific architecture

Currently not planned as part of SCE demo or not significantly interesting

X with no color may lead to multiple rows on second tab

						Informational impact of attack						Components potentially vulnerable to this type of attack (Candidate Components)							
Failure ID	Attack Category	Attack Target (Funtional)	Attack Type	Possible Result/Failure Mode		Distort	Disrupt	Destruct	Disclosure	Discovery		DFR/PMU	GPS (Substation)	USI Master	PDC	GPS (Control Center)	Historian	Phasor Gatevay	Network
T1	Timing	Network Time Distribution	Spoofing NTP/SNTP server	Clock error within C37.118 server		X						X	X		X	X			X
T2	Timing	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to alternate time source			X					X	X		X	X			X
T3	Timing	Network Time Distribution	DoS attack on NTP/SNTP server	C37.118 server reverts to internal clock			X					X	X		X	X			X
T4	Timing	IRIG-B Time Distribution	Substituting/Spoofing IRIG-B input	PMU clock error		X						X	X						
T5	Timing	IRIG-B Time Distribution	Disrupting IRIG-B input	PMU reverts to internal clock			X					X	X						
T6	Timing	GPS Signal Reception	GPS jamming	PMU or PDC reverts to internal clock			X						X			X			
T7	Timing	GPS Signal Reception	GPS spoofing	Clock error within C37.118 server		X							X			X			
T8	Timing	GPS Receiver	Unauthorized configuration change	Clock error within C37.118 server		X						X	X		X	X			
AL1	Application Layer	C37.118	Spoofing C37.118 server	False data stream transmitted to upstream C37.118 client		X						X			X		X	X	
AL2	Application Layer	C37.118	Spoofing C37.118 server	False configuration or header message transmitted to upstream C37.118 client		X						X			X		X	X	
AL3	Application Layer	C37.118	Spoofing C37.118 client	C37.118 server data stream redirected to imposter			X					X			X		X	X	
AL4	Application Layer	C37.118	Spoofing C37.118 client	Spoofed C37.118 client starts/stops PMU data			X					X			X		X	X	
AL5	Application Layer	C37.118	Man-In-The-Middle	Monitoring/eavesdropping of messages (header/configuration/data stream) from C37.118 server to C37.118 client					X			X			X		X	X	
AL6	Application Layer	C37.118	Man-In-The-Middle	altered configuration or header message sent to upstream C37.118 client		X						X			X		X	X	
AL7	Application Layer	C37.118	Man-In-The-Middle	altered data stream sent to upstream C37.118		X						X			X		X	X	
AL8	Application Layer	C37.118	Fuzzing C37.118 protocol	Abnormal behavior or termination of the application on target device			X					X			X		X	X	
AL9	Application Layer	C37.118	Unauthorized/rouge C37.118 client	Command message from unauthorized C37.118 client starts/stops PMU data stream			X					X			X		X	X	
AL10	Application Layer	IEC 61850-90-5																	
N1	Network	Network Infrastructure	Flooding (DoS)	Delayed receipt of data stream by upstream C37.118 client			X												X
N2	Network	Network Infrastructure	Flooding (DoS)	Message exchange interupted between C37.118 client and server			X												X
N3	Network	Network Infrastructure	ARP spoofing	Message exchange interupted between C37.118 client and server			X					X			X		X	X	X
H1	Host	Network Interface (NIC)	DoS	Device unable to access network			X					X	X	X	X	X	X	X	
H2	Host	Network Interface (NIC)	DoS	Abnormal behavior or termination of the			X					X	X	X	X	X	X	X	
H3	Host	Network Interface (NIC)	Port scanning	Open logical network interface to device discovered (e.g. ftp, telnet, http, etc.)						X		X	X	X	X	X	X	X	
H4	Host	Firmware/OS	Malware	Device utilized to gain access to other protected network resources						X		X	X	X	X	X	X	X	
H5	Host	Firmware/OS	Malware	Unexpected behavior of device			X					X	X	X		X	X	X	
H6	Host	Configuration	configuration	Phasor data within data stream incorrect		X						X			X			X	
H7	Host	Configuration	configuration	Mismatch between header/configuration messages and phasor data within data stream		X						X			X			X	
H8	Host	Database	uauthorized database access	Archieved/historical data modified		X											X		
H9	Host	Database	uauthorized database access	Archieved/historical data deleted				X									X		

Figure 5: Threat Matrix Table

4.1.4 Threat Analysis Results

The project team then utilized the key results from the threat analysis as inputs into the CAPMS Bayesian Network and Policy development as well as the detailed test plan development. The effort resulted in:

- Understanding of the potential sensor points and data sources required to detect activities and their impacts
- Basic understanding of the sensor logic and correlation logic to correctly detect these attacks

SCE selected a testing scenario associated with a device level attack. Out of the four categories of attacks, this was deemed the most likely to potentially occur as a result of physical security challenges associated with these devices. These challenges stem from the likelihood that a field deployed cyber asset, such as a PMU, will be installed in remote, unmanned facility where advanced physical security measures, such as those which may be found at a utility control center my not be practical or effective. These physical security challenges make it likely that an adversary may choose this route over an attack launched remotely due to the fewer number of cyber defenses that an attacker would need to circumvent or avoid.

Although there are numerous attacks that could be launched by an adversary when locally present within a remote facility such as a substation, the unauthorized change to a devices configuration is perhaps one of the most difficult to detect before an improper system operation occurs. A secondary benefit of focusing on this type of attack is that it may also be effective in detecting approved utility activity that may not have been properly coordinated.

The potential impact of this type of attack would alter data that operational applications consume. This altered data could potentially make it appear that a grid event is occurring when in fact one is not, or to mask or camouflage a grid event from detection in a timely manner. In either case, the result of such

altered data could lead to a scenario where a Grid Operator, or operational application through automation, takes inappropriate action in response to what appeared to be correct power system readings.

4.1.5 Use Cases

The final step of the threat analysis selected one attack scenario from each category and developed a more detailed version identifying not only the steps that an attacker might perform, but also impacts that these activities might induce. These impacts can range from grid level events such as an outage or equipment operation to secondary system events such as loss of communications or specific message exchanges. These four selected attack scenarios also become the primary candidates for testing and demonstration later in the project.

4.2 Security Policy Design

A security policy was crafted as a defense against this threat by analyzing the goals that the attacker would need to be successful in achieving in order to complete this attack. Several required attacker milestones were identified:

- Attacker achievement of physical access
- Attacker achievement of network access
- Modification of PMU configuration files.
- Login events for the PMU

In order to determine whether these attacker milestones were achieved and how these were related, the ViaSat and SCE teams collaborated to determine what sensors were required. In addition to this, the teams also worked to annotate the relationship between these states. The network graph shown in Figure 6 is a result of this work, which depicts the interrelationship between these conditions.

In addition to representing the interrelationship between the aforementioned milestones, the diagram also shows additional states. Many of these states exist because a response is needed given the state that has been achieved by the attacker. These responses are marked on the corresponding states.

Worth noting in the above diagram is the response assigned to the Unapproved Substation Access condition. When the model has determined that the attacker has achieved this goal, the response is to initiate a periodic attestation cycle at an elevated frequency. This is a noteworthy response because it is an investigative action. It accelerates the state machine by decreasing the time to detection of another state within the same model: the "Device Unhealthy" state. While normally this condition would only be detected by the standard 12 hour device attestation period, activation of the policy response will initiate a periodic device check cycle which occurs every 60 seconds.

Other responses depicted by the diagram include:

- Alerts
- Updates to LED's on the grid operator interfaces
- Notification to the cyber security operations team
- Notification to the physical security operations team
- Dispatch the physical security response team

Some of these responses were not intended to be autonomously invoked. As a dispatch of the physical security response team may cost money and may require additional context that requires operator involvement, this made an approval-only action. This was due to one of the findings that was uncovered over the course of the project – the emphasis on operator involvement for invocation of automated responses is of great importance to the overall system.

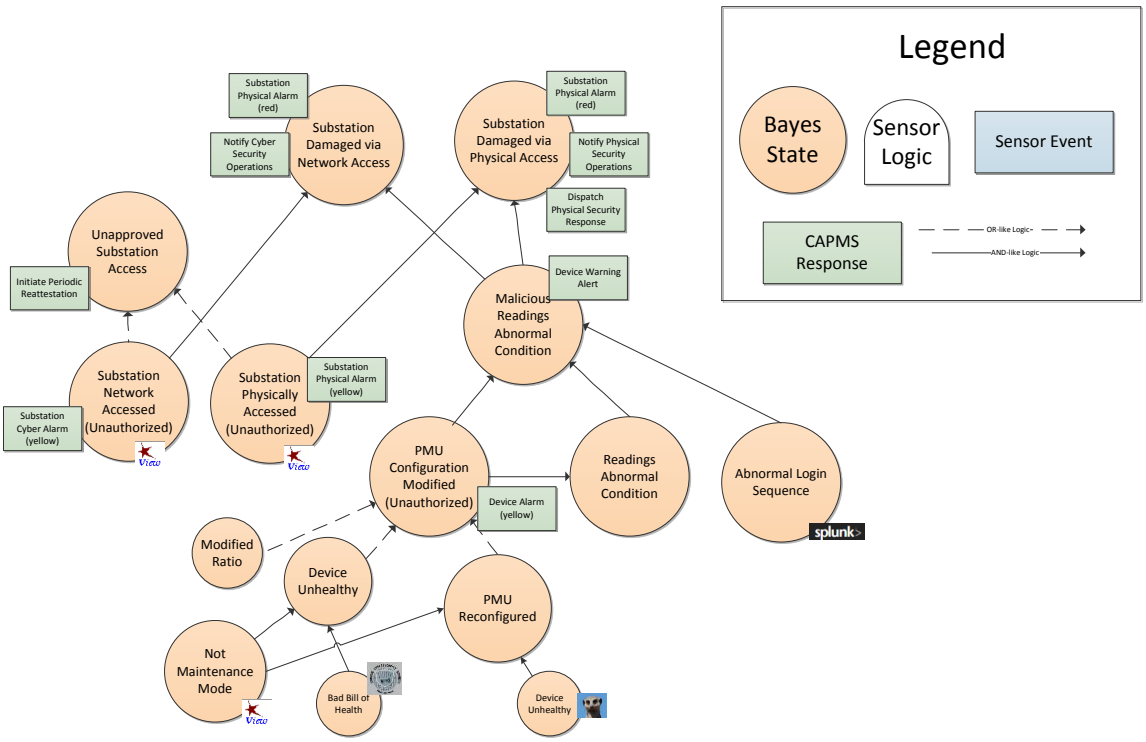

Figure 6: Bayesian State Network Diagram

4.3 Synchrophasor Demonstration Results

This demonstration showed that we could identify an attack from the set of threats identified and analyzed by Southern California Edison, and we implemented mitigations for the attack through close collaboration with the SCE team. Both ViaSat and SCE collaborated to identify how an attacker would carry out such an attack and identified sensor points and automatic response points at key increments throughout the attack.

The demonstration highlighted several key features of the CAPMS policy system:

- Policy distribution: The demonstration included the distribution of one simple policy, an upgrade to that policy, and a replacement of that policy within the system, all initiated through a user interface, which was tied to the TNP asset management system which was extended under the CAPMS grant.
- Approval-based automatic responses: This policy model worked with the SCE systems to institute automatic responses as well as bring about situational awareness for the TNP operator. The TNP operator was able to see key alerts as they were presented, and approve/deny automatic responses, which were tied to the policy's recommended actions.
- Auto response audit capabilities: The demonstration highlighted the ability to present the operator with an audit history of the automatic responses, which were applied by the CAPMS policy.

Development of this policy was also a key success for this demonstration – as there were many subsystems which were connected through the policy and integrated into a single correlative policy model. The demonstration also included several automatic response integrations with multiple systems, including the eDNA historian, Syslog-NG, Splunk, Suricata, TNP, and an SMTP server. This large range of system integration was simplified by the policy integration capabilities.

5 Substation Attack Scenario - Duke Energy

5.1 Simulation Design

The genesis of this scenario was the decision made by Duke Energy and ViaSat to present an early version of CAPMS at the 10th Annual Security Summit held by SANS on February 23, 2015 in Orlando, FL. For this presentation, we designed a simulated substation, designed an attack based on an adversary introducing malware on a rogue Raspberry Pi computer, and we detected and mitigated the attack using the CAPMS "policyd" system running in conjunction with ViaSat's Network Anomaly capabilities.

The demonstration network consists of an operations center and a substation connected over a simulated WAN link. An intruder attacks the relays in the substation, which is detected within the substation and reported and managed at the operations layer.

The simulated substation rack (shown in Figure 7) consists of four protection relays from ABB, Siemens, Schneider and Schweitzer controlled by the "SubStation Server" software from Subnet Solutions. The latter runs inside the substation on a SEL 3354 server. The SubNet system operates as both a DNP3 master station for the relays and as a DNP3 outstation to ABB MicroSCADA (which just sees this as four relays.) At the top of the rack are four LED lamps indicating the state of the four simulated 13.3KV distribution lines, i.e., red for closed or hot, green for open.

Figure 7: Substation Demonstration Rack

The MicroSCADA runs in a simulated operations center in a separate rack (not shown). Alongside MicroSCADA is an installation of ViaSat's TNP system, and as well as CAPMS security software. During the demonstration we showed normal operation of the substation through MicroSCADA (capturing voltage readings from the relays as well as opening and closing them) as well as using TNP to display security issues.

The operations center consists of three HP rack servers running ESXi (with the ViaSat Trusted Network Platform or "TNP" as a series of virtual machines) and a Dell PowerEdge server running ABB MicroSCADA. The MicroSCADA software provides a single line diagram and the ability to control relays over DNP3 in the substation. The TNP software monitors the security posture of nodes in the network and servers as a central management and alarm database. VLAN 10 isolates the back-office operations software from VLAN 30 which isolates the simulated substation. VLAN 20 exists to allow us to simulate a remotely located intelligent node containing the TNP client node and deep packet inspection (DPI) software. The WAN link between operations and the substation is simulated with a simple Ethernet cable.

The CAPMS "policyd" a new TNP component based on the open source package Suricata are also in the substation subnet. Suricata examines DNP3 messages between SubStation Server and the four relays. This software is able to decode and report on master and slave IDs, control points, commands (CROB messages) as well as data points. In the first demonstration this was accomplished by routing network

traffic over a particular VLAN to a VM running in one of the ESXi servers. For the final demo we used an SEL 3355 server in the substation itself to provide a more realistic distributed scenario.

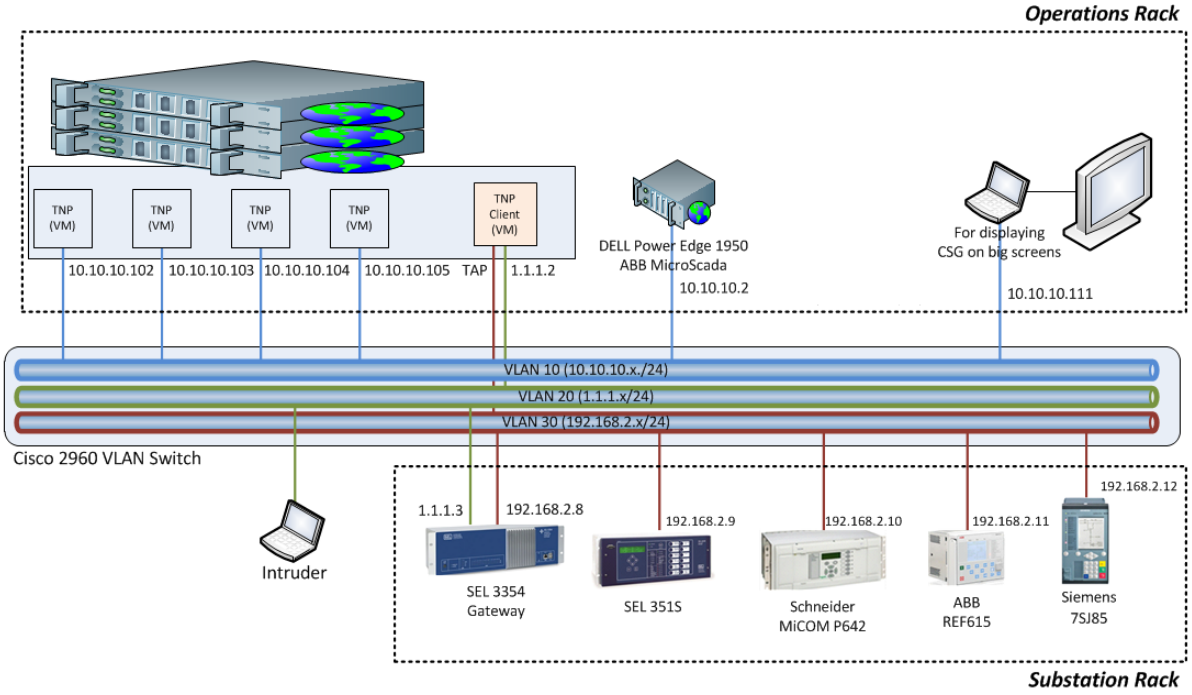

Figure 8: Substation Network

Suricata communicates using syslog over TCP/IP to policyd running in the operations center which in turn is responsible for interpreting and correlating events and for tracking the onset, progress and severity of an intrusion. The policyd service contains highly flexible and configurable policy rules that can be deployed and managed by the greater TNP framework.

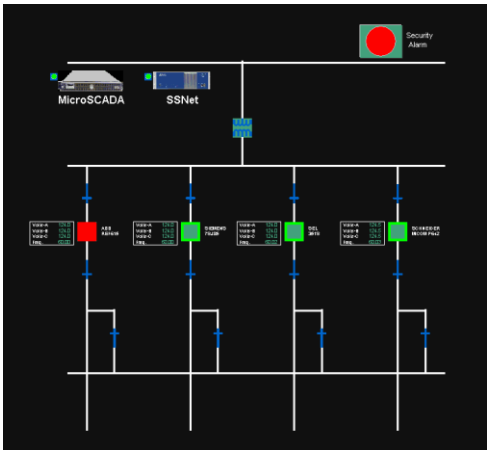

Figure 9: ABB MicroSCADA display with Security Alarm Showing Attack

In this program, we integrated ABB MicroSCADA with the CAPMS software using a file-based mechanism built into ABB MicroSCADA. This reflects what we see as an expected degree of cooperation between the security framework and other day-to-day operational software. We added a blank /yellow/red security indicator to the MicroSCADA single line diagram display to show the detection and severity progression of an intrusion to that display. This is in addition to the normal alarm display used in TNP.

5.2 Threat Analysis

In this scenario, an intruder gains access to a substation through some combination of social engineering and hand tools. This person might be an insider ("disgruntled employee") and might possibly have credentials to remove any protections there might be on the internal substation network, such as port protection. This person then installs a small computer, steals some copper (to misdirect suspicion) and leaves. The small computer in our case is a Raspberry Pi model B running Kali Linux and which has installed:

- Wireshark and its command line version, tshark
- arpspoof
- senddnp3, a command-line program based created by CAPMS based on OpenDNP3 (https://www.automatak.com/opendnp3 /) This program can send "direct operate" and "select then operate" DNP3 commands using a specified source IP,and master and outstation IDs.

DNP3 communications are neither encrypted nor authenticated. Mostly what utilities do is to use port protection and whitelisting on the substation premise router or switch. However, given direct physical access to this equipment it is theoretically possible to circumvent this by:

- Gaining console access to the switch console and disabling or reconfiguring port protection.
- Constructing an inexpensive network tap that can be spliced onto the CAT-5 network wires on any port to allow one's own device to take over the MAC address of an existing device.

We were aware of Crain and Sistrunk's work with DNP3 fuzzer testing and Project Robus and the vulnerabilities of DNP3 communications. We wanted to know how hard it would be use some of their same software (OpenDNP3) and see if DNP3 was as vulnerable as it looks and see how difficult it would be to perform a man-in-the-middle attack on actual control systems.

In DNP3 a "master" station has its IP address and a "master" ID number. It communicates with one or more "outstation" nodes with their own IP addresses and "outstation" ID number. A master may poll or it may allow the outstation to push data asynchronously. Messages can be categorized as either "points" (indexed data values of a small number of scalar types for integers and floating point values) or automation. Automation or "control relay output block" (CROB) messages can identify a function in a relay by point (index) and then provide a command to operate a relay. There are a small number of variations on relay commands depending on whether the device uses "pulse" or "latch" commands and whether or not the relay should perform a communications check with the relay before attempting the command (the "select before operate" mode.)

We discovered that the "arpspoof" command which is used for performing man-in-the-middle (MITM) attacks against servers and web users also works quite well for making a master accept an attack computer as its outstation, and also for making an outstation accept an attack computer as its master.

We also discovered that it was practical to construct our relay hijacking software using the "masterdemo" program that comes with the OpenDNP3 distribution. Mr. Crain helped on a couple of occasions by diagnosing some of our program bugs and also by adding a key feature – the ability to specify the source IP address – to the OpenDNP3 code on short notice so we could complete our work before the live demo in Florida.

Wireshark (or the command line version "tshark") readily shows the CROB values at the time that a relay is operated. If an intruder does not observe any relay commands then he or she is reduced to simply trying combinations of DNP3 CROB commands until part of a town's power goes out. This is not really a big problem as most of the time the outstation ID numbers start at 0, point codes start at 0, and there are less than 10 possible CROB values to try. We hypothesized that an intruder would either wait for CROB commands, or that an intruder would already know the CROB commands, or that an intruder would just do a "Brute Force" assault and try them all.

None of the systems involved (ABB MicroSCADA, SubNet Software, nor the protection relays) reported any errors when we broke communications to the relays and started controlling them. MicroSCADA reported "stale" communications. SubNet Software reported no errors when it eventually started communicating with it after the attack. Most but not all of the devices were configured to accept communication from a provisioned master station (by IP address.) None of them complained about the interruption in communications.

5.3 Security Policy Design

We showed that it was indeed straight forward to hijack and control DNP3 relays using readily available hardware and open source software. Once physical security and switch port protections were breached none of the control systems nor relay software could detect the attack or would report on what happened. A tiny attack computer could lie in wait for weeks or even years watching for a legitimate DNP3 CROB command or could come equipped with a WiFi or cellular radio and be controlled externally, perhaps as part of a geographically dispersed yet coordinated effort.

Suricata could readily monitor both the legitimate and spoofed relay commands and provide an extra layer of security. We noticed that during configuration of the system we would accidentally send bad CROB commands until MicroSCADA and each individual relay were set up. Bad CROB messages are indicated when the master or outstation IDs are wrong, or the point/index is wrong, or the wrong relay command is encoded in the CROB. These same messages could occur when an intruder is trying commands speculatively. We decided to flag bad relay commands as a warning and show a yellow security status indicator in MicroSCADA.

An insider might know the right CROB settings and simply trip all the relays. We decided the security policy needed to track the current state of the relays by watching CROB commands and report an error if all four were to be tripped. While it is certainly possible that a utility would intentionally cause a blackout on all distribution lines leaving a substation it is highly unlikely. This is also indicated by a yellow security status indicator in MicroSCADA.

(Shortly after our live demo at the 10th Annual ICS summit we came up with the notion of correlating operations that we can detect with work and maintenance schedules as a policy input. This was explored in more depth in the Southern California Edison scenario.)

If both conditions (bad CROB commands and all the relays become tripped) are true then we deemed the system to be fully compromised and used a red security status indicator in MicroSCADA. This allowed us to experiment with the notion of a security policy that could track the severity and progress of a cyber intrusion. This security policy resembles a simple AND gate although in reality the tree was implemented as a Bayes' rule graph:

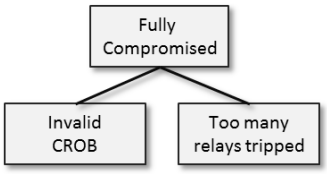

Figure 10: Substation Attack Tree "AND" Gate Model

What we did not do in this scenario was to provide a mechanism for the operator to make one or more of the following sorts of declarations and have it be acknowledged and used by the policy system:

- Bad CROB messages are OK at this time because we are re-configuring, adding or removing some relays.
- It is OK that all the relays are tripped.
- Even though only a few relays are tripped please behave as if too many have been.

- Declare the substation to be fully compromised.
- Reset all the states to "OK" (or, set the confidence level that any of these attack goals have been attained to 0.)

We were able to re-visit this concept later during the Duke Energy microgrid scenario, described below.

Autonomous actions in this scenario are problematic. None of the anomalies detected were by themselves proof of a cyber intrusion. Even if they were conclusive indications, operating the relays automatically remains out of the question for safety reasons.

We were convinced of the value of providing a visual indicator of the security posture of the system in the same screen that the operator uses on a daily basis. This meant that the security operations software only needed to be looked at carefully when there were indications of trouble.

Security policies also help to overcome alarm fatigue on the security operations side. When the security policy issues an alarm ("relay scan detected" or "improper tripping of all relays") then the security operations staff know they have a specific issue to look at which stands out from the daily chatter of certificates expiring or missing heartbeats from protected computers.

As mentioned above, "policyd" component has a message bus integration layer. Messages may enter the bus via a variety of network protocols, get filtered and transformed, handed to the policy layer for interpretation by both Python and the Bayesian subsystem, may be processed again by Python scripts and finally might get passed on to the TNP central operations server as TNP alerts. In this demo:

- Relay events enter policyd as syslog messages over TCP/IP.
- Events are filtered and interpreted so we could track the open/closed state of relays.
- Events were filtered so we could detect commands that were not whitelisted.
- Custom scripts in Python allowed us to interact with the ABB MicroSCADA display.
- Output events could be transmitted to the TNP "central" console and thus visible to the operations center staff.

This security policy is expressed in a JSON-based security policy language designed as part of the CAPMS project. A security policy ties together connections to outside systems, internal message flows, dispatching to the Bayesian statistics engine, generating alarms and alerts, and allows for custom actions expressed as Python code.

5.4 Substation Demonstration Results

This demo showed us that we could build a security solution that integrated a number of very different subsystems and that we could do this quickly and cost-effectively. A layered security system that also required a long integration phase would be too expensive to build and would never get updated. It would be too brittle and too narrowly focused to be useful in a production setting. While not strictly a security feature, the integration features of CAPMS make it practical for use in real-world situations.

The demonstration at the 10th Annual ICS Security Summit demonstrated the value of the basic system architecture. We next turned our attention to Duke's work around promoting the use of distributed computing and message bus architectures as a way to build resilient intelligent systems.

6 Microgrid Attack Scenario - Duke Energy

Duke has been promoting a distributed computing model since 2007, starting originally with the "comm node" radio and their "Coalition of the Willing" (CoW) programs to promote interoperability between different vendor's grid devices. Duke Energy's goals include trying to eliminate vendor lock-in and the inconvenience of multiple "management siloes" in the operations center. Duke also published a hardware specification titled "Distributed Intelligence Platform (DIP)" which has since been passed to the Industrial Internet Consortium to be used as a way to unify gateway and controller platforms.

Duke Energy's Emerging Technology Office passed along its work to define interoperable messaging to the Smart Grid Interoperability Panel (SGIP) Open Field Message Bus (or OpenFMB) standard. In such a model, vendor products interoperate by publishing and subscribing to standardized messages using a topic-based message bus. The OpenFMB project chose to demonstrate an integrated solar and storage microgrid at the group's annual meeting in November 2015. A central player in the demo is Green Energy whose software was used to simulate solar and battery inverters as well as a microgrid load.

6.1 Simulation Design

The CAPMS team at Duke Energy decided to align itself with the OpenFMB approach in advance of the OpenFMB demo taking place in November 2015. We chose to simulate a microgrid for our second security demonstration. We recruited Green Energy to help us build a new demonstration rack using their AMQP-based Green Bus system and intelligent controllers chosen by Duke Energy that were representative of Duke's OpenFMB plans described in more detail, below.

We joined the GreenBus AMQP bus with the CAPMS bus using a small GreenBus to CAPMS gateway program. This provided CAPMS with the entire range of energy system events. The longer term plan is to switch the scenario to the Object Management Group (OMB) Data Distribution Service (DDS) which is the standard chosen for the first OpenFMB demo. We anticipate that we will have this environment available for us in the Mt. Holly facility and that we can keep this working moving ahead as part of Duke Energy's work on the OpenFMB standard.

The value of a message bus is to simplify the task of integrating events from multiple sources: cyber, energy system and physical. A significant software feature of CAPMS is a flow-based message bus integration layer based on "enterprise integration patterns" (EIP.) Along with the goal of testing, the usefulness of combining events from many sources is the goal of testing our ability to integrate these sources quickly and in a manner that is cost effective.

Figure 11 shows our simulation network. A second simulated WAN link (Ethernet) connects the operations center with a new subnet for the distributed microgrid network (VLAN-50) to create a realistic network broadcast domain.

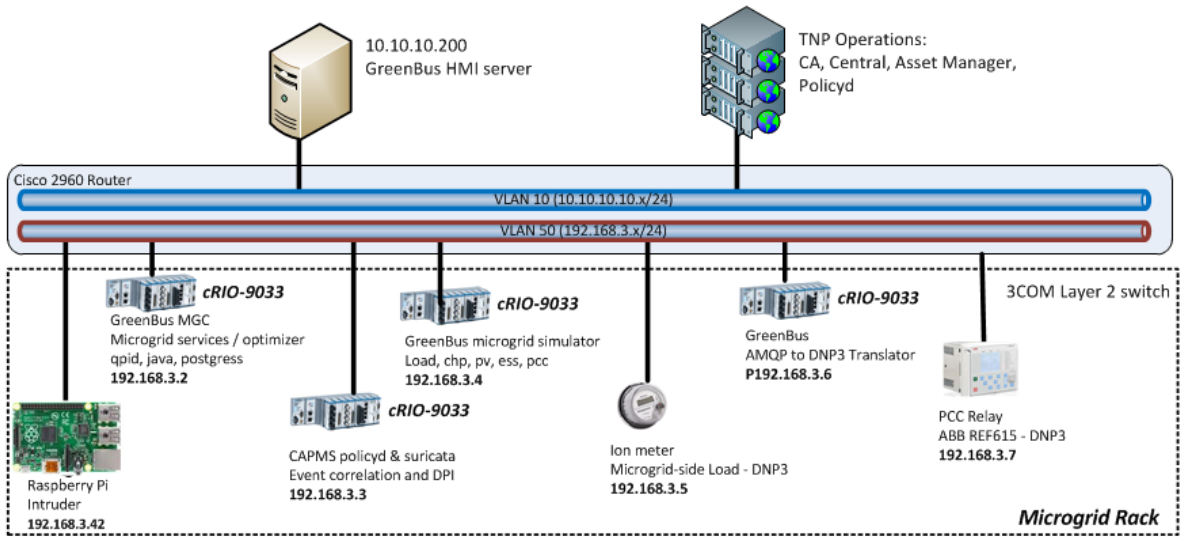

Figure 11: Microgrid Network

The control servers were mounted on a rack similar to the substation rack. The microgrid rack was populated with:

- A National Instruments cRIO-9033 running the ViaSat CAPMS "policyd" event correlation engine as well as the suricata DPI component. This CAPMS software performs local event correlation and models cyber intrusions against the microgrid. This "agent" can share events with "policyd" running in the operations center.
- A National Instruments cRIO-9033 running the Greenbus microgrid simulation. This includes both static and variable loads including optional loads that may be started or shed as needed. It also carries sample controllers for CHP (combined heat and power), PV (photovoltaic), ESS (energy storage system) and the PCC (point of common coupling.)
- A National Instruments cRIO-9033 running the MGC (Microgrid Controller) application. This controls charging/discharging mode of the battery, control of the CHP and PV, and control of the PCC in order to sell electricity to the grid when required to or not, to charge or discharge the battery, to collect data from various meters, and to operate the PCC.
- A National Instruments cRIO-9033 running the GreenBus AMQP to DNP3 gateway. This device assumes the role of the DNP3 master station in this network.
- ABB REF 615 protection relay controller controlled by the PCC node. This will have an LED red/green light similar to the indicator lamps used for the substation simulation.
- A Raspberry Pi attack computer that will be able to hijack the REF 615 relay, and which will be detectable by the CAPMS suricata component on the first cRIO-9033 device listed above.

Figure 12 shows the test rack with the four cRIO-9033s, the ABB REF 615 PCC with indicator lamp, and the ION meter. The monitor, keyboard and mouse on the right is connected to the RT-Linux desktop of the MGC.

The GreenBus HMI server (running at 10.10.10.200) provides a web browser interface to the MGC application. Through this interface an operator can see the predicted and actual load values, the schedule for solar charging, ESS charging and discharging, and microgrid load values. The operator can also visualize how the microgrid maximizes revenue by trying to use electricity from the grid when it is both cheapest and required, and to sell power to the grid when the price is best and extra power is available. The HMI can also monitors and controls the DNP3 devices including the PCC and the ION meter.

Figure 12: Microgrid Rack

GreenBus uses the AMQP network protocol to distribute events on its own event bus to all of its distributed components. In our network, there are two AMQP gateways.

1. GreenBus has a DNP3 gateway in which a software component assumes the role of DNP3 master station and interacts with the PCC and ION meter.
2. CAPMS has an AMQP to TCP/IP gateway using one of the CAPMS-provided integration components. This is an Apache "tomcat" server running a Java web application ("gateway.war"). A security control panel was added to this as a convenient way to visualize the progress of an attack and to control the demonstration.

Figure 13 shows the logic data flows for the system and explains the protocols used.

- The green arrows indicate the Green Bus protocol implemented as Google Protobuf (https://developers.google.com/protocol-buffers/?hl=en) payloads running over AMQP.
- The orange arrows indicate DNP3 between Green Bus components and the meter, and the PCC relay. This traffic may be sniffed by Suricata and may also be hijacked by the Raspberry Pi attack computer.
- Suricata and policyd (the distributed event correlation component built as part of the CAPMS program) communicate over syslog, entirely inside the CAPMS cRIO-9033.
- CAPMS components communicate using a well-known ZeroMQ (http://zeromq.org/) protocol. This covers command, control, status, and the installation of security policies.)

The operator will be able to manage and observe the state of the microgrid using a combination of the TNP "central" and "asset manager" consoles, and through the Green Energy MMC browser-based user interface.

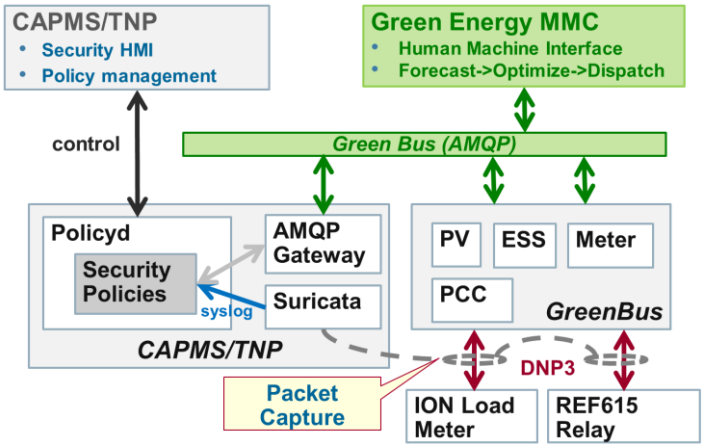

Figure 13: Microgrid Communication Protocols

6.2 Threat Analysis

DNP3 is used for reporting meter values and for operation the point of common coupling (PCC) relay. The ION meter is on the microgrid side of the PCC and the voltage tracks the load seen on the internal distribution lines. Spoofing those voltage readings could affect the microgrid differently depending on whether the microgrid was islanded or not and in extreme cases, a misreading of the load on the microgrid distribution lines could result in overheating or even damage to inverters. Unauthorized control of the PCC could result in the inability to sell power to the grid, the inability to charge the battery when power was cheapest, or equipment damage should the PCC re-connect before phase synchronization was ready.

During the building of the microgrid demonstration we had meetings with different Duke Energy constituents including people responsible for the physical security of remote energy assets. We talked about perimeter alarms, inputs from video systems, and work with gunshot detection. While we don't actually have instances of those systems available in Mt. Holly and we chose to simulate them by injecting events directly into policyd and then interpreting those events as part of a combined physical and cyber attack. These events originate in the Security HMI (built into the CAPMS AMQP gateway, as described above.)

Standardized bus messages simplify the task of writing malware. Each framework or standard is accompanied by tutorials, documentation and sample code. Malware or an insider with credentials would not need to use vulnerabilities around the edges of a single network. They could cut to the center of the most damaging vulnerabilities and create malware that would apply to a great many locations and even work across different utilities with varying networks and control systems. That said, standardized bus messages open the door for a system such as CAPMS that needs to observe what goes on in the network, and will try to interpret events in the context of its own model of what is good or bad. These observations apply for both AMQP (what the demo used) and for DDS (what we anticipate using after the project ends.)

Standards-compliant malware could send legal control and provisioning commands, which might not trigger a whitelist rule filter as we explored in the substation demo. Out-of-band changes such as mis-configuring devices could also pass unnoticed. Therefore we considered another sort of higher-level event detection such that we would layer a new state model of the energy system on top of what was already provided by the Green Energy. This model would watch for unexpected energy readings for voltage, phase, current, inverter modes, and so on. Even better would be situations where values between systems (the battery inverter and the load meter) could be compared. These would never be provided by the

individual vendors but instead could only arise during the integration and testing of the actual system in the field.

6.3 Security Policy Design

We composed a threat scenario based on fusing events from DNP3 monitoring, physical security, and GreenBus events. We invented a "warning" such that a warning represents a case where a particular *category* of attack was detected. Thus a flurry of DNP3 index or control point scans would be a single "warning" as would perimeter alarms, or attempts to confuse the energy management system. In term of a Bayes' Rule model, a warning would represent a "leaf" goal that would be achieved but once. This has the effect that the system can filter unwanted raw events.

We defined escalations based on the number of warnings (attack categories) and detecting when the number of warnings exceeded different thresholds. We named these "normal", "warning", "alert" and "attack" as shown in this simplified tree diagram:

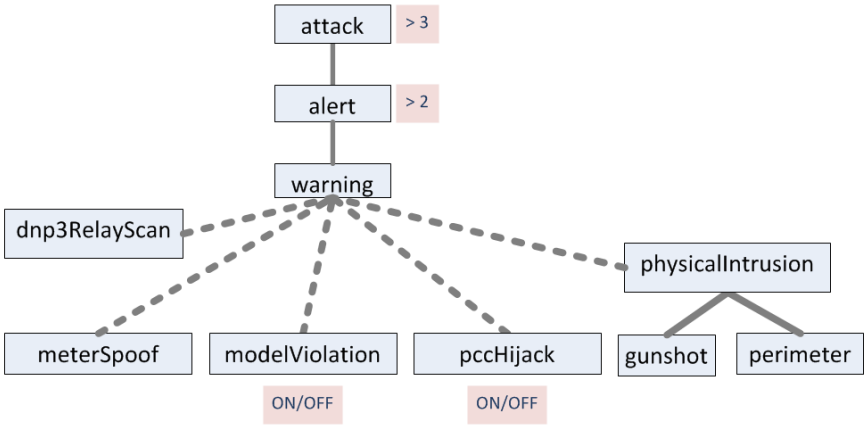

Figure 14: Attack-Defense Tree for Microgrid

We also wanted to showcase the difference between "OR" logic and "AND." The former shows how any sort of "leaf" node represents a warning. The latter is represented by "physicalIntrusion." Neither a nearby hunter nor a technician accidentally tripping a motion detector ought to register as a security warning. A case where someone appears to have shot a lock off and entered the grounds should.

6.4 Message Flow Design

The substation demonstration used a fairly simple data flow model. In the time between the substation and microgrid demonstrations the CAPMS team largely completed the first version of our integration layer of "policyd" and could use it in full. Figure 15 is a graphical representation of the flow model used in this demonstration.

Suricata events are filtered and processed by a Python module that detects improper DNP3 commands and can also track the open/close state of the PCC. Depending on what it finds, it can optionally tag an event with a "goal_id" and send it into the Bayesian attack-defense tree engine. The policy component can also optionally publish events to the alarm queue.

Events from the GreenBus queue are passed to a series of "router" components which determine how to they ought to be dispatched. For our scenarios we can treat these as physical alarms or energy system events. In the case of "MicrogridSecurityPolicy" the script represents a simple model of the energy system code which can optionally tag the event with a "goal_id" for use by the Bayesian rule engine. Note that is up to the attack-defense tree to perform the "AND" of gunshot and perimeter events.

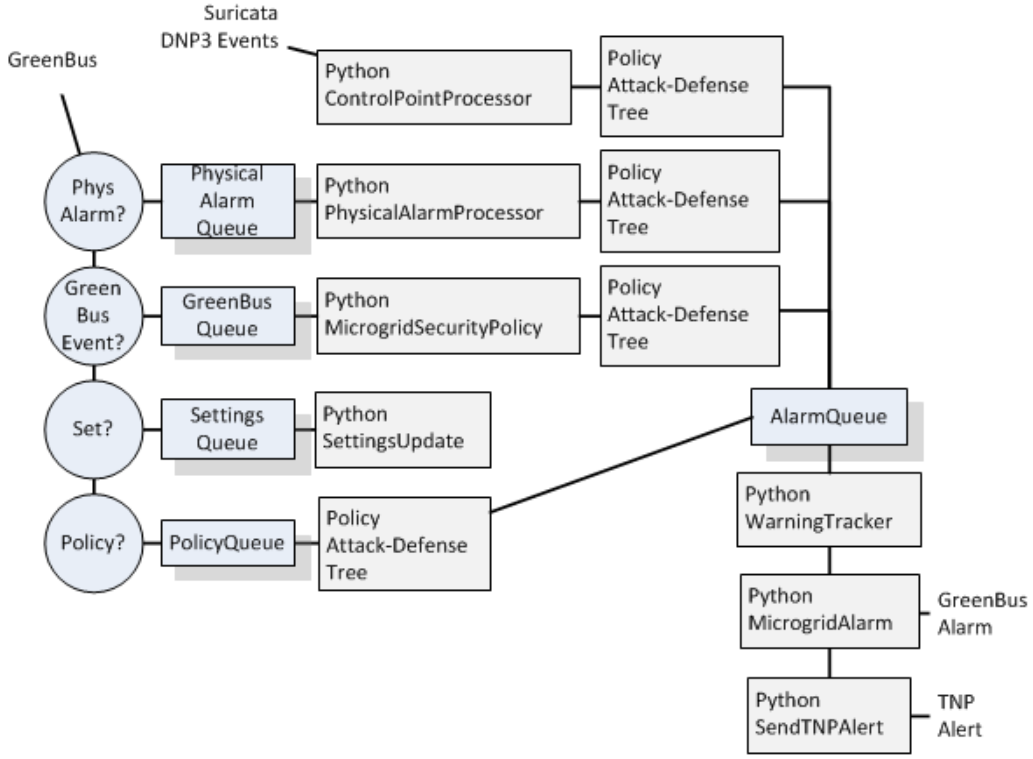

Figure 15: Microgrid Flow Model

Events can be tagged in various ways by Python scripts or by scripts in the Bayesian attack-defense tree engine. An event tagged as a "warning" can determine whether or not to escalate the severity level of the intrusion. Events tagged as "alarms" will show up ultimately in both the TNP console as well as the Green Energy alarm display.

The "settings" and "policy" flows at the bottom left are used to control the demonstration. The "settings" queue allows for re-setting the attack severity to "normal" and for optionally enabling or disabling certain security policies (more on this later.) The "PolicyQueue" flow allows for setting the confidence level of any goal in the attack-defense tree to a new value. This helps not just for testing and debugging the security policy, but also during operation as a way of adjusting the state of the attack or to perform a reset of the entire model.

6.5 Control Panel

As mentioned above, the AMQP gateway provided us with the opportunity to introduce a new user interface component to the microgrid operations center. We first used it to inject gunshot and perimeter events. We next added the ability to show at a glance the severity level of the intrusion (normal, warning, alert, attack) as well as the most recent triggering events. The "reset" button, originally conceived of as a convenience for testing and running the demo seemed to be of immediate value to an operator who was interacting with the system. The security policy was designed to interpret system events in the most pessimistic way possible. False positives were the norm and not the exception. Someone installing new equipment (maybe not white-listed yet) during hunting season could set our scenario into the highest "attack" level quite easily. There needed to be a way for the operator to quickly and easily quiet CAPMS down with a simple "reset" feature.

Other possible areas for false positives in our scenario are checking for opening or closing the PCC and for the energy model policy itself. Inside a valid maintenance window it might or might not be legitimate to trip the relay protecting access to the grid. In our demonstration scenario we found that the voltage value we were checking could go out of range but was not necessarily evidence of a cyber attack. We added controls to the control panel display to turn these on and off (and added the logic for these to the data flow logic and Python scripts as well.) Figure 16 shows the final control panel screen.

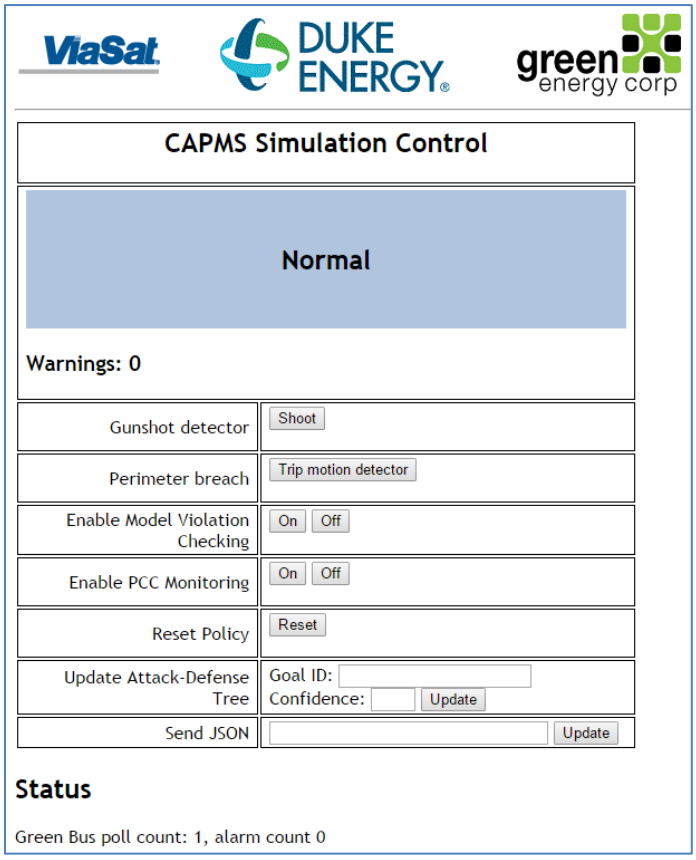

Figure 16: Microgrid Security Control Panel

Figure 17 shows the difference between the control panel and the TNP alarm window. The control panel provides much more useful information: the severity of the situation, the number of warnings that lead to the interpretation of the severity, and a message showing the system's current understanding of the attack. In the example shown, "ADT" means that a major attack goal has been achieved by the intruder as modeled by the attack-defense tree. If CAPMS had a way to display the Bayesian tree model then this would be a good place for it (A proposed feature for future implementations).

Figure 17: Microgrid Control Panel Alongside TNP Alert

6.6 Microgrid Demonstration Results

Our event monitoring system succeeded in tracking cyber, physical and energy system events and interpreting those events according to a model of attack severity. We had the opportunity to validate the viability of our enterprise integration pattern layer by combining events from a variety of systems in a very short time span even without the help of graphical development tools.

The natural emphasis on detecting problems seems to also lead to a system which is prone to false positives. The operator always knows far more about what is happing than can be determined from just the network traffic. We found that the user interface for the operator needs to provide the following features:

- A way to show the operator at a glance what the security system thinks might be going on.
- The ability to adjust the current security posture based on real-world observations.
- Techniques to adjust the sensitivity of the monitoring system in ways that can be understood by the operator in terms of the energy systems he or she operates.

For demonstration purposes our energy system model was very simple. We can foresee building a library of re-usable energy models that could be rapidly integrated into CAPMS-like security systems in the future.

7 Conclusion

We learned that to be successful CAPMS would have to capture data from as many sources as possible and as quickly and easily as possible. Although there are many similarities across electric utilities, each utility has its own unique network design, as well as organizational structure. This drove the design to come up with a system which could separate the problem of event collection from the problem of modeling and tracking cyber intrusions.

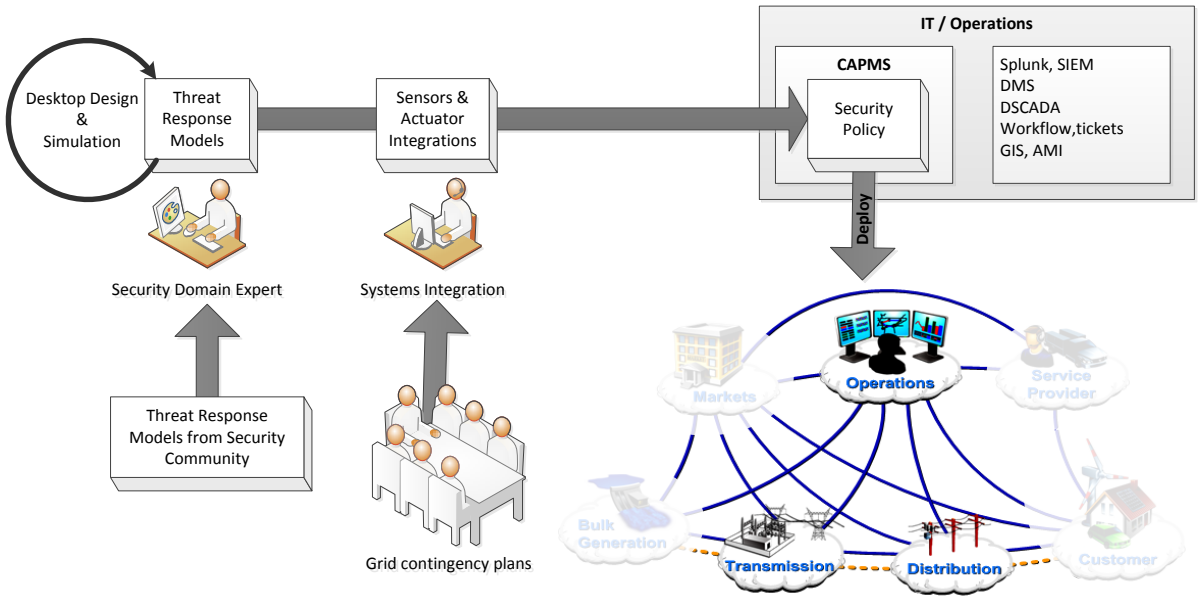

Figure 18: Policy Design and Deployment Flow Diagram

Much of the existing work done on modeling cyber intrusions is focused on risk assessment. Risk assessment considers mitigation costs and attack consequences so as to provide a rational framework for budgeting against potential attacks. While risk assessment helps explain the consequences of an attacker's actions it is of little help for describing all of the steps and stages an intruder would take, particularly when the attacker has a zero-day capability or is an insider such as a negligent or disgruntled employee.

The CAPMS program settled on a hybrid approach that combines Bayesian statistics and Python scripting. With this approach we found we could:

- Model situations where a number of possible attacks might be underway to some extent
- Interpret the severity of an attack by tracking the "goals" that an attacker has "achieved"
- Explain an attack in terms of the energy systems as it is understood and run by an operator

The CAPMS program took it as a given that the TNP software would be protecting the network from cyber intrusions outside the scope of industrial control systems and their protocols. For example, TNP can block communications according to a whitelist of hosts and ports, configure firewalls, detect host intrusions, detect network intrusions and denial of service attacks, and so on. From working with Duke and SCE we learned that:

- Legacy protocols are notoriously insecure. Inspired (and helped) by people such as Crain and Sistrunk we were able to both hijack DNP3 control messages and detect when it happened.
- Standard control protocols even when found to be both correctly used and secure might originate from an insider with functional credentials. All of these protocols/services (61850, web services,

SGIP OpenFMB) provide what are essentially how-to cookbooks for hackers in the form of software development documentation and example code.

- Operations software as supplied by the various manufacturers might handle some failure cases but none of it notices when an outsider is intentionally misconfiguring or operating it incorrectly. These systems pay no attention whatsoever to the other systems around them.
- Once the raw events that indicate an attack is detected, it isn't enough to simply pass them along to a log file. They need to be interpreted, their meaning extracted, and advice for what to do computed in near real-time. This information needs to be delivered to the right user in the right form that helps increase the operator's situational awareness relative to their particular system.

Our vision for the next area of research is on the policy layer execution and policy creation. CAPMS will benefit from tighter interaction with an operator who can indicate which situations are likely to be false alarms, which situations are more serious than the system can detect, and when to enable or disable key policies as an attack unfolds.

7.1 Products Developed

There were other products created as part of the work performed by the DOE funded CAPMS grant. These were in addition to expanding the capabilities of ViaSat's Trusted Network Platform. These include:

- Live demonstrations beyond the DOE demonstrations
- Technical papers
- Presentations of this effort at national conferences

Below is a complete list of the technology transfer items produced by ViaSat, Duke Energy and Southern California Edison as a result of the DOE grant.

Table 2 - CAPMS Technology Transfer Products

Work Product/Technology Transfer	References
2015 SAN ICS Security Summit Live Attack demonstration	Video of live presentation available on-line. https://youtu.be/stkCYuUX3EM
Two IEEE papers accepted for presentation entitled "Real-time Situational Awareness for Critical Infrastructure Protection" "Secure Interoperability with Commercial Open Standards"	Both papers presented and published for IEEE at the IEEE SmartGridComm conference in Orlando FL on Nov 3-4, 2015
DistribuTECH presentation based on CAPMS project entitled "How to Detect and Respond to Substation/Microgrid Hacks"	To be Presented by Duke Energy and ViaSat Inc. Track: Defending the Grid Session: New Concepts in Utility Security Date: 2/11/2016 Time: 10:30AM-12:00PM
CAPMS Demonstrations at DistribuTECH 2016	ViaSat will be hosting CAPMS demonstrations at the DOE booth
Abstract for CAPMS presentation submitted to RSA Data Security Conference 2016	Results to be announced Nov 2016
CAPMS was a Finalists for Fierce Innovation Awards: Energy Edition	Utility-reviewed awards program from the publishers of FierceEnergy and Smart Grid News. ViaSat was recognized as a finalist in the Technologies/Cybersecurity category. http://investors.viasat.com/releaseDetail.cfm?ReleaseID=939733

Work Product/Technology Transfer	References
Participation at Smart Grid Interoperability Panel (SGIP) Open Field Message Bus (Open FMB) standards and demonstrations events	Results of the CAPMS effort will be providing security and automated responses to Open FMB demonstrations. http://sgip.org/
Cybersecurity Benefits of a Distributed Interoperable Smart Grid presentation at EUCI conference in Scottsdale Az.	Co-presented by Duke Energy and ViaSat Inc.- Nov 2014